

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®

Cybersecurity Analyst (CySA+)

CS0-002



TROY McMILLAN

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide

Troy McMillan



Pearson

CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide

Copyright © 2021 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.

ISBN-13: 978-0-13-674716-1

ISBN-10: 0-13-674716-7

Library of Congress Control Number: 2020941742

ScoutAutomatedPrintCode

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.

Editor-in-Chief

Mark Taub

Product Line Manager

Brett Bartow

Executive Editor

Nancy Davis

Development Editor

Christopher Cleveland

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Bill McManus

Indexer

Erika Millen

Proofreader

Abigail Manheim

Technical Editor

Chris Crayton

Editorial Assistant

Cindy Teeters

Cover Designer

Chuti Prasertsith

Compositor

codeMantra

Contents at a Glance

| | | |
|-------------------|---|--------|
| | Introduction | xxxvii |
| CHAPTER 1 | The Importance of Threat Data and Intelligence | 3 |
| CHAPTER 2 | Utilizing Threat Intelligence to Support Organizational Security | 19 |
| CHAPTER 3 | Vulnerability Management Activities | 39 |
| CHAPTER 4 | Analyzing Assessment Output | 67 |
| CHAPTER 5 | Threats and Vulnerabilities Associated with Specialized Technology | 93 |
| CHAPTER 6 | Threats and Vulnerabilities Associated with Operating in the Cloud | 123 |
| CHAPTER 7 | Implementing Controls to Mitigate Attacks and Software Vulnerabilities | 141 |
| CHAPTER 8 | Security Solutions for Infrastructure Management | 173 |
| CHAPTER 9 | Software Assurance Best Practices | 253 |
| CHAPTER 10 | Hardware Assurance Best Practices | 295 |
| CHAPTER 11 | Analyzing Data as Part of Security Monitoring Activities | 317 |
| CHAPTER 12 | Implementing Configuration Changes to Existing Controls to Improve Security | 377 |
| CHAPTER 13 | The Importance of Proactive Threat Hunting | 401 |
| CHAPTER 14 | Automation Concepts and Technologies | 419 |
| CHAPTER 15 | The Incident Response Process | 433 |
| CHAPTER 16 | Applying the Appropriate Incident Response Procedure | 449 |
| CHAPTER 17 | Analyzing Potential Indicators of Compromise | 469 |
| CHAPTER 18 | Utilizing Basic Digital Forensics Techniques | 485 |
| CHAPTER 19 | The Importance of Data Privacy and Protection | 505 |
| CHAPTER 20 | Applying Security Concepts in Support of Organizational Risk Mitigation | 527 |
| CHAPTER 21 | The Importance of Frameworks, Policies, Procedures, and Controls | 549 |
| CHAPTER 22 | Final Preparation | 579 |

APPENDIX A Answers to the “Do I Know This Already?” Quizzes and Review Questions 585

APPENDIX B *CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide*
Exam Updates 651

Glossary of Key Terms 653

Index 689

Online Elements:

APPENDIX C Memory Tables

APPENDIX D Memory Tables Answer Key

APPENDIX E Study Planner

Glossary of Key Terms

Table of Contents

| | |
|---|----------|
| Introduction | xxxvii |
| Chapter 1 The Importance of Threat Data and Intelligence | 3 |
| “Do I Know This Already?” Quiz | 3 |
| Foundation Topics | 6 |
| Intelligence Sources | 6 |
| Open-Source Intelligence | 6 |
| Proprietary/Closed-Source Intelligence | 6 |
| Timeliness | 7 |
| Relevancy | 7 |
| Confidence Levels | 7 |
| Accuracy | 7 |
| Indicator Management | 7 |
| Structured Threat Information eXpression (STIX) | 8 |
| Trusted Automated eXchange of Indicator Information (TAXII) | 8 |
| OpenIOC | 9 |
| Threat Classification | 9 |
| Known Threat vs. Unknown Threat | 10 |
| Zero-day | 10 |
| Advanced Persistent Threat | 11 |
| Threat Actors | 12 |
| Nation-state | 12 |
| Organized Crime | 12 |
| Terrorist Groups | 12 |
| Hactivist | 12 |
| Insider Threat | 12 |
| <i>Intentional</i> | 13 |
| <i>Unintentional</i> | 13 |
| Intelligence Cycle | 13 |
| Commodity Malware | 14 |
| Information Sharing and Analysis Communities | 15 |
| Exam Preparation Tasks | 16 |

| | |
|---|-----------|
| Review All Key Topics | 16 |
| Define Key Terms | 16 |
| Review Questions | 17 |
| Chapter 2 Utilizing Threat Intelligence to Support Organizational Security | 19 |
| “Do I Know This Already?” Quiz | 19 |
| Foundation Topics | 21 |
| Attack Frameworks | 21 |
| MITRE ATT&CK | 21 |
| The Diamond Model of Intrusion Analysis | 22 |
| Kill Chain | 23 |
| Threat Research | 23 |
| Reputational | 24 |
| Behavioral | 24 |
| Indicator of Compromise (IoC) | 25 |
| Common Vulnerability Scoring System (CVSS) | 25 |
| Threat Modeling Methodologies | 29 |
| Adversary Capability | 29 |
| Total Attack Surface | 31 |
| Attack Vector | 31 |
| Impact | 32 |
| Probability | 32 |
| Threat Intelligence Sharing with Supported Functions | 33 |
| Incident Response | 33 |
| Vulnerability Management | 33 |
| Risk Management | 33 |
| Security Engineering | 33 |
| Detection and Monitoring | 34 |
| Exam Preparation Tasks | 34 |
| Review All Key Topics | 34 |
| Define Key Terms | 35 |
| Review Questions | 35 |
| Chapter 3 Vulnerability Management Activities | 39 |
| “Do I Know This Already?” Quiz | 39 |
| Foundation Topics | 41 |

| | |
|---|----|
| Vulnerability Identification | 41 |
| Asset Criticality | 42 |
| Active vs. Passive Scanning | 43 |
| Mapping/Enumeration | 44 |
| Validation | 44 |
| Remediation/Mitigation | 45 |
| Configuration Baseline | 45 |
| Patching | 46 |
| Hardening | 46 |
| Compensating Controls | 47 |
| Risk Acceptance | 47 |
| Verification of Mitigation | 47 |
| Scanning Parameters and Criteria | 49 |
| Risks Associated with Scanning Activities | 49 |
| Vulnerability Feed | 49 |
| Scope | 49 |
| Credentialed vs. Non-credentialed | 51 |
| Server-based vs. Agent-based | 52 |
| Internal vs. External | 53 |
| Special Considerations | 53 |
| <i>Types of Data</i> | 53 |
| <i>Technical Constraints</i> | 53 |
| <i>Workflow</i> | 53 |
| <i>Sensitivity Levels</i> | 54 |
| <i>Regulatory Requirements</i> | 55 |
| <i>Segmentation</i> | 56 |
| <i>Intrusion Prevention System (IPS), Intrusion Detection System (IDS), and Firewall Settings</i> | 57 |
| <i>Firewall</i> | 59 |
| Inhibitors to Remediation | 62 |
| Exam Preparation Tasks | 63 |
| Review All Key Topics | 63 |
| Define Key Terms | 64 |
| Review Questions | 64 |

| | | |
|------------------|--|-----------|
| Chapter 4 | Analyzing Assessment Output | 67 |
| | “Do I Know This Already?” Quiz | 67 |
| | Foundation Topics | 69 |
| | Web Application Scanner | 69 |
| | Burp Suite | 69 |
| | OWASP Zed Attack Proxy (ZAP) | 69 |
| | Nikto | 70 |
| | Arachni | 70 |
| | Infrastructure Vulnerability Scanner | 71 |
| | Nessus | 71 |
| | OpenVAS | 71 |
| | Software Assessment Tools and Techniques | 72 |
| | Static Analysis | 73 |
| | Dynamic Analysis | 74 |
| | Reverse Engineering | 75 |
| | Fuzzing | 75 |
| | Enumeration | 76 |
| | Nmap | 76 |
| | Host Scanning | 79 |
| | hping | 80 |
| | Active vs. Passive | 82 |
| | Responder | 82 |
| | Wireless Assessment Tools | 82 |
| | Aircrack-ng | 83 |
| | Reaver | 84 |
| | oclHashcat | 86 |
| | Cloud Infrastructure Assessment Tools | 86 |
| | ScoutSuite | 87 |
| | Prowler | 87 |
| | Pacu | 87 |
| | Exam Preparation Tasks | 88 |
| | Review All Key Topics | 88 |
| | Define Key Terms | 89 |
| | Review Questions | 89 |

Chapter 5 Threats and Vulnerabilities Associated with Specialized Technology 93

| | |
|---|-----|
| “Do I Know This Already?” Quiz | 93 |
| Foundation Topics | 97 |
| Mobile | 97 |
| Unsigned Apps/System Apps | 98 |
| Security Implications/Privacy Concerns | 99 |
| <i>Data Storage</i> | 99 |
| <i>Nonremovable Storage</i> | 99 |
| <i>Removable Storage</i> | 99 |
| <i>Transfer/Back Up Data to Uncontrolled Storage</i> | 99 |
| <i>USB OTG</i> | 99 |
| Device Loss/Theft | 100 |
| Rooting/Jailbreaking | 100 |
| Push Notification Services | 100 |
| Geotagging | 100 |
| OEM/Carrier Android Fragmentation | 101 |
| Mobile Payment | 101 |
| <i>NFC Enabled</i> | 101 |
| <i>Inductance Enabled</i> | 102 |
| <i>Mobile Wallet</i> | 102 |
| <i>Peripheral-Enabled Payments (Credit Card Reader)</i> | 102 |
| USB | 102 |
| Malware | 102 |
| Unauthorized Domain Bridging | 103 |
| SMS/MMS/Messaging | 103 |
| Internet of Things (IoT) | 103 |
| IoT Examples | 104 |
| Methods of Securing IoT Devices | 104 |
| Embedded Systems | 105 |
| Real-Time Operating System (RTOS) | 105 |
| System-on-Chip (SoC) | 105 |
| Field Programmable Gate Array (FPGA) | 105 |

| | |
|---|------------|
| Physical Access Control | 106 |
| Systems | 106 |
| Devices | 107 |
| Facilities | 107 |
| Building Automation Systems | 109 |
| IP Video | 109 |
| HVAC Controllers | 111 |
| Sensors | 111 |
| Vehicles and Drones | 111 |
| CAN Bus | 112 |
| Drones | 113 |
| Workflow and Process Automation Systems | 113 |
| Incident Command System (ICS) | 114 |
| Supervisory Control and Data Acquisition (SCADA) | 114 |
| Modbus | 118 |
| Exam Preparation Tasks | 118 |
| Review All Key Topics | 118 |
| Define Key Terms | 119 |
| Review Questions | 120 |
| Chapter 6 Threats and Vulnerabilities Associated with Operating in the Cloud | 123 |
| “Do I Know This Already?” Quiz | 123 |
| Foundation Topics | 126 |
| Cloud Deployment Models | 126 |
| Cloud Service Models | 127 |
| Function as a Service (FaaS)/Serverless Architecture | 128 |
| Infrastructure as Code (IaC) | 130 |
| Insecure Application Programming Interface (API) | 131 |
| Improper Key Management | 132 |
| Key Escrow | 133 |
| Key Stretching | 134 |
| Unprotected Storage | 134 |
| Transfer/Back Up Data to Uncontrolled Storage | 134 |
| Big Data | 135 |

| | | |
|---|---|------------|
| Logging and Monitoring | 136 | |
| Insufficient Logging and Monitoring | 136 | |
| Inability to Access | 136 | |
| Exam Preparation Tasks | 137 | |
| Review All Key Topics | 137 | |
| Define Key Terms | 137 | |
| Review Questions | 138 | |
| Chapter 7 | Implementing Controls to Mitigate Attacks and Software Vulnerabilities | 141 |
| “Do I Know This Already?” Quiz | 141 | |
| Foundation Topics | 143 | |
| Attack Types | 143 | |
| Extensible Markup Language (XML) Attack | 143 | |
| Structured Query Language (SQL) Injection | 145 | |
| Overflow Attacks | 147 | |
| <i>Buffer</i> | 147 | |
| <i>Integer Overflow</i> | 149 | |
| <i>Heap</i> | 150 | |
| Remote Code Execution | 150 | |
| Directory Traversal | 151 | |
| Privilege Escalation | 152 | |
| Password Spraying | 152 | |
| Credential Stuffing | 152 | |
| Impersonation | 154 | |
| Man-in-the-Middle Attack | 154 | |
| <i>VLAN-based Attacks</i> | 156 | |
| Session Hijacking | 158 | |
| Rootkit | 159 | |
| Cross-Site Scripting | 160 | |
| <i>Reflected</i> | 161 | |
| <i>Persistent</i> | 161 | |
| <i>Document Object Model (DOM)</i> | 162 | |
| Vulnerabilities | 163 | |
| Improper Error Handling | 163 | |
| Dereferencing | 163 | |

