PEARSON IT CERTIFICATION

Save 10% on Exam Voucher

See Inside

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA® Security+ SY0-701

LEWIS HEUERMANN

FREE SAMPLE CHAPTER

CompTIA Security+ SY0-701 Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonitcertification.com/register.
2. Enter the **print book ISBN**: 9780138293086.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

This page intentionally left blank

CompTIA® Security+ SY0-701 Cert Guide

Lewis Heuermann

Pearson

CompTIA® Security+ SY0-701 Cert Guide

Lewis Heuermann

Copyright © 2024 by Pearson Education, Inc.

Hoboken, New Jersey

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

ISBN-13: 978-0-13-829308-6
ISBN-10: 0-13-829308-2

Library of Congress Cataloging-in-Publication Data: 2024931504

$PrintCode

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screenshots may be viewed in full within the software version specified.

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

GM K12, Early Career and Professional Learning
Soo Kang

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Indexer
Timothy Wright

Proofreader
Barbara Mack

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Introduction xxxix

Part I: General Security Concepts

CHAPTER 1 Comparing and Contrasting the Various Types of Controls 3

CHAPTER 2 Summarizing Fundamental Security Concepts 15

CHAPTER 3 Understanding Change Management's Security Impact 37

CHAPTER 4 Understanding the Importance of Using Appropriate Cryptographic Solutions 53

Part II: Threats, Vulnerabilities, and Mitigations

CHAPTER 5 Comparing and Contrasting Common Threat Actors and Motivations 95

CHAPTER 6 Understanding Common Threat Vectors and Attack Surfaces 105

CHAPTER 7 Understanding Various Types of Vulnerabilities 127

CHAPTER 8 Understanding Indicators of Malicious Activity 149

CHAPTER 9 Understanding the Purpose of Mitigation Techniques Used to Secure the Enterprise 171

Part III: Security Architecture

CHAPTER 10 Comparing and Contrasting Security Implications of Different Architecture Models 189

CHAPTER 11 Applying Security Principles to Secure Enterprise Infrastructure 223

CHAPTER 12 Comparing and Contrasting Concepts and Strategies to Protect Data 271

CHAPTER 13 Understanding the Importance of Resilience and Recovery in Security Architecture 287

Part IV: Security Operations

CHAPTER 14 Applying Common Security Techniques to Computing Resources 305

CHAPTER 15 Understanding the Security Implications of Hardware, Software, and Data Asset Management 345

CHAPTER 16 Understanding Various Activities Associated with Vulnerability Management 357

CHAPTER 17 Understanding Security Alerting and Monitoring Concepts and Tools 381

CHAPTER 18 Modifying Enterprise Capabilities to Enhance Security 409

CHAPTER 19 Implementing and Maintaining Identity and Access Management 435

CHAPTER 20 Understanding the Importance of Automation and Orchestration Related to Secure Operations 471

CHAPTER 21 Understanding Appropriate Incident Response Activities 489

CHAPTER 22 Using Data Sources to Support an Investigation 509

Part V: Security Program Management and Oversight

CHAPTER 23 Summarizing Elements of Effective Security Governance 529

CHAPTER 24 Understanding Elements of the Risk Management Process 557

CHAPTER 25 Understanding the Processes Associated with Third-Party Risk Assessment and Management 585

CHAPTER 26 Summarizing Elements of Effective Security Compliance 599

CHAPTER 27 Understanding Types and Purposes of Audits and Assessments 617

CHAPTER 28 Implementing Security Awareness Practices 631

Part VI: Final Preparation

CHAPTER 29 Final Preparation 647

APPENDIX A Answers to the “Do I Know This Already?” Quizzes and Review Questions 649

Index 693

Online elements

APPENDIX B Study Planner

GLOSSARY OF KEY TERMS

Table of Contents

Introduction xxxix

Part I: General Security Concepts

Chapter 1 Comparing and Contrasting the Various Types of Controls 3

"Do I Know This Already?" Quiz 3

Foundation Topics 6

Control Categories 6

- Technical Controls 6
- Managerial Controls 6
- Operational Controls 6
- Physical Controls 7
- Summary of Control Categories 7

Control Types 8

- Preventive Controls 8
- Deterrent Controls 8
- Detective Controls 9
- Corrective Controls 9
- Compensating Controls 9
- Directive Controls 10
- Summary of Control Types 10

Chapter Review Activities 11

Review Key Topics 11

Define Key Terms 12

Review Questions 12

Chapter 2 Summarizing Fundamental Security Concepts 15

"Do I Know This Already?" Quiz 15

Foundation Topics 19

Confidentiality, Integrity, and Availability (CIA) 19

Non-repudiation 20

Authentication, Authorization, and Accounting (AAA) 21

Gap Analysis 22

Zero Trust 22

Physical Security 24

Bollards/Barricades 24

Access Control Vestibules 26

Fencing 27

Video Surveillance 28

Security Guards 28

Access Badges 29

Lighting 30

Sensors 30

Deception and Disruption Technology 31

Chapter Review Activities 32

Review Key Topics 32

Define Key Terms 33

Review Questions 33

Chapter 3 Understanding Change Management's Security Impact 37

"Do I Know This Already?" Quiz 37

Foundation Topics 41

Business Processes Impacting Security Operations 41

Approval Process 41

Ownership 41

Stakeholders 42

Impact Analysis 42

Test Results 42

Backout Plan 42

Maintenance Window 43

Standard Operating Procedure 43

Technical Implications 43

Allow Lists 44

Block Lists/Deny Lists 44

Restricted Activities 44

Downtime 45

Service Restart 45

Application Restart 46

Legacy Applications 46

Dependencies 46

Documentation 47
  Updating Diagrams 47
  Updating Policies/Procedures 48
Version Control 48
Chapter Review Activities 49
Review Key Topics 49
Define Key Terms 49
Review Questions 49
Chapter 4 Understanding the Importance of Using Appropriate Cryptographic Solutions 53
"Do I Know This Already?" Quiz 53
Foundation Topics 58
Public Key Infrastructure (PKI) 58
  Public Key 58
  Private and Public Key 58
Encryption 59
  Level 59
  Full Disk 59
  Partition 60
  File 60
  Volume 60
  Database 60
  Record 61
Transport/Communication 61
  Encryption at Rest, in Transit/Motion, and in Processing 61
Symmetric Versus Asymmetric Encryption 62
Key Exchange 64
Algorithms 65
Key Length 66
Tools 67
Trusted Platform Module 67
Hardware Security Module 68
Key Management System 68
Secure Enclave 69
Obfuscation 70

Steganography 70
Audio Steganography 71
Video Steganography 71
Image Steganography 72
Tokenization 72
Data Masking 74
Hashing 75
Salting 76
Digital Signatures 76
Key Stretching 77
Blockchain 78
Open Public Ledger 78
Certificates 79
Certificate Authorities 79
Certificate Revocation Lists 81
Online Certificate Status Protocol (OCSP) 82
Self-Signed 83
Third-Party 89
Root of Trust 89
Certificate-Signing Request 90
Wildcard 90
Chapter Review Activities 90
Review Key Topics 90
Define Key Terms 91
Review Questions 91

Part II: Threats, Vulnerabilities, and Mitigations

Chapter 5 Comparing and Contrasting Common Threat Actors and Motivations 95
"Do I Know This Already?" Quiz 95
Foundation Topics 98
Threat Actors 98
Attributes of Actors 99
Motivations 100
War 101

Chapter Review Activities 102
Review Key Topics 102
Define Key Terms 102
Review Questions 102

Chapter 6 Understanding Common Threat Vectors and Attack Surfaces 105

"Do I Know This Already?" Quiz 105
Foundation Topics 109
Message-Based 109
- Email 109
- Short Message Service (SMS) 109
- Instant Messaging (IM) 110
- Spam and Spam over Internet Messaging (SPIM) 110

Image-Based 111
File-Based 111
Voice Call 111
Removable Device 111
Vulnerable Software 112
Unsupported Systems and Applications 112
Unsecure Networks 113
Open Service Ports 114
Default Credentials 115
Supply Chain 116
Human Vectors/Social Engineering 116
- Phishing 117
- Vishing 120
- Smishing 121
- Misinformation/Disinformation 121
- Impersonation 121
- Business Email Compromise (BEC) 122
- Pretexting 122
- Watering Hole Attack 122
- Brand Impersonation 123
- Typosquatting 123

Chapter Review Activities 123
Review Key Topics 123
Define Key Terms 124
Review Questions 124
Chapter 7 Understanding Various Types of Vulnerabilities 127
"Do I Know This Already?" Quiz 127
Foundation Topics 130
Application 130
  Memory Injection 130
  Buffer Overflow 131
  Race Conditions 132
  Malicious Update 132
Operating System (OS)–Based 133
Web-Based 133
  Structured Query Language Injection (SQLi) Vulnerabilities 133
  Cross-Site Scripting (XSS) Vulnerabilities 134
Hardware 134
  Firmware 134
  End-of-Life (EOL) 134
  Legacy 135
Virtualization 135
  Virtual Machine (VM) Escape 135
  Resource Reuse 135
Cloud Specific 136
  Other "Cloud"-Based Concerns 140
Supply Chain 141
  Service Provider 141
  Hardware Provider 141
  Software Provider 142
Cryptographic 142
Misconfiguration 142
Mobile Device 142
  Side Loading 143
  Jailbreaking 143

Zero-Day Vulnerabilities 143
Chapter Review Activities 145
Review Key Topics 145
Define Key Terms 145
Review Questions 146
Chapter 8 Understanding Indicators of Malicious Activity 149
"Do I Know This Already?" Quiz 149
Foundation Topics 152
Malware Attacks 152
  Ransomware 152
  Trojans 153
  Worms 154
  Spyware 154
  Bloatware 155
  Virus 155
  Keylogger 155
  You Can't Save Every Computer from Malware! 156
  Logic Bomb 157
  Rootkit 157
Physical Attacks 158
  Brute-Force Attacks 159
  Radio Frequency Identification (RFID) Cloning 159
  Environmental 159
Network Attacks 160
  Distributed Denial-of-Service (DDoS) Attacks 160
  Domain Name System (DNS) Attacks 160
  Wireless Attacks 160
  On-Path Attacks 161
  Credential Replay 161
  Malicious Code 161
Application Attacks 162
  Injection 162
  Buffer Overflow 162
  Replay 162

Privilege Escalation 162

Forgery 163

Directory Traversal 163

Cryptographic Attacks 163

Downgrade 163

Collision 163

Birthday 164

Password Attacks 164

Password Spraying 165

Brute-Force Attacks 165

Indicators 165

Account Lockout 166

Concurrent Session Usage 166

Blocked Content 166

Impossible Travel 166

Resource Consumption 166

Resource Inaccessibility 166

Out-of-Cycle Logging 167

Published/Documented Indicators 167

Missing Logs 167

Chapter Review Activities 167

Review Key Topics 167

Define Key Terms 168

Review Questions 168

Chapter 9 Understanding the Purpose of Mitigation Techniques Used to Secure the Enterprise 171

“Do I Know This Already?” Quiz 171

Foundation Topics 175

Segmentation 175

Access Control 175

Access Control Lists (ACLs) 175

Permissions 176

Windows Permissions 176

Linux Permissions 177

Best Practices 177

Application Allow List 178

Isolation 179

Patching 180

Encryption 181

Monitoring 182

Least Privilege 182

Configuration Enforcement 182

Decommissioning 183

Hardening Techniques 183

Encryption 183

Installation of Endpoint Protection 184

Host-Based Firewall 184

Host-Based Intrusion Prevention System (HIPS) 184

Disabling Ports/Protocols 184

Default Password Changes 185

Removal of Unnecessary Software 185

Chapter Review Activities 185

Review Key Topics 185

Define Key Terms 186

Review Questions 186

Part III: Security Architecture

Chapter 10 Comparing and Contrasting Security Implications of Different Architecture Models 189

"Do I Know This Already?" Quiz 189

Foundation Topics 193

Architecture and Infrastructure Concepts 193

Cloud 193

Responsibility Matrix 193

Hybrid Considerations 194

Third-Party Vendors 195

Infrastructure as Code (IaC) 195

Serverless 196

Microservices 197

Network Infrastructure 197

Physical Isolation 198

Air-Gapped 198

Logical Segmentation 198

Software-Defined Network (SDN) 199

On-premises 201

Centralized Versus Decentralized 201

Centralized Systems 201

Decentralized Systems 202

Containerization 202

Virtualization 206

Security Implications 206

IoT 208

Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) 210

Real-Time Operating System (RTOS) 213

Embedded Systems 214

High Availability 214

Considerations 215

Availability 215

Resilience 215

Cost 216

Responsiveness 216

Scalability 216

Ease of Deployment 216

Risk Transference 217

Ease of Recovery 217

Patch Availability 217

Inability to Patch 218

Power 218

Compute 218

Chapter Review Activities 219

Review Key Topics 219

Define Key Terms 219

Review Questions 220

Chapter 11 Applying Security Principles to Secure Enterprise Infrastructure 223

"Do I Know This Already?" Quiz 223

Foundation Topics 226

Infrastructure Considerations 226

Device Placement 226

Security Zones 226

Attack Surface 227

Connectivity 228

Failure Modes 228

Device Attribute 229

Active vs. Passive 229

Inline vs. Tap/Monitor 229

Network Appliances 230

Jump Servers 230

Proxy Servers 230

Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) 233

Load Balancer 234

Sensors 235

Port Security 235

802.1X and EAP 236

IEEE 802.1X 239

Firewall Types 239

Web Application Firewall (WAF) 243

Unified Threat Management (UTM) 245

Next-Generation Firewall (NGFW) 246

Hardware vs. Software 247

Layer 4/Layer 7 248

Secure Communication/Access 249

Virtual Private Network (VPN) 249

Remote Access 251

Tunneling 254

Transport Layer Security (TLS) 254

Internet Protocol Security (IPsec) 257

IKEv1 Phase 1 257

IKEv1 Phase 2 261

IKEv2 264

Software-Defined Wide Area Network (SD-WAN) 265

Secure Access Service Edge (SASE) 265

Selection of Effective Controls 266

Chapter Review Activities 266

Review Key Topics 266

Define Key Terms 267

Review Questions 268

Chapter 12 Comparing and Contrasting Concepts and Strategies to Protect Data 271

"Do I Know This Already?" Quiz 271

Foundation Topics 274

Data Types 274

Data Classifications 275

General Data Considerations 276

Data States 276

Data at Rest 277

Data in Transit 277

Data in Use 278

Data Sovereignty 278

Geolocation 278

Methods to Secure Data 279

Geographic Restrictions 279

Encryption 279

Hashing 279

Masking 281

Tokenization 281

Obfuscation 281

Segmentation 281

Permission Restrictions 282

Chapter Review Activities 283

Review Key Topics 283

Define Key Terms 284

Review Questions 284

Chapter 13 Understanding the Importance of Resilience and Recovery in Security Architecture 287

