

Second Edition

Save 10%
on Exam Vouchers
Coupon Inside!

CompTIA® CySA+

STUDY GUIDE

EXAM CS0-002

Includes one year of FREE access after activation to the online
test bank and study tools:

2 custom practice exams
100 electronic flashcards
Searchable key term glossary



MIKE CHAPPLE
DAVID SEIDL

SYBEX
A Wiley Brand

Table of Contents

[Cover](#)

[Acknowledgments](#)

[About the Authors](#)

[About the Technical Editor](#)

[Introduction](#)

[What Does This Book Cover?](#)

[Objectives Map for CompTIA Cybersecurity Analyst \(CySA+\) Exam CS0-002](#)

[Setting Up a Kali and Metasploitable Learning Environment](#)

[Assessment Test](#)

[Answers to the Assessment Test](#)

[Chapter 1: Today's Cybersecurity Analyst](#)

[Cybersecurity Objectives](#)

[Privacy vs. Security](#)

[Evaluating Security Risks](#)

[Building a Secure Network](#)

[Secure Endpoint Management](#)

[Penetration Testing](#)

[Reverse Engineering](#)

[The Future of Cybersecurity Analytics](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 2: Using Threat Intelligence](#)

[Threat Data and Intelligence](#)

[Threat Classification](#)

[Attack Frameworks](#)

[Applying Threat Intelligence Organizationwide](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 3: Reconnaissance and Intelligence Gathering](#)

[Mapping and Enumeration](#)

[Passive Footprinting](#)

[Gathering Organizational Intelligence](#)

[Detecting, Preventing, and Responding to Reconnaissance](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 4: Designing a Vulnerability Management Program](#)

[Identifying Vulnerability Management Requirements](#)

[Configuring and Executing Vulnerability Scans](#)

[Developing a Remediation Workflow](#)

[Overcoming Risks of Vulnerability Scanning](#)

[Vulnerability Scanning Tools](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 5: Analyzing Vulnerability Scans](#)

[Reviewing and Interpreting Scan Reports](#)

[Validating Scan Results](#)

[Common Vulnerabilities](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 6: Cloud Security](#)

[Understanding Cloud Environments](#)

[Operating in the Cloud](#)

[Cloud Infrastructure Security](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 7: Infrastructure Security and Controls](#)

[Understanding Defense-in-Depth](#)

[Improving Security by Improving Controls](#)

[Analyzing Security Architecture](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 8: Identity and Access Management Security](#)

[Understanding Identity](#)

[Threats to Identity and Access](#)

[Identity as a Security Layer](#)

[Federation and Single Sign-On](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 9: Software and Hardware Development Security](#)

[Software Assurance Best Practices](#)

[Designing and Coding for Security](#)

[Software Security Testing](#)

[Hardware Assurance Best Practices](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 10: Security Operations and Monitoring](#)

[Security Monitoring](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 11: Building an Incident Response Program](#)

[Security Incidents](#)

[Phases of Incident Response](#)

[Building the Foundation for Incident Response](#)

[Creating an Incident Response Team](#)

[Coordination and Information Sharing](#)

[Classifying Incidents](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 12: Analyzing Indicators of Compromise](#)

[Analyzing Network Events](#)

[Investigating Host-Related Issues](#)

[Investigating Service and Application-Related Issues](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 13: Performing Forensic Analysis and Techniques](#)

[Building a Forensics Capability](#)

[Understanding Forensic Software](#)

[Conducting Endpoint Forensics](#)

[Network Forensics](#)

[Cloud, Virtual, and Container Forensics](#)

[Conducting a Forensic Investigation](#)

[Forensic Investigation: An Example](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 14: Containment, Eradication, and Recovery](#)

[Containing the Damage](#)

[Incident Eradication and Recovery](#)

[Wrapping Up the Response](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 15: Risk Management](#)

[Analyzing Risk](#)

[Managing Risk](#)

[Security Controls](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Chapter 16: Policy and Compliance](#)

