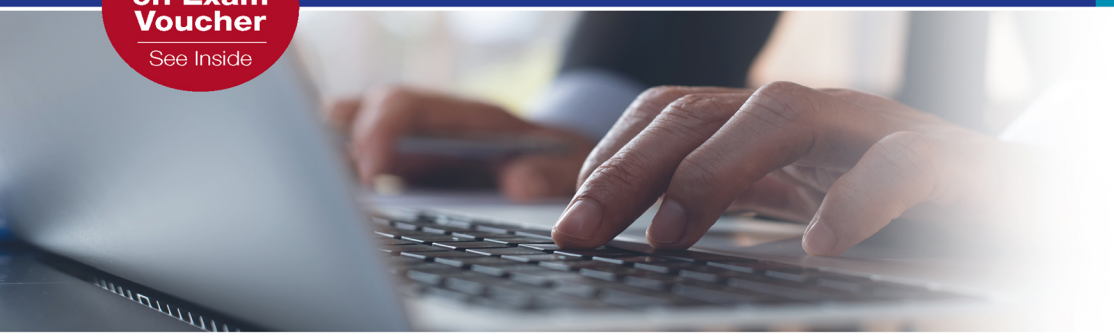
PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside



Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Security+

SY0-601

OMAR SANTOS
RON TAYLOR
JOSEPH MLODZIANOWSKI

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

CompTIA® Security+ SY0-601 Cert Guide

Omar Santos
Ron Taylor
Joseph Mlodzianowski

CompTIA® Security+ SY0-601 Cert Guide

ISBN-13: 978-0-13-677031-2

ISBN-10: 0-13-677031-2

Library of Congress Control Number: 2021935686

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Christopher A. Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Chuck Hutchinson

Indexer
Erika Millen

Proofreader
Abigail Manheim

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Table of Contents

About the Authors

Omar Santos is an active member of the cybersecurity community, where he leads several industry-wide initiatives. He is a best-selling author and trainer. Omar is the author of more than 20 books and video courses, as well as numerous white papers, articles, and security configuration guidelines and best practices. Omar is a principal engineer of the Cisco Product Security Incident Response Team (PSIRT), Security Research and Operations, where he mentors and leads engineers and incident managers during the investigation and resolution of cybersecurity vulnerabilities.

Omar co-leads the DEF CON Red Team Village, is the chair of the Common Security Advisory Framework (CSAF) technical committee, is the co-chair of the Forum of Incident Response and Security Teams (FIRST) Open Source Security working group, and has been the chair of several initiatives in the Industry Consortium for Advancement of Security on the Internet (ICASI). His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of their critical infrastructures. You can find additional information about Omar's current projects at h4cker.org and can follow Omar on Twitter @santosomar.

Ron Taylor has been in the information security field for more than 20 years working in various areas focusing on both offense and defense security roles. Ten of those years were spent in consulting. In 2008, he joined the Cisco Global Certification Team as an SME in information assurance. From there, he moved into a position with the Security Research and Operations group, where his focus was mostly on penetration testing of Cisco products and services. He was also involved in developing and presenting security training to internal development and test teams globally, and provided consulting support to many product teams as an SME on product security testing. His next role was incident manager for the Cisco Product Security Incident Response Team (PSIRT). Currently, Ron is a security architect specializing in the Cisco security product line. He has held a number of industry certifications, including GPEN, GWEB, GCIA, GCIH, GWAPT, RHCE, CCSP, CCNA, CISSP, PenTest+, and MCSE. Ron has also authored books and video courses, teaches, and is involved in organizing a number of cybersecurity conferences, including the BSides Raleigh, Texas Cyber Summit, Grayhat, and the Red Team Village at DEFCON.

Twitter: @Gu5G0rman

Linkedin: www.linkedin.com/in/-RonTaylor

Joseph Mlodzianowski is an information security aficionado and adventurer; he started multiple villages at RSA Conference, DEFCON, and BLACK HAT, among others, including founding the Red Team Village with the help of great friends. He has been in the information technology security field for more than 25 years working in infrastructure, security, networks, systems, design, offense, and defense. Joseph is currently an enterprise security architect of Cisco Managed Services. He spent more than 10 years in the Department of Defense as an operator, principal security network engineer, and SME designing and deploying complex technologies and supporting missions around the world in multiple theaters. He has consulted, investigated, and provided support for multiple federal agencies over the past 15 years. Joseph continues to contribute to content, reviews, and editing in the certification testing and curriculum process. He spent almost 15 years in the energy sector supporting refineries, pipelines, and chemical plants; specializing in industrial control networks; and building data centers. Joseph holds a broad range of certifications, including the Cisco CCIE, CNE, CSNA, CNSS-4012, CISSP, ITILv4, NSA IAM, NSA IEM, OIAC1180, FEMA IS-00317, ACMA, First Responder, Hazmat Certified, Member of Bexar County Sheriff's Office CERT, MCSE, and Certified Hacking Investigator. He also is a founding contributor to the CyManII | Cybersecurity Manufacturing Innovation Institute, a member of Messaging Malware Mobile Anti-Abuse Working Group (M3aawg.org), and founder of the Texas Cyber Summit and Grayhat Conferences. He believes in giving back to the community and supporting nonprofits.

Twitter: @Cedoxx

Linkedin: www.linkedin.com/in/mlodzianowski/

Dedication

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

—Omar

I would not be where I am today without the support of my family. Mom and Dad, you taught me the importance of work ethic and drive. Kathy, my wife of 20 years, you have supported me and encouraged me every step of the way. Kaitlyn, Alex, and Grace, you give me the strength and motivation to keep doing what I do.

—Ron

Without faith and spiritual guidance, none of us would be where we are. I would like to thank my Creator; Linda, my lovely wife of more than 20 years; and my daughter Lauren, for their unwavering support, patience, and encouragement while I work multiple initiatives and projects.

—Joseph

Acknowledgments

It takes a lot of amazing people to publish a book. Special thanks go to Chris Cleveland, Nancy Davis, Chris Crayton, and all the others at Pearson (and beyond) who helped make this book a reality. We appreciate everything you do!

