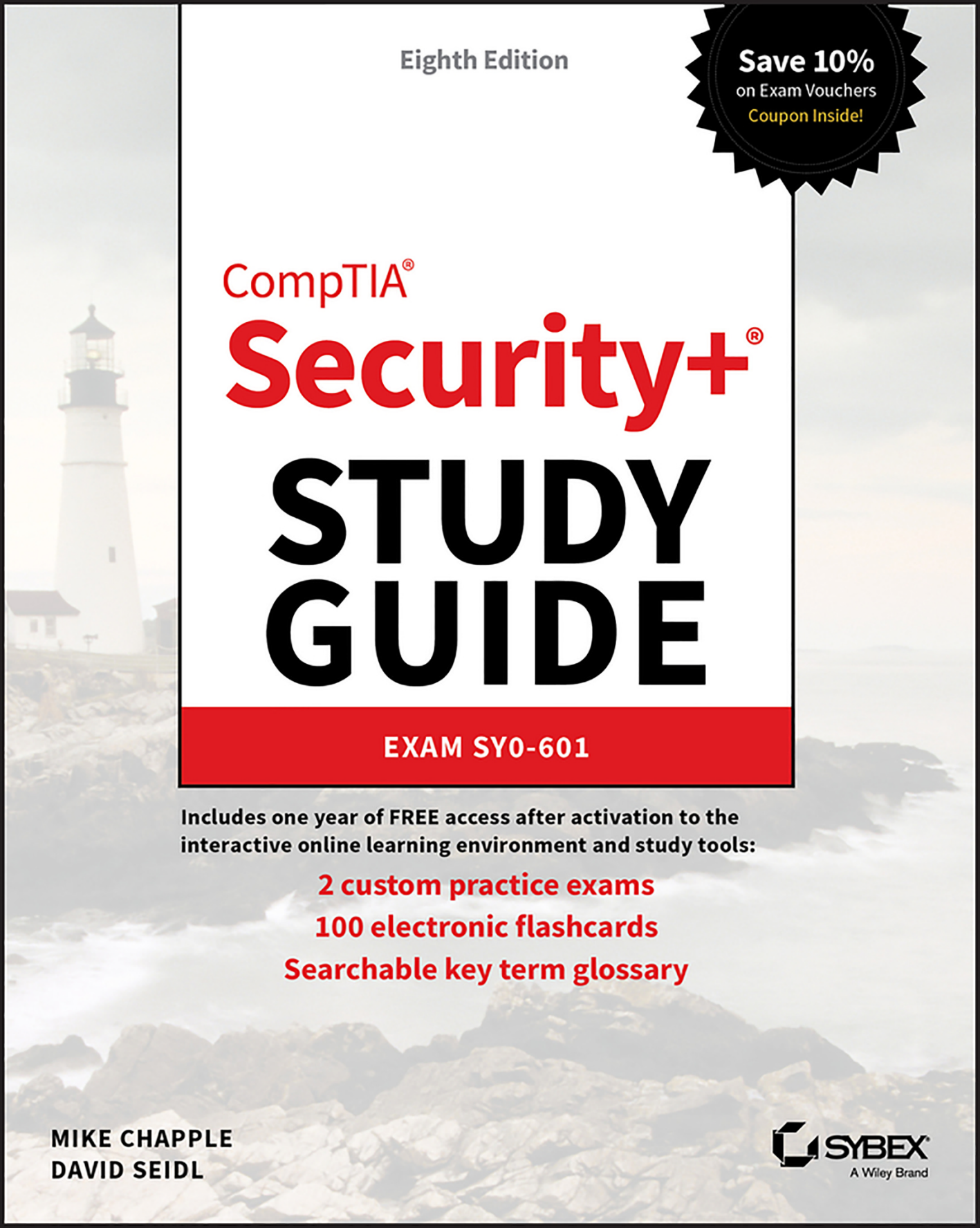
Eighth Edition
Save 10%
on Exam Vouchers
Coupon Inside!
CompTIA®
Security+®
STUDY GUIDE
EXAM SY0-601
Includes one year of FREE access after activation to the interactive online learning environment and study tools:
2 custom practice exams
100 electronic flashcards
Searchable key term glossary
MIKE CHAPPLE
DAVID SEIDL
SYBEX
A Wiley Brand

CompTIA®

Security+®

Study Guide

Exam SY0-601

Eighth Edition

Mike Chapple

David Seidl

SYBEX®
A Wiley Brand

Published simultaneously in Canada

ISBN: 978-1-119-73625-7
ISBN: 978-1-119-73627-1 (ebk.)
ISBN: 978-1-119-73626-4 (ebk.)

Library of Congress Control Number: 2020950197

To my mother, Grace. Thank you for encouraging my love of writing since I first learned to pick up a pencil.
—Mike

To my niece Selah, whose imagination and joy in discovery inspires me every time I hear a new Hop Cheep story, and to my sister Susan and brother-in-law Ben who encourage her to bravely explore the world around them.
—David

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 owe a great debt of gratitude to Runzhi "Tom" Song, Mike's research assistant at Notre Dame. Tom's assistance with the instructional materials that accompany this book was invaluable.

We also greatly appreciated the editing and production team for the book, including Tom Dinse, our project editor, who brought years of experience and great talent to the project; Nadean Tanner, our technical editor, who provided insightful advice and gave wonderful feedback throughout the book; and Saravanan Dakshinamurthy, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book. 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., CISSP, Security+, is author of 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 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 the Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP) certifications.

Learn more about Mike and his other security certification materials at his website, `CertMike.com`.

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 has written 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: 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 CISSP, CySA+, Pentest+, GPEN, and GCIH certifications.

