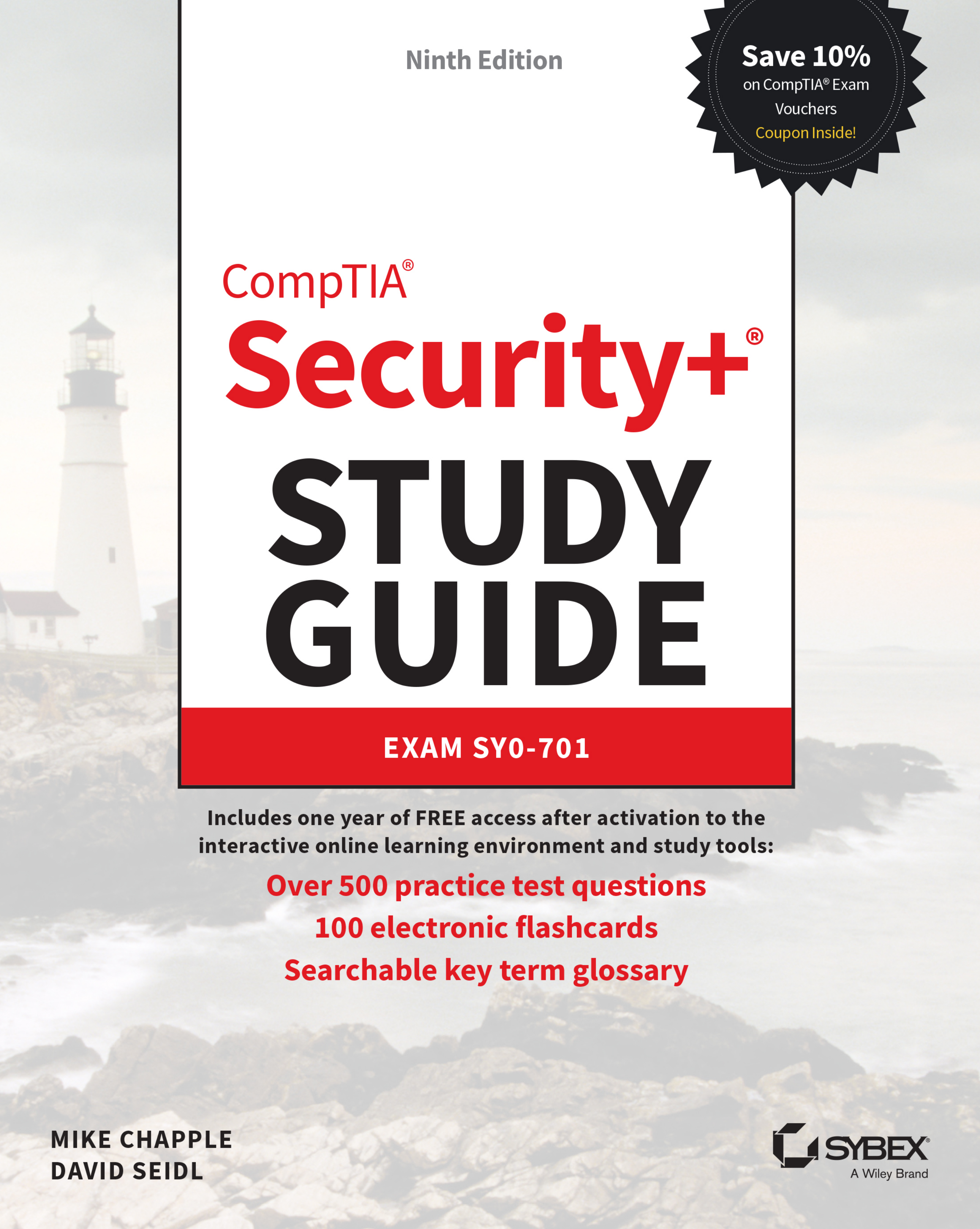

Ninth Edition

Save 10%
on CompTIA® Exam
Vouchers
Coupon Inside!

CompTIA® Security+® STUDY GUIDE

EXAM SY0-701

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

Over 500 practice test questions
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.

SYBEX®

CompTIA®

Security+®

Study Guide

Ninth Edition

CompTIA®

Security+®

Study Guide

Exam SY0-701

Ninth Edition

Mike Chapple

David Seidl

SYBEX®
A Wiley Brand

Copyright © 2024 by John Wiley & Sons, Inc. All rights reserved.

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

ISBNs: 9781394211418 (paperback), 9781394211432 (ePDF), 9781394211425 (ePub)

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. 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/permission.

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, 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.