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Introduction

Welcome to the *CompTIA Security+ SY0-601 Cert Guide*. The CompTIA Security+ certification is widely accepted as the first security certification you should attempt to attain in your information technology (IT) career. The CompTIA Security+ certification is designed to be a vendor-neutral exam that measures your knowledge of industry-standard technologies and methodologies. It acts as a great stepping stone to other vendor-specific certifications and careers. We developed this book to be something you can study from for the exam and keep on your bookshelf for later use as a security resource.

We would like to note that it's unfeasible to cover all security concepts in depth in a single book. However, the Security+ exam objectives are looking for a basic level of computer, networking, and organizational security knowledge. Keep this in mind while reading through this text, and remember that the main goal of this text is to help you pass the Security+ exam, not to be the master of all security. Not just yet, at least!

Good luck as you prepare to take the CompTIA Security+ exam. As you read through this book, you will be building an impenetrable castle of knowledge, culminating in hands-on familiarity and the know-how to pass the exam.

Goals and Methods

The number one goal of this book is to help you pass the SY0-601 version of the CompTIA Security+ certification exam. To that effect, we have filled this book and practice exams with hundreds of questions/answers and explanations, including two full practice exams. The exams are located in Pearson Test Prep practice test software in a custom test environment. These tests are geared to check your knowledge and ready you for the real exam.

The CompTIA Security+ certification exam involves familiarity with computer security theory and hands-on know-how. To aid you in mastering and understanding the Security+ certification objectives, this book uses the following methods:

- **Opening topics list:** This list defines the topics to be covered in the chapter.
- **Foundation Topics:** The heart of the chapter. The text explains the topics from a theory-based standpoint, as well as from a hands-on perspective. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. Each chapter covers a full objective from the CompTIA Security+ exam blueprint.
- **Key Topics:** The Key Topic icons indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.

- **Key Terms:** Key terms without definitions are listed at the end of each chapter. See whether you can define them, and then check your work against the complete key term definitions in the glossary.
- **Review Questions:** These quizzes and answers with explanation are meant to gauge your knowledge of the subjects. If an answer to a question doesn't come readily to you, be sure to review that portion of the chapter.
- **Practice Exams:** The practice exams are included in the Pearson Test Prep practice test software. These exams test your knowledge and skills in a realistic testing environment. Take them after you have read through the entire book. Master one; then move on to the next.

Who Should Read This Book?

This book is for anyone who wants to start or advance a career in computer security. Readers of this book can range from persons taking a Security+ course to individuals already in the field who want to keep their skills sharp or perhaps retain their job due to a company policy mandating they take the Security+ exam. Some information assurance professionals who work for the Department of Defense or have privileged access to DoD systems are required to become Security+ certified as per DoD directive 8570.1.

This book is also designed for people who plan on taking additional security-related certifications after the CompTIA Security+ exam. The book is designed in such a way to offer an easy transition to future certification studies.

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of IT administration experience with an emphasis on security. The CompTIA Network+ certification is also recommended as a prerequisite. Before you begin your Security+ studies, it is expected that you understand computer topics such as how to install operating systems and applications, and networking topics such as how to configure IP, what a VLAN is, and so on. The focus of this book is to show how to secure these technologies and protect against possible exploits and attacks. Generally, for people looking to enter the IT field, the CompTIA Security+ certification is attained after the A+ and Network+ certifications.

CompTIA Security+ Exam Topics

If you haven't downloaded the Security+ certification exam objectives, do it now from CompTIA's website: https://certification.comptia.org/. Save the PDF file and print it out as well. It's a big document; review it carefully. Use the exam objectives list and acronyms list to aid in your studies while you use this book.

The following tables are excerpts from the exam objectives document. Table I-1 lists the CompTIA Security+ domains and each domain's percentage of the exam.

Table I-1 CompTIA Security+ Exam Domains

Domain	Exam Topic	% of Exam
1.0	Attacks, Threats, and Vulnerabilities	24%
2.0	Architecture and Design	21%
3.0	Implementation	25%
4.0	Operations and Incident Response	16%
5.0	Governance, Risk, and Compliance	14%

The Security+ domains are then further broken down into individual objectives. Table I-2 lists the CompTIA Security+ exam objectives and their related chapters in this book. It does not list the bullets and sub-bullets for each objective.

Table I-2 CompTIA Security+ Exam Objectives

Objective	Chapter(s)
1.1 Compare and contrast different types of social engineering techniques.	1
1.2 Given a scenario, analyze potential indicators to determine the type of attack.	2
1.3 Given a scenario, analyze potential indicators associated with application attacks.	3
1.4 Given a scenario, analyze potential indicators associated with network attacks.	4
1.5 Explain different threat actors, vectors, and intelligence sources.	5
1.6 Explain the security concerns associated with various types of vulnerabilities.	6
1.7 Summarize the techniques used in security assessments.	7
1.8 Explain the techniques used in penetration testing.	8
2.1 Explain the importance of security concepts in an enterprise environment.	9
2.2 Summarize virtualization and cloud computing concepts.	10
2.3 Summarize secure application development, deployment, and automation concepts.	11
2.4 Summarize authentication and authorization design concepts.	12
2.5 Given a scenario, implement cybersecurity resilience.	13
2.6 Explain the security implications of embedded and specialized systems.	14
2.7 Explain the importance of physical security controls.	15
2.8 Summarize the basics of cryptographic concepts.	16
3.1 Given a scenario, implement secure protocols.	17

Objective	Chapter(s)
3.2 Given a scenario, implement host or application security solutions.	18
3.3 Given a scenario, implement secure network designs.	19
3.4 Given a scenario, install and configure wireless security settings.	20
3.5 Given a scenario, implement secure mobile solutions.	21
3.6 Given a scenario, apply cybersecurity solutions to the cloud.	22
3.7 Given a scenario, implement identity and account management controls.	23
3.8 Given a scenario, implement authentication and authorization solutions.	24
3.9 Given a scenario, implement public key infrastructure.	25
4.1 Given a scenario, use the appropriate tool to assess organizational security.	26
4.2 Summarize the importance of policies, processes, and procedures for incident response.	27
4.3 Given an incident, utilize appropriate data sources to support an investigation.	28
4.4 Given an incident, apply mitigation techniques or controls to secure an environment.	29
4.5 Explain the key aspects of digital forensics.	30
5.1 Compare and contrast various types of controls.	31
5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	32
5.3 Explain the importance of policies to organizational security.	33
5.4 Summarize risk management processes and concepts.	34
5.5 Explain privacy and sensitive data concepts in relation to security.	35

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the authors that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to www.pearsonitcertification.com/register and log in or create a new account.