[Understanding Policy Documents](#)

[Complying with Laws and Regulations](#)

[Adopting a Standard Framework](#)

[Implementing Policy-Based Controls](#)

[Security Control Verification and Quality Control](#)

[Summary](#)

[Exam Essentials](#)

[Lab Exercises](#)

[Review Questions](#)

[Appendix A: Practice Exam](#)

[Exam Questions](#)

[Appendix B: Answers to Review Questions and Practice Exam](#)

[Chapter 1: Today's Cybersecurity Analyst](#)

[Chapter 2: Using Threat Intelligence](#)

[Chapter 3: Reconnaissance and Intelligence Gathering](#)

[Chapter 4: Designing a Vulnerability Management Program](#)

[Chapter 5: Analyzing Vulnerability Scans](#)

[Chapter 6: Cloud Security](#)

[Chapter 7: Infrastructure Security and Controls](#)

[Chapter 8: Identity and Access Management Security](#)

[Chapter 9: Software and Hardware Development Security](#)

[Chapter 10: Security Operations and Monitoring](#)

[Chapter 11: Building an Incident Response Program](#)

[Chapter 12: Analyzing Indicators of Compromise](#)

[Chapter 13: Performing Forensic Analysis and Techniques](#)

[Chapter 14: Containment, Eradication, and Recovery](#)

[Chapter 15: Risk Management](#)

[Chapter 16: Policy and Compliance](#)

[Practice Exam Answers](#)

[Appendix C: Answers to Lab Exercises](#)

[Chapter 1: Today's Cybersecurity Analyst](#)

[Chapter 2: Using Threat Intelligence](#)

[Chapter 3: Reconnaissance and Intelligence Gathering](#)

[Chapter 5: Analyzing Vulnerability Scans](#)

[Chapter 7: Infrastructure Security and Controls](#)

[Chapter 8: Identity and Access Management Security](#)

[Chapter 9: Software and Hardware Development Security](#)

[Chapter 10: Security Operations and Monitoring](#)

[Chapter 11: Building an Incident Response Program](#)

[Chapter 12: Analyzing Indicators of Compromise](#)

[Chapter 13: Performing Forensic Analysis and Techniques](#)

[Chapter 14: Containment, Eradication, and Recovery](#)

[Chapter 15: Risk Management](#)

[Chapter 16: Policy and Compliance](#)

[Index](#)

[End User License Agreement](#)

List of Tables

Introduction

[TABLE I.1 Virtual machine network options](#)

Chapter 1

[TABLE 1.1 Common TCP ports](#)

Chapter 3

[TABLE 3.1 Cisco log levels](#)

Chapter 5

[TABLE 5.1 CVSS attack vector metric](#)

[TABLE 5.2 CVSS attack complexity metric](#)

[TABLE 5.3 CVSS privileges required metric](#)

[TABLE 5.4 CVSS user interaction metric](#)

[TABLE 5.5 CVSS confidentiality metric](#)

[TABLE 5.6 CVSS integrity metric](#)

[TABLE 5.7 CVSS availability metric](#)

[TABLE 5.8 CVSS scope metric](#)

[TABLE 5.9 CVSS Qualitative Severity Rating Scale](#)

Chapter 8

[TABLE 8.1 Comparison of federated identity technologies](#)

Chapter 9

[TABLE 9.1 Code review method comparison](#)

Chapter 10

[TABLE 10.1 grep flags](#)

Chapter 11

[TABLE 11.1 NIST functional impact categories](#)

[TABLE 11.2 Economic impact categories](#)

[TABLE 11.3 NIST recoverability effort categories](#)

[TABLE 11.4 NIST information impact categories](#)

[TABLE 11.5 Private organization information impact categories](#)

Chapter 12

[TABLE 12.1 Unauthorized use and detection mechanisms](#)

Chapter 13

[TABLE 13.1 Forensic application of Windows system artifacts](#)

[TABLE 13.2 Key iOS file locations](#)

