CCNA Cyber Ops

SECFND 210-250

Official Cert Guide

OMAR SANTOS, CISSP No. 463598
JOSEPH MUNIZ, CISSP No. 344594
STEFANO DE CRESCENZO CCIE No. 26025, CISSP 406579

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Cyber Ops SECFND 210-250 Official Cert Guide

Omar Santos
Joseph Muniz
Stefano De Crescenzo

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

1 17

Library of Congress Control Number: 2017931952

ISBN-10: 1-58714-702-5

ISBN-13: 978-1-58714-702-9

Warning and Disclaimer

This book is designed to provide information about the CCNA Cyber Ops SECFND #210-250 exam. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the United States, please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Ron Fligge

Product Line Manager: Brett Bartow

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Technical Editors: Pavan Reddy, Ron Taylor

Development Editor: Christopher Cleveland

Copy Editor: Bart Reed

Project Editor: Mandie Frank

Designer: Chuti Prasertsith

Composition: Tricia Bronkella

Editorial Assistant: Vanessa Evans

Indexer: Ken Johnson

Proofreader: The Wordsmithery LLC

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Authors

Omar Santos is an active member of the cyber security community, where he leads several industry-wide initiatives and standards bodies. 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.

Omar is the author of over a dozen 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), where he mentors and leads engineers and incident managers during the investigation and resolution of cyber security vulnerabilities. Additional information about Omar's current projects can be found at omarsantos.io, and you can follow Omar on Twitter @santosomar.

Joseph Muniz is an architect at Cisco Systems and security researcher. He has extensive experience in designing security solutions and architectures for the top Fortune 500 corporations and the U.S. government. Joseph's current role gives him visibility into the latest trends in cyber security, from both leading vendors and customers. Examples of Joseph's research include his RSA talk titled "Social Media Deception," which has been quoted by many sources (search for "Emily Williams Social Engineering"), as well as his articles in *PenTest Magazine* regarding various security topics.

Joseph runs The Security Blogger website, a popular resource for security, hacking, and product implementation. He is the author and contributor of several publications covering various penetration testing and security topics. You can follow Joseph at www.thesecurityblogger.com and @SecureBlogger.

Stefano De Crescenzo is a senior incident manager with the Cisco Product Security Incident Response Team (PSIRT), where he focuses on product vulnerability management and Cisco products forensics. He is the author of several blog posts and white papers about security best practices and forensics. He is an active member of the security community and has been a speaker at several security conferences.

Stefano specializes in malware detection and integrity assurance in critical infrastructure devices, and he is the author of integrity assurance guidelines for Cisco IOS, IOS-XE, and ASA.

Stefano holds a B.Sc. and M.Sc. in telecommunication engineering from Politecnico di Milano, Italy, and an M.Sc. in telecommunication from Danish Technical University, Denmark. He is currently pursuing an Executive MBA at Vlerick Business School in Belgium. He also holds a CCIE in Security #26025 and is CISSP and CISM certified.

About the Technical Reviewers

Pavan Reddy serves as a Security Principal in Cisco Security Services. Pavan has 20+ years of security and network consulting experience in Financial Services, Healthcare, Service Provider, and Retail arenas. Recent projects cover Technical Security Strategy and Architecture, Network Segmentation Strategy, Threat Intelligence Analytics, Distributed Denial-of-Service Mitigation Architectures, and DNS Architecture and Security. Pavan holds multiple CCIEs and BS in Computer Engineering.

Ron Taylor has been in the Information Security field for almost 20 years. Ten of those years were spent in consulting where he gained experience in many areas. In 2008, he joined the Cisco Global Certification Team as an SME in Information Assurance. In 2012, he moved into a position with the Security Research & Operations group (PSIRT), 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. Additionally, he provided consulting support to many product teams as an SME on product security testing. In his current role, he is a Consulting Systems Engineer specializing in Cisco's security product line. Certifications include GPEN, GWEB, GCIA, GCIH, GWAPT, RHCE, CCSP, CCNA, CISSP, and MCSE. Ron is also a Cisco Security Blackbelt, SANS mentor, Cofounder and President of the Raleigh BSides Security Conference, and a member of the Packet Hacking Village team at Defcon.

Dedications

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.

I also dedicate this book to my father, Jose, and to the memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

—Omar Santos

I would like to dedicate this book to the memory of my father, Raymond Muniz. He never saw me graduate from college or accomplish great things, such as writing this book. I would also like to apologize to him for dropping out of soccer in high school. I picked it back up later in life, and today play in at least two competitive matches a week. Your hard work paid off. Hopefully you somehow know that.

—Joseph Muniz

This book is dedicated to my wife, Nevena, and my beautiful daughters, Sara and Tea, who supported and inspired me during the development of this book. Specifically, Tea was born a few weeks before I started writing my first chapter, so she is especially connected with this book.

I would also like to mention my whole family: my mother, Mariagrazia, and my sister, Francesca, who supported my family and me while I was away writing. I also dedicate this book to the memory of my father, Cataldo.

—Stefano De Crescenzo

Acknowledgments

I would like to thank the technical editors, Pavan Reddy and Ron Taylor, for their time and technical expertise. They verified our work and contributed to the success of this book. I would also like to thank the Cisco Press team, especially Mary Beth Ray, Denise Lincoln, and Christopher Cleveland, for their patience, guidance, and consideration. Their efforts are greatly appreciated. Finally, I would like to acknowledge the Cisco Security Research and Operations teams, Cisco Advanced Threat Analytics, and Cisco Talos. Several leaders in the network security industry work there, supporting our Cisco customers, often under very stressful conditions, and working miracles daily. They are truly unsung heroes, and I am honored to have had the privilege of working side by side with them in the trenches while protecting customers and Cisco.

—Omar Santos

I would first like to thank Omar and Stefano for including me on this project. I really enjoyed working with these guys and hope we can do more in the future. I also would like to thank the Cisco Press team and technical editors, Pavan Reddy and Ron Taylor, for their fantastic support in making the writing process top quality and easy for everybody. Hey, Ron, you got this and the CTR comic. 2016 was great for you, Mr. Green.

I would also like to thank all the great people in my life who make me who I am.

Finally, a message for Raylin Muniz (age 7): Hopefully one day you can accomplish your dreams like I have with this book.

—Joseph Muniz

I would like to thank Omar and Joey for being fantastic mates in the development of this book. A special mention goes to my wife as well, for supporting me throughout this journey and for helping me by reviewing my work.

Additionally, this book wouldn't have been possible without the help of the Cisco Press team and in particular of Chris Cleveland. His guidance has been very precious. A big thanks goes to the technical reviewers, Pavan and Ron. Thanks for keeping me honest and to the point! A big thanks also to Eric Vyncke for his numerous suggestions.

—Stefano De Crescenzo

Contents at a Glance

Part VII Appendixes

Elements Available on the Book Website

Contents

Elements Available on the Book Website

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Congratulations! If you are reading this, you have in your possession a powerful tool that can help you to:

- Improve your awareness and knowledge of cyber security fundamentals
- Increase your skill level related to the implementation of that security
- Prepare for the CCNA Cyber Ops SECFND certification exam

Whether you are preparing for the CCNA Cyber Ops certification or just changing careers to cyber security, this book will help you gain the knowledge you need to get started and prepared. When writing this book, we did so with you in mind, and together we will discover the critical ingredients that make up the recipe for a secure network and how to succeed in cyber security operations. By focusing on covering the objectives for the CCNA Cyber Ops SECFND exam and integrating that with real-world best practices and examples, we created this content with the intention of being your personal tour guides as we take you on a journey through the world of network security.

The CCNA Cyber Ops: Understanding Cisco Cybersecurity Fundamentals (SECFND) 210-250 exam is required for the CCNA Cyber Ops certification. This book covers all the topics listed in Cisco's exam blueprint, and each chapter includes key topics and preparation tasks to assist you in mastering this information. Reviewing tables and practicing test questions will help you practice your knowledge in all subject areas.

About the 210-250 CCNA Cyber Ops SECFND Exam

The CCNA Cyber Ops: Understanding Cisco Cybersecurity Fundamentals (SECFND) 210-250 exam is the first of the two required exams to achieve the CCNA Cyber Ops certification and is aligned with the job role of associate-level security operations center (SOC) security analyst. The SECFND exam tests candidates' understanding of cyber security's basic principles, foundational knowledge, and core skills needed to grasp the more advanced associate-level materials in the second required exam: Implementing Cisco Cybersecurity Operations (SECOPS).

The CCNA Cyber Ops: Understanding Cisco Cybersecurity Fundamentals (SECFND) 210-250 exam is a computer-based test that has 55 to 60 questions and a 90-minute time limit. Because all exam information is managed by Cisco Systems and is therefore subject to change, candidates should continually monitor the Cisco Systems site for exam updates at http://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/secfnd.html.

You can take the exam at Pearson VUE testing centers. You can register with VUE at www.vue.com/cisco.

210-250 CCNA Cyber Ops SECFNC Exam Topics

Table I-1 lists the topics of the 210-250 SECFND exam and indicates the chapter in the book where they are covered.

Table I-1 *210-250 SECFND Exam Topics*

Exam Topic	Chapter
1.0 Network Concepts	
1.1 Describe the function of the network layers as specified by the OSI and the TCP/IP network models	Chapter 1
1.2 Describe the operation of the following:	
1.2.a IP	Chapter 1
1.2.b TCP	Chapter 1
1.2.c UDP	Chapter 1
1.2.d ICMP	Chapter 1
1.3 Describe the operation of these network services:	
1.3.a ARP	Chapter 1
1.3.b DNS	Chapter 1
1.3.c DHCP	Chapter 1
1.4 Describe the basic operation of these network device types:	
1.4.a Router	Chapter 1
1.4.b Switch	Chapter 1
1.4.c Hub	Chapter 1
1.4.d Bridge	Chapter 1
1.4.e Wireless access point (WAP)	Chapter 1
1.4.f Wireless LAN controller (WLC)	Chapter 1
1.5 Describe the functions of these network security systems as deployed on the host, network, or the cloud:	
1.5.a Firewall	Chapter 2
1.5.b Cisco Intrusion Prevention System (IPS)	Chapter 2
1.5.c Cisco Advanced Malware Protection (AMP)	Chapter 2
1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS)	Chapter 2
1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security (CES)	Chapter 2
1.6 Describe IP subnets and communication within an IP subnet and between IP subnets	Chapter 1
1.7 Describe the relationship between VLANs and data visibility	Chapter 1
1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices	Chapter 2
1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation	Chapter 2

Exam Topic	Chapter
1.10 Compare and contrast inline traffic interrogation and taps or traffic mirroring	Chapter 2
1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic	Chapter 2
1.12 Identify potential data loss from provided traffic profiles	Chapter 2
2.0 Security Concepts	
2.1 Describe the principles of the defense-in-depth strategy	Chapter 3
2.2 Compare and contrast these concepts:	
2.2.a Risk	Chapter 3
2.2.b Threat	Chapter 3
2.2.c Vulnerability	Chapter 3
2.2.d Exploit	Chapter 3
2.3 Describe these terms:	
2.3.a Threat actor	Chapter 3
2.3.b Runbook automation (RBA)	Chapter 3
2.3.c Chain of custody (evidentiary)	Chapter 3
2.3.d Reverse engineering	Chapter 3
2.3.e Sliding window anomaly detection	Chapter 3
2.3.f PII	Chapter 3
2.3.g PHI	Chapter 3
2.4 Describe these security terms:	
2.4.a Principle of least privilege	Chapter 3
2.4.b Risk scoring/risk weighting	Chapter 3
2.4.c Risk reduction	Chapter 3
2.4.d Risk assessment	Chapter 3
2.5 Compare and contrast these access control models:	
2.5.a Discretionary access control	Chapter 4
2.5.b Mandatory access control	Chapter 4
2.5.c Nondiscretionary access control	Chapter 4
2.6 Compare and contrast these terms:	
2.6.a Network and host antivirus	Chapter 4
2.6.b Agentless and agent-based protections	Chapter 4

Exam Topic	Chapter
2.6.c SIEM and log collection	Chapter 5
2.7 Describe these concepts:	
2.7.a Asset management	Chapter 5
2.7.b Configuration management	Chapter 5
2.7.c Mobile device management	Chapter 5
2.7.d Patch management	Chapter 5
2.7.e Vulnerability management	Chapter 5
3.0 Cryptography	
3.1 Describe the uses of a hash algorithm	Chapter 6
3.2 Describe the uses of encryption algorithms	Chapter 6
3.3 Compare and contrast symmetric and asymmetric encryption algorithms	Chapter 6
3.4 Describe the processes of digital signature creation and verification	Chapter 6
3.5 Describe the operation of a PKI	Chapter 6
3.6 Describe the security impact of these commonly used hash algorithms:	
3.6.a MD5	Chapter 6
3.6.b SHA-1	Chapter 6
3.6.c SHA-256	Chapter 6
3.6.d SHA-512	Chapter 6
3.7 Describe the security impact of these commonly used encryption algorithms and secure communications protocols:	
3.7.a DES	Chapter 6
3.7.b 3DES	Chapter 6
3.7.c AES	Chapter 6
3.7.d AES256-CTR	Chapter 6
3.7.e RSA	Chapter 6
3.7.f DSA	Chapter 6
3.7.g SSH	Chapter 6
3.7.h SSL/TLS	Chapter 6
3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation	Chapter 6
3.9 Describe these items in regard to SSL/TLS:	
3.9.a Cipher-suite	Chapter 6