| | | |
|------------------|---|------------|
| | Insecure Object Reference | 163 |
| | Race Condition | 164 |
| | Broken Authentication | 164 |
| | Sensitive Data Exposure | 165 |
| | Insecure Components | 165 |
| | <i>Code Reuse</i> | 166 |
| | Insufficient Logging and Monitoring | 166 |
| | Weak or Default Configurations | 167 |
| | Use of Insecure Functions | 168 |
| | <i>strcpy</i> | 168 |
| | Exam Preparation Tasks | 169 |
| | Review All Key Topics | 169 |
| | Define Key Terms | 170 |
| | Review Questions | 170 |
| Chapter 8 | Security Solutions for Infrastructure Management | 173 |
| | “Do I Know This Already?” Quiz | 173 |
| | Foundation Topics | 177 |
| | Cloud vs. On-premises | 177 |
| | Cloud Mitigations | 177 |
| | Asset Management | 178 |
| | Asset Tagging | 178 |
| | Device-Tracking Technologies | 178 |
| | <i>Geolocation/GPS Location</i> | 179 |
| | Object-Tracking and Object-Containment Technologies | 179 |
| | <i>Geotagging/Geofencing</i> | 179 |
| | <i>RFID</i> | 180 |
| | Segmentation | 180 |
| | Physical | 180 |
| | <i>LAN</i> | 181 |
| | <i>Intranet</i> | 181 |
| | <i>Extranet</i> | 181 |
| | <i>DMZ</i> | 181 |
| | Virtual | 182 |
| | Jumpbox | 183 |

| | |
|---|-----|
| System Isolation | 184 |
| <i>Air Gap</i> | 185 |
| Network Architecture | 185 |
| Physical | 186 |
| <i>Firewall Architecture</i> | 188 |
| Software-Defined Networking | 193 |
| <i>Virtual SAN</i> | 194 |
| Virtual Private Cloud (VPC) | 195 |
| Virtual Private Network (VPN) | 195 |
| <i>IPsec</i> | 197 |
| <i>SSL/TLS</i> | 199 |
| Serverless | 200 |
| Change Management | 201 |
| Virtualization | 201 |
| Security Advantages and Disadvantages of Virtualization | 201 |
| Type 1 vs. Type 2 Hypervisors | 203 |
| Virtualization Attacks and Vulnerabilities | 203 |
| Virtual Networks | 205 |
| Management Interface | 205 |
| Vulnerabilities Associated with a Single Physical Server Hosting Multiple Companies' Virtual Machines | 206 |
| Vulnerabilities Associated with a Single Platform Hosting Multiple Companies' Virtual Machines | 207 |
| Virtual Desktop Infrastructure (VDI) | 207 |
| Terminal Services/Application Delivery Services | 208 |
| Containerization | 208 |
| Identity and Access Management | 209 |
| Identify Resources | 210 |
| Identify Users | 210 |
| Identify Relationships Between Resources and Users | 210 |
| Privilege Management | 211 |
| Multifactor Authentication (MFA) | 211 |
| <i>Authentication</i> | 211 |
| <i>Authentication Factors</i> | 212 |

| | |
|-------------------------------------|-----|
| <i>Knowledge Factors</i> | 213 |
| <i>Ownership Factors</i> | 213 |
| <i>Characteristic Factors</i> | 214 |
| Single Sign-On (SSO) | 214 |
| <i>Kerberos</i> | 215 |
| Active Directory | 217 |
| SESAME | 219 |
| Federation | 219 |
| <i>XACML</i> | 220 |
| <i>SPML</i> | 220 |
| <i>SAML</i> | 221 |
| <i>OpenID</i> | 222 |
| <i>Shibboleth</i> | 224 |
| Role-Based Access Control | 224 |
| Attribute-Based Access Control | 225 |
| Mandatory Access Control | 228 |
| Manual Review | 229 |
| Cloud Access Security Broker (CASB) | 229 |
| Honeypot | 230 |
| Monitoring and Logging | 230 |
| Log Management | 230 |
| Audit Reduction Tools | 231 |
| NIST SP 800-137 | 232 |
| Encryption | 232 |
| Cryptographic Types | 233 |
| <i>Symmetric Algorithms</i> | 233 |
| <i>Asymmetric Algorithms</i> | 236 |
| <i>Hybrid Encryption</i> | 236 |
| Hashing Functions | 238 |
| <i>One-way Hash</i> | 238 |
| Message Digest Algorithm | 239 |
| <i>Secure Hash Algorithm</i> | 240 |
| Transport Encryption | 240 |
| SSL/TLS | 241 |

| | | |
|------------------|--|------------|
| | <i>HTTP/HTTPS/SHTTP</i> | 241 |
| | <i>SSH</i> | 242 |
| | <i>IPsec</i> | 242 |
| | Certificate Management | 242 |
| | Certificate Authority and Registration Authority | 243 |
| | Certificates | 243 |
| | Certificate Revocation List | 244 |
| | OCSP | 244 |
| | PKI Steps | 245 |
| | Cross-Certification | 245 |
| | Digital Signatures | 245 |
| | Active Defense | 246 |
| | Hunt Teaming | 247 |
| | Exam Preparation Tasks | 247 |
| | Review All Key Topics | 247 |
| | Define Key Terms | 250 |
| | Review Questions | 250 |
| Chapter 9 | Software Assurance Best Practices | 253 |
| | “Do I Know This Already?” Quiz | 253 |
| | Foundation Topics | 256 |
| | Platforms | 256 |
| | Mobile | 256 |
| | <i>Containerization</i> | 256 |
| | <i>Configuration Profiles and Payloads</i> | 256 |
| | <i>Personally Owned, Corporate Enabled</i> | 256 |
| | <i>Corporate-Owned, Personally Enabled</i> | 257 |
| | <i>Application Wrapping</i> | 257 |
| | <i>Application, Content, and Data Management</i> | 257 |
| | <i>Remote Wiping</i> | 257 |
| | SCEP | 258 |
| | NIST SP 800-163 Rev 1 | 258 |
| | Web Application | 260 |
| | Maintenance Hooks | 260 |
| | Time-of-Check/Time-of-Use Attacks | 260 |

| | |
|--|-----|
| <i>Cross-Site Request Forgery (CSRF)</i> | 261 |
| <i>Click-Jacking</i> | 262 |
| Client/Server | 263 |
| Embedded | 263 |
| <i>Hardware/Embedded Device Analysis</i> | 264 |
| System-on-Chip (SoC) | 265 |
| <i>Secure Booting</i> | 265 |
| <i>Central Security Breach Response</i> | 265 |
| Firmware | 266 |
| Software Development Life Cycle (SDLC) Integration | 267 |
| Step 1: Plan/Initiate Project | 267 |
| Step 2: Gather Requirements | 268 |
| Step 3: Design | 268 |
| Step 4: Develop | 269 |
| Step 5: Test/Validate | 269 |
| Step 6: Release/Maintain | 269 |
| Step 7: Certify/Accredit | 270 |
| Step 8: Change Management and Configuration Management/ Replacement | 270 |
| DevSecOps | 270 |
| DevOps | 270 |
| Software Assessment Methods | 272 |
| User Acceptance Testing | 272 |
| Stress Test Application | 272 |
| Security Regression Testing | 273 |
| Code Review | 273 |
| Security Testing | 274 |
| Code Review Process | 275 |
| Secure Coding Best Practices | 275 |
| Input Validation | 275 |
| Output Encoding | 276 |
| Session Management | 276 |
| Authentication | 277 |
| <i>Context-based Authentication</i> | 277 |

| | |
|--|------------|
| <i>Network Authentication Methods</i> | 279 |
| <i>IEEE 802.1X</i> | 281 |
| <i>Biometric Considerations</i> | 282 |
| <i>Certificate-Based Authentication</i> | 284 |
| Data Protection | 285 |
| Parameterized Queries | 285 |
| Static Analysis Tools | 286 |
| Dynamic Analysis Tools | 286 |
| Formal Methods for Verification of Critical Software | 286 |
| Service-Oriented Architecture | 287 |
| Security Assertions Markup Language (SAML) | 287 |
| Simple Object Access Protocol (SOAP) | 287 |
| Representational State Transfer (REST) | 288 |
| Microservices | 288 |
| Exam Preparation Tasks | 289 |
| Review All Key Topics | 289 |
| Define Key Terms | 290 |
| Review Questions | 291 |
| Chapter 10 Hardware Assurance Best Practices | 295 |
| “Do I Know This Already?” Quiz | 295 |
| Foundation Topics | 298 |
| Hardware Root of Trust | 298 |
| Trusted Platform Module (TPM) | 299 |
| Virtual TPM | 300 |
| Hardware Security Module (HSM) | 302 |
| MicroSD HSM | 302 |
| eFuse | 303 |
| Unified Extensible Firmware Interface (UEFI) | 303 |
| Trusted Foundry | 304 |
| Secure Processing | 305 |
| Trusted Execution | 305 |
| Secure Enclave | 307 |
| Processor Security Extensions | 307 |
| Atomic Execution | 307 |

| | |
|--|------------|
| Anti-Tamper | 308 |
| Self-Encrypting Drives | 308 |
| Trusted Firmware Updates | 308 |
| Measured Boot and Attestation | 310 |
| Measured Launch | 311 |
| Integrity Measurement Architecture | 311 |
| Bus Encryption | 311 |
| Exam Preparation Tasks | 312 |
| Review All Key Topics | 312 |
| Define Key Terms | 312 |
| Review Questions | 313 |
| Chapter 11 Analyzing Data as Part of Security Monitoring Activities | 317 |
| “Do I Know This Already?” Quiz | 317 |
| Foundation Topics | 320 |
| Heuristics | 320 |
| Trend Analysis | 320 |
| Endpoint | 321 |
| Malware | 323 |
| <i>Virus</i> | 323 |
| <i>Worm</i> | 324 |
| <i>Trojan Horse</i> | 325 |
| <i>Logic Bomb</i> | 325 |
| <i>Spyware/Adware</i> | 325 |
| <i>Botnet</i> | 325 |
| <i>Rootkit</i> | 326 |
| <i>Ransomware</i> | 326 |
| <i>Reverse Engineering</i> | 327 |
| Memory | 329 |
| <i>Memory Protection</i> | 329 |
| <i>Secured Memory</i> | 330 |
| <i>Runtime Data Integrity Check</i> | 330 |
| <i>Memory Dumping, Runtime Debugging</i> | 332 |
| System and Application Behavior | 333 |
| <i>Known-good Behavior</i> | 333 |

| | |
|---|-----|
| <i>Anomalous Behavior</i> | 334 |
| <i>Exploit Techniques</i> | 335 |
| File System | 339 |
| <i>File Integrity Monitoring</i> | 340 |
| User and Entity Behavior Analytics (UEBA) | 341 |
| Network | 342 |
| Uniform Resource Locator (URL) and Domain Name System (DNS) Analysis | 342 |
| DNS Analysis | 342 |
| Domain Generation Algorithm | 343 |
| Flow Analysis | 345 |
| NetFlow Analysis | 346 |
| Packet and Protocol Analysis | 348 |
| <i>Packet Analysis</i> | 348 |
| <i>Protocol Analysis</i> | 348 |
| Malware | 348 |
| Log Review | 348 |
| Event Logs | 349 |
| Syslog | 350 |
| Kiwi Syslog Server | 352 |
| Firewall Logs | 353 |
| <i>Windows Defender</i> | 353 |
| <i>Cisco Check Point</i> | 353 |
| Web Application Firewall (WAF) | 355 |
| Proxy | 356 |
| Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) | 357 |
| <i>Sourcefire</i> | 358 |
| <i>Snort</i> | 359 |
| <i>Zeek</i> | 360 |
| <i>HIPS</i> | 360 |
| Impact Analysis | 361 |
| Organization Impact vs. Localized Impact | 361 |
| Immediate Impact vs. Total Impact | 361 |

| | |
|---|------------|
| Security Information and Event Management (SIEM) Review | 361 |
| Rule Writing | 362 |
| Known-Bad Internet Protocol (IP) | 363 |
| Dashboard | 363 |
| Query Writing | 366 |
| String Search | 366 |
| Script | 366 |
| Piping | 367 |
| E-mail Analysis | 367 |
| E-mail Spoofing | 368 |
| Malicious Payload | 368 |
| DomainKeys Identified Mail (DKIM) | 368 |
| Sender Policy Framework (SPF) | 369 |
| Domain-based Message Authentication, Reporting, and Conformance (DMARC) | 369 |
| Phishing | 369 |
| <i>Spear Phishing</i> | 369 |
| <i>Whaling</i> | 370 |
| Forwarding | 370 |
| Digital Signature | 371 |
| E-mail Signature Block | 372 |
| Embedded Links | 372 |
| Impersonation | 372 |
| Exam Preparation Tasks | 372 |
| Review All Key Topics | 372 |
| Define Key Terms | 374 |
| Review Questions | 374 |
| Chapter 12 Implementing Configuration Changes to Existing Controls to Improve Security | 377 |
| “Do I Know This Already?” Quiz | 377 |
| Foundation Topics | 381 |
| Permissions | 381 |
| Whitelisting and Blacklisting | 381 |
| Application Whitelisting and Blacklisting | 382 |
| Input Validation | 382 |