2. On your Account page, tap or click the **Registered Products** tab, and then tap or click the **Register Another Product** link.
3. Enter this book's ISBN (9780136770312).
4. Answer the challenge question as proof of book ownership.
5. Tap or click the **Access Bonus Content** link for this book to go to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the preceding steps, please visit http://www.pearsonitcertification.com/contact and select the "Site Problems/Comments" option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

NOTE The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to www.PearsonTestPrep.com and select **Pearson IT Certification** as your product group.
2. Enter your email/password for your account. If you do not have an account on PearsonITCertification.com or InformIT.com, you will need to establish one by going to PearsonITCertification.com/join.

3. On the My Products tab, tap or click the **Activate New Product** button.
4. Enter this book's activation code and click **Activate**.
5. The product will now be listed on your My Products tab. Tap or click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser:

http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to http://www.pearsonitcertification.com/register and entering the ISBN: 9780136770312.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. Once the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
8. Once the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will synch together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card Mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode will not provide the detailed score reports that the other two modes will, so it should not be used if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download

any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and click the **Update Application** button. This will ensure you are running the latest version of the software engine.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 80 percent off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

Figure Credits

Cover image: TippaPatt/Shutterstock
Chapter opener image: Charlie Edwards/Photodisc/Getty Images
Figures 4-2 and 4-3 courtesy of Cisco Systems, Inc
Figure 5-1 © 2015-2021, The MITRE Corporation
Figure 7-5 courtesy of Cisco Systems, Inc
Figures 10-1, 10-7, 10-10 courtesy of Cisco Systems, Inc
Figure 10-8 © 2021, Amazon Web Services, Inc
Figure 12-3 courtesy of Secret Double Octopus
Figure 12-4 courtesy of Active-Directory-FAQ
Figure 12-5 courtesy of Robert Koczera/123RF
Figures 13-1 and 13-2 © AsusTek Computer Inc.
Figure 14-1 Raspberry Pi courtesy of handmadepictures/123RF
Figure 14-3 courtesy of CSS Electronics
Figure 14-4 courtesy of strajinsky/Shutterstock
Figure 14-5 courtesy of RingCentral
Figures 14-6 and 15-4 from rewelda/Shutterstock
Figure 15-1 courtesy of Kyryl Gorlov/123RF
Figure 15-2 courtesy of Aliaksandr Karankevich/123RF
Figures 16-9 and 16-10 courtesy of ssl2buy.com
Figure 17-1 courtesy of hostinger.com
Figure 17-3 courtesy of wiki.innovaphone.com
Figure 17-4 courtesy of Adaptive Digital Technologies
Figure 18-4 © Microsoft 2021
Figure 18-5 courtesy of Microsoft Corporation
Figure 18-7 courtesy of Checkmarx Ltd
Figure 19-1 courtesy of Cisco Systems, Inc
Figures 19-5, 19-8 through 19-11, 19-15, and 19-16 courtesy of Cisco Systems, Inc
Figure 19-21 © Microsoft 2021
Figures 20-2 and Figure 24-4 © Microsoft 2021
Figure 20-4 © D-Link Corporation
Figure 20-5 courtesy of Cisco Systems, Inc
Figures 21-1 and 21-2 © 1992-2020 Cisco
Figures 23-1 and 23-2 courtesy of Cisco Systems, Inc
Figures 23-5 through 23-9 © Microsoft 2021
Figures 24-2 and 24-5 courtesy of Cisco Systems, Inc
Figures 24-6 through 24-10 © Microsoft 2021
Figures 25-1 and 25-2 ©1998–2021 Mozilla Foundation
Figure 26-1 © OffSec Services Limited 2021
Figures 26-2, 26-5, 26-6, 26-10 through 26-15, 26-18, 26-19 © 2021 The Linux Foundation
Figures 26-3, 26-4, 26-7 through 26-9 © Microsoft 2021
Figure 26-16 © 2021 Tenable, Inc
Figure 26-17 © 2010-2020, Cuckoo Foundation
Figure 26-21 © Wireshark Foundation
Figure 26-22 © X-Ways Software Technology AG
Figure 27-3 courtesy of Cisco Systems, Inc
Figure 27-4 courtesy of Evolve IP, LLC
Figure 28-1 © 2021 Tenable, Inc

Figure 28-2 © 2021 LogRhythm, Inc
Figure 28-3 © MaxBelkov
Figure 28-4 © 1992-2020 Cisco
Figure 28-5, 28-6, 28-10, 28-11, and 28-18 © Microsoft 2021
Figures 28-7 through 28-9, 28-14, and 28-15 © 2021 The Linux Foundation
Figures 28-12 and 28-13 © 1992-2020 Cisco
Figure 28-16 © 2021 NXLog Ltd
Figure 28-20 © 2021 SolarWinds Worldwide, LLC
Figure 28-21 © 2003-2021 sFlow.org
Figure 28-22 © Plixer, LLC
Figure 28-23 © Microsoft 2021
Figures 29-1 and 29-2 © Microsoft 2021
Figure 33-1 © Microsoft 2021

CHAPTER 7

Summarizing the Techniques Used in Security Assessments

This chapter starts by introducing threat hunting and how the threat-hunting process leverages threat intelligence. Then you learn about vulnerability management tasks, such as keeping up with security advisories and performing vulnerability scans. You also learn about the importance of collecting logs (such as system logs [syslogs]) and analyzing those logs in a Security Information and Event Management (SIEM) system. In addition, you learn how security tools and solutions have evolved to provide Security Orchestration, Automation, and Response (SOAR) capabilities to better defend your network, your users, and your organizations overall.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Chapter Review Activities" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 7-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 7-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Threat Hunting	1–3
Vulnerability Scans	4–6
Syslog and Security Information and Event Management (SIEM)	7–8
Security Orchestration, Automation, and Response (SOAR)	9–10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What is the act of proactively and iteratively looking for threats in your organization that may have bypassed your security controls and monitoring capabilities?
   a. Threat intelligence
   b. Threat hunting
   c. Threat binding
   d. None of these answers are correct.

