Cengage

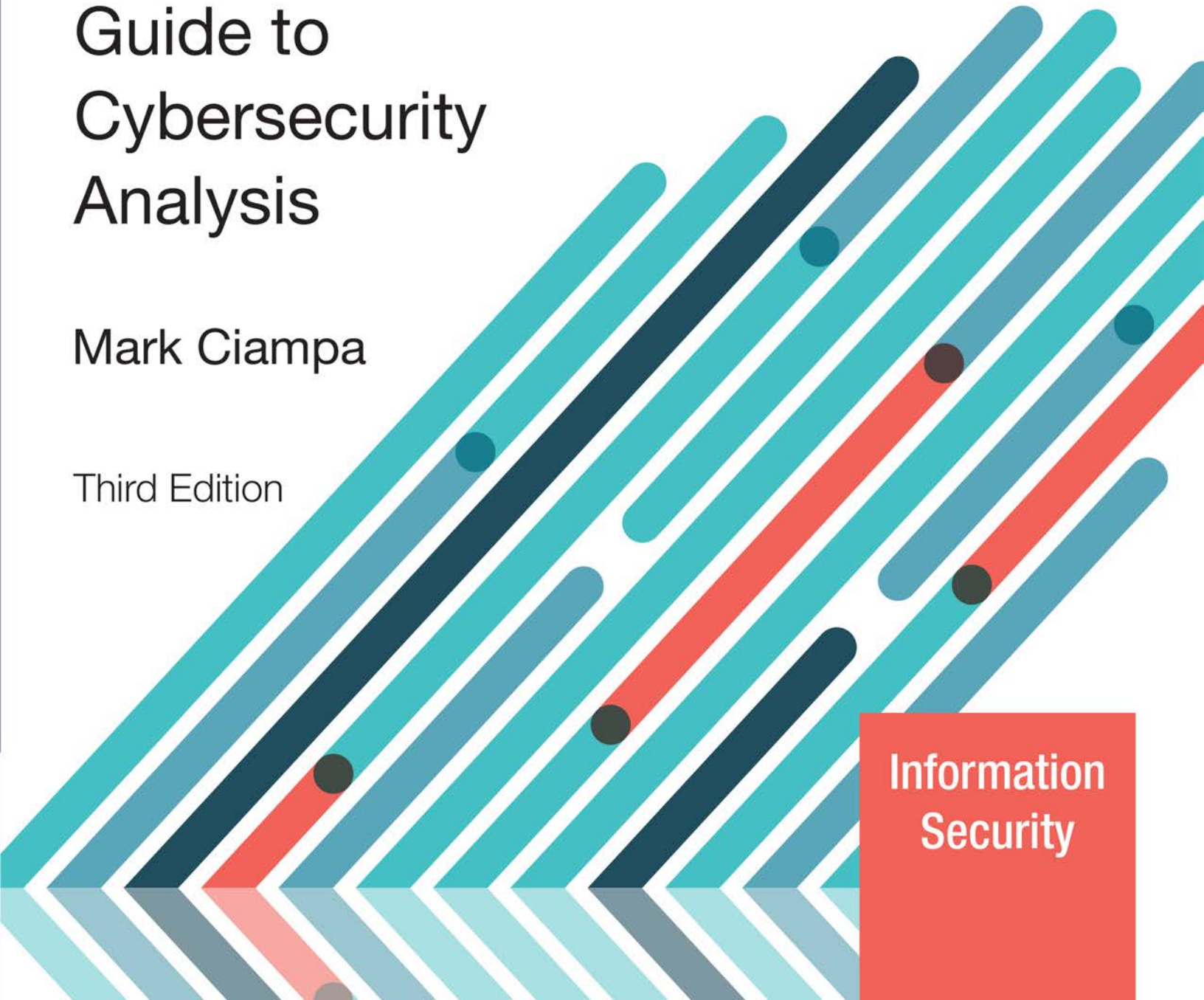
CompTIA

CompTIA® CySA+

Guide to Cybersecurity Analysis

Mark Ciampa

Third Edition



Information Security

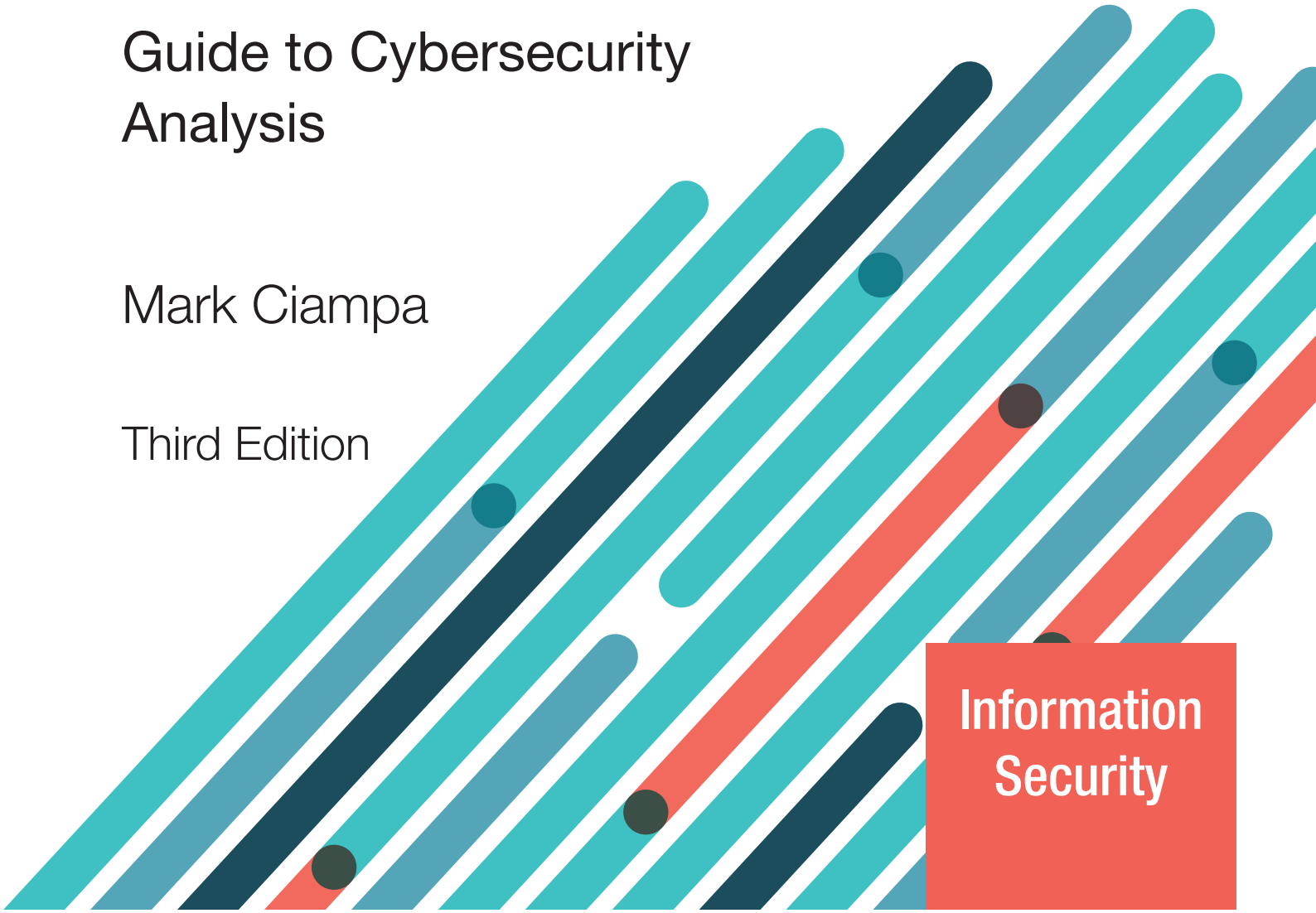
CompTIA®

CompTIA® CySA+

Guide to Cybersecurity Analysis

Mark Ciampa

Third Edition



Cengage

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Important Notice: Media content referenced within the product description or the product text may not be available in the eBook version.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Cengage

***CompTIA CySA+ Guide to Cybersecurity Analysis*, Third Edition**
Mark Ciampa

SVP, Product Management: Cheryl Costantini

VP, Product Management: Mark Santee

Portfolio Product Director: Rita Lombard

Portfolio Product Manager: Natalie Onderdonk

Product Assistant: Anh Nguyen

Learning Designer: Carolyn Mako

Senior Content Manager: Brooke Greenhouse

Digital Project Manager: Jim Vaughey

Technical Editor: Danielle Shaw

Developmental Editor: Lisa Ruffolo

Senior Director, Product and Platform Marketing: Charlotte McLaren

Senior Manager, Product Marketing: Neena Bali

Senior Product Marketing Managers: Cybèle Beckham

Content Acquisition Analyst: Callum Panno

Production Service: Straive

Senior Designer: Erin Griffin

Cover Image Source: sollia/Shutterstock.com

Copyright © 2025 Cengage Learning, Inc. ALL RIGHTS RESERVED.

Unless otherwise noted, all content is Copyright © Cengage Learning, Inc.

WCN: 02-300-527

No part of this work covered by the copyright herein may be reproduced or distributed in any form or by any means, except as permitted by U.S. copyright law, without the prior written permission of the copyright owner.

Microsoft is a registered trademark of Microsoft Corporation in the U.S. and/or other countries.

The names of all products mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners. Cengage Learning disclaims any affiliation, association, connection with, sponsorship, or endorsement by such owners.

Previous edition(s): ©2022, ©2021

For product information and technology assistance, contact us at
Cengage Customer & Sales Support, 1-800-354-9706
or support.cengage.com.

For permission to use material from this text or product, submit all requests online at **www.copyright.com**.

Library of Congress Control Number: 2024936071

ISBN: 979-8-214-01147-9
Looseleaf ISBN: 979-8-214-01148-6

Cengage
5191 Natorp Boulevard
Mason, OH 45040
USA

Cengage is a leading provider of customized learning solutions. Our employees reside in nearly 40 different countries and serve digital learners in 165 countries around the world. Find your local representative at: **www.cengage.com.**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com**.

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2024

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Brief Contents

Preface viii

Part 1
Cybersecurity Foundations 1

Chapter 1
Technology Underpinnings 3

Chapter 2
Threat Actors and Their Threats 33

Chapter 3
Cybersecurity Substrata 61

Part 2
Security Operations 87

Chapter 4
Identifying Indicators of Attack (IOA) 89

Chapter 5
Analyzing Indicators of Compromise (IOC) 115

Chapter 6
Threat Detection and Process Improvement 149

Part 3
Vulnerability Assessment and Management 177

Chapter 7
Vulnerability Scanning and Assessment Tools 179

Chapter 8
Addressing Vulnerabilities 211

Chapter 9
Vulnerability Management and Administration 237

Part 4
Incident Response Management 265

Chapter 10
Incident Response Planning 267

Chapter 11
Incident Response Activity Phases 293

Chapter 12
Data Protection and Utilization 321

Appendices

Appendix A
Preparing for the CompTIA CySA+ CS0-003 Certification Exam 347

Appendix B
CompTIA CySA+ CS0-003 Certification Exam Objectives 362

Glossary 373

Index 383

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Contents

Preface viii

Part 1

Cybersecurity Foundations 1

Chapter 1

Technology Underpinnings 3

Infrastructures and Architectures 5
- Infrastructure Concepts 5
- Network Architectures 9
- Operational Technology 15

Software 17
- Operating System Fundamentals 17
- Coding 22

Chapter 2

Threat Actors and Their Threats 33

Who Are the Threat Actors? 35
- Script Kiddies 36
- Organized Crime 37
- Insider Threat 37
- Hacktivists 38
- Nation-State Actors 39
- Other Threat Actors 40

Threat Actor Actions 41
- Tactics, Techniques, and Procedures (TTP) 41
- Known and Unknown Threats 42

Types of Attacks 44
- Web Server Application Attacks 44
- Remote Code Execution (RCE) 47
- Data Poisoning 47
- Obfuscated Links 48

Vulnerabilities 50
- Programming Vulnerabilities 50
- Broken Access Control 52
- Cryptographic Failures 53
- Dated Components 53
- Identification and Authentication Failures 53

Chapter 3

Cybersecurity Substrata 61

Identity and Access Management (IAM) 63
- Identity 63
- Access 70

Encryption 72
- Public Key Infrastructure (PKI) 73
- Secure Sockets Layer (SSL) Inspection 73

Secure Coding 74
- Secure Software Development Life Cycle (SDLC) 74
- Secure Coding Best Practices 75

Networking 77
- Zero Trust 77
- Secure Access Service Edge (SASE) 79

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Part 2

Security Operations 87

Chapter 4

Identifying Indicators of Attack (IOA) 89

Cybersecurity Indicators 91
- Indicators of Attack (IOA) 91
- Indicators of Compromise (IOC) 92

Network IOA 93
- Abnormal Network Traffic 93
- Stealth Transmissions 97
- Scans/Sweeps 100
- Rogue Network Devices 100

Endpoint IOA 101
- High-Volume Consumption of Resources 102
- Operating System Evidence 104
- Software-Related Evidence 105
- Data Exfiltration 106

Application IOA 106
- Unusual Activity 106
- New Account Creation 106
- Unexpected Outbound Communication 107
- Modified Application Log 107

Chapter 5

Analyzing Indicators of Compromise (IOC) 115

Common Techniques for Investigating IOC 117
- Diagnose Malware 117
- Analyze Email 121
- User Behavior Analysis (UBA) 125

Tools for IOC Analysis 127
- File Analysis Tools 127
- Tools for Analyzing Network IOC 131
- Flow Analysis 133
- Reputation Tools 134
- Log Correlation and Analysis Tools 136

Chapter 6

Threat Detection and Process Improvement 149

Threat Intelligence 150
- What Is Threat Intelligence (TI)? 150
- Threat Intelligence versus Threat Data 151
- The Intelligence Cycle 152
- Threat Intelligence Sources 153
- Confidence Levels 156

Threat Hunting 158
- What Is Threat Hunting? 158
- Hunters and Hunting 158
- Threat-Hunting Methodologies 160
- Steps in Threat Hunting 162

Improving Security Operation Processes 163
- Standardize Processes 163
- Streamline Operations 164
- Tool Automation and Integration 167

Part 3

Vulnerability Assessment and Management 177

Chapter 7

Vulnerability Scanning and Assessment Tools 179

Vulnerability Scanning Concepts 180
- What Is a Vulnerability Scan? 181
- Industry Frameworks 183

Vulnerability Scanning Methodologies 185
- Scanning Decisions 185
- Running a Vulnerability Scan 190

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Vulnerability Assessment Tools 193
Infrastructure 194
Networks 197
Software 200

Chapter 8

Addressing Vulnerabilities 211

Analyzing Vulnerability Scans 213
Validation 213
Context 213
Other Factors 214
Prioritizing Vulnerabilities 215
Reasons for Prioritizing and Escalating 216
Using the Common Vulnerability Scoring System (CVSS) 217
Managing Vulnerabilities 220
Using Controls 220
Patch Management 221
Configuration Management 223
Attack Surface Management (ASM) 224
Threat Modeling 225
Governance 228
Advanced Vulnerability Scanning 229

Chapter 9

Vulnerability Management and Administration 237

Identifying Vulnerabilities 239
Multipurpose Tools 239
Web Applications 244
Cloud Infrastructure 244
Wireless Networks 246
Responding to Vulnerabilities 247
Implement Action Plans 247
Combat Inhibitors to Remediation 248
Evaluate Metrics and Key Performance Indicators (KPIs) 249
Communicating and Reporting Vulnerabilities 250
Generate Reports 250
Calculate Risk Score 253
Minimize Recurrence 254
Conducting Exercises and Awareness Training 255
Cyberteam Exercises 255
User Awareness Training 256

Part 4

Incident Response Management 265

Chapter 10

Incident Response Planning 267

Charting an Incident Response Plan 269
Defining a Cyber Incident 269
What Is a Cyber Incident Response Plan? 269
Building a Cyber Incident Response Team 270
Testing and Training 271
Using Plans and Frameworks 271
Creating Preparatory Plans 272
Analyze Attack Methodology Frameworks 273
Reviewing Criticality of Data 277
Identifying Stakeholders 279
Internal Stakeholders 279
External Stakeholders 279
Constructing Communication Pathways 282
Reasons for Communications 282
Communications Best Practices 285

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 11

Incident Response Activity Phases 293

Detection and Analysis 295
- Did an Incident Occur? 296
- How Severe is it? 296
- What Is its Priority? 297

Containment 299

Eradication and Recovery 300

Post-Incident Activities 303
- Digital Forensic Analysis 303
- Generate IOC 310
- Update Incident Response Plan 310
- Assess the Cyber Incident 311
- Produce Incident Response Reports 313

Chapter 12

Data Protection and Utilization 321

Perils Against User Data 323
- Types of Data Collection 323
- Concerns Over Data Collection and Usage 323

Controls for Protecting Sensitive Data 325
- Technical Controls 325
- Nontechnical Controls 332

Using Data for Cybersecurity 334
- Data Analytics 335
- Artificial Intelligence (AI) 336

Appendix A

Preparing for the CompTIA CySA+ CS0-003 Certification Exam 347

Knowledge-Based Assessment Questions 347

Performance-Based Questions (PBQs) 350
- Ports 351
- Protocol IDs 353
- Sandboxes 353
- Command-Line/IP Utilities 354
- Packet Analyzers 359

Appendix B

CompTIA CySA+ CS0-003 Certification Exam Objectives 362

Glossary 373

Index 383

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Preface

CompTIA® CySA+ Guide to Cybersecurity Analysis, Third Edition, is intended to meet the needs of learners and professionals who are interested in mastering intermediate-level cybersecurity skills and knowledge. It is designed to prepare security analysts, threat intelligence analysts, and incident response handlers who will leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents as they apply to an organization's data, applications, and digital infrastructure. Although there is no designated prerequisite, *CompTIA® CySA+ Guide to Cybersecurity Analysis* is designed to build on the CompTIA Security+ certification or equivalent experience. Those seeking to pass CompTIA's CySA+ certification exam will find the course's content, approach, and numerous projects and study questions especially helpful. For more information on CompTIA CySA+ certification, visit CompTIA's website at comptia.org.

Intended Audience

This book is designed to meet the needs of students and professionals who want to master advanced-level cybersecurity skills and knowledge. The book is designed to build on the CompTIA Security+ certification or equivalent experience, though no prerequisite is specified. All of the CompTIA CySA+ CS0-003 certification exam objectives are covered in the text (see Appendix B).

The book's pedagogical features are designed to provide a truly interactive learning experience to help prepare you for the challenges of network and computer security. In addition to the information presented in the text, each module includes Review Questions that help prepare you for the certification exam. Each module also contains Case Projects that place you in the role of problem solver, requiring you to apply concepts presented in the chapter to achieve successful solutions.

Chapter Descriptions

The following list summarizes the topics covered in each chapter of this course:

Chapter 1, "Technology Underpinnings," covers the foundational topics that serve as the underpinnings upon which cybersecurity rests. These topics include infrastructures, network architectures, operational technology, and software operating systems and coding.

Chapter 2, "Threat Actors and Their Threats," covers who the threat actors are, the tactics they use, and the types of attacks that they launch against vulnerabilities.

Chapter 3, "Cybersecurity Substrata," looks at foundational topics of cybersecurity. These topics include identity and access management, encryption, secure coding, and networking.

Chapter 4, "Identifying Indicators of Attack (IOA)," explores IOA, which are indicators of a potential upcoming attack. The topics in this chapter are network IOA, endpoint IOA, and application IOA.

Chapter 5, "Analyzing Indicators of Compromise (IOC)," looks at the digital artifacts that serve as evidence of an attack, which can reveal how a completed attack occurred and how defensive deficiencies can be addressed. It covers common techniques for investigating IOC and tools for IOC analysis.

Chapter 6, "Threat Detection and Process Improvement," examines threat intelligence and threat hunting. It also looks at ways to improve security operation processes, including standardizing processes, streamlining operations, and tool and automation integration.

Chapter 7, "Vulnerability Scanning and Assessment Tools," introduces vulnerability scanning concepts and industry frameworks used in vulnerability scanning. It also explores methodologies for vulnerability scanning and different vulnerability assessment tools.

Chapter 8, "Addressing Vulnerabilities," looks at how to analyze vulnerability scans, prioritize vulnerabilities, and manage those vulnerabilities.

Chapter 9, "Vulnerability Management and Administration," examines how to identify vulnerabilities and respond to them. It also explores communicating and reporting vulnerabilities and how to conduct exercises and awareness training.

Chapter 10, "Incident Response Planning," looks at the topic of incident response planning and covers charting an incident response plan, using plans and frameworks, reviewing the criticality of data, and identifying stakeholders along with constructing communication pathways.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 11, "Incident Response Activity Phases," explores the different phases of incident response: detection and analysis, containment, eradication and recovery, and post-incident activities.

Chapter 12, "Data Protection and Utilization," concludes with an examination of the perils against user data and the controls for protecting sensitive data, both technical and nontechnical controls. It also explores ways for using data in cybersecurity through data analytics and artificial intelligence.

Appendix A contains tools for preparing for the CompTIA CySA+ CS0-003 certification exam. It provides knowledge-based assessment questions and performance-based questions that are designed to assess the test taker's skills in working with different cybersecurity tools. Many questions are presented in a scenario format to put the learner in a "you are there" setting when deciding which tools to use, why they should be used, and how to interpret and analyze the results.

Appendix B is a mapping of each CySA+ domain element, the chapter and section in which it is located, and how that material is covered based on Bloom's Taxonomy.

Features

To aid you in fully understanding cybersecurity analysis, this material includes many features designed to enhance your learning experience.

- **Maps to CompTIA objectives.** The material in this text covers all the CompTIA CySA+ CS0-003 exam objectives.
- **Chapter objectives.** Each chapter lists the concepts to be mastered within that chapter. This list serves as a quick reference to the chapter's contents and a useful study aid.
- **#TrendingCyber.** Each chapter opens with the details and explanation of a recent real-world cybersecurity event. This feature provides a real-world context for applying cybersecurity principles.
- **Figures and tables.** Numerous full-color diagrams illustrating abstract ideas and screenshots of cybersecurity tools help learners better visualize the concepts of cybersecurity, and tables provide details and comparisons that can be easily reviewed and referenced in the future.
- **Notes.** Each chapter's content is supplemented with Note features that provide additional insight and understanding.
- **Cautions.** The Caution features warn you about potential mistakes or problems and explain how to avoid them.
- **Two Rights & A Wrong.** Each section of every chapter includes a series of questions that can serve as a quick self-assessment of the material. This helps to ensure a complete understanding of the material.
- **Chapter summaries.** Each chapter reading concludes with a summary of the concepts introduced in that chapter. These summaries revisit the ideas covered in each chapter.
- **Key terms.** Following the chapter summary, all terms introduced in the chapter are gathered together in the Key Terms list. This list encourages a more thorough understanding of the chapter's key concepts and is a useful reference.
- **Review Questions.** The end-of-chapter assessment begins with a set of review questions that reinforce the main concepts in each chapter. These questions help you evaluate and apply the material you have learned.
- **Case Projects.** Although it is important to understand the theory behind cybersecurity technology, nothing beats real-world experience. To this end, each chapter includes several case projects aimed at providing practical implementation experience as well as practice in applying critical thinking skills to the concepts learned throughout the chapter.

New to This Edition

- Maps fully to the latest CompTIA CySA+ CS0-003 exam
- Completely revised and updated with expanded coverage on cybersecurity foundations, Indicators of Attack, Indicators of Compromise, and security operations
- New module units include Cybersecurity Foundations, Security Operations, Vulnerability Assessment and Management, and Incident Response Management
- All new "#TrendingCyber" opener in each chapter

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- All new Two Rights & A Wrong self-assessments that give you opportunities to quickly assess your understanding of the topics
- Expanded and new Case Projects that provide opportunities to explore topics in greater depth
- All new introductions to the Case Projects provide time estimates, objectives, and project descriptions
- All CS0-003 exam topics fully defined
- Each exam subdomain is linked to Bloom's Taxonomy (see Appendix B)

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The following icons and elements are used in this textbook:

Notes

Note elements draw your attention to additional helpful material related to the subject being described.

Caution

Caution icons warn you about potential mistakes or problems and explain how to avoid them.

Two Rights & A Wrong

These elements let you quickly assess your understanding of the topics. The answers to these assessments appear at the end of each module.

Certification

Certification icons indicate CompTIA CySA+ objectives covered under major chapter headings.

Instructor's Materials

Instructors, please visit cengage.com and sign in to access instructor-specific resources, which include the Instructor's Manual, Solution and Answer Guide, PowerPoint presentations, and Instructor Test Banks.

Instructor's Manual. The Instructor's Manual that accompanies this course provides additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.
Solution and Answer Guide. The instructor's resources include solutions to all end-of-chapter material, including review questions and case projects

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

PowerPoint presentations. This course comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Cengage testing powered by Cognero. This flexible, online system allows you to do the following:

- Author, edit, and manage test bank content from multiple Cengage solutions.
- Create multiple test versions in an instant.
- Deliver tests from your learning management system, your classroom, and wherever you want.

MindTap

MindTap for *CompTIA® CySA+ Guide to Cybersecurity Analyst, Third Edition*, is an online learning solution designed to help you master the skills you need in today's workforce. Research shows that employers need critical thinkers, troubleshooters, and creative problem solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, and certification test prep. MindTap guides you through assignments that help you progress from basic knowledge and understanding to more challenging problems. MindTap activities and assignments are tied to CompTIA CySA+ certification exam objectives. MindTap features include the following:

- **Live Virtual Machine labs** allow you to practice, explore, and try different solutions in a safe sandbox environment. Each chapter provides you with an opportunity to complete an in-depth project hosted in a live virtual machine environment. You implement the skills and knowledge gained in the chapter through real design and configuration scenarios.
- **Pre- and Post-Assessments** assess your understanding of key concepts at the beginning and end of the course and emulate the text.
- **Security for Life** assignments encourage you to stay current with what's happening in the field of cybersecurity.
- **Reflection** activities encourage classroom and online discussion of key issues covered in the chapters.

Instructors, MindTap is designed around learning objectives and provides analytics and reporting so you can easily see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as is, or pick and choose how your materials will integrate with the learning path. You control what the students see and when they see it. Learn more at cengage.com/mindtap/.

State of Cybersecurity in Information Technology

The sheer volume of cyberattacks has reached astronomical proportions. The AV-TEST Institute receives instances of over 450,000 new malicious programs (malware) and potentially unwanted applications (PUAs) each day. One shipping port receives over 40 million attempted intrusions each month. The total number of instances of malware has grown from 182 million in 2013 to over 1.34 billion today. The cost for an organization to recover from a cyberattack is enormous; the healthcare industry alone has spent over $10 billion recovering from cyberattacks. Cybercrime has been called the "greatest transfer of economic wealth in history." It is estimated that it could reach $10.5 trillion annually by 2025.

To defend against the increasing numbers of cyberattacks, annual cybersecurity spending by companies and governments worldwide continues to grow. An organization's cybersecurity budget as a percentage of its total technology budget has increased from just 8 percent in 2020 to almost 12 percent today. In some industries, it is almost 20 percent. Yet even though billions of dollars are spent each year on defenses, the expenditure appears to be having limited impact on the number of successful attacks.

This imbalance—large amounts of money spent on defenses that still do not stop threat actors—has caused many security professionals to call for a change in thinking about security defenses. Security professionals today must have the knowledge and expertise to analyze data about different types of attacks. They must also be able to discover any vulnerabilities in the network and devices attached to it and then strengthen them to resist attacks.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Certifications

As the need for high-level cybersecurity personnel becomes increasingly critical to protect an organization's assets, the CompTIA Cybersecurity Analyst (CySA+) certification stands out as one of the premiere certifications for cyber professionals. CySA+ is designed for cyber workers who are tasked with incident detection, prevention, and response through continuous security monitoring. The certification equips them to demonstrate competency regarding current cyberattacks and defenses. It also provides the skills and knowledge to proactively monitor and detect systems by analyzing indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management, endpoint detection and response, and extended detection and response. And it equips cyber employees with the ability to respond to threats, attacks, and vulnerabilities and then communicate with stakeholders to address security analysis and compliance.

The value of an information technology (IT) professional who holds a security certification is significant. IT professionals with an IT certification earn 3.5 percent more than industry peers who do not have one. Professionals with a security certification also earn 8.7 percent more than counterparts who do not have one.

Certification provides job applicants with more than just a competitive edge over their noncertified counterparts competing for the same IT positions. Some institutions of higher education grant college credit to students who successfully pass certification exams, moving them further along in their degree programs. For those already employed, achieving a new certification increases job effectiveness, which opens doors for advancement and job security. Certification also gives individuals who are interested in careers in the military the ability to move into higher positions more quickly.

About the Author

Dr. Mark Ciampa is Professor of Analytics and Information Systems and Program Director of the graduate Cybersecurity Data Analytics program in the Gordon Ford College of Business at Western Kentucky University in Bowling Green. Prior to this, he was an associate professor and served as the Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee, for 20 years. Dr. Ciampa has worked in the information technology industry as a computer consultant for businesses, government agencies, and educational institutions. He has published over 25 articles in peer-reviewed journals and books. He is also the author of over 30 technology textbooks from Cengage, including *CompTIA Security+ Guide to Network Security Fundamentals, Eighth Edition*; *CWNA Guide to Wireless LANs, Third Edition*; *Guide to Wireless Communications*; *Security Awareness: Applying Practical Cybersecurity in Your World, Sixth Edition*; and *Networking BASICS*. Dr. Ciampa holds a PhD in technology management with a specialization in digital communication systems from Indiana State University and has certifications in security and healthcare.

Acknowledgments

A large team of dedicated professionals all contributed to this project, and I am honored to be part of such an outstanding group. First, thanks go to Cengage Portfolio Product Manager Natalie Onderdonk for providing me with the opportunity to work on this project and for providing continual support. Thanks also to Senior Content Manager Brooke Greenhouse for answering all my questions, to Learning Designer Carolyn Mako for her helpful suggestions, and to Danielle Shaw for her technical reviews. And special recognition again goes to developmental editor Lisa Ruffolo. As always, Lisa managed the details and provided me with helpful suggestions so that I could focus on my work. It is truly a privilege and a pleasure to work with Lisa. I also appreciated the significant contributions of the reviewers for this edition: Dr. Seon A. Levius, State University of New York at Potsdam and Dr. Keith A. Morneau, ECPI University. To everyone on this team and at Cengage Learning, I extend my sincere thanks.

Finally, I want to thank my wonderful wife, Susan. Her patience, support, and love were always there for me. I could not have done this project without her.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Dedication

To Braden, Mia, Abby, Gabe, Cora, Will, and Rowan

Read This Before You Begin

CompTIA® CySA+ Guide to Cybersecurity Analysis is designed to meet the needs of learners and professionals who want to master intermediate cybersecurity skills. A fundamental knowledge of computers and networks is required, along with a solid understanding of fundamental computer security. Those seeking to pass the CompTIA CySA+ certification exam will find the text's approach and content especially helpful; all CySA+ CS0-003 exam objectives are covered in the text (see Appendix B). This book covers all aspects of network and computer security while satisfying the exam objectives.

The book's pedagogical features are designed to provide a truly interactive learning experience that helps prepare you for the challenges of network and computer security. In addition to the information presented in the text, each chapter includes one or more virtual lab activities that guide you through implementing practical hardware, software, network, and Internet security configurations step by step. Each chapter also contains case studies that place you in the role of problem solver, requiring you to apply concepts presented in the chapter to achieve successful solutions. Additional questions in Appendix A provide even more opportunities to practice using the necessary tools to master cybersecurity analysis.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CompTIA

Your Next Move Starts Here!

Get CompTIA certified to help achieve your career goals and gain a powerful, vendor-neutral credential that is trusted by employers.

Save 10%
when you purchase your exam voucher from CompTIA.org.

Use code:
Cengage10



Why get CompTIA certified?

Increase your confidence
91% of certification earners show increased confidence.*

Earn more money
77% of IT pros got a raise within six months of earning their certification.*

Stand out to employers
64% of IT decision makers say certified employers add additional value.**

Join a global community
92% of IT professionals hold at least one certification.**



Get ready for exam day.

- **Download the exam objectives:** Visit CompTIA.org to find the exam objectives for your IT certification and print them out. This is your roadmap!
- **Create your study plan:** Decide how many hours each week you are going to dedicate to studying, choose your preferred study tools and get to work. Studying is a unique experience. Download a study plan worksheet on CompTIA.org.
- **Get certified:** If you haven't already, use the coupon on this page when you purchase your exam voucher and schedule your exam. CompTIA offers flexible testing options to fit your busy life.



Choose your testing option.

Online testing
Earn a CompTIA certification online, from your home – or any quiet, distraction-free, secure location – at a time that's convenient for you.

In-person testing
Test at any of the Pearson VUE test centers around the world, where you can use their equipment under the supervision of a proctor.

To purchase your exam voucher and learn how to prepare for exam day, visit CompTIA.org.

*Pearson VUE 2021 Value of IT Certifications
**2021 Global Knowledge IT Skills and Salary Report

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Part 1

Cybersecurity Foundations

A proper foundation for a building is essential for the stability of the structure. But a foundation does more than just hold the building steady above ground. Building foundations also keep out moisture, insulate against the cold, and resist movement of the earth around them. In other words, a foundation holds up and keeps out. When studying advanced cybersecurity, it is likewise important to have a strong foundational knowledge, both to maintain defenses and keep out threat actors. The chapters in this first part lay the foundations of cybersecurity by explaining technology basics, identifying threat actors and their threats, and examining basic cybersecurity protections.

Chapter 1
Technology Underpinnings

Chapter 2
Threat Actors and Their Threats

Chapter 3
Cybersecurity Substrata

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 1

Technology Underpinnings

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Describe infrastructure concepts and network architectures
2. Identify different types of operation technology
3. Outline operating system fundamentals
4. Compare scripting languages, data exchange formats, and regular expressions

#TrendingCyber

Ask virtually anyone if they have heard of a cybersecurity job shortage, and the answer will invariably be a resounding "YES." Bleak numbers continue to flood online media sites, indicating the dearth of cybersecurity workers needed to protect systems. One recent report said that cybersecurity job vacancies grew by 350 percent from 2013 to 2021 and worldwide 3.5 million cybersecurity jobs will be unfilled by 2025, of which over 750,000 vacant positions are in the United States alone.

This dismal situation has led to the rapid rise of "cybersecurity bootcamps." These training organizations promise prospective students who have no background in either technology or business that in just a few short months they will be employable. One camp boldly advertises, "Become a Cybersecurity Professional in 12 Weeks" in a bootcamp designed for "beginners and students without any IT experience." Cybersecurity bootcamps claim that after completion, graduates will be in high demand and will receive a high-paying cybersecurity job. One camp says, "Cybersecurity bootcamp graduates often work as information security analysts" earning a median annual salary of almost $104,000. The costs of these cybersecurity bootcamps typically start around $10,000, while more expensive camps can cost $15,000 to $18,000.

But what is often overlooked in the news about cybersecurity job vacancies and claims by cybersecurity bootcamps are the *types* of positions that are needed.

Often information surrounding a "cybersecurity job shortage" implies that all cybersecurity jobs and information security professionals are created equal. However, that is not the case. Seasoned cybersecurity recruiters point out that there is not a shortage of "cybersecurity generalists." That's because there are few job roles that are looking for a cybersecurity generalist.

Cybersecurity recruiters point out that there are very few truly entry-level jobs for cybersecurity generalists. Most entry-level roles tend to be specific and focused on one part of the profession and as such they are not generalist roles. For example, a company may need a network security engineer with knowledge of networks or an identity management analyst with experience in identity systems; these are not jobs for a cybersecurity generalist. And most cybersecurity roles are not even considered entry level. Companies assume that applicants already have some other background, usually technical, before they are ready for a cybersecurity job. Without specific skills, it is difficult for a candidate to break into the cybersecurity profession.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The true shortage in cybersecurity is for information security professionals, developers, and engineers. These individuals have the necessary knowledge and skills to write code and implement technical security architectures. There is also a need for product security and application security specialists. And analysts with threat hunting and incident response skills are desperately needed. These are skills that simply cannot be obtained by taking a three-month bootcamp.

There are other issues contributing to the shortage of cybersecurity professionals. Many organizations do not pay market rates for information security professionals. These organizations create job listings with significant information security requirements, skills, education, and required industry certifications but offer salaries that are not much higher than other information technology (IT) entry-level salaries.

Another problem is a misunderstanding by the organization's human resources (HR) system. Most HR departments employ an HR generalist. This is someone who runs the daily functions of the HR department including hiring and interviewing staff; administering pay, benefits, and vacations; and dealing with HR policies and practices. For many positions for which the company is recruiting, an HR generalist is sufficient for drawing up job specifications and screening initial applicants.

However, when it comes to recruiting for a cybersecurity position, an HR generalist is usually not the right person for recruiting. Because cybersecurity requires unique talents, an HR generalist may lack the understanding to effectively advertise and interview competent job candidates. Often HR will start and end a hiring conversation by asking, "Are you a certified information systems security professional (CISSP)?" as if that is the only requirement that matters.

How can this problem be solved?

First, empirical and objective data around the cybersecurity job shortage is needed that highlights the types of cybersecurity jobs that are open. Second, the role of bootcamps needs to be made plain. Cybersecurity is a specialty within IT, which is the larger area of risk management. Just as there are specialties in medicine (a doctor can only enter specialties such as cardiology after completing a residency in internal medicine) so too cybersecurity requires a thorough understanding of risk management, generalized IT, networks, operating systems, threat actors and their actions, cybersecurity appliances, and more. This simply cannot be obtained in a bootcamp. (That's why there are no bootcamps for someone to become a cardiologist!). Without making the role of bootcamps plain, individuals may quit a job to spend thousands of dollars enrolling in bootcamps for a new job in cybersecurity that may never appear. Third, HR departments need to understand how to effectively hire security professionals. Expecting an HR generalist to find security specialists without clear guidance from the hiring manager is a difficult and frustrating endeavor. Instead, a hiring manager needs to be clear about what they want the candidate to be able to do and then provide that information to HR personnel before the job opening is even posted.

And finally, organizations should organically grow and cross-train their IT staff into cybersecurity professionals. Many IT employees are eager to enter cybersecurity. Creating an internal program to mentor and train them is a long-term, but highly effective, approach.

So, is there a cybersecurity jobs crisis? Yes. But the reasons behind the shortage and the solutions to it are not what most people think.

As the need for high-level cybersecurity personnel becomes increasingly critical in order to protect an organization's assets, the CompTIA Cybersecurity Analyst (CySA+) certification stands out as one of the premier certifications for cyber professionals. CySA+ is designed for cyber workers who are tasked with incident detection, prevention, and response through continuous security monitoring. The certification equips them to demonstrate competency regarding current cyberattacks and defenses. It also provides the skills and knowledge to proactively monitor and detect systems by analyzing indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management, endpoint detection and response, and extended detection and response. And it equips cyber employees with the ability to respond to threats, attacks, and vulnerabilities and then communicate with stakeholders to address security analysis and compliance.

Although CySA+ is considered an advanced certification, it is important to first have a solid basis in key areas, sometimes called *underpinnings*. A physical underpinning is the material and construction of a foundation that is used for support of a structure. The word is also figuratively used to refer to anything that serves as a foundation, basis, or support (such as, "The philosophical underpinnings of a classical education").

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In cybersecurity there are foundational topics that serve as the underpinnings upon which security rests. Having a good understanding of these topics is important, for without the knowledge of the foundations it is difficult or even impossible to provide protections over them.

In this chapter, you review technology underpinnings. These can be broken down into infrastructures and architectures and software foundations.

Infrastructures and Architectures

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

2.1 Given a scenario, implement vulnerability scanning methods and concepts.

Different infrastructures and architectures are considered foundational. These include infrastructure concepts, network architectures, and operational technologies.

Infrastructure Concepts

Generally, the word *concept* is used for an idea of what something is or how it works. In information technology (IT), there are concepts that make up the foundation of how the underlying infrastructure functions. These concepts are sometimes called "modern infrastructure concepts" because they reflect the recent developments in IT that have led to fundamental (and in some ways revolutionary) changes in how IT functions. Infrastructure concepts can be divided into virtualization, containerization, and serverless technologies.

Virtualization

Virtualization is a vital concept in IT and cybersecurity. Understanding virtualization includes knowing what it is and how it can be used along with its advantages and risks.

What Is Virtualization? **Virtualization** is a means of managing and presenting computer resources by function without regard to their physical layout or location. One type of virtualization in which an entire operating system (OS) environment is simulated is known as host virtualization. Instead of using a physical computer, a virtual machine (VM), which is a simulated software-based emulation of a computer, is created. The "host system" (the OS installed on the computer's hardware) runs a VM monitor program that supports one or more "guest systems" (a foreign virtual OS) that run applications. For example, a computer that boots to Windows 11 (host) could support a VM of Linux (guest) as well as another Windows 11 (guest) system. An example of virtualization is shown in Figure 1-1.

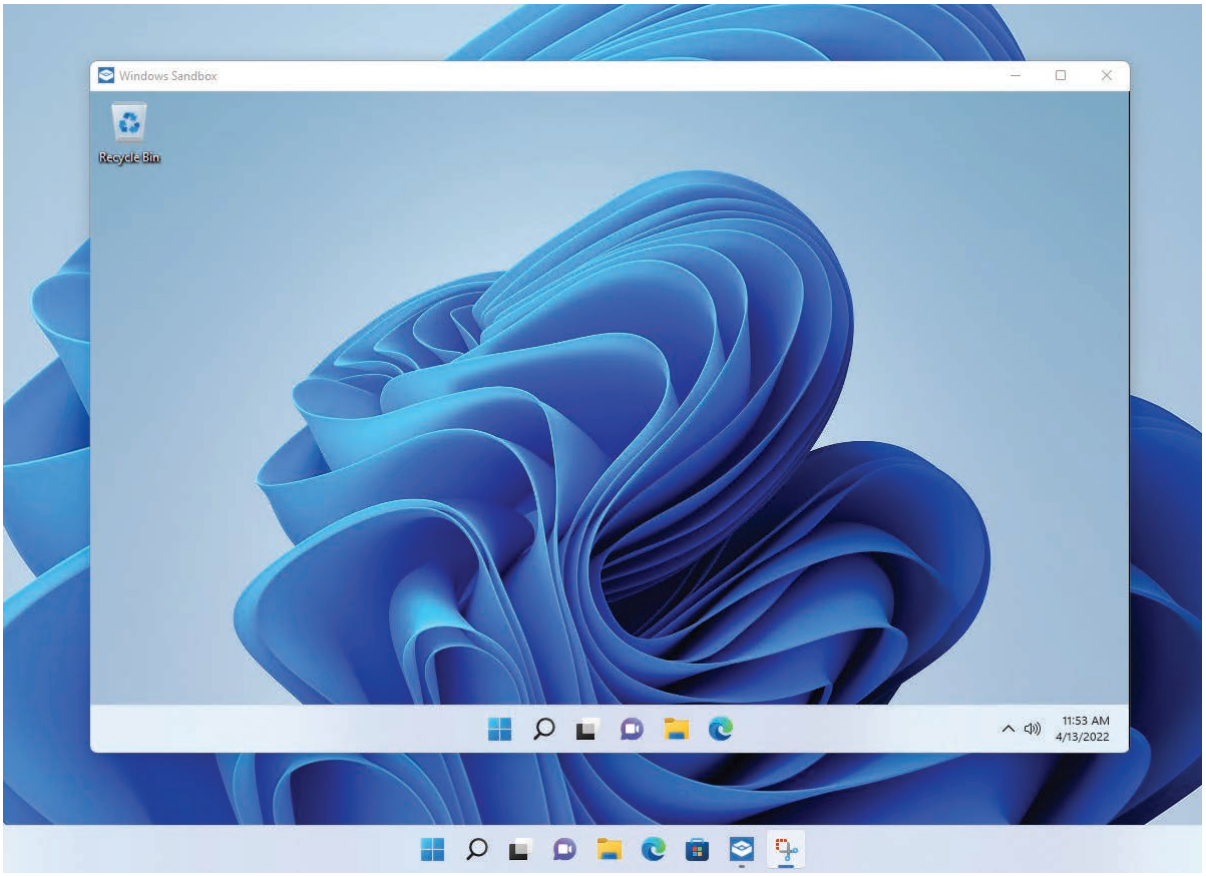
Note 1

Virtualization is not new. It was first developed by IBM in the 1960s for running multiple software "contexts" on its mainframe computers. It gained popularity over the last 20 years as data centers used it for migrating away from physical servers to more economical VMs.

In data centers, virtualization is used to consolidate multiple physical servers into VMs that can run on a single physical computer. Because a typical server uses only about 10 to 15 percent of its capacity, multiple VMs can run on a single physical server. Virtualization is also used extensively in cloud computing environments. It gives the flexibility necessary for rapid deployments. In fact, the adoption and popularity of cloud computing can be directly attributed to the widespread use of data center server virtualization.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

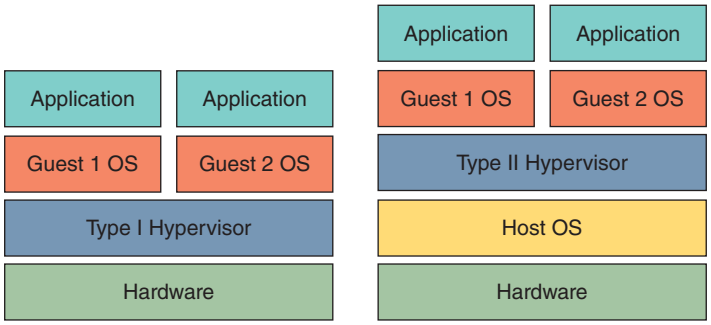
Figure 1-1 Virtualization



Source: Microsoft Corporation

A VM monitor program called a hypervisor manages the VM OSs. Hypervisors use a small layer of computer code in software or firmware to allocate resources in real time as needed, such as input/output functions and memory allocations. The two types of hypervisors are illustrated in Figure 1-2.

Figure 1-2 Type I and Type II hypervisors



- **Type I.** Type I hypervisors run directly on the computer's hardware instead of the underlying OS. They are sometimes called "native" or "bare metal" hypervisors.
- **Type II.** Instead of running directly on the computer hardware, Type II hypervisors run on the host OS, much like a regular application.

A common application of virtualization is virtual desktop infrastructure (VDI). VDI involves running a user desktop inside a remote VM that resides on a server. This enables personalized desktops for each user to be available on any computer or device that can access the server so that their personalized desktop and files can be accessed as if they were sitting at their own computer. VDIs allow mobile users to access their desktop from any location. It also provides flexibility: a user can access a

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Linux desktop using an Apple Mac computer in which the desktop is running on a Windows server. VDI also allows centralized management as opposed to the need for technical support personnel to access a system remotely or even visit a user's desk to troubleshoot, saving substantial time and money.

Advantages and Risks of Virtualization Virtualization has several advantages: new virtual server machines can be quickly made available, it can reduce costs by eliminating the need to purchase one physical server to run one network OS and instead run multiple VMs and host multiple OSs, and it can address "downtime" by quickly moving a VM from one server to another.

Host virtualization also has several security-related advantages:

- The latest security updates can be downloaded and run in a VM to determine compatibility, or the impact on other software or even hardware. This is used instead of installing the update on a production computer and then being forced to "roll back" to the previous configuration if it does not work properly.
- A snapshot of the state of a VM can be saved for later use. A user can make a snapshot before performing extensive modifications or alterations to the VM, and then the snapshot can be reloaded so that the VM is at the beginning state before the changes were made. Multiple snapshots can be made, all at different states, and loaded as needed.
- Testing the existing security configuration, known as security control testing, can be performed using a simulated network environment on a computer using multiple VMs. For example, one VM can virtually attack another VM on the same host system to determine vulnerabilities and security settings. This is possible because all the VMs can be connected through a virtual network.
- VMs can promote security segregation and isolation. Separating VMs from other machines can reduce the risk of infections transferring from one device to another.
- A VM can be used to test for potential malware. A suspicious program can be loaded into an isolated VM and executed. If the program is malware, it will impact only the VM, and it can easily be erased and a snapshot reinstalled.

Note 2

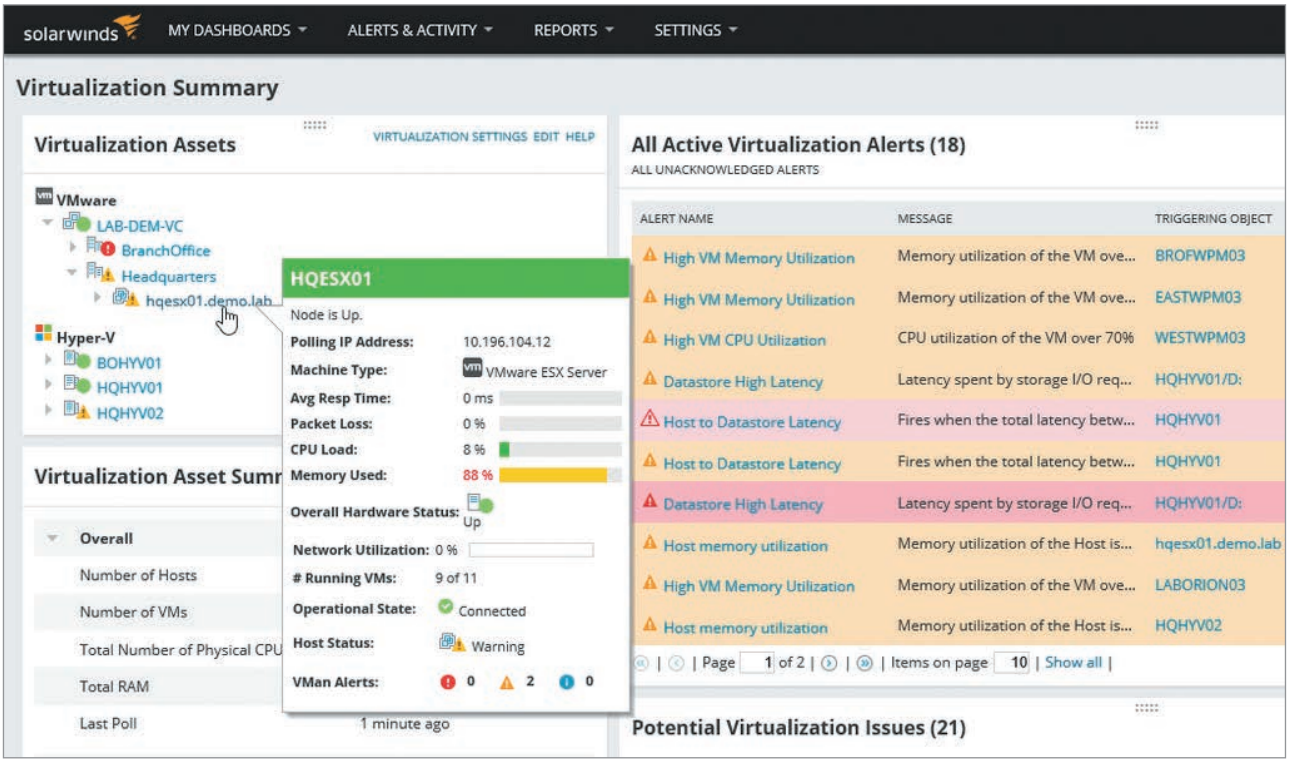
Threat actors have learned that when their malware is run in a VM, it most likely is being examined by a security professional. Many modern instances of malware will refuse to function and will self-destruct if it detects that it is being run in a VM.

However, there are security risks for virtualized environments:

- Not all hypervisors have the necessary security controls to keep out determined attackers. If a single hypervisor is compromised, multiple virtual servers are at risk.
- Traditional security tools, such as antivirus, firewalls, and intrusion detection systems (IDSs), were designed for single physical servers and do not always adapt well to multiple VMs. Instead, "virtualized" versions can be used instead, such as a firewall virtual appliance that is optimized for VMs.
- VMs must be protected from both outside networks and other VMs on the same physical computer. In a network without VMs, external devices such as firewalls and IDSs that reside between physical servers can help prevent one physical server from infecting another physical server, but no such physical devices exist between VMs.
- VMs may be able to "escape" from the contained environment and directly interact with the host OS. It is important to have VM escape protection so that it cannot directly interact with the host OS and potentially infect it, which could then be transmitted to all other VMs running on the host OS.
- Because VMs can easily and quickly be created and launched, this has led to VM sprawl, or the widespread proliferation of VMs without proper oversight or management. It is often easy for a VM to be created and then forgotten. A guest OS that has remained dormant for a period of time may not contain the latest security updates, even though the underlying host OS has been updated. When the guest is launched, it will be vulnerable until properly updated. One option for combating VM sprawl is to install a VM manager, which can provide a dashboard of the status of the VMs. A VM manager is shown in Figure 1-3.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 1-3 Virtual machine manager

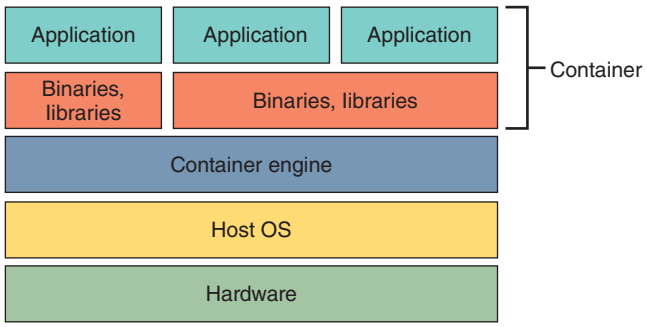


Source: SolarWinds

Containerization

One form of virtualization is **containerization**, which is a reduced instance of virtualization. With both Type I and Type II hypervisors, the entire guest OS must be started and fully functioning before an application can be launched. A container, on the other hand, holds only the necessary OS components (such as binary files and libraries) that are needed for that specific application to run. And in some instances, containers can even share binary files and libraries. This not only reduces the necessary hard drive storage space and random access memory (RAM) needed but also allows for containers to start more quickly because the entire OS does not have to be started. Containers can be easily moved from one computer to another. A container is illustrated in Figure 1-4.

Figure 1-4 Container

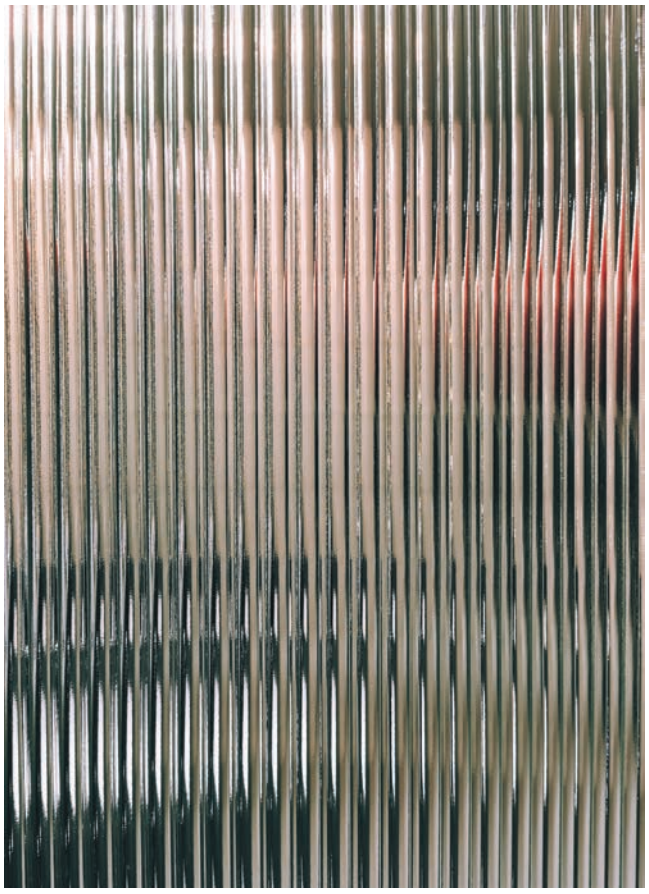


Serverless

Many offices have a frosted glass partition to separate public areas from restricted areas. These partitions not only separate the two areas, they also prevent outsiders from viewing employees or the work that is being conducted inside. A frosted glass partition is shown in Figure 1-5. Instead of being transparent (can clearly see through) the partition is opaque (cannot clearly see through).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 1-5 Office frosted glass partition



Fernstarphoto/Shutterstock.com

The word *opaque* is also used in IT to refer to a technology or process that is hidden from viewing or fully understanding. Opaque is a word that applies to a **serverless** infrastructure. A serverless infrastructure is one in which the capacity planning, installation, setup, and management are all opaque or "invisible" to the user because they are handled by another entity. Serverless essentially means that provisioning, deploying, and managing a physical server is no longer performed by the organization.

Note 3

The term "serverless" is actually a misnomer. Serverless does not mean that there are no servers present; there are servers somewhere that are managed by someone. It simply means that the organization or user does not perform that function.

Network Architectures

There are different network architectures that are also fundamental to IT. These can be divided into their locations and their architectures.

Locations

Today many networks are located remotely in the cloud. However, some networks are still located locally on an organization's campus in an on-premises environment.

Cloud Computing Different from traditional IT models, a divergent approach for computing has gained widespread use today. This approach is known as **cloud computing**. Although various definitions of cloud computing have been proposed, the definition from the National Institute of Standards and Technology (NIST) may be the most comprehensive: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

Cloud computing is a much more flexible approach to computing resources. Cloud computing allows an almost endless array of servers, software, and network appliances to be quickly and easily configured as needed. And it is a pay-per-use computing model in which customers pay only for the online computing resources they need. As computing needs increase or decrease, cloud computing resources can be quickly scaled up or scaled back. Because cloud resources are available online, users from virtually anywhere around the world can access them through opening a web browser without the need for installing additional software. Cloud computing is illustrated in Figure 1-6. Table 1-1 lists different advantages of cloud computing.

Figure 1-6 Cloud computing

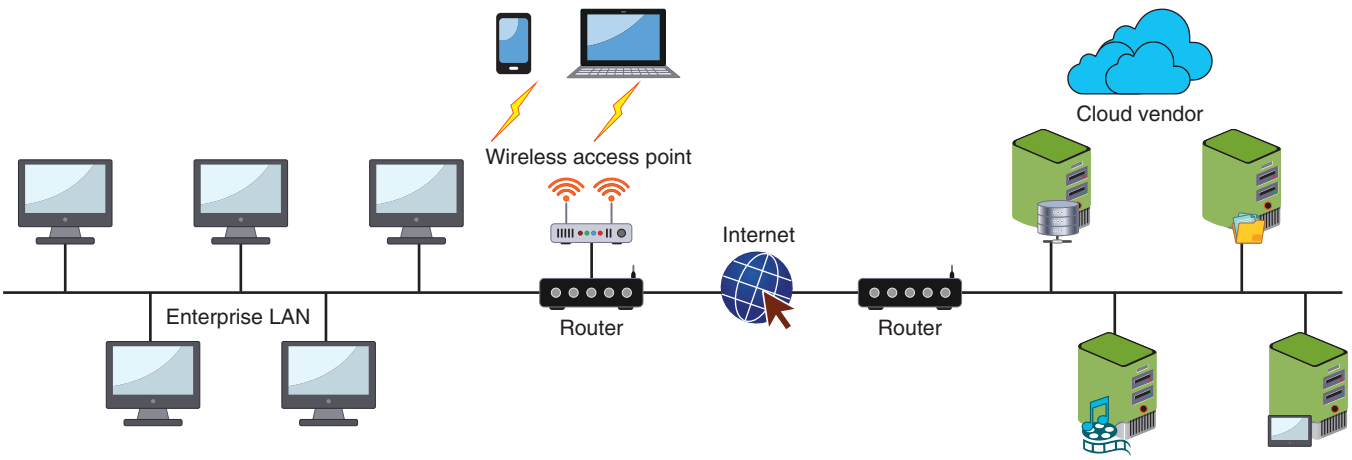


Table 1-1 Cloud computing advantages

Characteristic	Explanation
On-demand self-service	The consumer can make changes, such as increasing or decreasing computing resources, without requiring any human interaction from the service provider.
Universal client support	Virtually any networked device (desktop, laptop, smartphone, tablet, etc.) can access cloud computing resources.
Invisible resource pooling	The physical and virtual computing resources are pooled together to serve multiple, simultaneous consumers that are dynamically assigned or reassigned based on the consumers' needs; the customer has little or no control or knowledge of the physical location of the resources.
Immediate elasticity	Computing resources can be increased or decreased quickly to meet demands.
Metered services	Fees are based on the computing resources used.

There are different types of clouds. A public cloud is one in which the services and infrastructure are offered to all users, with access provided remotely through the Internet. Unlike a public cloud that is open to anyone, a community cloud is a cloud that is open only to specific organizations that have common concerns. For example, because of the strict data requirements of the Health Insurance Portability and Accountability Act (HIPAA), a community cloud open only to hospitals may be used. A private cloud is created and maintained on a private network. Although this type offers the highest level of security and control (because the company must purchase and maintain all the software and hardware), it also reduces cost savings. A **hybrid** cloud is a combination of public and private clouds.

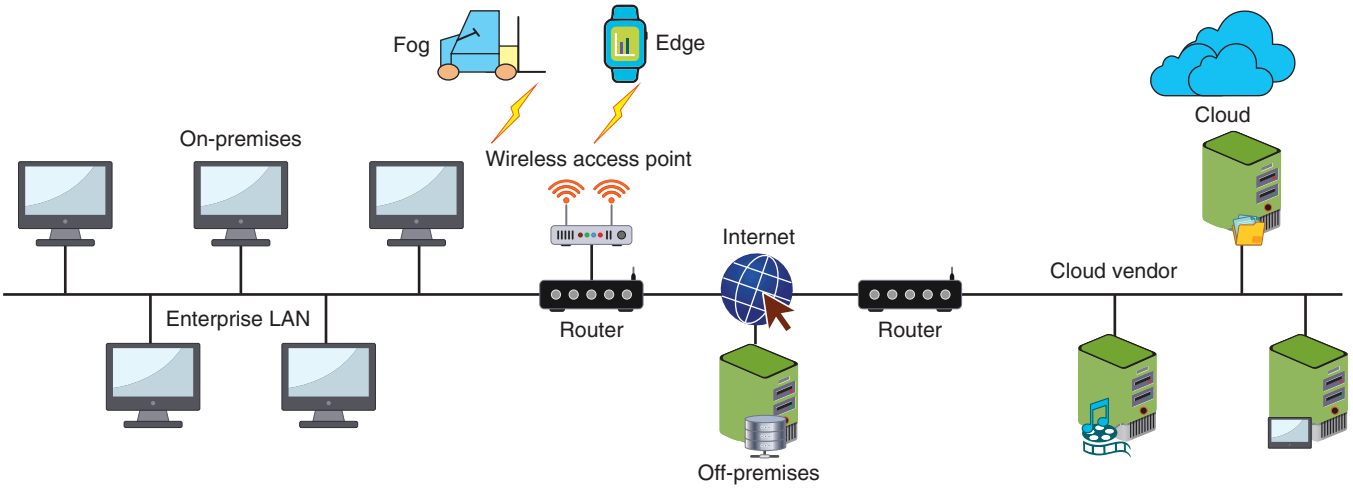
On-Premises The introduction of cloud computing has redefined the location of computing resources. Instead of using a centralized model in which equipment and personnel are located locally at an organization's campus, computing now takes place in several different locations (a decentralized model). However, for different reasons—including cybersecurity—not all computing resources have migrated to the cloud. **On-premises** refers to computing resources that are located on the campus of an organization ("on-prem"). The different locations of computing resources are listed in Table 1-2 and illustrated in Figure 1-7.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 1-2 Computing locations

Location	Description	Example
On-premises	Computing resources located on the campus of an organization ("on-prem")	Desktop computer, local area network, data center
Off-premises	A computing resource hosted and supported by a third party	Remote backup facility
Fog	A decentralized computing infrastructure in which data, compute capabilities, storage, and applications are located between the data source and the cloud	Automated guided vehicles on an industrial shop floor
Edge	Computing that is performed at or very near to the source of data instead of relying on the cloud or on-prem for processing	Internet of Things device
Cloud	A remote facility for computing	Artificial intelligence processing engine

Figure 1-7 Computing locations



How much of an enterprise's network architecture should be migrated to the cloud—and how much should remain on-prem? A traditional three-tier on-prem architecture is illustrated in Figure 1-8 (note that for simplicity no security appliances are illustrated). This multi-tiered design helps control connections, provide scaling, and increase security. An enterprise could migrate *Tier 1—Web servers* and *Tier 2—Application servers* to a cloud computing provider but keep *Tier 3—Database servers* on-prem for security. However, it could just as easily migrate all three tiers to the cloud computing provider. Such a decision will need to be based on several different factors.

Architectures

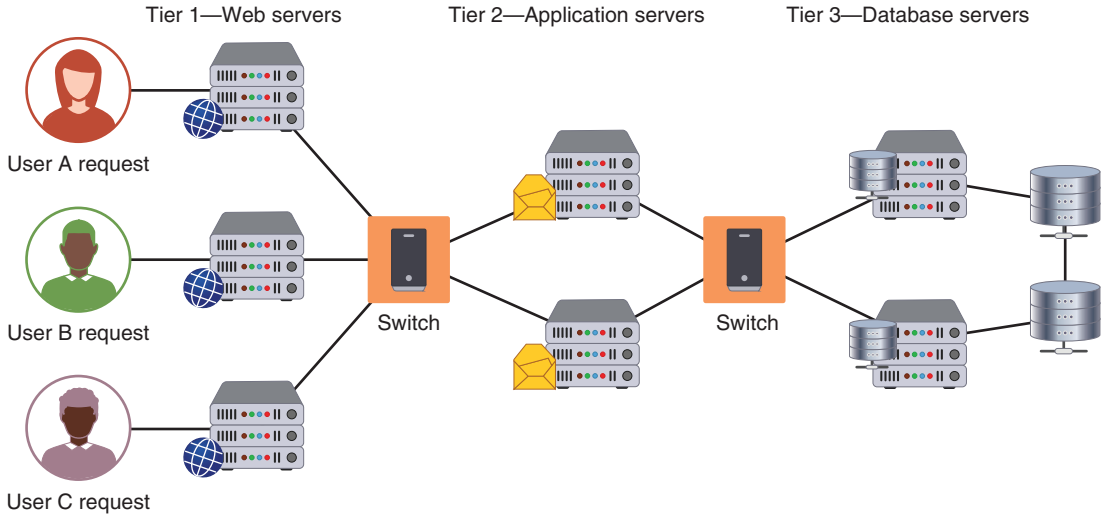
Network architectures include network segmentation and software-defined networking.

Network Segmentation It would be unthinkable to have an office building in which anyone could freely enter any room or office. Instead, office buildings have different areas with different levels of access. While a lobby is generally an open area for almost anyone to initially enter the building, security guards and technology devices restrict access to other areas, such as only allowing approved personnel to their own offices. And within those areas there are even more restrictions: a regular employee can enter their office but is restricted from entering the security operations center (SOC) that monitors and manages information security functions.

In a similar way, a network infrastructure should be designed like an office building, with some areas available for general access while other parts of the network having successively tighter restrictions. For example, a public-facing web server needs to

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 1-8 Three-tier architecture



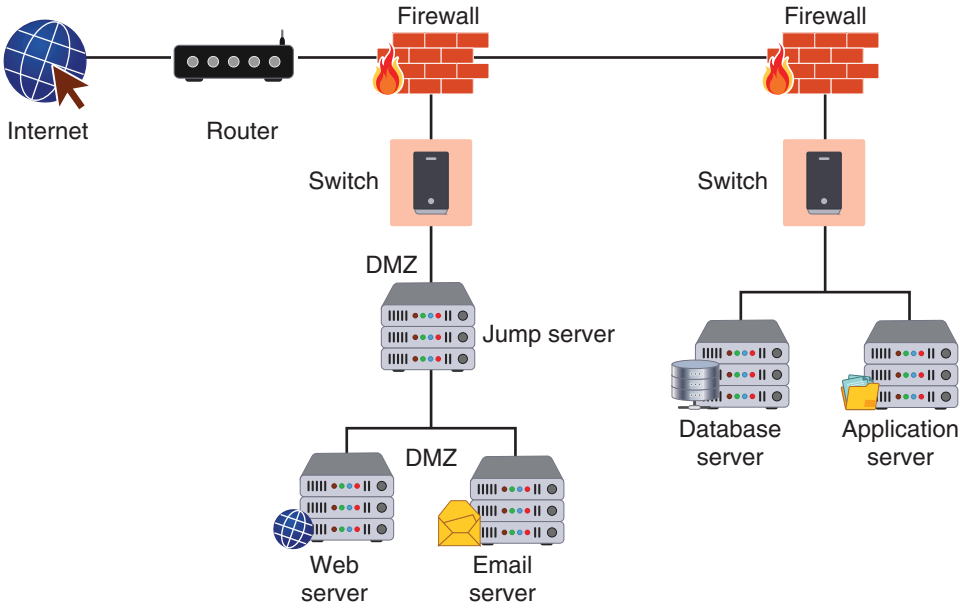
be in an area in which anyone can access it, while a server with sensitive corporate accounting data must be in a highly restricted area of the network. And the most restricted level of all can be a network that is physically isolated from all other networks or the Internet. By creating these security zones of different levels of access, it creates a higher level of security through network design. This is known as **network segmentation**.

Network segmentation can be achieved in two different ways. The first is by physical segmentation, or breaking down a larger computer network into a collection of smaller networks ("subnets"). A physical network appliance acts as the gateway into the subnet, controlling which traffic comes in and goes out. Physical segmentation is relatively straightforward to administer because the topology is fixed in the architecture. Logical segmentation creates subnets via "virtual networks" or through network addressing schemes. It is more flexible than physical segmentation because it requires no wiring or physical movement of network appliances to create the subnet, and automated provisioning can simplify the configuration of the smaller networks.

Two examples of cybersecurity network segmentation are a jump server and an air gap.

Jump Server A jump server, shown in Figure 1-9, is a minimally configured administrator server (either physical or virtual) within a restricted area of the network called a demilitarized zone (DMZ). Running only essential protocols and ports, it connects

Figure 1-9 Jump server



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

two dissimilar security zones while providing tightly restricted access between them. An administrator accesses the jump server, which is connected to the administrative interface of the devices within the DMZ.

Caution

To further limit the vulnerabilities of a jump server, administrators should ensure that all jump server software is regularly updated, limit the programs that can run on it, implement multifactor authentication for logins, do not allow outbound access or severely restrict access from the jump server, and use access control lists (ACLs) to restrict access to specific authorized users.

In recent years, an additional security configuration has been used to limit risks when administering a DMZ. Instead of an administrator connecting to a jump server from just any computer, only a dedicated secure admin workstation (SAW) can be used to connect to the jump server. Using a SAW prevents an administrator's infected computer from compromising the jump server.

Air Gap In order to keep a crucial network or endpoint from being compromised by infection or data exfiltration, an air gap can be utilized. This solution completely isolates the network or endpoint from all external sources, including any network connection or external ports (like a USB port) into which external media can be attached. This isolation is called an "air gap" because the devices to be protected have a separation between them and all other devices that only consist of air. Air gaps are often used in environments such as nuclear power plants in which computers and connected systems must be completely isolated from the external world.

Note 4

"Air-gapped" was not a term that originated with network infrastructure. It has been used for many years in the field of electricity, referring to the space between two objects magnetically related (like the rotor and the stator in a dynamo) or between two objects electrically related (such as the gap between an electrode and the tip of a spark plug).

Software-Defined Networking (SDN) Virtualization has been an essential technology in changing the face of computing over the last decade. Racks of individual physical servers running a single application have been replaced by only a few hardware devices running multiple VMs, simulated software-based emulations of computers. VMs have made cloud computing possible; as computing needs increase or decrease, cloud computing resources on VMs can be quickly scaled up or back. Networks can also be configured into logical groups to create a virtual local area network (VLAN). A VLAN allows scattered users to be logically grouped together even though they are physically attached to different switches. The computing landscape today would simply not be possible without virtualization.

Yet VMs and virtual LANs run into a bottleneck: the physical network. Dating back over 40 years, networks comprised of physical hardware like bridges, switches, and routers have collided with the world of VMs and VLANs.

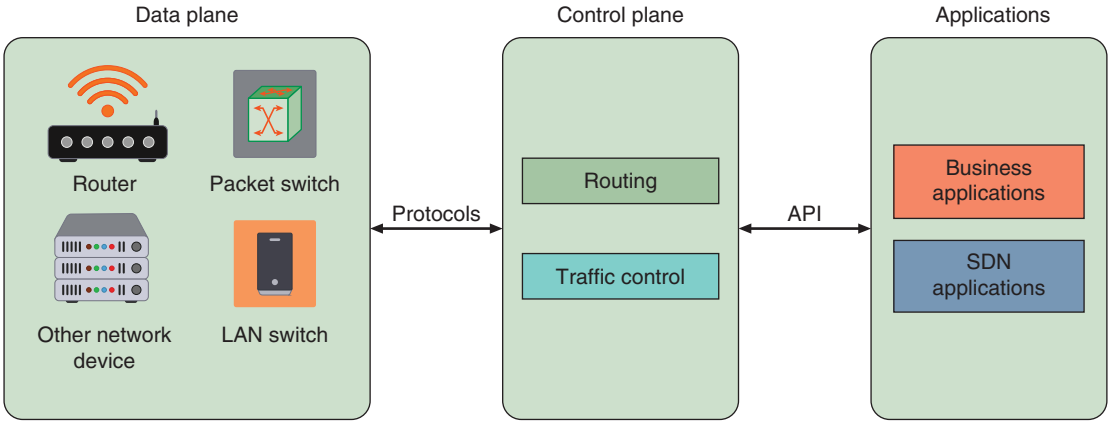
Consider this problem. A network manager needs to make sure the VLAN used by a VM is assigned to the same port on a switch as the physical server that is running the VM. But if the VM needs to be migrated, the manager must reconfigure the VLAN every time that a virtual server is moved. In a large enterprise, whenever a new VM is installed, it can take hours for managers to perform the necessary reconfiguration. In addition, these managers must configure each vendor's equipment separately, tweaking performance and security configurations for each session and application. This process is difficult to do with conventional network switches because the control logic for each switch is bundled together with the switching logic.

What is needed is for the flexibility of the virtual world to be applied to the network. This would allow the network manager to add, drop, and change network resources on the fly quickly and dynamically.

The solution is **software-defined networking (SDN)**. SDN virtualizes parts of the physical network so that it can be more quickly and easily reconfigured. This is accomplished by separating the control plane from the data plane, as illustrated in Figure 1-10. The control plane consists of one or more SDN servers and performs complex functions such as routing and security checks. It also defines the data flows through the data plane. The goal of an SDN is to allow a network administrator to shape, construct, and manage network resources, such as traffic and bandwidth, from a central console without modifying individual network hardware appliances.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 1-10 Software-defined networking



Note 5

In an SDN, the control plane is essentially an application running on a computer that can manage the physical plane.

If traffic needs to flow through the network, it first receives permission from the SDN controller, which verifies that the communication is permitted by the network policy of the enterprise. Once approved, the SDN controller computes a route for the flow to take and adds an entry for that flow in each of the switches along the path. Because all the complex networking functions are handled by the SDN controller, the switches simply manage "flow tables" whose entries are created by the controller. The communication between the SDN controller and the SDN switches uses a standardized protocol and application programming interface (API).

Note 6

The architecture of SDN is very flexible, using different types of switches from different vendors at different protocol layers. SDN controllers and switches can be implemented for Ethernet switches (Layer 2), Internet routers (Layer 3), Transport (Layer 4) switching, or Application layer switching and routing.

With the decoupling of the control and data planes, SDN enables applications to deal with one "abstracted" network device without any care for the details of how the device operates. This is because the network applications see only a single API to the controller. This makes it possible to quickly create and deploy new applications to orchestrate network traffic flow to meet specific enterprise requirements for performance or security.

From a security perspective, SDNs can provide stronger protection. SDN technology can simplify extending VLANs beyond just the perimeter of a building, which can help secure data. Also, an SDN can ensure that all network traffic is routed through a firewall. And because all network traffic flows through a single point, it can help capture data for network intrusion systems (NIDSs) and network prevention systems (NIPSs).

Note 7

Both network segmentation and SDN can be utilized in either the cloud or on-premises.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Operational Technology

Operational technology is becoming increasingly important across a wide range of industries. And protecting it has also become increasingly important. Operational technology involves defining it, knowing the types of operational technologies, and identifying its risks and weaknesses.

Defining Operational Technology (OT)

IT is defined as the development, management, and application of computer equipment, networks, software, and systems. IT is essential to modern business operations because it enables users to access technology for enhanced functionality. The core focuses of IT are summarized in Table 1-3.

Table 1-3 Core IT focuses

Focus	Description
Operations	Operations involve the day-to-day management of IT departments, which includes managing devices, maintaining networks, testing the security of applications and systems, and providing technical support.
Infrastructure maintenance	This includes the process of setting up and maintaining infrastructure equipment, such as cabling, laptops, wireless networks, servers, and VMs.
Governance	Governance is the process of ensuring that IT policies and services align with the needs and demands of the organization.

However, IT is not the only technology found in many organizations. **Operational technology (OT)** is using hardware and software to monitor and control physical processes and the devices connected to the infrastructure that support these processes. OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities. It ranges from monitoring pressures in pipes to controlling robots on a manufacturing floor.

Types of OT

There are different types of OT. **Industrial control systems (ICSs)** collect, monitor, and process real-time data so that machines can directly control devices such as valves, pumps, and motors without the need for human intervention. Often ICSs manage systems at remote locations.

Multiple ICSs are managed by a larger **supervisory control and data acquisition (SCADA)** system. SCADA systems are crucial today for industrial organizations. They help to maintain efficiency and provide information on issues to help reduce downtime.

ICSs can be divided into specialized systems and Internet of Things devices.

Specialized Systems Several types of specialized systems are designed for specific applications. One example of a specialized system measures the amount of utilities consumed. Traditionally households have had utilities such as electricity and water measured by an analog meter that records the amount of electricity or water being used. This requires an employee from the utility company to visit each home and read from the meter the amount that was consumed for the month so that a bill can be sent to the occupant. Digital smart meters are replacing these analog meters. Smart meters have several advantages over analog meters, and these are listed in Table 1-4.

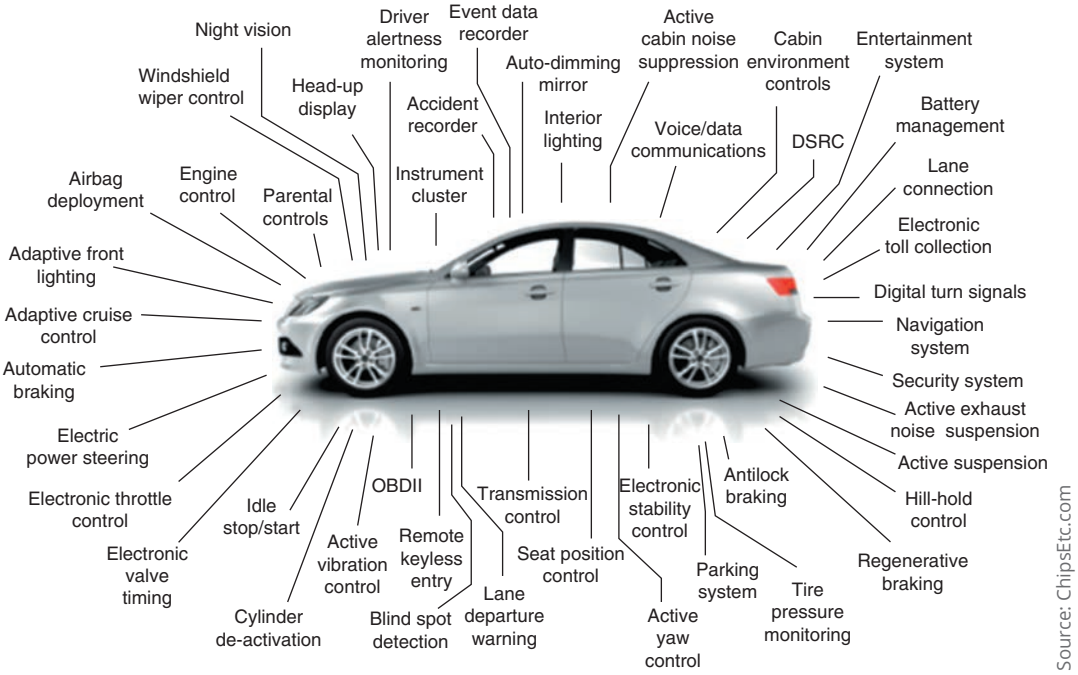
Other specialized systems include medical systems, aircraft, and vehicles. The progression of specialized systems in automobiles is an example of how these systems have dramatically changed human-to-machine interaction. The first automobile embedded systems appeared in mass-production vehicles in the mid-1970s in response to regulations calling for higher fuel economy and emission standards and handled basic functions such as engine ignition timing and transmission shifting. By the 1980s, more sophisticated computerized engine-management systems enabled the use of reliable electronic fuel-injection systems, and later active safety systems such as antilock braking and traction and stability control features were added, all controlled by embedded systems. Today embedded systems in cars use sonar, radar, and laser emitters to control brakes, steering, and the throttle to perform functions such as blind-spot and pedestrian collision warnings, automated braking, safe distance-keeping, fully automated parking, and even autonomous driving. Some of the specialized systems in cars are shown in Figure 1-11.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 1-4 Analog meters versus smart meters

Action	Analog meter	Smart meter
Meter readings	Employee must visit the dwelling each month to read the meter.	Transmits meter readings daily, hourly, or even by the minute to the utility company
Servicing	Annual servicing is required in order to maintain accuracy.	Battery replacement is every 20 years
Tamper protection	Data must be analyzed over long periods to identify anomalies.	Alerts utility in the event of tampering or theft
Emergency communication	None available	Transmits "last gasp" notification of a problem to utility company

Figure 1-11 Specialized systems in cars



Internet of Things The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) defines the Internet of Things (IoT) as "A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[2] More simply put, the IoT is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon.

Although this definition could encompass laptop computers and tablets, more often IoT refers to devices that heretofore were not considered as computing devices connected to a data network. IoT devices are spurring home automation with items such as thermostats, coffeemakers, tire sensors, slow cookers, keyless entry systems, washing machines, electric toothbrushes, headphones, and light bulbs, to name just a few. It is estimated that in 2022 the average number of connected devices per household was 22. The total number of IoT devices by 2025 is estimated to be 27 billion.[3]

OT Risks and Weaknesses

Despite their importance and widespread usage, there are significant risks associated with OT. Whereas a cybersecurity incident involving IT may involve the theft of customer data or a successful distributed denial-of-service (DDoS) attack, a successful attack on OT systems can be significantly more deadly and result in loss of life. A threat actor who can remotely manipulate the pressure in a pipeline so that it ruptures can inflict serious physical harm to a large number of persons.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Other OT systems provide vital services to a wide range of users, such as emergency services, water treatment plants, and traffic management. These are called **critical infrastructures** because of their importance. A single successful cybersecurity incident would result in a significant negative impact on the population. However, even a successful attack on OT organizations not responsible for a critical infrastructure can cause dire consequences. For example, a food production facility could ship unsafe food if a threat actor removes safety checks.

Note 8

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Some of these sectors include chemical, commercial facilities, communications, dams, energy, food, and wastewater.

For many years, OT cybersecurity protections have been marginalized. This is due to several factors:

- **Separate IT-OT networks.** Generally, IT and OT networks are kept separate. This results in gaps in security defenses and duplication of security efforts. Separate IT-OT networks result in complex networks that cannot track what is happening throughout the attack surface, cannot share information, and fail to provide full visibility.
- **Separate reporting structures.** Typically, OT networks report to the chief operating officer (COO) while IT reports to the chief information officer (CIO). This separate reporting structure results in two network security teams, each protecting half of the total network. This can make it difficult to even identify the boundaries of the attack surface because these disparate teams do not know what is attached to their own network, resulting in security gaps.
- **Lack of OT security focus**. Traditionally, OT cybersecurity was not necessary because OT systems were not connected to the Internet. Because they were not exposed to external threats, security was not considered a priority. However, as more OT systems have been connected to the external networks and the Internet for remote monitoring and administration, security measures have not been equally applied.

Two Rights & A Wrong

1. On a VM, the host system is the OS installed on the computer's hardware.
2. A Type I hypervisor runs on the host OS like an application.
3. A weakness of OT is that it is generally separate from IT networks.

See the answers at the end of the chapter.

Software

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

In addition to infrastructures and architectures, there are software technology underpinnings. These include the OS and coding.

Operating System Fundamentals

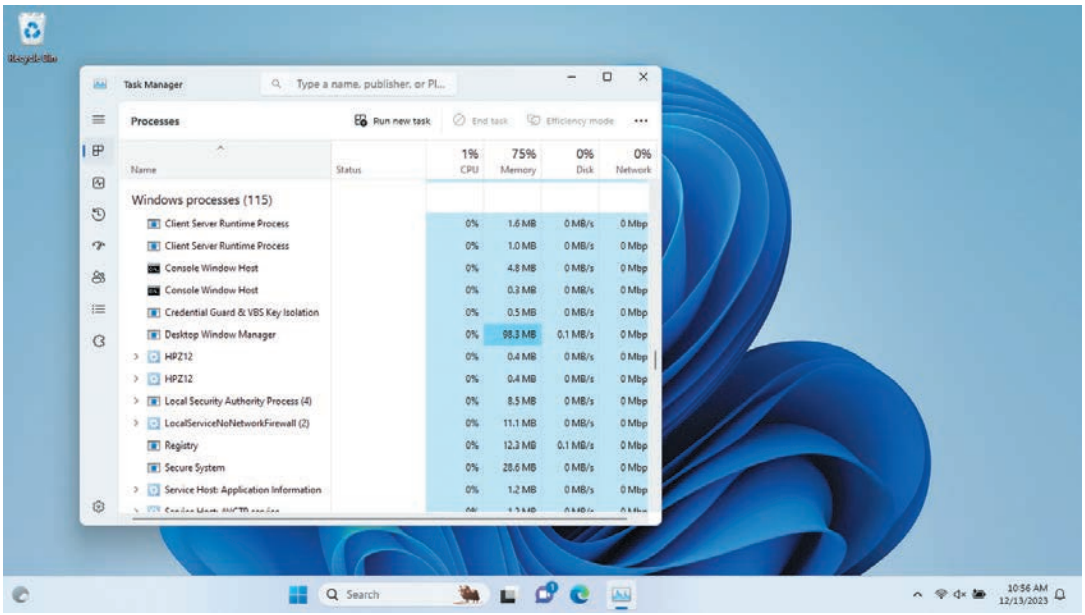
There are basic foundations of OSs. These include system processes, configuration files, and hardware architectures (as they apply to the OS). There are also steps to perform system hardening through the OS.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

System Processes

A computer program is a set of instructions. Programs are written using programming languages such as C#, Python, Java, or Rust, among many others. When that program is executed by the computer, it accomplishes one or more specific tasks. A process is a running program that is managed by the OS. A process can have one or more threads, which is a single sequential flow of activity that is being executed in a process. Processes running under Microsoft Windows are shown in Figure 1-12.

Figure 1-12 Microsoft Windows system processes



Note 9

The number of processes that should be running on a computer depends on its specific configuration and what programs are installed. Typically, a Windows system will normally have 60 to 70 processes running during regular usage. But it is not uncommon for over 200 processes to be running on a system, with many programs installed or running background tasks.

A special category of OS processes is **system processes**. The system processes are responsible for managing memory allocations, hosting OS drivers, and managing other processes. The system processes host threads that only run in a special mode known as kernel mode. Processes running in kernel mode have full and unrestricted access to the computer system and all its resources, and this mode is managed by the main system process.

Note 10

It is important for cybersecurity professionals to be familiar with the normal behavior of system processes since they run in kernel mode. This includes the relationships of one process invoking another process (called a "parent–child" relationship) and the number of instances that should be present on the computer. An abnormal relationship or number of system processes may indicate the presence of a threat actor.

Configuration Files

A file is a named collection of related information that is recorded on a storage device such as a solid-state drive, hard disk drive, USB flash drive, or optical disk. Files are stored on a device according to a required format that the OS can "understand" and manipulate. This is called a **file structure**.

One specific type of file is a configuration file, which contains initial settings and specific parameters for programs. Configuration files are used for both system processes and user applications. OSs store configuration files in a specific area based

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

on the OS, known as the **configuration file location**. For Linux and Unix systems along with Apple macOS, the system-wide software configuration files are stored in the */etc* directory. User applications often use a file or directory in the home directory prefixed with a period ("dotfile"). These configuration files are typically hidden from the user. Some newer applications create a folder in the *.config* directory, which is a standardized subdirectory of the home directory.

Instead of using separate configuration files, Microsoft uses a hierarchical database that contains configuration settings. This database is known as the **Windows Registry** and stores low-level settings for the Windows OS and applications. Device drivers, services, the OS kernel, and some security applications use the registry.

Note 11

Unexpected modifications or an abnormal registry setting (registry change or anomaly) can serve as an indication of compromise by a threat actor.

Hardware Architecture

Computer **hardware architecture** is the design and organization of the physical components that make up a computer system. The basic components of a computer hardware architecture are the central processing unit (CPU) that executes instructions and controls the operations; the memory where data and programs are stored and accessed; the input/output (I/O) devices or peripherals through which the user interacts with the computer and connected devices, such as the keyboard, mouse, monitor, printer, etc.; and the bus, which is the system of connectors that transfer signals between the various components.

One of the elements of hardware architecture often overlooked in securing endpoint computers is to confirm that the computer has started without any malicious activity taking place. Ensuring this secure startup involves the Unified Extensible Firmware Interface (UEFI) and its boot security features.

Unified Extensible Firmware Interface (UEFI)

Because a computer is unable to rely on external assistance when powered on, this process of a computer starting up by itself is called booting up or just booting. The booting process on early personal computers used firmware called the BIOS (Basic Input/Output System). The BIOS was a chip integrated into the computer's motherboard. When the computer was powered on, the BIOS software would "awaken" and perform the following steps in a legacy BIOS boot:

1. The BIOS would first test the various components of the computer to ensure that they were functioning properly (called the POST or Power-On Self-Test).
2. Next, the BIOS would reference the master boot record (MBR) that specified the computer's partition table, which instructed the BIOS where the computer's OS could be located.
3. Finally, the BIOS passed control over to the installed boot loader that launched the OS.

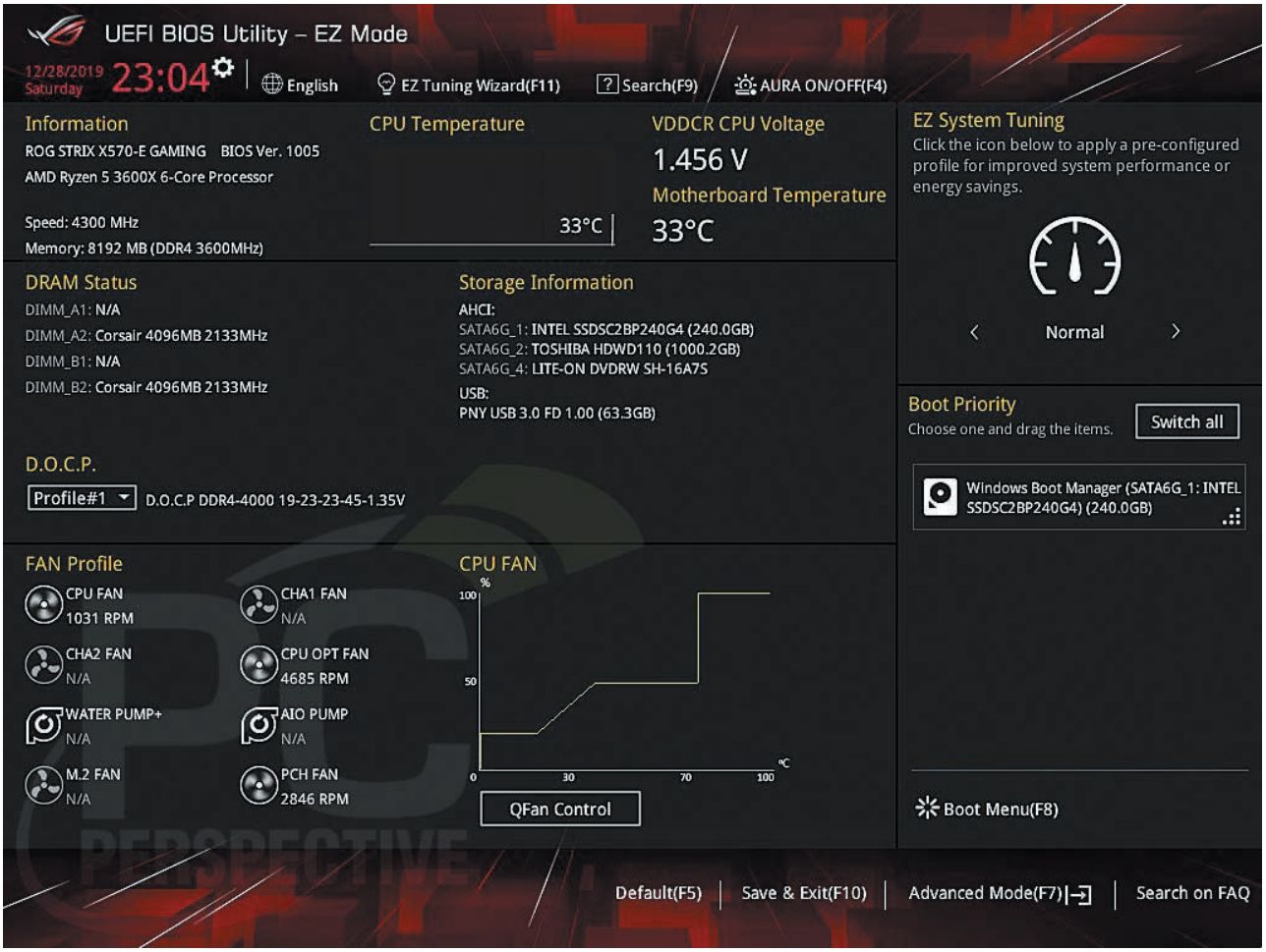
To add functionality, an improved firmware interface was developed to replace the BIOS. Known as UEFI (Unified Extensible Firmware Interface), it provides several enhancements over BIOS. This includes the ability to access hard drives that are larger than 2 terabytes (TB), support for an unlimited number of primary hard drive partitions, faster booting, and support for networking functionality in the UEFI firmware itself to aid in remote troubleshooting. UEFI also has a more advanced user interface for configurations and information, as shown in Figure 1-13.

UEFI is an attractive attack target for threat actors. This is due to several reasons:

- **Persistence.** Because UEFI infections can survive reboots and even reinstallation of the OS, UEFI firmware is a prime target of attackers. And it has other components that make it even more desirable, such as networking capabilities. This allows a threat actor to remotely access and update the infected firmware modules to maintain access indefinitely.
- **Stealth.** It is difficult to know what is actually present in UEFI firmware at installation time and hard to perform runtime security monitoring. There are few anti-malware and endpoint detection tools that can audit the UEFI boot sections, sound an alert when there are changes to the UEFI firmware, or attempt to recover from an infection. And because the CPU itself limits access to UEFI, it limits an OS from preventing or monitoring malicious activity against UEFI firmware.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 1-13 UEFI user interface



Source: ASUS

- **Difficulty patching.** While the UEFI specification allows for firmware patch updates, these updates may require manual steps such as downloading, verifying, installing, and resetting the core components. Threat actors can take advantage of these delays in patching to install malware on the UEFI.

Boot Security Another significant improvement of UEFI over BIOS relates to boot security. The ability to update the BIOS in firmware also opened the door for a threat actor to create malware to infect the BIOS. Called a BIOS attack, it would exploit the update feature of the BIOS. Because the BIOS resides in firmware and if infected would then persistently reinfect the computer whenever it was powered on, BIOS attacks were difficult to uncover and hard to disinfect. UEFI, used along with other components, is designed to combat these BIOS vulnerabilities and provide improved boot security.

Caution

UEFI by itself does not provide enhanced boot security. It must be paired with other boot security functions.

Boot security involves validating that each element used in each step of the boot process has not been modified. This process begins with the validation of the first element (boot software). Once the first element has been validated, it can then validate the next item (like software drivers) and so on until control has been handed over to the OS. This is called a chain of trust: each element relies on the confirmation of the previous element to know that the entire process is secure.

But how does the chain begin? What if a threat actor were to inject malware prior to the start of the chain of trust? If the starting point is software, it can be replaced or modified. That would then compromise each element of the chain. To prevent this, a chain of trust requires a strong starting point.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The strongest starting point is hardware, which cannot be modified like software. This is known as the hardware root of trust. Security checks are "rooted" in (begin with) hardware checks. Because this chain of trust begins with a hardware verification, each subsequent check can rely on it (called boot attestation).

Several different techniques can be used to ensure boot security, all relying on UEFI and some relying on the hardware root of trust. Different boot security modes are listed in Table 1-5.

Table 1-5 Boot security modes

Name	Description	Advantages	Disadvantages
Legacy BIOS Boot	Uses BIOS for boot functions	Compatible with older systems	No security features
UEFI Native Mode	Uses UEFI standards for boot functions	Security boot modules can be patched or updated as needed.	No validation or protection of the boot process.
Secure Boot	Each firmware and software executable at boot time must be verified as having prior approval.	All system firmware, bootloaders, kernels, and other boot-time executables are validated.	Custom hardware, firmware, and software may not pass without first being submitted to system vendors like Microsoft.
Trusted Boot	Windows OS checks the integrity of every component of the boot process before loading it.	Takes over where Secure Boot leaves off by validating the Windows 10 or 11 software before loading it	Requires using Microsoft OS
Measured Boot	Computer's firmware logs the boot process so OS can send it to a trusted server to assess the security.	Provides highest degree of security	Could slow down the boot process

System Hardening

There are several protections at the OS level that can provide overall system hardening and protection. These include:

- **Disabling unnecessary ports and protocols.** One of the primary OS security configurations involves disabling ports/protocols or closing unused ports and disabling unnecessary protocols. This also includes turning off unneeded services, such as Microsoft Windows ASP.NET State Service, Portable Device Enumerator Service, and Apple macOS Spotlight Indexing.
- **Application allow list.** An increasingly popular approach to OS security is to employ application allow listing. This is approving in advance only specific applications to run on the OS so that any item not approved will not function. Application allow listing requires preapproval for an application to run. The inverse of an allow list is a deny list, or a listing of unapproved software so that any item not on the list can run. Although often overlooked, application allow listing is a powerful tool to combat attacks. The elite Tailored Access Operations (TAO) section of the National Security Agency (NSA) is responsible for compromising networks owned by hostile nations to spy on them. The head of the TAO spoke at a security conference about the best practices of security from the NSA's perspective (in his own words, "What can you do to defend yourself to make my life hard?") and said one of the most important steps was to employ application allow listing for the software that runs on servers.[4]

Note 12

Microsoft 11 Windows Defender offers built-in ransomware protection based on an application allow listing called "controlled folder access" and allows only trusted apps to access protected folders. The apps can be executable files, scripts, or a dynamic-link library (DLL). There is a set of protected folders by default that typically contain user data (Documents, Pictures, Videos, Music, and Favorites), but users can also add additional folders to protect, and even add additional approved apps to access protected folders. In the event of a ransomware attack, a notification appears with a warning that an app attempted to modify a file in a protected folder.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Coding

Another fundamental of software is creating the software itself through a process known as coding. Coding languages are often categorized as scripting or scripting/programming languages. In addition, data exchange formats are required so that the application can "talk" to other applications and devices. And regular expressions are used to help match, locate, and manage text.

Scripting Languages

A scripting language is a type of coding language that is typically used to automate tasks. Unlike programming languages that are used to build large and complex applications, scripting languages are typically used for smaller tasks. They can even run inside another program, unlike a programming language in which instructions are only executed on a line-by-line basis. Common scripting languages are Visual Basic for Applications, shell scripts, and PowerShell.

Visual Basic for Applications (VBA) Visual Basic for Applications (VBA) is an "event-driven" Microsoft scripting language. VBA allows both developers and users to automate processes that normally would take multiple steps or levels of steps. It can be used to control many tasks of the host application, including manipulating user interface features like toolbars, menus, forms, and dialog boxes.

VBA is built into most Microsoft Office applications (Word, Excel, and PowerPoint, for example) for both Windows and Apple macOS platforms. It is also included in select non-Microsoft products. VBA can even control one application from another application using Object Linking and Embedding (OLE) automation. For example, VBA can automatically create a Microsoft Word report from data in a Microsoft Excel spreadsheet.

VBA is most often used to create macros. A macro is a series of instructions that can be grouped together as a single command. Macros are used to automate a complex task or a repeated series of tasks. Macros are generally written by using VBA and are stored within the user document (such as in an Excel .xlsx worksheet or Word .docx file) and can be launched automatically when the document is opened.

Although macros date back to the late 1990s, they continue to be a key attack vector. Microsoft has reported that 98 percent of all Office-targeted threats are a result of macro-based malware, and it has warned users that Office macros particularly in Excel are still used to compromise Windows systems.

Caution !

Unless there is a business requirement for macros, support for their use should be disabled across the Microsoft Office suite. If macros are required, only those that have been digitally signed by a trusted publisher should be allowed to execute. To prevent users or an adversary from bypassing macro security controls, all support for trusted documents and trusted locations should be disabled. Organizations can disable Trust Center settings and apply macro security controls using Group Policy settings.

Shell Script A **shell script** is a text file that contains a sequence of commands for a Linux or Unix OS. It is called a shell script because the "shell" is the OS command-line interface (CLI) and interpreter that are used to communicate with the OS. A shell script combines a sequence of commands into a single file that otherwise would have to be typed into the keyboard one command at a time. The shell script is activated by entering the file name on a command line. Shell scripts are typically used for repetitive processes such as executing routine backups.

Note 13

Shell scripts in Microsoft Windows are called "batch files" and date back to the predecessor of Windows, MS-DOS. Apple uses the shell Zsh.

One of the common shell scripts is called bash. Bash is the command language interpreter (shell) for the Linux/Unix OS and "bash scripting" is using Bash to create a script.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

Exploits have taken advantage of vulnerabilities in Bash. For example, one vulnerability allowed attackers to remotely attach a malicious executable file to a variable (a value that changes) that is executed when Bash is invoked.

PowerShell **PowerShell** is a task automation and configuration management framework from Microsoft. Initially PowerShell was a Microsoft Windows component known as Windows PowerShell and was built on the Windows .NET framework (a developer platform that can be used to write apps in specific programming languages). In 2016, it was updated and released both as an open-source and a cross-platform product running on Windows, macOS, and Linux platforms.

Administrative tasks in PowerShell are performed by *cmdlets* ("command-lets"), which are specialized .NET classes that implement a specific operation. PowerShell providers give access to data located in different data repositories, such as the file system or Windows registry. Users and developers can create and add their own cmdlets to PowerShell. PowerShell also provides a hosting API so the PowerShell runtime can even be embedded inside other applications. On the Microsoft Windows platform, PowerShell has full access to a range of OS components and APIs. It can run locally on an endpoint or across a network accessing other endpoint devices.

The power and reach of PowerShell also make it a prime target for threat actors. PowerShell allows attackers to inject code from the PowerShell environment into other processes without first storing any malicious code to the hard disk. This allows the commands to execute while bypassing security protections and leaves virtually no evidence behind. PowerShell can also be configured so that its commands are not detected by any anti-malware running on the computer. Because most applications flag PowerShell as a "trusted" application, its actions are rarely scrutinized.

Caution

It is important to understand that these are not vulnerabilities but rather are features of PowerShell as a result of its tight integration with the .NET Framework. It allows users an extremely powerful and easy means to access sensitive elements of an OS and is frequently used by developers and system administrators.

Scripting/Programming Languages

While virtually all languages fall into either the category of a scripting language or a programming language, there is one notable exception. **Python** is a popular general-purpose programming language that can run on several OS platforms. However, Python can also be used as a scripting language.

Python's syntax allows programmers to write code that takes fewer lines than in other programming languages like Java and C++. Python also supports object-oriented programming. It has a large standard library in which developers can use routines created by other developers.

Note 14

Python was created in the late 1980s by Dutch programmer Guido van Rossum as a side project during his Christmas vacation. Van Rossum needed a name that was short, unique, and slightly mysterious, so the language Python was named after *Monty Python's Flying Circus*, a BBC comedy series from the 1970s.

Python is widely used in cybersecurity. One of its primary usages is for automating repetitive and time-consuming tasks. These include the following:

- **Incident response.** Python is used to write scripts to automate incident response tasks, such as quarantining infected systems and collecting evidence of an attack.
- **Log analysis.** Python scripts can "comb through" and analyze massive log files from multiple sources looking for suspicious activity.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Network scanning.** Python can be used to write scripts to scan networks for open ports and devices.
- **Vulnerability assessment.** Scripts written in Python are used to assess vulnerabilities in systems and applications.

Note 15

Python is also used for developing cybersecurity tools. It has been used to create penetration testing tools and frameworks as well as to develop malware analysis tools, such as disassemblers, debuggers, and packet sniffers. Security researchers also use Python to develop new security tools and techniques. For example, it has been used to develop tools for identifying zero-day vulnerabilities.

Data Exchange Formats

Output from applications is not always displayed on a screen for a user to view; in fact, today this is rarely the case. Most applications send and exchange data with other applications, platforms, systems, and devices. This requires a common data format for data exchange.

One of the first common data exchange formats was **eXtensible Markup Language (XML)**. XML uses markup symbols called tags to define data. Figure 1-14 shows an example of an XML document that displays the names of three students.

Figure 1-14 XML code displaying three student names

```
<students>
   <student>
      <firstName>Giovanni</firstName> <IastName>Ricci</IastName>
   </student>
   <student>
      <firstName>Capucine</firstName> <IastName>Delisle</IastName>
   </student>
   <student>
      <firstName>Leticia</firstName> <IastName>Jimenez</IastName>
   </student>
</students>
```

However, XML has some deficiencies. As a markup language similar to HTML, XML stores data in a tree structure that presents layers of information. This makes XML more complex and verbose. In addition, the structure of XML makes it vulnerable to unauthorized modifications.

Note 16

XML security can be enhanced by turning off the document type declaration (DTD) feature.

An alternative to XML is **JavaScript object notation (JSON)**. JSON is considered to be more concise and compact so that it executes faster than XML. An example of JSON displaying the names of three students is seen in Figure 1-15.

Figure 1-15 JSON code displaying three student names

```
{"students":[
   {"firstName":"Giovanni", "IastName":"Ricci"},
   {"firstName":"Capucine", "IastName":"GarciaDelisle"},
   {"firstName":"Leticia", "IastName":"Jimenez"}
]}
```

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

There are several differences between XML and JSON that are listed in Table 1-6. JSON is often used for data exchange from a client to a server, while XML, which is used for other tasks besides just exchanging data, is commonly used for data exchanges between servers.

Table 1-6 Comparing JSON and XML

Category	JSON	XML
Format	Uses a "maplike" structure with key-value pairs	Stores data in a tree structure with names for different data categories
Syntax	Is compact and is considered easier to read and write	Is more "wordy"
Data types	Supports numbers, objects, strings, and Boolean arrays	Supports numbers, objects, strings, Boolean arrays, dates, and images
File size	Creates smaller files that can be transmitted more quickly	Creates larger files that take longer to transmit
Security	Is considered more secure than XML	Can be enhanced by turning off DTD

Regular Expressions

A **regular expression** (regex) is a special string of text for describing a search pattern. These patterns can match, locate, and manage text. Regular expressions can also be used from the command line and in text editors to find text within a file.

The wildcard notation **.txt* is commonly used to find all files that have *txt* as the file extension using the asterisk wildcard. The regex equivalent is *^.*\.txt$*. When searching for any email address that contains the @ symbol, the regex expression would be *\b[A-Z0-9._%+−]+@[A-Z0-9.−]+\.[A-Z]{2,}\b*.

Many software applications, scripts, and programming languages support regular expressions. And because regex can also be used to search and replace text, this allows users to quickly make changes across a large number of files.

Two Rights & A Wrong

1. Apple macOS uses a hierarchical database that contains configuration file information.
2. UEFI has replaced BIOS.
3. A regular expression is a special string of text for describing a search pattern.

See the answers at the end of the chapter.

Summary

- As the need for high-level cybersecurity personnel becomes increasingly critical to protect an organization's assets, the CompTIA CySA+ is considered one of the premiere certifications for cyber professionals. CySA+ is designed for cyber workers who are tasked with incident detection, prevention, and response through continuous security monitoring. The certification equips them to demonstrate competency regarding current cyberattacks and defenses while providing the skills and knowledge to proactively monitor and detect systems by analyzing indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management, endpoint detection and response, and extended detection and response. And it equips cyber employees with the ability to respond to threats, attacks, and vulnerabilities and then communicate with stakeholders.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- Basic concepts make up the foundation of how the underlying information technology (IT) infrastructure functions. Virtualization is a means of managing and presenting computer resources by function without regard to their physical layout or location. One type of virtualization in which an entire operating system (OS) environment is simulated is known as host virtualization. Instead of using a physical computer, a virtual machine (VM), which is a simulated software-based emulation of a computer, is created instead. While virtualization has several IT and cybersecurity advantages, there are risks when using virtualized environments. One form of virtualization is containerization, which is a reduced instance of virtualization. A container holds only the necessary OS components needed for that specific application to run. A serverless infrastructure is one in which the capacity planning, installation, setup, and management are all opaque to the user because they are handled by another entity.
- Different network architectures are also fundamental to IT. Cloud computing is a more flexible approach to computing resources because it allows an array of servers, software, and network appliances to be quickly and easily configured as needed. It is also a pay-per-use computing model in which customers pay only for the online computing resources they need. As computing needs increase or decrease, cloud computing resources can be quickly scaled up or scaled back. However, for different reasons—including cybersecurity—not all computing resources have migrated to the cloud. On-premises refers to computing resources that are located on the campus of an organization.
- Network segmentation divides secure network environments from those that are public facing. A jump server is a minimally configured administrator server (either physical or virtual) within a restricted area of the network called a DMZ. Running only essential protocols and ports, it connects two dissimilar security zones while providing tightly restricted access between them. Another network segmentation completely isolates the network or endpoint from all external sources, including any network connection or external ports (like a USB port) into which external media can be attached. This isolation is called an "air gap" because the devices to protect are separated by air.
- Software-defined networking (SDN) virtualizes parts of the physical network so that it can be more quickly and easily reconfigured. The goal of a SDN is to allow a network administrator to shape, construct, and manage network resources, such as traffic and bandwidth, from a central console without modifying individual network hardware. This is accomplished by separating the control plane from the data plane. The control plane consists of one or more SDN servers and performs complex functions such as routing and security checks. It also defines the data flows through the data plane. SDNs can provide stronger cybersecurity protection. SDN technology can simplify extending virtual LANs beyond just the perimeter of a building, which can help secure data. Also, an SDN can ensure that all network traffic is routed through a firewall.
- Operational technology (OT) is using hardware and software to monitor and control physical processes and the devices connected to the infrastructure that support these processes. OT is used in a variety of industries. There are different types of OT. Industrial control systems (ICSs) collect, monitor, and process real-time data so that machines can directly control devices such as valves, pumps, and motors without the need for human intervention. Multiple ICSs are managed by a larger supervisory control and data acquisition (SCADA) system. One type of ICS is specialized systems designed for specific applications. More broadly, Internet of Things (IoT) is used to connect any device to the Internet for the purpose of sending and receiving data to be acted upon.
- There are significant risks associated with OT. A cybersecurity incident involving IT may involve the theft of customer data, but a successful attack on OT systems can be significantly more deadly and result in loss of life. OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities. Other OT systems provide vital services to a wide range of users, such as emergency services, water treatment plants, and traffic management. These are called critical infrastructures because of their importance. A single successful cybersecurity incident would result in a significant negative impact on the population. For many years, OT cybersecurity protections have been essentially ignored for a variety of reasons.
- A special category of OS processes is system processes. The system processes are responsible for managing memory allocations, hosting OS drivers, and managing other processes. The system

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

processes host threads that only run in a special mode known as kernel mode. Files are stored on a device according to a required format that the OS can "understand" and manipulate. This is called a file structure. One specific type of file is a configuration file, which contains initial settings and specific parameters for programs. Configuration files are used for both system processes and user applications. OSs store configuration files in a specific area based on the OS, known as the configuration file location.

- Because a computer is unable to rely on external assistance when powered on, the process of starting up on its own is called booting up or just booting. The booting process on early personal computers used firmware called the BIOS (Basic Input/Output System). To add functionality, an improved firmware interface was developed to replace the BIOS. Known as UEFI (Unified Extensible Firmware Interface), it provides several enhancements over BIOS. UEFI is an attractive attack target for threat actors due to its persistence, stealth, and difficulty patching. Another significant improvement of UEFI over BIOS relates to boot security. Boot security involves validating that each element used in each step of the boot process has not been modified. This process begins with the validation of the first element (boot software). Once the first element has been validated, it can then validate the next item (like software drivers), and so on, until control has been handed over to the OS. This is called a chain of trust.
- There are several protections at the OS level that can provide overall system hardening and protection. Two common protections are disabling unnecessary ports and protocols that are not needed. An increasingly popular approach to OS security is to employ application allow listing. This is approving in advance only specific applications to run on the OS so that any item not approved will not function. Application allow listing requires preapproval for an application to run.
- A scripting language is a type of coding language that is typically used to automate tasks. Unlike programming languages that are used to build large and complex applications, scripting languages are typically used for smaller tasks. They can even run inside another program, unlike a programming language in which instructions are only executed on a line-by-line basis. Common scripting languages are Visual Basic for Applications, shell scripts, and PowerShell. While virtually all languages fall into either the category of a scripting language or a programming language, there is one notable exception. Python is a popular programming language that can run on several different OS platforms. It can also be used as a scripting language and is a useful cybersecurity tool.
- Output from applications is not always displayed on a screen for a user to view; in fact, today this is rarely the case. Most applications send and exchange data with other applications, platforms, systems, and devices. This requires a common data format for data exchange. One of the first common data exchange formats was eXtensible Markup Language (XML). XML uses markup symbols called tags to define data. An alternative to XML is JavaScript object notation (JSON). JSON is considered to be more concise and compact so that it executes faster than XML. A regular expression (regex) is a special string of text for describing a search pattern. These patterns can match, locate, and manage text. Regular expressions can also be used from the command line and in text editors to find text within a file.

Key Terms

cloud computing
configuration file location
containerization
critical infrastructures
eXtensible Markup Language (XML)
file structure
hardware architecture
hybrid
industrial control systems (ICSs)
JavaScript object notation (JSON)
network segmentation
on-premises
operational technology (OT)
PowerShell
Python
regular expression
serverless
shell script
software-defined networking (SDN)
supervisory control and data acquisition (SCADA)
system processes
virtualization
Windows Registry

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Review Questions

1. Which of the following is NOT correct about JSON?
   - **a.** It stores data in a tree structure.
   - **b.** It is compact and easy to read and write.
   - **c.** It creates files that can be transmitted quickly.
   - **d.** It executes quickly.
2. Which of the following is NOT a common scripting language?
   - **a.** VBA
   - **b.** Bash
   - **c.** PowerShell
   - **d.** RegExBa
3. Which of the following is NOT a cybersecurity skill for which the CySA+ certification will equip the user?
   - **a.** Equip to demonstrate competency regarding current cyberattacks and defenses.
   - **b.** Equip to respond to threats, attacks, and vulnerabilities and then communicate with stakeholders.
   - **c.** Equip to configure a firewall.
   - **d.** Equip to proactively monitor and detect systems by analyzing indicators of malicious activity using the most up-to-date methods and tools.
4. What does the term "serverless" mean in cloud computing?
   - **a.** The cloud network configuration does not require any servers.
   - **b.** Server resources are inconspicuous to the end user.
   - **c.** Servers are run as VMs.
   - **d.** All appliances are virtual and do not interact with physical servers.
5. Which type of hypervisor runs directly on the computer's hardware?
   - **a.** Type I
   - **b.** Type II
   - **c.** Type III
   - **d.** Type IV
6. Which of the following is NOT correct about containers?
   - **a.** Containers start more quickly.
   - **b.** Containers reduce the necessary hard drive storage space to function.
   - **c.** Containers require a full OS whenever APIs cannot be used.
   - **d.** Containers include components like binary files and libraries.
7. Which of the following is NOT a characteristic of cloud computing?
   - **a.** Metered services
   - **b.** Delayed elasticity
   - **c.** On-demand self-service
   - **d.** Universal client support
8. Which of the following is NOT a cloud computing cost saving?
   - **a.** Reduction in broadband costs
   - **b.** Resiliency
   - **c.** Scalability
   - **d.** Pay-per-use
9. Which type of cloud is a combination of public and private clouds?
   - **a.** Joint
   - **b.** Combined
   - **c.** Hybrid
   - **d.** Consolidated
10. Which computing location would be used to support IoT devices?
    - **a.** Edge
    - **b.** Fog
    - **c.** Off-premises
    - **d.** On-premises
11. Which type of network segmentation makes use of virtual networks?
    - **a.** Full segmentation
    - **b.** Physical segmentation
    - **c.** Reverse segmentation
    - **d.** Logical segmentation
12. Which of the following is the most secure for administration of a DMZ?
    - **a.** DMZ-X
    - **b.** SAW
    - **c.** Jump server
    - **d.** Credential box
13. Which part of an SDN consists of one or more SDN servers and performs complex functions such as routing and security checks?
    - **a.** Data plane
    - **b.** Routing plane
    - **c.** Access plane
    - **d.** Control plane

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

14. What is the function of a SCADA?

a. Remove remote vulnerabilities.
b. Manage multiple ICSs.
c. Configure WAS-X.
d. Collect and monitor data from valves and pumps.

15. Which of the following is NOT a reason security for OT has been overlooked?

a. Separate IT-OT networks
b. Separate reporting structures
c. Lack of OT security focus
d. Reluctance to use substandard OT network protocols

16. Which of the following is a special category of OS processes responsible for managing memory allocations and hosting OS drivers?

a. Cores
b. Threads
c. System processes
d. Languages

17. Where are Apple macOS configuration files stored?

a. Registry
b. Folder in the .config directory
c. ectc/etc directory
d. Hierarchical database structure (HDS)

18. Which of the following is NOT a reason UEFI is an attractive attack target?

a. Simplicity
b. Persistence
c. Stealth
d. Difficulty patching

19. Which of the following provides the highest degree of security?

a. Secure Boot
b. Trusted Boot
c. Measured Boot
d. UEFI Native Boot

20. Which of the following is both a programming language and a scripting language?

a. Python
b. VBA
c. XML
d. JSXON

Case Projects

Case Project 1-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. What are your thoughts? How could the information regarding the type of security positions that are needed be better advertised? Should cybersecurity bootcamps be required to be more transparent regarding what their students can expect upon graduation? What other suggestions would you have for helping users understand cybersecurity jobs? Write a one-page paper about how to address the issues surrounding cybersecurity jobs.

Case Project 1-2: Lack of Knowledge by Job Applicants

Estimated Time: 25 minutes
Objective: Identify reasons for knowledge gaps by cybersecurity job applicants.
Description: A security research and training firm recently conducted a survey of more than 500 cybersecurity practitioners at 284 different companies in an effort to determine the skills they find most useful in cybersecurity job candidates. They also asked which of these skills are most frequently lacking. The survey asked respondents to rank various skills from "critical" to "not needed." Almost 85 percent ranked networking as a critical or "very important" skill, followed by a mastery of the Linux OS (77 percent) and Windows (73 percent). These were followed by common exploitation techniques (73 percent), computer architectures and virtualization (67 percent), and data and cryptography (58 percent). However, when asked the percentage of cybersecurity job candidates who were

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

unable to perform even basic tasks, the topic of computer architecture was only 47 percent, while networking was 46 percent. And when asked about the percentage of job candidates who demonstrated hands-on mastery, only 12.5 percent attained that level with computer architectures and virtualization, while only 4 percent could achieve that level with the topic of networking.

What are the reasons that computer architectures and virtualization are so important in cybersecurity? Why are the percentages of job candidates who cannot perform basic tasks or demonstrate hands-on mastery so low? How should this be addressed? What steps should be taken to integrate computer architectures and virtualization with cybersecurity to create a better foundation? Write a one-page paper with your suggestions.

Case Project 1-3: Container Security

Estimated Time: 25 minutes
Objective: Research how to protect containers.
Description: Containers are often targets of attackers. It is important to understand the attack surface of a container in order to ensure there is adequate detection and mitigation of the attacks. The risks to containers are categorized as follows:

- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Impact

Select any three of these risks and research them as they apply to containers. How can each risk be mitigated? Write a one-page paper on your research.

Case Project 1-4: Serverless Security

Estimated Time: 20 minutes
Objective: Research how to secure a serverless environment.
Description: Use the Internet to research serverless security. Compile a list of practices that can secure a serverless environment. Write a one-page paper on your research.

Case Project 1-5: SDN Vulnerabilities

Estimated Time: 25 minutes
Objective: Research vulnerabilities that can be found in an SDN.
Description: Use the Internet to research software-defined networking vulnerabilities. Compile a list of weaknesses that can compromise an SDN. Write a one-page paper on your research.

Case Project 1-6: U.S. Critical Infrastructures

Estimated Time: 25 minutes
Objective: Research CISA U.S. critical infrastructures.
Description: The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has identified 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Use the Internet to research the CISA critical infrastructures. Select one of the infrastructures and write a one-page report on it, including why it is designated as being critical, how a compromise of it could impact the nation, and how it should be protected.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong: Answers

Infrastructures and Architectures

1. On a VM the host system is the OS installed on the computer's hardware.
2. A Type I hypervisor runs on the host OS like an application.
3. A weakness of OT is that it is generally separate from IT networks.

Answer: The wrong statement is #2.
Explanation: A Type II hypervisor runs on the host OS like an application.

Software

1. Apple macOS uses a hierarchical database that contains configuration file information.
2. UEFI has replaced BIOS.
3. A regular expression is a special string of text for describing a search pattern.

Answer: The wrong statement is #1.
Explanation: Microsoft Windows uses a hierarchical database that contains configuration file information.

References

1. Mell, Peter, and Grance, Tim, "The NIST definition of cloud computing," *NIST Computer Security Division Computer Security Resource Center*. Oct. 7, 2009, accessed Apr. 2, 2011, http://csrc.nist.gov/groups/SNS/cloud-computing/.
2. "Overview of the Internet of things, Series y: Global information infrastructure, internet protocol aspects and next-generation networks – Next Generation Networks – Frameworks and functional architecture models," June 2012, accessed May 18, 2017, www.itu.int/ITU-T/recommendations/rec.aspx?rec=13607.
3. G., Nick, "How many IoT devices are there in 2023? [All you need to know]," *TechJury*, Feb. 7, 2023, accessed Feb. 11, 2023, https://techjury.net/blog/how-many-iot-devices-are-there/#gref.
4. Horowitz, Michael, "The head of NSA TAO advises on defensive computing for networks," *Computerworld*, Feb. 1, 2016, accessed May 11, 2017, http://www.computerworld.com/article/3028025/security/defending-a-network-from-the-nsa.html.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 2

Threat Actors and Their Threats

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Summarize the different categories of threat actors
2. Describe the techniques used by threat actors
3. Contextualize types of attacks
4. Articulate different vulnerabilities that result in successful attacks

#TrendingCyber

One of the least publicized—but by no means least threatening—types of attacks is bit flipping. Bit flipping has the potential to allow a low-privilege app to have administrative control on a system. This would permit it to install malware, access passwords, and even break out of a security sandbox.

Bit flipping involves manipulating a computer's dynamic random access memory (DRAM). The basic building block of DRAM is a memory storage cell. The cell consists of a capacitor and a transistor to store one single bit of data. When a bit is stored, the capacitor will either charge (to represent a 1) or discharge (to represent a 0) the transistor, so that a charged transistor represents 1, while a discharged transistor represents a 0.

A bit flip is exactly what it sounds like: A DRAM bit is flipped from 0 to 1 or vice versa from what was initially stored. This occurs when an unexpected flow of electrons within a transistor changes the voltage that then changes the bit. (Technically it occurs when an unexpected flow of electrons within a transistor's gates changes the voltage between the part of the circuit where the flow originates and where the flow is received.)

There are a number of different causes for bit flips; in fact, at least 31 different causes have been identified. These include power supply and capacitor issues, bad motherboard pin connections, incorrect DRAM timings, central processing unit (CPU) clock issues, bad CPU pin connections, signal integrity issues, and DRAM design flaws. In one instance, during a 2003 election in Belgium, cosmic rays from outer space were widely believed to have caused bit flips that gave a political candidate an additional 4,096 votes before they were identified and corrected. (The number 4,096, which can also be expressed as 2^12, suggests there was a bit flip in the 12th bit.)

In 2014, a method was discovered to force bit flips. Storage cells are organized into a rectangular array of rows and columns. These are arranged into banks to form the dual in-line memory module (DIMM), which is a rectangular "stick" that plugs into the computer motherboard. When a computer accesses memory, it opens the rows to the cells storing the desired data and transfers it to the CPU. However, a program can be written that causes the computer to repeatedly "hammer" a DRAM row by rapidly activating the same memory rows over and over. This is called a RowHammer attack (the row that gets hammered is the "aggressor row" and the row where bits are flipped is the "victim row").

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A RowHammer attack can induce bit flips in adjacent victim rows. This occurs because memory cells interact electrically with each other.

Soon security researchers discovered several other ways that threat actors could weaponize bit flipping to their advantage. One method called Double-Sided RowHammer offers more fine-grained control of bit flips by repeatedly hammering two aggressor rows at once to induce bit flips in nearby victim rows. This increased precision led to even more bit flip techniques, such as Flip Feng Shui, which could target sensitive data stored in cloud-hosting environments.

There is one key defense in DIMM against bit flipping. Error-correcting code (ECC) is built into memory by storing redundant control bits next to the data bits inside the DIMMs. CPUs can use this added data to quickly detect and repair flipped bits. However, ECC has been defeated in RowHammer attacks against older Double Data Rate (DDR) version 3 memory. As a fallback, modern DDR4 chips equipped with ECC typically provide another form of protection. Known as target row refresh (TRR), it monitors the number of times a row is accessed and, when a certain threshold is reached, it recharges neighboring rows that may have had their bits flipped as a result. However, an updated RowHammer attack devised in 2021 successfully defeated TRR protection as well.

Now a new technique called RowPress can also circumvent TRR. Unlike RowHammer in which one or more aggressor rows are accessed in rapid succession, RowPress can perform bit flipping by increasing the amount of time an aggressor row is left open (called tAggON) while at the same time raising the temperature of the DIMM. The result can be dramatic: Instead of requiring tens of thousands of activations to the aggressor row with RowHammer, RowPress can flip bits much more quickly, in as few as 10 to 100 attempts.

The impact of bit flipping for cybersecurity is very significant. In late 2023, security researchers demonstrated for the first time that a large portion of cryptographic keys used to protect data in computer-to-server traffic is vulnerable to compromise while the connection is being established. An error as small as a single flipped memory bit is all that it takes to expose a user's private key.

DRAM from all three major manufacturers is vulnerable to RowPress, even when equipped with the latest defenses of ECC and TRR. One of the manufacturers said that they are aware of "industry concerns around the latest DDR4 DRAM RowPress attack scenario and have been implementing measures in tandem with industry partners to counter such schemes."

Why are "horror" films so popular year after year? Research has shown that one of the primary reasons is that the filmmakers create the element of mystery, which then creates tension. Often the mystery is the identity of the villain: who is the person doing these things? Lighting, costumes, camera angles, and incongruous sounds all work together to create a mystery of who the adversary is. Often only the sounds of footsteps or a creaking door are all that is known about the villain's presence, with no indication of who they are or what they can do. This is designed to keep the audience on the edge of their seat. And research has even shown that after watching the film, moviegoers are already wondering about the mystery of the next sequel (assuming there is one).

While not knowing the villain makes for a great movie, the same cannot be said for cybersecurity. Being in the dark about who is attacking us and why can only result in the attacker's success. It is critical for cybersecurity professionals to know all they can about attackers, their motivations, and their techniques in order to create a strong defense.

Note 1

One security professional noted that there are no major sporting events today in which two teams playing for the championship do not know in advance who their opponent will be. This is because knowing your opponent in advance gives you time to study their strengths and weaknesses to craft a plan that leads to victory. Likewise, in the "competition" known as cybersecurity, it is important to know who the attackers are and how they attack.

In this chapter, you unravel the mystery surrounding the opponents in cybersecurity. You examine who the threat actors are, the tactics they use, and the types of attacks that they launch against vulnerabilities.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Who Are the Threat Actors?

Certification

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

In cybersecurity a **threat actor**, also called a malicious actor, is a term used to describe individuals or entities who are responsible for cyberattacks. The generic term "attacker" is also commonly used.

Note 2

In the past, the term "hacker" referred to a person who used advanced computer skills to attack computers. Yet this term was not always accurate, so it was then qualified in an attempt to distinguish between different types of hackers. For example, a white hat hacker, also known as an ethical attacker, would probe a system for weaknesses and then provide that information back to the organization. However, today "hacker" is considered pejorative and instead more accurate terms should be used.

The very first cyberattacks that occurred were mainly for the threat actors to show off their technology skills (fame). However, that soon gave way to threat actors with the goal of financial gain (fortune), which is the primary focus today. This financial cybercrime can be divided into three categories based on different targets:

- **Individual users.** The first category focuses on individuals as the victims. The threat actors steal and use stolen data, credit card numbers, online financial account information, or Social Security numbers to profit from their victims or send millions of spam emails to peddle counterfeit drugs, pirated software, fake watches, and pornography.
- **Enterprises.** The second category focuses on enterprises and business organizations. Threat actors attempt to steal research on a new product from an enterprise so that they can sell it to an unscrupulous foreign supplier who will then build an imitation model of the product to sell worldwide. This deprives the legitimate business of profits after investing hundreds of millions of dollars in product development and, because these foreign suppliers are in a different country, they are beyond the reach of domestic enforcement agencies and courts.
- **Governments.** Governments are also the targets of threat actors. If the latest information on a new missile defense system can be stolen, it can be sold—at a high price—to that government's enemies. In addition, government information is often stolen and published to embarrass the government before its citizens and force it to stop what is considered a nefarious action.

The attributes or characteristic features of the different groups of threat actors vary widely. Some groups have a high level of knowledge and skills along with a massive network of resources and funding. Others are "lone wolves" with minimal skills and no resources. And whereas most groups of threat actors are external to the enterprise, some may originate from within it.

Today threat actors are classified into distinct categories, such as script kiddies, organized crime, insiders, hacktivists, nation-state actors, and others. Each of these groups have varying motivations, or the reasons they attack.

Note 3

This listing of threat actors is in ascending sequence of least sophisticated to most sophisticated.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Script Kiddies

To the surprise of the average user, high technical skills and knowledge are not a required prerequisite to attack a system. Instead, easy-to-use attack tools are freely available or can be purchased at a low cost in order to perform sophisticated attacks. Figure 2-1 illustrates a current, widely available software package that allows for a sophisticated attack to be launched by simply making selections from a menu. Individuals who want to perform attacks yet lack the technical knowledge to conduct these attacks are sometimes called **script kiddies** or unskilled attackers.

Figure 2-1 Menu of attack tools



Source: Kali Linux

Note 4

Since the early days of cybersecurity, the term "script kiddies" was used to describe unskilled attackers since they downloaded freely available automated attack software called scripts to perform malicious acts.

Script kiddies use these types of tools to conduct their attacks. They can often be successful in penetrating defenses, particularly if the defenses are weak. Their motivation is usually data exfiltration (unauthorized copying of data) or service disruption (obstructing the normal business electronic processes).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Organized Crime

Organized crime is a close-knit group of highly centralized enterprises set up for the purpose of engaging in illegal activities. Organized crime is usually run by a small number of experienced criminal networks who do not commit crimes themselves but act as entrepreneurs. Historically these organizations have engaged in crimes such as the theft of cargo, fraud, robbery, kidnapping for ransom, and demanding "protection" payments. The income from these activities has enabled organized crime to supply goods and services that are illegal but for which there is demand, such as gambling, drugs, prostitution, and loansharking.

In recent years, there has been evidence that organized crime has moved into cyberattacks, which they consider to be less risky and more rewarding than traditional crimes. The motivation by organized crime is generally financial gain by earning revenue.

Insider Threat

Another serious threat to an enterprise comes from its own employees, contractors, and business partners, called insiders. Known as an **insider threat**, these individuals have the distinct advantage of attacking from the position of a trusted source. The threats that come from insiders can be either intentional or unintentional. A special category of unintentional insider threats is shadow IT.

Intentional Insiders

A senior research scientist at a large tech platform stole confidential information about the company's advertising platform product. The compromised data included 570,000 files containing source code, backend architecture information, secret algorithms, and other intellectual property (IP). This scientist downloaded this data to personal storage devices minutes after receiving a job offer from one of the company's competitors.

This researcher is an example of an **intentional insider**. Intentional insiders steal IP or manipulate data from the position of having a trusted relationship with the organization. There are several motivations behind intentional insiders. A healthcare worker, for example, who is disgruntled about being passed over for a promotion might illegally gather health records on celebrities and sell them to the media in retaliation. Or a securities trader who loses billions of dollars on bad stock bets could use their knowledge of the bank's computer security system to conceal the losses through fake transactions. Attacks by intentional insiders are usually harder to recognize than other types of attacks. That is because they come from within the enterprise while the normal cybersecurity defensive focus is watching for those who are on the outside.

Note 5

In recent years government insiders have stolen large volumes of sensitive information and then published it to alert its citizens of clandestine governmental actions.

Intentional insider attacks are on the rise and can often be as costly as attacks from the outside. About 60 percent of data breaches are caused by insider threats. A recent study revealed that the number of insider security incidents has risen by 47 percent since 2018, and the cost of insider threats has risen 31 percent in the same time period.

Unintentional Insiders

Often the exposure of critical corporate data is the result of **unintentional insiders**. Although there may be no malicious intent, due to their action—or inaction—unintentional insiders can unwittingly cause harm or create a vulnerability for an external threat actor to then exploit. The reasons for their actions range from carelessness, too much multitasking, low situational awareness, and a general disinterest in practicing strong cyber defenses. Almost two out of every three organizations found that a careless employee or contractor was the root cause of most insider incidents.

Note 6

Insider carelessness often involves the employee not considering the consequences of an action. For example, over half of all employees admit to allowing a friend or family member to use employee-issued technology equipment while at home, which could expose access to highly sensitive data such as the organization's proprietary information or private customer data.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

One of the most common unintentional insider actions is also one of the simplest to perform: incorrectly addressing email. Because modern email software will automatically complete the name of a contact person after the first two or three characters are entered into the address line, often unintentional insiders assume they have entered the correct "Pia_Romanelli@example.com," when in reality the email is being sent to "Pia_Rosellini@example.net" so that the email reaches the wrong recipient. While this can range from amusing to annoying, it can also be a serious breach if that email contains sensitive information that was sent to someone outside of the organization. It is estimated that of companies with at least 1,000 employees, there are on average 800 emails sent to the wrong recipient.

Caution !

Some emails contain a disclaimer such as, "This email may contain proprietary, business-confidential and/or privileged material. If you are not the intended recipient of this message, be aware that any use, review, retransmission, distribution, reproduction, or any action taken in reliance upon this message is strictly prohibited. If you received this in error, please contact the sender and delete the material from all computers." However, email disclaimers are not legally binding and thus carry no weight. This is because for a contract to be legally binding, both parties must agree to the terms.

Shadow IT

It is not uncommon for employees to become frustrated with the slow pace of acquiring technology at their workplace. Arcane forms must be completed, multiple levels of signatures must be secured, and unending back-and-forth emails with the information technology (IT) department negotiating what can be purchased cause even the most patient employees to throw up their hands and scream!

A cumbersome purchasing process that may take months before a single item of hardware or software can be acquired have pushed some employees to order the item online and pay for it with their own credit card, circumventing the enterprise's approval process. However well-intentioned the employee might be, they may actually purchase software that contains malware or connect their hardware to the corporate network, which creates a security vulnerability. The process of bypassing corporate approval for technology purchases is known as shadow IT.

Shadow IT is a serious cybersecurity problem. It is estimated that one-third of all successful thefts of corporate data by threat actors are from data stored on unapproved hardware or accessed through unapproved software purchased via shadow IT.[1] And 52 percent of survey respondents said that individual employees are purchasing software apps without IT's knowledge or consent, and 69 percent of tech executives reported that shadow IT is their top security concern.[2]

Hacktivists

A group that is strongly motivated by philosophical or political beliefs or ideology for the sake of their principles is **hacktivists** (a combination of the words *hack* + *activism*). Most hacktivists do not explicitly call themselves "hacktivists," but the term is commonly used by security researchers and journalists to distinguish them from other types of threat actors.

Attacks by hacktivists are often used to "make a statement." For example, they may break into a website and change the contents on the site (one hacktivist group changed the website of the U.S. Department of Justice to read "Department of Injustice"). Other attacks are retaliatory: Hacktivists have disabled the website belonging to a bank because that bank stopped accepting online payments that were deposited into accounts belonging to groups that were supported by hacktivists. Today many hacktivists work through disinformation campaigns by spreading fake news and supporting conspiracy theories, making their motivation to disrupt or cause chaos to produce extreme confusion.