| | |
|--|------------|
| Firewall | 383 |
| NextGen Firewalls | 383 |
| Host-Based Firewalls | 384 |
| Intrusion Prevention System (IPS) Rules | 386 |
| Data Loss Prevention (DLP) | 386 |
| Endpoint Detection and Response (EDR) | 387 |
| Network Access Control (NAC) | 387 |
| Quarantine/Remediation | 389 |
| Agent-Based vs. Agentless NAC | 389 |
| 802.1X | 389 |
| Sinkholing | 391 |
| Malware Signatures | 391 |
| Development/Rule Writing | 392 |
| Sandboxing | 392 |
| Port Security | 394 |
| Limiting MAC Addresses | 395 |
| Implementing Sticky MAC | 395 |
| Exam Preparation Tasks | 396 |
| Review All Key Topics | 396 |
| Define Key Terms | 396 |
| Review Questions | 397 |
| Chapter 13 The Importance of Proactive Threat Hunting | 401 |
| “Do I Know This Already?” Quiz | 401 |
| Foundation Topics | 404 |
| Establishing a Hypothesis | 404 |
| Profiling Threat Actors and Activities | 405 |
| Threat Hunting Tactics | 406 |
| Hunt Teaming | 406 |
| Threat Model | 406 |
| Executable Process Analysis | 407 |
| Memory Consumption | 409 |
| Reducing the Attack Surface Area | 409 |
| System Hardening | 410 |
| Configuration Lockdown | 410 |

| | |
|--|------------|
| Bundling Critical Assets | 411 |
| Commercial Business Classifications | 411 |
| Military and Government Classifications | 412 |
| Distribution of Critical Assets | 412 |
| Attack Vectors | 412 |
| Integrated Intelligence | 413 |
| Improving Detection Capabilities | 413 |
| Continuous Improvement | 413 |
| Continuous Monitoring | 414 |
| Exam Preparation Tasks | 414 |
| Review All Key Topics | 414 |
| Define Key Terms | 415 |
| Review Questions | 415 |
| Chapter 14 Automation Concepts and Technologies | 419 |
| “Do I Know This Already?” Quiz | 419 |
| Foundation Topics | 422 |
| Workflow Orchestration | 422 |
| Scripting | 423 |
| Application Programming Interface (API) Integration | 424 |
| Automated Malware Signature Creation | 424 |
| Data Enrichment | 425 |
| Threat Feed Combination | 426 |
| Machine Learning | 426 |
| Use of Automation Protocols and Standards | 427 |
| Security Content Automation Protocol (SCAP) | 427 |
| Continuous Integration | 428 |
| Continuous Deployment/Delivery | 428 |
| Exam Preparation Tasks | 429 |
| Review All Key Topics | 429 |
| Define Key Terms | 430 |
| Review Questions | 430 |
| Chapter 15 The Incident Response Process | 433 |
| “Do I Know This Already?” Quiz | 433 |
| Foundation Topics | 435 |

| | |
|--|------------|
| Communication Plan | 435 |
| Limiting Communication to Trusted Parties | 435 |
| Disclosing Based on Regulatory/Legislative Requirements | 435 |
| Preventing Inadvertent Release of Information | 435 |
| Using a Secure Method of Communication | 435 |
| Reporting Requirements | 436 |
| Response Coordination with Relevant Entities | 436 |
| Legal | 436 |
| Human Resources | 437 |
| Public Relations | 437 |
| Internal and External | 437 |
| Law Enforcement | 437 |
| Senior Leadership | 438 |
| Regulatory Bodies | 438 |
| Factors Contributing to Data Criticality | 439 |
| Personally Identifiable Information (PII) | 439 |
| Personal Health Information (PHI) | 440 |
| Sensitive Personal Information (SPI) | 441 |
| High Value Assets | 441 |
| Financial Information | 441 |
| Intellectual Property | 442 |
| <i>Patent</i> | 442 |
| <i>Trade Secret</i> | 443 |
| <i>Trademark</i> | 443 |
| <i>Copyright</i> | 444 |
| <i>Securing Intellectual Property</i> | 444 |
| Corporate Information | 444 |
| Exam Preparation Tasks | 445 |
| Review All Key Topics | 445 |
| Define Key Terms | 446 |
| Review Questions | 446 |
| Chapter 16 Applying the Appropriate Incident Response Procedure | 449 |
| “Do I Know This Already?” Quiz | 449 |
| Foundation Topics | 452 |

| | |
|---|-----|
| Preparation | 452 |
| Training | 452 |
| Testing | 453 |
| Documentation of Procedures | 453 |
| Detection and Analysis | 454 |
| Characteristics Contributing to Severity Level Classification | 455 |
| Downtime and Recovery Time | 455 |
| Data Integrity | 456 |
| Economic | 456 |
| System Process Criticality | 457 |
| Reverse Engineering | 457 |
| Data Correlation | 458 |
| Containment | 458 |
| Segmentation | 458 |
| Isolation | 459 |
| Eradication and Recovery | 459 |
| Vulnerability Mitigation | 459 |
| Sanitization | 460 |
| Reconstruction/Reimaging | 460 |
| Secure Disposal | 460 |
| Patching | 461 |
| Restoration of Permissions | 461 |
| Reconstitution of Resources | 462 |
| Restoration of Capabilities and Services | 462 |
| Verification of Logging/Communication to Security Monitoring | 462 |
| Post-Incident Activities | 463 |
| Evidence Retention | 463 |
| Lessons Learned Report | 463 |
| Change Control Process | 464 |
| Incident Response Plan Update | 464 |
| Incident Summary Report | 464 |
| Indicator of Compromise (IoC) Generation | 465 |
| Monitoring | 465 |
| Exam Preparation Tasks | 465 |

| | |
|--|------------|
| Review All Key Topics | 465 |
| Define Key Terms | 466 |
| Review Questions | 466 |
| Chapter 17 Analyzing Potential Indicators of Compromise | 469 |
| “Do I Know This Already?” Quiz | 469 |
| Foundation Topics | 472 |
| Network-Related Indicators of Compromise | 472 |
| Bandwidth Consumption | 472 |
| Beaconing | 473 |
| Irregular Peer-to-Peer Communication | 473 |
| Rogue Device on the Network | 475 |
| Scan/Sweep | 476 |
| Unusual Traffic Spike | 476 |
| Common Protocol over Non-standard Port | 476 |
| Host-Related Indicators of Compromise | 477 |
| Processor Consumption | 477 |
| Memory Consumption | 477 |
| Drive Capacity Consumption | 477 |
| Unauthorized Software | 477 |
| Malicious Process | 478 |
| Unauthorized Change | 479 |
| Unauthorized Privilege | 479 |
| Data Exfiltration | 479 |
| Abnormal OS Process Behavior | 479 |
| File System Change or Anomaly | 479 |
| Registry Change or Anomaly | 480 |
| Unauthorized Scheduled Task | 480 |
| Application-Related Indicators of Compromise | 480 |
| Anomalous Activity | 480 |
| Introduction of New Accounts | 480 |
| Unexpected Output | 480 |
| Unexpected Outbound Communication | 481 |
| Service Interruption | 481 |
| Application Log | 481 |

| | |
|--|------------|
| Exam Preparation Tasks | 482 |
| Review All Key Topics | 482 |
| Define Key Terms | 482 |
| Review Questions | 482 |
| Chapter 18 Utilizing Basic Digital Forensics Techniques | 485 |
| “Do I Know This Already?” Quiz | 485 |
| Foundation Topics | 488 |
| Network | 488 |
| Wireshark | 488 |
| tcpdump | 490 |
| Endpoint | 490 |
| Disk | 491 |
| <i>FTK</i> | 491 |
| <i>Helix3</i> | 491 |
| <i>Password Cracking</i> | 491 |
| <i>Imaging</i> | 492 |
| Memory | 493 |
| Mobile | 494 |
| Cloud | 495 |
| Virtualization | 497 |
| Legal Hold | 497 |
| Procedures | 497 |
| EnCase Forensic | 498 |
| Sysinternals | 498 |
| Forensic Investigation Suite | 498 |
| Hashing | 499 |
| Hashing Utilities | 499 |
| Changes to Binaries | 500 |
| Carving | 500 |
| Data Acquisition | 501 |
| Exam Preparation Tasks | 501 |
| Review All Key Topics | 501 |
| Define Key Terms | 501 |
| Review Questions | 502 |

Chapter 19 The Importance of Data Privacy and Protection 505

| | |
|--|-----|
| “Do I Know This Already?” Quiz | 505 |
| Foundation Topics | 508 |
| Privacy vs. Security | 508 |
| Non-technical Controls | 508 |
| Classification | 508 |
| Ownership | 508 |
| Retention | 509 |
| Data Types | 509 |
| <i>Personally Identifiable Information (PII)</i> | 509 |
| <i>Personal Health Information (PHI)</i> | 510 |
| <i>Payment Card Information</i> | 510 |
| Retention Standards | 510 |
| Confidentiality | 510 |
| Legal Requirements | 510 |
| Data Sovereignty | 514 |
| Data Minimization | 515 |
| Purpose Limitation | 515 |
| Non-disclosure agreement (NDA) | 516 |
| Technical Controls | 516 |
| Encryption | 516 |
| Data Loss Prevention (DLP) | 516 |
| Data Masking | 516 |
| Deidentification | 517 |
| Tokenization | 517 |
| Digital Rights Management (DRM) | 517 |
| <i>Document DRM</i> | 520 |
| <i>Music DRM</i> | 520 |
| <i>Movie DRM</i> | 520 |
| <i>Video Game DRM</i> | 520 |
| <i>E-Book DRM</i> | 521 |
| <i>Watermarking</i> | 521 |
| Geographic Access Requirements | 521 |
| Access Controls | 521 |

| | |
|---|------------|
| Exam Preparation Tasks | 521 |
| Review All Key Topics | 522 |
| Define Key Terms | 522 |
| Review Questions | 523 |
| Chapter 20 Applying Security Concepts in Support of Organizational Risk Mitigation | 527 |
| “Do I Know This Already?” Quiz | 527 |
| Foundation Topics | 530 |
| Business Impact Analysis | 530 |
| Identify Critical Processes and Resources | 530 |
| Identify Outage Impacts and Estimate Downtime | 531 |
| Identify Resource Requirements | 531 |
| Identify Recovery Priorities | 531 |
| <i>Recoverability</i> | 532 |
| <i>Fault Tolerance</i> | 532 |
| Risk Identification Process | 532 |
| Make Risk Determination Based upon Known Metrics | 533 |
| Qualitative Risk Analysis | 533 |
| Quantitative Risk Analysis | 534 |
| Risk Calculation | 534 |
| Probability | 535 |
| Magnitude | 535 |
| Communication of Risk Factors | 536 |
| Risk Prioritization | 537 |
| Security Controls | 538 |
| Engineering Tradeoffs | 538 |
| MOUs | 538 |
| SLAs | 538 |
| Organizational Governance | 539 |
| Business Process Interruption | 539 |
| Degrading Functionality | 539 |
| Systems Assessment | 539 |
| ISO/IEC 27001 | 539 |
| ISO/IEC 27002 | 541 |

| | |
|--|------------|
| Documented Compensating Controls | 541 |
| Training and Exercises | 542 |
| Red Team | 542 |
| Blue Team | 542 |
| White Team | 543 |
| Tabletop Exercise | 543 |
| Supply Chain Assessment | 543 |
| Vendor Due Diligence | 543 |
| <i>OEM Documentation</i> | 543 |
| Hardware Source Authenticity | 544 |
| <i>Trusted Foundry</i> | 544 |
| Exam Preparation Tasks | 544 |
| Review All Key Topics | 544 |
| Define Key Terms | 545 |
| Review Questions | 545 |
| Chapter 21 The Importance of Frameworks, Policies, Procedures, and Controls | 549 |
| “Do I Know This Already?” Quiz | 549 |
| Foundation Topics | 552 |
| Frameworks | 552 |
| Risk-Based Frameworks | 552 |
| <i>National Institute of Standards and Technology (NIST)</i> | 552 |
| <i>COBIT</i> | 553 |
| <i>The Open Group Architecture Framework (TOGAF)</i> | 554 |
| Prescriptive Frameworks | 555 |
| <i>NIST Cybersecurity Framework Version 1.1</i> | 555 |
| <i>ISO 27000 Series</i> | 556 |
| <i>SABSA</i> | 559 |
| <i>ITIL</i> | 559 |
| <i>Maturity Models</i> | 559 |
| <i>ISO/IEC 27001</i> | 562 |
| Policies and Procedures | 562 |
| Code of Conduct/Ethics | 563 |
| Acceptable Use Policy (AUP) | 563 |

| | |
|---|------------|
| Password Policy | 564 |
| Data Ownership | 567 |
| Data Retention | 567 |
| Account Management | 568 |
| Continuous Monitoring | 569 |
| Work Product Retention | 570 |
| Category | 570 |
| Managerial | 570 |
| Operational | 571 |
| Technical | 571 |
| Control Type | 571 |
| Preventative | 572 |
| Detective | 572 |
| Corrective | 572 |
| Deterrent | 572 |
| Directive | 572 |
| Physical | 572 |
| Audits and Assessments | 573 |
| Regulatory | 573 |
| Compliance | 575 |
| Exam Preparation Tasks | 575 |
| Review All Key Topics | 575 |
| Define Key Terms | 576 |
| Review Questions | 576 |
| Chapter 22 Final Preparation | 579 |
| Exam Information | 579 |
| Getting Ready | 580 |
| Tools for Final Preparation | 582 |
| Pearson Test Prep Practice Test Software and Questions on the Website | 582 |
| Memory Tables | 582 |
| Chapter-Ending Review Tools | 582 |
| Suggested Plan for Final Review/Study | 583 |
| Summary | 583 |

