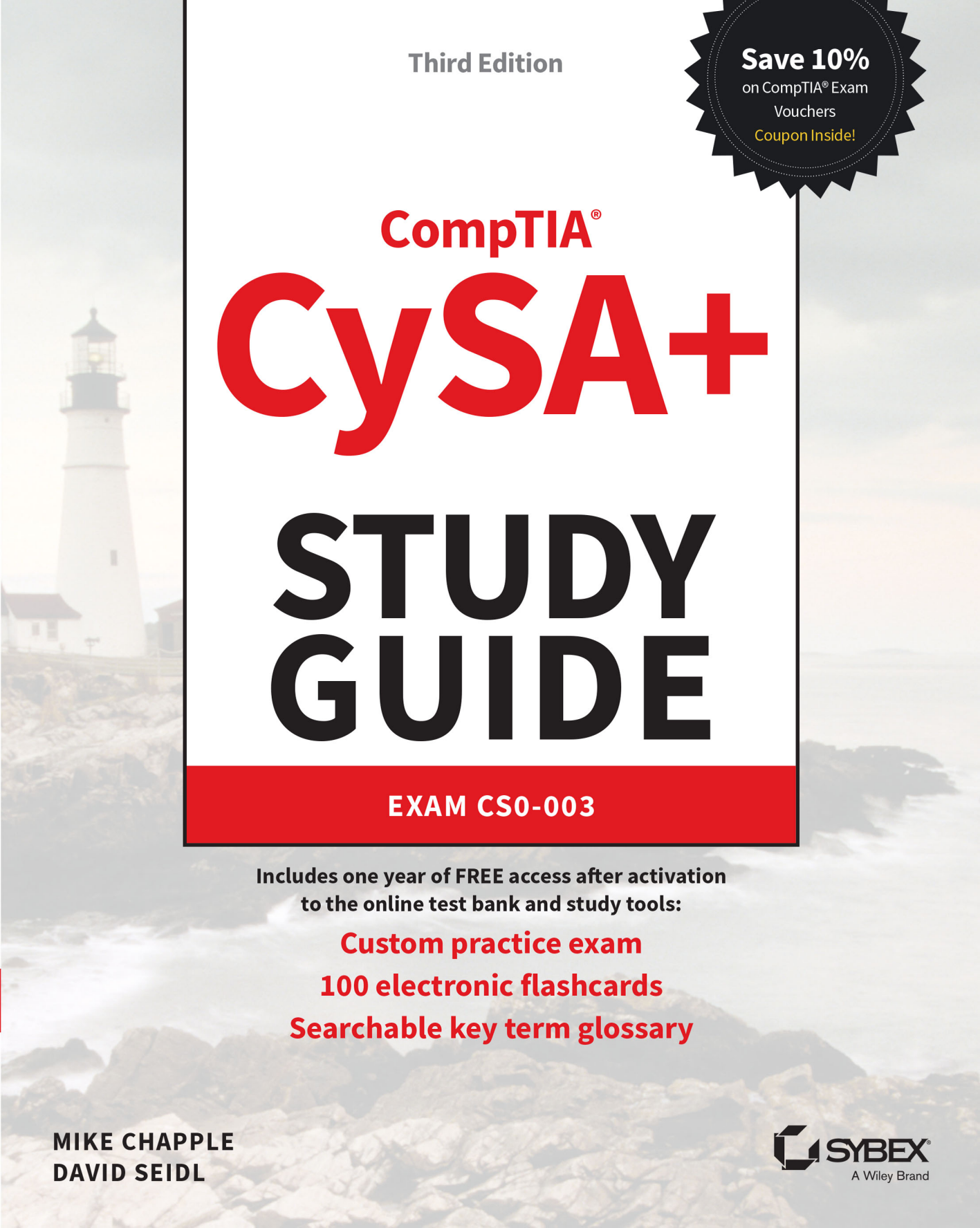

Third Edition
Save 10%
on CompTIA® Exam
Vouchers
Coupon Inside!
CompTIA®
CySA+
STUDY
GUIDE
EXAM CS0-003
Includes one year of FREE access after activation
to the online test bank and study tools:
Custom practice exam
100 electronic flashcards
Searchable key term glossary
MIKE CHAPPLE
DAVID SEIDL
SYBEX
A Wiley Brand