"Do I Know This Already?" Quiz 287

Foundation Topics 291

High Availability 291

Key Components 291

Cloud Environments 291

Site Considerations 292

Platform Diversity 294

Multi-Cloud System 294

Continuity of Operations 294

Capacity Planning 295

Testing 296

Tabletop Exercises 296

Failover 297

Simulations 298

Parallel Processing 299

Backups 299

Power 301

Uninterruptible Power Supply (UPS) 301

Generators 301

Chapter Review Activities 302

Review Key Topics 302

Define Key Terms 302

Review Questions 303

Part IV: Security Operations

Chapter 14 Applying Common Security Techniques to Computing Resources 305

"Do I Know This Already?" Quiz 305

Foundation Topics 309

Secure Baselines 309

Inventory Assessment 309

Vulnerability Scanning 309

Minimum Configuration Standards 310

- Documentation 310
- Deployment 310
- Ongoing Maintenance 311

Hardening Targets 311

Wireless Devices 315

Mobile Solutions 318

- Mobile Device Management 318
- MDM Security Feature Concerns: Application and Content Management 320
- MDM Security Feature Concerns: Remote Wipe, Geofencing, Geolocation, Screen Locks, Passwords and PINs, and Full Device Encryption 322
- Deployment Models 325
- Secure Implementation of BYOD, CYOD, and COPE 326

Connection Methods 328

- Secure Implementation Best Practices 330

Wireless Security Settings 331

- Wi-Fi Protected Access 3 (WPA3) 332
- Remote Authentication Dial-In User Service (RADIUS) Federation 332
- Cryptographic Protocols 334
- Authentication Protocols 335

Application Security 336

- Input Validations 337
- Secure Cookies 337
- Static Code Analysis 338
- Code Signing 339

Sandboxing 340

Monitoring 340

Chapter Review Activities 341

Review Key Topics 341

Define Key Terms 342

Review Questions 342

Chapter 15 Understanding the Security Implications of Hardware, Software, and Data Asset Management 345

"Do I Know This Already?" Quiz 345

Foundation Topics 348

Acquisition/Procurement Process 348

Assignment/Accounting 350

Monitoring/Asset Tracking 350

- Inventory 351
- Enumeration 351

Disposal/Decommissioning 351

- Sanitization 352
- Destruction 352
- Certification 353
- Data Retention 353

Chapter Review Activities 354

Review Key Topics 354

Define Key Terms 354

Review Questions 354

Chapter 16 Understanding Various Activities Associated with Vulnerability Management 357

"Do I Know This Already?" Quiz 357

Foundation Topics 360

Identification Methods 360

- Vulnerability Scan 360
- Application Security 362
- Threat Feed 364
- *Open-Source Intelligence (OSINT) 364*
- *Proprietary/Third-Party 364*
- *Information-Sharing Organization 364*
- *Dark Web 365*
- Penetration Testing 366
- Responsible Disclosure Program 366
- *Bug Bounty Program 367*
- System/Process Audit 367

Analysis 367
Confirmation 368
Prioritize 368
Common Vulnerability Scoring System (CVSS) 368
Practical Utility 370
Common Vulnerability Enumeration (CVE) 370
Vulnerability Classification 370
Exposure Factor 371
Environmental Variables 372
Industry/Organizational Impact 372
Risk Tolerance 372
Vulnerability Response and Remediation 374
Patching 374
Insurance 374
Segmentation 374
Compensating Controls 375
Exceptions and Exemptions 375
Validation of Remediation 376
Rescanning 376
Audit 376
Verification 376
Reporting 377
Chapter Review Activities 378
Review Key Topics 378
Define Key Terms 379
Review Questions 379
Chapter 17 Understanding Security Alerting and Monitoring Concepts and Tools 381
"Do I Know This Already?" Quiz 381
Foundation Topics 383
Monitoring and Computing Resources 383
Activities 386
Log Aggregation 386
Alerting 388
Scanning 389

Reporting 390

Archiving 391

Alert Response and Remediation/Validation 392

Tools 392

Security Content Automation Protocol (SCAP) 393

Benchmarks 395

Agents/Agentless 397

Security Information and Event Management (SIEM) 397

NetFlow 399

Antivirus Software 400

Data Loss Prevention (DLP) 401

Simple Network Management Protocol (SNMP) Traps 401

Vulnerability Scanners 403

Chapter Review Activities 405

Review Key Topics 405

Define Key Terms 406

Review Questions 406

Chapter 18 Modifying Enterprise Capabilities to Enhance Security 409

"Do I Know This Already?" Quiz 409

Foundation Topics 413

Firewall 413

Rules 414

Access Lists 415

Ports/Protocols 416

Screened Subnet 417

IDS/IPS 418

Trends 419

Signatures 419

Web Filter 421

Operating System Security 423

Implementation of Secure Protocols 424

DNS Filtering 427

Email Security 427

File Integrity Monitoring 429

DLP 429

Network Access Control (NAC) 430

Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR) 430

User Behavior Analytics 431

Chapter Review Activities 432

Review Key Topics 432

Define Key Terms 433

Review Questions 433

Chapter 19 Implementing and Maintaining Identity and Access Management 435

"Do I Know This Already?" Quiz 435

Foundation Topics 439

Provisioning/De-provisioning User Accounts 439

Permission Assignments and Implications 439

Identity Proofing 441

Federation 441

Single Sign-On (SSO) 443

- Lightweight Directory Access Protocol (LDAP) 443
- OAuth 444
- Security Assertion Markup Language 446

Interoperability 448

Attestation 449

Access Controls 450

- Role-Based Access Control 450
- Rule-Based Access Control 451
- Mandatory Access Control 451
- Discretionary Access Control 452
- Attribute-Based Access Control (ABAC) 454
- Time-of-Day Restrictions 455
- Least Privilege 456

Multifactor Authentication (MFA) 456

- Implementations 457
- *Biometrics 457*
- *Hard and Soft Authentication Keys 457*

Security Keys 458

Factors 459

Something You Know 459

Something You Have 459

Something You Are 460

Somewhere You Are 461

Password Concepts 461

Password Best Practices 461

Password Managers 464

Passwordless 465

Privileged Access Management Tools 465

Just-in-Time Permissions 466

Password Vaulting 466

Ephemeral Credentials 466

Chapter Review Activities 467

Review Key Topics 467

Define Key Terms 468

Review Questions 468

Chapter 20 Understanding the Importance of Automation and Orchestration Related to Secure Operations 471

"Do I Know This Already?" Quiz 471

Foundation Topics 474

Use Cases of Automation and Scripting 474

User Provisioning 474

Resource Provisioning 477

Guard Rails 477

Security Groups 477

Ticket Creation and Escalation 477

Continuous Integration and Testing 478

Integrations and Application Programming Interfaces (APIs) 479

Benefits 480

Efficiency/Time Saving 480

Enforcing Baselines 480

Standard Infrastructure Configurations 481

Scaling in a Secure Manner 481

Employee Retention 481

Reaction Time 482

Workforce Multiplier 482

Other Considerations 482

Complexity 482

Cost 483

Single Point of Failure 483

Technical Debt 483

Ongoing Supportability 484

Chapter Review Activities 485

Review Key Topics 485

Define Key Terms 486

Review Questions 486

Chapter 21 Understanding Appropriate Incident Response Activities 489

"Do I Know This Already?" Quiz 489

Foundation Topics 493

Process 493

Preparation 494

Detection 495

Analysis 496

Containment 496

Eradication 496

Recovery 497

Lessons Learned 497

Training 497

Testing 498

The Anatomy of a Tabletop Exercise 499

The Intricacies of Simulation Exercises 499

Mock Example of a Tabletop Exercise 500

Root Cause Analysis 501

Threat Hunting 502

Digital Forensics 502

Legal Hold 503

Chain of Custody 503

Acquisition 503

Reporting 505

Preservation 505

E-Discovery 506

Chapter Review Activities 506

Review Key Topics 506

Define Key Terms 506

Review Questions 507

Chapter 22 Using Data Sources to Support an Investigation 509

"Do I Know This Already?" Quiz 509

Foundation Topics 512

Log Data 512

Firewall Logs 513

Application Logs 513

Endpoint Logs 515

OS-Specific Security Logs 515

IPS/IDS Logs 517

Network Logs 518

Metadata 518

Data Sources 521

Vulnerability Scans 522

Automated Reports 522

Dashboards 523

Packet Captures 525

Chapter Review Activities 525

Review Key Topics 525

Define Key Terms 526

Review Questions 526

Part V: Security Program Management and Oversight

Chapter 23 Summarizing Elements of Effective Security Governance 529

"Do I Know This Already?" Quiz 529

Foundation Topics 532

Guidelines 532

Policies 532

- Acceptable Use 533
- Information Security Policies 533
- Business Continuity 535
- Disaster Recovery 535
- Incident Response 535
- Software Development Lifecycle (SDLC) 536
- Change Management 536

Standards 536

- Password Standards 537
- Access Control Standards 538
- Physical Security Standards 539
- Encryption Standards 539

Procedures 541

- Change Management 541
- Onboarding and Offboarding 542
- Playbooks 542

External Considerations 543

- Regulatory 543
- Legal 544
- Industry 544
- Local/Regional 544
- National 545
- Global 545

Monitoring and Revision 545

Types of Governance Structures 546

- Boards 546
- Committees 547
- Government Entities 547
- Centralized/Decentralized 548
- *Centralized Governance 548*
- *Decentralized Governance 548*

Roles and Responsibilities for Systems and Data 549

- Owners 549
- Controllers 550

Processors 551

Custodians/Stewards 552

Chapter Review Activities 553

Review Key Topics 553

Define Key Terms 553

Review Questions 554

Chapter 24 Understanding Elements of the Risk Management Process 557

"Do I Know This Already?" Quiz 557

Foundation Topics 561

Risk Identification 561

Risk Assessment 562

Ad Hoc 562

Recurring 562

One-time 562

Continuous 562

Risk Analysis 563

Qualitative Risk Assessment 565

Quantitative Risk Assessment 565

Probability 567

Data-Driven Decision Making 568

Risk Prioritization 568

Financial Planning 568

Scenario Analysis 568

Communication and Reporting 568

Continuous Monitoring and Adjustment 568

Likelihood 569

Risk Categorization 569

Decision-Making Frameworks 569

Resource Allocation 569

Sensitivity Analysis 569

Stakeholder Communication 569

Exposure Factor 570

Impact 571

Risk Register 572

Key Risk Indicators (KRIs) 572

Risk Owners 572

Risk Threshold 572

Risk Tolerance 574

Risk Appetite 574

Expansionary 574

Conservative 575

Neutral 575

Risk Management Strategies 575

Risk Transfer 576

Risk Acceptance 576

Risk Avoidance 576

Risk Mitigation 576

Risk Reporting 577

Business Impact Analysis 578

Recovery Time Objective (RTO) 579

Recovery Point Objective (RPO) 579

Mean Time to Repair (MTTR) 579

Mean Time Between Failures (MTBF) 580

Chapter Review Activities 582

Review Key Topics 582

Define Key Terms 582

Review Questions 583

Chapter 25 Understanding the Processes Associated with Third-Party Risk Assessment and Management 585

"Do I Know This Already?" Quiz 585

Foundation Topics 588

Vendor Assessment 588

Penetration Testing 589

Right-to-Audit Clause 589

Evidence of Internal Audits 590

Independent Assessments 590

Supply Chain Analysis 591

Vendor Selection 591

Due Diligence 592

Conflict of Interest 592

Agreement Types 593

Vendor Monitoring 594

Questionnaires 594

Rules of Engagement 595

Chapter Review Activities 595

Review Key Topics 595

Define Key Terms 596

Review Questions 596

Chapter 26 Summarizing Elements of Effective Security Compliance 599

"Do I Know This Already?" Quiz 599

Foundation Topics 602

Compliance Reporting 602

Internal Reporting 603

External Reporting 603

Consequences of Non-compliance 603

Fines 603

Sanctions 604

Reputational Damage 604

Loss of License 604

Contractual Impacts 605

Compliance Monitoring 605

Due Diligence/Care 605

Attestation and Acknowledgment 607

Internal and External 608

Automation 608

Privacy 609

Legal Implications 609

Data Subject 611

Controller vs. Processor 611

Ownership 612

Data Inventory and Retention 612

Right to Be Forgotten 613

Chapter Review Activities 613

Review Key Topics 613

Define Key Terms 614

Review Questions 614

Chapter 27 Understanding Types and Purposes of Audits and Assessments 617

"Do I Know This Already?" Quiz 617

Foundation Topics 620

Attestation 620

Internal 621

External 622

Penetration Testing 623

Chapter Review Activities 628

Review Key Topics 628

Define Key Terms 629

Review Questions 629

Chapter 28 Implementing Security Awareness Practices 631

"Do I Know This Already?" Quiz 631

Foundation Topics 634

Phishing 634

Anomalous Behavior Recognition 635

User Guidance and Training 638

Reporting and Monitoring 641

Development 642

Execution 642

Chapter Review Activities 643

Review Key Topics 643

Define Key Terms 643

Review Questions 644

Part VI: Final Preparation

Chapter 29 Final Preparation 647

Hands-on Activities 647

Suggested Plan for Final Review and Study 648

Summary 648

Appendix A Answers to the "Do I Know This Already?" Quizzes and Review Questions 649

Index 693

Online Elements

Appendix B Study Planner

Glossary of Key Terms

About the Author

Lewis Heuermann, CISSP, PMP, is a Navy submarine veteran and seasoned cybersecurity consultant who combines his extensive practical experience with deep academic insight to make cybersecurity accessible to all learners. His diverse background includes roles in systems and network engineering, network defense analysis, and cyber risk management. As a professor, he has developed and taught courses in cybersecurity and data analytics, utilizing tools like Python, SQL, Power BI, and Tableau. Lewis also holds several key IT certifications.