Note 7

Hacktivists were particularly active during the COVID-19 pandemic of 2020. One large group of what were considered far-right neo-Nazi hacktivists embarked on a months-long disinformation campaign designed to weaponize the pandemic by questioning scientific evidence and research. In another instance, thousands of breached email addresses and passwords from U.S. and global health organizations, including the National Institutes of Health, Centers for Disease Control and Prevention, and World Health Organization, were distributed on X (formerly known as Twitter) by these groups to harass and distract these organizations.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Nation-State Actors

Instead of using an army to march across the battlefield to strike an adversary, governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes. These are known as **nation-state actors**. Their foes may be foreign governments or even citizens of its own nation that are considered hostile or threatening. The motivation for nation-state actors may be espionage or reacting to armed hostile combat.

Note 8

A growing number of attacks from nation-state actors are directed toward businesses in other countries with the goal of causing financial harm or damage to the enterprise's reputation.

Many security researchers believe that nation-state actors might be the deadliest of any threat actors. When fortune motivates a threat actor, but the target's defenses are too strong, the attacker simply moves on to another promising target with less-effective defenses. With nation-state actors, however, the target is very specific, and the attackers keep working until they are successful. This is because state-sponsored attackers are highly skilled and have enough government resources to eventually breach almost any security defense.

There are two types of attacks that are often attributed to nation-state actors. These are advanced persistent threats and supply-chain attacks.

Advanced Persistent Threat (APT)

Nation-state actors are often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. This has created a new class of attacks called **advanced persistent threat (APT)**. These attacks use innovative attack tools (advanced) and, once a system is infected, it silently extracts data over an extended period of time (persistent). APTs are most commonly associated with nation-state actors.

Supply-Chain Attacks

An attack often used by nation-state actors takes advantage of a weak supply chain, known as a **supply-chain attack**. A supply chain itself is a network that moves a product from its creation to the end user. This chain is typically made up of suppliers (the first step in the chain) that provide the raw materials, manufacturers who convert the material into products, vendors who purchase the products to resell them, warehouses that store products, distribution centers that deliver products to the retailers, and retailers who sell the product ultimately to the consumer. Today's supply chains are global in scope, as shown in Figure 2-2. This makes each link in the chain potentially thousands of miles away overseas and cannot be under any direct and coordinated supervision and monitoring. Thus, each link in a supply chain can be a point for an infection by threat actors.

A supply-chain attack can either be a hardware infection or software infection.

Hardware Supply-Chain Infection The fact that products like computer hardware move through many different steps in the supply chain has opened the door for malware to be injected into this hardware during its manufacturing, storage, and distribution. These are called hardware supply-chain infections.

Hardware supply-chain infections are considered especially dangerous. Users receiving infected devices at the point of purchase are completely unaware that a brand-new computer or network appliance may be infected. Also, there is rarely any means by which the user can be contacted to inform them of an infected device. Because it is virtually impossible to closely monitor every step in the global supply chain, these hardware supply infections cannot be easily prevented.

Software Supply-Chain Infection More recently software supply chains, which sources software from a software provider (the software developer and supplier) for delivery to an end user, have been the target of attackers. In one well-publicized attack, threat actors targeted a company that sold network and computer management software tools to enterprises. One tool had over 33,000 clients. Threat actors were able to access the provider's software development and distribution pipeline. They inserted malicious code into the software so that it would then be distributed to the software provider's clients as a software update. This single infection then spread exponentially to tens of thousands of clients, who then passed it on to their customers, too.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 2-2 Supply chain



Source: Golden Sikorka/Shutterstock.com

Other software supply-chain infections, instead of targeting the originating software provider (supplier), have focused on the downstream "middlemen" service providers (a business that furnishes solutions or services to end users and organizations). IT service providers who manage networks, computers, cloud resources, and information security typically for small-to-medium enterprises (SMEs) are called managed service providers (MSPs). An infected MSP can distribute malicious software to its many SME clients.

A particularly alarming type of software supply-chain infection targets open-source software, which is software for which the source code is available for anyone to freely use without restrictions. Open-source software is usually supported by volunteer contributors, and rarely are the contributions vetted. This makes for an ideal situation for threat actors to add their malicious code to an open-source project, which is then downloaded and installed by many unsuspecting victims.

Note 9

The risks associated with supply-chain vulnerabilities can be seen in an incident in late 2021. The open-source software Log4j is used to log security and performance information. It is found in a wide variety of consumer and enterprise services, websites, and applications as well as in operational technology products. A vulnerability was discovered in Log4j on a Friday that resulted in over 100 attacks per minute. By Monday, just 72 hours later, over *1.2 million* attacks had been launched taking advantage of this single vulnerability.[3]

Other Threat Actors

In addition, there are other categories of threat actors. These are summarized in Table 2-1.

Often the perception of an attacker by the general public is a "hacker in a hoodie" who is a disgruntled teenager looking for an easy target. Nothing could be further from the truth. Threat actors today generally have excellent technology skills, are tenacious, and have strong financial backing. Attackers have even modeled their work after modern economic theories (such as finding the optimum "price point" in which victims will pay a ransom) and software development (attack tools that threat

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 2-1 Descriptions of other threat actors

Threat actor	Description	Explanation
Competitors	Launch attack against an opponents' system to steal classified information.	Competitors may steal new product research or a list of current customers to gain a competitive advantage.
Brokers	Sell their knowledge of a weakness to other attackers or governments.	Individuals who uncover weaknesses do not report it to the software vendor but, instead, sell them to the highest bidder, who are willing to pay a high price for the unknown weakness.
Cyberterrorists	Attack a nation's network and computer infrastructure to cause disruption and panic among citizens.	Targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.

actors sell are often software suites that receive regular updates). It is a serious mistake to not be aware of the different types and motivations of threat actors, which leads to an underestimation of the risks that they pose.

Note 10

The famous Chinese military strategist Sun Tzu said over 1,500 years ago in *The Art of War*, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Two Rights & A Wrong

1. Script kiddies are also called unskilled attackers.
2. A special category of intentional insider threats is shadow IT.
3. Nation-state actors may attack foreign governments or even the citizens of their own nation.

See the answers at the end of the chapter.

Threat Actor Actions

Certification

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

Just as the types of threat actors vary significantly, so do their actions. Threat actor behaviors can be classified as tactics, techniques, and procedures. Their actions can also be categorized as either known or unknown threats.

Tactics, Techniques, and Procedures (TTP)

The term **tactics**, **techniques**, **and procedures (TTP)** describe the behavior or actions of a threat actor in a cascading sequence:

- **Tactics.** A tactic is a high-level description of the actor's behavior in order to achieve their planned attack. It is the "why" the attack occurs. An example of a tactic is to gather personal information to sell to other actors.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Techniques.** Techniques give a more detailed description of behavior within the context of a tactic. Techniques are the intermediate methods or tools a threat actor uses to breach defenses by providing a more detailed description of the tactic. It describes the "what" of the attack, such as using malware or launching a phishing attack.
- **Procedures.** Procedures are a lower-level and highly detailed description of the actions of a technique. Procedures are what actors follow to achieve their goals. It describes "how" they will achieve their desired result. An example of a procedure are the detailed steps for exploiting an email server vulnerability in order to achieve a privilege escalation.

Note 11

Looking at TTP from the "bottom up," procedures are the sequence of actions performed using a technique in order to execute a tactic.

TTPs describe what threat actors do and how they will do it. This gives the opportunity for security professionals to proactively develop a broader contextual understanding across different incidents, threat actors, and campaigns. TTPs can define instances including the targets of the attack (such as the human resources representatives of finance companies), the attack patterns, and the details of the attack.

TTPs should not be confused with the evidence of an attack that is occurring. The evidence has been compared to the "breadcrumbs" that security professionals may see on a network or operating system (OS) that indicates an attack is occurring. When an attack is detected, the evidence will launch incident-response activities to protect valuable systems from threat actors. TTPs give the security team the background information they need to protect all possible attack paths.

Note 12

If threat actors were bank robbers, TTPs would be the strategies used to get inside the vault, while evidence would be what can be seen that indicates they are there, such as a smashed lock on the floor.

Known and Unknown Threats

At a U.S. Department of Defense (DoD) news briefing in 2002, the Secretary of Defense Donald Rumsfeld was asked a question regarding the lack of evidence linking a foreign government with the supply of weapons of mass destruction to terrorist groups. Secretary Rumsfeld responded:

> "Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones."[4]

Secretary Rumsfeld's statement is considered the first time the general public was exposed to the concept of "known knowns," "known unknowns," and "unknown unknowns." However, national security and intelligence professionals had for several years used a similar approach based on an analysis technique created in the mid-1950s. This technique was developed to help individuals understand their relationship with others and themselves. This is called the Johari window and is shown in Figure 2-3.

Note 13

At the time that Secretary Rumsfeld made his comments, he was criticized because some individuals felt that they did not make sense and were an unnecessarily complex way of explaining the issues around security intelligence. However, as time passed, his observation was considered insightful.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 2-3 Johari window

	Known to self	Unknown to self
Known to others	**Open** Things that are known by you and seen and acknowledged by others	**Blind** Things that are unknown by you but seen and acknowledged by others
Unknown to others	**Hidden** Things that are known by you but unknown by others	**Unknown** Things that are unknown by you and by others

Today cybersecurity professionals have adopted the Johari window as one means of classifying cybersecurity threats, particularly known threats or unknown threats, or classifying threats comparing the knowledge of the threat actor to security personnel. Figure 2-4 applies the Johari window to cybersecurity threats.

Figure 2-4 Johari window cybersecurity threats

	Known to self	Unknown to self
Known to others	**Open** Published vulnerabilities and attacks	**Blind** Security exploits only known to threat actors
Unknown to others	**Hidden** Internal security vulnerabilities not detectable from outside	**Unknown** Vulnerabilities not yet discovered by threat actors or security researchers

The four categories of these threats are:

- **Known knowns.** These are threats that both threat actors and security personnel are aware of, such as a virus that has been active for several years. The defense against these is established technologies and devices such as antivirus solutions and firewalls.
- **Known unknowns.** Known unknowns refer to vulnerabilities that the organization is aware of in their systems but outside threat actors have not discovered. A defense against these are actions taken by the organization to address the vulnerabilities.
- **Unknown knowns.** These are threats that are known to threat actors but not to security professionals. Often called zero-day attacks, these are unknown vulnerabilities and give victims no time (zero days) to prepare or defend against the attacks. There is no defense strategy against unknown knowns.
- **Unknown unknowns.** Unknown unknowns are security threats that are currently hidden from both threat actors as well as security professionals. There is no indication when—or if—they will be found. Like unknown knowns, there is no specific defense against these.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 14

Although the Johari window is a common means of classifying threats, there are others as well.

Two Rights & A Wrong

1. Procedures in TTP are a lower level and highly detailed description of the actions of a technique.
2. Known unknowns are vulnerabilities that the organization is aware of but threat actors have not yet discovered.
3. By definition, unknown unknowns are not possible.

See the answers at the end of the chapter.

Types of Attacks

Certification

1.2 Summarize fundamental security concepts.

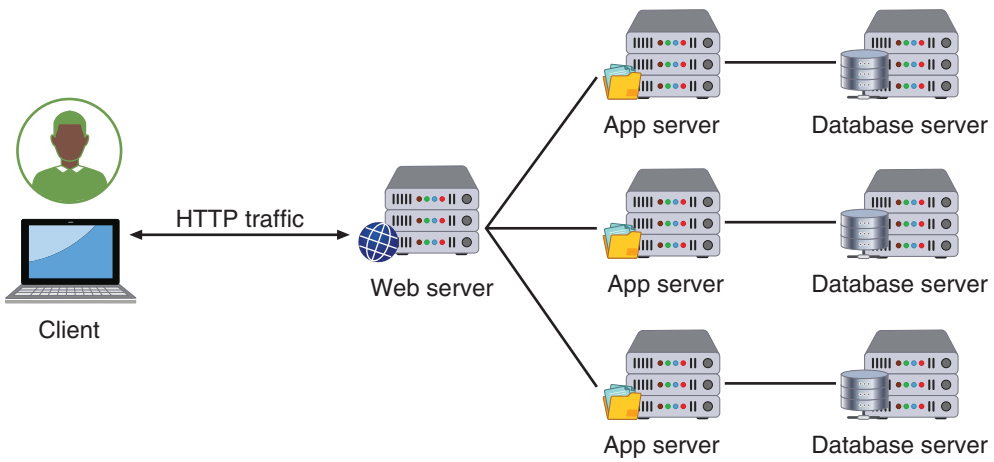
2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.

There are a variety of different types of attacks that come from threat actors. Some of the most common include web server application attacks, remote code execution, data poisoning, and obfuscated links.

Web Server Application Attacks

A web server provides services that are implemented as web applications through software programs running on the server. A typical web application infrastructure is shown in Figure 2-5. The client's web browser makes a request using the Hypertext Transport Protocol Secure (HTTPS) to a web server, which may be connected to one or more web app servers. These application servers run the specific web apps, which in turn are directly connected to database servers on the internal network. Information from these database servers is retrieved and returned to the web server so that the information can be sent back to the user's web browser.

Figure 2-5 Web server application infrastructure



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A web application infrastructure is a tempting target for attackers for multiple reasons:

- A successful compromise could impact all web users who access the web server.
- An attack could provide a pathway into the enterprise's network infrastructure.
- The multiple elements in a web application infrastructure provide for a range of vulnerabilities that can be used as different attack vectors.

Common web server application attack categories are request forgery and cross-site scripting attacks. In addition, directory traversal is another common attack.

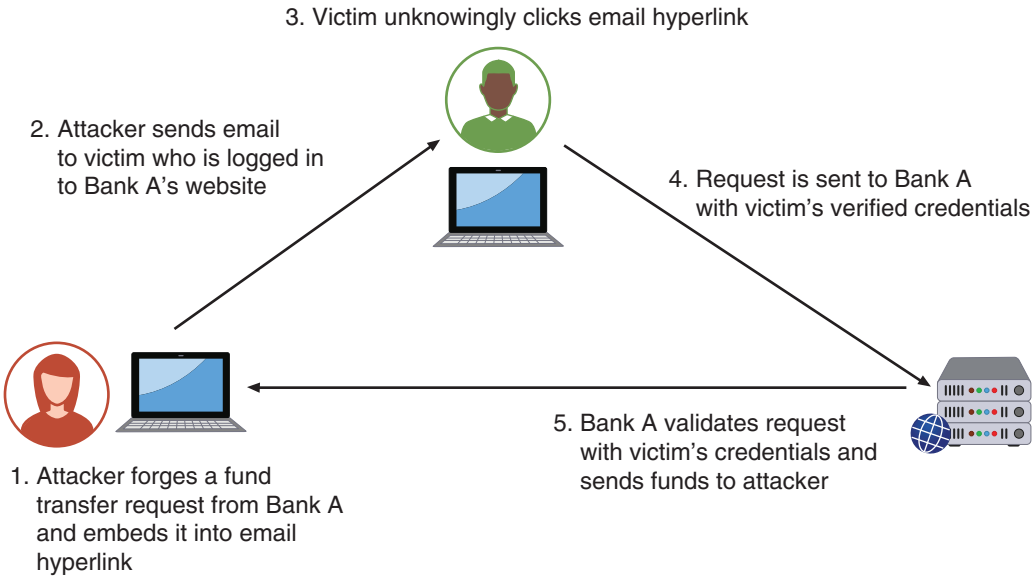
Request Forgery

As its name suggests, a "request forgery" attack is a request that has been fabricated (a "forgery"). There are two types of request forgeries. These are a cross-site request forgery (CSRF) and a server-site request forgery (SSRF).

Cross-Site Request Forgery (CSRF) A **cross-site request forgery (CSRF)** takes advantage of an authentication "token" that a website sends to a user's web browser. If a user is currently authenticated on a website and is then tricked into loading another webpage, the new page inherits the identity and privileges of the victim, who may then perform an undesired function on the attacker's behalf. In other words, in a CSRF attack, a *request* to a website is not from the authentic user but is a *forgery* that involves *crossing sites*.

Figure 2-6 illustrates a CSRF. Because a CSRF takes place on the client site, it is sometimes called a client-side request forgery.

Figure 2-6 Cross-site request forgery



Server-Side Request Forgery (SSRF) A **server-side request forgery (SSRF)** takes advantage of a trusting relationship between web servers (as opposed to a CSRF, which manipulates the trust from a user's browser to a server). SSRF attacks exploit how a web server processes external information received from another server. Some web applications are designed to read information from or write information to a specific uniform resource locator (URL). If an attacker can modify that target URL, they can potentially extract sensitive information from the application or inject untrusted input into it. Table 2-2 outlines the differences between a CSRF and a SSRF.

Table 2-2 CSRF and SSRF differences

Attack name	Attack target	Purpose of attack
CSRF	User	Force target to take action for attacker while pretending to be authorized user.
SSRF	Web server	Gain access to sensitive data or inject harmful data.

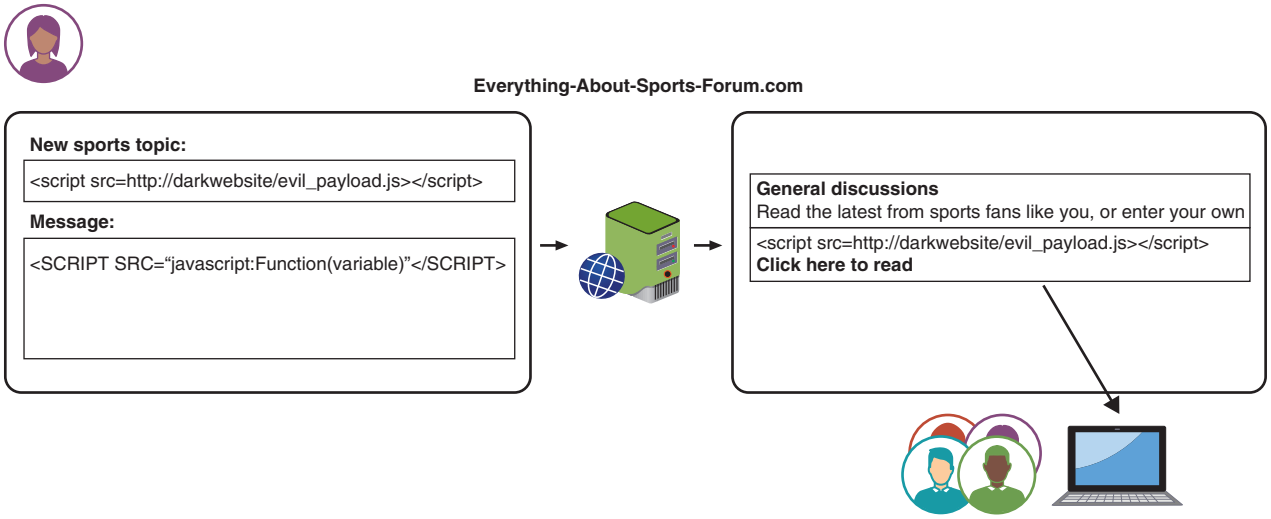
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Cross-Site Scripting

Most websites accept some type of user input, such as visitor comments, web-based collaborations, search terms, and so on. The underlying web applications then use the input from users to create dynamic display content. For example, a user could enter CENGAGE into a search box and then a webpage displays back to the user "You are searching for: CENGAGE." Or a user could enter a new topic about a recent player trade on a sports web forum that would then be displayed to subsequent users who access that same topic in the forum.

Threat actors can take advantage of this user input and display in a **cross-site scripting (XSS)** attack. The term "cross-site scripting" refers to an attack using scripting that originates on one site (the web server) to impact another site (the user's computer). XSS is essentially a client-side code injection attack using a web application. An attacker attempts to execute malicious scripts in the victim's web browser but not by directly injecting it into the user's web browser. Rather, the attacker inputs that malicious code on a website that accepts user input. The underlying web application that accepts the malicious code then becomes the vehicle to deliver the malicious script to every user's browser when they access that site. An XSS attack is shown in Figure 2-7.

Figure 2-7 XSS attack



Caution

Malicious code in an XSS attack can be executed in the user's browser through VBScript, ActiveX, and even Cascading Style Sheets (CSS). However, it is most commonly executed in JavaScript because this is fundamental to most browsing experiences. Although web browsers run JavaScript in a very tightly controlled environment with limited access to the OS and file system, it still has the potential to be misused by malware.

In order for a threat actor to launch an XSS attack, the attacker must identify a web application that accepts user input without validating it (called sanitizing) and then uses that input in a response back to the user. There are three main types of XSS attacks. These are summarized in Table 2-3.

A threat actor who controls a script that is executed in the victim's browser through XSS could fully compromise that user. The attacker can:

- Initiate interactions with other application users, including malicious attacks, that appear to originate from the trusted victim.
- Modify any information that the user is able to modify.
- Perform any action within the application that the user can perform.
- View any information that the user is able to view.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 2-3 Types of XSS attacks

Name	Description	Comments
Reflected XSS	A user enters input into a web application that is then immediately displayed back ("reflected") to initiate the attack.	The simplest form of XSS attack.
Persistent XSS	A threat actor enters input into a blog post or forum that is stored ("persistent") and an unsuspecting user later displays it to initiate the attack.	Also called stored XSS or second-order XSS.
Document Object Model XSS	A web application writes data to the Document Object Model on the web server without proper sanitization and the attacker can manipulate this data to include XSS content on the webpage.	The Document Object Model is a convention used to represent and work with objects in an HTML document (and other document types).

Directory Traversal

Web-based attacks frequently result in **directory traversal**. The "root" directory is a specific directory on a web server's file system, and users who access the server are usually restricted to the root directory and directories and files beneath the root directory, but they cannot access other directories. A directory traversal attack takes advantage of a vulnerability so that a user can move from the root directory to other restricted directories, viewing confidential files or entering commands to execute on the server.

Remote Code Execution (RCE)

Remote code execution (RCE) occurs when a threat actor accesses a target device to make changes to it. Because this is done through a network connection instead of physically—that is, the threat actor is not sitting at the device making changes—it is called "remote" execution.

Once threat actors have remotely accessed a device, the next step is typically to attempt a **privilege escalation**. Privilege escalation allows the attacker to gain illicit access to elevated rights or privileges beyond what is entitled for the user. Privilege escalation can be either horizontal (gaining access to rights of another account with similar privileges) or vertical (increasing the elevation of rights).

Once elevated privileges have been attained, then threat actors use this ability to execute code (malware) on the device to make it under their control. Attackers can then exfiltrate data from that device, perform network reconnaissance, or launch other attacks such as denial-of-service (DoS) or ransomware attacks.

Note 15

The Log4j attack mentioned previously provided threat actors with RCE over devices. A Log4j feature allows users to enter custom code in a log message. The vulnerability in Log4j allowed threat actors to inject malicious code for the log messages that Log4j then processed as instructions.

Data Poisoning

For hundreds of years armies at war have resorted to "well poisoning" against their enemies. As its name implies, well poisoning is a malicious act to contaminate resources of potable water used for drinking and food preparation. Well poisoning has been used both offensively (as a terror tactic to disrupt and depopulate an area) and defensively (as a "scorched earth" tactic to deny an invading army sources of clean water). Rotting animal corpses have been thrown down wells to pollute the water and, in extreme cases, human corpses known to have died from deadly transmissible diseases such as bubonic plague or tuberculosis were used in well poisoning.

In a similar fashion, threat actors use **data poisoning** to contaminate the data that is used in cybersecurity to identify an attack. For example, a defensive system can be used to detect unusual network traffic that could indicate suspicious activity. In a data poisoning attack, an attacker could slowly introduce their own "fake" data points seen as permissible activity in order

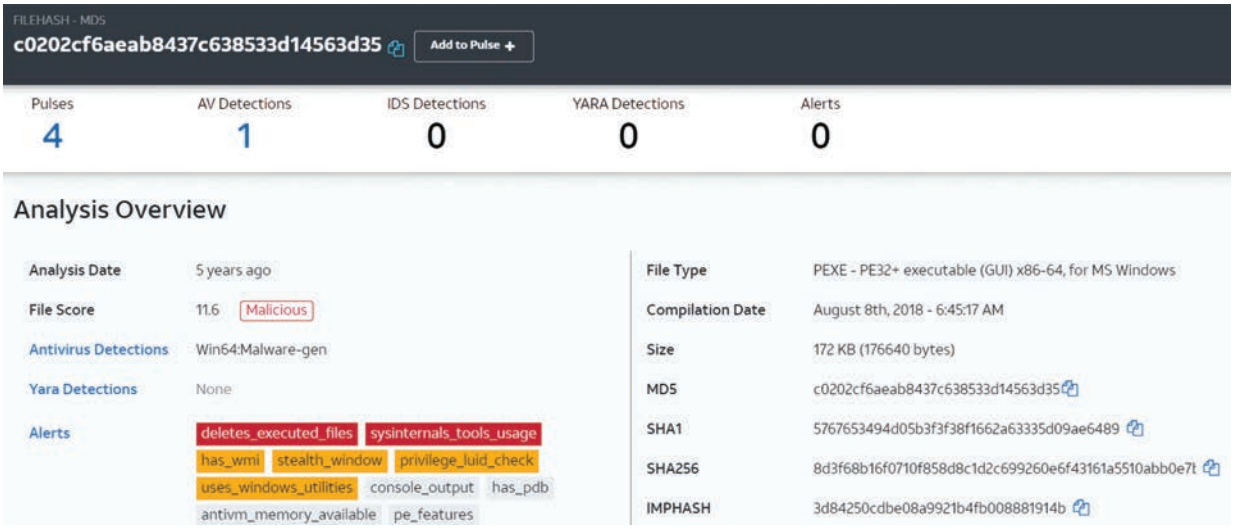
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

to decrease the accuracy of the system. Over time the system will eventually see the attacker's activity as permissible and will not flag it as suspicious.

Data poisoning attacks have often been conducted against spam filters used by email providers. Email systems regularly detect advanced spammer groups trying to "throw off" email filters. This can be accomplished by the spammers reporting to the filters massive amounts of spam emails as NOT SPAM in large-scale attempts to skew the spam classifier.

Another example involves online scanning services. Users can submit suspicious files to detect if they contain malware, as seen in Figure 2-8. Attackers have uploaded benign or harmless samples that have been falsely tagged by the threat actors as malicious. Anti-malware software vendors then download these results to update their own systems. However, the anti-malware software then reports these benign files as infected when in reality they are not, thus damaging the user's trust in the antimalware even to the point of turning it off.

Figure 2-8 Online scanning service



Source: Alienvault

Data poisoning is difficult to detect. The data models that are used to create attack profiles must periodically be retrained with newly collected data at certain intervals, depending on their intended use and their owner's preference. Since data poisoning usually happens over time through multiple training cycles, it can be detected when any prediction accuracy begins to shift.

Obfuscated Links

Not all attacks rely on technology vulnerabilities; in fact, most cyberattacks today rarely exploit a technology weakness as the initial first step. Instead, they start with social engineering. **Social engineering** is a means of eliciting information or convincing a user to take action that weakens security. Social engineering is almost always performed through deception and manipulation of the user. Because social engineering occurs through the exploitation of a person, it is sometimes said to be accomplished using "human vectors" as the attack surface.

Note 16

One reason most cybersecurity attacks are successful today is because they start with highly successful social engineering attacks, which then open the door for the next steps in the attack. It is estimated that cybercriminals use social engineering in 98 percent of their attacks.[5]

A growing trend in social engineering attacks is an attack that uses **obfuscated links**. To "obfuscate" is to render something obscure, unclear, or unintelligible. Threat actors craft deceptive URLs, which are the link addresses of a given resource on the web, to trick the user into thinking they are valid or secure links.

There are several techniques for hiding the destination of URLs in a web browser so that an unsuspecting user does not know where a URL will actually redirect them. One of the simplest techniques is to use the HTML attribute "a href." The HTML code * Your Bank *, instead of displaying "attacker_site.com," will display "Your Bank."

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Redirecting users to another resource or website but not displaying that destination URL in their web browser is known as stealth redirection. Another technique is to use a URL shortener. These online tools convert a longer URL (https://www.cengage.com/student/etextbooks/) to a shorter version (https://shorturl.at/mBLU0). Because this shorter version gives no indication of the destination, threat actors often mask their websites with a URL shortener.

Note 17

Stealth redirection is commonly performed using an iframe tag or an Apache rewrite directive.

While these techniques can hide a URL in a web browser, more advanced techniques are often used by threat actors to obfuscate URLs. There are three primary means by which obfuscated links are crafted today:

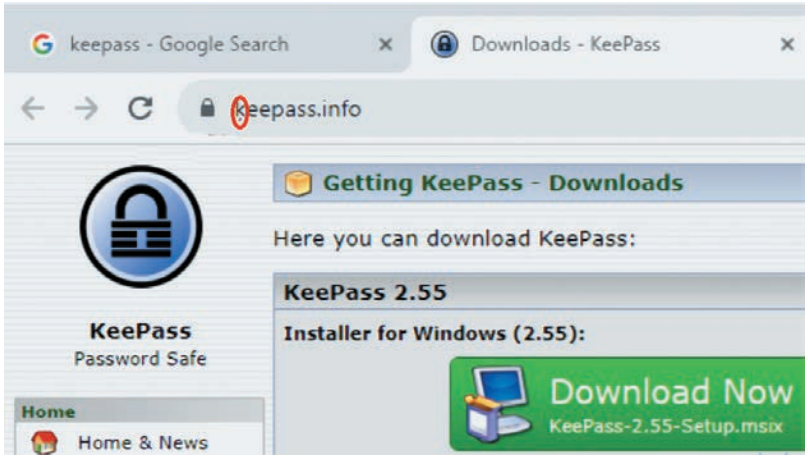
- **Manipulate the @ symbol.** The standard format of an HTTP URL is *http://<host>:<port>/<path>?<searchpart>*. Because no username (such as "anthonio" in anthonio@example.com) is allowed as part of a URL, when a browser interprets a URL with an @ symbol, it discards everything before the symbol—but then sends the request to the web resource following the @ symbol. The URL google.com@1157586936 treats google.com as a username and discards it, then sends the request to 1157586936, the decimal Internet Protocol (IP) address of a web resource.
- **Use alternative hostname formats.** In the previous example, 1157586936 may generate suspicion since it is rare for a server IP address to be depicted as an integer. To obfuscate 1157586936 even more, it could be displayed in an alternative hostname format such as google.com@0xC0.0xA8.0x0.0x1 (hexadecimal), google.com@0300.0250.0000.0001 (octal), or google.com@0300.0250.0000.0001 (mixed).

Caution !

By using obfuscated links, threat actors can create URLs such as your.bank.com@loginportal.onlinebanking.orly/loginPortal.php to redirect unsuspecting users.

- **Obfuscate with punycode.** Punycode is a representation of Unicode using the more limited American Standard Code for Information Interchange (ASCII) character subset. Punycode allows hostnames containing Unicode characters to be transcoded to ASCII. However, when transcoding characters from another alphabet, these unique characters may not be noticed. A recent attack using punycode is shown in Figure 2-9. While the URL at first glance appears normal, upon closer inspection the letter *K* is actually a different character altogether of *Ķ* (k-cedilla, the 17th letter of the Latvian alphabet that appears in ASCII with a comma beneath it). This obfuscated URL (Ķeepass.info) is completely different than the secure URL (Keepass.info) and clicking it will redirect the user to an imposter website.

Figure 2-9 Punycode obfuscation



Source: KeePassXC Team

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong

1. In an SSRF attack, a request to a website is not from the authentic user but is a forgery that involves crossing sites.
2. XSS is a client-side code injection attack using a web application.
3. In a data poisoning attack, threat actors contaminate the data that is used in cybersecurity to identify an attack.

See the answers at the end of the chapter.

Vulnerabilities

Certification

2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.

Attacks by threat actors are possible because of vulnerabilities that they exploit. No vulnerabilities, no successful attacks. Some vulnerabilities are the result of simply failing to properly configure the security protections that are available in hardware and software (**security misconfigurations**) while other vulnerabilities are more complex. Vulnerabilities can be grouped into programming vulnerabilities, broken access control, cryptographic failures, dated components, and identification and authentication failures.

Programming Vulnerabilities

There are many vulnerabilities that can be traced back to poor programming practices. Typical programming vulnerabilities include file inclusion vulnerabilities and overflow vulnerabilities. These can often be attributed to insecure program design.

File Inclusion Vulnerabilities

PHP is a widely used, open-source, general-purpose scripting language that is especially suited for web development. Over three out of every four websites use PHP. PHP scripts can even be embedded into HTML, with the embedded code enclosed in special start and end processing instructions (*<?php* and *?>*).

What distinguishes PHP from client-side code like JavaScript is that the PHP code is executed on the server, generating HTML, which is then sent to the client. The client receives the results of running the script but does not know what the underlying code is.

PHP code can also invoke files so that the instructions in these files can be executed. However, this file inclusion can be a security flaw in web applications, allowing unauthorized users to access confidential files, perform unauthorized downloads, search for protected information, and so on. The file inclusion vulnerability allows an attacker to include (access) their own malicious file.

There are two types of file inclusion vulnerabilities. Using a **local file inclusion (LFI)** vulnerability, the attacker first manipulates the PHP code to point away from an approved file on the web server to the attacker's own file that has been uploaded to that server. For example, a snippet of a vulnerable PHP code that could lead to LFI is *https://example.com/?page=good_file.php*. If the attacker can change the code to point to the file that they have uploaded (*https://example.com/?page=bad_file.php*) then the contents of this malicious file can be executed. A **remote file inclusion (RFI)** vulnerability allows the threat actor to access a file stored on a different server other than the server running the code.

The main cause for LFI and RFI vulnerabilities is improper input validation. Code should be written to ensure the input received is properly sanitized before allowing it to pass to an include function.

Note 18

RFI can also be mitigated by disabling the remote inclusion feature by setting the allow_url_include to 0 in the PHP configuration or disable the allow_url_fopen option to control the ability to open, include, or use a remote file.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

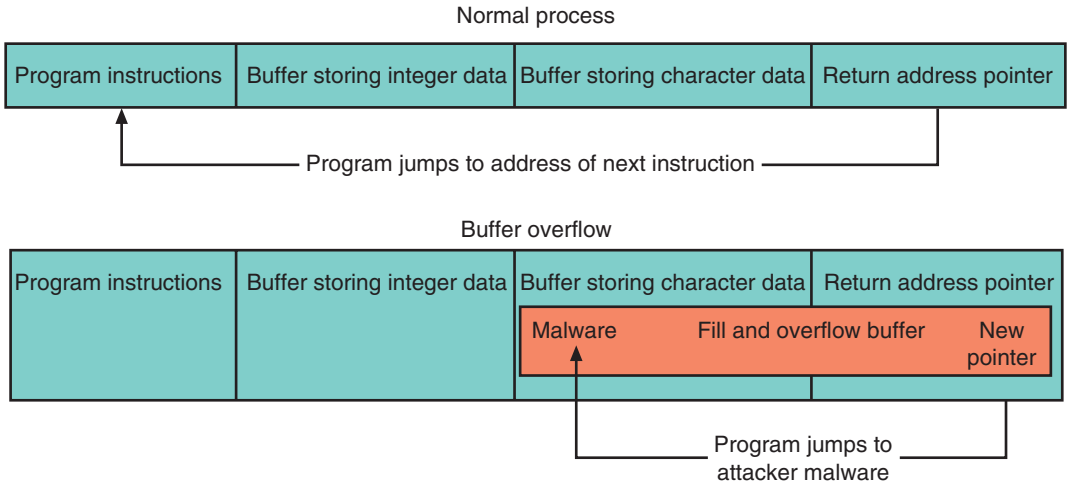
Overflow Vulnerabilities

Several attacks are directed at vulnerabilities associated with how a program uses random access memory (RAM) and are often the result of poor techniques (or laziness) by the software developer. Some memory-related attacks attempt to manipulate memory contents by inserting content. Because these attacks "inject" the vulnerabilities, they are sometimes called **injection flaws**. These types of attacks include buffer overflow attacks and integer overflow attacks.

Buffer Overflow A storage buffer on a computer typically contains the memory location of the software program that was being executed when another function interrupted the process; that is, the storage buffer contains the "return address" where the computer's processor should resume once the new process has finished. An attacker can substitute their own "return address" in order to point to a different area in the computer's memory that contains their malware code.

A **buffer overflow attack** occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer. This extra data overflows into the adjacent memory locations (a buffer overflow). Because the storage buffer typically contains the "return address," an attacker can overflow the buffer with a new address pointing to the attacker's malware code. A buffer overflow attack is shown in Figure 2-10.

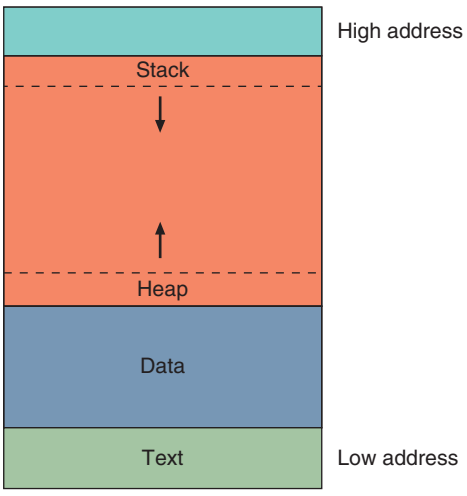
Figure 2-10 Buffer overflow attack



A buffer overflow attack can occur in one of two areas of computer memory. Memory is divided into four areas, as shown in Figure 2-11. These areas are:

- **Data.** This area stores global variables that are separated into initialized and uninitialized variables.
- **Heap.** The heap is dynamic memory for the programmer to allocate as necessary.
- **Stack.** The stack stores local variables that the program uses.
- **Text.** Text stores the code that is being executed.

Figure 2-11 Computer memory areas



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Each byte of computer memory has a unique address, beginning with zero (low address) to the largest possible address (high address). The stack area is near the top of the memory with high addresses. Whenever a function is called by a computer program, a portion of stack memory is allocated. When new local variables are declared, more stack memory is automatically allocated. These allocations make the stack grow "down" (from higher memory addresses to lower addresses). The heap area is allocated explicitly by the program and grows "up" (from lower addresses to higher addresses); it is not deallocated (freed) until the program explicitly mandates it. Because buffers are found in both the stack and heap areas, a buffer overflow attack can occur in either the stack (a **stack overflow**) or the heap (a **heap overflow**).

Integer Overflow An integer overflow is the condition that occurs when the result of an arithmetic operation—such as addition or multiplication—exceeds the maximum size of the integer type used to store it. When this integer overflow occurs, the interpreted value then wraps around from the maximum value to the minimum value. For example, an eight-bit signed integer has a maximum value of 127 and a minimum value of –128. If the value 127 is stored in a variable and 1 is added to it, the sum exceeds the maximum value for this integer type and wraps around to become –128.

In an **integer overflow** attack, an attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow. An attacker could use this type of attack to create a buffer overflow. If an integer overflow could be introduced during the calculations for the length of a buffer when a copy is occurring, it could result in a buffer that is too small to hold the data. Another example is a large positive value in a bank transfer could be wrapped around by an integer overflow attack to become a negative value, which could then reverse the flow of money; instead of adding this amount to the victim's account, it could withdraw that amount and later transfer it to the attacker's account.

Note 19

An extreme example of an integer overflow attack would be withdrawing $1 from an account that has a balance of 0, which could cause a new balance of $4,294,967,295!

Insecure Design

Programming vulnerabilities are not always the result of poor coding practices; they are often the result of a poor design of the program's logic and implementation that does not properly take into account cybersecurity protections. This is known as **insecure design**. Insecure design is considered a broad category that includes different program weaknesses that are due to missing or ineffective control design.

It should be noted that there is a difference between insecure design and insecure implementation of a program. This is because there are different root causes and remediations. A secure design can still have implementation defects that create vulnerabilities that may be exploited. However, an insecure design cannot be fixed by an improved (or even perfect) implementation. This is because the necessary security controls are missing from the design: they were never created to defend against specific attacks.

Note 20

Insecure designs are architectural flaws within the program itself that cannot be fixed by a simple software patch.

Broken Access Control

Access control enforces restrictions so that users cannot act outside of their intended permissions. **Broken access control** is a vulnerability that allows unauthorized users to access sensitive data or systems by circumventing security procedures. This typically occurs when authentication and authorization controls are not properly implemented or enforced, allowing attackers to gain illegitimate elevated privileges.

Broken access control can be the result of a wide range of vulnerabilities. One common category of vulnerabilities is related to application programming interfaces (APIs). An API is a link provided by an OS, web browser, or other platform that allows a developer access to resources at a high level. APIs provide direct access to data and an entry point to an application's functions. Often controls that should restrict access via APIs are weak or missing, resulting in broken access control. For example, APIs

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

with missing access controls for POST (send data to the server and create a new resource), PUT (update an existing resource), and DELETE (delete a resource) commands are common attack vectors.

Note 21

Broken access control should first be addressed by following basic cybersecurity best practices. For example, it is important to specify the degree of access permitted for each resource while denying all access by default to any resource that is not intended to be shared with the general public.

Cryptographic Failures

The phrase "cryptographic failures" may seem to imply that cryptographic algorithms are like OS software that contains numerous vulnerabilities just waiting to be exploited. This is not the case. Modern cryptographic algorithms are reviewed, tested, and vetted by specialists in cryptography over several years before they are released to the public for use.

Consider the recent competition for a new cryptographic algorithm presided over by the National Institute of Standards and Technology (NIST). Initially 82 algorithm submissions from all over the world were submitted, and 69 were considered robust enough to be a Round 1 candidate. After two more years of analysis, only 26 proposals advanced to Round 2, and eventually seven were announced as Round 3 finalists. Yet despite the ongoing rigorous testing, at least four of the Round 3 finalists were discovered to have flaws—just months before NIST was to make its final decision.

Note 22

One security professional likened the competition to a "demolition derby" in which only one algorithm will survive. This is important because the goal is to uncover weaknesses before an algorithm is released to the general public.

Although the cryptographic algorithms and structures may be considered secure, the improper implementation of cryptography can severely weaken it. This is known as a **cryptographic failure**. Examples of cryptography failure include:

- Improper key management
- Not validating server certificates and the trust chain
- Transmitting external data without using encryption
- Using deprecated hash functions (such as MD5 or SHA1) or weak cryptographic algorithms or protocols either by default or in older code
- Using passwords as cryptographic keys instead of a password base key derivation function

Dated Components

New hardware and software are introduced regularly that contain both new features as well as stronger security. The older features are then considered as no longer current (**outdated components**) and are eventually no longer supported (**end-of-life component**). However, not all users immediately upgrade to the latest hardware and software so that there is a mix of new and old technologies.

In order to support these older technologies, hardware and software often include backward compatibility so that a newer version can still function with the older version. However, in most instances, this means that the newer version must revert to the older and less secure version.

In a downgrade attack, an attacker leverages dated components. The attacker forces the system to abandon the current higher security mode of operation and instead "fall back" to implementing an older and less secure mode. This then allows the threat actor to attack the weaker mode.

Identification and Authentication Failures

The very foundation of security is restricting access to unknown entities while providing admittance to those who have been approved; in other words, it is "keeping the bad guys out while letting the good guys in." Today virtually every system and device first require some type of unique digital identity to be provided by the requester (a user, device, or system) before access is

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

granted. This identity serves to differentiate the requester from all other users. But it also requires the requester to provide proof that they are this unique user. This identity proofing is more commonly called authentication, which is the process of ensuring that the person or system desiring access to resources is authentic or "genuine" and not an imposter.

Note 23

Just as anyone knocking on a front door could claim to be a local utility repair person (identity), asking them to display an ID card would prove they are who they claim to be (identity proofing).

Failing to confirm the requester's identity or the requester's genuineness is **identification and authentication failure**. Previously known as "broken authentication," it is a vulnerability that has permitted untold damage. Identity and authentication failure may occur if there are one or more of these weaknesses:

- Exposing a session identifier in a URL or reusing a session identifier (a session identifier is data used in network communications to identify a session through a series of related message exchanges)
- Missing or ineffective multifactor authentication that requires more than one authentication credential
- Permitting automated password attacks such as brute-force attacks or credential stuffing
- Allowing default, weak, or well-known passwords
- Failing to properly store passwords

Two Rights & A Wrong

1. Using an LFI vulnerability, the attacker first manipulates the PHP code to point away from an approved file on the web server to the attacker's own file that has been uploaded to that server.
2. The stack is dynamic memory for the programmer to allocate as necessary.
3. Insecure design is considered a broad category that includes different program weaknesses that are due to missing or ineffective control design.

See the answers at the end of the chapter.

Summary

- In cybersecurity a threat actor, also called a malicious actor, is a term used to describe individuals or entities who are responsible for attacks. The generic term "attacker" is also used. The attributes of the different groups of threat actors vary widely. While some groups have a high level of knowledge and skills along with a massive network of resources and funding, others have minimal skills and no resources. Individuals who want to perform attacks yet lack the technical knowledge to conduct these attacks are sometimes called script kiddies. Script kiddies use automated tools to conduct their attacks and they can often be successful in penetrating defenses. Organized crime is a close-knit group of highly centralized enterprises set up for the purpose of engaging in illegal activities. Organized crime has moved into cyberattacks, which they consider to be less risky and more rewarding than traditional crimes. Their motivation is financial gain.
- Another serious threat to an enterprise comes from its own employees, contractors, and business partners, called insiders. These individuals have the distinct advantage of attacking from the position of a trusted source. Intentional insiders steal protected secrets or manipulate data, and they have several motivations. Although there may be no malicious intent, due to their actions or inactions, unintentional insiders can unwittingly cause harm or create a vulnerability for an external threat actor to exploit. The process of bypassing corporate approval for

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

technology purchases is known as shadow IT and employees who engage in such conduct are considered unintentional insiders.

- A group that is strongly motivated by philosophical or political beliefs or ideology for the sake of their principles is hacktivists. Instead of using an army to march across the battlefield to strike an adversary, governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes. These are known as nation-state actors. There are two types of attacks that are often attributed to nation-state actors: advanced persistent threats and supply-chain attacks. There are other categories of threat actors, such as competitors, brokers, and cyberterrorists.
- Tactics, techniques, and procedures (TTP) describe the behavior or actions of a threat actor in a cascading sequence. TTPs describe what threat actors do and how they will do it. These can define instances including the targets of the attack (such as the human resources representatives of finance companies), the attack patterns, and the details of the attack. Cybersecurity professionals use the Johari window as a means of classifying cybersecurity threats, particularly known threats or unknown threats, or classifying threats comparing the knowledge of the threat actor to security personnel.
- There are a variety of different types of attacks that come from threat actors. A web application infrastructure is a tempting target for attackers for multiple reasons. Common web server application attack categories are request forgery and cross-site scripting attacks. A request forgery attack is a request that has been fabricated. There are two types of request forgeries. A cross-site request forgery (CSRF) takes advantage of an authentication token that a website sends to a user's web browser. If a user is currently authenticated on a website and is then tricked into loading another webpage, the new page inherits the identity and privileges of the victim, who may then perform an undesired function on the attacker's behalf. A server-side request forgery (SSRF) takes advantage of a trusting relationship between web servers. SSRF attacks exploit how a web server processes external information received from another server.
- Threat actors can take advantage of user input and display on a web browser to launch a cross-site scripting (XSS) attack. XSS is a client-side code injection attack using a web application. There are three main types of XSS attacks: reflected XSS, persistent XSS, and Document Object Model XSS. A threat actor who controls a script that is executed in the victim's browser through XSS could fully compromise that user.
- A directory traversal attack takes advantage of a vulnerability so that a user can move from the root directory to other restricted directories, viewing confidential files or entering commands to execute on the web server. Remote code execution (RCE) occurs when a threat actor accesses a target device to make changes to it. Once threat actors have remotely accessed a device, the next step is typically to attempt a privilege escalation. Privilege escalation allows the attacker to gain illicit access to elevated rights or privileges beyond what is entitled for the user.
- Threat actors use data poisoning to contaminate the data that is used in cybersecurity to identify an attack. An attacker could slowly introduce their own "fake" data points seen as permissible activity in order to decrease the accuracy of a system. Not all attacks rely on technology vulnerabilities. Social engineering is a means of eliciting information or convincing a user to take action that weakens security. An attack using obfuscated links crafts deceptive uniform resource locators (URLs) to trick the user into thinking they are valid or secure links. There are several techniques for hiding URLs in a web browser so that an unsuspecting user does not know where a URL will actually redirect them. Threat actors often use more advanced techniques to obfuscate URLs.
- Attacks by threat actors are possible because of vulnerabilities that they exploit. Some vulnerabilities are the result of simply failing to properly configure the security protections that are available in hardware and software (security misconfigurations) while other vulnerabilities are more complex. There are many vulnerabilities that can be traced back to poor programming practices. A local file inclusion (LFI) vulnerability allows an attacker to point away from an approved file on the web server to the attacker's own file that has been uploaded to that server. A remote file inclusion (RFI) vulnerability allows the threat actor to access a file stored on a different server other than the server running the code.
- Several attacks are directed at vulnerabilities associated with how a program uses random access memory (RAM) and are often the result of poor techniques used by the software developer. A buffer overflow attack occurs when a process attempts to store data in RAM beyond the boundaries of a

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

fixed-length storage buffer. This extra data overflows into the adjacent memory locations. Because the storage buffer typically contains the "return address," an attacker can overflow the buffer with a new address pointing to the attacker's malware code. Because buffers are found in both the stack and heap areas, a buffer overflow attack can occur in either the stack (a stack overflow) or the heap (a heap overflow). In an integer overflow attack, an attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow. Programming vulnerabilities are not always the result of poor coding practices; they are often the result of a poor design of the program's logic and implementation that does not properly take into account cybersecurity protections. This is known as insecure design.

- Broken access control is a vulnerability that allows unauthorized users to access sensitive data or systems by circumventing security procedures. This typically occurs when authentication and authorization controls are not properly implemented or enforced, allowing attackers to gain illegitimate elevated privileges. The improper implementation of cryptography can severely weaken it and is known as a cryptographic failure. New hardware and software are introduced regularly that contain both new features as well as stronger security. The older features that are then considered as no longer current and are eventually no longer supported are called end-of-life components. In a downgrade attack, an attacker leverages dated components. Failing to confirm the requester's identity or the requester's genuineness is identification and authentication failure.

Key Terms

advanced persistent threat (APT)
broken access control
buffer overflow attack
cross-site request forgery (CSRF)
cross-site scripting (XSS)
cryptographic failure
data poisoning
directory traversal
end-of-life component
hacktivists
heap overflow
identification and authentication failure
injection flaws
insecure design
insider threat
integer overflow
intentional insider
local file inclusion (LFI)
nation-state actors
obfuscated links
organized crime
outdated components
persistent XSS
privilege escalation
reflected XSS
remote code execution (RCE)
remote file inclusion (RFI)
script kiddies
security misconfigurations
server-side request forgery (SSRF)
social engineering
stack overflow
supply chain attack
tactics, techniques, and procedures (TTP)
threat actor
unintentional insiders

Review Questions

1. Which of the following is NOT an accepted term to describe those who are responsible for cyberattacks?
   a. Malicious actor
   b. Hacker
   c. Attacker
   d. Threat actor
2. Which of the following is NOT a target of financial cybercrime?
   a. Nonprofit organizations
   b. Governments
   c. Individual users
   d. Enterprises
3. Which of the following is the least skilled category of attacker?
   a. Competitors
   b. Organized crime
   c. Script kiddies
   d. Brokers
4. What are the reasons that organized crime perform cyberattacks?
   a. It is less risky and more rewarding than traditional crimes.
   b. The avenues for the types of crimes committed previously are no longer available.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

c. Performing cyberattacks is a means of "showing off" their capabilities.
d. The punishment for cyberattacks is less than that for traditional crimes.

5. Which of the following is NOT true about unintentional insiders?

a. Carelessness, too much multitasking, and low situational awareness are all reasons for the actions of unintentional insiders.
b. Careless employees or contractors are rarely the cause of most insider incidents.
c. Many unintentional insiders have a general disinterest in practicing strong cyber defense.
d. Unintentional insiders can unwittingly cause harm or create a vulnerability for an external threat actor to then exploit.

6. Elodie decided to purchase with her own money a new wireless router that she then installed in the company breakroom. What category does her actions fall under?

a. Shadow IT
b. Express expenditure
c. Corporate circumvention
d. Exploitive actions

7. Which of the following is NOT a characteristic of hacktivists?

a. Hacktivists are strongly motivated by philosophical or political beliefs or ideology for the sake of their principles.
b. Most hacktivists are proud to call themselves "hacktivists."
c. Attacks by hacktivists are often used to "make a statement."
d. Today many hacktivists work through disinformation campaigns by spreading fake news and supporting conspiracy theories.

8. Who are the financiers that support nation-state actors?

a. Cyber zealots
b. Hacktivists
c. Organized crime
d. Governments

9. What is the class of attacks that are multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information?

a. RCE
b. APT
c. RCR
d. ABA

10. Why are supply-chain attacks difficult to defend against?

a. Because supply chains are global in scope, each link in the chain is thousands of miles away overseas and is not under any direct and coordinated supervision and monitoring.
b. Attackers can hide their exploits through firmware patches.
c. Supply-chain attacks only impact hardware that is difficult to trace.
d. Supply chains themselves are hidden networks.

11. Which software supply-chain target infection is considered particularly alarming today?

a. Corporate database software
b. Open-source software
c. OS software
d. Network software

12. Which threat actors sell their knowledge of a weakness to other attackers?

a. APTs
b. Cyber middlemen
c. Brokers
d. Cyberterrorists

13. Which of the following is a high-level description of a threat actor's behavior?

a. PTTs
b. Procedures
c. Tactics
d. Techniques

14. What tool is used to classify threats comparing the knowledge of the threat actor to security personnel?

a. Rumsfeld Graph
b. Johari Window
c. Fire Chart
d. Motivation Display

15. Which attack takes advantage of an authentication token that a website sends to a user's web browser?

a. FRFS
b. SSRF
c. CSRF
d. CSCS

16. Which attack takes advantage of user input and display on a web server?

a. CSCR
b. DOM XRS
c. CSS
d. XSS

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

17. Which type of attack occurs when a threat actor accesses a target device to make changes to it?

    a. XRC
    b. RCE
    c. CED
    d. CRC

18. Which of the following is NOT a means of how obfuscated links are crafted?

    a. Obfuscate with punycode.
    b. Use the HTML "x href" attribute.
    c. Manipulate the @ symbol.
    d. Use alternative hostname formats.

19. Which vulnerability manipulates code to point away from an approved file on the web server to the attacker's own file that has been uploaded to that server?

    a. RFI
    b. LFI
    c. XFI
    d. FFI

20. Which overflow attack manipulates the area of memory in which local variables are stored that a program uses?

    a. Data overflow
    b. Integer overflow
    c. Heap overflow
    d. Stack overflow

Case Projects

Case Project 2-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. What are your thoughts? Why is bit flipping an attack that is rarely discussed? Should DRAM manufacturers be more proactive in finding solutions to prevent it? Is there anything that a user can do to stop a bit flip attack? Write a one-page paper about bit flipping.

Case Project 2-2: Organized Crime as a Threat Actor

Estimated Time: 25 minutes
Objective: Research organized crime as a threat actor.
Description: Research how organized crime has become a threat actor today. What are their motivations? What types of attacks have they been involved in? What warnings have been published to the general public about organized crime cyber attackers? Write a one-page paper about your research.

Case Project 2-3: Shadow IT

Estimated Time: 25 minutes
Objective: Research shadow IT.
Description: Shadow IT is considered an unintentional insider threat that can have significant impact on an organization's security. Research shadow IT and focus your work on examples, dangers, and defenses. Write a one-page paper on your research.

Case Project 2-4: Acts of War

Estimated Time: 25 minutes
Objective: Decipher acts of war committed by nation-state actors.
Description: Does the work of nation-state actors backed by governments constitute an act of war? Does that open the door for targets of their attacks to retaliate? Use the Internet to research this question. Write a one-page paper on your research.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Project 2-5: Log4j Open-Source Attack

Estimated Time: 25 minutes
Objective: Identify vulnerabilities in open-source software and how to defend them.
Description: The Log4j attack had a significant impact on cybersecurity. When Log4j was discovered, the Cybersecurity & Infrastructure Security Agency director said, "This vulnerability is one of the most serious that I've seen in my entire career, if not the most serious." Research the Log4j vulnerability, attacks that resulted from it, and what can be done to protect open-source software. Write a one-page paper on your research.

Two Rights & A Wrong: Answers

Who Are the Threat Actors?

1. Script kiddies are also called unskilled attackers.
2. A special category of intentional insider threats is shadow IT.
3. Nation-state actors may attack foreign governments or even the citizens of their own nation.

Answer: The wrong statement is #2.
Explanation: A special category of unintentional insider threats is shadow IT.

Threat Actor Actions

1. Procedures in TTP are a lower level and highly detailed description of the actions of a technique.
2. Known unknowns are vulnerabilities that the organization is aware of but threat actors have not yet discovered.
3. By definition, unknown unknowns are not possible.

Answer: The wrong statement is #3.
Explanation: Unknown unknowns are security threats that are currently hidden from both threat actors as well as security professionals.

Types of Attacks

1. In an SSRF attack, a request to a website is not from the authentic user but is a forgery that involves crossing sites.
2. XSS is a client-side code injection attack using a web application.
3. In a data poisoning attack, threat actors contaminate the data that is used in cybersecurity to identify an attack.

Answer: The wrong statement is #1.
Explanation: In a CSRF attack, a request to a website is not from the authentic user but is a forgery that involves crossing sites.

Vulnerabilities

1. Using a LFI vulnerability, the attacker first manipulates the PHP code to point away from an approved file on the web server to the attacker's own file that has been uploaded to that server.
2. The stack is dynamic memory for the programmer to allocate as necessary.
3. Insecure design is considered a broad category that includes different program weaknesses that are due to missing or ineffective control design.

Answer: The wrong statement is #2.
Explanation: The heap is dynamic memory for the programmer to allocate as necessary.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

References

1. Goasduff, Laurence, "Protecting your organization from cyber and ransomware attacks," *Gartner*, Feb. 14, 2018, accessed Nov. 6, 2023, https://www.gartner.com/smarterwithgartner/protect-your-organization-from-cyber-and-ransomware-attacks.
2. "Nor Torii study reveals 69% of tech executives say shadow IT is top security concern," *Business Wire*, Apr. 20, 2022, accessed Nov. 6, 2023, https://www.businesswire.com/news/home/20220420005191/en/New-Torii-Study-Reveals-69-of-Tech-Executives-Say-Shadow-IT-is-Top-Security-Concern.
3. Murphy, Hannah, "Hackers launch more than 1.2m attacks through Log4J flaw," *Financial Times*, Dec. 14, 2021, accessed Nov. 6, 2023, https://www.ft.com/content/d3c244f2-eaba-4c46-9a51-b28fc13d9551.
4. "Known and unknown: Author's note," The Rumsfeld Papers, accessed Nov. 6, 2023, https://papers.rumsfeld.com/about/page/authors-note.
5. Galov, Nick, "17+ Sinister social engineering statistics for 2023," *Web Tribunal*, May 20, 2023, accessed Nov. 6, 2023, https://webtribunal.net/blog/social-engineering-statistics/#gref.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 3

Cybersecurity Substrata

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Investigate identity and access management principles
2. Explain public key infrastructure and secure sockets layer inspection
3. Summarize secure coding principles
4. Articulate zero trust and secure access service edge

#TrendingCyber

Cryptography is absolutely essential in today's world. It can prevent fraud in e-commerce and ensure the validity of financial transactions. It can prove a user's identity and protect their anonymity. It can keep troublemakers from defacing a webpage and prevent industrial competitors from reading confidential schematics. Everyone agrees that the Internet would be dramatically different today without cryptography, and some even go as far as to suggest that there would be no Internet at all without the confidentiality, integrity, and availability (CIA) cryptography helps to provide.

So, it's surprising that one of the fundamental cryptographic tools used today may be based on values derived from a phrase like "Jerry deserves a raise." A recently announced contest offering a $36,000 prize for uncovering the origin of the values may soon provide the final answer.

Unlike steganography, which hides the existence of a message, cryptography hides the meaning of the message. Cryptography is the practice of transforming ("scrambling") information so that its meaning cannot be understood by unauthorized parties but only by approved recipients. The process of changing the original text into a scrambled message is known as encryption, while the reverse process is changing the message back to its original form, or decryption.

The history of cryptography is often divided into two eras: the classical era and the modern era. The dividing line between the two occurred in 1977. This is when a completely radical approach to cryptography was announced. Instead of distributing and maintaining one single secure key among multiple users (symmetric encryption) as had been practiced for centuries, two mathematically related keys could be used instead (asymmetric encryption). These keys, known as the public key and private key, revolutionized cryptography and made it practical for everyday use by everyone for everything that needed protection. The asymmetric algorithm RSA was published in 1977 and soon was incorporated into many different products.

The basis of RSA asymmetric encryption security is prime numbers (a whole number that can only be divided by itself and 1). But as computers become faster and more powerful, the ability to break RSA asymmetric encryption by attacking prime numbers grew. Instead of using prime numbers as the basis, security researchers then looked at an obscure (and esoteric) branch of mathematics called elliptic curves. This led to abandoning the use of large prime numbers as with RSA and moving to elliptic curve cryptography (ECC).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

ECC has several advantages over RSA. It can use smaller keys to achieve the same level of security as larger RSA keys. For example, the security achieved with a 521-bit ECC key would require an RSA key of 15,360 bits. In addition to higher security using shorter keys, ECC provides faster processing, greater versatility, and better resistance to attacks. This is why ECC is used today for digital signatures, securing mobile devices, and protecting Internet of Things (IoT) security and as the foundation of the popular TLS cryptographic protocol.

The Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the most widely used ECC implementations today. It originated in 1999 and was soon adopted by the National Institute of Standards and Technology (NIST). The NIST specifications of ECDSA provide a set of standard elliptic curves of varying sizes and security levels. The specifications also publish a "seed" value that is then used to create other parameters of a curve. For example, the NIST P-256 curve specification standard says, "SEED = C49D3608 86E70493 6A6678E1 139D26B7 819F7E90."

But where did this seed come from? And why this value and not another?

It was later revealed that the National Security Agency (NSA) was behind the seeds, which were provided by the NSA to NIST and appeared in their specifications with no explanation as to their origin. Linking the NSA to cryptographic seeds created a firestorm and blistering criticism from mathematicians, civil liberties advocates, and security professionals. It had previously been revealed by a former NSA subcontractor that the NSA deliberately tried to subvert widely used crypto standards. One of those standards was a random number generator known as Dual EC_DRBG, which was the default method for generating crucial random numbers used in cryptography. In 2015, the agency's former research director admitted it was a mistake for the NSA to support a critical cryptographic function after researchers presented evidence that it contained a fatal flaw that could be exploited by U.S. intelligence.

The NSA's likely interference with previous cryptographic standards immediately led to speculation about ECDSA seeds. Did NSA pass to NIST seeds that have a weakness or a backdoor that only the NSA had knowledge of? Knowing the origin of the seeds could help provide the answer.

Security researchers were on the case.

Researchers eventually found the person responsible for providing the seeds: Jerry Solinas. Jerry was a long-time NSA employee who authored multiple cryptographic standards. He was approached and asked about the seeds. He admitted he generated the seeds for the NSA that were provided to NIST. When asked how he came up with the seeds, Jerry said that he took a phrase and hashed it, with the resulting hash (message digest) being used as the seed. A hash algorithm creates a unique "digital fingerprint" of a set of data; for example, a hash of the letter *a* is 86be7afa339d0fc-7cfc785e72f578d33. A hash is one-way only: knowing the hash (86be7afa339d0fc7cfc785e72f578d33) cannot reveal the underlying value (the letter *a*).

When Jerry was asked what underlying phrase he used to generate the hash to create the seed, he sheepishly replied that he could not exactly remember but he thought the phrase was "Jerry deserves a raise." Because the computer he used was later replaced, the exact phrase was lost to history. Jerry passed away in early 2023.

Other shadowy figures then stepped forward and said they had clues about the underlying phrase. Someone said they recalled Jerry telling them that the phrase had two names in it, like "Give Alice and Bob a raise." Another source said that he mentioned the phrase may have contained a number. But none of these suggestions ever generated the identical seeds, and the mystery remained.

In the fall of 2023, a contest was announced to uncover the underlying phrase. The winner who discovers it will earn $12,288 (increased from the original bounty of $8,192) and, if the recipient chooses to donate it to a charity, it will be tripled to $36,864. Those backing the contest said, "This is a call to arms . . . to join the search, help fill in a page of cryptographic history, and collect a large bounty or donate an even larger one to charity." The cryptographic security community is hopeful that the underlying phrase will be discovered, and this mystery can at last be put to rest.

Substrata is an underlying layer or substance, such as a layer of rock or soil beneath the surface of the ground. The word is used to describe a foundation or basis, such as "There is a broad substratum of truth in that statement."

There are numerous cybersecurity substrata topics that form the foundation or basis of protecting data. It is important to master these substrata before moving on to higher levels and more complex cybersecurity concepts.

In this chapter you study several of those substrata foundational topics of cybersecurity. You examine identity and access management, encryption, secure coding, and networking.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Identity and Access Management (IAM)

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

The basis of security is keeping the bad guys out while letting the good guys in. Virtually every device—laptop, smartphone, web server, and security appliance, to name just a few—has some means for the user or connected system to prove that they have approval to access the device. And once approved the users and systems are not granted complete access to everything on the device but only to what is absolutely necessary.

In information security, **identity and access management (IAM)** is the technologies that provide control over user validation and the resources that may be accessed. IAM ensures that the right users access the right digital resources at the right time for the right reasons.

IAM topics can be divided into two categories. These categories are those topics that address identity and those that cover access.

Identity

In information security, IAM requires a user accessing a device to first provide some type of unique digital identity. This identity serves to differentiate the user from all other users. But it also requires the user to provide proof that they are this unique user, called identity proofing. Just as anyone knocking on a front door could claim to be a local utility repair person (identity), asking them to display an ID card would prove they are who they claim to be (identity proofing). Identity proofing is also called authentication, which is the process of ensuring that the person or system desiring access to resources is authentic or "genuine" and not an imposter.

Caution

The word *identity* in IAM covers both identity proofing and authentication.

Consider this scenario. Riker, Peyton, and Paolo work on a local military base and each afternoon they go to the gym on the base to exercise. As they reach the entrance to the building, each must press their finger to the fingerprint reader to enter the building (a "No Tailgating" policy is strictly enforced). As they walk to the receptionist's desk, Riker holds up his ID card to the reader so the door to the locker room opens for him. As Peyton searches for his card, the receptionist, Li, waves him through to the locker room because she knows him. Riker laughs and says to Li, "It's only because of Peyton's flaming red hair that you recognize him, and it runs in his family!" Paolo, however, is new to the base and must sign in. After Li compares his signature to his membership application on file, she then allows him to enter. In the locker room, each of them opens their locker using a combination lock with a series of numbers that they have memorized.

In this scenario, the three men have been demonstrated to be authentic and not an imposter by the seven separate elements listed in Table 3-1. Because only the real or "authentic" person possesses one or more of these elements, these can be considered as types of authentication credentials.

Table 3-1 Elements that prove authenticity

Element	Description	Scenario example
Somewhere you are	Restricted location	Restricted military base
Something you are	Unique biological characteristic that cannot be changed	Fingerprint reader to enter building
Something you have	Possession of an item that nobody else has	Riker's ID card
Someone you know	Validated by another person	Li knows Peyton
Something you exhibit	Genetically determined characteristic	Peyton's flaming red hair
Something you can do	Perform an activity that cannot be exactly copied	Paolo's signature
Something you know	Knowledge that nobody else possesses	Combination to unlock locker

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 1

Three of these elements (something you know, something you have, and something you are) are called *factors*; the remaining four (somewhere you are, something you can do, something you exhibit, and someone you know) are called *attributes*. The element *something you exhibit* is often linked to more specialized attributes than hair color in the scenario and may even include neurological traits that can be identified by specialized medical equipment.

Any of these elements can be used as an authentication credential. However, the most common credential found in IAM is something you know, namely passwords. Despite the importance of protecting assets through identity, passwords have serious weaknesses. However, advances in authentication have provided an increased level of protection.

Password Deficiencies

A password is a secret combination of letters, numbers, and/or characters. Passwords are universally used for authentication and work in a standard format across devices and sites.

Note 2

The person credited with inventing the computer password, Fernando "Corby" Corbato, who passed away in late 2019, was a researcher for the Massachusetts Institute of Technology and worked on the Compatible Time-Sharing System (CTSS), which allowed multiple users to share computer time. He devised a way to isolate users from each other with password-protected user accounts. In his later years, Corbato lamented that passwords had become problematic. He said that the Internet made logins with passwords "kind of a nightmare."

The strength of passwords is based on human memory: Unless tricked by social engineering to reveal a password, a user's memory is considered a secure repository for passwords. This is because human memory cannot be compromised through a vulnerability the same way in which a technology device can be compromised.

However, the weakness of passwords is also based on human memory: Human beings can memorize only a limited number of items. And the longer and more complex the item, the more difficult it is to remember. Passwords place heavy loads on human memory in multiple ways:

- The most effective passwords are long and complex. However, these are difficult for users to memorize and then accurately recall when needed.
- Users must remember multiple passwords for many different accounts. Most users have accounts for different computers and mobile devices at work, school, and home; multiple email accounts; online banking; Internet site accounts; and so on. According to one study, in the United States, the average number of online accounts registered to a single email address was 130. The average number of accounts per Internet user is estimated to be 207.[1]
- For the highest level of security, each account password should be unique, which further strains human memory.
- Many information security policies mandate that passwords expire after a set period of time, such as every 45–60 days, when a new one must be created. Some security policies even prevent a previously used password from being recycled and used again, forcing users to repeatedly memorize new passwords.

Because of the burdens that passwords place on human memory, users take shortcuts to help them memorize and recall their passwords, thus creating passwords that are vulnerable to attacks (weak passwords). Weak passwords often use a common word as a password (*princess*), a short word (*tables*), a predictable sequence of characters (*123456*), or personal information (*Hannah*) in a password. Another common shortcut that dramatically weakens passwords is to reuse the same password (or a slight derivation of it) for multiple accounts. Although this makes it easier for the user, it also makes it easier for an attacker who compromises one account to then have access to all other accounts that use the same password.

Even when users attempt to create stronger passwords, they generally follow predictable patterns:

- **Appending.** When users combine letters, numbers, and punctuation (character sets), they do it in a pattern. Most often they only add a number after letters (*caitlin1* or *cheer99*). If they add all three-character sets, it is in the sequence letters+punctuation+number (*braden.8* or *chris#6*).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Replacing.** Users also use replacements in predictable patterns. Generally, a zero is used instead of the letter *o* (*passw0rd*), the digit *1* for the letter *I* (*denn1s*), or a dollar sign for an *s* (*be$tfriend*).

Caution

Attackers are aware of these patterns in passwords and can search for them, making it faster and easier to crack a password.

Security professionals decry the widespread use of weak passwords since they provide an easy attack vector. Four out of every five enterprise data breaches are caused by weak passwords, and half of all users use one password for all their accounts. And when forced to create a new password, two out of every three users create a password that is like the one they are replacing. The 10 most common passwords in 2023 are listed in Table 3-2, and three of the top four common passwords in this list have remained the same for over six years.[2]

Table 3-2 Ten most common passwords

Rank	Password
1	123456
2	123456789
3	qwerty
4	password
5	12345
6	qwerty123
7	1q2w3e
8	12345678
9	111111
10	1234567890

A noted security expert summarized the password problem well by stating:

> The problem is that the average user can't and won't even try to remember complex enough passwords to prevent attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it [down] and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications.[3]

Note

A recent study looked at users who had been told that the password to their account had been stolen in a data breach. Only one-third of the users then changed their passwords. And the users were in no rush to change their passwords: Only 3 percent changed their password within 30 days after the breach, while 12 percent waited between 60 and 90 days. Incredibly only 14 percent of users changed their password to a *stronger* password; all others created passwords that were actually weaker or the same strength as the stolen password by reusing character sequences from their previous password or creating a new password that was similar to other passwords they use.

In addition to the weaknesses of passwords due to human memory that compromises their strength, threat actors are continually attacking passwords because of their high value. There are different types of password attacks. Some attacks have very limited success at compromising an account, but they do not require much effort on the part of the threat actor. In some cases, the attacker may determine the user's password by more of a "lucky guess" than a focused and systematic attack. Other attacks are high-outcome attacks in which there is a high degree of success, but these require much more time and effort.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Authentication Advances

Because of the importance and widespread use of passwords, along with their deficiencies, strengthening authentication based on passwords has been an ongoing effort. There are several recent advances that have increased the strength of authentication via passwords. These include tokens, security keys, single sign-on, and passwordless systems.

Tokens In addition to authentication based on what the user knows, another type of authentication credential is based on the approved user having a specific item in their possession (something you have). One common item that is used for this type of authentication is called a token (a "token" is some type of object).

Originally tokens were a supplemental hardware device that users carried with them. A windowed token is typically a small device (usually one that can be affixed to a keychain called a key fob) with a window display. A windowed token is shown in Figure 3-1. A windowed token does not display a static value that never changes; instead, the value dynamically changes. This value is a one-time password (OTP) that can be used only once or for a limited period of time. The OTP takes the place of a user-entered password.

Figure 3-1 Windowed token



Note 4

There are two types of OTPs. A *time-based* one-time password *(TOTP)* changes after a set period of time, such as every 30 to 60 seconds, and this code is valid for only the brief period that it is displayed on the token. Instead of changing after a set number of seconds, a *hash-based message authentication code (HMAC) OTP (HOTP)* is "event driven" and changes when a specific event occurs, such as when a user enters a personal identification number (PIN) on the token's keypad.

There have been two changes to the process of using a windowed token to generate an OTP. First, instead of using a separate and dedicated physical hardware device like a windowed token, today smartphones are used instead. Because smartphones are ubiquitous and carried by users virtually everywhere, they can be used for authentication without the need for an additional physical device.

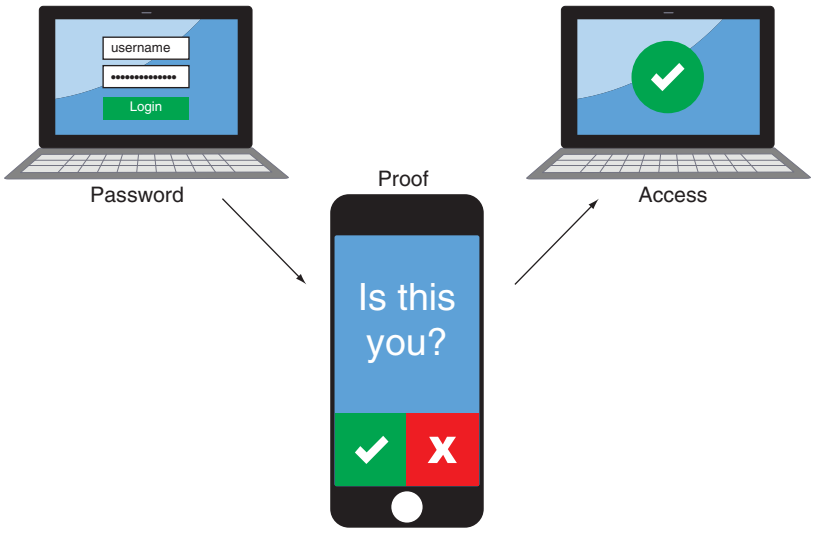
Second, instead of generating an OTP, an authentication code is sent in a text message to a smartphone. After entering a username and password, a text message with an authentication code is sent and the user must enter that code on the website to complete the authentication process. This can result in a higher degree of security because it combines more than one type of authentication credential: It uses both what a user knows (the password) and what the user has (a smartphone). Using two (or more) forms of authentication credentials is called **multifactor authentication (MFA)**.

An even simpler approach is an app installed on a smartphone that requests the user's approval. This prevents a remote attacker from impersonating a user by entering their password since it would require approval from the genuine user. A user who receives a request but was not attempting to log into an account with a password would simply deny the request. Using an authentication app is shown in Figure 3-2.

Security Keys A more secure option that is gaining acceptance is using a dedicated token key, known as a security key. As seen in Figure 3-3, a security key is a dongle that is inserted into the universal serial bus (USB) port or held near the device (such as a smartphone using near field communication or NFC). The key contains all the necessary cryptographic information to authenticate the user.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 3-2 Authentication app



Caution

Despite its convenience and ability to reach a wide range of users, using a text message sent to a smartphone for authentication is not considered a secure option. A text message can be "phished" (a user is tricked into providing the code to an attacker through a phishing attack), text messages can be intercepted, and an attack known as "MFA fatigue" generates a seemingly endless stream of MFA push notifications sent to the user's smartphone, who simply accepts the MFA push notification in order to stop being bothered.

Figure 3-3 Security keys



Source: Google LLC

One feature of security keys is attestation. Attestation is a key pair that is "burned" into the security key during manufacturing time and is specific to a device model. It can be used to cryptographically prove that a user has a specific model of device when it is registered. When a user creates a new credential key pair (that links to a specific service like Facebook or PayPal), the public key that is sent to the service is signed with the attestation private key. The service that is creating the new account for the user can verify that the attestation signature on the newly created public key came from the device.

Note 5

Because security keys do not transmit OTPs or authentication codes, many security professionals recommend that users choose security keys for authentication.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

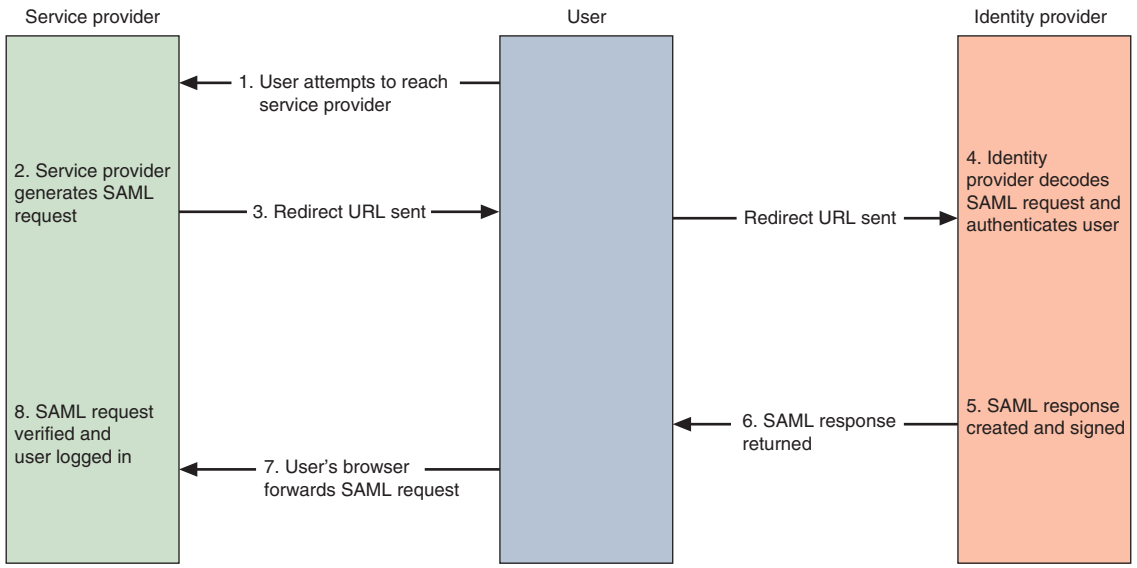
Single Sign-On (SSO) One of the problems facing users today is the fact that they have multiple accounts across multiple platforms that all should use a unique username and password. The difficulty in managing all of these different authentication credentials frequently causes users to compromise and select the least burdensome password and then use it for all accounts. A solution to this problem is to have one assigned username and password to gain access to all accounts so that the user has only one username and password to remember.

Using a single authentication credential that is shared across multiple networks and has interoperability (the ability of systems to exchange information) holds great promise for the user. When those networks are owned by different organizations, it is called **federation** (sometimes called federated identity management or FIM). One application of federation is **single sign-on (SSO)**, or using one authentication credential to access multiple accounts or applications. SSO holds the promise of reducing the number of usernames and passwords that users must memorize (potentially, to just one).

There are several current technologies for SSO. One of the most common is Security Assertion Markup Language (SAML). This is an XML standard that allows secure web domains to exchange user authentication and authorization data. It allows a user's login credentials to be stored with a single identity provider instead of being stored on each web service provider's server. SAML is used extensively for online e-commerce business-to-business (B2B) and business-to-consumer (B2C) transactions. The steps of a SAML transaction, which are illustrated in Figure 3-4, are:

1. The user attempts to reach a website of a service provider that requires a username and password.
2. The service provider generates a SAML authentication request that is then encoded and embedded into a URL.
3. The service provider sends a redirect URL to the user's browser that includes the encoded SAML authentication request, which is then sent to the identity provider.
4. The identity provider decodes the SAML request and extracts the embedded URL. The identity provider then attempts to authenticate the user either by asking for login credentials or by checking for valid session cookies.
5. The identity provider generates a SAML response that contains the authenticated user's username, which is then digitally signed using asymmetric cryptography.
6. The identity partner encodes the SAML response and returns that information to the user's browser.
7. Within the SAML response, there is a mechanism so that the user's browser can forward that information back to the service provider, either by displaying a form that requires the user to click a Submit button or by automatically sending it to the service provider.
8. The service provider verifies the SAML response by using the identity provider's public key. If the response is successfully verified, the user is logged in.

Figure 3-4 SAML transaction



There are other federation technologies as well. These are listed in Table 3-3.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 3-3 Federation systems technologies

Name	Description	Explanation
OAuth (Open Authorization)	Open-source federation framework	OAuth 2.0 is a framework to support the development of authorization protocols.
Open ID	Open standard decentralized authentication protocol	Authentication protocol that can be used in OAuth 2.0 as a standard means to obtain a user identity.
Shibboleth	Open-source software package for designing SSO	Uses federation standards to provide SSO and exchanging attributes.

Note 6

OAuth relies on token credentials. A user sends their authentication credentials to a server (such as a web application server) and also authorizes the server to issue token credentials to a third-party server. These token credentials are used in place of transferring the user's username and password. The tokens are not generic but are for specific resources on a site for a limited period of time.

Passwordless Systems For many years, technology pundits have said the death of the password is right around the next corner. However, these statements have turned out to be false. The promoted password alternatives, such as SSO, were sometimes found to introduce as many usability and security problems as they solved.

Now, however, cybersecurity may truly be on the verge of having strong and user-friendly authentication systems that do not use passwords, called **passwordless** systems. One passwordless system that is rapidly gaining popularity is called Passkey. Passkey is supported by Fast IDentity Online (FIDO), an open-source organization whose aim is to reduce reliance on passwords. It is backed by some of the world's biggest tech companies, such as Google, Apple, and Microsoft among its 250 members. FIDO standards are built in almost all web browsers, operating systems (OSs), and consumer devices used in online transactions. Websites that support Passkey display the new Passkey logo, shown in Figure 3-5.

Figure 3-5 Passkey logo



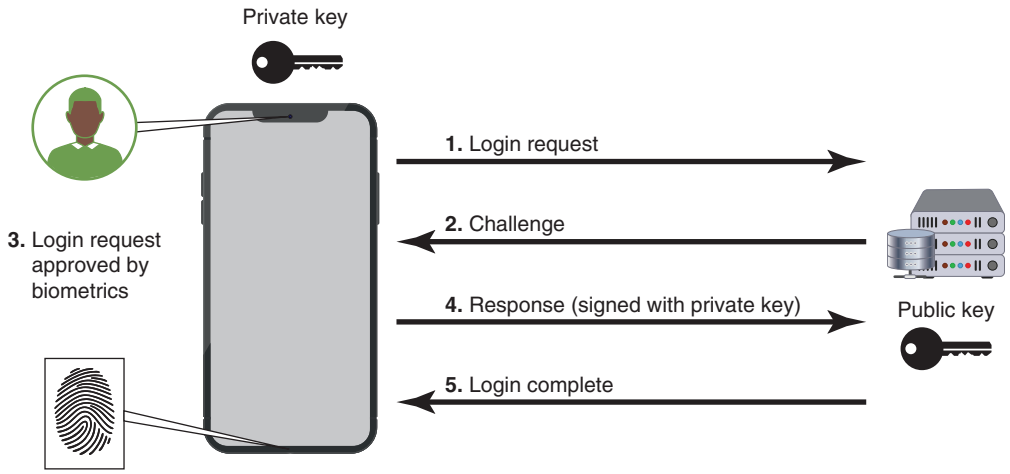
Instead of relying on passwords, Passkey utilizes a hardware device to verify a user's identity, such as a mobile device (smartphone or tablet), USB key, or an NFC-enabled device. Passkeys are based on WebAuthn, or Web Authentication, which uses public and private keys to verify a user's identity. The public key is shared with the website to which the user wishes to be authenticated while the private key is kept secret.

When a user signs up for a new account that utilizes Passkey, the website's server shares information and asks the user to confirm their authenticator. A passkey, including the public and private key pair, is then generated for that specific website. The public key is sent to the website's server for storage, while the private key remains securely stored in the user's authenticator.

When the user attempts to sign in using Passkey, the website will create a challenge that is sent to the user. The user's authenticator will first verify the user's identity through biometrics like a face or fingerprint (a master password can be used as an option) before signing the challenge using the private key and then sending the completed signature to the website. Finally, the website uses their copy of the user's public key to verify the signature's authenticity. Passkey is illustrated in Figure 3-6.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 3-6 Passkey



Passwordless systems like Passkey have several advantages:

- **Strong by default.** Because users no longer create passwords, there is no concern whether a password is strong. Instead, the authenticator device generates a strong and secure public and private key pair on the user's behalf.
- **No external exposure.** Since users no longer enter a password, it cannot be exposed to threat actors. The private key is stored on the device and retrieved automatically, and the public key is stored with the account provider.
- **Cannot be stolen.** Because the password is not stored on the remote website, there is nothing for threat actors to steal. And if the user's public key were to be stolen, it would be useless since by itself it cannot be used to gain access to the account.
- **Immune to social engineering attacks.** Threat actors who create impersonated fake websites and then use social engineering and phishing attacks to trick users into entering a password will find that these attacks are no longer effective. WebAuthn ensures that users cannot share their credentials with untrusted websites.

Note 7

In late 2023 Google announced that passkeys are now the default sign-in option across Google Accounts for all its services and platforms.

Access

A second category of IAM topics focuses on access. Two access technologies are privileged access management and a cloud access security broker.

Privileged Access Management (PAM)

Privileged access management includes knowing the definition of privilege, types of accounts, and why PAM is needed.

What Is Privilege? In cybersecurity *privilege* is more than the authority a given account or process has within a system or network. Instead, privilege is a special right; that is, it is an advantage or elevation above what is normal and is not ordinarily given to a wide range of users. Privilege provides the authorization to override or bypass important established security controls and may include permissions to perform actions such as shutting down systems, loading device drivers, configuring networks or systems, and provisioning and configuring accounts and cloud instances.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 8

Privileges serve an important operational purpose by enabling users, applications, and other system processes the elevated rights needed to access certain resources to complete necessary tasks.

Types of Accounts In virtually all organizations today there are two types of accounts: nonprivileged accounts and privileged accounts. Most users are assigned nonprivileged accounts, also called least privileged user accounts (LUAs). There are two types of nonprivileged accounts:

- **Standard user accounts.** Standard user accounts have a limited set of privileges, such as for Internet browsing, using certain types of applications like Microsoft Office, and for accessing a limited array of resources. These are defined by role-based access policies.
- **Guest user accounts.** Guest user accounts possess fewer privileges than standard user accounts. These accounts are usually restricted to basic application access and Internet browsing.

At the other extreme are privileged accounts. A privileged account provides access and privileges beyond those of regular (nonprivileged) accounts. Special types of privileged accounts, sometimes called "superuser accounts," are primarily used for administration by qualified and preapproved information technology (IT) employees. These employees must be approved because privileged accounts provide virtually unrestrained power to execute commands and make system changes.

Note 9

Superuser accounts are typically known as "Root" in Unix and Linux. In Windows systems they are simply called "Administrator."

Superuser account privileges can provide unrestricted access to files, directories, and resources with full read, write, and execute privileges; the power to render system-wide changes across a network; creating or installing files or software; modifying files and their settings; and deleting users and data. Superusers can even grant and revoke privileges permissions for other users.

Note 10

A Windows computer has at least one administrator account that allows the user to perform activities such as installing software and changing local configurations and settings. While Apple users may operate with root access as a default, a nonprivileged account should be created and used for routine computing.

However, there is also a middle ground between these two types of accounts. As a best practice most users only have a standard user account. But some users may need to occasionally perform higher-level activities. To facilitate this, these users are given both types of accounts: they login as a standard user to perform routine tasks but then log in using a superuser account to perform administrative activities.

Why PAM Is Needed Because of their elevated capabilities and access, privileged accounts pose considerably higher risks than nonprivileged accounts. It is important for these privileged accounts to be strictly managed and controlled. However, often these privileged accounts are not properly managed due to a variety of reasons:

- **Overprovisioning privileges.** Because user accounts are not always matched with job responsibilities, users may complain that they cannot "do their job." IT administrators then provide users with broad sets of privileges that go beyond what they need. Also, an employee's role can change and no longer require elevated privileges, or they have new responsibilities that allow them to access critical corporate data—but still have dangerous privileged accounts.
- **Lack of visibility and awareness.** Long-forgotten privileged accounts are commonly sprawled across organizations. These "orphaned" accounts may number in the hundreds or even thousands.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Manual and decentralized management.** Managing hundreds or thousands of privileged accounts manually is virtually impossible. Also, privileged accounts may be managed differently across different parts of the organization that leads to inconsistent enforcement of established best practices.
- **Lack of visibility into privileges.** Applications and service accounts often automatically execute privileged processes to perform actions, as well as to communicate with other applications, services, resources, and so on. Applications and service accounts frequently possess excessive privileged access rights by default.
- **Shared accounts.** IT teams commonly share root, Windows Administrator, and many other privileged credentials for convenience so workloads and duties can be seamlessly shared as needed. However, with multiple users sharing an account, it is impossible to tie actions performed with an account to a single individual. This creates security, auditability, and compliance issues.
- **Siloed processes.** Modern IT environments typically run across multiple platforms (Windows, Apple, Unix, and Linux) and environments (on-premises, Azure, Amazon Web Services, and Google Cloud). Each of these is often separately maintained and managed. This results in inconsistent administration, added complexity for users, and increased risks.

The solution is **privileged access management (PAM)**. PAM is the strategies and technologies for exerting control over privileged accounts and the access and permissions for users, accounts, processes, and systems. It provides visibility, control, and auditing capabilities. PAM is considered a subset of IAM. While IAM controls provide authentication of identities to ensure that the right user has the right access at the right time, PAM layers on more granular control over privileged accounts and session activities. Taken together, IAM and PAM can provide fine-tuned control, visibility, and the ability to audit across all credentials and privileges.

Cloud Access Security Broker (CASB)

As with applications running in an on-prem environment, cloud-based applications must also be protected. However, there are several common misperceptions about applications running in the cloud. One misperception is that application security is entirely the cloud provider's responsibility. Another misconception is that the native "out of the box" security of the applications being licensed will provide adequate security. In addition, misconfigurations of the application setup and insecure APIs or interfaces can provide vulnerabilities for threat actors to exploit.

One security protection for cloud computing application security is to use a **cloud access security broker (CASB)**. A CASB is a set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure. Acting as the gatekeeper, a CASB ensures that the security policies of the enterprise extend to its data in the cloud. For example, if the enterprise has a policy for encrypting data, a CASB can enforce that control and ensure that data is encrypted when it is copied from the cloud to a local device. Another security protection is to use cloud-based data loss prevention (DLP) to extend the enterprise's policies to data stored in the cloud.

Two Rights & A Wrong

1. IAM is the technologies that provide control over user validation and the resources that may be accessed.
2. There are three types of authentication credentials.
3. Passkey uses a hardware device to verify the user's identity.

See the answers at the end of the chapter.

Encryption

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

There are several important security elements using encryption. Two of these are public key infrastructure and Secure Sockets Layer inspection.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 11

Encryption has become so foundational to information security that in the latest CompTIA CySA+ exam objectives CS0-003, encryption is now included under "System and network architecture concepts in security operations."

Public Key Infrastructure (PKI)

Suppose that Alice wants to obtain a digital certificate for her personal use. She must go through the entire certificate signing request (CSR) generation process that involves multiple steps and interacting with multiple entities. She must use asymmetric cryptography to create her public and private keys, a registration authority must verify the request, an intermediate certificate authority (CA) must process the request, the digital certificate must be placed in a certificate repository (CR), and then finally moved to a certificate revocation list (CRL) when it expires. For one user creating a digital certificate through the CSR generation process, this involves multiple steps interacting with multiple entities.

Now consider the CSR generation process on a large scale ("at scale"), such as in a typical enterprise with hundreds, thousands, or tens of thousands of users. Multiple users have digital certificates, and sometimes a user may have multiple digital certificates. When going through the CSR generation process, the number of steps and number of entities grows exponentially to the point that it can quickly become overwhelming. And a single missed step or error could result in a digital certificate not being generated or even having a vulnerability. There needs to be a consistent means to manage digital certificates.

Public key infrastructure (PKI) is what one might expect from its name: It is the underlying infrastructure that serves as a key management system for controlling public keys, private keys, and digital certificates. Strictly speaking, PKI is the set of software, hardware, processes, procedures, and policies that are needed to create, manage, distribute, use, store, and revoke digital certificates across large user populations. The goal of a PKI is to establish the identity of people, devices, and services in order to control access to resources, protect data, and provide accountability. In short, PKI is digital certificate management at scale.

Secure Sockets Layer (SSL) Inspection

One of the early and most widespread cryptographic protocols is Secure Sockets Layer (SSL). This protocol was developed by Netscape in 1994 in response to the growing concern over Internet security. The design goal of SSL was to create an encrypted data path between a client and a server that could be used on any platform or operating system. However, the way in which SSL functions left it vulnerable to an attack. Transport Layer Security (TLS) is a widespread cryptographic protocol that is the replacement for SSL. The algorithms SSL and TLS are sometimes listed as being interchangeable or even in conjunction with each other (TLS/SSL), which is technically not correct. However, often today cryptographic protocols are simply referred to as "SSL."

Note 12

SSL is no longer developed or supported. In 2015, the Internet Engineering Task Force (IETF) had declared all versions of SSL deprecated due to vulnerabilities and its lack of critical security features.

In order to avoid malware detection, threat actors have turned to encrypting their Internet traffic. This makes it important for organizations to perform **Secure Sockets Layer (SSL) inspection** of traffic to uncover any malicious content. An SSL inspection service acts as a "man in the middle" between the user and the web server, allowing the service to intercept any malicious traffic. The steps in an SSL inspection service are:

1. A user opens a browser and sends an HTTPS request.
2. The SSL inspection service intercepts the HTTPS request.
3. Through a separate encrypted tunnel, the service sends its own HTTPS request to the destination server and conducts negotiations.
4. The destination server sends the service its certificate with the public key.
5. The service and destination server complete the SSL handshake and the application data and subsequent messages are sent through the SSL tunnel.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

6. The service conducts SSL negotiations with the user's browser.
7. The service and the browser complete the SSL handshake and the application data and subsequent messages are sent through the SSL tunnel.

Caution

Despite the importance of SSL inspection, it is highly compute-intensive and can impact overall network performance. This has led many organizations to bypass HTTPS inspection by appliances that cannot keep pace with the processing demands.

Two Rights & A Wrong

1. PKI is digital certificate management at scale.
2. Today cryptographic protocols are simply referred to as TLS.
3. An SSL inspection service acts as a "man in the middle" between the user and the web server, allowing the service to intercept any malicious traffic.

See the answers at the end of the chapter.

Secure Coding

Certification

2.5 Explain concepts related to vulnerability response, handling, and management.

The Common Weakness Enumeration (CWE) website is a community-developed and -maintained list of software and hardware weaknesses and vulnerabilities. The CWE maintains a list of the top 25 most dangerous software weaknesses. Some of the most critical vulnerabilities include out-of-bounds write (the application writes data past the end or before the beginning of the intended buffer), use after free (referencing memory after it has been freed), out-of-bounds read (reading data past the end or before the beginning of the intended buffer), and NULL pointer dereference (a pointer that should be valid but is NULL). The reason for most of these vulnerabilities are, in the words of the CWE, "simple programming omissions," often the result of poor coding (programming) techniques or not utilizing the features built into coding languages that can enhance security.

But why do these programming omissions occur? One reason is that developing an application is too often done in a haphazard fashion with the primary goal of completing the job as quickly as possible. When "speed to completion" is the most important goal, then other critical outcomes, such as security, are usually marginalized. And this is compounded even more when large teams of programmers are working on a software project, as is often the case today.

Coding secure apps is an important foundation of cybersecurity. Secure coding involves using the secure software development life cycle and implementing secure code best practices.

Secure Software Development Life Cycle (SDLC)

Instead of developing an application in a disorganized fashion, using a proven methodology is far more beneficial. A "methodology" is a body of rules and set of established procedures. The generally recognized steps in an application development methodology include:

1. Planning and requirements
2. Architecture and design
3. Test planning
4. Coding
5. Testing and results
6. Release and maintenance

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

One of the best-known methodologies for creating an application is the software development life cycle (SDLC). However, in the past it was common practice to perform security-related activities only as part of the SDLC testing phase. This "after-the-fact" approach—looking for vulnerabilities after the program had been designed and coded—introduced two serious problems. First, many security issues went undiscovered during testing. Second, vulnerabilities that were discovered late in the process would often be hurriedly corrected but by doing so would introduce another vulnerability or cause the software to perform erratically.

In recent years major software developers have instead focused their attention on developing secure applications through all steps instead of only at the SDLC testing phase. Integrating security activities across the entire process is called the **secure software development life cycle (SDLC)**. This helps to develop software that has fewer—if any—vulnerabilities and reduce the risk of imposing a new vulnerability while attempting to fix a newly discovered vulnerability.

Note 13

There are entire secure SDLC frameworks available. The Microsoft Security Development Lifecycle (MS SDL) was one of the first of its kind, and the National Institute of Standards and Technology (NIST) 800-64 is a framework that must be observed by U.S. federal agencies.

Some of the recognized secure SDLC best practices include:

- **Security requirements definition.** The optimal time to define the security requirements of software is during the initial design and planning stages. This also gives the development teams the ability to integrate security requirements early in the process and minimize later disruption. Different factors that influence security requirements typically include regulatory compliance requirements, internal standards, and known threats.
- **User acceptance testing.** An application with a poor user interface (UI) may result in software that is underutilized. It may also encourage users to try to circumvent the security provisions of the software that the user finds too cumbersome or restrictive. User acceptance testing can ensure that the UI is acceptable to users.
- **Application stress testing.** An application stress test determines if the software can withstand the workload placed on the software without crashing. This includes verifying that it can respond in a timely fashion to a high number of simultaneous users.

Secure Coding Best Practices

There are several coding techniques that should be used to create secure applications and limit data exposure or disclosing sensitive data to attackers. These best practices include:

- **Input validation.** All input from every source should go through **input validation** or ensuring that the data received is legitimate. This includes checking for the correct data type (date, string, integer, floating point, etc.), range, size, and appropriateness (such as filtering for an invalid date like May 32).

Caution !

It is a mistake for the application to attempt to sanitize input data on behalf of the user in order to correct errors. Instead, an error message should be generated back to the user.

- **Output encoding.** When dynamic information is displayed on the screen that was received from any data source (instead of being static information like a label), anything other than the text itself must be stripped away. This is called **output encoding**. For example, any HTML control characters (like <, >, and /) should be purged.
- **Parameterized queries.** When giving input into a database, a **parameterized query** should be used instead of passing input. A parameterized query uses predefined variables or prepared statements as placeholders for parameters.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Session management.** A web session is a sequence of multiple network HTTP request and response transactions that are all associated with the same user. Modern web applications are complex and require that the information or status of the user be retained for the duration of the multiple interactions for that session. Once a user has presented their credentials and been authenticated, all subsequent requests must be able to apply appropriate security access controls as well. It is necessary to implement **session management** capabilities that link both the authentication and access control (or authorization) modules that are commonly available in web applications.
- **Data protection.** Different schemes for securing the integrity of any data in which the application accesses (**data protection**) should be part of the application.
- **Authentication.** **Authentication** is the process of ensuring that the person or system desiring access to resources is authentic or "genuine" and not an imposter. Authentication secure coding best practices include never implementing a personally developed authentication system and always using MFA when possible.

Additional secure coding best practices are summarized in Table 3-4.

Table 3-4 Secure coding techniques

Coding technique	Description	Security advantage
Normalization	Organizing data within a database to minimize redundancy	Reduces footprint of data exposed to attackers.
Stored procedure	A subroutine available to applications that access a relational database.	Eliminates the need to write a subroutine that could have vulnerabilities.
Code signing	Digitally signing applications	Confirms the software author and guarantees the code has not been altered or corrupted.
Obfuscation/camouflaged code	Writing an application in such a way that its inner functionality is difficult for an outsider to understand	Helps prevent an attacker from understanding a program's function.
Dead code	A section of an application that executes but performs no meaningful function	Provides an unnecessary attack vector for attackers.
Server-side execution and validation or client-side execution and validation	Input validation generally uses the server to perform validation but can also have the client perform validation by the user's web browser.	Adds another validation to the process.
Code reuse of third-party libraries and SDKs	Code reuse is using existing software in a new application; a software development kit (SDK) is a set of tools used to write applications.	Existing libraries that have already been vetted as secure eliminate the need to write new code.

Two Rights & A Wrong

1. Integrating security activities across the entire process is called SDLC.
2. When dynamic information is displayed on the screen that was received from any data source, anything other than the text itself must be stripped away.
3. The purpose of normalization is to reduce the footprint of data exposed to attackers.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Networking

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

The final cybersecurity foundation category is networking. Topics in this category include zero-trust architecture and secure access service edge.

Zero Trust

A relatively new defense applied to networks has been growing in popularity. This is known as zero trust. It is important to understand what it is, its principles, and how it is applied through a zero-trust architecture.

What Is Zero Trust?

Twenty years ago, most networks were based on a traditional security model that operated on the assumption that everything inside an organization's network can be trusted. Because all users within the network are trusted users, all users in the network will act responsibly. However, as threat actors became increasingly adept at infiltrating networks, it was soon realized that this traditional network security model was no longer viable.

Note 14

In other words, relying exclusively on prevention was no longer a winning strategy.

Ten years ago, the focus again shifted. The goal this time was to rapidly detect any intruders who might break into the network. This would allow for a rapid response for action to be taken.

But just as the original network security model proved defective, so too was this revised model. By the time it was discovered that threat actors had infiltrated the network, these skilled attackers had moved into other parts of the network. Valuable time was wasted trying to understand the intention of the threat actor and what resources they were targeting.

Both flawed network security models resulted in security operations center (SOC) cybersecurity professionals focusing exclusively on stopping and blocking the attackers. This is because both flawed models relied on the same assumption: threat actors are trying to enter the network.

However, this assumption is false: attackers were *already* inside the network.

Modern threat actors are not trying to enter the network from the outside but are currently on the inside. Many users are shocked that attackers are already lurking inside a "secure" network. However, that has become the reality today. The network perimeter, by itself, does not keep attackers out, and it is not possible to detect and block a threat actor quickly enough when an attack is discovered. Instead, controls must be employed on a new assumption: every network is infiltrated and thus untrusted.

There is a control designed to address this assumption that the network is already infected. **Zero trust** is a strategic initiative about networks that is designed to stymie successful attacks by threat actors who are already within a network. As its name implies, zero trust attempts to eliminate the concept of trust from an organization's network architecture.

Zero trust acknowledges that implicit trust—trusting everyone within a network—is a vulnerability. This is because networks have been designed so that once inside the network, users can freely "move" to access or exfiltrate data. Yet because most networks have already been compromised, malicious attackers likewise can freely move through the network. Zero trust is not designed to make a system trusted. Instead, zero trust works to eliminate trust.

Note 15

The motto of zero trust is "Never trust, always verify."

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Zero-Trust Principles

There are several principles of zero trust:

- **Revise network security goals.** While at one time the goal of network security was to prevent all network breaches or respond quickly enough to fix them, these are not the goals of zero trust. Instead, by assuming a breach has already occurred, the goal is limiting and containing.
- **Eliminate implicit trust.** Prior security models assumed that any subject inside the network was there because they had been authenticated and approved, and thus they could access virtually any resource. Zero trust requires that every interaction between users, workloads, network resources, data, and devices must first be verified before it is allowed to occur.
- **Enforce granular least privilege.** While least privilege has often been used when referring to limiting a user's permissions to only those resources that are required, what about applications, devices, and integrated systems? These entities also must have least privilege enforced so that they can only access a resource to perform an authorized task—and no more than that.
- **Utilize allow lists.** An allow list is a model designed to block all traffic that is not specifically permitted. In the zero-trust model, nothing is implicitly trusted, and everything must be first verified through an allow list.
- **Move the line of trust.** At one time the dividing line between trusted and untrusted was the gateway into the Internet: anything on the corporate network side of the gateway was trusted while everything on the Internet was untrusted. Zero trust recognizes that because a threat actor has already infiltrated the network, then the network can no longer be trusted. Thus, the line between trusted and untrusted must be moved.
- **Prevent east–west lateral movement.** Once a threat actor infiltrates a network, they rarely, if ever, remain where the breach occurs. Instead, they quickly perform reconnaissance to become familiar with network hierarchies, host naming conventions, and the locations of assets; gather privileges like login credentials; and then move laterally (called "east–west") to the valuable and desired resources. Zero trust helps prevent this movement.

Another principle of zero trust is to segment the network into much smaller "pieces" called microsegmentations. This helps prevent lateral movement across data networks, campus networks, and even the cloud. Table 3-5 lists several approaches to zero-trust microsegmentation.

Table 3-5 Zero-trust microsegmentation

Microsegmentation	Description	Advantages and disadvantages
Network segmentation	Using Internet Protocol subnets (Layer 3) or virtual local area networks (VLANs; Layer 2) for microsegmentation leverages existing technologies	Management of these segments can be difficult or require the network to be rearchitected.
Firewall segmentation	Firewalls, common around the perimeter of the network, can be deployed inside a network for microsegmentation.	Using firewalls can be expensive due to the number of devices needed. Many require hundreds or thousands of firewall rules, and misconfigurations can break applications.
Software-defined networking (SDN)	SDN policies can funnel packets through a distributed set of virtual software firewalls.	This adds a layer of complexity and may be difficult to segment applications that do not fit within set network boundaries.
Host-based segmentation	Host-based segmentation uses workload telemetry to create a map of computer environments and applications that can then be used to determine what needs to be protected.	This is considered the best approach for zero trust due to its reliance on the host instead of other external devices.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

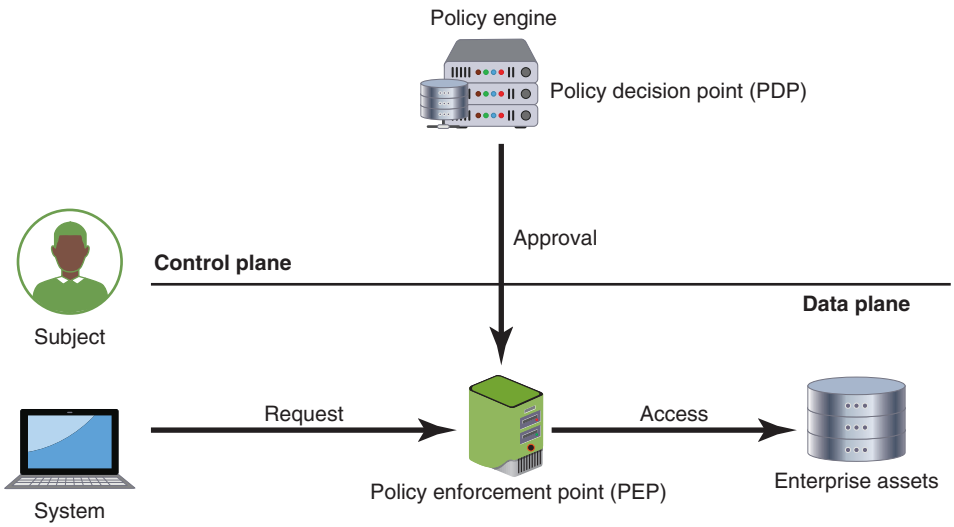
Zero-Trust Architecture (ZTA)

A zero-trust architecture (ZTA) is a framework for implementing zero trust in an enterprise. Zero trust focuses on authentication and authorization to shrink implicit trust while still maintaining availability. The goal of ZTA is to prevent unauthorized access to data and services by making access control enforcement as precise and granular as possible (policy-driven access control). When properly implemented, ZTA minimizes threats against assets (threat scope reduction).

A user (subject) or another device (system) requests access to a resource. The user is considered to be in an untrusted zone while the resource is in a secured zone that cannot be accessed without approval. Users are verified through adaptive identity, which takes into consideration more than just a username and password; it can also include the role of the user in the organization, their location, the resources being requested, and any prior behavior on the network that deviates from a baseline.

The policy engine is a component of the policy decision point (PDP) that provides input into the policy enforcement point (PEP) to make the decision whether to grant access for a request. The policy engine relies on policy automation that uses automated processes for referring to policies for approval. The control plane is used for communication while the data plane is used for the transfer of the resource if approved. A conceptual ZTA is illustrated in Figure 3-7.

Figure 3-7 Conceptual zero-trust architecture



Note 16

In early 2022, an executive order from the president of the United States mandated that all government agencies must achieve specific zero-trust security goals by the end of fiscal year 2024.

Secure Access Service Edge (SASE)

A change has taken place regarding where employees accessed IT resources for their jobs. Many employees now enjoy hybrid work, with time split between the office and working from home.

Note 17

It has been said that today "work" is viewed as an activity instead of a place.

Hybrid work has required organizations to make their IT resources accessible from virtually any location. This accelerated the shift to using the cloud for storing and processing data. Almost overnight, cloud models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) became part of the everyday IT vocabulary. Instead of being

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

confined to an on-prem data center, data was now moving from the local data center up to cloud services, which includes both public and hybrid clouds, and then moved back down to branch offices before returning back to the data center.

As increasing numbers of users as well as IT resources were remote, this resulted in organizations struggling to provide sufficient levels of connectivity while ensuring strong cybersecurity defenses. However, most network and cybersecurity products on the market at that time were not designed to handle all the types of traffic and security threats that organizations suddenly faced.

In order to handle these different requirements, organizations had to quickly adopt multiple appliances and products, such as secure web gateways (SWGs), firewalls, virtual private network (VPN) remote access, Multiprotocol Label Switching (MPLS), and software-defined wide area networks (SD-WANs). And for each of these appliances and products, architectures had to be deployed, policies had to be configured, interfaces had to be managed, and resulting logs had to be reviewed. This created a significant burden on SOCs in terms of costs and complexity. These also contributed to gaps in cybersecurity defenses.

Clearly a different solution was called for. What was needed was something that could help organizations embrace cloud, hybrid, and remote connectivity by providing network architecture and network cybersecurity services. And this needed to be accessed from a common cloud-delivered architecture.

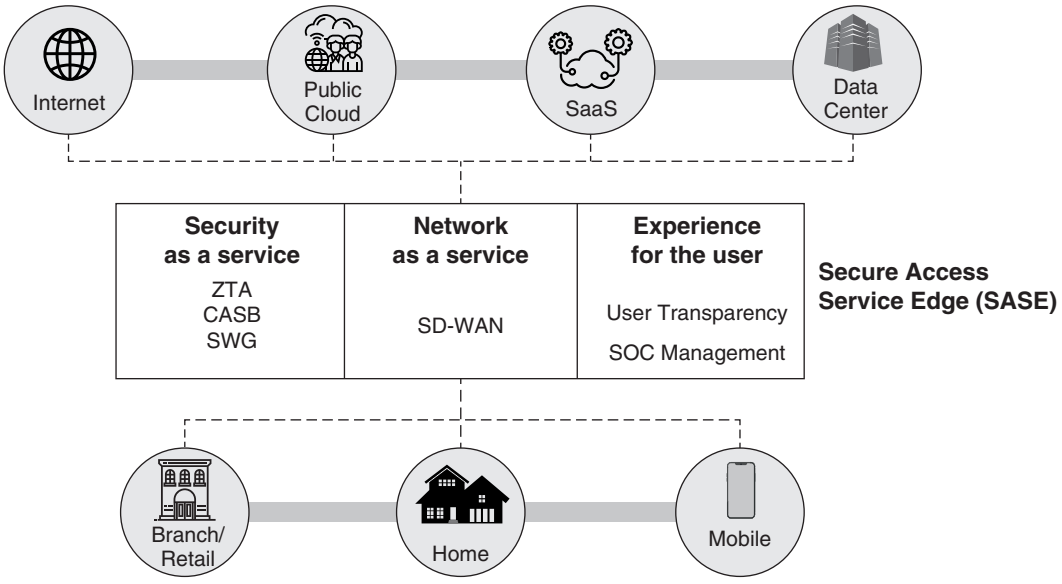
The solution is a **Secure Access Service Edge (SASE)**, pronounced "sassy." SASE is the convergence of several security services into a single, cloud-delivered service model. It has been defined as security functions delivered as a service that are based on the identity of the user or system and its real-time usage context. This allows for predefined enterprise security policies to be applied while continuously assessing security risks throughout the session.

Note 18

In other words, a SASE architecture identifies users and devices, applies policy-based security, and then delivers secure access to the appropriate application or data.

There are various technologies that combine to make up a SASE. These include CASB, ZTA, secure web gateways (SWGs), and wide area networking (WAN) technologies (WANs are a form of telecommunication networks that can connect devices from multiple remote locations and are established by telecommunication service providers that lease the network to businesses). A subset of SASE that only includes the security components and not the WAN is called a Security Services Edge (SSE). SASE is illustrated in Figure 3-8.

Figure 3-8 Secure Access Storage Edge (SASE)



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong

1. Zero trust acknowledges that implicit trust is a vulnerability.
2. The goal of ZTA is to prevent unauthorized access to data and services by making access control enforcement as precise and granular as possible.
3. SASE is the convergence of several security services into a single, on-prem service model.

See the answers at the end of the chapter.

Summary

- In information security, identity and access management (IAM) is the technologies that provide control over user validation and the resources that may be accessed. A password is a secret combination of letters, numbers, and/or characters. Passwords are universally used for authentication and work in a standard format across devices and sites. The weakness of passwords is also based on human memory because human beings can memorize only a limited number of items. Longer and more complex items are even more difficult to remember. Because of the burdens that passwords place on human memory, users take shortcuts to help them memorize and recall their passwords, thus creating passwords that are vulnerable to attacks.
- Because of the importance and widespread use of passwords, along with their deficiencies, strengthening authentication based on passwords has been an ongoing effort. There are several recent advances that have increased the strength of authentication via passwords. Originally tokens were a supplemental hardware device that users carried with them. Instead of using a separate and dedicated physical hardware device like a windowed token, today smartphones are used instead. Often an authentication code is sent in an SMS text to a smartphone. This can result in a higher degree of security because it combines more than one type of authentication credential: it uses both what a user knows (the password) and what the user has (a smartphone). Using two (or more) forms of authentication credentials is called multifactor authentication (MFA). A more secure option that is gaining acceptance is using a dedicated token key, known as a security key.
- Using a single authentication credential that is shared across multiple networks and has interoperability holds great promise for the user. When those networks are owned by different organizations, it is called federation. One application of federation is single sign-on (SSO) or using one authentication credential to access multiple accounts or applications. There are several current technologies for SSO. One of the most common is Security Assertion Markup Language (SAML). Strong and user-friendly authentication systems that do not use passwords, called passwordless systems, are increasing in popularity.
- In cybersecurity "privilege" is more than the authority a given account or process has within a system or network. Instead, privilege is a special right; that is, it is an advantage or elevation above what is normal and is not ordinarily given to a wide range of users. A privileged account provides access and privileges beyond those of regular or nonprivileged accounts. Because of their elevated capabilities and access, privileged accounts pose considerably higher risks than nonprivileged accounts. It is important for these privileged accounts to be strictly managed and controlled. Privileged access management (PAM) is the strategies and technologies for exerting control over privileged accounts and the access and permissions for users, accounts, processes, and systems. It provides visibility, control, and auditing capabilities. A security protection for cloud computing application security is to use a cloud access security broker (CASB). A CASB is a set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure. Acting as the gatekeeper, a CASB ensures that the security policies of the enterprise extend to its data in the cloud.
- Public key infrastructure (PKI) is the underlying infrastructure that serves as a key management system for controlling public keys, private keys, and digital certificates. PKI is the set of software, hardware, processes, procedures, and policies that

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

are needed to create, manage, distribute, use, store, and revoke digital certificates across large user populations. The goal of a PKI is to establish the identity of people, devices, and services in order to control access to resources, protect data, and provide accountability. In order to avoid malware detection, threat actors have turned to encrypting their Internet traffic. This makes it important for organizations to perform Secure Sockets Layer (SSL) inspection of traffic to uncover any malicious content. An SSL inspection service acts as a "man in the middle" between the user and the web server, allowing the service to intercept any malicious traffic.

- Instead of developing an application in a disorganized fashion, using a proven methodology is far more beneficial. A "methodology" is a body of rules and a set of established procedures. Integrating security activities across the entire process is called the secure software development life cycle (SDLC). This helps to develop software that has fewer vulnerabilities and reduce the risk of imposing a new vulnerability while attempting to fix a newly discovered vulnerability. There are several coding techniques that should be used to create secure applications and limit data exposure or disclosing sensitive data to attackers. These include input validation (ensuring that the data received is legitimate), output coding (stripping away anything other than the text itself), parameterized queries (using predefined variables or prepared statements as placeholders for parameters), session management (capabilities that link both the authentication and access control modules together), data protection (using different schemes for securing the integrity of data), and authentication (the process of ensuring that the person or system is not an imposter).
- Zero trust is a strategic initiative about networks that is designed to stymie successful attacks by threat actors who are already within a network. As its name implies, zero trust attempts to eliminate the concept of trust from an organization's network architecture. Zero trust acknowledges that implicit trust (trusting everyone within a network) is a vulnerability. This is because networks have been designed so that once inside the network, users can freely "move" to access or exfiltrate data. Zero trust is not designed to make a system trusted. Instead, it works to eliminate trust. A zero-trust architecture (ZTA) is a framework for implementing zero trust in an enterprise. It focuses on authentication and authorization to shrink implicit trust while still maintaining availability. A Secure Access Service Edge (SASE) is the convergence of several security services into a single, cloud-delivered service model. It allows for predefined enterprise security policies to be applied while continuously assessing security risks throughout the session.

Key Terms

authentication
cloud access security broker (CASB)
data protection
federation
identity and access management (IAM)
input validation
multifactor authentication (MFA)
output encoding
parameterized query
passwordless
privileged access management (PAM)
public key infrastructure (PKI)
Secure Access Service Edge (SASE)
Secure Sockets Layer (SSL) inspection
secure software development life cycle (SDLC)
session management
single sign-on (SSO)
zero trust

Review Questions

1. In which of the following authentication elements is biometrics used?
   a. Something you can do
   b. Something you exhibit
   c. Something you know
   d. Something you are
2. Which of the following is NOT correct about passwords and human memory?
   a. The strength of passwords is based on human memory.
   b. The weakness of passwords is based on human memory.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

c. A user's memory is not considered a secure repository for passwords.
d. Passwords place heavy loads on human memory in multiple ways.

3. What does a windowed token display?

a. Static value that never changes
b. OTP
c. OHTP
d. SMS

4. Which of the following is the most secure authentication option?

a. Security key
b. Windowed token
c. Authentication app
d. MFA OTP

5. Which of the following involves sharing authentication credentials across networks owned by different organizations?

a. FIM
b. OSSO
c. LSAM
d. XTRO

6. What does the Passkey passwordless system use to verify a user's identity?

a. A WebAuthn token
b. An SSO
c. A hardware device
d. The public key

7. Which of the following is NOT an advantage of a passwordless system?

a. Forces strong passwords
b. Strong by default
c. No external exposure
d. Immune to social engineering attacks

8. What is "privilege" in cybersecurity?

a. The authority a given account or process has within a system or network
b. An elevation above what is normal and is not ordinarily given to a wide range of users
c. A right granted to all users in order to perform their normal duties
d. An outdated approach to protecting resources

9. What is PAM?

a. The strategies and technologies for exerting control over privileged accounts and the access and permissions for users, accounts, processes, and systems.
b. A superset of IAM.
c. A cloud-based repository of security policies.
d. The technology for deleting authentication credentials that are no longer needed.

10. Which of the following is NOT true about CASB?

a. It is protection for cloud computing application security.
b. It requires a PAM box.
c. It is a set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure.
d. It ensures that the security policies of the enterprise extend to its data in the cloud.

11. Which of the following is NOT managed by PKI?

a. Hash digests
b. Private keys
c. Public keys
d. Digital certificates

12. What acts as a "man in the middle" between the user and the web server, allowing the service to intercept any malicious traffic?

a. RSTS examination
b. HTTPS inquiry
c. TLS peeking
d. SSL inspection

13. Which of the following is the most secure methodology?

a. SDLC
b. Secure SDLC
c. XLSL
d. SDL MS

14. Which of the following secure coding best practices uses predefined variables or prepared statements as placeholders?

a. Output validation
b. Input encoding
c. Session management
d. Parameterized query

15. Which of the following is incorrect about zero trust?

a. It is a strategic initiative designed to stop attacks by threat actors who are already within a network.
b. It attempts to eliminate the concept of trust from the network architecture.
c. It acknowledges that implicit trust is an asset.
d. It is not designed to make a system trusted.

16. Which of the following is a principle of zero trust?

a. Keep network security goals.
b. Enforce granular least privilege.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

c. Reinforce implicit trust.
d. Utilize block lists.

17. In a ZTA, what provides input into the PEP?

a. LPA
b. ZLA
c. PDP
d. VAX

18. Which of the following is NOT correct about a SASE?

a. It requires a local on-prem server.
b. It is the convergence of several security services.
c. It is based on the identity of the user or system and its real-time usage context.
d. It allows for predefined enterprise security policies to be applied.

19. Which of the following technologies is NOT part of a SASE?

a. ZTA
b. CASB
c. SWG
d. XRA

20. Which of the following secure coding techniques reduces the footprint of data exposed to attackers?

a. Normalization
b. Stored procedure
c. Code storage
d. Camouflaged code

Case Projects

Case Project 3-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. Does it surprise you that the foundation of the important ECDSA seeds may be based on such a simple phrase? Should there be more rigor in creating these seeds? If so, what should it be? And should the NSA even have a hand in developing cryptographic specifications? Would there be too great a temptation to weaken the encryption for their own benefit? Write a one-page paper about this.

Case Project 3-2: Authentication Elements Scenario

Estimated Time: 25 minutes
Objective: Create a scenario that incorporates authentication elements.
Description: Design your own scenario that uses all seven of the authentication elements in the story (like the scenario earlier in this chapter of Riker, Peyton, and Paolo at the gym). Then create a table like Table 3-1 that lists each element, a description, and your scenario example.

Case Project 3-3: Strengthen Authentication Using Passwords

Estimated Time: 20 minutes
Objective: Evaluate suggestions for strengthening authentication.
Description: Due to the importance of authentication based on passwords, suggestions continue to be made regarding how to make password authentication stronger. One suggestion is to not allow users to create their own passwords but instead have all passwords randomly generated and assigned to the user. Another suggestion is to not use the user's email address as the username in a password-based system. Obfuscating the username provides a higher degree of security because any data stolen by threat actors could not be clearly linked to the user. But would these suggestions create too much "friction" for users? Give your opinion about these two suggestions as to their feasibility from a security standpoint and then from a user standpoint. Then create your own two suggestions for stronger password-based security. Finally, rate all four of the suggestions with a grade of A–F. Write a one-page paper on your research.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Project 3-4: Security Keys

Estimated Time: 25 minutes
Objective: Research security keys.
Description: Security keys are considered one of the highest levels of authentication security for users. However, they do have disadvantages. Use the Internet to research security keys. Identify how they work and list their advantages and disadvantages. Then select three popular keys and compare their features. Would you use a security key? Why or why not? Write a one-page paper on your research.

Case Project 3-5: Passkey

Estimated Time: 25 minutes
Objective: Research the Passkey passwordless system.
Description: Passkey, supported by FIDO, is becoming the most popular passwordless system. Research Passkey, noting its advantages and disadvantages. Would you use a passwordless system? Why or why not? Write a one-page paper on your research.

Two Rights & A Wrong: Answers

Identity and Access Management (IAM)

1. IAM is the technologies that provide control over user validation and the resources that may be accessed.
2. There are three types of authentication credentials.
3. Passkey uses a hardware device to verify the user's identity.

Answer: The wrong statement is #2.
Explanation: There are seven types of authentication credentials: somewhere you are, something you are, something you have, someone you know, something you exhibit, something you can do, and something you know.

Encryption

1. PKI is digital certificate management at scale.
2. Today cryptographic protocols are simply referred to as TLS.
3. An SSL inspection service acts as a "man in the middle" between the user and the web server, allowing the service to intercept any malicious traffic.

Answer: The wrong statement is #2.
Explanation: Today cryptographic protocols are simply referred to as SSL, not TLS.

Secure Coding

1. Integrating security activities across the entire process is called SDLC.
2. When dynamic information is displayed on the screen that was received from any data source anything other than the text itself must be stripped away.
3. The purpose of normalization is to reduce the footprint of data exposed to attackers.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Answer: The wrong statement is #1.
Explanation: Integrating security activities across the entire process is called the secure software development life cycle (SDLC).

Networking

1. Zero trust acknowledges that implicit trust is a vulnerability.
2. The goal of ZTA is to prevent unauthorized access to data and services by making access control enforcement as precise and granular as possible.
3. SASE is the convergence of several security services into a single, on-prem service model.

Answer: The wrong statement is #3.
Explanation: SASE is the convergence of several security services into a single, cloud-delivered service model.

References

1. Le Bras, Tom, "Online overload – it's worse than you think," *Dashlane Blog*, accessed May 22, 2017, https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/.
2. Chang, Jenny, "55 important password statistics you should know: 2023 breaches & reuse data," *FinancesOnline*, Jan. 8, 2023, accessed Feb. 18, 2023, https://financesonline.com/password-statistics/.
3. Schneier, Bruce, *Secrets and lies: Digital security in a networked world* (New York: Wiley Computer Publishing), 2004.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Part 2

Security Operations

In most organizations cybersecurity defenders make up the security operations center (SOC), pronounced “sock.” While at one time this was a room (“center”) in which all the security personnel were housed, today with the growth of required defenses and the number of employees working remotely, a SOC is considered more as a function than a location. The chapters in this second part outline the types of activities that a SOC team typically performs. These make up the basic security operations of an organization.

Chapter 4
Identifying Indicators of Attack (IOA)

Chapter 5
Analyzing Indicators of Compromise (IOC)

Chapter 6
Threat Detection and Process Improvement

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 4

Identifying Indicators of Attack (IOA)

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Compare IOA and IOC
2. Explain different network IOA
3. Categorize various endpoint IOA
4. Describe application IOA

#TrendingCyber

Suppose local law enforcement is called to investigate a house that had been burglarized. Upon arriving, the police are surprised to learn that the doors to the house had no locks. And what was even more surprising was the owner of the house was a locksmith. As the police attempt to talk with the owner, they find him yelling at his son and berating him for his failure to close one of the lockless doors when he left for school. As the police attempt to calm down the locksmith homeowner, one of the law enforcement officers leans over and whispers to him, "Sir, does it really matter if your son left the door open when you didn't install your own locks on the doors?"

This scenario is a parallel to a recent cybersecurity incident in which the identity and authentication management (IAM) provider Okta suffered a serious data breach. Okta is widely known for its cloud-based software that helps companies manage and secure user authentication. Threat actors stole administrative credentials belonging to some of Okta's largest and well-known customers. While a published report by Okta on the attack focused on an Okta employee whose actions allowed the attackers in (the son who left the door open), the report minimized a larger contributing factor to the success of the attack: Okta had not applied its own IAM protections on its systems (the locksmith owner who did not install his own locks).

Okta's chief security officer, in a company blog post following the cyber incident, admitted that a threat actor gained access to parts of its customer support system. But how it determined this is chilling.

Okta first learned of suspicious activity when one of its own customers reported to them malicious activity tied to Okta's services. But instead of looking at their own systems, Okta instead focused its investigation back on the customer as the source of the breach; they suspected that one of the customer's employees had been the victim of a malware infection or a phishing attack. Okta failed to identify in its own log files evidence that attackers had compromised Okta systems and were exfiltrating data.

Three days later, a second customer reported similar issues, and they even provided Okta with an indicator of compromise, which was an Internet Protocol (IP) address associated with the threat actors. Still, Okta did not look internally to determine if its systems were the cause of the breach. Another 10 days later a third customer came forward. It was not until a full 18 days after the initial concern was raised that Okta finally looked at itself and then identified—in

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

its own log files—the IP address that had been provided to it earlier as the source of the attack. By this time 134 of its customers had been compromised.

After recognizing that its own systems were the source of the attack and not its customer's, Okta turned its investigation to how the threat actors entered its systems, looking at indicators of compromise. The Okta investigation found that one of their employees had been using the Google Chrome browser on their Okta laptop that accessed their personal Google profile, a violation of company policy. Threat actors were able to compromise the employee's personal Google account or the device itself, obtaining the Okta IAM credentials they wanted. And what they wanted were the credentials to give them access to the Okta service account, which the employee had accessed using their Chrome browser.

A service account is a "nonhuman" privileged account that is used to run applications or services. Service accounts are essentially proxies for performing limited actions for users that have no access to sensitive data and systems. Service accounts are necessary for persistent applications to run. In addition to running applications, a service account is used to execute automated services and provide device-to-device communications.

In its report, Okta laid blame at the feet of the employee who used their Okta laptop to access both their personal Google profile and the Okta service account. This provided the means for threat actors to access Okta's systems. But the employee's actions were overshadowed by Okta's much larger failures. Okta had not installed their own protections—the protections that they sold to other companies—on their own systems. And they failed to follow basic cybersecurity procedures. Okta's report did not mention this.

What exactly should Okta have done?

First, Okta should have had access controls in place besides a simple password to access service accounts. One way of doing this is to put conditions on the IP addresses that can connect to the account by using an "approved list" so that only listed IP addresses have access while all other IP addresses are blocked by default. Also, Okta should have never allowed any employee to use a service account password on their normal day-to-day computer. Instead, administration of a service account should only be done from a special jump server.

Second, Okta should have blocked Gmail access at their firewall. This would stop any employee who was not following the company's policies. And they should also have blocked access to Chrome's built-in password manager through a Windows Active Directory (AD) group policy setting.

Finally, Okta should have had visibility into its own network. They were not able to see evidence that they had been compromised but had to rely on information supplied by multiple customers that came from their indicators of compromise. Not being able to see inside its own networks allowed the threat actors more time to do harm.

While Okta did eventually make changes to their security, it was well after the damage had been done.

One employee who violated company policy allowed the threat actors to enter. But that is not the reason the attack was successful. Had Okta applied its own security tools and followed cybersecurity best practices, it is unlikely any of this would have happened.

Consider the Okta incident outlined in #TrendingCyber. There were multiple instances of evidence of an attack that Okta missed (such as log file entries) while their customers had provided them with their own evidence (such as an IP address). But such evidence, while important, is clearly after the fact: the threat actors had already successfully completed their mission. What if, instead of relying on evidence that an attack had already occurred, there could be clues that revealed an attack was imminent? In that way an impending attack could be minimized or completely stymied.

Looking for evidence of an attack while also uncovering clues of an impending attack are critical security operation tasks. Evidence of an attack helps provide insight into what happened, why, and what can be done about it for next time. But even more importantly, clues of an impending attack can minimize the impact or even stop an attack that may be about to begin.

In this chapter, you explore uncovering indicators that point to a potential attack. These indicators can be divided into the categories networking, endpoint, and application indicators.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Cybersecurity Indicators

Certification

1.2 Given a scenario, analyze indicators of potentially malicious activity.

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

Bob is a thief who wants to burglarize a jewelry store. He begins by using a friend's computer to look online for any information about the store, such as its owner and when it closes. He then drives by the store at different times of day and night. Bob later parks across the street and watches customers enter and leave the store. For several nights, he watches the store late into the evening to see when the owner leaves. Finally, Bob himself goes into the jewelry store pretending to look for a wedding ring for his fiancé. He takes note of the layout of the store, any alarm systems, where keys are stored, and asks the owner several questions before he is satisfied that he has the information that he needs to pull off his heist the following night.

However, Bob's questions arouse suspicion in the store owner, who then calls Alice, the local police chief. The paths of Alice and Bob had crossed before as Bob had often been charged with breaking and entering. Alice decides to check on his recent activities. Alice calls Bob's friend, who volunteers that Bob has been searching online for information about the jewelry store. She finds out from Bob's neighbors that he has been out late into the evening on several occasions recently, and one neighbor said she noticed Bob's car parked across the street from the jewelry store one night. Another neighbor said that he observed Bob putting a big crowbar and sledgehammer in the trunk of his car that afternoon along with what appeared to be a ski mask and gloves.

That night Bob puts his plan into action. He drives to the rear of the jewelry store, removes his tools, disables the alarm, and with much effort breaks down the door and enters. He makes his way to the jewelry display cases and fills his bag with stolen jewels, as shown in Figure 4-1. As he turns to leave, the lights of the store suddenly come on and Bob is face-to-face with Alice. Alice is holding as evidence the sledgehammer, crowbar, and gloves that Bob left by the door. "Hi, Bob," Alice says. "Are you ready to take a trip downtown with me?"

Figure 4-1 Bob the thief



Vector_KIF/Shutterstock.com

This fictional scenario helps illustrate the difference between two cybersecurity categories of indicators. These categories are indicators of attack and indicators of compromise.

Indicators of Attack (IOA)

The first category of indicators parallels the actions of Bob in preparation for breaking into the jewelry store. Bob searched online for information about the store, drove by the store and watched it, and entered the store pretending to be a customer. These actions are what Bob needed to do in order to gather information to rob the store.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In cybersecurity, these types of preliminary behaviors are called indicators of attack (IOA). A security operations center (SOC) searching for IOA is focused on detecting the intention of the threat actor as evidenced by their actions. IOA attempts to answer the question, "What do these actions tell us that the attackers want to do?" However, IOA is not evidence that an attack is already underway. Rather, IOA are one or more indicators of a *potential upcoming* attack.

Caution

Precise wording is essential when thinking about IOA. For example, the question "What are they trying to do?" may imply that the attack is already underway, when in reality only the "probing" has started. "Indicators of attack" does not mean that the attack itself has begun but that there are indicators of what could be an attack.

Several caveats of IOA likewise relate to the scenario with Bob:

- **Not conclusive.** Bob's actions of searching online for information on the jewelry store or driving by the store do not indicate that a break-in by Bob is imminent and will occur soon. Nor does it show that he even will break into the store. He could find the security of the jewelry store is too strong and he must abandon his efforts and look for another store. The same is true with cybersecurity: Threat actors who are probing for weaknesses may find they are unable to perform their intended attack. Finding an IOA is not conclusive that an attack will occur.
- **Irrespective of tools.** Bob did not look for only jewelry stores that could be entered by using a sledgehammer and crowbar. His probing did not focus on the tools that he might use but instead on the viability of performing the burglary. Likewise, cybersecurity IOA do not focus on the tools that the threat actors will use in their attacks.
- **Combinations of behaviors.** Had Bob only driven by the jewelry store, that would not have indicated he was planning to rob it. However, his combination of behaviors—parking outside the store, searching for information online, purchasing a crowbar and sledgehammer, and so on—when taken together can indicate a malicious intent. And as with cybersecurity, it is not a single IOA that indicates an imminent attack, but a combination of behaviors must be examined.

Indicators of Compromise (IOC)

The second category of indicators is the evidence that Alice collected on Bob's heist. This includes the sledgehammer, crowbar, and gloves that Bob used, along with the bag of jewels in his possession. These taken together likely will be sufficient evidence to convict Bob of the crime.

In cybersecurity, the digital artifacts that serve as evidence of an attack are called **indicators of compromise (IOC)**. An IOC is the evidence that a successful attack has occurred and how it happened. This evidence is used to determine what deficiencies exist and what should be fixed. IOC are one or more indicators of a *successfully completed* attack.

There are also caveats with IOC that can be illustrated by the scenario with Bob. One major caveat is not using IOC as IOA. Suppose that Bob's car was a green van that he had used in a previous robbery. Had Alice focused her attention on only looking for green vans, she would then have missed the fact that Bob had rented a red convertible for the jewelry store robbery. Cybersecurity professionals face a similar problem: They are tempted to focus on previous and often outdated IOC as being current IOA. Because a threat actor used one successful action in the past does not necessarily mean that it will be used again. Confusing IOC with IOA is considered to be a major challenge in a SOC.

Table 4-1 compares IOA with IOC.

Note 1

The CompTIA exam objectives use IOC, but they do not specifically use the term IOA. However, the objectives do use similar language, such as "Analyze indicators of potentially malicious activity."

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 4-1 IOA versus IOC

Elements	IOA	IOC
Definition	Indicators of a potential upcoming attack	Indicators of a successfully completed attack
Purpose	Determine if an attacker is probing system for future attack	Gather digital evidence from a past attack
Timeframe	Continuous	After successful attack
Mechanics	Dynamic and ever changing	Static
Goal	Identify weaknesses in order to stop an impending attack	Collect evidence to identify exploited vulnerabilities to prevent future attacks
Basis	Tactics, techniques, and procedures used by attacker	Known malicious activity
Scope	Detect and respond to a wide range of indicators	Document a specific attack
Position of attacker	Attempting to gain access to the system	Infiltrated system and performed successful attack

Two Rights & A Wrong

1. IOA are one or more indicators of a potential upcoming attack.
2. Tools are an important focus of IOA.
3. IOC are the digital artifacts that serve as evidence of an attack.