Limit of Liability/Disclaimer of Warranty: While the publisher and authors have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2023945962

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

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 collaborated 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 appreciate the editing and production team for this book, including Lily Miller, our project editor, who brought years of experience and great talent to the project; Chris Crayton, our technical editor, and Shahla Pirnia, our technical proofreader who both 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., Security+, CySA+, CISSP, 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 IT certification materials at his website, `CertMike.com`.

David Seidl, CySA+, CISSP, Pentest+, is Vice President for Information Technology and CIO at Miami University, where he leads an award-winning team of IT professionals. 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 services. 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. David is a best-selling author who specializes in cybersecurity certification and cyberwarfare and has written over 20 books on the topic.

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

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.

About the Technical Proofreader

Shahla Pirnia is a freelance technical editor and proofreader with a focus on cybersecurity and certification topics. She currently serves as a technical editor for `CertMike.com` where she works on projects including books, video courses, and practice tests.

Shahla earned BS degrees in Computer and Information Science and Psychology from the University of Maryland Global Campus, coupled with an AA degree in Information Systems from Montgomery College, Maryland. Shahla's IT certifications include the CompTIA Security+, Network+, A+ and the ISC2 CC.

Contents at a Glance

Introduction *xxxi*

Chapter 1 Today's Security Professional 1

Chapter 2 Cybersecurity Threat Landscape 21

Chapter 3 Malicious Code 49

Chapter 4 Social Engineering and Password Attacks 69

Chapter 5 Security Assessment and Testing 85

Chapter 6 Application Security 141

Chapter 7 Cryptography and the PKI 189

Chapter 8 Identity and Access Management 237

Chapter 9 Resilience and Physical Security 269

Chapter 10 Cloud and Virtualization Security 299

Chapter 11 Endpoint Security 337

Chapter 12 Network Security 375

Chapter 13 Wireless and Mobile Security 425

Chapter 14 Monitoring and Incident Response 455

Chapter 15 Digital Forensics 489

Chapter 16 Security Governance and Compliance 515

Chapter 17 Risk Management and Privacy 561

Appendix Answers to Review Questions 591

Index *629*

Contents

Introduction *xxxi*

Chapter 1 Today's Security Professional 1

Cybersecurity Objectives 2
Data Breach Risks 3
  The DAD Triad 4
  Breach Impact 5
Implementing Security Controls 7
  Gap Analysis 7
  Security Control Categories 8
  Security Control Types 9
Data Protection 10
  Data Encryption 11
  Data Loss Prevention 11
  Data Minimization 12
  Access Restrictions 13
  Segmentation and Isolation 13
Summary 13
Exam Essentials 14
Review Questions 16

Chapter 2 Cybersecurity Threat Landscape 21

Exploring Cybersecurity Threats 23
  Classifying Cybersecurity Threats 23
  Threat Actors 25
  Attacker Motivations 31
  Threat Vectors and Attack Surfaces 32
Threat Data and Intelligence 35
  Open Source Intelligence 35
  Proprietary and Closed-Source Intelligence 38
  Assessing Threat Intelligence 39
  Threat Indicator Management and Exchange 40
  Information Sharing Organizations 41
  Conducting Your Own Research 42
Summary 42
Exam Essentials 43
Review Questions 45

Chapter 3 Malicious Code 49

Malware 50
  Ransomware 51
  Trojans 52

Worms 54
Spyware 55
Bloatware 56
Viruses 57
Keyloggers 59
Logic Bombs 60
Rootkits 60
Summary 62
Exam Essentials 62
Review Questions 64

Chapter 4 Social Engineering and Password Attacks 69

Social Engineering and Human Vectors 70
Social Engineering Techniques 71
Password Attacks 76
Summary 78
Exam Essentials 78
Review Questions 80

Chapter 5 Security Assessment and Testing 85

Vulnerability Management 87
Identifying Scan Targets 87
Determining Scan Frequency 89
Configuring Vulnerability Scans 91
Scanner Maintenance 95
Vulnerability Scanning Tools 98
Reviewing and Interpreting Scan Reports 101
Confirmation of Scan Results 111
Vulnerability Classification 112
Patch Management 112
Legacy Platforms 113
Weak Configurations 115
Error Messages 115
Insecure Protocols 116
Weak Encryption 117
Penetration Testing 118
Adopting the Hacker Mindset 119
Reasons for Penetration Testing 120
Benefits of Penetration Testing 120
Penetration Test Types 121
Rules of Engagement 123
Reconnaissance 125
Running the Test 125
Cleaning Up 126

Audits and Assessments 126
Security Tests 127
Security Assessments 128
Security Audits 129
Vulnerability Life Cycle 131
Vulnerability Identification 131
Vulnerability Analysis 132
Vulnerability Response and Remediation 132
Validation of Remediation 132
Reporting 133
Summary 133
Exam Essentials 134
Review Questions 136