About the Technical Editor

Nadean H. Tanner, Security+, CASP+, A+, Network+, CISSP, and many other industry certifications, is the manager of Consulting-Education Services for Mandiant/FireEye. Prior to Mandiant, she was the lead instructor at Rapid7, teaching vulnerability management, incident detection and response, and Metasploit. For more than 20 years, she has worked in academia as an IT director of a private school and technology instructor at the university level as well as working for the U.S. Department of Defense. Nadean is the author of the *Cybersecurity Blue Team Toolkit* (Wiley, 2019) and the *CompTIA CASP+ Practice Tests: Exam CAS-003* (Sybex, 2020).

Contents at a Glance

Contents

Introduction

If you're preparing to take the Security+ exam, you'll undoubtedly want to find as much information as you can about computer and physical security. The more information you have at your disposal and the more hands-on experience you gain, the better off you'll be when attempting the exam. This study guide was written with that in mind. The goal was to provide enough information to prepare you for the test, but not so much that you'll be overloaded with information that's outside the scope of the exam.

This book presents the material at an intermediate technical level. Experience with and knowledge of security concepts, operating systems, and application systems will help you get a full understanding of the challenges you'll face as a security professional.

We've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. If you're already working in the security field, we recommend that you check out these questions first to gauge your level of expertise. You can then use the book mainly to fill in the gaps in your current knowledge. This study guide will help you round out your knowledge base before tackling the exam.

If you can answer 90 percent or more of the review questions correctly for a given chapter, you can feel safe moving on to the next chapter. If you're unable to answer that many correctly, reread the chapter and try the questions again. Your score should improve.

Don't just study the questions and answers! The questions on the actual exam will be different from the practice questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

The Security+ Exam

The Security+ exam is designed to be a vendor-neutral certification for cybersecurity professionals and those seeking to enter the field. CompTIA recommends this certification for those currently working, or aspiring to work, in roles, including the following:

- Systems administrator
- Security administrator
- Security specialist
- Security engineer
- Network administrator
- Junior IT auditor/Penetration tester
- Security consultant

The exam covers five major domains:

1. Threats, Attacks, and Vulnerabilities
2. Architecture and Design
3. Implementation
4. Operations and Incident Response
5. Governance, Risk, and Compliance

These five areas include a range of topics, from firewall design to incident response and forensics, while focusing heavily on scenario-based learning. That's why CompTIA recommends that those attempting the exam have at least two years of hands-on work experience, although many individuals pass the exam before moving into their first cybersecurity role.

The Security+ exam is conducted in a format that CompTIA calls "performance-based assessment." This means that the exam combines standard multiple-choice questions with other, interactive question formats. Your exam may include several types of questions such as multiple-choice, fill-in-the-blank, multiple-response, drag-and-drop, and image-based problems.

The exam costs $349 in the United States, with roughly equivalent prices in other locations around the globe. More details about the Security+ exam and how to take it can be found at

`www.comptia.org/certifications/security`

You'll have 90 minutes to take the exam and will be asked to answer up to 90 questions during that time period. Your exam will be scored on a scale ranging from 100 to 900, with a passing score of 750.

You should also know that CompTIA is notorious for including vague questions on all of its exams. You might see a question for which two of the possible four answers are correct—but you can choose only one. Use your knowledge, logic, and intuition to choose the best answer and then move on. Sometimes, the questions are worded in ways that would make English majors cringe—a typo here, an incorrect verb there. Don't let this frustrate you; answer the question and move on to the next one.

CompTIA frequently does what is called *item seeding*, which is the practice of including unscored questions on exams. It does so to gather psychometric data, which is then used when developing new versions of the exam. Before you take the exam, you will be told that your exam may include these unscored questions. So, if you come across a question that does not appear to map to any of the exam objectives—or for that matter, does not appear to belong in the exam—it is likely a seeded question. You never really know whether or not a question is seeded, however, so always make your best effort to answer every question.

Taking the Exam

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

`www.comptiastore.com/Articles.asp?ID=265&category=vouchers`

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."

`www.pearsonvue.com/comptia`

Now that 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 began offering online exam proctoring in 2020 in response to the coronavirus pandemic. As of the time this book went to press, the at-home testing option was still available and appears likely to continue. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

Due to the rapidly changing nature of the at-home testing experience, candidates wishing to pursue this option should check the CompTIA website for the latest details.

After the Security+ 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, to pay a renewal fee, and to 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 Security+ 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 covers everything you need to know to understand the job role and basic responsibilities of a security administrator and also to pass the Security+ exam.

Chapter 1: Today's Security Professional Chapter 1 provides an introduction to the field of cybersecurity. You'll learn about the crucial role that cybersecurity professionals play in protecting the confidentiality, integrity, and availability of their organization's data. You'll also learn about the types of risk facing organizations and the use of managerial, operational, and technical security controls to manage those risks.

Chapter 2: Cybersecurity Threat Landscape Chapter 2 dives deeply into the cybersecurity threat landscape, helping you understand the different types of threat actors present in today's environment and the threat vectors that they exploit to undermine security controls. You'll also learn about the use of threat intelligence sources to improve your organization's security program and the security issues that arise from different types of vulnerability.

Chapter 3: Malicious Code Chapter 3 explores the wide range of malicious code that you may encounter. Worms, viruses, Trojans, bots, the command-and-control networks that attackers use to control them, and a host of other types of malware are all covered in this chapter. Along the way you'll also learn about new threats like attacks against artificial intelligence and machine learning systems, and how attackers use built-in scripting and programming languages as part of their attacks in addition to malware.

Chapter 4: Social Engineering, Physical, and Password Attacks Chapter 4 dives into the human side of information security. Social engineering focuses on how individuals respond to various techniques like authority, intimidation, and trust, and how those