2. Which of the following provides a matrix of adversary tactics, techniques, and procedures that modern attackers use?
   a. ATT&CK
   b. CVSS
   c. CVE
   d. All of these answers are correct.

3. Which identifier is assigned to disclosed vulnerabilities?
   a. CVE
   b. CVSS
   c. ATT&CK
   d. TTP

4. Which broad term describes a situation in which a security device triggers an alarm, but no malicious activity or actual attack is taking place?
   a. False negative
   b. True negative
   c. False positive
   d. True positive

5. Which of the following is a successful identification of a security attack or a malicious event?
   a. True positive
   b. True negative
   c. False positive
   d. False negative

6. Which of the following occurs when a vulnerability scanner logs in to the targeted system to perform deep analysis of the operating system, running applications, and security misconfigurations?
   a. Credentialed scan
   b. Application scan
   c. Noncredentialed scan
   d. None of these answers are correct.

7. Which of the following are functions of a SIEM?
   a. Log collection
   b. Log normalization
   c. Log correlation
   d. All of these answers are correct.

8. Which solution allows security analysts to collect network traffic metadata?
   a. NetFlow
   b. SIEM
   c. SOAR
   d. None of these answers are correct.

9. Which solution provides capabilities that extend beyond traditional SIEMs?
   a. SOAR
   b. CVSS
   c. CVE
   d. IPFIX

10. Which of the following can be capabilities and benefits of a SOAR solution?
    a. Automated vulnerability assessment
    b. SOC playbooks and runbook automation
    c. Orchestration of multiple SOC tools
    d. All of these answers are correct.

Foundation Topics

Threat Hunting

No security product or technology in the world can detect and block all security threats in the continuously evolving threat landscape (regardless of the vendor or how expensive it is). This is why many organizations are tasking senior analysts in their computer security incident response team (CSIRT) and their security operations center (SOC) to hunt for threats that may have bypassed any security controls that are in place. This is why threat hunting exists.

Key Topic

Threat hunting is the act of proactively and iteratively looking for threats in your organization. This chapter covers details about threat-hunting practices, the operational challenges of a threat-hunting program, and the benefits of a threat-hunting program.

The threat-hunting process requires deep knowledge of the network and often is performed by SOC analysts (otherwise known as investigators, threat hunters, tier 2 or tier 3 analysts, and so on). Figure 7-1 illustrates the traditional SOC tiers and where threat hunters typically reside. In some organizations (especially small organizations), threat hunting could be done by anyone in the SOC because the organization may not have a lot of resources (analysts). The success of threat hunting completely depends on the maturity of the organization and the resources available.

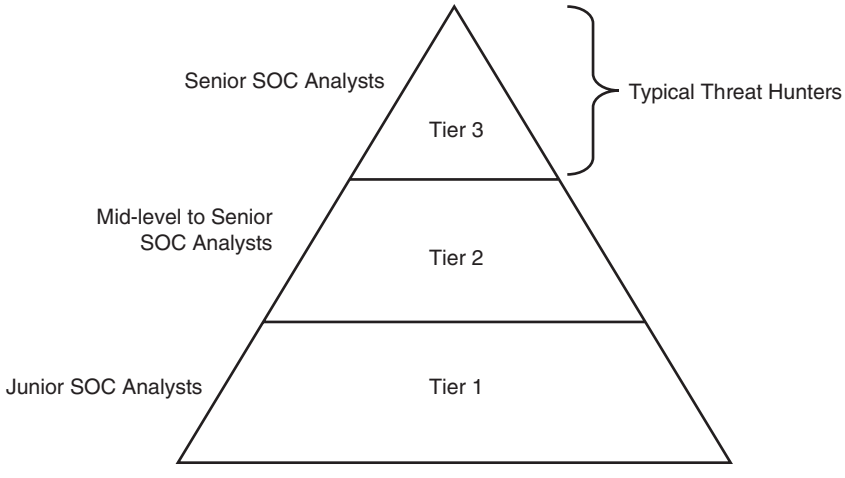


FIGURE 7-1 The SOC Tiers

Some organizations might have a dedicated team within or outside the SOC to perform threat hunting. However, one of the common practices is to have the hunters embedded within the SOC.

Threat hunters assume that an attacker has already compromised the network. Consequently, they need to come up with a hypothesis of what is compromised and how an adversary could have performed the attack. For the threat hunting to be successful, hunters need to be aware of the adversary tactics, techniques, and procedures (TTPs) that modern attackers use. This is why many organizations use MITRE's ATT&CK framework to be able to learn about the tactics and techniques of adversaries. Later in this chapter you learn more about how MITRE's ATT&CK can be used in threat hunting.

Threat hunting is not a new concept. Many organizations have performed threat hunting for a long time. However, in the last decade many organizations have adopted new ways to enhance the threat-hunting process with automation and orchestration.

Threat hunting is not the same as the traditional SOC incident response (reactive) activities. Threat hunting is also not the same as vulnerability management (the process of patching vulnerabilities across the systems and network of your organization, including cloud-based applications in some cases). However, some of the same tools and capabilities may be shared among threat hunters, SOC analysts, and vulnerability management teams. Tools and other capabilities such as data analytics, TTPs, vulnerability feeds, and ***threat feeds*** may be used across the different teams and analysts in an organization.

A high-level threat-hunting process includes the following steps:

Step 1. Threat hunting starts with a trigger based on an anomaly, threat intelligence, or a hypothesis (what could an attacker have done to the organization?). From that moment you should ask yourself: "Do we really need to perform this threat-hunting activity?" or "What is the scope?"

Step 2. Then you identify the necessary tools and methodologies to conduct the hunt.

Step 3. Once the tools and methodologies are identified, you reveal new attack patterns, TTPs, and so on.