Exam Topic	Chapter
3.9.b X.509 certificates	Chapter 6
3.9.c Key exchange	Chapter 6
3.9.d Protocol version	Chapter 6
3.9.e PKCS	Chapter 6
4.0 Host-based Analysis	
4.1 Define these terms as they pertain to Microsoft Windows:	
4.1.a Processes	Chapter 8
4.1.b Threads	Chapter 8
4.1.c Memory allocation	Chapter 8
4.1.d Windows Registry	Chapter 8
4.1.e WMI	Chapter 8
4.1.f Handles	Chapter 8
4.1.g Services	Chapter 8
4.2 Define these terms as they pertain to Linux:	
4.2.a Processes	Chapter 9
4.2.b Forks	Chapter 9
4.2.c Permissions	Chapter 9
4.2.d Symlinks	Chapter 9
4.2.e Daemon	Chapter 9
4.3 Describe the functionality of these endpoint technologies in regard to security monitoring:	
4.3.a Host-based intrusion detection	Chapter 10
4.3.b Antimalware and antivirus	Chapter 10
4.3.c Host-based firewall	Chapter 10
4.3.d Application-level whitelisting/blacklisting	Chapter 10
4.3.e Systems-based sandboxing (such as Chrome, Java, Adobe Reader)	Chapter 10
4.4 Interpret these operating system log data to identify an event:	
4.4.a Windows security event logs	Chapter 8
4.4.b Unix-based syslog	Chapter 9
4.4.c Apache access logs	Chapter 9
4.4.d IIS access logs	Chapter 8

Exam Topic	Chapter
5.0 Security Monitoring	
5.1 Identify the types of data provided by these technologies:	
5.1.a TCP Dump	Chapter 11
5.1.b NetFlow	Chapter 11
5.1.c Next-gen firewall	Chapter 11
5.1.d Traditional stateful firewall	Chapter 11
5.1.e Application visibility and control	Chapter 11
5.1.f Web content filtering	Chapter 11
5.1.g Email content filtering	Chapter 11
5.2 Describe these types of data used in security monitoring:	
5.2.a Full packet capture	Chapter 11
5.2.b Session data	Chapter 11
5.2.c Transaction data	Chapter 11
5.2.d Statistical data	Chapter 11
5.2.e Extracted content	Chapter 11
5.2.f Alert data	Chapter 11
5.3 Describe these concepts as they relate to security monitoring:	
5.3.a Access control list	Chapter 12
5.3.b NAT/PAT	Chapter 12
5.3.c Tunneling	Chapter 12
5.3.d TOR	Chapter 12
5.3.e Encryption	Chapter 12
5.3.f P2P	Chapter 12
5.3.g Encapsulation	Chapter 12
5.3.h Load balancing	Chapter 12
5.4 Describe these NextGen IPS event types:	
5.4.a Connection event	Chapter 11
5.4.b Intrusion event	Chapter 11
5.4.c Host or endpoint event	Chapter 11
5.4.d Network discovery event	Chapter 11
5.4.e NetFlow event	Chapter 11

Exam Topic	Chapter
5.5 Describe the function of these protocols in the context of security monitoring:	
5.5.a DNS	Chapter 12
5.5.b NTP	Chapter 12
5.5.c SMTP/POP/IMAP	Chapter 12
5.5.d HTTP/HTTPS	Chapter 12
6.0 Attack Methods	
6.1 Compare and contrast an attack surface and vulnerability	Chapter 13
6.2 Describe these network attacks:	
6.2.a Denial of service	Chapter 13
6.2.b Distributed denial of service	Chapter 13
6.2.c Man-in-the-middle	Chapter 13
6.3 Describe these web application attacks:	
6.3.a SQL injection	Chapter 13
6.3.b Command injections	Chapter 13
6.3.c Cross-site scripting	Chapter 13
6.4 Describe these attacks:	
6.4.a Social engineering	Chapter 13
6.4.b Phishing	Chapter 13
6.4.c Evasion methods	Chapter 13
6.5 Describe these endpoint-based attacks:	
6.5.a Buffer overflows	Chapter 13
6.5.b Command and control (C2)	Chapter 13
6.5.c Malware	Chapter 13
6.5.d Rootkit	Chapter 13
6.5.e Port scanning	Chapter 13
6.5.f Host profiling	Chapter 13
6.6 Describe these evasion methods:	
6.6.a Encryption and tunneling	Chapter 14
6.6.b Resource exhaustion	Chapter 14
6.6.c Traffic fragmentation	Chapter 14
6.6.d Protocol-level misinterpretation	Chapter 14

Exam Topic	Chapter
6.6.e Traffic substitution and insertion	Chapter 14
6.6.f Pivot	Chapter 14
6.7 Define privilege escalation	Chapter 13
6.8 Compare and contrast a remote exploit and a local exploit	Chapter 13

About the CCNA Cyber Ops SECFND 210-250 Official Cert Guide

This book maps to the topic areas of the 210-250 SECFND exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. This book is designed to help you pass the SECFND exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **"Do I Know This Already?" quiz:** Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.
- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter:
  - **Review All the Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The "Review All the Key Topics" activity lists the key topics from the chapter, along with their page numbers.

Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.

- **Complete the Tables and Lists from Memory:** To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the companion website. This document lists only partial information, allowing you to complete the table or list.
- **Define Key Terms:** Although the exam is unlikely to ask you to define a term, the CCNA Cyber Ops exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Q&A:** Confirm that you understand the content you just covered.

- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine, which allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 14 core chapters—Chapters 1 through 14. Chapter 15 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNA Cyber Ops SECFND exam. The core chapters are organized into parts. They cover the following topics:

Part I: Network Concepts

- **Chapter 1: Fundamentals of Networking Protocols and Networking Devices** covers the networking technology fundamentals such as the OSI model and different protocols, including IP, TCP, UDP, ICMP, DNS, DHCP, ARP, and others. It also covers the basic operations of network infrastructure devices such as routers, switches, hubs, wireless access points, and wireless LAN controllers.
- **Chapter 2: Network Security Devices and Cloud Services** covers the fundamentals of firewalls, intrusion prevention systems (IPSs), Advance Malware Protection (AMP), and fundamentals of the Cisco Web Security Appliance (WSA), Cisco Cloud Web Security (CWS), Cisco Email Security Appliance (ESA), and the Cisco Cloud Email Security (CES) service. This chapter also describes the operation of access control lists applied as packet filters on the interfaces of network devices and compares and contrasts deep packet inspection with packet filtering and stateful firewall operations. It provides details about inline traffic interrogation and taps or traffic mirroring. This chapter compares and contrasts the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic.

Part II: Security Concepts

- **Chapter 3: Security Principles** covers the principles of the defense-in-depth strategy and compares and contrasts the concepts of risks, threats, vulnerabilities, and exploits. This chapter also defines threat actor, runbook automation (RBA), chain of custody

(evidentiary), reverse engineering, sliding window anomaly detection, personally identifiable information (PII), protected health information (PHI), as well as the principle of least privilege and how to perform separation of duties. It also covers the concepts of risk scoring, risk weighting, risk reduction, and how to perform overall risk assessments.

- **Chapter 4: Introduction to Access Controls** covers the foundation of access control and management. It provides an overview of authentication, authorization, and accounting principles, and introduces some of the most used access control models, including discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC). Also, this chapter covers the actual implementation of access control, such as AAA protocols, port security, 802.1x, Cisco TrustSec, intrusion prevention and detection, and antimalware.
- **Chapter 5: Introduction to Security Operations Management** covers the foundation of security operations management. Specifically, it provides an overview of identity management, protocol and technologies, asset security management, change and configuration management, mobile device management, event and logging management, including Security Information and Event Management (SIEM) technologies, vulnerability management, and patch management.

Part III: Cryptography

- **Chapter 6: Fundamentals of Cryptography and Public Key Infrastructure (PKI)** covers the different hashing and encryption algorithms in the industry. It provides a comparison of symmetric and asymmetric encryption algorithms and an introduction of public key infrastructure (PKI), the operations of a PKI, and an overview of the IPsec, SSL, and TLS protocols.
- **Chapter 7: Introduction to Virtual Private Networks (VPNs)** provides an introduction to remote access and site-to-site VPNs, different deployment scenarios, and the VPN solutions provided by Cisco.

Part IV: Host-based Analysis

- **Chapter 8: Windows-Based Analysis** covers the basics of how a system running Windows handles applications. This includes details about how memory is used as well as how resources are processed by the operating system. These skills are essential for maximizing performance and securing a Windows system.
- **Chapter 9: Linux- and Mac OS X–Based Analysis** covers how things work inside a UNIX environment. This includes process execution and event logging. Learning how the environment functions will not only improve your technical skills but can also be used to build a strategy for securing these systems.
- **Chapter 10: Endpoint Security Technologies** covers the functionality of endpoint security technologies, including host-based intrusion detection, host-based firewalls, application-level whitelisting and blacklisting, as well as systems-based sandboxing.

Part V: Security Monitoring and Attack Methods

- **Chapter 11: Network and Host Telemetry** covers the different types of data provided by network and host-based telemetry technologies, including NetFlow, traditional and next-generation firewalls, packet captures, application visibility and control, and web

and email content filtering. It also provides an overview of how full packet captures, session data, transaction logs, and security alert data are used in security operations and security monitoring.

- **Chapter 12: Security Monitoring Operational Challenges** covers the different operational challenges, including Tor, access control lists, tunneling, peer-to-peer (P2P) communication, encapsulation, load balancing, and other technologies.
- **Chapter 13: Types of Attacks and Vulnerabilities** covers the different types of cyber security attacks and vulnerabilities and how they are carried out by threat actors nowadays.
- **Chapter 14: Security Evasion Techniques** covers how attackers obtain stealth as well as the tricks used to negatively impact detection and forensic technologies. Topics include encryption, exhausting resources, fragmenting traffic, manipulating protocols, and pivoting within a compromised environment.

Part VI: Final Preparation

- **Chapter 15: Final Preparation** identifies the tools for final exam preparation and helps you develop an effective study plan. It contains tips on how to best use the web-based material to study.

Part VII: Appendixes

- **Appendix A: Answers to the "Do I Know This Already?" Quizzes and Q&A Questions** includes the answers to all the questions from Chapters 1 through 14.
- **Appendix B: Memory Tables** (a website-only appendix) contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exam. This appendix is available in PDF format at the book website; it is not in the printed book.
- **Appendix C: Memory Tables Answer Key** (a website-only appendix) contains the answer key for the memory tables in Appendix B. This appendix is available in PDF format at the book website; it is not in the printed book.
- **Appendix D: Study Planner** is a spreadsheet, available from the book website, with major study milestones, where you can track your progress throughout your study.

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. Enter the ISBN 9781587147029.
3. Answer the challenge question as proof of purchase.
4. Click the "Access Bonus Content" link in the Registered Products section of your account page, to be taken 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 steps, please visit 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.

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 http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.
4. In the My Products tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product.
6. The product will now be listed in your My Products page. 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 the following 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 PearsonITCertification.com/register and entering the ISBN 9781587147029.
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 select **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 allows 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 a specific part in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters 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. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four 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, and 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 exam.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select 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 software, Windows desktop version, simply select the **Tools** tab and select the **Update Application** button. This will ensure you are running the latest version of the software engine.

This chapter covers the following topics:

- Describe the principles of the defense-in-depth strategy.
- What are threats, vulnerabilities, and exploits?
- Describe Confidentiality, Integrity, and Availability.
- Describe risk and risk analysis.
- Define what personally identifiable information (PII) and protected health information (PHI) are.
- What are the principles of least privilege and separation of duties?
- What are security operation centers (SOCs)?
- Describe cyber forensics.

CHAPTER 3

Security Principles

This chapter covers the principles of the defense-in-depth strategy and compares and contrasts the concepts of risk, threats, vulnerabilities, and exploits. This chapter also defines what are threat actors, run book automation (RBA), chain of custody (evidentiary), reverse engineering, sliding window anomaly detection, Personally Identifiable Information (PII), Protected Health Information (PHI), as well as what is the principle of least privilege, and how to perform separation of duties. It also covers concepts of risk scoring, risk weighting, risk reduction, and how to perform overall risk assessments.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you identify your strengths and deficiencies in this chapter's topics. The 11-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time. You can find the answers in Appendix A Answers to the "Do I Know This Already?" Quizzes and Q&A Questions.

Table 3-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 3-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
The Principles of the Defense-in-Depth Strategy	1–2
What Are Threats, Vulnerabilities, and Exploits?	3–6
Risk and Risk Analysis	7
Personally Identifiable Information and Protected Health Information	8
Principle of Least Privilege and Separation of Duties	9
Security Operation Centers	10
Forensics	11

1. What is one of the primary benefits of a defense-in-depth strategy?
   - **a.** You can deploy advanced malware protection to detect and block advanced persistent threats.
   - **b.** You can configure firewall failover in a scalable way.
   - **c.** Even if a single control (such as a firewall or IPS) fails, other controls can still protect your environment and assets.
   - **d.** You can configure intrusion prevention systems (IPSs) with custom signatures and auto-tuning to be more effective in the network.