CompTIA®

CySA+ Study Guide

Exam CS0-003

Third Edition

Mike Chapple

David Seidl

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394182909 (paperback), 9781394182923 (ePDF), 9781394182916 (ePub)

Library of Congress Control Number: 2022951784

Cover image: © Jeremy Woodhouse/Getty Images, Inc.

Cover design: Wiley

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 Lily Miller, 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; Archana Pragash, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book; and Elizabeth Welch, our copy editor, who helped the text flow well. 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., Security+, CySA+, CISSP, is author of over 50 books, including the best-selling *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021) and the *CISSP (ISC)² Official Practice Tests* (Sybex, 2021). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as a 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 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). He provides security certification resources on his website at `CertMike.com`.

David Seidl, CySA+, CISSP, PenTest+, 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 18 books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)² Official Practice Tests* (Sybex, 2021) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests* (Sybex, 2020, 2018).

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.

About the Technical Editor

Chris Crayton, MCSE, CISSP, CASP, CySA+, A+, N+, S+, is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He has also been recognized with many professional and teaching awards.

Contents at a Glance

Contents

Introduction

CompTIA® CySA+ (Cybersecurity Analyst) Study Guide: Exam CS0-003, Third Edition, provides accessible explanations and real-world knowledge about the exam objectives that make up the Cybersecurity Analyst+ certification. This book will help you to assess your knowledge before taking the exam, as well as provide a stepping-stone to further learning in areas where you may want to expand your skillset or expertise.

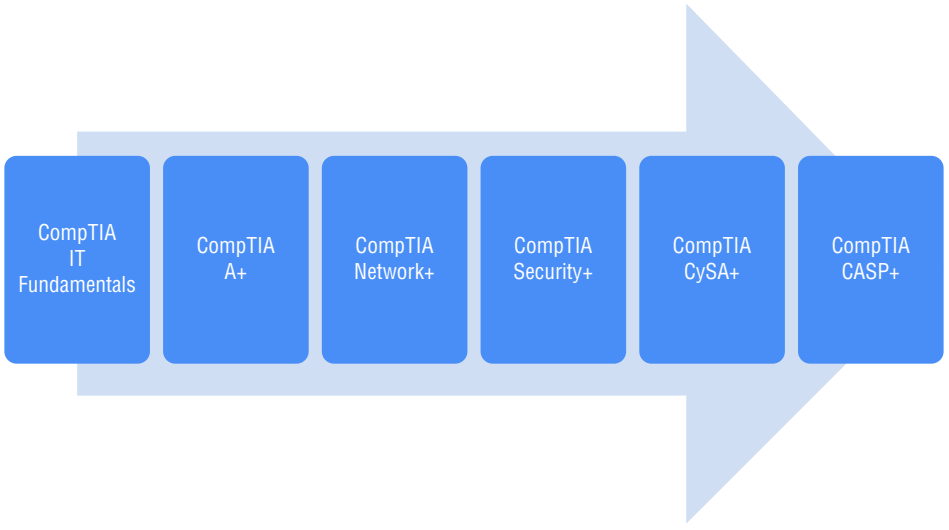
Before you tackle the CySA+ exam, you should already be a security practitioner. CompTIA suggests that test takers have about four years of existing hands-on information security experience. You should also be familiar with at least some of the tools and techniques described in this book. You don't need to know every tool, but understanding how to approach a new scenario, tool, or technology that you may not know using existing experience is critical to passing the CySA+ exam.

For up-to-the-minute updates covering additions or modifications to the CompTIA certification exams, as well as additional study tools, videos, practice questions, and bonus material, be sure to visit the Sybex website and forum at `www.sybex.com`.