See the answers at the end of the chapter.

Network IOA

Certification

1.2 Given a scenario, analyze indicators of potentially malicious activity.

One of the primary sources of IOA is found in the network since it serves as the perimeter line of defense. These IOA behaviors include abnormal network traffic, stealth transmissions, scan/sweeps, and rogue network devices.

Abnormal Network Traffic

Network traffic that is not usual can be an IOA. This type of traffic can be distinguished by either its high volume or its type of activity.

Volume

Bandwidth monitoring on a network is an important activity for a network of virtually any size. There are several reasons why general (non-cybersecurity related) bandwidth monitoring is needed:

- **Monitor bandwidth agreements.** Internet bandwidth purchased from an Internet service provider (ISP) typically guarantees that the speed will be at a specific level. By monitoring network bandwidth, it can be determined if the ISP is providing the agreed-upon bandwidth as specified in the service-level agreement (SLA).
- **Troubleshoot network performance.** Network bandwidth monitoring can help identify performance issues on a network that otherwise may be difficult to isolate. In one example, an organization had

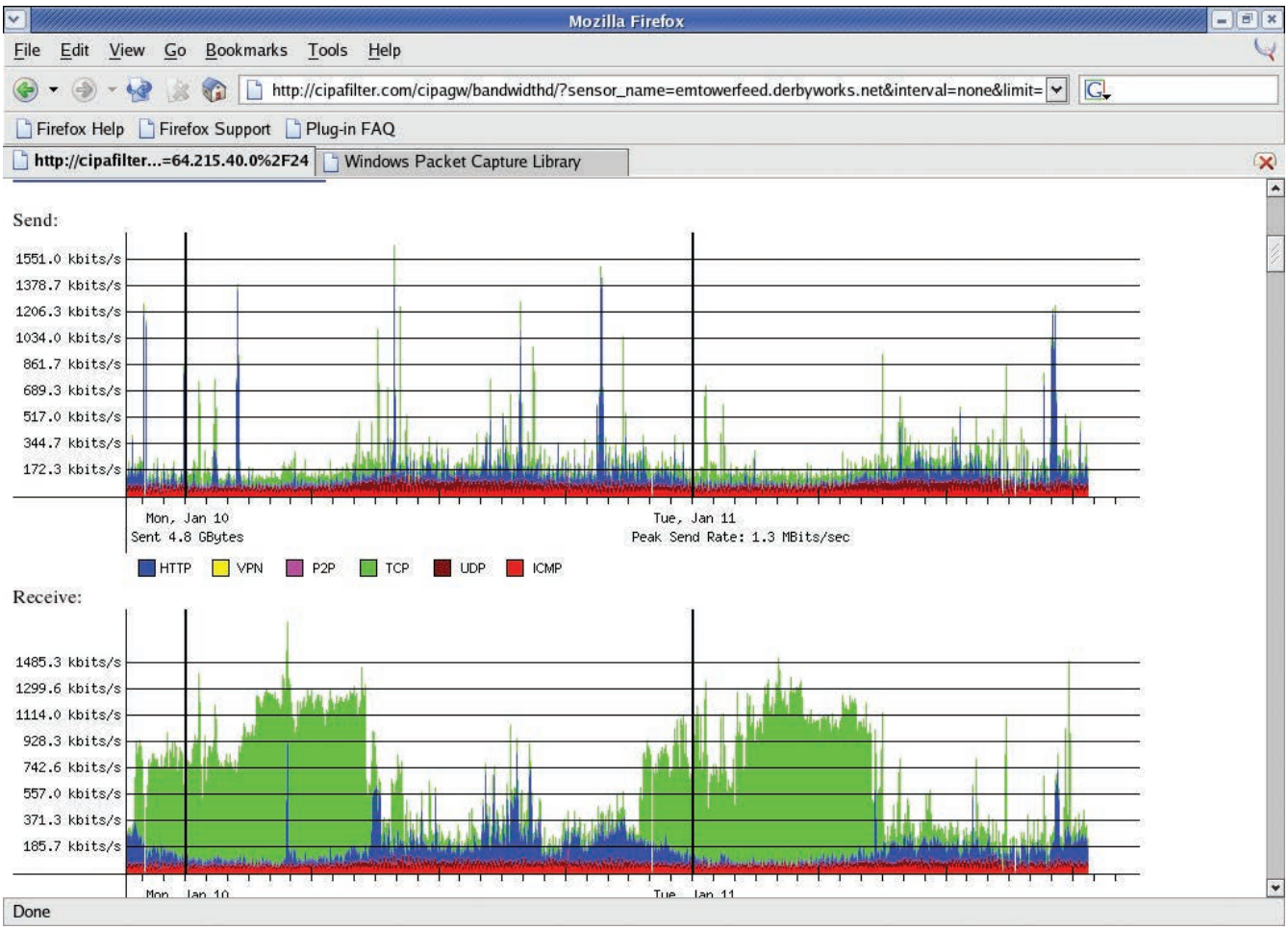
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

contracted with their ISP for what was considered an acceptable volume of bandwidth, but users constantly complained of very slow Internet access. A consultant was hired to investigate the problem. After several days of analysis, the consultant discovered that a faulty router interface was dropping packets that made up over half the entire bandwidth purchased from the ISP.

- **Identify network abuse.** With the proliferation of wireless connections, it is not uncommon for a handful of employees to monopolize wireless bandwidth to the detriment of other users. Or slow wireless network traffic may be the result of unauthorized users who are accessing the wireless network. A network bandwidth monitoring tool can analyze wireless access points (APs) and connected wireless clients to determine who is potentially abusing the network.
- **Plan for future network capacity.** By monitoring network bandwidth, organizations are better able to plan ahead for future bandwidth capacity.

A variety of tools can be used for bandwidth monitoring. Figure 4-2 shows the output graph of a basic bandwidth monitoring tool. However, more sophisticated bandwidth monitoring tools can provide enhanced dashboard data, as shown in Figure 4-3.

Figure 4-2 Basic bandwidth monitoring tool



Source: BandwidthD

Another use of network bandwidth monitoring is to look for IOA. These incidents of abnormal network traffic volume may appear as either unusual traffic spikes or overall bandwidth consumption.

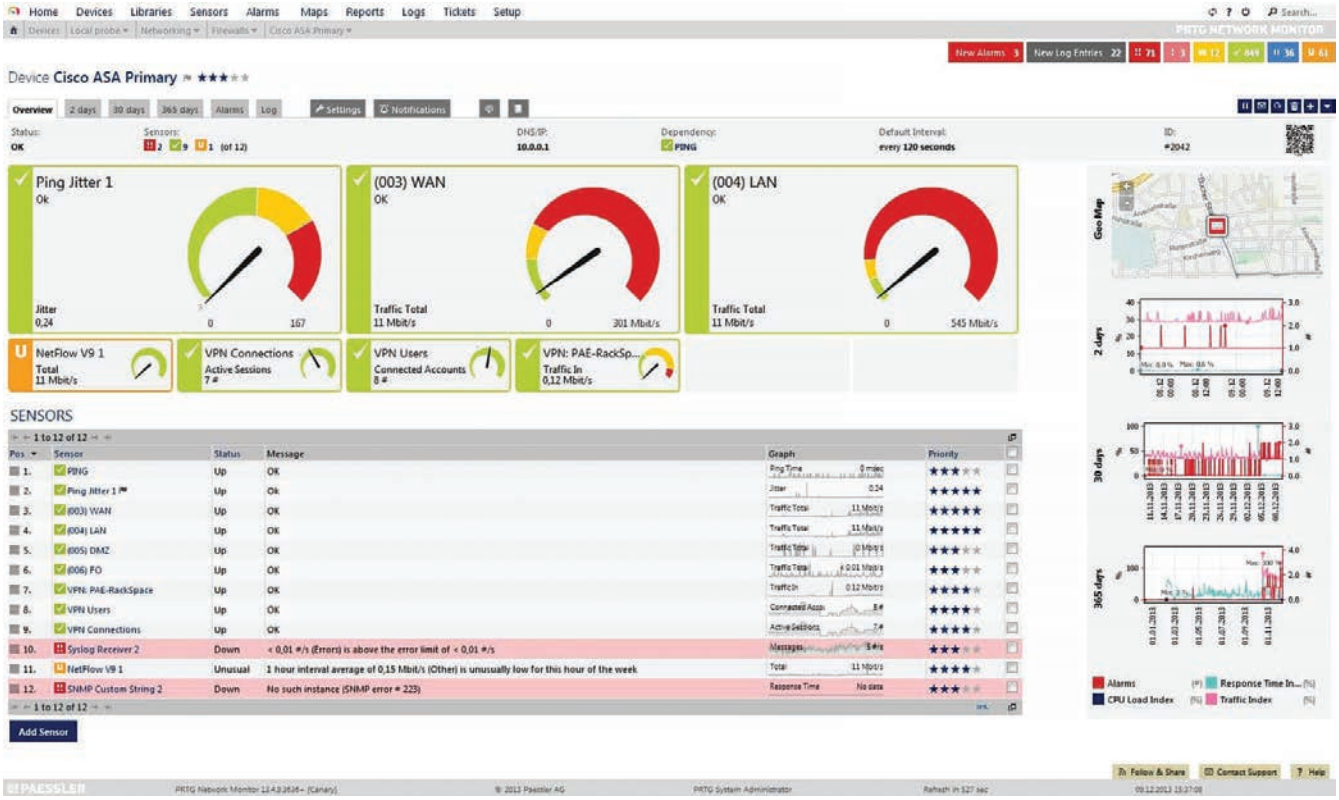
Unusual Traffic Spikes A sudden unexpected surge in network bandwidth utilization is called an **unusual traffic spike**. Figure 4-4 illustrates an unusual traffic spike.

There are several normal reasons why a network traffic spike may occur:

- **Scheduled internal backups.** Because backups contain large amounts of data, they likewise consume a large amount of bandwidth in order to be completed in a reasonable amount of time.

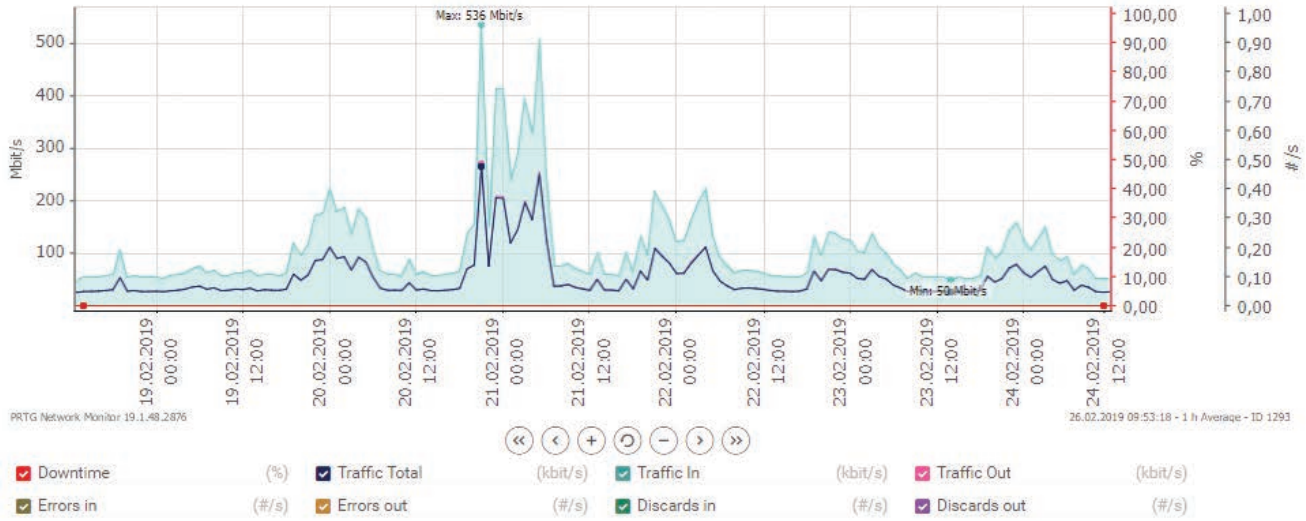
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 4-3 Enhanced bandwidth monitoring dashboard



Source: Paessler

Figure 4-4 Unusual traffic spike



Source: Paessler

- **Remote external backups.** Most organizations also perform remote backups to the cloud, which likewise may cause a traffic spike.
- **Software updates.** Operating system (OS) patches, application software updates, and other software updates can temporarily cause a spike.
- **Mail server problems.** When operating properly, an email server rarely has an impact on bandwidth. However, if a problem occurs in the delivery of email, a mail server may persistently try to send out the messages over a set period of time (usually 24 hours). If the emails contain large file attachments such as high-resolution photos or video clips, this can cause a spike.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

Traffic spikes that impact normal network functions can be damaging to the enterprise. One study revealed that for an ecommerce web service, just a one-second delay in the time it takes to load a webpage can result in a 12 percent loss in conversions (sales), while a two-second delay during transactions leads to shopping cart abandonment rates of up to 87 percent.[1]

However, traffic spikes may also be evidence of a cyber incident. In order to determine the cause of a traffic spike to know if it is normal or an IOA, a series of questions can be considered. These questions are listed in Table 4-2.

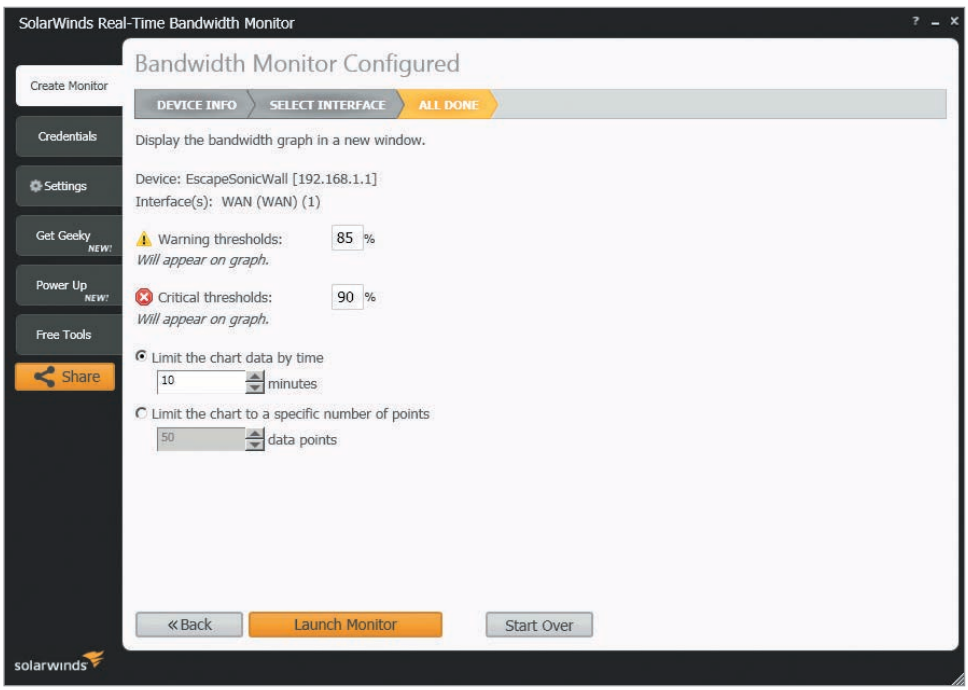
Table 4-2 Questions when determining the cause of a traffic spike

Question	Explanation
Do the spikes appear at the same time on the same day?	Identifying a pattern in the spikes may help indicate if this is a normal activity or a cyber incident.
Do the spikes occur during business hours or at other times?	A spike that occurs during business hours may indicate a user is causing the spike while a spike in off hours could be due to a scheduling issue, so further investigation is needed.
Do other monitoring points on the network match these patterns?	A CPU load spike on a server may be creating a corresponding network traffic spike.
Can the traffic be analyzed with a packet analyzer?	A packet analyzer can identify the data and underlying cause of the network spike.

However, using traffic spikes as evidence of a cyber incident is considered to be difficult for several reasons. First, because normal spikes are not uncommon, it is easy for the malware's spike to become camouflaged. In addition, malware can also be programmed to perform an event that causes a traffic spike on a regular interval, such as a large data exfiltration that occurs at 6:00 pm each Wednesday night, so that it looks like a normal event.

Bandwidth Consumption Whereas a sudden traffic spike may indicate an IOA, so can an overall increase in the amount of bandwidth being utilized (called **bandwidth consumption**). Most network bandwidth monitoring tools can be set to sound an alert when bandwidth consumption exceeds a certain threshold, as shown in Figure 4-5.

Figure 4-5 Bandwidth consumption alert



Source: SolarWinds Worldwide, LLC

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In order to set a bandwidth consumption alert, it is first important to know the normal amount of bandwidth that is being consumed. This requires that a baseline of normal bandwidth utilization be determined. Samples of bandwidth consumption should be taken over a period of time to establish the baseline.

Activity

Some types of activity on a network could indicate an IOA. Specifically, **activity on an unexpected port** could indicate that a threat actor is using a port and generating traffic that is normally not used for that purpose.

Consider a threat actor who wants to avoid detection. The attacker could use common protocols over nonstandard ports (a nonstandard port is one that is being used for a purpose other than its default assignment). For example, an infected endpoint could generate activity by using the common HTTPS protocol not over the normal Port 443 but instead over Port 143, which is normally used for Internet Message Access Protocol (IMAP) email communication.

Note 2

It is important to close unused ports, disable unnecessary protocols, and turn off unneeded services, such as Microsoft Windows ASP.NET State Service, Portable Device Enumerator Service, and Apple macOS Spotlight Indexing.

Stealth Transmissions

Stealth is defined as something done so as not to be seen or heard but instead is secretive, clandestine, or covert. Often secretive and unexpected network transmissions may be a symptom of an IOA. These stealth transmissions can be irregular internal peer-to-peer communication or external beaconing. Because threat actors go to great lengths to hide their stealth transmissions, security professionals should be vigilant in detecting them.

Irregular Peer-to-Peer Communication

Under normal network conditions, most communications will occur between multiple lower-level clients to fewer higher-level servers. However, if the clients unexpectedly begin irregular internal communication with other peers on the network (**irregular peer-to-peer communication**), this unusual symptom could be an indication of an IOA. An infected endpoint could be targeting another endpoint to spread malware or to pivot to other devices and services. This is especially true if the communications occur sporadically and at odd hours.

Beaconing

Beaconing occurs when infected devices attempt to contact the threat actor's external command and control (C&C) server. The purpose of communicating with the C&C server is usually two-way: to receive updated or new instructions from the C&C server and to upload stolen data to the C&C server.

Receive Instructions Not all compromised endpoints will access the C&C server to receive updated or new instructions with the same frequency; some endpoints will communicate on a more frequent basis than other endpoints, depending on the type of attack. One particular type of attack by its very nature receives a large number of instructions from a C&C server. This is an attack that places the infected device under the remote control of an attacker for the purpose of launching attacks on other remote devices. The infected robot computer is known as a bot or zombie. When hundreds, thousands, or even millions of bot computers are gathered into a logical computer network, they create a botnet under the control of a bot herder. Table 4-3 lists some of the attacks that can be generated through botnets.

Note 3

In early 2021, one of the most notorious botnets known as Emotet was taken down by law enforcement agencies seizing its C&C servers. The takedown required the participation and cooperation of law enforcement agencies from eight different countries. In existence since 2014, Emotet, which infected over one million endpoints, was used to spread a wide array of malware, most notably ransomware, and may be responsible for losses by victims exceeding $2.5 billion. And in an interesting twist, because the C&C servers are now under the control of law enforcement, an update will be sent to all infected endpoints from the C&C servers that will disable the malware on them.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 4-3 Uses of botnets

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of bots enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new bots and botnets. Bots have the ability to download and execute a file sent by the attacker.
Manipulating online polls	Because each bot has a unique IP address, each "vote" by a bot will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.
Denying services	Botnets can flood a web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests.

Steal Data Attacks that are designed to steal data will communicate with the C&C server as the means to transport the data back to the threat actors. A variety of techniques can be used, and it often depends on the cunning and ingenuity of the threat actors. This can be illustrated by the infamous attack on the point of sale (PoS) terminals at Target Corporation that lasted only three weeks but resulted in over 40 million credit and debit cards stolen along with 70 million records of personally identifiable information (PII) including the name, address, email address, and phone number of Target customers. As credit and debit card data was captured whenever a customer swiped their card at a PoS terminal, the card numbers were encrypted and uploaded back to the Target network to be deposited on Target internal servers that were under the control of the threat actors, who had also installed backdoors on three Target FTP (File Transfer Protocol) servers. These backdoors were created using carefully chosen usernames to blend in with network management software. At set intervals, the stolen information was sent to the closest Target FTP server and then transferred to C&C servers in Miami and Brazil.

Note 4

The impact of the attack on Target was substantial. Not only was the Target CEO forced to resign due to the incident, but Target registered a 46 percent decline in profits compared to the prior year, much of it attributed to consumer backlash at the attack. Target was also forced to spend over $100 million upgrading its PoS devices.

Hiding Transmissions

Threat actors use different techniques to hide their stealth transmissions so they are harder to detect. One technique is to use standard network protocols that do not attract attention. For example, when sending stolen data, the malware may use the HTTP protocol, which can easily blend into normal traffic. However, the volume of traffic may make the beaconing detectable: HTTP traffic generally has more volume incoming from external sources than outgoing, so that threat actors exporting large amounts of stolen data could be identified.

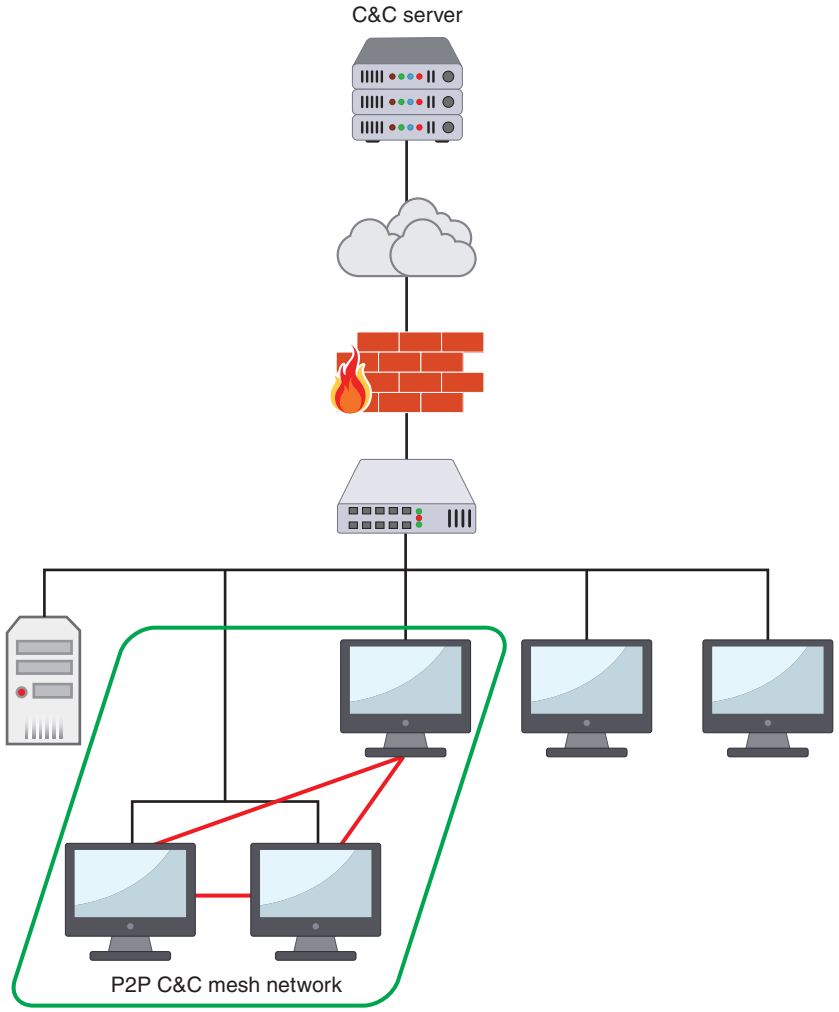
Note 5

In the Target attack, stolen data was only sent internally to the Target FTP servers during peak times of the day in order to hide evidence of communications. And because FTP was a common protocol used by Target, this did not raise suspicion.

A more advanced technique to mask both types of stealth transmissions—irregular peer-to-peer communications and data exfiltration through beaconing—is to combine standard protocols with an internal mesh network of infected devices so that the devices can communicate between each other easily. This allows for a single compromised endpoint to act as an internal C&C device. This one device receives instructions from the threat actor's main C&C server and then distributes these commands to other compromised endpoints, while also acting as the single exit point for sending stolen data back to the threat actor's main external C&C server. This is called a peer-to-peer command and control (P2P C&C) configuration and is illustrated in Figure 4-6.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 4-6 P2P C&C



A P2P C&C configuration has several advantages for a threat actor:

- **Reduced number of external beacons.** A P2P C&C has only one single device that performs beaconing with the C&C server instead of each device. This results in less traffic beyond the edge of the network that likely would not raise suspicion.
- **Aligns with traffic inspection prioritizations.** Most security technicians tend to maximize the priority of inspecting external traffic on the edge of the network while minimizing inspection on the internal network. The assumption is that there is more risk from external traffic than internal traffic. Because a P2P C&C has only one device communicating externally, it better aligns with this tendency.
- **Does not use restricted protocols.** Most networks treat certain classes of traffic differently depending on if it is used internally within the network or at the edge of the network for external communications. A P2P C&C does not have to rely on restricted protocols that draw attention.

One means of how a P2P C&C can circumvent restricted protocols can be illustrated in the following example. HTTP traffic (Port 80) is routinely allowed as outbound over the edge of the network so that employees may browse the Internet; however, HTTP traffic is restricted if it originates from internal servers or a high-value network subnet. A standard C&C approach that requires each infected device to maintain contact with restricted servers or high-value subnets using restricted protocols like HTTP will raise red flags.

In a P2P C&C configuration, external beaconing typically uses HTTP because this protocol is so common. For an internal network that uses Microsoft Windows devices, a common protocol widely used is Server Message Block (SMB). A named pipe is a logical connection (like a TCP session) between a client and server that uses SMB. The name of the pipe serves as the endpoint for communication in the same way that a port number serves as the endpoint for TCP sessions. Thus, named pipes, a native

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Windows technology that allows for interprocess communication across remote systems over the SMB access protocol, can be used for internal P2P C&C communication. This allows for the internal devices to communicate through the mesh network using common protocols without raising any alarms.

Note 6

SMB is not the only protocol that can be used internally for P2P C&C. Essentially any protocol that supports reading and writing data between two devices could be used. Other interprocess communication options on a Windows network include Windows Management Instrumentation (WMI), Windows Mailslots, and even Active Directory (AD).

Detecting Transmissions

It is generally recognized that detecting P2P C&C can be difficult since the traffic uses standard protocols to blend in with normal internal and external network traffic. However, some symptoms can be helpful in detecting a P2P C&C. These include:

- **Abnormal processes to named pipes.** After collecting and creating a baseline process to named pipe relationships, security professionals can watch for new events compared to the baseline.
- **Known malicious named pipe names.** If the threat actor does not change the default name of the named pipes that now generate large amounts of traffic, this could be a symptom of a cyber incident.
- **Abnormal named pipe security descriptors.** P2P C&C often applies a single security descriptor to a named pipe that allows full control to an *Everyone* group. Monitoring named pipe security descriptors can also be a symptom.

When examining networks for stealth transmissions the following may serve as symptoms:

- **Remote connections to named pipes.** Using a network tap or collector, SMB network traffic can be inspected to look for a remote connection to named pipes.
- **Abnormal host-to-host traffic.** If certain high-value servers rarely if ever create network connections with certain network subnets that contain user workstations but suddenly a high number of network connections is identified from one of these high-value servers to a workstation subnet, this could be identified as abnormal.

Note 7

Detection of a P2P C&C is considered difficult because it uses normal protocols and features. Generally speaking, it may be easier to detect malicious behaviors of the infected device itself.

Scans/Sweeps

In preparation for unleashing a cyber incident, threat actors will perform **scans/sweeps** on a network to uncover any vulnerabilities. These scans/sweeps include ping sweeps (determining if a device is "awake") and port scans (looking for available services on open ports). Any scans/sweeps originating from unknown IP addresses should serve as a potential IOA that should be investigated.

Rogue Network Devices

A final symptom of an IOA is unauthorized devices on a network, called **rogue devices on a network**. On a wired network, a rogue device may attempt to monitor network traffic. For example, a managed switch on an Ethernet network that supports port mirroring allows the network administrator to configure the switch to copy traffic that occurs on some or all ports to a designated monitoring port on the switch. A threat actor (or more likely an insider who is performing work for the threat actor) can connect a rogue monitoring computer to the mirror port and then view all network traffic moving through the switch (the monitoring computer can be a standalone device or a computer that runs protocol analyzer software).

On a wireless network, a rogue mobile device can connect to a weakly protected wireless network. These are particularly dangerous since they can provide unfettered access to the entire network, bypassing network security protections or tricking users into connecting with a sinister AP.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Several methods can be used to detect a rogue AP by continuously monitoring the radio frequency (RF) airspace. This requires a special sensor called a wireless probe, a device that can monitor the airwaves for traffic. There are four types of wireless probes:

- **Wireless device probe.** A standard wireless device, such as a portable laptop computer, can be configured to act as a wireless probe. At regular intervals during the normal course of operation, the device can scan and record wireless signals within its range and report this information to a centralized database. This scanning is performed when the device is idle and not receiving any transmissions. When a large number of mobile devices are used as wireless device probes, it can provide a high degree of accuracy in identifying rogue access points.
- **Desktop probe.** Instead of using a mobile wireless device as a probe, a desktop probe utilizes a standard desktop computer. A universal serial bus (USB) wireless adapter is plugged into the desktop computer to monitor the RF frequency in the area for transmissions.
- **Access point probe.** Some AP vendors have included in their APs the functionality of detecting neighboring APs, friendly as well as rogue. However, this approach is not widely used. The range for a single AP to recognize other APs is limited because APs are typically located so that their signals overlap only in such a way as to provide roaming to wireless users.
- **Dedicated probe.** A dedicated probe is designed to exclusively monitor the RF frequency for transmissions. Unlike access point probes that serve as both an AP and a probe, dedicated probes only monitor the airwaves. Dedicated probes look very similar to standard access points.

Note 8

Once a suspicious wireless signal is detected by a wireless probe, the information is sent to a centralized database where wireless LAN (WLAN) management system software compares it to a list of approved APs. Any device not on the list is considered a rogue AP. The WLAN management system can instruct the switch to disable the port to which the rogue AP is connected, thus severing its connection to the wired network.

Any unknown network device that is discovered connected to the network should be treated as an unauthorized device and immediately disconnected from the network. Further investigation should reveal if the device is being used by threat actors or is the result of a faulty change control process.

Two Rights & A Wrong

1. One of the primary sources of IOA is found in the network since it serves as the perimeter line of defense.
2. Using traffic spikes as an IOA is straightforward and transparent.
3. Beaconing occurs when infected devices attempt to contact the threat actor's external C&C server.

See the answers at the end of the chapter.

Endpoint IOA

Certification

1.2 Given a scenario, analyze indicators of potentially malicious activity.

Throughout the years, different words have been used to describe network-connected hardware devices. Forty years ago, when the TCP/IP protocol was becoming popular, the word *host* referred to any communicating device on the network (networks were made up of hosts). Thirty years ago, as servers became more popular, the word *client* was also used (clients made requests to servers). Twenty years ago, the term *workstation* described a special computer designed for scientific or highly technical applications.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Today, another word is commonly used when referring to network-connected hardware devices: *endpoints*. This change reflects the fact that today computing devices are far more than a desktop computer with a keyboard and monitor. Instead, devices ranging from mobile smartphones and tablets to wearable fitness trackers, industrial control system sensors, automotive telematics units, and even personal drones are all network-connected hardware devices. The word *endpoint* has become a more accurate description of today's technology devices.

This change in terminology also reflects the fact that increased risks have multiplied—exponentially—with the increasing number of these devices. They have become a prime target for attackers. And because the endpoints are connected to some type of network, a vulnerability on a single endpoint can result in an attack that penetrates the network and infects all other connected endpoints. Every endpoint can be a potential entry point for attackers.

IOA can also be found on endpoints. The evidence includes a high-volume consumption of resources, evidence that is OS and software related, and data exfiltration.

High-Volume Consumption of Resources

Consider a homeowner who receives a monthly electric bill. The bill lists both the amount due based on the current usage of electricity and also includes a comparison of that month against the same month over the last five years. Suppose one month the bill unexpectedly shows the amount due is triple what it has been over the last five years. The homeowner would certainly investigate why there was the sudden increase in electrical usage. Was it an unusually hot month that required the air conditioner to run around the clock? Was a window left open in an unoccupied room? Did an unscrupulous neighbor tap into the electrical connection to siphon off electricity? The unexpectedly high amount of electricity used would certainly serve as an indication that something unusual had occurred.

Likewise, with an endpoint system, an abnormally high volume of resource consumption can be an IOA. The categories of consumption of resources include processor, memory, and drive capacity.

Processor

Unlike previous generations of central processing units (CPUs) that contained only one core that received instructions and performed actions, modern processors contain multiple cores (usually 2–24). In addition, today's processors use simultaneous multithreading or hyperthreading that can split each core into multiple threads or virtual cores. Thus, a single physical CPU chip has the capacity of multiple CPUs all working together.

Note 9

Some software programs are better able to take advantage of multiple threads than others. Games are considered "lightly threaded" and do not benefit as much from multiple cores while video editing programs can run much faster with extra threads.

Intel brand CPUs now integrate two types of cores into a single CPU: powerful performance-cores (P-cores) and flexible efficient-cores (E-cores). These cores have different roles. The characteristics of P-cores are:

- Physically larger, high-performance cores designed for raw speed
- Tuned for higher frequencies and a higher number of instructions per cycle (IPC)
- Designed for "crunching" through the heavy single-threaded work
- Capable of hyperthreading (running two software threads simultaneously)

E-cores have these features:

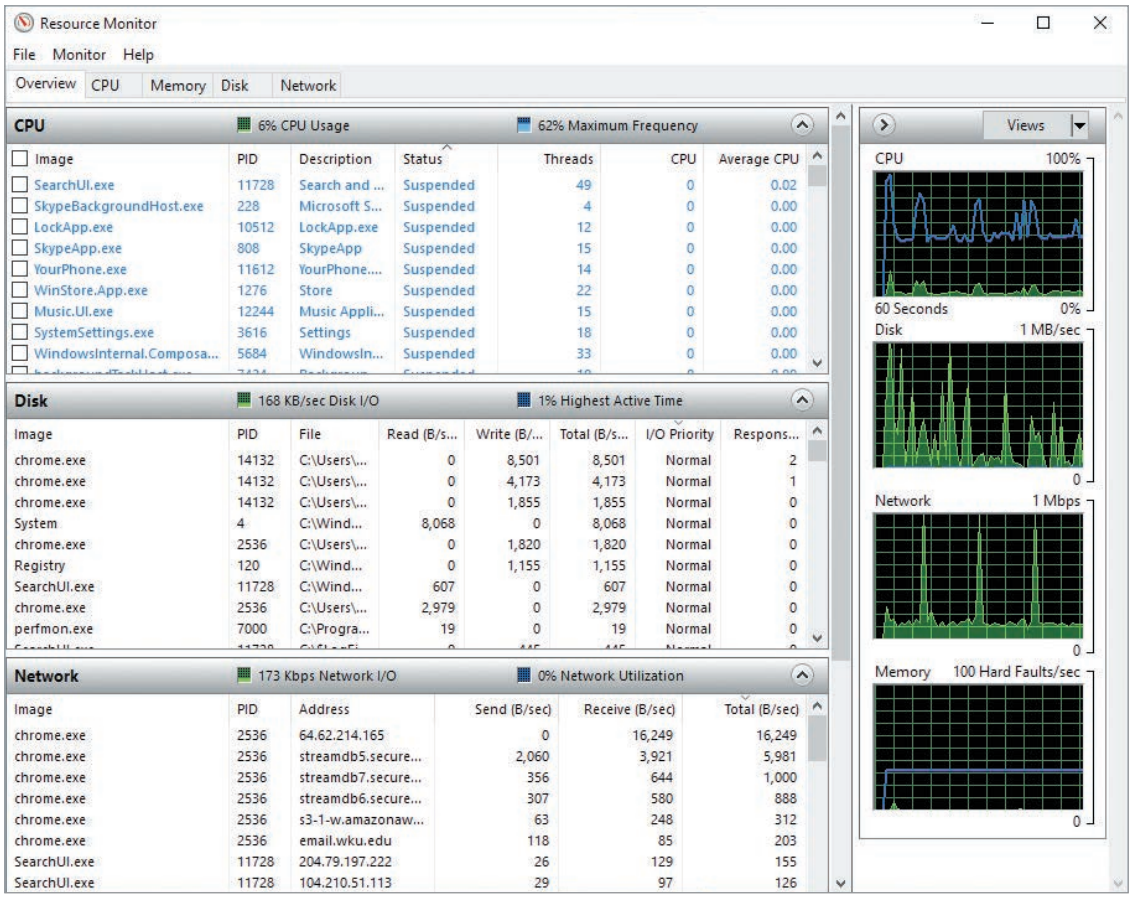
- Physically smaller, with multiple E-cores fitting into the physical space of one P-core
- Designed to maximize CPU efficiency
- Designed for scalable and multithreaded performance
- Work in concert with P-cores to accelerate "core-hungry" tasks such as rendering video
- Optimized to run background tasks efficiently so that smaller tasks can be offloaded to E-cores
- Capable of running a single software thread

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Threat actors take advantage of fast processors with multiple cores. Malware that infects an endpoint computer can run utilizing multiple cores and threads without any appreciable impact upon the normal tasks that the user is performing. This shows no impact on the processor's performance and thus the user is unaware of the presence of malware. However, if the malware performs a significantly complicated or lengthy task, then the processor may begin to slow down to the point that it becomes apparent.

Several tools can be used to determine if the reason the processor's resources are being taxed is a result of an IOA (called **processor consumption**). A resource monitor can audit and display the CPU along with other endpoint resources. Figure 4-7 shows the Microsoft Windows Resource Monitor.

Figure 4-7 Microsoft Windows Resource Monitor



Source: Microsoft Corporation

Memory

Abnormal **memory consumption** could likewise be a symptom of an IOA. As malware loads into RAM, it may consume large parts of memory, causing the host to slow down or become unstable. Memory consumption can be identified by resource monitor tools.

Drive Capacity

For over 40 years, hard disk drives (HDDs), which used spinning platters, actuator arms with read/write heads, and motors to store and retrieve data, were the mainstay of computer storage. However, today computers use solid-state drives (SSDs), which essentially store data on chips instead of magnetic platters. Because SSDs lack moving parts, they are more resistant to failure and thus are more reliable than HDDs. Most servers utilize both HDDs and SSDs: the server boots from an SSD (due to its speed and reliability) but stores its data on an HDD (due to the lower cost of these drives). Most user SSDs have capacities ranging from 120 gigabytes (GB) to 8 terabytes (TB) while larger systems can accommodate drives up to 30 TB.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 10

Data accumulated over 10 years on 230,921 HDDs and SSDs confirm that SSDs are more durable than HDDs. Over their first four years of service, SSDs fail at a lower rate than HDDs overall. In the fifth year, HDD failure rates begin going up much more quickly, while SSDs continue to fail at roughly the same rate (about 1 percent) as they did in prior years.

Drive capacity consumption refers to the unexpected loss of available drive space as a result of malware. This may be due to malware gathering files from several different hosts or servers prior to data exfiltration, or it can be because of continual scan sweeps performed by malware that results in the rapid increase in the size and number of log files. Resource monitor tools can help provide clues to determine if drive capacity consumption is a symptom of a cyber incident.

Note 11

With multicore CPUs, large RAM capacity, and drives that measure in the billions and trillions of bytes of storage, it is easy for malware to hide in these resources and not be detected. Establishing baselines can be helpful in identifying if high-volume consumption is a result of malware.

Operating System Evidence

Evidence of an IOA can most often be found in the OS running on the endpoint, as this is a frequent target of threat actors. Evidence from the OS includes:

- **Malicious process.** A process is the instance of a computer program that is being executed by one or more threads; that is, it is an application in execution. Threat actors often will create an unauthorized **malicious process** that the OS runs. These can be difficult to detect and trap. A single malicious process may launch ("spawn") multiple interdependent processes. These can easily hide among the normal processes from user programs along with the normal OS processes. This makes it easy for a malicious process to remain hidden.

Note 12

It is not uncommon for Microsoft Windows to run over 50 background processes and over 100 Windows processes in its normal operation.

- **Abnormal OS process behavior.** Threat actors will also attempt to change a normal process into performing a malicious action, known as **abnormal OS process behavior**.
- **File system changes.** Changes to files (**file system changes or anomaly**) may serve as an IOA as threat actors infect or modify a file. However, on a normal day, a system may see hundreds of file system changes on a single endpoint, making it difficult to identify abnormal file changes.
- **Changes to registry.** The Windows registry is a database that stores low-level settings for the Windows OS and applications. Device drivers, services, the OS kernel, and some security applications use the registry. Unexpected modifications or an abnormal registry setting (**registry changes or anomaly**) can serve as an IOA.
- **Unauthorized scheduled task.** A modern OS will run specific operations (tasks) at a certain time or when an event occurs (such as when a user logs on). In addition, users can also create their own tasks with "triggers" that launch the task but are modified by "conditions." An **unauthorized scheduled task** that was not approved and initiated by an administrator can often be an IOA.
- **Unauthorized changes.** Often threat actors will attempt to make changes to OS system settings, particularly as they relate to security. These **unauthorized changes** to system security policies are common. If the threat actor can manipulate the security settings, such as disabling anti-malware software, then their malicious software has a better chance of running undetected.
- **Unauthorized privileges.** Another change is **unauthorized privilege**. Access rights are privileges to access hardware and software resources that are granted to users or devices. OSs and many applications

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

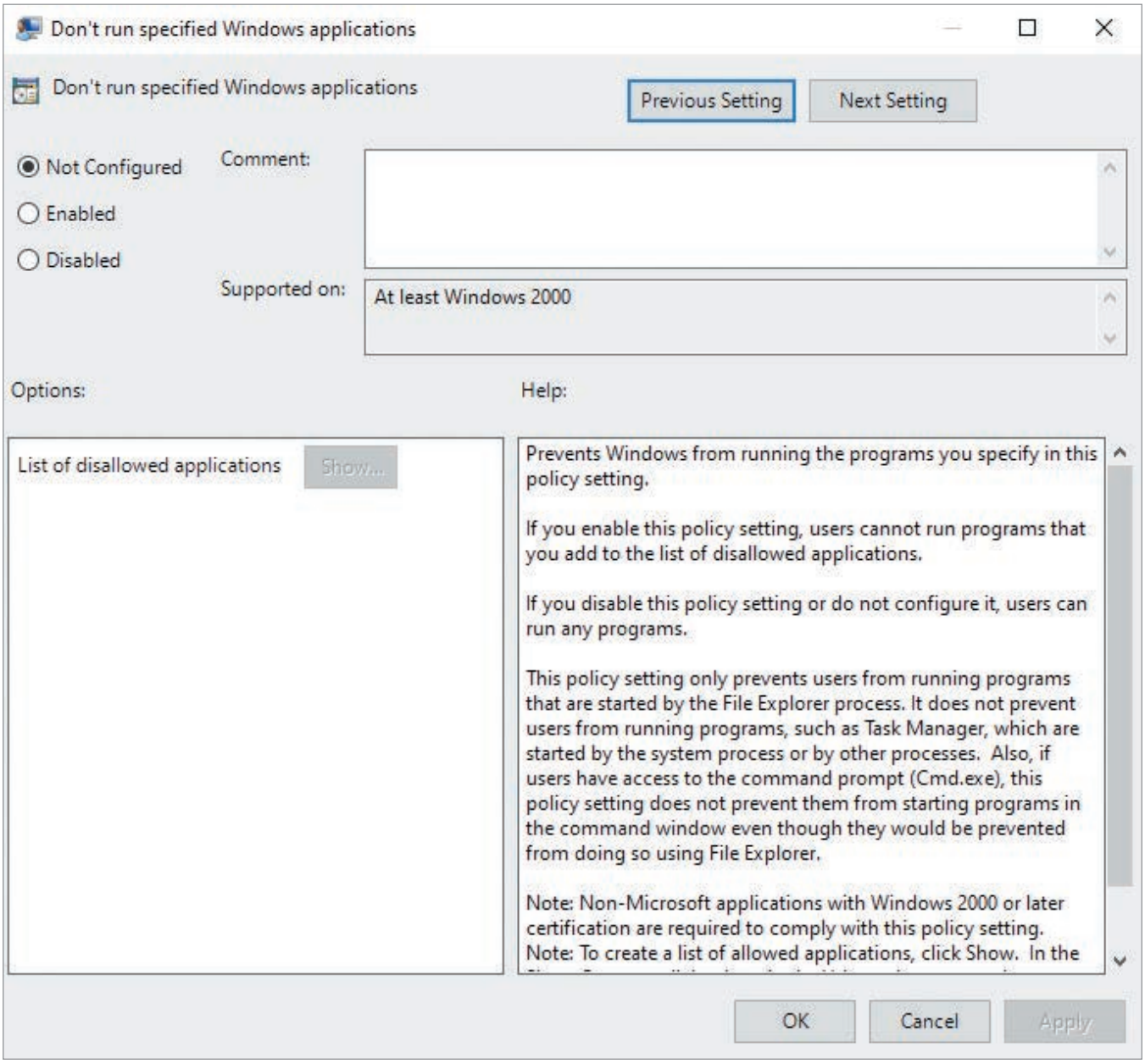
have the ability to restrict a user's privileges in accessing its specific functions. Creating unauthorized privileges is changing OS settings or exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from accessing.

Software-Related Evidence

Evidence of a cyber incident can also be found in software. The most obvious evidence is **unauthorized software** (applications that are not approved) that is silently installed by threat actors on the endpoint.

Most organizations simply restrict users from installing unauthorized software by configuring their user account to "standard" instead of "administrator" and thus not provide them with privileges to install software. However, restricting unauthorized software from running on a computer in which the user has administrative privileges can be much more difficult. Some OS configurations allow an administrator to create a preapproved list of software that is permitted to run. Figure 4-8 illustrates creating an approved list for a Microsoft Windows host using Group Policy; other Windows options include using Windows AppLocker or restricting through the Windows Registry.

Figure 4-8 Microsoft Windows Group Policy software approved list



Source: Microsoft Corporation

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Data Exfiltration

Another symptom is the attempts by threat actors to steal data and transfer it to an external source (**data exfiltration**). Symptoms often include drive consumption on select servers that serve as "staging areas" for accumulating the data into a single location before it is exported.

Two Rights & A Wrong

1. A process is the instance of a computer program that is being executed by one or more spawns.
2. Abnormal memory consumption can be identified by resource monitor tools.
3. Modern processors use simultaneous multithreading or hyperthreading, which can split each core into multiple threads or virtual cores.

See the answers at the end of the chapter.

Application IOA

Certification

1.2 Given a scenario, analyze indicators of potentially malicious activity.

Several IOA relate to applications. These include unusual activity, new account creation, unfamiliar outbound communications, and modified application logs.

Unusual Activity

An application that suddenly exhibits unusual activity from its normal activity may be the result of a cyber incident. These activities include:

- **Anomalous activity.** An application that has been functioning normally that suddenly exhibits unusual or strange behavior (**anomalous activity**) could indicate that the application simply needs to be reinstalled. However, it may also indicate that malware has altered an application in some way, such as a virus infecting an application and causing it to function erratically.
- **Unexpected output.** An application that suddenly gives output that is unanticipated, such as an error message that is poorly formatted or a request for unusual user input, may be an indication of a malware infection. This is called **unexpected output**.
- **Service interruptions.** Some applications link to other applications for data exchange or communication. For example, object linking and embedding (OLE) is a Microsoft technology that facilitates the sharing of application data and objects written in different formats from multiple sources and applications. When a **service interruption** occurs in this feature, it may be a symptom of a cyber incident.

New Account Creation

For a higher level of security, some applications require that a separate user account be created and stored in a database linked to the application. This means that a user must log in to the application, separate from logging in to the OS.

Malware can often attempt to compromise this user application database by creating a new account (**introduction of new accounts**). This could allow the threat actor to log in to the application or for a malicious running process to connect to the application itself. In either case, an unexpected new account creation should be immediately investigated.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

For enhanced security, some Windows applications can make the user application database dependent on the current Windows user account. This means that you can only log in to the application (open the application database) when you are logged in as the same Windows user when creating the database. However, caution should be used with this option. If the Windows user account is deleted or the OS must be reinstalled, you will no longer be able to open the application database. And creating a new Windows account on the new installation with the old username and password will still not allow you access to the application database.

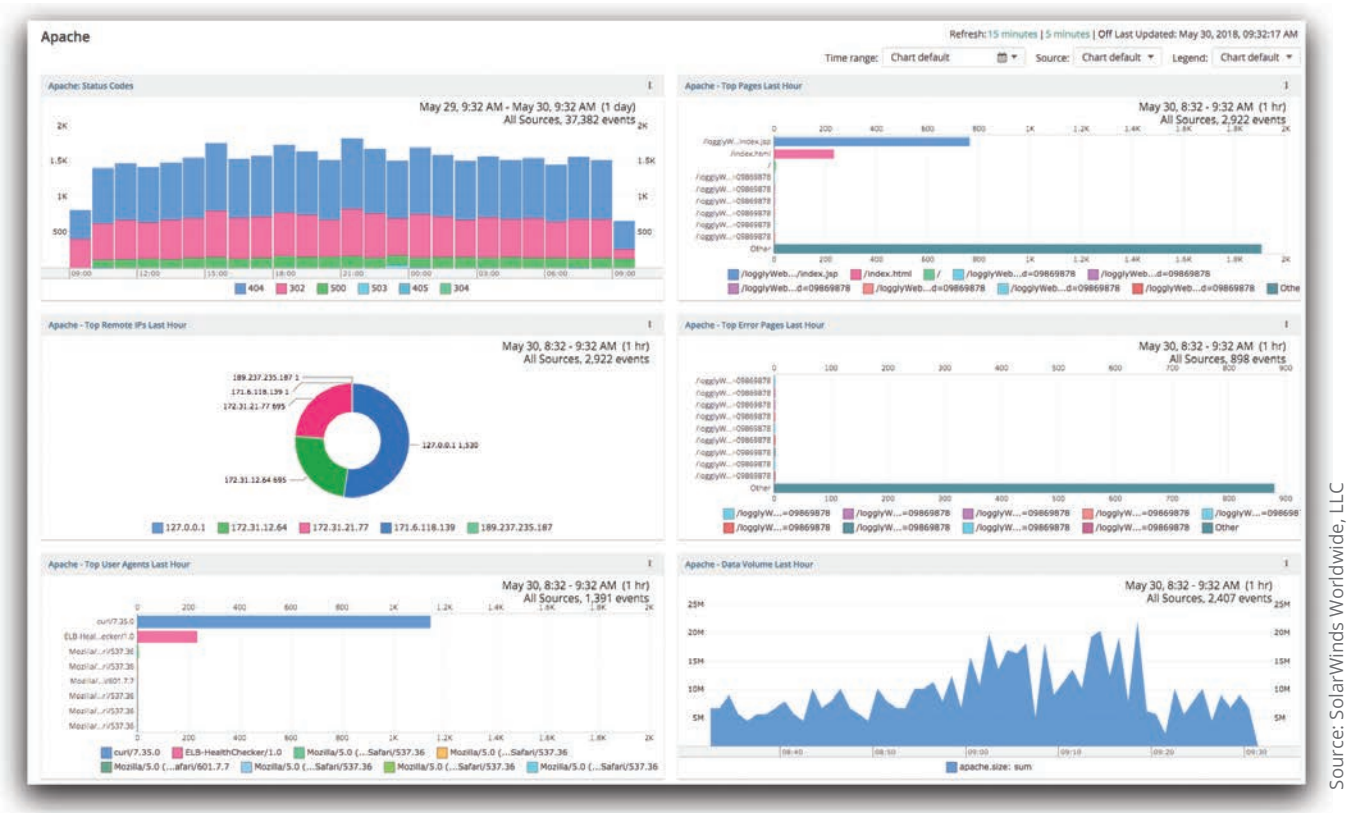
Unexpected Outbound Communication

An application that has the capacity for external communication, such as through an internal FTP feature, that unexpectedly begins performing outbound communication should be considered as compromised. Any unfamiliar and unanticipated outbound communication (**unexpected outbound communication**) is likely an indicator of an application compromise.

Modified Application Log

An **application log** records events, transactions, and errors that occur within a software application. It contains information such as timestamps, the severity of the event, and relevant supporting information for providing a "context" of the event. Figure 4-9 illustrates a web application log.

Figure 4-9 Application log



Source: SolarWinds Worldwide, LLC

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Application logs can be analyzed for performance analysis, auditing, and troubleshooting. Knowing this, threat actors, as a means of "covering their tracks," often attempt to edit the application log that reveals their actions, such as what applications were launched when and by whom. A changed log file, called a modified application log, can be used in cybersecurity as an IOA.

Note 13

In addition to attempting to edit an application log, the application logs themselves can contain sensitive information that attackers target. This includes user credentials or system configuration details.

Two Rights & A Wrong

1. An application that suddenly gives output that is unanticipated is called anomalous activity.
2. An application log typically contains timestamps and the severity of the event.
3. For a higher level of security, some applications require that a separate user account be created and stored in a database linked to the application.

See the answers at the end of the chapter.

Summary

- Preliminary behaviors of threat actors that are detected are called indicators of attack (IOA). A SOC searching for IOA is focused on detecting the intention of the threat actor as evidenced by their actions. IOA are not evidence that an attack is already underway but are one or more indicators of a potential upcoming attack. The digital artifacts that serve as evidence of an attack are called indicators of compromise (IOC). This evidence is used to determine what deficiencies exist and what should be fixed. IOC are one or more indicators of a successfully completed attack.
- One of the first IOA is found in the network. Bandwidth monitoring on a network is an important activity for normal network operations. Another use of network bandwidth monitoring is to look for evidence of a cybersecurity incident. A sudden unusual surge in network bandwidth utilization is called an unusual traffic spike, which may be evidence of an IOA. Whereas a sudden traffic spike may indicate a cyber incident, so can an overall increase in the amount of bandwidth being utilized, known as bandwidth consumption. Some types of activity on a network could indicate an IOA. For example, activity on an unexpected port could indicate that a threat actor is using a port and generating traffic that is normally not used for that purpose.
- Often secretive and unexpected network transmissions may serve as an IOA. Under normal network conditions most communications will occur between multiple lower-level clients to fewer higher-level servers. However, if the clients unexpectedly begin irregular internal communication with other peers on the network (irregular peer-to-peer communication), this unusual symptom could be an indication of a cyber incident. An infected endpoint could be targeting another endpoint to spread malware or to pivot to other devices and services. Beaconing occurs when infected devices attempt to contact the threat actor's external command and control (C&C) server. The purpose of communicating with the C&C server is usually two-way: to receive updated or new instructions from the C&C server and to upload stolen data to the C&C server.
- In order to mask or hide stealth transmissions to hinder or prevent detection, typically malware will not use a distinctive protocol that can be easily identified. Instead of distinctive protocols, threat actors may use standard network protocols that do not attract attention. For example, when sending stolen data, the malware may use the HTTP protocol, which can easily blend into normal traffic. However, the volume of traffic may make the beaconing detectable. Another technique used to mask stealth transmissions is to combine standard protocols with

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

an internal mesh network of infected devices so that the devices can communicate between each other easily. This allows for a single compromised endpoint to act as an internal C&C device. It is generally recognized that detecting P2P C&C can be difficult since the traffic uses standard protocols to blend in with normal internal and external network traffic.

- In preparation for unleashing a cyber incident, threat actors will attempt to perform scans/sweeps on a network to uncover any vulnerabilities. These include ping sweeps and port scans. Another symptom of a cyber incident is unauthorized devices on a network. On a wireless network, a rogue mobile device can connect to a weakly protected wireless network. These are particularly dangerous since they can provide unfettered access to the entire network, bypassing network security protections or tricking users into connecting with a sinister AP.
- IOA can also be found on endpoints. An endpoint system with an abnormally high volume of resource consumption is often an IOA. If malware infects an endpoint that performs a significantly complicated or lengthy task, then the processor may begin to slow down to the point that it becomes apparent. Abnormal memory consumption could likewise be a symptom of a cyber incident. Drive capacity consumption refers to the unexpected loss of available hard drive space as a result of malware. This may be due to malware gathering files from several different hosts or servers prior to data exfiltration, or it can be because of continual scan sweeps performed by malware that results in the rapid increase in the size and number of log files.
- Evidence of a compromise can most often be found in the OS running on the endpoint. Indicators include a malicious process, abnormal process behavior, file system changes, changes to the registry, an unauthorized scheduled task, unauthorized changes, and unauthorized privileges. Unauthorized software applications that are silently installed by attackers to an endpoint can also be an IOA. Another symptom is the attempts by threat actors to steal data and transfer it to an external source (data exfiltration). Symptoms often include hard drive consumption on select servers that serve as "staging areas" for accumulating the data into a single location before it is exported.
- Several indicators of a cyber incident relate to applications. An application that suddenly exhibits unusual activity from its normal activity may be the result of a cyber incident. These activities include anomalous activity, unexpected output, and service interruptions. Malware can often attempt to compromise this user application database by creating a new account. This could allow the threat actor to log in to the application or for a malicious running process to connect to the application itself. An application that has the capacity for external communication that unexpectedly begins performing outbound communication should be considered as IOA. A changed log file, called a modified application log, can be used in cybersecurity as an IOA.

Key Terms

abnormal OS process behavior
activity on an unexpected port
anomalous activity
application log
bandwidth consumption
beaconing
data exfiltration
drive capacity consumption
file system changes or anomaly
indicators of compromise (IOC)
introduction of new accounts
irregular peer-to-peer communication
malicious process
memory consumption
processor consumption
registry changes or anomaly
rogue devices on a network
scans/sweeps
service interruption
unauthorized changes
unauthorized privilege
unauthorized scheduled task
unauthorized software
unexpected outbound communication
unexpected output
unusual traffic spike

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Review Questions

1. Which types of indicators are focused on detecting the intention of the threat actor as evidenced by their actions?
   - **a.** IOC
   - **b.** IOD
   - **c.** IOA
   - **d.** IOZ
2. Which of the following is NOT a reason why bandwidth monitoring is needed?
   - **a.** Locate rogue AP.
   - **b.** Troubleshoot network performance.
   - **c.** Identify network abuse.
   - **d.** Monitor bandwidth agreements.
3. Which of the following is a valid reason for an unusual network traffic spike?
   - **a.** Mail server problems
   - **b.** Software updates
   - **c.** Scheduled internal backup
   - **d.** Remote email session
4. Why are unusual traffic spikes evidence of an IOA difficult to detect?
   - **a.** Attacks can perform an event that causes a traffic spike but appears as a normal event.
   - **b.** Threat actors use different techniques for beaconing other than using a network in order to not draw attention to the action.
   - **c.** There are no specific tools that can be used to detect an IOA unusual traffic spike.
   - **d.** There is always a time lag in detecting traffic spikes and by the time they are recognized as an IOA it is too late.
5. What is the name for an IOA in which a threat actor uses the HTTPS protocol over Port 443?
   - **a.** Masked activity
   - **b.** Activity on an unexpected port
   - **c.** Rogue transmission
   - **d.** Hidden communication
6. Which of the following is NOT correct about irregular peer-to-peer communication?
   - **a.** It could be evidence of an infected endpoint targeting another endpoint.
   - **b.** These communications always occur at set intervals on a regular schedule.
   - **c.** Under normal network conditions, most communications will occur between multiple lower-level clients to fewer higher-level servers.
   - **d.** It could be an indication that an infection is attempting to pivot to other devices and services.
7. What is the definition of beaconing?
   - **a.** A rogue network device connecting to an AP.
   - **b.** An infected device attempting to contact a C&C server.
   - **c.** Malware that spreads through the network by connecting to other devices.
   - **d.** A compromised device that downloads exfiltrated data.
8. What is the first step in monitoring bandwidth consumption to determine if there has been a cyber incident?
   - **a.** Identify an open port on the router.
   - **b.** Install a packet tracker on the network.
   - **c.** Receive permission from their Internet Service Provider (ISP).
   - **d.** Establish a baseline of normal bandwidth utilization.
9. Which of the following is NOT a type of attack that can be generated through a botnet?
   - **a.** Spamming
   - **b.** Spreading malware
   - **c.** Buffer overflows
   - **d.** Manipulating online polls
10. Which of the following is NOT true about a P2P C&C?
    - **a.** It can mask irregular peer-to-peer communications but not data exfiltration through beaconing.
    - **b.** A single compromised computer acts as an internal C&C device.
    - **c.** It uses an internal mesh network.
    - **d.** A P2P C&C uses common protocols.
11. Which of the following is false about beaconing?
    - **a.** Beaconing occurs when infected devices attempt to contact the threat actor's external C&C server.
    - **b.** Beaconing is a three-way communication process.
    - **c.** Beaconing is used to receive updated or new instructions from a C&C server.
    - **d.** Data exfiltration is accomplished through beaconing.
12. What is the name of the IOA in which threat actors steal data and transfer it to an external source?
    - **a.** Sweeping
    - **b.** Collecting
    - **c.** Gathering
    - **d.** Exfiltration
13. What category of IOA would the symptom of an application that suddenly exhibits unusual behavior be found?
    - **a.** Application instability
    - **b.** Unexpected output
    - **c.** Anomalous activity
    - **d.** Program interruption

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

14. If OLE between applications suddenly no longer functions, what IOA could that be indicative of?
    a. Activity impairment
    b. Service interruption
    c. Programming snap
    d. OLE-X

15. Which of the following is NOT true about an application log?
    a. It contains information such as timestamps and the severity of the event.
    b. It cannot be used for performance analysis.
    c. Threat actors attempt to edit the application log that reveals their actions.
    d. It records events, transactions, and errors that occur within a software application.

16. Which tool can help provide insight into high-volume consumption of resources?
    a. Consumption evaluator
    b. Flow graph
    c. Processor analyzer
    d. Resource monitor

17. Which of the following functions are NOT found in P-cores?
    a. Physically larger, high-performance cores designed for raw speed
    b. Tuned for higher frequencies and higher IPCs
    c. Capable of hyperthreading
    d. Designed to maximize CPU efficiency

18. Which of the following wireless probes does a standard wireless device like a laptop computer use to gather data?
    a. Dedicated
    b. Wireless device
    c. Desktop
    d. Access point

19. Which of the following can serve as a symptom when examining networks for stealth transmissions?
    a. Server Message Block to User Datagram Protocol
    b. Normal processes to named pipes
    c. Abnormal network-to-network power consumption
    d. Remote connections to named pipes

20. Which of the following questions is NOT used when determining if an unusual traffic spike is an IOA?
    a. Do the spikes appear at the same time on the same day?
    b. Do the spikes occur during business hours or at other times?
    c. Do other monitoring points on the network match these patterns?
    d. Do the spikes produce anomalous output?

Case Projects

Case Project 4-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. Why did Okta not apply its own security to its internal systems? Why does its report on the incident lack transparency? Should organizations be required to complete and distribute a standardized form that covers all aspects of an attack? Write a one-page paper about this.

Case Project 4-2: IOA versus IOC

Estimated Time: 25 minutes
Objective: Compare IOA and IOC.
Description: It is not uncommon for IOA and IOC to be confused. Create a document that compares IOA and IOC. Provide detailed definitions of each, how and when they are used, and give several examples of each.

Case Project 4-3: Identifying Unusual Traffic Spikes

Estimated Time: 20 minutes
Objective: Differentiate between normal and unusual traffic spikes.
Description: Suppose you are attempting to differentiate between unusual and normal traffic spikes. Where would you start? What type of analysis would you perform? What data would you be searching for? Expand Table 4-2 and create at least three additional questions you would ask when determining the cause of a traffic spike. Write a one-page paper on your research.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Project 4-4: Target Attack

Estimated Time: 25 minutes
Objective: Research Target attack.
Description: Despite the fact that the attack on Target occurred back in 2013, it continues to serve as an example of how threat actors can compromise a system and exfiltrate data without the organization being aware of the attack. It also illustrates the severe impact these attacks can have on an organization, no matter their size. Use the Internet to research the Target attack. How were threat actors able to breach Target's security? What did they steal? How long did the attack last? What was the impact on Target itself? Write a one-page paper on your research.

Case Project 4-5: Enhanced Processors

Estimated Time: 25 minutes
Objective: Research P-cores and E-cores.
Description: Use the Internet to research P-cores and E-cores. What are their advantages? How are they used? What proportion of P-cores to E-cores is considered optimal? What are Intel competitors doing to counteract these new cores? How can threat actors take advantage of these faster processors? Write a one-page paper on your findings.

Two Rights & A Wrong: Answers

Cybersecurity Indicators

1. IOA are one or more indicators of a potential upcoming attack.
2. Tools are an important focus of IOA.
3. IOC is the digital artifacts that serve as evidence of an attack.

Answer: The wrong statement is #2.
Explanation: Cybersecurity IOA do not focus on the tools that the threat actors will use in their attacks.

Network IOA

1. One of the primary sources of IOA is found in the network since it serves as the perimeter line of defense.
2. Using traffic spikes as an IOA is straightforward and transparent.
3. Beaconing occurs when infected devices attempt to contact the threat actor's external C&C server.

Answer: The wrong statement is #2.
Explanation: Using traffic spikes as evidence of a cyber incident is considered to be difficult for several reasons.

Endpoint IOA

1. A process is the instance of a computer program that is being executed by one or more spawns.
2. Abnormal memory consumption can be identified by resource monitor tools.
3. Modern processors use simultaneous multithreading or hyperthreading, which can split each core into multiple threads or virtual cores.

Answer: The wrong statement is #1.
Explanation: A process is executed by one or more threads.

Application IOA

1. An application that suddenly gives output that is unanticipated is called anomalous activity.
2. An application log typically contains timestamps and the severity of the event.
3. For a higher level of security, some applications require that a separate user account be created and stored in a database linked to the application.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Answer: The wrong statement is #1.
Explanation: An application that suddenly gives output that is unanticipated, such as an error message that is poorly formatted or a request for unusual user input, may be an indication of a malware infection, called unexpected output.

Reference

1. "What are peak traffic spikes?," *Netacea*, accessed Aug. 28, 2019, https://netacea.com/uploads/technical_showcase_report.pdf.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 5

Analyzing Indicators of Compromise (IOC)

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Compare different techniques for investigating IOC
2. Explain tools used for IOC analysis

#TrendingCyber

Public U.S. companies that issue shares of their stock through an exchange have long been required to make disclosures to their investors, the public, and government regulatory agencies. This is to provide relevant financial information about the organization and its financial status. But in recent years, new regulations requiring disclosures about cybersecurity incidents have been added to the list. While some see this as a good approach toward more transparency, cybersecurity professionals have raised alarms about the types and timing of the disclosures.

The Securities and Exchange Commission's (SEC) proposed new cyber disclosure rules in early 2023 go into effect later that year. This requirement mandated that corporations, after analyzing indicators of compromise following a cyber incident, must report that incident within four days if it is determined that it is "material to the business." In addition, the disclosure should describe what makes the attack material.

The original SEC-proposed rules had even more far-reaching cybersecurity requirements. In the original SEC proposal, organizations had to disclose details of the cyber incident along with technical information about their cybersecurity systems. In addition, the original proposal had a requirement for companies to disclose the cybersecurity expertise of their board of directors. However, these proposed rules were later weakened or even rescinded before becoming part of the final regulations. Now companies must describe the board's process for overseeing cybersecurity risks and management's role in handling those risks. The SEC also streamlined its requirements to focus more on the potential effects of a cyberattack, rather than the details of the incident itself.

The main focus of these new regulations—public reporting—is nothing new: listed corporations have long been required to disclose risks and incidents they deem material to investors. But SEC officials have said in recent years that disclosures of cyber incidents have been spotty. What is needed, they say, is more specific regulations for reporting material attacks and data breaches. This is said to lead to better incident-response planning and board oversight. A parallel raised by the SEC's chairperson is, "Whether a company loses a factory in a fire, or millions of files in a cybersecurity incident, it may be material to investors." According to the SEC, some advantages of these new reporting requirements are that they help corporations to fortify their cybersecurity risk management, they give regulators a consistent view of risk so that they can compare and contrast corporations, and they ensure that regulatory agencies like the SEC are delivering effective oversight of the organizations that they regulate in order to better "calibrate digital risk."

But concerns were raised as soon as the draft regulations were released for public comments. Some chief information security officers (CISOs) worried about how to help their companies comply with the SEC's cyber rules.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

For example, should the CISO be making the determination if a cyber incident is "material"? What if a disclosure turns out to be wrong but it triggered another material event, such as a stock sell-off? And with so many cyber incidents occurring, will the flood of these reports become "routine noise" to investors?

Another concern was that when a cyber event occurs, sometimes law enforcement asks corporations to remain quiet while they start their own separate investigation. Businesses had argued for exemptions from reporting when asked by law-enforcement agencies to stay quiet during the investigations, but the SEC did not include such a carve-out in its final rule.

Still another question was raised: Is four days enough time to accomplish everything required? Won't it be difficult for most corporations to determine that their incident qualifies, seek legal counsel, determine what the material impact may be, and then communicate it properly—all within four days? At least that is the question of a partner at a law firm who previously led the SEC's cyber unit within the division of enforcement.

Many cybersecurity professionals fear that the SEC's regulation may create additional compliance burdens for corporations that, in many cases, will soon be subject to additional incident-reporting rules passed by Congress. For example, critical infrastructure operators must report attacks within 72 hours. And the SEC is also proposing additional cybersecurity-related regulations that would require investment funds and advisers to report incidents within 48 hours. That means there are at least three different reporting deadlines. There have been requests for a coordination of government reporting requirements, but to no avail.

Another question raised regards sharing this information with other potential targets. Will these regulations complicate attempts to analyze data shared by critical infrastructure firms and share it across the public and private sectors, as is done now?

Perhaps the most significant pushback on these reporting regulations is that since these reports are public, the threat actors behind the attacks will have access to them. Would reporting an attack prompt the threat actors to steal data faster or speed up timelines on attacks such as ransomware strikes once they are tipped off that their attacks are successful? Would saying something publicly in four days warn the threat actors that they have been discovered and cause them to cloak other parts of the attack, so they are more difficult to find? As one commenter said, "The release prescribes regular disclosures, which seemed designed to better meet the needs of would-be hackers than investors' needs for financially material information."

And in a strange twist, threat actors are already using the new SEC disclosure rules against companies that they attack.

In mid-November 2023, the ALPHV/BlackCat cyber thieves conducted a successful data breach on MeridianLink, a publicly traded company that provides digital solutions for financial organizations such as banks, credit unions, and mortgage lenders. ALPHV/BlackCat then demanded from MeridianLink a payment in order to not publicly leak the stolen data and embarrass MeridianLink, which would cause its stock price to drop and its customers to flee to a competitor. However, MeridianLink refused to pay and did not even respond to ALPHV/BlackCat's demand to "negotiate a favorable payment."

So, ALPHV/BlackCat filed an online complaint with the SEC that MeridianLink had failed to report within four days their data breach per these new SEC regulations. ALPHV/BlackCat filled out the SEC's online "Tips, Complaints, and Referrals" webpage stating that MeridianLink had suffered a "significant breach" but did not disclose it as required. (Of course, ALPHV/BlackCat conveniently failed to mention that they were the ones responsible for the data breach.)

However, ALPHV/BlackCat made a critical error: The SEC's new cybersecurity rules did not take effect until December 15, 2023, almost one month after the attack occurred. Thus, MeridianLink was not bound by the new reporting rules—yet.

In cybersecurity, the digital artifacts that serve as evidence of an attack are called indicators of compromise (IOC). IOC are one or more signs of a successfully completed attack and show how it happened. This evidence can then be used to determine what defensive deficiencies exist.

After covering indicators of attack (IOA) in the previous chapter, which are preliminary behaviors that focus on detecting the intention of the threat actor as evidenced by their actions, in this chapter you analyze IOC. You explore common techniques for investigating IOC as well as tools for analysis.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Common Techniques for Investigating IOC

Certification

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

There are several common techniques that cybersecurity professionals use to examine an exploited system when looking for IOC. Typical techniques include diagnosing malware, analyzing email, and examining user behavior analysis.

Diagnose Malware

How can a cybersecurity professional determine if a file contains malware? There are different techniques that can be used to identify malware. The two major techniques are to compare message digests and use file analysis techniques.

Compare Message Digests

Not all cryptographic algorithms are designed to create ciphertext that can later be decrypted back into plaintext. Some algorithms create output that cannot be reversed. One of these "one-way" cryptographic algorithms is a hash algorithm that creates a unique "digital fingerprint" of a set of data. This process is called **hashing**, and the resulting fingerprint is a digest (sometimes called a message digest or simply a hash) that represents the contents.

Note 1

Although hashing and checksums are similar in that they both create a value based on the contents of a file, hashing is not the same as creating a checksum. A checksum is intended to verify ("check") the integrity of data and identify data-transmission errors, and a hash is designed to create a unique digital fingerprint of the data.

There are several common hash algorithms. Table 5-1 illustrates the digests generated from several one-way hash algorithms of the word "Cengage."

Table 5-1 Digests generated from one-time hash algorithms

Hash	Digest
RipeMD160	dd52a79bce64a1d145b51ce639e0dadda976516d
SHA-256	f6c8a86bf6a5128cbaf2ad251b0beaa3604c11c51587de518737537800098d76
SHA3-512	3a82d58e17f3991413c5f4e9811930b69513bba02a860eed82070f892ab381f9fd926a88cf68745565f51a93b97a1317ae8b84e2dfb798e4a2aa331187dc9e34
Whirlpool	1428cacf499fce9ef439f95a27f0efdc518e97edf9714e234cfffe0c22dcb0e2c4bd3f22a975670f4a229452062b8bd0c6c9244e4c986f22c61ce951de31c505

Hashing can be used to help determine if a file contains malware. Instead of spending hours or days examining the file's content, a message digest (hash) of the file can be generated and compared with a list of digests created from files that have previously been identified as malware. Using hashing algorithms to generate message digests on malware helps to standardize and simplify the exchange of IOC among cybersecurity researchers.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Use File Analysis Techniques

If a message digest comparison does not yield results, the next step is to look for evidence of malware within the file, called **file analysis**. There are two common techniques used when analyzing a file:

- **Dynamic file analysis.** Dynamic file analysis executes the program and then observes its behavior. Special software called "debuggers" can be used to watch the behavior of the file on a step-by-step basis and also note the effects on the computer to determine if they are malicious.
- **Static file analysis.** Static file analysis is also called code analysis because it looks at the different code components of the file. Static file analysis does not execute the file but instead studies each of its internal components to learn its intentions.

Caution

Modern malware uses evasive techniques to attempt to defeat static file analysis, such as embedding syntactic code errors that will confuse attempts at analysis but that will still allow the code to function.

Dynamic file analysis can be performed by monitoring commands, and static file analysis often relies on decomposing the contents of the file.

Monitor Commands

The basic technique for determining any malicious activity of a file is to monitor the actions of the file. This can be done by looking for evidence of operating system (OS) commands that the file initiates to perform a malicious activity (**interpret suspicious commands**).

Because malware typically launches other processes, uncovering the commands to invoke these processes can help identify malware. On a Microsoft Windows computer, threat actors will often invoke one of two different native command-line interfaces (CLIs). The more powerful CLI is called PowerShell, while a more limited CLI is the Windows Command Shell. Although it has a limited feature set compared to PowerShell, the Windows Command Shell has the advantage that its commands can be invoked without starting a new identifiable process on the computer. Typical Windows Command Shell operations used by threat actors are to bypass security controls, collect system information, execute files, and modify system settings.

There are limitations to determining malicious behavior by focusing on file behavior. Many applications legitimately invoke other OS processes. This can make it difficult to identify a malicious spawned activity and often results in a high number of false positives. In addition, malware may give their processes the same name as a legitimate process, such as the Local Security Authority Subsystem Service (lsass.exe) to escape detection.

Note 2

Instead of watching for a single suspicious command, it is often better to monitor process relationships; that is, is there a legitimate reason an application would invoke a specific process, such as a network connection to an external domain?

Decompose File Contents

Another technique used when analyzing a file is to use static file analysis to look into the code of the file for evidence of malware. This involves examining the file structure, recognizing patterns, and identifying dynamic URLs.

Examine File Structure

Viewing the internal structure of the file is an important starting point in decomposing a file to view its internal code. There are several sophisticated programs that can be used to examine the internal file structure. Figure 5-1 illustrates a program that exposes an internal file structure.

Recognize Patterns

Pattern recognition is the ability to detect arrangements of characters or data that can yield information. This can be done through examining **strings**, which are sequences of characters embedded within a file. Examining strings in a program can give clues about the program's functions. For example, if malware creates a file, then the filename of the new file is stored as a string within the malware. Strings extracted from a file can contain references to filenames, Uniform Resource Locators (URLs), domain names, Internet Protocol (IP) addresses, attack commands, Windows registry keys, and so on. An example of output from a string extractor program is shown in Figure 5-2.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-1 Internal file structure

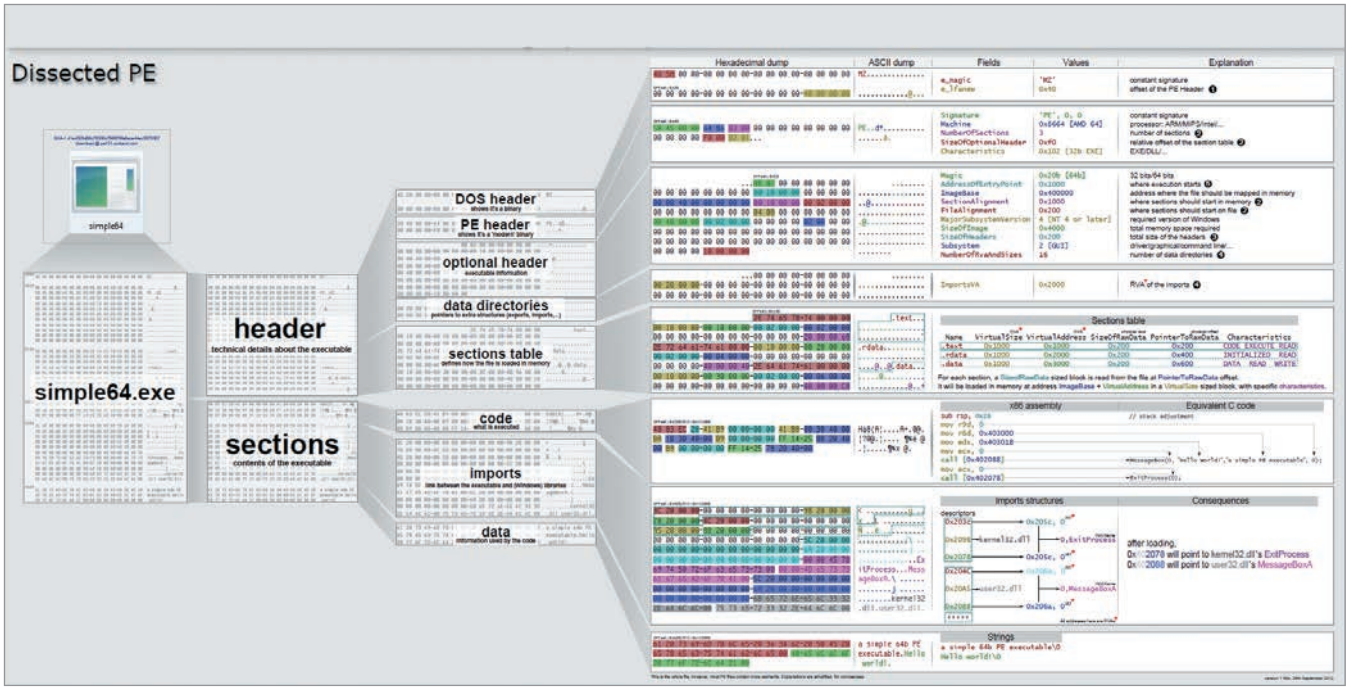
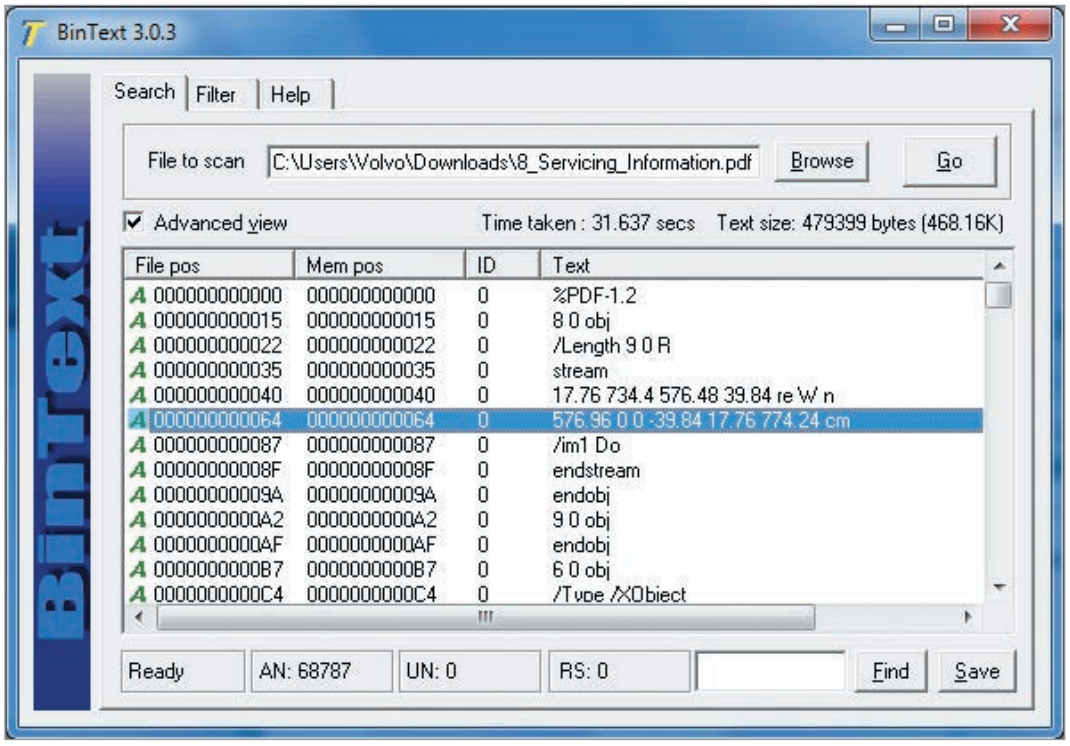


Figure 5-2 String extractor



Caution

Although strings do not always provide evidence of the underlying purpose or capability of a file, strings can give a hint about what the malware is attempting to perform and is capable of doing.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Identify Dynamic Command and Control URLs Because of the obvious telltale signs that strings can reveal, threat actors go to great lengths to mask their strings within programs. Techniques for masking strings include adding superfluous characters (caret symbols, commas, double quotes, parentheses, and semicolons), using coding techniques to create strings that are difficult to follow (such as embedded FOR loops), and creating environment variable substrings that are difficult to trace.

Threat actors also mask strings to hide URLs linked to online remote devices through which the attackers send commands back to infected devices. These infected devices receive instructions through a remote online **command and control (C&C)** structure managed by attackers. There are several ways for this communication to occur: (1) endpoints that sign into a third-party website, (2) commands via blogs, (3) specially coded attack commands through posts on X (formerly Twitter) or notes posted in Facebook, or (4) a "dead-drop" C&C mechanism used by creating a Google Gmail account. After creating the Gmail account, the C&C mechanism creates a draft email message that is never sent but contains commands that the bot receives when it logs in to Gmail and reads the draft. (Because the email message is never sent, there is no record of it and all Gmail transmissions are protected so that outsiders cannot view them.)

However, most often communication with a C&C involves the compromised device signing into a website that the threat actor operates. In the past, these C&C sites were "hard-coded" with a static URL string embedded in the malware. However, if this static URL string could be uncovered, it can be locally blocked to prevent any infected computers from communicating with the C&C, thus limiting the malware's impact.

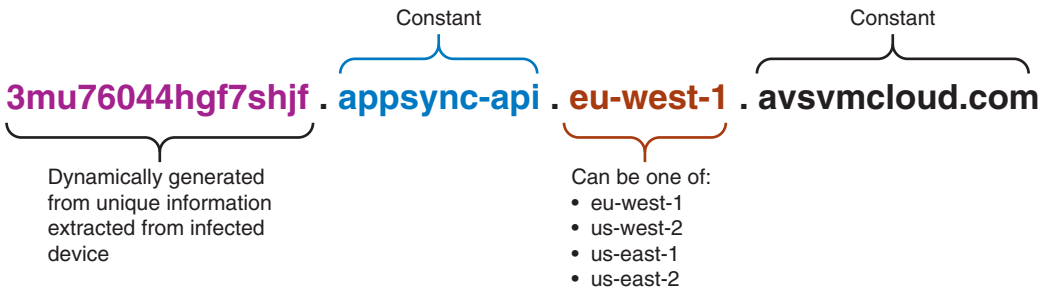
Note 3

In addition, once the URL of the C&C is known, then technology companies and law enforcement agencies can petition a judge for permission to seize the domain and stop all communications.

Today threat actors have turned to adding code to malware to create dynamic C&C URLs. This technique uses a domain generation algorithm (DGA) to create the URLs. These techniques can range from basic to very sophisticated.

An example of a basic DGA is to have part of the URL hard-coded while one element is dynamically generated. A threat actor may divide the URL into four parts, three of which are hard-coded strings within the malware, but one part is dynamically generated based on unique information extracted from the infected device. This information may, for example, be a combination of the physical address of the network interface, the domain name of the device, and the contents of a registry value MachineGUID (a unique identifier for each computer). An example of a basic DGA to generate a dynamic C&C URL domain is shown in Figure 5-3.

Figure 5-3 Basic DGA



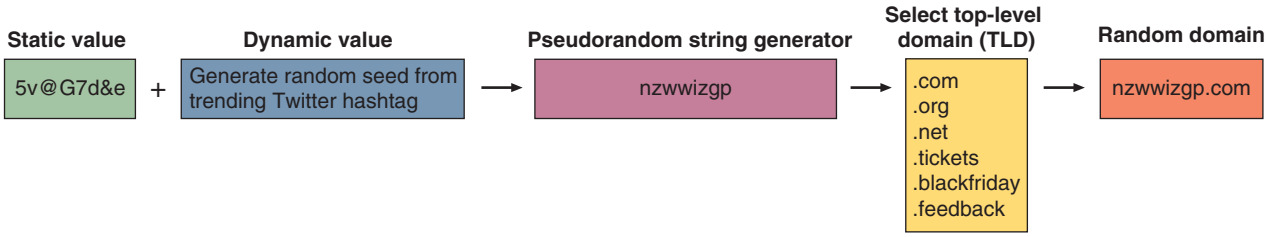
A more sophisticated DGA involves multiple steps and produces multiple potential C&C URLs, making it even harder to trace. The steps as illustrated in Figure 5-4 are as follows:

1. The threat actor embeds within the malware code a static value (such as a dictionary word or a predetermined string of numbers and letters), a link to a source that can generate a dynamic value (such as a trending X hashtag, the insignificant digits of a foreign exchange rate, and/or the current weather temperature in a specific city), a pseudorandom string generator, and a list of top-level domains (TLDs).
2. At a predefined time, the DGA in the malware inputs the dynamic string and then uses it and the static string as input into the pseudorandom string generator to create a domain name, and then it selects at random a TLD to finally create a random domain.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

3. The threat actor, also knowing the DGA and all the values, is able to generate a list of domains just like the malware can. They then choose one domain and register it to serve as a link to the C&C. This registration occurs a short period of time (sometimes as little as one hour) before the malware generates its random domains.
4. The malware attempts to connect to the first domain generated. None of these domains can be resolved through Domain Name System (DNS) queries by the malware except for the one domain that the threat actor has just registered. If the attempt succeeds, the malware has reached the correct URL C&C. If an attempt fails, the malware will then generate the next potential domain and attempt to reach it. This process continues until the malware is successful.
5. The malware receives its instructions from the C&C that applies for a specific period of time, such as 24 hours. Once that time is over, the process starts again for the malware to generate new potential domains to receive its next instructions for the next period of time.

Figure 5-4 Sophisticated DGA



Note 4

Early uses of DGA generated as few as 250 domain names daily. More recent malware generates up to 50,000 domain names each day.

Defending against DGA is very difficult due to the random generation of domain names. An alternative is to search for a reference to a dynamic link library that utilizes network functionality. For example, on a Microsoft Windows computer, searching for "ws2_32.dll" indicates that the malware uses the network.

Note 5

DGA has been called "one of the most important 'innovations' in malware in the past decade."[1]

Analyze Email

An email system likewise contains IOC. Analyzing email systems for IOC (**email analysis**) requires knowing the basics of how email works, the threats associated with email, and email defenses.

How Email Works

The basic components involved in sending and receiving email are the mail user agent (MUA) and mail transfer agent (MTA). A MUA is what is used to read and send mail from an endpoint. A MUA can be a separate app, a webmail interface, or a web browser. MTAs are programs that accept email messages from senders and route them toward their recipients.

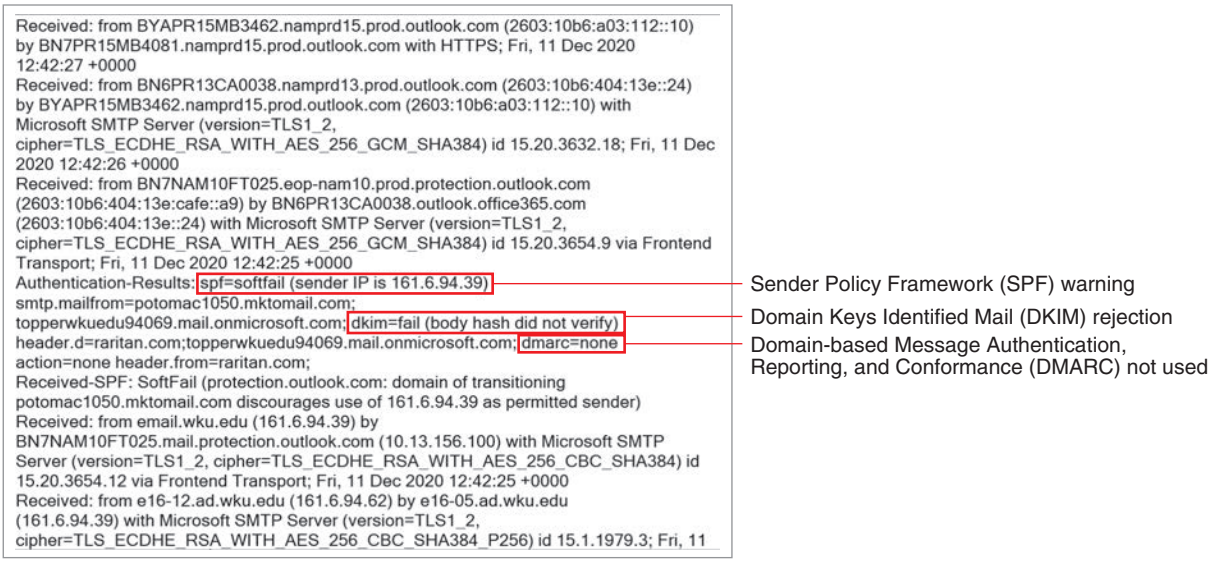
Note 6

Originally, email was sent to a mail server using the Simple Mail Transfer Protocol (SMTP). When it arrived at its destination, it was downloaded from the server using the Post Office Protocol (POP3). Today the Internet Access Message Protocol (IMAP) has replaced POP3.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

As email is transferred from MTA to MTA, information is added to the **email header**. The email header contains information about the sender, recipient, email's route through MTAs, and various authentication details. Each MTA along the path adds its own information to the top of the email header. This means that when reading an email header, the final destination MTA information will be at the top of the header, and reading down through each subsequent header will ultimately end at the sender MTA header information. Figure 5-5 shows a partial email header.

Figure 5-5 Email header



Email headers also contain an analysis of the email by the MTA. Table 5-2 shows the different analysis categories and abbreviations used by Microsoft Office 365.

Table 5-2 Microsoft Office 365 email analysis

Abbreviation	Category
BULK	Bulk
DIMP	Domain impersonation
GIMP	Mailbox intelligence-based impersonation
HPHISH	High-confidence phishing
HSPM	High-confidence spam
MALW	Malware
PHSH	Phishing
SPM	Spam
SPOOF	Spoofing
UIMP	User impersonation
AMP	Anti-malware
SAP	Safe attachments
OSPM	Outbound spam

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Email Threats

There are a variety of threats related to email. These include:

- **Phishing.** Phishing, one of the most common forms of social engineering, is sending an email that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information or taking action. Users are asked to respond to the email or are directed to a website where they are requested to update personal information, which is promptly captured by the threat actors.

Note 7

The word *phishing* is a variation on the word *fishing*, with the idea being that bait is thrown out knowing that while most will ignore it, some will "bite."

- **Malicious payload.** Often the email message itself contains an attack. This could be an attachment that, upon opening it, will launch an attack (malicious payload). Or users may receive a fictious overdue invoice that demands immediate payment, and in haste a payment is then made (called an invoice scam).
- **Embedded links.** Links that are contained within email messages (**embedded links**) are particularly dangerous. Because email messages are typically formatted in HTML, the displayed link (*Your Bank*) can be different than the underlying hyperlink (*attacker_site.com*).
- **Impersonation.** A threat actor who could gain access to the email account of a corporate executive could pretend to be that person (**impersonation**) and send out malicious emails that contained embedded links to sites belonging to the attacker. These impersonation emails could also have a malicious attachment with an email subject line such as "This attachment requires your immediate attention!" to trick the user into opening the attachment.
- **Forwarding.** While some users automatically forward all corporate emails to their personal user email account, there are risks associated with this. A personal email system may not have the same level of protection as the corporate email system so that sensitive email messages could be easier for unauthorized individuals to access. And if legal action is initiated and all email evidence must be surrendered (called eDiscovery), then critical emails that may have been erased from a personal email account may not have a backup available as with a corporate email system. Also, if an email message forwarded from a corporate account is flagged as "Spam" by a user's personal email account (not an uncommon occurrence), this could damage the "reputation score" of the corporate email used by email providers and spam filters, thus causing other email systems to block incoming email from the corporate email system thinking it is spam.

Email Defenses

There are different defenses that can be used to address email threats. Spam and phishing filters can help curtail phishing attacks while strong endpoint anti-malware can be used to minimize malicious payloads. In addition, other technologies can help provide a degree of email defense. For example, Apple's Hide My Email allows users who create an account with an app or visit a website that supports Sign in with Apple to use the user's normal email account or have it generate a unique and random email address. This random address can only be used by the specific app or website to send email to the user's normal email account where it can be read and responded to. Any other app or website that attempts to use this random email address is blocked. However, other email threats can only be addressed through improving user behavior, such as not clicking embedded links and not forwarding email to personal accounts. And some email threats—like impersonation based on a compromised account—have virtually no defenses.

There are technology defenses used to protect email. Although modern email is typically encrypted from MTA to MTA as data in-transmit using the Transmit Layer Protocol (TLS), this only protects email as it is being relayed from one MTA to another MTA along the delivery path; it does not address protection at the MTAs. If an email travels from the sender through three MTAs before reaching its recipient, any MTA along the way can alter the content of the message or change the header information.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

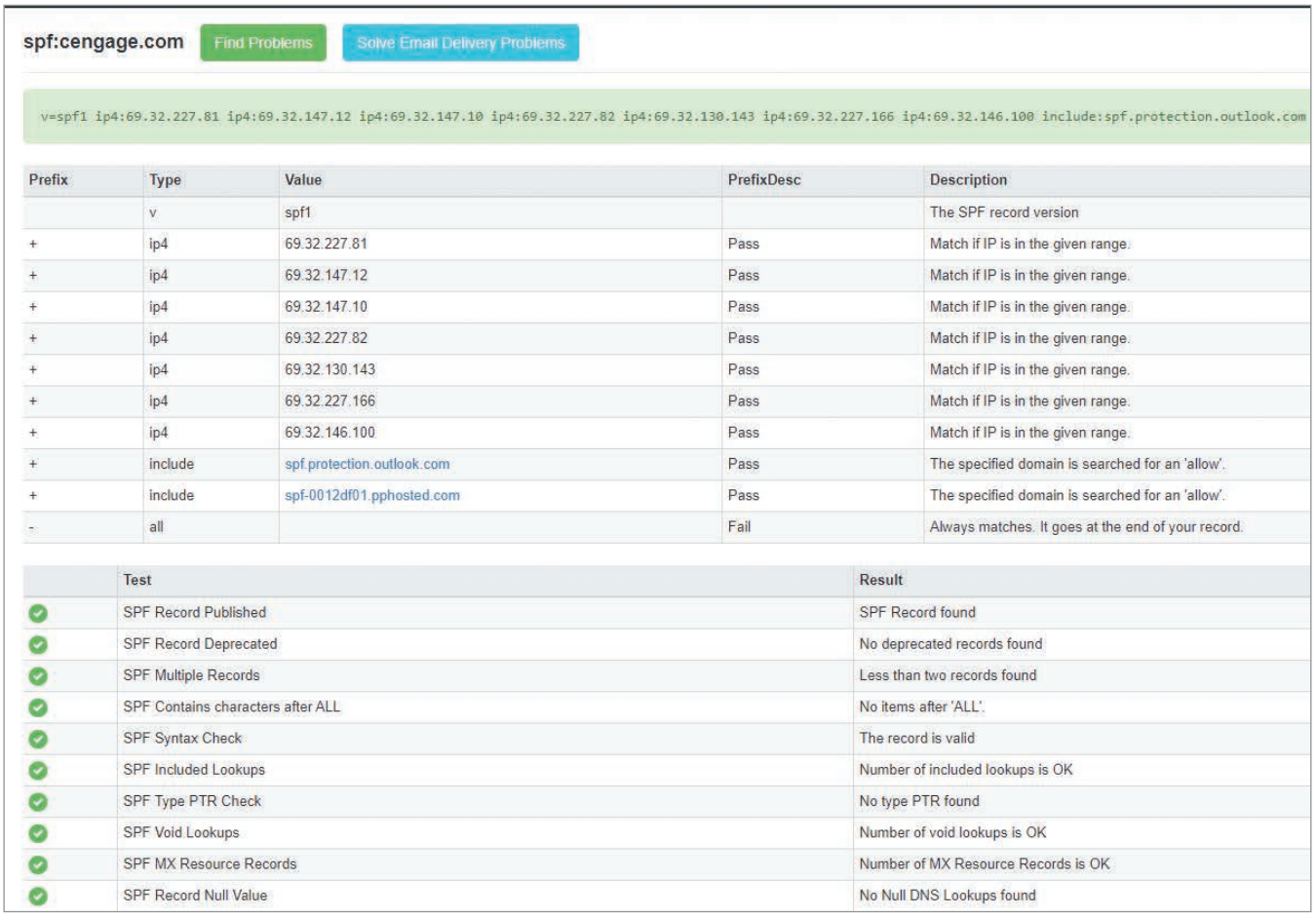
There are different email defenses that can be used to protect email. These include Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).

Sender Policy Framework (SPF) It is important to protect against forged emails that pretend to come from one domain but actually come from another domain. Threat actors who can forge a domain can send fake messages that appear to come from an organization (spoofing), and a recipient who trusts the domain would likewise trust the email. Spoofed messages can be used for malicious purposes to communicate false information, distribute malware, and trick users into giving out sensitive information. In addition, it is important that valid email messages are not erroneously marked as spam, thus preventing their delivery to the recipient MTA.

Sender Policy Framework (SPF) is an email authentication method that identifies who the MTA email servers are that have been authorized to send email for a domain. SPF helps protect a domain from spoofing and also helps prevent messages from a valid domain from being marked as unwanted spam. If a domain does not use SPF, then receiving MTA email servers cannot verify that messages appearing to be from a domain actually are from that domain. This could result in the receiving MTA servers forwarding valid emails into the recipients' spam folders or even rejecting valid messages.

The administrative owner of a domain can set a TXT record in its DNS that states what servers are allowed to send mail on behalf of that domain. For example, in Figure 5-6, the Cengage.com SPF record indicates that email from cengage.com should only come from the servers specified, namely Microsoft Outlook and PPHosted.com. Those coming from a different domain are met with a "SoftFail" warning that says to trust this message less than normal but do not completely invalidate it based on this alone.

Figure 5-6 Cengage SPF record



Source: MXToolbox

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 8

The email header in Figure 5-5 indicates a SoftFail warning (*spf=softfail*).

However, SPF headers in an email are not infallible. Once generated, there is no means of protecting the information. This makes SPF useful to the MTA servers themselves while transmitting the email, but the protection does not extend beyond that. However, SPF is still an excellent tool for quickly identifying and intercepting spam.

Domain Keys Identified Mail (DKIM) **Domain Keys Identified Mail (DKIM)** is an authentication technique that validates the content of the email message itself. This validation is accomplished through a digital signature. The administrative owner of the sending domain can generate an asymmetric public/private key pair and store the public key in a TXT record on the domain's DNS. Mail servers on the outer boundary of the domain's infrastructure then use the private DKIM key to generate a digital signature (which is an encrypted digest created with a hash algorithm) of the entire message body, including all headers accumulated by the different MTAs. Recipients can decrypt the DKIM signature using the public DKIM key retrieved from the DNS to ensure that the digests match.

Note 9

The email header in Figure 5-5 indicates a DKIM rejection: *dkim=fail (body hash did not verify)*.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** extends SPF and DKIM. It allows the administrative owner of a domain to publish a policy in their DNS records to specify which mechanism (DKIM, SPF, or both) is used when sending email from that domain. It also indicates how to check the "From:" field that is presented to end users and a reporting mechanism for actions performed under those policies.

Note 10

The email header in Figure 5-5 indicates DMARC is not being used (*dmarc=none*).

User Behavior Analysis (UBA)

Suppose that Gia is a close friend of yours whom you have known for many years. Gia is outgoing, funny, always has a smile on her face, and often wears clothes that reflect the latest fashion trends. You frequently meet Gia at a local coffee shop where she always orders a caramel macchiato.

After being gone for several weeks, you arrange to meet Gia to catch up. However, when she walks in the door, you can barely recognize her. She looks frightened and nervous, and her clothes are old and rumpled. She orders a plain cup of coffee and sits at the table across from you. She barely looks at you but keeps turning around to see who has walked in the door, and she hardly has anything to say. You would immediately recognize that something is amiss with your friend, even though she has said nothing. Just her change in behavior has revealed that something is wrong.

Just as a change in Gia's behavior can indicate something is not right—or at least not the same as before—so, too, can a change in the normal behavior of a technology or user reveal that something is not right. An endpoint that starts crashing multiple times each day, an application that keeps locking up, or a user account that suddenly starts trying to access restricted files may indicate that something is wrong, or at least something has changed.

Behavior-based monitoring continuously analyzes the behavior of processes and programs on a system and sounds an alert if it detects any abnormal actions, at which point a decision can be made. Behavior-based monitoring uses "normal" processes and actions as its standard (known-good behavior) instead of only searching for abnormalities (anomalous behavior). Monitoring behavior is considered adaptive and proactive instead of just being reactive.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Both users as well as technology systems have normal behaviors that can be monitored for any unusual activity. Examining user behavior is known as **user behavior analysis (UBA)**. Applying this analysis to both users as well as "entities" such as networks, devices, applications, and servers (called system and application behavior) is called user and entity behavior analysis (UEBA).

Two common examples of UBA are abnormal account activity and impossible travel. There are also limitations to UBA.

Abnormal Account Activity

Suppose you were to observe the technology-based actions of a user at an organization for 30 minutes each morning when they arrived at the office. But because the user is halfway around the world, instead of watching the user, you observed what they did by monitoring their laptop computer. Because humans are "creatures of habit," you likely would find a consistent pattern that emerges. You might observe that their email account is opened (the user starts each day by reading their emails), a web browser accesses specific online websites (the user is scanning certain websites about events that have occurred the previous day that may impact their organization and their work), certain company documents stored on a file server are opened (the user is engaged in their routine job duties), and so on. After just a few days, a pattern of normal account activity could be easily created by watching the user's laptop.

However, what if one morning you observe that the laptop attempts to open a company document on a secure server that had not been used before. Or that a new app that was not connected to a job function was downloaded and installed. Or that the web browser went to websites that had never been accessed before and were not job related.

This uncommon behavior or **abnormal account activity** may mean that the account has been compromised or the endpoint is under the remote control of a threat actor. Abnormal account activity compares a baseline of normal actions against irregular or unusual behavior in order to identify a potential issue. Other unusual user activities that can trigger an alert include an unusual number of multiple file download activities, file sharing or deletion activities, multiple virtual machine (VM) creation activities, and using different regions for accessing cloud resources.

Note 11

UBA has been used for several years for protecting users, particularly by financial institutions. For example, if a bank customer normally accesses their bank's website from their home computer on evenings and weekends, then this information can be used to establish a profile pattern based on the IP address of the computer, the time of day, the Internet service provider, and basic computer configuration. If a computer located in China suddenly attempts to access the bank customer's online account at 2:00 am, this might be an indication that an attacker is at work, and access is then immediately restricted.

Impossible Travel

Another example of user behavior analysis is **impossible travel**. Consider a situation in which the genuine user logs into the corporate network in New York at 10:00 am. However, an impostor who has stolen the user's credentials then attempts to log in from Los Angeles one hour later. Because it is not possible to travel that distance within that time, the imposter is not permitted to log in.

Impossible travel begins by using UBA to identify the genuine user, usually through a learning period of up to seven days, by observing the times and locations from which the user accesses the corporate network. This then becomes the baseline against which another login attempt is compared.

UBA Limitations

As promising as UBA sounds, it has weaknesses, and these can be targeted by different exploit techniques or methods for delivering malware. Building a complete understanding of each and every application is difficult to achieve. There are also challenges related to building a profile of users who access distributed applications. Some systems rely on software agents that are installed on the endpoints to gather this data; however, threat actors will often target these agents to disable them or bypass them so as to not raise an alarm.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 12

Some VMs now offer "service-defined" protection over applications, data, and users by building a profile of known-good behavior both on the endpoint and network. And this protection cannot be bypassed even if an attacker infects the guest OS because inspection can be made without the need for agents to be installed on the guest OS.

Two Rights & A Wrong

1. There are three types of file analysis techniques: dynamic, static, and hash.
2. Threat actors today add code to malware to create dynamic C&C URLs.
3. SPF is an email authentication method that identifies who the MTA email servers are that have been authorized to send email for a domain.

See the answers at the end of the chapter.

Tools for IOC Analysis

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

There are several different tools that can be used for uncovering IOC. These include file analysis tools, tools for analyzing networks, reputation tools, and log correlation and analysis tools.

File Analysis Tools

Analyzing files for evidence of malware should not be done on an unprotected computer since it would result in that computer becoming infected if malware were to be present. Instead, a fully protected environment should be used instead. This is called **sandboxing**. Sandboxing allows code to be observed and analyzed in a safe, isolated environment.

Sandboxing can be performed on a local computer. As an alternative, an online site can be used that both protects and automates the malware detection process.

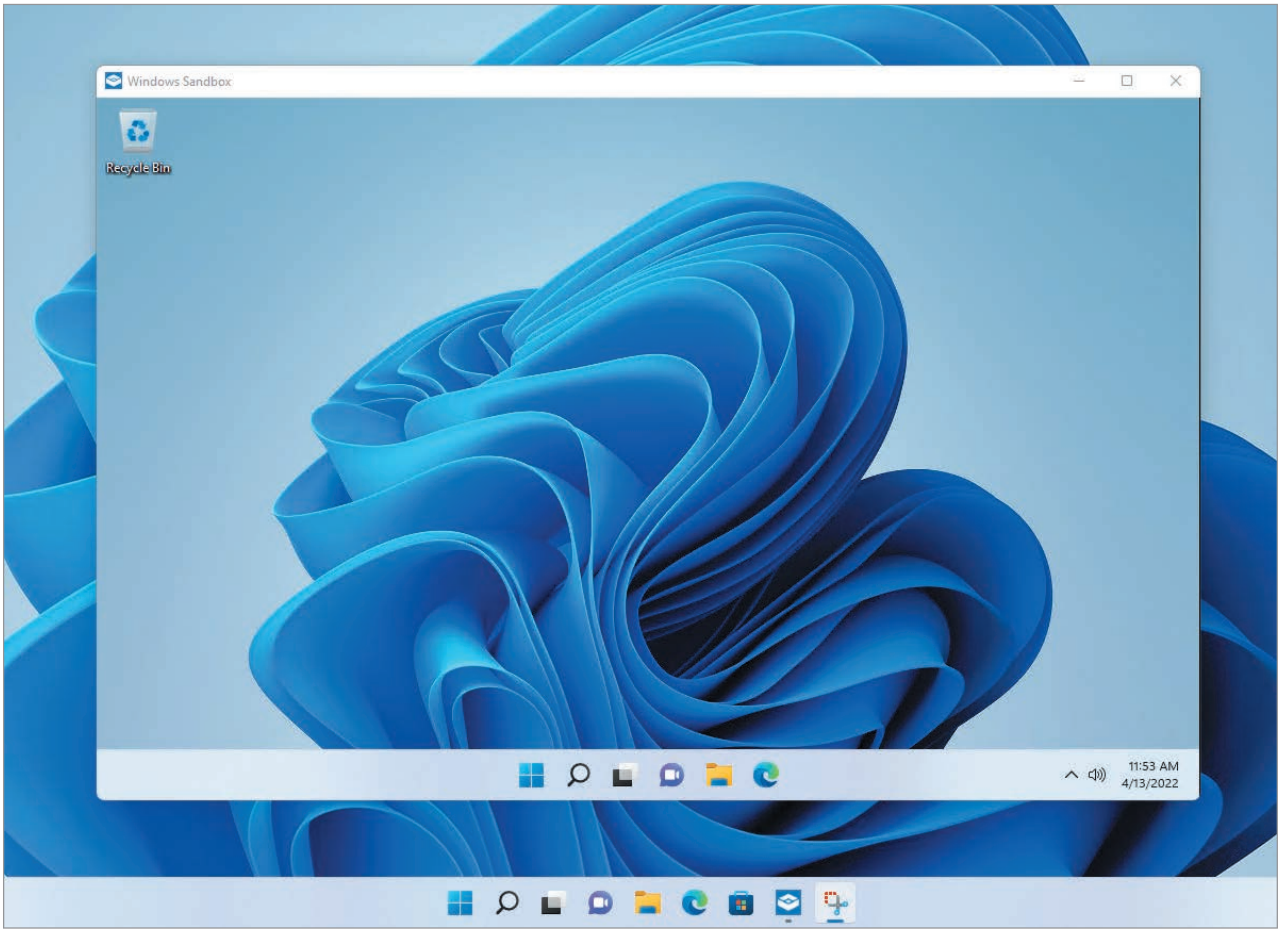
Local Sandboxing

A local sandbox is essentially an isolated VM: anything run within the sandbox will impact only the VM and not the underlying computer. Whatever occurs within the sandbox is not visible to other applications or the OS outside the sandbox. Also, the contents of the sandbox do not have to be saved when the sandbox is closed.

One means of setting up a local sandbox is to download and install a VM application and then install the OS within that environment. Users of Microsoft Windows can take advantage of the Microsoft Windows Sandbox, which is part of the Windows 11 OS. The Windows Sandbox is illustrated in Figure 5-7. The Windows Sandbox has the advantage of being included as part of Windows, so nothing has to be downloaded and installed. It relies on the Microsoft hypervisor to run a separate kernel that isolates the Windows Sandbox from the host. This makes it more efficient because it can take advantage of the Windows integrated kernel scheduler, smart memory management, and a virtual graphics processing unit. Apple computers have a similar function known as the App Sandbox.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-7 Windows Sandbox



Source: Microsoft Corporation

Note 13

An executable file from the host Windows environment can be pasted into the Windows Sandbox desktop to launch it.

When using local sandboxing, once the sandbox is created, a tool is downloaded to analyze the file for malware. Table 5-3 lists a sample of different tools for file analysis.

Table 5-3 File analysis tools

Tool name	Description	Usage
RegShot	Takes a clean snapshot of a Windows registry that can be used later for comparison after the malware sample is executed	This can reveal information about any changes in the registry, particularly when malware modifies registry keys to persist on the device.
SSDT View	Lists the most significant parts of the System Service Descriptor Table (SSDT), which includes system service indexes, system service addresses, system service names, and the module name corresponding to the system service address	SSDT View can indicate if a service is "hooked," which is a mechanism by which malware can intercept events such as messages, keystrokes, and mouse actions.
DriverView	Displays the list of all device drivers currently loaded on the system	For each driver loaded, DriverView displays the load address of the driver, description, version, product name, company that created the driver, and more to help identify drivers loaded by threat actors.

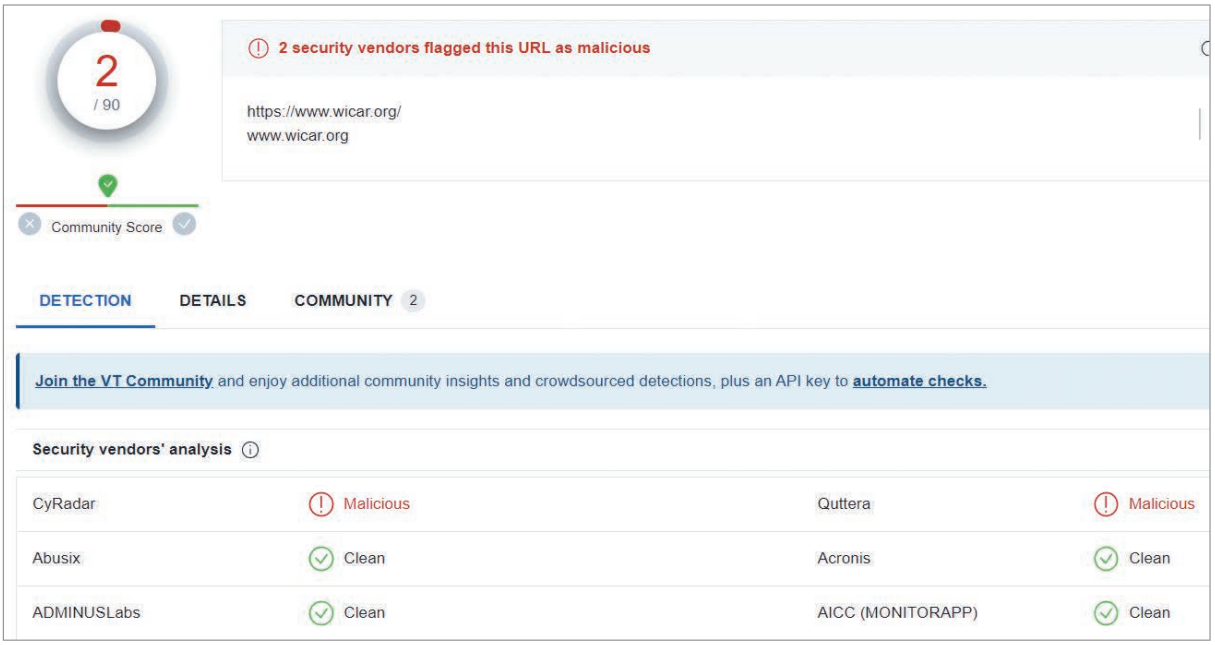
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Remote Sandboxing

As an alternative to creating a sandbox on a local computer, there are remote online sandbox sites to which malware can be uploaded and automatically evaluated. These include VirusTotal, Joe Sandbox, and Cuckoo Sandbox.

VirusTotal VirusTotal is a remote sandbox that inspects items using over 70 antivirus scanners and URL/domain blocklisting services that are updated frequently. VirusTotal is free to use and offers different submission methods, including the public web interface, desktop uploaders, and browser extensions. Figure 5-8 shows output from a VirusTotal scan.

Figure 5-8 VirusTotal scan



Source: VirusTotal

Note 14

Scanning reports produced by VirusTotal are shared with the public VirusTotal community. Users can contribute comments and vote on whether particular content is harmful or is a false positive.

The power of VirusTotal goes beyond simply submitting suspicious files for analysis. Modifiers can also be included along with the file for more precise scanning or identifying historical data. Sample modifiers are listed in Table 5-4.

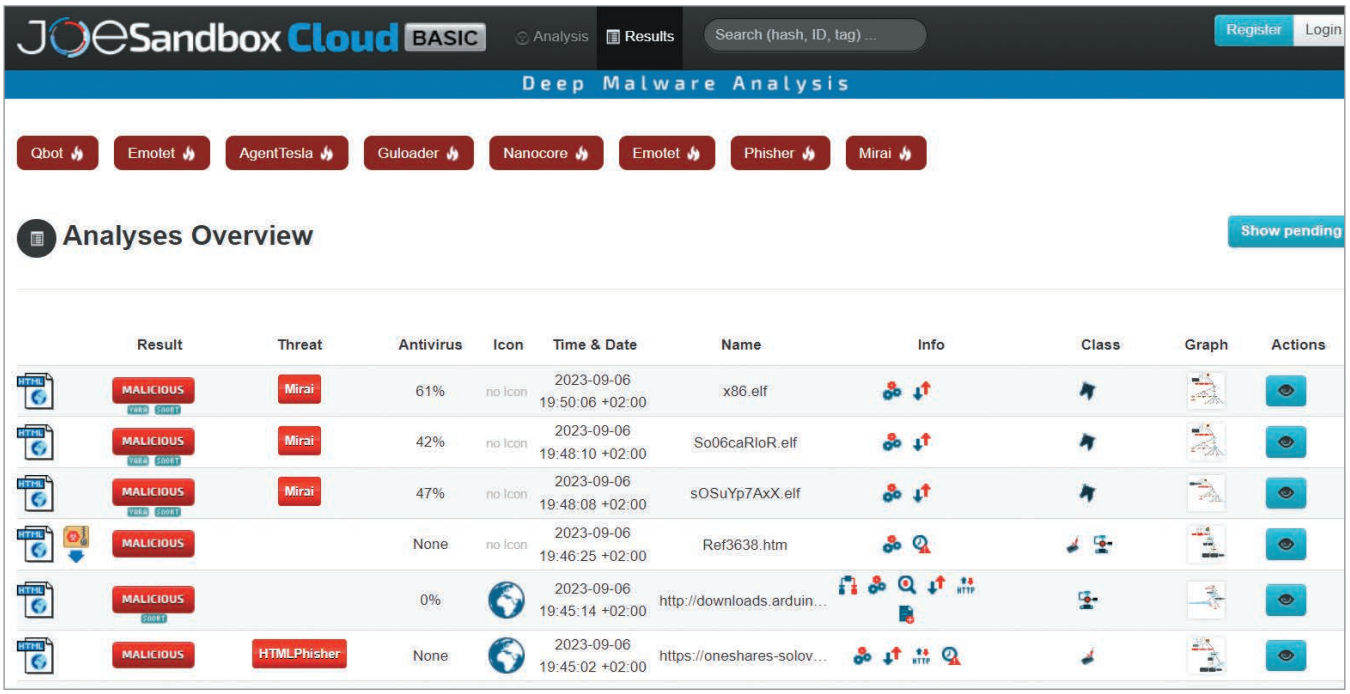
Table 5-4 Sample of VirusTotal modifiers

Modifier	Explanation
type: docx tag:macros p:5+ generated:30d+	Find recently created Word .DOCX documents with embedded macros that have been detected by at least five different antivirus tools.
type: xlsx tag:powershell fs:10d+	Identify Excel .XLSX files bundled with PowerShell scripts and uploaded to VirusTotal over the last 10 days.
type: docx tag:exe-pattern tag:run-file tag:obfuscated	Find documents with obfuscated Visual Basic for Application (VBA) code executing other files.
fs:"2023-09-06T00:00:00+" (signature:"43 bb 43 7d 60 98 66 28 6d d8 39 e1 d0 03 09 f5" OR signature:"14 78 1b c8 62 e8 dc 50 3a 55 93 46 f5 dc c5 18")	Search for leaked or stolen digital certificates using the submission timestamp after the leak date.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Joe Sandbox Joe Sandbox is an advanced automated and deep malware analysis engine. It enables users to upload for analysis files from Windows, macOS, Linux, Android, and iOS devices. File analysis includes IOC such as C&C domains, abnormal system behaviors, network behavior, and static file information. Figure 5-9 illustrates a Joe Sandbox scan.

Figure 5-9 Joe Sandbox scan



Source: Joe Security LLC

Note 15

One of the features of Joe Sandbox is the ability to interact with the sandbox directly from a web browser through the Live Interaction feature. This enables users to gain advanced insights into the actions of the malware.

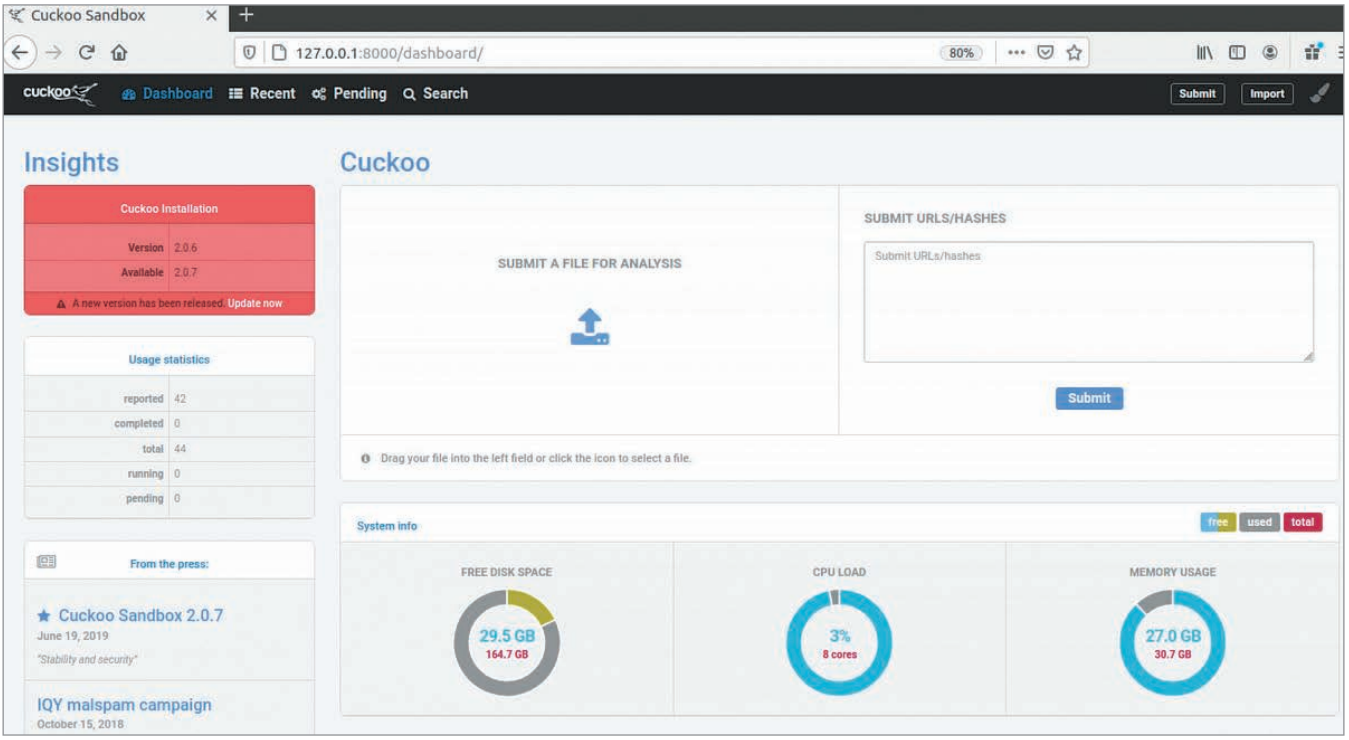
Cuckoo Sandbox Cuckoo Sandbox is an open-source automated malware file analysis system. It can be used to automatically run and analyze files to collect comprehensive analysis results that outline what the malware does while running inside an isolated OS. Figure 5-10 shows the Cuckoo Sandbox interface.

While examining the file, Cuckoo Sandbox can:

- Display traces of calls performed by all processes spawned by the malware.
- Monitor network traffic traces.
- Produce memory dumps of malware processes.
- Provide full memory dumps of the devices.
- Reveal files being created, deleted, and downloaded by the malware during its execution.
- Take screenshots during the execution of the malware.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-10 Cuckoo Sandbox interface



Source: Cuckoo Sandbox

Tools for Analyzing Network IOC

Network data packets that are "seized" as they travel through the network (**packet capture**) can be analyzed to uncover IOC. Analyzing the network for IOC involves performing packet, protocol, and flow analysis.

Packet Analysis

Network data packets can be analyzed to provide valuable network information. Some of the common uses of network packet analysis include troubleshooting network connectivity (determine packet loss, review Transmission Control Protocol (TCP) retransmission, and create graphs of high-latency packet responses), examining Application Layer sessions (captured packets can be used to view a full Hypertext Transfer Protocol (HTTP) session for both requests and responses, view Telnet session commands and responses, and even read email traffic), and solving Dynamic Host Configuration Protocol (DHCP) issues (examine DHCP client broadcasts, view DHCP offers with addresses and options, observe client requests for an address, and see the server's acknowledgment of the request).

These same captured data packets can also be analyzed to provide a wealth of valuable cybersecurity information. Packet analysis can detect unusual behavior (such as a high number of DNS responses) that could indicate the presence of malware, uncover unusual domains or IP address endpoints, and discover regular connections (beacons) to a threat actor's computer.

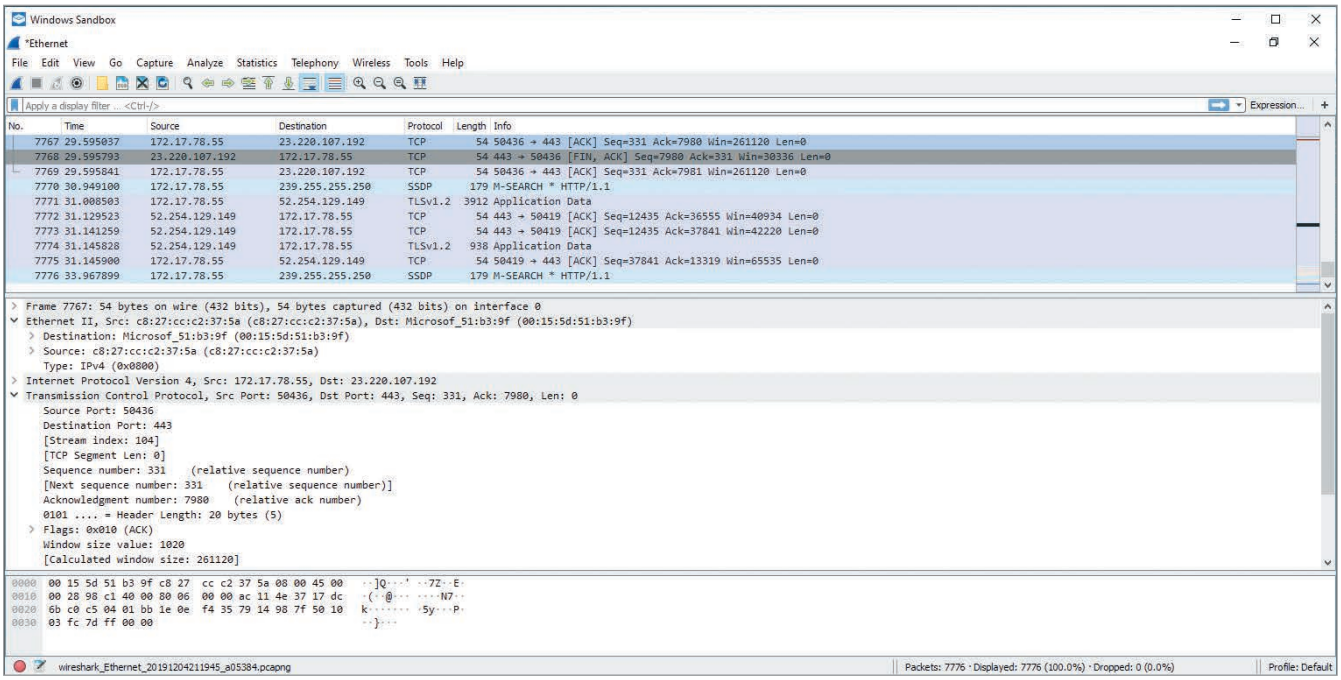
Note 16

Packet analysis typically examines the entire contents of the packet, which consists of both the header information and the payload. However, because all the information needed is rarely contained in a single packet, packet analysis involves the examination of multiple packets—often hundreds and even thousands of them— to "piece together" the information.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

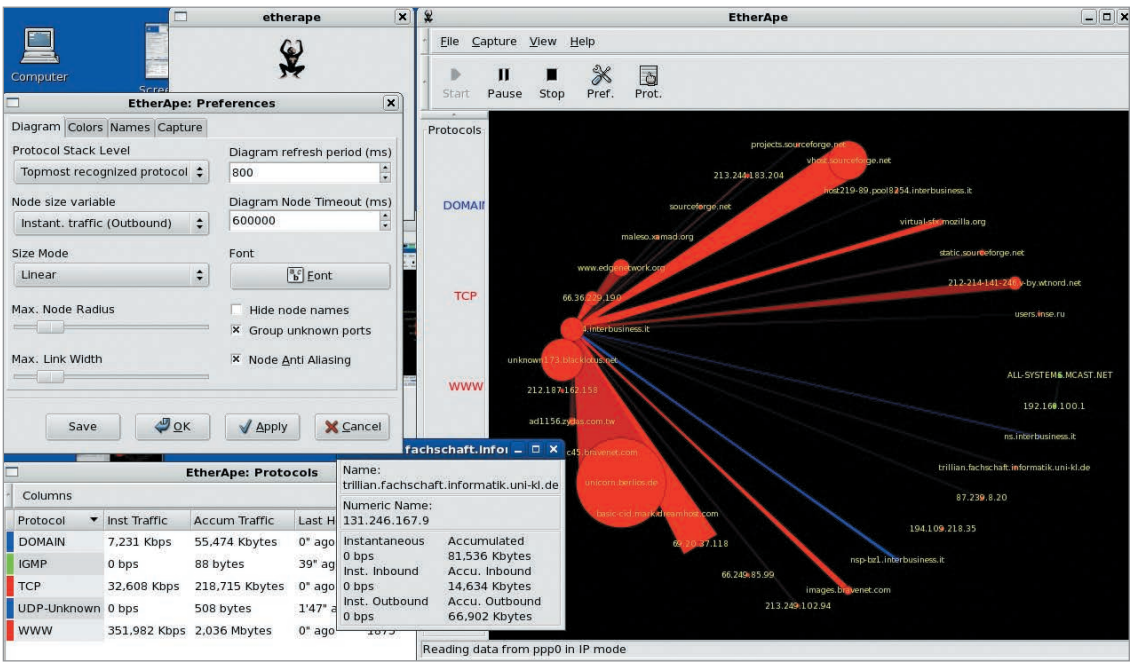
There are several tools that can be used for packet analysis. **Wireshark** is a popular GUI packet capture and analysis tool, shown in Figure 5-11. EtherApe is an open-source tool that is similar to Wireshark but is more focused on giving a virtual interpretation of the information, as illustrated in Figure 5-12. **Tcpdump** is a CLI packet analyzer. It displays TCP/IP packets and other packets being transmitted or received over a network and operates on UNIX and Linux OSs, and various forks of it are available for Windows computers. However, the output from tcpdump can be voluminous and difficult to parse. Tcpreplay is a tool for editing packets and then "replaying" the packets back onto the network to observe their behavior.

Figure 5-11 Wireshark packet capture and analysis tool



Source: Wireshark Software

Figure 5-12 EtherApe packet capture and analysis tool



Source: EtherApe

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Another means by which packet captures can be analyzed is by saving the entire results of the packet capture session and then feeding it into a processing engine that will analyze the packets. Most packet capture programs support an export format known as pcap (*p*acket *cap*ture). However, there are differences between pcap based on the OS being used. Some packet capture programs like Wireshark support two types of filters to support these two means of examining packet captures. A display filter limits what is shown to the user, and a capture filter limits what is saved via pcap for later processing.

Protocol Analysis

Protocol analysis is used to verify which approved protocols are being used and can identify an unauthorized protocol on the network that may be an indication of a successful attack that has penetrated the network. Whereas packet analysis examines the entire contents of the packet, which consists of both the header information and the payload, protocol analysis is only concerned with the header information that contains the protocol information.

Note 17

In a TCP/IP packet, the protocol is an 8-bit value that identifies the protocol being used. A packet analysis tool will automatically decode this value.

Flow Analysis

Although packet analysis is important, examining raw data packets is considered too slow to identify IOC. *Flow analysis* (also called *network traffic analysis*) is the evaluation of a collection of network data: instead of examining the individual performance of a device on the network by looking at raw data packets, network traffic analysis is an aggregate or collection of data from the network's different devices. One of the primary reasons why network traffic analysis is used in this way is because as the network itself becomes the connective link between local resources, virtual computing, and remote cloud servers, it has become the optimum means to view the security of the information technology (IT) infrastructure as a whole.

Flow analysis has been performed for many years in order to troubleshoot network issues and identify performance bottlenecks by identifying which applications are "hogging" resources and bandwidth. The analysis usually looks at overall network utilization and speed by generating statistics based on the flow of data through the network. However, flow analysis for cybersecurity is different than traditional network traffic flow for several reasons:

- **Eliminates monitoring agents.** Threat actors often attempt to disable separate software monitoring agents that are installed on each network device. And some systems, such as database servers, application servers, DNS and DHCP servers, Internet of Things devices, and embedded systems, cannot accept monitoring agents. However, by using network traffic analysis, network data can be collected passively and "quietly" so that threat actors cannot interfere with the data collection.
- **Uses deep packet inspection.** Unlike traditional network traffic analysis that only looks at the flow of data through the network, network traffic analysis for cybersecurity extracts metadata (data about data) from the network packets and then converts it into a readable format using what is called *deep packet inspection*. This can even facilitate decryption of application traffic and its contents so as to identify suspicious activities.
- **Provides richer information.** In addition to standard network analysis (such as identifying bottlenecks), deep packet inspection can identify what devices are active on the network, what applications and protocols they are using, and what data they are accessing. Also, alerts can be set to advise security administrators of any unusual activity or network anomalies.

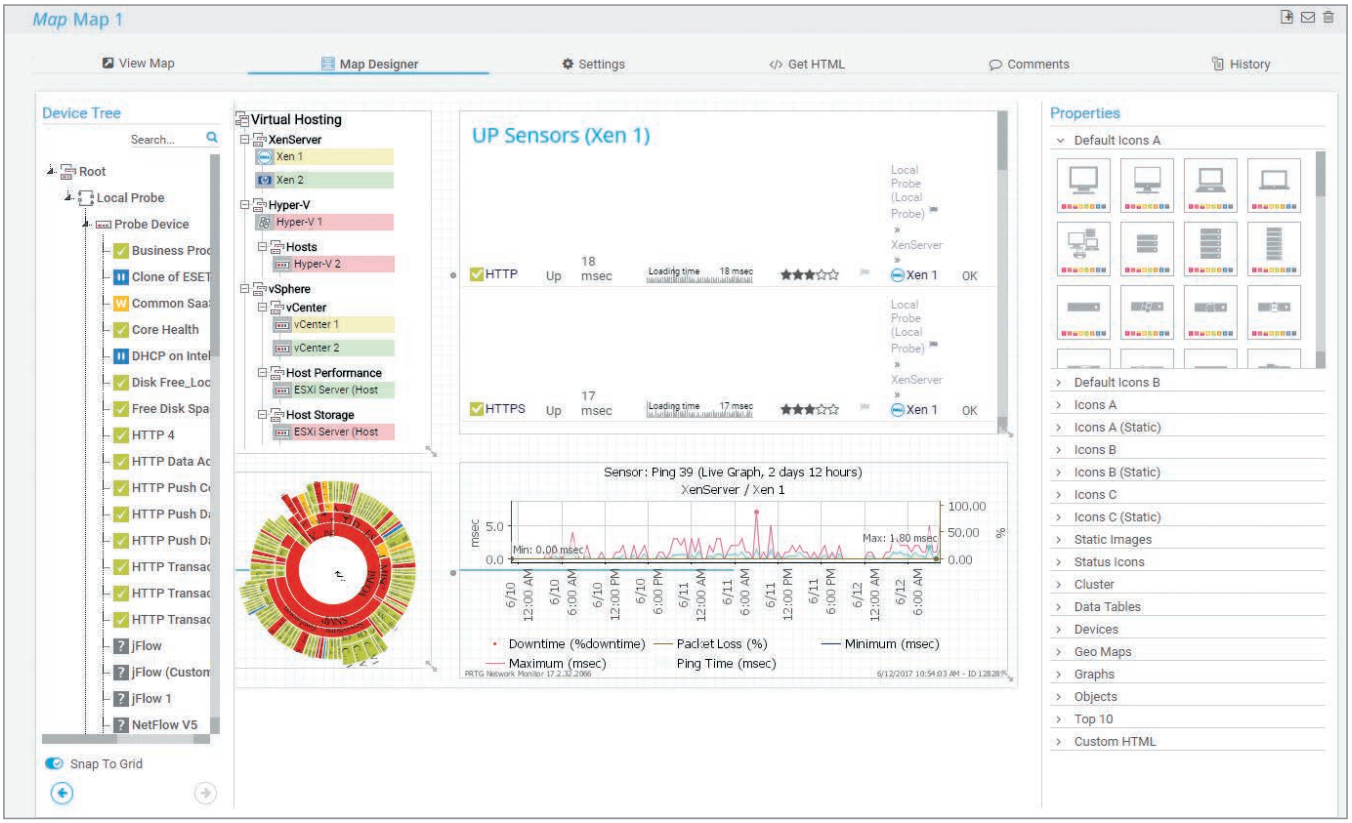
Note 18

Flow analysis is often used in identifying a ransomware attack. Flow analysis can detect when multiple file names are being changed, which is a typical indicator of a ransomware attack, and an alert can be generated in real time.