Chapter 16

[TABLE 16.1 NIST Cybersecurity framework implementation tiers](#)

List of Illustrations

Introduction

[FIGURE I.1 VirtualBox main screen](#)

[FIGURE I.2 Adding the Metasploitable VM](#)

[FIGURE I.3 Adding a NAT network](#)

[FIGURE I.4 Configuring VMs for the NAT network](#)

Chapter 1

[FIGURE 1.1 The three key objectives of cybersecurity programs are confidentiality, integrity, and availability](#)

[FIGURE 1.2 Risks exist at the intersection of threats and vulnerabilities. I...](#)

[FIGURE 1.3 The NIST SP 800-30 risk assessment process suggests that an organization should assess risk at the system, component, and data levels](#)

[FIGURE 1.4 Many organizations use a risk matrix to determine an overall risk level](#)

[FIGURE 1.5 In an 802.1x system, the device attempting to join the network must first be authenticated](#)

[FIGURE 1.6 A triple-homed firewall connects to three different networks, typically the Internet, an intranet, and a DMZ](#)

[FIGURE 1.7 A triple-homed firewall may also be used to isolate internal networks from the Internet](#)

[FIGURE 1.8 Group Policy Objects \(GPOs\) may be used to apply settings to many...](#)

[FIGURE 1.9 NIST divides penetration testing into four phases.](#)

[FIGURE 1.10 The attack phase of a penetration test uses a cyclical process t...](#)

Chapter 2

[FIGURE 2.1 Recent alert listing from the CISA website](#)

[FIGURE 2.2 The threat intelligence cycle](#)

[FIGURE 2.3 A Talos reputation report for a single host](#)

[FIGURE 2.4 The ATT&CK definition for Cloud Instance Metadata API attacks](#)

[FIGURE 2.5 A Diamond Model analysis of a compromised system](#)

[FIGURE 2.6 The Cyber Kill Chain.](#)

Chapter 3

[FIGURE 3.1 Zenmap topology view](#)

[FIGURE 3.2 Nmap scan results](#)

[FIGURE 3.3 Nmap service and version detection](#)

[FIGURE 3.4 Nmap of a Windows 10 system](#)

[FIGURE 3.5 Angry IP Scanner](#)

[FIGURE 3.6 Cisco router log](#)

[FIGURE 3.7 SNMP configuration from a typical Cisco router](#)

[FIGURE 3.8 Linux netstat -ta output](#)

[FIGURE 3.9 Windows netstat -o output](#)

[FIGURE 3.10 Windows netstat -e output](#)

[FIGURE 3.11 Windows netstat -nr output](#)

[FIGURE 3.12 Linux dhcpd.conf file](#)

[FIGURE 3.13 Nslookup for google.com](#)

[FIGURE 3.14 Nslookup using Google's DNS with MX query flag](#)

[FIGURE 3.15 Traceroute for bbc.co.uk](#)

[FIGURE 3.16 Whois query data for google.com](#)

[FIGURE 3.17 host command response for google.com](#)

[FIGURE 3.18 Responder start-up screen](#)

[FIGURE 3.19 Packet capture data from an nmap scan](#)

[FIGURE 3.20 Demonstration account from immersion.media.mit.edu](#)

Chapter 4

[FIGURE 4.1 FIPS 199 Standards](#)

[FIGURE 4.2 Qualys asset map](#)

[FIGURE 4.3 Configuring a Nessus scan](#)

[FIGURE 4.4 Sample Nessus scan report](#)

[FIGURE 4.5 Nessus scan templates](#)

[FIGURE 4.6 Disabling unused plug-ins](#)

[FIGURE 4.7 Configuring authenticated scanning](#)

[FIGURE 4.8 Choosing a scan appliance](#)

[FIGURE 4.9 Nessus vulnerability in the NIST National Vulnerability Database...](#)

[FIGURE 4.10 Nessus Automatic Updates](#)