CompTIA

CompTIA is a nonprofit trade organization that offers certification in a variety of IT areas, ranging from the skills that a PC support technician needs, which are covered in the A+ exam, to advanced certifications like the CompTIA Advanced Security Practitioner (CASP+) certification.

CompTIA recommends that practitioners follow a cybersecurity career path as shown here:



The Cybersecurity Analyst+ exam is a more advanced exam, intended for professionals with hands-on experience and who possess the knowledge covered by the prior exams.

CompTIA certifications are ISO and ANSI accredited, and they are used throughout multiple industries as a measure of technical skill and knowledge. In addition, CompTIA certifications, including the CySA+, the Security+, and the CASP+ certifications, have been approved by the U.S. government as Information Assurance baseline certifications and are included in the State Department's Skills Incentive Program.

The Cybersecurity Analyst+ Exam

The Cybersecurity Analyst+ exam, which CompTIA refers to as CySA+, is designed to be a vendor-neutral certification for cybersecurity, threat, and vulnerability analysts. The CySA+ certification is designed for security analysts and engineers as well as security operations center (SOC) staff, vulnerability analysts, and threat intelligence analysts. It focuses on security analytics and practical use of security tools in real-world scenarios. It covers four major domains: Security Operations, Vulnerability Management, Incident Response and Management, and Reporting and Communications. These four areas include a range of topics, from reconnaissance to incident response and forensics, while focusing heavily on scenario-based learning.

The CySA+ exam fits between the entry-level Security+ exam and the CompTIA Advanced Security Practitioner (CASP+) certification, providing a mid-career certification for those who are seeking the next step in their certification and career path.

The CySA+ exam is conducted in a format that CompTIA calls "performance-based assessment." This means that the exam employs hands-on simulations using actual security tools and scenarios to perform tasks that match those found in the daily work of a security practitioner. Exam questions may include multiple types of questions such as multiple-choice, fill-in-the-blank, multiple-response, drag-and-drop, and image-based problems.

CompTIA recommends that test takers have four years of information security–related experience before taking this exam. The exam costs $392 at the time this book was written in the United States, with roughly equivalent prices in other locations around the globe. More details about the CySA+ exam and how to take it can be found at `www.comptia.org/certifications/cybersecurity-analyst`.

Study and Exam Preparation Tips

A test preparation book like this cannot teach you every possible security software package, scenario, or specific technology that may appear on the exam. Instead, you should focus on whether you are familiar with the type or category of technology, tool, process, or scenario as you read the book. If you identify a gap, you may want to find additional tools to help you learn more about those topics.

Additional resources for hands-on exercises include the following:

- Exploit Exercises provides virtual machines, documentation, and challenges covering a wide range of security issues at `http://Exploit-Exercises.com`.
- Hacking-Lab provides capture the flag (CTF) exercises in a variety of fields at `hacking-lab.com`.
- PentesterLab provides a subscription-based access to penetration testing exercises at `http://pentesterlab.com/exercises`.

Since the exam uses scenario-based learning, expect the questions to involve analysis and thought, rather than relying on simple memorization. As you might expect, it is impossible to replicate that experience in a book, so the questions here are intended to help you be confident that you know the topic well enough to think through hands-on exercises.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

`http://store.comptia.org`

Currently, CompTIA offers two options for taking the exam: an in-person exam at a testing center and an at-home exam that you take on your own computer.

This book includes a coupon that you may use to save 10 percent on your CompTIA exam registration.

In-Person Exams

CompTIA partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your ZIP code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the Pearson Vue website, where you will need to navigate to "Find a test center."

`https://home.pearsonvue.com/comptia`

Once you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam on their site.