Appendix A Answers to the “Do I Know This Already?” Quizzes and Review Questions 585

Appendix B *CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide* Exam Updates 651

Glossary of Key Terms 653

Index 689

Online Elements:

Appendix C Memory Tables

Appendix D Memory Tables Answer Key

Appendix E Study Planner

Glossary of Key Terms

About the Author

Troy McMillan is a product developer and technical editor for Kaplan IT as well as a full-time trainer. He became a professional trainer 20 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. He has written or contributed to more than a dozen projects, including the following recent ones:

- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Author of *CISSP Cert Guide* (Pearson)
- Prep test question writer for *CCNA Wireless 640-722 Official Cert Guide* (Cisco Press)
- Author of *CompTIA Advanced Security Practitioner (CASP) Cert Guide* (Pearson)

Troy has also appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND1; and ICND2.

He delivers CISSP training classes for CyberVista, and is an authorized online training provider for (ISC)2.

Troy also creates certification practice tests and study guides for CyberVista. He lives in Asheville, North Carolina, with his wife, Heike.

Dedication

I dedicate this book to my wife, Heike, who has supported me when I needed it most.

Acknowledgments

I must thank everyone on the Pearson team for all of their help in making this book better than it would have been without their help. That includes Chris Cleveland, Nancy Davis, Chris Crayton, Tonya Simpson, and Mudita Sonar.

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. 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 teaching awards, and has served as a state-level SkillsUSA competition judge.

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 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@informat.com

Introduction

CompTIA CySA+ bridges the skills gap between CompTIA Security+ and CompTIA Advanced Security Practitioner (CASP+). Building on CySA+, IT professionals can pursue CASP+ to prove their mastery of the hands-on cybersecurity skills required at the 5- to 10-year experience level. Earn the CySA+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

CompTIA CySA+ certification is designed to be a “vendor-neutral” exam that measures your knowledge of industry-standard technology.

Goals and Methods

The number-one goal of this book is a simple one: to help you pass the 2020 version of the CompTIA CySA+ certification exam, CS0-002.

Because the CompTIA CySA+ certification exam stresses problem-solving abilities and reasoning more than memorization of terms and facts, this book is designed to help you master and understand the required objectives for each exam.

To aid you in mastering and understanding the CySA+ certification objectives, this book uses the following methods:

- The beginning of each chapter identifies the CompTIA CySA+ objective addressed in the chapter and defines the related topics covered in the chapter.
- The body of the chapter explains the topics from a hands-on and theory-based standpoint. This includes in-depth descriptions, tables, and figures that are geared toward building your knowledge so that you can pass the exam. The structure of each chapter generally follows the outline of the corresponding exam objective, which not only enables you to study the exam objectives methodically but also enables you to easily locate coverage of specific exam objectives that you think you need to review further.
- Key Topic icons identify important figures, tables, and lists of information that you should know for the exam. Key topics are interspersed throughout the chapter and are listed in a table at the end of the chapter.
- Key terms in each chapter are emphasized in ***bold italic*** and are listed without definitions at the end of each chapter. Write down the definition of each term and check your work against the complete key terms in the glossary.

Strategies for Exam Preparation

Strategies for exam preparation vary depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would consist of three or four years of hands-on security or related experience followed by rigorous study of the exam objectives.

Before and after you have read through the book, have a look at the current exam objectives for the CompTIA CySA+ Certification Exam, listed at <https://www.comptia.org/certifications/cybersecurity-analyst#examdetails>. If there are any areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams found on the website that accompanies this book. As you work through the practice exams, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed those areas, work through the practice exams a second time and rate your skills. Keep in mind that the more you work through the practice exams, the more familiar the questions will become.

After you have worked through the practice exams a second time and feel confident in your skills, schedule the CompTIA CySA+ CS0-002 exam through Pearson Vue (<https://home.pearsonvue.com>). To prevent the information from evaporating out of your mind, you should typically take the exam within a week of when you consider yourself ready to take it.

The CompTIA CySA+ certification credential for those passing the certification exams is now valid for three years. To renew your certification without retaking the exam, you need to participate in continuing education (CE) activities and pay an annual maintenance fee of \$50 (that is, \$150 for three years). See <https://www.comptia.org/continuing-education/learn/ce-program-fees> for fee details. To learn more about the certification renewal policy, see <https://certification.comptia.org/continuing-education>.

How the Book Is Organized

Table I-1 outlines where each of the CySA+ exam objectives is covered in the book. For a full dissection of what is covered in each objective, you should download the most recent set of objectives from <https://www.comptia.org/certifications/cybersecurity-analyst#examdetails>.

Table I-1 CySA+ CS0-002 Exam Objectives: Coverage by Chapter

| Exam Objective | Chapter Where This Objective Is Covered |
|---|--|
| Domain 1.0 Threat and Vulnerability Management (accounts for 22% of the exam) | |
| 1.1 Explain the importance of threat data and intelligence | Chapter 1 |
| 1.2 Given a scenario, utilize threat intelligence to support organizational security | Chapter 2 |
| 1.3 Given a scenario, perform vulnerability management activities | Chapter 3 |
| 1.4 Given a scenario, analyze the output from common vulnerability assessment tools | Chapter 4 |
| 1.5 Explain the threats and vulnerabilities associated with specialized technology | Chapter 5 |
| 1.6 Explain the threats and vulnerabilities associated with operating in the cloud | Chapter 6 |
| 1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities | Chapter 7 |
| Domain 2.0 Software and Systems Security (accounts for 18% of the exam) | |
| 2.1 Given a scenario, apply security solutions for infrastructure management | Chapter 8 |
| 2.2 Explain software assurance best practices | Chapter 9 |
| 2.3 Explain hardware assurance best practices | Chapter 10 |

| Exam Objective | Chapter Where This Objective Is Covered |
|--|--|
| Domain 3.0 Security Operations and Monitoring (accounts for 25% of the exam) | |
| 3.1 Given a scenario, analyze data as part of security monitoring activities | Chapter 11 |
| 3.2 Given a scenario, implement configuration changes to existing controls to improve security | Chapter 12 |
| 3.3 Explain the importance of proactive threat hunting | Chapter 13 |
| 3.4 Compare and contrast automation concepts and technologies | Chapter 14 |
| Domain 4.0 Incident Response (accounts for 22% of the exam) | |
| 4.1 Explain the importance of the incident response process | Chapter 15 |
| 4.2 Given a scenario, apply the appropriate incident response procedure | Chapter 16 |
| 4.3 Given an incident, analyze potential indicators of compromise | Chapter 17 |
| 4.4 Given a scenario, utilize basic digital forensics techniques | Chapter 18 |
| Domain 5.0 Compliance and Assessment (accounts for 13% of the exam) | |
| 5.1 Understand the importance of data privacy and protection | Chapter 19 |
| 5.2 Given a scenario, apply security concepts in support of organizational risk mitigation | Chapter 20 |
| 5.3 Explain the importance of frameworks, policies, procedures, and controls | Chapter 21 |

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section provides the following study activities that you should do to prepare for the exam:
 - **Review All Key Topics:** As previously mentioned, the Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.

- **Define Key Terms:** Although the CySA+ exam might be unlikely to ask a question such as “Define this term,” the exam does require that you learn and know a lot of cybersecurity-related terminology. This section lists the most important terms from the chapter, asking you to write a short definition of each and compare your answer to the glossary entry at the end of the book.
- **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Test Prep practice test software that enables you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

What’s New?

With every exam update, changes in the relative emphasis on certain topics can change. Here is an overview of some of the most important changes:

- Increased content on the importance of threat data and intelligence
- Increased emphasis on regulatory compliance
- Increased emphasis on the options and combinations available for any given command
- Increased emphasis on identifying attacks through log analysis
- Increased coverage of cloud security
- Increased coverage of forming and using queries

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book’s companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.pearsonITcertification.com and register your book.

To do so, simply go to www.pearsonitcertification.com/register and enter the ISBN of the print book: 9780136747161. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book’s companion website.

Note that if you buy the *Premium Edition eBook and Practice Test* version of this book from Pearson, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

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 steps at left, please visit 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 Practice Test Software

You have two options for installing and using the Pearson Test Prep practice test software: 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:

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique PTP code.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the www.pearsonITcertification.com website, the code will be populated on your account page after purchase. Just log in to www.pearsonITcertification.com, click **Account** to see details of your account, and click the **Digital Purchases** tab.
- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly from Amazon.
- **Other bookseller e-books:** Note that if you purchase an e-book version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

NOTE Do not lose the activation code because it is the only means with which you can access the QA content with the book.

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.
- Step 2.** Click the **Practice Exams** button.
- Step 3.** Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to www.pearsonestprep.com, establish a free login if you do not already have one, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

NOTE Amazon eBook (Kindle) customers: It is easy to miss Amazon's e-mail that lists your PTP access code. Soon after you purchase the Kindle eBook, Amazon should send an e-mail. However, the e-mail uses very generic text, and makes no specific mention of PTP or practice exams. To find your code, read every e-mail from Amazon after you purchase the book. Also do the usual checks for ensuring your e-mail arrives, like checking your spam folder.

NOTE Other eBook customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their eBook editions of this book.

Customizing Your Exams

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

- **Study mode:** Enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting 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 do, so you should not use it if you are trying to 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.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all test banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of 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 while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many 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 click 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 Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Credits

Cover image: New Africa/Shutterstock

Chapter opener image: Charlie Edwards/Photodisc/Getty Images

Figure 3-1 © Greenbone Networks GmbH

Figure 3-2 © Greenbone Networks GmbH

Figure 3-3 © 2020 Tenable, Inc

Figure 3-4 © 2020 Tenable, Inc

Figure 3-5 © 2020 Tenable, Inc

Figure 4-1 © Sarosys LLC 2010-2017

Figure 4-4 © Greenbone Networks GmbH

Figure 4-5 © Greenbone Networks GmbH

Quote, “the process of analyzing a subject system to identify the system’s components and their interrelationships, and to create representations of the system in another form or at a higher level of abstraction” © Institute of Electrical and Electronics Engineers (IEEE)

Figure 4-7 © Insecure.Com LLC

Figure 4-8 © Insecure.Com LLC

Figure 4-9 © Insecure.Com LLC

Figure 4-10 © Insecure.Com LLC

Figure 4-12 © 2020 KSEC

Figure 4-13 © 2009-2020 Aircrack-ng

Figure 4-14 © hashcat

Figure 4-15 © 2020 HACKING LAND

Figure 5-5 © U.S. Department of Health and Human Services

Figure 11-1 © 2020 Zoho Corp

Figure 11-5 © Microsoft 2020

Figure 11-8 © 2020 SolarWinds Worldwide, LLC

Figure 11-9 © Microsoft 2020

Figure 11-10 © 2020 SolarWinds Worldwide, LLC

Figure 11-11 © Microsoft 2020

Figure 11-13 © 2020 Cloudflare, Inc

Figure 11-14 © Microsoft 2020

Figure 11-15 © 2004-2018 Zentyal S.L.

Figure 11-17 © 1992-2020 Cisco

Figure 11-18 © 1992-2020 Cisco

Figure 11-19 © 2020 Apple Inc

Figure 11-20 © 2020 AT&T CYBERSECURITY

Figure 11-21 © 2005-2020 Splunk Inc.