Chapter 6 Application Security 141

Software Assurance Best Practices 143
The Software Development Life Cycle 143
Software Development Phases 144
DevSecOps and DevOps 146
Designing and Coding for Security 147
Secure Coding Practices 148
API Security 149
Software Security Testing 149
Analyzing and Testing Code 150
Injection Vulnerabilities 151
SQL Injection Attacks 151
Code Injection Attacks 155
Command Injection Attacks 155
Exploiting Authentication Vulnerabilities 156
Password Authentication 156
Session Attacks 157
Exploiting Authorization Vulnerabilities 160
Insecure Direct Object References 161
Directory Traversal 161
File Inclusion 163
Privilege Escalation 163
Exploiting Web Application Vulnerabilities 164
Cross-Site Scripting (XSS) 164
Request Forgery 167
Application Security Controls 168
Input Validation 168
Web Application Firewalls 170
Parameterized Queries 170

Sandboxing 171
Code Security 171
Secure Coding Practices 173
Source Code Comments 174
Error Handling 174
Hard-Coded Credentials 175
Package Monitoring 175
Memory Management 176
Race Conditions 177
Unprotected APIs 178
Automation and Orchestration 178
Use Cases of Automation and Scripting 179
Benefits of Automation and Scripting 179
Other Considerations 180
Summary 181
Exam Essentials 181
Review Questions 183

Chapter 7 Cryptography and the PKI 189

An Overview of Cryptography 190
Historical Cryptography 191
Goals of Cryptography 196
Confidentiality 197
Integrity 199
Authentication 200
Non-repudiation 200
Cryptographic Concepts 200
Cryptographic Keys 201
Ciphers 202
Modern Cryptography 202
Cryptographic Secrecy 202
Symmetric Key Algorithms 204
Asymmetric Key Algorithms 205
Hashing Algorithms 208
Symmetric Cryptography 208
Data Encryption Standard 208
Advanced Encryption Standard 209
Symmetric Key Management 209
Asymmetric Cryptography 211
RSA 212
Elliptic Curve 213
Hash Functions 214
SHA 215

MD5 216
Digital Signatures 216
HMAC 217
Public Key Infrastructure 218
Certificates 218
Certificate Authorities 219
Certificate Generation and Destruction 220
Certificate Formats 223
Asymmetric Key Management 224
Cryptographic Attacks 225
Brute Force 225
Frequency Analysis 225
Known Plain Text 226
Chosen Plain Text 226
Related Key Attack 226
Birthday Attack 226
Downgrade Attack 227
Hashing, Salting, and Key Stretching 227
Exploiting Weak Keys 228
Exploiting Human Error 228
Emerging Issues in Cryptography 229
Tor and the Dark Web 229
Blockchain 229
Lightweight Cryptography 230
Homomorphic Encryption 230
Quantum Computing 230
Summary 231
Exam Essentials 231
Review Questions 233

Chapter 8 Identity and Access Management 237

Identity 239
Authentication and Authorization 240
Authentication and Authorization Technologies 241
Authentication Methods 246
Passwords 247
Multifactor Authentication 251
One-Time Passwords 252
Biometrics 254
Accounts 256
Account Types 256
Provisioning and Deprovisioning Accounts 257
Access Control Schemes 259

Filesystem Permissions 260
Summary 262
Exam Essentials 262
Review Questions 264

Chapter 9 Resilience and Physical Security 269

Resilience and Recovery in Security Architectures 271
Architectural Considerations and Security 273
Storage Resiliency 274
Response and Recovery Controls 280
Capacity Planning for Resilience and Recovery 283
Testing Resilience and Recovery Controls and Designs 284
Physical Security Controls 285
Site Security 285
Detecting Physical Attacks 291
Summary 291
Exam Essentials 292
Review Questions 294

Chapter 10 Cloud and Virtualization Security 299

Exploring the Cloud 300
Benefits of the Cloud 301
Cloud Roles 303
Cloud Service Models 303
Cloud Deployment Models 307
Private Cloud 307
Shared Responsibility Model 309
Cloud Standards and Guidelines 312
Virtualization 314
Hypervisors 314
Cloud Infrastructure Components 316
Cloud Compute Resources 316
Cloud Storage Resources 319
Cloud Networking 322
Cloud Security Issues 325
Availability 325
Data Sovereignty 326
Virtualization Security 327
Application Security 327
Governance and Auditing of Third-Party Vendors 328
Hardening Cloud Infrastructure 328
Cloud Access Security Brokers 328
Resource Policies 329
Secrets Management 330