2. Which of the following planes is important to understand for defense in depth?
   a. Management plane
   b. Failover plane
   c. Control plane
   d. Clustering
   e. User/data plane
   f. Services plane
3. Which of the following are examples of vulnerabilities?
   a. Advanced threats
   b. CVSS
   c. SQL injection
   d. Command injection
   e. Cross-site scripting (XSS)
   f. Cross-site request forgery (CSRF)
4. What is the Common Vulnerabilities and Exposures (CVE)?
   a. An identifier of threats
   b. A standard to score vulnerabilities
   c. A standard maintained by OASIS
   d. A standard for identifying vulnerabilities to make it easier to share data across tools, vulnerability repositories, and security services
5. Which of the following is true when describing threat intelligence?
   a. Threat intelligence's primary purpose is to make money by exploiting threats.
   b. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.
   c. With threat intelligence, threat actors can become more efficient to carry out attacks.
   d. Threat intelligence is too difficult to obtain.
6. Which of the following is an open source feed for threat data?
   a. Cyber Squad ThreatConnect
   b. BAE Detica CyberReveal
   c. MITRE CRITs
   d. Cisco AMP Threat Grid

7. What is the Common Vulnerability Scoring System (CVSS)?
   a. A scoring system for exploits.
   b. A tool to automatically mitigate vulnerabilities.
   c. A scoring method that conveys vulnerability severity and helps determine the urgency and priority of response.
   d. A vulnerability-mitigation risk analysis tool.

8. Which of the following are examples of personally identifiable information (PII)?
   a. Social security number
   b. Biological or personal characteristics, such as an image of distinguishing features, fingerprints, x-rays, voice signature, retina scan, and geometry of the face
   c. CVE
   d. Date of birth

9. Which of the following statements are true about the principle of least privilege?
   a. Principle of least privilege and separation of duties can be considered to be the same thing.
   b. The principle of least privilege states that all users—whether they are individual contributors, managers, directors, or executives—should be granted only the level of privilege they need to do their job, and no more.
   c. Programs or processes running on a system should have the capabilities they need to "get their job done," but no root access to the system.
   d. The principle of least privilege only applies to people.

10. What is a runbook?
    a. A runbook is a collection of processes running on a system.
    b. A runbook is a configuration guide for network security devices.
    c. A runbook is a collection of best practices for configuring access control lists on a firewall and other network infrastructure devices.
    d. A runbook is a collection of procedures and operations performed by system administrators, security professionals, or network operators.

11. Chain of custody is the way you document and preserve evidence from the time you started the cyber forensics investigation to the time the evidence is presented at court. Which of the following is important when handling evidence?
    a. Documentation about how and when the evidence was collected
    b. Documentation about how evidence was transported
    c. Documentation about who had access to the evidence and how it was accessed
    d. Documentation about the CVSS score of a given CVE

Foundation Topics

In this chapter, you will learn the different cyber security principles, including what threats, vulnerabilities, and exploits are. You will also learn details about what defense in depth is and how to perform risk analysis. This chapter also provides an overview of what runbooks are and how to perform runbook automation (RBA).

When you are performing incident response and forensics tasks, you always have to be aware of how to collect evidence and what the appropriate evidentiary chain of custody is. This chapter provides an overview of chain of custody when it pertains to cyber security investigations. You will learn the details about reverse engineering, forensics, and sliding window anomaly detection. You will also learn what personally identifiable information (PII) and protected health information (PHI) are, especially pertaining to different regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

In this chapter, you will also learn the concepts of principle of least privilege. It is important to know how to perform risk scoring and risk weighting in the realm of risk assessment and risk reduction. This chapter provides an overview of these risk assessment and risk reduction methodologies.

The Principles of the Defense-in-Depth Strategy

If you are a cyber security expert, or even an amateur, you probably already know that when you deploy a firewall or an intrusion prevention system (IPS) or install antivirus or advanced malware protection on your machine, you cannot assume you are now safe and secure. A layered and cross-boundary "defense-in-depth" strategy is what is needed to protect your network and corporate assets. One of the primary benefits of a defense-in-depth strategy is that even if a single control (such as a firewall or IPS) fails, other controls can still protect your environment and assets. Figure 3-1 illustrates this concept.

The following are the layers illustrated in Figure 3-1 (starting from the top):

- Nontechnical activities such as appropriate security policies and procedures, and end-user and staff training.
- Physical security, including cameras, physical access control (such as badge readers, retina scanners, and fingerprint scanners), and locks.
- Network security best practices, such as routing protocol authentication, control plane policing (CoPP), network device hardening, and so on.
- Host security solutions such as advanced malware protection (AMP) for endpoints, antiviruses, and so on.
- Application security best practices such as application robustness testing, fuzzing, defenses against cross-site scripting (XSS), cross-site request forgery (CSRF) attacks, SQL injection attacks, and so on.
- The actual data traversing the network. You can employ encryption at rest and in transit to protect data.

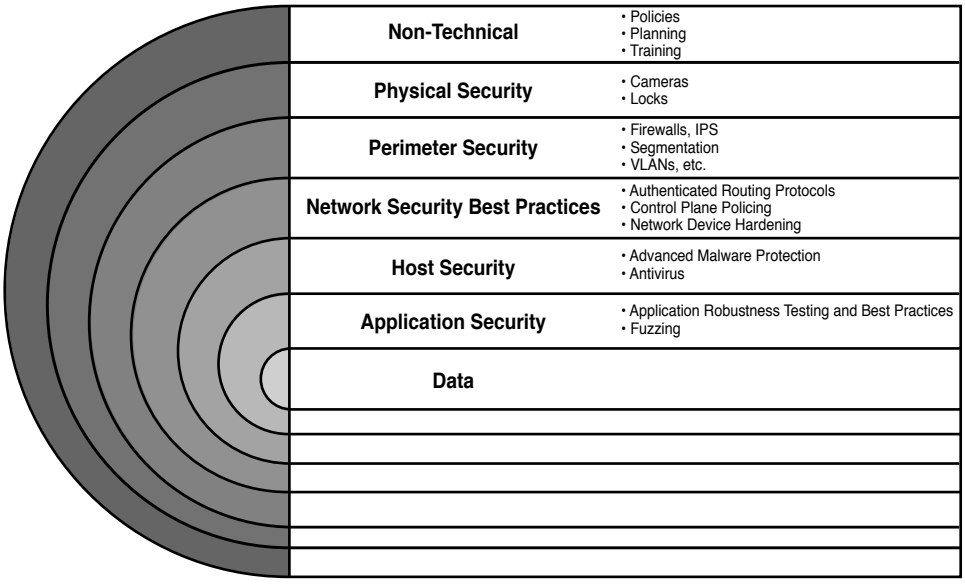

Figure 3-1 *Defense in Depth*

TIP Each layer of security introduces complexity and latency, while requiring that someone manage it. The more people are involved, even in administration, the more attack vectors you create, and the more you distract your people from possibly more important tasks. Employ multiple layers, but avoid duplication—and use common sense.

The first step in the process of preparing your network and staff to successfully identify security threats is achieving complete network visibility. You cannot protect against or mitigate what you cannot view/detect. You can achieve this level of network visibility through existing features on network devices you already have and on devices whose potential you do not even realize. In addition, you should create strategic network diagrams to clearly illustrate your packet flows and where, within the network, you could enable security mechanisms to identify, classify, and mitigate the threats. Remember that network security is a constant war. When defending against the enemy, you must know your own territory and implement defense mechanisms.

In some cases, onion-like diagrams are used to help illustrate and analyze what "defense-in-depth" protections and enforcements should be deployed in a network. Figure 3-2 shows an example of one of these onion diagrams, where network resources are protected through several layers of security.

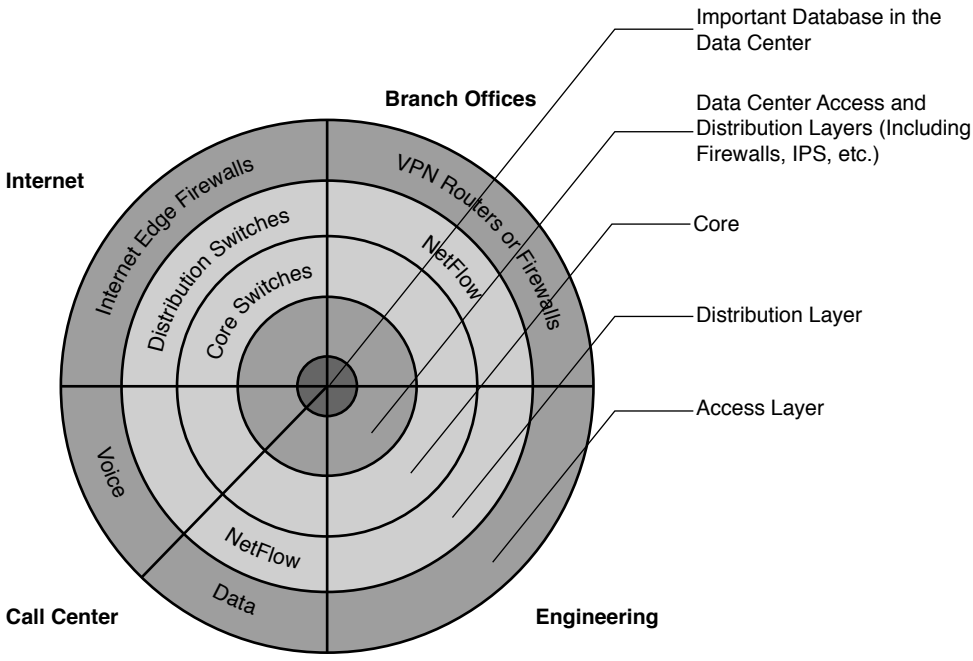

Figure 3-2 *Layered Onion Diagram Example*

You can create this type of diagram, not only to understand the architecture of your organization, but also to strategically identify places within the infrastructure where you can implement telemetry mechanisms such as NetFlow and identify choke points where you can mitigate an incident. Notice that the access, distribution, and core layers/boundaries are clearly defined.

These types of diagrams also help you visualize operational risks within your organization. The diagrams can be based on device roles and can be developed for critical systems you want to protect. For example, identify a critical system within your organization and create a layered diagram similar to the one in Figure 3-2. In this example, an "important database in the data center" is the most critical application/data source for this company. The diagram includes the database in the center.

You can also use this type of diagram to audit device roles and the types of services they should be running. For example, you can decide in what devices you can run services such as Cisco NetFlow or where to enforce security policies. In addition, you can see the life of a packet within your infrastructure, depending on the source and destination. An example is illustrated in Figure 3-3.

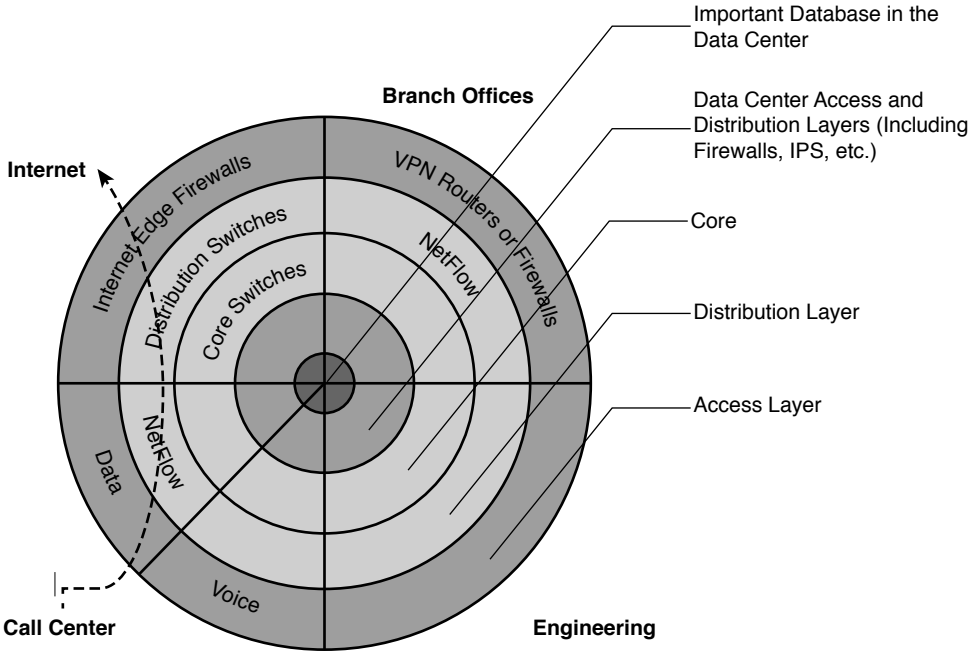

Figure 3-3 *Layered Onion Diagram Example*

In Figure 3-3, you can see a packet flow that occurs when a user from the call center accesses an Internet site. You know exactly where the packet is going based on your architecture as well as your security and routing policies. This is a simple example; however, you can use this concept to visualize risks and to prepare your isolation policies.

When applying defense-in-depth strategies, you can also look at a roles-based network security approach for security assessment in a simple manner. Each device on the network serves a purpose and has a role; subsequently, you should configure each device accordingly. You can think about the different planes as follows:

- **Management plane**: This is the distributed and modular network management environment.
- **Control plane**: This plane includes routing control. It is often a target because the control plane depends on direct CPU cycles.
- **User/data plane**: This plane receives, processes, and transmits network data among all network elements.
- **Services plane**: This is the Layer 7 application flow built on the foundation of the other layers.
- **Policies**: The plane includes the business requirements. Cisco calls policies the "business glue" for the network. Policies and procedures are part of this section, and they apply to all the planes in this list.

You should also view security in two different perspectives, as illustrated in Figure 3-4:

- Operational (reactive) security
- Proactive security

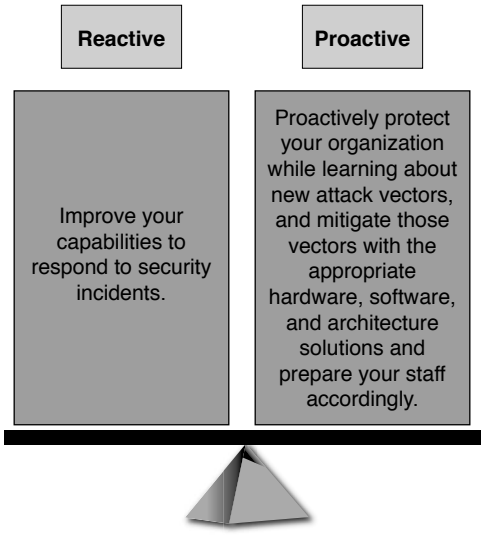

Figure 3-4 *Reactive vs. Proactive Security*

You should have a balance between proactive and reactive security approaches. Prepare your network, staff, and organization as a whole to better identify, classify, trace back, and react to security incidents. In addition, proactively protect your organization while learning about new attack vectors, and mitigate those vectors with the appropriate hardware, software, and architecture solutions.