Step 4. You refine your hunting tactics and enrich them using data analytics. Steps 2–3 can take one cycle or be iterative and involve multiple loops (depending on what you find and what additional data and research need to be done).

Step 5. A successful outcome could be that you identify and mitigate the threat. However, you need to recognize that in some cases this may not be the case. You may not have the necessary tools and capabilities, or there was no actual threat. This is why the success of your hunting program depends on the maturity of your capabilities and organization as a whole.

You can measure the maturity of your threat-hunting program within your organization in many ways. Figure 7-2 shows a matrix that can be used to evaluate the maturity level of your organization against different high-level threat-hunting elements.

These threat-hunting maturity levels can be categorized as easily as level 1, 2, and 3, or more complex measures can be used.

When it comes to threat intelligence and threat hunting, automation is key! Many organizations are trying to create threat ***intelligence fusion*** techniques to automatically extract threat intelligence data from heterogeneous sources to analyze such data. The goal is for the threat hunter and network defender to maneuver quickly—and faster than the attacker. This way, you can stay one step ahead of threat actors and be able to mitigate the attack.

Security Advisories and Bulletins

Key Topic

In Chapter 5, "Understanding Different Threat Actors, Vectors, and Intelligence Sources," you learned how vendors, coordination centers, security researchers, and others publish ***security advisories*** and bulletins to disclose vulnerabilities. Most of the vulnerabilities disclosed to the public are assigned ***Common Vulnerability and Exposure (CVE)*** identifiers. CVE is a standard created by MITRE (www.mitre.org) that provides a mechanism to assign an identifier to vulnerabilities so that you can correlate the reports of those vulnerabilities among sites, tools, and feeds.

NOTE You can obtain additional information about CVE at https://cve.mitre.org.

One of the most comprehensive and widely used vulnerability databases is the National Vulnerability Database (NVD) maintained by the National Institute of Standards and Technology (NIST). NVD provides information about vulnerabilities disclosed worldwide.

NOTE You can access the NVD and the respective vulnerability feeds at https://nvd.nist.gov.

Threat Hunting High-level Elements	Threat Hunting Maturity Level: Initial (Minimal) Level 1	Intermediate Level 2	Innovative and Leading Level 3
Threat Intelligence and Data Collection	Limited access of threat intelligence and collection of data	High collection of certain types of threat intelligence and data	High collection of many types of threat intelligence and data
Hypothesis Creation	Responds only to existing SIEM, IPS/IDS, firewall logs, etc.	Combines traditional logs with TTPs and threat intelligence	Combines traditional logs with TTPs and threat intelligence and develops automated threat risk scoring
Tools and Techniques for Hunting Hypothesis Testing	Reactive alerts and SIEM searches	Simple tools and analytics leveraging some visualizations, but mostly a manual effort	Advanced search capabilities, visualizations, creating new tools and not depending on traditional tools
TTP Detection	None, only traditional SIEM reactive detection	Identification of indicators of compromise (IoCs) and new attack trends	Able to detect adversary TTPs, IoCs, and create automation for the SOC to routinely detect them in the future
Analytics and Automation	None	Limited analytics and automation	Create automated tools for the SOC to routinely detect threats in the future

FIGURE 7-2 Threat-Hunting Maturity

Most mature vendors such as Microsoft, Intel, and Cisco publish security advisories and bulletins in their websites and are CVE Numbering Authorities (CNAs). CNAs can assign CVEs to disclosed vulnerabilities and submit the information to MITRE and subsequently to NVD.

NOTE You can find additional information about CNAs at https://cve.mitre.org/cve/cna.html.

The following links include examples of security advisories and bulletins published by different vendors:

- **Cisco:** https://www.cisco.com/go/psirt
- **Microsoft:** https://www.microsoft.com/en-us/msrc
- **Red Hat:** https://access.redhat.com/security/security-updates
- **Palo Alto:** https://security.paloaltonetworks.com

Vulnerability disclosures in security advisories are often coordinated among multiple vendors. Most of the products and applications developed nowadays use open-source software. Vulnerabilities in open-source software could affect hundreds or thousands of products and applications in the industry. In addition, vulnerabilities in protocols such as TLS, TCP, BGP, OSPF, and WPA could also affect numerous products and software. Patching open-source and protocol-related vulnerabilities among upstream and downstream vendors is not an easy task and requires good coordination. Figure 7-3 shows the high-level process of a coordinated vulnerability disclosure and underlying patching.

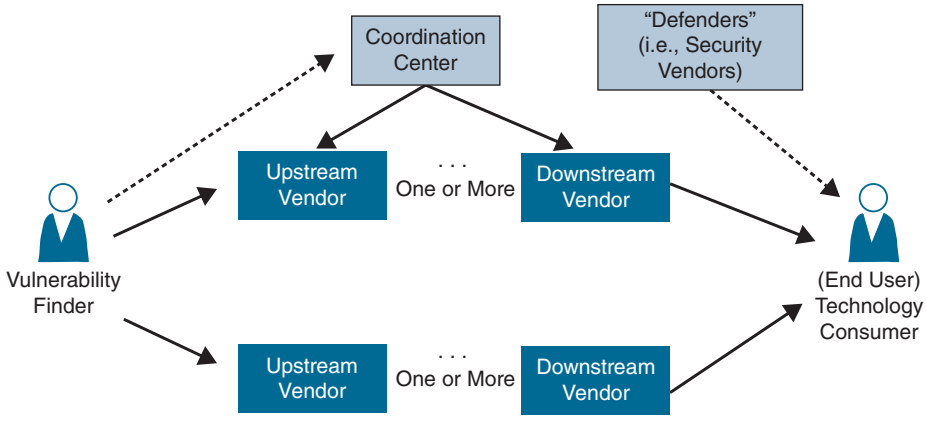


FIGURE 7-3 Coordinated Vulnerability Disclosures

The following steps are illustrated in Figure 7-3:

1. The finder (this can be anyone—a security researcher, customer, security company, an internal employee of a vendor) finds a security vulnerability and reports it to a vendor. The finder can also contact a vulnerability coordination center (such as www.cert.org) to help with the coordination and disclosure.
2. The upstream vendors triage and patch the vulnerability.
3. There could be one or more downstream vendors that also need to patch the vulnerability. In some cases, the coordination center may also interact with downstream vendors in the notification.
4. Security vendors (such as antivirus/antimalware, intrusion detection, and prevention technology providers) may obtain information about the vulnerability and create signatures or any other capabilities to help the end user detect and mitigate an attack caused by the vulnerability.
5. The end user is notified of the patch and the vulnerability.