[FIGURE 4.11 Vulnerability management life cycle](#)
[FIGURE 4.12 Qualys dashboard example](#)
[FIGURE 4.13 Nessus report example by IP address](#)
[FIGURE 4.14 Nessus report example by criticality](#)
[FIGURE 4.15 Detailed vulnerability report](#)
[FIGURE 4.16 Qualys scan performance settings](#)
[FIGURE 4.17 Nikto web application scanner](#)
[FIGURE 4.18 Arachni web application scanner](#)
[FIGURE 4.19 Nessus web application scanner](#)
[FIGURE 4.20 Zed Attack Proxy \(ZAP\)](#)
[FIGURE 4.21 Burp Proxy](#)

Chapter 5

[FIGURE 5.1 Nessus vulnerability scan report](#)
[FIGURE 5.2 Qualys vulnerability scan report](#)
[FIGURE 5.3 Scan report showing vulnerabilities and best practices](#)
[FIGURE 5.4 Vulnerability trend analysis](#)
[FIGURE 5.5 Vulnerabilities exploited in 2015 by year of initial discovery](#)
[FIGURE 5.6 Missing patch vulnerability](#)
[FIGURE 5.7 Unsupported operating system vulnerability](#)
[FIGURE 5.8 Dirty COW website](#)
[FIGURE 5.9 Code execution vulnerability](#)
[FIGURE 5.10 FTP cleartext authentication vulnerability](#)

[FIGURE 5.11 Debug mode vulnerability](#)

[FIGURE 5.12 Outdated SSL version vulnerability](#)

[FIGURE 5.13 Insecure SSL cipher vulnerability](#)

[FIGURE 5.14 Invalid certificate warning](#)

[FIGURE 5.15 DNS amplification vulnerability](#)

[FIGURE 5.16 Internal IP disclosure vulnerability](#)

[FIGURE 5.17 Inside a virtual host](#)

[FIGURE 5.18 SQL injection vulnerability](#)

[FIGURE 5.19 Cross-site scripting vulnerability](#)

[FIGURE 5.20 Alice communicating with a bank web server](#)

[FIGURE 5.21 Man-in-the-middle attack](#)

[FIGURE 5.22 First vulnerability report](#)

[FIGURE 5.23 Second vulnerability report](#)

Chapter 6

[FIGURE 6.1 Google's Gmail is an example of SaaS computing.](#)

[FIGURE 6.2 Slate is a CRM tool designed specifically for higher education ad...](#)

[FIGURE 6.3 AWS provides customers with access to IaaS computing resources.](#)

[FIGURE 6.4 Heroku is a popular PaaS offering that supports many popular prog...](#)

[FIGURE 6.5 HathiTrust is an example of community cloud computing.](#)

[FIGURE 6.6 AWS Outposts offer hybrid cloud capability.](#)

[FIGURE 6.7 Shared responsibility model for cloud computing](#)

[FIGURE 6.8 Creating an EC2 instance through the AWS web interface](#)

[FIGURE 6.9 Creating an EC2 instance with CloudFormation JSON](#)

[FIGURE 6.10 Results of an AWS Inspector scan.](#)

[FIGURE 6.11 ScoutSuite dashboard from an AWS account scan](#)

[FIGURE 6.12 EC2 security issues reported during a ScoutSuite scan](#)

[FIGURE 6.13 Partial listing of the exploits available in Pacu](#)

[FIGURE 6.14 Partial results of a Prowler scan against an AWS account](#)

Chapter 7

[FIGURE 7.1 Layered security network design](#)

[FIGURE 7.2 Network segmentation with a protected network](#)

[FIGURE 7.3 Linux permissions](#)

[FIGURE 7.4 A fully redundant network edge design](#)

[FIGURE 7.5 Single points of failure in a network design](#)

[FIGURE 7.6 Single points of failure in a process flow](#)

[FIGURE 7.7 Sample security architecture](#)

Chapter 8

[FIGURE 8.1 A high-level logical view of identity management infrastructure](#)