Figure 13-3 © Microsoft 2020

Figure 13-4 © Microsoft 2020

Figure 17-1 © 2004-2020 Rob Dawson

Figure 17-4 © Microsoft 2020

Figure 17-5 © Microsoft 2020

Figure 18-1 © wireshark

Figure 18-2 © wireshark

Figure 18-3 © wireshark

Figure 18-4 © 2001-2014 Massimiliano Montoro

Figure 18-7 © Microsoft 2020

Figure 19-1 courtesy of Wikipedia

Threats and Vulnerabilities Associated with Operating in the Cloud

Placing resources in a cloud environment has many benefits, but also introduces a host of new security considerations. This chapter discusses these vulnerabilities and some measures that you can take to mitigate them.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these eight self-assessment questions, you might want to skip ahead to the “Exam Preparation Tasks” section. Table 6-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A.

Table 6-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

| Foundation Topics Section | Question |
|--|-----------------|
| Cloud Deployment Models | 1 |
| Cloud Service Models | 2 |
| Function as a Service (FaaS)/Serverless Architecture | 3 |
| Infrastructure as Code (IaC) | 4 |
| Insecure Application Programming Interface (API) | 5 |
| Improper Key Management | 6 |
| Unprotected Storage | 7 |
| Logging and Monitoring | 8 |

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 the 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. In which cloud deployment model does an organization provide and manage some resources in-house and has other resources provided externally via a public cloud?
 - a. Private
 - b. Public
 - c. Community
 - d. Hybrid

2. Which of the following cloud service models is typically used as a software development environment?
 - a. SaaS
 - b. PaaS
 - c. IaaS
 - d. FaaS

3. Which of the following is an extension of the PaaS model?
 - a. FaaS
 - b. IaC
 - c. SaaS
 - d. IaaS

4. Which of the following manages and provisions computer data centers through machine-readable definition files?
 - a. IaC
 - b. PaaS
 - c. SaaS
 - d. IaaS

5. Which of the following can enhance security of APIs?
 - a. DPAPI
 - b. SGX
 - c. SOAP
 - d. REST

6. Which of the following contains recommendations for key management?
 - a. NIST SP 800-57 REV. 5
 - b. PCI-DSS
 - c. OWASP
 - d. FIPS

7. Which of the following is the most exposed part of a cloud deployment?
 - a. Cryptographic functions
 - b. APIs
 - c. VMs
 - d. Containers

8. Which of the following is lost with improper auditing? (Choose the best answer.)
 - a. Cryptographic security
 - b. Accountability
 - c. Data security
 - d. Visibility

Foundation Topics

Cloud Deployment Models

Cloud computing is all the rage these days, and it comes in many forms. The basic idea of cloud computing is to make resources available in a web-based data center so the resources can be accessed from anywhere. When a company pays another company to host and manage this type of environment, it is considered to be a public cloud solution. If the company hosts this environment itself, it is considered to be a private cloud solution. The different cloud deployment models are as follows:

Key Topic

- **Public:** A *public cloud* is the standard cloud deployment model, in which a service provider makes resources available to the public over the Internet. Public cloud services may be free or may be offered on a pay-per-use model. An organization needs to have a business or technical liaison responsible for managing the vendor relationship but does not necessarily need a specialist in cloud deployment. Vendors of public cloud solutions include Amazon, IBM, Google, Microsoft, and many more. In a public cloud deployment model, subscribers can add and remove resources as needed, based on their subscription.
- **Private:** A *private cloud* is a cloud deployment model in which a private organization implements a cloud in its internal enterprise, and that cloud is used by the organization's employees and partners. Private cloud services require an organization to employ a specialist in cloud deployment to manage the private cloud.
- **Community:** A *community cloud* is a cloud deployment model in which the cloud infrastructure is shared among several organizations from a specific group with common computing needs. In this model, agreements should explicitly define the security controls that will be in place to protect the data of each organization involved in the community cloud and how the cloud will be administered and managed.
- **Hybrid:** A *hybrid cloud* is a cloud deployment model in which an organization provides and manages some resources in-house and has others provided externally via a public cloud. This model requires a relationship with the service provider as well as an in-house cloud deployment specialist. Rules need to be defined to ensure that a hybrid cloud is deployed properly. Confidential and private information should be limited to the private cloud.

Cloud Service Models

There is trade-off to consider when a decision must be made between cloud architectures. A private solution provides the most control over the safety of your data but also requires the staff and the knowledge to deploy, manage, and secure the solution. A public cloud puts your data's safety in the hands of a third party, but that party is more capable and knowledgeable about protecting data in such an environment and managing the cloud environment. With a public solution, various cloud service models can be purchased. Some of these models include the following:

Key Topic

- **Software as a Service (SaaS):** With SaaS, the vendor provides the entire solution, including the operating system, the infrastructure software, and the application. The vendor may provide an email system, for example, in which it hosts and manages everything for the customer. An example of this is a company that contracts to use Salesforce or Intuit QuickBooks using a browser rather than installing the application on every machine. This frees the customer company from performing updates and other maintenance of the applications.
- **Platform as a Service (PaaS):** With PaaS, the vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software. The customer is still involved in managing the system. An example of this is a company that engages a third party to provide a development platform for internal developers to use for development and testing.
- **Infrastructure as a Service (IaaS):** With IaaS, the vendor provides the hardware platform or data center, and the customer installs and manages its own operating systems and application systems. The vendor simply provides access to the data center and maintains that access. An example of this is a company hosting all its web servers with a third party that provides the infrastructure. With IaaS, customers can benefit from the dynamic allocation of additional resources in times of high activity, while those same resources are scaled back when not needed, which saves money.

Figure 6-1 illustrates the relationship of these services to one another.

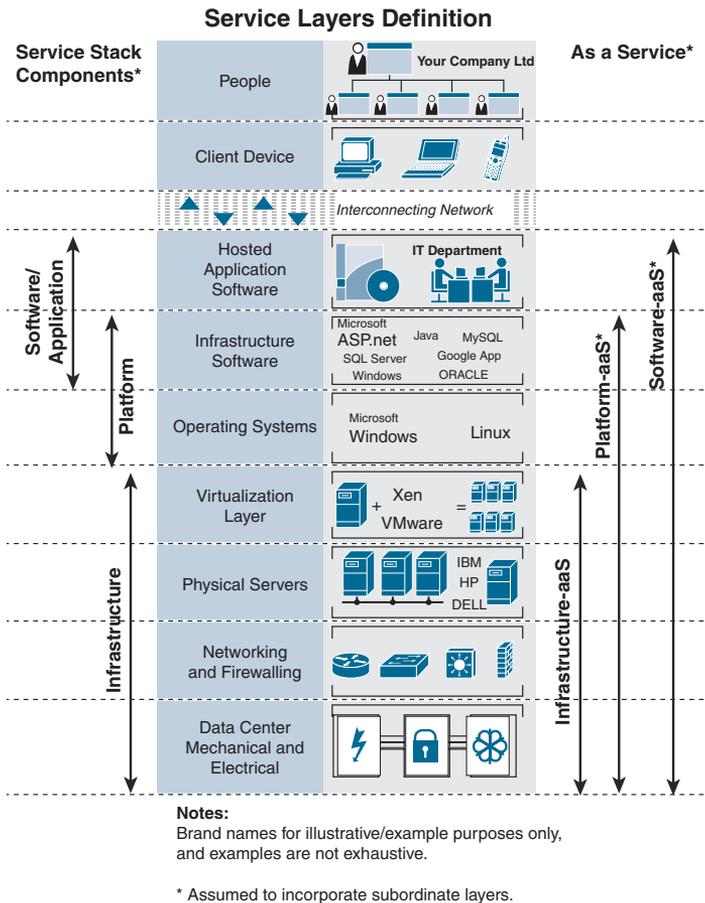


FIGURE 6-1 Cloud Service Models

Function as a Service (FaaS)/Serverless Architecture

Function as a Service (FaaS) is an extension of PaaS that goes further and completely abstracts the virtual server from the developers. In fact, charges are based not on server instance sizes but on consumption and executions. This is why it is sometimes also called *serverless architecture*. In this architecture, the focus is on a function, operation, or piece of code that is executed as a function. These services are event-driven in nature.

Although FaaS is not perfect for every workload, for transactions that happen hundreds of times per second, there is a lot of value in isolating that logic to a function that can be scaled. Additional advantages include the following:

Key Topic

- **Ideal for dynamic or burstable workloads:** If you run something only once a day or month, there's no need to pay for a server 24/7/365.
- **Ideal for scheduled tasks:** FaaS is a perfect way to run a certain piece of code on a schedule.

Figure 6-2 shows a useful car analogy for comparing traditional computing (own a car), cloud computing (rent a car), and FaaS/serverless computing (car sharing). VPS in the rent-a-car analogy stands for virtual private server and refers to provisioning a virtual server from a cloud service provider.

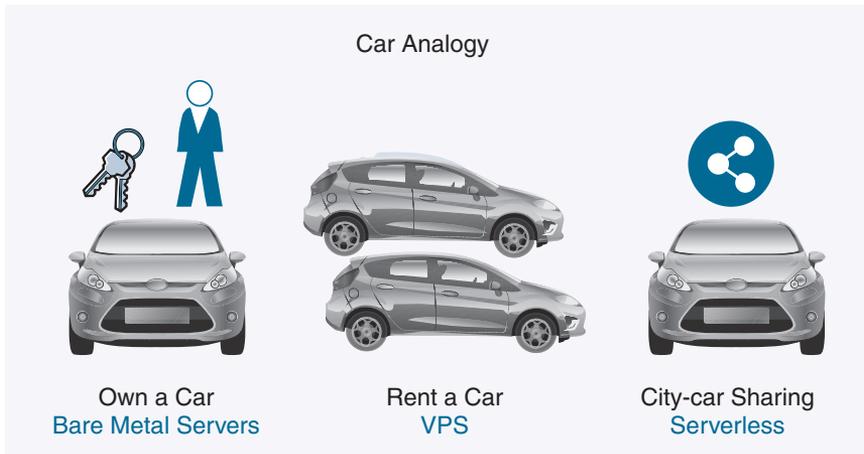


FIGURE 6-2 Car Analogy for Serverless Computing

The following are top security issues with serverless computing:

Key Topic

- **Function event data injection:** Triggered through untrusted input such as through a web API call
- **Broken authentication:** Coding issues ripe for exploit and attacks, which lead to unauthorized authentication
- **Insecure serverless deployment configuration:** Human error in setup
- **Over-privileged function permissions and roles:** Failure to implement the least privilege concept

Infrastructure as Code (IaC)

In another reordering of the way data centers are handled, *Infrastructure as Code (IaC)* manages and provisions computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. IaC can use either scripts or declarative definitions, rather than manual processes, but the term more often is used to promote declarative approaches.

Naturally, there are advantages to this approach:

Key Topic

- Lower cost
- Faster speed
- Risk reduction (remove errors and security violations)

Figure 6-3 illustrates an example of how some code might be capable of making changes on its own without manual intervention. As you can see in Figure 6-3, these code changes can be made to the actual state of the configurations in the cloud without manual intervention.



FIGURE 6-3 IaC in Action

Security issues with Infrastructure as Code (IaC) include

Key Topic

- **Compliance violations:** Policy guardrails based on standards are not enforced
- **Data exposures:** Lack of encryption
- **Hardcoded secrets:** Storing plain text credentials, such as SSH keys or account secrets, within source code
- **Disabled audit logs:** Failure to utilize audit logging services like AWS CloudTrail and Amazon CloudWatch
- **Untrusted image sources:** Templates may inadvertently refer to OS or container images from untrusted sources

Insecure Application Programming Interface (API)

Interfaces and APIs tend to be the most exposed parts of a system because they're usually accessible from the open Internet. APIs are used extensively in cloud environments. With respect to APIs, a host of approaches—including Simple Object Access Protocol (SOAP), REpresentational State Transfer (REST), and JavaScript Object Notation (JSON)—are available, and many enterprises find themselves using all of them.

The use of diverse protocols and APIs is also a challenge to interoperability. With networking, storage, and authentication protocols, support and understanding of the protocols in use is required of both endpoints. It should be a goal to reduce the number of protocols in use in order to reduce the attack surface. Each protocol has its own history of weaknesses to mitigate.

One API that can enhance cloud security is the *Data Protection API (DPAPI)* offered by Windows. Let's look at what it offers. Among other features, DPAPI supports in-memory processing, an approach in which all data in a set is processed from memory rather than from the hard drive. In-memory processing assumes that all the data is available in memory rather than just the most recently used data, as is usually the case when using RAM or cache memory. This results in faster reporting and decision making in business. Securing in-memory processing requires encrypting the data in RAM. DPAPI lets you encrypt data using the user's login credentials. One of the key questions is where to store the key, because storing it in the same location as the data typically is not a good idea (the next section discusses key management). Intel's Software Guard Extensions (SGX), shipping with Skylake and newer CPUs, allows you to load a program into your processor, verify that its state is correct (remotely), and protect its execution. The CPU automatically encrypts everything leaving the processor (that is, everything that is offloaded to RAM) and thereby ensures security.