TIP The preceding process can take days, weeks, months, or even years! Although this process looks very simple in an illustration like the one in Figure 7-3, it is very complicated in practice. For this reason, the Forum of Incident Response and Security Teams (FIRST) has created a Multi-Party Coordination and Disclosure special interest group (SIG) to help address these challenges. You can obtain details about guidelines and practices for multiparty vulnerability coordination and disclosure at https://www.first.org/global/sigs/vulnerability-coordination/multiparty/.

Vulnerability Scans

Vulnerability management teams often use other tools such as vulnerability scanners and software composition analysis (SCA) tools. Figure 7-4 illustrates how a typical automated vulnerability scanner works.

The following are the steps illustrated in Figure 7-4. Keep in mind that vulnerability scanners are all different, but most follow a process like this:

1. In the discovery phase, the scanner uses a tool such as Nmap to perform host and port enumeration. Using the results of the host and port enumeration, the scanner begins to probe open ports for more information.
2. When the scanner has enough information about the open port to determine what software and version are running on that port, it records that information in a database for further analysis. The scanner can use various methods to make this determination, including banner information.

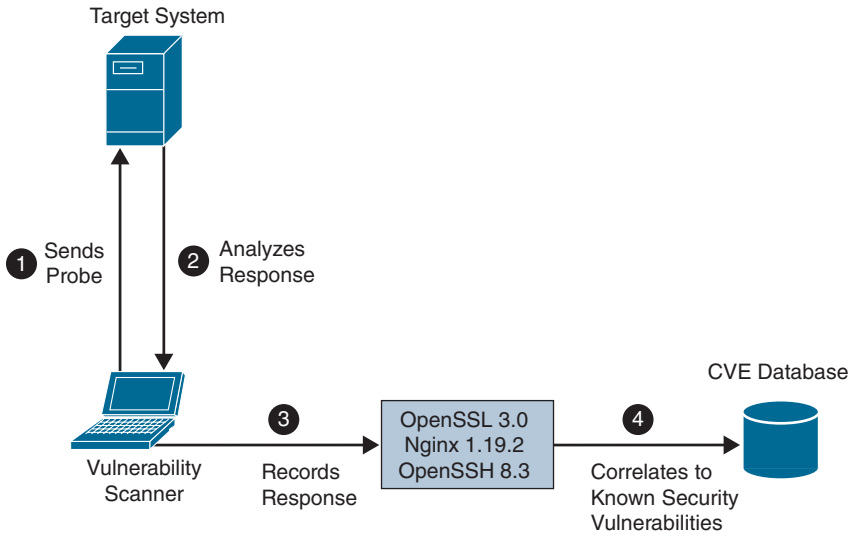


FIGURE 7-4 Coordinated Vulnerability Disclosures

3. The scanner tries to determine if the software that is listening on the target system is susceptible to any known vulnerabilities. It does this by correlating a database of known vulnerabilities against the information recorded in the database about the target services.
4. The scanner produces a report on what it suspects could be vulnerable. Keep in mind that these results are often false positives and need to be validated.

Key Topic

One of the main challenges with automated vulnerability scanners is the number of false positives and false negatives. ***False positive*** is a broad term that describes a situation in which a security device triggers an alarm, but no malicious activity or actual attack is taking place. In other words, false positives are false alarms, and they are also called benign triggers. False positives are problematic because by triggering unjustified alerts, they diminish the value and urgency of real alerts. Having too many false positives to investigate becomes an operational nightmare, and you most definitely will overlook real security events.

There are also ***false negatives***, which is the term used to describe a network intrusion device's inability to detect true security events under certain circumstances—in other words, a malicious activity that is not detected by the security device.

A ***true positive*** is a successful identification of a security attack or a malicious event. A ***true negative*** occurs when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.

There are also different types of vulnerability scanners:

- ***Application scanners*:** Used to assess application-specific vulnerabilities and operate at the upper layers of the OSI model
- ***Web application scanners*:** Used to assess web applications and web services (such as APIs)
- ***Network and port scanners*:** Used to determine what TCP or UDP ports are open on the target system

Key Topic

Credentialed vs. Noncredentialed

To reduce the number of false positives, some vulnerability scanners have the capability to log in to a system to perform additional tests and see what programs, applications, and open-source software may be running on a targeted system. These scanners can also ***review logs*** on the target system. They can also perform ***configuration reviews*** to determine if a system may be configured in an unsecure way.

Key Topic

Intrusive vs. Nonintrusive

Vulnerability scanners sometimes can send numerous IP packets at a very fast pace (***intrusive***) to the target system. These IP packets can potentially cause negative effects and even crash the application or system. Some scanners can be configured in such a way that you can throttle the probes and IP packets that it sends to the target system in order to be ***nonintrusive*** and to not cause any negative effects in the system.

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (or ***CVSS***) is an industry standard used to convey information about the severity of vulnerabilities. In CVSS, a vulnerability is evaluated under three aspects, and a score is assigned to each of them. These three aspects (or groups) are the base, temporal, and environmental groups.

- The ***base group*** represents the intrinsic characteristics of a vulnerability that are constant over time and do not depend on a user-specific environment. This is the most important information and the only mandatory information to obtain for a vulnerability score.
- The ***temporal group*** assesses the vulnerability as it changes over time.
- The ***environmental group*** represents the characteristic of a vulnerability taking into account the organization's environment.

The CVSS score is obtained by taking into account the base, temporal, and environmental group information. The score for the base group is between 0 and 10, where 0 is the least severe and 10 is assigned to highly critical vulnerabilities (for example, for vulnerabilities that could allow an attacker to remotely compromise a system and get full control). Additionally, the score comes in the form of a vector string that identifies each of the components used to make up the score. The formula used to obtain the score takes into account various characteristics of the vulnerability and how the attacker is able to leverage these characteristics. CVSS defines several characteristics for the base, temporal, and environmental groups.