[FIGURE 8.2 LDAP directory structure](#)

[FIGURE 8.3 Kerberos authentication flow](#)

[FIGURE 8.4 OAuth covert redirects](#)

[FIGURE 8.5 A sample account life cycle](#)

[FIGURE 8.6 Phishing for a PayPal ID](#)

[FIGURE 8.7 Authentication security model](#)

[FIGURE 8.8 Google Authenticator token](#)

[FIGURE 8.9 Context-based authentication](#)

[FIGURE 8.10 Federated identity high-level design](#)

[FIGURE 8.11 Attribute release request for LoginRadius.com](#)

[FIGURE 8.12 Simple SAML transaction](#)

[FIGURE 8.13 OAuth authentication process](#)

Chapter 9

[FIGURE 9.1 High-level SDLC view](#)

[FIGURE 9.2 The Waterfall SDLC model](#)

[FIGURE 9.3 The Spiral SDLC model](#)

[FIGURE 9.4 Agile sprints](#)

[FIGURE 9.5 Rapid Application Development prototypes](#)

[FIGURE 9.6 The CI/CD pipeline](#)

[FIGURE 9.7 Fagan code review](#)

[FIGURE 9.8 Tamper Data session showing login data](#)

Chapter 10

[FIGURE 10.1 Windows Event Viewer entries](#)

[FIGURE 10.2 Linux syslog entries in auth.log with sudo events](#)

[FIGURE 10.3 UFW blocked connection firewall log entry examples](#)

[FIGURE 10.4 ModSecurity log entry examples](#)

[FIGURE 10.5 SIEM data acquisition, rule creation, and automation](#)

[FIGURE 10.6 The Windows 10 Resource Monitor](#)

[FIGURE 10.7 Linux ps output](#)

[FIGURE 10.8 SolarWinds network flow console](#)

[FIGURE 10.9 Wireshark packet analysis with packet content detail](#)

[FIGURE 10.10 Headers from a phishing email](#)

Chapter 11

[FIGURE 11.1 Incident response process](#)

[FIGURE 11.2 Incident response checklist](#)

Chapter 12

[FIGURE 12.1 Routers provide a central view of network traffic flow by sendin...](#)

[FIGURE 12.2 NetFlow data example](#)

[FIGURE 12.3 Passive monitoring between two systems](#)

[FIGURE 12.4 PRTG network overview](#)

[FIGURE 12.5 Beaconing in Wireshark](#)

[FIGURE 12.6 Unexpected network traffic shown in flows](#)

[FIGURE 12.7 nmap scan of a potential rogue system](#)

[FIGURE 12.8 The Windows Resource Monitor view of system resources](#)

[FIGURE 12.9 The Windows Performance Monitor view of system usage](#)

[FIGURE 12.10 The Windows Task Scheduler showing scheduled tasks and creation...](#)

Chapter 13

[FIGURE 13.1 Sample chain-of-custody form](#)

[FIGURE 13.2 Carving a JPEG file using HxD](#)

[FIGURE 13.3 Advanced Office Password Recovery cracking a Word DOC file](#)

[FIGURE 13.4 Wireshark view of network traffic](#)

[FIGURE 13.5 Tcpdump of network traffic](#)

[FIGURE 13.6 Virtualization vs. containerization](#)

[FIGURE 13.7 Order of volatility of common storage locations](#)

[FIGURE 13.8 dd of a volume](#)

[FIGURE 13.9 FTK image hashing and bad sector checking](#)

[FIGURE 13.10 USB Historian drive image](#)

[FIGURE 13.11 Initial case information and tracking](#)

[FIGURE 13.12 Case information and tracking partly through the indexing proce...](#)

[FIGURE 13.13 Email extraction](#)

[FIGURE 13.14 Web search history](#)

[FIGURE 13.15 iCloud setup log with timestamp](#)

[FIGURE 13.16 CCleaner remnant data via the Index Search function](#)