Summary 331
Exam Essentials 331
Review Questions 333

Chapter 11 Endpoint Security 337

Operating System Vulnerabilities 339
Hardware Vulnerabilities 340
Protecting Endpoints 341
  Preserving Boot Integrity 342
  Endpoint Security Tools 344
Hardening Techniques 350
  Hardening 350
  Service Hardening 350
  Network Hardening 352
  Default Passwords 352
  Removing Unnecessary Software 353
Operating System Hardening 353
  Configuration, Standards, and Schemas 356
  Encryption 357
Securing Embedded and Specialized Systems 358
  Embedded Systems 358
  SCADA and ICS 361
  Securing the Internet of Things 362
  Communication Considerations 363
  Security Constraints of Embedded Systems 364
Asset Management 365
Summary 368
Exam Essentials 369
Review Questions 371

Chapter 12 Network Security 375

Designing Secure Networks 377
  Infrastructure Considerations 380
  Network Design Concepts 380
  Network Segmentation 383
  Zero Trust 385
  Network Access Control 387
  Port Security and Port-Level Protections 388
  Virtual Private Networks and Remote Access 390
  Network Appliances and Security Tools 392
  Deception and Disruption Technology 399
  Network Security, Services, and Management 400
Secure Protocols 406

Using Secure Protocols 406
Secure Protocols 407
Network Attacks 410
On-Path Attacks 411
Domain Name System Attacks 412
Credential Replay Attacks 414
Malicious Code 415
Distributed Denial-of-Service Attacks 415
Summary 418
Exam Essentials 419
Review Questions 421

Chapter 13 Wireless and Mobile Security 425

Building Secure Wireless Networks 426
Connection Methods 427
Wireless Network Models 431
Attacks Against Wireless Networks and Devices 432
Designing a Network 435
Controller and Access Point Security 438
Wi-Fi Security Standards 438
Wireless Authentication 440
Managing Secure Mobile Devices 442
Mobile Device Deployment Methods 442
Hardening Mobile Devices 444
Mobile Device Management 444
Summary 448
Exam Essentials 449
Review Questions 450

Chapter 14 Monitoring and Incident Response 455

Incident Response 457
The Incident Response Process 458
Training 462
Threat Hunting 463
Understanding Attacks and Incidents 464
Incident Response Data and Tools 466
Monitoring Computing Resources 466
Security Information and Event Management Systems 466
Alerts and Alarms 469
Log Aggregation, Correlation, and Analysis 470
Rules 471
Benchmarks and Logging 478
Reporting and Archiving 478

Mitigation and Recovery 479
Secure Orchestration, Automation, and Response (SOAR) 479
Containment, Mitigation, and Recovery Techniques 479
Root Cause Analysis 482
Summary 483
Exam Essentials 484
Review Questions 485

Chapter 15 Digital Forensics 489

Digital Forensic Concepts 490
Legal Holds and e-Discovery 491
Conducting Digital Forensics 493
Acquiring Forensic Data 493
Acquisition Tools 497
Validating Forensic Data Integrity 500
Data Recovery 502
Forensic Suites and a Forensic Case Example 503
Reporting 507
Digital Forensics and Intelligence 508
Summary 508
Exam Essentials 509
Review Questions 511

Chapter 16 Security Governance and Compliance 515

Security Governance 518
Corporate Governance 518
Governance, Risk, and Compliance Programs 520
Information Security Governance 520
Types of Governance Structures 521
Understanding Policy Documents 521
Policies 522
Standards 524
Procedures 526
Guidelines 528
Exceptions and Compensating Controls 529
Monitoring and Revision 530
Change Management 531
Change Management Processes and Controls 532
Version Control 534
Documentation 535
Personnel Management 535
Least Privilege 535

Separation of Duties 535
Job Rotation and Mandatory Vacations 536
Clean Desk Space 536
Onboarding and Offboarding 536
Nondisclosure Agreements 537
Social Media 537
Third-Party Risk Management 537
Vendor Selection 537
Vendor Assessment 538
Vendor Agreements 538
Vendor Monitoring 539
Winding Down Vendor Relationships 540
Complying with Laws and Regulations 540
Common Compliance Requirements 541
Compliance Reporting 541
Consequences of Noncompliance 542
Compliance Monitoring 543
Adopting Standard Frameworks 543
NIST Cybersecurity Framework 544
NIST Risk Management Framework 546
ISO Standards 547
Benchmarks and Secure Configuration Guides 549
Security Awareness and Training 550
User Training 551
Ongoing Awareness Efforts 553
Summary 554
Exam Essentials 555
Review Questions 557

Chapter 17 Risk Management and Privacy 561

Analyzing Risk 563
Risk Identification 564
Risk Assessment 565
Risk Analysis 567
Managing Risk 570
Risk Mitigation 571
Risk Avoidance 572
Risk Transference 572
Risk Acceptance 573
Risk Tracking 574
Risk Register 575
Risk Reporting 576