What Are Threats, Vulnerabilities, and Exploits?

In this section, you will learn the difference between vulnerabilities, threats, and exploits.

Vulnerabilities

Key Topic

A *vulnerability* is an exploitable weakness in a system or its design. Vulnerabilities can be found in protocols, operating systems, applications, hardware, and system designs. Vulnerabilities abound, with more discovered every day. You will learn many examples of vulnerability classifications in Chapter 13, "Types of Attacks and Vulnerabilities." However, the following are a few examples:

- SQL injection vulnerabilities
- Command injections
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- API abuse vulnerabilities

- Authentication vulnerabilities
- Privilege escalation vulnerabilities
- Cryptographic vulnerabilities
- Error-handling vulnerabilities
- Input validation vulnerabilities
- Path traversal vulnerabilities
- Buffer overflows
- Deserialization of untrusted data
- Directory restriction error
- Double free
- Password management: hardcoded password
- Password plaintext storage

Vendors, security researchers, and vulnerability coordination centers typically assign vulnerabilities an identifier that's disclosed to the public. This identifier is known as the *Common Vulnerabilities and Exposures (CVE)*. CVE is an industry-wide standard. CVE is sponsored by US-CERT, the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Operating as DHS's Federally Funded Research and Development Center (FFRDC), MITRE has copyrighted the CVE List for the benefit of the community in order to ensure it remains a free and open standard, as well as to legally protect the ongoing use of it and any resulting content by government, vendors, and/or users. MITRE maintains the CVE list and its public website, manages the CVE Compatibility Program, oversees the CVE Naming Authorities (CNAs), and provides impartial technical guidance to the CVE Editorial Board throughout the process to ensure CVE serves the public interest.

The goal of CVE is to make it easier to share data across tools, vulnerability repositories, and security services.

More information about CVE is available at http://cve.mitre.org.

Threats

Key Topic

A *threat* is any potential danger to an asset. If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized. If someone is actively launching an attack against your system and successfully accesses something or compromises your security against an asset, the threat is realized. The entity that takes advantage of the vulnerability is known as the *malicious actor*, and the path used by this actor to perform the attack is known as the *threat agent* or *threat vector*.

A *countermeasure* is a safeguard that somehow mitigates a potential risk. It does so by either reducing or eliminating the vulnerability, or it at least reduces the likelihood of the threat agent to actually exploit the risk. For example, you might have an unpatched machine on your network, making it highly vulnerable. If that machine is unplugged from the network and ceases to have any interaction through exchanging data with any other device, you have

successfully mitigated all those vulnerabilities. You have likely rendered that machine no longer an asset, though—but it is safer.

Threat Actors

Key Topic

Threat actors are the individuals (or group of individuals) who perform an attack or are responsible for a security incident that impacts or has the potential of impacting an organization or individual. There are several types of threat actors:

- **Script kiddies**: People who uses existing "scripts" or tools to hack into computers and networks. They lack the expertise to write their own scripts.
- **Organized crime groups**: Their main purpose is to steal information, scam people, and make money.
- **State sponsors and governments**: These agents are interested in stealing data, including intellectual property and research-and-development data from major manufacturers, government agencies, and defense contractors.
- **Hacktivists**: People who carry out cyber security attacks aimed at promoting a social or political cause.
- **Terrorist groups**: These groups are motivated by political or religious beliefs.

Threat Intelligence

Key Topic

Threat intelligence is referred to as the knowledge about an existing or emerging threat to assets, including networks and systems. Threat intelligence includes context, mechanisms, indicators of compromise (IoCs), implications, and actionable advice. Threat intelligence is referred to as the information about the observables, indicators of compromise (IoCs) intent, and capabilities of internal and external threat actors and their attacks. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.

Converting these definitions into common language could translate to threat intelligence being evidence-based knowledge of the capabilities of internal and external threat actors. This type of data can be beneficial for the security operations center (SOC) of any organization. Threat intelligence extends cyber security awareness beyond the internal network by consuming intelligence from other sources Internet-wide related to possible threats to you or your organization. For instance, you can learn about threats that have impacted different external organizations. Subsequently, you can proactively prepare rather than react once the threat is seen against your network. Providing an enrichment data feed is one service that threat intelligence platforms would typically provide.

Forrester defines a five-step threat intelligence process (see Figure 3-5) for evaluating threat intelligence sources:

Step 1. Planning and direction

Step 2. Collection

Step 3. Processing

Step 4. Analysis and production

Step 5. Dissemination

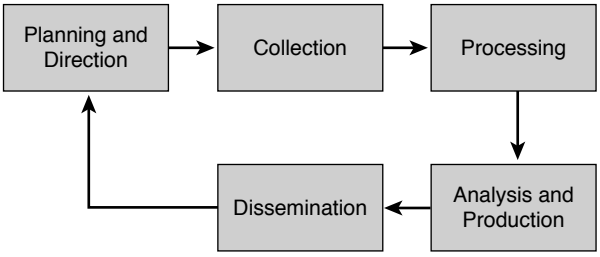

Figure 3-5 *Threat Intelligence*

Many different threat intelligence platforms and services are available in the market nowadays. Cyber threat intelligence focuses on providing actionable information on adversaries, including indicators of compromise (IoCs). Threat intelligence feeds help you prioritize signals from internal systems against unknown threats. Cyber threat intelligence allows you to bring more focus to cyber security investigation because instead of blindly looking for "new" and "abnormal" events, you can search for specific IoCs, IP addresses, URLs, or exploit patterns. The following are a few examples:

- **Cyber Squad ThreatConnect:** An on-premises, private, or public cloud solution offering threat data collection, analysis, collaboration, and expertise in a single platform. You can obtain more details at http://www.threatconnect.com.
- **BAE Detica CyberReveal:** A multithreat monitoring, analytics, investigation, and response product. CyberReveal brings together BAE Systems Detica's heritage in network intelligence, big-data analytics, and cyber threat research. CyberReveal consists of three core components: platform, analytics, and investigator. Learn more at http://www.baesystems.com.
- **Lockheed Martin Palisade:** Supports comprehensive threat collection, analysis, collaboration, and expertise in a single platform. Learn more at http://www.lockheedmartin.com.
- **MITRE CRITs:** Collaborative Research Into Threats (CRITs) is an open source feed for threat data. Learn more at https://crits.github.io.
- **Cisco AMP Threat Grid:** Combines static and dynamic malware analysis with threat intelligence into one unified solution.

A number of standards are being developed for disseminating threat intelligence information. The following are a few examples:

- **Structured Threat Information eXpression (STIX):** An express language designed for sharing of cyber attack information. STIX details can contain data such as the IP address of command-and-control servers (CnC), malware hashes, and so on. STIX was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at http://stixproject.github.io.

- **Trusted Automated eXchange of Indicator Information (TAXII):** An open transport mechanism that standardizes the automated exchange of cyber threat information. TAXII was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at http://taxiiproject.github.io.
- **Cyber Observable eXpression (CybOX):** A free standardized schema for specification, capture, characterization, and communication of events of stateful properties that are observable in the operational domain. CybOX was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at https://cyboxproject.github.io.
- **Open Indicators of Compromise (OpenIOC):** An open framework for sharing threat intelligence in a machine-digestible format. Learn more at http://www.openioc.org.

It should be noted that many open source and non-security-focused sources can be leveraged for threat intelligence as well. Some examples of these sources are social media, forums, blogs, and vendor websites.

Exploits

Key Topic

An *exploit* is software or a sequence of commands that takes advantage of a vulnerability in order to cause harm to a system or network. There are several methods of classifying exploits; however, the most common two categories are remote and local exploits. A *remote exploit* can be launched over a network and carries out the attack without any prior access to the vulnerable device or software. A *local exploit* requires the attacker or threat actor to have prior access to the vulnerable system.

NOTE Exploits are commonly categorized and named by the type of vulnerability they exploit.

There is also the concept of exploit kits. An *exploit kit* is a compilation of exploits that are often designed to be served from web servers. Their main purpose is identifying software vulnerabilities in client machines and then exploiting such vulnerabilities to upload and execute malicious code on the client. The following are a few examples of known exploit kits:

- Angler
- MPack
- Fiesta
- Phoenix
- Blackhole
- Crimepack
- RIG

NOTE Cisco Talos has covered and explained numerous exploit kits in detail, including Angler. You can obtain more information about these type of threats at Talos's blog, http://blog.talosintel.com, and specifically for Angler at http://blog.talosintel.com/search/label/angler.

Confidentiality, Integrity, and Availability: The CIA Triad

Key Topic

Confidentiality, integrity and availability, is often referred to as the CIA triad. This is a model that was created to define security policies. In some cases, you may also see this model referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the United States Central Intelligence Agency.

The idea is that confidentiality, integrity and availability should be guaranteed in any system that is considered secured.

Confidentiality

The ISO 27000 standard has a very good definition: "confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." One of the most common ways to protect the confidentiality of a system or its data is to use encryption. The Common Vulnerability Scoring System (CVSS) uses the CIA triad principles within the metrics used to calculate the CVSS base score.

NOTE You will learn more about CVSS throughout the following chapters, and you can obtain more information about CVSS at: https://www.first.org/cvss/specification-document

Integrity

Integrity is the ability to make sure that a system and its data has not been altered or compromised. It ensures that the data is an accurate and unchanged representation of the original secure data. Integrity applies not only to data, but also to systems. For instance, if a threat actor changes the configuration of a server, firewall, router, switch or any other infrastructure device, it is considered that he or she impacted the integrity of the system.

Availability

Availability refers that a system or application must be "available" to authorized users at all times. According to the CVSS version 3 specification, the availability metric "measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g., information, files) used by the impacted component, this metric refers to the loss of availability of the impacted component itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component."

A common example of an attack that impacts availability is a denial of service (DoS) attack.

Risk and Risk Analysis

Key Topic

According to the Merriam-Webster dictionary, risk is "the possibility that something bad or unpleasant will happen." In the world of cyber security, risk can be defined as the possibility of a security incident (something bad) happening. There are many standards and methodologies for classifying and analyzing cyber security risks. The Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment)

to help financial institutions identify their risks and determine their cyber security preparedness. This guidance/tool can be useful for any organization. The FFIEC tool provides a repeatable and measurable process for organizations to measure their cyber security readiness.

According to the FFIEC, the assessment consists of two parts:

- **Inherent Risk Profile and Cybersecurity Maturity**: The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cybersecurity Maturity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. Although management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cyber security maturity level.
- **The International Organization for Standardization (ISO) 27001:** This is the international standard for implementing an information security management system (ISMS). ISO 27001 is heavily focused on risk-based planning to ensure that the identified information risks (including cyber risks) are appropriately managed according to the threats and the nature of those threats. ISO 31000 is the general risk management standard that includes principles and guidelines for managing risk. It can be used by any organization, regardless of its size, activity, or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

  The ISO/IEC 27005 standard is more focused on cyber security risk assessment. It is titled "Information technology—Security techniques—Information security risk management."

  The following is according to ISO's website:

  "The standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:

  - Establish the risk management context (e.g. the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization's risk tolerance or appetite);
  - Quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk;'
  - Treat (i.e. modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those 'levels of risk' to prioritize them;
  - Keep stakeholders informed throughout the process; and
  - Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes."

There are also standards to score the overall "risk" of a vulnerability. The most commonly used is the Common Vulnerability Scoring System (CVSS) developed by the Forum of Incident Response and Security Teams (FIRST). CVSS is a standards-based scoring method

that conveys vulnerability severity and helps determine the urgency and priority of response. CVSS is used by many Product Security Incident Response Teams (PSIRTs), vulnerability coordination centers, security researchers, and consumers of security vulnerability information.

NOTE You will learn about CVSS in more detail in Chapter 5, "Introduction to Security Operations Management," and can obtain more information at FIRST's website, https://www.first.org/cvss.

There are also several additional scoring systems:

- **Common Weakness Scoring System (CWSS):** A methodology for scoring software weaknesses. CWSS is part of the Common Weakness Enumerator (CWE) standard. More information about CWSS is available at http://cwe.mitre.org/cwss.
- **Common Misuse Scoring System (CMSS):** A standardized way to measure software feature misuse vulnerabilities. More information about CMSS is available at http://scap.nist.gov/emerging-specs/listing.html#cmss.
- **Common Configuration Scoring System (CCSS):** More information about CCSS can be found at http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf.

Personally Identifiable Information and Protected Health Information

Many regulations as well as the United States government require organizations to identify personally identifiable information (PII) and protected health information (PHI) and handle them in a secure manner. Unauthorized release or loss of such data could result in severe fines and penalties for the organization. Given the importance of PII and PHI, regulators and the government want to oversee the usage more efficiently. This section explains what PII and PHI are.