TIP You can read and refer to the latest CVSS specification documentation, examples of scored vulnerabilities, and a calculator at www.first.org/cvss.

The base group defines exploitability metrics that measure how the vulnerability can be exploited, and impact metrics that measure the impact on confidentiality, integrity, and availability. In addition to these two, a metric called scope change (S) is used to convey the impact on systems that are affected by the vulnerability but do not contain vulnerable code.

Exploitability metrics include the following:

- **Attack Vector (AV):** Represents the level of access an attacker needs to have to exploit a vulnerability. It can assume four values:
  - Network (N)
  - Adjacent (A)
  - Local (L)
  - Physical (P)
- **Attack Complexity (AC):** Represents the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. The values can be one of the following:
  - Low (L)
  - High (H)
- **Privileges Required (PR):** Represents the level of privileges an attacker must have to exploit the vulnerability. The values are as follows:
  - None (N)
  - Low (L)
  - High (H)

- **User Interaction (UI):** Captures whether user interaction is needed to perform an attack. The values are as follows:
  - None (N)
  - Required (R)
- **Scope (S):** Captures the impact on systems other than the system being scored. The values are as follows:
  - Unchanged (U)
  - Changed (C)

The Impact metrics include the following:

- **Confidentiality Impact (C):** Measures the degree of impact to the confidentiality of the system. It can assume the following values:
  - Low (L)
  - Medium (M)
  - High (H)
- **Integrity Impact (I):** Measures the degree of impact to the integrity of the system. It can assume the following values:
  - Low (L)
  - Medium (M)
  - High (H)
- **Availability Impact (A):** Measures the degree of impact to the availability of the system. It can assume the following values:
  - Low (L)
  - Medium (M)
  - High (H)

The temporal group includes three metrics:

- **Exploit code maturity (E):** Measures whether or not public exploits are available

- **Remediation Level (RL):** Indicates whether a fix or workaround is available
- **Report Confidence (RC):** Indicates the degree of confidence in the existence of the vulnerability

The environmental group includes two main metrics:

- **Security Requirements (CR, IR, AR):** Indicate the importance of confidentiality, integrity, and availability requirements for the system
- **Modified Base Metrics (MAV, MAC, MAPR, MUI, MS, MC, MI, MA):** Allow the organization to tweak the base metrics based on specific characteristics of the environment

For example, a vulnerability that could allow a remote attacker to crash the system by sending crafted IP packets would have the following values for the base metrics:

- Access Vector (AV) would be Network because the attacker can be anywhere and can send packets remotely.
- Attack Complexity (AC) would be Low because it is trivial to generate malformed IP packets.
- Privilege Required (PR) would be None because no privileges are required by the attacker on the target system.
- User Interaction (UI) would also be None because the attacker does not need to interact with any user of the system in order to carry out the attack.
- Scope (S) would be Unchanged if the attack does not cause other systems to fail.
- Confidentiality Impact (C) would be None because the primary impact is on the availability of the system.
- Integrity Impact (I) would be None because the primary impact is on the availability of the system.
- Availability Impact (A) would be High because the device becomes completely unavailable while crashing and reloading.

CVSS also defines a mapping between a CVSS Base Score quantitative value and a qualitative score. Table 7-2 provides the qualitative-to-quantitative score mapping.

Table 7-2 Qualitative-to-Quantitative Score Mapping

Rating	CVSS Base Score
None	0.0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

TIP Organizations can use the CVSS score as input to their own risk management processes to evaluate the risk related to a vulnerability and then prioritize the vulnerability remediation.

Logs and Security Information and Event Management (SIEM)

Key Topic

Security Information and Event Management (SIEM) is a specialized device or software used for ***security monitoring***; it collects, correlates, and helps security analysts analyze logs from multiple systems. SIEM typically allows for the following functions:

- **Log collection:** This includes receiving information from devices with multiple protocols and formats, storing the logs, and providing historical reporting and log filtering. A ***log collector*** is software that is able to receive logs from multiple sources (***data input***) and in some cases offers storage capabilities and log analysis functionality.
- **Log normalization:** This function extracts relevant attributes from logs received in different formats and stores them in a common data model or template. This allows for faster event classification and operations. Non-normalized logs are usually kept for archive, historical, and forensic purposes.
- ***Log aggregation*:** This function aggregates information based on common information and reduces duplicates.
- **Log correlation:** This is probably one of the most important SIEM functions. It refers to the capability of the system to associate events gathered by various systems, in different formats and at different times, and create a single actionable event for the security analyst or investigator. Often the quality of SIEM is related to the quality of its correlation engine.

- **Reporting:** Event visibility is also a key functionality of SIEM. Reporting capabilities usually include real-time monitoring and historical base reports.

Most modern SIEMs also integrate with other information systems to gather additional contextual information to feed the correlation engine. For example, they can integrate with an identity management system to get contextual information about users or with NetFlow collectors to get additional flow-based information.

NOTE NetFlow is a technology created by Cisco to collect network metadata about all the different "flows" of traffic on your network. There's also the Internet Protocol Flow Information Export (***IPFIX***), which is a network flow standard led by the Internet Engineering Task Force (IETF). IPFIX was designed to create a common, universal standard of export for flow information from routers, switches, firewalls, and other infrastructure devices. IPFIX defines how flow information should be formatted and transferred from an exporter to a collector. IPFIX is documented in RFC 7011 through RFC 7015 and RFC 5103. Cisco NetFlow Version 9 is the basis and main point of reference for IPFIX. IPFIX changes some of the terminologies of NetFlow, but in essence they are the same principles of NetFlow Version 9.

Several commercial SIEM systems are available. Here's a list of some commercial SIEM solutions:

- Micro Focus ArcSight
- LogRhythm
- IBM QRadar
- Splunk

Figure 7-5 shows how SIEM can collect and process logs from routers, network switches, firewalls, intrusion detection, and other security products that may be in your infrastructure. It can also collect and process logs from applications, antivirus, antimalware, and other host-based security solutions.