Dedication

To Katie, my loving wife, whose unwavering support and encouragement have been my constant. Your ability to keep me caffeinated and focused during those long-day and late-night writing sessions has been nothing short of miraculous. You were the one who finally convinced me to stop saying "One day…" when I talked about writing a book and instead say "Today…."

To Dominique, thank you for being a steadfast presence during all those early years of countless nights I spent on the phone troubleshooting network and server issues. Your patience, encouragement, and understanding during those challenging years played a significant role in my journey.

And to my wonderful children: When people tell you that you "can't," it just means they couldn't. Keep pushing and keep learning because "can't" never could do anything.

—Lewis

Acknowledgments

I extend my heartfelt thanks to the Pearson team, whose collective efforts have been instrumental in bringing this book to fruition. Ellie, your remarkable skill in making all the pieces of this complex puzzle fit seamlessly together is truly amazing. Chris, your meticulous attention to detail has elevated the quality of this work beyond my wildest imagination. Kitty, your sharp copyediting eye and expert grammar makes the pages sing!

Nancy, you have been the foundation of our team, guiding us with kindness, support, and an unwavering commitment to our collective goal. You saw something in me early and helped turn my dream into a reality. To all of my many mentors over the years, thank you for taking the time to slowly explain things to me when you didn't have the time to slow down. Each of you has contributed to this journey in unique and meaningful ways, and for that, I am eternally grateful.

About the Technical Reviewer

Chris Crayton 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 authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *CompTIA Security+ SY0-701 Cert Guide* for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780138293086 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to *CompTIA Security+ SY0-701 Cert Guide*. The CompTIA Security+ certification is widely accepted as one of the first security certifications you should attempt to attain in your information technology (IT) career. The CompTIA Security+ certification exam is designed to be a vendor-neutral exam that measures your knowledge of industry-standard technologies and methodologies. It acts as a great stepping stone to other vendor-specific certifications and careers. We developed this book to be something you can study from for the exam and keep on your bookshelf for later use as a security resource.

We would like to note that it would not be possible to cover all security concepts in depth in a single book. However, the Security+ exam objectives are looking for a basic level of computer, networking, and organizational security knowledge. Keep this in mind while reading through this text and remember that the main goal of this text is to help you pass the Security+ exam, not to have an encyclopedic knowledge of everything security—though you might get there someday!

As you read through this book, you will begin building your foundational knowledge, gaining hands-on familiarity and the know-how to pass the CompTIA Security+ exam. Good luck on the exam!

Goals and Methods

The number-one goal of this book is to help you pass the SY0-701 version of the CompTIA Security+ certification exam. To that effect, we have filled this book and practice exams with hundreds of questions/answers and explanations, including two full practice exams. The exams are located in Pearson Test Prep practice test software, in a custom test environment. These tests are meant to check your knowledge and prepare you for the real exam.

The CompTIA Security+ certification exam requires familiarity with computer security theory and hands-on knowledge. To aid you in understanding the Security+ certification objectives, this book uses the following methods:

- **Opening topics list:** This list defines the topics covered in the chapter.
- **Foundation Topics:** This is the heart of the chapter, explaining various topics from a theory-based standpoint as well as from a hands-on perspective. This section of each chapter includes in-depth descriptions, tables, and figures that are geared toward helping you build your knowledge so that you can pass the exam. Each chapter covers a full objective from the CompTIA Security+ exam blueprint.

- **Key Topics:** The Key Topic icons indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.
- **Key Terms:** Key terms without definitions are listed at the end of each chapter. See whether you can define them and then check your work against the definitions provided in the glossary.
- **Review Questions:** These questions and answers with explanations are meant to gauge your knowledge of the subjects covered in the chapter. If an answer to a question doesn't come readily to you, be sure to review the corresponding portion of the chapter.
- **Practice Exams:** Practice exams are included in the Pearson Test Prep practice test software. These exams test your knowledge and skills in a realistic testing environment. Take them after you have read through the entire book. Gain a thorough understanding of each one before moving on to the next one.

Who Should Read This Book?

This book is for anyone who wants to start or advance a career in computer security. Readers of this book may range from persons taking a Security+ course to individuals already in the field who want to keep their skills sharp or perhaps retain their job due to a company policy mandating that they take the Security+ exam. Some information assurance professionals who work for the Department of Defense (DoD) or have privileged access to DoD systems are required to become Security+ certified as per DoD directive 8570.01-Manual.

This book is also designed for people who plan on taking additional security-related certifications after the CompTIA Security+ exam. The book is designed in such a way to offer an easy transition to future certification studies.

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of IT administration experience, with an emphasis on hands-on and technical security concepts. The CompTIA Network+ certification is also recommended as a prerequisite. Before you begin your Security+ studies, you are expected to understand computer topics such as how to install operating systems and applications and networking topics such as how to configure IP addressing and what a VLAN is. This book shows you how to secure these technologies and protect against possible exploits and attacks. Generally, for people looking to enter the IT field, the CompTIA Security+ certification is attained after the A+ and Network+ certifications.

CompTIA Security+ Exam Topics

If you haven't downloaded the Security+ certification exam objectives from the CompTIA website (https://certification.comptia.org), do so now. Save the PDF file and print it out as well. It's a big document, and you should review it carefully. Use the blueprint's exam objectives list and acronyms list to aid in your studies while you use this book.

The following tables are excerpts from the exam objectives document. Table I-1 lists the CompTIA Security+ domains and each domain's percentage of the exam.

Table I-1 CompTIA Security+ Exam Domains

Domain	Exam Topic	% of Exam
1.0	General Security Concepts	12%
2.0	Threats, Vulnerabilities, and Mitigations	22%
3.0	Security Architecture	18%
4.0	Security Operations	28%
5.0	Security Program Management and Oversight	20%

The Security+ domains are further broken down into individual objectives. Table I-2 lists the CompTIA Security+ exam objectives and their related chapters in this book. It does not list the bullets and sub-bullets for each objective.

Table I-2 CompTIA Security+ Exam Objectives

Objective	Chapter(s)
1.1 Compare and contrast various types of security controls.	1
1.2 Summarize fundamental security concepts.	2
1.3 Explain the importance of change management processes and the impact to security.	3
1.4 Explain the importance of using appropriate cryptographic solutions.	4
2.1 Compare and contrast common threat actors and motivations.	5
2.2 Explain common threat vectors and attack surfaces.	6
2.3 Explain various types of vulnerabilities.	7
2.4 Given a scenario, analyze indicators of malicious activity.	8

Objective	Chapter(s)
2.5 Explain the purpose of mitigation techniques used to secure the enterprise.	9
3.1 Compare and contrast security implications of different architecture models.	10
3.2 Given a scenario, apply security principles to secure enterprise infrastructure.	11
3.3 Compare and contrast concepts and strategies to protect data.	12
3.4 Explain the importance of resilience and recovery in security architecture.	13
4.1 Given a scenario, apply common security techniques to computing resources.	14
4.2 Explain the security implications of proper hardware, software, and data asset management.	15
4.3 Explain various activities associated with vulnerability management.	16
4.4 Explain security alerting and monitoring concepts and tools.	17
4.5 Given a scenario, modify enterprise capabilities to enhance security.	18
4.6 Given a scenario, implement and maintain identity and access management.	19
4.7 Explain the importance of automation and orchestration related to secure operations.	20
4.8 Explain appropriate incident response activities.	21
4.9 Given a scenario, use data sources to support an investigation.	22
5.1 Summarize elements of effective security governance.	23
5.2 Explain elements of the risk management process.	24
5.3 Explain the processes associated with third-party risk assessment and management.	25
5.4 Summarize elements of effective security compliance.	26
5.5 Explain types and purposes of audits and assessments.	27
5.6 Given a scenario, implement security awareness practices.	28

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials, as well as additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicting that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access the companion website, follow these steps:

Step 1. Go to **www.pearsonitcertification.com/register** and log in or create a new account.

Step 2. On your Account page, tap or click the **Registered Products** tab and then tap or click the **Register Another Product** link.

Step 3. Enter this book's ISBN: **9780138293086**.

Step 4. Answer the challenge question to provide proof of book ownership.

Step 5. Tap or click the **Access Bonus Content** link for this book to go to the page where your downloadable content is available.

NOTE Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the preceding steps, please visit http://www.pearsonitcertification.com/contact and select the Site Problems/Comments option. Our customer service representatives will assist you.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780138293086) on pearsonitcertification.com/register. Make sure to use the print book ISBN, regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
- Premium Edition: If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonitcertification.com, click Account to see details of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website as shown earlier in this Introduction under the heading, "Companion Website."

Step 2. Click the **Practice Test Software** button.

Step 3. Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode enables you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time allowed for taking the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires that you be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the **Tools** tab and click the **Update Application** button. Doing so enables you to ensure that you are running the latest version of the software engine.

Figure Credits

Cover: greenbutterfly/Shutterstock

Figure 2-2: Kyryl Gorlov/123RF

Figure 2-3: Aliaksandr Karankevich/123RF

Figure 2-5: rewelda/Shutterstock

Figure 8-1: WannaCry ransomware

Figure 10-1: Amazon Web Services, Inc

Figures 11-2, 11-9, 19-2, 19-6, 19-9, 22-2–22-4: Microsoft Corporation

Figures 14-2, 14-3: Cisco Systems, Inc

Figure 19-7: Robert Koczera/123RF

Figure 22-1: MaxBelkov

Figure 22-5: Google LLC

Figure 22-6: Tenable®, Inc

Figure 22-7: LogRhythm, Inc

CHAPTER 3

Understanding Change Management's Security Impact

This chapter examines the critical role of change management processes in fortifying an organization's cybersecurity posture. Change management is more than just an administrative task; it is a significant component of audit and compliance requirements, providing a structured approach for reviewing, approving, and implementing changes to information systems. Change management minimizes unplanned outages due to unauthorized alterations by helping to manage cybersecurity and operational risks. The process typically involves well-defined steps, such as requesting, reviewing, approving, or rejecting and testing, scheduling, implementing, and documenting changes. These steps can serve as a blueprint for standard operating procedures (SOPs) in change management, ensuring that each alteration is systematically vetted and executed. As you will see throughout this chapter, a structured approach is vital for maintaining the integrity and resilience of security mechanisms in the face of a constantly evolving threat landscape.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Chapter Review Activities" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 3-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Business Processes Impacting Security Operations	1–4
Technical Implications	5–7
Documentation	8, 9
Version Control	10

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following can be a consequence of an ineffective approval process?
   a. It can lead to poorly vetted changes being implemented, inadvertently introducing new system vulnerabilities.
   b. It can lead to a more comprehensive security solution.
   c. It can lead to failure of asset ownership protocols.
   d. It can cause communication problems between stakeholders.

2. Who is responsible for defining an asset's security requirements, managing its risk profile, and addressing any vulnerabilities in the system?
   a. Stakeholders
   b. Customers
   c. Owners
   d. Approvals

3. Who are stakeholders, in the context of security operations in an organization?
   a. Only the IT staff
   b. Only individuals or groups external to the business
   c. Only customers
   d. Any individual or group vested in the organization's security posture, which can include system users, IT staff, management, customers, investors, and any entity affected by a security breach or whose actions could impact the organization's security posture

4. What is the role of an approval process in an organization's security operations?
   a. To define the asset's security requirements
   b. To manage the risk profile of assets
   c. To dictate how changes impacting security are approved and who holds the authority to make such decisions
   d. To establish the accountability of asset owners

5. What is the primary purpose of an allow list in a system's security?
   a. To list all actions that are disallowed in the system
   b. To approve inputs a user or machine can perform in the system
   c. To list all the modifications to security protocols
   d. To identify the potential consequences or effects of a technology-related decision or event

6. What is the purpose of restricted activities in a computer or network system?
   a. To disrupt business operations and negatively impact employee productivity
   b. To list the potential consequences of a technology-related decision
   c. To uphold cybersecurity standards by limiting or prohibiting specific actions or operations
   d. To approve specific actions or operations

7. Why is understanding the technical implications of any new or existing system crucial in security operations?
   a. It is needed for the approval process.
   b. It helps in maintaining functionality and security for the system.
   c. It helps in defining the restricted activities.
   d. It assists in implementing deny lists.