PII

Key Topic

According to the Executive Office of the President, Office of Management and Budget (OMB) and the U.S. Department of Commerce, Office of the Chief Information Officer, PII refers to "information which can be used to distinguish or trace an individual's identity." The following are a few examples:

- The individual's name
- Social security number
- Biological or personal characteristics, such as an image of distinguishing features, fingerprints, x-rays, voice signature, retina scan, and the geometry of the face
- Date and place of birth
- Mother's maiden name
- Credit card numbers
- Bank account numbers

- Driver license number
- Address information, such as email addresses or street addresses, and telephone numbers for businesses or personal use

PHI

Key Topic

The Health Insurance Portability and Accountability Act (HIPAA) requires health care organizations and providers to adopt certain security regulations for protecting health information. The Privacy Rule calls this information "protected health information," or PHI. This information includes, but is not limited to, the following:

- Individual's name (that is, patient's name)
- All dates directly linked to an individual, including date of birth, death, discharge, and administration
- Telephone and fax numbers
- Email addresses and geographic subdivisions such as street addresses, ZIP Codes, and county.
- Medical record numbers and health plan beneficiary numbers
- Certificate numbers or account numbers
- Social security number
- Driver license number
- Biometric identifiers, including voice or fingerprints
- Photos of the full face or recognizable features
- Any unique number-based code or characteristic
- The individual's past, present, and future physical or mental health or condition
- The provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual

Principle of Least Privilege and Separation of Duties

Key Topic

Two additional key concepts in information security are the principle of least privilege and separation of duties. This section defines these two key concepts.

Principle of Least Privilege

The principle of least privilege states that all users—whether they are individual contributors, managers, directors, or executives—should be granted only the level of privilege they need to do their jobs, and no more. For example, a sales account manager really has no business having administrator privileges over the network, or a call center staff member over critical corporate financial data.

The same concept of principle of least privilege can be applied to software. For example, programs or processes running on a system should have the capabilities they need to "get their job done," but no root access to the system. If a vulnerability is exploited on a system that runs "everything as root," the damage could extend to a complete compromise of the

system. This is why you should always limit users, applications, and processes to access and run as the least privilege they need.

TIP Somewhat related to the principle of least privilege is the concept of "need to know," which means that users should get access only to data and systems that they need to do their job, and no other.

Separation of Duties

Separation of duties is an administrative control that dictates that a single individual should not perform all critical- or privileged-level duties. Additionally, important duties must be separated or divided among several individuals within the organization. The goal is to safeguard against a single individual performing sufficiently critical or privileged actions that could seriously damage a system or the organization as a whole. For instance, security auditors responsible for reviewing security logs should not necessarily have administrative rights over the systems. Another example is that a network administrator should not have the ability to alter logs on the system. This is to prevent such individuals from carrying out unauthorized actions and then deleting evidence of such action from the logs (in other words, covering their tracks).

Think about two users having two separate keys in order to open a safety deposit box. Separation of duties is similar to that concept, where the safety deposit box cannot be opened by a user without the other key.

Security Operation Centers

Key Topic

Security operation centers (SOCs) are facilities where an organization's assets, including applications, databases, servers, networks, desktops, and other endpoints, are monitored, assessed, and protected. Establishing SOC capabilities requires careful planning. The planning phase helps you decide on and formalize yourself with the objectives that justify having an SOC, and to develop a roadmap you can use to track your progress against those predefined objectives. The success of any security program (including the SOC) depends on proper planning. There are always challenges that are specific to an organization, and these challenges are introduced because of issues related to governance, collaboration, lack of tools, lack of automation, lack of threat intelligence, skill sets, and so on. Such challenges must be identified and treated, or at least acknowledged, at an early stage of an SOC establishment program. SOCs are created to be able to address the following challenges:

- How can you detect a compromise in a timely manner?
- How do you triage a compromise to determine the severity and the scope?
- What is the impact of the compromise to your business?
- Who is responsible for detecting and mitigating a compromise?
- Who should be informed or involved, and when do you deal with the compromise once detected?
- How and when should you communicate a compromise internally or externally, and is that needed in the first place?

To build and operate an effective SOC, you must have the following:

- Executive sponsorship.
- SOC operating as a program. Organizations should operate the SOC as a program rather than a single project. Doing so depends on the criticality and the amount of resources required to design, build, and operate the various services offered by the SOC. Having a clear SOC service strategy with clear goals and priorities will shape the size of the SOC program, timeline, and the amount of resources required to deliver the program objectives.
- A governance structure. Metrics must be established to measure the effectiveness of the SOC capabilities. These metrics should provide sufficient and relevant visibility to the organization's management team on the performance of the SOC and should identify areas where improvements and investments are needed.
- Effective team collaboration.
- Access to data and systems.
- Applicable processes and procedures.
- Team skill sets and experience.
- Budget (for example, will it be handled in-house or outsourced?).

Runbook Automation

Organizations need to have capabilities to define, build, orchestrate, manage, and monitor the different operational processes and workflows. This is achieved by implementing runbooks and runbook automation (RBA). A *runbook* is a collection of procedures and operations performed by system administrators, security professionals, or network operators. According to Gartner, "the growth of RBA has coincided with the need for IT operations executives to enhance IT operations efficiency measures." Gartner, Inc. is an American research and advisory firm providing information technology related insight for IT and other business leaders.

Here are some of the metrics to measure effectiveness:

- Mean time to repair (MTTR)
- Mean time between failures (MTBF)
- Mean time to discover a security incident
- Mean time to contain or mitigate a security incident
- Automating the provisioning of IT resources

Many different commercial and open source RBA solutions are available in the industry. An example of a popular open source RBA solution is Rundeck (http://rundeck.org/). Rundeck can be integrated with configuration management platforms such as Chef, Puppet, and Ansible. A commercial RBA example is the Cisco Workload Automation (CWA), which can manage different business processes across a comprehensive set of applications and systems. You can obtain more information about Cisco CWA at http://www.cisco.com/c/en/us/products/analytics-automation-software/tidal-enterprise-scheduler/index.html.

Forensics

The United States Computer Emergency Response Team (CERT) defines cyber forensics as follows:

> "If you manage or administer information systems and networks, you should understand cyber forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word forensics means 'to bring to the court.') Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive."

Cyber forensics is often referred to as "computer forensics." However, "cyber forensics" is a more appropriate term than "computer forensics."

The two primary objectives in cyber forensics are to find out what happened and to collect data in a manner that is acceptable to the court. Any device that can store data is potentially the object of cyber forensics, including, but not limited to, the following:

- Computers (servers, desktop machines, and so on)
- Smartphones
- Tablets
- Network infrastructure devices (routers, switches, firewalls, intrusion prevention systems)
- Network management systems
- Printers
- Even vehicle GPSs

Chain of custody is critical to forensics investigations. The following section describes chain of custody in detail.

Evidentiary Chain of Custody

Key Topic

Chain of custody is the way you document and preserve evidence from the time that you started the cyber forensics investigation to the time the evidence is presented at court. It is extremely important to be able to show clear documentation of the following:

- How the evidence was collected
- When it was collected
- How it was transported
- How is was tracked
- How it was stored
- Who had access to the evidence and how it was accessed

TIP If you fail to maintain proper chain of custody, it is likely you cannot use that evidence in court. It is also important to know how to dispose of evidence after an investigation.

When you collect evidence, you must protect its integrity. This involves making sure that nothing is added to the evidence and that nothing is deleted or destroyed (this is known as *evidence preservation*).

TIP A method often used for evidence preservation is to only work with a copy of the evidence—in other words, not directly working with the evidence itself. This involves creating an image of any hard drive or any storage device.

Several forensics tools are available on the market. The following are two of the most popular:

- Guidance Software's EnCase (https://www.guidancesoftware.com/)
- AccessData's Forensic Toolkit (http://accessdata.com/)

Another methodology used in evidence preservation is to use write-protected storage devices. In other words, the storage device you are investigating should immediately be write-protected before it is imaged and should be labeled to include the following:

- Investigator's name
- The date when the image was created
- Case name and number (if applicable)

Additionally, you must prevent electronic static or other discharge from damaging or erasing evidentiary data. Special evidence bags that are antistatic should be used to store digital devices. It is very important that you prevent electrostatic discharge (ESD) and other electrical discharges from damaging your evidence. Some organizations even have cyber forensic labs that control access to only authorized users and investigators. One method often used involves constructing what is called a "Faraday cage." This "cage" is often built out of a mesh of conducting material that prevents electromagnetic energy from entering into or escaping from the cage. Also, this prevents devices from communicating via Wi-Fi or cellular signals.

What's more, transporting the evidence to the forensics lab or any other place, including the courthouse, has to be done very carefully. It is critical that the chain of custody be maintained during this transport. When you transport the evidence, you should strive to secure it in a lockable container. It is also recommended that the responsible person stay with the evidence at all times during transportation.

Reverse Engineering

Key Topic

Reverse engineering is the methodology for acquiring architectural information about anything originally created by someone else. Reverse engineering has been around since long before computers or modern technology. Nowadays, reverse engineering is not only used to steal or counterfeit technology and to "reverse" cryptographic algorithms, but also to perform malware analysis and cyber security forensics. Reverse engineering can even be useful to software developers to discover how to interoperate with undocumented or partially documented software, or even to develop competing software (which in some cases may be illegal).

Reverse engineering can be used for exploit development to locate vulnerabilities in a system and compromise the system, but it also can be used on malware. Security researchers and forensics experts can trace every step the malware takes and assess the damage it could cause, the expected rate of infection, how it could be removed from infected systems, and how to potentially proactively defend against such a threat. Malware analysis extends to identifying whether malware is present on a given system and studying the malware to understand how it functions. Doing this can reveal the purpose of the malware, and even its author.

Two additional uses of reverse engineering are to "reverse" cryptographic algorithms to decrypt data as well as Digital Rights Management (DRM) solutions. Threat actors use DRM reverse-engineering techniques to steal music, movies, books, and any other content protected by DRM solutions.

Many tools are available for performing reverse engineering. The following are a few examples:

- **System-monitoring tools**: Tools that sniff, monitor, explore, and otherwise expose the program being reversed.
- **Disassemblers**: Tools that take a program's executable binary as input and generate textual files that contain the assembly language code for the entire program or parts of it.
- **Debuggers**: These tools allow reverse engineers to observe the program while it is running and to set breakpoints; they also provide the ability to trace through code. Reverse engineers can use debuggers to step through the disassembled code and watch the system as it runs the program, one instruction at a time.
- **Decompilers**: Programs that take an executable binary file and attempt to produce readable high-level language code from it.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 3-2 Key Topics

Key Topic Element	Description	Page
Summary	Describe what are vulnerabilities	166
Summary	Define what are threats	167
Summary	Define threat actors	168
Summary	Describe what is threat intelligence and why is it useful	168
Summary	Define what are exploits	170
Summary	Describe confidentiality, integrity, and availability	171
Summary	Describe risk and risk analysis	171
Summary	Define and provides examples of PII	173
Summary	Define and provides examples of PHI	174
Summary	Decribe the principle of least privilege	174
Summary	Define what is a security operations center	175
Summary	Describe runbook automation	176
Summary	Define and describe chain of custody	177
Summary	Describe what is reverse engineering	178

Define Key Terms

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

Vulnerabilities, threats, threat actors, exploits

Q&A

The answers to these questions appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Questions." For more practice with exam format questions, use the exam engine on the website.

1. Which of the following statements are true about vulnerabilities?
   a. A vulnerability is a threat on a system.
   b. A vulnerability is an exploitable weakness in a system or its design.
   c. Vulnerabilities can be found in protocols, operating systems, applications, hardware, and system designs.
   d. Vulnerabilities are exploits that are discovered every day in software and hardware products.
2. On which of the following can exploit kits be run from?
   a. Web servers
   b. Email servers
   c. NTP servers
   d. Firewalls
3. Which of the following are examples of exploit kits?
   a. Angler
   b. Mangler
   c. Blackhole
   d. Black ICE
4. Which of the following describe what a threat is?
   a. Threats and vulnerabilities are the same.
   b. A threat is an exploit against a patched vulnerability.
   c. A threat is any potential danger to an asset.
   d. A threat is a piece of software aimed at exploiting a vulnerability.
5. What is an IoC?
   a. An indicator of compromise
   b. An indicator of containment
   c. An intrusion operating control
   d. An intrusion of compromise
6. Which of the following are provided by threat intelligence feeds?
   a. Indicators of compromise
   b. IP addresses of attacking systems
   c. The overall risk score of all vulnerabilities in the corporate network
   d. The overall risk score of threats in the corporate network

7. The way you document and preserve evidence from the time you start the cyber forensics investigation to the time the evidence is presented in court is referred to as which of the following?
   a. Chain of compromise
   b. Custody of compromise
   c. Chain of forensics
   d. Chain of custody
8. What are decompilers?
   a. Programs that take an executable binary file and attempt to produce readable high-level language code from it
   b. Programs that take a non-executable binary file and attempt to produce compiled code from it
   c. Programs that take a non-executable binary file and attempt to produce encrypted code from it
   d. Programs that execute a binary file and attempt to crack the encryption of it
9. Which of the following are metrics that can measure the effectiveness of a runbook?
   a. Mean time to repair (MTTR)
   b. Mean time between failures (MTBF)
   c. Mean time to discover a security incident
   d. All of the above
10. What is PHI?
   a. Protected HIPAA information
   b. Protected health information
   c. Personal health information
   d. Personal human information

Index

Numbers

A

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

Q-R

S

T

U

V

W

X

Y-Z

Connect, Engage, Collaborate

The Award Winning Cisco Support Community

Attend and Participate in Events

Ask the Experts
Live Webcasts

Knowledge Sharing

Documents
Blogs
Videos

Top Contributor Programs

Cisco Designated VIP
Hall of Fame
Spotlight Awards

Multi-Language Support

https://supportforums.cisco.com

CISCO

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA Cyber Ops SECOPS 210-255

OMAR SANTOS, CISSP® NO. 463598
JOSEPH MUNIZ, CISSP® NO. 344594

ciscopress.com

CCNA Cyber Ops SECOPS

210-255 **Official** Cert Guide

OMAR SANTOS, CISSP No. 463598
JOSEPH MUNIZ, CISSP No. 344594

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Cyber Ops SECOPS 210-255 Official Cert Guide

Omar Santos, CISSP No. 463598
Joseph Muniz, CISSP No. 344594

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing June 2017

Library of Congress Control Number: 2017937634

ISBN-13: 978-1-58714-703-6

ISBN-10: 1-58714-703-3

Warning and Disclaimer

This book is designed to provide information about the CCNA Cyber Ops SECOPS 210-255 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.
For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Product Line Manager: Brett Bartow

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Eleanor Bru

Project Editor: Mandie Frank

Cover Designer: Chuti Prasertsith

Business Operation Manager, Cisco Press: Ronald Fligge

Technical Editors: Jeremy McGuinn, Justin Poole

Copy Editor: Bart Reed

Editorial Assistant: Vanessa Evans

Composition: Bronkella Publishing

Indexer: Ken Johnson

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Authors

Omar Santos is an active member of the cybersecurity community, where he leads several industry-wide initiatives and standards bodies. 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.