The output from a flow analysis network traffic analyst tool is shown in Figure 5-13.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-13 Network traffic analysis output



Source: Paessler

Flow analysis data can be accumulated from different sources. NetFlow is a session sampling protocol feature on Cisco routers that collects IP network traffic as it enters or exits an interface and uses TCP/IP Internet Control Message Protocol (ICMP) Echo request packets. sFlow is a packet sampling protocol that gives a statistical sampling instead of the actual flow of packets. IPfix (IP Flow Information Export) is similar to NetFlow but adds additional capabilities, such as integrating Simple Network Management Protocol (SNMP) information directly into the IPfix information so that all the information is available instead of the need to query the SNMP server separately.

Reputation Tools

In 1989 Tim Berners-Lee, a British scientist, created the World Wide Web while working at CERN, the European Organization for Nuclear Research. The first website was fittingly CERN (info.cern.ch). By 1992 the web had grown to 10 websites, but two years later there were 3,000 websites. In 1996 Google was launched and started scanning the 2 million websites that were then in existence. As of mid-2023 there were over 1 billion websites on the Internet, with a quarter of a million new sites added daily.

Note 19

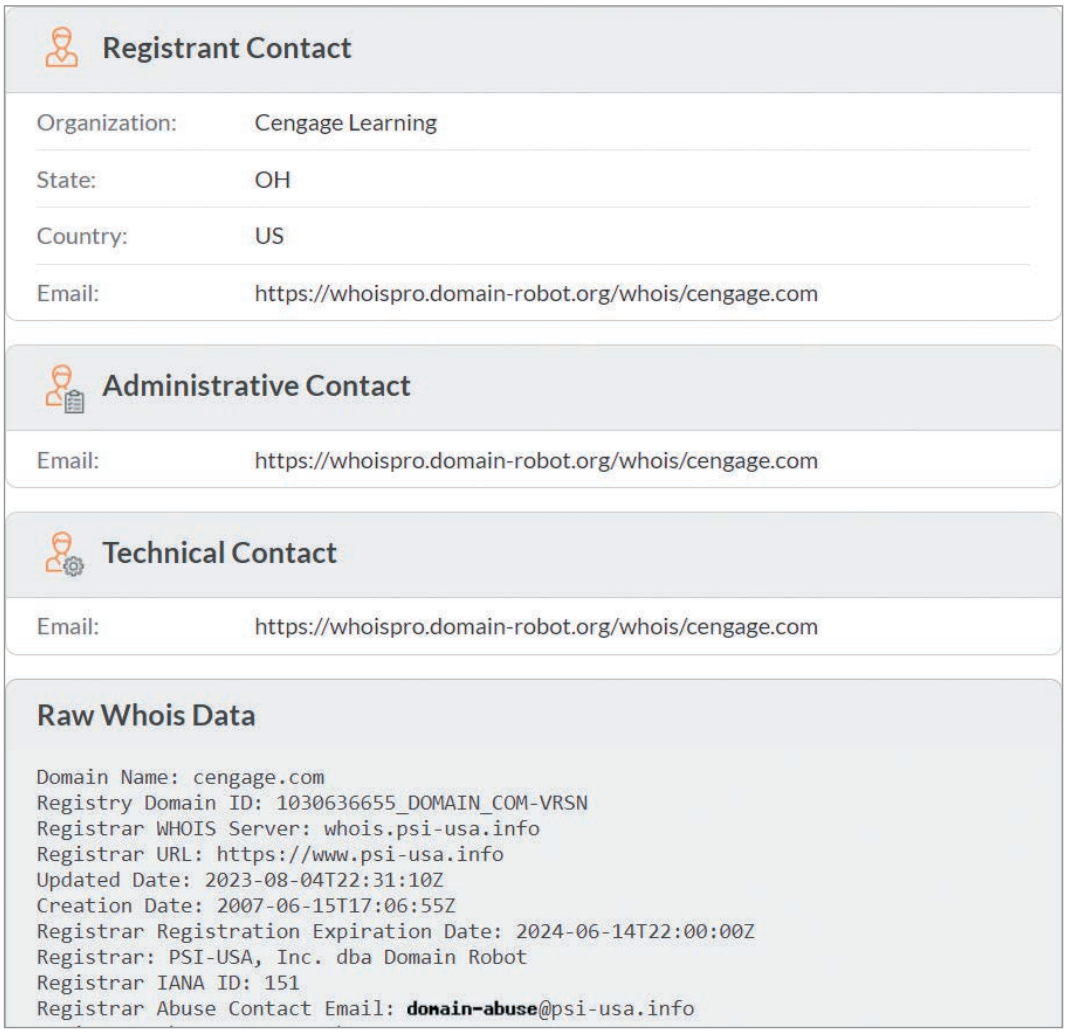
The most visited website in the world is Google, followed by YouTube, Facebook, X (Twitter), and Wikipedia.

However, just as new websites are added to the Internet every hour, so too has the proliferation of malicious websites increased. It is estimated there are over 67 million malicious domains and URLs. Is it possible to identify the "reputation" of website (as to it being legitimate or malicious) to which a device has connected by examining its IP information or DNS information in order to uncover an IOC? This is known as **DNS and IP reputation**.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

One reputation tool is **WHOIS**, which is a TCP/IP query/response protocol for accessing information about Internet resources, most notably domain names and IP addresses as well as internal contact information for websites. It was originally designed to identify those individuals who are responsible for the different network resources but today is used to obtain domain name information. However, much of that information can now be hidden ("redacted") for privacy purposes. A WHOIS lookup for www.cengage.com in Figure 5-14 shows a typical response with limited information for determining the reputation of a website.

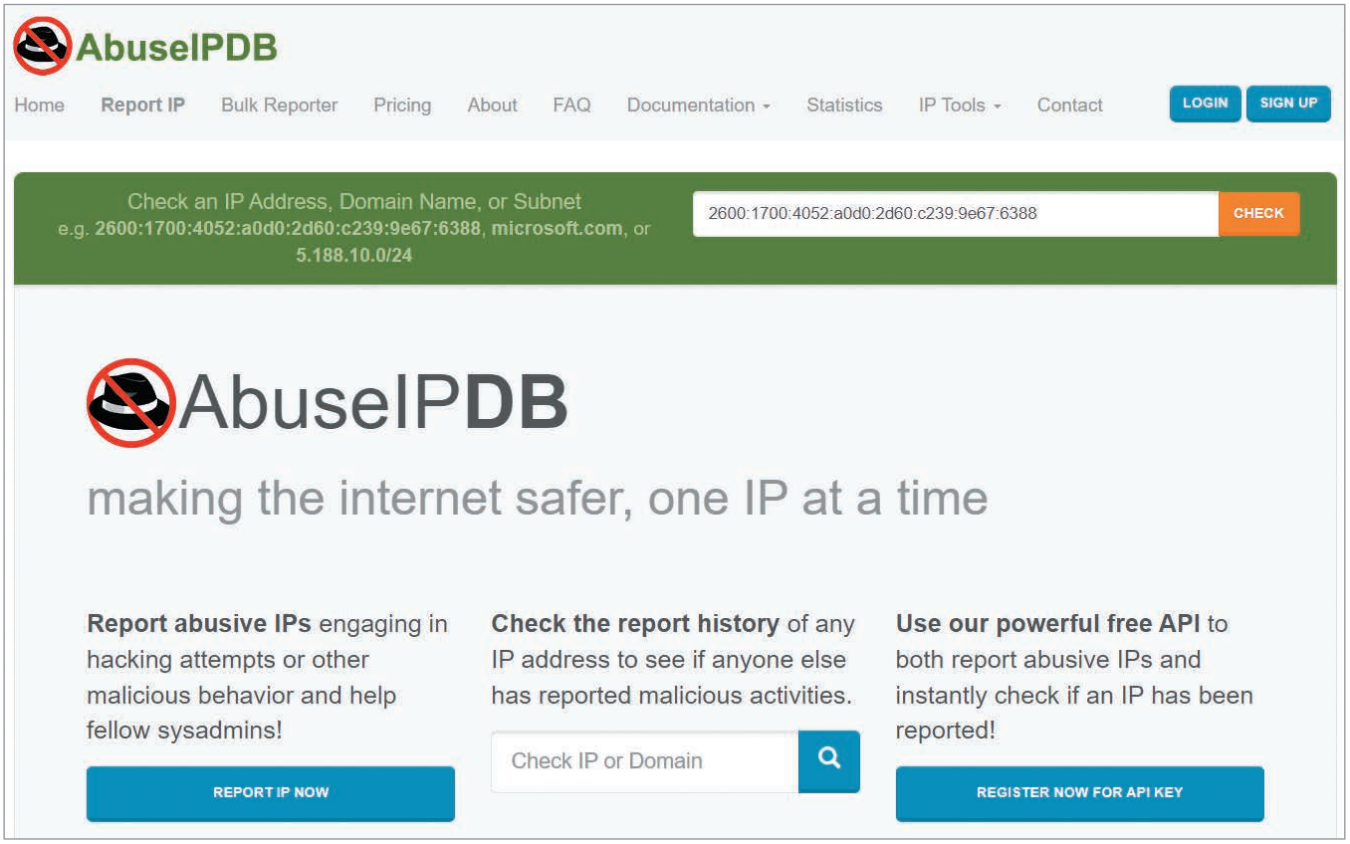
Figure 5-14 WHOIS lookup



Another reputation tool is **AbuseIPDB**. This website serves as a central repository to identify IP addresses that have been reported as being associated with malicious activity online. AbuseIPDB serves as a deny list that can be downloaded and used to block access to malicious sites. In addition, malicious sites can also be reported to AbuseIPDB to be added to the deny list. The AbuseIPDB website is seen in Figure 5-15.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-15 AbuseIPDB website



Source: AbuseIPDB LLC

Note 20

The AbuseIPDB website receives over 22 million submissions each month.

Log Correlation and Analysis Tools

Logs play a critical role in identifying IOC. There are issues surrounding log management, and it is important that logs be consolidated for analysis.

Log Management Issues

A log is a record of events that occur. Cybersecurity logs are particularly important for an IOC because they can reveal the type of attack that was directed at the network and how it successfully circumvented existing security defenses. Categories of logs that typically provide the most beneficial cybersecurity data for an IOC are listed in Table 5-5.

However, the logs listed in Table 5-5 are *categories* of logs and not a listing of the individual logs that are produced. Within each category there are multiple *types* of devices that produce these logs: firewalls, IDSs, IPSs, web application firewalls (WAFs), network address translation gateways, next-generation firewalls, unified threat management (UTM) devices, proxy servers, and so on. And each type of device may have multiple *devices* producing logs; that is, multiple firewalls each produce their own individual logs. Finally, the volume of *detail* in each log produced is granular.

Consider a single basic firewall log that displays the connections that are permitted or denied through the firewall. Typically, a basic firewall log would contain the selected fields listed in Table 5-6. However, there is no standard; vendors include their own choices of information.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 5-5 Categories of log files

Device	Explanation
Firewall logs	Firewall logs can be used to determine whether new IP addresses are attempting to probe the network and if stronger firewall rules are necessary to block them. Outgoing connections, incoming connections, denied traffic, and permitted traffic should all be recorded.
Intrusion detection system (IDS)/intrusion prevention system (IPS) logs	Intrusion detection and intrusion prevention systems record detailed security log information on suspicious behavior as well as any attacks that are detected. In addition, these logs also record any actions IPS used to stop the attacks.
Application logs	Application log files can give information about attacks focused on different applications. If an application log identifies an app that has been the source of a compromise, software can be used to create a dump file, which is a snapshot of the process that was executing and any modules that were loaded for an app at a specific point in time.
Endpoint logs	Endpoint logs can provide a wide range of reports and alerts with events classified by their severity level, such as system events, software installations, removable disk activity, Windows registry changes, and login and session activity.
OS-specific security logs	OS logs typically record system events that are operational actions performed by OS components, such as shutting down the system or starting a service, and audit records that contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account creation and deletion, and use of privileges.
Network logs	Network logs can come from different appliances, such as router and switch logs that provide general information about network traffic.
Metadata logs	Metadata is "data about data," or data that describes information about other data.

Table 5-6 Basic firewall log fields

Field Name	Explanation	Field contents
date	The date of the connection request	The date is in the format *YYYY-MM-DD*
time	The local time of the connection request	The time is in the format *HH:MM:SS*; all times are in 24-hour format
action	The action of the firewall as it processed the request	Possible actions are DROP (refuse the connection), OPEN (allow the connection), CLOSE (terminate the connection), OPEN-INBOUND (inbound session opened to the local computer), or INFO-EVENTS-LOST (processed by the firewall but not recorded in the log)
protocol	The protocol used	TCP, UDP, or ICMP
src-ip	The source IP address	The IP address of the computer attempting to establish communication
dst-ip	The destination IP address	The IP address of the computer to which a connection is attempted
src-port	The source port number	The port number on the sending computer from which the connection was attempted
dst-port	The destination port number	The port on the receiving computer to which the sending computer was trying to make a connection
size	The size of the packet	The packet size in bytes
tcpflags	TCP control flags	Information about TCP control flags in the TCP headers

(*continues*)

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 5-6 (*Continued*)

Field Name	Explanation	Field contents
tcpsyn	The TCP sequence number	The TCP sequence number in the packet
tcpack	The TCP acknowledgment number	The TCP acknowledgment number in the packet
tcpwin	The TCP window size	The TCP window size in bytes
icmptype	The ICMP type	Information about the ICMP message type
icmpcode	The ICMP code	Information about the ICMP code type
info	The information on the action	An entry that depends on the type of action that occurred
path	The direction of the communication	SEND, RECEIVE, FORWARD, or UNKNOWN

It quickly becomes apparent that there is a massive amount of log data generated related to cybersecurity. And the amount of data is not the only issue surrounding log management, which is defined as transmitting, collecting, analyzing, and disposing of log data. Other log management issues include:

- **All events recorded.** Devices record all events, even those that are not cybersecurity related, which increases the amount of data that is generated.
- **Conflicting interpretations.** Each type of device may interpret an event in a different context, so that a router looks at an event differently than a firewall does. And this can produce different alerts: one device may see an event as only a warning while another device may interpret it as a serious event. This can create a confusing mix of log data.
- **Different log formats.** Different devices record log information in different formats and even with different data captured. Manually combining multiple logs, each with a different format, can be a major challenge.

Log Ingestion

One solution to the problems surrounding cybersecurity log management is **log ingestion**, which is the process of formatting and uploading log data from the different sources that generate log data to a central location for analysis. Log ingestion also transforms unstructured log data into a structured format so that it can be queried and filtered more easily. Log ingestion involves synchronizing timestamps of the different logs and identifying the various logging levels.

Time Synchronization

Because log ingestion involves combining log data from a variety of sources, it is critical that the recorded times of a single event all match (**time synchronization**). Otherwise, it would not be possible to see the impact of a single event on multiple devices, or erroneously think (because the times do not align) that the same event was actually two separate events.

Typically, network administrators implement the Network Time Protocol (NTP) to synchronize timekeeping across a set of distributed time servers and clients. NTP runs over the User Datagram Protocol (UDP) using port 123. The NTP network of servers typically obtains its time from highly accurate atomic clocks or GPS clocks linked to time servers, and NTP is used to distribute this time across internal networks.

Logging Levels

A **logging level** is a means of classifying log entries in terms of urgency. Classifying helps filter log files by controlling the amount of data in a log. Table 5-7 lists the different logging levels from most data accumulated to least data accumulated.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 5-7 Logging levels

Level	Description	Usage examples
ALL	All logging information is recorded.	This is rarely used due to the large volume of log data accumulated.
TRACE	The most granular information is recorded with TRACE and is very detailed.	TRACE is only used in rare cases where the full visibility of what is happening inside an application and the third-party libraries is needed.
DEBUG	DEBUG is less granular compared to the TRACE level but is more than is necessary for everyday use.	The DEBUG log level should be used for information that may be needed for diagnosing issues and troubleshooting or when running an application in a test environment.
INFO	This is the standard log level indicating that something occurred, such as an application entered a certain state.	The information logged using the INFO log level is purely informative to the degree that not consulting this data on a regular basis would not result in missing key information.
WARN	WARN indicates that something unexpected happened in the application or that a situation arose that might disturb one of the processes (it does not mean that that the application itself failed).	The WARN level provides information about situations that are unexpected, but the application continues to function, such as a parsing error occurring that resulted in a certain document not being processed.
ERROR	The ERROR log level provides information about an application experiencing an issue preventing one or more functions from properly working.	The ERROR log level can reveal when a function is no longer available, such as one of the payment systems in an e-commerce site, but the process can still continue (another option functions to check out the basket).
FATAL	This log level indicates that the application encountered an event or entered a state in which one of the crucial business functionalities is no longer working.	A FATAL log level reveals when the application is not able to function, such as connecting to a crucial data store like a database.
OFF	No log information is recorded.	Rarely would logging be completely turned off for any reason.

Note 21

An example of the different logging levels can be illustrated by a user logging into a system. Successfully logging in is normal and logs an INFO event. However, a user who enters the wrong password is rejected and logs a WARN event. After three unsuccessful attempts, the user is locked out of their account, and this generates an ERROR event.

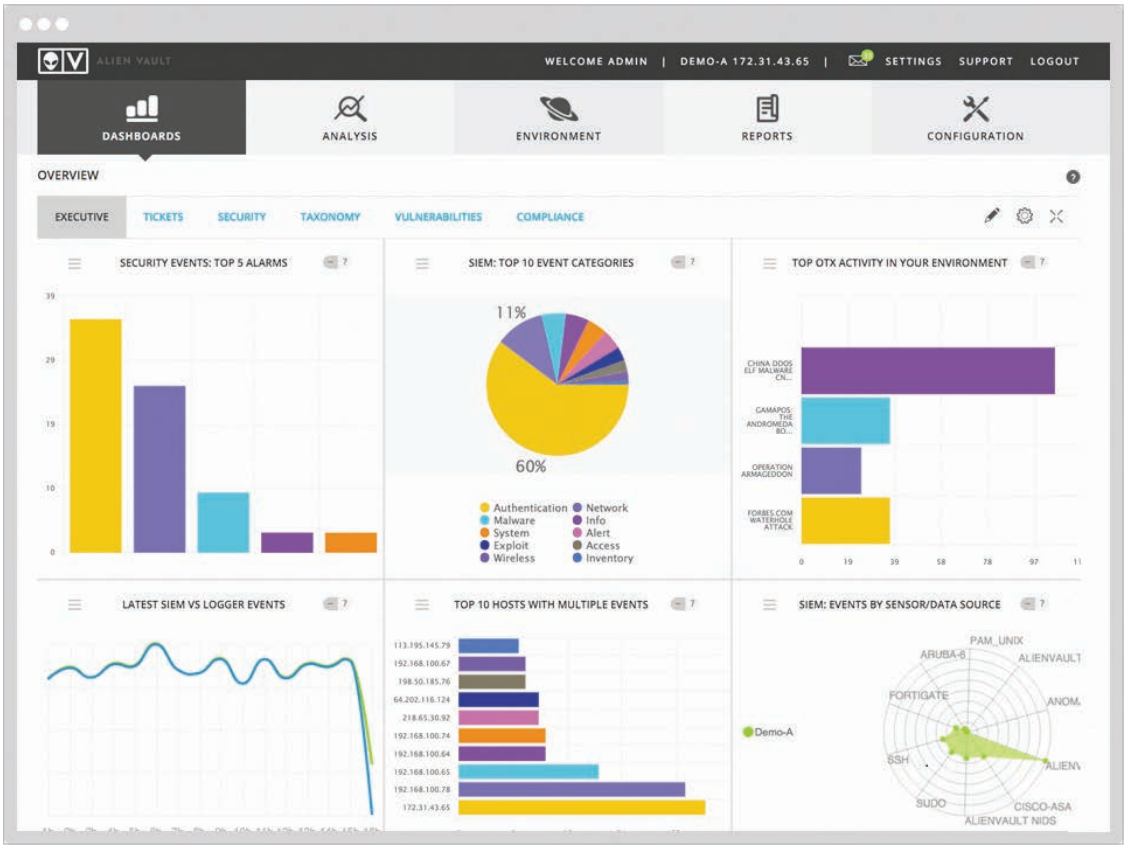
Log Analysis Tools

Despite the value of log ingestion, it does not solve log management issues. There is a need for highly automated log analysis tools. Some of the primary tools are security information and event management; security orchestration, automation, and response; and endpoint detection and response.

Security Information and Event Management (SIEM) A **security information and event management (SIEM)** product (usually pronounced *seem* instead of *sim*) consolidates real-time monitoring and management of security information with analysis and reporting of security events. A SIEM product can be a separate device, software that runs on a computer, or even a service provided by a third party. A SIEM dashboard is shown in Figure 5-16.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-16 SIEM dashboard



Source: AT&T Cybersecurity

A SIEM typically has the following features:

- **Aggregation.** SIEM aggregation combines data from multiple data sources, such as network security devices, servers, and software applications, to build a comprehensive picture of attacks.
- **Correlation.** The SIEM correlation feature searches the data acquired through SIEM aggregation to look for common characteristics, such as multiple attacks coming from a specific source.
- **Automated alerting and triggers.** SIEM automated alerting and triggers can inform security personnel of critical issues that need immediate attention. A sample trigger may be "Alert when a firewall, router, or switch indicates 40 or more drop/reject packet events occur from the same IP source address occurring within 60 seconds."
- **Time synchronization.** SIEM time synchronization can help correctly identify an event as one single event and not multiple events that have varying timestamps.
- **Event duplication.** When the same event occurs that is detected by multiple devices, each will generate an alert. The SIEM event duplication feature can help filter the multiple alerts into a single alarm.
- **Regulatory compliance.** SIEM devices usually provide a built-in template to support and record specific regulatory compliance. SIEM logs can also be retained for future analysis and to show that the enterprise has been in compliance with regulations.

Security Orchestration, Automation, and Response (SOAR) An orchestra is a large instrumental ensemble (group) that plays a variety of types of music. Composed of four families of instruments (strings, brass, woodwinds, and percussion), a full symphony orchestra can have over 100 members, while a smaller chamber orchestra may still have up to 40 different members, depending on the music being played. The conductor is responsible for bringing the orchestra to a specific interpretation of the piece being played while leading rehearsals. The conductor "takes apart" the piece of music during rehearsals to practice with the different families and groups of instruments before bringing everything together in the performance. A symphony orchestra is seen in Figure 5-17.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-17 Symphony orchestra



Source: Dziurek/Shutterstock.com

Note 22

A symphony orchestra is defined by its string family; without the strings it would be classified as a band.

In recent years, the concept of a musical orchestra in which many varied instruments all work together, called orchestration, has made its way into cybersecurity. Often called "workflow orchestration," it involves the automation and combination of many different individual tasks and processes. In contrast to cybersecurity automation that only automates one task, workflow orchestration involves organizing many tasks into a functional process (workflow) that is automated. In other words, workflow orchestration is automation used for entire processes instead of for a single task. The various components of workflow orchestration are large and complex. This is because they cross multiple platforms and involve hardware, software, middleware, and services and use multiple automated (and sometimes semi-automated) tasks to automatically execute a workflow.

Caution !

Although on occasion cybersecurity literature will use cybersecurity automation and workflow orchestration synonymously, this is incorrect. Security automation is setting a single security operations-related task to run on its own without the need for human intervention, whereas workflow orchestration is automating multiple tasks that make up an entire process.

Workflow orchestration has given rise to a new type of cybersecurity platform known as a **security orchestration, automation, and response (SOAR)** platform. SOAR is a combination of software programs and tools that allow organizations to synthesize and automate a range of security operations, threat intelligence, and incident response in a single platform. Figure 5-18 illustrates a SOAR dashboard.

Note 23

In Figure 5-18, the SOAR dashboard displays a "Dollars saved" amount, which is a common feature.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 5-18 SOAR dashboard



Source: Metron Labs

The function of a SOAR platform can most clearly be seen when compared to a SIEM product. A SIEM consolidates real-time monitoring and management of security information with analysis and reporting of security events. It can perform automated alerts and triggers to inform security personnel of critical issues that need immediate attention. A SOAR, on the other hand, can go farther and automatically take immediate action against the threat; this means that a SOAR can perform as both an IOC and an IOA. Consider a threat actor who is attempting to use a brute-force attack against a login prompt. Normally this would result in a human security administrator receiving an alert. The administrator would then have to open the firewall app and manually block the IP address of the attacker. However, when using a SOAR platform, the SOAR can automatically and immediately block the IP address of a computer that is attempting to brute-force a login.

Note 24

SIEM and SOAR devices are not competitive and alternative technologies (either/or) but are complementary tools (both/and) that help organizations respond to security threats. Whereas a SIEM helps SOC teams detect threats based on data collected from applications and the infrastructure, a SOAR responds to threats in a more efficient manner.

Endpoint Detection and Response (EDR)

Endpoint detection and response (EDR) tools have a similar functionality to host-based intrusion detection systems (HIDS) of monitoring endpoint events and of HIPS of taking immediate action. However, EDR tools are considered more robust than HIDS and HIPS. First, an EDR can aggregate data from multiple endpoint computers to a centralized database so that security professionals can perform further IOC investigation and also gain a better picture of events that are occurring across multiple endpoints instead of just on a single endpoint. This can help determine if an attack is more widespread across the enterprise and if more comprehensive and higher-level action needs to be taken. Second, EDR tools can perform more sophisticated analytics that identify patterns and detect anomalies. This can help detect unusual or unrecognized activities by performing baseline comparisons of normal behavior.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 25

Many EDRs also allow for a manual or user analysis of the data.

Two Rights & A Wrong

1. VirusTotal is an app to download and install on a local device.
2. Tcpdump is a command-line packet analyzer for UNIX and Linux OSs.
3. Flow analysis uses deep packet inspection.

See the answers at the end of the chapter.

Summary

- The digital artifacts that serve as evidence of an attack are called indicators of compromise (IOC). This evidence is used to determine what deficiencies exist and what should be fixed. IOC are one or more indicators of a successfully completed attack. There are several common techniques that cybersecurity professionals use to examine an exploited system when looking for IOC. When diagnosing a file to determine if it contains malware, a message digest (hash) of the file can be generated and compared with a list of digests created from files that have previously been identified as malware. Using hashing algorithms to generate message digests on malware helps to standardize and simplify the exchange of IOC among cybersecurity researchers. Another approach is to examine the file itself for evidence of malware. Dynamic file analysis executes the program and then observes its behavior. Static file analysis is also called code analysis because it looks at the different code components of the file. This involves examining the file structure, recognizing patterns in strings, and identifying dynamic URLs used for C&C. However, threat actors go to great lengths to create dynamic C&C URLs.
- A sometimes-overlooked system that requires monitoring is the email system. The basic components involved in sending and receiving email are the mail user agent (MUA) and mail transfer agent (MTA). A MUA is what is used to read and send mail from an endpoint and could be an app or a webmail interface. MTAs are programs that accept email messages from senders and route them toward their recipients. As email is transferred from MTA to MTA, information is added to the email header. The email header contains information about the sender, recipient, email's route through MTAs, and various authentication details. There are a variety of threats related to email. There are different email defenses that can be used to protect email. These include Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).
- Behavior-based monitoring continuously analyzes the behavior of processes and programs on a system and sounds an alert if it detects any abnormal actions, at which point a decision can be made. Behavior-based monitoring uses "normal" processes and actions as its standard (known-good behavior) instead of only searching for abnormalities (anomalous behavior). Both users as well as technology systems have normal behaviors and can be monitored for any unusual activity. Examining user behavior is known as user behavior analysis (UBA). Applying this analysis to both users as well as "entities" such as networks, devices, applications, and servers (called system and application behavior) is called user and entity behavior analysis (UEBA). Two common examples of UBA are abnormal account activity and impossible travel. However, there are limitations to UBA.
- There are several different tools that can be used for uncovering IOC. Analyzing files for evidence of malware should be done in a fully protected environment. This is called sandboxing. Sandboxing allows code to be observed and analyzed in a safe,

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

isolated environment. A local sandbox is essentially an isolated virtual machine (VM); anything run within the sandbox will impact only the VM and not the underlying computer. Whatever occurs within the sandbox is not visible to other applications or the operating system outside the sandbox. Also, the contents of the sandbox do not have to be saved when the sandbox is closed. There are remote online sandbox sites to which malware can be uploaded and automatically evaluated. These include VirusTotal, Joe Sandbox, and Cuckoo Sandbox.

- Network data packets can be analyzed to provide valuable network performance information. This same data can also be analyzed to provide a wealth of valuable cybersecurity information. There are several tools that can be used for packet analysis. Wireshark is a popular GUI packet capture and analysis tool. Tcpdump is a command-line packet analyzer and operates on UNIX and Linux operating systems, and various forks of it are available for Windows computers. However, the output from tcpdump can be voluminous and difficult to parse. Another means by which packet captures can be analyzed is by saving the entire results of the packet capture session and then feeding it into a processing engine that will analyze the packets. Protocol analysis is used to verify which approved protocols are being used and can identify an unauthorized protocol on the network that may be an indication of a successful attack that has penetrated the network. Flow analysis, also called network traffic analysis, is the evaluation of a collection of network data for analysis.
- With over one billion websites in existence today, it can be difficult to identify the reputation of a website as to whether it is legitimate or malicious. This is known as examining the site's DNS and IP reputation. One reputation tool is WHOIS, which can be used to obtain domain name information. Another reputation tool is AbuseIPDB. This website serves as a central repository to identify IP addresses that have been reported as being associated with malicious activity online.
- A log is a record of events that occur. Cybersecurity logs are particularly important for an IOC because they can reveal the type of attack that was directed at the network and how it successfully circumvented existing security defenses. However, a problem with log files is the massive amount of log data generated. There are multiple categories of logs and within each category there are multiple types of devices that produce these logs. And each type of device may have multiple devices producing logs; that is, multiple firewalls each produce their own individual logs. Finally, the volume of detail in each log produced is granular. Other log management issues include that all events are recorded whether or not they are cybersecurity related, there can be conflicting interpretations, and the log formats differ.
- One solution to the problems surrounding cybersecurity log management is log ingestion, which is the process of formatting and uploading log data from the different sources that generate log data to a central location for analysis. Log ingestion also transforms unstructured log data into a structured format so that it can be queried and filtered more easily. Log ingestion involves synchronizing timestamps of the different logs and identifying the various logging levels. Despite the value of log ingestion, it does not solve log management issues.
- There is a need for highly automated log analysis tools. A security information and event management (SIEM) product consolidates real-time monitoring and management of security information with analysis and reporting of security events. A SIEM product can be a separate device, software that runs on a computer, or even a service provided by a third party. A security orchestration, automation, and response (SOAR) platform is a combination of software programs and tools that allow organizations to synthesize and automate a range of security operations, threat intelligence, and incident response in a single platform. While a SIEM consolidates real-time monitoring and management of security information with analysis and reporting of security events and can perform automated alerts and triggers to inform security personnel of critical issues that need immediate attention, a SOAR, on the other hand, can go farther and automatically take immediate action against the threat; this means that a SOAR can perform as both an IOC and an IOA. Endpoint detection and response (EDR) tools can aggregate data from multiple endpoint computers to a centralized database so that security professionals can perform further IOC investigation.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Key Terms

abnormal account activity
AbuseIPDB
command and control (C&C)
Cuckoo Sandbox
DNS and IP reputation
Domain-based Message Authentication, Reporting, and Conformance (DMARC)
Domain Keys Identified Mail (DKIM)
email analysis
email header
embedded links
endpoint detection and response (EDR)
file analysis
hashing
impersonation
impossible travel
interpret suspicious commands
Joe Sandbox
log ingestion
logging level
packet capture
pattern recognition
sandboxing
security information and event management (SIEM)
security orchestration, automation, and response (SOAR)
Sender Policy Framework (SPF)
strings
tcpdump
time synchronization
user behavior analysis (UBA)
VirusTotal
WHOIS
Wireshark

Review Questions

1. Which types of indicators are focused on detecting a successfully completed attack and show how it happened?
   - **a.** IOC
   - **b.** IOD
   - **c.** IOA
   - **d.** IOZ
2. Which technique of file analysis uses debuggers to watch the behavior of a file?
   - **a.** Federated
   - **b.** Open
   - **c.** Dynamic
   - **d.** Static
3. Which of the following is a remote online structure for sending commands to infected devices?
   - **a.** C&D
   - **b.** C&C
   - **c.** C&A
   - **d.** R&C
4. Which of the following remote sandboxing tools inspects items with over 70 antivirus scanners and URL/domain blocklisting services?
   - **a.** Joe Sandbox
   - **b.** SSDT View
   - **c.** Cuckoo Sandbox
   - **d.** VirusTotal
5. Which website serves as a central repository to identify IP addresses that have been reported as being associated with malicious activity online?
   - **a.** WHOIS
   - **b.** AbuseIPDB
   - **c.** CERN-X
   - **d.** WEBx
6. Which of the following logging levels accumulates all logging information?
   - **a.** ALL
   - **b.** TRACE
   - **c.** DEBUG
   - **d.** INFO
7. Which of the following email defenses uses a digital signature?
   - **a.** DKIM
   - **b.** SPC
   - **c.** DMARC
   - **d.** It depends on whether or not the email payload has been encrypted.
8. Which of the following is NOT correct regarding forwarding emails?
   - **a.** The best policy is to only forward highly sensitive emails.
   - **b.** Employees may decide to auto-forward corporate emails to utilize enhanced spam filtering.
   - **c.** Forwarded emails may not be available for eDiscovery.
   - **d.** Unauthorized users could access forwarded emails.
9. Which of the following is NOT correct about an email header?
   - **a.** As email is transferred from MTA to MTA, information is added to the email header.
   - **b.** Email headers are encrypted to prevent someone from altering the contents.
   - **c.** The email header contains information about the sender, recipient, email's route through MTAs, and various authentication details.
   - **d.** Each MTA along the path adds its own information to the top of the email header.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

10. Which tool would a threat actor use in malware to generate random dynamic URLs?

a. DGA
b. RSA
c. X-SPING
d. RCSC

11. Why would a threat actor choose Windows Command Shell over PowerShell?

a. Windows Command Shell is being deprecated and will no longer be supported in future versions of Microsoft Windows products.
b. Using PowerShell in malware requires a complicated registry "hack."
c. Windows Command Shell commands can be invoked without starting a new identifiable process.
d. Windows Command Shell is faster than PowerShell.

12. Which email authentication method identifies who the MTA email servers are that have been authorized to send email for a domain?

a. TLL
b. MTU
c. MTA
d. SPF

13. Which of the following is NOT a limitation of UBA?

a. Threat actors will often target agents that collect data to disable them or bypass them so as to not raise an alarm.
b. UBA imposes a serious processing burden on systems and networks.
c. There are also challenges related to building a profile of users who access distributed applications.
d. Building a complete understanding of each and every application is difficult to achieve.

14. Which packet analyzer tool uses a CLI?

a. Wireshark
b. EtherApe
c. Tcpdump
d. ARC-View

15. Which of the following is NOT a reason flow analysis for cybersecurity is different than traditional network traffic flow analysis?

a. Eliminates monitoring agents
b. Uses deep packet inspection
c. Provides richer information
d. Executes faster

16. Which of the following tools is limited because information can be redacted for privacy purposes?

a. AbuseIPDB
b. WHOIS
c. Joe Sandbox
d. VirusTotal

17. Which of the following category of logs records detailed cybersecurity log information on suspicious behavior as well as any attacks that are detected and then blocked?

a. Firewall
b. Endpoint
c. Metadata
d. IDS/IPS

18. Which of the following is NOT a cybersecurity log management issue?

a. Only events that have previously been analyzed can be recorded in a log.
b. Log formats can vary.
c. There are conflicting interpretations of events by different devices.
d. All events are recorded.

19. Which of the following is the difference between a SIEM and a SOAR?

a. Only a SIEM can perform as both an IOC and an IOA.
b. A SIEM performs automated alerts and triggers to inform security personnel of critical issues while a SOAR can automatically take immediate action against a threat.
c. There are no appreciable differences between a SIEM and a SOAR.
d. SIEMs can only operate on endpoint devices while SOARs are network based.

20. Which of the following is NOT correct about EDR tools?

a. EDR tools can aggregate data from multiple endpoint computers to a centralized database so that security professionals can perform further IOC investigation.
b. They can perform more sophisticated analytics that identify patterns and detect anomalies to help detect unusual or unrecognized activities by performing baseline comparisons of normal behavior.
c. EDR tools require network-based sensors to gather data for analysis.
d. They have a similar functionality to HIDS of monitoring endpoint events and of HIPS of taking immediate action.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Projects

Case Project 5-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. What are your thoughts about these new SEC regulations? For this week's discussion, list one reason you would favor these new SEC regulations and two reasons you would not (that's because more "no" reasons are discussed than "yes" reasons). Should reporting be streamlined? Is it reasonable to even have such reporting requirements today? Finally, give your suggestion about how to handle this. Write a one-page paper about this.

Case Project 5-2: Domain Generation Algorithm Tactics

Estimated Time: 25 minutes
Objective: Identify advanced DGA tactics used by threat actors.
Description: Today threat actors have turned to adding code to malware to create dynamic C&C URLs. This technique uses a DGA to create the URLs, and the techniques can range from basic to very sophisticated. Use the Internet to identify a sophisticated DGA that has been used by threat actors. "Dissect" the DGA as much as possible and explain how it works. Finally, give a defense as to how it could be recognized.

Case Project 5-3: File Analysis Tool

Estimated Time: 30 minutes
Objective: Compare file analysis tools.
Description: Remote online sandbox sites allow you to upload malware so that it can be automatically evaluated. Compare the results of two file analysis tools, VirusTotal and Joe Sandbox. Start by downloading an anti-malware test file from EICAR (https://www.eicar.org/download-anti-malware-testfile/). Note that this is only a test file and will not infect a computer with malware. Also, it may be necessary to temporarily turn off anti-malware software in order to download the test file. Then, upload the file to VirusTotal (https://www.virustotal.com/gui/home/upload) for analysis. Note the different options available, and experiment with several of these. Now do the same with Joe Sandbox (https://www.joesandbox.com/#windows). Which of these file analysis tools provide the most helpful information? Why? Write a one-page paper on your research.

Case Project 5-4: Wireshark

Estimated Time: 25 minutes
Objective: Research the uses of Wireshark in cybersecurity.
Description: Wireshark is a popular packet analysis tool. Use the Internet to research how Wireshark can be used for cybersecurity. Detail one use case that describes its usage in recognizing attacks. Write a one-page paper on your research.

Case Project 5-5: Security Information and Event Management versus Security Orchestration, Automation, and Response

Estimated Time: 25 minutes
Objective: Compare SIEM and SOAR.
Description: Use the Internet to research the differences between SIEM and SOAR. When would you use each technology? How can they be used together? What are the advantages and disadvantages of each? Write a one-page paper on your findings.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong: Answers

Common Techniques for Investigating IOC

1. There are three types of file analysis techniques: dynamic, static, and hash.
2. Threat actors today add code to malware to create dynamic C&C URLs.
3. SPF is an email authentication method that identifies who the MTA email servers are that have been authorized to send email for a domain.

Answer: The wrong statement is #1.

Explanation: If a message digest (hash) comparison does not yield results, the next step is to perform a file analysis, looking for evidence of malware within the file. There are two common techniques used when analyzing a file: dynamic file analysis and static file analysis.

Tools for IOC Analysis

1. VirusTotal is an app to download and install on a local device.
2. Tcpdump is a command-line packet analyzer for UNIX and Linux OSs.
3. Flow analysis uses deep packet inspection.

Answer: The wrong statement is #1.

Explanation: VirusTotal is a remote sandbox that inspects items using over 70 antivirus scanners and URL/domain blocklisting services that are updated frequently.

Reference

1. "Threat Brief: Understanding Domain Generation Algorithms (DGA)," *Paloalto*, Feb. 7, 2019, accessed Jan. 9, 2021, https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 6

Threat Detection and Process Improvement

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Explain threat intelligence
2. Contrast different roles and methodologies of threat hunting
3. Describe the different means to improve security operation processes

#TrendingCyber

Cybersecurity threat intelligence (TI) is a booming segment within the cybersecurity industry. The commercial market for TI products and services is valued at more than $5 billion globally, and it is predicted to triple over the next five years.

TI helps address a major challenge facing all organizations, namely identifying and understanding all relevant cybersecurity threats. Some TI can be extracted from an organization's security devices, such as a firewall log that captures the external Internet Protocol (IP) addresses of a threat actor attempting a brute-force attack on passwords or a spam filter that can identify emails that contain a phishing Uniform Resource Locator (URL). These IP addresses and URLs, known as indicators of compromise (IOA), can then be fed into the organization's Security Information and Event Management (SIEM) tool or an intrusion detection system (IDS) to ward off the attacks. But these "local" IOA are only a fraction of the total threat landscape at any given moment. Instead of relying on their own TI, most organizations turn to external sources that can not only provide information about a broader range of attacks but can also extract more information from the data to reveal new patterns and trends.

There are different sources of TI. Open-source TI typically consists of public lists of indicators, sometimes called *abuse feeds* or *blacklists*. Shared TI is a collaboration between trusted communities in which the members exchange their own threat information. Another source is paid TI in which organizations subscribe for a fee to be supplied relevant and current TI. This not only provides TI information as electronic "feeds" (input) into security appliances but also typically gives in-depth research and even specialized services for a specific market sector, such as government or financial services. A recent survey of security professionals in North America and the United Kingdom found that 44 percent of respondents say that paid TI is the primary source of TI for their organization.

How accurate is this data from paid TI providers? These providers do not openly share their information with outsiders or researchers so that it can be compared and evaluated. In fact, they rarely even advertise the cost of their services (estimates range up to $650,000 annually, depending on the size of the organization). However, security researchers were recently able to analyze and compare paid TI.[1] What they found was surprising.

When comparing TI feeds from paid TI sources, the researchers discovered little if any overlap, that is, a threat identified from one paid TI source was not identified by another TI source. In fact, only 1.3 percent of the IOA of Paid IT Source #2 were found in Paid IT Source #1. In one analysis, the researchers tracked 22 threat actors in two separate

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

feeds and found only 2.5 to 4.0 percent of the indicators were in both TI feeds. Even the highest overlap was only 21 percent, which was the IP address of a specific threat actor. The researchers concluded that each paid TI source observes unique indicators of cybersecurity incidents, and that helps to explain why information from one TI source is not found in the feed from another TI source.

When they looked at the timeliness of the TI, they found that one TI paid source identified a threat one month earlier than another source, which could leave organizations subscribing to the second source unprotected for 30 days. Although it could be assumed that paid TI sources would provide the information more quickly than other types of sources, they were faster in only half of the analyzed cases. That means that half of the time, the open-source and shared TI were quicker in getting their alerts out.

Another surprising insight was how the subscriber organizations use the data. Many organizations highly value the more selective and curated TI from a paid source—but not just because it is used for network detection of attacks. Rather, they value the TI because it decreases the time that their internal cybersecurity analysts must spend poring over the data (open-source and shared TI usually contain large volumes of data and are not vetted).

While TI is important for organizations to protect themselves from cybersecurity attacks, the researchers concluded that the true value of TI data from paid TI sources may not be as high as it should be. Given that 44 percent of organizations use paid TI as their primary source, this could result in gaping holes in their defenses.

"No man is an island; no man lives alone" is part of a famous poem by John Donne. While this is true in virtually all walks of life, it can particularly be applied to cybersecurity. Imagine an organization that strictly kept to itself and did not monitor the outside world to keep abreast of the latest tactics, techniques, and procedures (TTP) of threat actors. Without a knowledge of the current landscape, they would be unable to adequately shore up their defenses for the onslaught of attacks. This knowledge can come about not only through their own analysis but also that combined from other attack victims as well.

Being aware of the most recent attacks goes beyond gathering information. It likewise involves actively seeking and searching for indicators that threat actors have already infiltrated the organization's network. This information is then used for improving the processes surrounding overall security operations.

In this chapter you explore these three areas, namely threat intelligence, threat hunting, and improving security operation processes.

Threat Intelligence

Certification

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

Threat intelligence is an important tool for organizations defending themselves against attacks. Using TI involves understanding what it constitutes, how it compares to threat data, knowing the intelligence cycle, and understanding its categories of sources and confidence levels.

What Is Threat Intelligence (TI)?

At one time, organizations were reluctant to share information about successful attacks on their assets. Would the release of such information make the organization look bad? Would it hinder ongoing investigations by law enforcement agencies into the attack? Would reporting an attack prompt the threat actors to speed up attacks once they learned how successful they were? Would it warn the threat actors that they have been discovered and cause them to cloak other parts of the attack, so they are even more difficult to uncover?

Today it is recognized that the advantages of sharing information outweigh the disadvantages. Organizations are pooling their experiences and knowledge gained about the latest attacks with the broader security community. Making this information

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

available to others can help other organizations repel a widespread attack that they may also be experiencing soon. Sharing this type of information has become an important tool to help everyone shore up their defenses.

Threat intelligence, also known as *cyber threat intelligence (CTI)*, is information gathered from a range of sources about current or potential attacks that is analyzed, refined, and organized to create a defensive strategy to minimize and mitigate cybersecurity risks. TI that is collected from various sources and then disseminated to others is known as **threat intelligence sharing**.

In addition to identifying an imminent attack by sharing indicators of attack (IOA), TI sharing can also aid in other areas such as **incident response** (handling a cyberattack or data breach), **vulnerability management** (identifying and addressing security vulnerabilities), **risk management** (controlling threats to assets), **security engineering** (building systems to resist attacks), and **detection and monitoring** (uncovering and managing vulnerabilities).

Threat Intelligence versus Threat Data

What is the difference between data, information, knowledge, and intelligence? Although these terms are often used synonymously, there is significant variation between them. Table 6-1 provides definitions and an example that illustrates the differences between these terms.

Table 6-1 Differences between data, information, knowledge, and intelligence

Element	Definition	Example
Data	Discrete, objective facts	101, 700, A, 701, B
Information	Organized data that has been processed so it has meaning and value	Course 101-700 is offered in the A-Term
Knowledge	Expert skills and experience applied to information in order to make informed decisions	Enrollment in CIS 101-700 A-Term has increased over CIS 101-701 in the B-Term
Intelligence	Administering knowledge so that it is practical	Multiple sections of CIS 101 should be offered in the A-Term

As Table 6-1 illustrates, there is a difference between "data" and "intelligence." Unfortunately, the terms "threat intelligence" and "threat data" are often erroneously used as synonyms. The difference between them can be illustrated by comparing two different types of weather forecasts.

Consider a weather forecast for an entire nation as a whole. It may indicate that a sweeping cold front is on its way within the next several days resulting in lower temperatures and rain across the country. However, this is of little value when deciding if a coat or umbrella is needed tomorrow. And the cold front could stall out and not even have an effect.

What is also needed is localized weather information for the immediate area. This local forecast can give the current temperature, wind speed, barometric pressure, dew point, precipitation percentages, and so on, which can be used to help create a forecast of weather changes and when to best expect these changes. This local weather data is much more useful when planning what to wear or when to carry an umbrella. This is illustrated in Figure 6-1.

Figure 6-1 Local weather forecast



Vitalex/Shutterstock.com

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The national weather forecast is analogous to cybersecurity threat data. These threat data feeds provide a high-level view of the wide cybersecurity landscape. For example, it is useful to know that a zero-day vulnerability has been uncovered in a specific software package. However, if that software is not used by the organization, then it is of little value. Also, knowing which threat actors and attacks are currently active is useful. But if these threat actors are targeting sectors other than that of the organization, such as targeting schools while the organization is a manufacturing plant, the value of this threat data is again limited.

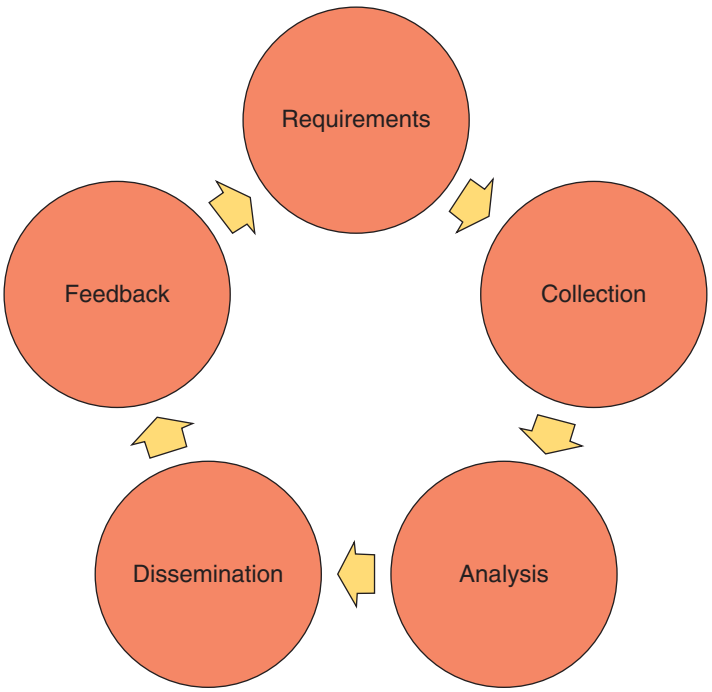
Threat data, while useful like a national weather forecast, lacks the local specificity needed to be helpful. TI, on the other hand, is threat data that has been refined to a localized situation that then produces actionable steps.

The Intelligence Cycle

Cybersecurity threat data comes from a variety of sources: sensors, malware analysis platforms, vendors, and so on. It provides raw data (such as hashes, IP addresses, and malicious URLs) that an organization can then import into their own cybersecurity tools. By using automation technology along with human analysis, an organization can turn threat data into TI and then share it with similar organizations.

The process through which threat data becomes useful TI is illustrated by the intelligence cycle, also called the *threat intelligence life cycle*. Figure 6-2 illustrates the intelligence cycle. This cycle is considered a multistep cyclical process: there is more than one step involved and the process continues to cycle with no endpoint.

Figure 6-2 Intelligence cycle



Caution

A multitude of intelligence cycles relate to cybersecurity, each with any number of steps using different terminology. The intelligence cycle presented here is the core of most intelligence cycles.

The steps of the intelligence cycle are:

- **Requirements.** This involves determining the information assets and business processes that need to be protected, the potential impacts of losing those assets or interrupting those processes, and the priorities in what order to provide protection. This phase helps determine the types of TI needed to

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

protect assets and respond to threats. For example, if a goal is to understand likely threat actors, this could be framed as the question, "Which actors on underground forums are actively soliciting data concerning our organization?"

- **Collection.** Collection is the process of gathering information to address the most important intelligence requirements. There are numerous sources of this threat information. An organization can gather log information and metadata from internal networks and security devices by conducting targeted interviews with knowledgeable security sources, scanning security news and blogs, harvesting information from user forums, scraping attacker data posted on public sites (called "pastes"), and even infiltrating threat actor closed sources. Increasingly, organizations are subscribing to threat data feeds from industry organizations and cybersecurity vendors for TI.
- **Analysis.** The data gathered at the collection stage typically will be a combination of finished information (such as intelligence reports from cybersecurity experts and vendors) along with raw data (like malware signatures or pasted leaked credentials). This data must be processed into a format usable by the organization in the analysis phase. Different collection methods often require different means of processing. For example, an analysis may involve extracting IP addresses from a security vendor's report or extracting indicators from an email before enriching them with other information.
- **Dissemination.** The results of the analysis phase will drive decisions about how this information should be acted on and distributed to where it needs to go (dissemination). Typical decisions involve whether to investigate a potential threat, what actions to take immediately to stop an attack (such as communicating with endpoint protection tools for automated blocking), how to strengthen security controls, or how much investment in additional security resources may be needed. These decisions then drive how the TI is disseminated.

Note 1

Most organizations have multiple security-related teams that need TI. The process of dissemination should be determined in advance by asking the teams how best to provide the information to them. There are several questions that could be asked: What TI do you they need? How can external information support your activities? How should the intelligence be presented to make it easily understandable and actionable for you? How often should we provide updates and other information? Through what media should the intelligence be disseminated?

- **Feedback.** The final phase is feedback regarding how effective the TI was. Feedback can be viewed as answering the basic question "What did we do right and what did we do wrong?" The answers then become input back into the requirements phase to improve the overall intelligence cycle.

Threat Intelligence Sources

There are two broad categories of TI sources. These are open-source and closed-source intelligence.

Open-Source Intelligence

TI that is freely available, called **open-source intelligence (OSINT)**, has become a vital resource. This information is often collected and then disseminated through public information-sharing centers.

Multiple open-source sources provide valuable information to cybersecurity professionals. Some of the most prominent include:

- **Computer Emergency Response Team (CERT).** The Department of Homeland Security, which is responsible for protecting the nation's critical infrastructure from physical and cyber threats, maintains the U.S. **Computer Emergency Readiness Team (CERT)**. By coordinating national defense against and response to cyberattacks, CERT is responsible for analyzing and reducing cyber threats and vulnerabilities by disseminating cyber threat warning information. CERT collaborates with federal agencies, the private sector, the research community, state and local governments, and

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

international entities. It analyzes incidents reported by these entities and coordinates with national security incident response centers who then respond to incidents on both classified and unclassified systems. One of the primary roles of CERT is to distribute "reasoned and actionable cyber security information to the public."

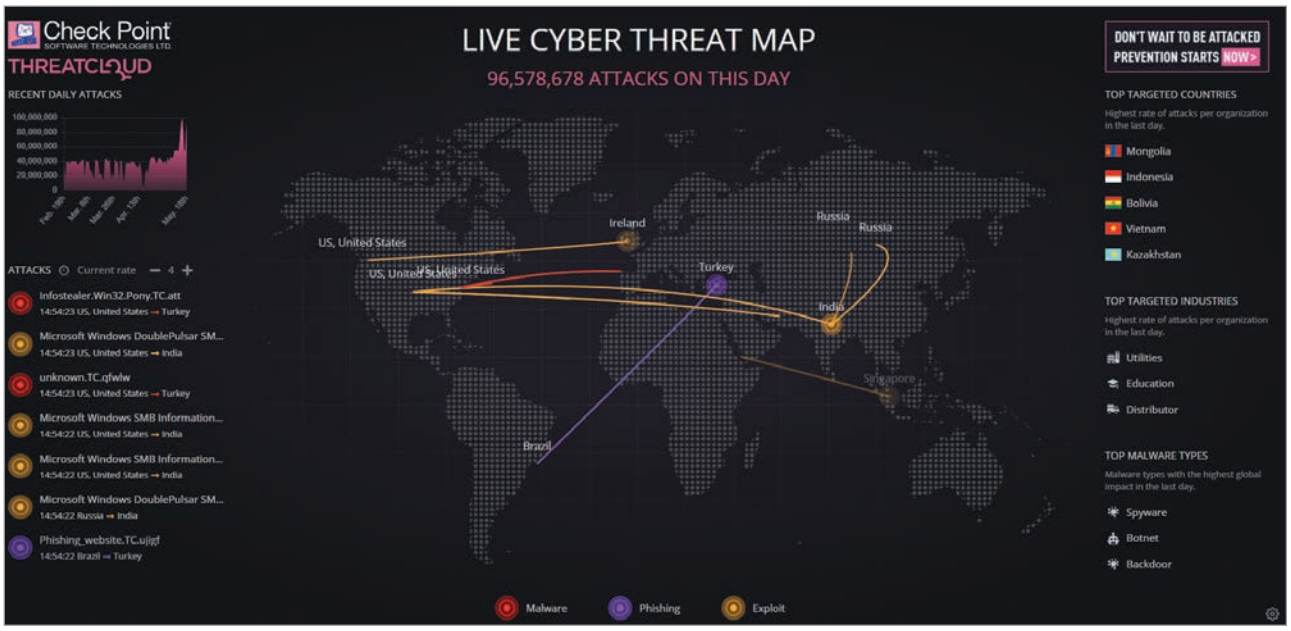
- **Cyber Security Incident Response Team (CSIRT).** The **Cyber Security Incident Response Team (CSIRT)** provides services regarding cybersecurity intelligence to any user, company, government agency, or organization. As a single point of contact for reporting computer security incidents worldwide, CSIRT acts as the clearinghouse that provides the means for reporting incidents and for disseminating important incident-related information. Because organizations share in the responsibility of coordinating their response efforts with similar institutions, CSIRT facilitates gathering intelligence information from all sources and providing it to other similar organizations.

Note 2

CSIRT is a privately held company that began business in 2001.

- **Deep/dark web.** The **deep/dark web**, considered to be part of the world wide web, is the domain of threat actors and is beyond the reach of a normal search engine. Using special software that masks the user's identity allows for malicious activity such as selling drugs and stolen personal information and buying and selling malicious software used for attacks to take place. Some security professionals and organizations use the deep/dark web on a limited basis to look for signs that information critical to that enterprise is being sought out or sold.
- **Threat maps.** A cybersecurity threat map illustrates cyber threats overlaid on a diagrammatic representation of a geographical area. Figure 6-3 illustrates a threat map. Threat maps are promoted as helping to visualize attacks and provide a limited amount of context of the source and the target countries, the attack types, and historical and near real-time data about threats. Although threat maps may look impressive, in reality they provide limited valuable information. Many maps are simply a playback of previous attacks and, because threat maps show anonymized data, it is impossible to know the identity of the attackers or the victims. As a result, many cybersecurity professionals question the true value of threat maps.

Figure 6-3 Threat map



Check Point Software Technologies Ltd.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **File and code repositories.** Another source of TI is file and code repositories. Victims of an attack can upload malicious files and software code that can then be examined by others to learn more about these attacks and craft their defenses. Often samples of recently discovered malware variants are uploaded to malware aggregation repositories along with published detailed malware analysis reports (MARs) containing IOC for each malware variant.
- **Public vulnerability databases.** A vulnerability database is a repository of known vulnerabilities and information as to how they have been exploited. These databases create feeds of the latest cybersecurity incidences that can be downloaded in a variety of different formats (such as comma-separated values [CSV] or JavaScript Object Notation [JSON]) for input into security appliances. Common cybersecurity data feeds include vulnerability feeds that provide information on the latest vulnerabilities and threat feeds that outline current threats and attacks.
- **Other.** There are other open-source methods and sources of relevant information. These include **social media** (websites and applications that enable users to create and share content), **blogs** (posts and comments created by authors and organized into categories), **forums** (topics and comments created by members organized into different subforums), and **government bulletins** (an official publication from the federal government).

Caution

Finding information on the deep/dark web is difficult. First, it requires using Tor or IP2, which prevents a device's IP address from being traced. Second, although there are some deep/dark web search engines, they are unlike regular search engines like Google. The deep/dark web search engines are difficult to use and notoriously inaccurate. One reason is because merchants who buy and sell stolen data or illicit drugs are constantly on the run and their dark websites appear and then suddenly disappear with no warning. Finally, deep/dark websites use a naming structure that results in dark website URLs such as *p6f47s5p3dq3qkd.onion*. All of these are hurdles that keep out anyone who does not understand these inner workings.

One of the challenges of OSINT is that because it comes from a variety of sources, the data may be in a variety of formats. To overcome this challenge, OpenIOC (Open Indicators of Compromise) was developed as an open framework for sharing OSINT in a machine-readable format. The data is formatted in the eXtensible Markup Language (XML) and comes with 500 predefined base indicators, which can easily be customized for adding additional intelligence. An example of an OpenIOC feed is shown in Figure 6-4.

Figure 6-4 OpenIOC example

```
<OpenIOC xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/200
  <metadata>
    <short_description>LAZARUS GROUP CAMPAGN TARGETNG THE CRYPTOCURRENCY VERTICAL</shor
    <description>LAZARUS GROUP CAMPAGN TARGETING THE CRYPTOCURRENCY VERTICAL</descripti
    <keywords/>
    <authored_by>343XCR-Guy OTX</authored_by>
    <authored_date>2020-09-28T18:31:07</authored_date>
    <links>
      <link rel="https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-laza
      <link rel="https://otx.alienvault.com/pulse/5f44efcd13c6da6b9fd3d3f7" href="https
    </links>
  </metadata>
  <criteria>
    <Indicator id="86fd3c88-d4d8-4002-a299-4e46da7a0ccb" operator="OR">
      <IndicatorItem id="1f5c5543-679d-4e66-a658-d88b4199250c" condition="contains" pr
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">googledrive.download</Content>
      </IndicatorItem>
      <IndicatorItem id="ab5a5446-e685-4b51-b301-6d02b2e570c4" condition="contains" pr
        <Context document="DnsEntryItem" search="DnsEntryItem/Host" type="mir"/>
        <Content type="string">antlercap.com</Content>
      </IndicatorItem>
```

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Closed-Source Intelligence

Closed-source intelligence is the opposite of open source. It is proprietary, meaning that it is owned by an entity that has an exclusive right to it. Examples of closed-source intelligence include:

- **Internal sources.** Some TI data can be extracted from an organization's own security devices (**internal sources**), such as a firewall log that captures the external IP addresses of a threat actor attempting a brute force attack on passwords or a spam filter that can identify emails that contain a phishing URL. These IP addresses and URLs can then be fed into the organization's SIEM tool or an IDS to protect against attacks.
- **Paid feeds.** Because they are the result of only the attacks that the organization has witnessed, internal sources are localized TI data that is a small fraction of the total threat landscape. Instead of only relying on their own TI, most organizations pay professional external providers who can provide a broader range of data to reveal patterns and trends. Known as **paid feeds**, these providers not only send this data as electronic feeds for their customer's security appliances, but they also provide in-depth research. Some providers give specialized services for specific market sectors, such as government or financial services.
- **Information-sharing organizations.** There are a large number of organizations that share closed-source information, called **information-sharing organizations**. These include the areas of healthcare, financial services, aviation, government, and critical infrastructure. Organizations that are participants in closed-source information are part of private information-sharing centers that restrict both access to data and participation. Whereas private sharing centers are similar to public sharing centers in that members share TI information, insights, and best practices, private sharing centers are restrictive regarding who may participate. All candidates must go through a vetting process and meet certain criteria.

Confidence Levels

There are concerns surrounding TI gathered from external sources, either open source or closed source. To what degree can this data be trusted? Is it applicable and helpful (**relevancy**)? Is it correct and free from errors (**accuracy**)? Together all these qualities of TI make up the **confidence level** of the information, or how much trust should be placed in it.

In addition to relevancy and accuracy, the timeliness and privacy of shared information are also concerns that impact the confidence level of TI.

Timeliness

It is critical that TI be distributed at the right time, which for cybersecurity is as quickly as possible. Information can be of limited value to block an attack if the attack has already occurred. This is known as the **timeliness** of the TI.

To rely on email alerts that require a human to read them and then react takes far too much time. As an alternative, Automated Indicator Sharing (AIS) can be used instead. AIS enables the exchange of cyber threat indicators between parties through computer-to-computer communication and not email communication. Threat indicators like malicious IP addresses or the sender address of a phishing email can be quickly distributed to enable others to repel these attacks.

Note 3

Those participating in AIS generally are connected to a managed system controlled by the public information-sharing center that allows bidirectional sharing of cyber threat indicators. Not only do participants receive indicators but they can also share indicators they have observed in their own network defenses to the public center, which then distributes them to all participants.

There are two tools that facilitate AIS. Structured Threat Information Expression (STIX) is a language and format used to exchange CTI. All information about a threat can be represented with objects and descriptive relationships. STIX information can be visually represented for a security analyst to view or stored in a lightweight format to be utilized by a computer. Trusted Automated Exchange of Intelligence Information (TAXII) is an application protocol for exchanging CTI over Hypertext Transfer Protocol Secure (HTTPS). TAXII defines an application programming interface (API) and a set of requirements for TAXII clients and servers.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 4

AIS is used more extensively with public information-sharing centers than private centers.

Privacy

A concern about using public information-sharing centers is that of privacy. An organization that is the victim of an attack must be careful that no proprietary or sensitive information is shared when providing TI.

As a safeguard most public information-sharing centers have protections in place to prevent the disclosure of protected information. An example of the safeguards can be seen in the sharing center of the U.S. Department of Homeland Security (DHS) known as the Cyber Information Sharing and Collaboration Program (CISCP). With the DHS serving as the coordinator, the CISCP enables its members (called "partners") to not only share threat and vulnerability information but also take advantage of the DHS's cyber resources. Table 6-2 lists the privacy protections of the CISCP.

Table 6-2 CISCP privacy protections

Protection	Explanation	Example
Cybersecurity Information Sharing Act (CISA)	CISA is a federal law passed in 2015 that provides authority for cybersecurity information sharing between the private sector, state and local governments, and the federal government.	CISA requires a nonfederal entity to remove any information from a cyber threat indicator that it knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.
Freedom of Information Act (FOIA)	FOIA was passed in 1967 and provides the public the right to request access to records from any federal agency.	Although federal agencies are required to disclose any information requested under the FOIA, there are nine exemptions, one of which protects interests such as personal privacy.
Traffic-Light Protocol (TLP)	TLP is a set of designations used to ensure that sensitive information is shared only with the appropriate audience.	TLP uses four colors (red, amber, green, and white) to indicate the expected sharing limitations to be applied by the recipients.
Protected Critical Infrastructure Information (PCII)	The PCII Act of 2002 protects private-sector infrastructure information that is voluntarily shared with the government for the purposes of homeland security.	To qualify for PCII protections, information must be related to the security of the critical infrastructure and is voluntarily submitted and not submitted in place of compliance with a regulatory requirement.

Note 5

The CISCP program is free to join and use. It offers services such as analyst-to-analyst technical exchanges, a portal that can be accessed through which partners can receive analysis of products and threats, cross-industry orchestration in which partners can share lessons learned and share their expertise with peers across common sectors, and digital malware analysis. Those interested must sign an agreement that enables DHS and its partners to exchange anonymized information.

Two Rights & A Wrong

1. The requirements phase of the intelligence cycle sets the "high-level" goals for the TI program.
2. Two tools that facilitate the privacy of TI are STIX and TAXII.
3. Many cybersecurity professionals question the true value of threat maps.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Threat Hunting

Certification

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

Threat hunting has become an important defense for cybersecurity protection. Threat hunting involves understanding what it is, who the hunters are, hunting methodologies, and the steps in the threat-hunting processes.

What Is Threat Hunting?

"Reactive" is defined as responding to an event that has already occurred. It is an action based on something that happened in the past. "Proactive" is taking steps in anticipation of a future event that has not yet occurred. In a reactive mode, problems are solved as they arise, and this can even spark creativity while focusing on a solution. A proactive mode, on the other hand, attempts to address problems before they become an issue; however, being proactive may result in lost time if the event never occurs or has a much smaller impact than anticipated.

While both reactive and proactive actions are necessary, cybersecurity has for many years been considered solely reactive: Following a successful infiltration and attack by the threat actors, steps are taken after the fact to fix the problem. This obviously is too late to prevent damage from occurring.

However, that posture is now changing. Cybersecurity is becoming more proactive than strictly reactive. This can most clearly be seen in **threat hunting**. Threat hunting is an emergent activity that combines a proactive, repetitive (iterative), and predominantly human (instead of exclusively automated) activity. Because threat hunting is not reactive but proactive, it is sometimes called an **active defense** instead of a passive defense.

The goal of threat hunting is the identification of a cyber invasion into a network or endpoints that thus far evaded detection by existing normal security controls. Threat hunting assumes that the network is already infected, and attackers are not just trying to enter from the outside but are currently inside.

Note 6

Threat hunting has been described as "incident response—but without the incident"!

Hunters and Hunting

Understanding the hunters and their hunting can be broken down into four areas. This includes roles, levels, approaches, and focus areas.

Roles

Despite the fact that the roles of the threat hunter and other security personnel may have similarities and sometimes even overlap, they actually are quite different. These differences in roles are listed in Table 6-3 and the comparisons can help to define the work of threat hunters.

Levels

Not all threat hunting occurs at the same level. Table 6-4 lists the levels of "maturity" of threat hunting along with the people, processes, and tools needed.

Note 7

Threat hunting should continue to strive for the highest level and, once there, maintain that level.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 6-3 Security roles

Title	Role	Goal	Task	Driving force	Time frame
Incident responder	Reactive	Secure environment after alarm has been raised	Minimize impact of attack on the organization through formal process	Business continuity	Immediate
Penetration tester	Proactive	Secure environment through controlled offensive exercises	Mimic actions of threat actors to test and validate security posture	Uncover vulnerabilities	Soon
Threat hunter	Proactive	Identify suspicious activity before alarm has been raised	Seek evidence of malicious behavior	Prevent infection from spreading	Longer

Table 6-4 Levels of threat hunting

Threat-hunting level	People	Processes	Tools
Initial (Level 1)	Existing security operations center (SOC) personnel	Ad-hoc hunts with little data collected	Standard SOC reactive tools with little automation
Managed (Level 2)	Threat hunting performed by volunteer	Uses basic threat feeds with IOC; hunts only occasionally	Searching for text strings and automatic matching of IOCs
Defined (Level 3)	Dedicated threat hunter	Formal hunting process that occurs regularly with data collection from key areas	Use of statistical analysis techniques
Quantitatively Managed (Level 4)	SOC analysts rotated into threat-hunting team	Hunts occur frequently with moderate data collection	Use of dashboards and visualization tools
Optimized (Level 5)	Threat-hunting teams integrated across a SOC with proper resources integration into process	Hunts occur continuously and data shared across security community	Takes advantage of machine learning

Approaches

There are three common approaches to threat hunting:

- **Structured hunting.** Structured hunting involves the systematic search for specific threats based on predefined criteria or TI. This approach typically starts with a well-defined question about a potential threat, such as, "Are there any signs of a specific malware strain within our network?" or "Is there any evidence of unauthorized access to our sensitive data?" Threat hunters use TI and other sources to search for patterns of activity or behavior anomalies that may indicate the presence of a threat. This process may involve the use of automated tools and queries, along with manual analysis and correlation of data.
- **Unstructured hunting.** Unstructured hunting, also known as exploratory hunting, is an open-ended approach to threat hunting that does not strictly rely on TI. Instead, threat hunters use their expertise and intuition to search for potential threats or vulnerabilities. This approach involves the use of a range of data sources, such as TI, network logs, endpoint data, and other techniques and tools that search to identify patterns, anomalies, or other IOA. Unstructured hunting is particularly useful for identifying unknown or emerging threats because threat hunters think "outside the box" and search for signs of malicious activity that may not fit traditional IOA.
- **Situational hunting.** Situational hunting is a targeted approach that focuses on specific events or situations that pose a heightened risk to an organization. Examples of events include high-profile mergers

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

and acquisitions, product launches, or company expansions, as well as specific targets of high-value assets like the laptops of "C-suite executives" or third-party vendors and their service accounts that can access the network. Situational hunting often involves the use of both structured and unstructured hunting techniques.

Note 8

Some threat-hunting teams partner with their own human resources organization to track new hires and departing employees, as both are potential targets for threat actors.

Focus Areas

Where should threat hunters be looking? Are there areas of the corporate network that are the most tempting to threat actors? Are there high-value assets that attackers crave? There are several particular spaces and targets in which threat hunters may center their attention (**focus areas**) when conducting threat hunting. These include:

- **Isolated networks.** Networks that are used for supporting testing and other nonproduction functions, called **isolated networks**, are areas in which threat actors may lurk. Because these networks are not used to the same extent as regular production networks, they can be overlooked. Threat hunters should examine these networks as evidence of penetration.
- **Configurations/misconfigurations.** Many penetrations by threat actors into corporate networks come as a result of an incorrect or "suboptimal" setting applied to hardware or software **(configurations/misconfigurations)**. These are areas in which a threat hunter should focus their attention.
- **Business-critical assets.** Because not all assets have the same value, threat hunting should focus on those assets that are essential to the operation of the organization (**business-critical assets**). A failure of a business-critical asset can negatively impact the ability to generate revenue or reach an organization's goals.

Threat-Hunting Methodologies

There are four generally recognized threat-hunting methodologies. These are intelligence hunting, assumption hunting, IOA hunting, and hybrid hunting.

Intelligence Hunting

Intelligence-based threat hunting is an active threat-hunting technique designed to react according to input primarily derived from threat data feeds and TI, including IP addresses, hash values, and domain names. Another source of intelligence is data provided by CERTs and CISRT. Intelligence hunting can be integrated with a SIEM tool and other TI tools, which use the intelligence to hunt for threats. Intelligence can often input the information into a SIEM system using TAXII and STIX.

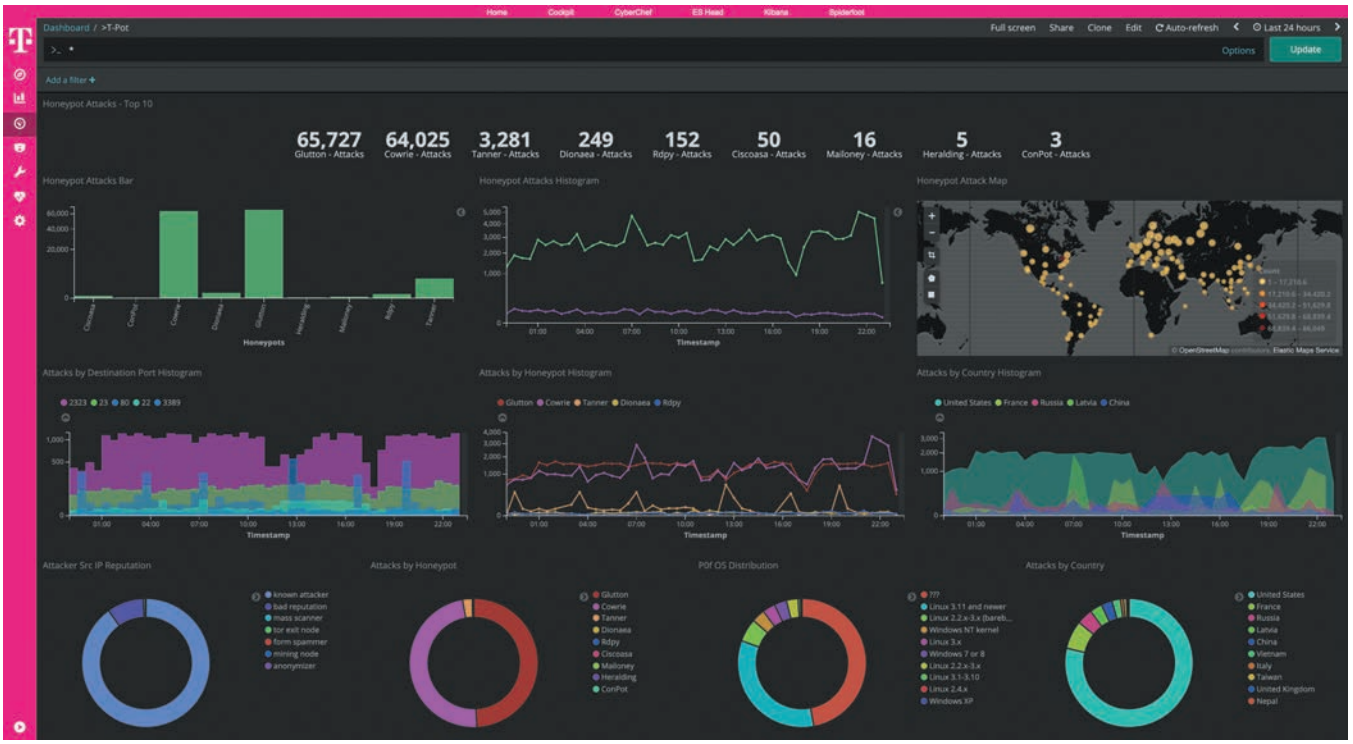
One particularly valuable source of intelligence can come from a technology "lure" that serves as bait to attract threat actors. A **honeypot** lure is a computer located in an area with low security that serves as bait to threat actors because it is intentionally configured with security vulnerabilities, making it open to attacks. A honeypot can trick threat actors into revealing their attack techniques and, once discovered, can then be used as a source of intelligence. Figure 6-5 shows the results from a honeypot dashboard that lists attacker probes by time and country.

Note 9

The number of attempts against a honeypot is staggering. In one study, 10 honeypots around the world were created that simulated the Secure Shell (SSH) service. One of the honeypots started receiving login attempts just *52 seconds* after it went online. Once all 10 of the honeypots were discovered, a login attempt was made about every *15 seconds on each one*. At the end of one month, over 5 million attacks had been attempted on these honeypots.[2]

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 6-5 Honeypot dashboard



Source: Honeypot

Assumption Hunting

Assumption threat hunting involves creating and then testing different types of assumptions (conjectures or suppositions) regarding a threat. Whereas intelligence hunting is based quantifiable data, assumption hunting is more of a speculation. However, the assumptions are not wild guesses but do have a foundation. These foundations can be:

- **Intelligence based.** Driven by malware analysis, vulnerability scans, Internet-discovered exploits, and intelligence reports and feeds, intelligence-based hunting uses this information as a starting point but is then augmented by assumptions.
- **Situation based.** Situational-based hunting looks at specific events or situations that pose a heightened risk to an organization.
- **Analytics based.** Analytics-based hunting makes use of advanced data techniques and user and entity behavior analytics (UEBA) to develop aggregated risk scores that then can be used to formulate speculations.

IOA Hunting

The most proactive threat-hunting technique is investigation using IOA. After identifying a behavior, the threat hunter attempts to locate patterns by searching log repositories for matching hashes or events and monitoring ongoing activities. The goal is locating, identifying, and then isolating the threat to prevent its spread or proliferation.

Hybrid Hunting

The hybrid threat-hunting technique combines all of the above methods: intelligence hunting, assumption hunting, and IOA hunting. It usually incorporates industry-based hunting with situational awareness, combined with specified hunting requirements. This hybrid hunting approach allows security analysts to highly customize the hunt.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Steps in Threat Hunting

There are three broad categories of steps in threat hunting, particularly as they relate to IOCs. These steps are gathering the IOC and related data from different sources (**collection**), scrutinizing them for evidence (**analysis**), and then using them to generate a hypothesis (**application**). More specifically, the steps in threat hunting are:

- **Select the attack model.** It is important for an organization to decide how it envisions the process that the threat actors use in order to compromise their assets. This helps define the philosophy of how threat hunting will occur and identify who the threat actors are and how they function (called *profiling threat actors and activities*). It is important for an organization to select an attack model and use that as a foundation for their threat hunting.
- **Identify the most concerning threats.** Not all potential threats are of the same importance. There are a variety of factors that should be considered when identifying the threats that are of the highest level of concern. Depending on the threat model chosen, this step involves going through each of the phases in the model to identify the attacker activities that are most concerning.
- **Create a calendar.** The next step is to create a calendar of how frequently to hunt for specific threats. Those activities that are found near the end of the chosen threat model are those of the highest importance because these are the activities that the attacker is about to implement to achieve their desired result, and thus they need to be identified and stopped immediately. The various activities can be organized as having a low impact, medium impact, or high impact. High-impact activities should be hunted more frequently than those with a lower impact.
- **Generate a hypothesis.** A hypothesis is a tentative assumption that is made and will then be tested to determine if it is valid. Threat hunting begins with a threat hunter asking basic questions, such as "How would a threat actor infiltrate our network?" For example, a hypothesis of looking for an instance of ransomware may be, "We hypothesize that if our network is infected with WannaCry ransomware, we will see an increase in the rate of file renaming."
- **Investigate the hypothesis.** Once the hypothesis is developed, the threat hunter "follows up" on it by investigating through different tools and techniques.
- **Act on results.** Now that the hypothesis has been examined, it will be found to be either true or false. If the hypothesis is found to be false—for example, there is not an increase in the rate of file renaming—it may be concluded that the ransomware has not infected the system. However, this is not an indication of failure; rather, it simply means that there is no indication of an infiltration based on the specifics of the hypothesis. There could be evidence elsewhere that must be uncovered. What happens if a hypothesis is proven correct? First, this information should be turned over to the SOC so that the infiltration can be "rooted out" and more secure defensive barriers erected. Second, when possible, successful hunts should be automated to maximize the efficient use of the threat-hunting team's time. This can also limit the need to continuously repeat the same hunts.

Two Rights & A Wrong

1. Threat hunting assumes that the network is already infected, and attackers are not trying to enter from the outside but are currently inside.
2. The Optimized level of threat hunting is performed by volunteers.
3. Unstructured hunting, also known as exploratory hunting, is an open-ended approach to threat hunting that does not rely on TI.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Improving Security Operation Processes

Certification

1.5 Explain the importance of efficiency and process improvement in security operations.

Due to the importance of security operations in an organization, it is vital that these operations be continually monitored for efficiency. Are the operations effective? Are they productive? Do they give a good return on investment? Do they meet all required regulations? Do they really make the business more secure?

Improving security operations involves standardizing processes and streamlining operations. It also involves using appropriate tools and integration.

Standardize Processes

In the late 19th century, engineer Frederick Taylor began to analyze how factory workers did their jobs. His goal was to identify which movements could be standardized. In 1911, he published the book *The Principles of Scientific Management* that called for a system of "work rationalization" that could increase productivity by ensuring that the same steps were performed in the same way. This concept, known as Taylorism, was incorporated by Henry Ford when he created his assembly lines for building cars.

Today, organizations **standardize processes** by documenting and formalizing the steps and activities involved in a task or procedure. Often called "process standardization," its goal is to create a consistent and repeatable method for completing a task or achieving a specific outcome.

Note 10

Process standardization can be applied to virtually any process, task, or procedure that is conducted in an organization. It begins with identifying the different ways a problem is solved across an organization, working out a unified solution, and then implementing that single solution.

There are several advantages to process standardization:

- **Avoid variations in processes.** Because the steps of processes belong to the entire organization and not just to the whim of one or two employees, standardizing workflows ensures that activities are always performed the same way. This helps to mitigate inconsistencies, variations in the quality of work, and unexpected changes in general.
- **Highlight processes.** Process standardization can help an organization to know and better understand the work that it performs and provide a more accurate idea of what results should be achieved.
- **Identify responsibilities.** A lack of process standardization leads to uncertainties regarding who is responsible for which task. Standardization ensures that all processes have a process "owner" who can optimize deliveries and provide control.
- **Improve results.** Clear processes ensure that the optimum skills are applied to each task, improving overall results.
- **Meet regulatory requirements.** Organizations must meet the needs of regulatory requirements of their operating market and process standardization helps document that these are being met.
- **Reduce costs.** When efficiency is improved in all stages in a process, then cost reduction will invariably follow as resource optimization makes it easier to produce more at a lower cost.

Process standardization is an important element in improving the efficiency of security operations. As all security personnel "follow the same playbook," it creates an environment in which a higher level of protection and quicker reaction to events can be accomplished. Standardizing processes should be applied to manual processes as well as automated processes.

Cybersecurity process standardization for automation begins with the discovery of recurring manual activities that lend themselves to being replaced or supplemented by an automated process (**identification of tasks suitable for automation**).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The manual activities that are considered most suitable have two characteristics: they occur on a repetitive basis and can be performed independently of security personnel (**repeatable/do not require human interaction**). When identifying these independent and repeatable tasks suitable for automation, it is important to involve all security personnel who may have played a role—albeit even a small role—in the manual process (**team coordination to manage and facilitate automation**). This helps achieve the broadest range of valuable input.

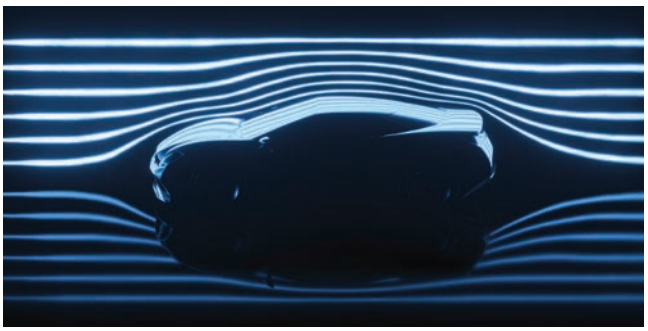
Note 11

"Engage everyone" is a common principle of process standardization. Building an all-inclusive team to manage and facilitate the automation workforce is the most effective approach so that the organization's goals, new development strategies, and other process standardization changes can be taken into account and updated to all the stakeholders.

Streamline Operations

The word *streamline* comes from the world of aerodynamic engineering. It means to design a shape that minimizes resistance against a flow like air or water. Reducing this "drag" (something that slows down) against the shape helps to increase speed and ease of movement. "People movers" like airplanes, trains, boats, and automobiles are particularly sensitive to this resistance of air and water, and extensive testing is performed to develop the optimum streamline shape to "slip" through the environment, as illustrated in Figure 6-6.

Figure 6-6 Testing to streamline shape



Ktsdesign/Shutterstock.com

Note 12

The aerodynamic efficiency of a car is measured by its coefficient of drag multiplied by its frontal area, known as its CdA. This takes into account both its shape and size. In order to reduce drag, most cars today have a low sloping hood, flush headlights, recessed wipers, and imbedded door handles.

In cybersecurity there is also a "drag" that slows down cybersecurity defenders: the lack of automation that forces a reliance on human involvement. Although security devices themselves are obviously automated, the work done by security personnel has been highly manual. Security personnel have been forced to work manually to search for evidence of attacks, uncover the techniques used by the malware, and then configure devices for protection.

It is important to streamline cybersecurity operations from the drag of a lack of automation. This involves minimizing human engagement by using automation and orchestration.

Minimize Human Engagement

In recent years, a shift has occurred in which more automation is becoming available to cybersecurity personnel. Instead of relying on human power to battle attacks, automation is providing significant advancements. The goal of this cybersecurity automation is to reduce the work required of personnel to fight attacks (**minimize human engagement**). By stopping more threats and compensating for a lack of personnel, automation helps to streamline security processes and make them more efficient. Some of the benefits of using cybersecurity automation are summarized in Table 6-5.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 6-5 Cybersecurity automation benefits

Benefit	Description
Furnish an agile incident response	By using automated rapid detection and incident response, cybersecurity automation can help predict and handle incidents and be "nimbler" as threats continue to morph.
Minimize attack severity	Automation can block threats early in their progression and limit their spread.
Enable smarter resource allocation	Because organizations often struggle with adequate resources, especially qualified security personnel, cybersecurity automation can reduce overburdening employees with cumbersome manual tasks and allocate resources more effectively.
Provide scalable solutions	An important benefit of automation is the controls that can be readily scaled as needed to handle different security requirements.
Reduce alerts	Cybersecurity automation can filter out false positives while correctly categorizing true alerts, which helps keep personnel from being distracted and enables them to focus on actual risks.

Note 13

Using cybersecurity automation is called a "force multiplier," which is one or more factors that allows a group to be more effective than they would be without those factors.

Embrace Cybersecurity Automation

Cybersecurity defenders who operate in an organization's SOC, which is responsible for detecting, analyzing, and responding to cybersecurity incidents, typically use manual processes augmented with automated processes. However, using manual processes—*any* manual processes—tips the balance of the scale over to the threat actors. Modern cyberattacks are highly automated. Any organization that is forced to try to defend against these attacks manually will spend precious time looking for evidence of an attack and how to counteract it while the attack spreads at lightning speed. This results in a losing fight between "man versus machine."

The solution is to "fight fire with fire" or, in this case, fight attack automation with defense automation. Known as cybersecurity automation, it uses automated processes instead of manual processes to better predict behaviors and execute protections much faster. If implemented appropriately and with the right tools, automation can aid in the prevention of successful cyberattacks. Cybersecurity automation levels the playing field, reduces the volume of threats, and allows for faster prevention of zero-day attacks of new and previously unknown threats.

Two examples of cybersecurity automation are data correlation and software development.

Data Correlation An example of the necessity of cybersecurity automation is seen in correlating threat data from various sources. Organizations need to collect global TI outside of their infrastructure across all attack vectors and from security technologies within their own network. Finding the linkages (correlations) from these multiple data sources can result in more accurate results and reduces the likelihood of false positives. And this data correlation analysis must also have the ability to scale (increase) to meet ever-increasing threats (and ever-increasing data).

Although SOCs collect voluminous amounts of this threat data, it is of limited value unless it is organized into actionable next steps. Yet it is virtually impossible to perform the necessary correlations manually. However, by applying cybersecurity automation to processes like data correlation it can provide the needed insights in a timely fashion.

Software Development Software development has long been considered a highly manual process. As such, it has always been ripe for the introduction of security vulnerabilities due to human errors. However, implementing an automated process can not only produce code more quickly but the code itself will be more secure. Table 6-6 lists the basic processes found in enhancing software development by automation.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

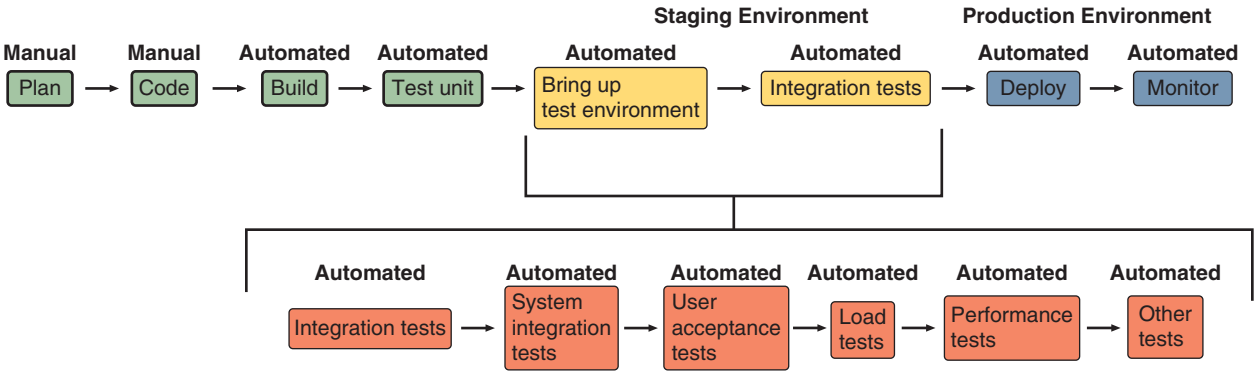
Table 6-6 Automated software development processes

Process name	Description	Advantage	Explanation
Continuous integration (CI)	Developers merge their changes back to the main branch of code as often as possible, even several times each day.	Changes are validated by creating a build and running automated tests against it so that any problems can easily be identified as coming from a smaller segment of code.	Continuously integrating different changes from different developers prevents surprises on release day at the end of the project when all changes are merged into the release branch.
Continuous delivery (CD or CDE)	Developers automatically deploy all code changes to a testing and/or production environment after the source code has been compiled (build stage).	An extension of CI, it allows application deployment more quickly and easily while making troubleshooting easier as small batches of code are released.	Software can be released daily or weekly based on business requirements.
Continuous deployment (CD)	Every change that passes all stages of the production pipeline is immediately released to customers.	No human intervention is needed and only a failed test will prevent a new change to be deployed to production.	An excellent way to accelerate the feedback loop with customers and take pressure off developers because there is not a single release day.

Using automation for software development is one of the cornerstones of a specific type of software methodology that heavily incorporates secure coding practices and techniques to create secure software applications and is called *SecDevOps*. SecDevOps (also known as *DevSecOps* and *DevOpsSec*) is the process of integrating secure development best practices and methodologies into application software development and deployment processes. It is a set of best practices designed to help organizations implant secure coding deep in the heart of their applications.

Figure 6-7 illustrates continuous integration, continuous deployment, and continuous development.

Figure 6-7 Continuous integration, continuous deployment, and continuous development



Apply Orchestration

Cybersecurity **orchestration** involves the automation and combination of many different individual tasks and processes. In contrast to cybersecurity automation, which only automates one task, workflow orchestration involves organizing many tasks into a functional process or workflow that is highly automated. The purpose of workflow orchestration is to streamline and optimize repeatable processes and ensure the correct execution of tasks. Whenever a process becomes repeatable and its tasks have the capability of being automated, workflow orchestration can be used to optimize the process and eliminate redundancies, speed up completion time, and reduce errors. Cybersecurity orchestration can be seen in orchestration appliances as well as in analyzing threat feeds.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Orchestration Appliances Workflow orchestration has given rise to a new type of cybersecurity platform known as a security orchestration, automation, and response (SOAR) platform. SOAR is a combination of software programs and tools that allow organizations to synthesize and automate a range of security operations, TI, and incident response in a single platform.

Consider a threat actor who is attempting to use a brute-force attack against a login prompt. Normally this would result in a human security administrator receiving an alert. The administrator would then have to open the firewall app and manually block the IP address of the attacker. However, when using a SOAR platform, it can automatically and immediately block the IP address of a computer that is attempting to brute-force a login.

Analyzing Threat Feeds Most organizations monitor their networking environment to determine what normally occurs, and this data is then used to create a database of key risk indicators (KRIs), which is a metric of the upper and lower bounds of specific indicators of normal network activity. These indicators may include the total network logs per second, the number of failed remote logins, network bandwidth, and outbound email traffic. Once a KRI exceeds its normal bounds this could be (but not always) evidence of an IOA. This information aids in discovering an attack before it occurs.

As vital as these threat feeds are, however, it is critical that cybersecurity automation be used to analyze them. There are two technologies with corresponding tools that can enhance threat feeds by cybersecurity automation. These are data enrichment and threat feed combination.

Data Enrichment As its name implies, **data enrichment** is the enhancement of data for cybersecurity analysis. This enhancement is both broad as well as deep. Expanding data sources from a single organization and then combining that with similar data from other organizations (breadth) as well as providing contextual data (depth) is the formal definition of data enrichment.

Consider a single organization that gathers information from its security appliances. Although valuable, it still only reflects one organization and information from one type of security device. However, if this were expanded to include other sources from that organization, such as log data from network routers and proxy servers or endpoint devices, the visibility from a broader amount of data would help significantly to identify attacks. And if all the information from security appliances and log data were then combined with that same type of data from other organizations, it would provide an even clearer picture by providing a broad scope of the data.

In addition to being broader, data can also be deeper. This involves appending or otherwise enhancing collected data with relevant context obtained from additional sources. For example, if a username is found within an application log that is associated with a potential security event, that information may be of some value. However, if that username can be referenced against a central identity and access management (IAM) system to obtain the user's actual name, departmental roles, privileges, and so on, this additional information enriches the original log data with context.

As another example, if an IP address can be added to enrich a firewall log file, it could then be used to reference IP reputation servers for external addresses to see if there is a known threat activity associated with that IP address. And "drilling down" even further, that IP address could be referenced with geolocation services to determine the physical location of the IP address by country, state, or postal code.

Adding context data can occur in one of two ways. The first method is by performing a lookup at the time of collection and then appending the contextual information into the log data. Another method is to perform a lookup later at the time the event is analyzed. Appending the data at the time of collection prevents errors that may occur as the network environment changes (for example, if IP addresses are provided via the Dynamic Host Configuration Protocol [DHCP], the IP associated with a specific log could be different at the time of collection than at the time of analysis). However, this significantly increases the amount of stored information.

Threat Feed Combination **Threat feed combination** is an enhancement upon data enrichment. It adds third-party threat feeds for the broadest possible picture of both breadth and depth. This can significantly refine the data used by cybersecurity automation.

Tool Automation and Integration

There are several tools that are used to automate cybersecurity for efficiency and process improvement. The tools include application programming interfaces, webhooks, and plugins. Tools can also facilitate integration such as a single pane of glass.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Application Programming Interface (API)

Uber, Airbnb, Instagram, and WhatsApp exemplify the modern business environment. These tech corporations are forerunners of the sharing economy and digital disruption, with valuations exceeding $1 billion. They are seen as being more agile and able to adapt faster and adjust better to changing market conditions than large enterprises. In fact, they are often held up as models for today's business environment.

One driving factor that helped these companies succeed was how they created their customer and internal platforms. Instead of writing all software code from scratch, they relied heavily on **application programming interfaces (APIs)**. An API is a link provided by an operating system, web browser, or other platform that allows a developer access to resources at a high level. An example of an API is when a user visits a website and the message "This site wants to know your location" appears. The website is attempting to the use geolocation API available in the web browser. APIs relieve the developer from the need to write code for specific hardware and software. Because APIs provide direct access to data and an entry point to an application's functions, they can be used to create code much more rapidly.

Note 14

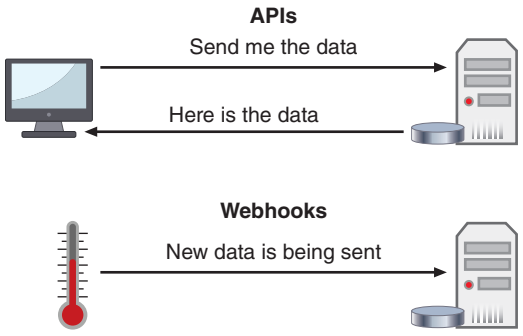
This use of APIs has led to a technology called API integration or integration platform as a service (iPaaS). This is a set of automated tools for connecting software applications that are deployed in different environments. API integration is used to integrate on-premises applications and data with cloud applications and data. It provides pre-built connectors and business technologies that ease the development of integration flows and API management. It also offers custom development kits for linking legacy applications with mobile and social applications.

Webhooks

There are two key features of APIs. First, they must be "asked" or invoked to pull (gather) or modify data. Second, communication is two-way: Application A requests information from Application B, and then Application B sends the information back to Application A.

A **webhook** is a type of event-driven API. Instead of sending information in response to another app's request, a webhook sends information or performs a specific function in response to a "trigger" (such as clicking a button, receiving a form submission, or a temperature reaching a critical level). Webhooks enable lightweight data sharing between software when a specific action takes place. Since the application sending the data initiates the transfer, webhooks are often called "reverse APIs." The difference between an API and a webhook is illustrated in Figure 6-8.

Figure 6-8 APIs compared to webhooks



Note 15

Generally, if a notification or update information needs to be sent as soon as a certain criterion is met, a webhook is preferable. If that data fluctuates or there is a need to modify data rather than push a notification, then an API is the preferred architecture.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Webhooks can be used in a variety of ways for enhancing cybersecurity automation. For example, a monitoring system using webhooks can alert security personnel when there has been a security breach, so that they can react quickly to address the breach and limit the amount of data loss or harm. Webhooks can also be used for an application to receive automatic notifications about a security event occurring in another application.

However, it is critical to properly secure webhooks so that they do not themselves become victims of an attack. Each of the three independent webhook components—the generating or broadcasting system, the listening function, and the communications channel between them—must all be protected. Without good security controls, threat actors could explore webhooks for malicious activities such as sending fake events to taint a system, obtain confidential information, or corrupt data. Many webhook providers provide capabilities to verify the sender, validate the data sent, and mitigate specific attacks.

Plugins

Several tools can be used for running a vulnerability scan. One of the best-known and most widely used vulnerability scanners is Nessus. It is a product of Tenable and contains a wide array of prebuilt templates. However, with the number of new attacks released daily, how can Tenable keep Nessus updated to scan for the latest attack?

Nessus, along with many vulnerability scan products, are modular in nature instead of a single enormous software package. This allows for updates to be made available automatically to enhance its functionality or provide stronger security. A module update, known as a **plugin**, can be downloaded and installed to scan for the latest vulnerability.

Caution

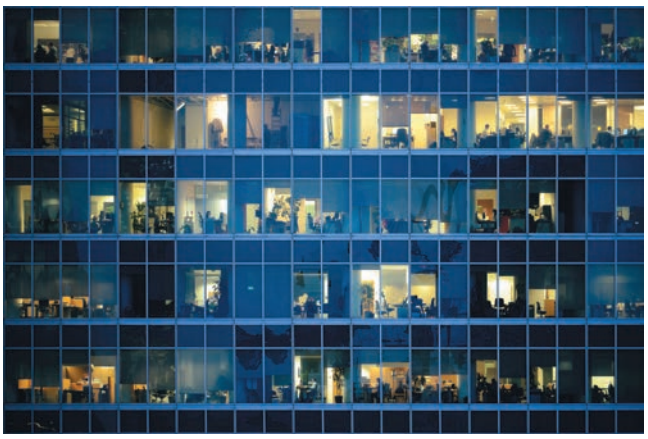
Plugins have long been associated with web browsers. Browser plugins are essentially a small piece of software code that performs a function or adds a feature to a browser to support dynamic actions, such as playing music, viewing videos, or displaying special graphical images within the browser that normally it could not play or display. However, because a plugin lives outside of the "space" that a browser uses on the computer for processing and serves as the link to external programs that are independent of the browser, almost all major web browsers have dropped support for automatic plugins due to their security risks.

Tenable writes its plugins using the Nessus proprietary scripting language called Nessus Attack Scripting Language (NASL). The plugins contain vulnerability information, remediation recommendations, and actions. And because plugins can be associated with the Common Vulnerability Scoring System (CVSS), they can also help calculate the determining risk factors. Once a vulnerability becomes public, Nessus begins creating a new plugin to identify this vulnerability. Nessus advertises that a plugin is available as soon as 24 hours after a new vulnerability is disclosed.

Single Pane of Glass

Suppose you were looking at an office building with glass windows as seen in Figure 6-9. Imagine how difficult it would be to keep track of everything that is occurring in each of the offices behind each window.

Figure 6-9 Office building windows



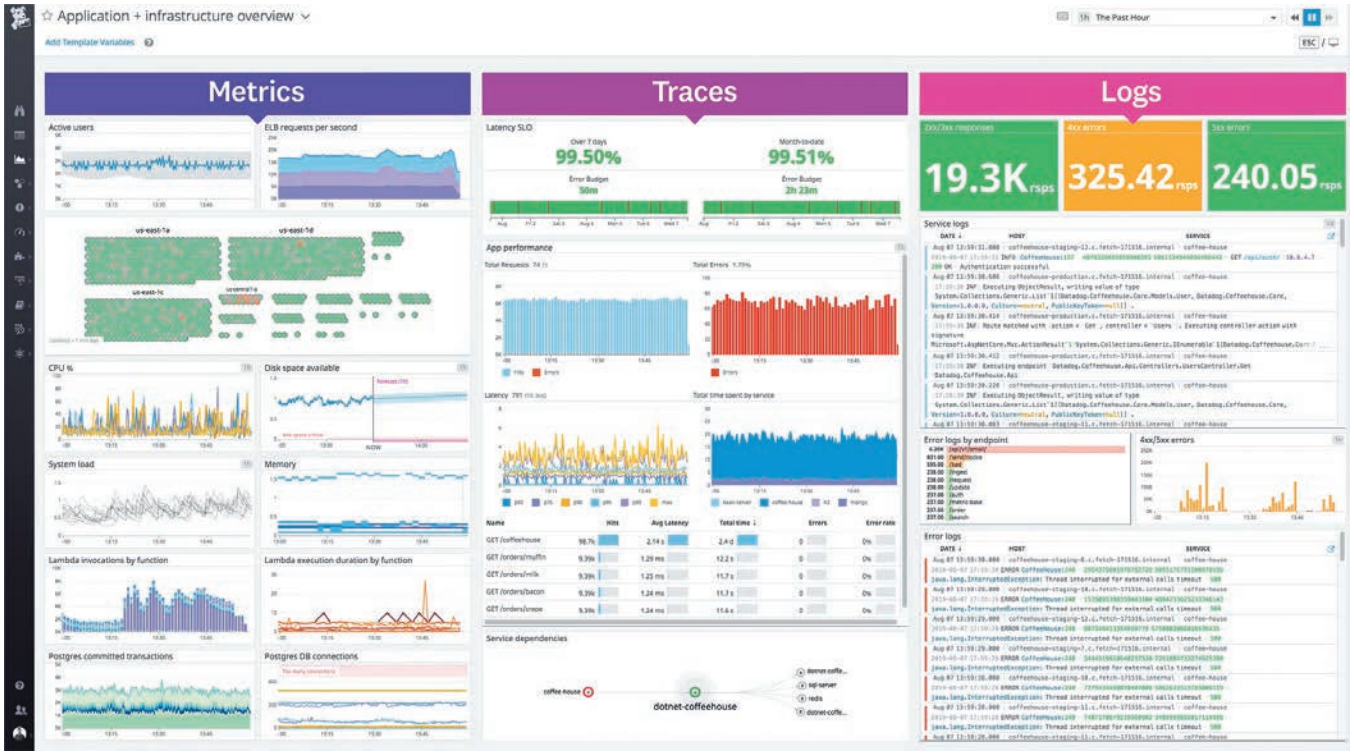
Locomotive74/Shutterstock.com

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The same holds true for cybersecurity. Inputs are constantly arriving from a multitude of security devices and sensors from across the network and from remote locations. Trying to keep up with all the various inputs and take necessary actions is virtually impossible.

Fortunately, today the various inputs can be consolidated into a single management console that presents data from multiple sources in a unified display. This is known as a **single pane of glass**, sometimes simply called a *dashboard*. The single pane of glass is the starting point from which security personnel can see the "big picture" in a way that is easy to read and interpret. These displays can also be customized to meet specific needs. A single pane of glass is seen in Figure 6-10.

Figure 6-10 Single pane of glass display



Source: Datadog

Two Rights & A Wrong

1. An advantage of standardizing processes is that it highlights processes.
2. Orchestration involves the automation and combination of many different individual tasks and processes.
3. Workflow orchestration has given rise to a new type of cybersecurity platform known as a SIEM.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Summary

- The advantages of sharing information outweigh the disadvantages. Organizations are pooling their experiences and knowledge gained about the latest attacks with the broader security community. Threat intelligence (TI) is information gathered from a range of sources about current or potential attacks that is analyzed, refined, and organized to create a defensive strategy to minimize and mitigate cybersecurity risks. TI that is collected from various sources and then disseminated to others is known as TI sharing. In addition to identifying an imminent attack by sharing indicators of attack, TI sharing can also aid in other areas such as incident response, vulnerability management, risk management, security engineering, and detection and monitoring.
- Threat data feeds provide a high-level view of the wide cybersecurity landscape, while TI has been refined to a localized situation that then produces actionable steps. The process through which threat data becomes useful TI is illustrated by the intelligence cycle, also called the TI life cycle. This cycle is considered a multistep cyclical process because there is more than one step involved and the process continues to cycle with no endpoint. The steps of the intelligence cycle are requirements, collection, analysis, dissemination, and feedback.
- There are two broad categories of TI sources. TI that is freely available, called open-source intelligence (OSINT), has become a vital resource. This information is often collected and then disseminated through public information-sharing centers. Multiple open-source sources provide valuable information to cybersecurity professionals. Some of the most prominent include information from the Computer Emergency Readiness Team (CERT) and the Cyber Security Incident Response Team (CSIRT), the deep/dark web, threat maps, file and code repositories, public vulnerability databases, social media, blogs, forums, and government bulletins. Closed-source intelligence sources include internal sources, paid feeds, and information-sharing organizations. There are concerns surrounding TI gathered from external sources, whether they are open source or closed source. These make up the confidence level of the information, or how much trust should be placed in it.
- Threat hunting is an emergent activity that combines a proactive, repetitive (iterative), and predominantly human (instead of exclusively automated) activity. Because threat hunting is not reactive but proactive, it is sometimes called an active defense instead of a passive defense. The goal of threat hunting is the identification of a cyber invasion into a network or endpoints that thus far evaded detection by existing normal security controls. Threat hunting assumes that the network is already infected, and attackers are not just trying to enter from the outside but are currently inside. Despite the fact that the roles of the threat hunter and the other security personnel may have similarities and sometimes even overlap, they actually are different.
- Not all threat hunting occurs at the same level. There are three common approaches to threat hunting: structured hunting, unstructured hunting, and situational hunting. There are several particular spaces and targets in which threat hunters may center their attention, called a focus area, when conducting threat hunting. There are four generally recognized threat-hunting methodologies. These are intelligence hunting, assumption hunting, IOA hunting, and hybrid hunting. There are three broad categories of steps in threat hunting, particularly as they relate to IOCs. These steps are gathering the IOC and related data from different sources (collection), scrutinizing them for evidence (analysis), and then using them to generate a hypothesis (application).
- Due to the importance of security operations in an organization, it is vital that these operations be continually monitored for efficiency. Organizations standardize processes by documenting and formalizing the steps and activities involved in a task or procedure. The goal of process standardization is to create a consistent and repeatable method for completing a task or achieving a specific outcome. Cybersecurity process standardization for automation begins with the discovery of recurring manual activities that can be replaced or supplemented by an automated process. The manual activities that are considered most suitable have two characteristics: they occur on a repetitive basis and can be performed independently of security personnel. When identifying tasks suitable for automation it is important to involve all security personnel who may have played a role in the manual process.
- Although security devices themselves are automated, the work done by security personnel has been highly manual. Security personnel have been forced to

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

work manually to search for evidence of attacks, uncover the techniques used by the malware, and then configure devices for protection. In recent years, a shift has occurred in which more automation is becoming available to cybersecurity personnel. Two examples of cybersecurity automation are data correlation and software development.

- Orchestration involves the automation and combination of many different individual tasks and processes. While cybersecurity automation only automates one task, orchestration involves organizing many tasks into a functional process (workflow) that is automated. The tasks that make up workflow orchestration are large and complex scenarios, and these tasks often involve multiple platforms. The automated coordination involves hardware, software, middleware, and services and uses multiple automated and even semi-automated tasks to automatically execute a complex process or workflow. Workflow orchestration has given rise to a new type of cybersecurity platform known as a security orchestration, automation, and response (SOAR) platform. SOAR is a combination of software programs and tools that allow organizations to synthesize and automate a range of security operations, TI, and incident response in a single platform.
- There are two technology corresponding tools that can enhance threat feeds by cybersecurity automation. Data enrichment is the enhancement of data for cybersecurity analysis. This enhancement is both broad as well as deep. Expanding data sources from a single organization and then combining that with similar data from other organizations (breadth) as well as providing contextual data (depth) produces data enrichment. Threat feed combination is an enhancement upon data enrichment by adding third-party threat feeds for the broadest possible picture of both breadth and depth. This can significantly refine the data used by cybersecurity automation.
- There are several tools that are used to automate cybersecurity for efficiency and process improvement. Application programming interfaces (APIs) are links provided by an OS, web browser, or other platform that allows a developer access to resources at a high level. APIs relieve the developer from the need to write code for specific hardware and software. Because APIs provide direct access to data and an entry point to an application's functions, they can be used to create code much more rapidly. A webhook is a type of event-driven API. Instead of sending information in response to another app's request, a webhook sends information or performs a specific function in response to a "trigger." Webhooks enable lightweight data sharing between software when a specific action takes place. Module updates called a plugin can be downloaded and installed to scan for the latest vulnerability. A single pane of glass (dashboard) is the starting point from which security personnel can see the "big picture" in a way that is easy to read and interpret.

Key Terms

accuracy
active defense
analysis
application
application programming interfaces (APIs)
blogs
business-critical assets
collection
Computer Emergency Readiness Team (CERT)
confidence level
configurations/misconfigurations
Cyber Security Incident Response Team (CSIRT)
data enrichment
deep/dark web
detection and monitoring
focus area
forums
government bulletins
honeypot
identification of tasks suitable for automation
incident response
information-sharing organizations
internal sources
isolated networks
minimize human engagement
open-source intelligence (OSINT)
orchestration
paid feeds
plugin
relevancy
repeatable/do not require human interaction
risk management
security engineering
single pane of glass
social media
standardize processes
team coordination to manage and facilitate automation
threat feed combination
threat hunting
threat intelligence sharing
timeliness
vulnerability management
webhook

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Review Questions

1. Which of the following is NOT a benefit of cybersecurity automation?
   - **a.** Enable smarter resource allocation
   - **b.** Furnish an agile incident response
   - **c.** Increase alerts
   - **d.** Provide scalable solutions
2. Which of the following is NOT an advantage to process standardization?
   - **a.** Create variations in processes
   - **b.** Identify responsibilities
   - **c.** Meet regulatory requirements
   - **d.** Avoid variations in processes
3. What is an event-driven API that responds to a trigger?
   - **a.** Webhook
   - **b.** Plugin
   - **c.** Inverse API
   - **d.** TriggerSet
4. Which of the following is NOT true about a single pane of glass?
   - **a.** It presents data from multiple sources in a unified display.
   - **b.** It is also called a dashboard.
   - **c.** It cannot be customized to meet specific needs.
   - **d.** It is used for managing inputs from security devices and sensors.
5. Which of the following is NOT a focus area of threat hunting?
   - **a.** Isolated networks
   - **b.** Process isolation
   - **c.** Configurations/misconfigurations
   - **d.** Business-critical assets
6. Which of the following is NOT an area in which threat intelligence is used in cybersecurity?
   - **a.** Incident response
   - **b.** Vulnerability management
   - **c.** SIEM data feeds
   - **d.** Security engineering
7. What is the first step of the intelligence cycle?
   - **a.** Collection
   - **b.** Requirements
   - **c.** Analysis
   - **d.** Clustering
8. Which of the following is maintained by the U.S. Department of Homeland Security for analyzing and reducing cyber threats and vulnerabilities by disseminating cyber threat warning information?
   - **a.** CTIXS
   - **b.** CXCS
   - **c.** CSIRT
   - **d.** CERT
9. Which of the following is NOT correct about paid feeds?
   - **a.** Paid feeds are restricted to only organizations that have been victims of a recent attack.
   - **b.** Organizations pay professional external providers who can provide a range of data to reveal patterns and trends.
   - **c.** Providers send this data as electronic feeds for their customer's security appliances, but they also provide in-depth research.
   - **d.** Some providers give specialized services for specific market sectors, such as government or financial services.
10. Which of the following is a language and format used to exchange cyber threat intelligence?
    - **a.** TAXII
    - **b.** BRICK
    - **c.** STIX
    - **d.** FLOWII
11. What type of defense is threat hunting?
    - **a.** Active defense
    - **b.** Remote defense
    - **c.** Circumstantial defense
    - **d.** Web defense
12. Which level of threat hunting uses dashboards and visualization tools with SOC analysts rotated into threat-hunting teams?
    - **a.** Initial (Level 1)
    - **b.** Managed (Level 2)
    - **c.** Defined (Level 3)
    - **d.** Quantitively Managed (Level 4)
13. Which of the following approaches to threat hunting is the systematic search for specific threats based on TI?
    - **a.** Abstract hunting
    - **b.** Structured hunting
    - **c.** Refined hunting
    - **d.** Unstructured hunting

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

14. Which of the following is NOT considered a focus area for threat hunting?
    a. Managed networks
    b. Remote networks
    c. Business-critical assets
    d. Isolated networks

15. Which of the following is the first step in threat hunting?
    a. Select the attack model.
    b. Identify the least concerning threats.
    c. Create a calendar.
    d. Investigate the hypothesis.

16. Which of the following is NOT an advantage of process standardization?
    a. Identify responsibilities
    b. Highlight processes
    c. Increased costs
    d. Avoid variations in processes

17. Which of the following orchestration appliance is a combination of software programs and tools that allow organizations to synthesize and automate a range of security operations, threat intelligence, and incident response in a single platform?
    a. SOAR
    b. EMIS
    c. SOAP
    d. RTAP

18. What tool is a database of the metrics of the upper and lower bounds of specific indicators of normal network activity?
    a. RISI
    b. UEBB
    c. XTSO
    d. KRI

19. Which of the following data enhancements adds third-party threat feeds?
    a. Data enrichment
    b. Threat feed combination
    c. Global feed aggregation
    d. TI supplement

20. Which of the following is NOT correct about APIs?
    a. The usage of APIs requires written permission of the site.
    b. APIs allow a developer to access resources at a high level.
    c. APIs relieve the developer from the need to write code for specific hardware and software.
    d. An API is a link provided by an operating system, web browser, or other platform.

Case Projects

Case Project 6-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this module. What are your thoughts about paid feeds? Should these companies be more transparent about their offerings? Should "report cards" be required that compare and rate paid feeds? How would you recommend comparing paid feeds? Write a one-page paper about this topic.

Case Project 6-2: Intelligence Cycles

Estimated Time: 25 minutes
Objective: Identify different intelligence cycles.
Description: There are a wide variety of intelligence cycles. Use the Internet to research different intelligence cycles. Create and label a cycle that is different than that presented in this chapter. Include a description of each of the steps.

Case Project 6-3: Trusted Automated Exchange of Intelligence Information and Structured Threat Information Expression

Estimated Time: 30 minutes
Objective: Compare TAXII and STIX tools.
Description: Search the Internet for information on TAXII and STIX. Write a two-paragraph explanation of each technology, how it is used, its strengths and weaknesses, and so on.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Project 6-4: Application Programming Interface Security

Estimated Time: 25 minutes
Objective: Research API security.
Description: Just as allowing a person to use an application introduces a risk of abuse, an API introduces the risk that an API client will abuse the service. Another API risk is that web API calls travel over the Internet and can be intercepted, spoofed, or modified just like any other data transfer over a network. Use the Internet to research API security and how the risks can be mitigated.

Case Project 6-5: Threat-Hunting Hypothesis

Estimated Time: 25 minutes
Objective: Develop a threat-hunting hypothesis.
Description: Developing a hypothesis for threat hunting is one of the most important steps in threat hunting. Use the Internet to research threat-hunting hypotheses. Create at least six different hypotheses that could be used.

Two Rights and A Wrong: Answers

Threat Intelligence

1. The requirements phase of the intelligence cycle sets the "high-level" goals for the TI program.
2. Two tools that facilitate the privacy of TI are STIX and TAXII.
3. Many cybersecurity professionals question the true value of threat maps.

Answer: The wrong statement is #2.
Explanation: STIX and TAXII facilitate the timeliness of TI and not the privacy.

Threat Hunting

1. Threat hunting assumes that the network is already infected, and attackers are not trying to enter from the outside but are currently inside.
2. The Optimized level of threat hunting is performed by volunteers.
3. Unstructured hunting, also known as exploratory hunting, is an open-ended approach to threat hunting that does not rely on TI.

Answer: The wrong statement is #2.
Explanation: The Managed level of threat hunting is performed by volunteers.

Improving Security Operation Processes

1. An advantage of standardizing processes is that it highlights processes.
2. Orchestration involves the automation and combination of many different individual tasks and processes.
3. Workflow orchestration has given rise to a new type of cybersecurity platform known as a SIEM.

Answer: The correct answer is #3.
Explanation: Workflow orchestration has given rise to a new type of cybersecurity platform known as a security orchestration, automation, and response (SOAR) platform.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

References

1. Bouwman, Xander; Griffioen, Harm; Egbers, Jelle; Doerr, Christian; Klievink, Bram; and van Eeten, Michel, "A Different Cup of TI? The Added Value of Commercial Threat Intelligence," *29th USENIX Security Symposium*, retrieved Aug. 8, 2020, www.cyber-threat-intelligence.com/publications/Usenix2020-PaidCTI.pdf.
2. Boddy, Matt, "Exposed: Cyberattacks on Cloud Honeypots," *Sophos*, Apr. 9, 2019, accessed June 5, 2019, www.sophos.com/en-us/press-office/press-releases/2019/04/cybercriminals-attack-cloud-server-honeypot-within-52-seconds.aspx.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Part 3

Vulnerability Assessment and Management

A key element in cybersecurity involves handling vulnerabilities. Vulnerability assessment and management is a process that helps organizations identify, evaluate, address, and then report on cybersecurity vulnerabilities. The chapters in this third part examine how to uncover, address, and report vulnerabilities.

Chapter 7
Vulnerability Scanning and Assessment Tools

Chapter 8
Addressing Vulnerabilities

Chapter 9
Vulnerability Management and Administration

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 7

Vulnerability Scanning and Assessment Tools

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Define vulnerability scanning concepts
2. Explain methods for scanning for vulnerabilities
3. Categorize vulnerability assessment tools

#TrendingCyber

Complacency is one of the most dangerous attitudes to have. This is a mindset of feeling self-satisfaction that is accompanied by an unawareness of actual dangers or deficiencies. A complacent person is pleased with their situation and feels that they do not need to do anything more, even in the face of uncertainty or risk. "We don't need to worry about that" is perhaps the best way to characterize complacency.

There are numerous examples of an attitude of complacency resulting in serious repercussions. In 1988, the supermarket chain Kroger was the number-one grocery retailer in the United States. Then Walmart announced that it was entering the business by selling groceries in its stores. Instead of examining its business practices and developing a strategy to counteract Walmart's decision, Kroger's management said, "We don't need to worry about that," and assumed that Walmart would never succeed in the grocery retail business as Kroger had. However, their complacency led to an opening for Walmart to thrive. Today Walmart generates about 60 percent of its total revenue from selling food and consumables and commands one-quarter of all grocery sales in the United States. Kroger is now in a distant second place.

Complacency is also responsible for an untold number of cybersecurity vulnerabilities. Because software and hardware developers had an attitude of "We don't need to worry about that," it has opened the door for threat actors to thrive. One example of this is the shocking revelation in late 2023 of an attack dubbed LogoFAIL.

When a computer first boots up, a logo of the hardware vendor is displayed on the screen, such as Dell, ASUS, or Beelink. The code that displays this logo is known as an image parser. Some image parsers even allow users to create their own custom logos to appear when booting up. However, these image parsers have numerous vulnerabilities that can be exploited by an attacker. By replacing the legitimate code with code that generates an identical-looking logo but also contains malware (a classic example of a Trojan) that is specially crafted to exploit these vulnerabilities, LogoFAIL makes it possible to execute malicious code at the most sensitive stage of the boot process, known as the Driver Execution Environment (DXE). This enables LogoFAIL to bypass all defenses that have been created to avoid such an attack.

By executing code in the early DXE stage, when most of the system initialization is performed, LogoFAIL bypasses security defenses such as Secure Boot and the hardware-based verified boot mechanisms Intel Boot Guard, AMD Hardware-Validated Boot, and ARM TrustZone-based Secure Boot. Because LogoFAIL executes its malicious code before the main operating system (OS) has even started, then all OS-based defenses are also bypassed. And since the malware code is stored in the firmware and not on the local hard drive, no anti-malware or endpoint protection software can detect it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In the words of the security researchers who discovered LogoFAIL, once malware code execution is achieved during the DXE stage, it's "game over" for any and all current security defenses on the device.

How did the security researchers uncover LogoFAIL? The researchers found the vulnerabilities by running the image parsers through a tool known as a fuzzer. Fuzzers are designed to identify programming bugs by repeatedly executing small parts of code with small variations in the input each time. Whenever a "crash" of the code occurs, the fuzzer notes the memory address along with the input that triggered it. Further analysis using other tools enables researchers to isolate and identify a potential vulnerability. Using fuzzers, the security researchers behind LogoFAIL identified 24 vulnerabilities, 13 of which they believe are exploitable by threat actors.

But if the security researchers were able to find vulnerabilities using fuzzers, why didn't the developers discover them? The security researchers concluded, "The results from our fuzzing campaign unequivocally say that none of these image parsers were ever tested."

Evidently the developers were complacent.

Because LogoFAIL allows infections that are impossible to detect or remove using current defense mechanisms, users should install unified extensible firmware interface (UEFI) security updates distributed by the manufacturer of the device or of the motherboard inside it. It is also recommended, when possible, to configure UEFIs to use multiple layers of defenses. Besides using Secure Boot, this includes both Intel Boot Guard and, when available, Intel BIOS Guard. There are similar additional defenses available for devices running AMD or ARM central processing units.

Because the image-parser vulnerabilities exploited by LogoFAIL reside in the UEFI, smartphones, and other devices that rely on alternative boot mechanisms are not affected. Apple computers are also not impacted because their image files are "hard-coded" into the UEFI, making it impossible to swap the legitimate one for a malicious lookalike. Also, many devices sold by Dell are not directly exploitable because they too do not permit logo customization. Although these designs effectively close off the LogoFAIL attack surface, the security researchers still recommend patching the vulnerable image parsers on these devices since they represent "a hazard that could inadvertently turn into a security issue."

In other words, don't be complacent.

A laurel is a shrub that was traditionally used to weave wreaths and crowns that were symbols of victory in the sporting events of ancient Greece. This gave rise to the expression "rest on one's laurels," which means to be so satisfied with what has already been achieved that no further effort is needed. In short, it is being complacent.

Complacency is one of the deadliest mindsets in cybersecurity. An organization that thinks for even a moment that they have achieved the optimum level of defense and thus can relax is only destined for a crisis. With the continual barrage of attacks occurring around the clock that probe for the tiniest crack in defenses to exploit, no one can be complacent. All organizations must continually look for vulnerabilities in their own defenses and address these weaknesses.

In this chapter, you examine managing vulnerabilities through vulnerability scanning. There is a methodology for vulnerability scanning along with tools for identifying and addressing vulnerabilities.

Vulnerability Scanning Concepts

Certification

2.1 Given a scenario, implement vulnerability scanning methods and concepts.

Vulnerability management, also called *infrastructure risk visibility and assurance*, is an ongoing examination of the organization's security. Vulnerability management seeks to answer such questions as "Where are we exposed?" "What should we prioritize?" "Are we reducing our exposure over time?" and even "How do we compare with our peers?"

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

At the heart of vulnerability management is identifying vulnerabilities so that they can then be addressed. Searching for vulnerabilities, called *vulnerability scanning*, involves understanding what it is and how industry frameworks can be used.

What Is a Vulnerability Scan?

One useful means of defining a vulnerability scan is to compare it to a penetration test. Knowing the reasons for conducting a scan can also help define a vulnerability scan. However, there are also challenges associated with a vulnerability scan.

Vulnerability Scan versus Penetration Test

Consider Rocco, who sees his doctor for an annual physical but only because it is required by his employer. His blood pressure is taken, and it is just barely below the upper limits that would require intervention. Rocco leaves the office satisfied that he is in good health (and happy that he does not have to start exercising or change his diet), that he has met the requirements mandated by his employer, and that he can wait another year before returning for his next physical.

Now consider Azzurra, who likewise visits her physician for her annual physical. However, she does so because she is concerned about maintaining good health and not just meeting an employer requirement. Her blood pressure is taken in the doctor's office and is in the normal range. Azzurra also uses a wearable fitness tracker so that her blood pressure is continually and automatically monitored, and she views the results every evening with an app on her smartphone.

Which patient has a higher probability of detecting a sudden and prolonged spike in blood pressure and then immediately taking steps to manage it? Is it Rocco, who has it checked manually once per year at the doctor's office, or Azzurra, who has it continually monitored?

Obviously, Azzurra has a much higher probability of catching a change in her blood pressure than Rocco. This is because Azzurra is continually and automatically monitoring her health, while Rocco is only reviewing it annually. In addition, because Azzurra is genuinely concerned about maintaining good health and is not just having her vital signs taken in order to meet a requirement, this attitude in itself will play a role in a more proactive approach to good health.

The difference between Rocco and Azzurra in this scenario is similar to the difference between a penetration test and a vulnerability scan. A penetration test is a single event using a predominately manual process in which the testers act like a threat actor to find vulnerabilities to exploit. However, much like Rocco, once the pen test is over, it is forgotten about until the next time it is required. A **vulnerability scan**, on the other hand, is a frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress. In other words, a vulnerability assessment is a cyclical and continual process of ongoing scanning and continuous monitoring to reduce the attack surface. Table 7-1 contrasts a vulnerability scan with a penetration test.

Table 7-1 Vulnerability scan versus penetration test

	Vulnerability scan	Penetration test
Purpose	Reduce attack surface	Identify deep vulnerabilities
Procedure	Scan to find weaknesses and then mitigate	Act like a threat agent to find vulnerabilities to exploit
Frequency	Usually ongoing scanning and continuous monitoring	When required by regulatory body or on a predetermined schedule
Personnel	Internal security personnel	External third parties or internal security personnel
Process	Usually automated with a handful of manual processes	Mostly manual process
Goal	Identify risks by scanning systems and networks	Gain unauthorized access and exploit vulnerabilities
Final report audience	Executive summary for less technical audience; technical details for security professionals	Several different audiences

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Reasons for Conducting a Scan

There are several reasons for conducting a vulnerability scan besides providing continuous monitoring. These include meeting regulatory requirements and following corporate policies.

Meet Regulatory Requirements Conducting a vulnerability scan is necessary to meet **regulatory requirements**, which is following specific actions mandated by an external regulatory body. Examples of regulatory compliance laws and regulations include the Dodd-Frank Act, Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Sarbanes-Oxley Act.

Caution !

Although aligning with regulatory standards is important, the primary goal of a vulnerability scan or even pen test should never be just to meet compliance standards. Compliance cybersecurity standards are absolute minimal protection. In other words, compliance does not equal security!

Follow Corporate Policies At its core, a security policy is a recorded document that states how an organization plans to protect the company's information technology (IT) assets. The policy outlines the protections that should be enacted to ensure that the organization's assets face minimal risks. A security policy, along with the accompanying procedures, standards, and guidelines, is key to implementing information security in an organization. Having a written security policy empowers an organization to take appropriate action to safeguard its data. A policy is considered the correct tool for an organization to use when establishing security because a policy applies to a wide range of hardware or software (it is not a standard) and is required (it is not just a guideline).

Note 1

If the question "What is a security policy?" were posed to both a manager and a security technician, the answers would likely be different. A manager might say that a security policy is a set of management statements that defines an organization's philosophy of how to safeguard its information. A security technician might respond that a security policy is the cybersecurity configuration settings in a system. These two responses are not conflicting but are complementary: a written policy dictates what technology configuration settings should be used.

Most corporate policies require regular vulnerability scans. The ongoing scanning and continuous monitoring features of such a scan can meet the goals of an organization as outlined in its security policy.

Vulnerability Scan Challenges

Despite its importance, there are several challenges that are associated with vulnerability scanning. Some of these can even be considered risks and include:

- **Volume of scan data.** Vulnerability scans can produce large amounts of data that must be analyzed.
- **Identification of vulnerabilities.** A vulnerability scanner must be able to perform two tasks: (1) locate and identify devices, software, open ports, and other system information and (2) correlate that information with known vulnerabilities from one or more repositories of vulnerabilities. Not every identified system element may be an actual vulnerability and, if a system element is not part of the vulnerability repository, then a weakness may be overlooked.
- **Technical limitations.** Vulnerability scanning that is configured to be aggressive or intrusive can impact performance or even stability of the systems being scanned. Scanning could also cause bandwidth issues on networks. These technical limitations of a vulnerability scan could have an effect on the timeliness and usefulness of the scan.
- **Remediations.** Due to several different factors, such as a high cost to remediate or a very low risk of exploitation, not all identified vulnerabilities may be addressed. The process for making these determinations can often be challenging and highly debated.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Industry Frameworks

An **industry framework** is a set of designs for businesses in a specific industry and is based on consensus from industry representatives. There are several industry frameworks that can facilitate overall vulnerability management and specific vulnerability scanning. For example, these can assist in defining policies and procedures for implementing and managing security controls in an enterprise environment as they relate to vulnerability management. These frameworks include the Payment Card Industry Data Security Standard (PCI DSS), the Open Web Application Security Project (OWASP), Center for Internet Security (CIS) benchmarks, and the International Organization for Standardization (ISO) 27000 series.

Payment Card Industry Data Security Standard (PCI DSS)

An example of a framework standard as it relates to information security is the **Payment Card Industry Data Security Standard (PCI DSS)**. The PCI DSS compliance standard was introduced to provide a minimum degree of security for handling customer card information. For example, Requirement 11 of the latest standard (PCI DSS 3.2.1) states that organizations must "Regularly test security systems and processes" using both vulnerability scans and penetration tests. A partial list of the PCI DSS Requirement 11 standards is shown in Table 7-2.

Table 7-2 PCI DSS Requirement 11 standards

Standard	Description	Frequency
11.1	Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points.	Quarterly
11.2	Run internal and external network vulnerability scans to address vulnerabilities and perform rescans as needed until passing scans are achieved. External scans must be performed by an Approved Scanning Vendor (ASV), while scans conducted after network changes and internal scans may be performed by internal staff.	At least quarterly and after any significant change in the network
11.3	Develop and implement a methodology for penetration testing that includes external and internal testing. If segmentation is used to reduce PCI DSS scope, perform penetration tests to verify that the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls.	At least annually and after any significant upgrade or modification; service providers must perform penetration testing at least every six months and after making changes to controls

Note 2

PCI DSS version 3.2.1, which has been in place since early 2018, will be replaced by version 4.0, which goes into effect on March 31, 2024. While some requirements will be effective immediately, many will not be required for another 12 months, giving businesses a year-long transition period to implement the more challenging requirements. Version 4.0 has 63 new requirements addressing such topics as phishing, social engineering, and evolving attacks against e-commerce payment applications.

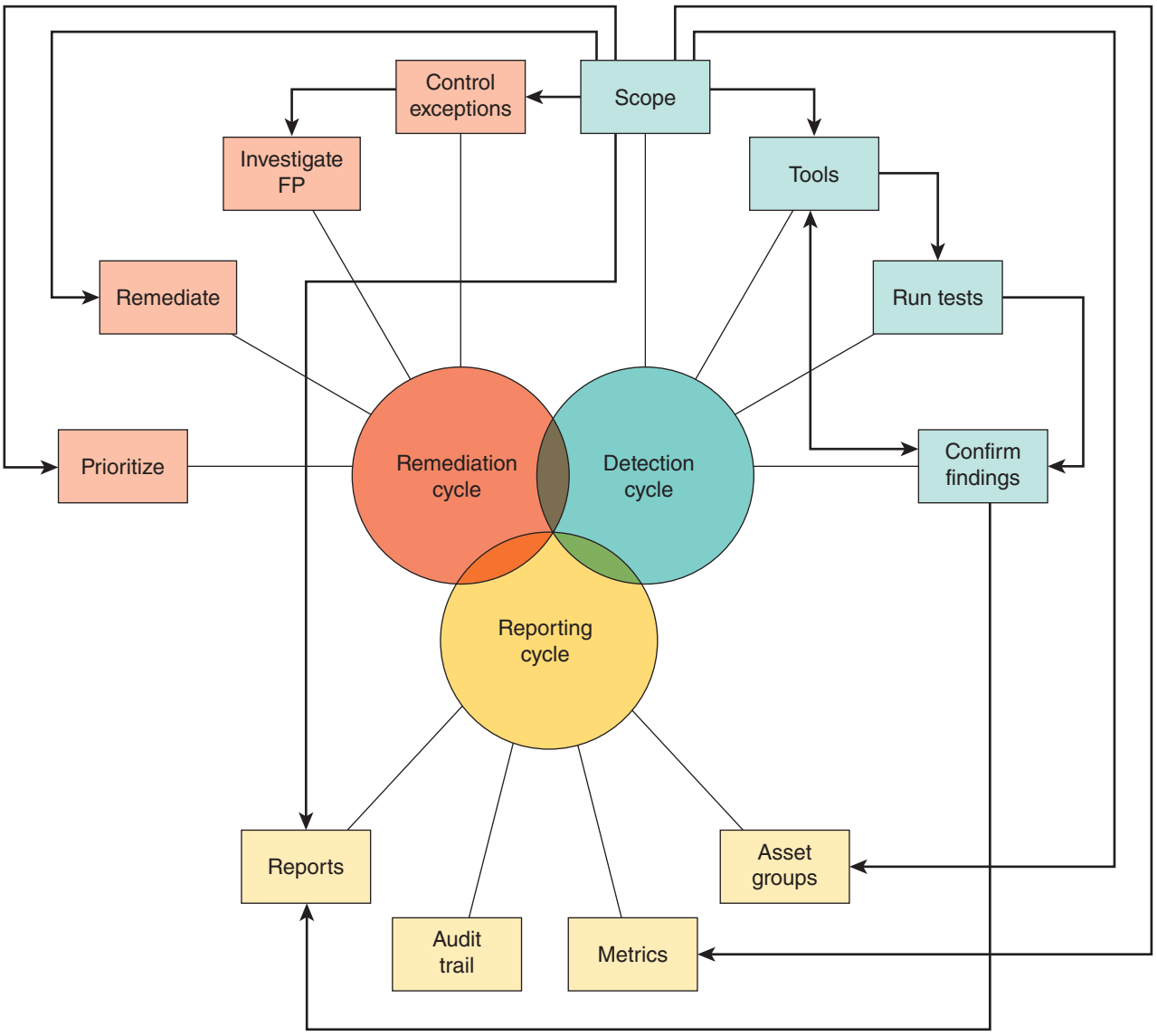
Open Worldwide Application Security Project (OWASP)

The **Open Worldwide Application Security Project (OWASP)** is a nonprofit foundation that works to improve the security of software. Their goal is to enable organizations to "conceive, develop, acquire, operate, and maintain applications that can be trusted." Currently there are over 250 local chapters worldwide that support community-led open-source software projects. All OWASP projects, tools, documents, forums, and chapters are free and open to all.

The OWASP Vulnerability Management Guide (OWASP VMG) project provides guidance on the best practices that organizations can use to establish a vulnerability management program within their organization. The guide provides in-depth coverage of the full vulnerability management life cycle, including the preparation phase, vulnerability identification/scanning phase, reporting phase, and remediation phase. Figure 7-1 shows the components of the OWASP VMG.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-1 Open Worldwide Application Security Project Vulnerability Management Guide



Center for Internet Security (CIS)

Over 20 years ago, a small group of business and government leaders met in Washington, D.C., to discuss an increase in cyberattacks. From that 2000 meeting a vision emerged for an independent, mission-driven, nonprofit organization dedicated to preventing and mitigating new cyber threats. The outgrowth of this meeting became the **Center for Internet Security (CIS)**. Through a collaborative global effort, the CIS has developed standards in the form of the CIS Controls and CIS Benchmarks, along with specialized technology tools to help security practitioners implement and manage cyber defenses.