8. Why is maintaining up-to-date documentation crucial in IT or cybersecurity operations?
   a. It is essential for updating policies and procedures.
   b. It ensures a clear understanding of system operations, facilitates staff training, and helps in troubleshooting issues.
   c. It helps in updating diagrams of systems or networks.
   d. It assists in managing network interfaces.

9. What is the significance of updating diagrams in IT and cybersecurity?
   a. It aids in creating user guides and technical specifications.
   b. It assists in understanding the rules governing how IT systems are used and secured.

   c. It ensures that everyone has an accurate and current picture of the systems, enhancing troubleshooting and system upgrades.
   d. It helps in updating policies and procedures.

10. Why is version control vital in IT and cybersecurity domains?
    a. It makes it possible to track changes to files, pinpoint when and by whom those changes were made, and, if necessary, revert to an earlier version.
    b. It helps to ensure the security of the data in the files.
    c. It allows the user to duplicate files for various purposes.
    d. It aids in the encryption of the files.

Foundation Topics

Key Topic

Business Processes Impacting Security Operations

Security operations in any organization are often heavily influenced by various business processes. A ***business process*** is a set of coordinated tasks and procedures that an organization uses to accomplish a specific organizational goal or to deliver a particular product or service. Each process—be it approval mechanisms, ownership protocols, stakeholder interactions, impact analysis, or test results evaluation—has the potential to shape the organization's security posture. For instance, an ineffective approval process could lead to poorly vetted changes being implemented and new system vulnerabilities inadvertently being introduced. It's important to note that the effectiveness of business processes is often gauged using performance baselines. A performance baseline serves as a standard measure to assess the impact of any changes on security, ensuring alignment with organizational security objectives.

On the other hand, a robust ownership protocol ensures that each asset, such as a data set or an application, has an assigned custodian, and ensures that its security requirements are regularly reviewed and addressed. Understanding the interaction between these business processes and security operations is crucial for maintaining a strong security stance and safeguarding an organization's assets.

Approval Process

The ***approval process*** is a crucial business procedure that dictates how changes impacting security are approved and who holds the authority to make such decisions. The approval process typically follows a step-by-step verification process to ensure that all necessary precautions are considered and the planned change will not introduce new vulnerabilities.

Ownership

In the context of security, ***ownership*** refers to the individual or team that is responsible for specific assets, such as databases or applications, and that is accountable for their security. Owners are typically responsible for defining an asset's security requirements, managing its risk profile, and addressing any vulnerabilities in the system. A crucial component of recognizing ownership is establishing accountability. Ownership ensures that each asset is consistently maintained, protected, and updated according to the security requirements of a specific system.

Stakeholders

Stakeholders are individuals or groups vested in an organization's security posture who can directly impact security procedures and policies. Stakeholders may include system users, IT staff, management, customers, investors, or any entity that would be affected by a security breach or whose actions could impact the security posture of an organization. Involving stakeholders in security decision-making processes can lead to more comprehensive security solutions, as diverse perspectives help in identifying potential threats and vulnerabilities. Remember that stakeholders can be internal or external to specific internal business departments or external to the business.

Impact Analysis

Impact analysis is a process that involves assessing the potential effects of changes on the organization's security landscape. You may encounter impact analysis in the form of a business impact analysis (BIA), which we will explore in depth in Chapter 24, "Understanding Elements of the Risk Management Process." An impact analysis also helps in proactively identifying possible security risks or issues to a system. Security analysts should conduct an impact analysis to better understand how to effectively allocate resources such as staff, budget, and tools.

Test Results

A ***test result*** is an outcome of a specific test, such as a penetration test, vulnerability assessment, or simulated attack. The test results of newly implemented security measures play a crucial role in determining the effectiveness of those measures and any adjustments needed.

Test results offer insights into the strengths and weaknesses of a system's security, informing decisions about necessary improvements or adjustments. Essentially, they serve as a report card for the organization's cybersecurity measures. It's crucial to note what type of test result you are reviewing and how the results were generated. A test result from a vulnerability scanner will show detailed technical insights specific to each system and will generally lack bias. A human-generated test result, such as a result in a cybersecurity risk assessment, might have subjective content and require additional context to be understood.

Backout Plan

Every change in an IT system or process needs a ***backout plan***—a meticulously outlined procedure designed to revert any changes that negatively impact security or business operations. A backout plan is more than just a rollback strategy; it's a critical IT service management framework component. A backout plan adheres to a predefined action list and should be created before any software or system upgrade, installation, integration, or transformation occurs. This plan typically includes detailed steps and techniques for uninstalling a new system and reversing process changes to a pre-change working state. The objective is to ensure that automated system business operations continue smoothly, especially if post-implementation testing reveals that the new system fails to meet expectations. As a best practice, you should avoid making changes during peak business hours and always have a comprehensive backout plan.

Maintenance Window

A ***maintenance window*** is a designated time frame for performing system updates or changes that is strategically chosen to minimize disruptions. We used to say, "Maintenance on a Friday is guaranteed work on a Saturday." Choose your maintenance windows carefully to balance impacts on the business and plan for any unexpected operational impacts that result from your maintenance.

You might find that in a software as a service (SaaS) company, you need to do maintenance on the company's virtual private network (VPN). Engineers may use the VPN for secure remote access and use it frequently throughout the day to connect to development systems, but the usage levels may drop drastically after 6:00 p.m. You would therefore want to plan your maintenance window from 7:00 p.m. to minimize outages to any critical work happening at the company.

Standard Operating Procedure

A ***standard operating procedure (SOP)*** is a step-by-step instruction set to help workers carry out complex routine operations. SOPs are crucial for maintaining consistency, enhancing security, and ensuring that all team members follow best practices in daily operations. SOPs should be vetted all the way through the senior leadership team to ensure executive support for planned activities.

Key Topic

Technical Implications

Technical implications refer to the potential consequences or effects of a technology-related decision or event in the cybersecurity landscape. Technical implications could involve alterations to network infrastructure, modifications to security protocols, or the need for additional server capacity following the implementation of new software or systems. It is important to ensure that you understand all technical implications of any new or existing system to ensure that you can maintain functionality and security for that system.

Allow Lists

Key Topic

Allow lists, or whitelists, are lists of approved inputs a user or machine can enter on a system. Using an allow list is an easy and safe way to ensure well-defined inputs such as numbers, dates, or postal codes because it allows you to clearly specify permitted values and reject everything else. With HTML5 form validation, you get predefined allow list logic in the built-in data type definitions, so if you indicate that a field contains an email address, you have ready email validation. If only a handful of values are expected, you can use regular expressions to explicitly include them on an allow list.

Using an allow list gets tricky with free-form text fields, where you need some way to allow the vast majority of available characters, potentially in many different alphabets. Unicode character categories can be useful for allowing, for example, only letters and numbers in a variety of international scripts. You should also apply normalization to ensure that all input uses the same encoding, and no invalid characters are present. An allow list needs to be continuously updated as the company works with new applications and removes old ones, and a lot of resource time is required to maintain it. We will explore allow lists in greater detail in Chapter 9, "Understanding the Purpose of Mitigation Techniques Used to Secure the Enterprise."

Block Lists/Deny Lists

Key Topic

In the context of input validation, a ***deny list*** is a list of specific elements, characters, or patterns that are disallowed from being entered into a system. When approaching input validation from a security perspective, you might be tempted to implement it by simply disallowing elements that might be used in an injection attack. For example, you might try to ban apostrophes and semicolons to prevent SQL injection (SQLi), parentheses to stop malicious users from inserting a JavaScript function, or angle brackets to eliminate the risk of someone entering HTML tags. Limiting or blocking specific inputs is called block listing or deny listing, and it's usually a bad idea because a developer can't possibly know or anticipate all possible inputs and attack vectors. Blocklist-based validation is hard to implement and maintain and very easy for an attacker to bypass.

Let's say you want to use deny lists despite their issues. These lists are an additional maintenance point, and you need to understand that these lists can potentially break things, and your upper layer programming should not depend on deny lists to stop attacks.

Restricted Activities

Restricted activities are specific actions or operations within a computer or network system that are limited or prohibited to maintain cybersecurity standards. These limitations are often defined through allow lists and deny lists, which, as you've just seen, explicitly outline what is permitted and what is not. For example, restricted activities may include accessing specific system components or downloading unapproved software.

Clearly defined restricted activities are crucial for upholding secure environments and effectively communicating IT systems' acceptable use to internal and external stakeholders. These restrictions are commonly introduced during the employee onboarding process through key documentation like acceptable use policies (AUPs). In change management, access to critical areas like the production environment and change management software is typically restricted to authorized personnel only to ensure that only qualified individuals can make or approve changes, reducing the risk of unauthorized or harmful modifications.

Downtime

Downtime is time during which a system, network, or software application is unavailable to end users or completely offline. Downtime can be scheduled, such as during maintenance windows, as discussed earlier, or it can be unplanned, sometimes due to technical problems or even cyberattacks. Acceptable downtime might be for critical system patching or planned upgrades. A common standard of availability is 99.999%, commonly referred to as "five 9s" availability. "Two 9s" would be a system that guarantees 99% availability in a one-year period, allowing up to 1% downtime, or 3.65 days of unavailability. You might find that if you leverage third-party services, you need to ensure that their systems match, or exceed, your published service-level agreements (SLAs). You may need to implement a change if there is a misalignment between the SLA you have with your clients and what any third-party services provide to you. Unplanned downtime can disrupt business operations, negatively impact employee productivity, and potentially result in data loss. IT professionals are often focused on reducing downtime, which is crucial in cybersecurity and IT management. It's essential to have strategies to address issues when they happen and minimize the duration and impact of unplanned downtime.

Planned downtime is needed to conduct IT maintenance activities, software installation or upgrades, and other activities requiring non-active systems. You might need to upgrade a firewall on the network, which would require turning off the current system. To prevent making the network and end users vulnerable, you would schedule downtime, typically in off-hours/non-peak time, to replace the network device.

Service Restart

In your role as an IT or security professional, one task you'll likely encounter is a ***service restart***, which involves halting and then reactivating a system service to implement updates, patches, or configuration changes. This process is similar to turning off a car that's encountering a minor glitch and then restarting it.

The key aspect to note here is to understand the potential implications of a service restart, such as a momentary disruption of service. You need to ensure that potential users of the system are aware of any time impacts. You also need to thoroughly map the connections the service might have with other systems. You don't want to restart a service connected to a critical database that could make the organization or its data vulnerable to attackers. To minimize disruption to users, it is crucial to ensure that this action occurs during a predetermined maintenance window.

Application Restart

Software application restarts are sometimes necessary procedures. An ***application restart*** is like a service restart, but it is concentrated on a specific software application. An example you're no doubt familiar with is an app on your phone freezing and needing to be restarted to function correctly again.

Application restarts are common in IT and cybersecurity. You may often need to restart applications or systems to load patches and enforce updates. Again, communication and coordination with the stakeholders of the application are key.

Legacy Applications

In the course of your career, you will likely encounter older systems still running on a network for a variety of reasons. Handling ***legacy applications***, which are older software programs still serving a critical function in an organization, is a typical duty you might face.

Legacy applications allow you to leverage uncommon technology, and they can be fun, especially if the original engineers are still working on the system. However, dealing with legacy applications often requires understanding older technologies and the specific nuances associated with them, which can be especially challenging if the original engineers have moved on. It is important to understand any connection the legacy application requires to function. You might find limitations in the types of operating systems the organization must maintain if the legacy application requires a certain OS to run properly.

Dependencies

When working with software components, grasping dependencies is crucial. ***Dependencies*** refer to the relationships where one software component or service relies on another to function correctly. Think of the roof on a house. The roof may be supported by large beams of wood or stone columns. If you were to remove any of the beams or columns, you would jeopardize the integrity of the roof. Understanding dependencies is critical when troubleshooting issues, managing updates, and implementing changes in the IT environment.

Services, newer applications, and legacy applications are all likely to have critical dependencies that you need to understand before you do any maintenance on them.

Key Topic

Documentation

An essential part of any IT or cybersecurity professional's role is the creation and maintenance of documentation. ***Documentation*** is written material that provides information about a system or process. It might include user guides, technical specifications, or system descriptions. Documentation may also be written for specific products (for example, product documentation, user guides) or for specific processes (for example, installation instructions, uninstallation guides, patching processes). Documentation can also include policies, procedures, standards, and guidelines. Many organizations have their own security policies that cover critical security topics such as change management and change control policies, information security policies, acceptable use policies (AUPs), and business continuity planning (BCP)/ disaster recovery policies (DRPs).

Good documentation ensures a clear understanding of system operations, making it easier to train new staff and troubleshoot issues. It is often a good idea to begin with documentation when trying to ascertain any dependencies software or a system may require for operations and to map any dependencies.

Updating Diagrams

In the ever-evolving landscape of your IT environment, the process of updating diagrams plays a vital role. ***Updating diagrams*** is the process of editing current diagrams of systems or networks and inserting any changes that have occurred since the diagrams were originally created. As a best practice, you should ensure strong version control and put a version control number on every diagram. Diagrams can be visualized as maps or blueprints of your network or flowcharts of a process.

Updating diagrams ensures that everyone has an accurate and current picture of the systems. This clarity can significantly enhance troubleshooting and system upgrades. A good configuration management process helps to prevent small or large changes from going undocumented. Undocumented changes can lead to poor performance, inconsistencies, or noncompliance and can negatively impact business operations and security. Poorly documented changes add to instability and downtime. Having good network diagrams and well-written and up-to-date documentation is crucial and allows you to not only troubleshoot problems but also respond quickly to security incidents.