Security operation center analysts and security engineers often collect ***packet captures*** during the investigation of a security incident. Packet captures provide the greatest detail about each transaction happening in the network. Full packet capture has been used for digital forensics for many years. However, most malware and attackers use encryption to be able to bypass and obfuscate their transactions. IP packet metadata can still be used to potentially detect an attack and determine the attacker's tactics and techniques.

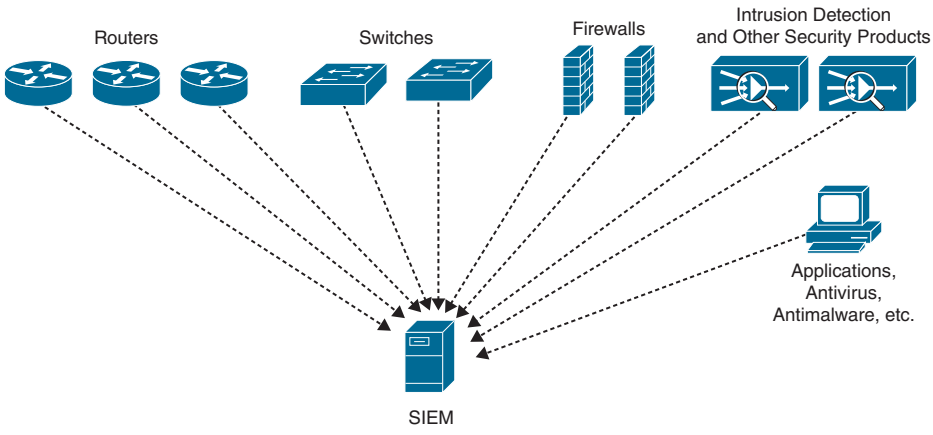


FIGURE 7-5 SIEM Collecting and Processing Logs from Disparate Systems

One of the drawbacks of collecting full packet captures in every corner of your network is the requirement for storage because packet captures in busy networks can take a significant amount of disk space. This is why numerous organizations often collect network metadata with NetFlow or IPFIX and store such data longer than when collecting packet captures.

Several sophisticated security tools also provide ***user behavior analysis*** mechanisms in order to potentially find insiders (internal attackers). Similarly, they provide insights of user behavior even if they do not present a security threat.

Organizations can also deploy ***sentiment analysis*** tools and solutions to help monitor customer sentiment and brand reputation. Often these tools can also reveal the intent and tone behind social media posts, as well as keep track of positive or negative opinions. Threat actors can also try to damage a company's reputation by creating fake accounts and bots in social media platforms like Twitter, Facebook, or Instagram. Attackers can use these fake accounts and bots to provide negative public comments against the targeted organization.

Security Orchestration, Automation, and Response (SOAR)

Key Topic

CSIRT analysts typically work in an SOC utilizing many tools to monitor events from numerous systems (firewalls, applications, IPS, DLP, endpoint security solutions, and so on). Typically, these logs are aggregated in a SIEM. Modern SOCs also use ***Security Orchestration, Automation, and Response (SOAR)*** systems that extend beyond traditional SIEMs.

The tools in the SOC are evolving and so are the methodologies. For example, now security analysts not only respond to basic cyber events but also perform threat hunting in their organizations. SOAR is a set of solutions and integrations designed to allow organizations to collect security threat data and alerts from multiple sources. SOAR platforms take the response capabilities of SIEM to the next level. SOAR solutions supplement, rather than replace, the SIEM. They allow the cybersecurity team to extend its reach by automating the routine work of cybersecurity operations.

TIP Unlike traditional SIEM platforms, SOAR solutions can also be used for threat and vulnerability management, security incident response, and security operations automation.

Deploying SOAR and SIEM together in solutions makes the life of SOC analysts easier. SOAR platforms accelerate incident response detection and eradication times because they can automatically communicate information collected by SIEM with other security tools. Several traditional SIEM vendors are changing their products to offer hybrid SOAR/SIEM functionality.

Another term adopted in the cybersecurity industry is Extended Detection and Response (XDR). XDR is a series of systems working together that collects and correlates data across hosts, mobile devices, servers, cloud workloads, email messages, web content, and networks, enabling visibility and context into advanced threats. The goal of an XDR system is to allow security analysts to analyze, prioritize, hunt, and remediate cybersecurity threats to prevent data loss and security breaches.

Chapter Review Activities

Use the features in this section to study and review the topics in this chapter.

Review Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 7-3 lists a reference of these key topics and the page number on which each is found.

Key Topic

Table 7-3 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Paragraph	Defining threat hunting	175
Paragraph	Understanding security advisories, bulletins, and what a CVE is	177
Paragraph	Understanding false positives and false negatives	181
Section	Credentialed vs. Noncredentialed	182
Section	Intrusive vs. Nonintrusive	182
Paragraph	Defining what SIEM is	186
Paragraph	Understanding the SOAR concept	188

Define Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

threat hunting, threat feeds, intelligence fusion, security advisories, Common Vulnerability and Exposures (CVE), false positives, false negatives, true positive, true negative, application scanners, web application scanners, network and port scanners, review logs, configuration reviews, intrusive, nonintrusive, CVSS, base group, temporal group, environmental group, Security Information and Event Management (SIEM), security monitoring, log collector, data input, Log aggregation, IPFIX, packet captures, user behavior analysis, sentiment analysis, Security Orchestration, Automation, and Response (SOAR)

Review Questions

Answer the following review questions. Check your answers with the answer key in Appendix A.

1. What type of vulnerability scanner can be used to assess vulnerable web services?
2. What documents do vendors, vulnerability coordination centers, and security researchers publish to disclose security vulnerabilities?
3. What term is used to describe an organization that can assign CVEs to vulnerabilities?

4. What public database can anyone use to obtain information about security vulnerabilities affecting software and hardware products?
5. How many score "groups" are supported in CVSS?
6. A vulnerability with a CVSS score of 4.9 is considered a _____ severity vulnerability.
7. What is the process of iteratively looking for threats that may have bypassed your security controls?

Index

Symbols

A

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z