International Organization for Standardization (ISO) 27000

The **International Organization for Standardization (ISO) 27000** series provides an overview of what is called information security management systems (ISMSs). It also provides terms and definitions commonly used in the ISMS family of standards. The ISO 27000 recommends best practices for managing information risks by implementing security controls within the framework of an overall ISMS. It is very similar to standard management systems such as those for quality assurance and environmental protection. These frameworks apply to all types and sizes of organizations, including commercial enterprises, government agencies, and not-for-profit organizations.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong

1. A vulnerability scan is a frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress.
2. A challenge of a vulnerability scan is the low volume of data that a scan produces.
3. The PCI DSS, OWASP, CIS, and ISO all provide vulnerability management frameworks.

See the answers at the end of the chapter.

Vulnerability Scanning Methodologies

Certification

2.1 Given a scenario, implement vulnerability scanning methods and concepts.

A methodology is a set of procedures. There are different procedures to follow when running a vulnerability scan. However, these vary depending on decisions that are made in advance.

Scanning Decisions

There are several decisions that must be made prior to conducting a scan if it is to be impactful. **Secure baseline scanning** uses specific security frameworks as comparison benchmarks to identify weaknesses. These may be dictated by regulatory requirements and can play a role in the decisions. The prerequisite scanning decisions typically include determining what should be scanned and how and when it should be scanned.

What Should Be Scanned?

One of the first decisions before conducting a scan is to determine what should be scanned. It is axiomatic that critical infrastructure components should be scanned, such as operational technology (OT), which is using hardware and software to monitor and control physical processes and the devices connected to the infrastructure that support these processes. Whereas a cybersecurity incident involving IT may be the theft of customer data, a successful attack on OT systems can be significantly more deadly and result in significant loss of life. A threat actor who can remotely manipulate the pressure in a pipeline so that it ruptures can inflict serious physical harm to a large number of persons.

Beyond critical infrastructure components, often decisions must be made about which assets (devices) should be included in a vulnerability scan. This is because not all assets have the same value: Some assets are critical while others can be of lessor importance. To continuously scan low-value assets may take away from scanning and focusing on high-value assets.

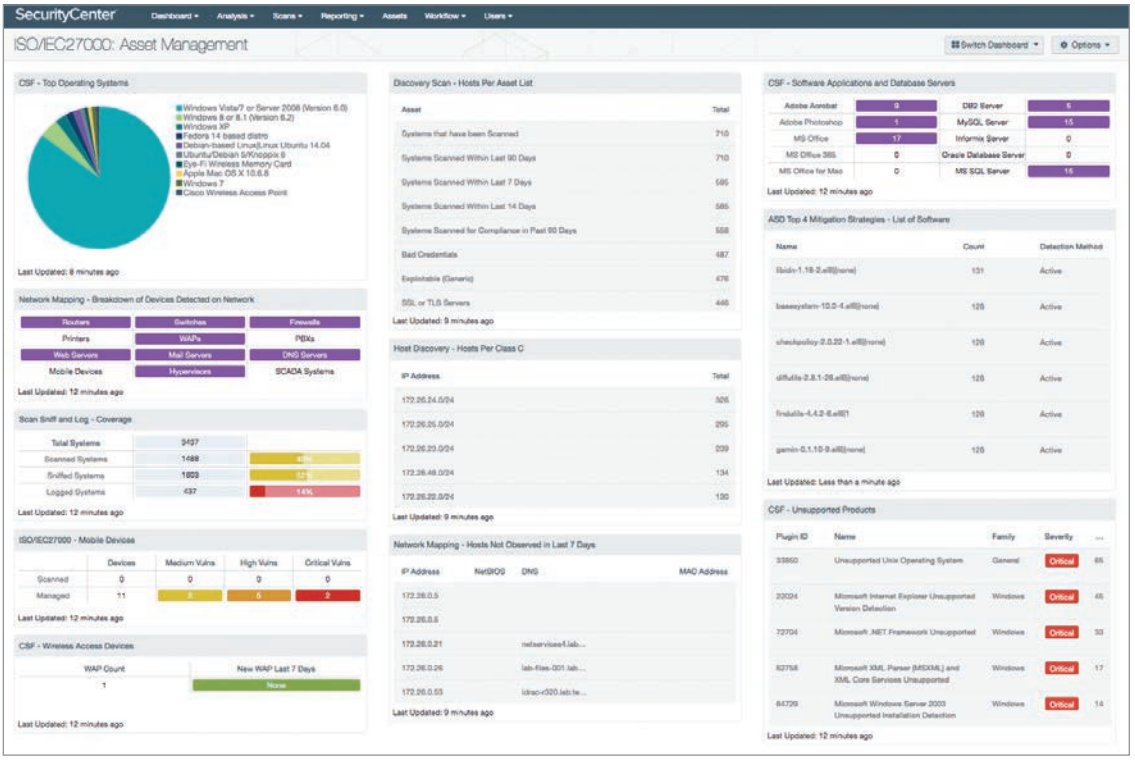
Determining what should be scanned first involves asset discovery. A higher level of asset discovery and identification is digital fingerprinting.

Asset Discovery Due to the large number of devices that are part of an organization today, identifying these (called **asset discovery**) is an important step in determining what should be scanned. However, in order to create this list of assets to be scanned, an asset inventory or listing of all significant assets needs to be consulted. For those organizations that maintain an up-to-date asset inventory through regular asset management, the asset inventory can be reviewed to identify the systems that should be scanned. However, what if there is no asset inventory available, or it is out of date so that it cannot be trusted as being accurate?

Fortunately, most vulnerability scanning tools allow for an asset discovery inventory scan that only searches for devices attached to the network instead of conducting a full vulnerability scan that looks for vulnerabilities. Figure 7-2 shows the hardware asset management screen of a vulnerability scanner. Software assets can also be identified as shown in Figure 7-3.

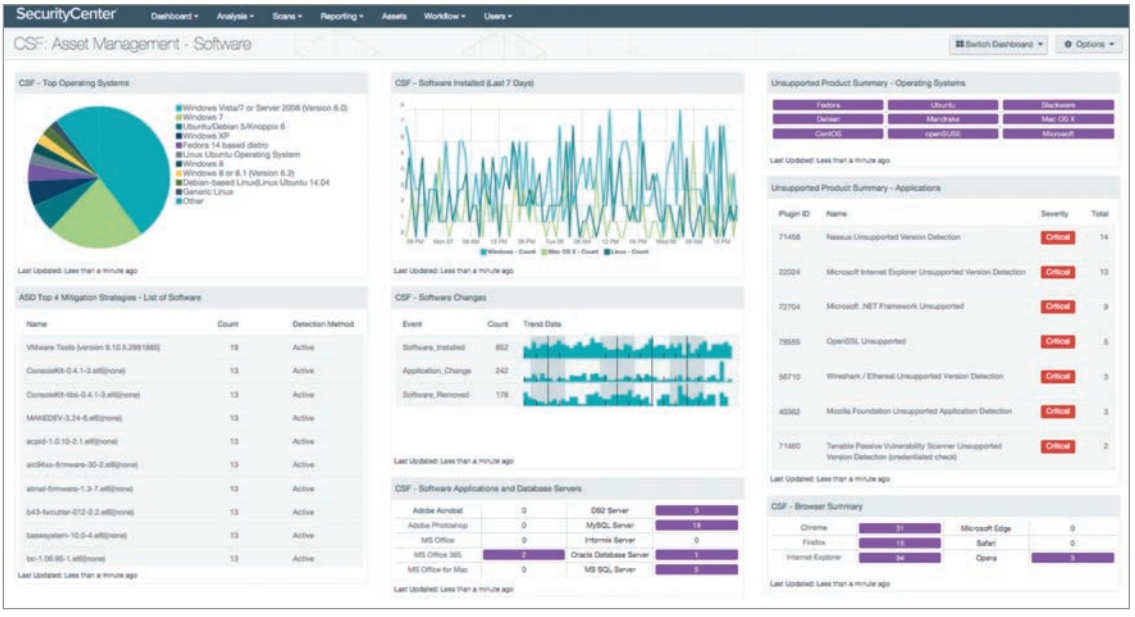
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-2 Hardware asset management



Source: Tenable

Figure 7-3 Software asset management



Source: Tenable

Device Fingerprinting Asset discovery can identify devices that are connected electronically to the computer network. However, it is not uncommon for devices to be moved from one location to another without physical inventory records being updated. Thus, a device that appears in an asset discovery scan that must be physically accessed may no longer be in that originally recorded location. Is there a means for identifying assets in a more unique and granular fashion? The answer is yes. This involves both static device fingerprinting and dynamic network fingerprinting.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Static Device Fingerprinting Static **device fingerprinting** is the process of collecting information about a device's installed hardware and software configuration in order to create a unique identifier. These attributes can include the device's OS version, screen resolution, installed fonts, browser plugins, time zone, and much more. By combining these attributes, a unique fingerprint is created for each device, allowing it to be distinguished from others. This can be beneficial when performing an asset discovery for a vulnerability scan.

Note 3

Device fingerprinting is also used outside of cybersecurity. Website personalization, in which e-commerce sites recognize a returning user so as to offer customized recommendations or remember prior preferences, relies on device fingerprinting. It is also used by media streaming platforms and content providers to enforce digital rights management policies to prevent unauthorized access and distribution of copyrighted content.

There are different techniques by which information for device fingerprinting can be gathered. Several of these are listed in Table 7-3.

Table 7-3 Device fingerprinting techniques

Technique	Explanation
User agent tracking	Involves collecting data about the user's browser, OS, and device by using JavaScript, server-side code, or browser plugins.
Canvas fingerprinting	Uses JavaScript to draw an invisible image on the user's browser page, which creates a unique fingerprint based on the device's graphics capabilities.
Cookies	A small text file stored on the user's device that can be used to track their activity across different websites and is usually combined with other techniques for digital fingerprinting.
Web beacon tracking	Embeds a tiny and invisible HTML element called an *inline frame (iframe)* to track user behavior and collect data about the user's device and location.
Audio and video fingerprinting	Involves using JavaScript or other tools to collect data about the device's audio and video hardware.

Caution !

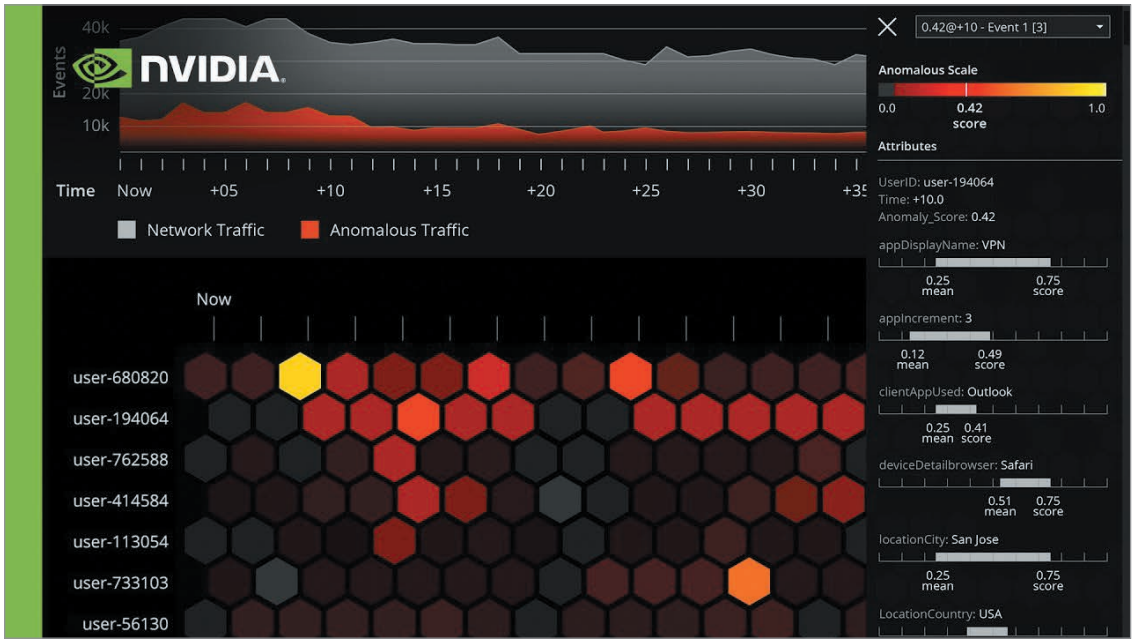
However, threat actors also use device fingerprinting. Device fingerprints can be used for device spoofing: threat actors can create a device fingerprint that mimics a legitimate device, making it difficult for security protections to distinguish between genuine users and impostors.

Dynamic Network Fingerprinting A growing trend in digital fingerprinting is to not just fingerprint the static characteristics of a device but also consider the dynamic usage of a device. Consider employees at an organization. They have unique characteristics and different ways by which they interact with the corporate network depending on their job role and responsibilities. A typical employee may interact with 100 or more networked applications daily while doing their job. And the integrations between these applications mean that there may be tens of thousands of interconnections and permissions shared across these 100 applications.

Fingerprinting these day-to-day and even minute-by-minute interactions of users with their devices across the network can create a more robust digital fingerprint known as dynamic network fingerprinting. Some of the network data that can be captured to create this network fingerprint includes TCP options, ICMP requests, DHCP requests, IP Time-to-Live (TTL) values, IP addresses and ID values, Don't Fragment bit setting, and window size. This dynamic network fingerprint can be used to both authenticate a user as being genuine while also identifying the abnormal behavior of a threat actor. Figure 7-4 illustrates a system that is used for unusual (anomalous) traffic based on dynamic network fingerprinting.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-4 Dynamic network fingerprinting



Note 4

Dynamic network fingerprinting relies heavily on artificial intelligence (AI) using "pretrained workflow models." This allows for massive amounts of network data and hundreds of thousands, or even millions, of models to be managed. Critical anomalies can be immediately identified for security analysis.

How Should It Be Scanned?

Another scanning decision involves how the assets should be scanned. Three categories of options include active versus passive scanning, internal versus external scanning, and full network versus segmentation scanning.

Active versus Passive Scanning It is necessary for a vulnerability scan to collect data on the assets that are to be examined. For example, data such as the device name, IP address, OS version, installed software, and patches applied are all needed to then determine if there is a vulnerability. Extracting this data is called enumeration and is intended to create a picture of the endpoint and network. This process is called building **map scans**.

There are two different approaches to gathering this data. **Active scanning** sends test traffic transmissions into the network and monitors the responses of the endpoints. **Passive scanning**, on the other hand, does not send any transmissions but instead only listens for normal traffic to learn the needed information.

A primary advantage of conducting active scanning over passive scanning is that active scanning can accelerate the collection of the data; it is not necessary to wait for normal network traffic to or from each asset to generate a complete profile of information. In addition, not all parts of a network may always be available, which can limit the ability to passively monitor traffic.

Note 5

Some active scanners can also immediately take action if a serious vulnerability is uncovered (such as blocking an open port) or even launch a simulated attack to observe the response.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

However, there are disadvantages to active scanning. These include:

- Smaller networks can become overloaded with high volumes of test traffic.
- Sending test traffic increases the risk of the endpoints malfunctioning if incompatible queries are sent.
- Some devices such as Internet of Things (IoT) devices may not be able to perform their normal tasks while receiving and returning test traffic and could become overloaded.
- Many IoT devices are proprietary and may react differently to test traffic.

Internal versus External Scanning Another option regarding how the assets should be scanned involves the "vantage point" of the scan. An **internal vulnerability scan** is performed from the vantage point inside the internal network; that is, it is launched and then conducted from inside the corporate network. An internal vulnerability scan typically has the primary benefit of identifying at-risk systems.

An **external vulnerability scan** is performed from the vantage point outside the network. It targets specific IP addresses that are within the network to identify vulnerabilities. An external scan can also detect open ports and protocols.

Note 6

An external vulnerability scan is in some ways similar to a penetration test.

Full Network versus Segmentation Scanning Attempting to run a vulnerability scan on a very large network in a single scan job is generally not advisable. This is because vulnerability scans can consume large amounts of system resources and reduce overall system response time, thus negatively impacting the **operations** (activities and tasks used to produce goods and services) of the organization. Although some scans can have better **performance** (run faster) because they are performing fundamental actions such as looking for open ports and finding software that will respond to requests, full network scans can nevertheless have a perceptible impact.

The best practice when running a vulnerability network scan on a large network is to divide it into smaller sections (called **segmentation**) for the purpose of the scan. This will ensure more rapid results, as a scan on a smaller network segment will finish far more quickly than a scan on a larger segment. It will also reduce the load placed on system resources, thus ensuring optimum performance and responsiveness at all times.

Note 7

Most scanners allow for a new segment to be defined prior to the start of the scan, and then this segment is retained so that it does not need to be configured again.

When Should It Be Scanned?

Another consideration is when and how frequently a vulnerability scan should be conducted. The optimum frequency for vulnerability scanning is continual—all systems are scanned all the time. However, there are different constraints that call for scanning on a routine basis instead of around the clock. These constraints include:

- **Technical constraints.** Limitations based on technology can dictate how frequently a scan may be performed. For an organization with a very large network with many devices, it simply may not be possible to scan the entire network within the desired time period. Other technical constraints include limitations on network bandwidth and vulnerability scan software license limitations. When dealing with technical constraints, spreading out the scans to run at specific times may be a necessary alternative.
- **Workflow interruptions.** Continual vulnerability scans may impact the response time of a system so that the daily workflow or normal business processes are hindered. Moving the scans to "off hours" such as nights or weekends can limit these interruptions.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Regulatory requirements.** Specific regulations can dictate how frequently a vulnerability scan must be performed. For example, PCI DSS states how often vulnerability scans must be conducted.
- **Risk appetite.** A final consideration is the organization's tolerance for exposure to a vulnerability, or risk appetite. The risk appetite for various systems may be different: those systems with sensitive data for which there is a low-risk appetite may be scanned more frequently than those systems that contain only public data and have a high-risk appetite.

Caution

When determining the risk appetite, longer intervals between scans results in a greater risk for a vulnerability to be exploited.

The regular interval when vulnerability scans are conducted (called **scheduling**) will vary between each organization due to these and other factors. Generally, scan schedules can be set to specific intervals by the hour, day, week, or month.

Running a Vulnerability Scan

Running the vulnerability scan itself generally involves updating the vulnerability scan software, configuring the software, and then executing the scan.

Updating the Scan Software

Before running a vulnerability scan, it is important that the software be updated. As with virtually any software today, updates are available to enhance its functionality or provide stronger security. Vulnerability scan software is no exception. In addition to the usual software updates, vulnerability scan software updating includes plugin updates and vulnerability feeds.

Plugin Updates As attacks continue to evolve, vulnerability scan software must be "nimble" so that information regarding new attacks can be regularly added and updated. Many vulnerability scan products are modular in nature instead of a single enormous software package. These module updates, known as plugins, can be downloaded and installed as needed.

However, plugins generally go beyond basic updates. Many plugins contain advanced vulnerability information, a set of remediation actions, and updated algorithms to test for the presence of a security issue.

Vulnerability Feeds Vulnerability scanning software looks for the presence of a vulnerability by comparing software that is scanned against a set of known vulnerabilities. This is known as signature-based monitoring because it compares activities against a predefined signature. Signature-based monitoring requires access to an updated database of signatures along with a means to actively compare and match current software against a collection of signatures.

Note 8

One of the weaknesses of signature-based monitoring is that the signature databases must be constantly updated and, as the number of signatures grows, the behaviors must be compared against an increasingly large number of signatures.

Various vulnerability feeds provide a set of vulnerability data to vulnerability scan software. Some of the best-known vulnerability feeds are the NIST National Vulnerability Database (NVD), Mitre Common Vulnerabilities and Exposures (CVE), CERT Vulnerability Notes Database, and VulnDB.

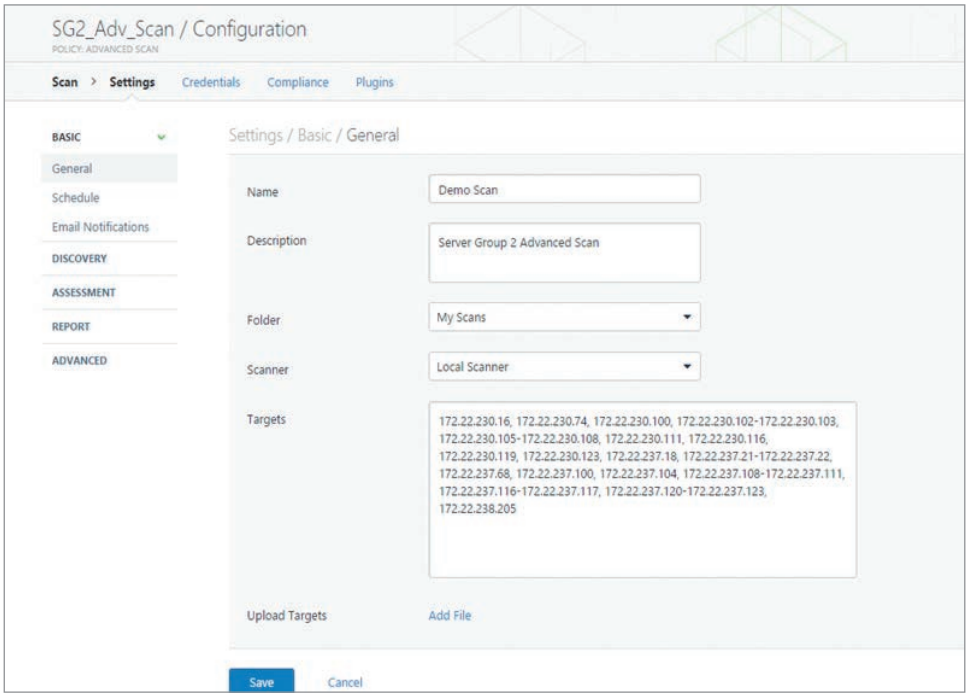
Configuring the Scan Software

Configuring vulnerability scan software involves setting specific parameters so that the scan meets the intended objective. These parameters include the scope, sensitivity levels, and data types.

Scope The scope of a vulnerability scan is the target devices to be scanned. This generally will include a range of hosts or subnets, as shown in Figure 7-5. The scope of a scan should be designed to meet the intended goals of the scan. If a specific vulnerability for Windows 11 computers is being targeted in the scan, for example, then it makes sense to only scan those systems running that OS and the specific version.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-5 Vulnerability scan scope



Source: Tenable

Note 9

Limiting the scope can also reduce the impact on the overall performance of the network.

Sensitivity Level While the scope represents the breadth of the scan, the **sensitivity level** is the depth of a scan; that is, what type of vulnerabilities are being searched for? While a general scan may search for all vulnerabilities, often a scan is looking for a specific type of vulnerability. The sensitivity configuration variable can be used to limit how deeply a system is examined.

Data Type Another configuration setting specifies the data types to be scanned. Like the sensitivity level, this can be used to "drill down" when searching for a specific vulnerability in a known file type instead of searching all files on a system.

Executing the Scan

When executing the scan, there are different scanner options that can impact running the scan. The options include credentialed versus noncredentialed scans and agent verses agentless scans. There are also other considerations when executing a scan.

Credentialed versus Non-credentialed Scans A threat actor who can compromise a network can cause a significant degree of harm. Yet a threat actor who can compromise a network and has in their possession valid authentication credentials (such as usernames and passwords, certificates, and public keys) can potentially cause catastrophic harm. Which of these should a vulnerability scan imitate: a threat actor who does not have stolen credentials or one who does?

Fortunately, most vulnerability scanners allow for both types of scans. A **credentialed scan** is a scan for which valid authentication credentials are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials, while a **noncredentialed scan** provides no such authentication information.

Noncredentialed scans will run faster because they are performing fundamental actions such as looking for open ports and finding software that will respond to requests. Credentialed scans are slower but can provide a deeper insight into the system by being able to access a fuller range of software installed on the system and examine the software's configuration settings and current security posture.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Agent versus Agentless Scans There are two means by which devices interact with a vulnerability scanner. A software **agent** is a package deployed to each device that needs to be scanned. Once installed, the agent collects data that indicates whether the device may have vulnerabilities. The agent then passes this data back to collection servers that gather it across the entire infrastructure and consolidate the results into a single pane of glass interface for analysis. This simplifies the administration and analysis process for the security team and helps address regulatory compliance requirements.

There are several advantages of agent-based scanners:

- **Device network flexibility.** Assets using dynamic addressing or that are located off-site behind private subnets are still accessible with agent-based scanning. These devices can connect back to the collection servers through their normal network connections instead of a scan needing special permissions to access the device through its network connection.
- **Include disconnected devices.** Devices that are disconnected from a network can still scan themselves and return the results when a connection is reestablished. This feature is beneficial for employees working from home or for business travelers with intermittent network access.
- **No device credential requirements.** Agent-based scanners are designed to circumvent the need for credentials. This is because the agents are installed directly on the device and collect information to be sent to the collection servers instead of the collection servers accessing the device with credentials.
- **Personal device support.** The increasing use of personal devices for corporate usage creates security concerns for organizations. Having agents installed on any personal user device can help provide a higher degree of security.
- **Reduced network traffic.** Preinstalled agents reduce overall network traffic. Frequent vulnerability scans can be replaced by rules that set event-driven or periodic scheduled internal scans.

There are some disadvantages of agent-based vulnerability scanning. Agents are OS dependent. Also, threat actors can compromise agents to mask the presence of their malware. And agents generally cannot access network assets like routers, switches, and firewalls.

Agentless scanning, on the other hand, does not require agents to be installed on each device. Instead, the server "reaches out" to each asset. While the data collected is similar to an agent-based approach, it eliminates installing and managing additional software on all devices.

Other advantages of agentless scanning include:

- **Additional data.** Agentless scanning can provide data not accessible by agent-based scanning. For example, agentless vulnerability scanners can locate Secure Sockets Layer (SSL) certificates that are not stored on a device.
- **Network scanning.** Agentless scanning can observe the entire network and identify all hosts and devices connected. This allows the identification and scanning of assets that might be missed by agent-based scanning.
- **Inclusive coverage.** Because there are no OS compatibility requirements to detect and scan assets, this allows for IoT and network-based devices such as routers and switches to be included in scans.

A disadvantage of agentless scanning is that it requires a consistent network connection. In a remote work environment with users behind home networks, their devices are not always accessible to agentless scanners. Also, agentless access does not have the depth of visibility that agent-based solutions have. This is because agent-based software can see deeper vulnerabilities due to its privileged access to the OS.

Generally, agent-based scanning is preferred in environments that are widely distributed or have many remote employees. For environments where most of the devices are located within corporately controlled networks, agentless scanning allows for wider network analysis and assessment of all varieties of network devices.

Note 10

Many organizations use both agent-based and agentless scanning.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Other Scan Considerations There are also other considerations that need to be addressed when running a vulnerability scan. These include scanner permissions, network appliance configurations, and access approval.

Scanner Permissions A well-protected network ideally should hinder or even block a scanner from performing a vulnerability scan, just as it would prevent a threat actor from conducting their own scan for reconnaissance. In such cases, network security would prevent the vulnerability scanner from being able to accurately examine the devices on the network. It may be necessary for network security to have appropriate scanner permissions added so that it is able to access the devices on the network.

Network Appliance Configurations Vulnerability scanners should set off alarms on security appliances such as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and firewalls. One approach is to mitigate these alarms by instructing the IDS/IPS to ignore attacks originating at the vulnerability scanner and to also configure the vulnerability scanner to correspond to the IDS/IPS.

However, a preferred approach is to use this as an opportunity to validate the behavior of both the vulnerability scanner and IDS/IPS. By knowing that the vulnerability scanner should set off alarms on other security appliances, it is possible to predict the behavior of the IDS/IPS in response to the vulnerability scanner. Analyzing the behavior of both devices can serve as a check to ensure that they are operating properly.

Note 11

If you choose to have the IDS/IPS not ignore the vulnerability scanner, you should configure the IDS/IPS to record the predicted events but set them to a very low priority for generating alerts.

Access Approval Yet just as the scanner needs permissions to access the network, from another standpoint, an additional set of scanner permissions are also needed. These are permissions for a user to access and use the scanner itself. It is no surprise that a vulnerability scanner may uncover significant vulnerabilities, to the extent that if executed on a system not owned by the organization, it would allow the tester access to the system via uncovered vulnerabilities. This obviously raises serious legal and ethical issues. Testers using a vulnerability scanner should have permissions from internal supervisors to use the software, and this software should only be used to access approved systems.

Two Rights & A Wrong

1. Secure baseline scanning uses industry standards as comparison benchmarks to identify weaknesses.
2. Static device fingerprinting is the process of collecting information about a device's installed hardware and software configuration in order to create a unique identifier.
3. Vulnerability scanning software looks for the presence of a vulnerability by comparing software that is scanned against a set of known vulnerabilities, called signature-based monitoring.

See the answers at the end of the chapter.

Vulnerability Assessment Tools

Certification

2.1 Given a scenario, implement vulnerability scanning methods and concepts.

2.2 Given a scenario, analyze output from vulnerability assessment tools.

There are several different diagnostic tools that can be used to assess assets for vulnerabilities. These tools can be classified based on the asset that is being examined. These assets include infrastructures, networks, and software.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

The CompTIA CySA+ CS0-003 exam objectives state that a test-taker should be able to analyze the output from the vulnerability assessment tools listed in this section. Because of the number of tools, an in-depth evaluation of each tool and its output is not possible. It is important for those taking the CS0-003 exam to spend time becoming familiar with the different outputs.

Infrastructure

Although several tools are available for examining an infrastructure for vulnerabilities, there are two assessment tools that are usually recognized as being the most powerful. These include Nessus and OpenVAS.

Nessus

Nessus is one of the most popular and highly regarded infrastructure vulnerability scanning tools. Its advantages include:

- Nessus is an open-source vulnerability scanner that uses the Common Vulnerability Scoring System (CVSS).
- It has a modular architecture consisting of centralized servers that conduct scanning and remote client agents that interact with the servers.
- Nessus uses the Nessus Attack Scripting Language (NASL), which is a basic language that can be used for describing individual threats and potential attacks.
- It can detect security vulnerabilities in local or remote hosts and identify missing security updates and patches by simulating attacks to pinpoint vulnerabilities.
- Nessus is compatible with a variety of different computers and servers and supports Windows, macOS, Linux, and Unix.

The basic steps for installing and running a vulnerability scan on Nessus are:

- **Download Nessus software.** Nessus software consists of the vulnerability scanning manager Nessus Essentials (a free version for schools or hobbyists), Professional (for security practitioners), or Nessus Manager (an enterprise-based package for managing numerous Nessus Agents). An alternative is to use Tenable.io, which is a subscription-based cloud service that allows different teams to share scanners, schedules, scan policies, and scan results. Nessus Agents can also be downloaded to provide a flexible way of scanning hosts without the need to provide authentication, and the agents enable scans to be carried out even when the hosts are offline.

Note 12

Nessus can also be downloaded on a virtual machine.

- **Install Nessus.** By default, Nessus is installed and managed using the Hypertext Transfer Protocol Secure (HTTPS) and SSL through port 8834. It may be necessary to allow Nessus to operate through a firewall and any installed antivirus software product. Because the installation of Nessus uses a self-signed SSL certificate, a security warning of "Untrusted Site" or "Unsecure Connection" may appear in the installation web browser; these warnings can be dismissed.

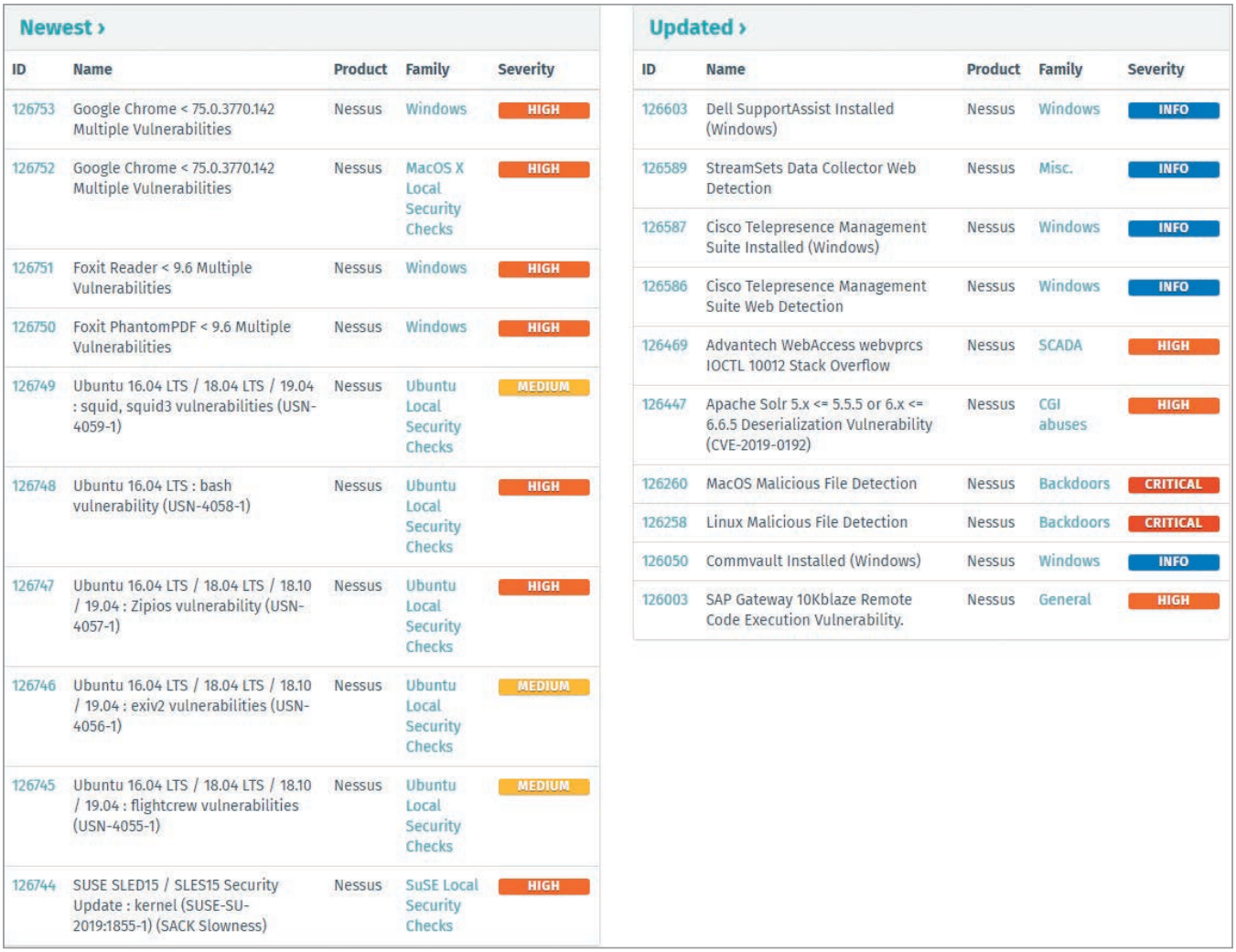
Caution

To avoid a warning about the self-signed Nessus SSL certificate, a customized SSL certificate specific to the organization can be created instead.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Download plugins.** As information about new vulnerabilities is discovered, programs to detect these vulnerabilities are created. These programs are called plugins and are written in NASL. The plugins contain vulnerability information, a simplified set of remediation actions, and the algorithm to test for the presence of the security issue. In addition to new plugins, updated plugins are also available, as shown in Figure 7-6.

Figure 7-6 Nessus plugins



Newest ›

ID	Name	Product	Family	Severity
126753	Google Chrome < 75.0.3770.142 Multiple Vulnerabilities	Nessus	Windows	HIGH
126752	Google Chrome < 75.0.3770.142 Multiple Vulnerabilities	Nessus	MacOS X Local Security Checks	HIGH
126751	Foxit Reader < 9.6 Multiple Vulnerabilities	Nessus	Windows	HIGH
126750	Foxit PhantomPDF < 9.6 Multiple Vulnerabilities	Nessus	Windows	HIGH
126749	Ubuntu 16.04 LTS / 18.04 LTS / 19.04 : squid, squid3 vulnerabilities (USN-4059-1)	Nessus	Ubuntu Local Security Checks	MEDIUM
126748	Ubuntu 16.04 LTS : bash vulnerability (USN-4058-1)	Nessus	Ubuntu Local Security Checks	HIGH
126747	Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : Zipios vulnerability (USN-4057-1)	Nessus	Ubuntu Local Security Checks	HIGH
126746	Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : exiv2 vulnerabilities (USN-4056-1)	Nessus	Ubuntu Local Security Checks	MEDIUM
126745	Ubuntu 16.04 LTS / 18.04 LTS / 18.10 / 19.04 : flightcrew vulnerabilities (USN-4055-1)	Nessus	Ubuntu Local Security Checks	MEDIUM
126744	SUSE SLED15 / SLES15 Security Update : kernel (SUSE-SU-2019:1855-1) (SACK Slowness)	Nessus	SuSE Local Security Checks	HIGH

Updated ›

ID	Name	Product	Family	Severity
126603	Dell SupportAssist Installed (Windows)	Nessus	Windows	INFO
126589	StreamSets Data Collector Web Detection	Nessus	Misc.	INFO
126587	Cisco Telepresence Management Suite Installed (Windows)	Nessus	Windows	INFO
126586	Cisco Telepresence Management Suite Web Detection	Nessus	Windows	INFO
126469	Advantech WebAccess webvprcs IOCTL 10012 Stack Overflow	Nessus	SCADA	HIGH
126447	Apache Solr 5.x <= 5.5.5 or 6.x <= 6.6.5 Deserialization Vulnerability (CVE-2019-0192)	Nessus	CGI abuses	HIGH
126260	MacOS Malicious File Detection	Nessus	Backdoors	CRITICAL
126258	Linux Malicious File Detection	Nessus	Backdoors	CRITICAL
126050	Commvault Installed (Windows)	Nessus	Windows	INFO
126003	SAP Gateway 10Kblaze Remote Code Execution Vulnerability.	Nessus	General	HIGH

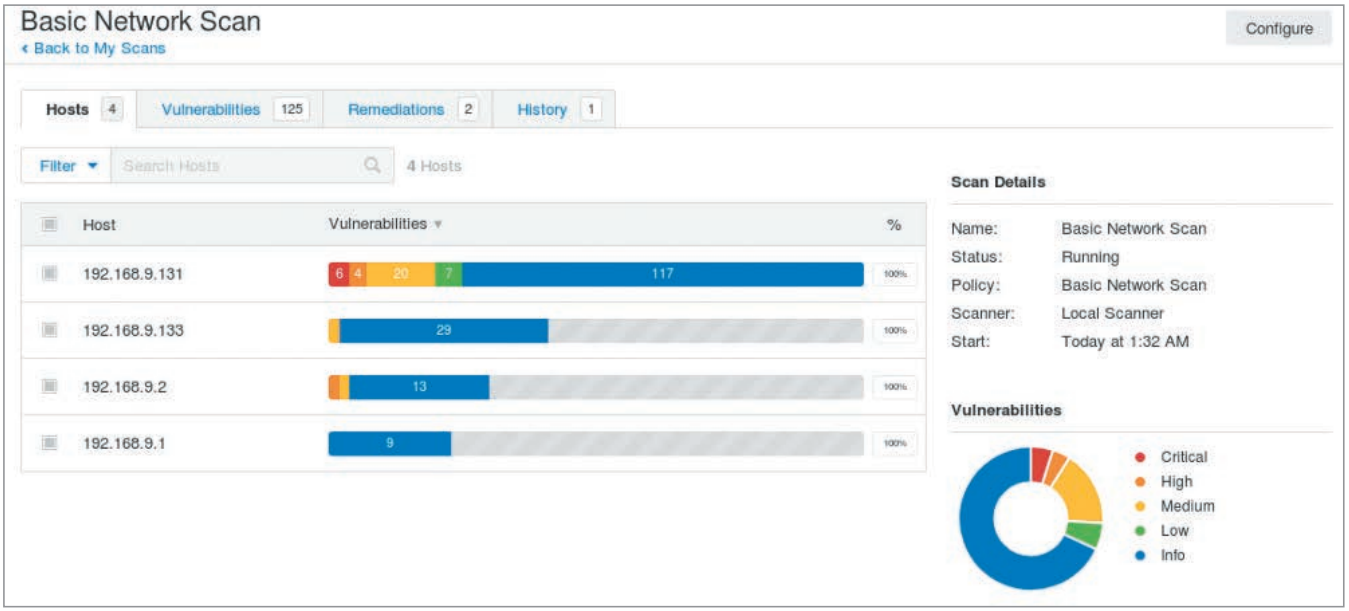
Source: Tenable

- **Select scan template.** Vulnerability scans can be facilitated by using Nessus scan templates, which are predefined scan configurations. There are currently over 20 different templates that cover different levels of scans (Advanced Scan, Basic Network Scan, Malware Scan, Mobile Device Scan, Web Application Tests), scans that meet regulatory requirements (Internal PCI Network Scan, PCI Quarterly External Scan, Policy Compliance Auditing, SCAP, and OVAL Auditing), scans that look for specific widespread vulnerabilities (Bash Shell-Shock Detection and Credentialed Patch Auditing), and scans that target the latest vulnerabilities (Shadow Brokers Scan, Spectre, and Meltdown Scan).
- **Determine scan settings.** Scan templates can be further tweaked by configuring specific scan settings, such as scheduling the scan frequency (Once, Daily, Weekly, Monthly, or Yearly), who is to be notified when the scan is completed and what report type is distributed, the scan type (Quick, Normal, Thorough, or Custom), the discovery methods (such as for Port Scanning for determining the port range to be scanned), and the accuracy of the scan, among other settings.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

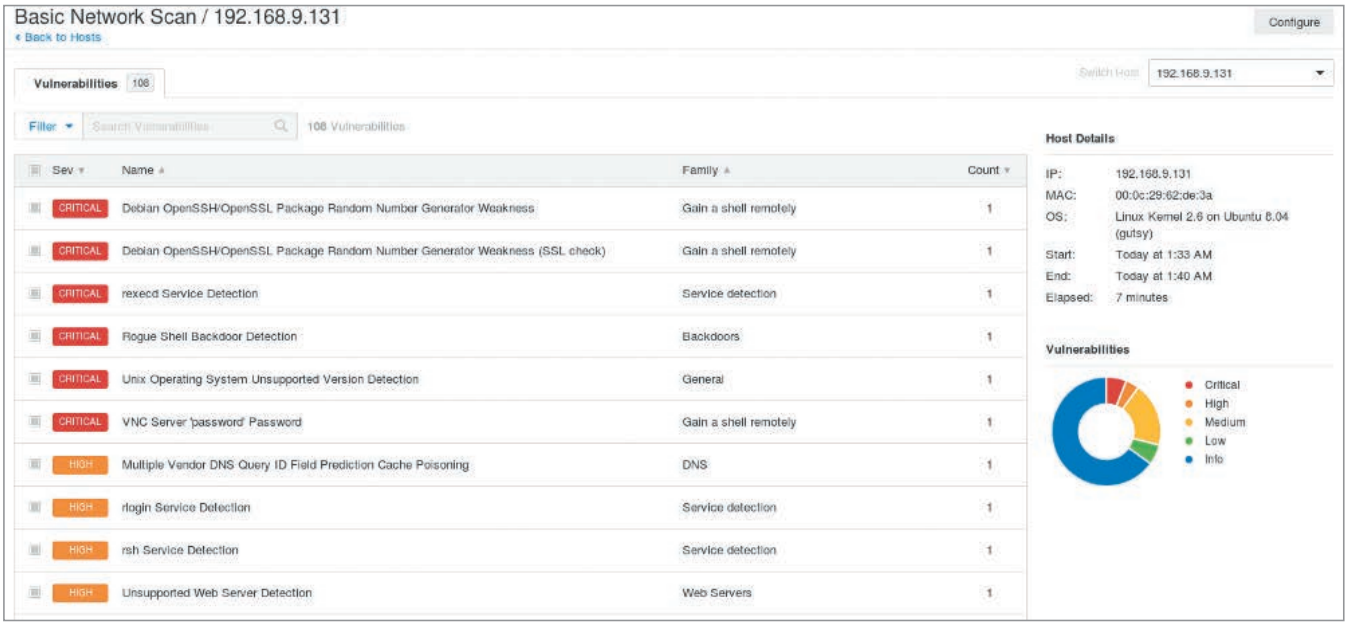
Once the scan is configured, it can then be executed. When the scan is finished, a summary dashboard is displayed as an overview of the results, as shown in Figure 7-7. A more detailed report on each of the vulnerabilities detected can also be viewed, as shown in Figure 7-8.

Figure 7-7 Nessus scan summary



Source: Tenable

Figure 7-8 Nessus scan details



Source: Tenable

Each vulnerability from the Nessus vulnerability scan can then be explored in greater detail by selecting that vulnerability. Figure 7-9 displays the details for a single vulnerability. The vulnerabilities details page displays a Description of the vulnerability and a Solution to the problem in the center pane. The right pane gives the Plugin Details such as its Severity, Version, and dates Published and Modified. It also contains an area called Risk Information.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-9 Nessus vulnerability details



Source: Tenable

OpenVAS

Open Vulnerability Assessment Scanner (**OpenVAS**) is considered a full-featured vulnerability scanner that currently includes over 50,000 vulnerability tests. It receives daily vulnerability feeds. Greenbone Networks has maintained OpenVAS since 2009 and serves as part of Greenbone's proprietary vulnerability management system. However, OpenVAS itself has been contributed as open source under the GNU General Public License (GNU GPL).

Other Infrastructure Scanners

There are other infrastructure vulnerability scanners that are popular. Nexpose is a well-known vulnerability scanner from Rapid7. A Nexpose Community Edition is a scaled-down version of Rapid7's more comprehensive vulnerability scanner. The Community Edition will run on physical machines under either Windows or Linux and is also available as a virtual appliance to run within a virtual machine. However, the Community Edition has several limitations: only a maximum of 32 IP addresses can be scanned, and it can only be used for 12 months.

The infrastructure vulnerability scanner Qualys can detect vulnerabilities on virtually any networked assets, including servers; network devices such as routers, switches, and firewalls; peripherals; and endpoints. Qualys can assess any device that has an IP address. It is unique in its delivery platform. Qualys is a cloud-based Software-as-a-Service (SaaS) delivery model, allowing users to access it from any web browser. For organizations that require an on-premise solution, a private cloud can be set up in the organization's own data center.

Networks

Diagnosing networks for vulnerabilities can be performed in one of two states: passive ("watching and listening" but not performing any overt actions against the network) or active (taking some type of action with the network or network server such as injecting packets). Two common tools are Angry IP scanner and Maltego.

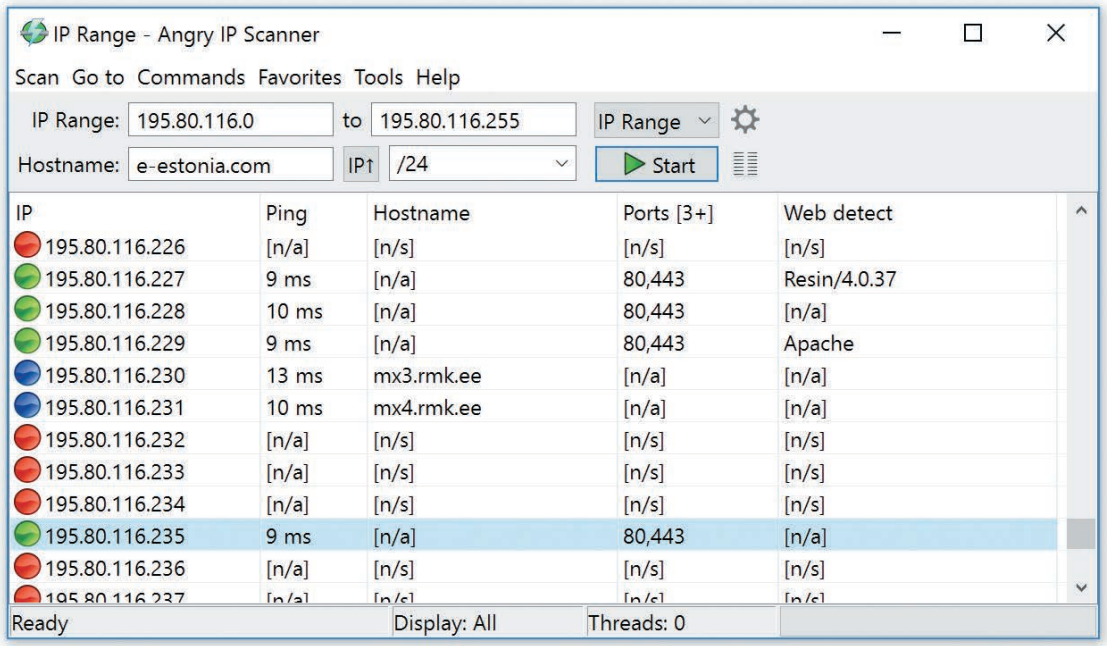
Angry IP Scanner

Angry IP scanner is primarily an IP address and port scanner. It can scan IP addresses in any range as well as any associated ports, determine if the system is active ("alive"), resolve hostnames, and identify if the IP address applies to a web server. Angry IP scanner output is seen in Figure 7-10.

There are also additional features as part of Angry IP scanner. These include the ability to retrieve NetBIOS information (computer name, workgroup name if utilized, and currently logged-in Windows user). There are additional plugins available, and users can write new plugins using Java.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-10 Angry IP scanner output



Angry IP scanner

Note 13

Angry IP scanner is cross-platform and runs on Linux, Windows, and macOS. It is also lightweight and can be run without requiring any installation. As an open-source product, it can be freely copied and used.

One of the primary features of Angry IP scanner is its speed. Angry IP "pings" each requested IP address. However, in order to increase scanning speed, it uses a multi-threaded approach in which a separate scanning thread is created for each scanned IP address.

Maltego

Maltego is an open-source network mapping tool that can be used to fingerprint an entire network infrastructure beginning from a single domain name. It builds a comprehensive visual overview of "data points" by pulling data from dispersed sources, then mapping the data relationships into a visual graph. These graphs can range from basic, as seen in Figure 7-11, to sophisticated, as illustrated in Figure 7-12. This can help identify patterns and connections that may otherwise go unnoticed.

Note 14

Because Maltego is a Java application, it is platform agnostic and can run on any OS platform.

There are three basic steps when using Maltego:

1. **Mine.** The mine step gathers data from dispersed data sources. Up to 1 million entities can be viewed on a single Maltego graph.
2. **Merge.** Merging data involves automatically linking and combining all mined data into a single graph. Algorithms can automatically detect different entity types.
3. **Map.** Once the data has been mined and merged, a visual map can be created. There are a variety of different graphical layouts that can be used to create a map, such as block, hierarchical, circular, and organic. Weights of different entity types can be used to help detect patterns in large graphs.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-11 Basic Maltego graph

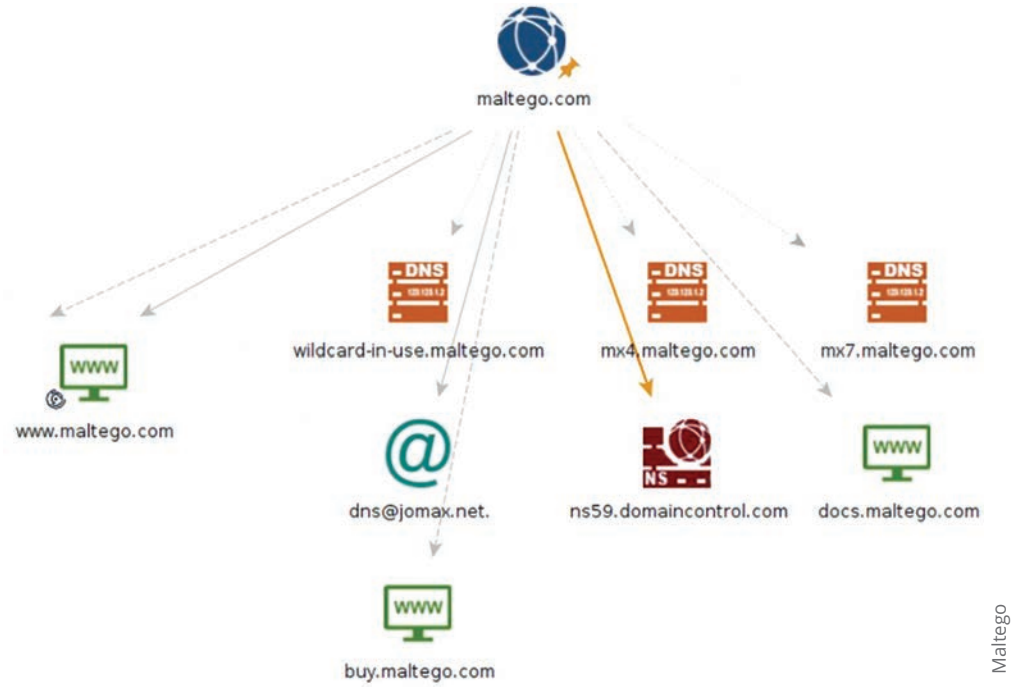
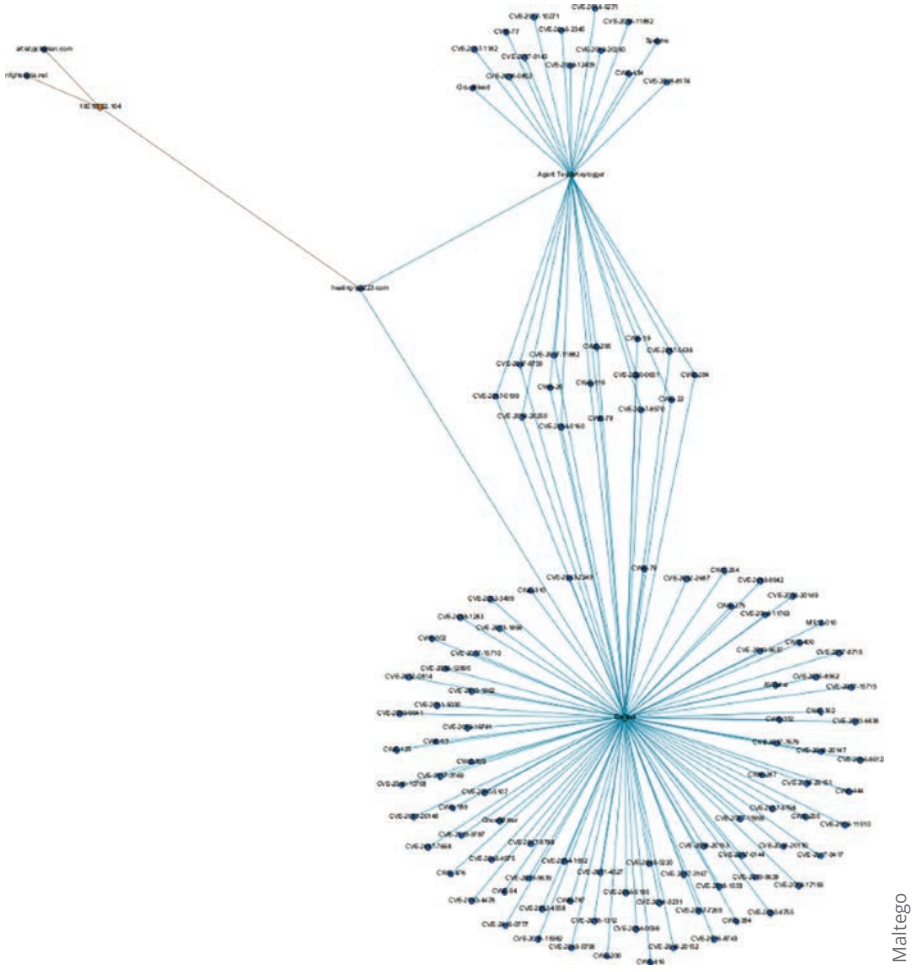


Figure 7-12 Sophisticated Maltego graph



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 15

Maltego is not just for security professionals. It is often used by a broad range of users, ranging from forensic investigators to investigative journalists and researchers.

Although a very powerful tool, Maltego can be overwhelming for beginners. It is not uncommon for a single page of one map to generate 40 pages of explanation. And mastering Maltego can take an extended period of time and effort.

Software

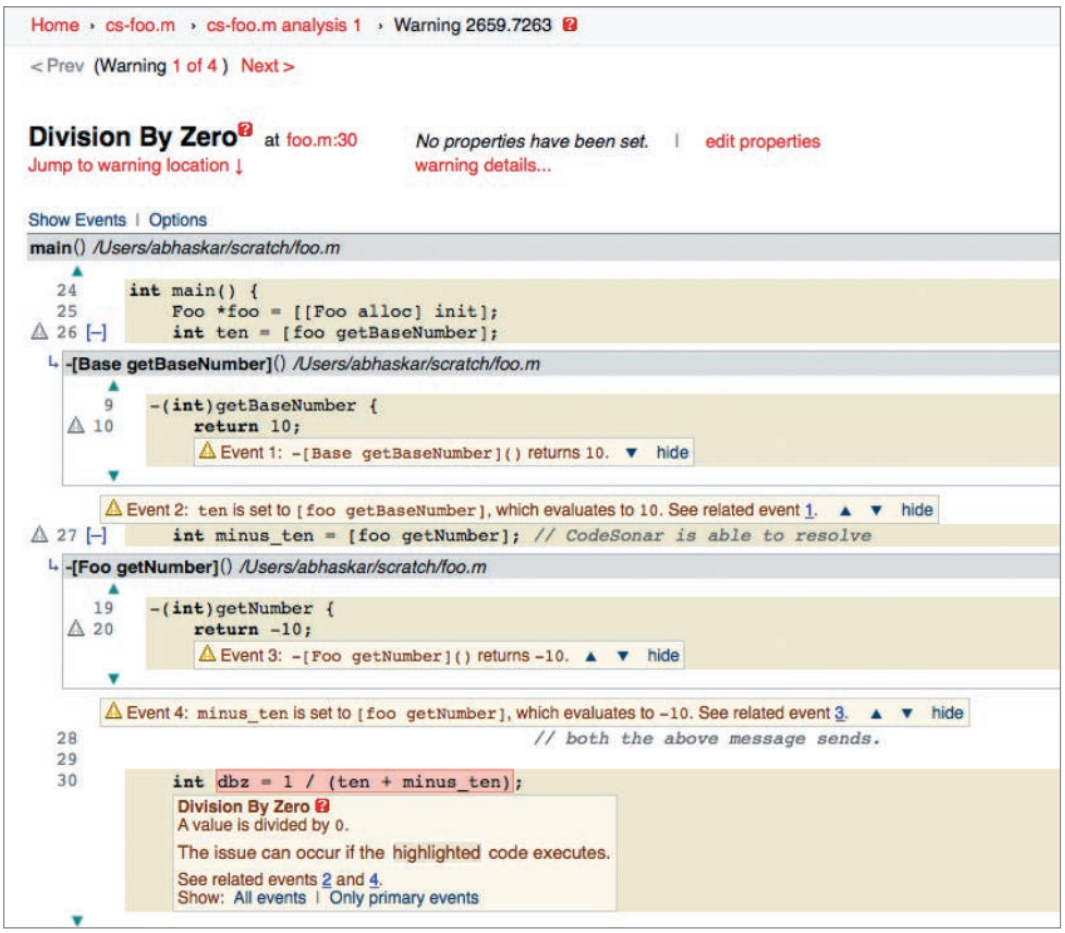
Examining software for unintentional vulnerabilities has long been considered important. However, today software and "apps" are also being examined for intentional malware. While at one time commercial software packages were considered as untainted by malware because they were written by trusted software engineers, that is no longer the case. Increasingly, software programs are being developed by nation-state actors and other threat actors so that the software appears benign but actually contains malware.

There are two types of software analysis for vulnerabilities and malware. These are static analysis and dynamic analysis.

Static Analysis

Typically, the software development process involves software engineers writing source code using a programming language that is then compiled into binary machine code. When looking for vulnerabilities, the testing of the software should occur before the source code is compiled. These tests are called **static analysis**. Figure 7-13 illustrates an automated static code analysis tool.

Figure 7-13 Automated static code analysis tool



Source: GrammaTech

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 16

Automated static code analysis may also be accompanied by manual peer reviews in which the software engineers and developers, paired together or in larger teams, laboriously examine each line of source code looking for vulnerabilities.

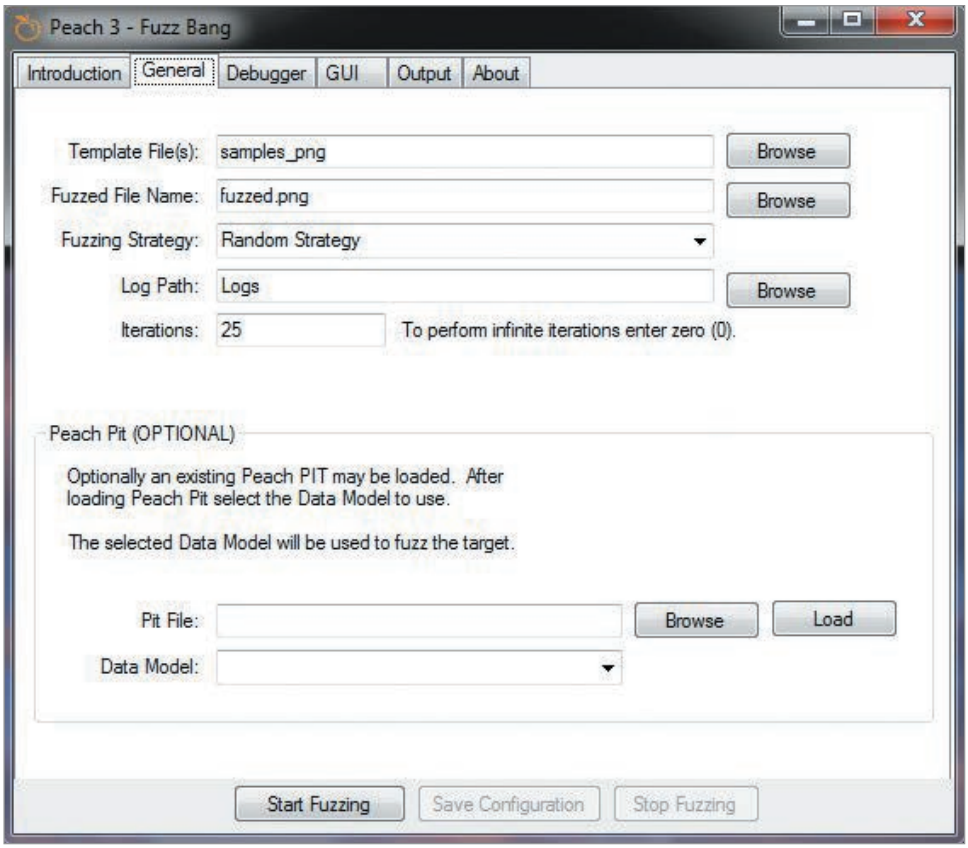
Dynamic Analysis

Security testing can also be performed after the source code is compiled, although it is more difficult to find flaws. This is called **dynamic analysis** or run-time verification when all components are integrated and running. This analysis is typically achieved using a tool or suite of prebuilt attacks or testing tools that specifically monitor the application's behavior for memory corruption, user privilege issues, and other critical security problems.

Common dynamic analysis tools are those that perform fuzzing, reverse engineering, and debugging.

Fuzzing Some of the most common dynamic code analysis tools use a process called **fuzzing**. Fuzzing provides random input to a program to attempt to trigger exceptions, such as memory corruption, program crashes, or security issues. An advantage of fuzzing is it produces a record of what input triggered the exception so that it can be reproduced in order to track down the problem within the code. Fuzzing test software consists of an execution engine and an input generator, which usually allows the tester to configure the types of inputs. This is seen in Figure 7-14.

Figure 7-14 Fuzzer input generator



Source: Déjà vu Software

Note 17

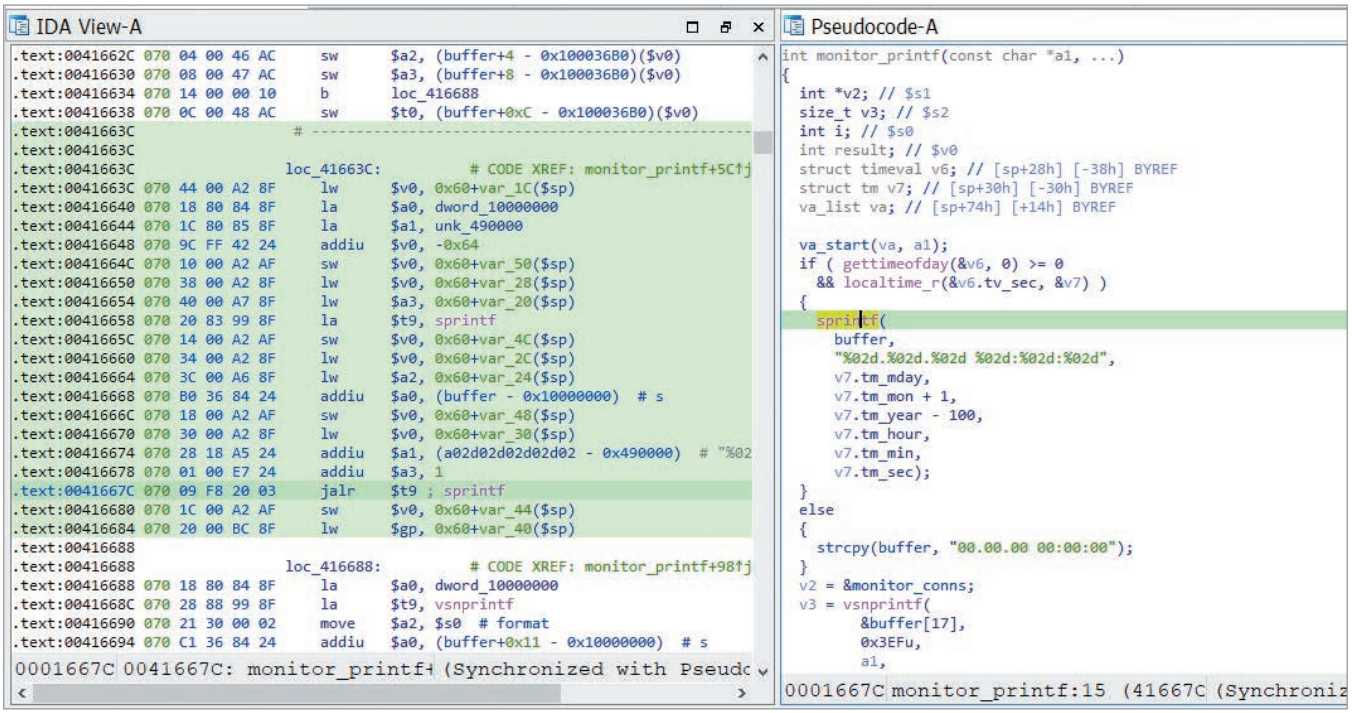
A single pass of a fuzzer is unlikely to find all exceptions in software, due to the randomness in the fuzzing process. This is because the mutation of the inputs relies on randomness to determine where to mutate input and what to mutate. Fuzzers require multiple trials and statistical tests.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Reverse Engineering How can an organization that has purchased or leased software examine the compiled code to determine if it contains malware? In this case, dynamic analysis can also be used. Instead of relying on a suite of prebuilt attack tools to look for vulnerabilities, **reverse engineering** can be performed. Reverse engineering is disassembling and analyzing a product. A common usage of reverse engineering is to facilitate the maintenance associated with a software program by better understanding how the underlying code functions. Software reverse engineering is often used in cybersecurity to analyze malware to determine how the code works and what its intentions are.

Software tools are available to reverse-engineer or transform compiled binary code into a text form. A disassembler maps processor instruction codes into instruction mnemonics on a one-to-one basis. A decompiler can also create text from binary code but the code is at a much higher level and is more concise and easier to analyze. Figure 7-15 illustrates the output from a decompiler that converts compiled binary code in the left pane to a more readable "pseudocode" in the right pane.

Figure 7-15 Decompiler output



Debugging A **debugger** is a tool that can be used for not only tracing the flow of a program but also for altering its execution. Debuggers can monitor the program's functions and then modify the values of the internal variables, and it can even call functions independently that are not part of the program's regular behavior. Two common ones are Immunity Debugger and GNU Debugger.

Immunity Debugger **Immunity Debugger** is a tool that is often used to analyze malware. However, it can also reverse-engineer compiled binary files so that new exploits can be created.

Note 18

Immunity Debugger boasts that it "cuts exploit development by 50 percent" and has connectivity to "exploit development tools."

Immunity Debugger includes both a graphical user interface (GUI) and a command-line interface (CLI). Python commands can even be run directly from the CLI. It can create a standard analysis of the actions of a program. Figure 7-16 traces variable sizes and how they are used in a program and can also allow users to modify the contents of variables. Another feature is the ability to provide a graph that shows the interactions of selected functions. This is illustrated in Figure 7-17.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 7-16 Variable usage in Immunity Debugger

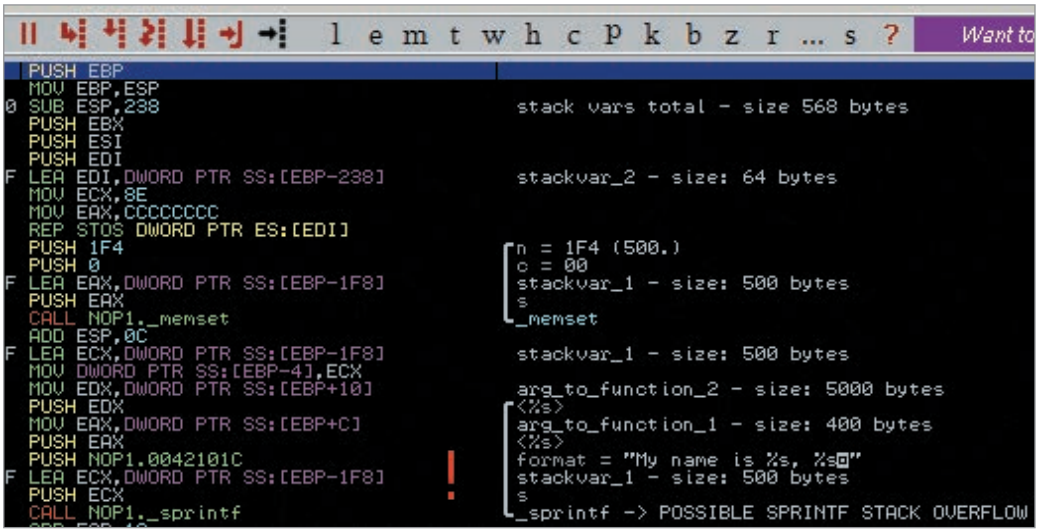
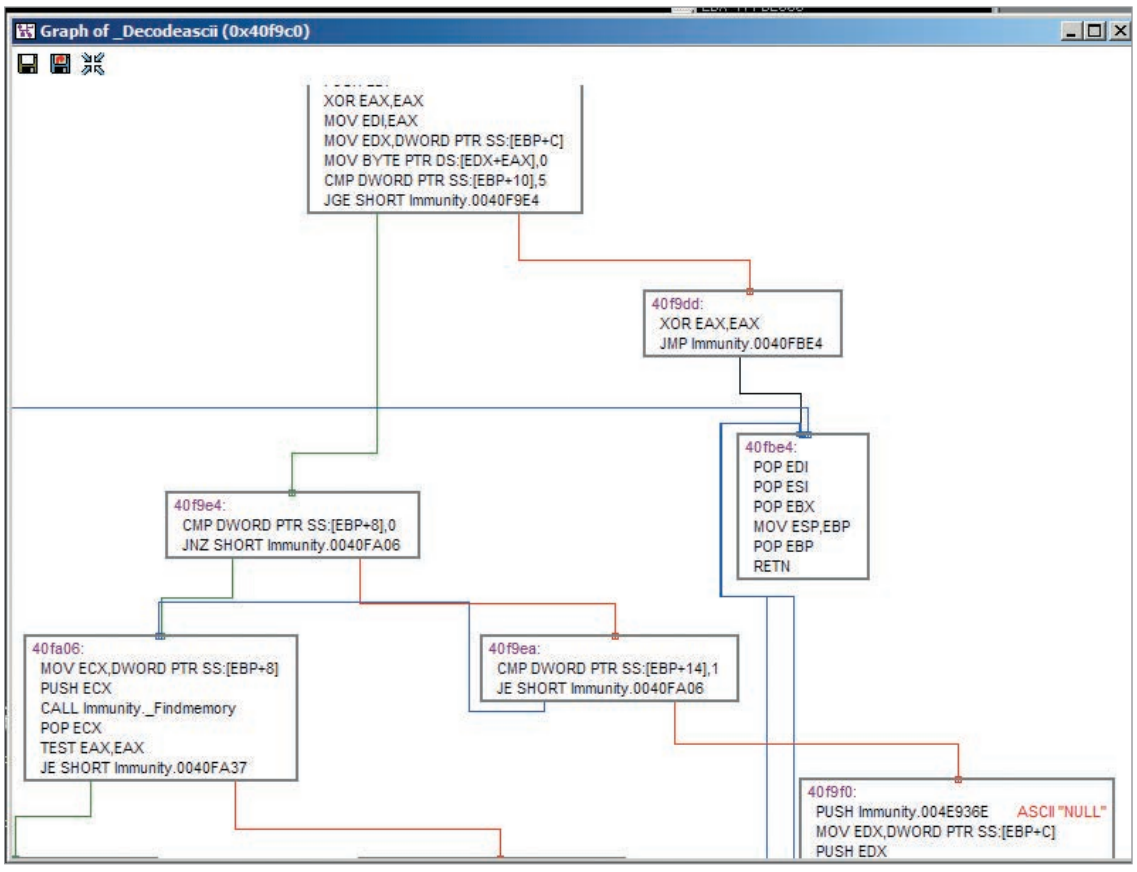


Figure 7-17 Immunity Debugger graph of functions



Most debuggers offer only one method to attach to a process that is generated by the application, usually by either the process identifier (PID) or the process name. Using Immunity Debugger, a process can be attached through the PID or process name but also through services within that process, TCP/UDP ports that the process is listening on, complete binary name, and window name. This allows very quick and easy access to the exact process to be analyzed and manipulated.

GNU Debugger

GNU Debugger (GDB) can debug several different programming languages, including Assembly, C, C++, Go, and Rust. It runs on many Unix-like systems as a CLI. Although it has no GUI, it does have a text user interface (TUI).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 19

GDB was first written back in 1986.

GDB uses a system call known as process trace (ptrace). Through this, it can observe and control the execution of another process. It can also view and change the process's memory and registers.

Two Rights & A Wrong

1. Nessus provides predefined scan configurations.
2. Maltego is an open-source network mapping tool that can be used to fingerprint an entire network infrastructure beginning from a single domain name.
3. Debugging is a static analysis of software.

See the answers at the end of the chapter.

Summary

- Vulnerability management, also called infrastructure risk visibility and assurance, is an ongoing examination of an organization's security. At the heart of vulnerability management is identifying vulnerabilities so that they can then be addressed. A vulnerability scan is a frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress. Unlike a penetration test, which is a single event using a manual process that is often performed only to comply with regulatory requirements, a vulnerability assessment is a cyclical and continual process of ongoing scanning and continuous monitoring to reduce the attack. There are several reasons for conducting a vulnerability scan besides providing continuous monitoring. These include meeting regulatory requirements and following corporate policies. Despite its importance, there are several challenges that are associated with vulnerability scanning.
- An industry framework is a set of designs for businesses in a specific industry based on consensus from industry representatives. There are several industry frameworks that can facilitate overall vulnerability management and specific vulnerability scanning. These can assist in defining policies and procedures for implementing and managing security controls in an enterprise environment as they relate to vulnerability management. These frameworks include the Payment Card Industry Data Security Standard (PCI DSS), the Open Web Application Security Project (OWASP), Center for Internet Security (CIS) benchmarks, and the International Organization for Standardization (ISO) 27000 series.
- There are several different procedures when running a vulnerability scan. A set of decisions must be made prior to conducting a scan if it is to be impactful. One of the first decisions before conducting a scan is to determine what should be scanned. Critical infrastructure components should always be scanned. Beyond critical infrastructure components, decisions must often be made about which assets should be included in a vulnerability scan. This is because not all assets have the same value; some assets are critical while others can be of lessor importance. Identifying assets, called asset discovery, to be included in a scan is an important step in determining what should be scanned. Most vulnerability scanning tools allow for an asset discovery inventory scan that only searches for devices attached to the network. Device fingerprinting is the process of collecting information about a device's installed hardware and software configuration in order to create a unique identifier. A growing trend in digital fingerprinting is to not just fingerprint the static characteristics of a device but also consider the dynamic usage of a device.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- Another scanning decision involves how the assets should be scanned. Active scanning sends test traffic transmissions into the network and monitors the responses of the endpoints. Passive scanning, on the other hand, does not send any transmissions but instead only listens for normal traffic to learn the needed information. An advantage of active scanning over passive scanning is that active scanning can accelerate the collection of the data; it is not necessary to wait for normal network traffic to or from each asset to generate a complete profile of information. Also, not all parts of a network may always be available, which can limit the ability to passively monitor traffic.
- An internal vulnerability scan is performed from the vantage point inside the internal network; that is, it is launched and then conducted from inside the corporate network. An internal vulnerability scan typically has the primary benefit of identifying at-risk systems. An external vulnerability scan is performed from the vantage point outside the network. It targets specific IP addresses that are within the network to identify vulnerabilities. An external scan can also detect open ports and protocols. Attempting to run a vulnerability scan on a very large network in a single scan job is generally not advisable. This is because vulnerability scans can consume large amounts of system resources and reduce overall system response time. The best practice when running a vulnerability network on a large network is to divide it into smaller sections, called segmentation, for the purpose of the scan.
- Another consideration is when and how frequently a vulnerability scan should be conducted. The optimum frequency for vulnerability scanning is continual—all systems are scanned all the time. However, there are different constraints that call for scanning on a routine basis instead of continuously. The regular interval when vulnerability scans are conducted will vary between each organization due to a variety of factors. Generally, scan schedules can be set to specific intervals by the hour, day, week, or month.
- Before running a vulnerability scan, it is important that the software be updated. Many vulnerability scan products are modular in nature instead of a single enormous software package. These module updates, known as plugins, can be downloaded and installed as needed. Vulnerability scanning software looks for the presence of a vulnerability by comparing software that is scanned against a set of known vulnerabilities. Various vulnerability feeds provide a set of vulnerability data to vulnerability scan software.
- Configuring vulnerability scan software involves setting specific parameters so that the scan meets the intended objective. The scope of a vulnerability scan is the target devices to be scanned. The sensitivity level is the depth of a scan. Another configuration setting specifies the data types to be scanned.
- When executing the scan, there are different scanner options that can impact running the scan. A credentialed scan is a scan for which valid authentication credentials are supplied to the vulnerability scanner to mimic the work of a threat actor who possesses these credentials, while a noncredentialed scan provides no such authentication information. There are two means by which devices interact with a vulnerability scanner. A software agent is a package deployed to each device that needs to be scanned. Once installed, the agent collects data that indicates whether the device may have vulnerabilities. Agentless scanning does not require agents to be installed on each device; instead, the server "reaches out" to each asset. There are also other considerations that need to be addressed when running a vulnerability scan. These include scanner permissions, network appliance configurations, and access approval.
- There are several different diagnostic tools that can be used to assess assets for vulnerabilities. These tools can be classified based on the asset that is being examined. When examining an infrastructure for vulnerabilities, Nessus is one of the most popular and highly regarded infrastructure vulnerability scanning tools. Open Vulnerability Assessment Scanner (OpenVAS) is considered a full-featured vulnerability scanner. There are other infrastructure vulnerability scanners that are popular.
- Diagnosing networks for vulnerabilities can be performed in one of two states: passive, which is watching and listening but not performing any overt actions against the network, or active, which is taking some type of action against the network or network server such as injecting packets. Angry IP scanner is primarily a network IP address and port scanner. Maltego is an open-source network mapping tool that can be used to fingerprint an entire network infrastructure beginning from a single domain name. It builds a comprehensive visual overview of all data points by pulling data from dispersed sources then mapping the data relationships into a visual graph.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- There are two types of software analysis for vulnerabilities and malware. Static analysis examines the program code itself for vulnerabilities. Dynamic analysis (run-time verification) involves viewing all components while the program is being executed. This analysis is typically achieved using a tool or suite of prebuilt attacks or testing tools that specifically monitor the application's behavior for memory corruption, user privilege issues, and other critical security problems. Some of the most common dynamic code analysis tools use a process called fuzzing. Fuzzing provides random input to a program to attempt to trigger exceptions, such as memory corruption, program crashes, or security issues. Instead of relying on a suite of prebuilt attack tools to look for vulnerabilities, reverse engineering, which is disassembling and analyzing a product, can be used. A debugger is a tool that can be used for not only tracing the flow of a program but also for altering its execution. Debuggers can monitor the program's functions and then modify the values of the internal variables, and it can even call functions independently that are not part of the program's regular behavior.

Key Terms

active scanning
agent
agentless
Angry IP scanner
asset discovery
Center for Internet Security (CIS)
credentialed scan
debugger
device fingerprinting
dynamic analysis
external vulnerability scan
fuzzing
GNU Debugger (GDB)
Immunity Debugger
industry framework
internal vulnerability scan
International Organization for Standardization (ISO) 27000
Maltego
map scans
Nessus
noncredentialed scan
Open Worldwide Application Security Project (OWASP)
OpenVAS
operations
passive scanning
Payment Card Industry Data Security Standard (PCI DSS)
performance
regulatory requirements
reverse engineering
scheduling
secure baseline scanning
segmentation
sensitivity level
static analysis
vulnerability management
vulnerability scan

Review Questions

1. Which of the following vulnerability scanning tools is open source?
   a. Qualys
   b. OpenVAS
   c. Nexpose
   d. Nessus
2. Which parameter in a vulnerability scan specifies the devices that need to be included in the scan?
   a. Sensitivity level
   b. Data type
   c. Scope
   d. Segment
3. Which of the following do plugins NOT contain?
   a. Advanced vulnerability information
   b. A listing of vulnerable local IP addresses
   c. Remediation actions
   d. Updated algorithms
4. How can the impact of a vulnerability scan on operations be mitigated?
   a. Perform the scans at night.
   b. Alternate the scans so they run every other hour.
   c. Execute scans after completing a pen test.
   d. It is not possible to mitigate the impact on operations.
5. Which of the following is NOT a regulatory compliance regulation that requires a vulnerability scan?
   a. Payment Card Industry Data Security Standard (PCI DSS)
   b. Federal Information Security Management Act (FISMA)
   c. Federal Education Rights and Privacy Act (FERPA)
   d. Health Insurance Portability and Accountability Act (HIPAA)

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

6. Which of the following does NOT apply to a vulnerability scan?
   a. Identify vulnerabilities by scanning systems and networks.
   b. Scan to find weaknesses and then mitigate.
   c. Use automated processes with a handful of manual processes.
   d. Act like a threat actor to find vulnerabilities to exploit.
7. Which of the following is NOT a question that vulnerability management seeks to answer?
   a. "How do we compare with our peers?"
   b. "How did we reduce our exposure over time?"
   c. "What should we prioritize?"
   d. "Where are we exposed?"
8. Which of the following applies to a vulnerability scan?
   a. Identify deep vulnerabilities.
   b. Act like a threat agent to find vulnerabilities to exploit.
   c. Reduce attack surface.
   d. Gain unauthorized access and exploit vulnerabilities.
9. Which of the following is NOT a challenge associated with vulnerability scanning?
   a. Remediations
   b. Complying with industry frameworks
   c. Identification of vulnerabilities
   d. Large volume of generated data
10. Which of the following provides an overview of ISMS?
    a. PCI DSS
    b. OWASP VMG
    c. CIS
    d. ISO 27000
11. Which of the following uses specific security frameworks as comparison benchmarks to identify weaknesses?
    a. Secure baseline scanning
    b. OWPSA
    c. Standardized framework analysis (SFA)
    d. Hybrid comparison testing
12. Which of the following should always be included in a vulnerability scan?
    a. User devices
    b. Remote networks
    c. XS
    d. OT
13. Which of the following is NOT true about device fingerprinting?
    a. Attributes used can include the device's OS version, screen resolution, installed fonts, browser plugins, and time zone.
    b. A common fingerprint is created for groups of like devices.
    c. Device fingerprinting can be beneficial when performing an asset discovery for a vulnerability scan.
    d. Static device fingerprinting is the process of collecting information about a device's installed hardware and software configuration.
14. Which type of scanning sends test traffic transmissions into the network and then monitors the response of endpoints?
    a. Passive scanning
    b. Network monitoring
    c. Active scanning
    d. Remote scanning
15. Which type of vulnerability scan is similar to a pen test?
    a. External vulnerability scan
    b. Internal vulnerability scan
    c. Passive vulnerability scan
    d. Compressed vulnerability scan
16. Which parameter in a vulnerability scan represents the depth of the scan?
    a. Scope
    b. Data type
    c. Sensitivity level
    d. X-scan
17. Which type of vulnerability scan is appropriate for environments in which there are widely distributed remote employees?
    a. Remote scanning
    b. Network scanning
    c. Scanning using agents
    d. Agentless scanning
18. Which of the following is primarily an IP address and port scanner?
    a. Maltego
    b. Angry IP scanner
    c. OWSAP
    d. CIS scanner
19. Which tool is used to provide random input to a program to attempt to trigger exceptions, such as memory corruption, program crashes, or security issues?
    a. Debugging
    b. Fuzzing
    c. Reverse engineering
    d. Decompiling
20. Which tool can debug several different programming languages?
    a. GNU Debugger (GDB)
    b. Immunity Debugger
    c. Ptrace Debugger
    d. Malto Debugger

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Projects

Case Project 7-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. How can complacency be combated in the context of cybersecurity? Should there be standards mandated for testing software before it is released to the public? How should the standards be enforced? Write a one-page paper about this.

Case Project 7-2: Vulnerability Feed

Estimated Time: 25 minutes
Objective: Research vulnerability feeds.
Description: Visit the website abuse.ch and research the different features that are available for a vulnerability feed. How up to date does the information appear to be? How many malware instances have been submitted? What strengths are there of this feed? What weaknesses exist? And how could a threat actor use this site? Write a one-page paper on your research.

Case Project 7-3: Nessus

Estimated Time: 20 minutes
Objective: Summarize the features of the Nessus vulnerability scanner.
Description: Perhaps the best-known and most widely used vulnerability scanner is Nessus, which contains a wide array of prebuilt templates. Nessus advertises that new plugins are available as soon as 24 hours after a new vulnerability is disclosed. Visit the Nessus website at www.tenable.com/products/nessus and read the information on Nessus. Write a one-page paper on your research about Nessus. You can also download the free Nessus Essentials software and run a vulnerability scan on a maximum of 16 IP addresses.

Case Project 7-4: Scanning Decisions

Estimated Time: 25 minutes
Objective: Decide which scanning options to use.
Description: Identify a network at your school or business or a personal network to evaluate and develop the scanning decisions if you were to perform a vulnerability scan on it. Include what should be scanned (data classification, asset criticality, and network segmentation), how it should be scanned (active vs. passive and internal vs. external), and when it should be scanned. For each of these have a justification as to why you made this decision and the weakness of the alternative. Create a one-page paper on your scanning decisions.

Case Project 7-5: Open Worldwide Application Security Project Vulnerability Management Guide

Estimated Time: 25 minutes
Objective: Research OWASP VMG.
Description: Use the Internet to research OWASP VMG. How is it used? What are its advantages and disadvantages? Would you recommend it? Write a one-page paper on your findings.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong: Answers

Vulnerability Scanning

1. A vulnerability scan is a frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress.
2. A challenge of a vulnerability scan is the low volume of data that a scan produces.
3. The PCI DSS, OWASP, CIS, and ISO all provide vulnerability management frameworks.

Answer: The wrong statement is #2.
Explanation: Vulnerability scans can produce large amounts of data that must be analyzed.

Vulnerability Scanning Methodologies

1. Secure baseline scanning uses industry standards as comparison benchmarks to identify weaknesses.
2. Static device fingerprinting is the process of collecting information about a device's installed hardware and software configuration in order to create a unique identifier.
3. Vulnerability scanning software looks for the presence of a vulnerability by comparing software that is scanned against a set of known vulnerabilities, called signature-based monitoring.

Answer: The wrong statement is #1.
Explanation: Secure baseline scanning uses specific security frameworks as comparison benchmarks to identify weaknesses.

Vulnerability Assessment Tools

1. Nessus provides predefined scan configurations.
2. Maltego is an open-source network mapping tool that can be used to fingerprint an entire network infrastructure beginning from a single domain name.
3. Debugging is a static analysis of software.

Answer: The wrong statement is #3.
Explanation: Debugging is a dynamic analysis of software.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 8

Addressing Vulnerabilities

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Apply vulnerability scans
2. Prioritize vulnerabilities
3. Document ways to manage vulnerabilities

#TrendingCyber

"Possibly the most advanced exploit ever," "This is no ordinary vulnerability," "Definitely the most sophisticated attack chain we've ever seen." These are all statements from security researchers who uncovered an exploit that was using not one but four software zero-day vulnerabilities along with what some are calling an unprecedented hardware zero-day vulnerability. This exploit was active for over four years and even after one year of intense investigation there are still a host of unanswered questions surrounding it.

A mass backdoor campaign, called Triangulation, infected the Apple iPhones of thousands of people working inside diplomatic missions and embassies in Russia, according to the cybersecurity company Kaspersky. The infections were delivered in iMessage texts that installed malware through a complex exploit chain that did not require the user of the device to perform any action. The malware was "full-featured spyware" that, among other things, secretly turned on the iPhone's microphone to record conversations and then sent them along with photos, geolocations, and other sensitive data back to command-and-control (C&C) servers.

There were at least three key features that made Triangulation an off-the-charts exploit in the eyes of security researchers.

First, Triangulation made use of not one but four software zero-day vulnerabilities. A zero-day vulnerability is one in which the threat actors know it exists but nobody else knows. So called because there are zero days of warning, it is considered extremely serious because systems are open to attack with no knowledge that the attack is occurring, plus there are no security fixes currently available. While malware using just one zero-day vulnerability is relatively rare, an attack using four zero-day vulnerabilities is almost unprecedented.

Second, not only were four software zero-day vulnerabilities exploited but also a previously unknown hardware feature was also used. Apple devices are equipped with protection so that threat actors cannot inject malicious code into other processes, modify kernel code, or access sensitive kernel data. These protections are so strong they have rarely been defeated. However, Triangulation bypassed the protections by using an unknown function not in software but in the hardware central processing unit (CPU) chip itself.

Hardware registers, which provide memory addresses for CPUs to interact with peripheral components such as Universal Serial Buses (USBs) and memory controllers, support memory-mapped input/outputs (MMIOs) that allow the CPU to write to the specific hardware register of a peripheral device. Security researchers found that the attackers

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

used several MMIO addresses to bypass the memory protections in place. Yet these functions were not identified in any device tree, which is a machine-readable description of a particular set of hardware used for reverse engineering. Even after the researchers scoured source codes, kernel images, and firmware, they were still unable to find any documentation regarding the MMIO addresses. Thus, Triangulation relied on a previously unknown hardware function that some are calling a hardware zero-day vulnerability.

Finally, the sophistication of the chain of steps that Triangulation used was "impressive." It all started with attackers sending a malicious iMessage attachment, which is immediately processed by the iPhone without showing any signs to the user. The iMessage attachment exploited a software zero-day vulnerability based on an undocumented Apple instruction used since the early 1990s. The malware then executed a privilege escalation exploit (written in 11,000 lines of JavaScript code so obfuscated it was almost completely unreadable) that exploited a debugging feature using application programming interface (API) functions. It also used an integer overflow vulnerability to attain read/write access to all physical memory of the device from the user level. After exploiting these vulnerabilities, the JavaScript exploit could do whatever it wanted to on the device—and keep doing it. Although an infected device could be cleared of the malware when the device was rebooted, the attackers kept their campaign alive simply by sending devices a new malicious text shortly after they were restarted that then relaunched the infection all over again.

One of the features of Triangulation that has received the most attention is the secret hardware function. Some have speculated that this is a flaw in the hardware design that was not discovered and somehow made its way into the chip itself (unlikely). Conspiracy theorists have said that secret government agents working in production facilities that manufacture Apple devices could have taken the CPU chip, altered it, and then put their new vulnerable chip in Apple devices when they were manufactured (highly unlikely). Others have more rationally suggested that the function is likely a debug and testing mechanism used by Apple engineers that allows them to directly write to a cache memory location using hardware debug registers instead of to the memory itself, and inexplicably this function was left in the CPU when it should have been removed (more likely).

In any event, the question remains of how threat actors were able to discover and exploit this hardware feature. Was it an obscure disclosure by Apple about firmware or source code that the attackers learned about (although security researchers cannot find any of these disclosures)? Did threat actors simply stumble upon it through hardware reverse engineering? Or was there some other means they used? The security researchers concluded, "We have no idea how attackers would know how to use it."

Despite the fact that the four zero-day software vulnerabilities impacted a wide range of Apple devices besides iPhones (including Macs, iPods, iPads, Apple TVs, and Apple Watches), users do not have to fear that their devices will be (or already are) the next victims. All of these vulnerabilities have been addressed (CVE-2023-42434, CVE-2023-32435, CVE-2023-39606, and CVE-2023-419900) through patches distributed by Apple.

Who was behind Triangulation? Nobody knows, but the level of sophistication clearly indicates that nation-state attackers are the most likely culprits.

Triangulation highlights the fact that zero-day vulnerabilities, whether in software or hardware, can be frightening.

Suppose a major windstorm were to blow through a residential area. Once the storm had passed, the homeowner would likely step outside and perform three tasks. First, the homeowner would do a quick analysis of any damage to the home. Second, they would prioritize any damage so that the most serious would be addressed first. For example, if shingles were missing and other damage had been done to the roof, it is more important for the roof to be immediately repaired than to pick up downed tree limbs in the backyard. Finally, once the repairs were made, the homeowner would likely take steps to prevent future damage from the next storm, such as enhancing the roof deck attachment and locking down the roof edges.

These same three basic steps—analyze, prioritize, and fortify—are similar steps that are taken by cybersecurity professionals following a vulnerability scan. Once decisions are made concerning a vulnerability scan (what should be scanned, how it should be scanned, and when the scan should occur) and the scan is then conducted using vulnerability assessment tools, the next steps are to analyze the scan, prioritize discovered vulnerabilities, and then fortify to further protect assets against future attacks.

In this chapter you explore addressing vulnerabilities through analyzing, prioritizing, and fortifying.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Analyzing Vulnerability Scans

Certification

2.3 Given a scenario, analyze data to prioritize vulnerabilities.

It would be a mistake to accept the results of a vulnerability scan at face value. Instead, it is important for the scan to be analyzed to determine if the results may have mitigating circumstances that should be considered. Analyzing a scan involves performing validation, examining the context, and exploring other factors.

Validation

When examining results of a vulnerability scan, it is important to validate its results for accuracy. Has the vulnerability scan identified genuine vulnerabilities and not missed any? If the scan were 100 percent accurate, then the organization would know that a future attack would accurately trigger an alarm (**true positive**) while the absence of an attack would not trigger an alarm (**true negative**). However, it is possible that the scan could generate an error. There are two particular types of errors:

- **False positive.** A **false positive** is an alarm that is raised when there is no problem.
- **False negative.** A **false negative** is the failure to raise an alarm when there is an issue.

Vulnerability scans may produce false positives for several different reasons; for example, scan options may not have been well defined or missed in a configuration review, or the scanner might not recognize a control that is already in place to address an existing vulnerability. The results of a false positive in a vulnerability scan create a large amount of unnecessary work looking for a vulnerability when none exists. Security professionals should attempt to identify false positives in a scan report, especially those that would require extensive effort to address.

The results of a false negative, however, are much more serious: the scan overlooked an existing vulnerability that a threat actor may find and exploit. One means of identifying false positives is for the vulnerability scan data to be correlated with several internal data points. The most common are related log files. Because a log is simply a record of events that occur, system event logs document any unsuccessful events and the most significant successful events. The types of information recorded might include the date and time of the event; a description of the event; its status, error codes, and service name; and the user or system that was responsible for launching the event. An analysis of log data can be used to identify false positives.

Note 1

Logs can be particularly helpful internal data points when correlating with vulnerability scan results. For example, if a scan indicates that a vulnerability in a software application was found on a specific device but a follow-up investigation revealed that the application was no longer vulnerable, log files could indicate whether that program's configuration had been changed between the time of the scan and the follow-up analysis.

Context

The concept of "context" has become a key factor in cybersecurity. Context within cybersecurity refers to the circumstances or conditions surrounding a particular cybersecurity risk that may affect an organization's security posture. **Context awareness** is the use of supplemental information to improve security decisions at the time they are made. This can result in more accurate security decisions and support more dynamic business and information technology (IT) environments. Some context awareness information is **internal** to the organization and comes from within it (such as the types of firewalls being used) whereas other information is **external** to the organization and comes from outside sources. Other information is **isolated** from the organization and is not part of it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 2

The most commonly cited context information types are environmental (such as location and time). However, context information valuable to information security also includes the Internet Protocol (IP) address, information regarding the type of device and its configuration, and the Uniform Resource Locator (URL) being accessed. It can also use non-IT information, such as the business value context of the data being attacked and the threat context.

Context awareness can act as a filter to prioritizing vulnerabilities. For example, if a vulnerability impacts older Windows 32-bit versions of the OS but the organization is using 64-bit versions, then this context would not require security technicians to immediately begin trying to patch systems. On the other hand, if a vulnerability does directly impact the organization—which is determined by the context—then it must be prioritized and may require an immediate response.

Caution !

Context awareness is more than focusing on the technology being used in an organization. It also includes the goals and functions of the organization, the types of data that are used, the criticality of different data types, and many other elements.

Other Factors

There are other factors that should be considered when analyzing vulnerability scans. These include exploitability/weaponization, asset value, and zero-day vulnerabilities.

Exploitability/Weaponization

Suppose you were writing a research paper and you needed information from a book in the library. As you walk through the door into the library, you stop and look at all the books on the shelves. From that distance all the different books—fiction, nonfiction, children's books, atlases, and all other books—would likely look the same: they are all books. However, as you more closely examine the books, you could differentiate among the types of books. You can then, for example, move away from the children's books and atlases to the section that contains the book for which you are searching. From a distance they all look the same, but upon closer examination the differences between the books become apparent.

The same is true with vulnerability scans. A scan will likely reveal multiple vulnerabilities and, at first glance, they may all appear to be critical. However, the vulnerabilities need to be examined more closely to determine which vulnerabilities require immediate attention (if any attention at all).

What are some criteria for examining the different vulnerabilities to determine their importance? One criterion is to determine which exposed assets matter most to an organization. Another criterion is to determine if the vulnerabilities are actively being exploited and capitalized upon by threat actors, known as **exploitability/weaponization**. Without considering weaponization, organizations may end up focusing on vulnerabilities that are not being exploited and fail to address those that should require immediate attention because they expose more sensitive assets.

Note 3

A vulnerability is only as bad as the threat that is actively and directly exploiting it.

Overall (and fortunately), the percentage of all vulnerabilities that are weaponized by threat actors is typically low. This means that an organization should consider weaponized vulnerabilities that could result in the greatest damage to the organization. This helps make a security remediation program more manageable and effective.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Asset Value

One of the first decisions before conducting a scan is to determine what should be scanned. Beyond critical infrastructure components, often decisions must be made about which assets (devices) should be included in a vulnerability scan. This is because not all assets have the same importance or worth to the organization (**asset value**); some assets are critical whereas others can be of lessor importance.

In addition, the results of a scan that reveal vulnerabilities associated with assets of lessor value should also be closely evaluated in light of asset value. It may be that vulnerabilities associated with low-value assets may take away from focusing on vulnerabilities of high-value assets.

Zero-Day Vulnerabilities

Security updates are created and distributed when the software developer learns of a vulnerability and corrects it. But what happens if it is not the developer who uncovers the vulnerability but instead is a threat actor who finds it first? In this case the vulnerability can be exploited by attackers before anyone else even knows it exists. This is called a **zero-day** vulnerability because there are zero days of warning. Zero-day vulnerabilities are considered extremely serious because systems are open to attack with no knowledge of the attack or security fixes available.

Note 4

How widespread are zero-day attacks? Google's Project Zero, which tracks these vulnerabilities, has reported a sharp increase. In 2014, the year records were first kept by Project Zero, there were only 14 vulnerabilities, but in 2023, there were 55 zero-day vulnerabilities used by attackers. To date attackers have taken advantage of 307 previously unknown vulnerabilities to launch attacks.

A vulnerability scan is unable to detect zero-day vulnerabilities because scans rely on known vulnerabilities. The best defense is to ensure that any vulnerabilities associated with high-value assets are immediately addressed.

Two Rights & A Wrong

1. A false positive is the failure to raise an alarm when there is no issue.
2. Context awareness can act as a filter to prioritizing vulnerabilities.
3. A vulnerability scan is unable to detect zero-day vulnerabilities.

See the answers at the end of the chapter.

Prioritizing Vulnerabilities

Certification

2.3 Given a scenario, analyze data to prioritize vulnerabilities.

2.5 Explain concepts related to vulnerability response, handling, and management.

It is important to prioritize vulnerabilities that are uncovered from a vulnerability scan. There are important reasons for prioritizing and escalating vulnerabilities. One means for prioritizing rests on the Common Vulnerability Scoring System (CVSS).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Reasons for Prioritizing and Escalating

The word *triage* originates from the French word "trier," which is used to describe the processes of sorting and organization. Triage is used extensively in the healthcare community to categorize patients based on the severity of their injuries and, by extension, the order in which multiple patients receive care. The history of emergency triage originated in the military for field doctors. As early as the 18th century, field surgeons would quickly look over soldiers and determine the most critical wounds and the order in which they should be addressed. Today, triage is deeply integrated into healthcare. Triage is performed both at the scene of an event and upon arrival at the hospital, as seen in Figure 8-1. Various triage systems are implemented around the world, but the universal goal of triage is to supply effective and prioritized care to patients while optimizing resource usage and timing.

Figure 8-1 Hospital triage



Dan Frioli/Shutterstock.com

In a similar fashion, it is important for cybersecurity personnel to "triage" lists of vulnerabilities for many of the same reasons: to provide effective attention to those vulnerabilities that are most critical in order to optimize limited resources.

However, conducting triage on vulnerabilities is a surprise to many new security personnel. Should not all vulnerabilities be treated as equally critical and be immediately addressed? The answer is no.

First, not all vulnerabilities are as potentially damaging as others. Second, although a scanner might assign a medium rating to a vulnerability, not all organizations will react to that rating in the same way. To one organization, this vulnerability may be critical, but to another it is not worth the effort to fix. Finally, because many vulnerabilities are complex to unravel and take an extended amount of time to address, there may not be enough time to solve all of them.

It is important to remember this principle: *It is rarely possible, and often not desirable, to address all uncovered vulnerabilities.*

Instead of attempting to address all vulnerabilities, it is preferable to determine which vulnerabilities need to be addressed (**prioritize**) out of all those uncovered. And those vulnerabilities that have the greatest negative risk and that impact the assets most critical to the organization are then "moved to the top" or become more important within the prioritized list (**escalate**). Cybersecurity personnel must not only prioritize those vulnerabilities that are considered critical in terms of their impact but also address those that are important to the organization. This means that the most critical and the most important are addressed early on, while others may wait until later or are not even addressed.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Using the Common Vulnerability Scoring System (CVSS)

One of the aids for prioritizing vulnerabilities is using a numeric score assigned to a vulnerability that can then be used as a comparison value. This score is based on the Common Vulnerability Scoring System (CVSS). It is important to know what the CVSS is, its metrics, and how prioritization can be utilized with CVSS.

What Is CVSS?

A numeric score assigned to a vulnerability is often based on the **Common Vulnerability Scoring System (CVSS)**. Numeric scores are generated using a complex formula that considers such variables as the access vector, attack complexity, authentication, confidentiality of the data, and the system's integrity and availability.

The CVSS is often confused with the Common Vulnerabilities and Exposures (CVE) and the National Vulnerability Database (NVD). The differences between these are outlined in Table 8-1.

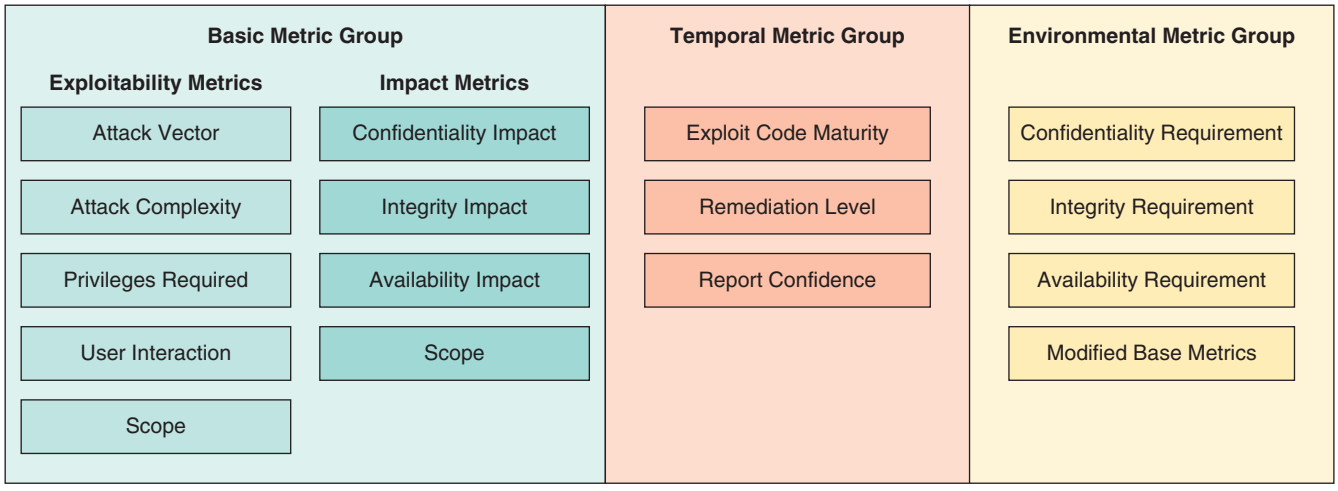
Table 8-1 CVSS, CVE, and NVD

Name	Description	Comparison	Explanation
Common Vulnerability Scoring System (CVSS)	A system widely used in vulnerability management programs.	The CVSS score is not reported in the CVE listing, but users must access the NVD to find assigned CVSS scores.	CVSS indicates the severity of an information security vulnerability.
Common Vulnerabilities and Exposures (CVE)	A list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE Corporation.	The CVE list feeds into the NVD so that both are continually synchronized.	The CVE includes the CVE ID, a description, dates, and comments.
National Vulnerability Database (NVD)	A database of known vulnerabilities maintained by the National Institute of Standards and Technology (NIST).	The NVD provides enhanced information beyond what is included in the CVE list, including patch availability and severity scores.	The NVD provides an easier mechanism to search on a wide range of variables.

CVSS Metrics

CVSS numeric scores are generated using a complex formula that considers a range of vulnerabilities based on different groupings. The groupings of these vulnerabilities are illustrated in Figure 8-2 and are called "metrics" (measurements).

Figure 8-2 Common Vulnerability Scoring System groups



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The Temporal Metric group shows how a vulnerability changes in severity as a result of actions taken by software vendors and by adversaries. For example, if a new update is made available by the software vendor, the Temporal score goes down; if adversaries create and distribute easy-to-use exploit code, the Temporal score goes up.

The metric group that illustrates how the severity of a vulnerability changes due to specific aspects of an organization is part of the Environmental Metric group.

The Basic Metric group shows the attributes inherent in a vulnerability that do not change over time. These attributes are divided into exploitability metrics and impact metrics. The exploitability metrics are listed in Table 8-2. The metrics are sometimes abbreviated as attack vector (AV), attack complexity (AC), privileges required (PR), user interaction (UI), and scope (S).

Table 8-2 Basic Metric group exploitability metrics

Vulnerability name	Description	Scoring method
Attack vector	Indicates the level of access required for an attacker to exploit the vulnerability. A vulnerability that requires physical access to a target system is much more difficult to exploit than one that can be remotely exploited over the Internet.	Network (N): A vulnerability that is remotely exploitable. Adjacent (A): A vulnerability that requires the attack to be launched from the same physical or logical network. Local (L): Vulnerabilities that are not exploitable over a network, such as using social engineering to trick an unsuspecting user. Physical (P): When the attacker must physically interact with the target system.
Attack complexity	Indicates conditions beyond the attacker's control that must exist in order to exploit the vulnerability, such as user interaction or specific configurations of the target system.	Low (L): There are no specific preconditions required for exploitation. High (H): There are conditions required, such as preparatory steps like gathering reconnaissance data or becoming a man-in-the-middle.
Privileges required	Describes the level of access privileges an attacker must have.	None (N): There is no privilege or special access required to conduct the attack. Low (L): The attacker requires basic user-level privileges to leverage the exploit. High (H): Administrative or similar access privileges are required for a successful attack.
User interaction	Describes whether a user other than the attacker is required to perform an action or participate in the exploitation of the vulnerability.	None (N): No user interaction is required. Required (R): A user must complete some steps for the exploit to succeed, such as install malware.
Scope	Determines whether a vulnerability in one system or component can carry over to impact another system or component.	Changed (C): An exploited vulnerability can have carryover impact to another system. Unchanged (U): The exploited vulnerability is limited to only the local system.

Note 5

CVSS is used extensively by the Nessus vulnerability assessment tool. It displays risk information and lists two numeric scores: the CVSS Base Score, which represents the characteristics (Nessus calls these intrinsic qualities) of the vulnerability when it was first discovered, and the CVSS Temporal Score, which reflects the current characteristics of a vulnerability that may have changed over time.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Impact metrics measure the impact on the confidentiality (C), integrity (I), and availability (A) of the impacted system. It answers the question regarding what is the final negative outcome that occurs as a result of exploitation. The impact metrics of the Basic Metric group are listed in Table 8-3.

Table 8-3 Basic Metric group impact metrics

Impact	Description	Scoring
Confidentiality	Refers to the disclosure of sensitive information to authorized and unauthorized users, with the goal being that only authorized users are able to access the target data.	High (H): The attacker has full access to all resources in the impacted system, including highly sensitive information such as encryption keys. Low (L): The attacker has partial access to information, with no control over what specifically they are able to access. None (N): No data is accessible to unauthorized users as a result of the exploit.
Integrity	Refers to whether the protected information has been changed in any way.	None (N): There is no loss of the integrity of any information. Low (L): A limited amount of information might be modified but there is no serious impact on the system. High (H): The threat actor can modify any or all information, resulting in a complete loss of integrity.
Availability	Means that information must be accessible as needed.	None (N): There is no loss of availability. Low (L): Availability might be intermittently limited or performance could be negatively impacted as a result of a successful attack. High (H): There is a complete loss of availability of the impacted system or information.

Prioritizing with CVSS

The vulnerabilities with the highest numeric CVSS scores are generally considered to require early attention. However, the vulnerabilities with higher CVSS scores may not always be the ones that should be addressed first. Instead, it is important to look at scores and the entire vulnerability scan in the context of the organization. The following questions about a vulnerability may help in identifying which ones need early attention:

- Can the vulnerability be addressed in a reasonable amount of time, or would it take several days or even a week to fix?
- Can an external threat actor exploit the vulnerability, or would exploitation require that the person be sitting at a computer in a vice president's office?
- If the vulnerability led to a threat actor infiltrating the system, would they be able to pivot to more important systems or would they be isolated?
- Is the data on the affected device sensitive or is it public?
- Is the vulnerability on a critical system that runs a core business process, or is it on a remote device that is rarely used?

Note 6

Prioritizing vulnerabilities is an inexact and sometimes difficult process. However, attention should first be directed toward vulnerabilities deemed to be critical (those that can cause the greatest degree of harm to the organization). Another part of prioritizing is making sure that the difficulty and time for implementing the correction is reasonable.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong

1. The NVD provides an easier mechanism to search on a wide range of variables.
2. The Environmental Metric group shows how a vulnerability changes in severity as a result of actions taken by software vendors and by adversaries.
3. The attack complexity metric indicates conditions beyond the attacker's control that must exist in order to exploit the vulnerability, such as user interaction or specific configurations of the target system.

See the answers at the end of the chapter.

Managing Vulnerabilities

Certification

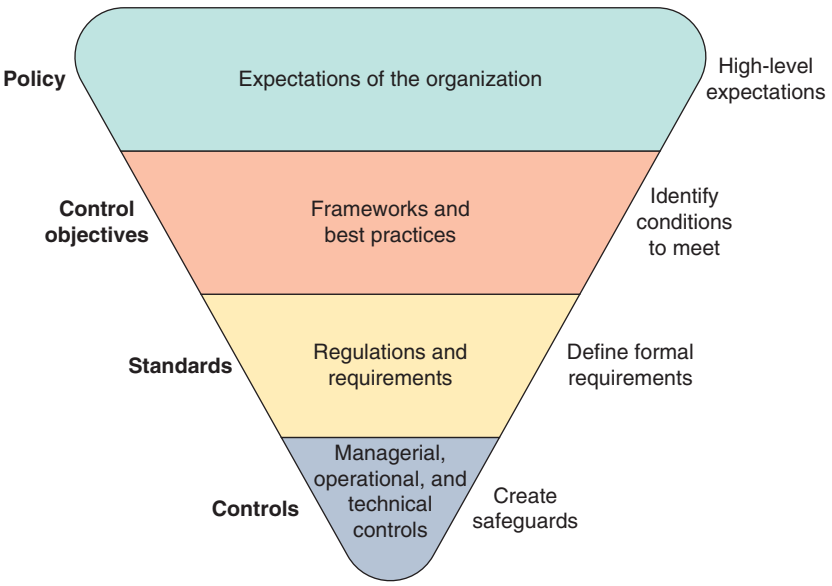
2.5 Explain concepts related to vulnerability response, handling, and management.

After vulnerability scans have been analyzed and the vulnerabilities prioritized, the next step is to manage the uncovered vulnerabilities. Managing vulnerabilities involves using controls, patch management, configuration management, attack surface management, threat modeling, and governance. It also involves consideration of the advantages of advanced vulnerability scanning techniques.

Using Controls

A security **control** is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data. It attempts to limit exposure to a danger. Cybersecurity controls play a key role in a cybersecurity strategy. This is illustrated in Figure 8-3.

Figure 8-3 Strategy for cybersecurity governance



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

There are three broad categories of controls: managerial, operational, and technical. These are listed in Table 8-4 using phishing as an example.

Table 8-4 Categories of controls

Control category	Description	Phishing example
Managerial	Controls that use administrative methods	An acceptable-use policy that specifies users should not visit malicious websites.
Operational	Controls implemented and executed by people	Conducting workshops to help train users to identify and delete phishing messages.
Technical	Controls incorporated as part of hardware, software, or firmware	Unified threat management (UTM) device that performs packet filtering, antiphishing, and web filtering.

At a granular level, there are specific types of controls that are found within the three broad categories of controls. These include:

- **Compensating controls.** A **compensating control** provides an alternative to normal controls that for some reason cannot be used.
- **Corrective controls.** **Corrective controls** are implemented after an incident has occurred to minimize damage, facilitate recovery, and repair weaknesses.
- **Deterrent controls.** A deterrent control attempts to discourage security violations before they occur.
- **Physical controls.** A physical control implements security in a defined structure and location.

Between the three broad categories and the granular specific types of controls there are three classes of controls:

- **Preventive controls.** A **preventive control** works to prevent the threat from coming in contact with the vulnerability.
- **Detective controls.** A **detective control** is designed to identify, log, and alert a threat that has reached the system.
- **Responsive controls.** A **responsive control** is designed to launch remediations to counter adverse events. Examples of technical response controls include updating a system after a software vulnerability has been uncovered, quarantining a computer after malware has been identified, or shutting down a process after malicious activity has been exposed.

Detective controls are considered a prerequisite for establishing responsive controls. That is, the security issue must first be identified before it can be remediated. Once identified, a response can be activated to respond to the security issue.

Note 7

There is no universal agreement on the categories, classes, and types of controls. Some classes are listed as types of controls while types of controls are listed as functions of controls. On some occasions, controls are presented as functions that have types. Additionally, other control types such as recovery controls (measures used to restore a system to normal operations) can be found.

Patch Management

As previously noted, not all vulnerabilities that receive a high CVSS score must immediately be addressed. Rather, depending on multiple factors (risk score, recurrence, context awareness, and weaponization, to name a few) there may be deviations (**exceptions**) from a policy of strictly pursuing all remediations based only on a high score.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

However, one category of vulnerability that is always of high priority is software that is out of date and is missing software updates. Over time, the responsive controls that address out-of-date and vulnerable software have proven to be one of the, if not *the*, most important vulnerabilities to address. In addition, it is often the easiest, quickest, and most economical approach and generally will address a high number of exposed vulnerabilities.

Early operating systems (OSs), such Microsoft Windows, Apple macOS, and Linux, were simply "program loaders" whose job was to launch applications. As more features and graphical user interfaces (GUIs) were added, OSs became more complex.

Note 8

Today's Windows 11 is estimated to have over 50 million lines of code, Linux Debian has 68 million, and Apple macOS may have upward of 86 million. In contrast, Microsoft's first OS, MS-DOS v1.0, had only 4,000 lines of code.

Due to the increased complexity of OSs, unintentional vulnerabilities were introduced that could be exploited by attackers. In addition, new attack tools made what were once considered secure functions and services on OSs now vulnerable. In order to address the vulnerabilities in OSs that are uncovered after the software has been released to the general public as well as to provide ongoing additional features, OS vendors deploy updates to users' computers through an automatic online update service. The user's computer interacts with the vendor's online update service to receive the latest updates. **Patch management** involves installing and managing these software security updates ("patches") in a timely and effective fashion.

There are several reasons why the timely installation of patches through patch management is important. Threat actors often watch for the release of a patch and then immediately craft an attack around the vulnerability that the patch addresses, knowing that many users and organizations are lax in applying patches. Or threat actors may reverse-engineer patches to look for the vulnerability that is being fixed and then craft a completely new attack based on that vulnerability. In either case, promptly installing patches is considered an important step to protecting a device.

Effective patch management involves two types of tools to administer patches. The first type includes tools for patch reception, and the second type involves patch distribution. Some organizations find it necessary to test patches before allowing them to be distributed.

Patch Reception

Endpoint devices can be configured regarding the installation of patches. Prior versions of Microsoft Windows gave users several options regarding accepting or even rejecting patches. These options included "Download updates but let me choose whether to install them," "Check for updates but let me choose whether to download and install them," and "Never check for updates." However, this approach frequently resulted in important security patches being ignored by users and putting their computers at risk.

The patch update options for Microsoft Windows 11 are far less lenient, as shown in Figure 8-4. Updates can also be delayed from one to five weeks. After that time, the updates will resume. Other options include setting a time range when the computer will restart after an update has been installed and optimizing delivery options that depend on the connection type. Apple macOS has similar features. Users can receive a notification that software updates are available, choose when to install the updates, or choose to be reminded the next day.

Testing Patches

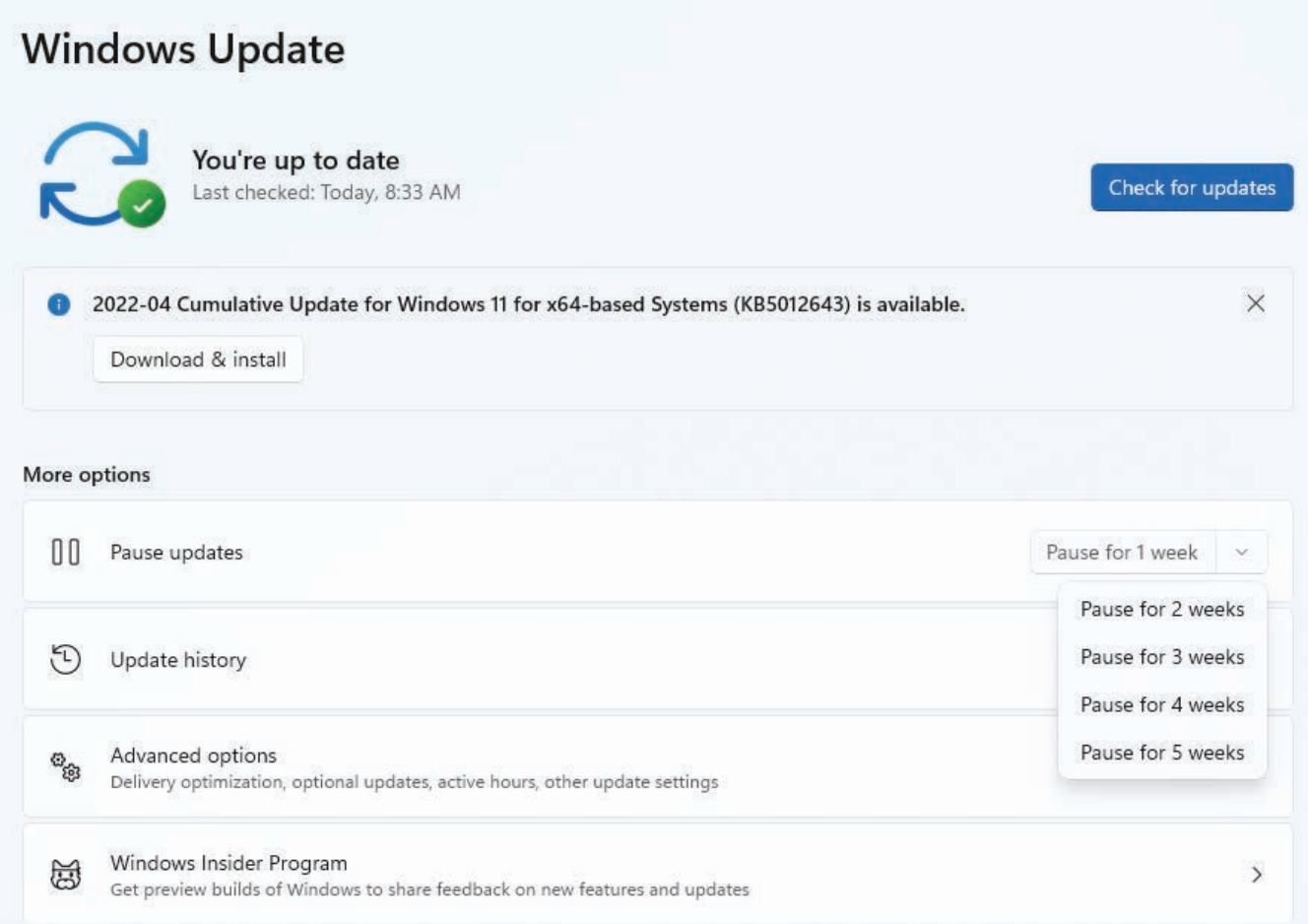
Patches can sometimes create new problems for an organization, such as preventing a custom application from running correctly and then requiring the patches to be "backed out" so the systems can be restored to their original state (**rollback**). Organizations that have these types of applications usually first put the patches through a series of processes. The **testing** process is used to determine if the patch will adversely affect any customized applications. Once this is confirmed (**validation** process) the patches are installed (**implementation** process). Often the installation is performed during a **maintenance window**, which is a scheduled outage of services over a digital platform in order to implement planned changes, upgrades, or repairs.

Patch Distribution

How can an organization prevent its employees from installing the latest patch until it has passed testing and still ensure that all users download and install the necessary patches? The answer is to employ automated patch management tools. These tools are used to manage patches within the enterprise instead of relying on the vendor's online update service. Automated patch management tools typically consist of a component installed on one or more servers inside the corporate network. Because

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 8-4 Windows 11 update options



Source: Microsoft Corporation

these servers can replicate information among themselves, usually only one of the servers must be connected to the vendor's online update service, as seen in Figure 8-5.

There are several advantages to automated patch management tools, including:

- Downloading patches from a local server instead of using the vendor's online update service can save bandwidth and time because each computer does not have to connect to an external server.
- Administrators can approve or decline updates for client systems, force updates to be installed by a specific date, and obtain reports on what updates each computer needs.
- Administrators can approve updates for "detection" only; this allows them to see which computers require the update without installing it.

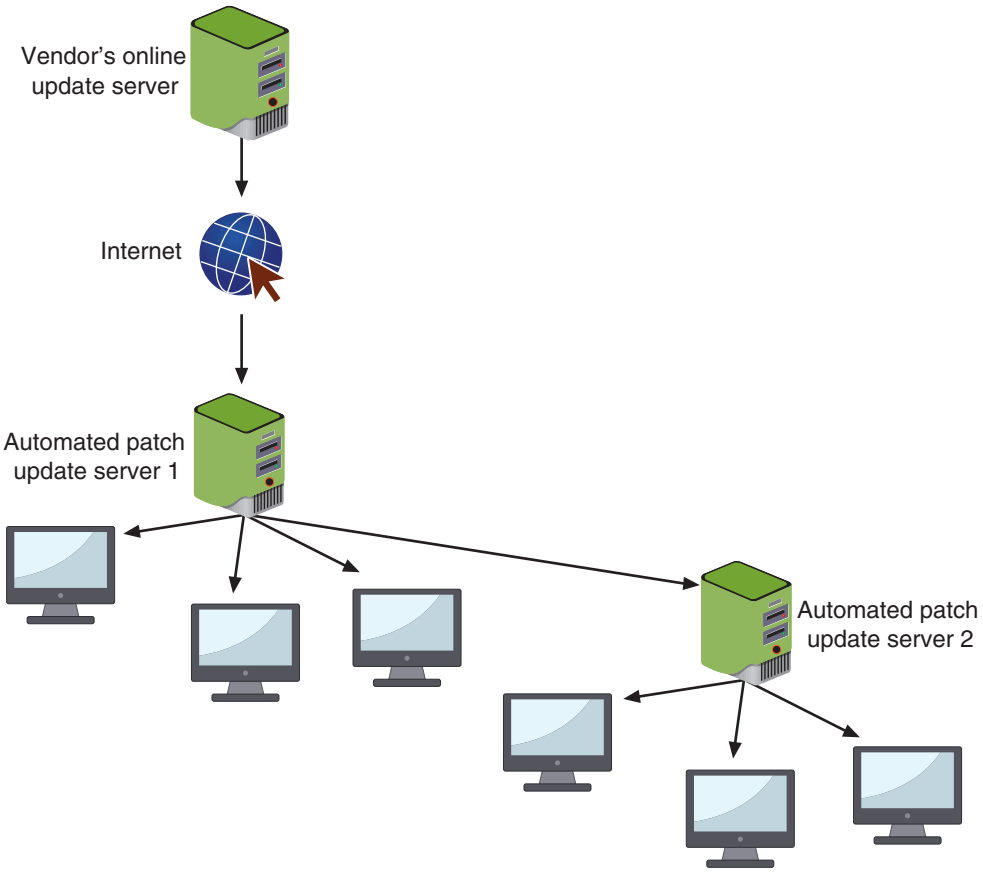
Configuration Management

Configuration management is a process for maintaining computer systems, servers, applications, network devices, and other IT components in a desired state. Configuration management involves establishing a clear approach to documentation, maintenance, and change control so that systems can be configured consistently and accurately across environments. In short, configuration management helps ensure that a system performs as expected, even after many changes are made over time.

Configuration management databases (CMDBs) track individual configuration items (CIs). A CI is any asset or component involved in the delivery of IT services. The CMDBs store information about a CI's attributes, dependencies, and changes to its configuration that may occur over time. This allows IT teams to map and maintain the relationships that tie the CIs together. Using configuration management tools, administrators can set up an IT system like a server or endpoint and then build similar systems with the same settings. In addition, tools such as configuration assessments and drift analyses can continuously scan and identify systems that have strayed from the desired system state and need to be updated, reconfigured, or patched.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 8-5 Automated patch update service



Attack Surface Management (ASM)

Virtually every organization's "digital footprint" has expanded dramatically over the last few years. The major drivers of this expansion are the adoption of cloud technologies, the growth of remote work by employees, and the shift to digital transformation (the process of using digital technologies to create new or modify existing business processes, cultures, and customer experiences to meet changing business and market requirements).

However, the expanding digital footprint has also widened every organization's attack surface. The attack surface is the sum of vulnerabilities, pathways, or methods that attackers will use to launch an attack, breach a network, or access sensitive data. According to one report, two out of every three organizations have seen their attack surfaces expand in just the preceding two years.

Consider, for example, cloud computing. Whereas at one time an organization had its digital assets protected in a secure data center, today those same assets stored in the cloud not only make them vulnerable to virtually anyone with a web browser, but the protection of these assets relies heavily on the security of the cloud provider, who may or may not provide the desired level of security.

This has created a new security defense known as **attack surface management (ASM)**. ASM is the ongoing discovery, analysis, remediation, and monitoring of security vulnerabilities and potential attack vectors that make up an organization's total attack surface. The goal of ASM is to lessen the number of points a threat actor can exploit (called **attack surface reduction**).

Note 9

Unlike some other security methods, ASM is viewed from the attacker's perspective. It identifies targets and assesses risks based on the opportunities they present to a malicious threat actor by mimicking methods and resources that they use.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

ASM includes the following security defenses:

- **Edge discovery.** Edge computing is processing data where the data is being collected instead of it being transmitted back to the traditional on-premises data center for processing. Because it is furthest away from the data center (it is "at the edge"), edge computing can enable processing at greater speeds and volumes, leading to improved action-generated results in real time. Internet of Things (IoT) devices, sensors, wearables like fitness bands, and even self-driving cars and autonomous robots are examples of edge computing. However, it introduces security risks. These devices are not fully protected by the organization's perimeter and may be subject to sustained attacks that can compromise not only the device but also the secure network to which it is attached. **Edge discovery** is a component of ASM that takes efforts to identify these edge devices so that they can be recognized and protected.
- **Passive discovery.** Active discovery scans networks for new items, such as hardware devices or software applications. This can be done manually or through automated scanning tools that map out all existing records in detail. **Passive discovery**, on the other hand, operates more continuously with no manual intervention required. By monitoring historical activity patterns, it can identify any unknown devices connected to the network.
- **Security controls testing.** **Security controls testing** is the evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. As a part of ASM, security controls testing is an important analysis of overall security and if it functions as intended.
- **Penetration testing.** A vulnerability scan is a frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress. A **penetration test**, on the other hand, is a single event often using a manual process in which the testers act like a threat actor (called **adversary emulation**) to find vulnerabilities to exploit. Both vulnerability scans and penetration tests are important to manage attack surfaces and uncover weaknesses to be addressed.
- **Bug bounties.** A common practice of large enterprises is to pay security researchers who uncover security vulnerabilities in their products and then privately report them so that these bugs can be patched before threat actors find them. This is called a **bug bounty** program. Organizations can use the data gathered from their bug bounty program to reduce their attack surface.

Note 10

Google, who started its bug bounty program back in 2010, pays from $100 to $31,337 per reported bug. To date, Google has paid out over $45 million in bounties and even maintains a bug bounty "Leaderboard" hall of fame listing those who have revealed the most bugs. Zerodium, on the other hand, pays up to $2.5 million for information on a single vulnerability and does not reveal who supplied information on the bug.

Threat Modeling

Consider the following principles about a cyberattack:

- Defenders cannot always assume the most likely course of action by the threat actor.
- Defenders must take into account all unlikely events and be prepared for them.
- Given the same tool, different adversaries may have different capabilities to use it.
- Only the attacker knows when an attack starts and ends.
- Principles in the physical world may not always translate into the cyber world.
- Some attacks can be from an individual while others can be from a large group.
- There is a wide spectrum of the adversaries' abilities, capabilities, and goals.

These principles illustrate the difficulty in not only anticipating attacks but also being able to defend against them. One method that has gained increasing popularity in cybersecurity defense is threat modeling. What was once a theoretically interesting concept, threat modeling has now moved into a cybersecurity standard of significant value to enterprises. Threat modeling involves defining the concept, knowing the components of the modeling process, and understanding different threat-modeling methodologies.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Definition of Threat Modeling

At its core, **threat modeling** is a proactive strategy for evaluating risks. It involves identifying potential threats and developing tests to detect and respond to those threats. Threat modeling has several advantages:

- **Address new threats.** When performed routinely, threat modeling can also help security teams ensure that protections are in line with evolving threats.
- **Become more proactive.** Threat modeling enables enterprises to perform a proactive cybersecurity threat assessment. Security teams can use threat-modeling insights to evaluate risks.
- **Develop a deeper level of understanding.** Threat modeling helps an enterprise understand how threats may impact systems, how to better classify threats, and how and why to apply appropriate countermeasures.
- **Prioritize threats and mitigation.** Security teams can use threat modeling to prioritize threats to ensure that resources and attention are distributed effectively for mitigation. Because it is a model, the prioritization can be applied during planning, design, and implementation of cybersecurity to ensure that the solutions are effective.

Components of a Threat-Modeling Process

There are several components that must be considered when performing threat modeling. These components are listed in Table 8-5.

Table 8-5 Threat-modeling components

Component	Definition	Explanation
Adversary capability	Assessing the attacker's intent, ability, capability, skills, tenacity, and available resources	Nation-state actors have a higher adversary capability than unintentional insiders.
Total attack surface	The sum total of the number of different attack points	Typically, larger enterprises have a higher total attack surface.
Attack vector	The method used to compromise a vulnerability	Examples include weak authentication credentials, misconfigurations, malware, and poorly implemented cryptography.
Impact	The effect or influence of the attack on the enterprise	Includes reputational damage, fines by government or regulatory agencies, and loss of customers.
Likelihood	The probability of an attack occurring and being successful	This can range from low to very high.

Threat-Modeling Methodologies

An enterprise can design its own threat-modeling process that encompasses the necessary components. One of the first threat-modeling methodologies that an enterprise could create had the basic goals of better understanding who the attackers are, why they attack, and what types of attacks might occur. This early threat modeling often built scenarios of the types of threats that assets can face by the construction of an attack tree, which is a visual image of the attacks that may occur against an asset. Drawn as an inverted tree structure, an attack tree displays the goal of the attack, the types of attacks that may occur, and the techniques used in the attacks.

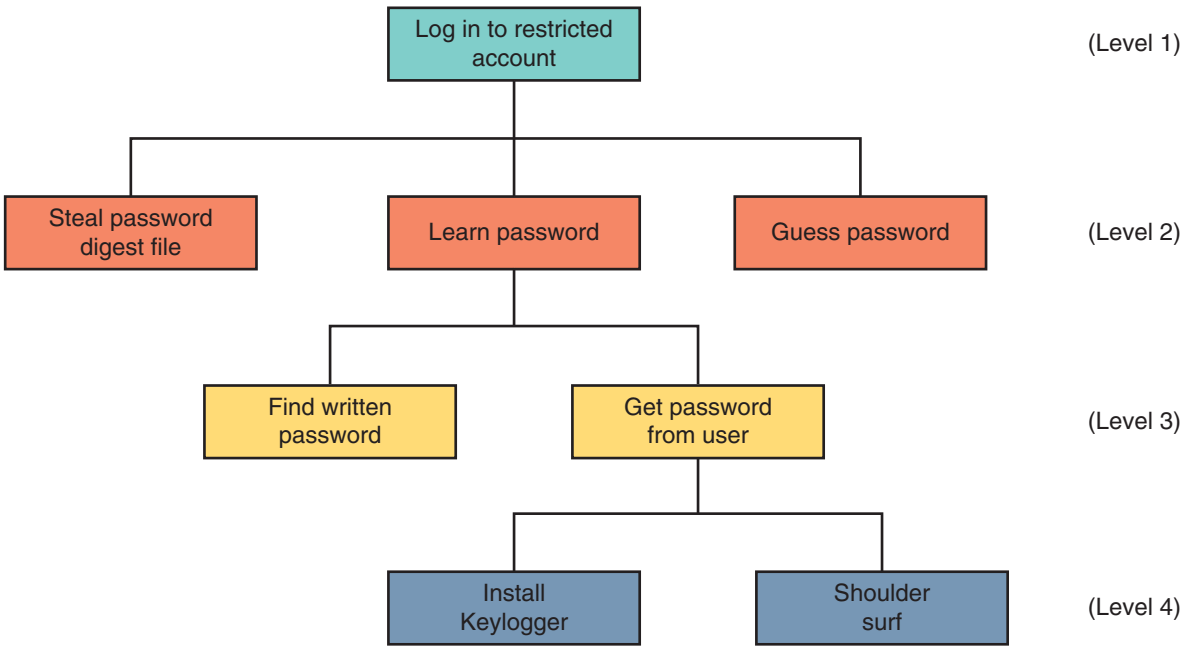
Note 11

The concept of attack trees was developed by Counterpane Internet Security.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 8-6 shows a partial attack tree for an attacker who is attempting to log into a restricted account. The attacker may attempt to learn the password (Level 2) by looking for one that is written down and stored under a mouse pad in an office (Level 3). They could also try to get the password from the user (Level 3) by installing a keylogger on the computer or by shoulder surfing (Level 4). An alternative approach may be to steal the password digest file to use offline cracking (Level 2). Attack trees help list the types of attacks that can occur and trace how and from where they may originate.