Updating Policies/Procedures

One crucial responsibility you will shoulder is updating policies and procedures. In the cybersecurity landscape, ***policies*** are the rules governing how IT systems are used and secured, whereas ***procedures*** are the specific steps required to implement these rules. It's worth noting that policies and procedures are directive controls and help communicate expectations to an organization. You must continuously revise policies and procedures to align with technological advancements, environmental shifts, or system modifications. Doing so ensures smooth, efficient, and secure operation of your IT infrastructure.

You should generally pay special attention to legacy applications that require unique user instructions. For instance, a legacy terminal application that is used to manage network interfaces could inadvertently expose privileged access if a policy changes but the corresponding procedures are not updated.

Key Topic

Version Control

Understanding and effectively implementing version control is vital in IT and cybersecurity domains and extends into areas like documentation. ***Version control*** is a system that records changes to a file or set of files over time so that you can recall specific versions later. It allows you to track modifications, pinpoint when and by whom changes were made, and, if necessary, revert to an earlier version.

For example, in modern IT environments, code is often checked into a version control repository like GitLab or GitHub. Each change is integrated and tested with the rest of the software system. Organizations that lack proper version control face challenges in tracking bug fixes and security patches. Similarly, vendors and software providers that lack appropriate version control make it difficult for consumers to correlate, triage, and patch security vulnerabilities. Proper version control is a best practice and a necessity for maintaining a secure and efficient operational environment.

Failure to maintain version control can lead to confusion and potential problems. Consider, for instance, a potential issue when a team member says, "Aren't we on version 2.3?" only to discover that the system was updated to version 4.0 weeks ago. Effective version control not only aids in managing changes and troubleshooting issues in a collaborative environment but also plays a crucial role in communicating updates to policies and procedures throughout an organization. It's an essential component of any well-run organization.

Chapter Review Activities

Use the features in this section to study and review the topics in this chapter.

Review Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-2 lists these key topics and the page number on which each is found.

Key Topic

Table 3-2 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Section	Business Processes Impacting Security Operations	41
Section	Technical Implications	43
Paragraph	Allow lists	44
Paragraph	Deny list	44
Section	Documentation	47
Section	Version Control	48

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

business process, approval process, ownership, stakeholder, impact analysis, test result, backout plan, maintenance window, standard operating procedure (SOP), technical implications, allow list, deny list, restricted activity, downtime, service restart, application restart, legacy application, dependency, documentation, updating diagrams, policy, procedure, version control

Review Questions

Answer the following review questions. Check your answers with the answer key in Appendix A.

1. What is the primary purpose of patch management in an organization's security operations?
2. What is the role of business processes in security operations?

3. What is the significance of an approval process in an organization's security posture?
4. How does ownership of assets influence security operations in an organization?
5. Define the term *technical implications* in the context of cybersecurity.
6. What is an allow list, and what role does it play in system security?
7. What is the downside of relying solely on a block list, or deny list, for input validation?
8. What are restricted activities in the context of cybersecurity?
9. What is the importance of documentation in IT and cybersecurity operations?
10. Why is version control essential in IT and cybersecurity domains?

This page intentionally left blank

Index

Numbers

2FA (two-factor authentication), 22
5 Whys technique, 501–502
802.1X, 236, 237–238, 239

A

AAA (authentication, authorization, and accounting), 21–22
ABAC (attribute-based access control), 451, 454, 538
access control, 175, 450
  allow list, 321–322
  attribute-based, 454, 538
  centralized, 201–202
  decentralized, 202
  discretionary, 452–454, 538
  least privilege, 456
  list, 175–176
  mandatory, 451–452, 538
  mobile device, 318
  network, 430
  permissions, 176
    Linux, 177
    Windows, 176–177
  policy-driven, 22
  role-based, 450
  rule-based, 450–451
  standards, 538
  time-of-day restrictions, 455–456
  vestibule, 26–27
access point, rogue, 160
account lockout, 166, 455
accounting, 21
acknowledgment, 607–608
ACL (access control list), 175–176, 241, 415–416
acquisition, 503–505. *See also* procurement
active device, 229
Active Directory, 443
active reconnaissance, 628
ad hoc risk assessment, 562
adaptive identity, 23
AES (Advanced Encryption Standard), 62
AES-GCM (Advanced Encryption Standard in Galois/Counter Mode), 258
agent
  -based solution, 397
  -based web filter, 421
agentless
  security, 112
  solution, 397
agreement types, 593–594. *See also* SLA (service-level agreement)
air-gapping, 198
ALE (annualized loss expectancy, 566–567
alert/ing, 388–389, 392
  response process
  tuning, 392
algorithm, 65–66
  cypher suite, 65
  digital signature, 76–77
  hashing, 75, 163–164, 258
  key length, 66–67

allow list, 44, 178–179, 321–322
amplified DDoS attack, 160
analysis
  incident, 495
  risk, 563–564
  risk impact, 578
  root cause, 501–502
  scenario, 568
  sensitivity, 569
  supply chain, 591–592
  vulnerability, 367
analytics, user behavior, 431–432
anomalous behavior recognition, 635
  risky behavior, 635–636
  unexpected behavior, 636
  unintentional behavior, 637
antenna
  beamforming, 315
  omnidirectional, 315
anti-malware, 155
anti-ram bollard, 25
antivirus software, 400
Apache Mesos, 206
APEC (Asia-Pacific Economic Cooperation) Privacy Framework, 611
API (application programming interface), 156, 197, 479
application/s. *See also* container/ization
  allow list, 178–179, 321–322
  attack, 162
  buffer overflow, 162
  legacy, 46
  -level gateway, 242, 417
  log, 513–514
  monitoring, 384
  restart, 46
  scanning, 132
  security, 336, 362
    dynamic analysis, 363
    package analysis, 363–364
    static analysis, 362–363
  unsupported, 112–113
  vulnerability
    buffer overflow, 131–132
    malicious update, 132–133
    memory injection, 130–131
    race condition, 132
approval process, 41
APT (advanced persistent threat), 98–99, 101
apt-get install snmp snmpwalk command, 403
architecture
  centralized, 201–202
  cloud/cloud computing
    hybrid, 194–195
    on-premises, 201
  cost, 216
  decentralized, 202
  ease of deployment, 216–217
  ease of recovery, 217
  IoT (Internet of Things), 209–210
  patch availability, 217–218
  resilience, 215–216
  responsiveness, 216
  risk transference, 217
  SCADA (supervisory control and data acquisition), 210–213
  scalability, 216
  serverless, 196–198
archiving, 391
ARO (annualized rate of occurrence), 565–567
ASLR (Address Space Layout Randomization), 130
assessment
  audit, 623
  risk, 562
    ad hoc, 562
    continuous, 562–563
    one-time, 562
    qualitative, 565
    quantitative, 565–567
    recurring, 562

self-, 622
  vendor, 590–591
asset. *See also* hardware; inventory assessment; software
  classification, 350
  destruction, 352–353
  disposal/decommissioning, 351–352, 353
  enumeration, 351
  management
    assignment and accounting process, 350
    procurement process, 348–349
  ownership, 41, 350
  tagging, 309
  tracking, 350–351
assignment and accounting process, 350
asymmetric encryption, 62–64
attack. *See also* malware; threat; vulnerability/ies
  application, 162
  cryptographic, 163
    birthday, 164
    collision, 163–164
    downgrade, 163
  Evil Maid, 157–158
  forgery, 163
  injection, 162
  memory injection, 130
  mobile device, 319–320
  network
    DDoS (distributed denial-of-service), 160
    DNS, 160
    wireless, 160–161
  password, 164–165
    brute-force, 165
    spraying, 165
  on-path, 161
  phishing, 109, 117–118
  physical, 158–159
  ransomware, 152–153
  replay, 162
  smishing, 109, 121
  spoofing, 161
  surface, 227
  vishing, 120–121
  watering hole, 122–123
  whaling, 117–118
attestation, 449, 607, 620
audio, steganography, 71
audit, 545
  assessment, 623
  attestation, 620
  code, 131
  committee, 621–622
  evidence of internal, 590
  external, 622–623
  independent third-party, 623
  internal, 621–622
  regulatory, 622–623
  right-to-, 589–590
  system/process, 367
  trail, 310
  vulnerability, 376
AUP (acceptable use policy), 533, 638
authentication, 21–22. *See also* password
  biometric, 457
  context-aware, 323
  digital signature, 76–77
  key, 457–458
  multifactor, 22, 139, 323, 456–457, 639
    something you are, 460
    something you have, 459–460
    something you know, 459
    somewhere you are, 460–461
  OAUTH, 444–445
  passwordless, 465
  protocols, 335–336
  RADIUS (Remote Authentication Dial-In User Service) federation, 332–334

remote
CHAP (Challenge-Handshake Authentication Protocol), 252–253
RAS (Remote Access Service), 251
TACACS (Terminal Access Controller Access Control System), 253
security key, 458
single-factor, 22
token-based, 458
two-factor, 22
VPN, 249–250
WPA3 (Wi-Fi Protected Access 3), 331–332, 334–335
authorization, 21
challenge/response, 109–110
model, 22
automation
benefits
efficiency/time saving, 480
employee retention, 481
enforcing baselines, 480–481
reaction time, 482
scaling in a secure manner, 481
standard infrastructure configuration, 481
workforce multiplier, 482
CI/CT (continuous integration/ continuous testing), 478–479
complexity, 482
cost, 483
facility, 209
firewall, 413–414
guard rails, 477
reporting, 522–523
resource provisioning, 477
security group, 477
single point of failure, 483
supportability, 484
technical debt, 483–484
ticket creation and escalation, 477–478
user provisioning, 474–476
availability, 19–20, 215
on the cloud, 140
five 9s, 45, 214–215
high, 214–215
AWS (Amazon Web Services) Lambda, 196–197

B

backout plan, 42–43
backup, 299–301
barricade, 25–26
BCP (business continuity plan), 495
beamforming, 315
BEC (business email compromise), 122
behavior
risky, 635–636
unexpected, 636
unintentional, 637
BER (Basic Encoding Rules), 87
BIA (business impact analysis), 42, 570
biometric identifier, 457
birthday attack, 164
bloatware, 155
block cypher, 66
block rule, 422
blockchain, 78
block/deny list, 44, 322
blocked content, 166
Bluejacking, 328
Bluesnaring, 328
Bluetooth, 113, 327–328
board, 546
bollard, 24–25
BPA (business partners agreement), 588
brand impersonation, 123
brute-force attack, 159, 165
buffer overflow, 131–132, 162
bug bounty program, 367
business continuity policy, 535
business process, 41
approval process, 41
backout plan, 42–43

impact analysis, 42
maintenance window, 43
ownership, 41
SOP (standard operating procedure), 43
stakeholders, 42
technical implications, 43
test result, 42
BYOD (bring your own device), 318–319, 326–327

C

CA (certificate authority), 78–81
architecture, 71
chain of trust, 88
installation, 88
root of trust, 89
third-party, 89
caching proxy, 231
capacity planning, 295
CCPA (California Consumer Privacy Act), 610
CCTV (closed-circuit television), 28
cellular connection, 329
centralized proxy, 421–422
centralized system, 201–202, 548
CER (Canonical Encoding Rules), 87
certificate, 78–79
attributes, 82–83
authority, 78–81
chain, 86
formats and extensions, 87–88
mapping, 81
pinning, 88
revocation list, 81
root of trust, 89
self-signed, 83–86
third-party, 89
wildcard, 90
certification, disposal/d ecommissioning, 353
chain of custody, 503
chain of trust, 88
challenge/response, 109–110
change management, 37. *See also* business process
policy, 536
procedures, 541
CHAP (Challenge-Handshake Authentication Protocol), 252–253
chgrp command, 177
chmod command, 177, 439
chown command, 177
CIA (confidentiality, integrity, and availability) triad, 19–20
CI/CT (continuous integration/ continuous testing), 478–479
circuit-level gateway, 242, 417
CISO (chief information security officer), 483
classification
asset, 350
data, 275–276
vulnerability, 370–371
clean desk policy, 640
CLI (command-line interface), 199
client-based security, 112
cloud/cloud computing, 185, 193
community, 138
confidentiality, 138–139
data protection, 139–140
HA (high availability), 291
clustering, 292
load balancing, 291–292
hardening techniques, 312
hybrid, 138, 194–195
IaaS (infrastructure as a service), 136, 194
IaC (infrastructure as code), 195–196
MaaS (monitoring as a service), 137
PaaS (platform as a service), 137
on-premises, 201
private, 137
public, 137
responsibility matrix, 193–194
SaaS (software as a service), 136