Even the most secure devices have some sort of API that is used to perform tasks. Unfortunately, untrustworthy people use those same APIs to perform unscrupulous tasks. APIs are used in the Internet of Things (IoT) so that devices can speak to each other without users even knowing they are there. APIs are used to control and monitor things we use every day, including fitness bands, home thermostats, lighting, and automobiles. Comprehensive security must protect the entire spectrum of devices in the digital workplace, including apps and APIs. API security is critical for an organization that is exposing digital assets.

Guidelines for providing API security include the following:

- Use the same security controls for APIs as for any web application in the enterprise.
- Use Hash-based Message Authentication Code (HMAC).
- Use encryption when passing static keys.



- Use a framework or an existing library to implement security solutions for APIs.
- Implement password encryption instead of single key-based authentication.

Improper Key Management

Key management is essential to ensure that the cryptography provides confidentiality, integrity, and authentication in cloud environments. If a key is compromised, it can have serious consequences throughout an organization.

Key management involves the entire process of ensuring that keys are protected during creation, distribution, transmission, and storage. As part of this process, keys must also be destroyed properly. When you consider the vast number of networks over which the key is transmitted and the different types of systems on which a key is stored, the enormity of this issue really comes to light.

As the most demanding and critical aspect of cryptography, it is important that security professionals understand key management principles.

Keys should always be stored in ciphertext when stored on a noncryptographic device. Key distribution, storage, and maintenance should be automatic by integrating the processes into the application.

Because keys can be lost, backup copies should be made and stored in a secure location. A designated individual should have control of the backup copies, and other individuals should be designated to serve as emergency backups. The key recovery process should also require more than one operator, to ensure that only valid key recovery requests are completed. In some cases, keys are even broken into parts and deposited with trusted agents, who provide their part of the key to a central authority when authorized to do so. Although other methods of distributing parts of a key are used, all the solutions involve the use of trustee agents entrusted with part of the key and a central authority tasked with assembling the key from its parts. Also, key recovery personnel should span across the entire organization and not just be members of the IT department.

Organizations should also limit the number of keys that are used. The more keys that you have, the more keys you must ensure are protected. Although a valid reason for issuing a key should never be ignored, limiting the number of keys issued and used reduces the potential damage.

When designing the key management process, you should consider how to do the following:

- Securely store and transmit the keys
- Use random keys



- Issue keys of sufficient length to ensure protection
- Properly destroy keys when no longer needed
- Back up the keys to ensure that they can be recovered

Systems that process valuable information require controls in order to protect the information from unauthorized disclosure and modification. Cryptographic systems that contain keys and other cryptographic information are especially critical. Security professionals should work to ensure that the protection of keying material provides accountability, audit, and survivability.

Accountability involves the identification of entities that have access to, or control of, cryptographic keys throughout their life cycles. Accountability can be an effective tool to help prevent key compromises and to reduce the impact of compromises when they are detected. Although it is preferred that no humans be able to view keys, as a minimum, the key management system should account for all individuals who are able to view plaintext cryptographic keys. In addition, more sophisticated key management systems may account for all individuals authorized to access or control any cryptographic keys, whether in plaintext or ciphertext form.

Two types of audits should be performed on key management systems:

Key Topic

- **Security:** The security plan and the procedures that are developed to support the plan should be periodically audited to ensure that they continue to support the key management policy.
- **Protective:** The protective mechanisms employed should be periodically reassessed with respect to the level of security they currently provide and are expected to provide in the future. They should also be assessed to determine whether the mechanisms correctly and effectively support the appropriate policies. New technology developments and attacks should be considered as part of a protective audit.

Key management survivability entails backing up or archiving copies of all keys used. Key backup and recovery procedures must be established to ensure that keys are not lost. System redundancy and contingency planning should also be properly assessed to ensure that all the systems involved in key management are fault tolerant.

Key Escrow

Key escrow is the process of storing keys with a third party to ensure that decryption can occur. This is most often used to collect evidence during investigations. Key recovery is the process whereby a key is archived in a safe place by the administrator.

Key Stretching

Key stretching, also referred to as key strengthening, is a cryptographic technique that involves making a weak key stronger by increasing the time it takes to test each possible key. In key stretching, the original key is fed into an algorithm to produce an enhanced key, which should be at least 128 bits for effectiveness. If key stretching is used, an attacker would need to either try every possible combination of the enhanced key or try likely combinations of the initial key. Key stretching slows down the attacker because the attacker must compute the stretching function for every guess in the attack. Systems that use key stretching include Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Wi-Fi Protected Access (WPA), and WPA2. Widely used password key-stretching algorithms include Password-Based Key Derivation Function 2 (PBKDF2), bcrypt, and scrypt.

Unprotected Storage

While cloud storage may seem like a great idea, it presents many unique issues. Among them are the following:

Key Topic

- **Data breaches:** Although cloud providers may include safeguards in service-level agreements (SLAs), ultimately the organization is responsible for protecting its own data, regardless of where it is located. When this data is not in your hands—and you may not even know where it is physically located at any point in time—protecting your data is difficult.
- **Authentication system failures:** These failures allow malicious individuals into the cloud. This issue sometimes is made worse by the organization itself when developers embed credentials and cryptographic keys in source code and leave them in public-facing repositories.
- **Weak interfaces and APIs:** Interfaces and APIs tend to be the most exposed parts of a system because they're usually accessible from the open Internet.

Transfer/Back Up Data to Uncontrolled Storage

In some cases, users store sensitive data in cloud storage that is outside the control of the organization, using sites such as Dropbox. These storage providers have had their share of data loss issues as well. Policies should address and forbid this type of storage of data from mobile devices.

Cloud services give end users more accessibility to their data. However, this also means that end users can take advantage of cloud storage to access and share company data from any location. At that point, the IT team no longer controls the data. This is the case with both public and private clouds.



With private clouds, organizations can ensure the following:

- That the data is stored only on internal resources
- That the data is owned by the organization
- That only authorized individuals are allowed to access the data
- That data is always available

However, a private cloud is only protected by the organization's internal resources, and this protection can often be affected by the knowledge level of the security professionals responsible for managing the cloud security.

With public clouds, organizations can ensure the following:

- That data is protected by enterprise-class firewalls and within a secured facility
- That attackers and disgruntled employees are unsure of where the data actually resides
- That the cloud vendor provides security expertise and maintains the level of service detailed in the contract

However, public clouds can grant access to any location, and data is transmitted over the Internet. Also, the organization depends on the vendor for all services provided. End users must be educated about cloud usage and limitations as part of their security awareness training. In addition, security policies should clearly state where data can be stored, and ACLs should be configured properly to ensure that only authorized personnel can access data. The policies should also spell out consequences for storing organizational data in cloud locations that are not authorized.

Big Data

Big data is a term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications. These data sets are often stored in the cloud to take advantage of the immense processing power available there. Specialized applications have been designed to help organizations with their big data. The big data challenges that may be encountered include data analysis, data capture, data search, data sharing, data storage, and data privacy.

While big data is used to determine the causes of failures, generate coupons at checkout, recalculate risk portfolios, and find fraudulent activity before it ever has a chance to affect the organization, its existence creates security issues. The first issue is its unstructured nature. Traditional data warehouses process structured data and can store large amounts of it, but there is still a requirement for structure.

Big data typically uses Hadoop, which requires no structure. Hadoop is an open source framework used for running applications and storing data. With the Hadoop Distributed File System, individual servers that are working in a cluster can fail without aborting the entire computation process. There are no restrictions on the data that this system can store. While big data is enticing because of the advantages it offers, it presents a number of issues when deployed in the cloud.

**Key
Topic**

- Organizations still do not understand it very well, and unexpected vulnerabilities can easily be introduced.
- Open source codes are typically found in big data, which can result in unrecognized backdoors. It can contain default credentials.
- Attack surfaces of the nodes may not have been reviewed, and servers may not have been hardened sufficiently.

Logging and Monitoring

Without proper auditing, you have no accountability. You also have no way of knowing what is going on in your environment. While the next two chapters include ample discussion of logging and monitoring and its application, this section briefly addresses the topic with respect to cloud environments.

Insufficient Logging and Monitoring

Unfortunately, although most technicians agree with and support the notion that proper auditing is necessary, in the case of cloud deployments, the logging and monitoring can leave much to be desired. “Insufficient Logging and Monitoring” is one of the categories in the Open Web Application Security Project’s (OWASP) Top 10 list and covers the list of best practices that should be in place to prevent or limit the damage of security breaches.

Security professionals should work to ensure that cloud SLAs include access to logging and monitoring tools that give the organization visibility into the cloud system in which their data is held.

Inability to Access

One of the issue with utilizing standard logging and monitoring tools in a cloud environment is the inability to access the environment in a way that renders visibility into the environment. In some cases, the vendor will resist allowing access to its environment. The time to demand such access is when the SLA is in the process of being negotiated.

Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have several choices for exam preparation: the exercises here, Chapter 22, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 6-2 lists a reference of these key topics and the page numbers on which each is found.



Table 6-2 Key Topics in Chapter 6

| Key Topic Element | Description | Page Number |
|-------------------|---|-------------|
| Bulleted list | Cloud deployment models | 126 |
| Bulleted list | Cloud service models | 127 |
| Bulleted list | Advantages of FaaS | 129 |
| Bulleted list | Top security issues with serverless computing | 129 |
| Bulleted list | Advantages of IaC | 130 |
| Bulleted list | Security issues with Infrastructure as Code (IaC) | 130 |
| Bulleted list | Guidelines for providing API security | 131 |
| Bulleted list | Designing the key management process | 132 |
| Bulleted list | Types of audit that should be performed on key management systems | 133 |
| Bulleted list | Security issues with cloud storage | 134 |
| Bulleted list | Capabilities with private and public clouds | 135 |
| Bulleted list | Issues with big data | 136 |

Define Key Terms

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

Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), public cloud, private cloud, community cloud, hybrid cloud, Function as a Service (FaaS), Infrastructure as Code (IaC), Data Protection API (DPAPI), NIST SP 800-57 REV. 5, key escrow, key stretching, big data

Review Questions

1. With _____, the vendor provides the entire solution, including the operating system, the infrastructure software, and the application.
2. Match the terms on the left with their definitions on the right.

| Terms | Definitions |
|-------|---|
| FaaS | Manages and provisions computer data centers through machine-readable definition files. |
| IaC | The vendor provides the hardware platform or data center, and the customer installs and manages its own operating systems and application systems. |
| PaaS | The vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software. |
| IaaS | Completely abstracts the virtual server from the developers. |

3. List at least one advantage of IaC.
4. _____ tend to be the most exposed parts of a cloud system because they're usually accessible from the open Internet.
5. APIs are used in the _____ so that devices can speak to each other without users even knowing the APIs are there.
6. List at least one of the security issues with serverless computing in the cloud.
7. Match the key state on the left with its definition on the right.

| Terms | Definitions |
|----------------------|---|
| Pre-activation state | Temporarily inactive |
| Suspended state | Keys may be used to cryptographically protect information |
| Deactivated state | Discovered by an unauthorized entity |
| Active state | Key has been generated but has not been authorized for use |
| Compromised state | Keys are not used to apply cryptographic protection, but in some cases, they may be used to process cryptographically protected information |

8. In the _____ phase of a key, the keying material is not yet available for normal cryptographic operations.
9. List at least one security issue with cloud storage.
10. _____ is a term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications.