Omar is the author of more than a dozen 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), where he mentors and leads engineers and incident managers during the investigation and resolution of cybersecurity vulnerabilities. Additional information about Omar's current projects can be found at omarsantos.io, and you can follow Omar on Twitter @santosomar.

Joseph Muniz is an architect at Cisco Systems and security researcher. He has extensive experience in designing security solutions and architectures for the top Fortune 500 corporations and the U.S. government. Joseph's current role gives him visibility into the latest trends in cybersecurity, from both leading vendors and customers. Examples of Joseph's research include his RSA talk titled "Social Media Deception," which has been quoted by many sources (search for "Emily Williams Social Engineering"), as well as his articles in *PenTest Magazine* regarding various security topics.

Joseph runs The Security Blogger website, a popular resource for security, hacking, and product implementation. He is the author and contributor of several publications covering various penetration testing and security topics. You can follow Joseph at www.thesecurityblogger.com and @SecureBlogger.

About the Technical Reviewers

Jeremy McGuinn is a support engineer in the Applied Security Intelligence group at Cisco Systems where he focuses on the detection of cyber attacks. Before spending 10 years in security roles at Cisco, Jeremy was an enterprise systems administrator for both government and private sector networks. Jeremy was *Time*® magazine's person of the year in 2006 and lives in Raleigh, North Carolina.

Justin Poole, CCIE No. 16224 (R&S, Security), CISSP, is a consulting systems engineer at Cisco Systems, specializing in Cybersecurity, Secure Data Center, and Enterprise Network architectures and solutions. Justin supports customers across the U.S. public sector market. He has been at Cisco for 11 years and in the industry for more than 15 years.

Dedications

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.

I also dedicate this book to my father, Jose, and to the memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

—Omar Santos

I would like to dedicate this book to the memory of my father, Raymond Muniz. He never saw me graduate from college or accomplish great things, such as writing this book. I would also like to apologize to him for dropping out of soccer in high school. I picked it back up later in life, and today play in at least two competitive matches a week. Your hard work paid off. Hopefully you somehow know that.

—Joseph Muniz

Acknowledgments

I would like to thank Joey Muniz for accepting to co-author this book with me. I really enjoyed working with Joey on this book and also on the CCNA Cyber Ops SECFND book as well. I would also like to thank the technical editors, Jeremy McGuinn and Justin Poole, for their time and technical expertise. They verified our work and contributed to the success of this book. I would also like to thank the Cisco Press team, especially Mary Beth Ray, Denise Lincoln, and Christopher Cleveland, for their patience, guidance, and consideration. Their efforts are greatly appreciated. Finally, I would like to acknowledge the Cisco Security Research and Operations teams, Cisco Advanced Threat Analytics, and Cisco Talos. Several leaders in the network security industry work there, supporting our Cisco customers, often under very stressful conditions, and working miracles daily. They are truly unsung heroes, and I am honored to have had the privilege of working side by side with them in the trenches while protecting customers and Cisco.

—Omar Santos

I would first like to thank Omar for including me on this project. I really enjoyed working with him and hope we can do more in the future. I also would like to thank the Cisco Press team and technical editors, Jeremy McGuinn and Justin Poole, for their fantastic support in making the writing process top quality and easy for everybody.

I would also like to thank all the great people in my life who make me who I am.

Finally, a message for Raylin Muniz (age 7): Hopefully one day you can accomplish your dreams like I have with this book.

—Joseph Muniz

Contents at a Glance

Contents

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Congratulations! If you are reading this, you have in your possession a powerful tool that can help you to:

- Improve your awareness and knowledge of cybersecurity operations
- Increase your skill level related to operational security
- Prepare for the CCNA Cyber Ops SECOPS certification exam

Whether you are preparing for the CCNA Cyber Ops certification or just changing careers to cybersecurity, this book will help you gain the knowledge you need to get started and prepared. When writing this book, we did so with you in mind, and together we will discover the critical ingredients that make up the recipe for a secure network and how to succeed in cybersecurity operations. By focusing on covering the objectives for the CCNA Cyber Ops SECOPS exam and integrating that with real-world best practices and examples, we created this content with the intention of being your personal tour guides as we take you on a journey through the world of network security.

The CCNA Cyber Ops: Implementing Cisco Cybersecurity Operations (SECOPS) 210-255 exam is required for the CCNA Cyber Ops certification. This book covers all the topics listed in Cisco's exam blueprint, and each chapter includes key topics and preparation tasks to assist you in mastering this information. Reviewing tables and practicing test questions will help you practice your knowledge in all subject areas.

About the 210-255 CCNA Cyber Ops SECOPS Exam

The CCNA Cyber Ops: Implementing Cisco Cybersecurity Operations (SECOPS) 210-255 exam is the second of the two required exams to achieve the CCNA Cyber Ops certification and is aligned with the job role of associate-level security operations center (SOC) security analyst. The SECOPS exam tests candidates' understanding of cybersecurity operation principles, foundational knowledge, and core skills needed to detect and respond to cybersecurity incidents and protect their organization from modern threats.

The CCNA Cyber Ops: Implementing Cisco Cybersecurity Operations (SECOPS) 210-255 exam is a computer-based test that has 50 to 60 questions and a 90-minute time limit. Because all exam information is managed by Cisco Systems and is therefore subject to change, candidates should continually monitor the Cisco Systems site for exam updates at https://learningnetwork.cisco.com/community/certifications/ccna-cyber-ops.

You can take the exam at Pearson VUE testing centers. You can register with VUE at www.vue.com/cisco.

210-255 CCNA Cyber Ops SECOPS Exam Topics

Table I-1 lists the topics of the 210-255 SECOPS exam and indicates the chapter in the book where they are covered.

Table I-1 *210-255 SECOPS Exam Topics*

Exam Topic	Chapter
1.0. Endpoint Threat Analysis and Computer Forensics	
1.1. Interpret the output report of a malware analysis tool such as AMP Threat Grid or Cuckoo Sandbox	***Chapter 1***
1.2. Describe these terms as they are defined in the CVSS 3.0	***Chapter 1***
1.2.a. Attack vector	Chapter 1
1.2.b. Attack complexity	Chapter 1
1.2.c. Privileges required	Chapter 1
1.2.d. User interaction	Chapter 1
1.2.e. Scope	Chapter 1
1.3. Describe these terms as they are defined in the CVSS 3.0	***Chapter 1***
1.3.a. Confidentiality	Chapter 1
1.3.b. Integrity	Chapter 1
1.3.c. Availability	Chapter 1
1.4. Define these items as they pertain to the Microsoft Windows file system	***Chapter 2***
1.4.a. FAT32	Chapter 2
1.4.b. NTFS	Chapter 2
1.4.c. Alternative data streams	Chapter 2
1.4.d. MACE	Chapter 2
1.4.e. EFI	Chapter 2
1.4.f. Free space	Chapter 2
1.4.g. Timestamps on a file system	Chapter 2
1.5. Define these terms as they pertain to the Linux file system	***Chapter 2***
1.5.a. Ext4	Chapter 2
1.5.b. Journaling	Chapter 2
1.5.c. MBR	Chapter 2
1.5.d. Swap file system	Chapter 2
1.5.e. MAC	Chapter 2
1.6. Compare and contrast three types of evidence	***Chapter 2***
1.6.a. Best evidence	Chapter 2
1.6.b. Corroborative evidence	Chapter 2
1.6.c. Indirect evidence	Chapter 2

Exam Topic	Chapter
1.7. Compare and contrast two types of image	*Chapter 2*
1.7.a. Altered disk image	Chapter 2
1.7.b. Unaltered disk image	Chapter 2
1.8. Describe the role of attribution in an investigation	*Chapter 2*
1.8.a. Assets	Chapter 2
1.8.b. Threat actor	Chapter 2
2.0. Network Intrusion Analysis	
2.1. Interpret basic regular expressions	Chapter 3
2.2. Describe the fields in these protocol headers as they relate to intrusion analysis	Chapter 3
2.2.a. Ethernet frame	Chapter 3
2.2.b. IPv4	Chapter 3
2.2.c. IPv6	Chapter 3
2.2.d. TCP	Chapter 3
2.2.e. UDP	Chapter 3
2.2.f. ICMP	Chapter 3
2.2.g. HTTP	Chapter 3
2.3. Identify the elements from a NetFlow v5 record from a security event	Chapter 4
2.4. Identify these key elements in an intrusion from a given PCAP file	Chapter 3
2.4.a. Source address	Chapter 3
2.4.b. Destination address	Chapter 3
2.4.c. Source port	Chapter 3
2.4.d. Destination port	Chapter 3
2.4.e. Protocols	Chapter 3
2.4.f. Payloads	Chapter 3
2.5. Extract files from a TCP stream when given a PCAP file and Wireshark	Chapter 3
2.6. Interpret common artifact elements from an event to identify an alert	Chapter 3
2.6.a. IP address (source / destination)	Chapter 3
2.6.b. Client and server port identity	Chapter 3
2.6.c. Process (file or registry)	Chapter 3
2.6.d. System (API calls)	Chapter 3

Exam Topic	Chapter
2.6.e. Hashes	Chapter 3
2.6.f. URI/URL	Chapter 3
2.7. Map the provided events to these source technologies	Chapter 3
2.7.a. NetFlow	Chapter 4
2.7.b. IDS/IPS	Chapter 3
2.7.c. Firewall	Chapter 3
2.7.d. Network application control	Chapter 3
2.7.e. Proxy logs	Chapter 3
2.7.f. Antivirus	Chapter 3
2.8. Compare and contrast impact and no impact for these items	Chapter 3
2.8.a. False Positive	Chapter 3
2.8.b. False Negative	Chapter 3
2.8.c. True Positive	Chapter 3
2.8.d. True Negative	Chapter 3
2.9. Interpret a provided intrusion event and host profile to calculate the impact flag generated by Firepower Management Center (FMC)	Chapter 3
3.0. Incident Response	
3.1. Describe the elements that should be included in an incident response plan as stated in NIST.SP800-61 r2	Chapter 5
3.2. Map elements to these steps of analysis based on the NIST.SP800-61 r2	Chapter 5
3.2.a. Preparation	Chapter 5
3.2.b. Detection and analysis	Chapter 5
3.2.c. Containment, eradication, and recovery	Chapter 5
3.2.d. Post-incident analysis (lessons learned)	Chapter 5
3.3. Map the organization stakeholders against the NIST IR categories (C2M2, NIST.SP800-61 r2)	Chapter 5
3.3.a. Preparation	Chapter 5
3.3.b. Detection and analysis	Chapter 5
3.3.c. Containment, eradication, and recovery	Chapter 5
3.3.d. Post-incident analysis (lessons learned)	Chapter 5
3.4. Describe the goals of the given CSIRT	Chapter 6
3.4.a. Internal CSIRT	Chapter 6

Exam Topic	Chapter
3.4.b. National CSIRT	Chapter 6
3.4.c. Coordination centers	Chapter 6
3.4.d. Analysis centers	Chapter 6
3.4.e. Vendor teams	Chapter 6
3.4.f. Incident response providers (MSSP)	Chapter 6
3.5. Identify these elements used for network profiling	Chapter 8
3.5.a. Total throughput	Chapter 8
3.5.b. Session duration	Chapter 8
3.5.c. Ports used	Chapter 8
3.5.d. Critical asset address space	Chapter 8
3.6. Identify these elements used for server profiling	Chapter 8
3.6.a. Listening ports	Chapter 8
3.6.b. Logged in users/service accounts	Chapter 8
3.6.c. Running processes	Chapter 8
3.6.d. Running tasks	Chapter 8
3.6.e. Applications	Chapter 8
3.7. Map data types to these compliance frameworks	Chapter 7
3.7.a. PCI	Chapter 7
3.7.b. HIPAA (Health Insurance Portability and Accountability Act)	Chapter 7
3.7.c. SOX	Chapter 7
3.8. Identify data elements that must be protected with regard to a specific standard (PCI-DSS)	Chapter 7
4.0. Data and Event Analysis	
4.1. Describe the process of data normalization	Chapter 9
4.2. Interpret common data values into a universal format	Chapter 9
4.3. Describe 5-tuple correlation	Chapter 9
4.4. Describe the 5-tuple approach to isolate a compromised host in a grouped set of logs	Chapter 9
4.5. Describe the retrospective analysis method to find a malicious file, provided a file analysis report	Chapter 9
4.6. Identify potentially compromised hosts within the network based on a threat analysis report containing malicious IP address or domains	Chapter 9
4.7. Map DNS logs and HTTP logs together to find a threat actor	Chapter 9