SECaaS (security as a service), 137
serverless architecture, 196–198
service provider, 193–194
third-party vendor, 195
vulnerabilities, 136–141
clustering, 292
code
auditing, 131
infrastructure as, 195–196
malicious, 161–162
signing, 339
cold site, 293
collision attack, 163–164
command
docker images, 203–204
docker ps, 204
docker search, 205
Linux
apt-get install snmp snmpwalk, 403
chgrp, 177
chmod, 177, 439
chown, 177
netstat, 114
committee, 547, 621–622
community cloud, 138
compensating control, 9–10, 11, 375
compiler tools, 131
acknowledgment, 607–608
attestation, 607, 620
audit, 621
automation, 608–609
monitoring, 605
due diligence/due care, 605–607
external, 608
internal, 608
non-, consequences, 603
contractual impacts, 605
fines, 603–604
loss of license, 604–605
reputational damage, 604
sanctions, 604
report/ing, 602–603
external, 603
internal, 603
SOC 2 (Service Organization Control 2), 607
compute resources, 218
concurrent session usage, 166
confidential data, 275
confidentiality, 19, 138–139
configuration
enforcement, 182–183
fail-open, 228
confirmation, 368
conflict of interest, 592
connection/connectivity, 228
Bluetooth, 327–328
cellular, 329
dial-up, 253
multihomed, 245
SATCOM (satellite communication), 329
conservative risk appetite, 575
container/ization, 202. *See also* Docker
Docker, 202, 203, 481
image, 203
Kubernetes, 205–206
registry, 202
containment, 496
content categorization, 422
content management, mobile device, 320–322
context-aware authentication, 323
continuous monitoring and adjustment, 568
continuity planning, 295
continuous risk assessment, 562–563
control plane, 22–23
controller, 550–551, 611
control/s
compensating, 9–10, 11, 375
corrective, 9, 11
detective, 9, 11
deterrent, 8

directive, 10, 11
 effective, 266
 managerial, 6, 7
 operational, 6, 7
 physical, 7
 preventive, 8
 technical, 7
COOP (continuity of operations planning), 294–295
COPE (corporate-owned, personally enables), 325, 326–327
corrective controls, 9, 11
cost, 216, 483
credential/s
 default, 115–116, 185
 ephemeral, 466
 replay, 161
CRL (certificate revocation list), 81
cryptography/cryptographic. *See also* encryption
 attack, 163
  birthday, 164
  collision, 163–164
  downgrade, 163
 block cypher, 66
 digital signature, 76–77
 HSM (hardware security module), 68
 key exchange, 64–65
 KMS (key management system), 58, 68–69
 PKI (public key infrastructure), 58
  private key, 58
  public key, 58
 protocols, 334–335
 salting, 76
 stream cypher, 65–66
 TPM (Trusted Platform Module), 67–68
 vulnerability, 142
cryptoviral extortion, 152
CSA (Cloud Security Alliance), 137
CSR (certificate signing request), 89–90
custodian/steward, 552–553
CVE (common vulnerabilities and exposures), 86, 328, 370
CVSS (Common Vulnerability Scoring System), 368. *See also* vulnerability/ies
 base score, 369
 core groups, 368–369
 practical utility, 370
CWE (Common Weaknesses Enumeration), 394
CWSS (Common Weaknesses Scoring System), 394
cyber warfare, 101
cyberattack, 101
cybercriminal, 98
cybersecurity
 activity, 386
  alert response and remediation/validation, 392
  alerting, 388–389
  archiving, 391
  log aggregation, 386–388
  reporting, 390–391
  scanning, 389–390
 insurance, 6, 374
 situational awareness, 638–639
 tool, 392–393
  agents/agentless, 397
  NetFlow, 399–400
  SCAP (Security Content Automation Protocol), 393–395
  SIEM (security information and event management), 397–399
  vulnerability scanner, 403–405
CYOD (choose your own device), 325, 326–327
cypher
 block, 66
 stream, 65–66
 suite, 65

D

DAC (discretionary access control), 452–454, 538
dark web, 141, 365
dashboard, 522–524
DAST (dynamic application security testing), 360, 363
data
  availability, 140
  classification, 275–276
  confidential, 275
  -driven decision making, 568
  erasure, 613
  human- and non-human-readable, 275
  integrity, 19
  inventory, 612
  leakage, 207
  log, 512
  masking, 74, 281
  in motion, 61
  ownership, 612
  private, 276
  in processing, 61
  processor, 612
  protection, 139–140
  protection officer, 551
  regulated, 274
  at rest, 61, 277
  restricted, 276
  retention, 353, 612–613
  salt, 77–78
  sanitization, 352
  securing
    encryption, 279
    geographic restrictions, 279
    hashing, 279–280
    permission restrictions, 282–283
  sensitive, 275
  sources, 521
  sovereignty, 278
  states, 276–277
  subject, 611
  tokenization, 72–74, 281
  in transit, 277–278
  in use, 278
database
  blockchain, 78
  encryption, 60
  OVS (Open vSwitch), 200
DCS (distributed control system), 212–213
DDoS (distributed denial-of-service) attack, 160
decentralized system, 202, 548–549
deception technology
  honeyfile, 32
  honeypot, 31–32
  honeytoken, 32
  spam honeypot, 31
decision making
  data driven, 568
  framework, 569
decommissioning, 183
  asset, 351–352
  certification, 353
deep web, 365
default credentials, 115–116, 185, 209–210
defensive penetration testing, 626
delegation of access, 444
deny list, 44, 322
DEP (Data Execution Prevention), 130
dependency, 46–47
deployment, 310
DER (Distinguished Encoding Rules), 87
descriptive metadata, 519
destruction, hardware, 352–353
detection phase, incident response, 495
detective controls, 9, 11
deterrent controls, 8
  CI/CT (continuous integration/ continuous testing), 478–479

code signing, 339
security awareness program, 642
static code analysis, 338–339
training, 131
device. *See also* network/s, appliance
attribute, 229
active vs. passive, 229
inline vs. tap/monitor, 229–230
bring your own, 318–319
choose your own, 325
isolation, 179–180
placement, 226
smart, 209
diagram, updating, 47
dial-up, 253
digital certificate, 64
digital forensics, 502–503
acquisition, 503–505
chain of custody, 503
e-discovery, 506
legal hold, 503
preservation, 505
reporting, 505
digital signature, 20, 76–77
directive controls, 10, 11
directory traversal, 163
disaster recovery, 292
MTTR (mean time to repair), 579
policy, 535
RPO (recovery point objective), 579
RTO (recovery time objective), 579
disinformation, 121
disposal, asset, 351–352
DKIM (DomainKeys Identified Mail), 428
DLP (data loss prevention), 401, 429–430
DLT (distributed ledge technology), 78
DMARC (Domain-Based Message Authentication Reporting and Conformance), 427–428
DNS (Domain Name System)
attack, 160
filtering, 427
Docker, 202, 203, 481
docker images command, 203–204
docker ps command, 204
docker search command, 205
Docker Swarm, 206
documentation, 47, 310
reporting, 505
version control, 48
DoS (denial-of-service) attack, 161
downgrade attack, 163
downtime, 45
DPO (data protection officer), 551, 611
due diligence/due care, 592, 605–607

E

ease of deployment, 216–217
ease of recovery, 217
Easter egg, 157
e-discovery, 506
EDR (endpoint detection and response), 430
EF (exposure factor), 371–372, 570–571
email
-based threat, 109, 122
gateway, 429
phishing, 117–118
security, 427
DKIM (DomainKeys Identified Mail), 428
DMARC (Domain-Based Message Authentication Reporting and Conformance), 427–428
SPF (Sender Policy Framework), 428
spam, 109, 110
embedded system, 214, 313
encryption, 59, 139, 181–182, 183–184, 279
algorithm
cypher suite, 65

hashing, 75, 163–164
key length, 66–67
asymmetric, 62–64
block cypher, 66
cracking, 161
database, 60
file, 60
full-disk, 59
HSM (hardware security module), 68
level, 59
mobile device, 320–321, 322
obfuscation, 70
partition, 59–60
record-level, 60–61
at rest, 61
secure enclave, 69
standards, 539–541
strength, 66
symmetric, 61–62
volume, 60
endpoint
log, 515
protection, 184
environmental
threat, 159
variable, 372
EOL (end-of-life), 112, 134–135
ephemeral credentials, 466
EU (European Union), GDPR (General Data Protection Regulation), 610
Event Viewer, 515–517
evidence
acquisition, 503–505
e-discovery, 506
of internal audits, 590
preservation, 505
Evil Maid Attack, 157–158
examination, 623
expansionary risk appetite, 574–575
exploit
privilege escalation, 162
SSO (single sign-on), 441
external audit, 622–623
external compliance
monitoring, 608
reporting, 603

F

facility automation, 209
failover
redundancy, 581
testing, 297–298
failure mode, 228
false negative, 385
federation, 441–443
fencing, 27–28
file
-based threat, 111
encryption, 60
integrity monitoring, 429
stego-, 71
filter, phishing, 116
final preparation
hands-on activities, 647
suggested plan for final review and study, 647–648
financial information, 274–275
financial planning, 568
firewall, 115, 239–240, 413
ACL (access control list), 241, 415–416
application-level gateway, 242
automation, 413–414
circuit-level gateway, 242
“in front of”/”behind”, 243
hardware-based, 247–248
host-based, 184
Layer 4/Layer 7, 248–249
logging, 243, 513
NAT gateway, 242
next-generation, 235, 246–247
packet filtering, 241, 416
placement, 417
rules, 413, 414–415
web application, 243–245

firmware, vulnerability, 134
five nines, 214–215
forgery attack, 163
format, certificate, 87–88
forward proxy, 232
full-disk encryption, 59
funding, threat actor, 100

G

gap analysis, 22
gateway
  application-level, 242, 417
  circuit-level, 242, 417
  email, 429
  NAT, 242, 417
GDPR (General Data Protection Regulation), 610
generator, 301
geographically distant site, 293
geolocation, 278–279, 455
geotagging, 455
global considerations, governance, 545
governance. *See also* compliance
  board, 546
  centralized, 548
  committee, 547
  controller, 550–551
  custodian/steward, 552–553
  decentralized, 548–549
  external considerations, 543
  global considerations, 545
  government entities, 547–548
  guidelines, 532
  industry-specific considerations, 544
  legal considerations, 544
  local/regional considerations, 544–545
  monitoring and revision, 545–546
  national considerations, 545
  owner, 549–550
  policy, 208, 532–533
    acceptable use, 533
    business continuity, 535
    change management, 536
    disaster recovery, 535
    incident response, 535–536
    information security, 533–534
    SDLC (software development lifecycle), 536
  procedures, 541
    change management, 541
    onboarding and offboarding, 542
  processor, 551–552
  regulatory considerations, 543
  standards, 536–537
    access control, 538
    encryption, 539–541
    password, 537–538
    physical security, 539
GPS (Global Positioning System), 278, 322–323, 329
Group Policy, 423
guard rails, 477
GUI (graphical user interface), 199
guideline, 532

H

HA (high availability), 214–215, 291
  in cloud environments, 291
    clustering, 292
    load balancing, 291–292
hacktivist, 98
hardening techniques, 183, 311
  cloud infrastructure, 312
  default password change, 185
  disabling ports/protocols, 184–185
  embedded system, 313
  encryption, 183–184
  HIPS (host-based intrusion prevention system), 184
  host-based firewall, 184
  installation of endpoint protection, 184
  IoT (Internet of Things), 314
  mobile device, 311
  router, 312

RTOS (real-time operating system), 313–314
SCADA system, 313
server, 313
switch, 312
workstation, 311–312
hardware
-based firewall, 247–248
decommissioning, 183
destruction, 352–353
legacy, 135
provider, 141–142
vulnerabilities, 134
EOL (end-of-life), 134–135
firmware, 134
hash/ing, 75, 279–280
algorithm, 163–164, 258
birthday attack, 164
heat map, 317
honeyfile, 32
honeynet, 31
honeypot, 31–32
honeytoken, 32
host-based firewall, 184
host-based IPS, 184
HSM (hardware security module), 67, 68
HTTP, proxy, 231–232
HTTPS, 256
human- and non-human-readable information, 275
hybrid cloud, 138, 194–195
hybrid work, 640–641
hypervisor-based keylogger, 156

I

IaaS (infrastructure as a service), 136, 194
IAM (identity and access management)
interoperability, 448
SAML (Security Association Markup Language), 446–448
IAST (interactive application security testing), 360
ICS (industrial control systems), 211–213
identity/identification
attestation, 449
risk, 561–562
spoofing, 440–441
SSO (single sign-on), 441–443
IdP (identity provider), 441
IDS (intrusion detection system), 233–234, 418–419
logs, 517
signature, 419–421
trends, 419
IKE (Internet Key Exchange), 257
phase 1, 257–261
phase 2, 261–266
version 2, 264–265
IM (Instant Messaging)
-based threat, 110
spam, 110
image
-based threat, 111
container, 203
Docker, 203
steganography, 71–72
impact, 571
impersonation, 121–122, 123
Implicit Trust Zone, 24
impossible travel, 166
incident response
containment, 496
detection, 495
eradication, 496–497
handbook, 638
lessons learned, 497
lifecycle, 493–494
plan, 498
playbook, 495, 542–543
policy, 535–536
preparation, 494–495
process audit, 493
recovery, 497
tabletop exercise, 499–501

testing, 498
training, 497–498
independent assessment, 590–591
independent third-party audit, 623
indicator, 165
account lockout, 166
blocked content, 166
of compromise, 496
concurrent session usage, 166
impossible travel, 166
key risk, 572
missing logs, 167
out-of-cycle logging, 167
performance, 377
resource consumption, 166
resource inaccessibility, 166
industry/industrial, 544
impact, 372
SCADA (supervisory control and data acquisition), 211
-specific governance consideration, 544
information
confidentiality, 19
financial, 274–275
legal, 274
mis-/dis-, 121
security policy, 533–534, 638
infrared sensor, 31
infrastructure, 295
attack surface, 227
as code, 195–196
connectivity, 228
device attribute, 229
active vs. passive, 229
inline vs. tap/monitor, 229–230
device placement, 226
failure mode, 228
monitoring, 384–385
network, 197
air-gapped, 198
logical segmentation, 198–199
physical isolation, 198
SDN (software-defined networking), 199–201
security zones, 226–227
initial reporting, 641
inline monitoring, 229
input validation, 336–337
insider threat, 99, 639
installation
CA (certificate authority), 88
endpoint protection, 184
insurance, 374
integrated penetration testing, 626
integrity, 19
internal audit, 621–622
internal compliance
monitoring, 608
reporting, 603
interoperability, 448
inventory, 351
assessment, 309
data, 612
IoC (indicator of compromise), 496
IoT (Internet of Things), 208–209
facility automation, 209
hardening techniques, 314
sensors, 209
smart devices, 209
weak defaults, 209–210
wearables, 209
IP (intellectual property), 274
IP proxy, 230–231
IPS (intrusion prevention system), 233–234, 250–251, 418–419
host-based, 184
logs, 517
signature, 419–421
trends, 419
IPsec, 257
attributes, 262
IKEv1 phase 1, 257–261
IKEv1 phase 2, 261–266
passthrough, 261