Figure 8-6 Attack tree



Although originally helpful, attack trees were too simplistic to be of real value to an enterprise. Today there are different threat-modeling methodologies that can be used. Several of these have a specific focus. The most popular modeling methodologies (with the focus in parenthesis) are:

- **OCTAVE (Practice).** The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology was one of the first created specifically for cybersecurity threat modeling. OCTAVE is designed for assessing nontechnical organizational risks that may result from compromised data. Using OCTAVE, an organization's information assets are identified and the datasets they contain are assigned attributes based on the type of data stored. Drawbacks are the documentation can become very large and it lacks scalability as more users and applications are added.
- **Trike (Acceptable risk).** Trike is an open-source threat-modeling process that is designed to satisfy the security auditing process from a cyber risk-management perspective. The foundation of Trike is a "requirements model" that ensures the assigned level of risk for each asset is acceptable to the various stakeholders. Once the requirements model is in place, a data flow diagram (DFD) is then developed to illustrate how data moves through the system and the actions users can perform within it. However, Trike requires an overall view of the entire system before conducting an attack surface analysis. This can be difficult to scale to larger systems.
- **PASTA (Attacker).** The Process for Attack Simulation and Threat Analysis (PASTA) is a relatively new threat-modeling methodology. It is a seven-step process for risk analysis that does not depend on which platform is being used. The goal of PASTA is to align business objectives with technical requirements while taking into account business impact analysis and compliance requirements. PASTA combines an attacker-centric perspective on potential threats with risk and impact analysis. It, however, requires a significant investment in training.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **STRIDE (Developer).** STRIDE stands for Spoofing Tampering Repudiation Information Message Disclosure Denial of Service and Elevation of Privilege. The goal of STRIDE is to ensure that an application meets the security properties of Confidentiality, Integrity, and Availability (CIA), along with Authorization, Authentication, and Non-Repudiation. Once the security subject matter experts construct the DFD threat model, system engineers or other subject matter experts check the application against the STRIDE threat model classification scheme. STRIDE is most useful when creating a risk-aware corporate culture and is very customizable to an organization's specific security objectives and risk environment.
- **VAST (Enterprise).** The Visual, Agile, and Simple Threat (VAST) modeling methodology was developed to address the weaknesses and implementation challenges in the other threat-modeling methodologies. The founding principle is that threat modeling must scale across the infrastructure and entire application development (DevOps) library and provide actionable, accurate, and consistent outputs for developers, security teams, and senior executives. A fundamental difference of VAST is its practical approach. Recognizing the security concerns of development teams are distinct from those of an infrastructure team, this methodology calls for two types of threat models.

When choosing a threat-modeling methodology, there are three primary considerations. First, the outputs of the model should be considered. While all methodologies may be capable of identifying potential threats, the number and type of threats identified will vary significantly, as will their quality, consistency, and value. Another consideration should be scalability. At the enterprise level, the ability to scale across hundreds or even thousands of threat models must be taken into consideration.

The final consideration is the overall goal. Some enterprises are looking for a model that will generate relevant financial and productivity reports for executive financial reporting. Other enterprises may have the goal of reducing the organization's overall threat profile, attack surface, and risk portfolio.

Governance

Governance can also play a role in addressing vulnerabilities. Governance requires knowing what it is, its bodies, and the mechanisms for applying it.

What Is Governance?

Governance refers to the structures, systems, and practices an organization has in place to assign, oversee, and report. These three activities include:

- **Assign.** Governance is involved in assigning decision-making responsibilities, defining how decisions are to be made, and establishing the organization's strategic direction.
- **Oversee.** A key element of governance is overseeing the delivery of its services; the implementation of its policies, plans, programs, and projects; and the monitoring and mitigation of risks.
- **Report.** Governance involves reporting on performance toward achieving intended results and then using that performance information to drive ongoing improvements and corrective actions (monitoring and revising).

Governance Bodies

Different bodies perform governance responsibilities. Governance bodies can be either internal or external to an organization. Those that are external can be categorized by their proximity to the organization; some cover just the immediate area (local/regional body) while others cover an entire nation (national body) or are worldwide in scope (global body). Some governance bodies are centralized in which all authority is vested into a single body while others are decentralized so that planning and decision making are distributed to smaller groups within it. Table 8-6 lists various typical governance bodies.

Governance Mechanisms

There are several mechanisms for applying governance in an organization. The uppermost level of a governance mechanism is perhaps the most elusive to define. This is because the word for this mechanism can have different meanings in different contexts. A **policy** is a formal statement that outlines specific requirements or rules that must be met based on a decision by a governing body. It outlines the principle that should be followed by its intended audience and should address issues concerning the achievement of the overall purpose of the organization.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 8-6 Governance bodies

Name	Scope	Description
Board	Internal	A board is composed of internal directors who approve strategic organizational goals and policies.
Committee	Internal	The board governance committee is a subset of the board of directors that manages governance issues.
Government entity	External	National governments direct organizations through governance directives.
Regulatory	External	Regulatory agencies are responsible for distributing and enforcing government directives.
Legal	Internal	Internal corporate legal departments interpret internal and external governance policies.
Industry	External	Different industries create and audit governance policies for organizations that make up that industry.

Note 12

A policy should link with the strategic objectives of the organization, such as improved service quality, reduced costs, or fewer workplace injuries.

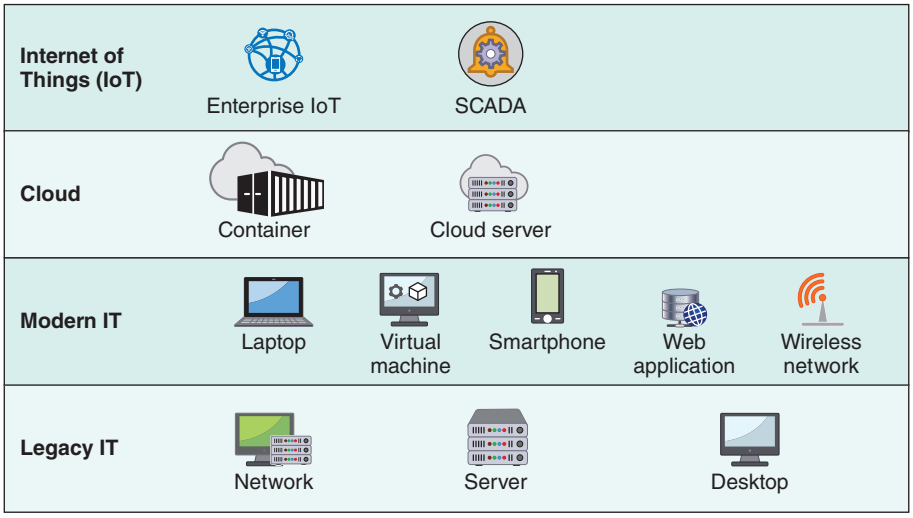
Another mechanism is an external agreement. A service-level agreement (SLA) is a service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service. A **service-level objective (SLO)** is an agreement within an SLA concerning a specific metric. While the SLA serves as the formal agreement, the SLOs are the individual "promises" that are being made.

Both a policy and an SLO can have an impact on determining the priority of a vulnerability and how it should be managed.

Advanced Vulnerability Scanning

The concept of all an organization's servers residing in an on-premises data center that serves resources to desktop computers is a historical relic. Computer servers, networks, and endpoints have evolved more rapidly over the last decade than perhaps in any time in the history of information technology. Cloud computing, mobile smartphones, virtual machines, and IoT devices, just to name a few, have dramatically increased today's enterprise's IT capabilities—and correspondingly have dramatically increased its attack surface. This is shown in Figure 8-7.

Figure 8-7 Today's enterprise information technology



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

However, performing static vulnerability scans, in the eyes of many security professionals, may no longer provide the visibility into system and network vulnerabilities that they once did. Legacy scans that are ad hoc and siloed are usually labor intensive and expensive, resulting in limited deployments and incomplete visibility. These scans often lack comprehensive, continuous, and accurate visibility into where vulnerabilities reside and how businesses might be impacted. And without this visibility, it is difficult or even impossible to prioritize and manage risks.

Among the specific limitations of legacy vulnerability management are:

- **Focus on traditional assets.** Legacy vulnerability scanning focuses on traditional IT assets such as network infrastructures, servers, and desktop computers. These tools are not always designed to discover and scan new assets such as cloud instances, containers, web applications, and IoT devices.
- **Reliance on active scanning technologies.** Active vulnerability scanning tools, while essential, can only capture a snapshot at a single point in time. They often entirely miss devices that are not always connected to the corporate network or that do not have static IP addresses (such as smartphones or remote employees' laptop computers), short-lived assets such as containers, and resources like cloud repositories. Vulnerability scanning was simply not designed for today's dynamic assets and does not always give an accurate picture of their security.
- **Limitations of scanning.** Active vulnerability scanning tools should not be used on all systems. For example, many industrial control systems, IoT devices, and medical devices have not been designed to be scanned and thus scanning may cause disruption or even an entire outage.
- **Lack of insight and prioritization.** A legacy scan gives a large amount of detail on assets and their vulnerabilities. Yet it does not provide tailored information and actionable steps that allow security personnel to quickly prioritize remediation efforts. In addition, it lacks any data analytics that can be used to more easily evaluate and manage the overall cyber risk.

As a result, advanced vulnerability scanning tools and processes have recently been introduced to reflect the changes in IT. A new category of security tools, sometimes called cyber exposure platforms, are specifically designed to continuously perform asset inventory and then assess not only traditional IT infrastructures and devices but also cloud, mobile, IoT, and other assets across the entire organization. In addition, these tools can help quickly evaluate vulnerabilities, prioritize issues, take appropriate corrective steps, and finally measure and report on the vulnerability from both a technical and business perspective.

Two Rights & A Wrong

1. A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data. It attempts to limit exposure to a danger.
2. A detective control is designed to launch remediations to counter adverse events.
3. Passive discovery operates continuously with no intervention required.

See the answers at the end of the chapter.

Summary

- Following a vulnerability scan, it is important to analyze the scan results, prioritize, and fortify against future attacks. When examining results of a vulnerability scan it is important to validate its results for accuracy. A false positive is an alarm that is raised when there is no problem. A false negative is the failure to raise an alarm when there is an issue. Vulnerability scans may produce false positives for several different reasons. The result of a false negative is much more serious. Context awareness is the use of supplemental information to improve security decisions at the time they are

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

made. This can result in more accurate security decisions and support more dynamic business and IT environments. Some context awareness information is internal to the organization while other information is external to the organization that comes from outside sources.

- A criterion is to determine which exposed assets matter most to an organization, or even if the vulnerabilities exposing them are actively being exploited and capitalized on by threat actors is exploitability/weaponization. Without considering weaponization, organizations may end up focusing on vulnerabilities that are not being exploited and fail to address those that should require immediate attention because they expose more sensitive assets. The results of a scan that reveal vulnerabilities associated with assets of lessor value should also be closely evaluated in light of asset value. A zero-day vulnerability with no days of warning is considered extremely serious because systems are open to attack with no knowledge of the attack or security fixes available.
- It is important to prioritize vulnerabilities that are uncovered from a vulnerability scan. This is because it is rarely possible, and often not desirable, to address all uncovered vulnerabilities. Cybersecurity personnel must not only prioritize those vulnerabilities that are considered critical in terms of their impact but also address those that are important to the organization. This means that the most critical that are most important are addressed early on, while others may wait until later or are not even addressed.
- One of the aids for prioritizing vulnerabilities is using a numeric score assigned to a vulnerability that can then be used as a comparison value. This score is based on the Common Vulnerability Scoring System (CVSS). Numeric scores are generated that take into consideration variables such as the access vector, attack complexity, authentication, confidentiality of the data, and the system's integrity and availability. CVSS numeric scores are generated using a complex formula that considers a range of vulnerabilities based on different groupings. The Temporal Metric group shows how a vulnerability changes in severity as a result of actions taken by software vendors and by adversaries. The Environmental Metric group illustrates how the severity of a vulnerability changes due to specific aspects of an organization. The Base Metric group shows the attributes inherent in a vulnerability that do not change over time. These attributes are divided into exploitability metrics and impact metrics. The vulnerabilities with the highest numeric CVSS scores are generally considered to require early attention but it is important to look at scores and the entire vulnerability scan in the context of the organization.
- After vulnerability scans have been analyzed and the vulnerabilities prioritized, the next step is to manage the uncovered vulnerabilities. A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data. It attempts to limit exposure to a danger. There are three broad categories of controls: managerial, operational, and technical. At a granular level, there are specific types of controls that are found within the three broad categories of controls. Between the three broad categories and the granular specific types of controls there are three classes of controls. However, there is no universal agreement on the categories, classes, and types of controls.
- One category of vulnerability that is always of high priority is software that is out of date and is missing software updates. Patch management involves installing and managing these software security updates ("patches") in a timely and effective fashion. Endpoint devices can be configured regarding the installation of patches. Patches can sometimes create new problems for an organization, such as preventing a custom application from running correctly. To avoid this, many organizations use automated patch management tools. These tools are used to manage patches within the enterprise instead of relying on the vendor's online update service. Configuration management is a process for maintaining computer systems, servers, applications, network devices, and other IT components in a desired state. Configuration management involves establishing a clear approach to documentation, maintenance, and change control so that systems can be configured consistently and accurately across environments.
- Vulnerability management, also called infrastructure risk visibility and assurance, is an ongoing examination of the organization's security. At the heart of vulnerability management is identifying vulnerabilities so that they can then be addressed. A vulnerability scan is a frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress. Unlike a penetration test, which is a single event

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

using a manual process that is often performed only to comply with regulatory requirements, a vulnerability assessment is a cyclical and continual process of ongoing scanning and continuous monitoring to reduce the attack. There are several reasons for conducting a vulnerability scan besides providing continuous monitoring. These include meeting regulatory requirements and following corporate policies. Despite its importance, there are several challenges that are associated with vulnerability scanning.

- Attack surface management (ASM) is the ongoing discovery, analysis, remediation, and monitoring of security vulnerabilities and potential attack vectors that make up an organization's total attack surface. The goal of ASM is to lessen the number of points a threat actor can exploit. Edge discovery is a component of ASM that takes efforts to identify edge devices so that they can be recognized and defended. Passive discovery operates continuously with no manual intervention required. Security controls testing is the evaluation of security controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired results. A penetration test, on the other hand, is a single event using a manual process in which the testers act like a threat actor, called adversary emulation. A common practice of large enterprises is to pay security researchers who uncover security vulnerabilities in their products and then privately report them so that these bugs can be patched before threat actors find them. This is called a bug bounty program.
- Threat modeling is a proactive strategy for evaluating risks by identifying potential threats and developing tests to detect and respond to them. Several components must be considered when performing threat modeling. An enterprise can design its own threat-modeling process that encompasses the necessary components. Today different threat-modeling methodologies can also be used, several of which have a specific focus. When choosing a methodology, there are three primary considerations: the outputs of the model, its scalability, and the overall goal.
- Governance can also play a role in addressing vulnerabilities. Governance refers to the structures, systems, and practices an organization has in place to assign, oversee, and report. Different bodies perform governance responsibilities. Governance bodies can be either internal or external to an organization. There are several mechanisms for applying governance in an organization. A policy is a formal statement that outlines specific requirements or rules that must be met based on a decision by a governing body. Another mechanism is an external agreement. A service-level objective (SLO) is an agreement within a service-level agreement concerning a specific metric.
- Performing static vulnerability scans, in the eyes of many security professionals, may no longer provide the visibility into system and network vulnerabilities that they once did. Legacy scans that are ad hoc and siloed are usually labor intensive and expensive, resulting in limited deployments and incomplete visibility. Advanced vulnerability scanning tools and processes have recently been introduced to reflect the changes in IT. A new category of security tools, sometimes called cyber exposure platforms, are specifically designed to continuously perform asset inventory and then assess not only traditional IT infrastructures and devices but also cloud, mobile, IoT, and other assets across the entire organization. In addition, these tools can help quickly evaluate vulnerabilities, prioritize issues, take appropriate corrective steps, and finally measure and report on the vulnerability from both a technical and business perspective.

Key Terms

adversary emulation
asset value
attack complexity
attack surface management (ASM)
attack surface reduction
attack vector
availability
bug bounty
Common Vulnerability Scoring System (CVSS)
compensating control
confidentiality
configuration management
context awareness
control
corrective control
detective control
edge discovery
escalate
exceptions
exploitability/weaponization
external
false negative
false positive
governance
implementation
integrity
internal
isolated
maintenance window

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

managerial controls
operational controls
passive discovery
patch management
penetration test
policy
preventive controls
prioritize
privileges required
responsive control
rollback
Scope
security controls testing
service-level objective (SLO)
technical controls
testing
threat modeling
true negative
true positive
user interaction
validation
zero-day

Review Questions

1. Which of the following CVSS vulnerability metrics indicates conditions beyond the attacker's control that must exist in order to exploit the vulnerability?
   a. Attack vector
   b. Attack complexity
   c. Privileges required
   d. Scope
2. Which of the following is NOT an example of ASM?
   a. Security controls testing
   b. Edge discovery
   c. Passive discovery
   d. Active discovery
3. Which of the following is NOT a variable used in CVSS?
   a. Access vector
   b. Attack complexity
   c. Time of attack
   d. Confidentiality of data
4. What is threat modeling?
   a. A proactive strategy for evaluating risks
   b. Using CVS data as input into a threat engine
   c. Using old threat intelligence data to create new threat intelligence data
   d. A standard for assigning a qualitative label to a threat
5. Which threat model has the developer as its primary focus?
   a. MAGELLAN
   b. STRIDE
   c. Trike
   d. PASTA
6. If a vulnerability scan were to fail to raise an alarm when there is an issue, what type of error is this?
   a. False positive
   b. False negative
   c. True positive
   d. True negative
7. What is the use of supplemental information to improve security decisions at the time they are made?
   a. Sensitivity level
   b. Context awareness
   c. Scope of project
   d. Auxiliary threat intelligence (ATI)
8. Which of the following is NOT correct about exploitability/weaponization?
   a. It is used to determine if the vulnerabilities exposing the organization are actively being exploited and capitalized on by threat actors.
   b. Without it, organizations may end up focusing on vulnerabilities that are not being exploited.
   c. It helps address those vulnerabilities that require immediate attention because they expose more sensitive assets.
   d. It requires that CVSS scores be high enough to warrant action.
9. Which of the following is NOT correct about zero-day vulnerabilities?
   a. A vulnerability scan can easily detect zero-day vulnerabilities.
   b. A good defense is to ensure that any vulnerabilities associated with high-value assets are immediately addressed.
   c. They are considered very dangerous.
   d. No security fixes are available for zero-day vulnerabilities that are utilized by threat actors.
10. Which of the following is NOT a reason for prioritizing vulnerabilities?
    a. Not all organizations will react to scan ratings in the same way.
    b. Only qualified cybersecurity personnel can make prioritization decisions about vulnerabilities.
    c. Many vulnerabilities are complex to unravel and take an extended amount of time to address.
    d. Not all vulnerabilities are as potentially damaging as others.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

11. How does CVSS compare with NVD and CVE?

- **a.** All three are identical.
- **b.** CVSS is managed by Barry and Associates while NVD and CVE are not.
- **c.** CVSS scores are not reported in the CVE, but users must access the NVD to find assigned scores.
- **d.** CVE scores are calculated differently than CVSS scores.

12. Which CVSS metric group shows how a vulnerability changes in severity as a result of actions taken by software vendors and by adversaries?

- **a.** Temporal Metric
- **b.** Basic Metric
- **c.** Environmental Metric
- **d.** Core Metric

13. Which of the following is NOT a Basic Metric group impact?

- **a.** Timeliness
- **b.** Availability
- **c.** Integrity
- **d.** Confidentiality

14. Which of the following controls is implemented and executed by people?

- **a.** Managerial
- **b.** Technical
- **c.** Tactical
- **d.** Operational

15. Which control is implemented after a cybersecurity incident has occurred?

- **a.** Deterrent
- **b.** Compensating
- **c.** Corrective
- **d.** Physical

16. Which of the following is NOT an advantage to automated patch management tools?

- **a.** Downloading patches from a local server instead of using the vendor's online update service can save bandwidth and time because each computer does not have to connect to an external server.
- **b.** Administrators can approve or decline updates for client systems, force updates to be installed by a specific date, and obtain reports on what updates each computer needs.
- **c.** Administrators can approve updates for "detection" only that allows them to see which computers require the update without installing it.
- **d.** It speeds up the process of testing patches prior to their distribution.

17. Which of the following tracks individual configuration items using configuration management tools?

- **a.** JB
- **b.** XCR
- **c.** CI
- **d.** CMDB

18. Which of the following ASMs operates continuously with no manual intervention required?

- **a.** Surface reduction
- **b.** Edge discovery
- **c.** Passive discovery
- **d.** Active scanning

19. Which of the following is NOT an advantage of threat modeling?

- **a.** Address new threats
- **b.** Prioritize threats and mitigation
- **c.** Develop a deeper level of understanding
- **d.** Become less dependent on modeling

20. Which of the following modeling methodologies focuses on the attacker?

- **a.** VAST
- **b.** OWSAP
- **c.** Trike
- **d.** PASTA

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Projects

Case Project 8-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. Is there anything that can be done to address zero-day vulnerabilities? Should it be a crime to use or share a zero-day vulnerability and not report it to the hardware or software developer? Write a one-page paper about this.

Case Project 8-2: Threat Models

Estimated Time: 25 minutes
Objective: Research threat models.
Description: Select one of the threat models (OCTAVE, Trike, PASTA, STRIDE, or VAST) discussed in this chapter and use the Internet to research this model. How is it used? What are its advantages? What are its disadvantages? Write a one-page paper on your research.

Case Project 8-3: Researching Zero-Day Vulnerabilities

Estimated Time: 20 minutes
Objective: Summarize zero-day vulnerabilities.
Description: Research zero-day vulnerabilities. Select three major attacks that utilized zero-day vulnerabilities. Document the impact of these attacks. Who is suspected of being behind the attacks using the zero-day vulnerability? Is there any evidence regarding how they were able to acquire the vulnerability? How long did it take for the vulnerability to be patched? Write a one-page paper on your research.

Case Project 8-4: Prioritizing Vulnerabilities

Estimated Time: 25 minutes
Objective: Decide how to prioritize vulnerabilities.
Description: Create a list of seven criteria that you would use when prioritizing a vulnerability. Then rank those criteria in order of most important to least important. Finally, identify a recent attack and apply your criteria to that attack. Create a one-page paper on your work.

Case Project 8-5: Common Vulnerability Scoring System

Estimated Time: 25 minutes
Objective: Research CVSS.
Description: Use the Internet to research CVSS. What is its history? Who maintains it now? What are its strengths? What are its weaknesses? How reliable is the data that it produces? Write a one-page paper on your findings.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong: Answers

Analyzing Vulnerability Scans

1. A false positive is the failure to raise an alarm when there is no issue.
2. Context awareness can act as a filter to prioritizing vulnerabilities.
3. A vulnerability scan is unable to detect zero-day vulnerabilities.

Answer: The wrong statement is #1.
Explanation: A false positive is an alarm that is raised when there is no problem.

Prioritizing Vulnerabilities

1. The NVD provides an easier mechanism to search on a wide range of variables.
2. The Environmental Metric group shows how a vulnerability changes in severity as a result of actions taken by software vendors and by adversaries.
3. The attack complexity metric indicates conditions beyond the attacker's control that must exist in order to exploit the vulnerability, such as user interaction or specific configurations of the target system.

Answer: The wrong statement is #2.
Explanation: The Temporal Metric group shows how a vulnerability changes in severity as a result of actions taken by software vendors and by adversaries.

Managing Vulnerabilities

1. A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data. It attempts to limit exposure to a danger.
2. A detective control is designed to launch remediations to counter adverse events.
3. Passive discovery operates continuously with no intervention required.

Answer: The wrong statement is #2.
Explanation: A detective control is designed to identify, log, and alert a threat that has reached the system.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 9

Vulnerability Management and Administration

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Identify vulnerabilities
2. Explain how to respond to vulnerabilities
3. List the elements that make up a vulnerability report
4. Discuss how to conduct exercises and awareness training

#TrendingCyber

It's hard enough for a business to address and manage all its cybersecurity vulnerabilities while reporting them to affected stakeholders. Just think how difficult it would be for an entire nation to do that. But that's what happened recently.

Tokelau is a dependent territory of New Zealand located in the southern Pacific Ocean. Tokelau is officially referred to as a nation by the New Zealand government. It is a free and democratic country holding elections every three years. Tokelau consists of three tropical coral atolls that have a combined land area of only 4 square miles (10 square kilometers). And with a population of approximately 1,500 people, it has the fourth-smallest population of any sovereign state or dependency in the world.

Technology has not come easily to Tokelau. It is so remote that it was the last place on Earth to know about the outbreak of World War I. Regular shortwave radio was not available until the 1970s. And it was the last country to be connected by telephone in 1997.

So, it was a surprise in 2000 when the islands received correspondence (via a fax, naturally) with an interesting business proposition. The correspondence was from Joost Zuurbier, an entrepreneur in Amsterdam. Joost offered to manage Tokelau's country-code top-level domain, or ccTLD (the short string of characters at the end of a URL like .us or .uk). Until then, Tokelau did not even know it had been assigned a ccTLD. In fact, Tokelau was the second-smallest location to receive a ccTLD domain from the Internet Corporation for Assigned Names and Numbers (ICANN), a group tasked with maintaining Internet domain names. The general manager of Teletok, Tokelau's sole telecom operator, did some investigating and discovered that Tokelau did indeed have its own ccTLD: ".tk."

Joost made Tokelau an unexpected offer. He would manage their domain through his company Freenom. What's more, instead of asking Tokelau to pay him, Joost would pay Tokelau. In exchange, Tokelau would allow him to use the .tk domain. Why would Joost make such an offer? His business model was simple: Joost would give Internet users a free domain name ending in .tk for one year in exchange for having advertisements hosted on their websites. If the users wanted to avoid the ads or keep their .tk domain name longer, they would pay Joost an annual fee. In short, the revenue streams from advertisements and fees would be shared by Joost with Tokelau.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The offer to use a country's ccTLD in exchange for payment is nothing new. The nation of Tuvalu has managed to turn its ccTLD ".tv" into approximately 10 percent of its annual gross domestic product (GDP). Micronesia's ".fm" is used heavily by radio stations and podcasters. Tonga's ".to" has been favored by websites distributing and downloading files using the BitTorrent (often called torrent) protocol. More recently, Anguilla in the Caribbean has started heavily marketing its ".ai" ccTLD to artificial intelligence technology startups.

The offer to Tokelau from Joost sounded like a win–win proposal. Joost would have a revenue stream and Tokelau would have someone to manage their ccTLD for free. Plus, they would receive a share of the revenue for essentially doing nothing. What could go wrong?

As it turns out, plenty.

The webpage for Teletok, Tokelau's telecom operation, was the first domain registered with .tk. But soon the number of domains with .tk grew—exponentially. In a short period of time the .tk domain had more users than any other country in the world. What's more, these users all had something in common: they were cybercriminals.

The allure of a free .tk domain offered by Joost turned out to be too tempting for spammers, phishers, and other cybercriminals to pass up. Threat actors quickly realized they could use a free ccTLD .tk domain that allowed them to avoid providing any personal information (albeit fictitious) when registering a regular domain name. Soon attackers were creating .tk websites that harvested user passwords and payment information, served as command-and-control (C&C) sites, and delivered malware to users. And once word got out, the .tk domain became a haven for the worst domains on the Internet. There were .tk websites that abounded with pornography. Jihadists and the Ku Klux Klan were registering .tk websites to promote their extremism. And Chinese nation-state attackers were using .tk websites for espionage campaigns.

How bad was it? Over 25 million domains were registered using .tk, the most of any nation in the world (there still was only one legitimate webpage, Teletok, that was located on Tokelau). In 2016, the Anti-Phishing Working Group found that, along with .tk, the Australian Cocos Islands (.cc) and Palau (.pw), plus with the ubiquitous .com, made up 75 percent of all malicious domain registrations worldwide.

Allowing other domains to use .tk turned out to be a public relations disaster for Tokelau. Tokelau received large numbers of complaints from across the Internet community as users assumed that the nation was behind these malicious threat actors. And to add insult to injury, Freenom soon stopped sending any money to Tokelau after Joost became overwhelmed with requests for the .tk domain.

However, recently things have started to improve for Tokelau's .tk domain. In December 2022, courts in the Netherlands found in favor of an investor suing Freenom for lack of payment. And in March 2023 Meta (the owner of Facebook, Instagram, and WhatsApp) also sued Freenom for damages, claiming that sites hosted on .tk and other domains they managed were engaging in cybersquatting and trademark infringement. Meta said the websites faceb00k.tk, whatsaap.tk, and Instaqram.tk—all with a .tk domain—were created by threat actors with the purpose of deceiving users.

Today all of Tokelau's email and website addresses are currently hosted on New Zealand's .nz domain (as of January 2023, it is no longer possible to register a .tk domain). However, this experience has had an impact on the psyche of the nation as a whole. By having a .nz domain, Tokelau is often viewed as part of New Zealand instead of being a sovereign nation. The current general manager of Tokelau's government wants to see its Internet domain make a triumphant return to demonstrate that the islands are turning a new page. He said, "We are building nationhood here. We are on a pathway toward self-determination. We want to use the .tk as a catalyst to promote our nationhood and be proud of it—our domain name and our identity among the Internet community."

Vulnerability management and administration is an ongoing, regular process for identifying, assessing, and remediating cyber vulnerabilities. But it does not stop there. It also involves reporting on vulnerabilities to stakeholders. And it includes awareness, education, and training in order to reduce the attack surface by empowering employees to become "human firewalls." In short, vulnerability management and administration tasks are far-reaching and make up a key element in an organization's overall security.

In this chapter, you look at the elements of vulnerability management and administration. This includes identifying and responding to vulnerabilities, vulnerability reporting, and the steps for creating meaningful training and exercises.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Identifying Vulnerabilities

Certification

2.2 Given a scenario, analyze output from vulnerability assessment tools.

Identifying vulnerabilities can often be a challenge. However, a variety of diagnostic tools can be used to assess assets to discover vulnerabilities. These tools can be classified as multipurpose tools as well as specific tools for identifying vulnerabilities in web applications, cloud infrastructures, and wireless networks.

Multipurpose Tools

The word *multipurpose* is used to describe something that can serve more than a single function. Phrases such as "multipurpose room" or "multipurpose cleaner" indicate that these are versatile, all-around, and even "one-size-fits-all" entities that can serve a variety of functions.

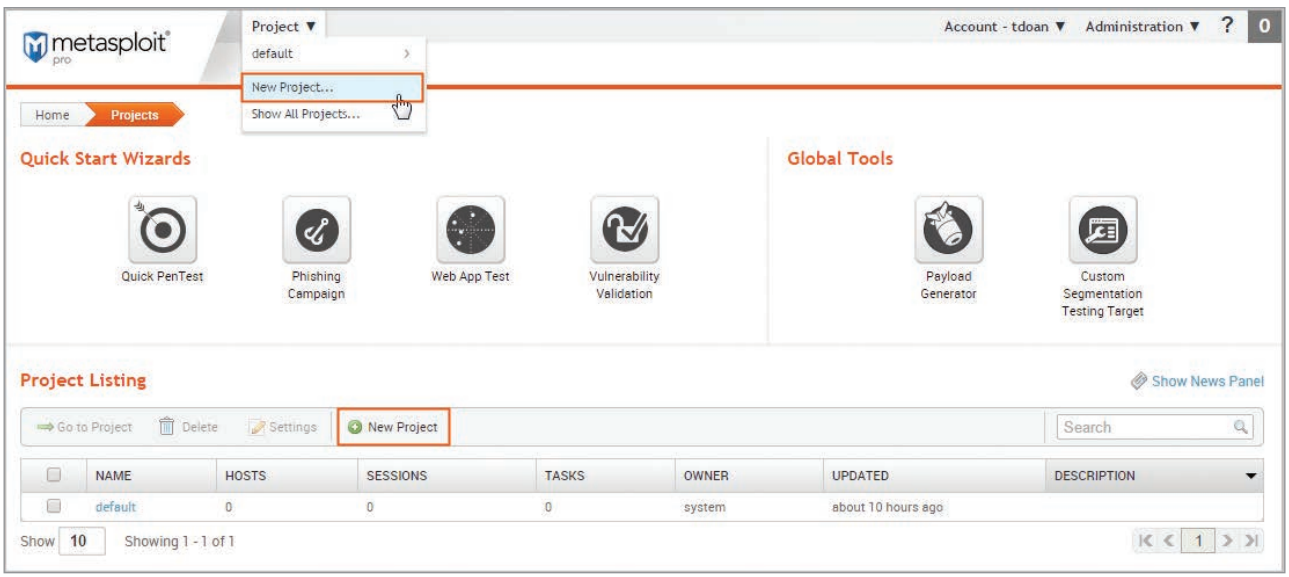
Several vulnerability diagnostic tools fit into the description of being multipurpose tools. These tools include the Metasploit framework, Recon-ng, Nmap, and other tools.

Metasploit Framework (MSF)

The **Metasploit framework (MSF)** is a flexible and modular penetration-testing platform. Its flexibility can be seen in two ways. First, MSF contains over 2,000 different exploits that can be used to test security vulnerabilities and evasion techniques, execute penetration attacks, and enumerate (gather information about) networks. Second, it enables security professionals to write, test, and then execute their own exploit code.

MSF is based on the programming language Ruby and contains a Ruby compiler that can be used for incorporating user-created code into the framework. Figure 9-1 illustrates the MSF graphical user interface (GUI) launching a new project.

Figure 9-1 Metasploit graphical user interface



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 1

There are two editions of Metasploit: Metasploit Pro and Metasploit Free. Metasploit Free is an open-source package that includes the same core features as the commercial Metasploit Pro but has fewer features and limited performance capabilities. Metasploit Pro has an advanced GUI and reporting functions along with a more comprehensive set of tools for scheduling scans, running multiple scans in parallel, and automatically generating reports.

An MSF session typically involves four phases, as seen in Figure 9-2. The test begins with the information-gathering phase (Discover Devices). Once a weakness is identified, users can choose an exploit and payload for exploitation (Gain Access). MSF offers various exploitation tools for privilege escalation, packet sniffing, keylogging, and screen capturing, along with tools to pivot to other systems. If the exploit is successful, the payload is executed on the target device. The user is also given a shell to interact with the payload (Take Control) along with a persistent backdoor that can be installed so that if the target device is rebooted access is still available. The final phase (Collect Evidence) is used to document the exploit.

Figure 9-2 Metasploit exploit session



Note 2

The comprehensive nature of MSF can be illustrated in the Discover Devices phase. By default, its discovery scan includes a User Datagram Protocol (UDP) scan, which sends UDP probes to the most common UDP ports, such as Simple Network Management Protocol (SNMP), Network Basic Input/Output System (NetBIOS), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS). MSF also has its own built-in discovery scanner that uses Nmap to perform basic Transmission Control Protocol (TCP) port scanning, testing approximately 250 ports that are typically exposed.

MSF has several advantages. It is very effective in identifying and taking advantage of a wide array of recognized security flaws. It can also support different operating systems (OSs) such as Windows, macOS, and Linux. Its modular architecture allows for flexibility and customization. And because Metasploit Free is considered open source, it allows for continuous enhancements and improvements from the global community.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

In the wrong hands, MSF can be used in a nefarious manner by threat actors to exploit systems.

However, MSF has some disadvantages. Because of its intricate structure and advanced features, it can be difficult for beginners to navigate and utilize MSF effectively. Some of the MSF modules have become outdated against updated or newer systems, and antivirus or intrusion detection systems can recognize Metasploit's actions and stop them.

Recon-ng

Recon-ng is a full-featured reconnaissance framework. Like MSF, Recon-ng is a completely modular open-source framework to which developers may contribute. It even has a look and feel similar to MSF. However, unlike MSF, Recon-ng is a web-based tool instead of a tool that must be downloaded and installed on a local device. Recon-ng is essentially a website and web application scanner that can gather information to then be used to search for vulnerabilities. Recon-ng is not considered as an alternative to MSF but a complement to it.

Note 3

MSF and Recon-ng are both called open-source intelligence (OSINT) tools.

Recon-ng runs under Linux as a command-line interface (CLI). There are a wide range of options and switches when using Recon-ng, as seen in Figure 9-3. An example of using Recon-ng is to discover the subdomains of a single domain along with their Internet Protocol (IP) addresses that would be implemented by using the command *use recon/domains-hosts/findsubdomains*. This is illustrated in Figure 9-4.

Figure 9-3 Recon-ng options

```
root@kali:~# recon-cli -h
usage: recon-cli [-h] [-w workspace] [-C command] [-c command] [-G]
                 [-g name=value] [-M] [-m module] [-O] [-o name=value] [-x]
                 [--no-version] [--no-analytics] [--no-marketplace]
                 [--stealth] [--version] [--analytics]

recon-cli - Tim Tomes (@lanmaster53)

options:
  -h, --help          show this help message and exit
  -w workspace        load/create a workspace
  -C command          runs a command at the global context
  -c command          runs a command at the module context (pre-run)
  -G                  show available global options
  -g name=value       set a global option (can be used more than once)
  -M                  show modules
  -m module           specify the module
  -O                  show available module options
  -o name=value       set a module option (can be used more than once)
  -x                  run the module
  --no-version        disable version check. Already disabled by default in
                      Debian
  --no-analytics      disable analytics reporting. Already disabled by default
                      in Debian
  --no-marketplace    disable remote module management
  --stealth           disable all passive requests (--no-*)
  --version           displays the current version
  --analytics         enable analytics reporting. Send analytics to google
```

Recon-ng

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 9-4 Recon-ng discovery

```
[recon-ng][default][hackertarget] > show hosts
 +-------------------------------------------------
  | rowid |            host          |    ip_address
  +-------------------------------------------------
  | 1     | tesla.com                | 104.119.104.74
  | 2     | o7.ptr6980.tesla.com     | 149.72.144.42
  | 3     | vpn1.tesla.com           | 8.45.124.215
  | 4     | apacvpn1.tesla.com       | 8.244.131.215
  | 5     | cnvpn1.tesla.com         | 114.141.176.215
  | 6     | vpn2.tesla.com           | 8.47.24.215
  | 7     | model3.tesla.com         | 205.234.27.221
  | 8     | o3.ptr1444.tesla.com     | 149.72.152.236
  | 9     | o2.ptr556.tesla.com      | 149.72.134.64
  | 10    | o5.ptr8466.tesla.com     | 149.72.172.170
  | 11    | o6.ptr9437.tesla.com     | 168.245.123.10
  | 12    | o4.ptr1867.tesla.com     | 149.72.163.58
  | 13    | marketing.tesla.com      | 13.111.47.196
  | 14    | o1.ptr2410.link.tesla.com | 149.72.247.52
```

Recon-ng

Note 4

Recon-ng comes pre-installed with Kali Linux.

Nmap

Another open-source tool is **nmap** (*N*etwork *Map*per), which is a utility for network discovery and security auditing. Using IP packets, nmap can determine what hosts are available on a network; what services the hosts are offering, such as application name and version; and what types of packet filters or firewalls are in use. Nmap can also be used for OS fingerprinting as well as discovering characteristics of a specific host computer ("host scanning"). One of the advantages of nmap is its ability to quickly scan very large networks. Table 9-1 shows several common commands in the command-line version of nmap.

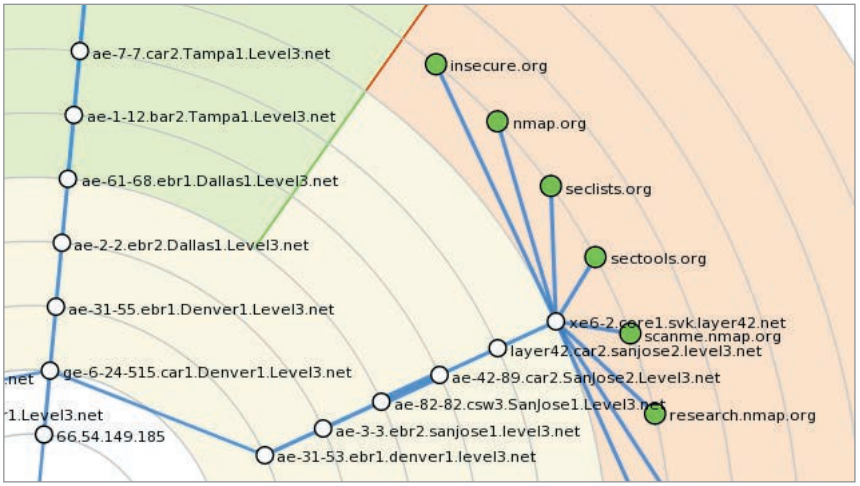
Table 9-1 Common nmap commands

Command	Description
nmap www.cengage.com	Scan one host
nmap 192.168.1.1	Scan one IP address
nmap 192.168.1.1-20	Scan a range of IP addresses
nmap 192.168.1.0/24	Scan an entire subnet
nmap -p 22 192.168.1.1	Scan one port
nmap -p 1-100 192.168.1.1	Scan a range of ports
nmap -p- 192.168.1.1	Scan all 65,535 ports
nmap -A 192.168.1.1	Detect the OS and services on the specific host computer
nmap -sV 192.168.1.1	Detect the services on the host computer
nmap -sV --version-intensity 5 192.168.1.1	Conduct an aggressive service detection scan

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A GUI version of nmap called Zenmap is also available. Zenmap can even be used for creating a visual map of a network, as shown in Figure 9-5.

Figure 9-5 Zenmap network map



Source: Nmap.org

Other Tools

Other multipurpose tools can be used in reconnaissance to help identify vulnerabilities. These include hping (a command-line TCP/IP packet assembler and analyzer) and responder (a tool that can manipulate name resolution services to uncover sensitive information).

In addition to these third-party tools, there are network utilities that are part of the OS that can also be utilized. As its name implies, netstat (*net*work *stat*istics) provides detailed information about current network connections. It is a command-line utility included in virtually all OSs (Windows, macOS, Linux, and so on.) that provides network protocol statistics as well as network connections for the TCP, network interfaces, and routing tables. Netstat commands can be tailored by using one or more parameters called "switches" (such as *netstat -a*). Table 9-2 lists some of the most commonly used netstat switches.

Table 9-2 Common netstat switches

Switch	Description
-a	All active connections and the ports that the computer is listening on
-e	Ethernet data such as number of bytes and packets sent and received
-g	Multicast group membership data
-n	Active TCP connections (addresses and port numbers displayed numerically)
-r	Contents of routing table
-s	Statistics by protocol
-n	Redisplays data every *n* seconds until Ctrl+C is pressed

Note 5

All operating systems also have unique netstat switches. For example, you can use the *-o* switch in Windows to include the process ID, and you can use the *-t* switch in Linux to display only TCP connections.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

In addition to netstat, other OS tools can be useful in gathering network information:

- **ipconfig** (*ifconfig* in Linux). *I*nternet *P*rotocol *config*uration (ipconfig) is a tool that displays TCP/IP network connection data, such as the IP address, subnet mask, and default gateway for all network adapters. It also displays DNS information.
- **tracert** (*traceroute* in Linux). This tool can give basic information about the path that a packet takes.
- **ping.** This is a networking program to test whether a particular host can be reached.
- **nslookup** (*dig* in Linux). The nslookup (*n*ame *s*erver *lookup*) tool can be used to obtain the IP address or domain name of a host.

Web Applications

Vulnerabilities in web applications continue to be a leading attack vector today; in fact, by some estimates these vulnerabilities in web applications may account for almost half of all successful security incidents. There are several tools that can be used to diagnose vulnerabilities in web applications. These tools take a variety of different approaches:

- **Passive scanning.** A web application vulnerability diagnostic tool that performs passive scanning examines each page of the web application delivered by the web server and then looks at the HTML in responses from the web application. Passive scanning does not change responses in any way and is considered safe; in addition, it is performed in a background thread and will not impact the response of the application to other users. Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted.
- **Active scanning.** Active scanning attempts to find other vulnerabilities by using known attacks against the selected targets. It attacks all the discovered pages by testing their functionality and parameters. Because active scanning is an attack on those targets and can put them at risk, its usage must be controlled so as not to negatively impact the web server and its applications.
- **Dynamic analysis.** Dynamic analysis searches for flaws from outside the application with no knowledge of the software's structure or source code.
- **Static analysis.** Static analysis examines the web application code from the inside to look for common vulnerabilities such as Structured Query Language (SQL) injection and cross-site scripting, as well as coding errors like buffer overflows and unhandled error conditions.

The OWASP **Zed Attack Proxy (ZAP)** is considered the premiere open-source tool for diagnosing web applications. ZAP is a Java-based tool with a highly usable GUI allowing testers to perform fuzzing, scripting, and other actions to attack web apps. Because it is a Java tool, ZAP can run on most OSs that support Java. An example of ZAP output is shown in Figure 9-6.

Other web application vulnerability diagnostic tools include **Burp Suite** (a tool that performs both a static and dynamic analysis), **Nikto** (a command-line open-source tool), and **Arachni** (a modular open-source tool).

Cloud Infrastructure

There are several different tools that can be used to identify vulnerabilities in cloud platforms. These include:

- **Prowler.** **Prowler** is a command-line tool for diagnosing vulnerabilities in services using the Amazon Web Services (AWS) cloud. It looks at cloud configurations and compares them with over 150 cloud security best practices. The output from a Prowler assessment is shown in Figure 9-7.
- **Scout Suite.** **Scout Suite** is an open-source multicloud security-auditing tool. It can be used to assess the security posture of different cloud environments. Scout Suite uses the application programming interfaces (APIs) that are exposed by the cloud providers to gather configuration data for manual inspection and highlight areas of risk. Scout Suite supports AWS, Microsoft Azure, Google Cloud Platform, Alibaba Cloud, and Oracle Cloud.
- **Pacu.** **Pacu** is an exploitation framework for AWS. It has over 35 modules that range from reconnaissance, persistence, privilege escalation, enumeration, data exfiltration, log manipulation, and miscellaneous general exploitation.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 9-6 Zed Attack Proxy output

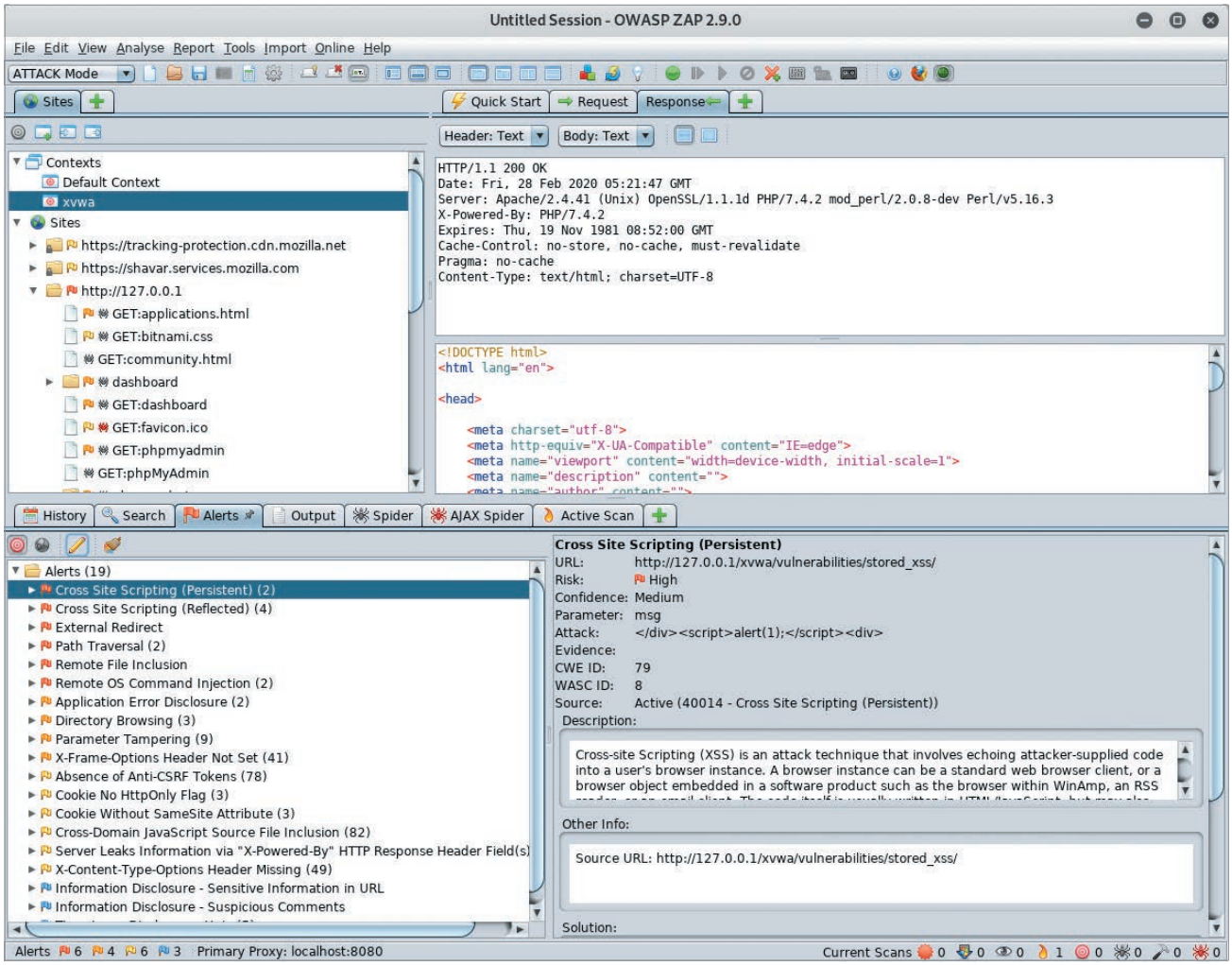


Figure 9-7 Prowler



Source: Prowler

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

However, a new direction in identifying cloud infrastructure vulnerabilities is now taking place. Instead of the user utilizing these tools to search for vulnerabilities, cloud providers are offering these services. Amazon's AWS Security Hub aggregates, organizes, and prioritizes vulnerabilities from multiple AWS services and AWS partners so that users can quickly assess their security posture. The AWS Security Hub performs evaluations of cloud security against controls and provides high-priority security alerts across all AWS accounts.

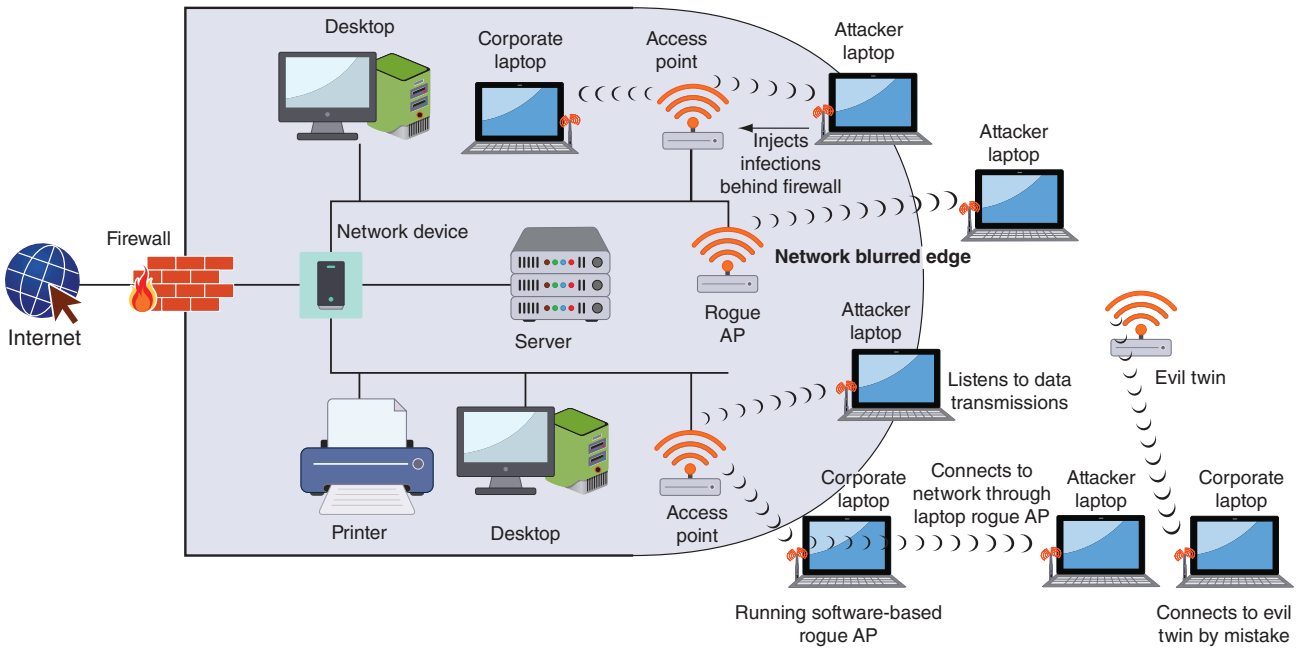
In addition, cloud providers are now offering users the ability to allow cyber insurance companies to access their web security information from the user's AWS Security Hub. This gives potential insurers a list of controls that are enabled on a particular account, information on vulnerabilities, and other details. Cyber insurance carriers can quickly evaluate the organization's application for cyber insurance against AWS's standards for security best practices and their own underwriting standards. It can decrease the time for an insurer to evaluate a new or updated policy request from multiple weeks down to as little as 48 hours. In addition, insurers often offer discounts since they have full visibility into the organization's security posture.

Wireless Networks

In a traditional wired network, a well-defined boundary or "hard edge" protects data and resources. There are two types of hard edges. The first is a network hard edge. A wired network typically has one point (or a limited number of points) through which data must pass from an external network to the secure internal network. This single data entry point makes it easier to defend against because any attack must likewise pass through this one point. Security appliances can be used to block attacks from entering the network. The combination of a single entry point plus security appliances that can defend it make up a network's hard edge, which protects important data and resources. The second hard edge is made up of the walls of the building that house the enterprise. Because these walls keep out unauthorized personnel, attackers cannot access the network. In other words, the walls serve to physically separate computing resources from attackers.

The introduction of wireless local area networks (WLANs) in enterprises, however, has changed these hard edges to "blurred edges." Instead of a network hard edge with a single data entry point, a WLAN can contain multiple entry points. The radio frequency (RF) signals from access points (APs) create several data entry points into the network through which attackers can inject attacks or steal data. This makes it difficult to create a hard network edge. In addition, because RF signals extend beyond the boundaries of the building, the walls cannot be considered as a physical hard edge to keep away attackers. A threat actor sitting in a car well outside of the building's security perimeter can still easily pick up a wireless RF signal to eavesdrop on data transmissions or inject malware behind the firewall. An AP whose security settings have not been set or have been improperly configured can allow attackers access to the network, resulting in several different wireless attacks directed at the enterprise. These include rogue access points, evil twins, intercepting wireless data, and wireless denial of service attacks, illustrated in Figure 9-8.

Figure 9-8 Wireless attacks



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

There are different tools that can be used to diagnose wireless vulnerabilities. These tools typically discover wireless vulnerabilities through exploitation. Because of the nature of wireless transmissions most wireless vulnerability tools utilize Linux. Aircrack-ng can monitor wireless networks and perform attacks to uncover vulnerabilities. Other Linux-based wireless vulnerability tools include BoopSuite, Airgeddon, Trackerjacker, and WPSIK.

Two Rights & A Wrong

1. An MSF session typically involves four phases.
2. Recon-ng is a proprietary framework.
3. Dynamic analysis searches for flaws from the outside of an application with no knowledge of the software's structure or source code.

See the answers at the end of the chapter.

Responding to Vulnerabilities

Certification

4.1 Explain the importance of vulnerability management reporting and communication.

It is naturally important to respond to vulnerabilities once they have been identified through assessment tools. Responding involves implementing an action plan, combating inhibitors to remediation, and evaluating metrics and key performance indicators.

Implement Action Plans

Action plans are comprised of all the steps of the tasks that are needed to meet an objective. They are different from a "to-do" list in that they focus on the achievement of a single goal, while a to-do list is typically a set of unrelated tasks. Action plans are considered useful because they can efficiently provide a framework for thinking about how to complete a project in its totality. They can also help ensure that key steps are not overlooked and can identify which tasks can be delegated or outsourced.

While action plans vary when responding to vulnerabilities, most plans cover the basic steps of using compensating controls, enforcing patching, and executing configuration management.

Use Compensating Controls

A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data. It attempts to limit exposure to a danger. There are three broad categories of controls: managerial, operational, and technical. At a granular level there are specific types of controls that are found within the three broad categories. These include corrective controls (implemented after an incident has occurred to minimize damage, facilitate recovery, and repair weaknesses), deterrent controls (attempts to discourage security violations before they occur), and physical controls (implements security in a defined structure and location).

Another granular control is a compensating control, which provides an alternative to normal controls that for some reason cannot be used. Compensating controls in cybersecurity involve taking preventive measures and implementing proactive strategies to protect information systems from cyber threats. An action plan in itself can be considered a compensating control.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Enforce Patching

Due to the increased complexity of OSs, unintentional vulnerabilities were introduced that could be exploited by attackers. In addition, new attack tools made what were once considered secure functions and services on OSs now vulnerable. To address the vulnerabilities in OSs that are uncovered after the software has been released, vendors "fix" software through a patch. Patch management involves installing and managing patches in a timely and effective fashion.

Addressing out-of-date and vulnerable software through patches is considered an important step in an action plan to respond to vulnerabilities. This is because it is the easiest, quickest, and most economical approach to managing vulnerabilities and generally will address a high number of exposed vulnerabilities.

Execute Configuration Management

Configuration management is a process for maintaining computer systems, servers, applications, network devices, and other information technology (IT) components in a desired state. It includes establishing a clear approach to documentation, maintenance, and change control so that systems can be configured consistently and accurately across environments. Configuration management helps ensure that a system performs as expected, even after many changes are made over time. Executing configuration management is an important step in an action plan.

Combat Inhibitors to Remediation

At first sight, the idea seems unthinkable of someone or something inhibiting a change to a system to address a vulnerability. However, there are often external factors that may impact how, when, or even if a change can be made to address a vulnerability.

Often inhibitors are due to interoperability agreements, or formal contractual relationships. These agreements include the following:

- A **service-level agreement (SLA)** is a service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service.
- A **service-level objective (SLO)** is an agreement within an SLA concerning a specific metric. While the SLA serves as the formal agreement, the SLOs are the individual "promises" that are being made.
- A **memorandum of understanding (MOU)** describes an agreement between two or more parties. It demonstrates a "convergence of will" between the parties so that they can work together. An MOU is generally not a legally enforceable agreement but is more formal than an unwritten agreement.
- An interconnection security agreement (ISA) minimizes security risks for data transmitted across a network. Examples of network interconnections usually include corporate virtual private network (VPN) tunnels that are used to connect to a network. The ISA ensures the adequate security of both entities as they share data across networks.
- A nondisclosure agreement (NDA) is a legal contract between parties that specifies how confidential material will be shared between the parties but restricted to others. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information.

Note 6

Any of these formal relationships may hinder addressing a vulnerability. For example, an MOU may state that specific changes will not be made to a remote system, even if a vulnerability is discovered on that system.

Another inhibitor can be the organizational governance of the company. **Organizational governance** is defined as the system by which an organization makes and then implements decisions. While the optimum would be for everyone at the organization to agree with the necessity of addressing cybersecurity vulnerabilities, this is not always the case. Due to in-fighting, multiple levels of bureaucracy, and extensive "red tape," it is not uncommon for correcting a vulnerability to be delayed for an extended period, particularly if it may cause an interruption to the normal business processes.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

On some occasions addressing a vulnerability may change or even eliminate a function of an application for the sake of making it more secure. This is known as **degrading functionality** and may invoke stiff resistance when users have been accustomed to a function or option. One means of addressing degrading functionality is to remind users of the relationship between *security* and *convenience*: as security is increased, convenience is often decreased. That is, the *more* secure something is, the *less* convenient it may become to use (security is said to be "inversely proportional" to convenience).

Another "pushback" from the organization to implementing tighter security by addressing vulnerabilities is the reluctance by the organization to make any changes to a system that is properly functioning. Today businesses and industrial processes function in a "just-in-time" environment in which processing time has been significantly reduced in order to increase overall efficiency. This essentially results in no "slack" in the system. There may be stiff resistance to bringing the key critical devices (**priority systems**) offline to address vulnerabilities when this could negatively impact the entire production system. In many instances, these are older systems with specialized software that cannot be easily replaced (**legacy systems**) and thus there is no alternative for bringing them offline. This is known as **business process interruption**, and it is not uncommon for there to be a lack of support from higher levels of management to addressing vulnerabilities if it may interrupt normal functions.

Evaluate Metrics and Key Performance Indicators (KPIs)

How can an organization know that they are taking the right steps to ensure that it is safe against cyberattacks and data breaches? In other words, how do they know that what they are doing is actually working? What exactly should they look at to determine if they are taking the right steps? And how can all this be done given the ever-shifting landscape of cybersecurity when unknown zero-day attacks lurk in the shadows, when there are new cybersecurity **trends** (movements in attacks and defenses), when **critical vulnerabilities** (vulnerabilities that should be prioritized for immediate remediation) may surface at any time, and when there are **changing business requirements** (adjustments in the attributes, capabilities, and characteristics of a business)?

It is critical for an organization to track their cybersecurity progress as well as lack of progress. This tracking includes quantitative information that demonstrates the efforts to protect the organization's data and other technology assets. This data can lead to a review of which efforts are proving useful, which need adjustments, and which need to be overhauled. It gives a larger and clearer picture of the organization's security situation in order to make better and more informed decisions.

Note 7

It has long been observed that if you cannot measure your efforts, you cannot make proper decisions. And a famous management consultant once said, "What gets measured, gets managed."

There are tools that can help cybersecurity teams determine if they are taking the right steps. **Key performance indicators (KPIs)** are designed to clearly articulate and provide insight into what an organization needs to measure. Cybersecurity **metrics** are the cybersecurity data that an organization tracks on a daily, weekly, monthly, and annual basis. In other words, KPIs indicate *what* should be measured while metrics *are* the measurements.

Although the list varies, the generally recognized **top 10 KPIs** (those considered the most important) are summarized in Table 9-3.

Table 9-3 Top 10 KPIs

KPI	Description
Intrusion attempts versus actual security incidents	This KPI offers general insight into existing vulnerabilities, the state of preparedness, and how the organization responds to attacks.
Mean time to detect (MTTD)	This is an important KPI because the faster an organization identifies an attack, the greater the odds it can contain it with minimal damage.
Mean time to respond (MTTR)	The ability to neutralize a threat and get systems back online is critical because the longer the response, risks and costs increase.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

KPI	Description
Mean time to contain (MTTC)	This refers to the average time required to shut down all attack vectors across all endpoints and minimize the probability of any further damage.
Unidentified devices on the network	The ability to discover and tag unidentified devices greatly reduces the odds that a threat actor has unauthorized access to the network.
Patching cadence and effectiveness	This KPI measures how frequently patches are applied, how they are prioritized, and their overall effectiveness.
Training effectiveness	This measures the positive value of employee cybersecurity defense training.
Peer and industry benchmark data	Using independent data, an organization can know how it is performing compared to others in the same industry.
Security audit compliance	This KPI metric measures if the compliance required from external entities is being followed.
Third-party risk and compliance	This looks at supply chains, third-party vendor apps, privileges, and relationships with external entities that have "hooks" into the organization's data.

Two Rights & A Wrong

1. Action plans are different from a "to-do" list in that they focus on the achievement of a single goal.
2. An action plan can be considered as a compensating control.
3. An SLA is an agreement between two or more parties that demonstrates a convergence of will.

See the answers at the end of the chapter.

Communicating and Reporting Vulnerabilities

Certification

4.1 Explain the importance of vulnerability management reporting and communication.

While it is not uncommon to think that once vulnerabilities have been identified and addressed, then the work is over. But that is not the case. Vulnerability management communication and reporting is a necessary and important step. This not only serves to inform all relevant stakeholders of the vulnerabilities identified but also documents **mitigation** efforts (reducing the harm of a hazard) toward protecting assets (**affected hosts**). Three important tasks include generating reports, calculating the risk score, and minimizing recurrence.

Generate Reports

There are different levels of reports that should be distributed to specific audiences who have a vested interest ("stake"), sometimes called **stakeholder identification and communication**. Because these stakeholders are both internal and external to the organization, the scope and depth of the reports vary. However, the reports have common elements.

Internal Stakeholder Reports

Some stakeholders who should receive reports about vulnerabilities and their mitigations are internal to the organization. Table 9-4 illustrates the different levels of reports and their intended internal stakeholders.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 9-4 Internal stakeholder reports

Internal stakeholder	Level of report	Explanation
Management	A general report that outlines the impact to the organization	Management will be interested in how the latest scan compares with previous scans, how serious the vulnerabilities are, and how long it will take to address these latest vulnerabilities.
System and network engineers	A technical report that outlines what needs to be addressed	Engineers will want a listing of the devices with vulnerabilities and specific details regarding how to fix the problems.
Application developers	A report that lists the applications that contain vulnerabilities and what those vulnerabilities are	Developers will want to know which of their applications are vulnerable and as much as possible the location of that vulnerability in their code.
Security teams	A very specific report relating to the technical security details	Security teams want to know what systems were vulnerable, the details as to why they could be exploited, and what remediation steps are necessary.

The internal stakeholder reports illustrated in Table 9-4 are specific in their detail and scope. This is because the audience is part of the organization itself and requires more in-depth information so that it can be acted upon. For the internal technical stakeholders (system and network engineers, application developers, and security teams), the information in the report will be very specific and detailed. This level of detail is made possible because modern vulnerability scanning tools can provide extensive information through reporting to assist different audiences. For example, for a website that contains a SQL injection vulnerability, the vulnerability scan software can provide to application developers the name of the application, the input to the web application that triggered the vulnerability and the corresponding output, and even the specific variable within the application that resulted in the compromise.

External Stakeholder Reports

However, to external stakeholders, the granular level of reporting that is provided to internal stakeholders is not necessary—and in many instances should be avoided. Providing too much detailed information could prove to be an aid to threat actors who will then leverage this information for a subsequent attack.

One common external stakeholder report is directed at external regulatory bodies that create and enforce regulatory compliance laws and regulations. Examples include the Dodd-Frank Act, Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Sarbanes-Oxley Act. A report to one of these external regulatory bodies is called a **compliance report**. This report is a document that summarizes the findings and recommendations of the assessment to demonstrate the organization's adherence to regulations, deviations from it, and how they will be addressed.

Report Contents

As noted, the contents of the reports will vary depending on the audience. In general, a report typically has these elements: executive summary, background and context, methodology, findings, recommendations, and limitations.

Executive Summary The executive summary is the first section of the report and should provide a concise overview of the main content of the report about the assessment. Its purpose is to capture the attention and interest of the readers so that the significance of the assessment and its findings can be clearly communicated. The executive summary should highlight the most critical vulnerabilities and risks, as well as the suggested mitigation steps and timelines.

As its name suggests, the executive summary should be written in clear and nontechnical language for "executives" who may not have a deep technical background or expertise in cybersecurity. An executive summary should use clear, plain, and concise language while avoiding technical terms.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 8

It is important to remember that some readers may only read the executive summary. This means that its role in summarizing key findings and recommendations clearly and concisely is critically important.

Background and Context The background and context section should explain the reasons and goals for conducting the assessment, such as complying with regulations, improving the security posture, or addressing specific issues. This helps the readers understand the scope and significance of the assessment. Providing the necessary "backdrop" for readers allows them to understand why the assessment was conducted and the broader context in which vulnerabilities exist.

The background and context section should also give essential details about the assessed systems, such as the assets assessed and their purpose, function, components, users, dependencies, and so on. This helps the readers grasp the detailed assessment's scope and significance in subsequent sections.

Methodology The assessment methodology section should describe the tools, techniques, standards, and criteria that were used to perform the assessment. It should explain how the system or network was scanned, tested, and analyzed and how the vulnerabilities and risks were identified, classified, and scored. In short, the assessment methodology section demonstrates the validity and reliability of the assessment process by describing the tools that were used, techniques followed, and criteria used in scanning, testing, and analysis. Giving this transparency helps to ensure the validity and reliability of the assessment process and its results.

Findings The assessment findings section presents the detailed and comprehensive results of the assessment. It lists and describes all the vulnerabilities and risks that were detected, along with their severity, impact, likelihood, and exploitability. It also gives evidence to support the findings, such as scan reports, test logs, and vulnerability descriptions. The assessment findings section should be organized and formatted in a clear and consistent way using tables, charts, or graphs. In short, the assessment findings section presents the vulnerabilities and their risks organized in a format for easy reading comprehension.

Note 9

One useful but often omitted item is the Common Vulnerability Scoring System (CVSS) score of the finding. By including the score, it ensures the testers and report writers are not introducing too much subjectivity. The Base CVSS score is considered essential, and if the readers have more business knowledge, then the CVSS environment metrics can also be helpful. And mapping to the OWASP framework is considered useful as well.

Recommendations The assessment recommendations section should provide the specific and actionable steps that need to be taken to address and resolve the vulnerabilities and risks uncovered in the assessment. It should prioritize recommendations based on the urgency and importance of the vulnerabilities, assign responsibilities for correcting, and give deadlines for each task. However, recommendations should be realistic and feasible.

One question often raised is the order in which vulnerabilities and mitigations should be presented. Often recommendations are sorted strictly by Common Vulnerabilities and Exposures (CVE) ratings and level of criticality. However, sometimes the recommendation section adds an optional element that rates the ease of remediation. Some remediation sections add an optional secondary report that is sorted in groupings of actions. For example, a finding that identifies an outdated TLS is placed next to other security protocol misconfigurations so that these can be addressed simultaneously.

Limitations The assessment limitations section should acknowledge and disclose any factors that could affect the accuracy, completeness, or relevance of the assessment results and recommendations. These could include technical constraints, human errors, time constraints, scope limitations, or assumptions. The assessment limitations section should also indicate how these factors were addressed or mitigated and how they could be improved or avoided in future assessments. This section should be transparent and should not undermine the credibility or value of the assessment.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

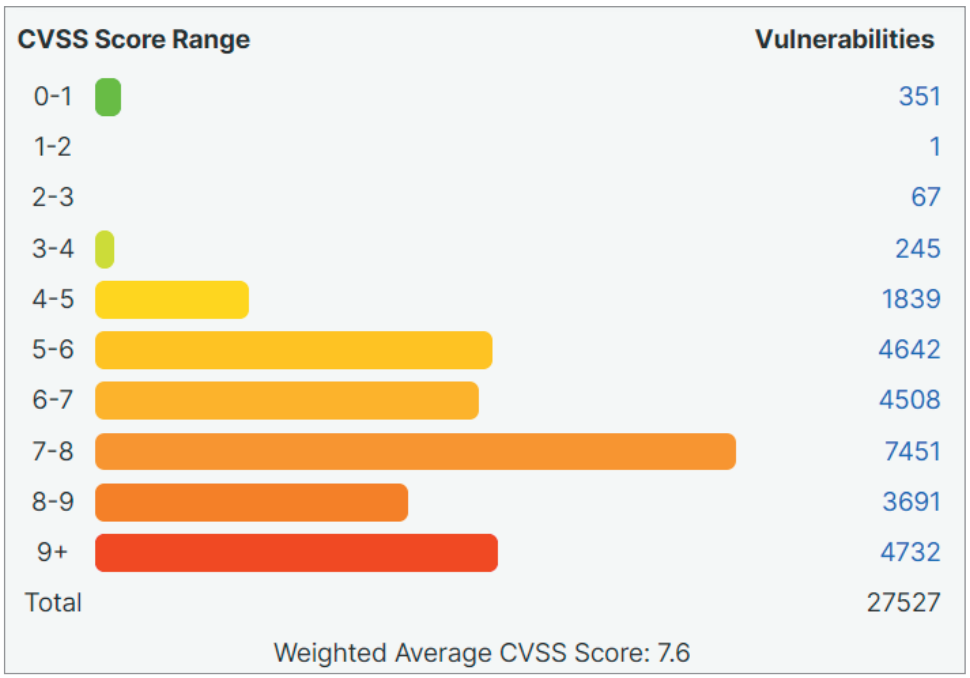
If the vulnerability scan is conducted by an outside third party, it is essential that an agreement first be reached regarding how and where the report will be stored and transmitted. Due to its high value to threat actors, a listing of vulnerabilities should be encrypted while at rest and in transit and only shared with approved personnel.

Calculate Risk Score

A numeric score is usually assigned to a vulnerability based on the CVSS, ranging from 0 (lowest priority) to 10 (most critical). These numeric scores are generated using a complex formula that considers such variables as the access vector, attack complexity, authentication, confidentiality of the data, and the system's integrity and availability. The vulnerabilities with the highest numeric CVSS scores are generally considered to require immediate attention.

However, CVSS scores are not perfect. The scores cannot take into account the risk toward an asset within a specific organization since there is no insight by CVSS into the organization's security defenses. Also, it has been noted that CVSS scores tend to skew high. Figure 9-9 illustrates the CVSS scores over a 12-month period. These have a weighted average score of 7.6 out of 10.

Figure 9-9 Common Vulnerability Scoring System scores over a 12-month period



Note 10

Over a 20-year period, the weighted average score was still very high at 7.5.

Several security vendors have created their **risk score** by supplementing CVSS scores with additional data to determine the impact of a vulnerability. One vendor adds data that is summarized in Table 9-5. The goal of these risk scores is to determine the top 3 percent of vulnerabilities that should be remediated first.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 9-5 Data supplements to CVSS scores

Data supplement	Explanation
Vulnerability priority rating	This rating is created by assessing over 150 data points from third-party vulnerability and threat data that is fed into a machine-learning algorithm to analyze all the vulnerabilities in the National Vulnerability Database (NVD) to predict which vulnerabilities have the greatest risk of being exploited in the near future.
Predictive prioritization	Predictive prioritization uses a customized risk-based approach to vulnerability management to determine a probability an attacker may leverage a weakness against the specific organization.
Asset criticality rating	The asset criticality rating represents how critical each asset is in an organization based on several key metrics associated with the asset, such as including business purpose, asset type, location, connectivity, capabilities, and third-party data.

Minimize Recurrence

Another element of vulnerability management communication and reporting are vulnerabilities that continue to occur (**recurrence**). There are several situations in which a vulnerability may reoccur:

- **Restarting a disabled service.** A vulnerable service, such as a web server, may have been initially found to be vulnerable but because it was no longer needed, the remediation was to simply turn it off. However, at a later time the web server was needed and was then restarted, although it still was vulnerable.
- **New firewall rule.** A discovered vulnerability may be blocked by a firewall rule to prevent access from the Internet and other external networks. If a change to a firewall rule opens a port that was blocking access to the vulnerable service, the vulnerability will reoccur.
- **Vulnerable open software libraries.** Because many applications today rely on open software libraries that are out of the control of the organization, this can introduce recurring vulnerabilities. For example, the libraries may be repeatedly compromised by threat actors that then become part of the software codebase or an app may rely on open-source components that are no longer maintained. In addition, if software installations are performed in a manner that downgrades a library, this may reintroduce a vulnerability.

Simply reporting the vulnerability again and waiting for it to be remediated does not address a more critical issue, namely a fundamental flaw in the management process. Vulnerabilities that were once mitigated but now recur represent security processes and organizational issues that must be handled differently.

Caution !

Recurring vulnerabilities are a "red flag" that require a more in-depth analysis of the processes of the organization.

Two Rights & A Wrong

1. The executive summary is the first section of the report and should provide a concise overview of the main content of the report about the assessment.
2. The findings section of a report lists and describes all the vulnerabilities and risks that were detected, along with their severity, impact, likelihood, and exploitability.
3. Several security vendors have created their risk score by supplementing CVE scores with additional data to determine the impact of a vulnerability.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Conducting Exercises and Awareness Training

Certification

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.

4.1 Explain the importance of vulnerability management reporting and communication.

All too often vulnerability management and administration are viewed exclusively through the lens of technical security controls. However, nontechnical controls are equally important. An often-overlooked nontechnical control for reducing vulnerabilities and risk is conducting **awareness, education, and training** regarding the risks associated with cybersecurity attacks and how to properly defend against these attacks. Awareness, education, and training should be administered as cybersecurity team exercises and user awareness training.

Cyberteam Exercises

Specific cybersecurity exercises for cyberteams can reduce vulnerabilities and risk by preparing these teams to properly identify and react to cybersecurity events. One valuable exercise is an "in-house pen test." An organization will divide security employees into opposing teams to conduct a "war game" scenario. Table 9-6 lists the composition and duties of the teams in a pen test war game.

Table 9-6 Penetration-testing war game teams

Team name	Role	Duties	Explanation
Red team	Attackers	Scans for vulnerabilities and then exploits them	Has prior and in-depth knowledge of existing security, which may provide an unfair advantage
Blue team	Defenders	Monitors for Red team attacks and shores up defenses as necessary	Scans log files, traffic analysis, and other data to look for signs of an attack
White team	Referees	Enforces the rules of the penetration testing	Makes notes of the Blue team's responses and the Red team's attacks
Purple team	Bridge	Provides real-time feedback between the Red and Blue teams to enhance the testing	The Blue team receives information that can be used to prioritize and improve their ability to detect attacks while the Red team learns more about technologies and mechanisms used in the defense

Note 11

Sometimes organizations add an incentive called a *capture the flag (CTF)* exercise. A series of challenges with varying degrees of difficulty are outlined in advance. When one challenge is solved, a "flag" is given to the pen tester, and the points are totaled once time has expired. The winning player or team is the one that earns the highest score. CTF events are often hosted at information security conferences or by schools.

Another exercise is to test an incident response plan by conducting simulated testing exercises to make necessary adjustments. The different types of exercises are summarized in Table 9-7.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 9-7 Incident response testing exercises

Exercise name	Description	Example
Tabletop	A monthly 30-minute discussion of a scenario conducted in an informal and stress-free environment	This scenario is presented: An employee casually remarks about how generous it is of a vendor to provide the box of USB drives on the conference room table, embossed with the company logo. After making some inquiries, you find the vendor did not provide USB drives to employees. What do we do?
Walkthrough	A review by IT personnel of the steps of the plan by paying particular attention to the IT systems and services that may be targeted in an attack	A technician with knowledge of the current system will walk through the proposed recovery procedures to determine if there are omissions, gaps, errors, or false assumptions.
Simulation	A hands-on simulation exercise using a realistic scenario to thoroughly test each step of the plan	A simulation of a senior vice president who opens a malicious attachment and introduces malware into the network is presented.
Failover	Testing the process of temporarily switching to backup procedures after an attack	The connection to a server is terminated to determine if the backup server will take over.
Parallel processing	Conducting the same tests simultaneously in multiple environments	A test of an attack against a firewall at the main campus is also conducted at a remote site to determine if the same procedures are applicable.

User Awareness Training

While it is important to conduct exercises for cyber teams, it is likewise important to provide cybersecurity user awareness training to all users. This helps raise the understanding of what cybersecurity risks exist, their potential impacts, and how they can be managed. Training helps make users aware of common risks and how they can become a "human firewall" to help mitigate these risks.

The goal of security awareness training is to help users achieve anomalous behavior recognition (be able to distinguish between what is normal and what is not normal). Training should also empower users to make a determination between that which is unexpected (not anticipated) and unintentional (not done on purpose) and as such it becomes risky (carries a high risk). This is also known as situation awareness.

However, not all user awareness training is effective. There is common training today that is marginally effective and may actually cause more harm than good.

Marginal Training

Suppose one day you received a company email from the HR department about updated employee job descriptions and were asked to verify your current position from the attached document. Or you received an email from the company with the subject line, "Thank You for Being a Valuable Employee" that said you were being recognized by a supervisor and rewarded with a gift card that could be redeemed by clicking a link. Or you received an email from the company's IT staff that said there were changes to the company policies about personal cell phones and you were instructed to click the link to read new policies and sign off by tomorrow. As a dutiful employee, you opened the attachment as instructed or clicked the link.

Gotcha!

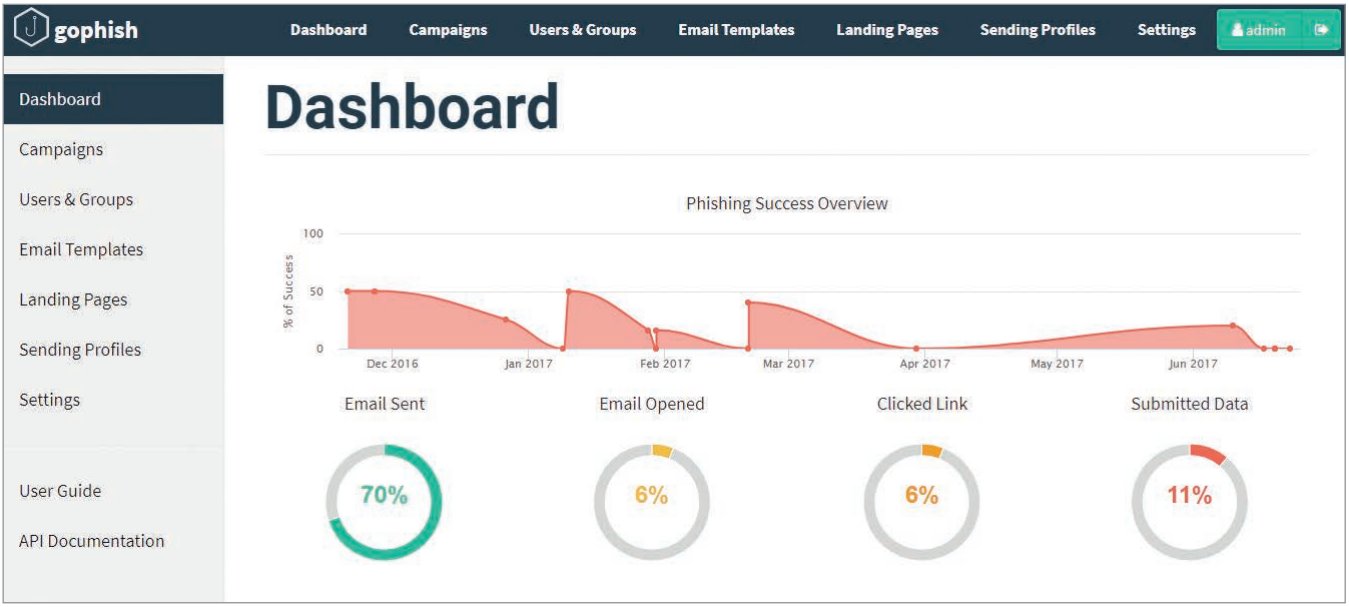
Each of these are actual emails sent by different companies to their employees. While they were legitimate in that they did come from the company itself, they contained fictitious information.

They were all part of a "phishing campaign" simulation test. Employees who received these emails were being tested to see if they would open an attachment or click a link as they might do if they were to receive a legitimate phishing email from a threat actor. Employees who failed the test had to watch hours of online training videos and pass an online test and then be subject to additional unannounced phishing tests.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

These phishing campaigns have become increasingly popular as a means for organizations to test their employees' knowledge of phishing. One security company that specializes in conducting phishing campaigns for organizations typically sends 17,600 emails in one month. They also provide online dashboards so that the organization can monitor test results, as shown in Figure 9-10.

Figure 9-10 Phishing campaign dashboard



Source: gophish

This security company also crafts seasonal emails, such as a notice of Valentine's Day flowers being delivered. In all they have created 20,000 different phishing templates from which organizations may choose to use to test their employees. They also have a "controversial" category of phishing emails that "push the limits" of the test. An example is an HR department distributing updated pay scales in an email attachment.

Although the security company claims that their phishing campaigns reduce the number of employees who fail the test from 33 percent to 5 percent, security researchers claim the opposite. Phishing campaign tests conducted by researchers have found that these campaigns only reduced the overall rate by 1–2 percent. Other phishing campaign tests conducted by researchers found no difference in the rate, and one study showed that any slight improvements disappeared after several months.

But more than being marginally (if at all) effective, phishing campaigns have been shown to have a negative impact on employees:

- Employees resent being tricked and tested without their knowledge.
- Often employees say the advice companies provide on how to combat phishing, like checking every link before clicking or never opening attachments, is impractical and difficult to follow. One IT employee who tried to follow all suggested precautions frequently missed important emails and was reprimanded by their supervisor.
- Phishing campaigns make employees more anxious and experience unnecessary stress.
- These campaigns result in employees distrusting their cybersecurity team, whose purpose is to protect the company and its employees.

Caution

Organizations should consider the broader impacts of phishing campaigns before deciding whether to use them. While there is no surefire way to teach employees how to detect phishing, there are alternative approaches that do not lead to distrust and resentment.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Effective Training

There are techniques that can be used for effective user training. These include:

- **Computer-based training (CBT).** CBT uses a computer to deliver the instruction. It is frequently used for user training due to its flexibility (training can be done from any location and at any time) and ability to provide feedback about the progress of the learner. However, CBT is not always considered the best means of training. Instead, a variety of other modalities, such as specialized face-to-face instruction or informal "lunch-and-learn" sessions, may provide better overall learning results.
- **Role-based awareness training.** Many organizations use role-based awareness training. This involves specialized training that is customized to the specific role that an employee holds in the organization. An office associate, for example, should be provided security training that is different from that provided to an upper-level manager because the duties and tasks of these two employees are significantly different.
- **Gamification.** The fast-growing field of digital gaming is generally divided into two distinct markets: recreational gaming for entertainment and instructional gaming for training and education. Gamification is using game-based scenarios for instruction. User training can often include gamification in an attempt to heighten the interest and retention of the learner.

The content of user awareness training should be such that it provides practical guidance to the users. However, first and foremost, training should clearly emphasize that all computer users in an organization have a shared responsibility to protect the assets of the organization. It cannot be assumed that all users have the knowledge and skill to protect these assets. Instead, users need training on the importance of securing information, the roles that they play in security, and the steps they need to take to prevent attacks. And because new attacks appear regularly, and new security vulnerabilities are continuously being exposed, user awareness and training must be ongoing. User training is an essential element of security.

Note 12

Education in an enterprise is not limited to only certain employees. HR personnel need to keep abreast of security issues because in many organizations, it is their role to train new employees on all aspects of the organization, including security. Even upper management needs to be aware of the security threats and attacks that the organization faces, if only to acknowledge the necessity of security in planning, staffing, and budgeting.

In addition, an awareness program should include the following:

- Recognition of insider threats
- Understanding of operational security
- Attacks through social engineering
- Instruction on password management
- Risks associated with removable media
- Security difference between office work and hybrid/remote work environments
- Security material found in policies and handbooks

Two Rights & A Wrong

1. A Blue team scans for vulnerabilities and then exploits them.
2. A failover is testing the process of temporarily switching to backup procedures following an attack.
3. Role-based training involves specialized training that is customized to the specific role that an employee holds in the organization.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Summary

- While identifying vulnerabilities can be a challenge, there are a variety of diagnostic tools that can be used to assess assets for vulnerabilities. Several vulnerability diagnostic tools are considered as multipurpose tools. The Metasploit framework (MSF) is a flexible and modular penetration-testing platform. MSF is very effective in identifying and taking advantage of a wide array of recognized security flaws, it can support different operating systems (OSs), and its modular architecture allows for flexibility and customization. However, due to its intricate structure and advanced features, it can be difficult for beginners to navigate and use MSF effectively. Recon-ng is a full-featured and open-source reconnaissance framework. It is a web-based tool instead of software that must be downloaded and installed on a local device. Recon-ng is not considered as an alternative to MSF but a complement to it. Another tool is nmap, which is a utility for network discovery and security auditing. Using IP packets, nmap can determine what hosts are available on a network, what services the hosts are offering, such as application name and version, and what types of packet filters or firewalls are in use.
- Vulnerabilities in web applications continue to be a leading attack vector today. The OWASP Zed Attack Proxy (ZAP) is considered the premiere open-source tool for diagnosing web applications. ZAP is a Java-based tool with a highly usable GUI that allows testers to perform fuzzing, scripting, and other actions to attack web apps. Other web application vulnerability diagnostic tools include Burp Suite (a tool that performs both a static and dynamic analysis), Nikto (a command-line open-source tool), and Arachni (a modular open-source tool). Several can be used to identify vulnerabilities in cloud platforms, such as Prowler, Scout Suite, and Pacu. However, instead of the user utilizing these tools to search for vulnerabilities, cloud providers are now offering these services so that users can quickly assess their security posture.
- The introduction of WLANs has increased the attack surface for threat actors, creating several data entry points into the network through which attackers can inject attacks or steal data. Different tools can be used to diagnose wireless vulnerabilities. These tools, based on Linux, typically discover wireless vulnerabilities through exploitation. Aircrack-ng can monitor wireless networks and perform attacks to uncover vulnerabilities. Other Linux-based wireless vulnerability tools include BoopSuite, Airgeddon, Trackerjacker, and WPSIK.
- It is important to respond to vulnerabilities once they have been identified through assessment tools. Action plans are comprised of all the steps of the tasks needed to meet an objective. They are different from a "to-do" list in that they focus on the achievement of a single goal while a to-do list is typically a set of unrelated tasks. Although action plans vary when responding to vulnerabilities, most plans cover the basic steps of using compensating controls, enforcing patching, and executing configuration management. A compensating control is a control that provides an alternative to normal controls that for some reason cannot be used. Compensating controls in cybersecurity involve taking preventive measures and implementing proactive strategies to protect information systems from cyber threats. An action plan in itself can be considered a compensating control. Addressing out-of-date and vulnerable software through patches is considered an important step in an action plan to respond to vulnerabilities. This is because it is the easiest, quickest, and most economical approach to managing vulnerabilities, and generally will address a high number of exposed vulnerabilities. Configuration management is a process for maintaining computer systems, servers, applications, network devices, and other IT components in a desired state. It includes establishing a clear approach to documentation, maintenance, and change control so that systems can be configured consistently and accurately across environments.
- There are often external factors that may impact how, when, or even if a change can be made to address a vulnerability. These inhibitors are often due to interoperability agreements, or formal contractual relationships. These agreements include a service-level agreement (SLA), a service-level objective (SLO), a memorandum of understanding (MOU), an interconnection security agreement (ISA), and a nondisclosure agreement (NDA). Another inhibitor can be the organizational governance of the company. On some occasions, addressing a vulnerability may change or even eliminate a function of an application for the sake of making

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

it more secure. This is known as degrading functionality and may invoke stiff resistance when users have been accustomed to a function or option. Another "pushback" from the organization to implementing tighter security by addressing vulnerabilities is the reluctance by the organization to make any changes to a system that is properly functioning.

- There are tools that can help cybersecurity teams determine if they are taking the right steps. Key performance indicators (KPIs) are designed to clearly articulate and provide insight into what an organization needs to measure. Cybersecurity metrics are the cybersecurity data that an organization tracks on a daily, weekly, monthly, and annual basis. KPIs indicate what should be measured while metrics are the measurements themselves. There are generally recognized top 10 KPIs, which are considered the most important.
- Vulnerability management communication and reporting is a necessary and important step. This not only serves to inform all relevant stakeholders of the vulnerabilities identified but also documents mitigation efforts to reduce the harm of a hazard toward protecting assets. There are different levels of reports that should be distributed to specific audiences who have an interest, sometimes called stakeholder identification and communication. Because these stakeholders are both internal and external to the organization, the scope and depth of the reports vary. The internal stakeholder reports are specific in their detail and scope. This is because the audience is part of the organization itself and requires more in-depth information so that it can be acted upon. However, to external stakeholders, detailed reporting that is provided to internal stakeholders is not necessary and, in many instances, should be avoided. One common external stakeholder report is directed at external regulatory bodies that create and enforce regulatory compliance laws and regulations called a compliance report.
- The contents of reports will vary depending on the audience. In general, a report typically has common elements. The executive summary is the first section of the report and should provide a concise overview of the main content of the report about the assessment. Its purpose is to capture the attention and interest of the readers so that the significance of the assessment and its findings can be clearly communicated. The background and context section should explain the reasons and goals for conducting the assessment, such as complying with regulations, improving the security posture, or addressing specific issues. The assessment methodology section should describe the tools, techniques, standards, and criteria that were used to perform the assessment. It should explain how the system or network was scanned, tested, and analyzed and how the vulnerabilities and risks were identified, classified, and scored. The assessment findings section presents the detailed and comprehensive results of the assessment. The assessment recommendations section should provide the specific and actionable steps that need to be taken to address and resolve the vulnerabilities and risks uncovered in the assessment. The assessment limitations section should acknowledge and disclose any factors that could affect the accuracy, completeness, or relevance of the assessment results and recommendations.
- A numeric score is usually assigned to a vulnerability based on the Common Vulnerability Scoring System (CVSS), ranging from 0 (lowest priority) to 10 (most critical). These numeric scores are generated using a complex formula that considers such variables as the access vector, attack complexity, authentication, confidentiality of the data, and the system's integrity and availability. However, CVSS scores cannot take into account the risk toward an asset within a specific organization since there is no insight by CVSS into the organization's security defenses. Several security vendors have created their risk score by supplementing CVSS scores with additional data to determine the impact of a vulnerability. Another element of vulnerability management communication and reporting are vulnerabilities that continue to occur, called recurrence. There are several situations in which a vulnerability may reoccur. Vulnerabilities that were once mitigated but now recur represent security processes and organizational issues that must be handled differently.
- An often-overlooked nontechnical control for reducing vulnerabilities and risk is conducting awareness, education, and training regarding the risks associated with cybersecurity attacks and how to properly defend against these attacks. Specific cybersecurity exercises for cyberteams can reduce vulnerabilities and risk by preparing these teams to properly identify and react to cybersecurity events. One valuable exercise is an "in-house pen test" in which an organization will divide security

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

employees into opposing teams to conduct a "war game" scenario. Another exercise is to test an incident response plan by conducting simulated testing exercises to make necessary adjustments. While it is important to conduct exercises for cyber teams, it is likewise important to provide cybersecurity user awareness training to all users. However, not all user awareness training is effective. Controversial phishing campaigns have been shown to be marginally effective and often create a backlash from employees who resent being tricked or tested. Techniques for effective user training include computer-based training (CBT), role-based awareness training, and gamification.

Key Terms

action plan
affected hosts
Arachni
awareness, education, and training
Burp Suite
business process interruption
changing business requirements
compliance report
critical vulnerabilities
degrading functionality
key performance indicators (KPIs)
legacy systems
memorandum of understanding (MOU)
Metasploit framework (MSF)
metrics
mitigation
Nikto
nmap
organizational governance
Pacu
priority systems
Prowler
Recon-ng
recurrence
risk score
Scout Suite
service-level agreement (SLA)
service-level objective (SLO)
stakeholder identification and communication
tabletop
top 10 KPIs
trends
Zed Attack Proxy (ZAP)

Review Questions

1. Which of the following is NOT a feature of MSF?
   a. It has a CLI instead of a GUI.
   b. There are two available editions.
   c. It is a module penetration-testing platform.
   d. It is based on the programming language Ruby.
2. Which of the following is a web-based reconnaissance vulnerability assessment tool?
   a. MSF Cloud
   b. Recon-ng
   c. GDB
   d. Arachni
3. Which of the following is NOT correct about nmap?
   a. Nmap cannot scan large networks.
   b. It uses IP packets.
   c. Nmap can be used for OS fingerprinting.
   d. It can determine what types of packet filters or firewalls are in use on the network.
4. Which of the following is NOT an OS tool?
   a. Nikto
   b. Ping
   c. Traceroute
   d. Dig
5. Which tool is an exploitation framework for AWS?
   a. ARC
   b. Prowler
   c. Scout Suite
   d. Pacu
6. What is the change in direction regarding identifying cloud infrastructure vulnerabilities?
   a. Regulatory bodies have relaxed their requirements regarding cloud infrastructure security.
   b. Fewer cloud infrastructure tools are available than in the past.
   c. Cloud providers are offering services to assess a user's cloud security.
   d. Scanning a cloud infrastructure for vulnerabilities takes too long given the increase of users who now have cloud accounts.
7. Which of the following tools would NOT be used to uncover vulnerabilities in a wireless network?
   a. Airgeddon
   b. Prowler
   c. BoopSuite
   d. WPSIK

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

8. How does an action plan compare with a to-do list?

   a. Action plans are identical to a to-do list.
   b. To-do lists are considered more complicated than an action plan.
   c. To-do lists can provide a framework for thinking about how to complete a project in its totality while an action plan cannot.
   d. Action plans focus on the achievement of a single goal while a to-do list is typically a set of unrelated tasks.

9. Which of the following is a service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service?

   a. ISA
   b. MOU
   c. SLO
   d. SLA

10. What is the term used to describe addressing a vulnerability that may change a function of an application?

    a. Application obsolescence
    b. Priority failure
    c. Degrading functionality
    d. Regression creep

11. Which tool can help cybersecurity teams determine if they are taking the right steps?

    a. XRSs
    b. KPIs
    c. XPSs
    d. AWRs

12. Which of the following refers to the average time required to shut down all attack vectors across all endpoints and minimize the probability of any further damage?

    a. MTTA
    b. MTTR
    c. MTTD
    d. MTTC

13. Which of the following is NOT a recipient of an internal stakeholder report?

    a. Security teams
    b. Application developers
    c. System and network engineers
    d. Regulatory bodies

14. Which of the following sections of a report describes the tools, techniques, standards, and criteria that were used to perform the assessment?

    a. Findings
    b. Background and context
    c. Methodology
    d. Executive summary

15. Which of the following is NOT true about the assessment limitations section of a report?

    a. It should indicate how limiting factors were addressed or mitigated.
    b. It may include technical constraints, human errors, time constraints, scope limitations, or assumptions.
    c. It should acknowledge and disclose any factors that could affect the accuracy, completeness, or relevance of the assessment results and recommendations.
    d. It should avoid recommendations for future assessments.

16. What is a risk score?

    a. Another name for a CVSS score.
    b. The percentage of probability of an attack based on a vulnerability.
    c. A value created by the Paclou tool to indicate the likelihood of an attack.
    d. An additional score that is created by vendors to supplement CVSS scores.

17. Which of the following would NOT cause a recurrence?

    a. Restarting a disabled service
    b. Implementing a new firewall rule
    c. Using a vulnerable open software library
    d. Installing a vulnerability scanner

18. Which team provides real-time feedback to enhance an in-house pen test?

    a. Purple team
    b. Red team
    c. Blue team
    d. Orange team

19. Which incident response testing exercise is a monthly 30-minute discussion of a scenario conducted in an informal and stress-free environment?

    a. Runthrough
    b. Simulation
    c. Tabletop
    d. Walkthrough

20. Which of the following is NOT a technique that can be used for effective user awareness training?

    a. Computer-based training (CBT)
    b. Phishing campaign
    c. Role-based awareness training
    d. Gamification

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Projects

Case Project 9-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. What should Tokelau have done to avert this problem? What should ICANN have done to prevent this issue? How can Tokelau create a positive Internet image while also demonstrating self-determination? Write a one-page paper about this topic.

Case Project 9-2: Cyber Insurance Access

Estimated Time: 25 minutes
Objective: Contextualize the potential advantages and disadvantages of cyber insurance access to web security information.
Description: Cloud providers are now offering users the ability to allow cyber insurance companies to access their web security information from the user's AWS Security Hub. This gives potential insurers a list of controls that are enabled on a particular account, information on vulnerabilities, and other details. Cyber insurance carriers can quickly evaluate the organization's application for cyber insurance against AWS's standards for security best practices and their own underwriting standards. Insurers often offer discounts since they have full visibility into the organization's security. But what are the downsides of allowing cyber insurers to access this information? Could it be weaponized and used against the company? Are there other parallels you can find about allowing insurance companies access to data? Debate the pros and cons of allowing cyber insurance companies access to security information. Write a one-page paper on your research.

Case Project 9-3: Web Application Tool Comparison

Estimated Time: 20 minutes
Objective: Compare and contrast web application tools.
Description: The OWASP Zed Attack Proxy (ZAP) is considered the premiere open-source tool for diagnosing web applications. Other web application vulnerability diagnostic tools include Burp Suite (a tool that performs both a static and dynamic analysis), Nikto (a command-line open-source tool), and Arachni (a modular open-source tool). Use the Internet to research these four tools. Identify their strengths and weaknesses along with their use cases. Write a one-page paper comparing these tools.

Case Project 9-4: Review Vulnerability Reports

Estimated Time: 25 minutes
Objective: Critique a vulnerability report.
Description: Use the Internet to find samples of at least three vulnerability reports. Compare these samples. Do the reports have all the elements that should be in a report (executive summary, background and context, methodology, findings, recommendations, and limitations)? Which section is the strongest? Which is the weakest? How would you make the report better? Create a one-page paper on your analysis.

Case Project 9-5: Phishing Campaigns

Estimated Time: 25 minutes
Objective: Research the value of phishing campaigns.
Description: Phishing campaigns have come under increasing attack by employees but are increasingly being used by companies to test employees. What do you think about phishing campaigns? Do their benefits outweigh their disadvantages? If you were responsible for training employees, would you use phishing campaigns? If so, at

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

what level: a basic phishing campaign or a "controversial" campaign? What alternatives to phishing campaigns can help employees see the risks associated with phishing attacks? Finally, research the Internet for recommendations regarding how not to succumb to a phishing email. Are these reasonable? Is there a clear and consistent means to know that an email is phishing? Write a one-page paper on your findings.

Two Rights & A Wrong: Answers

Identifying Vulnerabilities

1. An MSF session typically involves four phases.
2. Recon-ng is a proprietary framework.
3. Dynamic analysis searches for flaws from the outside of an application with no knowledge of the software's structure or source code.

Answer: The wrong statement is #2.
Explanation: Recon-ng is an open-source framework.

Responding to Vulnerabilities

1. Action plans are different from a "to-do" list in that they focus on the achievement of a single goal.
2. An action plan can be considered as a compensating control.
3. An SLA is an agreement between two or more parties that demonstrates a convergence of will.

Answer: The wrong statement is #3.
Explanation: An MOU is an agreement that demonstrates a convergence of will.

Communicating and Reporting Vulnerabilities

1. The executive summary is the first section of the report and should provide a concise overview of the main content of the report about the assessment.
2. The findings section of a report lists and describes all the vulnerabilities and risks that were detected, along with their severity, impact, likelihood, and exploitability.
3. Several security vendors have created their risk score by supplementing CVE scores with additional data to determine the impact of a vulnerability.

Answer: The wrong statement is #3.
Explanation: Several security vendors have created their risk score by supplementing CVSS scores with additional data to determine the impact of a vulnerability.

Conducting Exercises and Awareness Training

1. A Blue team scans for vulnerabilities and then exploits them.
2. A failover is testing the process of temporarily switching to backup procedures following an attack.
3. Role-based training involves specialized training that is customized to the specific role that an employee holds in the organization.

Answer: The wrong statement is #1.
Explanation: A Red team, not a Blue team, scans for vulnerabilities and then exploits them.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Part 4

Incident Response Management

Vulnerability management seeks to uncover how exposed the organization may be to threats and how to mitigate those vulnerabilities. However, despite the best efforts at building a defense, attacks will be successful. Cyber incident response management addresses how to react to a successful attack in order to contain it, minimize its impact, restore the systems to their pre-attack state, and make the necessary changes to stop future attacks. The chapters in this final part focus on incident response management. Chapter 10 examines the planning for incident response, Chapter 11 looks at the activity phases of how organizations respond to a cyber incident, and Chapter 12 concludes by examining data protection and utilization.

Chapter 10
Incident Response Planning

Chapter 11
Incident Response Activity Phases

Chapter 12
Data Protection and Utilization

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 10

Incident Response Planning

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Describe an incident response plan
2. Explain how to use plans and frameworks
3. Discuss how to review the criticality of data
4. Identify stakeholders and the information to be shared with them
5. Explain methods for creating communication pathways

#TrendingCyber

Incident response management addresses how to react to a successful attack in order to contain the attack, minimize its impact, and restore systems back to their normal state. Whereas incident response is a challenge for any organization, there are two types of organizations that are having the most difficulty. What's particularly concerning is that, unlike a compromised business enterprise in that only their customers are affected, these organizations provide services to all individuals in a geographic area. And the services that they provide are considered critical. What are the two types of organizations that have the most difficulty with incident response? They are local governments and publicly owned utilities that provide electricity, gas, water, and sewer services.

Local government agencies are an increasingly attractive target for threat actors, particularly public schools and public hospitals. These agencies from Baltimore to Los Angeles have experienced high-profile attacks in recent years. The number of K–12 public schools suffering ransomware attacks now number about 2,000 annually (these attacks almost doubled from 2021 to 2022). This increase is likely related to the fact that public education has dramatically increased its use of technology for instruction in recent years. This increase was rapidly accelerated by the COVID-19 pandemic that forced schools to pivot overnight to new instructional technologies to support remote learning. It has been recognized that this rapidly increased usage and reliance on technology in public education came without cybersecurity protections being first planned and then implemented.

Likewise, public hospitals' reliance on technology has also dramatically increased. This has been accelerated by more technology being used to optimize administrative operational functions, such as using "bots" to determine patient eligibility and manage billing processes. In addition, more hospitals are using remote patient monitoring through medical Internet of Things (IoT) devices. And there has been a shift to online telehealth services, which grew from 0.1 out of every 100 appointments pre-pandemic to a quarter of all appointments conducted online during the pandemic (that number has now decreased to 7 out of every 100).

This rapid adoption of technology in both public education and public hospitals has unfortunately not resulted in a parallel rapid increase in cybersecurity protection. Most local governments lack the funds to invest in state-of-the-art cyber-defense technology. While there is cyber insurance available for purchase, the costs can be prohibitive for smaller government agencies. And many cyber personnel in these public agencies are paid far less than what they

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

could earn in a large enterprise. This has resulted in a continual "churn" of experienced cyber technicians leaving public agencies for higher-paying jobs. And recent college graduates are quickly being "snapped up" and employed by enterprises instead of working for public organizations. These factors leave public schools and public hospitals particularly vulnerable to attacks.

And these attacks are now having an even worse impact on local governments.

Local government agencies are rarely fully supported through taxes. Instead, they must issue municipal bonds ("munis") to raise money. Munis are debt securities issued by states, cities, counties, and other governmental entities to fund day-to-day obligations and to finance capital projects such as building schools, roads, and sewer systems. Investors who purchase munis are lending their money to the municipality bond issuer in exchange for a promise of regular interest payments plus the return of the original investment (principal). A muni bond is attractive to investors because of their stability (a government rarely declares bankruptcy) and the ability to provide a steady income stream. In addition, the interest earned is exempt from federal taxes and often state and local taxes.

Due to the rash of cyberattacks on these government agencies, investors are now seeking answers to cybersecurity questions before buying munis—or opting for a safer investment elsewhere. Ratings firms are asking local governments (called "due diligence") who are issuing munis questions about their cybersecurity protections that they have in place, such as whether they have cyber insurance and the details of their incident response plans, particularly how quickly they are prepared to respond and recover in a cyberattack. Cybersecurity has now become a risk factor in buying munis and, because of the higher risk from cyberattacks, some investors are shying away from purchasing them. In order to entice investors, government entities may have to offer a higher interest rate, which then results in higher costs that can reduce the total amount of money that can be raised through a muni. Researchers have found that following a ransomware attack, local governments have spent 50 percent more on technology protections, but bond yields (the return an investor expects to receive) fell by 0.03 percentage points. Thus, local governments are being "squeezed" to spend more on cybersecurity at a time when they may have less money to spend.

The second type of organization that has difficulty with incident response are public and private utilities that provide electricity, gas, water, and sewer services. Utilities fall into three ownership types: investor-owned utilities, cooperatives, and publicly owned utilities (POUs). POUs include those run by federal, state, and local municipalities. In addition to government entities, political subdivisions may run POUs, which are called public utility districts. The United States has 1,958 POUs that provide electricity to an average of 12,100 customers each.

These smaller POUs have likewise been increasingly under attack. In November 2023, the North Texas Municipal Water District was the victim of a ransomware attack, and the Municipal Water Authority of Aliquippa in Pennsylvania was breached by attackers who were targeting Israeli-manufactured equipment. Although neither attack resulted in disruptions to the water supply for their customers, they caused the U.S. government to issue an alert warning of software vulnerabilities in technology that is widely used by heavy industry operators such as water plants. However, an incident in February 2021 at a water plant in Oldsmar, Florida, resulted in an attacker reportedly increasing the levels of lye in drinking water to dangerous levels before being spotted by an employee.

Recent efforts to strengthen cyber standards in utilities have not been successful. Regulations proposed by the Environmental Protection Agency (EPA) that would have forced water utility operators to include cybersecurity in periodic assessments were strongly opposed by the industry. The EPA eventually withdrew the regulations after challenges from trade associations, lawmakers, and state attorneys general in Iowa, Arkansas, and Missouri.

Organizations use reconnaissance for gathering information about users and the organization's network to uncover patterns or correlations in the data in order to mitigate uncovered vulnerabilities. Penetration testing attempts to exploit those vulnerabilities just as a threat actor would. And vulnerability management is an ongoing examination of the organization's security posture.

However, despite these well-established processes for protection, significant gaps in cybersecurity still exist. Only 30 percent of U.S. organizations are considered "cyber-ready" to ward off attacks, and fewer than half (45 percent) have a formal cybersecurity strategy in place while only two-thirds consistently deploy anti-malware technologies.[1] As a result, attacks will invariably be successful on a large number of organizations. And those organizations that do practice good cybersecurity only need a single vulnerability for attackers to exploit in order to become a victim.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

This is where incident response comes into play. Incident response equips an organization to be prepared for the inevitable successful attack so it can address the incident and return to normal operations as quickly as possible. In this chapter, we explore incident response planning.

Charting an Incident Response Plan

Certification

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.

As with virtually all meaningful activities in life, the most important step lies in preparation. The same is particularly true of cybersecurity incident response: preparing in advance for a successful cyberattack is essential. Without advanced preparation, the time to recover from a cyber incident will triple or even quadruple, inflating from days to weeks and even months—and in some instances an organization will never recover. The importance of preparation for a cyber incident can never be underestimated.

Charting an incident response plan involves first defining a cyber incident and a cyber incident response plan. It also involves building a cyber incident response team and employing testing and training.

Defining a Cyber Incident

Which sounds worse: a breach, attack, or incident?

Most users would probably say that breach or attack sounds worse than an incident. That is likely because the word *incident* is often used to refer to an event or occurrence that is either positive ("That was as wonderful an incident as you could imagine") or negative ("As small as that incident was, it marked a change in their behavior").

However, in cybersecurity, an incident carries a different definition. A "cyber incident" is the act of violating an explicit or implied security policy. A cyber incident does not necessarily have to be successful: a failed attempt likewise qualifies as a cyber incident. Any of the following may be considered a cyber incident, whether failed or successful:

- Gaining unauthorized access to a system or its data
- Causing unwanted disruption or denial of service
- Accessing a system for the processing or storage of data
- Making changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

Note 1

Sometimes a further distinction is made between a "security event" (any occurrence in a system, network, or application that may have security implications but is not necessarily malicious or dangerous), an "adverse security event" (a security event that has negative consequences), and a "security incident" (adverse security events that have either caused or threatened to cause a violation of the organization's security policies).

As the term implies, a cyber incident response is the actions that an organization takes in reaction to a cyber incident. Cyber incident response involves creating and managing a cyber incident response plan.

What Is a Cyber Incident Response Plan?

A cyber **incident response plan** is a detailed document that clearly outlines the roles, responsibilities, and processes for responding to a cyber incident. While the number may vary as they are combined or separated, there are generally seven actionable goals to a cyber incident response plan, as seen in Figure 10-1. The actionable goals are detailed in Table 10-1.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 10-1 Cyber incident actionable goals

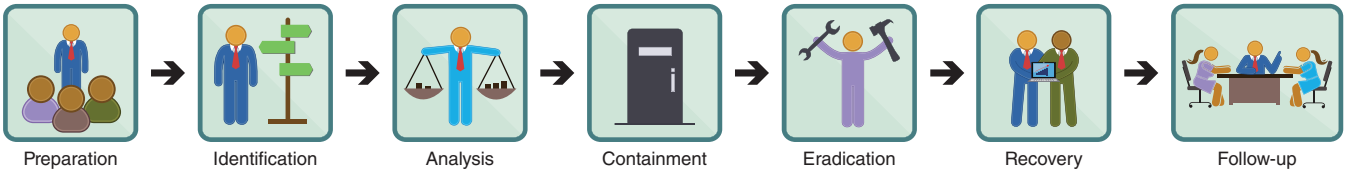


Table 10-1 Goals of cyber incident response plan

Plan item	Goal
Preparation	Equip users and systems to handle incidents as they occur
Identification	Decide if the action is a cybersecurity incident that requires an immediate response
Analysis	Determine how the incident functions, identify the affected systems, and gauge the overall impact
Containment	Isolate the affected systems to prevent further damage
Eradication	Remove affected systems from production to eliminate the root cause
Recovery	Permit affected systems back into the production environment
Follow-up	Review and analyze results to improve future efforts

A cyber incident response plan is also called an incident response **playbook**. A playbook lists specific actions or a set of rules that describe steps to take in response to a security incident. Playbooks are intended and designed to help organizations respond quickly and effectively to cyberattacks. Playbooks most often include steps designed to identify threats, contain incidents, analyze cyber events, and communicate and document incidents.

Building a Cyber Incident Response Team

A cyber incident response plan should be facilitated by a cyber incident response team. Such a team is the "engine" behind the plan that analyzes information, takes appropriate actions, and shares important communications across all stakeholders. The incident response team's primary objective is to coordinate and align the key resources during a cyber security incident to minimize its impact and to restore operations as quickly as possible. This includes tasks such as investigation and analysis, communications, documentation, and timeline development. At a minimum, a cyber incident response team should have the members outlined in Table 10-2.

Table 10-2 Members of a cyber incident response team

Role	Responsibility
Team leader	Leads and coordinates all incident response team activity and helps the team to focus on minimizing damage and recovering quickly from an incident.
Lead investigator	Collects and analyzes evidence to determine the root cause and then directs other security analysts to implement recovery.
Communications coordinator	Actively informs all stakeholders both inside and outside of the organization.
Documenter	Records all team activities, including investigation and discovery and recovery tasks, and creates a workable timeline for each stage.
Legal council	Keeps the team informed of any legal issues that may impact the incident and recovery.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Because an incident may occur at any time, team members must be on call around the clock during their tenure on the team. It is recommended that each team member be provided a "go bag" that contains all the important **incident response tools** needed for an immediate reaction. These tools include a journal, the incident response team contact list, USB flash drives, anti-malware utilities, a laptop computer, and various computer and network tool kits.

Testing and Training

No incident response plan is complete without three key elements: documentation, testing, and training. These include the following:

- **Documentation of procedures.** It is important that all phases of the incident response procedures be clearly recorded (documentation of procedures) in the incident response plan. These procedures should clearly explain the roles and responsibilities and be accessible to all personnel who play a role in the response. These procedures should also be reviewed and revised as necessary on a regular basis.
- **Training.** All personnel involved in responding should receive adequate instruction and coaching (**training**) on how they are to react to an incident.
- **Testing.** Testing is an important step in incident response preparation. This serves as an assessment of all parts of the incident response preparation phase that can uncover weaknesses to be addressed. Incident response "drill" scenarios and "mock" data breaches are critical to evaluating an incident response plan and procedures. And the more prepared employees are through testing, the less likely they will make critical mistakes when an event occurs.

Caution !

Another element of the preparation phase is to ensure that all parts of the incident response plan (such as training, execution, and hardware and software resources) are approved and funded in advance.

Two Rights & A Wrong

1. A cyber incident is the act of violating an explicit or implied security policy whether or not it is successful.
2. The final item in an incident response plan is follow-up.
3. The role of the lead investigator is to lead and coordinate all incident response team activity.

See the answers at the end of the chapter.

Using Plans and Frameworks

Certification

3.1 Explain concepts related to attack methodology frameworks.

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.

When crafting a cyber incident response plan, there are different tools to assist in its development. These include preparatory plans and attack methodology frameworks.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Creating Preparatory Plans

There are different plans that can serve as "preparatory" plans to a cyber incident response plan. These plans are complementary to an incident response plan and cover areas related to—but different from—the incident response plan. Often these plans have been created in advance of a cyber incident response plan and can help shape the plan. These preparatory plans include a business continuity plan, business impact analysis, and disaster recovery plan.

Business Continuity (BC) Plan

Business continuity can be defined as the ability of an organization to maintain its operations and services in the face of a disruptive event or a major disaster. These disasters may be environmental disasters (like floods, hurricanes, and tornados), human-made disasters (like industrial mishaps, chemical spills, and terrorist attacks), or a cyberattack. Although most disasters to threaten an organization are external disasters (like environmental disasters), some are internal (like a fire in a data center).

Business continuity planning is the process an organization undertakes to determine a plan of action to protect itself in advance of a disaster. The outcome of this planning is a **business continuity (BC) plan**, which is a strategic document that provides alternative modes of operation for business activities that, if interrupted, could result in a significant loss to the enterprise. Creating a BC plan involves identifying exposure to threats, creating preventive and recovery procedures, and then testing them to determine if they are sufficient. In short, a BC plan is designed to ensure that an organization can continue to function, known as continuity of operations in the event of an environmental disaster or human-made disaster.

Note 2

A BC plan is essentially recovery planning.

A BC plan should address the following elements:

- **High availability.** A BC plan should address high availability, which is the ability to withstand all outages—planned and unplanned outages and environmental and internal disasters—while providing continuous processing for critical applications. For example, a high-availability solution for critical e-commerce servers and databases could require a fully automated failover to a backup system so that sales can continue functioning without any disruption.
- **Scalability.** Organizations continue to grow and expand on a regular basis. A BC plan that only looks at the organization as it stands today will find that the plan is out of date tomorrow. Instead, a BC plan must have the capability to cover increased capacity; in other words, a BC plan must have scalability.
- **Diversity.** Just as a BC plan must have scalability as capacity increases, it must also include diversity as different technologies, third-party vendors, controls, and even cryptographic solutions are added.
- **On-prem and cloud.** As more and more resources are moved from on-premises to the cloud, a BC plan should have the flexibility to address this movement without needing to rewrite the plan regularly.

Note 3

Similar to creating a BC plan is continuity of operation planning (COOP). This is a federal initiative intended to encourage organizations (and departments within an organization) to address how critical operations will continue under a broad range of negative circumstances. COOP addresses emergencies from an "all-hazards approach" instead of focusing more narrowly on a specific event. It is designed to establish requirements for ensuring that critical functions continue and even includes how personnel and resources can be relocated in case of emergencies.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Business Impact Analysis (BIA)

A business impact analysis (BIA) identifies business processes and functions and then quantifies the impact a loss of these functions may have on business operations. These impacts include the impact on property (tangible assets), finance (monetary funding), safety (physical protection), reputation (status), and even life (well-being). By identifying the critical processes and functions through a site risk assessment (a detailed evaluation of the processes performed at a site and how they can be impacted), a BIA can then be the foundation for a functional recovery plan that addresses the steps to take to restore those processes if necessary.

Caution

An organization with remote sites sometimes assumes that all sites perform essentially the same functions as the main headquarters. However, that is not always the case. For example, a third-party vendor was hired to perform a BIA but was told to only look at the headquarters. The vendor convinced the organization to examine all the sites. They found that the headquarters performed over 80 different functions, of which half were centrally managed and implemented. The other 40 functions could be performed at the satellite offices in various combinations, which would have been overlooked if the BIA were not conducted at each site.

A BIA is designed to identify those processes that are critically important to an enterprise. A BIA will help determine the mission-essential function or the activity that serves as the core purpose of the enterprise. For example, a mission-essential function for a hospital could be to "Deliver healthcare services to individuals and their families," while a nonessential function is to "Generate and distribute a monthly online newsletter." In addition, a BIA can help identify critical systems that in turn support the mission-essential function. In a hospital setting, a critical system could be "Maintain an emergency medical facility for the community." Even though this is a critical system, it is not the core purpose of the hospital.

Identifying the single point of failure, which is a component or entity in a system that, if it no longer functions, will disable the entire system, is also a goal of a BIA. A patient information database in a hospital could be considered a single point of failure. Minimizing these single failure points results in a system that can function for an extended period with little downtime.

Disaster Recovery (DR) Plan

Whereas a BC plan looks at the needs of the business as a whole in recovering from a catastrophe, a subset of it focuses on continuity in the context of information technology (IT). This is called a **disaster recovery (DR) plan**, which is involved with restoring IT functions and services. A DR plan is a written document that details the process for restoring IT resources following an event that causes a significant disruption in service. Comprehensive in scope, a DR plan is intended to be a detailed document that is updated regularly.

Most DR plans cover a standard set of topics. One common topic is the sequence in restoring systems. After a disaster has occurred, what should be the sequence in which different systems are reinstated (restoration order)? That is, which systems should have priority and be restored before other systems?

There are several factors that may be considered. One factor is obvious dependencies; that is, the network must be restored before applications that rely on the network are restored. A second factor is the processes that are of fundamental importance to an enterprise: critical systems that support the mission-essential function and those systems that require high availability need to be restored before other systems. Another factor is the alternative business practices, or those "workaround" activities that can temporarily substitute for normal business activities. How long can a manual workaround process meet the temporary needs without causing bigger problems such as unmanageable backlogs?

Analyze Attack Methodology Frameworks

A cybersecurity framework is a series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment. Frameworks are also available that outline in detail how attacks occur. These are called **attack methodology frameworks** or exploitation frameworks. They serve as models of the thinking and actions of today's threat actors.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The most common attack frameworks are the Open Source Security Testing Methodology Manual (OSSTMM), the Open Source Foundation for Application Security (OWASP) Testing Guide, MITRE ATT&CK, Diamond Model of Intrusion Analysis, and Cyber Kill Chain.

Open Source Security Testing Methodology Manual (OSSTMM)

The **Open Source Security Testing Methodology Manual (OSSTMM)** is a peer-reviewed methodology for security testing. It is maintained by the Institute for Security and Open Methodologies (ISECOM) and is updated biannually. ISECOM states that its main objective with the OSSTMM is to provide a scientific process for the accurate characterization of operation security that can be used for penetration testing, ethical hacking, and other security testing. ISECOM focuses on verified facts to make sure that organizations using the OSSTMM for their own penetration testing methodologies can know they are making fact-based decisions.

The OSSTMM provides guidance on how to test the operational security of five channels so that organizations can understand the full extent of their security and determine how well their security processes function. These five channels include:

- **Human security.** The security of human interaction and communication is evaluated operationally as a means of testing.
- **Physical security.** The OSSTMM tests physical security, defined as any tangible element of security that takes physical effort to operate.
- **Wireless communications.** Electronic communications, signals, and emanations are all considered wireless communications that are part of operational security testing.
- **Telecommunications.** Whether the telecommunication network is digital or analog, any communication conducted over telephone or network lines is tested in the OSSTMM.
- **Data networks.** The security testing of data networks includes electronic systems and data networks that are used for communication or interaction via cable and wired network lines.

Open Source Foundation for Application Security (OWASP) Testing Guide

The **Open Source Foundation for Application Security (OWASP) Testing Guide** is designed to help software developers and engineers test web applications to identify security issues. The testing guide describes a general testing framework and techniques required to implement that framework. OWASP also produces guidance for desktop apps, mobile applications, application programming interfaces (APIs), and other forms of software. These testing guides outline five testing principles that can be used to measure software security before, during, and after development. These principles are:

- Define
- Design
- Develop
- Deploy
- Maintain

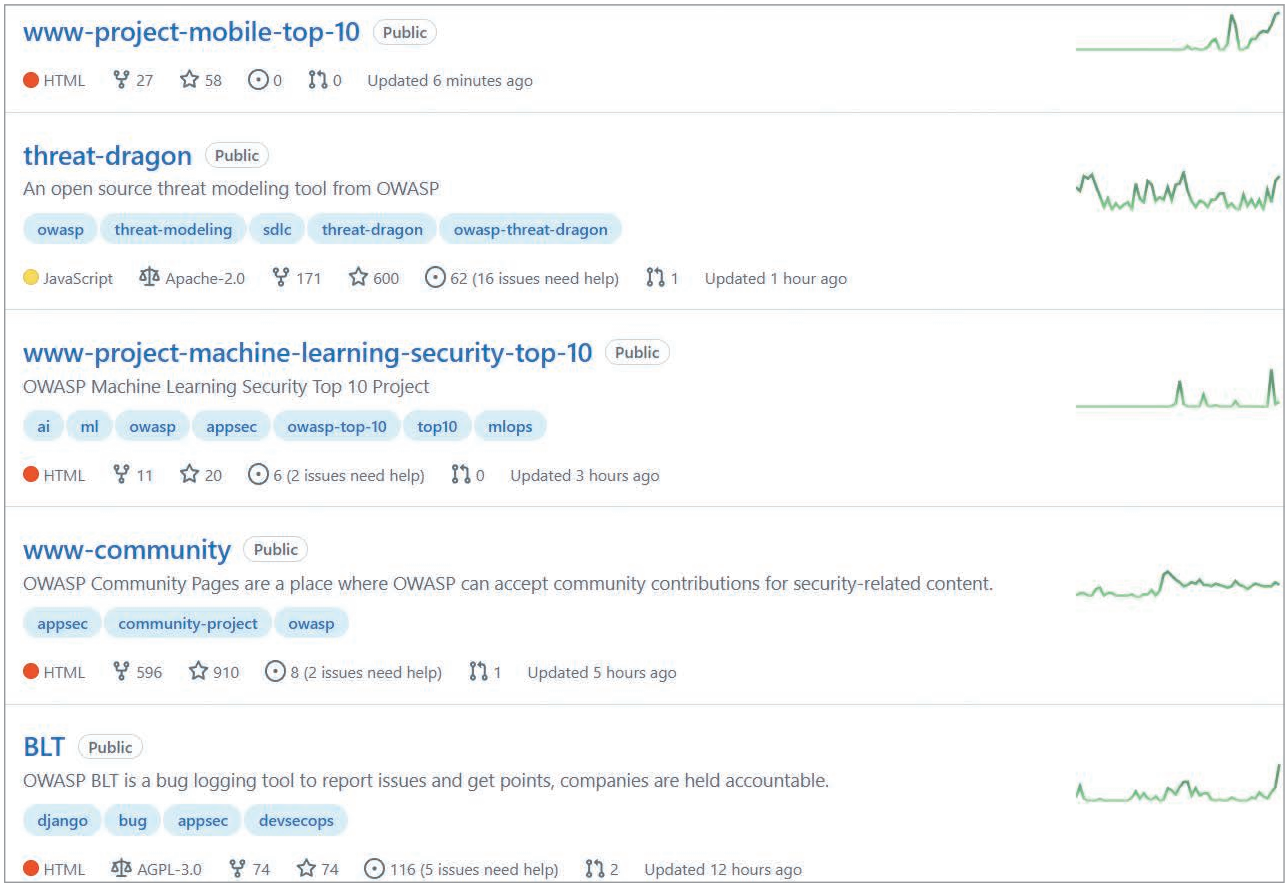
OWASP testing guides are freely available online, along with graphs that indicate the activity over the last year, as seen in Figure 10-2.

MITRE ATT&CK

MITRE ATT&CK is a knowledge base of attacker techniques that have been broken down and contain classification in detail. The attacks are offensively oriented actions that can be used against particular platforms. The focus of ATT&CK is not on the tools and malware that attackers use but instead looks at how they interact with systems during an operation. These techniques are arranged into a set of tactics to help explain and provide context for the technique. Figure 10-3 displays a sample of the ATT&CK framework.

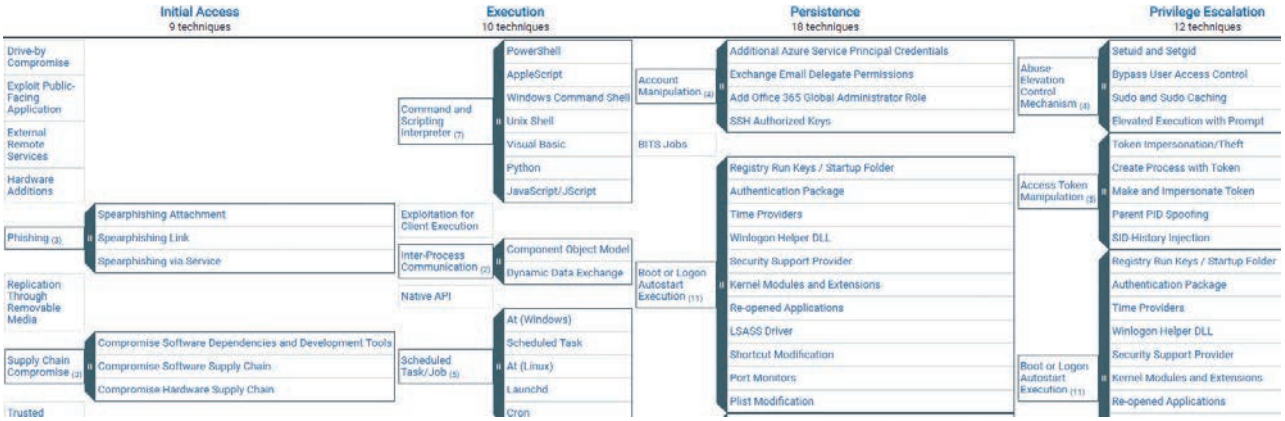
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 10-2 OWASP testing guides and graph activity indicators



OWASP

Figure 10-3 MITRE ATT&CK framework



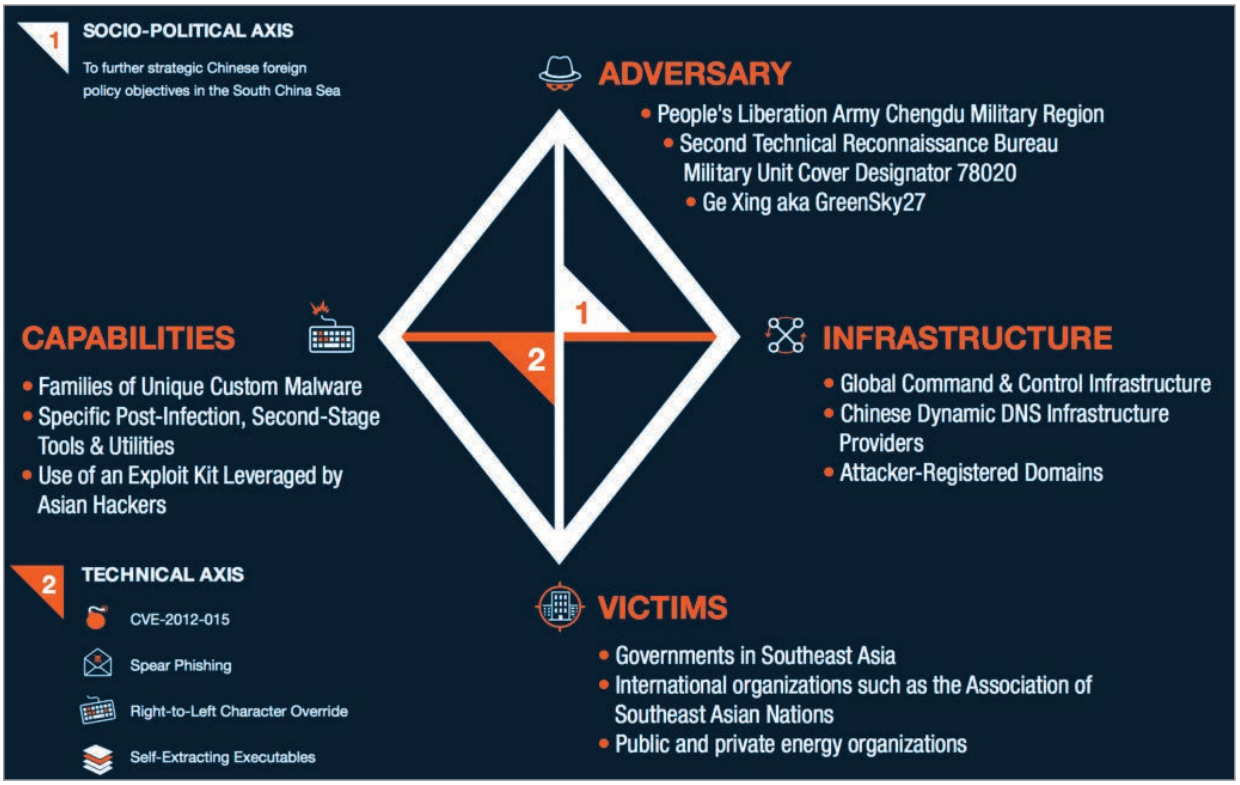
The MITRE Corporation.

Diamond Model of Intrusion Analysis

The **Diamond Model of Intrusion Analysis** is a framework for examining network intrusion events. This framework derives its name and shape from the four core interconnected elements that comprise any event: adversary, infrastructure, capability, and victim. Analyzing security incidents involves piecing together the Diamond using information collected about these four facets to understand the threat in its full context. Figure 10-4 illustrates the Diamond Model.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 10-4 Diamond Model of Intrusion Analysis

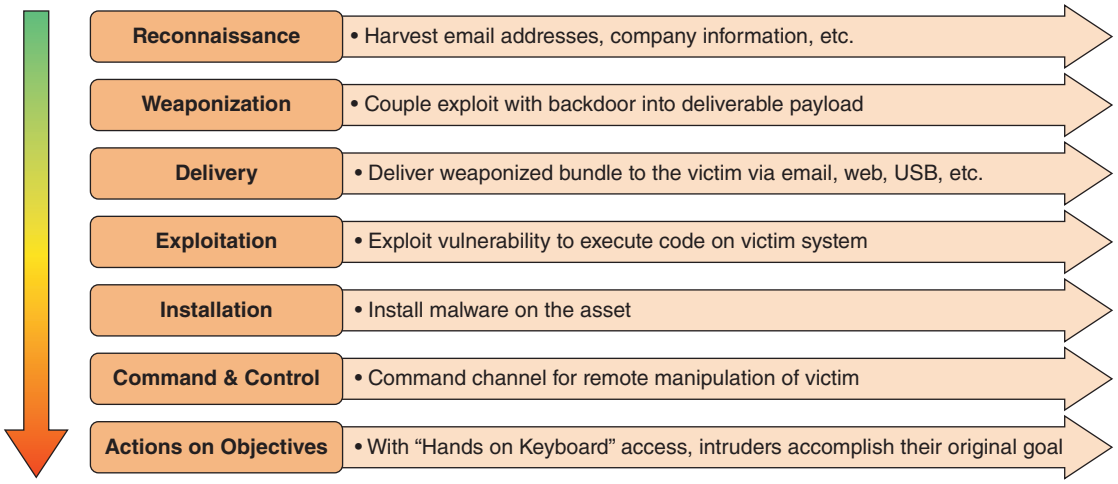


ThreatConnect, Inc.

Cyber Kill Chain

A "kill chain" is a military term used to describe the systematic process to target and engage an enemy. An attacker who attempts to break into a web server or computer network actually follows these same steps. Known as the **Cyber Kill Chain™**, it outlines the steps of an attack. Figure 10-5 shows the Cyber Kill Chain. Its underlying purpose is to illustrate that attacks are an integrated and end-to-end process like a "chain." Disrupting any one of the steps will interrupt the entire attack process, but the ability to disrupt the early steps of the chain is the most effective and least costly.

Figure 10-5 Cyber Kill Chain



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong

1. A BC can be defined as the ability of an organization to maintain its operations and services in the face of a disruptive event or a major disaster.
2. A DR is designed to identify those processes that are critically important to an enterprise.
3. The OSSTMM provides guidance on how to test the operational security of five channels so that organizations can understand the full extent of their security and determine how well their security processes function.

See the answers at the end of the chapter.

Reviewing Criticality of Data

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

Incident response preparation also involves reviewing the criticality of data, known as sensitive data protection. This part of cyber incident response planning is intended to identify the organization's critical data. These "crown jewels" are the assets that require special vigilance and a high degree of protection. Table 10-3 lists critical data types.

Table 10-3 Critical data types

Data type	Description	Examples	Reason for high value
Personally identifiable information (PII)	Data that could identify a specific individual	Full name, Social Security number, driver's license number, bank account number(s), passport number	Can be used by threat actor to steal the identity of a user or conduct financial transactions in the user's name.
Sensitive personal information (SPI)	Information that does not directly identify an individual but is related to the person and communicates information that is private or could potentially harm an individual should it be made public	Biometric data, genetic information, gender, political party affiliation, union membership	Inferences can be made about the data and applied to the individual to place the person in a specific "category" that may or may not be accurate.
Personal health information (PHI)	Information as it relates to a person's health data, transactions, and history	Mental health history, healthcare services used, payments for healthcare services	Federal Health Insurance Portability and Accountability Act (HIPAA) laws require many of the key persons and organizations that handle PHI to have policies and security safeguards in place or face fines.
Financial information	The storage, processing, and transmission of information related to a financial transaction; for an individual, it could be transactions initiated with a credit/debit card and, for an enterprise, it may be detailed accounting data in electronic or paper form that support a financial statement	Name, credit/debit card number, expiration date, card verification value (CVV) for individuals; ledgers, journals, and spreadsheets for enterprises	Loss of data could result in fraudulent purchases by a threat actor in the cardholder's name; loss of accounting data prevents an organization from providing stakeholders an accurate picture of its financial health.

(*continues*)

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 10-3 (*Continued*)

Data type	Description	Examples	Reason for high value
Intellectual property	Creations of the mind, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce	Trademarks, copyrights, patents	These serve to uniquely identify the organization to the public, so any compromise would seriously impact brand recognition and revenue.
High-value asset (HVA) information	Information that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business	Assets, systems, and datasets that contain sensitive controls, instructions, or data used in critical operations, or they may house unique collections of data	The direct exploitation of the data can cause a loss of confidence by the public in the organization.
Corporate information	Data that is confidential to the organization, such as that used to support the consolidation of companies or assets through various types of financial transactions (mergers, acquisitions, consolidations, tender offers, purchase of assets, and management acquisitions)	Discounted cash flow (DCF), replacement cost, enterprise-value-to-sales (EV/Sales) ratio, price-to-earnings (P/E) ratio	The unauthorized premature disclosure of this information could severely impact an organization, such as preventing a merger or acquisition from occurring.