Exam Topic	Chapter
4.8. Map DNS, HTTP, and threat intelligence data together	Chapter 9
4.9. Identify a correlation rule to distinguish the most significant alert from a given set of events from multiple data sources using the Firepower Management Console	Chapter 9
4.10. Compare and contrast deterministic and probabilistic analysis	Chapter 9
5.0. Incident Handling	
5.1. Classify intrusion events into these categories as defined in the Diamond Model of Intrusion	Chapter 10
5.1.a. Reconnaissance	Chapter 10
5.1.b. Weaponization	Chapter 10
5.1.c. Delivery	Chapter 10
5.1.d. Exploitation	Chapter 10
5.1.e. Installation	Chapter 10
5.1.f. Command and control	Chapter 10
5.1.g. Action on objectives	Chapter 10
5.2. Apply the NIST.SP800-61 r2 incident handling process to an event	Chapter 10
5.3. Define these activities as they relate to incident handling	Chapter 10
5.3.a. Identification	Chapter 10
5.3.b. Scoping	Chapter 10
5.3.c. Containment	Chapter 10
5.3.d. Remediation	Chapter 10
5.3.e. Lesson-based hardening	Chapter 10
5.3.f. Reporting	Chapter 10
5.4. Describe these concepts as they are documented in NIST SP 800-86	Chapter 10
5.4.a. Evidence collection order	Chapter 10
5.4.b. Data integrity	Chapter 10
5.4.c. Data preservation	Chapter 10
5.4.d. Volatile data collection	Chapter 10
5.5. Apply the VERIS schema categories to a given incident	Chapter 5

About the CCNA Cyber Ops SECOPS #210-255 Official Cert Guide

This book maps to the topic areas of the 210-255 SECOPS exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. This book is designed to help you pass the SECOPS exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **"Do I Know This Already?" quiz:** Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.
- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter:
  - **Review All the Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The "Review All the Key Topics" activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - **Complete the Tables and Lists from Memory:** To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the companion website. This document lists only partial information, allowing you to complete the table or list.

- **Define Key Terms:** Although the exam is unlikely to ask you to define a term, the CCNA Cyber Ops exams do require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Q&A:** Confirm that you understand the content you just covered.

- **Web-based practice exam:** The companion website includes the Pearson Test Prep practice test software, which allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 10 core chapters—Chapters 1 through 10. Chapter 11 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNA Cyber Ops SECOPS exam. The core chapters are organized into parts. They cover the following topics:

Part I Threat Analysis and Computer Forensics

- **Chapter 1: Threat Analysis** covers details about the vectors, complexity, scope, and required privileges of cyber attacks in respect to the Common Vulnerability Scoring System version 3 (CVSSv3). This chapter also describes the confidentiality, integrity, and availability impacts of cyber attacks.
- **Chapter 2: Forensics** covers fundamentals about forensics in Windows and Linux-based systems. It covers the Windows file system, defines terms as they pertain to the underlying operating system, master boot record, and other architectural components.

Part II Network Intrusion Analysis

- **Chapter 3: Fundamentals of Intrusion Analysis** covers the common artifact elements and sources of security events. In this chapter, you will gain an understanding of regular expressions, protocol headers, and intrusion analysis. You will also learn how to use packet captures for intrusion analysis.
- **Chapter 4: NetFlow for Cybersecurity** covers the details about NetFlow, all NetFlow versions, and how to use NetFlow for cybersecurity operations.

Part III Incident Response

- **Chapter 5: Introduction to Incident Response and the Incident Handling Process** provides an introduction to incident response, the incident response plan, the incident response process, and details about information sharing and incident coordination. This chapter covers the different incident response team structures.
- **Chapter 6: Incident Response Teams** covers the different types of incident response teams, including Computer Security Incident Response Teams (CSIRTs), Product Security Incident Response Teams (PSIRTs), national CSIRTs, and Computer Emergency Response Teams (CERTs), coordination centers, and incident response providers and managed security service providers (MSSPs).

- **Chapter 7: Compliance Frameworks** provides an introduction to the different industry compliance frameworks, including the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act of 2002 (SOX).

- **Chapter 8: Network and Host Profiling** covers how to perform network and host profiling. The results of these profiling methodologies may be used to determine the access rights that will be granted to the system, to identify potentially malicious behavior, to troubleshoot, to audit for compliance, and so on.

Part IV Data and Event Analysis

- **Chapter 9: The Art of Data and Event Analysis** covers how to normalize security event data and also how to use the 5-tuple correlation to respond to security incidents. This chapter also covers what retrospective analysis is and identifying malicious files with different security tools in the industry, such as Cisco AMP. In this chapter, you will also learn how to map threat intelligence with DNS and other artifacts to respond to security incidents and identify malicious files and transactions in your network. At the end of this chapter, you will learn the difference between deterministic and probabilistic analysis.

Part V Incident Handling

- **Chapter 10: Intrusion Event Categories** covers the different intrusion event categories. You will learn what the Diamond Model of Intrusion is as well as how to apply the VERIS schema categories to a given incident.

Part VI: Final Preparation

- **Chapter 11: Final Preparation** identifies the tools for final exam preparation and helps you develop an effective study plan. It contains tips on how to best use the web-based material to study.

Part VII Appendixes

- **Appendix A: Answers to "Do I Know This Already?" Quizzes and Q&A Questions** includes the answers to all the questions from Chapters 1 through 10.

- **Appendix B: Memory Tables and Lists** (a website-only appendix) contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exam. This appendix is available in PDF format on the book website; it is not in the printed book.

- **Appendix C: Memory Tables and Lists Answer Key** (a website-only appendix) contains the answer key for the memory tables in Appendix B. This appendix is available in PDF format on the book website; it is not in the printed book.

- **Appendix D: Study Planner** (a website-only appendix) is a spreadsheet with major study milestones, where you can track your progress throughout your study.

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. Enter the ISBN 9781587147036.
3. Answer the challenge question as proof of purchase.
4. Click the "Access Bonus Content" link in the Registered Products section of your account page, to be taken 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 steps, please visit 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.

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 http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.
4. In the My Products tab, click the **Activate New Product** button.

5. Enter the access code printed on the insert card in the back of your book to activate your product.
6. The product will now be listed in your My Products page. 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 the following 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 PearsonITCertification.com/register and entering the ISBN 978158714706.
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 then follow the onscreen instructions to complete the registration.
8. Once the installation is complete, launch the application and select 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 allows 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 a specific part in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters 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. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four 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, and 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 exam.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select 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 select the **Update Application** button. This will ensure you are running the latest version of the software engine.

This chapter covers the following topics:

- Introduction to incident response
- The incident response plan
- The incident response process
- Information sharing and coordination
- Incident response team structure

CHAPTER 5

Introduction to Incident Response and the Incident Handling Process

This chapter starts with an introduction to incident response and the different guidelines provided by the National Institute of Standards and Technology (NIST). In this chapter, you will learn the details about how to create an incident response plan and a good incident response process. You will also learn details about information sharing and coordination and the different incident response team structures.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you identify your strengths and deficiencies in this chapter's topics. The 10-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time. Table 5-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 5-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Introduction to Incident Response	1
The Incident Response Plan	2–3
The Incident Response Process	4–6
Information Sharing and Coordination	7–8
Incident Response Team Structure	9–10

1. What NIST special publication covers the incident response process?
   - **a.** Special Publication 800-61
   - **b.** Judiciary, private, and individual investigations
   - **c.** Public, private, and corporate investigations
   - **d.** Government, corporate, and private investigations
2. Which of the following is not part of the policy elements described in NIST's Special Publication 800-61?
   - **a.** Statement of management commitment
   - **b.** Purpose and objectives of the incident response policy
   - **c.** The scope of the incident response policy
   - **d.** Definition of QoS policies in network infrastructure devices

3. Which of the following is NIST's definition of standard operating procedures (SOPs)?
   a. A delineation of the specific IPS signatures to be deployed in the network
   b. A delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team
   c. A delineation of the specific firewall rules to be deployed in the network
   d. A suspect-led approach that's mostly used in private investigations
4. Which of the following is not a phase of the incident response process?
   a. Preparation
   b. Containment, eradication, and recovery
   c. Post-incident activity
   d. Network monitoring phase
5. Incident prioritization is part of which phase of the incident response process?
   a. Preparation
   b. Containment, eradication, and recovery
   c. Post-incident activity
   d. Detection and analysis
6. Which of the following is not part of the post-incident activity phase?
   a. Lessons learned
   b. Identifying the attacking hosts
   c. Using collected incident data
   d. Evidence retention
7. Which of the following is a good example of an information-sharing community?
   a. The National Institute of Security and Technology (NIST)
   b. The National Institute of Standards and Technology (NIST)
   c. The Cyber Services Information Sharing and Analysis Center (CS-ISAC)
   d. The Financial Services Information Sharing and Analysis Center (FS-ISAC)
8. During the investigation and resolution of a security incident, you may also need to communicate with outside parties regarding the incident. Which of the following are examples of those external entities?
   a. Law enforcement
   b. Internet service providers (ISPs)
   c. The vendor of your hardware and software products
   d. Coordination centers

9. Which of the following is not an example of a type of incident response team?

- **a.** Product Security Incident Response Team (PSIRT)
- **b.** National CSIRT and Computer Emergency Response Team (CERT)
- **c.** Incident response team of a security vendor and managed security service provider (MSSP)
- **d.** Penetration testing team

10. Which of the following is not an example of the most common incident response team structures?

- **a.** Product Security Incident Response Team (PSIRT)
- **b.** Centralized incident response team
- **c.** Distributed incident response team
- **d.** Coordinating team

Foundation Topics

This chapter starts with an introduction to incident response. Then it describes, in detail, the incident response plan and incident response process, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61. This chapter also touches on how to share information and coordinate with external parties during the investigation of security incidents. You will also learn the different incident response team structures.

Introduction to Incident Response

Key Topic

Computer security incident response is a critical component of information technology (IT) programs. The incident response process and incident handling activities can be very complex. In order for you to establish a successful incident response program, you must dedicate substantial planning and resources. Several industry resources were created to help organizations establish a computer security incident response program and learn how to handle cybersecurity incidents efficiently and effectively. One of the best resources available is NIST Special Publication 800-61, which can be obtained from the following URL:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST developed Special Publication 800-61 due to statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

You will learn the basics of the guidelines provided in NIST Special Publication 800-61 in this chapter, as required for the CCNA Cyber Ops SECOPS exam, but you should also read it and become familiar with all the topics discussed in that publication.

What Are Events and Incidents?

Key Topic

Before you learn the details about how to create a good incident response program within your organization, you must understand the difference between security "events" and security "incidents." The following is from NIST Special Publication 800-61:

> "An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data."

According to the same document, "a computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

NOTE In Chapter 3, "Fundamentals of Intrusion Analysis," you learned that some security events can also be false positives or true positives.

Figure 5-1 lists a few examples of security incidents.

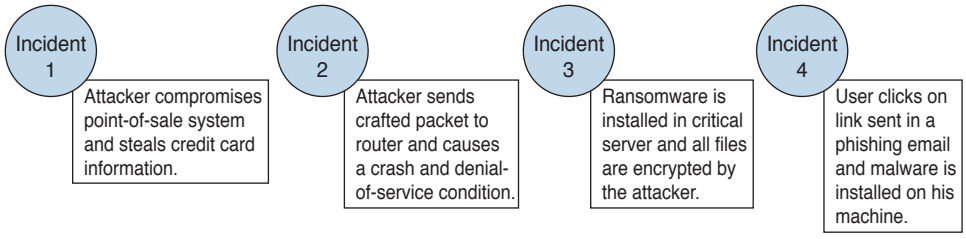

Figure 5-1 *Sample Security Events*

Key Topic

The Incident Response Plan

Having a good incident response plan and incident response process will help you minimize loss or theft of information and disruption of services caused by incidents. It will also help you enhance your incident response program by using lessons learned and information obtained during the security incident.

Section 2.3 of NIST Special Publication 800-61 goes over the incident response policies, plans, and procedures, including information on how to coordinate incidents and interact with outside parties. The policy elements described in NIST Special Publication 800-61 include the following:

- Statement of management commitment
- Purpose and objectives of the incident response policy
- The scope of the incident response policy
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms

NIST's incident response plan elements include the following:

- Incident response plan's mission
- Strategies and goals of the incident response plan
- Senior management approval of the incident response plan
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

NIST also defines standard operating procedures (SOPs) as "a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations."

The Incident Response Process

NIST Special Publication 800-61 goes over the major phases of the incident response process in detail. You should become familiar with that publication, as it provides additional information that will help you succeed in your security operations center (SOC). The important key points are summarized here.

NIST defines the major phases of the incident response process as illustrated in Figure 5-2.