Index

Numbers

3DES, 235

802.1X, 389–391, 653

A

A (Availability) metric, 27, 656

AACS (Advanced Access Content System), 520, 653

ABAC (attribute-based access control), 143, 225–227, 655

AC (Attack Complexity) metric, 26, 481

acceptable use policy (AUP), 563–564, 572, 653

acceptance of risk, 47, 538, 677

access control lists (ACLs), 12, 47, 182, 458, 510

access control provisioning life cycle, 569

access management. *See* identity and access management

access points, rogue, 336, 475, 678

accounts

introduction of, 334, 480

maintenance of, 260

management policy for, 568–569

privileged, 211

accreditation, 270, 653, 681, 683, 685

accuracy, 282, 653

ACK flag, 76

ACLs (access control lists), 12, 47, 182, 458, 510

action factor authentication, 212

Active Cyber Defense Cycle, 246–247

active defense, 246–247, 653

Active Directory (AD), 217–218, 653

active enumeration, 82, 653

active reader/active tag (ARAT), 180

active reader/passive tag (ARPT), 180

active scans, 43–44

active vulnerability scanners (AVSs), 43, 653

ActiveX, 323, 337

AD (Active Directory), 217–218, 653

Adaptive Wireless IPS, 475

addresses, MAC (media access control), 155

limiting, 394

sticky MAC, 394, 682

AddressSanitizer, 332, 493

ADEPT (Adobe Digital Experience Protection Technology), 521

administrative controls, 508, 570. *See also individual controls*

Adobe Digital Experience Protection Technology (ADEPT), 521

Advanced Access Content System (AACS), 520, 653

advanced persistent threats (APT), 11, 653

adversary capability, 29–30

adware, 325, 681

AEG (automatic exploit generation), 427

AES 128/256-bit encryption, 99, 235

AGCC (Aviation Government Coordinating Council), 15

- agent-based scans, 52
 - agent-based SIEM collection, 362
 - agentless SIEM collection, 362
 - aggregation, 340, 654
 - AH (Authentication Header), 197, 655
 - AI (artificial intelligence), 426–427
 - AIK (attestation identity key), 300
 - air gap, 185, 654
 - Aircrack-ng, 83, 654
 - AirDefense, 475
 - AirMagnet Enterprise, 475
 - airodump-ng command, 83
 - AirTight WIPS, 475
 - Akana, 392
 - ALE (annual loss expectancy), 535, 654
 - algorithms
 - asymmetric, 236, 655
 - DGA (domain generation algorithm), 343, 662
 - Diffie-Hellman, 198, 236
 - DSA (Digital Security Algorithm), 246
 - MD (Message Digest), 239–240
 - SHA (Secure Hash Algorithm), 240, 499
 - symmetric, 233–236, 682
 - block ciphers, 235–236, 656
 - stream-based ciphers, 234–235, 682
 - Alibaba Cloud, 87
 - AlienVault, 365
 - Amazon Kindle, 521
 - Amazon Payments, 102
 - Amazon Web Services (AWS), 87
 - Android
 - Device Manager, 257
 - fragmentation, 101
 - Lost Android app, 257
 - annual loss expectancy (ALE), 535, 654
 - annualized rate of occurrence (ARO), 535, 654
 - Anomali ThreatStream, 426
 - anomalous behavior/anomaly analysis, 24–25, 334–335, 480
 - anomaly-based IDSs, 57
 - anti-malware, 322, 328
 - anti-tamper technology, 308, 654
 - Apache Log Viewer, 394
 - APIs (application programming interfaces)
 - in cloud environments, 131–132
 - integration of, 424, 654
 - Apktool, 328
 - Apple
 - Apple Pay, 101
 - Configurator, 98
 - Find My iPhone, 257
 - Application log, 481, 654
 - application programming interfaces. *See* APIs (application programming interfaces)
 - application-based IDSs, 58
 - application-level proxies, 60, 385
 - application-related IOCs (indicators of compromise), 480–481
 - anomalous activity, 480
 - Application log, 481, 654
 - introduction of new accounts, 480
 - service interruption, 481
 - unexpected outbound communication, 481
 - unexpected output, 480
 - applications. *See also* software assurance behavior, 333–339
 - anomalous behavior, 334–335
 - known-good behavior, 333–334
 - logs, 481
 - streaming, 208
 - system, 98
 - unsigned, 98
 - vetting process, 258–259
 - wrapping, 257, 654
- APs (access points), 336, 475
 - APTs (advanced persistent threats), 11, 653
 - Arachni, 70–496, 654

- architecture. *See* network architecture
- ArcSight, 364
- ARMIS security firm, 105
- ARO (annualized rate of occurrence), 535, 654
- ARP spoofing, 154
- ARPT (active reader/passive tag), 180
- artificial intelligence (AI), 426–427
- assessments, 683. *See also* scans/sweeps
- compliance, 575
 - definition of, 573
 - regulatory, 573–574
 - risk, 532–534
 - definition of, 677
 - goals of, 532–533
 - metrics, 533
 - qualitative risk analysis, 534, 676
 - quantitative risk analysis, 534, 676
 - risk assessment matrix, 537–538
 - software, 72–76, 272–275
 - code review, 273–274, 275
 - dynamic analysis, 74, 286
 - fuzzing, 75–76
 - reverse engineering, 75
 - SDLC (software development life cycle), 72–76
 - security regression, 273
 - security testing, 274–275
 - static analysis, 73–74, 286
 - stress testing, 272–273
 - user acceptance testing, 272
- asset management, 178–180
- asset tagging, 178, 654
 - critical assets, 42–43, 411–412, 456, 531, 654
 - data classification policy, 411
 - sensitivity and criticality, 411
 - device-tracking technologies, 178–179
 - high value assets, 441
 - object-tracking and object-containment technologies, 179–180
- asset value (AV), 534, 654
- asymmetric algorithms, 236, 655
- AT&T Cybersecurity, 365
- atomic execution, 260, 307, 655
- Attack Complexity (AC) metric, 26, 653
- attack frameworks
 - definition of, 21, 655
 - Diamond Model of Intrusion Analysis, 22–23, 661
 - kill chain, 23, 669
 - MITRE ATT&CK, 21–22, 670
- attack surface area, reduction of, 409–410
 - configuration lockdown, 410, 659
 - system hardening, 410
- attack vector (AV), 26, 31–32, 412–413, 653, 655
- attacks. *See also* threat classification; threat intelligence
- backdoors/trapdoors, 338, 656
 - buffer overflow, 337
 - credential stuffing, 152–154, 660
 - DDoS (distributed denial-of-service) attacks, 337, 472
 - directory traversal, 151–152, 661
 - DoS (denial-of-service), 183, 337, 472, 661
 - dumpster diving, 336
 - emanations, 337
 - file system
 - file integrity monitoring, 340–341
 - terminology for, 339–340
 - identity theft, 336
 - impersonation, 154, 666
 - malware. *See* malware
 - man-in-the-middle, 154–155, 205, 669
 - mobile code, 337
 - overflow, 147–150
 - buffer, 147–149, 656
 - definition of, 672
 - heap, 150, 665
 - integer, 149–150, 667
 - password spraying, 152, 673
 - phishing/pharming, 335, 369–370, 674

- privilege escalation, 152
- remote code execution, 150, 677
- rogue access points, 336, 678
- rogue endpoints, 336
- rootkit, 159–160, 678
- servers, 337–338
- services, 338–339
- session hijacking, 158, 681
- shoulder surfing, 336
- social engineering, 335–336
- SQL injection, 145–146, 682
- SYN flood, 490
- time-of-check/time-of-use, 260, 684
- virtualization, 203–206
- VLAN-based, 156–158
- XML (Extensible Markup Language), 143–144, 663
- XSS (cross-site scripting), 160–162
 - definition of, 660
 - DOM (document object model), 162, 662
 - example of, 160–161
 - persistent, 161, 673
 - reflective, 161, 677
- attestation
 - AIK (attestation identity key), 300
 - definition of, 655
 - measured boot and, 310–311, 670
- attribute-based access control (ABAC), 143, 225–227, 655
- audits
 - audit reduction tools, 231
 - compliance, 575
 - definition of, 573
 - regulatory, 573–574
- AUP (acceptable use policy), 563–564, 572, 653
- authentication, 277–285
 - authentication period, 566, 655
 - biometric considerations, 282–284
 - certificate-based, 284–285
 - context-based, 277–279
 - IEEE 802.1X, 281–282
 - MFA (multifactor authentication), 211–214
 - authentication factors, 212
 - characteristic factors, 212, 214, 657
 - definition of, 670
 - identification versus authentication, 211–212
 - knowledge factors, 212, 213, 669
 - ownership factors, 212, 213, 672
 - network authentication protocols, 279–280
 - vulnerabilities in, 164
- Authentication Header (AH), 197, 655
- authentication servers, 281, 655
 - 802.1X, 389
 - RADIUS (Remote Authentication Dial-in User Service), 389–391
 - TACACS+ (Terminal Access Controller Access Control System Plus), 389–391
- authenticators, 281, 389, 655
- authenticity, hardware, 544
- authorization, 233
- automated malware signature creation, 424, 655
- automated static analysis engine, 328
- automatic exploit generation (AEG), 427
- automation, 104. *See also* IoT (Internet of Things)
 - AI (artificial intelligence), 426–427
 - API integration, 424, 654
 - automated malware signature creation, 424, 655
 - data enrichment, 425, 660
 - machine learning, 426–427, 669
 - scripting, 423
 - standards and protocols
 - continuous deployment/delivery, 428, 659
 - continuous integration, 428, 659
 - SCAP (Security Content Automation Protocol), 44, 49, 426–427

- threat feed, 426, 683
- workflow orchestration, 422–423, 687
- automation systems
 - building, 109
 - threats to, 113
- AV (asset value), 534, 654
- AV (attack vector), 26, 31–32, 412–413, 653, 655
- availability, 27, 510, 656
- Aviation Government Coordinating Council (AGCC), 15
- aviation sector, data sharing in, 15
- avoidance of risk, 47, 538, 678
- AVSs (active vulnerability scanners), 43, 653
- AWS (Amazon Web Services), 87
- AWStats, 394
- AXELOS, 561
- Azure, 87

B

- backdoors, 338, 656
- BACnet (Building Automation and Control Networks), 111, 117, 656
- bandwidth consumption, 472
- BandwidthD, 472
- Barnes and Nobles Nook, 521
- BAS (building automation systems), 109
- Base metric group (CVSS), 26–27
- Basel II, 513, 656
- baselines, 45–46, 333, 659
- bash, 423, 656
- bastion hosts, 61, 188–189, 656
- BCP (Business Continuity Planning) committees, 531, 657
- bcrypt, 134
- beaconing, 473, 656
- behavior. *See* system behavior
- behavioral analysis, 24–25
- benchmarks, 333
- BIA (business impact analysis), 530–532
 - critical processes and resources, 531
 - definition of, 657
 - outage impact and downtime, 531
 - recovery priorities, 531–532
 - resource requirements, 531
- big data, 135–136, 656
- binary files, changes to, 500
- Binary Guard True Bare Metal, 393
- binding, 299
- biometric technologies, 282–284
- BIOS, flashing, 309
- BitBlaze Malware Analysis Service, 393
- BitLocker/BitLocker to Go, 300
- BitMeter OS, 472
- black hats, 406
- black-box testing, 274–275
- blacklisting, 275, 381, 656
- blind signatures, 245
- block ciphers, 235–236, 656
- Blowfish, 235
- blue teams, 542, 656
- Bluetooth hacking gear, 475
- boot sector viruses, 324
- booting, secure, 265, 303, 310–311
- botnets, 325, 473–474, 656
- bridging, domain, 103–104, 662
- bring your own device (BYOD) policies, 97–98, 656
- British Standard 7799 (BS7799), 556
- broken authentication, 164
- buffer overflow, 147–149, 337, 656
- Building Automation and Control Networks (BACnet), 111, 117, 656
- building automation systems (BAS), 109
- Burp Suite, 69, 656
- buses
 - CAN (Controller Area Network), 112, 659
 - encryption, 311, 656
- business classifications, 412
- Business Continuity Planning (BCP) committees, 531, 657

- business impact analysis. *See* BIA (business impact analysis)
- business process interruption, 62, 539
- BYOD (bring your own device) policies, 97–98, 656
- C**
- C (Confidentiality) metric, 27, 659
- CA (certificate authority), 243, 258, 285, 371, 657
- /CACHESIZE=X switch (SFC), 341
- Cain and Abel, 491, 657
- calculation of risk, 534–535
- calculators, CVSS (Common Vulnerability Scoring System), 29
- CALEA (Communications Assistance for Law Enforcement Act), 512, 658
- call lists, 454, 657
- CAM (content-addressable memory), 155
- CAN (Controller Area Network) bus, 112, 659
- CAP (Cyber Intelligence Analytics Platform) v2.0, 6
- Capability Maturity Model Integration (CMMI), 561, 657
- CAPTCHA passwords, 154, 565
- Carbon Black CB Response, 387
- cars, smart, 104. *See also* IoT (Internet of Things)
- carving, 500, 657
- CASB (cloud access security broker), 229, 657
- cat command, 367
- categories
 - definition of, 570
 - managerial, 570
 - operational, 571
 - technical, 571
- cause-and-effect rules, 363
- CCE (Common Configuration Enumeration), 427, 658
- CCTV (closed-circuit television), 107–108
- Cellebrite, 494, 657
- Center for Internet Security (CIS), 413
- central security breach response, 265–266
- centralized VDI model, 207
- CER (crossover error rate), 283
- certificate authority (CA), 657
- certificate management, 242–246
 - CA (certificate authority), 243, 258, 285, 371, 657
- certificate-based authentication, 284–285
- CRLs (certificate revocation lists), 244, 657
- cross-certification, 245
- digital signatures, 245–246, 661
- OSCP (Online Certificate Status Protocol), 244, 672
- PKI (public key infrastructure), 198, 245, 284–285
- RA (registration authority), 243, 677
- Verisign, 244
- X.509 certificates, 243–244
- certification, system/software, 270, 539, 657
- certification exam preparation. *See* exam preparation process
- CFAA (Computer Fraud and Abuse Act), 511, 658
- chain of custody, 498
- Challenge Handshake Authentication Protocol (CHAP), 279–281
- change management, 201–208, 464, 657
- Channel services, 8–9
- CHAP (Challenge Handshake Authentication Protocol), 279–281
- characteristic factor authentication, 214, 657
- checksums, 237
- CIA (confidentiality, integrity, and availability), 42, 411, 510