Note 4

In the European Union, even the IP address of an Internet subscriber may also be classified as PII.

In addition, for organizations that are involved with customer retail financial transactions, **cardholder data (CHD)** is also considered critical data to be protected. CHD is comprised of the elements listed in Table 10-4.

Table 10-4 Cardholder data elements

Element	Explanation	Example
Primary account number (PAN)	Unique card number identifying both the card issuer and cardholder	4005550000000019
Cardholder name	Name of cardholder	Lia Shultz
Expiration date	Date that the card expires	04/2026
Service Code	A three- or four-digit code distinguishing between local or international transactions or identifying usage restrictions	111

Two Rights & A Wrong

1. SPI is data that could identify a specific individual.
2. HVA information includes assets, systems, and datasets that control sensitive controls.
3. CHD is considered critical data to be protected.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Identifying Stakeholders

Certification

4.2 Explain the importance of incident response reporting and communication.

Different audiences have a vested interest ("stake") when a cyber incident occurs. Who are these audience members, and what should be communicated to them? The process of identifying them and determining the types of communication for them is known as **stakeholder identification and communication**. Because these stakeholders are both internal and external to the organization, the scope and depth of the communication will vary.

Internal Stakeholders

There are two categories of internal stakeholders with whom there should be coordination of efforts and information. These can be divided by their roles:

- **Technical.** The responsibilities of the technical staff are to identify and then react to the cyber incident. This involves determining the impact of the cyber incident and using forensics to investigate it. They must coordinate and communicate clearly with the cyber incident response team and keep that team continually informed of the impact, the vulnerability that was exposed, the type of threat, and the severity of the threat.
- **Management.** As the cyber incident response team receives information from the technical staff, they are responsible for coordination with the organization's managerial teams. The management teams can then provide input and make the appropriate business-level decisions based on the cyber incident. Management stakeholders include **public relations** (specialists who manage an organization's public image and reputation), human resources (because a cyber incident may impact employee contracts and employment laws, those who handle the human assets may need to be involved), **legal** (the department that handles legal matters for ensuring compliance with laws and regulations), and senior leadership (the executive-level managers).

External Stakeholders

There are also external stakeholders who need to be identified for communications. These include customers, media, law enforcement agencies, and incident response providers.

Customers

Although sometimes used synonymously, "customers" differ from "clients" in several ways:

- **Client.** A client is a person or entity that purchases professional services from a business, which may include advice and solutions as well as products. Clients typically have long-term relationships with the organizations from whom they purchase, and they tend to make purchases based on experience and trust. They tend to remain loyal to the business for a long period of time.
- **Customer.** A customer is someone who buys products or services from a company. The factors that typically influence their purchasing decisions are low prices and high value. Customers may end their engagements with businesses once they receive the goods or services they purchase, and they often migrate to another business from which to purchase if it has lower prices or higher value.

Because customers tend to only have a limited relationship with an organization and not a longer-term trusting relationship like a client, customers often react more swiftly and negatively when news of a cybersecurity incident occurs due to a vulnerability in the organization's security. This makes it critical for public relations to craft messages to customers (**customer communications**) that focus on providing clear and straightforward information that serves to allay fears. Characteristics of good customer communications are summarized in Table 10-5.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 10-5 Characteristics of good customer communications

Characteristic	Explanation
Timeliness	Waiting too long can allow misinformation to spread rapidly; as soon as possible, but not before facts are established, customer communication should begin.
Transparency	Organizations should be open and honest to customers about what has occurred.
Repetition	Following up with repeated updates can help assure customers that action is being taken and the incident is not forgotten.
Ownership	Attempting to "shift the blame" to another entity for the cyber incident can come off as trying to avoid responsibility.
Clarity	A clear explanation of what occurred should answer questions such as, "What happened?", "What customer data was involved?", "What are we doing?", and "What can you do?"

Caution

Public relations employees must be cautious in customer communications to make sure they sound genuine. Well-worn statements such as "The security of your data is very important to us" immediately after a major security breach can sound insincere, condescending, and even patronizing.

Media

The news media, often just called the **media**, is the industry that delivers news to the general public. This includes print media, broadcast media, and Internet-based media.

It is important to remember that the goals of the media are very different from those of customers. Customers want reassurance while the media is seeking to gain an audience by being the first to "break the news." This means that when information about a cyber incident occurs, then reporters will often report that story with or without the help of the organization's public relations team. The media will often tell their audience what is known at the moment—even if the information is incomplete—with the promise that more details will follow later.

Instead of shutting out reporters, which opens the door to wild speculation, savvy public relations employees understand that the media can be their greatest ally. Through the media, public relations employees can minimize the spread of misinformation and reach their constituents with the truth more quickly. And by offering accurate and available information, the organization can appear responsive, credible, concerned, and helpful.

Best-practices public relations should follow when dealing with the media include:

- Be available initially at any time to work with reporters, who may have varying deadlines.
- Be respectful, professional, courteous, responsive, and cooperative.
- Give reporters a reasonable timeframe as to when to expect updates.
- Never say "No comment" but instead tell reporters that the situation is still being reviewed and a statement will be made as soon as more facts are available.
- Frame the information provided to media requests in order to define and control public perceptions of how the organization is handling the crisis.

Caution

It is vital for public relations to respond quickly to reporters even if there is little to say. When an organization does not respond, it appears they have something to hide. If it is not possible to release any information at that time, public relations should take control of the story by explaining why that is the case. By offering an explanation, they appear responsive and cooperative even if they do not have anything pertinent to share.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Law Enforcement Agencies

While a data breach may require that an organization contact the affected parties, the question is often raised regarding the need to contact **law enforcement agencies** (entities that are authorized to prevent, detect, investigate, or prosecute criminal law violations) after a cyber incident has occurred. In one study, it was revealed that only 28 percent of businesses in the United Kingdom reported a cybercrime to law enforcement agencies.[2] In the United States, the FBI estimates that only 15 percent of victims report their crimes.[3] There are several reasons often cited for the reluctance to report cyber incidents to law enforcement agencies:

- Identifying threat actors, especially when attacks come from abroad, is notoriously difficult for domestic law enforcement agencies and often leads to no arrests or convictions.
- While the interest of the organization is to resume operations as quickly as possible, the interest of law enforcement is to identify, track down, and prosecute the perpetrator. This may result in competing interests and may impede the organization resuming normal operations as law enforcement seeks to retain evidence and launch their own investigation.
- Reporting an incident may lead to it becoming public knowledge and will harm the organization's reputation unnecessarily.

However, there are advantages to reporting a cyber incident:

- Law enforcement agencies can work with foreign counterparts to stop organized cybercrime gangs, which can help reduce the number of overall attacks on a business.
- Large federal law enforcement agencies have many resources and experience and can even make the company's own internal investigation easier by having these experts on hand.
- Companies reporting to law enforcement can help provide information toward intelligence-sharing efforts.
- Many law enforcement agencies stress that a business might have the missing piece of the jigsaw puzzle that can be used to help capture repeat cyber criminals.

Note 5

The primary federal law enforcement agencies that investigate domestic crime on the Internet include the Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF).

Different law enforcement agencies have responsibilities to investigate different types of cybercrime. These agencies are listed in Table 10-6.

Table 10-6 Law enforcement agencies' responsibilities

Type of cybercrime	Law enforcement agency responsible
Computer intrusion, password trafficking	FBI local office, Secret Service, Internet Crime Complaint Center
Child pornography or exploitation	FBI local office, Immigration and Customs Enforcement (if material originated overseas), Internet Crime Complaint Center
Internet fraud	FBI local office, Secret Service, Federal Trade Commission, Securities and Exchange Commission (if involves investment-related fraud), Internet Crime Complaint Center
Harassment	FBI local office

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Incident Response Providers

Due to the complexities of a cyber incident response, some businesses turn to a third-party organization to provide assistance. These organizations are called incident response providers. Although these providers may not perform the communication themselves, they can help facilitate communication between the different parties. These providers can give assistance to any or all parts of cyber incident investigation, including preparation, incident response management, data identification, evidence collection, and data recovery.

One area of specialization is providing litigation support to help their clients be successful if a cyber incident results in legal actions against an organization. Incident response providers can author expert reporting declarations and affidavits to support the case based on the collected evidence and key findings of the investigation. Independent assessments of compliance with consent decrees, agreements, court orders, contractual obligations, and other requirements can also be provided.

Note 6

Some incident response providers even offer expert witness training by law professors and attorneys to assist employees who must testify in court.

Two Rights & A Wrong

1. The two categories of external stakeholders are technical and management.
2. A client is not the same as a customer.
3. Password trafficking falls under the jurisdiction of the FBI local office, Secret Service, and Internet Crime Complaint Center.

See the answers at the end of the chapter.

Constructing Communication Pathways

Certification

4.2 Explain the importance of incident response reporting and communication.

One of the most important elements of a cyber incident response plan is determining a communication plan. This plan will indicate how, when, and what type of information about the incident will be distributed and to whom. There are also communications best practices.

Reasons for Communications

Why should an organization communicate that a cyberattack against them has been successful? Wouldn't revealing the news just bring bad publicity? Why not then keep the news hidden in the hopes that over time it will simply fade away?

The importance of communicating can be illustrated in the infamous Yahoo data breach. Yahoo suffered data breaches in 2014 and 2016 impacting 3 billion customers but said nothing to its customers, investors, and regulators for two years. However, eventually the truth came out. The following day it was revealed, Yahoo's stock price dropped, resulting in a loss of $1.3 billion in market capitalization. It was later fined $35 million by the Securities and Exchange Commission (SEC) and also had to pay $80 million in a federal securities class action settlement, the first of its kind based on a cyberattack. Numerous shareholder actions against Yahoo were filed, and a consumer data breach class action lawsuit resulted in a $117 million settlement. Eventually, Yahoo liquidated its assets and it no longer exists.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

This cautionary tale illustrates the negative impact of trying to hide a cyber incident. Yahoo's attempt to hide it from the public and investors by not providing timely and accurate communications resulted in a devastating financial impact and generated a large amount of ill-will that significantly contributed to its downfall. It proves that proper communication during a cyber incident is not negotiable but is essential.

There are reasons for communicating information about the incident, which include limiting adverse reactions, preventing inadvertent release of information, satisfying state legislative mandates, and meeting federal regulatory requirements.

Limit Adverse Reactions

One reason for communicating during a cyber incident is so that the organization can limit adverse reactions. This is done by "controlling the conversation" surrounding the incident. Controlling the conversation means that the organization works to be "out in front" of the discussion instead of being placed on the defensive and always responding to adverse reactions to the cyber incident.

Considering the Yahoo incident, in hindsight had Yahoo been forthcoming and timely with the information about it, they could have controlled the conversation. Yahoo could have set the tone by communicating information while finding ways to work in their own messages of vision, safety, and quality by emphasizing timelines, the expertise of their security team, a description of specific events, and how they were being addressed.

Caution !

Media consultants often coach organizations regarding how to interact with the news media regarding a cyber incident. For example, consultants stress that there is a difference between *answering* a question and *responding* to a question from the media. Answering a question only provides data. Responding to a question provides data but in a context so that the response contains information, intent, direction, and management. Such a response to questions can infuse power and meaning into it rather than just giving an answer.

Prevent Inadvertent Release of Information

Another reason for communicating during a cyber event is to prevent the inadvertent release of information (providing information unintentionally). The Yahoo incident also illustrates this principle. Whereas Yahoo had been able to keep the incident quiet for almost two years, they ultimately were forced to release the information as part of a required filing with the SEC. This unintentional and unplanned release of information immediately put Yahoo on the defensive with no means to explain or exonerate themselves.

Note 7

Had Yahoo communicated in a timely and open fashion, they would have been in control of releasing information about the incident. As unpleasant as it would have been to admit to a breach, nevertheless by Yahoo releasing the information on their own terms, they would have prevented an unplanned release of information.

Satisfy State Legislative Mandates

In the United States, there currently is no federal law that requires notification of a specific type of cyber incident. However, there are state legislative mandates regarding communication that must be satisfied (disclosing based on legislative requirements). Since the initial passage of California's Database Security Breach Notification Act in 2003, by 2018 all other states had passed similar notification laws mandating that users be promptly notified (reporting requirements). Initially these laws all used the same definitions:

- **Personal information.** Personal information is defined as an individual's first name or first initial and last name plus one or more of the following data elements: Social Security number; driver's license number or state-issued ID card number; or account number, credit card number or debit card number combined with any security code, access code, PIN, or password needed to access an account.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 8

Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

- **Breach of security.** This is defined as the unlawful and unauthorized acquisition of personal information that compromises its security, confidentiality, or integrity.

Note 9

The California Consumer Privacy Act (CCPA) of 2018 allows users to know what personal data is being collected about them, to know whether their personal data is sold or disclosed and to whom, to say no to the sale of personal data, to access their personal data, and to request a business delete any personal information about a consumer that has been collected from that consumer. It does not address notification in the event of a data breach.

However, due to a lack of comprehensive federal regulation regarding data breach notification, many states have amended their breach notification laws from these basic definitions. As a result, no two state laws are the same.

Caution !

The differences between state laws vary widely. For example, in Arkansas notification is not required if, after a reasonable investigation, the business determines that there is no reasonable likelihood of harm to customers. Colorado requires additional notice to be provided to the state attorney general. The Hawaiian statute applies to personal information in any form, whether computerized, paper, or otherwise.

Meet Federal Regulatory Requirements

There are several federal regulatory requirements that mandate communication from an organization if a specific cyber event occurs (**regulatory reporting**). Those companies that perform business in the European Union (EU) are legally obligated under the General Data Protection Regulation (GDPR) to inform the EU's Information Commissioner's Office (ICO) if they suffer a breach involving personal information of customers or employees. The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada likewise protects user data.

Note 10

The GDPR not only applies to organizations that are located within the EU but also applies to those located outside of the EU if they offer goods or services to or monitor the behavior of EU data that pertains to its subjects. GDPR also applies to all companies processing and holding the personal data of subjects residing in the EU regardless of the company's location.

There are several U.S. federal laws that require communication if a cyber incident involves the disclosure of specific information. These include the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (Sarbox), and the Gramm-Leach-Bliley Act (GLBA).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 11

Sarbox requires that in the event of a data breach, customers should be provided a general description of the incident and the information that was the subject of unauthorized access, a telephone number for further information and assistance, a recommendation that incidents of suspected identity theft be reported promptly, and a general description of the steps taken by the financial institution to protect the information from further unauthorized access or use. It should also contain a reminder for customers "to remain vigilant" over the next 12 to 24 months.

Communications Best Practices

There are several different best practices for communications regarding a cyber incident:

- **Limit communication to trusted parties.** Unless necessary, a cyber incident should not be broadcast to the general public. Instead, communication should be restricted to trusted parties who are stakeholders.
- **Use a secure method of communication.** In order to avoid any inadvertent release of information, it is important to use a secure communication method. When sending emails, the contents of the messages should be encrypted. Likewise, when using text messages, an app should be used that provides end-to-end encryption.
- **Be transparent but be careful.** Transparent communication builds trust; however, in a cyber incident initially there often are few facts that are certain. It is important to avoid providing any details that may change as the investigation progresses and to refrain from speculation on who was behind the incident. All public comments should demonstrate that the issue is being taken seriously.
- **Focus on what is being done.** Communicating the steps that are being taken and what is being done to protect information is important.
- **Provide a context.** In a cyber incident, there may be a temptation for public speculation. Businesses should counter this speculation with facts and a context to reduce the risk of undermining public trust. Where possible, it should include investigation timelines.
- **Respond quickly.** Waiting too long can allow misinformation to spread rapidly. The communication should begin as soon as possible, but not too soon before any facts are known.
- **Use social media appropriately.** Organizations should assess whether it would be helpful to suspend planned social media campaigns in light of a cyber incident. Because social media can take unpredictable turns, it should direct the public back to the official statement on the issue, which should be posted on the organization's website. The tone of social media communications is usually casual, but in a cyber incident it should use a more formal, just-the-facts approach while maintaining the organization's voice. It is important to promote posts as necessary. A counter-message should be ready for dissemination if necessary and as soon as possible.

Two Rights & A Wrong

1. One reason for an organization to be open and truthful about a cyber incident is to limit adverse reactions.
2. In the United States, there currently is no federal law that requires notification of a specific type of cyber incident.
3. Companies that perform business in the EU are legally obligated under Sarbox to inform the EU's ICO if they suffer a breach.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Summary

- Cyber incident response management addresses how to react to a successful attack in order to contain the attack, minimize its impact, restore the systems to their pre-attack state, and make the necessary changes to stop future attacks. A cyber incident response is the actions that an organization takes in reaction to a cyber incident. A cyber incident response plan is a detailed document that clearly outlines the roles, responsibilities, and processes for responding to a cyber incident. Also called an incident response playbook, it lists specific actions or a set of rules that describes steps to take in response to a security incident. A cyber incident response plan should be facilitated by a cyber incident response team, which analyzes information, takes appropriate actions, and shares important communications with all stakeholders. The incident response team's primary objective is to coordinate and align the key resources during a cyber security incident. No incident response plan is complete without documentation, testing, and training.
- When crafting a cyber incident response plan, there are different tools to assist in its development. Different plans can serve as "preparatory" plans to a cyber incident response plan. Often prepared in advance, these plans are complementary to an incident response plan, cover areas related to the incident response plan, and can therefore help shape it. A business continuity (BC) plan is a strategic document that provides alternative modes of operation for business activities that, if interrupted, could result in a significant loss to the enterprise. Creating a BC plan involves identifying exposure to threats, creating preventive and recovery procedures, and then testing them to determine if they are sufficient. A business impact analysis (BIA) identifies business processes and functions and then quantifies the impact a loss of these functions may have on business operations. A disaster recovery (DR) plan involves restoring IT functions and services following an event that causes a significant disruption in service.
- A cybersecurity framework is a series of documented processes used to define policies and procedures for implementation and management of security controls in an enterprise environment. Frameworks are also available that outline in detail how attacks occur and serve as models of the thinking and actions of threat actors; they are called attack methodology frameworks or exploitation frameworks. The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed methodology for security testing. The Open Source Foundation for Application Security (OWASP) Testing Guide is designed to help software developers and engineers test web applications to identify security issues. MITRE ATT&CK is a knowledge base of attacker techniques that have been broken down and contain classification in detail. The Diamond Model of Intrusion Analysis is a framework for examining network intrusion events. This framework derives its name and shape from the four core interconnected elements that comprise any event: adversary, infrastructure, capability, and victim. The Cyber Kill Chain illustrates that attacks are an integrated and end-to-end process like a "chain." Disrupting any one of the steps will interrupt the entire attack process, but the ability to disrupt the early steps of the chain is the most effective and least costly.
- Another part of cyber incident response planning is to identify the organization's critical data. This data includes personally identifiable information (PII), personal health information (PHI), sensitive personal information (SPI), high-value asset data, financial information, intellectual property, and corporate information. Because not all threats have the same impact, it is important in the planning phase to be able to classify these threats. This helps identify the "high-value" threats that must be immediately dealt with, while setting aside lesser-value threats until the high-value threats have been mitigated. In addition, for organizations that are involved with customer retail financial transactions, cardholder data (CHD) is also considered critical data to be protected.
- Incident response also involves coordination with stakeholders. Different individuals or groups of individuals should be involved in the coordination and even receive different communications. There are two categories of internal stakeholders with whom there should be coordination of efforts and information: technical and management. Management stakeholders include public relations, human resources, legal, and senior leadership. External stakeholders include customers, media, law enforcement agencies, and incident response providers.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- One of the most important elements of a cyber incident response plan is determining a communication plan as to how, when, and what type of information about the incident will be distributed and to whom. The reasons for communicating information about the incident include limiting adverse reactions, preventing inadvertent release of information, satisfying state legislative mandates, and meeting federal regulatory requirements.
- There are best practices for communications regarding a cyber incident. Unless necessary, a cyber incident should not be broadcast to the general public. Instead, communication should be restricted to trusted stakeholders. To avoid any inadvertent release of information, it is important to use a secure communication method. When sending emails, the contents of the messages should be encrypted. Likewise, when using text messages, an app should be used that provides end-to-end encryption. Transparent communication builds trust; however, in a cyber incident, initially few facts are certain. It is Important to avoid providing any details that may change as the investigation progresses and not to speculate who was behind the incident. All public comments should demonstrate that the issue is being taken seriously. Communicating the steps that are being taken and what is being done to protect information is important. In a cyber incident, there may be a temptation for public speculation. Businesses should counter this speculation with facts and a context to reduce the risk of undermining public trust. Where possible, it should include investigation timelines. Waiting too long can allow misinformation to spread rapidly. Organizations should assess whether it would be helpful to suspend planned social media campaigns in light of a cyber incident. Because social media can take unpredictable turns, it should direct the public back to the official statement on the issue, which should be posted on the organization's website.

Key Terms

attack methodology frameworks
business continuity (BC) plan
cardholder data (CHD)
customer communications
Cyber Kill Chain
Diamond Model of Intrusion Analysis
disaster recovery (DR) plan
incident response plan
incident response tools
law enforcement agencies
legal
media
MITRE ATT&CK
Open Source Foundation for Application Security (OWASP) Testing Guide
Open Source Security Testing Methodology Manual (OSSTMM)
playbook
public relations
regulatory reporting
stakeholder identification and communication
training

Review Questions

1. What is the act of violating an explicit or implied security policy that may or may not be successful?
   - **a.** Cyber breach
   - **b.** Cyber incident
   - **c.** Security event
   - **d.** Adverse cyber security event
2. Which of the following is NOT an actionable goal of a cyber incident response plan?
   - **a.** Identification
   - **b.** Denial
   - **c.** Analysis
   - **d.** Recovery
3. Which member of a cyber incident response team has the responsibility of helping the team to focus on minimizing damage and recovering quickly from a cyber incident?
   - **a.** Assistant director
   - **b.** Coordinator
   - **c.** Team leader
   - **d.** Lead investigator
4. Which data category would contain a user's personal bank account number?
   - **a.** PII
   - **b.** PHI
   - **c.** SPI
   - **d.** HVAC

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

5. Which of the following is NOT an example of intellectual property?

   a. Trademark
   b. Brand image
   c. Copyright
   d. Patent

6. Why is financial information data considered to have a high value?

   a. Federal laws prohibit the backup of corporate accounting data so the loss cannot be replaced.
   b. The loss of accounting data prevents an organization from providing stakeholders with an accurate picture of its financial health.
   c. Accounting data is very detailed and would require a significant effort to restore it.
   d. Corporate accounting data only has a high value if it is part of a merger and acquisition.

7. Which of the following techniques is a peer-reviewed methodology for security testing that is updated biannually?

   a. CIT
   b. OWASP
   c. OSSTMM
   d. Series 27000

8. Which attack framework is a knowledge base of attacker techniques that have been broken down and contain classification in detail?

   a. Cyber Kill Chain
   b. MITRE ATT&CK
   c. Diamond Model of Intrusion Analysis
   d. AXITI

9. What is the best way for an organization to limit adverse public reactions to a cyber incident?

   a. By responding defensively
   b. By keeping the news of a cyber incident secret
   c. By controlling the conversation
   d. By communicating only with stakeholders

10. Which of the following is NOT a reason for communications in a cyber incident?

    a. Limit adverse reactions.
    b. Meet federal regulatory requirements.
    c. Allow for unplanned release of information.
    d. Satisfy state legislative mandates.

11. Which of the following is false regarding state legislative mandates about communication in a cyber incident?

    a. Some states have a broader definition of personal information.
    b. No two state laws are identical.
    c. Only California has a state security breach notification law.
    d. Providing notice to the state attorney general is required in some states.

12. What EU requirement covers communicating with affected parties in a cyber incident?

    a. PIPEDA
    b. ICO
    c. GDPR
    d. S-BOX

13. Which of the following is NOT a reason for contacting law enforcement agencies in the event of a cyber incident?

    a. They can work with foreign counterparts to stop organized cybercrime.
    b. They have many resources and experience.
    c. Identifying threat actors often leads to no arrests or convictions.
    d. Companies providing information can assist in intelligence-sharing efforts.

14. Who should be the first to be notified in the event of a cyber incident?

    a. Law enforcement agencies
    b. Cyber incident response team
    c. CEO
    d. Local media

15. Which of the following lists specific actions or a set of rules that describe steps to take in response to a security incident?

    a. Playbook
    b. Handbook
    c. Map book
    d. Response book

16. Which of the following is a strategic document that provides alternative modes of operation for business activities that, if interrupted, could result in a significant loss to the enterprise?

    a. BC
    b. AIB
    c. RSA
    d. CR

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

17. Which of the following is a written document that details the process for restoring IT resources following an event that causes a significant disruption in service?

    a. BIA
    b. DR
    c. CBB
    d. EUR

18. Which of the following is NOT an attack methodology framework?

    a. Cyber Kill Chain
    b. Diamond Model of Intrusion Analysis
    c. OWASP Testing Guide
    d. Business Impact and Continuity Analysis

19. Which of the following is NOT an element of CHD?

    a. PAN
    b. Cardholder name
    c. Renewal date
    d. Service code

20. For internal communications, which two categories are often used?

    a. Security and networking
    b. Senior level and junior level
    c. Technical and management
    d. Communication and cyber

Case Projects

Case Project 10-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. What can local government agencies do to better protect themselves? Should rewards be offered for those students who have a cybersecurity degree, such as a waiver of student loans, if they work for one of these agencies for a period of time? Should businesses be charged an excise tax to specifically fund cybersecurity improvements? What other solutions would work? Write a one-page paper about this.

Case Project 10-2: Comparing Cyber Incident Response Plans

Estimated Time: 25 minutes
Objective: Compare and contrast cyber incident response plans.
Description: Use the Internet to locate four different cyber incident response plans. Compare each plan for its strengths and weaknesses. Finally, from the strengths of each plan, create your own plan. Explain why you chose the specific items to include.

Case Project 10-3: State Data Breach Requirement

Estimated Time: 25 minutes
Objective: Evaluate state data breach requirements.
Description: Identify three state legislative data breach requirements and compare them, one of which is for the state in which you currently reside. What is the strength of each requirement? What is the weakness? What changes would you suggest to your state's requirements? Why? Write a one-page summary of your research.

Case Project 10-4: Sensitive Personal Information (SPI)

Estimated Time: 25 minutes
Objective: Research sensitive personal information (SPI).
Description: Use the Internet to research SPI. What type of information is covered by SPI? Why is it necessary to protect this type of data that cannot directly identify an individual? What are three additional data elements that SPI should cover? Create a one-page paper of your research.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Project 10-5: Comparing Attack Methodology Frameworks

Estimated Time: 25 minutes
Objective: Compare attack methodology frameworks.
Description: Select two of the five attack methodology frameworks introduced in this chapter. Analyze them and identify their strengths and weaknesses. Which did you find most helpful? Why? How would you use this if you were a cybersecurity professional? Write a one-page paper on your research.

Two Rights & A Wrong: Answers

Charting an Incident Response Plan

1. A cyber incident is the act of violating an explicit or implied security policy whether or not it is successful.
2. The final item in an incident response plan is follow-up.
3. The role of the lead investigator is to lead and coordinate all incident response team activity.

Answer: The wrong statement is #3.
Explanation: The role of the team leader is to lead and coordinate all incident response team activity.

Using Plans and Frameworks

1. A BC can be defined as the ability of an organization to maintain its operations and services in the face of a disruptive event or a major disaster.
2. A DR is designed to identify those processes that are critically important to an enterprise.
3. The OSS TMM provides guidance on how to test the operational security of five channels so that organizations can understand the full extent of their security and determine how well their security processes function.

Answer: The wrong statement is #2.
Explanation: A BIA is designed to identify those processes that are critically important to an enterprise.

Reviewing Criticality of Data

1. SPI is data that could identify a specific individual.
2. HVA information includes assets, systems, and datasets that control sensitive controls.
3. CHD is considered critical data to be protected.

Answer: The wrong statement is #1.
Explanation: PII is data that could identify a specific individual.

Identifying Stakeholders

1. The two categories of external stakeholders are technical and management.
2. A client is not the same as a customer.
3. Password trafficking falls under the jurisdiction of the FBI local office, Secret Service, and Internet Crime Complain Center.

Answer: The wrong statement is #1.
Explanation: The two categories of internal stakeholders are technical and management.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Constructing Communication Pathways

1. One reason for an organization to be open and truthful about a cyber incident is to limit adverse reactions.
2. In the United States, there currently is no federal law that requires notification of a specific type of cyber incident.
3. Companies that perform business in the EU are legally obligated under Sarbox to inform the EU's ICO if they suffer a breach.

Answer: The wrong statement is #3.

Explanation: Companies that perform business in the EU are legally obligated under GDPR to inform the EU's ICO if they suffer a breach.

References

1. "Hiscox Cyber Readiness Report 2018," *Hiscox*, July 29, 2019, https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf.
2. "Cyber Security Underpinning the Digital Economy," *IoD*, Mar. 3, 2016, Aug. 16, 2019, https://www.iod.com/cyber-security-for-your-business/articles/cyber-security-underpinning-the-digital-economy.
3. "2022 Internet Crime Report," *IC3*, Jan. 31, 2024, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 11

Incident Response Activity Phases

Chapter Objectives

After completing this chapter, you should be able to do the following:

1. Explain the activities of the detection and analysis activity phase
2. Analyze the containment activity phase
3. List steps associated with the eradication and recovery activity phase
4. Categorize activities of the post-incident activity phase

#TrendingCyber

1234. Or 1111.

Would you use a simple four-digit code like this to protect all your finances and virtually your entire digital life? Certainly, all users would scream "NEVER!" But that is what many users of Apple iPhones are doing because of the way in which Apple has implemented its security features. Fortunately, a change is now taking place—if users choose to turn it on.

In increasing numbers, thieves have been exploiting what some security professionals say is a design flaw of over 1 billion Apple iPhones. It all centers around the passcode, which is a short string of numbers (like 1234) that grants access to the device and its settings. With this passcode, a cybercriminal can within a few seconds turn the life of the phone's owner upside down. As a detective of the New York City police said, "Once you get into the phone, it's like a treasure box."

Consider these actual events. One evening Reece was having a drink with his girlfriend at a bar when his iPhone suddenly went missing. The next morning when he tried to log into his Apple account from a different device, the account password had been changed. Reece then discovered that thousands of dollars of merchandise had been charged to his credit cards via the Apple Pay app that was on the stolen iPhone, and another $1,500 was stolen from his Venmo account through the phone. Another victim, David, lost his iPhone at a pizza shop. By the time he realized it was missing, someone had attempted to charge $15,000 to his credit card via Apple Pay, and a new Apple credit card had been opened in his name. When David finally got back into his Apple account a few days later, he found that photos he had previously taken of sensitive documents (passport, driver's license, paycheck direct-deposit form, and health-insurance paperwork) had all been viewed and transferred to a new photo album. According to police, there have been hundreds of these crimes just in New York City over the past two years, and the number continues to grow.

How are these cybercriminals getting their hands on the victim's iPhone? And how are they uncovering the passcode?

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

For many victims (and cybercriminals say that college-age males are the best targets), it begins with trickery. Pairs of cybercriminals will go to a bar, restaurant, or similar establishment. One of the thieves will strike up a friendly conversation with someone. Soon they will be sharing jokes and buying drinks. Eventually the cybercriminal will ask their new friend to open Snapchat or another social media app on their phone. However, the other cybercriminal is now positioned behind the victim and watches them unlock the iPhone with the short passcode, taking note of the code. If this doesn't work, the thief will pull out his own phone and take a picture with their new friend and then ask for their friend's phone to do the same. After the soon-to-be victim hands over their phone, the cybercriminal takes a photo and then subtly locks the phone before handing it back so the accomplice can watch again for the passcode to be entered. Or, once handed the iPhone, the thief might "accidentally" lock the phone and say, "Hey, your phone is locked. What's your passcode?"

Then there are techniques used to steal the iPhone itself. Sometimes a thief, after watching the victim enter the passcode, simply waits for them to set the phone down. Their accomplice momentarily distracts the victim while the thief grabs the phone. Or an unsuspecting victim may hand their phone to the thief to snap a selfie—but the thief then runs out the door with phone in hand. The phone can also be snatched out of the victim's hands. In some extreme cases the victim is physically assaulted or intimidated into handing over their phone and passcode. Some victims even report being drugged and waking up the next morning with no memory of what happened—and no phone.

Once an Apple iPhone passcode is used by a cybercriminal to get into a stolen phone, they can initiate an Apple ID password change (Apple does not require the old password entered before creating a new one), change the Apple ID's backup email and phone number to their own, and force all other Apple devices, such as Macs or iPads, to be signed out of the victim's Apple account. This prevents the victim from using another device to regain access to their account and iPhone. The thief will then disable Find My iPhone, which prevents victims from locating their phones or remotely erasing its data. Finally, thieves will replace the owner's biometrics with their own face and fingerprint.

Now the cybercriminal can start transferring money through the phone. They often access money apps on the phone like Venmo to siphon funds from the victim's account. Or they may apply to open a new Apple credit card through Apple's Wallet app (the Apple Card application will even autofill the application with information stored on the iPhone, such as the owner's name, address, and birthday). Thieves can also access Apple's iCloud keychain password manager to unlock any account that is password-protected.

When the cybercriminal is finished with the phone, they often sell it to another cybercriminal, who will then sell it as a used iPhone. One cybercriminal (who was caught and now incarcerated) claims that they made over $20,000 selling stolen phones each weekend—not counting money stolen from victims' bank apps or new credit cards.

But what about security protections on an iPhone? Won't they prevent this from happening?

Many iPhone apps use multifactor authentication (MFA), which requires that a confirmation be approved before permitting a change. Unfortunately, these confirmations go right to the stolen iPhone that the thief is holding in their hands.

And another Apple security protection for iPhones can actually make it even worse than just losing a phone.

In 2020, Apple introduced an optional recovery key, a unique 28-digit code to (ironically) protect users from cybercriminals. Once a recovery key has been enabled, it must be used to regain access to a locked Apple account. However, if a recovery key has already been set on the iPhone, the phone thief will generate a new one that locks out the original user from their Apple account (if no recovery key has been set, then thieves simply set their own). Once a recovery key is enabled, Apple's policy prevents users—even the valid owners of the phone—back into their Apple accounts without that recovery key. Even contacting Apple for assistance, as many victims have done, proves to be futile.

However, Apple announced that in 2024 a new security feature called Stolen Device Protection will be available on its iPhones. Once enabled, if a user wants to change their Apple ID password when they are away from a familiar location, the device will also require Face ID or Touch ID biometric approval. That launches a 60-minute countdown, after which time the requester must again reconfirm with Face ID or Touch ID before the password can be changed. And changing the recovery key or trusted phone number will also require biometric scans one hour apart.

Yet there are still weaknesses to Stolen Device Protection. A thief with a user's iPhone and passcode can still unlock the phone, even when Stolen Device Protection is turned on. Any app installed on the phone that is not protected by an additional password or PIN is vulnerable, as are accounts that can be reset by MFA or email. And Apple Pay still works with a passcode if Face ID or Touch ID fails.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Users should practice good practical security with their iPhones. They should turn on Stolen Device Protection. Users should never hand their phone to someone else, and a phone should never be set down in public but always placed in a pocket or handbag. And users should also switch from simple four-digit passcodes to longer alphanumeric codes and add access codes to any cash or crypto apps installed on their iPhones.

In the event that an iPhone is stolen, it is important to remember that the information on the phone is exponentially more valuable than the phone itself. Users should immediately take steps to remotely "wipe" the device of its contents so that it is not accessible to cybercriminals. This can be done by accessing the online find services (icloud.com/find) from any device so that they can sign in to find devices, locate a device, play a sound on a device, use Lost Mode (this lets them lock the devices so that nobody can access personal information), or erase a device.

As #TrendingCyber illustrates, the best way to prevent a cybercriminal from accessing a user's Apple account is to take the necessary precautions to prevent the iPhone and passcode from being stolen. However, if a theft occurs, users should immediately take steps to remotely erase the device of its contents.

Preventing the phone from being stolen is analogous to vulnerability management. But remotely erasing a stolen phone is like incident response management. Cyber incident response management addresses how to react to a successful attack in order to contain the attack, minimize its impact, restore the systems to their pre-attack state, and make the necessary changes to stop future attacks.

In this chapter, you examine the activity phases related to incident response for an organization. These phases include incident detection and analysis, containment, eradication and recovery, and post-incident activities.

Note 1

Although there are slight variations in these phases from different organizations, they are remarkably similar. The National Institute of Standards and Technology (NIST) combines containment, eradication, and recovery into a single phase and thus has four phases, while the SANS (SysAdmin, Audit, Network, and Security) organization splits them out and has six phases. Nevertheless, they all cover the same activities.

Detection and Analysis

Certification

3.2 Given a scenario, perform incident response activities.

A cybersecurity event just occurred that was brought on by a threat actor, so we must take immediate action! But wait—was it something that requires action? And, if so, what action is required, when, and how?

The first phase in incident response is the detection of an incident. This is followed by an analysis of that incident. The detection and analysis can be answered by three sets of questions: Did an incident occur? How severe is it? And what is its priority for being addressed?

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Did an Incident Occur?

One of the most difficult steps in an incident response and recovery process is the initial analysis: *Did a cyber incident just occur?* Although it may seem that this is a simple question to answer, in reality it can be difficult. The reasons for the difficulty include:

- **Inaccurate security indicators.** Security information and event management (SIEM) devices often report false positives so that every alarm may not be the result of a cyber incident.
- **Multiple indicators.** Depending on the size and scope of the network, the total number of indicators may reach the hundreds of thousands each day. Sorting through these to identify any that are related to a cyber incident can be overwhelming.
- **Lack of multiple clear symptoms.** The goal of a threat actor is to hide any evidence of their actions so that they can remain undetected. A seemingly innocent and insignificant symptom, such as a change in a single configuration file, may be the only indicator of a cyber incident.
- **Faulty human statements.** Reports from employees of a device acting erratically are often attributed by that employee to a "computer virus," while in reality it may be the result of any number of reasons.

How can a security professional properly analyze events and then decide what to do? There are several general principles that are helpful. First, the professional should rely on their experience and training: if an indicator *seems* important then it should not be ignored. Second, collaborating with other security personnel is very helpful. Third, every situation should be handled in a similar fashion whether or not it is a security incident. Finally, determining if it is an incident may simply be a matter of educated judgment. This is because not all successful attacks result in a detectable irregular activity and thus do not produce a steady stream of clear and valid indicators. A security professional needs to be thorough and even flexible when analyzing incidents in order to determine if it is malicious.

However, there are some signals that can be used to determine if an incident did occur. Two such signals include indicators of compromise and data and log analysis.

Indicators of Compromise (IOC)

In cybersecurity, indicators of attack (IOA) are preliminary behaviors that focus on detecting the intention of the threat actor as evidenced by their actions. The digital artifacts that serve as evidence of an attack are called indicators of compromise (IOC). IOC are one or more indicators of a successfully completed attack and show how it happened.

IOC can serve as signals that a cyber incident did occur. There are several different tools that can be used for uncovering IOC. These include file analysis tools, tools for analyzing networks, and reputation tools.

Data and Log Analysis

Logs play a critical role in identifying IOC. Cybersecurity logs can reveal the type of attack that was directed at the network and how it successfully circumvented existing security defenses. However, because there is a massive amount of log data generated related to cybersecurity, identifying an IOC from log data can be challenging. And there are other log management issues as well. Devices record all events, even those that are not cybersecurity-related, which increases the amount of data that is generated. Each type of device may interpret an event in a different context, so that a router looks at an event differently than a firewall does. This can produce different alerts: One device may see an event as only a warning while another device may interpret it as a serious event and may create a confusing mix of log data. And different devices record log information in different formats and even with different data captured. Manually combining multiple logs, each with a different format, can be a major challenge.

However, in spite of these challenges, examining different log files (**data and log analysis**) is important for identifying IOC.

How Severe is it?

Suppose you are a member of the cyber incident response team and you received a communication from the team leader that these three events have just occurred in rapid succession:

- A senior vice president opened an email attachment that contained malware that has now infected their computer and established connections with an external host.
- A distributed denial of service (DDoS) attack appears to be directed at a web server.
- A firewall has blocked a remote connection attempt.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Determining the severity of an incident is a critical step. That is because giving attention to an incident that is not critical can give a different critical incident time to cause widespread damage.

When faced with determining the severity of an incident, it is important to consider its impact in the context of security as a whole. In the previous examples, a security "novice" might be drawn to the firewall incident as the most severe. However, a firewall that has blocked a remote connection attempt is a normal security action: the firewall properly functioned and, as a result, no data was threatened (although a continued effort by a threat actor may need to be investigated). Once these low-level security "nonincidents" have been eliminated, the severity of the remaining incidents can be determined. This can be done based on the value of the data being compromised, the extent of the threat, and even organizational priorities.

What Is its Priority?

Which has the highest priority, a DDoS attack that has brought down the company's public web server so that customers are unable to make any purchases or an unauthorized root-level access to a device that is allowing the theft of personally identifiable information (PII)? If determining if an incident occurred is one of the most difficult steps, then prioritizing is perhaps the most critical step. A security professional must be able to quickly prioritize events in order to respond to the most damaging event first. Or, if two events have an almost equal priority, a decision must be made as to the order they both should be addressed.

Caution

Cyber incidents must always be prioritized; they should never be handled simply as they occur on a first-come, first-served basis.

One approach to determining the priority of incidents is to perform a two-step process. The first step in the process is to eliminate (or postpone) those incidents that have lesser consequences. Sometimes called a "triage," this identifies those incidents that should be immediately addressed with the available resources. Table 11-1 lists general principles to be considered when performing a first-level triage of cybersecurity incidents.

Table 11-1 General principles for first-level triage

Principle	Explanation
Consider both current and future consequences	Limiting prioritization to incidents that only have an immediate consequence on the functionality of a business system could inadvertently ignore the more serious long-term impact.
Consider who will be affected	Today a cyber incident often has a much wider impact on one or more other organizations or the public at large.
Consider the ability to recover	Some incidents cannot be fully recovered from (such as the theft and release of PII that cannot be undone), so consideration should be given as to the level of recoverability.

Each of these general principles can also be further subdivided. For example, when considering the ability to recover, the amount of effort needed should also be considered. The amount of effort can be subdivided into these categories:

- **Normal.** The time to recover can be accomplished with a reasonable estimate of time by using current resources.
- **Supplementary.** The time to recover can be accomplished with a reasonable estimate of time but additional resources are necessary.
- **Expanded.** The time to recover is unknown and additional resources are necessary.
- **Unrecoverable.** It is not possible to fully recover to the state prior to the incident (such as securing PII that has already been stolen and posted online).

Once the list has been reduced to only cybersecurity incidents that should be quickly addressed, there is a second stage of evaluation. This is used to sort the incidents so that the most critical receive the highest level and must be addressed immediately.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

These are called *characteristics contributing to severity-level classification* (also called *scope of impact*). These characteristics can help identify the incident (or incidents) that are the most serious. These characteristics include:

- **Downtime.** The length of time that the incident interrupts the normal business processes, or downtime, is a major criterion to consider when identifying the most serious incidents. Downtime ranges from incidents that limit some of the normal activities to a complete interruption of all services.
- **Recovery time.** Recovery time is not the same as downtime. Recovery time is the length of time needed for the information technology (IT) systems to be disinfected and return to their normal functions.
- **Data integrity.** A cybersecurity incident that compromises the "soundness" (correctness and completeness) of the data, called *data integrity*, is perhaps the most important characteristic. An incident that impacts the organization's data should be considered as having a very high level of priority. This is because data that is corrupted may be difficult to clearly and completely identify and using suspicious data in normal business processes can have a widespread and serious impact on the organization.
- **System process criticality.** The degree to which the impacted systems affect the overall functionality of the entire system, called *system process criticality*, can also play a role in prioritization. Those systems that are essential to the organization, such as a web application server, may escalate the priority over auxiliary or systems of lessor importance.
- **Economic impact.** The financial effect of an incident is also an important criterion to consider when prioritizing incidents. The economic impact can be either short term or long term and can be the result of any or all of the previous criteria.

These characteristics may not always be easy to determine given the attack. For example, for malware it may be necessary to perform reverse engineering to determine its characteristics. It may also be necessary to collect global threat intelligence outside of the organization's infrastructure across all attack vectors and from security technologies within their own network to find the linkages (data correlations) so that these multiple data sources can result in more accurate results and reduces the likelihood of false positives.

Because every organization is different, no two lists of characteristics will or should look the same. However, for those organizations that are part of a larger entity, a common scope of impact is often used. This common scope can assist in compiling similar data from a range of sources. For example, the US-CERT (United States Computer Emergency Readiness Team) requires that all federal government departments and agencies must submit incident notifications within one hour of being identified by the US-CERT cybersecurity incident response team. Part of the requirements when reporting to US-CERT are for impacted organizations to identify the current level of impact on agency functions or services (functional impact); identify the type of information lost, compromised, or corrupted (information impact); and estimate the scope of time and resources needed to recover from the incident (recoverability). Table 11-2 lists the information impact severity levels.

Table 11-2 US-CERT information impact severity levels

Impact severity level	Description
No impact	No known data impact.
Suspected but not identified	A data loss or impact to availability is suspected but no direct confirmation exists.
Privacy data breach	Confidential PII or personal health information (PHI) was compromised.
Proprietary information breach	The confidentiality of unclassified proprietary information, such as intellectual property or trade secrets, was compromised.
Destruction of noncritical systems	Destructive techniques, such as master boot record (MBR) overwrite, have been used against a noncritical system.
Critical systems data breach	Data pertaining to a critical system has been copied and transferred to an unauthorized remote system (exfiltrated).
Core credential compromise	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
Destruction of critical system	Destructive techniques, such as MBR overwrite, have been used against a critical system.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

A common error is for an organization to replicate another organization's scope of impact without considering its own uniqueness. Each organization should develop its own scope of impact priority rating system based on what functions it provides to its stakeholders.

Two Rights & A Wrong

1. The first step in the detection and analysis activity phase is to determine if a cyber incident actually occurred.
2. Both IOC and data and log analysis can serve as indicators of a cyber incident.
3. "Recovery time" is the same as downtime.

See the answers at the end of the chapter.

Containment

Certification

3.2 Given a scenario, perform incident response activities.

4.2 Explain the importance of incident response reporting and communication.

Once it has been determined through detection and analysis that an incident did occur, an announcement goes out to relevant parties and the importance of addressing this incident is elevated (**incident declaration and escalation**). This includes implementing the incident response plan, reviewing the criticality of data, and identifying stakeholders.

The next activity phase of incident response is **containment**. Containment is designed to keep the incident under control by limiting its impact. Without containment, an incident will increase not only the degree of damage but also may result in other types of damage; in fact, without containment, it could even overwhelm resources to the point that a response may no longer be possible.

Containment often begins by examining three elements:

- **Scope.** In a cyber incident, it is important to sort the vulnerabilities and results of the incident so that the most critical receive the highest level of attention and can be addressed immediately. These characteristics that contribute to severity-level classifications are called the **scope**.
- **Impact.** While scope is the breadth and depth of the cyber incident, **impact** is the significance of the incident measured in the magnitude of harm that is caused. There are different types of impacts, such as functional impact (the current level of impact on agency functions or services) and information impact (the type of information lost, compromised, or corrupted).
- **Remediation.** **Remediation** is neutralizing or eliminating the vulnerability responsible for the cyber incident. Often remediation can be addressed by a compensating control, which is a control that provides an alternative to normal controls that for some reason cannot be used.

There are different containment techniques or strategies for containing a cyber incident. How these are implemented will depend on the situation and type of attack. The most common containment techniques include:

- **Removal.** The removal containment technique is the simplest: The affected system is removed from the network by disabling the switch port or disconnecting it from the network connection. However, removal by "pulling the plug" on the affected system may not always be the best action

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

for several reasons. First, the incident may be multifaceted and impact multiple systems; removing multiple systems from the network without proper planning can have widespread consequences and, in some instances, do more harm than the cyber incident itself. Second, containing one system by removal when that system is not the primary target may not actually contain the attack. Finally, efforts need to be taken to preserve as much evidence as possible for a forensic investigation or for law enforcement, and immediately containing a system by removal may limit the preservation of evidence.

- **Isolation.** Instead of disconnecting the system from the network, the **isolation** containment technique permits the device to continue to function. However, all network communication is redirected to a sinkhole so that evidence may continue to be gathered and the malware analyzed. However, this isolation technique may alert the threat actors that the attack has been uncovered.
- **Segmentation.** Similar to isolation, the segmentation containment technique continues to allow the affected device to talk to the command and control (C&C) system, but the communication is filtered.
- **Reverse engineering.** The reverse-engineering containment technique is similar to the segmentation containment technique: It allows the device to talk to the C&C with filtered communication. However, at the same time, the malware is closely examined through reverse engineering. This helps to determine how the malware functions and if any additional systems are infected. It also allows for evidence to be gathered and determines what communications with the C&C should be blocked or altered.

Two Rights & A Wrong

1. Once it has been determined through detection and analysis that an incident did occur, an announcement goes out to relevant parties and the importance of addressing this incident is elevated.
2. Scope is the significance of the incident measured in the magnitude of harm that is caused.
3. The removal containment technique is the simplest to implement.

See the answers at the end of the chapter.

Eradication and Recovery

Certification

3.2 Given a scenario, perform incident response activities.

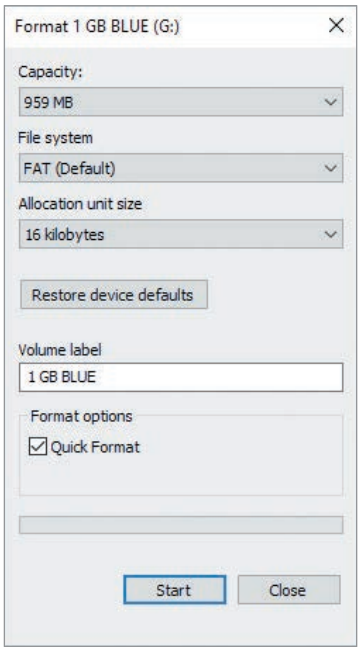
After the incident has been contained, then **eradication**, which is the elimination of the infection, should be performed. In addition, at this step, the necessary procedures for recovery of the systems back to their necessary performance (restoration of capabilities and services) are also begun. Of course, recovery does not mean restoring the systems back to their original state, for this would also reintroduce the vulnerability. Instead, vulnerability mitigation, which is the step to reduce or eliminate vulnerabilities, is also implemented.

There are different eradication techniques to clean malware that has infected the hard disk drive of a system. The first step is to physically erase the data from the drive. There are several methods that should *not* be used for eradicating malware:

- **Delete.** Using the operating system's *Delete* utility is not considered safe, since the data itself is not removed. Instead, what is deleted are the "pointers" to the data and not the data.
- **Format.** Reformatting a drive is likewise not considered safe. When using Microsoft Windows, for example, a Quick format only deletes the organizational structure of the files on the drive without removing the data files themselves. The Quick format option is shown in Figure 11-1.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 11-1 Quick format option



A more secure approach is data sanitization (also called data wipe). This method performs a complete data destruction of all contents of the drive by "overwriting" the entire drive, which is replacing data on the drive by writing other data over it. The new data could be *1s*, *0s*, or random characters.

Caution

There is disagreement as to how many passes should be made over the existing data. Some researchers maintain that a single pass is sufficient, while others claim that multiple passes should be made. Most data sanitation programs can be customized as to the characters used and the number of passes. For example, it could be configured to overwrite the data with a *0* on the first pass, a *1* on the second pass, and then random characters on subsequent passes.

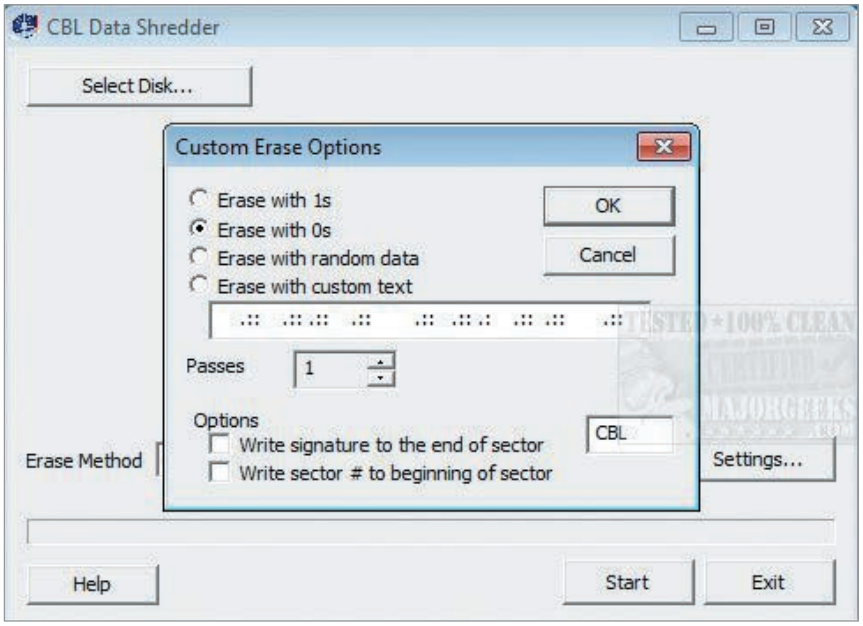
Table 11-3 lists some of the common data sanitization methods and software that is based on these methods. Figure 11-2 lists the configuration options of CBL Data Shredder.

Table 11-3 Sanitation methods and software

Sanitation method	Description	Characters and passes	Software
Secure Erase	Uses the commands embedded in the firmware of drives	Writes a *1* or *0* on one pass	N/A
DoD 5220-22-M	Department of Defense standard and one of most commonly used	Writes a *1* on first pass, a *0* on second pass, and a random character on third pass	DBAN, CBL Data Shredder, Eraser, Freeraser
Schneier	Considered the most secure method	Writes a *1* on first pass, a *0* on second pass, and a random character on passes 3–7	CyberShredder, EASUS

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 11-2 CBL Data Shredder options



Source: CBL Data Recovery

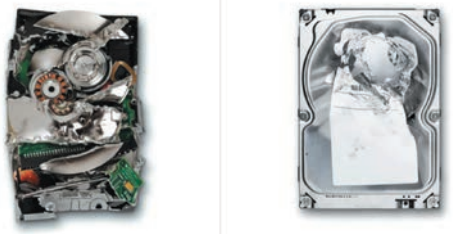
Note 2

Several methods also perform a verification after writing a character over the data to ensure that the contents were destroyed. Because verifying the entire drive after each pass takes a significant amount of time, many software packages contain the option to configure verification, such as verify only once at the end of the last pass.

Once the drive has been sanitized, it can be restored (reconstruction) by installing the operating system (OS), application programs, and data files. Due to the amount of time needed to reconstruct a drive "from scratch," most organizations maintain a digital "snapshot" (image) of the drive. Applying a saved image to a sanitized drive is called **reimaging**.

If the drive cannot be sanitized and reconstructed or reimaged, the drive should be completely destroyed. This is known as secure disposal. Third-party secure disposal services can destroy hard drives through *shearing* (slicing the entire drive into small pieces using 40,000 pounds of force) or *crushing* (punching a hole through the drive). Shearing and crushing are illustrated in Figure 11-3.

Figure 11-3 Shearing and crushing hard drives



Shearing Crushing

Source: Shred-it

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

After the malware has been eradicated and before it is fully integrated back into the system (reconstitution of resources), it is important to take actions to ensure that the repaired systems will not be susceptible to the same incident again. This is known as validation, or the action of making something officially acceptable. There are several steps in the validation process. These include:

- **Patching.** All patches to the OS and application software should be applied. If the cyber incident was the result of a missing patch, an investigation as to why this patch was overlooked should be conducted and necessary changes to procedures should be implemented. If the cyber incident was the result of a zero-day attack, then other controls should be implemented to prevent another incident.
- **Permissions.** Before reapplying permissions (restoration of permissions), it is important to first review the permissions that were on the compromised system to determine if any changes need to be made. Also, a common technique of threat actors is, after compromising one system, to attempt to change the permissions on other systems as well. A more extensive review of permissions on other systems should be conducted as well.
- **Scanning.** Once the system is functioning, a vulnerability scanner should be used to identify any issues.
- **Security monitoring.** As a final step, a check should be made to ensure that the system is being monitored correctly (verification of logging/communication to security monitoring). This includes reviewing the collection of log data using Syslogs, intrusion detection system (IDS) data, and SIEM information.

Two Rights & A Wrong

1. After the incident has been contained, then eradication should be performed.
2. Data formatting performs a complete data destruction of all contents of the drive by "overwriting" the entire drive by replacing data on the drive by writing other data over it.
3. Applying a saved image to a sanitized drive is called reimaging.

See the answers at the end of the chapter.

Post-Incident Activities

Certification

3.2 Given a scenario, perform incident response activities.

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.

4.2 Explain the importance of incident response reporting and communication.

Once the impacted system has been restored, the final phase is to perform various tasks (**post-incident activities**). These are designed to lessen the chance of a reoccurrence by taking corrective actions and to document the event. These include forensic analysis, generating IOC, updating the incident response plan, assessing the cyber incident, and producing incident response reports.

Digital Forensic Analysis

Digital forensics is an important element in incident investigation. In fact, many users equate incident investigation with digital forensics, although they are not exactly the same: forensics is one important part of incident investigation. Understanding digital forensics involves knowing the procedures for conducting an analysis and applying specialized forensics.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

What Is Digital Forensics?

In a general sense, "forensics" is the application of science to questions that are of interest to the legal profession. One example of forensics (and which most users associate with forensics) is analyzing evidence from a murder scene. A subset of forensics is digital **forensic analysis**. Digital forensic analysis involves the retrieval of difficult-to-obtain data, which may be hidden, altered, or even deleted by the threat actor. A digital forensics specialist searches for evidence pertaining to the incident or to damage that occurred during a cyber incident. In short, it is using technology to hunt for technology-based evidence. This is particularly the case when evidence is collected that may be used in the prosecution of the threat actor through the legal system.

Digital forensics is often confused with e-discovery, although they are not the same. When preparing for trial, both the prosecution and the defense engage in what is called "discovery." This is the formal process of exchanging information between the two parties about witnesses and evidence that will be presented at a trial. Discovery, since its inception in 1938, enables the parties to know before the trial begins what evidence may be presented. E-discovery is the electronic counterpart of manually sifting through documents in discovery.

Note 3

Despite what is commonly seen in movies when a last-minute witness suddenly appears, discovery is designed to prevent this "trial by ambush," where one side does not learn of the other side's evidence until after trial begins and there is no time to obtain counterevidence.

Forensics Procedures

When responding to an incident that requires an examination of a local endpoint or a network appliance in a data center using digital forensics, five basic steps are followed, which are similar to those of standard forensics. The steps are to secure the crime scene, preserve the evidence, document the chain of custody, examine the evidence, and create a report.

Secure the Scene When an incident occurs that involves technology, action must be taken immediately. A delay of even a few minutes can allow digital evidence to be overwritten in the normal function of the device, become contaminated by other users, or give the perpetrator time to destroy the evidence. A digital forensics incident response team is contacted and, upon arrival, their first job is to secure the scene. This involves documenting the physical surroundings, identifying and tagging all cables connected to the device, and taking custody of the device along with any peripherals.

Preserve the Evidence The next task is **preservation of evidence** or ensuring that important proof is not corrupted or even destroyed. Preserving evidence can also help mitigate nonrepudiation, or denial by the perpetrator that they were involved or did anything wrong.

Evidence from a suspected device should be placed in bags that have tags or identifying labels that have a description of the item, a numeric identifier, the date, the collection location, and other relevant information. These bags are then sealed to serve as protection against evidence being altered. One type of seal that is commonly used is a tamper-evident seal that cannot be removed and reapplied without leaving obvious visual evidence. If the seal or tape is lifted or removed, a clearly visible *OPENED* message appears on the packaging. For additional traceability and security, the tape is often labeled with a unique sequential number every 9 inches (22 centimeters). Tamper-evident tape is shown in Figure 11-4.

Depending on the type and severity of the incident, it may be necessary to immediately involve the judicial system to help collect and preserve the digital evidence. This ensures that the integrity of the evidence is maintained and can be held up in a court of law (admissibility). Once data has been identified, it can be placed under a **legal hold**, meaning that it cannot be modified, deleted, erased, or otherwise destroyed.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 11-4 Tamper-evident tape



Source: American Casting MFG

Caution

There is a tendency to issue legal holds that are too broad in scope. For example, placing a legal hold on all email correspondence may result in retaining thousands or millions of unneeded messages and associated attachments, while placing a legal hold on all portable devices requiring them to be locked away makes them useless to the organization. Instead, appropriate filters should be used to capture only data that is relevant.

Document Chain of Custody As soon as the team begins its work, it must start and maintain a strict chain of custody. Documenting the evidence from the very beginning is called *provenance*. The **chain of custody** documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence. A chain of custody includes documenting all the serial numbers of the systems involved, who handled and had custody of the systems and for what length of time, how the device was transported, and any other steps in the process. In short, a chain of custody is a detailed document describing where the evidence was at all times from the beginning of the investigation.

Caution

Gaps in a chain of custody can result in severe legal consequences. Courts have dismissed cases involving computer forensics because a secure chain of custody could not be verified.

A chain of custody form helps to document that evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt it, as shown in Figure 11-5.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 11-5 Chain of custody form

Property Record Number: _____

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Official: (Name/ID#) _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	**Date/Time**	**Released by** (Signature & ID#)	**Received by** (Signature & ID#)	**Comments/Location**

Final Disposal Authority

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Official: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian
_____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record.

Examine for Evidence When examining a device for evidence, there are specialized tools that should be used to gather evidence. The proper use of these tools can help confirm that the data has not been tampered with (**validate data integrity**). However, it is essential that these tools be used properly.

Digital Forensics Tools

There are different software digital forensics tools available for analysis. These tools are specialized for digital forensics to capture the system image, or a snapshot of the current state of these elements that contains all current settings and data. One common software tool is a mirror image backup, also called a bit-stream backup. This is an evidence-grade backup because its accuracy meets evidence standards.

A mirror image backup is not the same as a normal copy of the data. Standard file copies or backups include only files. Mirror image backups replicate all sectors of a computer hard drive, including all files and any hidden data storage areas. A mirror image backup will also capture the swap file or pagefile that contains data that has been moved from random access memory (RAM) to the drive due to a lack of RAM space, and this should be examined for evidence.

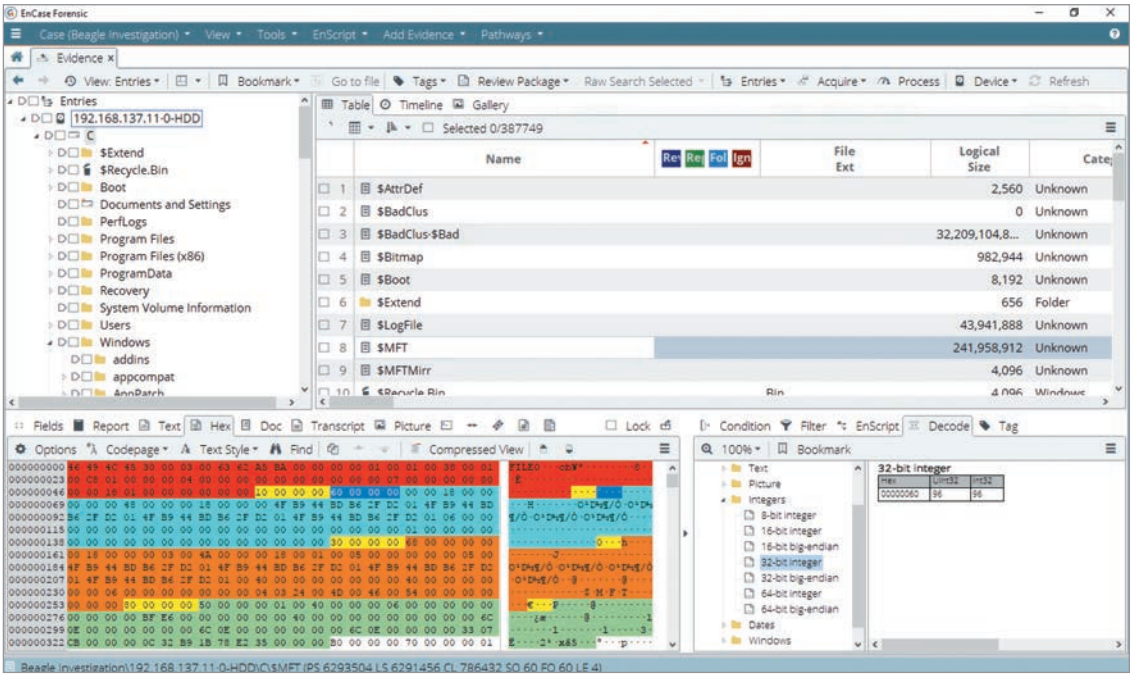
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

Using a standard copy procedure can miss significant data and can taint the evidence. For example, copying a file may change file date information on the source drive, which is information that is often critical in a computer forensic investigation.

Products are available that package multiple digital forensics tools into a single suite that has a common user interface and can more easily exchange information among the different tools. Two of the most common forensic suites are EnCase (shown in Figure 11-6) and FTK Imager. Other popular forensics software tools are memdump, a Linux utility that "dumps" system memory; WinHex, a hexadecimal editor that can be used for forensics; and Autopsy, a digital forensics platform.

Figure 11-6 EnCase software



Source: Open Text Corporation

Instead of gathering different forensics software tools, a digital forensic workstation, which is a computer that is specially configured to perform forensics activities, can be used instead. Digital forensic workstations are typically configured with the latest computer hardware, such as multiple gigabit network ports and Universal Serial Bus (USB) ports, along with "hot swap" bays to hold as multiple drives for examination.

Note 4

Digital forensic workstations are expensive. Depending on the options installed, such a workstation might cost over $20,000.

Acquisition of Evidence When examining technology devices that may contain evidence (**evidence acquisition**), it is critical to follow a specific order. This is because different data sources have different degrees of preservation. An order of volatility must be followed to preserve the most fragile data first. Table 11-4 lists the order of volatility.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 11-4 Order of volatility

Order	Examples	Description
1	Registers and CPU cache	Registers and the CPU cache are extremely volatile and change constantly.
2	Routing tables, ARP cache, process table, kernel statistics, RAM	The network routing and process tables have data located on network devices that can change quickly while the system is in operation, and kernel statistics are moving between cache and main memory, which make them highly volatile. RAM information can be lost if power is lost.
3	Temporary file systems	Temporary file systems are not subject to the degree of rapid changes as the prior elements.
4	Hard drive	Hard drive data is relatively stable.
5	Remote logging and monitoring data	Although remote logging and monitoring data is more volatile than drive data, the data on a drive is considered more valuable and should be preserved first.
6	Physical configuration and network topology	These items are not considered volatile and do not have a significant impact on an investigation.
7	Archival media	Data that has been preserved in archival form is not volatile.

Note 5

The first two levels are considered the most volatile because they can change very quickly. A cache is a type of high-speed memory that stores recently used information so that it can be quickly accessed again at a later time. After retrieving this volatile data, the next focus is on the drive.

An additional source of hidden clues can be gleaned from metadata. Some electronic files may contain hundreds of pieces of such information. Examples of metadata include the file type, authorship, and edit history. Another example of metadata is the date and time that a file was created or accessed.

Create Report Upon completion of the examination, a detailed written description of the acquisition and analysis of the evidence is required. It lists the steps that were taken and any evidence that was uncovered in the forensic investigation. When using products that package multiple digital forensics tools into a single suite, a report can be automatically generated.

Specialized Forensics

There are also specialized forensics for platforms other than standard computers. These include mobile devices, virtualized images, and cloud resources.

Mobile Device Due to their very nature, mobile device forensics is different from performing forensics on an endpoint computer. Although mobile devices are sometimes characterized merely as "portable computers," they actually contain a broader wealth of information than a desktop or laptop computer. Mobile devices are almost continually in a user's possession, unlike a standard computer, and thus can more accurately reveal the user's actions. Forensic information that can be uniquely extracted from a mobile device includes the following:

- **Call detail records.** This information can reveal the date and time a telephone call was started and ended, the terminating and originating cell phone towers that were used, whether the call was outgoing or incoming, the call's duration, who was called, and who made the call.
- **Global positioning system (GPS) data.** GPS data can accurately pinpoint the location of a user and what activities they were performing in a specific location.
- **App data.** Many apps store and access data such as media files, contact lists, and a gallery of all the photos on the device.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- **Text messages.** Text messaging is a popular means of communication. It leaves electronic records of dialogue that can be used as evidence.
- **Photos and videos.** Media recorded as photos and videos on a mobile device can often contain incriminating evidence.

Virtualized Images Performing a forensics investigation on a standard endpoint computer can be a delicate operation. Preserving elements in volatile memory before they change or disappear is especially important. However, what if the entire device has been virtualized and resides only in memory? This is the challenge when performing forensics in a virtualized environment (virtualization forensics).

Analyzing a virtual device is different from investigating an endpoint computer. For example, after capturing the contents of registers, the CPU and ARP cache, process table, kernel statistics, RAM, and temporary file systems on a standard computer, it can then be powered down in order to transport it to another location for more in-depth analysis. However, powering down a virtual machine (VM), which is a simulated software-based emulation of a computer, and then resuming it later will change the volatile evidence. And attempting to perform a "live" analysis on a running VM may change information that resides in memory or cause open network connections to be terminated.

Note 6

Research has shown that how a VM is powered down can impact the amount of data available for analysis.

When performing virtualization forensics, there are two basic options. When using the first option, the VM is suspended and resumed later under forensic analysis so that the forensics investigator can use normal procedures to analyze the VM. However, when resuming, the VM files that are stored could change, destroying critical evidence.

The second option is to create a snapshot of the VM and then work directly with the VM files that are stored on the host system. By taking a snapshot, the state of the hard disk is preserved and any changes to the disk are stored in a separate file, while the virtual memory of the VM is stored in a file and any state changes are written to another virtual memory file. This can ensure that evidence is preserved and can be presented to court as forensically sound evidence.

Note 7

Both EnCase and FTK support conversion of VMware .vmdk files to raw (dd) format. However, FTK also converts the snapshot along with any previous snapshots and the base .vmdk files.

Cloud Resources If the incident is the result of a breach of cloud-based resources, it is not possible to secure the scene to perform a forensics investigation on the cloud (cloud forensics) as in an on-prem incident. When dealing with a cloud incident, the following should be considered:

- A primary concern is to ensure that the digital evidence has not been tampered with by third parties so it can be admissible in a court of law. In Software as a Service (SaaS) and Platform as a Service (PaaS) models, because customers do not have control of the hardware, they must depend on the cloud service providers for accumulating log data. A right-to-audit clause in a cloud contract gives the customer the legal right to review the logs, and these should be negotiated in advance.
- When a cloud customer is notified by its cloud service provider that an incident occurred, the immediate response from the customer's in-house legal and IT teams will be to ask for details about the scope of the impact. Unless they are contractually obligated, the cloud provider may take weeks or even months to provide its client with details as they perform an investigation. However, once the cloud customer has been notified, the "clock has started ticking" regarding data breach notification law deadlines. This can place the cloud customer in an awkward situation.
- The legal regulatory/jurisdiction laws that govern the site in which the cloud data resides may present difficulties. For example, a court order issued in a jurisdiction where the cloud data center is located will likely not be applicable to another jurisdiction in another country.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Caution

When creating a cloud platform, the customer can often choose the region in which the data will reside. It is at this time that issues regarding jurisdiction should be considered, and the region chosen carefully.

Generate IOC

Post-incident activities cannot be accurately performed unless the evidence of the attack has been retained (evidence retention). Preserving critical electronic evidence during a cybersecurity incident is essential to use after the incident to fully understand all the parts of the attack. Evidence retention is also vital to establish a basis for further investigation.

Note 8

Incident responders must be properly trained in order to be fully prepared to contain and remediate the incident as quickly as possible. However, responders must be careful not to rush the collection of evidence because this could destroy or compromise items of evidentiary value, which could identify attackers' methodology and how the system was compromised. Items of evidence must also be appropriately collected in accordance with established regulations so that evidence can assist law enforcement in successful prosecution of the crime.

One of the primary uses of retained evidence is to generate IOC. IOC can be used to clean up and identify the compromised endpoints within the organization, create custom signatures for future detections, and share them with the broader security community.

Evidence and artifacts left by attackers such as running malware processes, dropped malware into systems, and logs that show adversary lateral movement can all be used to generate IOC. Other IOC include hashes of executable malware, identification of C&C Internet Protocol (IP) addresses, domains and subdomains used by threat actors, and changes to network traffic levels. Sharing IOC with the security community at large is also important.

Update Incident Response Plan

While it may be difficult to see any "silver lining" to a cyber incident, in one respect a cyber incident can serve to thoroughly test and expose any weaknesses in the cyber incident response plan. Each of the different actionable goals of the incident response plan should be analyzed in light of the cyber incident to determine the updates that need to be made. Table 11-5 lists the different cyber incident response plan goals and the type of questions that should be asked of each when reviewing the plan.

Table 11-5 Cyber incident response plan goal review questions

Plan item	Question
Preparation	Did we equip our users and systems to handle the incident as it happened?
Identification	Were we able to promptly decide if the action was a cybersecurity incident that required an immediate response?
Analysis	Could we determine how the incident functioned? Did we identify the affected systems? How accurate was our assessment of the overall impact?
Containment	Did we isolate the affected systems promptly to prevent further damage?
Eradication	Did we make the correct determination as to how to remove the affected system from production?
Recovery	Were our recovery efforts timely?
Follow-up	Was our review clear and detailed?

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Assess the Cyber Incident

"Assessing" means to evaluate or judge. It is critical to evaluate the cyber incident so as to lessen the chance of a reoccurrence by taking corrective actions and documenting the event. This is also called creating **lessons learned**. Assessing a cyber incident involves examining metrics and key performance indicators and performing a root-cause analysis.

Examine Metrics and Key Performance Indicators (KPIs)

Metrics are the quantifiable results that come from measuring while key performance indicators are used to measure crucial security initiatives. Metrics and KPIs can be used in helping assess cyber incidents. Table 11-6 lists several cybersecurity KPIs. These are illustrated in Figure 11-7.

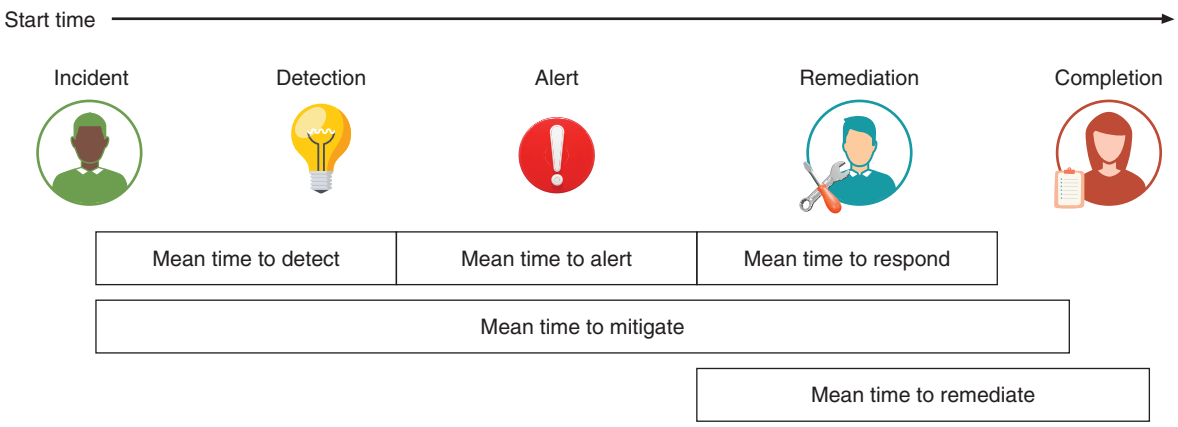
Table 11-6 Cybersecurity KPIs for incident assessment

Key performance indicator (KPI)	Description
Mean time to detect	Mean time to detect is the average time it takes for a cybersecurity team to discover an incident in the organization's environment
Mean time to alert	The mean time to alert is the average time for a system to generate an alert so that action is taken by either a human or an automated system
Mean time to respond	The mean time to respond is the average time to react to a cyber incident from when the alert first occurred
Mean time to mitigate	The mean time to mitigate is from the customer's point of view as to when they are no longer affected or stop seeing problems (although the security operations center or SOC may still be working on the problem, but it is no longer apparent to the customer)
Mean time to remediate	"Remediate" applies to when the incident response is completed from the responder's perspective, so the mean time to remediate is the average time for the response to be finished

Caution

Although sometimes abbreviations are used with the KPIs, there are a number of KPIs with overlapping abbreviations that can cause confusion. For example, the "R" in "MTTR" can stand for repair, recovery, respond, or resolve, and each of these are cybersecurity KPIs. To avoid confusion, it is recommended that abbreviations be avoided.

Figure 11-7 Comparison of KPIs



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

The industry values of cybersecurity KPIs are shocking. In 2023, the mean time to detect and respond to a ransomware attack was 326 days and 277 days for other types of data breaches. The most common cause of data breaches, stolen or compromised credentials, took 327 days to identify.

One reason for poor KPIs is attributed to extremely high **alert volume**, or the number of notifications that a SOC continually receives. This produces fatigue and makes it difficult for a SOC analyst to identify true threats, remediate the threats, and spend time on strategy and process improvements.

Note 9

The numbers associated with potential attacks are mind-boggling. The SOC at the Los Angeles port authority stops about 40 million attempted cyberattacks each month. Managed service provider (MSP) Netcraft analyzes from its customers over 5 million threat reports and suspicious web addresses daily.

Perform Root-Cause Analysis (RCA)

A **root-cause analysis (RCA)** is a method of identifying and solving the underlying factors that contributed to a cybersecurity incident. The goal of an RCA is to mitigate or prevent future attacks and improve the overall security posture by learning from mistakes.

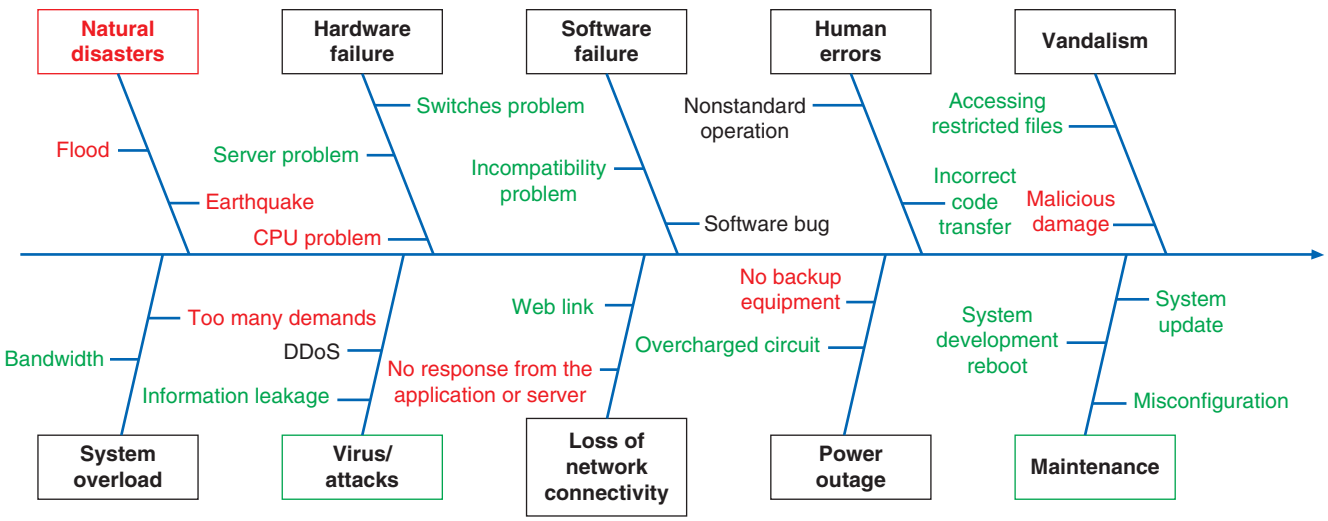
RCA is a systematic and team-oriented process of finding and addressing the underlying causes of an incident. This is different than simply treating the symptoms and the immediate consequences. It looks at understanding why an incident occurred, what factors enabled and facilitated it, and what actions or changes are needed to prevent or reduce the likelihood of recurrence again. RCAs can improve security controls and processes by identifying and eliminating vulnerabilities, gaps, or weaknesses.

Note 10

An RCA can also enhance the security culture and awareness of an organization by fostering a mindset that is always learning. It also encourages accountability and transparency in the organization.

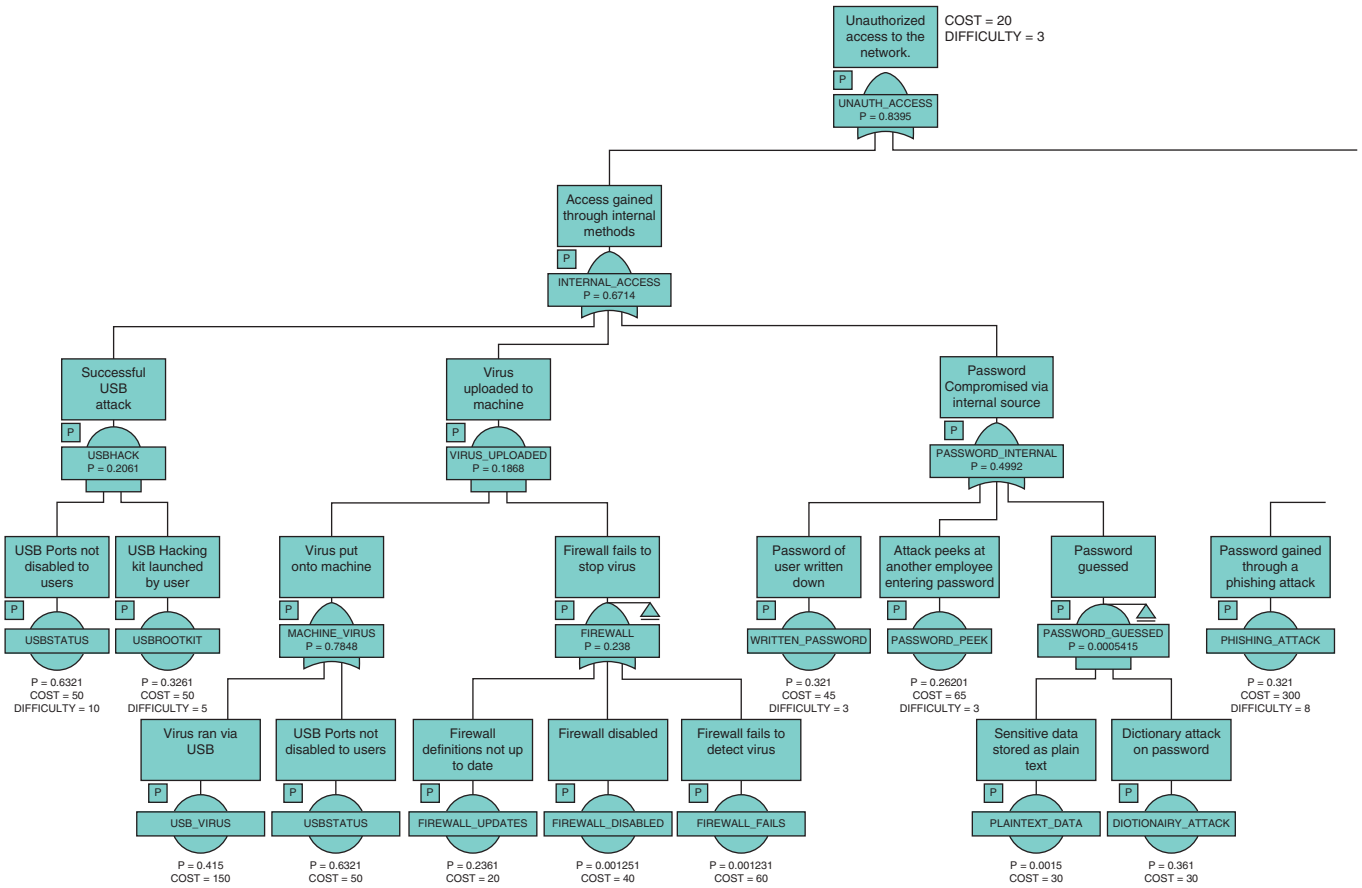
There are several common steps for conducting an RCA. The first step is to define the incident clearly and objectively using data and evidence that has been accumulated from all sources, such as incident response reports, metrics and KPIs, logs, reports, interviews, and surveys. The next step involves identifying and prioritizing all potential root causes. Applying tools such as fishbone diagrams and fault tree analysis is helpful. These are illustrated in Figures 11-8 and 11-9. It is then important to validate for verification the root causes through tests, experiments, and simulations. Finally, corrective and preventive actions should be implemented.

Figure 11-8 Fishbone diagram



Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 11-9 Fault tree analysis



Produce Incident Response Reports

There are different sections in an incident response report that should be created following an incident. The **executive summary** is the first section of the report and should provide a concise overview of the main content. As its name suggests, the executive summary should be written in clear and nontechnical language for "executives" who may not have a deep technical background or expertise in cybersecurity. It should use clear, plain, and concise language while avoiding technical terms.

The report should likewise include specific technical information about the incident. The details of the entire cyber incident from initial detection to final remediation and follow-up should be included. This report attempts to answer the "5 Ws" commonly used in any investigation: **who, what, when, where, and why**. As applied to an incident response report, they can provide information such as the name of the person reporting the incident and the responsible parties that responded (who), a description of the incident (what), the time that it occurred (when), the location (where), and the reason for it occurring (why).

Other important information includes the sequence of events that occurred (**timeline**), the effect on the organization (impact), the documentation regarding the incident (evidence), the breadth of the incident (scope), and finally any suggestions for improvement (recommendations).

Using a standard template for an incident response report can help provide a consistent set of information. Figure 11-10 illustrates an incident response report template.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 11-10 Incident response report template

Section 1: Incident Information

(This section to be completed by the Reporting Individual to the extent possible at the time of the report.)

Date/Time of Initial Report:
Date/Time Activity First Detected:
Incident Tracking Number:

Reporting Individual Contact Information			
First Name	**Last Name**	**Email**	
Office Number	**Cell Number**	**Department**	**UserID**

Incident Description *(This section should be updated as the incident is handled.)*	**Description**
How was this incident detected/discovered?	
What triage/analysis has been performed?	
Is the incident contained? How?	
What recovery/remediation action has taken place?	

Functional Impact

☐ No Impact
☐ No Impact to Services
☐ Minimal Impact to Non-Critical Services
☐ Minimal Impact to Critical Services
☐ Significant Impact to Non-Critical Services
☐ Denial of Non-Critical Services
☐ Significant Impact to Critical Services
☐ Denial of Critical Services/Loss of Control

Information Impact

☐ No Impact
☐ Suspected But Not Identified
☐ Privacy Data Breach
☐ Proprietary Information Breach
☐ Destruction of Non-Critical Systems
☐ Critical Systems Data Breach
☐ Core Credential Compromise
☐ Destruction of Critical System

Attack Vector

☐ Unknown
☐ External/Removable Media
☐ Improper Usage
☐ Loss or Theft of Equipment
☐ Impersonation/Spoofing
☐ Attrition
☐ Web
☐ Email/Phishing
☐ Other

Two Rights & A Wrong

1. The first step in digital forensics is to preserve the evidence.
2. The chain of custody documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence.
3. Mean time to remediate applies to when the incident response is completed from the responder's perspective.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Summary

- There are several activity phases related to incident response for an organization. The first phase in incident response is the detection of an incident followed by an analysis of it. One of the most difficult steps in an incident response and recovery process is the initial analysis of determining if a cyber incident occurred. Although it may seem that this is a simple question to answer, in reality it can be difficult. There are several general principles that are helpful. In addition, there are some signals that can be used to determine if an incident did occur. Two such signals include indicators of compromise and data and log analysis. Determining the severity of an incident is another critical step. That is because giving attention to an incident that is not critical can give a different critical incident time to cause widespread damage. If determining if an incident occurred is one of the most difficult steps, then prioritizing is perhaps the most critical step. A security professional must be able to quickly prioritize events in order to respond to the most damaging event first.
- The next activity phase of incident response is containment, which is designed to keep the incident under control by limiting its impact. Containment often begins by examining the scope, impact, and remediation. Characteristics that contribute to severity-level classifications are called the scope. Impact is the significance of the incident measured in the magnitude of harm that is caused. Remediation is neutralizing or eliminating the vulnerability responsible for the cyber incident. There are different containment techniques or strategies for containing a cyber incident. How these are implemented will depend on the situation and type of attack. The most common containment techniques are removal, isolation, segmentation, and reverse engineering.
- After the incident has been contained, then eradication, which is the elimination of the infection, should be performed. In addition, at this step the necessary procedures for recovery of the systems back to their necessary performance (restoration of capabilities and services) are also begun. Recovery does not mean restoring the systems back to their original state, for this would also reintroduce the vulnerability. Instead, vulnerability mitigation, which is the step to reduce or eliminate the vulnerabilities, is also implemented.
- There are different eradication techniques to clean malware that has infected the hard disk drive of a system. The first step is to physically erase the data from the hard drive. The most secure approach is data sanitization. This method performs a complete data destruction of all contents of the drive by "overwriting" the entire drive, which is replacing data on the drive by writing other data over it. If the hard drive cannot be sanitized and reconstructed or reimaged, the drive should be completely destroyed. After the malware has been eradicated and before it is fully integrated back into the system (reconstitution of resources), it is important to take actions to ensure that the repaired systems will not be susceptible to the same incident again.
- Once the impacted system has been restored, the final phase is to perform various tasks known as post-incident activities. These are designed to lessen the chance of a reoccurrence by taking corrective actions and to document the event. Digital forensic analysis involves the retrieval of difficult-to-obtain data, which may be hidden, altered, or even deleted by the threat actor. It is using technology to hunt for technology-based evidence, which is particularly important when evidence is collected that may be used in the prosecution of the threat actor through the legal system.
- When responding to an incident that requires an examination of a local endpoint or a network appliance in a data center using digital forensics, five basic steps are followed, which are similar to those of standard forensics. When an incident occurs that involves technology, action must be taken immediately. A delay of even a few minutes can allow digital evidence to be overwritten in the normal function of the device, become contaminated by other users, or give the perpetrator time to destroy the evidence. The next task is preservation of evidence or ensuring that important proof is not corrupted or even destroyed. Preserving evidence can also help mitigate nonrepudiation, or a denial by the perpetrator that they were involved or did anything wrong. Documenting the evidence from the very beginning is called provenance. The chain of custody documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence. When examining a device for evidence, there are specialized tools that should be used to gather

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

evidence. Upon completion of the examination, a detailed written description of the acquisition and analysis of the evidence is required. There are also specialized forensics for platforms other than standard computers. These include mobile devices, virtualized images, and cloud resources.

- Post-incident activities cannot be accurately performed unless the evidence of the attack has been retained (evidence retention). One of the primary uses of retained evidence is to generate indicators of compromise (IOC). IOC can be used to clean up and identify the compromised endpoints within the organization, create custom signatures for future detections, and share them with the broader security community. Another important post-incident activity is to update the incident response plan based on the attack. It is critical to evaluate the cyber incident so as to lessen the chance of a reoccurrence by taking corrective actions and documenting the event. This is also called evaluating lessons learned. Metrics are the quantifiable results that come from measuring while key performance indicators (KPIs) are used to measure crucial security initiatives. Metrics and KPIs can be used in helping assess cyber incidents. A root-cause analysis (RCA) is a method of identifying and solving the underlying factors that contributed to a cybersecurity incident. The goal of an RCA is to mitigate or prevent future attacks and improve the overall security posture by learning from mistakes.
- There are different sections in an incident response report that should be created following an incident. The executive summary is the first section of the report and should provide a concise overview of the main content. The report should likewise include specific technical information about the incident that answers the "5 Ws" commonly used in any investigation (who, what, when, where, and why). Other important information includes the sequence of events that occurred (timeline), the effect on the organization (impact), the documentation regarding the incident (evidence), the breadth of the incident (scope), and finally any suggestions for improvement (recommendations).

Key Terms

alert volume
chain of custody
containment
data and log analysis
eradication
evidence acquisition
executive summary
forensic analysis
impact
incident declaration and escalation
isolation
legal hold
lessons learned
mean time to remediate
post-incident activities
preservation of evidence
reimaging
remediation
root-cause analysis (RCA)
scope
timeline
validate data integrity
who, what, when, where, and why

Review Questions

1. Which of the following is NOT a reason it is difficult to determine if a cyber event occurred?
   a. Inaccuracy of security indicators
   b. Multiple indicators
   c. Faulty human statements
   d. Slow speed of vulnerability assessments

2. Which of the following is a general principle for determining if a cyber incident occurred?
   a. It may simply be a matter of educated judgment.
   b. It requires analyzing CVSS-ARC statements.
   c. It demands analysis before a data breach occurs.
   d. It must always be based on factual evidence.

3. Which of the following is NOT correct about determining the severity of a cyber incident?
   a. When faced with determining the severity, it is important to consider its impact in the context of security as a whole.
   b. The severity of a cyber incident is generally considered to be a task that novice security personnel should evaluate due to the time needed for analysis.
   c. Once low-level security incidents have been eliminated, the severity of the remaining incidents can be determined.
   d. Giving attention to an incident that is not critical can give a different critical incident time to cause widespread damage.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

4. Which of the following is NOT a general principle for first-level priority triage?

   a. Consider the level of expertise of the threat actor.
   b. Consider who will be affected.
   c. Consider the ability to recover.
   d. Consider current and future consequences.

5. Which of the following is NOT considered a category of the amount of effort needed to recover from an incident?

   a. Supplementary
   b. Normal
   c. Infinite
   d. Unrecoverable

6. What is system process criticality?

   a. The degree to which the impacted systems affect the overall functionality of the entire system
   b. A KPI metric
   c. The final determination in judging a containment strategy
   d. An unpatched system

7. Which containment element addresses the significance of the incident measured in the magnitude of harm that is caused?

   a. Affect
   b. Scope
   c. Impact
   d. Influence

8. Which containment technique would allow an affected device to continue to communicate with a C&C system but would filter the communication?

   a. Removal
   b. Compartmentalization
   c. Isolation
   d. Segmentation

9. Which eradication technique for removing malware from an infected drive is the most secure?

   a. Delete
   b. Format
   c. Data wipe
   d. Erase

10. What is reimaging?

    a. Patching a drive that has been deleted
    b. Applying a saved image to a sanitized drive
    c. Moving a drive image to a VM
    d. Overwriting a drive with unprintable codes

11. Which of the following is NOT a step in the validation process?

    a. Patching
    b. Eradication
    c. Scanning
    d. Permissions

12. Which of the following is NOT correct about securing the scene following a cyber incident?

    a. A digital forensics incident response team should be contacted.
    b. Law enforcement personnel must be contacted to take custody of all devices.
    c. Cable should be identified and tagged.
    d. Action must be taken immediately.

13. How can data be protected so that it cannot be modified, deleted, erased, or destroyed?

    a. Place it under a legal hold.
    b. Copy the data to a secure device.
    c. Make images of the drive to be stored remotely.
    d. Data cannot be protected to that extent.

14. Which has the highest level of volatility?

    a. Registers and CPU cache
    b. ARP cache
    c. Temporary file systems
    d. Kernel statistics

15. Which type of forensic information is NOT uniquely available on a mobile device?

    a. CPU registers
    b. SMS texts
    c. GPS data
    d. App data

16. Which of the following is NOT IOC that can be left by threat actors?

    a. Changes to XRC files
    b. Identification of C&C IPs
    c. Hashes of executable malware
    d. Running malware processes

17. Which of the following applies to when the incident response is completed from the responder's perspective?

    a. Mean time to completion
    b. Mean time to mitigation
    c. Mean time to respond
    d. Mean time to remediate

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

18. What is a method of identifying and solving the underlying factors that contributed to a cybersecurity incident?

a. ADR
b. ACDR
c. ACA
d. RCA

19. What is the first section of an incident response report that provides a concise overview of the main content of the report about the incident?

a. Technical overview
b. Lessons learned
c. Executive summary
d. Management mistakes

20. Which of the following makes up the questions commonly used in any investigation?

a. Who, what, when, where, and why?
b. How did the threat actor enter the system?
c. Which vulnerabilities were the most critical that were compromised?
d. How can this be prevented in the future?

Case Projects

Case Project 11-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. Should Apple make Stolen Device Protection a default setting instead of a user option? What other changes should be made in order to make it more secure? Why do passcodes have a minimum length of only four digits? Should a longer alphanumeric code be required instead? Write a one-page paper about this topic.

Case Project 11-2: General Principles for First-Level Triage

Estimated Time: 25 minutes
Objective: Differentiate between different principles of first-level triage.
Description: Review Table 11-1. Now add two additional columns to the table. The first column will contain an example of a cyber incident that illustrates the principle that would increase the importance of the incident, while the second column contains an example that would decrease the importance of the incident. What have you learned from this exercise about determining how to prioritize incidents? Is there a way to streamline the process? Write a one-page paper on your research.

Case Project 11-3: Examples of United States Computer Emergency Readiness Team Severity Levels

Estimated Time: 30 minutes
Objective: Identify different examples of severity levels.
Description: Review Table 11-2. Use the Internet to find eight examples of cyber incidents, each of which applies to one of the severity levels. Would you agree with the impact severity level? Should it have been more or less? Write a one-page paper on your research.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Case Project 11-4: Sanitation Methods

Estimated Time: 25 minutes
Objective: Categorize contemporary sanitation methods.
Description: Use the Internet to find samples of at least three additional sanitation methods besides those listed in Figure 11-3. Create a table that lists the method, a description, the characters and passes, and any software that performs the function.

Case Project 11-5: Root-Cause Analysis (RCA)

Estimated Time: 25 minutes
Objective: Research root-cause analysis (RCA).
Description: Use the Internet to research root-cause analysis (RCA). How is it used? What examples can you find of RCA? What steps are involved in the process of an RCA? Write a one-page paper on your findings.

Two Rights & A Wrong: Answers

Detection and Analysis

1. The first step in the detection and analysis activity phase is to determine if a cyber incident actually occurred.
2. Both IOC and data and log analysis can serve as indicators of a cyber incident.
3. "Recovery time" is the same as downtime.

Answer: The wrong statement is #3.
Explanation: Recovery time is not the same as downtime. Recovery time is the length of time needed for the IT systems to be disinfected and return to their normal functions. The length of time that the incident interrupts the normal business processes is downtime.

Containment

1. Once it has been determined through detection and analysis that an incident did occur, an announcement goes out to relevant parties and the importance of addressing this incident is elevated.
2. Scope is the significance of the incident measured in the magnitude of harm that is caused.
3. The removal containment technique is the simplest to implement.

Answer: The wrong statement is #2.
Explanation: While scope is the breadth and depth of the cyber incident, impact is the significance of the incident measured in the magnitude of harm that is caused.

Eradication and Recovery

1. After the incident has been contained, then eradication should be performed.
2. Data formatting performs a complete data destruction of all contents of the drive by "overwriting" the entire drive by replacing data on the drive by writing other data over it.
3. Applying a saved image to a sanitized hard drive is called reimaging.

Answer: The wrong statement is #2.
Explanation: Data formatting performs a complete data destruction of all contents of the drive by "overwriting" the entire drive.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Post-Incident Activities

1. The first step in digital forensics is to preserve the evidence.
2. The chain of custody documents that the evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence.
3. Mean time to remediate applies to when the incident response is completed from the responder's perspective.

Answer: The wrong statement is #1.
Explanation: The first step in digital forensics is to secure the scene.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Chapter 12

Data Protection and Utilization

Chapter Objectives

After completing this module, you should be able to do the following:

1. Describe the perils against user data
2. Explain the controls used for protecting sensitive data
3. Describe how to use data for cybersecurity

#TrendingCyber

What device do you own that captures 25 gigabytes (GB) of your personal data every hour? Is it your phone? Computer? Fitness tracker?

It's none of these. The answer may surprise you: it's your car. On average, in one hour of driving time, your car collects 25 GB of data about the vehicle, how and where it is driven, and even the driver and passengers. To put it in perspective, you would have to surf the Internet 24 hours a day for 2 months, stream video for 34 hours, stream music for 263 hours, upload 5,133 photos, or play an online game for 1,280 hours to equal the same amount of data usage that your car collects in just 60 minutes.

Your car knows a lot about you. And over the past decade, its ability to record data has increased exponentially. While modern cars have been described as "computers on wheels," a more apt description is they are "smartphones on wheels." Just as our smartphones collect a wealth of data on which apps we use, where we go, who we interact with, which websites we visit, and virtually every other event of our daily digital lives, our cars collect even more data. Most car owners understand very little about what data their cars can collect—and many car manufacturers like it that way. While the level of detail and transparency varies across car manufacturers, no car steers clear of gathering reams of data.

It all started with diagnostic data. For many years, all cars gathered diagnostic information in order to watch for worn parts or mechanical issues. This data remained in the car itself until a mechanic used a device to view it. But that is no longer the case: vehicle diagnostic data is wirelessly (and silently) sent off to the manufacturer, who can then alert the driver via messages on the car's dashboard or emails as to a mechanical issue.

However, car data collection and transmission did not stop at diagnostic data. Today that's only the tip of the iceberg.

Through purchase records, state vehicle registration, and insurance companies, car manufacturers know your name, address, driver's license number, Social Security number, phone number, email, and other personal information. Linked to this personal information is data from your car. Called your "driving behavior," it includes details of all trips (the date and time when you start and end, the starting location and destination, the route taken, the weather, and so on) along with your speed, acceleration, and braking data. It may also collect images taken by your car's external

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

cameras and sensors. Since most users connect their smartphone to their cars, the information on their phones can also be accessed by the car itself (many car manufacturers are silent on whether their cars collect data from phones that are synced with its vehicles, but their silence may speak volumes).

And it doesn't stop there. Some cars can collect very detailed information about your vehicle (such as fuel levels, tire pressure, and battery charge status). And it can likewise collect very detailed driver behavior information while the car is being driven. This can include the pedal position, engine speed, steering angle, and "braking and swerving/cornering events," among other data. There is also information about how you use the "infotainment" system in your vehicle, such as search content, call history, and voice commands. It is even possible for the car to listen to your conversations with other occupants while driving. Your face and fingerprint data may be collected if you use services such as digital keys. And most drivers and riders would be shocked to learn that today's airbag system in a car can collect the body weight of each of the occupants!

But wait, there's more.

One popular electric vehicle (EV) gathers charging data, driving characteristics such how you push the pedals, and seatbelt-related data. And voice recognition systems in some EV vehicles can gather information when you give commands. Their "media analytics" capture information about what you listen to in your car, including radio presets, volume, channels, and media sources along with the song title, artist, and music genre. Data from stability control or anti-lock events, security/theft alerts, and Wi-Fi data usage can be collected. The car company can even collect information about your home energy usage if you plug in your car to recharge the battery when at home.

Drivers are trying to push back on this mass collection from our cars—but so far with little success. In late 2023, a class-action lawsuit alleged that five major car manufacturers recorded and intercepted car owners' private text messages and call logs when their phones were connected to the vehicles' infotainment systems. However, a federal judge dismissed the cases because they did not satisfy the state's statutory injury requirement where the suit was filed, which says plaintiffs must allege an injury to their person, reputation, or business. The judge said that the plaintiffs' allegation that a violation of the statute itself did not satisfy the requirement that there was "injury to a person," and intercepting text messages was not an "injury."

Soon cars will be able to collect even more data. One leading car manufacturer in early 2024 announced that its vehicles will have the artificial intelligence ChatGPT chatbot integrated into its voice assist feature. According to the manufacturer, this offers a "multitude of new capabilities that go far beyond the previous voice control." For example, the car's ChatGPT voice assistant can be used to control the infotainment, navigation, and air conditioning systems or answer general knowledge questions. In the future, it will provide additional information in response to a driver's questions and "can be helpful on many levels during a car journey by enriching conversations, clearing questions, interacting in intuitive language, receiving vehicle-specific information, and much more." There is no indication that this artificial intelligence data will not be collected by the car manufacturers.

As #TrendingCyber illustrates, our private lives are anything *but* private. The volume of data collected about us in our normal daily routines is almost beyond comprehension. And where does this data go? Who sees it? How is it being used?

Consider the following examples. One fitness tracker, which remotely collects data on how its users exercise, reported that over a one-year period, there has been a dramatic increase in the specific exercise activities of Pilates (up 49 percent), stair climbing (31 percent), strength training (30 percent), and yoga (23 percent) while other activities like indoor biking and outdoor running rose only slightly (5 percent each). Yet few fitness tracker users realize that their data is being collected and used in this way.

Or consider cars again. Recently Tesla initiated a "recall" of about two million vehicles, which is nearly all the cars it has sold so far in the United States. This recall did not require Tesla owners to visit a dealership to have work done on the cars, but it updated the Autopilot software and installed new safeguards to prevent driver misuse. Tesla did this by beaming a software update to vehicles through a wireless connection to add new controls and alerts that ensure drivers stay focused on the road. But Tesla also announced that with these more visible alerts, the software update would implement a suspension policy: drivers who repeatedly failed to use the system properly will find that the Autopilot feature is disabled for up to one week and, once reactivated, stricter requirements for driver attentiveness, including when a vehicle approaches traffic lights and stop signs off-highway, will be enforced.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

These examples and many others illustrate that serious questions surrounding the collection and utilization of user data are at the forefront of our world today.

But it would be a serious mistake to think that *all* data is bad. In fact, the proper usage of data in cybersecurity is also at the forefront of our world today. By utilizing artificial intelligence and data analytics tools, data can be used today to protect users and even predict attacks before they occur.

In this final chapter, you explore perils against user data, controls for protecting sensitive data, and the beneficial utilization of data for cybersecurity.

Perils Against User Data

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

The perils of user data are due to the types of data collection that gather the data. This has raised serious concerns over the collection and usage of the data.

Types of Data Collection

There are two types of data collections of user private data that occur. The first is an "overt and legitimate" gathering of this data by an organization. For example, an organization may have a valid business need to ask a customer for their address and mobile phone number, and then keep this data on file. And the request for the data comes from asking the customer to provide it; it is not collected surreptitiously (secretly).

The second type of data collection is a "concealed and questionable" gathering of user data. It is concealed because it is usually done in secret without the user's clear knowledge and express consent; it is questionable because there is not a clear business case for gathering it.

The ability of an organization to collect user data in a "concealed and questionable" manner is founded on the fact that every time a user interacts with technology, they leave behind a "data trail," which is a digital record of their activity. This includes obvious activities such as sending an email, browsing the Internet, and making a purchase—in short, any direct user activity using technology.

But today, data is predominantly collected by using tracking features (trackers) that are embedded in virtually every app on a smartphone; in fact, the average app has six trackers. Trackers allow third parties to collect data from the user's interaction with the app along with exactly where the user is located. And as more and more activities of a user's everyday life are performed electronically using more and more interconnected devices, the volume of data compiled on each user grows exponentially each day.

Note 1

Smartphones are not the only devices that collect user data. It is becoming increasingly difficult to purchase an appliance or even a smaller household "gadget" that does not require an Internet connection. Almost all high-end washing machines, dishwashers, dryers, refrigerators, and ovens require Wi-Fi connectivity. These connections allow the manufacturers to gather data on user activities and then transport the data back to their company—which it then combines with other data to build a comprehensive profile. Some companies are now intentionally disabling features until the appliance is connected to a Wi-Fi network—despite the fact that these same features have been available on older unconnected appliances for over 75 years!

Concerns Over Data Collection and Usage

There are significant issues raised with how both types of data collection—overt/legitimate and concealed/questionable—are used. These often overlap and are summarized in Table 12-1.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 12-1 Issues regarding how private data is collected and used

Issue	Explanation
Data is gathered and kept in secret.	Users have no formal rights to find out what private information is being gathered, who gathers it, or how it is being used.
The accuracy of the data cannot be verified.	Because users do not have the right to correct or control what personal information is gathered, its accuracy may be suspect. In some cases, inaccurate or incomplete data may lead to erroneous decisions made about individuals without any verification.
Identity theft can impact the accuracy of data.	Victims of identity theft will often have information added to their profile that was the result of actions by the identity thieves, and even this vulnerable group has no right to see or correct the information.
Unknown factors can impact overall ratings.	Ratings are often created from combining thousands of individual factors or data streams, including race/ethnicity, religion, age, gender, household income, zip code, presence of medical conditions, transactional purchase information from retailers, and hundreds more data points about individual consumers. How these different factors impact a person's overall rating is unknown.
Informed consent is usually missing or is misunderstood.	Statements in a privacy policy such as "We may share your information for marketing purposes with third parties" is not clearly informed consent to freely allow the use of personal data. Often users are not even asked for permission to gather their information.
Data is being used for increasingly important decisions.	Private data is being used on an ever-increasing basis to determine eligibility in significant life opportunities, such as jobs, consumer credit, insurance, and identity verification.
Targeted ads based on private data can lead to discrimination.	Targeted advertising can perpetuate and reinforce harmful stereotypes. For example, research has shown that online employment ads for science, technology, engineering, and mathematics are disproportionately shown to men and hidden from women.

One particular type of information over which there are serious concerns regarding its collection is **personally identifiable information (PII)**. This is data that could identify a specific individual. It includes the person's full name, Social Security number, driver's license number, bank account number, passport number, and similar information. Other types of information that likewise raise concerns include sensitive personal information (SPI), which is information that does not directly identify an individual but is related to an individual and communicates information that is private or could potentially harm an individual should it be made public (biometric data, genetic information, sex, political party affiliation, union membership, and so on). Inferences can be made about the data and applied to the individual to place them in a specific "category" that may or may not be accurate. Protected health information (PHI) is information as it relates to a person's health data, transactions, and history like mental health history, healthcare services used, and payments for healthcare services.

Two Rights & A Wrong

1. There are two types of data collection: overt/legitimate and concealed/questionable.
2. One concern regarding data collection is that the accuracy of the data cannot be verified.
3. PII includes biometric data, genetic information, sex, and political party affiliation.

See the answers at the end of the chapter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Controls for Protecting Sensitive Data

Certification

1.1 Explain the importance of system and network architecture concepts in security operations.

2.5 Explain concepts related to vulnerability response, handling, and management.

There are two categories of controls that should be used by organizations to protect both sensitive user data as well as important corporate data. These categories are technical controls and nontechnical controls.

Technical Controls

The different technical controls for protecting data can be grouped into four classifications. There are controls to prevent access to data, limit access to data, hide data, and destroy data.

Preventing Access to Data

One classification of technical controls is to prevent access to the data so that an unapproved third party simply cannot access it. These controls include encryption, data loss prevention, geographic access requirements, and access controls.

Encryption Perhaps the most obvious means of preventing access to data is to use encryption. Whereas cryptography is the science of concealing information by using a secret key (the method), encryption is the means to "scramble" the information (the process).

There are several common use cases (situations) for encryption that can provide a range of security protections. One of the most important protections is confidentiality, which can protect the information by ensuring that only authorized parties can view it. When private information, such as a list of employees to be laid off, is transmitted across the network or stored on a file server, its contents can be encrypted, which allows only authorized individuals who have the key to read it. Table 12-2 lists the different information protections afforded by cryptography.

Table 12-2 Information protections by cryptography

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key.
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered the data	Encrypted information cannot be changed except by authorized users who have the key.
Authentication	Provides proof of the genuineness of the user	Proof that the sender was legitimate and not an imposter can be obtained.
Nonrepudiation	Proves that a user performed an action	Individuals are prevented from fraudulently denying that they were involved in a transaction.
Obfuscation	Makes something obscure or unclear	By making it obscure, the original information cannot be determined.

Note 2

The European Union's (EU) 2018 General Data Protection Regulation (GDPR) does not consider encryption or replacing identifying information as strong enough measures that can fully anonymize data to remove all PII.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Data Loss Prevention (DLP) While the threat of data collection from outside the organization remains high, inside employees are increasingly being careless or making mistakes when handling confidential data. Employee carelessness with data has been identified in two primary areas. First, against company policy, many employees routinely send confidential data to their own private email accounts so they can easily access it when needed. About one-third of employees admit to sending corporate data to their personal email accounts up to three times each month. Second, sensitive data is often sent to an approved third-party organization as an email attachment—but to the wrong recipient. Almost three-fourths of employees admit to sending data to the wrong recipient once per month.[1]

Note 3

Surprisingly, research has shown that security awareness training has not had an impact on employee mishandling of sensitive data. The percentage of employees who admit to sending misdirected emails is the highest in organizations that provide security awareness training most frequently. And these same employees are almost twice as likely to send company data to their personal email accounts.

One means of securing internal corporate data is through **data loss prevention (DLP)**. DLP is a system of security tools used to recognize and identify data that is critical to the organization and ensure it is protected. This protection involves monitoring who is using the data, how it is being accessed, and sounding an alert and blocking the export of restricted data. DLP is considered as rights management, or the authority of the owner of the data to impose restrictions on its use.

Most DLP systems use content inspection. Content inspection is a security analysis of the transaction within its approved context. Content inspection looks at not only the security level of the data but also who is requesting it, where the data is stored, when it was requested, and where it is going. DLP systems can also use index matching. Documents that have been identified as needing protection, such as the program source code for a new software application, are analyzed by the DLP system and complex computations are conducted based on the analysis. Thereafter, if even a small part of that document is leaked, the DLP system can recognize the snippet as being from a protected document.

DLP begins with an administrator creating DLP rules based on the data (what is to be examined) and the policy (what to check for). DLPs can be configured to look for specific data (such as Social Security and credit card numbers), lines of computer software source code, words in a sequence (to prevent a report from leaving the network), maximum file sizes, and file types. These rules are then loaded into a DLP server.

If a policy violation is detected by the DLP agent, it is reported back to the DLP server. Different actions can then be taken. These could include blocking the data, redirecting it to an individual who can examine the request, quarantining the data until later, or alerting a supervisor of the request.

Note 4

One of the drawbacks of DLP is that rules must be continually created and maintained as new employees, third-party agent contractors, and customers are added and new datasets are created. Increasingly, machine learning is used by DLP to continually create and modify the criteria for protecting data.

Geographic Access Requirements Whereas DLP restricts data based on its content, another control technology can be used to restrict data based on the location of the user. This requires that the user be in a specific location in order to access the data. This is known as geographic access requirements or, more commonly, geofencing.

Note 5

Geofencing is often used by the court system. As a condition of release until a trial, an accused individual is put under house arrest and is fitted with an ankle bracelet that will alert authorities if they leave the house.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Geofencing begins by taking advantage of the global positioning System (GPS), which is a satellite-based navigation system that provides information to a GPS receiver anywhere on (or near) Earth where there is an unobstructed line of sight to four or more GPS satellites. Mobile devices with GPS capabilities typically support geolocation, or the process of identifying the geographical location of the device. By identifying the location of the device (and hence the person carrying it), geolocation can tell the location of a close friend or the address of the nearest coffee shop. Location services are used extensively by social media, navigation systems, weather systems, and other mobile-aware applications.

Note 6

Banks are expanding the use of geolocation to help reduce bank card fraud. When a user makes a purchase at a specific store, the bank can immediately check the location of the cell phone. If the cell phone and the bank card are in the same place, then the purchase may be considered legitimate. But if the cell phone is in Nashville and someone is trying to make a purchase in a store in Tampa, then the payment may be rejected. Geolocation can also help prevent rejecting valid purchases (a false positive). One credit card issuer says that this can reduce these unnecessary declines by as much as 30 percent.[2]

By using GPS, geofencing can define the geographical boundaries within which an app can be used to access specific data. For example, a tablet containing patient information that leaves the hospital grounds or an employee who attempts to enter a restricted area with a device can result in blocking data access as well as sending an alert to an administrator.

Note 7

There are also risks of geolocation. Mobile device users using geolocation are at increased risk of targeted physical attacks since an attacker can determine where the user with the mobile device is currently located and then use that information to follow the user to steal the device or inflict harm on the person. A related risk is geotagging, which is adding geographical identification data to media such as digital photos taken on a mobile device. A user who, for example, posts a photo on a social networking site may inadvertently be identifying a specific private location to anyone who can access the photo.

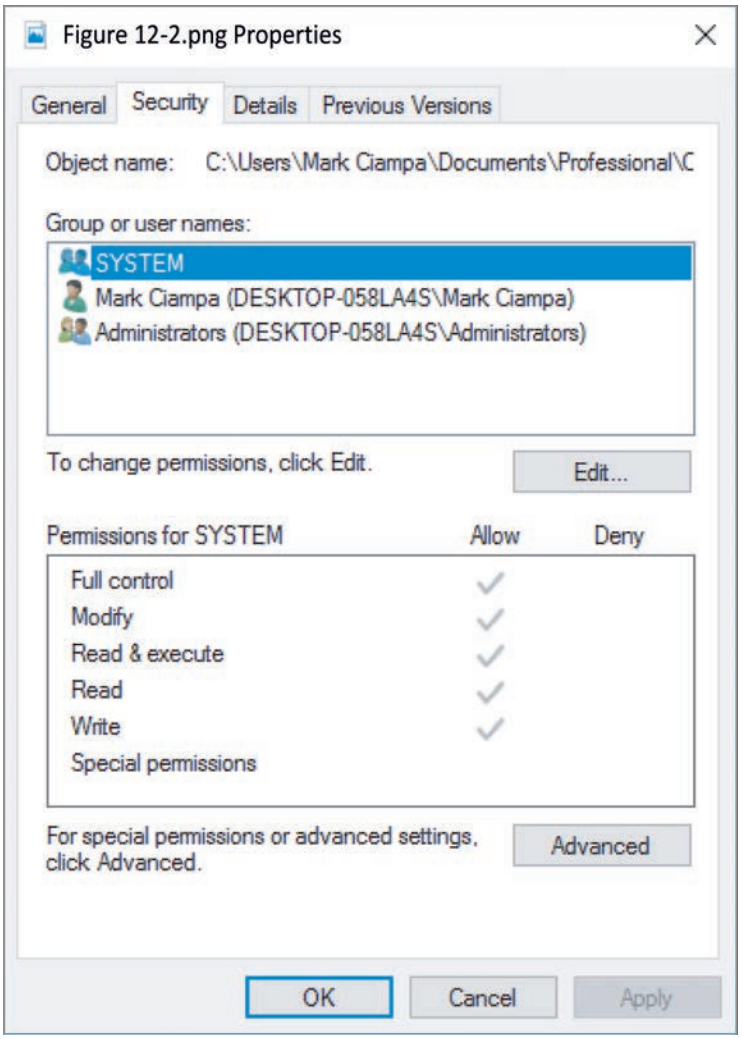
Access Controls As its name implies, access control is granting or denying approval to use specific resources; it is limiting or controlling access to assets. While physical access control consists of fencing or hardware door locks to limit contact with devices, technical access control consists of technology restrictions that limit users on digital devices from accessing resources and data. Using access controls for preventing access to data involves access control schemes and access control lists.

Access Control Schemes The task of a system administrator who needs to act as an access control data custodian/steward for multiple employees using hundreds of thousands of files scattered across a multitude of different servers can be made easier by the fact that the hardware and software have a predefined framework that the custodian can use for controlling access. This framework, called an access control scheme, is embedded in the software and hardware. The custodian/steward can use the appropriate scheme to configure the necessary level of control. Using these schemes is part of privileged access management, which is the technologies and strategies for controlling elevated (privileged) access and permissions.

There are several major access control schemes. The discretionary access control (DAC) scheme is one of the most common but also the least restrictive. With the DAC scheme, every object has an owner, who has total control over that object. Most importantly, the owner has discretion (the choice) as to who can access their objects and can grant permissions to other subjects over these objects. DAC is used on all major operating systems (OSs). Figure 12-1 illustrates the DAC that a Microsoft Windows owner has over an object. These controls can be configured so that another user can have full or limited access over a file, printer, or other object.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 12-1 Windows discretionary access control (DAC)



Source: Microsoft Corporation

The rule-based access control scheme, also called the rule-based role-based access control (RB-RBAC) scheme or automated provisioning, is more robust and can dynamically assign roles to subjects based on a set of rules defined by a custodian (called conditional access). Each resource object contains a set of access properties based on the rules. When a user attempts to access that resource, the system checks the rules contained in that object to determine if access is permissible.

Access Control Lists (ACLs) An ACL contains rules that administer the availability of digital assets by granting or denying access to the assets. There are two types of ACLs. The first type is a filesystem ACL that filters access to files and directories on an endpoint (a filesystem is a method for storing and organizing computer files to facilitate access). Filesystem ACLs provide filesystem permissions for protecting files managed by the OS by telling it who can access the device and what privileges they are allowed. The second type is networking ACLs that filter access to a network. Network ACLs are often found on routers.

Note 8

ACLs are the oldest and most basic form of access control. These became popular in the 1970s with the growth of multiuser systems, particularly UNIX systems, when it became necessary to limit access to files and data on shared systems. Later, as multiuser OSs for personal use became popular, the concept of ACLs was added to them. Today all major OSs make use of ACLs at some level.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Limiting Access to Data

In not all instances is it feasible to strictly prevent access to data. There are several cases in which many users, who may or may not be trustworthy, must nevertheless be able to access data. In cases where preventing access to data is not possible, it is then important to apply the control of limiting access to the data.

Limiting access to data often involves specific data and is not applied for more general data such as PII, PHI, or SPI. This specific data usually includes intellectual property (IP), which is a work or invention that is the result of creativity.

The primary reason for limiting access to IP through a technical control is so that the creator of the IP can maintain specific rights over the content by limiting who can use it, how it can be used, and how it may be distributed. These limitations are necessary so that creators can be duly compensated for their work, generally through earning royalties. Without these technological limitations, creators' work would likely be freely copied and distributed, depriving them of any royalties.

Note 9

In addition to technology controls, the creator may apply for a copyright, patent, trademark, or similar legal protection. These legal protections do not by themselves limit technical access to IP. Rather, they can be applied in a civil (not criminal) court when the content is used in such a way that violates the protections.

However, IP is by its very nature designed to be accessible to a large number of users. Book authors, for example, would generally not want the completed manuscript locked away in a vault; rather, it is intended to be published and distributed so that the author receives payment (royalties) for their efforts. The same is true of films, music, poems, or similar works. The difficulty rests in making the IP accessible—but not *too* accessible. That is, a book may be published in a specific electronic format so that it can be read on a user's mobile device, but not published in a general electronic format like an unprotected Portable Document Format (PDF) file that could be easily distributed through the Internet for anyone to download. This would deprive authors of the royalties for their efforts.

For many years, protecting IP has been attempted through digital rights management (DRM). DRM is a broad category of access control technologies that are designed to restrict the use and duplication of digital content across a wide range of devices. DRM is intended to grant control and protection over IP for the creators and content providers who own the digital media.

Note 10

DRM is much like a multisided prism that looks different to different individuals. To IP creators, rights holders, and publishers, DRM is all the technologies that protect their IP from illegal theft. For the average content consumer, it is sometimes seen as an inconvenient burden that gets in the way when trying to read electronic books, listen to music, or watch films that have been legitimately purchased. And for pirates who want to steal the IP, DRM is viewed as the enemy that must be destroyed.

There have been several technologies that have been developed to support DRM. Table 12-3 lists several of these technologies.

Often used in conjunction with DRM is watermarking. A watermark is an invisible and unique embedded piece of information that is added to the content. If the content is transcoded, resized, shrunk, or altered, the watermark still persists. Watermarking is a means by which pirated content can be easily traced back to the offending user. Watermarking is added in postproduction ("post") after the content is encoded but before it is protected by DRM.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 12-3 DRM technologies

Media	DRM name	Description	Explanation
Broadcast TV – U.S.	Broadcast flag	A set of status bits indicating the permission status of the TV signal or stream	Although the Federal Communications Commission (FCC) mandated that new television receivers manufactured after July 2005 must support the broadcast flag, after numerous struggles with the Supreme Court, the FCC eliminated the broadcast flag in 2011.
Broadcast TV – Europe	DVB Content Protection and Copy Management (DVB-CPCM)	A set of flags (Usage State Information) that are transmitted with the content that describe how the content can be consumed, copied, or exported and can also specify limits on either the viewing time or the number of concurrent devices streaming the content	Similar to broadcast flags, it is concerned only with how content is handled after it is delivered.
E-books	Over 30 competing formats	Formats include EPUB, DAISY, Djvu, iBook, and TomeRaider	EPUB is the most popular e-book format but is not natively supported by the most popular e-reader, Amazon Kindle.
Computer games	Most streaming gaming services and gaming consoles support DRM	Proprietary formats	A limited number of DRM-free games are available.
Music	Apple FairPlay, Sony OpenMG	With streaming music overtaking digital music downloads, it has reduced the need for music DRM	One of the first DRMs for music was Sony's Extended Copy Protection (XCP) that installed a Sony rootkit on the user's computer and sparked a public outrage and a class-action lawsuit.

Caution !

Many traditional DRM technologies have been plagued by usability and legal issues. Other DRM technologies were defeated by pirates and rendered useless. As a result, many publishers in the industry developed their own proprietary DRM technology. However, this only served to segment the market, requiring users to purchase specific DRM software to run on specific DRM hardware.

Hiding Data

Another technical control for protecting data is to hide the data so that it cannot be identified and used (deidentification). These technologies include data masking and tokenization.

Data Masking Data masking involves creating a copy of the original data but using obfuscation (making unintelligible) any sensitive elements such as a user's name or Social Security number. Proper data masking provides no means to reverse the process to restore the data back to its original state. Data masking should replace all actual information that is not absolutely required. Data masking is one means of performing data sanitization, which is the process of cleaning data to provide privacy protection.

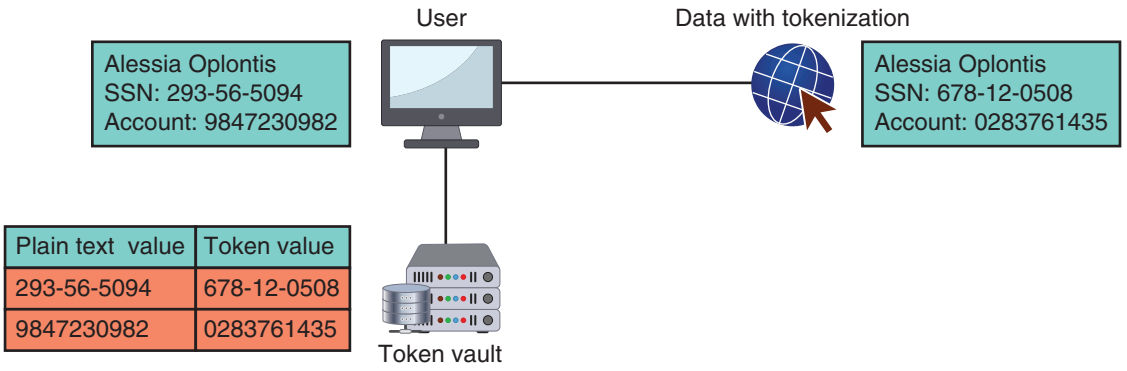
Note 11

Data masking is often used for testing purposes, such as determining if a new app functions properly. It involves creating a copy of the original data but obfuscates any sensitive elements. This enables testers to use actual data but prevents it from being exposed to the tester.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Tokenization Similar to data masking, tokenization obfuscates sensitive data elements, such as an account number, into a random string of characters (token). The original sensitive data element and the corresponding token are then stored in a database called a token vault so that if the actual data element is needed, it can be retrieved. Unlike encryption, which requires the use of an algorithm and a key, tokenization can hide the data while making the retrieval process more seamless. Because it is possible to restore the original data, tokenization is called pseudo-anonymization. Tokenization is illustrated in Figure 12-2.

Figure 12-2 Tokenization



Destroying Data

In 2013, an information technology (IT) engineer in England had two identical hard drives and accidentally threw away the wrong drive into his trash, which was then picked up by the local municipality and deposited into a landfill. On this hard drive was the only private key to unlocking 7,500 bitcoins of cryptocurrency that he owned (he did not have a backup of the key). After he realized his mistake, the engineer asked the city council for permission to search the city's landfill site for his hard drive, but his request was denied. However, since that time, the value of bitcoins has increased dramatically. His bitcoins (and the missing hard drive) are now worth almost $420 million.

Note 12

The engineer who threw away the hard drive returned to the city council in 2021 and offered 25 percent of his bitcoins (worth about $72 million) to set up a COVID-19 relief fund for the city's residents if he was given permission to review the landfill log records, isolate the area in which the dump was made, and then search a small area of the landfill. The engineer stated that he had already received backing from a hedge fund that was willing to make the donation to the city before the search for the hard drive even began.

This cautionary tale serves to illustrate the fact that media that contains valuable data can be inadvertently disposed of before the device is examined and the data erased or retrieved. It is not uncommon for media that contains sensitive user data to be disposed of but later retrieved by threat actors. Thus, destroying data is an important (albeit final) technical control for protecting data.

Because data itself is intangible, destroying data that is no longer needed involves destroying the media on which the data is stored. If any data other than data labeled public is on paper, that media should never be thrown away in a dumpster, recycle bin, or trash receptacle. Paper media can be destroyed by burning (lighting it on fire), shredding (cutting it into small strips or particles), pulping (breaking the paper back into wood cellulose fibers after the ink is removed), or pulverizing ("hammering" the paper into dust).

If data is on electronic media, the data should never be erased using the OS "delete" command (purging). This is because the data could still be retrieved by using third-party tools. Instead, data sanitation tools can be employed to securely remove data. One technique is called wiping (overwriting the disk space with zeros or random data). For a magnetic-based hard disk drive, degaussing will permanently destroy the entire drive by reducing or eliminating the magnetic field. Normally degaussing is a third-party solution because it is a specialized technique requiring special equipment.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 13

There is no universal agreement on the differences between purging and wiping.

Consideration on which data destruction technique to use may hinge upon the need to verify the destruction for regulatory purposes. Some techniques cannot provide this verification. For example, degaussing cannot provide verification that the drive was destroyed. In this instance, it may be necessary to first perform a wiping of the drive to verify that all data has been destroyed before then degaussing the drive to destroy it completely and permanently.

Nontechnical Controls

In addition to technical controls for protecting data, there are also nontechnical controls. These controls include conforming to legal data protections, applying risk management principles, implementing data retention practices, and limiting data collection.

Conform to Legal Regulations

There are different legal regulations that are in place to protect the privacy of user data, and following these regulations can be considered a nontechnical control. To violate these regulations may have significant ramifications (legal implications). Currently there are no universal protections (global data protections) to which all nations adhere. There are, however, protections that apply to a country or group of countries (national data protections).

In the European Union (EU), data protections cover what are called data subjects, which is any living individual whose personal data is collected and stored by an organization. The fundamental EU principle of data protection is the right to be forgotten, which means that data subjects have a legal right to have the private data erased. The regulation states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay." However, there are a number of conditions that apply, such as the data is no longer necessary for the purpose an organization originally collected it.

Note 14

"Undue delay" is interpreted to be about 30 days.

The United States, however, has no "right to be forgotten" regulation. This is in part due to the fact that the ownership or legal possession and control of the data has not been firmly established. Different states have passed privacy laws so that they are local/regional data protections, but these vary widely. This means that U.S. data protections are primarily those established as industry regulations that an organization takes to be in compliance. These regulations typically outline the tasks of a controller versus a processor, how organizations should monitor collected data (data inventory), and the length of time data should be kept (retention).

Caution !

Some entities try to differentiate between data privacy, data security, and data protection. However, there are no clear and agreed-upon definitions for these terms, and they often are contradictory. Users should be cautioned about using these terms in a rigid fashion.

Apply Risk Management Principles

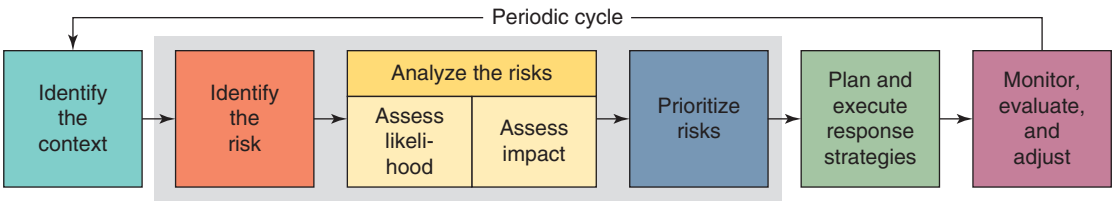
Another nontechnical means of protecting sensitive data is to apply **risk management principles** toward the protection of sensitive data. Organizations must determine how realistic is the chance that a given threat will compromise an asset, called the likelihood of occurrence. This is stated in terms of risk. At a basic level, risk is defined as a situation that involves exposure

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

to some type of danger. At a more advanced level, it is described as a function of threats, consequences of those threats, and the resulting vulnerabilities.

It is important to periodically review risks as new assets are added and new threats are identified. Figure 12-3 illustrates this risk review cycle.

Figure 12-3 Risk review cycle



One of the most critical steps in the risk review cycle is to determine the appropriate response to each risk. The goal of this step is to identify ways to keep the risk aligned with the risk appetite (tolerance) in a way that is as cost-effective as possible. Is the exposure associated with each risk within acceptable levels based on the potential consequences? If not, what cost-effective risk response options can be chosen to achieve the determined objectives?

Caution

It is important to remember that these responses in themselves may introduce new risks. For example, adding multifactor authentication (MFA) to an identity and access management (IAM) system may reduce an access control risk. However, it may also introduce a new risk of decreased productivity when users have difficulty using the new technology and a higher-than-normal number of calls to the help desk that can be manipulated through social engineering.

There are four different strategies for dealing with cybersecurity risks. These strategies are summarized in Table 12-4.

Table 12-4 Risk strategies

Strategy	Explanation
Accept	The risk is accepted within the levels of risk tolerance. No further response is necessary except for monitoring.
Transfer	For risks that fall outside of tolerance levels, they can be reduced to an acceptable level by sharing a portion of the consequences with another party such as a cybersecurity insurance company. However, while some consequences may be transferrable (like financial loss), there are often other consequences that cannot be transferred (such as the loss of customer trust).
Mitigate	Mitigation involves applying actions through security controls that reduce the threats, vulnerabilities, and impacts of a risk to an acceptable level. Responses may include those that can help prevent a loss by reducing the probability of occurrence or that limit a loss by decreasing the amount of damage and liability.
Avoid	This involves applying the appropriate response so that the risk does not occur and is considered the best option if there is no cost-effective method for reducing the cybersecurity risk to an acceptable level. However, the cost of the lost opportunity should also be considered.

Implement Data Retention Practices

Another nontechnical control for protecting data is not to keep the data any longer than is necessary. Purging unnecessary data eliminates the risk of a threat actor accessing that data. Data retention involves determining how long data must be kept. Many regulatory bodies set specifications for the length of time that data should be retained (retention standards).

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Most organizations address data retention through an internal data retention policy that outlines how to maintain information for a predetermined length of time. Different types of data may require different lengths of retention. In addition to describing how long various types of information must be maintained in the user's possession, retention policies usually describe the procedures for archiving the information and special mechanisms for handling the information when under litigation.

Basic principles for data retention include:

- Do not keep personal data for longer than needed. Personal data may be retained after the need has expired only if it is kept for public interest archiving, scientific or historical research, or statistical purposes.
- Organizations must be able to justify how long they keep personal data. Although this will depend on the purposes for holding the data, a solid reason must be established.
- A data retention policy setting standard retention periods must be in place.
- It is important to periodically review the data being held and erase or tokenize it when it is no longer needed.
- Any challenges that arise in the retention of data should be thoughtfully considered and not immediately dismissed.

Limit Data Collection

There are also restrictions that should be followed regarding the collection and usage of data. These include:

- **Data minimization.** Data minimization limits the collection of personal information to that which is directly relevant and necessary to accomplish a specific task. In other words, the collection of privacy data should be adequate, relevant, and not excessive in relation to the designated purpose. Organizations should periodically review their privacy data collection to ensure that it is following the principle of data minimization.
- **Purpose limitation.** Purpose limitation is a principle that data collected for one specified purpose should not be used for a new or incompatible purpose. For example, collecting user Social Security numbers for the purpose of filing insurance claims is a justifiable action. However, using all or part of the Social Security number as a unique identifier should be prohibited.

Note 15

Under the EU General Data Protection Regulation (GDPR), purpose limitation is a requirement that personal data be collected for specified, explicit, and legitimate purposes and not be processed (used) further in a manner incompatible with those purposes. The only exceptions for additional usage are if the person consents to the new usage, if the usage is on the basis of the EU or an EU member-state law, or if usage is for public interest purposes.

Two Rights & A Wrong

1. There are two categories of controls that should be used by organizations to protect both sensitive user data as well as important corporate data: technical controls and nontechnical controls.
2. DLP is a system of security tools used to recognize and identify data that is critical to the organization and ensure it is protected.
3. Data masking obfuscates sensitive data elements into a random string of characters and then the original sensitive data element and the corresponding string are stored in a database.

See the answers at the end of the chapter.

Using Data for Cybersecurity

The proper usage of data in cybersecurity can significantly enhance protection. Using data for cybersecurity can be divided into using data analytics and using artificial intelligence.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Data Analytics

Using data analytics for cybersecurity involves first knowing what data analytics is and then how it can be applied to the field of cybersecurity.

What is Data Analytics?

Data analytics is a process that examines large datasets in order to draw conclusions about the information they contain. It involves using techniques and tools to identify patterns and trends in the data, which can create insights for informed decision making.

For example, an online retailer may collect historical data on customer behavior, product searches, purchase histories, and so on. In applying "data-mining" techniques, data analysts use tools like the programming language R or Python to sift through the data to identify patterns and trends, such as looking for the most popular search term over a given period. This information can then help prepare for a surge in future orders by increasing the inventory of that product.