On the day of the test, take two forms of identification, and make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

At-Home Exams

CompTIA also offers an at-home testing option that uses the Pearson Vue remote proctoring service. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

You can learn more about the at-home testing experience by visiting:

`www.comptia.org/testing/testing-options/take-online-exam`

After the Cybersecurity Analyst+ Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

Maintaining Your Certification

CompTIA certifications must be renewed on a periodic basis. To renew your certification, you can either pass the most current version of the exam, earn a qualifying higher-level CompTIA or industry certification, or complete sufficient continuing education activities to earn enough continuing education units (CEUs) to renew it.

CompTIA provides information on renewals via their website at:

`www.comptia.org/continuing-education`

When you sign up to renew your certification, you will be asked to agree to the CE program's Code of Ethics, pay a renewal fee, and submit the materials required for your chosen renewal method.

A full list of the industry certifications you can use to acquire CEUs toward renewing the CySA+ can be found at:

`www.comptia.org/continuing-education/choose/renew-with-a-single-activity/earn-a-higher-level-comptia-certification`

What Does This Book Cover?

This book is designed to cover the four domains included in the CySA+ exam.

Chapter 1: Today's Cybersecurity Analyst The book starts by teaching you how to assess cybersecurity threats, as well as how to evaluate and select controls to keep your networks and systems secure.

Chapter 2: System and Network Architecture Understanding the underlying architecture that makes up your organization's infrastructure will help you defend your

organization. In this chapter you will explore concepts like serverless and containerization technology as well as virtualization. You will also explore logs and logging, network architecture and design concepts, identity and access management concepts, and how encryption can be used for security and data protection.

Chapter 3: Malicious Activity Analyzing events and identifying malicious activity is a key part of many security professionals roles. In this chapter you will explore how to monitor for and detect host-based, network-based, and application-based attacks and indicators of compromise. You will also explore how logs, email, and other tools and data sources can be used as part of your investigations.

Chapter 4: Threat Intelligence Security professionals need to fully understand threats in order to prevent them or to limit their impact. In this chapter, you will learn about the many types of threat intelligence, including sources and means of assessing the relevance and accuracy of a given threat intelligence source. You'll also discover how to use threat intelligence in your organization.

Chapter 5: Reconnaissance and Intelligence Gathering Gathering information about an organization and its systems is one of the things that both attackers and defenders do. In this chapter, you will learn how to acquire intelligence about an organization using popular tools and techniques. You will also learn how to limit the impact of intelligence gathering performed against your own organization.

Chapter 6: Designing a Vulnerability Management Program Managing vulnerabilities helps to keep your systems secure. In this chapter, you will learn how to identify, prioritize, and remediate vulnerabilities using a well-defined workflow and continuous assessment methodologies.

Chapter 7: Analyzing Vulnerability Scans Vulnerability reports can contain huge amounts of data about potential problems with systems. In this chapter, you will learn how to read and analyze a vulnerability scan report, what CVSS scoring is and what it means, as well as how to choose the appropriate actions to remediate the issues you have found. Along the way, you will explore common types of vulnerabilities and their impact on systems and networks.

Chapter 8: Responding to Vulnerabilities In this chapter, we turn our attention to what happens after a vulnerability is discovered—the ways that organizations respond to vulnerabilities that exist in their environments. We'll begin with coverage of the risk management process and then dive into some of the specific ways that you can respond to vulnerabilities.

Chapter 9: Building an Incident Response Program This chapter focuses on building a formal incident response handling program and team. You will learn the details of each stage of incident handling from preparation, to detection and analysis, to containment, eradication, and recovery, to the final post-incident recovery, as well as how to classify incidents and communicate about them.

Chapter 10: Incident Detection and Analysis Security professionals monitor for indicators of compromise, and once found they are analyzed to determine if an incident happened. In this chapter you will explore IoCs related to networks, systems, services, and applications. You will also dive into data and log analysis as well as evidence acquisition and analysis.

Chapter 11: Containment, Eradication, and Recovery Once an incident has occurred and the initial phases of incident response have taken place, you will need to work on recovering from it. That process involves containing the incident to ensure that no further issues occur and then working on eradicating malware, rootkits, and other elements of a compromise. Once the incident has been cleaned up, the recovery stage can start, including reporting and preparation for future issues.

