

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

**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®

Security+®

Study Guide

Exam SY0-601

Eighth Edition



Mike Chapple

David Seidl

 **SYBEX®**
A Wiley Brand

Copyright © 2021 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-73625-7

ISBN: 978-1-119-73627-1 (ebk.)

ISBN: 978-1-119-73626-4 (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 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 booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020950197

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 and Security+ are registered trademarks of CompTIA Properties, LLC. 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.

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 *Cyber-*

security Blue Team Toolkit (Wiley, 2019) and the *CompTIA CASP+ Practice Tests: Exam CAS-003* (Sybex, 2020).

Contents at a Glance

<i>Introduction</i>	<i>xxv</i>
<i>Assessment Test</i>	<i>xxxvi</i>
Chapter 1	Today's Security Professional 1
Chapter 2	Cybersecurity Threat Landscape 19
Chapter 3	Malicious Code 45
Chapter 4	Social Engineering, Physical, and Password Attacks 65
Chapter 5	Security Assessment and Testing 83
Chapter 6	Secure Coding 129
Chapter 7	Cryptography and the Public Key Infrastructure 179
Chapter 8	Identity and Access Management 229
Chapter 9	Resilience and Physical Security 257
Chapter 10	Cloud and Virtualization Security 285
Chapter 11	Endpoint Security 323
Chapter 12	Network Security 361
Chapter 13	Wireless and Mobile Security 419
Chapter 14	Incident Response 449
Chapter 15	Digital Forensics 485
Chapter 16	Security Policies, Standards, and Compliance 511
Chapter 17	Risk Management and Privacy 539
Appendix	Answers to Review Questions 565
<i>Index</i>	<i>603</i>

Contents

<i>Introduction</i>	<i>xxv</i>
<i>Assessment Test</i>	<i>xxxvi</i>
Chapter 1	Today's Security Professional 1
	Cybersecurity Objectives 2
	Data Breach Risks 3
	The DAD Triad 3
	Breach Impact 5
	Implementing Security Controls 7
	Security Control Categories 7
	Security Control Types 8
	Data Protection 9
	Summary 12
	Exam Essentials 12
	Review Questions 14
Chapter 2	Cybersecurity Threat Landscape 19
	Exploring Cybersecurity Threats 20
	Classifying Cybersecurity Threats 20
	Threat Actors 22
	Threat Vectors 28
	Threat Data and Intelligence 30
	Open Source Intelligence 31
	Proprietary and Closed-Source Intelligence 33
	Assessing Threat Intelligence 35
	Threat Indicator Management and Exchange 36
	Public and Private Information Sharing Centers 37
	Conducting Your Own Research 38
	Summary 38
	Exam Essentials 39
	Review Questions 40
Chapter 3	Malicious Code 45
	Malware 46
	Ransomware 47
	Trojans 47
	Worms 48
	Rootkits 48
	Backdoors 49
	Bots 50
	Keyloggers 52
	Logic Bombs 53
	Viruses 53

	Fileless Viruses	53
	Spyware	54
	Potentially Unwanted Programs (PUPs)	55
	Malicious Code	55
	Adversarial Artificial Intelligence	57
	Summary	58
	Exam Essentials	59
	Review Questions	61
Chapter 4	Social Engineering, Physical, and Password Attacks	65
	Social Engineering	66
	Social Engineering Techniques	67
	Influence Campaigns	72
	Password Attacks	72
	Physical Attacks	74
	Summary	76
	Exam Essentials	76
	Review Questions	78
Chapter 5	Security Assessment and Testing	83
	Vulnerability Management	84
	Identifying Scan Targets	84
	Determining Scan Frequency	86
	Configuring Vulnerability Scans	87
	Scanner Maintenance	92
	Vulnerability Scanning Tools	95
	Reviewing and Interpreting Scan Reports	96
	Validating Scan Results	106
	Security Vulnerabilities	107
	Patch Management	107
	Legacy Platforms	108
	Weak Configurations	109
	Error Messages	110
	Insecure Protocols	111
	Weak Encryption	112
	Penetration Testing	113
	Adopting the Hacker Mindset	114
	Reasons for Penetration Testing	115
	Benefits of Penetration Testing	115
	Penetration Test Types	116
	Rules of Engagement	118
	Reconnaissance	119
	Running the Test	120