[FIGURE 13.17 Resignation letter found based on document type](#)

[FIGURE 13.18 Sample forensic finding from Stroz Friedberg's Facebook contrac...](#)

Chapter 14

[FIGURE 14.1 Incident response process](#)

[FIGURE 14.2 Proactive network segmentation](#)

[FIGURE 14.3 Network segmentation for incident response](#)

[FIGURE 14.4 Network isolation for incident response](#)

[FIGURE 14.5 Network removal for incident response](#)

[FIGURE 14.6 Patching priorities](#)

[FIGURE 14.7 Sanitization and disposition decision flow](#)

Chapter 15

[FIGURE 15.1 Risk exists at the intersection of a threat and a corresponding ...](#)

[FIGURE 15.2 Qualitative risk assessments use subjective rating scales to eva...](#)

[FIGURE 15.3 \(a\) STOP tag attached to a device \(b\) Residue remaining on devic...](#)

[FIGURE 15.4 Cover sheets used to identify classified U.S. government informa...](#)

Chapter 16

[FIGURE 16.1 Excerpt from CMS roles and responsibilities chart](#)

[FIGURE 16.2 Excerpt from UC Berkeley Minimum Security Standards for Electron...](#)

[FIGURE 16.3 NIST Cybersecurity Framework Core Structure](#)

[FIGURE 16.4 Asset Management Cybersecurity Framework](#)

[FIGURE 16.5 ITIL service life cycle](#)

**Take the Next Step
in Your IT Career**

**Save
10%
on Exam Vouchers***
(up to a \$35 value)
*Some restrictions apply. See web page for details.

CompTIA.

Get details at
www.wiley.com/go/sybextestprep

To get the discount code, you'll need to register and log on the test bank. Then go to Resources.



CompTIA® Cybersecurity Analyst (CySA+) Study Guide Exam CS0-002

Second Edition



Mike Chapple

David Seidl



Copyright © 2020 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada and the United Kingdom

ISBN: 978-1-119-68405-3

ISBN: 978-1-119-68408-4 (ebk.)

ISBN: 978-1-119-68411-4 (ebk.)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at

<http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020937966

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CompTIA is a registered trademark of Computing Technology Industry Association, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

I dedicate this book to my father, who was a role model of the value of hard work, commitment to family, and the importance of doing the right thing. Rest in peace, Dad.

—Mike Chapple

This book is dedicated to Ric Williams, my friend, mentor, and partner in crime through my first forays into the commercial IT world. Thanks for making my job as a “network janitor” one of the best experiences of my life.

—David Seidl

Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank senior acquisitions editor Kenyon Brown. We have worked with Ken on multiple projects and consistently enjoy our work with him.

We also greatly appreciated the editing and production team for the book, including Kezia Endsley, our project editor, who brought years of experience and great talent to the project, Chris Crayton, our technical editor, who provided insightful advice and gave wonderful feedback throughout the book, Saravanan Dakshinamurthy, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book, and Liz Welch, our copy editor, who helped the text flow well. Thanks also to Runzhi “Tom” Song, Mike’s research assistant at Notre Dame who helped fact-check our work. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families and significant others who support us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Mike Chapple, Ph.D., CySA+, is author of the best-selling *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (Sybex, 2018) and the *CISSP (ISC)² Official Practice Tests* (Sybex, 2018). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike is technical editor for *Information Security Magazine* and has written more than 25 books. He earned both his B.S. and Ph.D. degrees from Notre Dame in computer science and engineering. Mike also holds an M.S. in computer science from the University of Idaho and an MBA from Auburn University. Mike holds certifications in Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP).

David Seidl is Vice President for Information Technology and CIO at Miami University. During his IT career, he has

served in a variety of technical and information security roles, including serving as the Senior Director for Campus Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business, and he has written books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)² Official Practice Tests* (Sybex, 2018) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests: Exam CS0-001*.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as certifications in CISSP, CySA+, Pentest+, GPEN, and GCIH.