IRP (incident response plan), 296
ISAC (information sharing and analysis center), 364–365
isolation, 179–180
IT, shadow, 99

J

jailbreaking, 143
JavaScript-based keylogger, 156
JIT (just-in-time) permissions, 465–466

K

Katacoda, 205
kernel-based keylogger, 156
key
  exchange, 64–65
  length, 66–67
  stretching, 77–78
keygen, 153–154
keylogger, 155–156
  API-based, 156
  hypervisor-based, 156
  JavaScript-based, 156
  kernel-based, 156
  memory-injection-based, 156
  web form-grabbing, 156
KMS (key management system), 58, 67–69. *See also* PKI(public key infrastructure)
known environment penetration testing, 626
KPI (key performance indicator), 377, 500
KRI (key risk indicator), 572
Kubernetes, 205–206

L

Layer 4 firewall, 248–249
Layer 7 firewall, 248–249
LDAP (Lightweight Directory Access Protocol), 443–444
Lean, 501–502
least privilege, 182, 456
legacy hardware, 135
legal hold, 503
legal information, 274
lessons learned, 497
levels of encryption, 59
lifecycle
  incident response, 493–494
  penetration testing, 624–625
lighting, 30
likelihood, 569–570
Linux
  apt-get install snmp snmpwalk command, 403
  chgrp command, 177
  chmod command, 177, 439
  chown command, 177
  permission assignment, 439
  permissions, 177
load balancing, 234–235, 291–292
local/regional considerations, governance, 544–545
logic bomb, 157
logical segmentation, 198–199
login
  account lockout, 166
  impossible travel time, 166, 455
logistics, SCADA (supervisory control and data acquisition), 212–213
log/s and logging
  aggregation, 386–388
  application, 513–514
  data, 512
  endpoint, 515
  false negative, 385
  firewall, 243, 513
  IDS/IPS, 517
  missing, 167
  network, 517–518
  OS-specific security, 515–517
  out-of-cycle, 167
  rsyslog, 387

SNMP (Simple Network Management Protocol), 385
syslog, 384–385, 386–387, 512–513
third-party tools, 385
LSB (least significant bit) substitution, 72

M

MaaS (monitoring as a service), 137
MAC (mandatory access control), 451–452, 538
maintenance, 310–311
maintenance window, 43
malicious code, 161–162
malicious update, 132–133
malware, 152
anti-, 155
bloatware, 155
indicators, 165
keylogger, 155–156
API-based, 156
hypervisor-based, 156
JavaScript-based, 156
kernel-based, 156
memory-injection-based, 156
web form-grabbing, 156
logic bomb, 157
ransomware, 152–153
spyware, 154
Trojan horse, 153–154
virus, 155
worm, 154
managerial controls, 6, 7
manufacturing, SCADA (supervisory control and data acquisition), 211–212
MBR (master boot record), 157–158
MD5 (Message Digest 5), 163–164
MDM (mobile device management), 318. *See also* mobile device
access control, 318
application and content management, 320–322
BYOD (bring your own device), 318–319
context-aware authentication, 323
encryption, 322
GPS tracking, 322–323
memory injection, 130–131, 156
message-based threat, 109
email, 109
IM (Instant Messaging), 110
smishing, 121
SMS (Short Message Service), 109–110
spam, 110
metadata, 518
cellphone, 519
descriptive, 519
preservation, 519
structural, 518
use, 519
Metasploit, 366
metric/s. *See also* risk
EF (exposure factor), 570–571
KPI (key performance indicator), 500
probability, 568
MFA (multifactor authentication), 22, 456–457, 639
mobile device, 323
something you are, 460
something you have, 459–460
something you know, 459
somewhere you are, 460–461
MIB (Management Information Base), 403
microservices, 197
microwave sensor, 31
minimum configuration standard, 310
misconfiguration, 142
misinformation, 121
mobile device
allow list, 321–322
attacks, 319–320
cellphone metadata, 519
connectivity, Bluetooth, 327–328

COPE (corporate-owned, personally enables), 325
deployment models, 325–326
encryption, 320–321, 322
GPS (Global Positioning System), 322–323, 329
hardening, 311
MFA (multifactor authentication), 323
screen lock, 323
secure implementation best practices, 330
security, 320
security concerns and countermeasures, 324–325
vulnerabilities, 142–143
jailbreaking, 143
side loading, 143
model
authorization, 22
monitoring, 115, 182, 340–341, 545–546
application, 384
asset, 350–351
inventory, 351
compliance, 605
due diligence/due care, 605–607
external, 608
internal, 608
computing resources, 383
continuous, 568
dark web, 365
file integrity, 429
infrastructure, 384–385
inline, 229
package, 363–364
recurring, 642
as a service, 137
systems, 383
vendor, 594
motivation, threat actor, 99–101
MSP (managed service provider), 116
MTBF (mean time between failures), 580–581
MTTR (mean time to repair), 579
multi-cloud system, 294
multifactor authentication, 139
multihomed connection, 245
MU-MIMO (multi-user multiple-input and multiple-output), 315

N

NAC (network access control), 430
NAT (Network Address Translation), 242, 417
nation-state actor, 99
NetFlow, 235, 399–400
netstat command, 114
network/s. *See also* infrastructure
appliance
jump server, 230
proxy server, 230–233
attack
DDoS (distributed denial-of-service), 160
DNS, 160
wireless, 160–161
infrastructure, 197
air-gapped, 198
logical segmentation, 198–199
physical isolation, 198
SDN (software-defined networking), 199–201
log, 517–518
P2P, 141
segmentation, 175, 197, 281–282, 374–375
unsecured, 113–114
virtual private. *See* VPN (virtual private network)
neutral risk appetite, 575
NGFW (next-generation firewall), 235, 245–247
Nimda, 154
NIST (National Institute of Standards and Technology)

incident response lifecycle, 493–494
SP 800–63B, 537–538
SP 800–83, 180
SP 800–123, 180
SP 800–145, 195
Nomad, 206
non-repudiation, 20

O

OAuth, 444–445
obfuscation, 70, 281
object, 451
OCSP (Online Certificate Status Protocol), 81–83, 88
ODL (OpenDaylight), 200
offboarding, 319
offensive penetration testing, 625–626
omnidirectional antenna, 315
onboarding and offboarding, 319, 542, 638
on-path attack, 161
one-time risk assessment, 562
open public ledger, 78
open service ports, 114–115
operating system
-based vulnerability, 133
security, 423. *See also* Linux; Windows
Group Policy, 423
SELinux, 423–424
operational controls, 6, 7
Orange Book, 452
OSINT (open-source intelligence), 364
OTP (one-time password), 109–110
out-of-cycle logging, 167
OVS (Open vSwitch), 200
OVSDB (OVS Database), 200
owner/ship, 41, 350
data, 612
governance, 549–550
risk, 572

P

P2P network, 141
PaaS (platform as a service), 137
package analysis, 363–364
packet
capture, 524–525
filtering, 241, 416
sniffing, 160
padding, 75
PAM (privileged access management), 465
parallel processing, 298–299
partially known environment penetration testing, 627
partition, 59–60
passive device, 229
passive reconnaissance, 627–628
password
age, 463
best practices, 461
brute-force attack, 165
complexity, 462–463
concepts, 461
defaul, 185
default, 115–116, 209–210
expiration, 463
-generation methods, 464
key stretching, 77–78
length, 462
management, 464–465, 639
mobile device, 320
one-time, 109–110
policy, 463
reuse, 463
spraying, 165
standards, 537–538
strong, 138
vaulting, 466
patch/ing, 115, 132, 180–182, 207, 374
availability, 217–218
inability to, 218

path traversal, 163
penetration testing, 366, 589, 623–624. *See also* vulnerability/ies
  defensive, 626
  integrated, 626
  known environment, 626
  lifecycle, 624–625
  offensive, 625–626
  partially known environment, 627
  physical, 625
  reconnaissance, 627–628
  unknown environment, 627
PEP (policy enforcement point), 24
performance, indicator, 377
permission/s, 176, 282–283
  automation, 477–478
  JIT (just-in-time), 465–466
  Linux, 177, 439
  risks of assigning, 440
  types, 439–440
  Windows, 176–177, 434–439
phishing, 109, 117–118, 634
  campaign, 634
  filter, 116
  Wi-Fi, 161
physical attack, brute-force, 159
physical controls, 7
physical isolation, 198
physical security
  access badge, 29
  access control vestibule, 26–27
  barricade, 25–26
  bollard, 24–25
  fencing, 27–28
  lighting, 30
  security guard, 28–29
  sensors, 30–31
  standards, 539
  video surveillance, 28
PIPEDA (Personal Information Protection and Electronic Documents Act), 610
PKI (public key infrastructure), 58, 258
  digital certificate, 64
  private key, 58
  public key, 58, 62–63
platform diversity, 294
playbook, 495, 542–543
point-to-multipoint network, 315–316
point-to-point network, 316
policy, 21. *See also* Group Policy
  acceptable use, 533, 638
  administrator, 23
  business continuity, 535
  BYOD (bring your own device), 318–319
  change management, 536
  clean desk, 640
  cybersecurity insurance, 374
  disaster recovery, 535
  -driven access control, 23, 139
  engine, 23
  governance, 208, 532–533
  guidelines, 10
  incident response, 535–536
  information security, 533–534, 638
  password, 463
  versus procedure, 48
  remote work, 638, 640–641
  SDLC (software development lifecycle), 536
  updating, 48
port/s, 425–426
  disabling, 184–185
  open, 114–115
  scanning, 114
  security, 235–236
    802.1X, 236, 237–238, 239
    EAP (Extensible Authentication Protocol), 236
  selection, 424–425

power
  consumption, 218
  management, 301
    generator, 301
    UPS (uninterruptible power supply), 301
PPTP (Point-to-Point Tunneling Protocol), 249
on-premises, 201
preparation, incident response, 494–495
preservation
  evidence, 505
  metadata, 519
pressure sensor, 31
pretexting, 122
preventive controls, 8
principle of least privilege, 182, 456
prioritization
  risk, 568
  vulnerability, 368
privacy, 609
  legal implications, 609–610
  national laws, 610
private cloud, 137
private data, 276
private key, 58
privilege escalation, 162
probability, 567
  data-driven decision making, 568
  versus likelihood, 569
procedures, 541
  change management, 541
  onboarding and offboarding, 542
  playbook, 542–543
process audit, 367
processor, 551–552, 612
procurement, 348
  review, 348–349
  TPRM (third-party risk management), 349
proprietary threat feed, 364
protocol, 416, 425–426
  authentication, 335–336
  cryptographic, 334–335
  disabling, 184–185
  selection, 424
  SSH (Secure Shell), 426
  TLS (Transport Layer Security), 426
proxy, 230–232
  centralized, 421–422
  forward, 232
  HTTP, 231–232
  reverse, 232, 256–257
public cloud, 137
public key, 58, 62–63

Q

qualitative risk assessment, 565
quantitative risk assessment, 565–567
quarantine, 392
questionnaire, 594–595

R

RA (registration authority), 80
race condition, 132
RADIUS (Remote Authentication Dial-In User Service) federation, 332–334
Rainbow Series, 452
RAS (Remote Access Service), 251
RBAC (role-based access control), 450
RC4, 62
reconnaissance, 627–628
record-level encryption, 60–61
recurring risk assessment, 562
reflected DDoS attack, 160
registry, container, 202
regulated data, 274
regulations, 543
regulatory compliance
  acknowledgment, 607–608
  attestation, 607, 620
  consequences of non-compliance

contractual impacts, 605
fines, 603–604
loss of license, 604–605
reputational damage, 604
sanctions, 604
monitoring, 605
external, 608
internal, 608
report/ing, 602–603
external, 603
internal, 603
SOC 2 (Service Organization Control 2), 607
remote access, 251. *See also* authentication
CHAP (Challenge-Handshake Authentication Protocol), 252–253
RAS (Remote Access Service), 251
TACACS (Terminal Access Controller Access Control System), 253
remote work policy, 638, 640–641
removable device threat, 111–112
replay attack, 162
report/ing, 390–391, 505
automated, 522–523
compliance, 602–603
external, 603
internal, 603
initial, 641
recurring, 641
risk, 577–578
SOC 2, 607
vulnerability, 377–378, 522
reputational damage, 604
reputation-based filtering, 422
rescanning, 376
resilience, 215–216
resource/s
allocation, 569
compute, 218
consumption, 166
exhaustion, 207
inaccessibility, 166
provisioning, 477
reuse, 135–136
threat actor, 100
responsibility matrix, 193–194
responsible disclosure program, 366–367
responsiveness, 216
restart, service, 45–46
restricted activity, 44–45
restricted data, 276
reverse proxy, 256–257
revision, 545
RFC (request for comments)
6749, 444
8446, 65
RFID cloning, 159
right
-to-audit clause, 589–590
to be forgotten, 613
risk. *See also* third-party risk assessment
acceptance, 576
analysis, 563–564
EF (exposure factor), 570–571
impact, 571
likelihood, 569–570
probability, 567–568
appetite, 574
conservative, 575
expansionary, 574–575
neutral, 575
assessment, 562
ad hoc, 562
continuous, 562–563
one-time, 562
qualitative, 565
quantitative, 565–567
recurring, 562
avoidance, 576
categorization, 569
EF (exposure factor), 371–372
environmental variables, 372
identification, 561–562
impact analysis, 578

management, third-party, 349
matrix, 495
mitigation, 574–576
owner, 572
permission assignment, 440
prioritization, 568
register, 572, 573–574
reporting, 577–578
threshold, 572
tolerance, 372–374, 574
compensating controls, 375
exceptions and exemptions, 375–376
insurance, 374
verification, 376
transfer, 576
transference, 217
risky behavior, 635–636
rogue access point, 160
rollback plan, 310
root cause analysis, 501–502
root of trust, 89
rootkit, 157–158
router
hardening techniques, 312
Onion, 365
RPO (recovery point objective), 579
rsyslog, 387
RTO (recovery time objective), 579
RTOS (real-time operating system), 213–214, 313–314
rule/s
ACL (access control list), 175, 241
-based access control, 450–451
block, 422
of engagement, 595
firewall, 413, 414–415
regulatory, 543