	Cleaning Up	120
	Training and Exercises	120
	Summary	122
	Exam Essentials	122
	Review Questions	124
Chapter 6	Secure Coding	129
	Software Assurance Best Practices	130
	The Software Development Life Cycle	130
	Software Development Phases	131
	Software Development Models	133
	DevSecOps and DevOps	136
	Designing and Coding for Security	138
	Secure Coding Practices	138
	API Security	139
	Code Review Models	139
	Software Security Testing	143
	Analyzing and Testing Code	143
	Injection Vulnerabilities	144
	SQL Injection Attacks	145
	Code Injection Attacks	148
	Command Injection Attacks	149
	Exploiting Authentication Vulnerabilities	150
	Password Authentication	150
	Session Attacks	151
	Exploiting Authorization Vulnerabilities	154
	Insecure Direct Object References	154
	Directory Traversal	155
	File Inclusion	156
	Privilege Escalation	157
	Exploiting Web Application Vulnerabilities	157
	Cross-Site Scripting (XSS)	158
	Request Forgery	160
	Application Security Controls	161
	Input Validation	162
	Web Application Firewalls	163
	Database Security	163
	Code Security	166
	Secure Coding Practices	168
	Source Code Comments	168
	Error Handling	168
	Hard-Coded Credentials	170
	Memory Management	170
	Race Conditions	171

	Unprotected APIs	172
	Driver Manipulation	172
	Summary	173
	Exam Essentials	173
	Review Questions	175
Chapter 7	Cryptography and the Public Key Infrastructure	179
	An Overview of Cryptography	180
	Historical Cryptography	181
	Goals of Cryptography	186
	Confidentiality	187
	Integrity	188
	Authentication	188
	Nonrepudiation	189
	Cryptographic Concepts	189
	Cryptographic Keys	189
	Ciphers	190
	Modern Cryptography	191
	Cryptographic Secrecy	191
	Symmetric Key Algorithms	192
	Asymmetric Key Algorithms	193
	Hashing Algorithms	196
	Symmetric Cryptography	197
	Data Encryption Standard	197
	Triple DES	199
	Advanced Encryption Standard	200
	Symmetric Key Management	200
	Asymmetric Cryptography	203
	RSA	203
	Elliptic Curve	204
	Hash Functions	205
	SHA	206
	MD5	207
	Digital Signatures	207
	HMAC	208
	Digital Signature Standard	209
	Public Key Infrastructure	209
	Certificates	209
	Certificate Authorities	211
	Certificate Generation and Destruction	212
	Certificate Formats	215
	Asymmetric Key Management	216
	Cryptographic Attacks	217
	Emerging Issues in Cryptography	220

	Tor and the Dark Web	220
	Blockchain	220
	Lightweight Cryptography	221
	Homomorphic Encryption	221
	Quantum Computing	222
	Summary	222
	Exam Essentials	222
	Review Questions	224
Chapter 8	Identity and Access Management	229
	Identity	230
	Authentication and Authorization	231
	Authentication and Authorization Technologies	232
	Directory Services	236
	Authentication Methods	237
	Multifactor Authentication	237
	One-Time Passwords	239
	Biometrics	241
	Knowledge-Based Authentication	243
	Managing Authentication	244
	Accounts	245
	Account Types	245
	Account Policies and Controls	245
	Access Control Schemes	248
	Filesystem Permissions	249
	Summary	251
	Exam Essentials	252
	Review Questions	253
Chapter 9	Resilience and Physical Security	257
	Building Cybersecurity Resilience	258
	Storage Resiliency: Backups and Replication	260
	Response and Recovery Controls	266
	Physical Security Controls	269
	Site Security	269
	Summary	278
	Exam Essentials	279
	Review Questions	281
Chapter 10	Cloud and Virtualization Security	285
	Exploring the Cloud	286
	Benefits of the Cloud	287
	Cloud Roles	289
	Cloud Service Models	289
	Cloud Deployment Models	293

	Shared Responsibility Model	295
	Cloud Standards and Guidelines	298
	Virtualization	300
	Hypervisors	300
	Cloud Infrastructure Components	302
	Cloud Compute Resources	302
	Cloud Storage Resources	304
	Cloud Networking	307
	Cloud Security Issues	311
	Availability	311
	Data Sovereignty	311
	Virtualization Security	312
	Application Security	312
	Governance and Auditing	313
	Cloud Security Controls	313
	Cloud Access Security Brokers	314
	Resource Policies	314
	Secrets Management	316
	Summary	316
	Exam Essentials	316
	Review Questions	318
Chapter 11	Endpoint Security	323
	Protecting Endpoints	324
	Preserving Boot Integrity	325
	Endpoint Security Tools	326
	Hardening Endpoints and Systems	332
	Service Hardening	333
	Operating System Hardening	335
	Hardening the Windows Registry	336
	Configuration, Standards, and Schemas	336
	Disk Security and Sanitization	338
	File Manipulation and Other Useful Command-Line Tools	341
	Scripting, Secure Transport, and Shells	343
	Securing Embedded and Specialized Systems	344
	Embedded Systems	345
	SCADA and ICS	346
	Securing the Internet of Things	348
	Specialized Systems	349
	Communication Considerations	350
	Security Constraints of Embedded Systems	351
	Summary	352
	Exam Essentials	354
	Review Questions	356