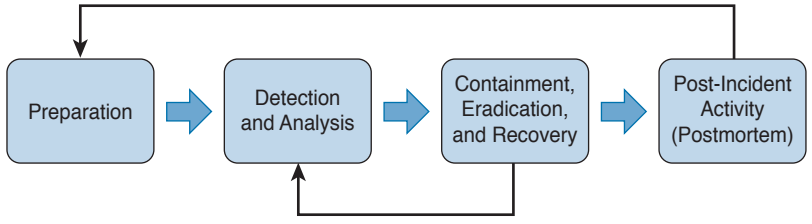

Figure 5-2 *The Major Phases of the Incident Response Process*

The Preparation Phase

The preparation phase includes creating and training the incident response team, as well as deploying the necessary tools and resources to successfully investigate and resolve cybersecurity incidents. In this phase, the incident response team creates a set of controls based on the results of risk assessments. The preparation phase also includes the following tasks:

- Creating processes for incident handler communications and the facilities that will host the security operation center (SOC) and incident response team
- Making sure that the organization has appropriate incident analysis hardware and software as well as incident mitigation software
- Creating risk assessment capabilities within the organization
- Making sure the organization has appropriately deployed host security, network security, and malware prevention solutions
- Developing user awareness training

The Detection and Analysis Phase

The detection and analysis phase is one of the most challenging phases. While some incidents are easy to detect (for example, a denial-of-service attack), many breaches and attacks are left undetected for weeks or even months. This is why detection may be the most difficult task in incident response. The typical network is full of "blind spots" where anomalous traffic goes undetected. Implementing analytics and correlation tools is critical to eliminating these network blind spots. As a result, the incident response team must react quickly

to analyze and validate each incident. This is done by following a predefined process while documenting each step the analyst takes. NIST provides several recommendations for making incident analysis easier and more effective:

- Profile networks and systems
- Understand normal behaviors
- Create a log retention policy
- Perform event correlation
- Maintain and use a knowledge base of information
- Use Internet search engines for research
- Run packet sniffers to collect additional data
- Filter the data
- Seek assistance from others
- Keep all host clocks synchronized
- Know the different types of attacks and attack vectors
- Develop processes and procedures to recognize the signs of an incident
- Understand the sources of precursors and indicators
- Create appropriate incident documentation capabilities and processes
- Create processes to effectively prioritize security incidents
- Create processes to effectively communicate incident information (internal and external communications)

Containment, Eradication, and Recovery

The containment, eradication, and recovery phase includes the following activities:

- Evidence gathering and handling
- Identifying the attacking hosts
- Choosing a containment strategy to effectively contain and eradicate the attack, as well as to successfully recover from it

NIST Special Publication 800-61 also defines the following criteria for determining the appropriate containment, eradication, and recovery strategy:

- The potential damage to and theft of resources
- The need for evidence preservation
- Service availability (for example, network connectivity as well as services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (for example, partial containment or full containment)
- Duration of the solution (for example, emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, or permanent solution)

Post-Incident Activity (Postmortem)

The post-incident activity phase includes lessons learned, how to use collected incident data, and evidence retention. NIST Special Publication 800-61 includes several questions that can be used as guidelines during the lessons learned meeting(s):

- Exactly what happened, and at what times?
- How well did the staff and management perform while dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations be improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Information Sharing and Coordination

During the investigation and resolution of a security incident, you may also need to communicate with outside parties regarding the incident. Examples include, but are not limited to, contacting law enforcement, fielding media inquiries, seeking external expertise, and working with Internet service providers (ISPs), the vendor of your hardware and software products, threat intelligence vendor feeds, coordination centers, and members of other incident response teams. You can also share relevant incident indicator of compromise (IoC) information and other observables with industry peers. A good example of information-sharing communities includes the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Your incident response plan should account for these types of interactions with outside entities. It should also include information about how to interact with your organization's public relations (PR) department, legal department, and upper management. You should also get their buy-in when sharing information with outside parties to minimize the risk of information leakage. In other words, avoid leaking sensitive information regarding security incidents with unauthorized parties. These actions could potentially lead to additional disruption and financial loss. You should also maintain a list of all the contacts at those external entities, including a detailed list of all external communications for liability and evidentiary purposes.

Incident Response Team Structure

In Chapter 6, "Incident Response Teams," you will learn all the details about incident response teams. There are different incident response teams. The most popular is the

Computer Incident Response Team (CSIRT) within your organization. Others include the following:

- Product Security Incident Response Team (PSIRT)
- National CSIRTs and Computer Emergency Response Team (CERT)
- Coordination center
- Incident response teams of security vendors and managed security service providers (MSSP)

The following are the most common incident response team structures:

- Centralized incident response team
- Distributed incident response team
- Coordinating team

The following are the most common incident response team staffing models:

- Employees
- Partially outsourced
- Fully outsourced

The Vocabulary for Event Recording and Incident Sharing (VERIS)

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a collection of schemas and a common language for describing security incidents in a standard way. VERIS was first created by a team of cybersecurity professionals from Verizon and other industry peers. It has now been adopted by many security teams in the industry.

Key Topic

The VERIS documentation can be found at: http://veriscommunity.net/index.html

TIP You will learn all the elements of the VERIS schema in this chapter, but it is recommended that you review and become familiar with the VERIS documentation at the VERIS website (http://veriscommunity.net). You can also access several tools that the community has created at their GitHub repository at: https://github.com/vz-risk.

The VERIS schema and examples can be accessed at the VERIS GitHub repository at: https://github.com/vz-risk/veris.

The VERIS schema is divided into the following five main sections:

- Incident Tracking
- Victim Demographics
- Incident Description
- Discovery & Response
- Impact Assessment

Figure 5-3 includes a mind-map that illustrates these five sections and their related elements.

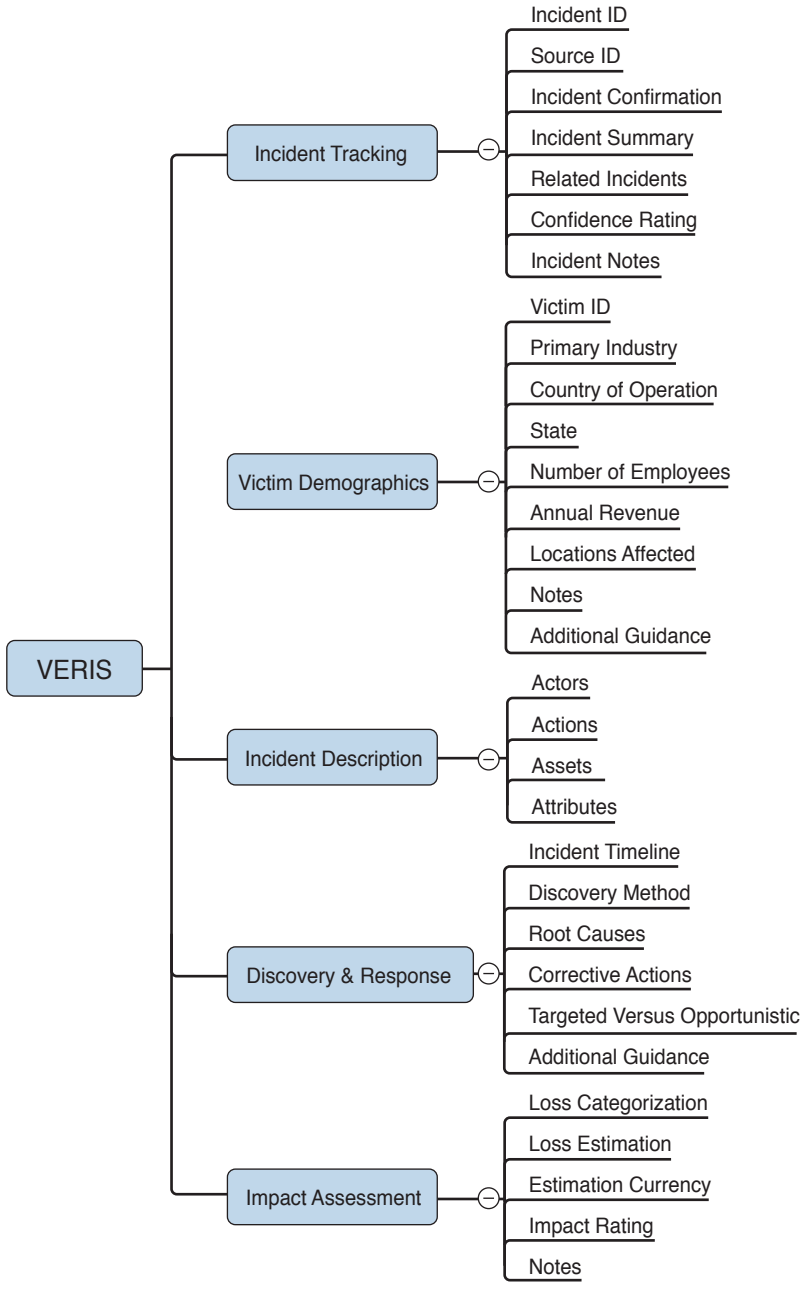

Figure 5-3 *The VERIS Schema*

As you can see in Figure 5-3, the Incident Tracking section contains the following elements:

- Incident ID—an identifier for the incident.
- Source ID—the source or handler ID of the incident.
- Incident Confirmation—whether the security incident has been confirmed or not confirmed.
- Incident Summary—the summary of the incident.
- Related Incidents—any other related incidents.
- Confidence Rating—an enumerated list that describes how certain you are that the information pertaining to this incident is complete.
- Incident Notes—any additional notes that may be relevant to the incident description.

The Victim Demographics section contains the following elements:

- Victim ID—an identifier of the victim.
- Primary Industry—the victim's primary industry (for example, healthcare, manufacturing, banking, IT, and so on).
- Country of Operation—the country the victim operates in
- State—the state or region of operation.
- Number of Employees—the number of employees of the victim organization.
- Annual Revenue—the annual revenue of the victim organization.
- Locations Affected—the locations affected by the incident.
- Notes—any additional notes about the victim.
- Additional Guidance—any additional guidance you may want to provide about the victim and incident.

The Incident Description section contains the following elements:

- Actors—the known threat actors.
- Actions—the actions taken by the threat actor(s).
- Assets—the assets that were compromised.
- Attributes—any additional attributes related to the CIA triad.

The Discovery & Response section contains the following elements:

- Incident Timeline—the incident timeline.
- Discovery Method—the methodology used to discover the incident.
- Root Causes—the incident root cause(s).
- Corrective Actions—any corrective actions to mitigate and remediate the incident.
- Targeted vs. Opportunistic—to describe if the incident was targeted or opportunistic.
- Additional Guidance—any additional guidance about the incident.

The Impact Assessment section contains the following elements:

- Loss Categorization—describes the different types of losses experienced as a result of the incident (direct or indirect losses).
- Loss Estimation—an estimate of all the losses experienced because of the incident.
- Estimation Currency—the currency used in the loss estimation (for example, US dollar, EURO, and so on)
- Impact Rating—a rating used to describe the overall impact of the incident.
- Notes—any additional notes about the impact and losses.

One of the main purposes of VERIS is to categorize incident data so that it can be used as lessons learned and shared among security professionals and many organizations. VERIS created an open source database of incident information called the VERIS Community Database (VCDB). This database can be accessed at the following GitHub repository: https://github.com/vz-risk/VCDB.

There is also a useful tool that can get you started adopting VERIS called the VERIS Incident Recording Tool and it can be accessed at: https://incident.veriscommunity.net/s3/example You can play with this tool to become familiar with all the different fields, the VERIS schema, and how to apply VERIS to your incident handling process.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 5-2 lists these key topics and the page numbers on which each is found.

Key Topic

Table 5-2 Key Topics

Key Topic Element	Description	Page
Paragraph	What is incident response?	144
Summary	What are security events and incidents?	144
Summary	Understanding the incident response plan.	145
Summary	Understanding the incident response process.	146
Summary	Understanding information sharing and coordination.	148
Summary	Applying VERIS to the incident response and incident handling process.	149

Complete Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables," (found on the book website), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key," also on the website, includes completed tables and lists to check your work.

Define Key Terms

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

security event, security incident, standard operating procedure

Q&A

The answers to these questions appear in Appendix A, "Answers to the 'Do I Know This Already' Quizzes and Q&A." For more practice with exam format questions, use the exam engine on the website.

1. What is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices?
   - **a.** Exploit
   - **b.** Vulnerability
   - **c.** Threat
   - **d.** Computer security incident

2. What is a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team?
   a. CSIRT team plan
   b. Standard operating procedure (SOP)
   c. Standard incident plan (SIP)
   d. Operation and incident plan (OIP)
3. What is any observable occurrence in a system or network?
   a. Security event
   b. Security incident
   c. Security vulnerability
   d. An exploit
4. Which of the following is not an example of the most common incident response team staffing models?
   a. Employees
   b. Partially outsourced
   c. Fully outsourced
   d. PSIRT
5. The containment, eradication, and recovery phase includes which of the following? (Choose two.)
   a. Choosing a firewall to be able to block traffic proactively or during an attack
   b. Choosing an intrusion prevention system to be able to block traffic proactively or during an attack
   c. Choosing a containment strategy to effectively contain and eradicate the attack, as well as to be able to successfully recover from it
   d. Evidence gathering and handling
6. Which phase in the incident response process includes lessons learned, how to use collected incident data, and evidence retention?
   a. Post-incident activity (postmortem)
   b. Containment, eradication, and recovery
   c. The detection and analysis phase
   d. The preparation phase
7. Which phase in the incident response process includes creating processes for incident handler communications and the facilities that will host the security operation center (SOC) and incident response team?
   a. The preparation phase
   b. The detection and analysis phase
   c. Containment, eradication, and recovery
   d. Post-incident activity (postmortem)

8. Which of following are examples of the most common incident response team structures? (Choose two.)

   a. Centralized incident response team
   b. Partially outsourced
   c. Fully outsourced
   d. Distributed incident response team

9. Which of following is not an example of the VERIS main schema categories?

   a. Incident Tracking
   b. Victim Demographics
   c. Incident Description
   d. Incident Forensics ID

10. Which of following is not an example of an element in the Incident Description section of the VERIS schema?

    a. Actors
    b. Actions
    c. Victims and Losses
    d. Attributes