Chapter 12: Reporting and Communication Communications and reporting are key to ensuring organizations digest and use information about vulnerabilities and incidents. In this chapter you'll explore both communication related to vulnerability management and incident response. You'll explore how to leverage vulnerability management and risk scores while understanding the most common inhibitors to remediation. You'll also look at incident reports, how to engage stakeholders, and how lessons learned can be gathered and used.

Chapter 13: Performing Forensic Analysis and Techniques for Incident Response Understanding what occurred on a system, device, or network, either as part of an incident or for other purposes, frequently involves forensic analysis. In this chapter, you will learn how to build a forensic capability and how the key tools in a forensic toolkit are used.

Appendix: Answers to Review Questions The appendix has answers to the review questions you will find at the end of each chapter.

Study Guide Elements

This study guide uses a number of common elements to help you prepare. These include the following:

Summaries The Summary section of each chapter briefly explains the chapter, allowing you to easily understand what it covers.

Exam Essentials The Exam Essentials focus on major exam topics and critical knowledge that you should take into the test. The Exam Essentials focus on the exam objectives provided by CompTIA.

Review Questions A set of questions at the end of each chapter will help you assess your knowledge and if you are ready to take the exam based on your knowledge of that chapter's topics.

Lab Exercises The written labs provide more in-depth practice opportunities to expand your skills and to better prepare for performance-based testing on the CySA+ exam.

Exam Note

These special notes call out issues that are found on the exam and relate directly to CySA+ exam objectives. They help you prepare for the why and how.

Interactive Online Learning Environment and Test Bank

We've put together some really great online tools to help you pass the CompTIA CySA+ exam. The interactive online learning environment that accompanies CompTIA® CySA+ Study Guide: Exam CS0-003 provides a test bank and study tools to help you prepare for the exam. By using these tools you can dramatically increase your chances of passing the exam on your first try.

Go to `www.wiley.com/go/sybextestprep` to register and gain access to this interactive online learning environment and test bank with study tools.

Like all exams, the Exam CS0-003: CompTIA® CySA+ is updated periodically and may eventually be retired or replaced. At some point after CompTIA is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

The online test bank includes the following:

Sample Tests

Many practice questions are provided throughout this book and online, including the questions in the Assessment Test, which you'll find at the end of this introduction, and the questions in the Chapter Tests, which include the review questions at the end of each chapter. In addition, there is a custom practice exam. Use all these practice questions to test your knowledge of the Study Guide material. The online test bank runs on multiple devices.

Flashcards

The online text bank includes over 100 flashcards especifically written to test your knowledge, so don't get discouraged if you don't ace your way through them at first! They're there to ensure that you know critical terms and concepts and you're really ready for the exam. And no worries—armed with the review questions, practice exam, and flashcards,

you'll be more than prepared when exam day comes! Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Other Study Tools

A glossary of key terms from this book and their definitions are available as a fully searchable PDF.

Objectives Map for CompTIA CySA+ Exam CS0-003

The following objectives' map for the CompTIA CySA+ certification exam will enable you to find the chapter in this book that covers each objective for the exam.

Objectives Map

Objective	Chapter(s)
1.0 Security Operations	
1.1 Explain the importance of system and network architecture concepts in security operations	2
1.2 Given a scenario, analyze indicators of potentially malicious activity	3
1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity	3
1.4 Compare and contrast threat intelligence and threat-hunting concepts	4
1.5 Explain the importance of efficiency and process improvement in security operations	1
2.0 Vulnerability Management	
2.1 Given a scenario, implement vulnerability scanning methods and concepts	1, 5, 6, 7, 8
2.2 Given a scenario, analyze output from vulnerability assessment tools	5, 6, 8
2.3 Given a scenario, analyze data to prioritize vulnerabilities	7
2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities	7