Chapter 12	Network Security	361
	Designing Secure Networks	363
	Network Segmentation	365
	Network Access Control	366
	Port Security and Port-Level Protections	367
	Port Spanning/Port Mirroring	369
	Virtual Private Network	370
	Network Appliances and Security Tools	371
	Network Security, Services, and Management	377
	Deception and Disruption	382
	Secure Protocols	383
	Using Secure Protocols	383
	Secure Protocols	384
	Attacking and Assessing Networks	389
	On-Path Attacks	389
	Domain Name System Attacks	391
	Layer 2 Attacks	393
	Distributed Denial-of-Service Attacks	394
	Network Reconnaissance and Discovery Tools and Techniques	398
	Summary	411
	Exam Essentials	412
	Review Questions	414
Chapter 13	Wireless and Mobile Security	419
	Building Secure Wireless Networks	420
	Connectivity Methods	421
	Wireless Network Models	425
	Attacks Against Wireless Networks	426
	Designing a Network	430
	Controller and Access Point Security	432
	Wi-Fi Security Standards	433
	Wireless Authentication	434
	Managing Secure Mobile Devices	436
	Mobile Device Deployment Methods	436
	Mobile Device Management	438
	Specialized Mobile Device Security Tools	442
	Summary	442
	Exam Essentials	443
	Review Questions	445
Chapter 14	Incident Response	449
	Incident Response	450
	The Incident Response Process	451
	Attack Frameworks and Identifying Attacks	457

	Incident Response Data and Tools	461
	Security Information and Event Management Systems	462
	Alerts and Alarms	464
	Correlation and Analysis	465
	Rules	465
	Mitigation and Recovery	473
	Summary	477
	Exam Essentials	478
	Review Questions	480
Chapter 15	Digital Forensics	485
	Digital Forensic Concepts	486
	Legal Holds and e-Discovery	487
	Conducting Digital Forensics	488
	Acquiring Forensic Data	489
	Acquisition Tools	493
	Validating Forensic Data Integrity	496
	Data Recovery	499
	Forensic Suites and a Forensic Case Example	499
	Reporting	504
	Digital Forensics and Intelligence	504
	Summary	505
	Exam Essentials	505
	Review Questions	507
Chapter 16	Security Policies, Standards, and Compliance	511
	Understanding Policy Documents	512
	Policies	512
	Standards	515
	Procedures	517
	Guidelines	518
	Exceptions and Compensating Controls	519
	Personnel Management	520
	Least Privilege	520
	Separation of Duties	521
	Job Rotation and Mandatory Vacations	521
	Clean Desk Space	522
	Onboarding and Offboarding	522
	Nondisclosure Agreements	522
	Social Media	522
	User Training	522
	Third-Party Risk Management	523
	Winding Down Vendor Relationships	524

	Complying with Laws and Regulations	524
	Adopting Standard Frameworks	525
	NIST Cybersecurity Framework	525
	NIST Risk Management Framework	528
	ISO Standards	529
	Benchmarks and Secure Configuration Guides	531
	Security Control Verification and Quality Control	531
	Summary	533
	Exam Essentials	534
	Review Questions	535
Chapter 17	Risk Management and Privacy	539
	Analyzing Risk	540
	Risk Identification	541
	Risk Calculation	542
	Risk Assessment	543
	Managing Risk	547
	Risk Mitigation	547
	Risk Avoidance	549
	Risk Transference	549
	Risk Acceptance	549
	Risk Analysis	550
	Disaster Recovery Planning	552
	Disaster Types	552
	Business Impact Analysis	553
	Privacy	553
	Sensitive Information Inventory	554
	Information Classification	554
	Data Roles and Responsibilities	556
	Information Lifecycle	557
	Privacy Enhancing Technologies	557
	Privacy and Data Breach Notification	558
	Summary	559
	Exam Essentials	559
	Review Questions	560
Appendix	Answers to Review Questions	565
	Chapter 1: Today's Security Professional	566
	Chapter 2: Cybersecurity Threat Landscape	567
	Chapter 3: Malicious Code	569
	Chapter 4: Social Engineering, Physical, and Password Attacks	572
	Chapter 5: Security Assessment and Testing	574
	Chapter 6: Secure Coding	576
	Chapter 7: Cryptography and the Public Key Infrastructure	578

Chapter 8: Identity and Access Management	579
Chapter 9: Resilience and Physical Security	582
Chapter 10: Cloud and Virtualization Security	584
Chapter 11: Endpoint Security	586
Chapter 12: Network Security	589
Chapter 13: Wireless and Mobile Security	591
Chapter 14: Incident Response	594
Chapter 15: Digital Forensics	596
Chapter 16: Security Policies, Standards, and Compliance	598
Chapter 17: Risk Management and Privacy	600
<i>Index</i>	603

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