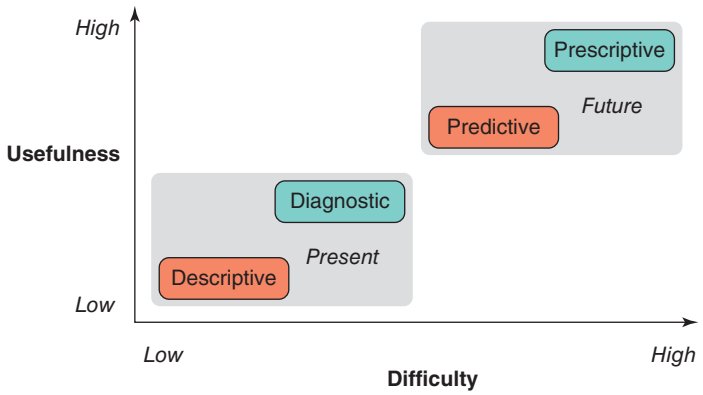
Data analytics relies on data analysts to manually create algorithms designed to learn patterns by testing assumptions based on historical data. The results can provide insights that can then be used to anticipate future events.

Data analytics can typically perform four types of analysis:

- **Descriptive**: What is happening now?
- **Diagnostic**: Why is this happening?
- **Predictive**: What is likely to happen soon?
- **Prescriptive**: What can be done about it?

These four types of analysis, their difficulty level and usefulness, and how they relate to the present and future are illustrated in Figure 12-4.

Figure 12-4 Types of data analysis



One of the most critical features of data analytics is that it is not limited to just observing what is presently happening (descriptive) and why it is happening (diagnostic). It can also be used to look ahead as to what will likely happen in the future (predictive) and prepare for it (prescriptive).

Data Analytics and Cybersecurity

Many users are surprised to learn that data analytics has been utilized for many years. For example, insurers have been performing deep levels of predictive data analytics for over two decades. In recent years, users have been exposed to data analytics through advertising. While millions of users are convinced that their smartphones are listening into their conversations and then serving up ads based on these conversations, in reality the advertisements are the result of predictive data analytics.

Note 16

Insurers must be able to predict the likelihood of future events to accurately set premium rates. When insurers cannot quantify a future risk, they charge higher premiums or decline to cover it. Today climate change is a major unknown future variable that insurers wrestle with.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Today, data analytics is used in a broad range of areas beyond insurance and advertising; data analytics is used in sales, marketing, human resources, supply-chain operations, and many other areas. In fact, over 90 different job profiles—many of which are outside IT—are recognized today as utilizing data analytics.

Data analytics has likewise been used for many years as a tool in cybersecurity. Cybersecurity data analytics is a proactive approach to cybersecurity that uses data collection, aggregation, and analysis capabilities to perform functions that include detecting, analyzing, and mitigating cyberthreats. With the ability to detect threats at early stages, security professionals can stop them before they infiltrate the network infrastructure and compromise valuable data and assets.

Data for cybersecurity is typically gathered from different sources, including:

- Business applications
- Endpoint detection and response (EDR)
- User behavior analysis (UBA)
- External threat intelligence
- Firewalls
- OS event logs
- Network appliances
- Anti-malware scanners

By combining and correlating this data, organizations create one primary dataset to use. This allows security professionals to apply algorithms and create rapid searches to identify early indicators of attack (IOA). These IOA can then preemptively identify and address security threats and vulnerabilities before an attack occurs.

Artificial Intelligence (AI)

One of the most talked-about topics in recent memory is artificial intelligence. It is important to understand the definition of artificial intelligence and its history, how it is used in cybersecurity, and its limitations and the risks. Threat actors can also leverage artificial intelligence.

Defining AI

A *buzzword* is defined as a term that has quickly spread beyond its original field so that those outside use the word imprecisely and pretentiously. IT has had its fair share of buzzwords, such as *cloud*, *Internet of Things*, and *virus*, to name a few. A current buzzword is *artificial intelligence*. This term has quickly become fashionable in popular culture; however, few users can define exactly what it is.

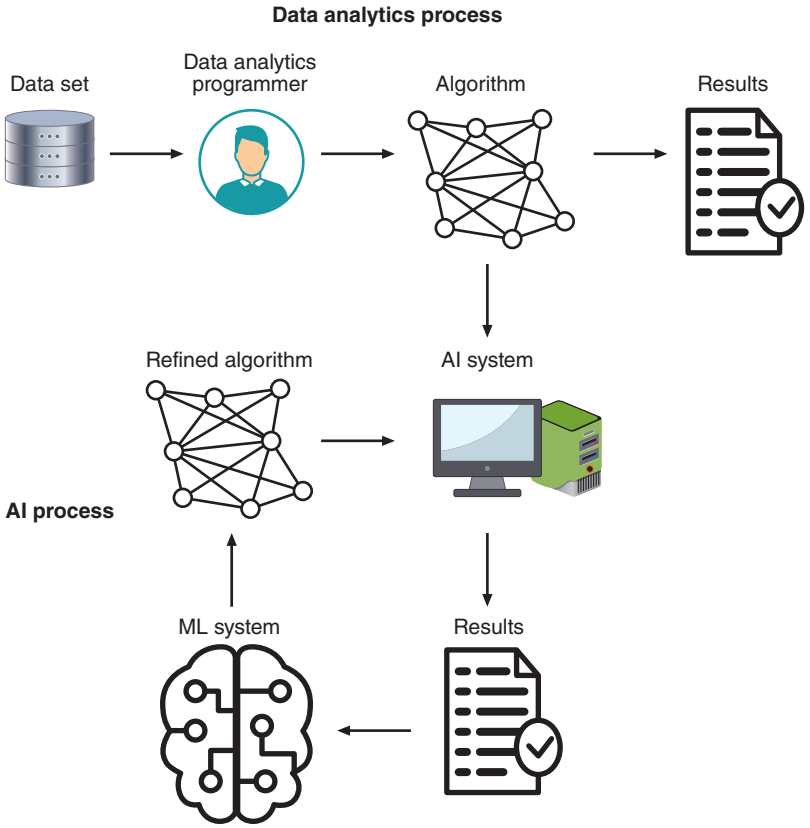
When defining AI, it is important to understand that it is not a term that is used in isolation; rather, it is directly related to other similar (although sometimes equally confusing) terminology. The best way to define AI is to see it in the context of these other terminologies:

- **Data analytics.** Data analytics is a manual process that examines large datasets in order to draw conclusions about the information they contain. Researchers manually create algorithms designed to query data and test assumptions, looking for patterns and correlations from historical data.
- **Artificial intelligence (AI).** A subset of data analytics is artificial intelligence. While AI involves data analytics, AI is autonomous: it works on its own without immediate or continual human assistance. Using data analytics, users create algorithms designed to learn patterns and correlations from data. AI can then use these algorithms to create its own additional predictive models—but by itself and without human intervention. AI systems also get "smarter" as they analyze more data, and thus they become increasingly capable. In short, AI refers to technologies that can act by themselves: they are "artificially" intelligent.
- **Machine learning (ML).** Machine learning (ML) is a subset of AI. It uses statistical techniques to give computer systems the ability to "learn" or progressively improve their performance using data rather than being explicitly programmed by a human. An ML system can create a refined algorithm for the next iteration. ML works best when aimed at a specific task rather than a wide-ranging mission.

The relationships between data analytics, AI, and ML are illustrated in Figure 12-5.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Figure 12-5 Data analytics, AI, and ML relationship



Note 17

Two other related systems besides AI are expert systems and neural networks. Expert systems are programs designed to solve problems within specialized domains while neural networks use a biologically inspired programming paradigm that enables a computer to learn from observational data.

History of AI

The birth of AI can be traced all the way back to the beginning of digital computers. Shortly after their development in the 1940s, scientists, mathematicians, and philosophers began talking about machines that could "think" and act on their own.

Renowned British mathematician Alan Turing explored the mathematical possibility of AI, suggesting that because humans use available information as well as reason in order to solve problems and make decisions, why can't machines do the same? This became the framework of his seminal 1950 paper, "Computing Machinery and Intelligence," in which he discussed how to build intelligent machines and then test their intelligence through the famous "Turing Test."

To the general public, however, AI exploded onto the scene with the release of ChatGPT in November 2022. ChatGPT is an AI chatbot built on a large language model (LLM) and trained on vast amounts of data to produce human-like content. Known as "generative AI," it can be used to create new content like text, images, music, audio, and videos. The most common way to train a generative AI model is to use "supervised learning" in which the model is given a set of human-created content. It then learns to generate content that is similar to the human-created content. In short, generative AI is trained by using an ML model to learn the patterns and relationships in a dataset of human-created content and then uses the learned patterns to generate new content.

Since the introduction of ChatGPT, a virtual "arms race" has ensued as developers have tried to outdo one another by incorporating AI into their products. Microsoft released an AI-powered version of its Bing search engine in early 2023, and

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Google immediately followed with Google Bard (now known as Gemini), described as "your creative and helpful collaborator, here to supercharge your imagination, boost your productivity, and bring your ideas to life." Microsoft then announced a new multibillion-dollar investment in ChatGPT maker Open AI.

Microsoft infused its popular workplace software Microsoft 365 with the technology behind ChatGPT; it is called Microsoft 365 Copilot. Through natural-language input, users can generate documents, presentations, and original text. For example, a Word user can highlight a paragraph and the AI will offer different options for a rewritten version of it. An entire PowerPoint presentation, complete with text and images, can automatically be created based on the text from a document, and the email client Outlook can automatically reply to emails in depth using the same "voice" of the email recipient.

Note 18

To handle the requirements of AI, central processing unit (CPU) chips are now available that have a neural processing unit (NPU) included. Much like graphics processing units (GPUs) that are specifically designed for rendering images and graphics on a screen, NPUs handle workloads that CPUs cannot perform efficiently, such as AI and ML tasks.

Using AI in Cybersecurity

Organizations face many challenges relating to cybersecurity, such as:

- Hundreds, thousands, or hundreds of thousands of endpoint devices per organization
- Large numbers of daily vulnerabilities including unknown zero-day vulnerabilities
- Massive amounts of security-related data that is generated each minute
- A serious shortage of trained security personnel

AI is ideally suited to address many of these challenges. AI technologies currently exist to properly train a self-learning AI system to gather data continuously and independently from millions—or even billions—of data points that can be immediately analyzed to identify patterns of an attack. AI technologies can search large volumes of alerts and data concerning cyber incidents with a speed and degree of accuracy that users cannot match. It can also automate the detection of events that normally require human analysis, reducing the number of "mundane" tasks security personnel must perform. AI can even detect nuanced attacks, enhance decision making during threat hunting, uncover previously undetectable tampering in devices, and quantify the risks associated with current IT system vulnerabilities.

AI can assist organizations *before* an attack (provide visibility and identify threats and anomalies early in the attack cycle, automatically investigate all anomalies, and identify high-risk attack behaviors), *during* an attack (force-multiply the security team with automated root-cause analysis to help them understand the full scope of the threat, automate incident workflow and remediation continuously, and collect ongoing evidence for forensics), and *after* an attack (continuously tune detection mechanisms based on lessons learned and adapt models to respond with increasing accuracy to future threats).

Note 19

Because AI can act on its own (unlike data analytics that relies on users to create the algorithms), it has the potential to become a "game-changer" in cyber defense.

Table 12-5 lists several of the specific tasks that AI cybersecurity can perform.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table 12-5 AI cybersecurity tasks

Task	Explanation
Analyze controls	AI systems can provide insight into current controls, their strengths and particularly weaknesses, and identify gaps in controls.
Reduce threat exposure	Because threat actors regularly change their tactics, AI-based security systems can provide up-to-date information of global and industry specific threats to help an organization make critical prioritization decisions based on what could be used and what is likely to be used in an attack.
Conduct asset inventory	AI systems can help organizations gain a more accurate inventory of all devices, users, and applications with any access to information systems and also provide assistance in categorization and the measurement of business criticality.
Perform breach risk prediction	Accounting for IT asset inventory, threat exposure, and controls effectiveness, AI-based systems can predict how and where an organization is most likely to be breached so that organizations can plan for resource and tool allocation toward areas of weakness while configuring and enhancing existing controls.
Manage incident response	When a security incident occurs, AI systems can provide an improved context of the attack to help prioritize and quickly respond to security alerts.
Provide descriptive explanations	Because securing "buy-in" from stakeholders across the organization is important for information security, AI systems can help provide understanding of the impact of various security systems and reporting to end users, security operations, chief information security officers, auditors, CIOs, CEOs, and boards of director.

Note 20

AI information security tools based on ChatGPT started appearing soon after the chatbot's release. BurpGPT is an AI vulnerability scanner that "leverages the power of AI to detect security vulnerabilities that traditional scanners might miss." It offers customizable prompts that enable tailored web traffic analysis to meet the specific needs of each user. PentestGPT is a ChatGPT-based penetration testing tool.

AI Concerns and Risks

However, there are concerns about AI and cybersecurity in its current form. Some chief information security officers (CISOs) say that they see the potential of AI but are unconvinced that in its current form AI provides significant benefits today for security operations centers (SOCs). They note that ML technology has already been in place for several years performing data analytics functions. Other CISOs say that due to the risk of inaccurate results from generative AI tools in their current form, generative AI cannot be used without human supervision. That is, generative AI has not reached the "leap of faith" moment yet where companies could rely on it without employees overseeing the outcome. Because of these concerns, some organizations use it only to complement what is already known.

The result is that different organizations have adapted AI at different levels. While virtually all CISOs say that AI holds great promise in cybersecurity, some say that there needs to be more maturation in AI for it to be truly impactful and even revolutionary.

Although the use of AI in cybersecurity is important and growing, there are associated risks. These include:

- AI needs huge volumes of high-quality data to function accurately; however, many organizations do not have enough, or good enough, data.
- AI tends to generate too many false positives.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- It can be hard to "tune" an AI system for the specific needs of individual customers, especially smaller organizations without extensive data.
- There is a lack of transparency in how the AI system makes decisions, so this can be a challenge for the SOC that needs to understand these decisions in order to make their own subsequent choices.
- The algorithmic models can degrade over time if they are not properly maintained by data analytics experts.

Adversarial AI

The risks of AI in cybersecurity are not limited to SOC operations. Threat actors themselves can attack AI systems and take advantage of AI. This is called adversarial AI and includes the following:

- **Compromise the algorithms.** Just as all hardware and software is subject to being infiltrated by threat actors, AI-powered security applications and their devices likewise have vulnerabilities. These could be attacked, compromised, and then the algorithms altered by threat actors to ignore attacks, much like a rootkit can instruct an OS to ignore malicious actions.
- **Taint ML training data.** Attackers can attempt to alter the training data that is used by ML in order to produce false negatives to cloak themselves.
- **Circumvent defenses.** Threat actors themselves can turn to using AI for attacks in order to circumvent defenses. Attackers can use AI to break through defenses and develop mutating malware that changes its structure to avoid detection.
- **Generate attacks.** Threat actors have already started using AI to create more realistic phishing and social engineering attacks, making them more effective, efficient, and harder to detect. AI will make cyberattacks more impactful because threat actors can analyze exfiltrated data faster and more effectively and then use it to train their own AI models to create more focused attacks.

Although all types of threat actors have started using AI, how they use it varies. Table 12-6 outlines projections of how different threat actors will likely use AI in the near future and the level of increase in the sophistication of attacks that AI will provide over current levels, organized by types of attacks.

Note 21

The levels of increase in Table 12-6 are low (1), moderate (2), significant (3), and high (4).

Table 12-6 Threat actor use of AI

	Nation-state actors	Organized crime and other threat actors	Script kiddies
Use of AI	High (4)	High (4)	Moderate (2)
Reconnaissance	Moderate (2)	Moderate (2)	Significant (3)
Social engineering, phishing, password attacks	Significant (3)	Significant (3)	High (4)
Using tools to generate malware or exploits	Significant (3)	Low (1)	Moderate (2)
Lateral movement in network	Low (1)	Low (1)	None
Exfiltration of data	Significant (3)	Significant (3)	Significant (3)
Area of impact	Will use AI in advanced operations against networks and malware creation	Will use AI in reconnaissance, social engineering, and exfiltration and provide AI tools to novice cyber actors	Will increase volume of successful compromise of devices and accounts

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Two Rights & A Wrong

1. "Descriptive" data analytics asks the question, "Why is this happening?"
2. Data analytics has been used for many years as a tool in cybersecurity.
3. An AI cybersecurity task that it can perform is to reduce threat exposure.

See the answers at the end of the chapter.

Summary

- There are two types of data collections of user private data that occur. The first is an "overt and legitimate" gathering of this data by an organization. The second type of data collection is a "concealed and questionable" collection of user data. This collection is usually done in secret without the user's clear knowledge and express consent and is questionable because there is no clear business case for gathering it. Significant issues are raised with how data gathered through both types of data collection are used. One particular type of information that raises serious concerns regarding its collection is personally identifiable information (PII). This is data that could identify a specific individual. It includes the person's full name, Social Security number, driver's license number, bank account number, passport number, and similar information.
- There are different technical controls that can be applied for protecting data, both sensitive user data and important corporate data. One control is to prevent access to the data so that a threat actor cannot reach it. Encryption is the practice of transforming information so that it cannot be understood by unauthorized parties and thus is protected. It can provide a range of security protections, including confidentiality, integrity, authentication, nonrepudiation, and obfuscation. Another means of preventing access to data is to implement data loss prevention (DLP). DLP allows the owner of the data to impose restrictions on its use. DLP is a system of security tools that is used to recognize and identify data that is critical to the organization and ensure that it is protected. Whereas DLP restricts data based on the content of the data, another control technology can be used to restrict data based on the location of the user. This requires the user to be in a specific location to access the data. This is known as geographic access requirements (geofencing).
- Access control is granting or denying approval to use specific resources; it is limiting or controlling access to assets. While physical access control consists of fencing or hardware door locks, technical access control consists of technology restrictions that limit users on digital devices from accessing resources and data. A framework called an access control scheme is embedded in the software and hardware and a custodian/steward can use the appropriate scheme to configure the necessary level of control. The discretionary access control (DAC) scheme is one of the most common but also the least restrictive. The rule-based access control scheme is more robust and can dynamically assign roles to subjects based on a set of rules defined by a custodian. Each resource object contains a set of access properties based on the rules. An access control list (ACL) contains rules that administer the availability of digital assets by granting or denying access to the assets.
- Sometimes it is not possible to strictly prevent access to data. In cases where preventing access to data is not possible, it is then important to apply the control of limiting access to the data. For many years, protecting intellectual property (IP) has been attempted through digital rights management (DRM). DRM is a broad category of access control technologies that are designed to restrict the use and duplication of digital content across a wide range of devices. DRM is intended to grant control and protection over IP for the creators and content providers who own the digital media. Watermarking is also used in conjunction with DRM. A watermark is an invisible

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

and unique embedded piece of information that is added to the content so that any pirated content can be easily traced back to the offending user.

- Another technical control for protecting data is to hide the data so that it cannot be identified and used, called deidentification. Data masking involves creating a copy of the original data but makes unintelligible any sensitive elements such as a user's name or Social Security number. By replacing the actual information with fictitious information, testing can still be carried out without using sensitive data. Tokenization obfuscates sensitive data elements, such as an account number, into a random string of characters called a token. The original sensitive data element and the corresponding token are then stored in a database called a token vault so that if the actual data element is needed, it can be retrieved. Destroying data is the final technical control for protecting data. Because data itself is intangible, destroying data that is no longer needed involves destroying the media on which the data is stored.
- In addition to technical controls for protecting data, there are also nontechnical controls. Different legal regulations are in place to protect the privacy of user data, and following these regulations can be considered a nontechnical control. Violating these regulations may have significant legal implications. Another nontechnical means of protecting sensitive data is to apply risk management principles toward its protection. Organizations must determine how realistic is the chance that a given threat will compromise an asset, called the likelihood of occurrence. This is stated in terms of risk.
- Another nontechnical control for protecting data is to not keep the data any longer than is necessary. Purging unnecessary data eliminates the risk of a threat actor accessing it. Data retention involves determining how long data must be kept. Many regulatory bodies set specifications for the length of time that data should be retained (retention standards). There are also restrictions that should be followed regarding the collection and usage of data. Data minimization limits the collection of personal information to that which is directly relevant and necessary to accomplish a specific task. Purpose limitation is a principle that data collected for one specified purpose should not be used for a new or incompatible purpose.
- The proper usage of data in cybersecurity can significantly enhance protection. Data analytics is a process that examines large datasets in order to draw conclusions about the information they contain. It involves using techniques and tools to identify patterns and trends in the data, which can create insights for informed decision making. One of the most critical features of data analytics is that it is not limited to just observing what is presently happening (descriptive) and why it is happening (diagnostic). It can also be used to look ahead as to what will likely happen in the future (predictive) and prepare for it (prescriptive). Data analytics has been used for many years as a tool in cybersecurity. Cybersecurity data analytics is a proactive approach to cybersecurity that uses data collection, aggregation, and analysis capabilities to perform functions that include detecting, analyzing, and mitigating cyberthreats.
- A subset of data analytics is artificial intelligence (AI). While AI involves data analytics, it is autonomous: it works on its own without immediate or continual human assistance. Using data analytics, users create algorithms designed to learn patterns and correlations from data. AI can then use these algorithms to create its own additional predictive models—but by itself and without human intervention. AI is ideally suited to address many of the challenges of cybersecurity. AI technologies currently exist to properly train a self-learning AI system to gather data continuously and independently from millions or billions of data points that can be immediately analyzed to identify patterns of an attack. AI technologies can search large volumes of alerts and data concerning cyber incidents with a speed and a degree of accuracy that users cannot match. However, there are concerns about AI and cybersecurity in its current form. Some CISOs say that they see the potential of AI but are unconvinced that in its current form it provides significant benefits today. Although the use of AI in cybersecurity is important and growing, there are risks associated with using it in cybersecurity. Threat actors themselves can attack AI systems and take advantage of AI, called adversarial AI.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Key Terms

accept
avoid
data loss prevention (DLP)
mitigate
personally identifiable information (PII)
risk management principles
transfer

Review Questions

1. Which step in the risk review cycle has as its goal to keep the risk aligned with the risk appetite?
   a. Identify the context
   b. Identify the risk
   c. Determine the appropriate response
   d. Monitor and evaluate
2. Which risk strategy would utilize a cybersecurity insurance company?
   a. Accept
   b. Transfer
   c. Combat
   d. Prevent
3. Which risk strategy requires no additional response except for monitoring?
   a. Accept
   b. Enforce
   c. Mitigate
   d. Avoid
4. If a tester does not want the sensitive elements of the testing data to be exposed, what technology should be used?
   a. PII Hiding
   b. Tokening
   c. Masking
   d. Data Object Obfuscation (DOO)
5. Which access control scheme is the least restrictive?
   a. Role-based access control
   b. DAC
   c. Rule-based access control
   d. MAC
6. Which permissions are attached to an object?
   a. Object modifier
   b. ACL
   c. SXRE
   d. Entity attribute (EnATT)
7. Which mechanism will provide both filesystem security and network security?
   a. DBAs
   b. DAPs
   c. HAPs
   d. ACLs
8. What is another name for geographic access requirements?
   a. Geolocating
   b. Geofencing
   c. Geotagging
   d. Geoidentifying
9. Which of the following is NOT a protection provided by encryption?
   a. Confidentiality
   b. Nonrepudiation
   c. Accounting
   d. Integrity
10. Which of the following is used to protect IP?
    a. BLB
    b. DRM
    c. ARC
    d. XLS
11. Which of the following is NOT correct about watermarking?
    a. It is invisible.
    b. It is used in conjunction with DRM.
    c. It can be erased if the content is altered.
    d. It allows for unauthorized duplications to be traced back to the source.
12. Which of the following allows deidentified material to be retrieved as needed?
    a. Data masking
    b. Tokenization
    c. Element obfuscation
    d. Reordering

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

13. Which of the following is NOT covered by DRM?

    a. E-books
    b. PHI
    c. Music
    d. Computer games

14. Which of the following is NOT correct about legal regulations as they apply to protecting data?

    a. A fundamental EU principle of data protection is the right to be forgotten.
    b. National data protections that apply to a country or group of countries do not exist.
    c. To violate a regulation may have significant ramifications known as legal implications.
    d. Currently there are no global data protections.

15. Which of the following is NOT a type of analysis to be performed by data analytics?

    a. Predictive
    b. Diagnostic
    c. Distinctive
    d. Prescriptive

16. Which of the following is NOT a basic principle when considering the retention of data?

    a. Always retain data for six months after it is no longer used.
    b. Organizations must be able to justify their decisions.
    c. Periodic reviews of the data being held are necessary.
    d. A policy must be in place.

17. Which of the following is a principle that data collected for one specified purpose should not be used for a new purpose?

    a. Data amalgamation
    b. Purpose limitation
    c. Reuse restriction
    d. Data specificity

18. Which of the following is a subset of AI?

    a. RU
    b. Data analytics
    c. ML
    d. GPT

19. Which of the following is NOT a cybersecurity task that AI can perform?

    a. Perform breach risk prediction.
    b. Manage incident response.
    c. Reduce threat exposure.
    d. Implement controls.

20. Which of the following is NOT adversarial AI?

    a. Create algorithms.
    b. Taint training data.
    c. Generate attacks.
    d. Circumvent defenses.

Case Projects

Case Project 12-1: #TrendingCyber

Estimated Time: 15 minutes
Objective: Summarize your thoughts on the #TrendingCyber opener.
Description: Read again the opening #TrendingCyber in this chapter. Should car manufacturers make it plain what data is being collected in their cars? Should drivers and passengers be able to "opt out" of specific types of data collection? What restrictions should be placed on how this data is used? Write a one-page paper about this.

Case Project 12-2: Geofencing Examples

Estimated Time: 25 minutes
Objective: Summarize examples and use cases of geofencing.
Description: Use the Internet to research geographic access requirements (geofencing). Identify at least four examples of geofencing as it relates to cybersecurity. Then devise at least three geofencing implementations that would apply to your school or place of work. Write a one-page paper on your work.

Case Project 12-3: Digital Rights Management (DRM)

Estimated Time: 30 minutes
Objective: Identify different examples of DRM.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Description: Research the current state of DRM. Select one area (e-books, music, film, TV, or games) and investigate the technologies that are currently being used and what the projects are for future use. Are these adequate? How intrusive are they for users? Is there a balance that can be achieved? Or do you have an alternative recommendation that can protect the creator while still making the content available electronically? What do you think the future of DRM is? Why? Write a one-page paper on your findings.

Case Project 12-4: Should Governments Purchase Private User Data?

Estimated Time: 25 minutes
Objective: Summarize issues surrounding governments bypassing user protections.
Description: In countries like the U.S. that have laws in place to protect government agencies from accessing user private data, some government entities have bypassed this restriction by purchasing from third parties user data that has been collected. This allows these entities to acquire private data about users without being restricted. Both the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) have admitted to buying records from data brokers detailing which websites and apps American citizens use. Should this be permitted? Does the advantage of law enforcement being able to track citizens to identify terrorists or locate criminal suspects through this data outweigh personal data privacy protections? Should citizens sacrifice their private data for the greater protection of the nation? Write a one-page paper on this controversial issue.

Case Project 12-5: Healthcare Data Breaches

Estimated Time: 25 minutes
Objective: Research data breaches impacting healthcare organizations.
Description: Healthcare organizations continue to be one of the most targeted organizations by threat actors to exfiltrate data. In 2023, more than 540 organizations reported healthcare data breaches impacting upward of 112 million individuals. Research the latest attacks on healthcare. Why are they victims of these attacks? What can be done about these attacks? Write a one-page paper on your research.

Two Rights & A Wrong: Answers

Perils Against User Data

1. There are two types of data collection: overt/legitimate and concealed/questionable.
2. One concern regarding data collection is that the accuracy of the data cannot be verified.
3. PII includes biometric data, genetic information, sex, and political party affiliation.

Answer: The wrong statement is #3.
Explanation: Sensitive personal information (SPI), which is information that does not directly identify an individual but is related to an individual and communicates information that is private or could potentially harm an individual should it be made public, includes biometric data, genetic information, sex, political party affiliation, union membership, and so on.

Controls for Protecting Sensitive Data

1. There are two categories of controls that should be used by organizations to protect both sensitive user data as well as important corporate data: technical controls and non-technical controls.
2. DLP is a system of security tools used to recognize and identify data that is critical to the organization and ensure it is protected.
3. Data masking obfuscates sensitive data elements into a random string of characters and then the original sensitive data element and the corresponding string are stored in a database.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Answer: The wrong statement is #3.
Explanation: Tokenization obfuscates sensitive data elements into a random string of characters (token). The original sensitive data element and the corresponding token are then stored in a database called a token vault so that if the actual data element is needed, it can be retrieved.

Using Data for Cybersecurity

1. "Descriptive" data analytics asks the question, "Why is this happening?"
2. Data analytics has been used for many years as a tool in cybersecurity.
3. An AI cybersecurity task that it can perform is to reduce threat exposure.

Answer: The wrong statement is #1.
Explanation: "Diagnostic" data analytics asks the question, "Why is this happening?"

References

1. "The state of data loss prevention 2020: What you need to know," *Tessian*, May 28, 2020, accessed June 26, 2020, https://www.tessian.com/blog/the-state-of-data-loss-prevention-2020-what-you-need-to-know/.
2. Samuely, Alex, "Visa leverages geo-location to enhance travelers' card payment experiences," *Retail Dive*, accessed Feb. 20, 2021, https://www.retaildive.com/ex/mobilecommercedaily/visa-leverages-geo-targeting-to-enhance-travelers-card-payment-experiences.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Appendix A

Preparing for the CompTIA CySA+ CS0-003 Certification Exam

The CompTIA CySA+ CS0-003 certification exam contains two categories of questions. The first category is *knowledge-based* assessment questions (multiple choice, multiple answer, ranking and ordering, etc.). The second category is *performance-based questions (PBQs)* that are designed to assess the test taker's skills in working with different cybersecurity tools.

This appendix provides instruction and practice of both knowledge-based questions and PBQs as may be found on the CySA+ certification exam. For those who may not be taking the CySA+ certification exam, this appendix can help provide an assessment and a more detailed understanding of different cybersecurity tools and how they are used.

Knowledge-Based Assessment Questions

1. At the SOC, Bohdan is suddenly seeing a wide variety of very sophisticated attacks, many of which she has not seen before. As Bohdan continues to observe these attacks, she finds that, unlike other attacks, they do not diminish over time but instead they continue to be "ferocious" and seemingly unending. What type of threat is Bohdan likely witnessing?
   A. Zero-day
   B. APT
   C. Software supply chain
   D. Data poisoning
2. Renate is working as a freelance security consultant for a small rural hospital to help secure the database of employee information. This database contains employee names, ages, contact information, employment history, Social Security numbers, and bank account numbers for payroll direct deposit. What is the classification of this type of information?
   A. SPI
   B. PII
   C. PHI
   D. IPI
3. Which of the following TTPs describe "how" an attack occurs?
   A. Tactics
   B. Techniques
   C. Procedures
   D. Processes

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

4. Ilse is tracking a particularly persistent instance of malware on the corporate network that is attempting to take advantage of a vulnerability due to improper input validation. Her analysis so far indicates that this vulnerability would allow the threat actor to access a file that they have stored on a server different than the server running the PHP code. What type of vulnerability is this?
   A. LFI
   B. RFI
   C. IRI
   D. ISISA
5. Kaspar is examining a zero-day vulnerability that is being actively exploited. This vulnerability requires no user interaction (UI) or privilege escalation (PR) but has a significant impact to confidentiality (C) and integrity (I) but not to availability. Which of the following would be the most accurate CVSS for this threat?
   A. CVSS: 31/AV:A/AC:H/PR:N/UI:R/S:U/C:X/I:N/A:N
   B. CVSS: 31/AV:P/AC:M/S:U/C:N/A:N/X:CR
   C. CVSS: 31/AV:R/AC:X/PR:L/UI/D/S:X/C:H/I:K/A:W
   D. CVSS: 31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
6. List the order of the steps of the intelligence cycle.
   A. Analysis
   B. Collection
   C. Dissemination
   D. Feedback
   E. Requirements
7. Bente has been investigating how a malicious threat actor was able to exfiltrate PII from a web server to a C&C. Upon completing her analysis, she was asked by the CTO to recommend a tool to prevent the exposure of PII outside the organization. Which of the following tools would she recommend?
   A. MAPI
   B. DLP
   C. Trusted Boot
   D. INDS
8. The CISO called Anhelina to discuss a wave of new attacks that were occurring 15 days after a patch was released. Anhelina was asked to recommend the best protection for the organization. Which of the following would Anhelina recommend as the best protection?
   A. MTRT of 15 days
   B. MTTC of 2 days
   C. MTTR of 5 days
   D. MTXR of 5 days
9. The Help Desk has started receiving calls saying that the company's internal portal can be accessed only through HTTP while at other times it is only accessible through HTTPS. At the same time, the SOC has been made aware that several user accounts have been compromised. Which of the following is the most likely reason for these problems?
   A. The SSL certificate has expired and all traffic to Port 443 is now blocked.
   B. The portal is flooded by a DDoS attack and must reroute all user requests to Port 80.
   C. An error in the company's internal routers is the cause of the problem.
   D. An insider with internal access is forcing users to Port 80.
10. You have been asked to perform a vulnerability scan on a network. However, the CSO does not want additional network traffic to be sent across the network since it is already saturated. What type of scan will you perform?
    A. Active scan
    B. Passive scan

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

C. Token scan

D. Restricted scan

11. Aart has been asked to look into supplementing the threat feeds that the organization receives by adding third-party threat feeds to it. What activity is Aart performing?

A. Feed collection

B. Threat aggregation

C. Threat feed combination

D. Data enrichment

12. A vulnerability scan has returned the following results. What is the best explanation for this event?

Detailed Results

171.96.167.101 (Apache 2.4)

Windows Shares

Category: Windows

CVE ID:

Vendor Ref: Microsoft

Bugtraq ID: 0000000000

Service Modified: 2.24.2022

Enumeration Results:

print$ c:\windows\system32\spool\drivers

files c:\FileShare\Accounting

Temp c:\temp

A. Because there is no CVE, this can be considered as a false positive by the Apache software running on the Windows server.

B. The anti-malware software has a known vulnerability that must be resolved.

C. Connecting to the host using a null session allows the enumeration of the share names on the host.

D. The missing Bugtraq ID indicates a zero-day vulnerability.

13. You have been presented with the result of a vulnerability scan and asked to prioritize the list. Which of the following questions would you NOT consider in your analysis?

A. Is the vulnerability on a critical system that runs a core business process or is it on a remote device that is rarely used?

B. Is the data on the affected device sensitive or is it public?

C. Is the vulnerability a recent vulnerability or one that was identified in the past?

D. If the vulnerability led to a threat actor infiltrating the system, would they be able to pivot to more important systems or would they be isolated?

E. Can the vulnerability be exploited by an external threat actor or would exploitation require that the person be sitting at a computer in an executive's office?

F. Can the vulnerability be addressed in a reasonable amount of time or would it take several days or even a week to fix?

14. Oleksandra has been tasked by the new CISO to ensure that mission-critical services are available in the event of a cyber incident. Which plan will most likely ensure that?

A. BC

B. BIA

C. DR

D. AM

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

15. Consider the following email log. What indicates that a digital signature was not used to validate the content of the email message?

Received: from BYAPR15MB3462.namprd15.prod.outlook.com (2603:10b6:a03:112::10) by BN7PR15MB4081.namprd15.prod.outlook.com with HTTPS; Fri, 11 Dec 2020 12:42:27 +0000

Received: from BN6PR13CA0038.namprd13.prod.outlook.com (2603:10b6:404:13e::24) by BYAPR15MB3462.namprd15.prod.outlook.com (2603:10b6:a03:112::10) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3632.18; Fri, 11 Dec 2020 12:42:26 +0000

Received: from BN7NAM10FT025.eop-nam10.prod.protection.outlook.com (2603:10b6:404:13e:cafe::a9) by BN6PR13CA0038.outlook.office365.com (2603:10b6:404:13e::24) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.3654.9 via Frontend Transport; Fri, 11 Dec 2020 12:42:25 +0000

Authentication-Results: spf=softfail (sender IP is 161.6.94.39) smtp.mailfrom=potomac1050.mktomail.com; topperwkuedu94069.mail.onmicrosoft.com; dkim=fail (body hash did not verify) header.d=raritan.com; topperwkuedu94069.mail.onmicrosoft.com; dmarc=none action=none header.from=raritan.com;

Received-SPF: SoftFail (protection.outlook.com: domain of transitioning potomac1050.mktomail.com discourages use of 161.6.94.39 as permitted sender)

---

a. dkim=fail (body hash did not verify)
b. spf=softfail
c. dmarc=none
d. action=none header.from=raritan.com

Performance-Based Questions (PBQs)

The CompTIA CySA+ certification exam contains several performance-based questions (PBQs) that are designed to assess the test taker's skills in working with different cybersecurity tools. CompTIA explains its PBQs as follows:

> In addition to traditional multiple-choice questions, some CompTIA certification exams include performance-based questions (PBQs). PBQs test a candidate's ability to solve problems in a simulated environment. Please be aware that the environment is not a live lab, and therefore, it may have restricted system functionality. PBQs are often an approximation of a virtual environment, such as a firewall, network diagram, terminal window, or operating system (OS).

PBQs typically do not require the test taker to *perform* a specific task; rather, the test taker is asked to *decide* which tool would be best to use in a specific situation or to *analyze* the results of using a tool. For example, a sample PBQ may include the following:

> Several employees of Company X were victims of a recent phishing attack. Here are email log files, file server logins, and output from a SIEM. Indicate how many employees replied to the phishing email, the number of computers that were infected, and the type of malware that was distributed by the attack.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

To be prepared for PBQs, students must understand when different cybersecurity tools should be used and how to interpret the results. Students must also know how to compare different results from different sources in order to paint a more complete picture of a cybersecurity incident. This appendix covers some of the cybersecurity tools that relate to PBQs.

Ports

Modern computers run multiple applications simultaneously. In a Transmission Control Protocol/Internet Protocol (TCP/IP) client/server network, a server in particular runs different applications while receiving different data requests from multiple client computers. The server's response back to the hosts is combined (*multiplexed*) into a single signal sent across a shared medium. When the server's response is received by the client, it must then be determined which client application (*process*) should receive the data. This requires an additional addressing element besides the client's IP address to give a more specific "location" (the software application process) to be identified within that client. In TCP/IP, this Transport layer address is called a *port*.

Note 1

The term *port* has other definitions besides the software application process that should receive a response. For example, a physical outlet in a network device is also called a port. Generally, the context in which the term is used helps to distinguish between a hardware connection and a software application process.

Because TCP and User Datagram Protocol (UDP) port numbers are 16 bits, valid port numbers may have a value of 0 to 65535. It is necessary to manage the port number address space. The range of TCP and UDP port numbers is divided into three ranges:

- **Well-known (privileged) port numbers (0–1023).** These port numbers are reserved for only the most universal TCP/IP applications and are assigned only to protocols that have been or will be standardized. On most computers, only server processes run by system administrators or privileged users use well-known port numbers. These processes generally correspond to processes that implement key IP applications, such as web servers or FTP servers.

Note 2

Well-known port numbers are sometimes called system port numbers.

- **Registered (user) port numbers (1024–49151).** Many applications must use TCP/IP for data transmission, but these applications are not as universally used as others, so they do not require a well-known port number. However, to ensure that these different applications do not conflict with each other, the vast majority of port number ranges are registered port numbers. Anyone who creates a viable TCP/IP server application can request to reserve one of these port numbers; if approved, the port number will be registered and assigned to the application.

Note 3

Because any user can generally access registered port numbers, they are called user port numbers.

- **Private/dynamic port numbers (49152–65535).** Private port numbers can be used for any purpose. These numbers are appropriate for a private protocol that only a particular organization uses.

You should be familiar with the most commonly used ports and their corresponding applications, listed in Table A-1.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table A-1 Common ports and applications

Well-known (privileged) port numbers (0–1023)	
Port number	**Description**
20	FTP (Send file data)
21	FTP (Session info)
22	SSH, SFTP, SCP
23	Telnet
25	SMTP
49	TACACS+
53	UDP/TCP – DNS
67	UDP – DHCP and BOOTP
69	TFTP
80	HTTP
88	Kerberos
110	POP3
119	NNTP (Network News Transfer Protocol)
123	NTP (Network Time Protocol)
137, 138, 139	NetBIOS
143	IMAP
161	SNMP (Agents receive requests)
162	SNMP (Controller receives data)
389	LDAP (Lightweight Directory Access protocol)
443	HTTPS over TLS
445	SMB/SAMBA (Server Messaging Block)
465	SMTP over TLS
500	IKE (Internet Key Exchange)
636	LDAPS w/ TLS
990	FTPS

Registered (user) port numbers (1024–49151)	
Port number	**Description**
1433	SQL
1701	L2TP, L2F
1720	H.323
1723	PPTP
1812, 1813	RADIUS
2427	MGCP (Media Gateway Control Protocol)
3389	RDP
5004	RTP

(*continues*)

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table A-1 Common ports and applications (*Continued*)

Registered (user) port numbers (1024–49151)	
Port number	**Description**
5005	RTP (Default)
5060	SIP (Unencrypted)
5061	SIP w/TLS

Protocol IDs

The protocol ID is a number embedded into the header of a TCP/IP packet. It is used to identify a protocol that is not identified by a port number. Table A-2 lists the protocol ID numbers.

Table A-2 Protocol IDs

ID	Description
1	ICMP (Internet Control Message Protocol)
2	IGMP (Internet Group Management Protocol)
6	TCP (Transmission Control Protocol)
17	UDP (User Datagram Protocol)
50	IPsec ESP (Internet Protocol Security Encapsulating Security Payload)
51	IPsec AH (Internet Protocol Security Authentication Header)

Sandboxes

A sandbox is an isolated virtual machine (VM). Anything run within a sandbox will impact only the VM and not the underlying computer. Sandboxes are how antivirus software can be used with heuristic monitoring to spot the characteristics of a virus.

The Microsoft Windows Sandbox is part of the Windows 11 operating system and can help provide users a higher degree of security and flexibility. The Windows Sandbox is an isolated desktop VM in which you can install software without being concerned that it will affect your computer. Although other programs are available that perform a sandbox function, the Windows Sandbox has the advantage of being included as part of Windows, so nothing has to be downloaded and installed. It relies on the Microsoft hypervisor to run a separate kernel that isolates the Windows Sandbox from the host. This makes it more efficient because it can take advantage of the Windows integrated kernel scheduler, smart memory management, and a virtual GPU. Once you close the Windows Sandbox, nothing remains on your computer; when you launch the Windows Sandbox again, it starts as a clean image.

To enable the Windows Sandbox, follow these steps.

1. You must be running Windows 11 Professional, Enterprise, or Education (not Home) version. To determine which version you are running, click the **Start** button, click **Settings**, click **System**, and then click **About**.
2. Next, check to make sure your system has virtualization turned on. Right-click the taskbar at the bottom of the screen, select **Task Manager**, and then click the **Performance** tab. Under Virtualization, the Enabled option must be selected. If the option is disabled, you must reboot, enter your BIOS or UEFI, and turn on virtualization. Also note that with older BIOS setups, you may need to disable other settings, such as Hyper-threading.
3. Enable Windows Sandbox. In the Windows search box, enter **Windows Features** to launch Windows Features. Click the **Windows Sandbox** box to turn on the feature.
4. To launch Windows Sandbox, click the **Start** button, scroll down, and click **Windows Sandbox**.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A protected VM sandbox starts; it looks like another Windows instance. You can download a program through the Microsoft Edge application in Windows Sandbox. (Edge is included within Windows Sandbox along with a handful of other Windows applications, including access to OneDrive.) You can also copy an executable file from your normal Windows environment and then paste it into the Windows Sandbox desktop to launch it. When you are finished, close the Windows Sandbox and everything will be discarded.

Command-Line/IP Utilities

A security professional should be familiar with several command-line and IP utilities. Some of them are explained in this section.

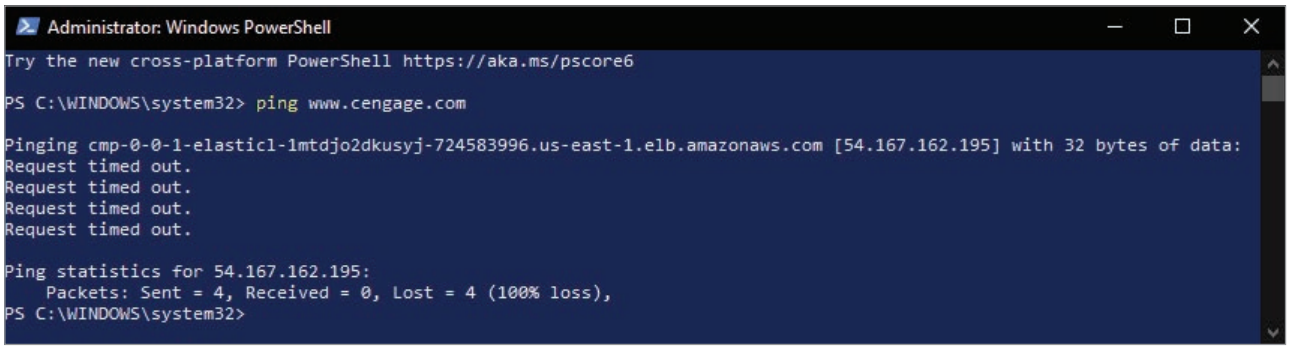
Note 4

To use command-line/IP utilities and perform the following activities, you must open a command prompt. On a Windows computer, right-click the Start button, and select Windows PowerShell (Admin).

Ping

Ping is a command-line tool that tests the ability of the source computer to reach a specified destination computer. At its basic level, the ping command is used to verify that a computer can communicate over a network with another computer or network device. The ping command sends Internet Control Message Protocol (ICMP) Echo Request messages; the number of responses returned and how long it takes for them to return are the two items of information the command provides. Figure A-1 shows the ping command being used to determine if www.cengage.com can be accessed.

Figure A-1 Pinging www.cengage.com



Source: Microsoft Corporation

Note 5

The word *ping* has found its way into our everyday vocabulary. For example, you can "ping" a friend (send her a message) to remind her of a meeting.

Several parameter options (called *switches*) can be used to fine-tune a command-line utility like ping. Table A-3 lists the most common switches for the ping command.

Note 6

A switch consists of a switch specifier, either a dash (-) or a forward slash (/), followed by the name of the switch, which is usually a single alphabetic letter.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table A-3 Common ping switches

Switch	Explanation
-t	Force the target to respond until you press Ctrl+C.
-a	Resolve the hostname of an IP address target.
-i TTL	Set the Time to Live (TTL) value up to 255.
-R	Trace the round-trip path.
-r count	Specify the number of hops between the computer and the target computer.
-6	Use IPv6 when specifying a hostname.
-n count	Specify the number of echo requests to send (the default is 4).
-l size	Set the length in bytes of the echo request packet (32 to 65527).

Ping Activities Miguel is investigating suspicious activity he has noted in a log file. He is using the ping command in his investigation.

1. The log file shows the IP address as 146.18.2.91. What ping command would he use to determine the hostname of that address?
2. The ping command displays the hostname as www.xresult.io. What ping command would Miguel use to determine if that host is active by using the hostname instead of the IP address?
3. What ping command would he use to send 11 packets of 1,000 bytes each to that host?
4. As Miguel reviews the results from the ping command, he notes that ping indicates the remote device is not responding. He opens a sandbox on his computer and launches a web browser within the sandbox. He enters the address of the remote device site and finds that it can be reached through the browser. Why does the ping command indicate that the remote device is not responding when it can be reached through a browser?

Netstat

The netstat (*net*work *stat*istics) command gives detailed information about current network connections. This information includes network protocol statistics and network connections for the TCP, network interfaces, and routing tables. Netstat commands can be tailored by using one or more optional parameters. Table A-4 lists some of the most commonly used netstat switches. In addition, all operating systems have their own unique netstat switches. For example, you can use the -o switch in Windows to include the process ID, and you can use the -t switch in Linux to display only TCP connections.

Table A-4 Common netstat switches

Switch	Description
-a	Show all active connections and the ports that the computer is listening on.
-e	Show Ethernet data such as number of bytes and packets sent and received.
-f	Display the fully qualified domain name (FQDN) when possible.
-g	Display multicast group membership data.
-n	Display active TCP connections. (Addresses and port numbers are displayed numerically.)
-o	Display the process identifier (PID) of the connection.
-r	Display the contents of a routing table.
-s	Display statistics by protocol.
-n	Redisplay data every *n* seconds until Ctrl+C is pressed.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Netstat Activities After conducting a network reconnaissance, Freja notices unusual activity on the network. She decides to use the netstat command to dig deeper into this activity.

1. What netstat command would Freja use to display all active TCP connections?
2. Freja notes more than one connection that raises her suspicion. What netstat command would she use to display the FQDN computer name of those connections along with the IP address?
3. What netstat command would Freja use to display all connections along with their corresponding protocols?
4. As Freja reviews the results, she is concerned that one specific connection may be exfiltrating data. What netstat command would she use to determine if malware or even normally legitimate software is exfiltrating information? (*Hint*: This command is also useful for determining which software is utilizing a large portion of existing bandwidth.)
5. Freja needs to determine which process is responsible for exfiltrating the data. What netstat command would she use?

Ipconfig

The ipconfig utility (*ifconfig* in Linux) displays network configuration information such as the IP address, network mask, and gateway for all physical and virtual network adapters. The typical ipconfig switches are listed in Table A-5.

Table A-5 Common ipconfig switches

Switch	Explanation
-all	Displays detailed configuration information about all network interfaces
-release [adapter]	Terminates the Dynamic Host Configuration Protocol (DHCP) lease on the specified adapter or on all interfaces
-renew [adapter]	Manually renews the DHCP lease on the specified adapter or on all interfaces
-displaydns	Displays the contents of the Domain Name Service (DNS) resolver cache
-flushdns	Clears the DNS resolver cache
-registerdns	Renews all DHCP leases
-showcallis	Displays DHCP class IDs associated with an adapter
-setclassic [adapter][classid]	Modifies the DHCP class ID for an adapter

Ipconfig Activities Adam is performing a basic forensics examination of a laptop computer. He is using the ipconfig command.

1. What ipconfig command would Adam use to display detailed configuration information on each of the laptop's network adapters?
2. Next, Adam needs to terminate any active TCP/IP connections on all network adapters. What ipconfig command would he use?
3. Now Adam needs to reestablish TCP/IP connections on all network adapters. What ipconfig command would he use?

Nslookup

Domain Name Service (DNS) is an essential element of TCP/IP networks. DNS allows hosts to be accessed using easily remembered names (www.cengage.com) rather than numerical IP addresses (99.15.116.1). Two different types of devices are involved in DNS: DNS name servers that store information about domains and DNS resolvers that query DNS servers to transform names into addresses.

A Windows DNS diagnostic utility is nslookup (for *n*ame *s*erver *lookup*). Although it can be used in interactive mode, the noninteractive version of nslookup is easier and is therefore used more often. Instead of typical switches, parameters are used with nslookup. The typical nslookup parameters are listed in Table A-6.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Table A-6 Common nslookup parameters

Parameter	Explanation
host	Look up the host using the default server.
host [server]	Look up the host using the specified server.
-server	Launch interactive mode using the server.
No parameter	Launch interactive mode using the default server.

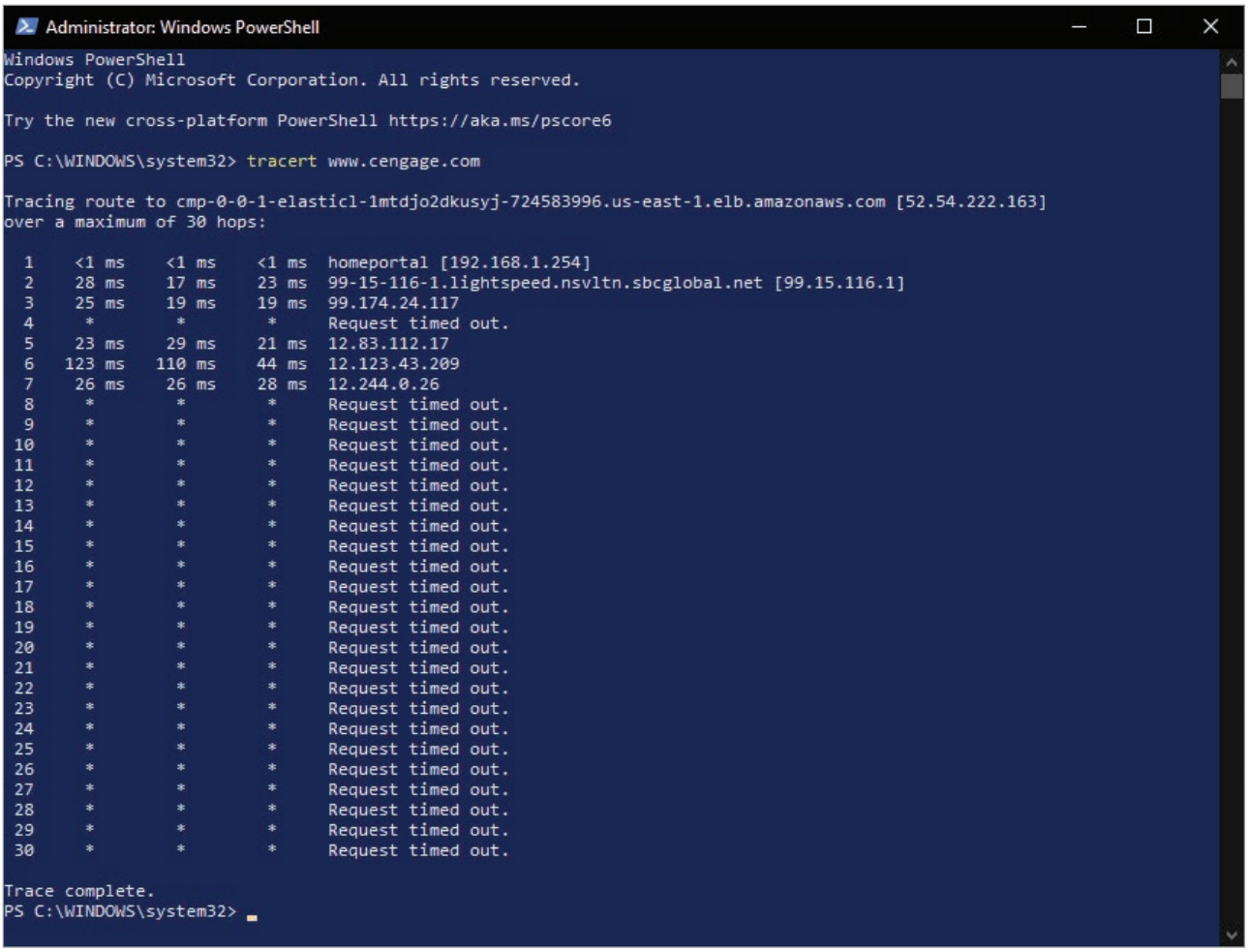
Nslookup Activities Paul suspects that a security alert he just received was caused by a misconfigured DNS server that may be compromised by threat actors. He is using the nslookup utility.

1. Paul has multiple nslookup commands to enter, so he decides to use interactive lookup mode. What command would Paul use to enter interactive lookup mode and then find the IP address of www.xdnslookup.io?
2. He now wants to switch DNS servers to a DNS open server at 208.67.222.222. What nslookup command would he use?
3. Paul also suspects that the mail server at www.transfermail.io is misconfigured, and he wants to use the nslookup command to find mail servers for that domain. What command would he use?

Tracert

Tracert (*traceroute* in Linux) is a command-line utility that shows details about the path a packet takes from a computer or device to a destination. Figure A-2 shows how to trace a packet from the computer to the Cengage website.

Figure A-2 Tracert for www.cengage.com



Source: Microsoft Corporation

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

A limited number of switches are available for the tracert command; several of these are listed in Table A-7.

Table A-7 Common tracert switches

Switch	Explanation
-d	Displays the route using numeric addresses and prevents tracert from resolving IP addresses to hostnames for a faster display
-h hops	Specifies the maximum number of hops while searching for the target (the default setting is 30)
-w milliseconds	Specifies a time in milliseconds to allow each reply (the default setting is 4000)
-4	Uses IPv4 only
-6	Uses IPv6 only
target	Specifies a destination (either an IP address or hostname)

Although the ping utility is helpful for determining whether devices can communicate with each other, it provides very little information about what is going on between those two devices. If ping shows either an inability to communicate or intermittent connectivity with high loss of transmitted data, it is important to know more about what is happening to the packets as they traverse the network. When these communication problems arise, it is useful to be able to trace the route taken by the packets between devices. Tracert is a special route-tracing utility for this function.

Note 7

Tracert is an abbreviation of the name *traceroute*, which is the UNIX/Linux name of the program. The shorter version of the name was necessitated by the old eight-character filename limit for Microsoft DOS program names and has never been updated.

There are several differences between the Windows tracert command and the Linux traceroute command. On modern Linux "distros," the traceroute utility uses UDP datagrams with a port number of 33434. The traceroute utility sets the Time to Live (TTL) field in the packets to a value too low to allow them to reach their destination, thus forcing each router in a route to report back to the sending device. Rather than UDP packets, tracert uses TCP Internet Control Message Protocol (ICMP) Echo requests (type 8), sometimes called "ping packets." It sends ICMP Echo messages with increasing TTL values and knows it has reached the final host when it receives a final Echo Reply message.

Note 8

A special ICMP traceroute message, which was intended to improve the efficiency of traceroute by eliminating the need to send several UDP messages for each route tracing, was developed in 1993. Yet, despite its technical advantages, it never became a formal Internet standard and is rarely used.

Tracert Activities

Victor is working with Hannah, who is in the "job shadowing" program at the local community college. Hannah is enrolled in her first computer information systems course at the college. She is watching Victor perform activities using the tracert command and asking questions.

1. Victor begins by tracing a packet from the computer to the community college site southwest.cc.cc.us. What tracert command would he use?
2. Hannah looks at the results from the tracert command and asks Victor why three times are listed for each hop. What would be Victor's explanation?
3. Hannah also notes that the tracert output displays "RTT," so she asks Victor what it means. What would be Victor's explanation?

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

4. The tracert output displays an asterisk (*) for RTT on several lines. How would Victor explain to Hannah what this means?
5. Hannah also asks, "What does 'Request timed out' mean?" How would Victor answer this question?

Consolidated Command-Line/IP Utility Activity

Brianna is performing network reconnaissance on a new branch location for her company. She wants to connect to the edge router of the new branch and determine which devices and networks are attached. She is only using command-line/IP utilities.

1. What command would Brianna use to verify the IP address configuration for the host device SALES?
2. Brianna discovered a new web server named 2XSERVER.IO. What command would Brianna use to determine the IP address for this server?
3. What command would she use to determine the path between SALES and 2XSERVER.IO?

Packet Analyzers

A packet analyzer is a very useful tool for environmental reconnaissance. It can be used to identify protocols that are running but are prohibited to identify attacks and to determine if unencrypted data is being transmitted.

Note 9

It is recommended that you download and install packet analyzers using the Windows Sandbox, unless you want to have them permanently installed on your computer.

Tcpdump

Tcpdump is a command-line packet analyzer. It displays TCP/IP packets and other packets being transmitted or received over a network. Tcpdump operates on UNIX and Linux operating systems, and various forks (derivatives of the original code) of it are available for Windows computers.

Note 10

WinDump was once a widely used Windows version of tcpdump; however, it has not been updated for several years. An alternative, tcpdump for Windows, is supported and maintained by Microolap (www.microolap.com/products/network/tcpdump/).

Several switches are available for tcpdump; they are listed in Table A-8. Note that these switches are case-sensitive.

Table A-8 Common tcpdump switches

Switch	Explanation
-c count	Capture a specified number of packets and then terminate.
-A	Display each packet in ASCII.
-D	List network interfaces.
-e	Display the link-level header.
-I interface	Listen on a specific network interface.
-v, -vv, -vvv	Display increasing verbose output.
-n	Do not translate hostnames or ports.
-c number	Specify the number of packets to capture.
-XX	Display packet data in hexadecimal and ASCII.

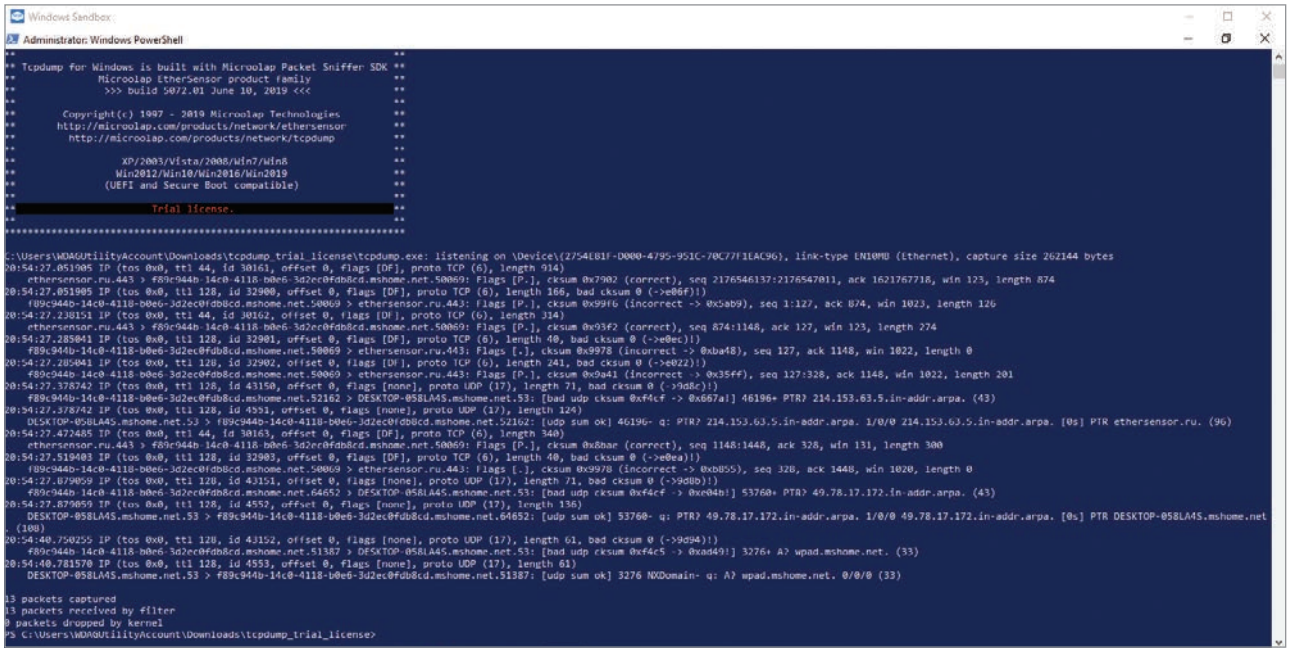
Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Note 11

A complete list of tcpdump switches is available at www.tcpdump.org/manpages/tcpdump.1.html.

The output from tcpdump can be voluminous and difficult to parse. Figure A-3 displays the output of only 13 packets.

Figure A-3 Tcpdump output



Source: Microsoft Corporation

Tcpdump Activities Cora suspects that unauthorized protocols are being run on the network. She needs to run tcpdump to analyze packets.

1. What tcpdump command would she use to list the available network interfaces?
2. After identifying the interface, Cora wants to capture HTTP packets with the highest level of detail. What tcpdump command would she use?
3. The results of Cora's command are shown in Figure A-4. Did she capture HTTP packets in order to examine them?

Figure A-4 Tcpdump attempt to capture HTTP traffic



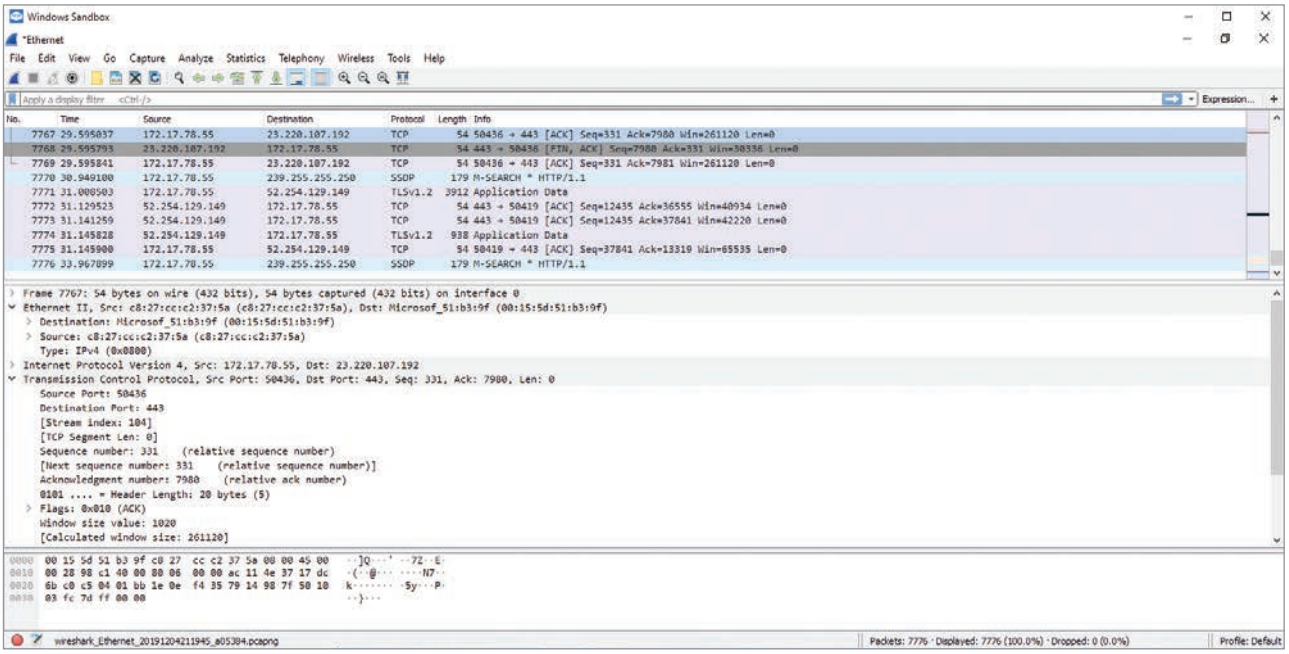
Source: Microsoft Corporation

Wireshark

Wireshark is a widely used network protocol analyzer. It enables a technician to perform deep inspection of hundreds of different protocols and provides decryption for a wide variety of protocols, such as IPsec, Kerberos, SSL/TLS, and WPA2. Figure A-5 shows the Wireshark main screen.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

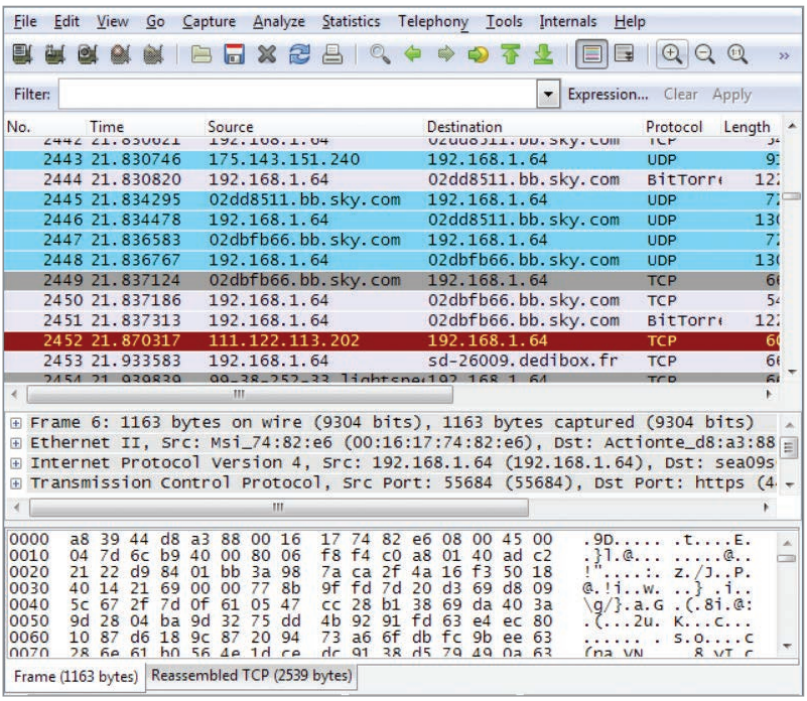
Figure A-5 Wireshark main screen



Source: Wireshark Foundation

Wireshark Activities Cora decides to use Wireshark to continue looking for unauthorized protocols that are being run on the network. Figure A-6 shows the Wireshark results.

Figure A-6 Wireshark results



Source: Wireshark Foundation

1. What unauthorized protocol is running?
2. What is the IP address of the host that is running this protocol?

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Appendix B

CompTIA CySA+ CS0-003 Certification Exam Objectives

Bloom's Taxonomy is an industry-standard classification system used to help identify the level of ability that learners need to demonstrate proficiency. It is often used to classify educational learning objectives into different levels of complexity. The Bloom's Taxonomy column in the following table reflects the level of coverage for the respective CS0-003 objective domains.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
1.0 Security Operations			
1.1 Explain the importance of system and network architecture concepts in security operations.			
• Log ingestion ◦ Time synchronization ◦ Logging levels	5	Tools for IOC Analysis	Understand
• Operating system (OS) concepts ◦ Windows Registry ◦ System hardening ◦ File structure ▪ Configuration file locations ◦ System processes ◦ Hardware architecture	1	Software	Apply
• Infrastructure concepts ◦ Serverless ◦ Virtualization ◦ Containerization			
• Network architecture ◦ On-premises ◦ Cloud ◦ Hybrid ◦ Network segmentation ◦ Zero trust ◦ Secure access secure edge (SASE) ◦ Software-defined networking (SDN)			
• Identity and access management ◦ Multifactor authentication (MFA) ◦ Single sign-on (SSO) ◦ Federation ◦ Privileged access management (PAM) ◦ Passwordless ◦ Cloud access security broker (CASB)	3	Identity and Access Management (IAM)	Apply
• Encryption ◦ Public key infrastructure (PKI) ◦ Secure sockets layer (SSL) inspection	3	Encryption	Understand
• Sensitive data protection ◦ Data loss prevention (DLP) ◦ Personally identifiable information (PII)	12	Perils Against User Data	Understand
◦ Cardholder data (CHD)	10	Reviewing Criticality of Data	Remember

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
1.2 Given a scenario, analyze indicators of potentially malicious activity.			
• Network related ◦ Bandwidth consumption ◦ Beaconing ◦ Irregular peer-to-peer communication ◦ Rogue devices on the network ◦ Scans/sweeps ◦ Unusual traffic spikes ◦ Activity on unexpected ports	4	Network IOA	Analyze
• Host related ◦ Processor consumption ◦ Memory consumption ◦ Drive capacity consumption ◦ Unauthorized software ◦ Malicious processes ◦ Unauthorized changes ◦ Unauthorized privileges ◦ Data exfiltration ◦ Abnormal OS process behavior ◦ File system changes or anomalies ◦ Registry changes or anomalies ◦ Unauthorized scheduled tasks		Endpoint IOA	Apply
• Application related ◦ Anomalous activity ◦ Introduction of new accounts ◦ Unexpected output ◦ Unexpected outbound communication ◦ Service interruption ◦ Application logs		Application IOA	Apply
• Other ◦ Social engineering attacks ◦ Obfuscated links	2	Types of Attacks	Understand

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.			
• Tools ◦ Packet capture ▪ Wireshark ▪ Tcpdump ◦ Log analysis/correlation ▪ Security information and event management (SIEM) ▪ Security orchestration, automation, and response (SOAR) ◦ Endpoint security ▪ Endpoint detection and response (EDR) ◦ Domain name service (DNS) and Internet Protocol (IP) reputation ▪ WHOIS ▪ AbuseIPDB ◦ File analysis ▪ Strings ▪ VirusTotal ◦ Sandboxing ▪ Joe Sandbox ▪ Cuckoo Sandbox	5	Tools for IOC Analysis	Understand
• Common techniques ◦ Pattern recognition ▪ Command and control ◦ Interpreting suspicious commands ◦ Email analysis ▪ Header ▪ Impersonation ▪ DomainKeys Identified Mail (DKIM) ▪ Domain-based Message Authentication, Reporting, and Conformance (DMARC) ▪ Sender Policy Framework (SPF) ▪ Embedded links ◦ File analysis ▪ Hashing ◦ User behavior analysis ▪ Abnormal account activity ▪ Impossible travel		Common Techniques for Investigating IOC	Apply
• Programming languages/scripting ◦ JavaScript Object Notation (JSON) ◦ Extensible Markup Language (XML) ◦ Python ◦ PowerShell ◦ Shell script ◦ Regular expressions	1	Software	Understand

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
1.4 Compare and contrast threat-intelligence and threat-hunting concepts.			
• Threat actors ◦ Advanced persistent threat (APT) ◦ Hacktivists ◦ Organized crime ◦ Nation-state ◦ Script kiddie ◦ Insider threat ▪ Intentional ▪ Unintentional ◦ Supply chain	2	Who Are the Threat Actors?	Understand
• Tactics, techniques, and procedures (TTP) ◦ Nessus ◦ OpenVAS ◦ Qualys	2	Threat Actor Actions	Apply
• Confidence levels ◦ Timeliness ◦ Relevancy ◦ Accuracy • Collection methods and sources ◦ Open source ▪ Social media ▪ Blogs/forums ▪ Government bulletins ▪ Computer emergency response team (CERT) ▪ Cybersecurity incident response team (CSIRT) ▪ Deep/dark web ◦ Closed source ▪ Paid feeds ▪ Information sharing organizations ▪ Internal sources • Threat intelligence sharing ◦ Incident response ◦ Vulnerability management ◦ Risk management ◦ Security engineering ◦ Detection and monitoring	6	Threat Intelligence	Understand
• Threat hunting ◦ Indicators of compromise (IoC) ▪ Collection ▪ Analysis ▪ Application ◦ Focus areas ▪ Configurations/misconfigurations ▪ Isolated networks ▪ Business-critical assets and processes ◦ Active defense ◦ Honeypot		Threat Hunting	Analyze

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
1.5 Explain the importance of efficiency and process improvement in security operations. • Standardize processes ◦ Identification of tasks suitable for automation ▪ Repeatable/do not require human interaction ◦ Team coordination to manage and facilitate automation • Streamline operations ◦ Automation and orchestration ▪ Security orchestration, automation, and response (SOAR) ◦ Orchestrating threat intelligence data ▪ Data enrichment ▪ Threat feed combination ◦ Minimize human engagement • Technology and tool integration ◦ Application programming interface (API) ◦ Webhooks ◦ Plugins • Single pane of glass	6	Improving Operation Processes	Apply
2.0 Vulnerability Management			
2.1 Given a scenario, implement vulnerability scanning methods and concepts. • Asset discovery ◦ Map scans ◦ Device fingerprinting • Special considerations ◦ Scheduling ◦ Operations ◦ Performance ◦ Sensitivity levels ◦ Segmentation ◦ Regulatory requirements • Internal vs. external scanning • Agent vs. agentless • Credentialed vs. non-credentialed • Passive vs. active • Static vs. dynamic ◦ Reverse engineering ◦ Fuzzing • Critical infrastructure ◦ Operational technology (OT) ◦ Industrial control systems (ICS) ◦ Supervisory control and data acquisition (SCADA) • Security baseline scanning • Industry frameworks ◦ Payment Card Industry Data Security Standard (PCI DSS) ◦ Center for Internet Security (CIS) benchmarks ◦ Open Web Application Security Project (OWASP) ◦ International Organization for Standardization (ISO) 27000 series	7 1 7	Vulnerability Scanning Methodologies Operational Technology Vulnerability Scanning Concepts	Apply Understand Understand

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
2.2 Given a scenario, analyze output from vulnerability assessment tools.			

• Tools
  ○ Network scanning and mapping
  ▪ Angry IP Scanner
  ▪ Maltego
	7	Vulnerability Assessment Tools	Understand

○ Web application scanners
  ▪ Burp Suite
  ▪ Zed Attack Proxy (ZAP)
  ▪ Arachni
  ▪ Nikto
	9	Identifying Vulnerabilities	Understand

○ Vulnerability scanners
  ▪ Nessus
  ▪ OpenVAS
○ Debuggers
  ▪ Immunity debugger
  ▪ GNU debugger (GDB)
	7	Vulnerability Assessment Tools	Understand

○ Multipurpose
  ▪ Nmap
  ▪ Metasploit framework (MSF)
  ▪ Recon-ng
	9	Identifying Vulnerabilities	Understand

○ Cloud infrastructure assessment tools
  ▪ Scout Suite
  ▪ Prowler
  ▪ Pacu			

2.3 Given a scenario, analyze data to prioritize vulnerabilities.			

• Common Vulnerability Scoring System (CVSS) interpretation
  ○ Attack vectors
  ○ Attack complexity
  ○ Privileges required
  ○ User interaction
  ○ Scope
  ○ Impact
  ▪ Confidentiality
  ▪ Integrity
  ▪ Availability
	8	Prioritizing Vulnerabilities	Analyze

• Validation
  ○ True/false positives
  ○ True/false negatives
	8	Analyzing Vulnerability Scans	Analyze

• Context awareness
  ○ Internal
  ○ External
  ○ Isolated
• Exploitability/weaponization
• Asset value
• Zero-day			

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy

2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.
• Cross-site scripting
  ○ Reflected
  ○ Persistent
• Overflow vulnerabilities
  ○ Buffer
  ○ Integer
  ○ Heap
  ○ Stack
• Data poisoning
• Broken access control
• Cryptographic failures
• Injection flaws
• Cross-site request forgery
• Directory traversal
• Insecure design
• Security misconfiguration
• End-of-life or outdated components
• Identification and authentication failures
• Server-side request forgery
• Remote code execution
• Privilege escalation
• Local file inclusion (LFI)/remote file inclusion (RFI)
	2	Types of Attacks	Apply

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
2.5 Explain concepts related to vulnerability response, handling, and management.			
• Compensating control • Control types ◦ Managerial ◦ Operational ◦ Technical ◦ Preventative ◦ Detective ◦ Responsive ◦ Corrective • Maintenance windows • Exceptions	8	Managing Vulnerabilities	Understand
• Risk management principles ◦ Accept ◦ Transfer ◦ Avoid ◦ Mitigate	12	Controls for Protecting Sensitive Data	Remember
• Policies, governance, and service-level objectives (SLOs) • Prioritization and escalation • Attack surface management ◦ Edge discovery ◦ Passive discovery ◦ Security controls testing ◦ Penetration testing and adversary emulation ◦ Bug bounty ◦ Attack surface reduction	8	Managing Vulnerabilities	Understand
• Secure coding best practices ◦ Input validation ◦ Output encoding ◦ Session management ◦ Authentication ◦ Data protection ◦ Parameterized queries • Secure software development life cycle (SDLC)	3	Secure Coding	Apply
• Threat modeling	8	Managing Vulnerabilities	Apply

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
3.0 Incident Response and Management			
3.1 Explain concepts related to attack methodology frameworks. • Cyber kill chains • Diamond Model of Intrusion Analysis • MITRE ATT&CK • Open Source Security Testing Methodology Manual (OSSTMM) • OWASP Testing Guide	10	Using Plans and Frameworks	Remember
3.2 Given a scenario, perform incident response activities. • Detection and analysis ◦ IoC ◦ Evidence acquisitions ▪ Chain of custody ▪ Validating data integrity ▪ Preservation ▪ Legal hold ◦ Data and log analysis	11	Detection and Analysis	Apply
• Containment, eradication, and recovery ◦ Scope ◦ Impact ◦ Isolation ◦ Remediation ◦ Re-imaging ◦ Compensating controls	11	Containment	Understand
3.3 Explain the preparation and post-incident activity phases of the incident management life cycle. • Preparation ◦ Incident response plan ◦ Tools ◦ Playbooks ◦ Tabletop ◦ Training ◦ Business continuity (BC)/disaster recovery (DR)	10	Charting an Incident Response Plan	Apply
• Post-incident activity ◦ Forensic analysis ◦ Root-cause analysis ◦ Lessons learned	11	Post-Incident Activities	Apply

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CySA+ Exam Objective Domain/Objectives	Chapter	Section	Bloom's Taxonomy
4.0 Reporting and Communication			

4.1 Explain the importance of vulnerability management reporting and communication.
• Vulnerability management reporting
  ○ Vulnerabilities
  ○ Affected hosts
  ○ Risk score
  ○ Mitigation
  ○ Recurrence
  ○ Prioritization
	9	Communicating and Reporting Vulnerabilities	Apply

• Compliance reports
• Action plans
  ○ Configuration management
  ○ Patching
  ○ Compensating controls
  ○ Awareness, education, and training
  ○ Changing business requirements
• Inhibitors to remediation
  ○ Memorandum of understanding (MOU)
  ○ Service-level agreement (SLA)
  ○ Organizational governance
  ○ Business process interruption
  ○ Degrading functionality
  ○ Legacy systems
  ○ Proprietary systems
• Metrics and key performance indicators (KPIs)
  ○ Trends
  ○ Top 10
  ○ Critical vulnerabilities and zero-days
  ○ SLOs
• Stakeholder identification and communication
	9	Responding to Vulnerabilities	Apply

4.2 Explain the importance of incident response reporting and communication. • Stakeholder identification and communication	10	Identifying Stakeholders	Remember
• Incident declaration and escalation	11	Containment	Understand

• Incident response reporting
  ○ Executive summary
  ○ Who, what, when, where, and why
  ○ Recommendations
  ○ Timeline
  ○ Impact
  ○ Scope
  ○ Evidence			

• Communications
  ○ Legal
  ○ Public relations
  ▪ Customer communication
  ▪ Media
  ○ Regulatory reporting
  ○ Law enforcement
	10	Identifying Stakeholders	Understand

• Root-cause analysis
• Lessons learned
• Metrics and KPIs
  ○ Mean time to detect
  ○ Mean time to respond
  ○ Mean time to remediate
  ○ Alert volume
	11	Post-Incident Activities	Analyze

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Glossary

A

abnormal account activity Uncommon behavior identified by comparing a baseline of normal actions against irregular or unusual behavior.

abnormal OS process behavior A technique used by threat actors to change a normal process into performing a malicious action.

AbuseIPDB A website that serves as a central repository to identify Internet Protocol (IP) addresses that have been reported as being associated with malicious activity online.

accept A risk strategy that accepts a risk within the levels of risk tolerance.

accuracy Information that is correct and free from errors.

action plan A framework comprised of all the steps of the tasks that are needed to meet an objective.

active defense Taking steps in anticipation of an attack.

active scanning Sending test traffic transmissions into the network to monitor the responses of the endpoints.

activity on an unexpected port Network traffic that could indicate that a threat actor is using a port and generating traffic that is normally not used for that purpose.

advanced persistent threat (APT) Attacks that use innovative attack tools to silently extract data over an extended period of time.

adversary emulation Penetration testers who act like threat actors to find vulnerabilities to exploit.

affected hosts Assets that should be protected.

agent A vulnerability scanning software package deployed to each device that needs to be scanned.

agentless A type of vulnerability scanning that has a server "reach out" to each asset rather than requiring agents to be installed on each device.

alert volume The number of notifications that a security operations center continually receives.

analysis Scrutinizing indicators of compromise (IOC) for evidence of an attack.

Angry IP scanner An Internet Protocol (IP) address and port scanner.

anomalous activity Unusual or strange behavior by an application.

application Using indicators of compromise (IOC) to generate a threat-hunting hypothesis.

application log A record of events, transactions, and errors that occur within a software application.

application programming interface (API) A link provided by an operating system, web browser, or other platform that allows a developer access to resources at a high level.

Arachni A web application vulnerability diagnostic tool that is a modular open-source tool.

asset discovery Identifying assets to determine what should be included in a vulnerability scan.

asset value The importance or worth of an asset to an organization.

attack complexity A metric that indicates conditions beyond the attacker's control that must exist in order to exploit the vulnerability.

attack methodology frameworks Models of the thinking and actions of threat actors.

attack surface management (ASM) The ongoing discovery, analysis, remediation, and monitoring of security vulnerabilities and potential attack vectors that make up an organization's total attack surface.

attack surface reduction Lessening the number of points that a threat actor can exploit.

attack vector An indicator of the level of access required for an attacker to exploit the vulnerability.

authentication The process of ensuring that the person or system desiring access to resources is authentic or "genuine" and not an imposter.

availability Information that is accessible as needed.

avoid A risk strategy that applies the appropriate response so that the risk does not occur.

awareness, education, and training A nontechnical control for reducing vulnerabilities.

B

bandwidth consumption An overall increase in the amount of bandwidth being utilized.

beaconing The process of infected devices attempting to contact the threat actor's external command and control (C&C) server.

blogs Posts and comments created by authors and organized into categories.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

broken access control A vulnerability that allows unauthorized users to access sensitive data or systems by circumventing security procedures.

buffer overflow attack An attack that occurs when a process attempts to store data in random access memory (RAM) beyond the boundaries of a fixed-length storage buffer.

bug bounty A program of large enterprises to pay security researchers who uncover security vulnerabilities in their products.

Burp Suite A web application vulnerability diagnostic tool that performs both a static and dynamic analysis.

business continuity (BC) plan A strategic document that provides alternative modes of operation for business activities.

business-critical assets Assets that are essential to the operation of an organization.

business process interruption The interruption of normal business functions.

C

cardholder data (CHD) Critical data to be protected by organizations that are involved with customer retail financial transactions.

Center for Internet Security (CIS) A center that has developed control and benchmark standards along with specialized technology tools.

chain of custody Documenting that evidence was always under strict control and no unauthorized person was given the opportunity to corrupt the evidence.

changing business requirements Adjustments in the attributes, capabilities, and characteristics of a business.

cloud access security broker (CASB) A set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure.

cloud computing An on-demand infrastructure to a shared pool of configurable computing resources that can be rapidly provisioned and released.

collection Gathering indicators of compromise (IOC) from different sources.

command and control (C&C) Online remote structure managed by attackers to send commands to infected devices.

Common Vulnerability Scoring System (CVSS) A numeric score assigned to a vulnerability based on a complex formula.

compensating control A control providing an alternative to normal controls that for some reason cannot be used.

compliance report A report to an external regulatory body.

Computer Emergency Readiness Team (CERT) A unit of the U.S. Department of Homeland Security responsible for analyzing and reducing cyber threats and vulnerabilities by disseminating cyber threat warning information.

confidence level Qualities of threat intelligence (TI) that determine how much trust should be placed in it.

confidentiality The disclosure of sensitive information to authorized and unauthorized users.

configuration file location The area where an operating system stores configuration files.

configuration management A process for maintaining computer systems, servers, applications, network devices, and other information technology (IT) components in a desired state.

configuration/misconfiguration An incorrect or "suboptimal" setting applied to hardware or software.

containerization A reduced instance of virtualization.

containment Keeping a cybersecurity incident under control by limiting its impact.

context awareness The use of supplemental information to improve security decisions at the time they are made.

control A safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of a technology system and its data.

corrective control A control intended to mitigate or lessen the damage caused by an incident.

credentialed scan A scan for which valid authentication credentials are supplied to the vulnerability scanner.

critical infrastructures Important operational technology (OT) systems that provide vital services to a wide range of users.

critical vulnerabilities Vulnerabilities that should be prioritized for immediate remediation.

cross-site request forgery (CSRF) An attack that takes advantage of an authentication token that a website sends to a user's web browser.

cross-site scripting (XSS) An attack in which threat actors take advantage of user input and display on a web server.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

cryptographic failure The improper implementation of cryptography that can severely weaken it.

Cuckoo Sandbox An open-source automated malware file analysis system.

customer communications Messages to customers that focus on providing clear and straightforward information that serves to allay fears.

Cyber Kill Chain™ A document that outlines the steps of an attack.

Cyber Security Incident Response Team (CSIRT) An organization that provides services regarding cybersecurity intelligence to any user, company, government agency, or organization.

D

data and log analysis Examining different log files to identify indicators of compromise.

data enrichment The enhancement of data for cybersecurity analysis.

data exfiltration Stealing data and transferring it to an external source.

data loss prevention (DLP) A system of security tools used to recognize and identify data that is critical to the organization and ensure it is protected.

data poisoning An attack that contaminates the data that is used in cybersecurity to identify an attack.

data protection Schemes for securing the integrity of any data that the application accesses.

debugger A tool for tracing the flow of a program and altering its execution.

deep/dark web Part of the world wide web that is the domain of threat actors.

degrading functionality Addressing a vulnerability that may change or even eliminate a function of an application for the sake of making it more secure.

detection and monitoring Uncovering and managing vulnerabilities.

detective control A control designed to identify any threat that has reached the system.

device fingerprinting Collecting information about a device's installed hardware and software configuration to create a unique identifier.

Diamond Model of Intrusion Analysis A framework for examining network intrusion events.

directory traversal An attack in which a threat actor takes advantage of a vulnerability to move from the root directory to other restricted directories.

disaster recovery (DR) plan A written document that details the process for restoring information technology (IT) resources following an event that causes a significant disruption in service.

DNS and IP reputation Identifying the legitimacy of a website through its Internet Protocol (IP) address or Domain Name System (DNS) information.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) A means for extending Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) by allowing the administrative owner of a domain to publish a policy in their DNS records to specify which mechanism (DKIM, SPF, or both) is used when sending email from that domain.

Domain Keys Identified Mail (DKIM) An authentication technique that validates the content of the email message itself.

drive capacity consumption The unexpected loss of available hard drive space as a result of malware.

dynamic analysis A run-time verification of software when all components are integrated and running.

E

edge discovery Efforts to identify edge devices so that they can be recognized and defended.

email analysis Analyzing email systems for indicators of compromise.

email header The part of the email that contains information about the sender, recipient, email's route through mail transfer agents, and various authentication details.

embedded links Hypertext links that are contained within email messages.

end-of-life component A feature that is no longer supported.

endpoint detection and response (EDR) Tools to aggregate data from multiple endpoint computers to a centralized database.

eradication The elimination of an infection.

escalate Moving the most critical vulnerabilities to the top of a prioritized list.

evidence acquisition Examining technology devices that may contain evidence.

exceptions Deviations from a policy of strictly pursuing all remediations based only on a high Common Vulnerability Scoring System (CVSS) score.

executive summary The first section of a report that provides a concise overview of the main content.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

exploitability/weaponization Vulnerabilities that are actively being exploited and capitalized on by threat actors.

eXtensible Markup Language (XML) One of the first common data exchange formats that uses markup symbols to define data.

external Context awareness information that comes from outside an organization.

external vulnerability scan A scan performed from the vantage point outside the network.

F

false negative The failure to raise an alarm when a vulnerability exists.

false positive An alarm that is inaccurately raised when no vulnerability exists.

federation The ability of systems to exchange information when those networks are owned by different organizations.

file analysis Looking for evidence of malware within a file.

file structure A storage format on a device.

file system change or anomaly A change to files by a threat actor.

focus area Areas of highest concern in threat hunting.

forensic analysis The retrieval of difficult-to-obtain data that may be hidden, altered, or deleted by a threat actor.

forums Topics and comments created by members organized into different subforums.

fuzzing Providing random input to a program to attempt to trigger exceptions.

G

GNU Debugger (GDB) A tool that can debug different programming languages.

governance The structures, systems, and practices an organization has in place to assign, oversee, and report.

government bulletin An official publication from the federal government.

H

hacktivists A group strongly motivated by philosophical or political beliefs or ideology for the sake of their principles.

hardware architecture The design and organization of the physical components that make up a computer system.

hashing The process of creating a digital fingerprint.

heap overflow A buffer overflow attack that occurs in the heap.

honeypot A computer located in an area with low security that serves as bait to threat actors to reveal their attack techniques.

hybrid A cloud computing environment that is a combination of public and private clouds.

I

identification and authentication failure Failing to confirm the requester's identity or genuineness.

identification of tasks suitable for automation Discovery of recurring manual activities that lend themselves to being replaced or supplemented by an automated process.

identity and access management (IAM) The technologies that provide control over user validation and the resources that may be accessed.

Immunity Debugger A tool used to analyze malware.

impact The significance of an incident measured in the magnitude of harm that is caused.

impersonation Pretending to be someone else in order to send emails that purport to come from that person.

implementation The process of applying patches.

impossible travel Detecting the presence of an imposter by a geographical distance impossible to travel within a specific time.

incident declaration and escalation An announcement to relevant parties and raising the elevation of importance regarding a cyber incident.

incident response Handling a cyberattack or data breach.

incident response plan A detailed document that clearly outlines the roles, responsibilities, and processes for responding to a cyber incident.

incident response tool A tool used by members of an incident response team.

indicators of compromise (IOC) The digital artifacts that serve as evidence of an attack.

industrial control system (ICS) A system that collects, monitors, and processes real-time data so that machines can directly control devices such as valves, pumps, and motors without the need for human intervention.

industry framework A set of designs for businesses in a specific industry based on consensus from industry representatives.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

information-sharing organization An organization that shares closed-source information.

injection flaw An attack that inserts vulnerabilities into random access memory (RAM).

input validation Ensuring that the data received is legitimate.

insecure design A broad category that includes different program weaknesses that are due to missing or ineffective control design.

insider threat Attacks that come from an enterprise's own employees, contractors, and business partners.

integer overflow An attack in which the attacker changes the value of a variable to something outside the range that the programmer had intended.

integrity Whether the protected information has been changed in any way.

intentional insider Insiders who steal or manipulate data from the position of having a trusted relationship with the organization.

internal Context awareness information that comes from within an organization.

internal source Threat intelligence (TI) data that is extracted from an organization's own security devices.

internal vulnerability scan A scan performed from a vantage point inside the internal network.

International Organization for Standardization (ISO) 27000 A compliance standard that provides an overview of information security management systems.

interpret suspicious commands Looking for evidence of operating system commands that a file initiates to determine if it performs a malicious activity.

introduction of new accounts An attempt to compromise user applications by creating a new account.

irregular peer-to-peer communication The unexpected and sporadic internal communication between infected peers on a network.

isolated Context awareness information that is not part of an organization.

isolated network A network that is used for supporting testing and other nonproduction functions.

isolation Permitting a compromised device to continue to function but directing all network communication to a sinkhole.

J

JavaScript object notation (JSON) A data exchange format that is concise and compact.

Joe Sandbox An advanced automated and deep malware analysis engine.

K

key performance indicator (KPI) A checklist designed to clearly articulate and provide insight into what an organization needs to measure.

L

law enforcement agency An entity that is authorized to prevent, detect, investigate, or prosecute criminal law violations.

legacy system An older system with specialized software that cannot be easily replaced.

legal The department that handles legal matters for ensuring compliance with laws and regulations.

legal hold A restriction that prevents data from being modified, deleted, erased, or otherwise destroyed.

lessons learned Evaluating a cyber incident so as to lessen the chance of a reoccurrence by taking corrective actions and documenting the event.

local file inclusion (LFI) A vulnerability that allows an attacker to point to a file that they have uploaded.

log ingestion The process of formatting and uploading log data from the different sources that generate log data to a central location for analysis.

logging level A means of classifying log entries in terms of urgency.

M

maintenance window A scheduled outage of services over a digital platform in order to implement planned changes, upgrades, or repairs.

malicious process An unauthorized process initiated by threat actors.

Maltego An open-source network mapping tool.

managerial control A control that uses administrative methods.

map scans The process of extracting data to create a picture of the endpoint and network.

mean time to remediate The average time for a response to a cyber incident to be finished.

media The industry that delivers news to the general public.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

memorandum of understanding (MOU) An agreement between two or more parties so that they can work together.

memory consumption An abnormal usage of random access memory (RAM) by a threat actor.

Metasploit framework (MSF) A flexible and modular penetration-testing platform.

metrics Cybersecurity data that an organization tracks.

minimize human engagement Reducing the work required of personnel to fight attacks by using automation.

mitigate A risk strategy that applies actions to reduce the threats, vulnerabilities, and impacts.

mitigation Efforts toward reducing the harm of a hazard.

MITRE ATT&CK A knowledge base of attacker techniques that have been broken down and contain classification in detail.

multifactor authentication (MFA) Using two (or more) forms of authentication credentials.

N

nation-state actor A state-sponsored attacker who launches cyberattacks against government foes.

Nessus One of the most popular and highly regarded infrastructure vulnerability scanning tools.

network segmentation Creating different security zones of different levels of access within a network for a higher level of security through network design.

Nikto A web application vulnerability diagnostic tool that is a command-line open-source tool.

nmap An open-source utility for network discovery and security auditing.

noncredentialed scan A scan for which no valid authentication credentials are supplied to the vulnerability scanner.

O

obfuscated link A deceptive URL that tricks the user into thinking it is a valid or secure link.

on-premises Computing resources located on the campus of an organization.

Open Source Foundation for Application Security (OWASP) Testing Guide A guide designed to help software developers and engineers test web applications to identify security issues.

open-source intelligence (OSINT) Threat intelligence (TI) that is freely available.

Open Source Security Testing Methodology Manual (OSSTMM) A peer-reviewed methodology for security testing.

Open Worldwide Application Security Project (OWASP) A nonprofit foundation that works to improve the security of software.

OpenVAS A full-featured vulnerability scanner.

operational control A control that is implemented and executed by people.

operational technology (OT) Using hardware and software to monitor and control physical processes and the devices connected to the infrastructure that support these processes.

operations Activities and tasks used to produce the goods and services of an organization.

orchestration The automation and combination of different individual cybersecurity tasks and processes.

organizational governance The system by which an organization makes and then implements decisions.

organized crime A close-knit group of highly centralized enterprises set up for the purpose of engaging in illegal activities.

outdated component An older feature that is considered no longer current.

output encoding Stripping anything other than text before it is displayed.

P

packet capture The process of grabbing packets as they travel through the network for analysis.

Pacu An exploitation framework for Amazon Web Services.

paid feeds Using organization professional external providers who can provide a broad range of data to reveal patterns and trends.

parameterized query Using predefined variables or prepared statements as placeholders for parameters.

passive discovery Scanning that operates continuously with no manual intervention required.

passive scanning Listening for normal network traffic to learn needed information.

passwordless Authentication systems that do not use passwords.

patch management Installing and managing software security updates in a timely and effective fashion.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

pattern recognition The ability to detect arrangements of characters or data that can yield information.

Payment Card Industry Data Security Standard (PCI DSS) A compliance standard to provide a minimum degree of security for handling customer card information.

penetration test A single event using a manual process to uncover vulnerabilities.

performance The ability of a scan to run faster.

persistent XSS A cross-site scripting attack in which a threat actor enters input into a blog post or forum that is stored to be used against subsequent users.

personally identifiable information (PII) Data that could identify a specific individual.

playbook A document that lists specific actions or a set of rules that describes steps to take in response to a security incident.

plugin A module update.

policy A formal statement that outlines specific requirements or rules that must be met based on a decision by a governing body.

post-incident activities The final activity phase of an incident response.

PowerShell A task automation and configuration management framework from Microsoft.

preservation of evidence Ensuring that important proof is not corrupted or destroyed.

preventive controls A control that attempts to prevent the threat from coming in and reaching contact with the vulnerability.

prioritize The process of determining which vulnerabilities need to be addressed.

priority systems Key critical devices.

privilege escalation An attempt by threat actors to escalate to more advanced resources that are normally protected from an application or user.

privileged access management (PAM) Strategies and technologies for exerting control over privileged accounts and the access and permissions for users, accounts, processes, and systems.

privileges required A description of the level of access privileges an attacker must have.

processor consumption A taxing of an endpoint processor by a threat actor.

Prowler A command-line tool for diagnosing vulnerabilities in services using the Amazon Web Services cloud.

public key infrastructure (PKI) The underlying infrastructure that serves as a key management system for controlling public keys, private keys, and digital certificates.

public relations Specialists who manage an organization's public image and reputation.

Python A popular programming and scripting language that can run on several different operating system platforms.

R

Recon-ng A full-featured web-based reconnaissance framework.

recurrence Vulnerabilities that continue to occur.

reflected XSS A cross-site scripting attack in which the input a user enters into a web application is then immediately displayed back to initiate the attack.

registry change or anomaly An unexpected modification or an abnormal registry setting made by threat actors.

regular expression (regex) A special string of text for describing a search pattern.

regulatory reporting Communication from an organization required by federal regulatory requirements if a specific cyber event occurs.

regulatory requirements The process of following specific actions mandated by an external regulatory body.

reimaging Applying a saved image to a sanitized hard drive.

relevancy Information that is applicable and helpful.

remediation Neutralizing or eliminating the vulnerability responsible for a cyber incident.

remote code execution (RCE) An attack in which a threat actor accesses a target device to make changes to it.

remote file inclusion (RFI) A vulnerability that allows an attacker to access a file stored on a different server other than the server running the code.

repeatable/do not require human interaction Activities that occur on a repetitive basis and can be performed independently of security personnel.

responsive control A control designed to launch remediations to counter adverse events.

reverse engineering Disassembling and analyzing a product.

risk management Controlling threats to assets.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

risk management principles A nontechnical means of protecting sensitive data by determining how realistic is the chance that a given threat will compromise an asset.

risk score Supplementing Common Vulnerability Scoring System scores with additional data to determine the impact of a vulnerability.

rogue devices on a network Locating unauthorized devices on a network infrastructure.

rollback Requiring the patches to be "backed out" so the systems can be restored to their original state.

root-cause analysis (RCA) A method of identifying and solving the underlying factors that contributed to a cybersecurity incident.

S

sandboxing Creating a fully protected environment for analyzing malicious files.

scans/sweeps Using ping sweeps and port scans to identify vulnerabilities.

scheduling The regular interval when vulnerability scans are conducted.

scope Characteristics that contribute to severity-level classifications; also, a metric that determines whether a vulnerability in one system or component can carry over to impact another system or component.

Scout Suite An open-source multicloud security-auditing tool.

script kiddies Unskilled attackers who want to perform attacks yet lack the technical knowledge to conduct these attacks.

Secure Access Service Edge (SASE) The convergence of several security services into a single, cloud-delivered service model.

secure baseline scanning Using specific security frameworks as comparison benchmarks to identify weaknesses.

Secure Sockets Layer (SSL) inspection Examining traffic to uncover any malicious content.

secure software development life cycle (SDLC) Integrating security activities across the entire process.

security controls testing The evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

security engineering Building systems to resist attacks.

security information and event management (SIEM) A product that consolidates real-time monitoring and management of security information with analysis and reporting of security events.

security misconfiguration A vulnerability that results from failing to properly configure the security protections available in hardware and software.

security orchestration, automation, and response (SOAR) A platform that is a combination of software programs and tools that allow organizations to synthesize and automate a range of security operations, threat intelligence, and incident response.

segmentation Dividing a network into smaller sections.

Sender Policy Framework (SPF) An email authentication method that identifies who the mail transfer agent email servers are that have been authorized to send email for a domain.

sensitivity level The depth of a vulnerability scan.

server-side request forgery (SSRF) An attack that takes advantage of a trusting relationship between web servers.

serverless A cloud infrastructure in which the capacity planning, installation, setup, and management are all invisible to the user because the cloud provider handles them.

service interruption An intrusion in a data exchange or communication.

service-level agreement (SLA) A service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service.

service-level objective (SLO) An agreement within a service-level agreement concerning a specific metric.

session management Monitoring and controlling the authentication and access control (or authorization) modules in web applications.

shell script A text file that contains a sequence of commands for a Linux or UNIX operating system.

single pane of glass A single management console that presents data from multiple sources in a unified display.

single sign-on (SSO) Using one authentication credential to access multiple accounts or applications.

social engineering A means of eliciting information or convincing a user to take action that weakens security.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

social media Websites and applications that enable users to create and share content.

software-defined networking (SDN) A technology that virtualizes parts of the physical network so that it can be more quickly and easily reconfigured.

stack overflow A buffer overflow attack that occurs in the stack.

stakeholder identification and communication Identifying and distributing reports to specific audiences who have a vested interest.

standardize processes Creating a consistent and repeatable method for completing a task or achieving a specific outcome by documenting and formalizing the steps and activities involved in a task or procedure.

static analysis Testing software before the source code is compiled.

string A sequence of characters embedded within a file.

supervisory control and data acquisition (SCADA) Multiple industrial control systems (ICSs) that are managed by a larger system.

supply chain attack An attack used by nation-state actors to take advantage of a weak supply chain.

system processes A special category of operating system processes that are responsible for managing memory allocations, hosting operating system drivers, and managing other processes.

T

tabletop A monthly 30-minute discussion of a scenario conducted in an informal and stress-free environment.

tactics, techniques, and procedures (TTP) The behavior or actions of a threat actor described in a cascading sequence.

Tcpdump A command-line packet analyzer.

team coordination to manage and facilitate automation Involving all security personnel who may have played a role in the manual process to automate processes.

technical control A control that is incorporated as part of hardware, software, or firmware.

testing The process used to determine if a patch will adversely affect any customized applications.

threat actor A term used to describe individuals or entities who are responsible for cyberattacks.

threat feed combination An enhancement of data enrichment that adds third-party threat feeds.

threat hunting An activity that combines a proactive, repetitive (iterative), and predominantly human (instead of exclusively automated) approach to seeking threat actors.

threat intelligence sharing Threat intelligence (TI) that is collected from various sources and then disseminated to others.

threat modeling A proactive strategy for evaluating risks.

time synchronization Ensuring that recorded times of a single event in multiple log files match.

timeline The sequence of events that occurred.

timeliness Threat intelligence (TI) that has been distributed quickly at the best possible time.

top 10 KPIs Key performance indicators considered the most important.

training Instruction and coaching on how to react to a cyber incident.

transfer A risk strategy that shares a portion of the consequences with another party.

trend A movement in attacks and defenses.

true negative Accurately failing to trigger an alarm when no vulnerability is detected.

true positive Accurately triggering an alarm based on the detection of a vulnerability.

U

unauthorized change An alteration by threat actors to operating system settings particularly as they relate to security.

unauthorized privilege Changing operating system settings or exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from accessing.

unauthorized scheduled task A task that was not approved and initiated by an administrator.

unauthorized software Applications that are not approved.

unexpected outbound communication Any unfamiliar and unanticipated outbound communication.

unexpected output The result of an infected application that produces output that is unanticipated.

unintentional insiders Employees who unwittingly cause harm or create a vulnerability for an external threat actor to then exploit.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

unusual traffic spike A sudden unusual surge in network bandwidth utilization.

user behavior analysis (UBA) Analyzing user behavior to identify anomalous behavior.

user interaction A metric that describes whether a user other than the attacker is required to perform an action or participate in the exploitation of the vulnerability.

V

validate data integrity Confirming that data has not been tampered with.

validation The process of confirming that patches can be installed.

virtualization A means of managing and presenting computer resources by function without regard to their physical layout or location.

VirusTotal A remote sandbox that inspects items with over 70 antivirus scanners and URL/domain blocklisting services.

vulnerability management Identifying and addressing an organization's security vulnerabilities.

vulnerability scan A frequent and ongoing process that is automated to continuously identify vulnerabilities and monitor cybersecurity progress.

W

webhook A type of event-driven application programming interface (API) that sends information or performs a specific function in response to a trigger.

who, what, when, where, and why Questions commonly used in an investigation.

WHOIS A Transmission Control Protocol/Internet Protocol (TCP/IP) query/response protocol for accessing information about internet resources, most notably domain names and Internet Protocol (IP) addresses as well as internal contact information for websites.

Windows Registry A hierarchical database that contains configuration settings for Windows applications and the operating system.

Wireshark A popular graphical user interface (GUI) packet capture and analysis tool.

Z

Zed Attack Proxy (ZAP) The premiere open-source tool for diagnosing web applications.

zero-day A vulnerability for which there is no advance warning.

zero trust A strategic initiative about networks that is designed to stymie successful attacks by threat actors who are already within a network.

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Index

A

abnormal account activity, 126
abnormal network traffic, 93–97
abnormal OS process behavior, 104
AbuseIPDB, 135–136
access control lists (ACLs), 328
access control scheme, 327–328
access management, 70–72
access point probe, 101
accounts, types of, 71
accuracy, 156
action plan, 247
active defense, 158
active scanning, 188–189, 244
activity on an unexpected port, 97
advanced persistent threat (APT), 39
advanced vulnerability scanning, 229–230
adversarial AI, 340
adversary emulation, 225
affected host, 250
agent, 192
agent-based scanning, 192
agentless scanning, 192
agreements, 248, 253
"a href", 48
air gap, 13
alert volume, 312
ALPHV/BlackCat, 116
alternative hostname format, 49
Amazon's AWS Security Hub, 246
analog meters, 15, 16
analysis, in threat hunting, 162
Angry IP scanner, 197–198
anomalous activity, 106
API integration, 168
Apple, email defense, 123
application, 162
application indicators of attack, 106
  modified application logs, 107–108
  new account creation, 106–107
  unexpected outbound communications, 107
  unusual activity, 106
application logs, 107–108, 137
application programming interfaces (APIs), 52–53, 168
application stress testing, 75
Arachni, 244
artificial intelligence (AI)
  adversarial, 340
  in cybersecurity, 338–339
  definition, 336
  history of, 337–338
  risks, 339–340
  threat actor use of, 340
asset discovery, 185
asset value, 215
assumption hunting, 161
@ symbol, manipulation of, 49
attack methodology frameworks, 273
  Cyber Kill Chain™, 276
  Diamond Model of Intrusion Analysis, 275–276
  MITRE ATT&CK, 274
  OSSTMM, 274
  OWASP Testing Guide, 274, 275
attacks
  buffer overflow, 51–52
  cross-site scripting, 46–47
  complexity, 218
  data poisoning, 47–48
  directory traversal, 47
  distributed denial-of-service, 16
  integer overflow, 52
  Log4j, 40, 47
  MFA fatigue, 67
  obfuscated links, 48–49
  remote code execution, 47
  request forgery, 45
  RowHammer, 33–34
  social engineering, 48
  supply-chain, 39–40
  on Target, 98
  trees, 226, 227
  vector, 218
  web server application, 45–47
  wireless, 246
attack surface management (ASM), 224–225
attack surface reduction, 224
attestation, 67
authentication, 54, 63–64, 76, 325
  advances, 66–70
  app, 66, 67
  broken, 54
  multifactor, 66, 294
Automated Indicator Sharing (AIS), 156–157
automated patch management, 222–224
automation
  benefits, 165
  data correlation, 165
  force multiplier, 165
  minimizing human engagement, 164
  repeatable tasks, 164
  software development, 165–166
  task identification, 163
  team coordination, 164
  webhooks, 169
availability, 219
awareness, education, and training, 255

B

bandwidth consumption, 96–97
bandwidth monitoring, 93–95
Bash, 22–23
Basic Input/Output System (BIOS), 19, 20
beaconing, 97–98
bit flipping, 33
blogs, 155
Bloom's Taxonomy, 362
boot security, 20–21
botnets, 98
breach of security, 284
broken access control, 52–53
brokers, 41
browser plugins, 169
buffer overflow attack, 51–52
bug bounties, 225
Burp Suite, 244
business continuity (BC) plan, 272
business-critical assets, 160
business impact analysis (BIA), 273
business process interruption, 249

C

capture the flag (CTF) exercise, 255
car data collection and transmission, 321–322
cardholder data (CHD), 278
CBL Data Shredder, 301, 302
Center for Internet Security (CIS), 184
central processing unit (CPU), 19, 102
chain of custody, 305–306
chain of trust, 20–21
changing business requirements, 249
ChatGPT, 337, 339
checksums, 117
clients, 279
closed-source intelligence, 156
cloud access security broker (CASB), 72
cloud computing, 9–11
  advantages of, 10
  cloud types, 10
  virtualization, 5
cloud forensics, 309–310
cloud infrastructure, 244–246
code reuse, 76
coding, 22–25
command and control (C&C), 120–121
command-line interfaces (CLIs), 118
command-line/IP utilities, 354–359
commands
  interpret suspicious, 118
  monitoring, 118
Common Vulnerabilities and Exposures (CVE), 217
Common Vulnerability Scoring System (CVSS), 217, 252–254
  groups, 217–218
  metrics, 217–219
  prioritizing, 219
Common Weakness Enumeration (CWE), 74
communication
  best practices, 285
  with C&C, 120
  customer, 279–280
  cyber incident, 282–285
  federal regulatory requirements, 284
  irregular peer-to-peer, 97
  limit adverse reactions, 283
  prevent inadvertent release of information, 283
  reasons for, 282–284
  state legislative mandates, 283–284
  transparent, 285
  unexpected outbound, 107
  vulnerability, 250–254
community cloud, 10
compare message digests, 117
compensating control, 221, 247
competitors, 41
complacency, 179, 180
compliance report, 251
CompTIA CySA+ CS0-003 certification exam
  knowledge-based assessment questions, 347–350
  objectives, 362–372
  performance-based questions, 350–351
computer-based training (CBT), 258
Computer Emergency Response Team (CERT), 153–154
confidence level, 156–157
confidentiality, 219
configuration file location, 19
configuration files, 18–19
configuration management, 223, 248
configuration management databases (CMDBs), 223
configurations/misconfigurations, 160
containerization, 8
containment, 299–300
context awareness, 213–214
continuity of operation planning (COOP), 272
continuous delivery (CD), 166
continuous deployment (CD), 166
continuous integration (CI), 166
control, 220–221, 247
cookies, 187
corporate information, 278
corporate policies, 182
corrective control, 221, 247
credentialed scan, 191
critical infrastructures, 17
criticality of data, 277–278
critical vulnerabilities, 249
cross-site request forgery (CSRF), 45
cross-site scripting (XSS) attack, 46–47
crushing, 302
cryptographic failure, 53
cryptography, 325
  algorithms, 61–62
  history of, 61
Cuckoo Sandbox, 130–131
customer
  clients *vs.*, 279
  communication, 279–280
cyber disclosure rules, 115–116
cyber incident, 269. *See also concepts related to incident response*
  assessment, 311–313
  communication, 282–285
  data integrity, 298
  downtime, 298
  economic impact, 298
  impact, 299
  lessons learned, 311
  priority of, 297–299
  reasons for, 296
  recovery time, 298
  scope, 299
  severity, 296–297
  triage, 297
Cyber Information Sharing and Collaboration Program (CISCP), 157
Cyber Kill Chain™, 276
cybersecurity
  bootcamps, 3, 4
  indicators, 91–93
  job shortage, 3–4
Cyber Security Incident Response Team (CSIRT), 154
Cybersecurity Information Sharing Act (CISA), 157
cyberteam exercises, 255–256
cyberterrorists, 41
cyber threat intelligence (CTI). *See* threat intelligence (TI)

D

data
  collection, 162
  correlation, 165
  critical, 277–278
  in cybersecurity, 334–341
  destroying, 331–332
  exchange formats, 24–25
  exfiltration, 106
  hiding, 330–331
  integrity, 298, 306
  limiting access to, 329–330
  minimization, 334
  retention, 333–334
  sanitization, 301, 330
  stealing, 98
data analytics
  and cybersecurity, 335–336
  definition of, 335, 336
  types of, 335
data and log analysis, 296
data collection
  concealed/questionable, 323
  issues, 323–324
  overt/legitimate, 323
  purpose limitation, 334
  restrictions on, 334
data enrichment, 167
data loss prevention (DLP), 326
data poisoning, 47–48

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

data protection, 76, 325
  access control, 325–328
  conforming to legal regulations, 332
  data destruction technique, 331–332
  data loss prevention, 326
  data masking, 330
  DRM, 329–330
  encryption, 325
  geofencing, 326–327
  nontechnical controls, 332–334
  tokenization, 331
dated components, 53
dead code, 76
debugger, 202–204
dedicated probe, 101
deep/dark web, 154, 155
degrading functionality, 249
desktop probe, 101
detection and monitoring, 151
detective control, 221
deterrent control, 221, 247
device fingerprinting, 186–188
Diamond Model of Intrusion Analysis, 275–276
digital forensics, 304. *See also* forensics
digital rights management (DRM), 329–330
directory traversal, 47
disaster recovery (DR) plan, 273
discretionary access control (DAC), 327–328
distributed denial-of-service (DDoS) attack, 16, 297
DNS and IP reputation, 134
Document Object Model XSS, 47
domain-based message authentication, reporting, and conformance (DMARC), 125
domain generation algorithm (DGA), 120–121
domain keys identified mail (DKIM), 125
Domain Name Service (DNS), 356
Double-Sided RowHammer, 34
drag, 164
drive capacity consumption, 103–104
DriverView, 128
dual in-line memory module (DIMM), 33, 34
dynamic analysis, 201, 244
  debugging, 202–204
  fuzzing, 201
  reverse engineering, 202
dynamic file analysis, 118
dynamic network fingerprinting, 187–188
dynamic random access memory (DRAM), 33

E

edge discovery, 225
efficient-cores (E-cores), 102
electric vehicles (EVs), 322
elliptic curve cryptography (ECC), 61–62
Elliptic Curve Digital Signature Algorithm (ECDSA), 62
email
  analysis, 121–125
  defense, 123–125
  disclaimer, 38
  forwarding, 123
  header, 122
  mail transfer agent, 121, 123
  mail user agent, 121
  server problem, 95
  threats, 123
embedded links, 123
Emotet, 97
EnCase software, 307
encryption, 72–74, 325
end-of-life component, 53
endpoint detection and response (EDR), 142–143
endpoint indicators of attack, 101–102
  data exfiltration, 106
  high-volume consumption of resources, 102–104
  OS evidence, 104–105
  software-related evidence, 105
endpoint logs, 137
Environmental Protection Agency (EPA), 268
eradication, 300–303
error-correcting code (ECC), 34
escalation, 216
EtherApe, 132
evidence
  acquisition, 307–308
  operating system, 104–105
  software-related, 105
exceptions, 221
executive summary, 251–252, 313
exercise
  capture the flag, 255
  cyberteam, 255–256
  incident response testing, 256
exploitability/weaponization, 214
eXtensible Markup Language (XML), 24, 25
external context awareness, 213
external stakeholders
  identification and communication, 279–282
  reports, 251
external vulnerability scan, 189

F

false negative, 213
false positive, 213
Fast IDentity Online (FIDO), 69
fault tree analysis, 312, 313
federation, 68
file analysis, 118
file and code repositories, 155
file inclusion vulnerabilities, 50
file structure, 18, 118, 119
file system changes/anomaly, 104
financial cybercrime, 35
financial information, 277
firewall log, 136–138
firewall segmentation, 78
fishbone diagrams, 312
flow analysis, 133–134
focus areas, 160
forensic analysis, 304
forensics
  chain of custody, 305–306
  cloud, 309–310
  digital, 304
  evidence acquisition, 307–308
  mobile device, 308–309
  preservation of evidence, 304–305
  procedures, 304–308
  report, 308
  software tools, 306–307
  virtualization, 309
forums, 155
Freedom of Information Act (FOIA), 157
FTK Imager, 307
full network vulnerability scanning, 189
fuzzers, 180
fuzzing, 201

G

gamification, 258
General Data Protection Regulation (GDPR), 284, 325, 334
geofencing, 326–327
global positioning system (GPS), 327
GNU debugger (GDB), 203–204
Google
  bug bounty program, 225
  passkeys, 70
governance
  activities, 228
  bodies, 228, 229
  cybersecurity, 220
  definition of, 228
  mechanisms, 228, 229
  organizational, 248
government bulletins, 155
guest user accounts, 71

H

hacker, 35
hacktivists, 38
hard disk drives (HDDs), 103–104
hardware architecture, 19–21
hardware asset management, 185–186
hardware supply-chain infection, 39
hash-based message authentication code (HMAC) OTP (HOTP), 66
hashing, 117
heap overflow, 52
high-value asset (HVA) information, 278
high volume of resource consumption, 102
  drive capacity, 103–104
  memory, 103
  processor, 102–103
honeypot, 160–161
host-based segmentation, 78
host virtualization, 5, 7
hybrid cloud, 10
hybrid hunting, 161
hypertext transfer protocol (HTTP) traffic, 98, 99
hypervisors, 6

I

IBM, virtualization, 5
identification and authentication failure, 53–54
identity and access management (IAM), 63
identity proofing, 63
immunity debugger, 202–204
impersonation, 123
implementation, patch, 222
impossible travel, 126
incident declaration and escalation, 299
incident response, 151
  providers, 282
  reports, 313–314
  team, 270–271
  testing exercises, 255–256
  tools, 271
incident response activity phases, 295
  containment, 299–300
  detection and analysis, 295–299
  eradication and recovery, 300–303
  post-incident activities, 303–314
incident response plan
  actionable goals, 269–270
  attack methodology frameworks, 273–276
  business continuity plan, 272
  business impact analysis, 273
  critical data, 277–278
  disaster recovery plan, 273
  documentation, 271
  testing, 271
  training, 271
  updating, 310
indicators of attack (IOA), 91–92
  application, 106–108
  endpoint, 101–106
  hunting, 161
  IOC *vs.*, 93
  network, 93–101
indicators of compromise (IOC), 92, 296
  diagnosing malware, 117–121
  email analysis, 121–125
  file analysis tools, 127–131
  generation, 310
  IOA *vs.*, 93
  log correlation and analysis tools, 136–143
  network analysis tools, 131–134
  reputation tools, 134–136
  user behavior analysis, 125–127
industrial control systems (ICSs), 15
industry framework, 183
information security management systems (ISMSs), 184
information-sharing organizations, 156
information technology (IT), 15, 38
infrastructure
  containerization, 8
  serverless, 8–9
  virtualization, 5–8
infrastructure vulnerability scanners
  Nessus, 194–197
  Nexpose, 197
  OpenVAS, 197
  Qualys, 197
injection flaws, 51
input validation, 75
insecure designs, 52
insider threat, 37–38
integer overflow attack, 52
integration platform as a service (iPaaS), 168
integrity, 219
intellectual property (IP), 278, 329
intelligence cycle, 152–153
intelligence hunting, 160–161
intentional insiders, 37
interconnection security agreement (ISA), 248
internal context awareness, 213
internal file structure, 118, 119
internal sources, 156
internal stakeholder
  categories of, 279
  reports, 250–251
internal vulnerability scan, 189
International Organization for Standardization (ISO) 27000, 184
Internet of Things (IoT), 16
interpret suspicious commands, 118
introduction of new accounts, 106–107
intrusion detection system (IDS), 137
ipconfig, 356
iPhone
  recovery key, 294
  security, 293–295
  Stolen Device Protection, 294
irregular peer-to-peer communication, 97
isolated networks, 160
isolation, 213
isolation containment technique, 300

J

JavaScript object notation (JSON), 24–25
Joe Sandbox, 130
Johari window, 42, 43
jump server, 12–13

K

key performance indicators (KPIs), 249–250, 311–312
key risk indicators (KRIs), 167
known threats, 42–44
Kroger, 179

L

law enforcement agencies, 281
least privileged user accounts (LUAs), 71
legacy systems, 249
legal department, 279
legal hold, 304, 305
links
  embedded, 123
  obfuscated, 48–49

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

local file inclusion (LFI) vulnerability, 50
local government agencies, 267–268
local sandboxing, 127–128
log(s), 136, 213, 296
  categories of, 137
  firewall, 136–138
  ingestion, 138–139
  management issues, 136–138
log analysis tools, 139
  endpoint detection and response (EDR), 142–143
  security information and event management (SIEM), 139–140, 142
  security orchestration, automation, and response (SOAR), 140–142
logging level, 138–139
logical segmentation, 12
Log4j attack, 40, 47
LogoFAIL, 179–180

M

machine learning (ML), 337
macros, 22
maintenance window, 222
malicious actor. *See* threat actor
malicious process, 104
Maltego, 198–200
malware diagnosis, 117–121
managed service providers (MSPs), 40
managerial control, 221
map scans, 188
mean time to alert, 311
mean time to contain (MTTC), 250
mean time to detect (MTTD), 249, 311
mean time to mitigate, 311
mean time to remediate, 311
mean time to respond (MTTR), 249, 311
media, 280, 283, 285
memorandum of understanding (MOU), 248
memory consumption, 103
MeridianLink, 116
metadata logs, 137
Metasploit framework (MSF), 239–241
Metasploit Free, 240
Metasploit Pro, 240
metrics, 249
MFA fatigue attack, 67
Microsoft 365, 338
Microsoft Security Development Lifecycle (MS SDL), 75
Microsoft Windows
  discretionary access control, 327–328
  Quick format option, 300–301
  Resource Monitor, 103
  system processes, 18
mirror image backup, 306
misconfigurations, 160
mitigation, 250
MITRE ATT&CK, 274
mobile device forensics, 308–309
modified application logs, 107–108
multifactor authentication (MFA), 66, 294

N

National Institute of Standards and Technology (NIST), 53, 62, 295
National Security Agency (NSA), 62
National Vulnerability Database (NVD), 217
nation-state actors, 39–40
Nessus, 169, 194–197, 218
Nessus Attack Scripting Language (NASL), 169, 194
NetFlow, 134
netstat
  activities, 356
  switches, 243, 355
network
  architectures, 9–11
  indicators of attack, 93–101
  logs, 137
  scans/sweeps, 100
  segmentation, 11–13, 78
  traffic, 93–97
  vulnerability scanning, 197–200
network time protocol (NTP), 138
network traffic analysis. *See* flow analysis
Nexpose, 197
Nikto, 244
nmap, 242–243
noncredentialed scan, 191
nondisclosure agreement (NDA), 248
nslookup, 356–357

O

OAuth, 69
obfuscated links, 48–49
OCTAVE, 227
Okta incident, 89–90
one-time password (OTP), 66
online scanning services, 48
on-premise architecture, 10–12
Open ID, 69
Open Indicators of Compromise (OpenIOC), 155
Open Source Foundation for Application Security (OWASP) Testing Guide, 274, 275
open-source intelligence (OSINT), 149, 153–156
Open Source Security Testing Methodology Manual (OSSTMM), 274
Open Vulnerability Assessment Scanner (OpenVAS), 197
Open Worldwide Application Security Project (OWASP), 183–184
operating system (OS), 17, 222
  configuration files, 18–19
  evidence, 104–105
  hardware architecture, 19–21
  system processes, 18
operational control, 221
operational technology (OT), 15, 185
  risks and weaknesses, 16–17
  types of, 15
operations, 189
orchestration, 166–167
order of volatility, 307–308
organizational governance, 248
organized crime, 37
outdated components, 53
output encoding, 75
overflow vulnerabilities, 51–52

P

packet analyzer, 359–361
packet capture, 131–133
Pacu, 244
paid feeds, 156
parameterized query, 75
passive discovery, 225
passive scanning, 188, 244
Passkey, 69–70
passwordless systems, 69–70
passwords, 64
  changing, 65
  one-time password, 66
  strong, 64–65
  weak, 64, 65
PASTA, 227
patch, 248, 303
  automated management tools, 222–224
  implementation, 222
  management, 222
  reception, 222
  rollback, 222
  testing, 222
  validation, 222
pattern recognition, 118
Payment Card Industry Data Security Standard (PCI DSS), 183
peer-to-peer command and control (P2P C&C) configuration, 98–100
penetration test, 181, 225
performance, of vulnerability scan, 189
performance-cores (P-cores), 102
permissions, 303
persistent XSS, 47
personal health information (PHI), 277
personal information, 283–284
personally identifiable information (PII), 277, 324
phishing, 123
phishing campaigns, 256–257
PHP, 50
physical control, 221, 247
physical segmentation, 12
ping, 354–355
playbook, 270
plugins, 169
policy, 228, 229
ports, 351–353
post-incident activities, 303
  assessing the cyber incident, 311–313
  forensic analysis, 303–310
  generating IOC, 310
  incident response reports, 313–314
  updating the incident response plan, 310
PowerShell, 23, 118
preservation of evidence, 304–305
preventive control, 221
prioritizing
  with CVSS, 219
  vulnerabilities, 215–216, 219
priority systems, 249
privileged access management (PAM), 70–72
privilege escalation, 47
privileges, 70–71, 104–105, 218
probes, 101
process
  standardization, 163–164
  streamlining, 164–167
processor consumption, 102–103
programming vulnerabilities, 50–52
Protected Critical Infrastructure Information (PCII), 157
protected health information (PHI), 324
protocol analysis, 133
protocol ID, 353
Prowler, 244, 245
public cloud, 10
public key infrastructure (PKI), 73
publicly owned utilities (POUs), 268
public relations, 279, 280
punycode, 49
Python, 23–24

Q

Qualys, 197

R

ransomware attack protection, 21
Recon-ng, 241–242
recurrence, 254
recurring vulnerabilities, 254
reflected XSS, 47
registry changes/anomaly, 104
RegShot, 128
regular expression (regex), 25
regulatory reporting, 284
regulatory requirements, 182
reimaging, 302
relevancy, 156
remediation, 299
remote code execution (RCE), 47
remote file inclusion (RFI) vulnerability, 50
remote sandboxing
  Cuckoo Sandbox, 130–131
  Joe Sandbox, 130
  VirusTotal, 129
removal containment technique, 299–300
reports
  compliance, 251
  contents, 251–252
  external stakeholder, 251
  forensic, 308
  incident response, 313–314
  internal stakeholder, 250–251
reputation tools, 134–136
request forgery attack, 45
responsive control, 221
reverse engineering, 202
reverse-engineering containment technique, 300
risk(s)
  acceptance, 333
  AI in cybersecurity, 339–340
  avoidance, 333
  mitigation, 333
  review cycle, 333
  transfer, 333
risk management, 151
risk management principles, 332
risk score, 253
rogue devices on a network, 100–101
role-based awareness training, 258
rollback, 222
root-cause analysis (RCA), 312–313
RowHammer attack, 33–34
RowPress, 34
RSA algorithm, 61
rule-based role-based access control (RB-RBAC) scheme, 328
Rumsfeld, Donald, 42

S

sandbox(ing), 127, 353–354
  local, 127–128
  remote, 129–131
sanitation methods, 301
scans/sweeps, 100
scheduling, 190
scope, 218
scope of impact, 298, 299
Scout Suite, 244
scripting language, 22–23
script kiddies, 36
SecDevOps, 166
Secure Access Service Edge (SASE), 79–80
secure baseline scanning, 185
secure coding, 74–76
Secure Sockets Layer (SSL) inspection, 73–74
secure software development life cycle (SDLC), 74–75
Securities and Exchange Commission (SEC) rules, 115–116
Security Assertion Markup Language (SAML), 68
security controls testing, 225
security engineering, 151
security information and event management (SIEM), 139–140, 142
security keys, 66, 67
security misconfigurations, 50
security orchestration, automation, and response (SOAR), 140–142, 167
security policy, 182
segmentation, 189
segmentation containment technique, 300
sender policy framework (SPF), 124–125
sensitive personal information (SPI), 277, 324
serverless infrastructure, 8–9
Server Message Block (SMB), 99–100
server-side request forgery (SSRF), 45
service interruption, 106
service-level agreement (SLA), 229, 248
service-level objective (SLO), 229, 248
session management, 76

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

sFlow, 134
shadow IT, 38
shared accounts, 72
shearing, 302
shell script, 22
Shibboleth, 69
Simple Mail Transfer Protocol (SMTP), 121
single pane of glass, 169–170
single sign-on (SSO), 68–69
situational hunting, 159–160
smart meters, 15, 16
smartphones, 323
social engineering, 48
social media, 155, 285
software asset management, 185–186
software-defined networking (SDN), 13–14, 78
software development, 165–166
software supply-chain infection, 39–40
software vulnerability assessment, 200
  dynamic analysis, 201–204
  static analysis, 200–201
solid-state drives (SSDs), 103–104
specialized systems, 15–16
SSDT View, 128
stack overflow, 52
stakeholder identification and communication, 250, 279
stakeholders
  external, 251, 279–282
  internal, 250–251, 279
standardize processes, 163–164
standard user accounts, 71
static analysis, 200–201, 244
static device fingerprinting, 187
static file analysis, 118
stealth redirection, 49
stealth transmissions, 97–100
steganography, 61
stored procedure, 76
streamlining, 164–167
STRIDE, 228
string extractor, 118, 119
strings, 118
structured hunting, 159
Structured Threat Information Expression (STIX), 156
Sun Tzu, 41
superuser accounts, 71
supervisory control and data acquisition (SCADA) system, 15
supply chain, 39, 40
supply-chain attacks, 39–40
system hardening, 21
system process, 18
system process criticality, 298

T

tabletop, 256
tactics, techniques, and procedures (TTP), 41–42
tamper-evident tape, 304, 305
Target, 98
target row refresh (TRR), 34
Taylor, Frederick, 163
Taylorism, 163
tcpdump, 132, 359–360
Tcpreplay, 132
team coordination, 164
technical control, 221
Tesla, 322
testing, patch, 222
threat actor, 35
  AI usage, 340
  categories of, 35–41
  tactics, techniques, and procedures, 41–42
threat data, 151–152
threat feed combination, 167
threat hunting, 158
  analysis, 162
  application, 162
  collection, 162
  focus areas, 160
  goal of, 158
  levels, 158, 159
  methodologies, 160–161
  roles, 158, 159
  situational, 159–160
  steps in, 162
  structured, 159
  unstructured, 159
threat intelligence (TI), 150–151
  closed-source, 156
  confidence level, 156–157
  life cycle, 152–153
  open-source, 149, 153–156
  paid, 149
  privacy, 157
  shared, 149
  sources, 153–156
  threat data *vs.*, 151–152
  timeliness, 156
threat intelligence sharing, 151
threat maps, 154
threat modeling, 225
  advantages, 226
  components, 226
  definition of, 226
  methodologies, 226–228
time-based one-time password (TOTP), 66
timeline, 313
timeliness, 156
time synchronization, 138, 140
Tokelau, 237–238
token(ization), 66, 331
top 10 KPIs, 249–250
tracert, 357–359
Traffic-Light Protocol (TLP), 157
traffic spikes, 94–96
training, 255, 271
  effective, 258
  marginal, 256–257
  user awareness, 256–258
Transmission Control Protocol/Internet Protocol (TCP/IP), 351
Transport Layer Security (TLS), 73
trends, cybersecurity, 249
triage, 216, 297
Triangulation, 211–212
Trike, 227
true negative, 213
true positive, 213
Trusted Automated Exchange of Intelligence Information (TAXII), 156
Turing, Alan, 337
type I hypervisors, 6
type II hypervisors, 6

U

unauthorized changes, 104
unauthorized privilege, 104–105
unauthorized scheduled task, 104
unauthorized software, 105
unexpected outbound communications, 107
unexpected output, 106
Unified Extensible Firmware Interface (UEFI), 19–20
unintentional insiders, 37–38
United States Computer Emergency Readiness Team (US-CERT), 298
unknown threats, 42–44
unstructured hunting, 159
unusual traffic spikes, 94–96
URL
  hiding, 48
  shortener, 49
use file analysis techniques, 118–121
user acceptance testing, 75
user awareness training, 256–258
user behavior analysis (UBA), 125–126
  abnormal account activity, 126
  impossible travel, 126
  limitations, 126
User Datagram Protocol (UDP), 351
user interaction, 218

V

validation, 222, 303, 306
Van Rossum, Guido, 23
VAST, 228
virtual desktop infrastructure (VDI), 6–7
virtualization, 5
  advantages, 7
  forensics, 309
  host, 5, 7
  risks, 7
virtual local area network (VLAN), 13
virtual machine manager, 7–8
virtual machine (VM), 309
VirusTotal, 129
Visual Basic for Applications (VBA), 22
vulnerability
  communication and reporting, 250–254
  critical, 249
  database, 155
  escalation, 216
  feeds, 190
  file inclusion, 50
  identification, 239–247
  mitigation, 300
  overflow, 51–52
  prioritizing, 215–216, 219
  recurring, 254
  response to, 247–250
vulnerability assessment tools, 193
  infrastructure, 194–197
  network, 197–200
  software, 200–204
vulnerability management, 151, 180–181
  attack surface management, 224–225
  configuration management, 223
  governance, 228–229
  legacy, 230
  patch management, 221–224
  threat modeling, 225–228
  using controls, 220–221
vulnerability scan, 169
  access approval, 193
  active *vs.* passive, 188–189
  advanced, 229–230
  agent *vs.* agentless, 192
  analysis, 213–215
  asset discovery, 185–186
  asset value, 215
  challenges, 182
  corporate policies, 182
  credentialed *vs.* non-credentialed, 191
  device fingerprinting, 186–188
  exploitability/weaponization, 214
  frequency of, 189–190
  full network *vs.* segmentation, 189
  internal *vs.* external, 189
  network appliance configurations, 193
  vs. penetration test, 181
  performance, 189
  regulatory requirements, 182
  running, 190–193
  scanner permissions, 193
  scheduling, 190
  scope of, 190–191
  sensitivity level, 191
  signature-based monitoring, 190
  software configuration, 190–191
  software updation, 190
  third party, 253
  validation, 213
  zero-day vulnerabilities, 215

W

walkthrough, 256
Walmart, 179
watermarking, 329
web applications, 244
webhooks, 168–169
web server application
  attacks, 45–47
  infrastructure, 44–45
website personalization, 187
WHOIS, 135
Windows 11, 222, 223
Windows Command Shell, 118
Windows Defender, 21
Windows PowerShell, 23
Windows Registry, 19
Windows Sandbox, 127, 128, 353
WinDump, 359
wireless device probe, 101
wireless local area networks (WLANs), 101, 246
wireless networks, 246–247
Wireshark, 132, 360–361
workflow orchestration, 141, 166–167
work rationalization, 163
5 Ws (who, what, when, where, and why), 313

Y

Yahoo incident, 282–283

Z

Zed Attack Proxy (ZAP), 244, 245
Zenmap, 243
zero-day vulnerability, 211, 215
zero trust, 77
  microsegmentation, 78
  principles of, 78
zero-trust architecture (ZTA), 79

Copyright 2025 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.