S

SaaS (software as a service), 136
safety bollard, 25
salting, 76
SAML (Security Association Markup Language), 441, 446–448
sandboxing, 339–340
sanitization, 352
SASE (secure access service edge), 265–266
SAST (static application security testing), 360, 362–363
SATCOM (satellite communication), 329
SCA (software composition analysis), 360, 361
SCADA (supervisory control and data acquisition), 210, 211–213
architecture, 210–211
hardening techniques, 313
security, 211
scalability, 216
scanning
application, 132
re-, 376
URL (universal resource locator), 422
vulnerability, 309, 360–362, 389–390, 403–405
SCAP (Security Content Automation Protocol), 393–395
scenario analysis, 568
screen lock, 323
screened subnet, 417–418
script/ing. *See also* automation
cross-site, 134
kiddie, 98
Tcl, 199
ticket system, 474
SDLC (software development lifecycle), 536
SDN (software-defined networking), 195, 199, 199–200
SDV (software-defined visibility), 201
SD-WAN (software-defined wide area network), 265

secure baseline
- deployment, 310
- documentation, 310
- inventory assessment, 309
- minimum configuration standard, 310
- ongoing maintenance, 310–311
- vulnerability scanning, 309

secure cookie, 337

secure enclave, 69

security. *See also* threat/threat actor
- AAA (authentication, authorization, and accounting), 21
- agentless, 112
- application, 336, 362
  - dynamic analysis, 363
  - package analysis, 363–364
  - static analysis, 362–363
- awareness program
  - development, 642
  - execution, 642–643
- baseline, 480–481
- benchmark, 395–397
- CIA (confidentiality, integrity, and availability) triad, 19–20
- client-based, 112
- email, 427
  - DKIM (DomainKeys Identified Mail), 428
  - DMARC (Domain-Based Message Authentication Reporting and Conformance), 427–428
  - gateway, 429
  - SPF (Sender Policy Framework), 428
- engineer, 413
- gap analysis, 22
- governance. *See* governance
- group, 477
- IDS (intrusion detection system), 233–234
- IPS (intrusion prevention system), 233–234
- key, 458
- mobile device, 320, 324–325. *See also* MDM (mobile device management); mobile device
- non-repudiation, 20
- operating system, 423
- operational, 640
- physical
  - access badge, 29
  - access control vestibule, 26–27
  - barricade, 25–26
  - bollard, 24–25
  - fencing, 27–28
  - lighting, 30
  - security guard, 28–29
  - sensors, 30–31
  - video surveillance, 28
- port, 235–236, 237–238, 239
- SCADA (supervisory control and data acquisition), 211
- supply chain, 116
- Wi-Fi, 328
- Zero Trust, 22–23
- zones, 226–227

segmentation, 175, 281–282, 374–375
- logical, 198–199
- micro, 197

self-assessment, 622

self-signed certificate, 83–86

SELinux, 423–424. *See also* Linux

sensitive data, 275

sensitivity analysis, 569

sensor, 31, 209, 235

server
- hardening techniques, 313
- load balancing, 234–235, 291–292
- proxy, 230–233
- web, 256–257

service restart, 45–46

SET (Social Engineering Toolkit), 118–120

SFA (single-factor authentication), 22

SHA (Secure Hash Algorithm), 163–164

shadow IT, 99
SID (security identifier), 176
side loading, 143
SIEM (security information and event management), 360, 385, 386, 397–399, 522–524
signal jammer, 317
signature, 419–421
simulation, 298, 499–501
single point of failure, 483
site
-to-site VPN, 250
  cold, 293
  geographically distant, 293
  hot, 293
  survey, 315, 316–317
  warm site, 293
situational awareness, 638–639
SLA (service-level agreement), 45, 588
SLE (single loss expectancy), 370–372, 565–567, 568–570
smart card, 29
smart device, 209
smishing, 109, 121
SMS (Short Message Service), 109–110
SNMP (Simple Network Management Protocol), 385
  trap, 401–402
  version 3, 402–403
SNMPWALK, 403
SOC 2 (Service Organization Control 2) report, 607
social engineering, 81, 117, 640
  BEC (business email compromise), 122
  impersonation, 121–122
  misinformation, 121
  phishing, 117–118, 634–635
  pretexting, 122
  smishing, 121
  toolkit, 118–120
  typosquatting, 123
  vishing, 120–121
  watering hole attack, 122–123
software. *See also* malware; SDN (software-defined networking)
  antivirus, 400
  decommissioning, 183
  -defined visibility, 201
  dependency, 46–47
  patching, 180–182, 374
  provider, 142
  rootkit, 157–158
  vulnerability, 112
SOP (standard operating procedure), 43
sovereignty, data, 278
spam, 109, 110
spam honeypot, 31–32
SPF (Sender Policy Framework), 428
split tunneling, 251
spoofing, 161, 440–441
spyware, 154
SQLi (SQL injection), 133
SSH (Secure Shell), 426
SSID (service set identifier), 245
SSO (single sign-on), 441–443
stakeholder, 42, 569–570
standards, 452, 536–537
  access control, 538
  encryption, 539–541
  password, 537–538
  physical security, 539
static code analysis, 338–339
steganography, 70–71
  audio, 71
  image, 71–72
  video, 71
stream cipher, 65–66
strong password, 138
structural metadata, 518
subject, 451
substitution, 74
supply chain
  analysis, 591–592
  security, 116

vulnerabilities
hardware provider, 141–142
service provider, 141
software provider, 142
surveillance, video, 28
switch, 312
symmetric encryption, 61–62, 64
syslog, 384–385, 386–387, 512–513
system audit, 367
system authentication, 21–22
system monitoring, 383

T

tabletop exercise, 296–297, 499–501
TACACS (Terminal Access Controller Access Control System), 253
tap mode, 229–230
technical controls, 6, 7
technical debt, 483–484
technical implications, 43
application restart, 46
downtime, 45
legacy application, 46
restricted activities, 44–45
service restart, 45–46
software dependency, 46–47
technology capacity planning, 295
test/ing, 296. *See also* penetration testing
continuous, 478–479
dynamic application security, 363
failover, 297–298
incident response, 498
penetration, 366, 589
result, 42
static application security, 362–363
static code analysis, 338–339
validation, 310
third-party certificate, 89
third-party risk assessment, 588
agreement types, 593–594
due diligence, 592
evidence of internal audits, 590
independent assessment, 590–591
penetration testing, 589
right-to-audit clause, 589–590
supply chain analysis, 591
vendor, 195, 588
threat, 98
actor
cybercriminal, 98
funding, 100
hacktivist, 98
insider, 99
intent and motivation, 99–100
level of sophistication, 99–100
motivation, 100–101
nation-state, 99
resources, 100
script kiddie, 98
unskilled attacker, 98
advanced persistent, 98–99, 101
conflict of interest, 592
default credentials, 115–116
environmental, 159
feed, 364
dark web, 365
ISAC (information sharing and analysis center), 364–365
OSINT (open-source intelligence), 364
proprietary, 364
file-based, 111
human vectors, 116
hunting, 502
image-based, 111
insider, 639
message-based, 109
email, 109
IM (Instant Messaging), 110
SMS (Short Message Service), 109–110
open service ports, 114–115
removable device, 111–112
scope reduction, 23

supply chain, 116
unsecured network, 113–114
unsupported systems and applications, 112–113
voice call, 111
ticket system, 477–478
timeline analysis, 501
time-of-day restrictions, 455–456
TIP (threat intelligence platform), 360
TLS (Transport Layer Security), 65, 181–182, 254–257, 426
TOC (time-of-check), 132
tokenization, 72–74, 458
tool/s
agents/agentless, 397
compiler, 131
NetFlow, 399–400
penetration testing, 366
SCAP (Security Content Automation Protocol), 393–395
SET (Social Engineering Toolkit), 118–120
SIEM (security information and event management), 397–399
SNMPWALK, 403
TPM (Trusted Platform Module), 67–68
vulnerability scanner, 360–362, 403–405
Tor (The Onion Router), 365
TOU (time-of-use), 132
TPM (Trusted Platform Module), 67–68
TPRM (third-party risk management), 349
trade secret, 274
training
developer, 131
incident response, 494, 497–498
personnel, 484–485
user, 131
transport/communication, 61, 426
trend, 419
Trojan horse, 153–154
trust
chain of, 88
root of, 89
web of, 88
trustworthy computing, 157
tunneling, 254–257
typosquatting, 123

U

UBA (user behavior analytics), 431–432
Ukraine, 101
ultrasonic sensor, 31
unexpected behavior, 636
unknown environment penetration testing, 627
unskilled attacker, 98
update
diagram, 47
malicious, 132–133
policy, 48
UPS (uninterruptible power supply), 301
URL (universal resource locator) scanning, 422
use metadata, 519
user account provisioning, 434–439, 474–476
UTM (unified threat management), 245–246, 250. *See also* firewall

V

validation
input, 336–337
of remediation, 376
testing, 310
vendor. *See also* third-party risk assessment
agreement types, 593–594
independent assessment, 590–591
monitoring, 594
questionnaire, 594–595

rules of engagement, 595
selection, 591–592
version control, 48, 309
video
steganography, 71
surveillance, 28
virtualization, 206
security implications, 206–208
vulnerability, 135
resource reuse, 135–136
VM escape, 135
virus, 155
vishing, 120–121
VM
escape, 135
sprawl, 207
voice recognition, 457
volume encryption, 60
VPN, 249
authentication, 249–250
IPsec, 250–251, 257
IKEv1 phase 1, 257–261
IKEv1 phase 2, 261–266
PPTP (Point-to-Point Tunneling Protocol), 249
site-to-site, 250
split tunneling, 251
TLS (Transport Layer Security), 254–257
Windows, 250
vulnerability/ies, 143–145. *See also* indicators; risk
analysis, 367
application
buffer overflow, 131–132
malicious update, 132–133
memory injection, 130–131
race condition, 132
audit, 376
bug bounty program, 367
classification, 370–371
cloud-specific, 136–141
cryptographic, 142
exceptions and exemptions, 375–376
firmware, 134
hardware, 134
industry/organizational impact, 372
misconfiguration, 142
mobile device, 142–143
jailbreaking, 143
side loading, 143
operating system-based, 133
prioritization, 368
reporting, 377–378
rescanning, 376
response and remediation, 374
responsible disclosure program, 366–367
scan/scanner, 309, 360–362, 389–390, 403–405,521–522
supply chain, 141
hardware provider, 141–142
service provider, 141
validation of remediation, 376
virtualization, 135
resource reuse, 135–136
VM escape, 135
web-based, 133
SQLi (SQL injection), 133
XSS (cross-site scripting), 134
zero-day, 143

W

WAF (web application firewall), 243–245
war
-dialing, 121
as threat actor motivation, 101
warm site, 293
watering hole attack, 122–123
wearables, 209
web browser, mobile device, 320–321
web filter, 421
agent-based, 421
block rules, 422
centralized proxy, 421–422

content categorization, 422
reputation-based, 422
URL scanning, 422
web form-grabbing keylogger, 156
web of trust, 88
web server, 256–257
web-based vulnerability, 133
SQLi (SQL injection), 133
XSS (cross-site scripting), 134
whaling, 117–118
whitelisting, 130, 178–179
Wi-Fi, 328
jamming, 161
phishing, 161
wildcard certificate, 90
Windows
CA (certificate authority), 81, 88
DAC (discretionary access control), 452–453
Event Viewer, 515–517
permission assignment, 434–439
permissions, 176–177
VPN, 250
wireless network, 113
attacks, 160–161
authentication
RADIUS (Remote Authentication Dial-In User Service) federation, 332–334
WPA3 (Wi-Fi Protected Access 3), 331–332, 334–335
channel selection, 316
heat map, 317
MU-MIMO (multi-user multiple-input and multiple-output), 315
point-to-multipoint, 315–316
point-to-point, 316
site survey, 315, 316–317
worm, 154
WPA3 (Wi-Fi Protected Access 3), 331–332, 334–335
WSUS (Windows Server Update Services), 480–481

X

XDR (extended detection and response), 431
XOR (exclusive OR), 65
XSS (cross-site scripting), 134

Y-Z

Zero Trust, 22
control plane, 22–23
data plane, 23–24
Implicit Trust Zone, 24
policy administrator, 23
policy engine, 23
secured zones, 23
zero-day vulnerability, 143
zoning, 226–227