- ciphers
 - block, 235–236, 656
 - stream-based, 234–235, 682
- circuit-level proxies, 60, 385
- CIS (Center for Internet Security), 413
- CISA (Cybersecurity and Infrastructure Security Agency), 15
- Cisco Adaptive Wireless IPS, 475
- Cisco Check Point, 353–355
- Cisco Meraki, 98
- Cisco Systems Manager, 98
- Cisco Talos IP, 24
- Citrix, 203, 311
- classifications, threat. *See* threat classification
- clearing data, 461, 657
- click-jacking, 262, 657
- client-based application virtualization, 208
- client/server platforms, 263
- closed-circuit television (CCTV), 107–108
- closed-source intelligence, 6
- cloud access security broker (CASB), 229, 657
- cloud computing
 - API security, 131–132
 - big data, 135–136, 656
 - cloud-based scanning, 495–496
 - community cloud, 126, 658
 - deployment models, 126
 - FaaS (Function as a Service), 128–129, 665
 - hybrid cloud, 126, 666
 - IaC (Infrastructure as Code), 130
 - key management, 132–134
 - key escrow, 133
 - key stretching, 134
 - principles of, 132–133
 - logging and monitoring, 136
 - mitigations, 177–178
 - on-premises versus, 177
 - private cloud, 126, 675
 - public cloud, 126, 675
 - service models, 127–128
 - storage threats, 134–135
 - VPC (virtual private cloud), 195, 686
- cloud infrastructure assessment tools, 86–88
 - Pacu, 87–88, 673
 - Prowler, 87, 675
 - ScoutSuite, 87, 679
- CMaaS (Continuous Monitoring as a Service), 414
- CMI (copyright management information), 444
- CMMI (Capability Maturity Model Integration), 561, 657
- COBIT (Control Objectives for Information and Related Technologies), 553, 657
- code of conduct/ethics, 563, 658
- code reuse, 166
- code review, 273–274, 275, 286–287
- coding, secure, 275–285
 - authentication, 277–285
 - authentication period, 566, 655
 - biometric considerations, 282–284
 - certificate-based, 284–285
 - context-based, 277–279
 - definition of, 233, 655
 - IEEE 802.1X, 281–282
 - MFA (multifactor authentication), 211–214
 - network authentication protocols, 279–280
 - vulnerabilities in, 164
 - data protection, 285
 - input validation, 275–276, 382
 - output encoding, 276, 672
 - parameterized queries, 285, 673
 - session management, 276–277
- cognitive passwords, 565, 658
- collection, 8, 13

- combination passwords, 564
- Combine threat feed, 426
- commands
 - aircrack-ng, 83
 - airodump-ng, 83
 - cat, 367
 - dcfldd, 492–493
 - dd, 492–493, 660
 - grep, 366
 - hping, 80–82
 - hping3, 80–82
 - less, 367
 - nmap, 76–79
 - port security mac-address, 394
 - reaver, 84–85
 - SFC, 340–341
 - strncpy, 168, 682
 - switchport mode access, 157
 - switchport mode trunk, 157
 - switchport port security, 394
 - wash, 85–86
- commercial business classifications, 411
- commodity malware, 14, 658
- Common Configuration Enumeration (CCE), 427, 658
- Common Platform Enumeration (CPE), 427, 658
- Common Vulnerabilities and Exposures (CVE), 165, 427, 658
- Common Vulnerability Scoring System (CVSS), 44, 412
- Common Weakness Enumeration (CWE), 44, 427, 658
- communication plans, 435–436, 536–537.
 - See also* response coordination
- Communications Assistance for Law Enforcement Act (CALEA), 512, 658
- community cloud, 126, 658
- Comodo Automated Analysis System and Valkyrie, 393
- companion viruses, 324
- compartmented security mode (MAC), 228
- compensating controls, 47, 658
- complex passwords, 564, 658
- compliance audits/assessments, 575
- components, vulnerabilities in, 165–166
- compromise, indicators of. *See* IOCs (indicators of compromise)
- Computer Fraud and Abuse Act (CFAA), 511, 658
- Computer Security Act, 512, 658
- concentrators, VPN, 196
- conditional access, 257
- conduct, code of, 563, 658
- confidence levels, 7, 659
- confidentiality, 27, 42, 233, 411, 412, 510, 659
- configurations, 377
 - 802.1X, 389–391, 653
 - baselines, 45–46, 659
 - blacklisting, 381
 - development/rule writing, 392
 - DLP (data loss prevention), 386–387, 660
 - EDR (endpoint detection and response), 387, 663
 - firewalls, 59–62, 383
 - architecture of, 61–62
 - comparison of, 385
 - definition of, 383, 664
 - host-based, 384–385, 666
 - NGFWs (next-generation firewalls), 383–384, 671
 - types of, 59–61, 383–385
 - input validation, 382
 - IPS rules, 386
 - lockdown of, 410, 659
 - malware signatures, 391–392
 - NAC (network access control), 387–389, 671
 - permissions, 381, 673
 - port security, 394, 674

- enabling, 394
- MAC addresses, limiting, 394
- sticky MAC, 394, 682
- profiles and payloads for, 256
- sandboxing, 392–394
- sinkholing, 391, 681
- vulnerabilities in, 167–168
- whitelisting, 381
- containerization, 208–209, 256, 659
- containment, 458–459
 - isolation, 459, 668, 683
 - segmentation, 458–459
- contamination, 340, 659
- Content Scrambling System (CSS), 520, 659
- content-addressable memory (CAM), 155
- context-based authentication, 277–279
- continuous deployment/delivery, 428, 659
- continuous improvement, 413–414
- continuous integration, 428, 659
- continuous monitoring, 413–414, 569–570
- Continuous Monitoring as a Service (CMaaS), 413–414
- control categories, 570, 571. *See also specific controls*
 - administrative, 508
 - corrective, 572, 659
 - detective, 572, 661
 - deterrent, 572, 661
 - directive, 572, 661
 - managerial, 570, 669
 - operational, 571, 672
 - physical, 572, 674
 - preventative, 572, 674
 - responsive, 677
 - technical, 571, 683
- control configuration, 377
 - 802.1X, 389–391, 653
 - blacklisting, 381
 - development/rule writing, 392
 - DLP (data loss prevention), 386–387, 660
 - EDR (endpoint detection and response), 387, 663
 - firewalls, 59–62, 383
 - architecture of, 61–62
 - comparison of, 385
 - definition of, 383, 664
 - host-based, 384–385, 666
 - NGFWs (next-generation firewalls), 383–384, 671
 - types of, 59–61, 383–385
 - input validation, 382
 - IPS rules, 386
 - malware signatures, 391–392
 - NAC (network access control), 387–389, 671
 - permissions, 381, 673
 - port security, 394, 674
 - enabling, 394
 - MAC addresses, limiting, 394
 - sticky MAC, 394, 682
 - sandboxing, 392–394
 - sinkholing, 391, 681
 - whitelisting, 381
- control flow graphs, 73
- Control Objectives for Information and Related Technologies (COBIT), 553, 657
- control plane, 193, 659
- controlled security mode (MAC), 229
- Controller Area Network (CAN) bus, 112
- COPE (corporate-owned, personally enabled) policy, 256, 659
- copyright management information (CMI), 444
- copyrights, 444, 659
- core dump, 493–494
- corporate information, 444–445
- corporate-owned, personally enabled (COPE) policy, 256, 659
- corrective controls, 572, 659

- correlation, 458, 660
 - CPE (Common Platform Enumeration), 427, 658
 - crackers, 405, 660
 - CRCs (cyclic redundancy checks), 237
 - CREATE TABLE statement, 145
 - credential stuffing, 152–154, 660
 - credentialed scans, 51, 660
 - credit card readers, 102
 - critical infrastructure sector, data sharing in, 15
 - criticality, 411, 439–445
 - analysis of, 457
 - corporate information, 444–445
 - critical assets, 411–412, 456, 531
 - commercial business classifications, 411
 - data classification policy, 411
 - distribution of critical assets, 412
 - military and government classifications, 412
 - sensitivity and criticality, 411
 - definition of, 660
 - financial information, 441–442
 - high value assets, 441
 - intellectual property, 442–444
 - copyright, 444, 659
 - definition of, 667
 - patents, 442–443, 673
 - security for, 444
 - trade secrets, 443, 684
 - trademarks, 443, 684
 - PHI (protected health information), 55, 436, 440–441, 674
 - PII (personally identifiable information), 55, 436, 439–440, 674
 - SPI (sensitive personal information), 441, 680
 - CRLs (certificate revocation lists), 244, 657
 - cross-certification, 219, 245
 - crossover error rate (CER), 283
 - cross-site request forgery (CSRF), 261–262, 660
 - cross-site scripting. *See* XSS (cross-site scripting)
 - cryptography. *See* encryption
 - cryptoperiod, 660
 - CS&C (Office of Cybersecurity and Communications), 8
 - CSRF (cross-site request forgery), 261–262, 660
 - CSS (Content Scrambling System), 520, 659
 - CTI (cyber threat information), 8
 - CVE (Common Vulnerabilities and Exposures), 165, 427, 658
 - CVSS (Common Vulnerability Scoring System), 44, 412
 - calculators, 29
 - metric groups, 25–29
 - CWE (Common Weakness Enumeration), 44, 427, 658
 - Cyber Intelligence Analytics Platform (CAP) v2.0, 6
 - cyber threat information (CTI), 8
 - Cybereason Total Enterprise Protection, 387
 - Cybersecurity and Infrastructure Security Agency (CISA), 15
 - cyclic redundancy checks (CRCs), 237
 - CYFIRMA, 6
- D**
- DAI (Dynamic ARP Inspection), 154, 662
 - Dalvik Executable (.dex/.odex) format, 328
 - dashboard, SIEM, 363–365
 - data analysis
 - availability, 510
 - data acquisition, 501
 - e-mail analysis, 367–372
 - digital signatures, 371

- DKIM (DomainKeys Identified Mail), 368, 662
- DMARC (Domain-based Message Authentication, Reporting, and Conformance), 369, 662
- e-mail signature blocks, 372, 662
- e-mail spoofing, 368
- embedded links, 372, 663
- forwarding, 370
- impersonation, 372
- malicious payloads, 368
- phishing/pharming, 335, 369–370
- spam, 370
- SPF (Sender Policy Framework), 369, 680
- endpoint, 321–341
 - definition of, 321
 - malware, 323–329
 - memory, 329–332
 - NIST SP 800–128, 322–323
 - system and application behavior, 333–339
 - UEBA (user and entity behavior analytics), 24, 341
- heuristics, 320
- impact analysis, 361
 - definition of, 361, 666
 - immediate versus total impact, 361
 - impact modeling, 32
 - organization versus localized impact, 361
- log review, 345–360
 - event logs, 346–350
 - firewall logs, 353–355
- IDSs (intrusion detection systems), 357–360
- IPSs (intrusion prevention systems), 357–360
- Kiwi Syslog Server, 352
- proxy servers, 356–357
- syslog, 350–352
- WAF (web application firewall), 355–356
- network, 342–345
 - DGA (domain generation algorithm), 343, 662
 - DNS (domain name system) analysis, 342–343
 - flow analysis, 345, 664
 - NetFlow analysis, 342–346
 - packet analysis, 342–343, 673
 - protocol analysis, 343, 675
 - URL (uniform resource locator) analysis, 342
- query writing, 366–367
 - pipings, 367, 674
 - scripts, 366, 679
 - Sigma, 366
 - string searches, 366, 682
- reverse engineering, 75, 327–329, 457
- SIEM (security information and event management) system, 48, 166, 361–365, 426, 458
 - agent-based collection, 362
 - agentless collection, 362
 - dashboard, 363–365
 - known-bad Internet Protocol, 363
 - rule writing, 362–363
- trend analysis, 320, 684
- data classification, 439, 508, 510
 - commercial business, 411
 - distribution of critical assets, 412
 - military and government, 412
 - policy, 411
 - security level classification, 455
 - sensitivity and criticality, 411
- data correlation, 458, 660
- data criticality. *See* criticality
- data encryption key (DEK), 308
- data enrichment, 425, 660
- data exfiltration, 479, 660
- data exposure, 165
- data flow analysis, 73

- data haven, 514
- data integrity, 233, 298, 456, 510
- data loss prevention (DLP), 386–387, 660
- data masking, 516–517, 660
- data minimization, 515
- data mining warehouses, 340
- data ownership policy, 567
- data plane, 193, 660
- data privacy
 - access controls, 521
 - definition of, 505–508
 - non-technical controls, 508–516
 - PIA (privacy impact assessment), 508
 - security versus, 505–508
 - technical controls, 516–521
- data protection, 285
- Data Protection API (DPAPI), 131, 660
- Data Protection Directive (EU), 514, 663
- data remnants, 204
- data retention policy, 509, 567–568
- data sensitivity, 411, 439
- data sovereignty, 514–515, 660
- data storage
 - nonremovable storage, 99
 - removable storage, 99
 - uncontrolled storage, 99
 - vulnerabilities with, 99–100
- data types, 53, 509–510
- dcfldd command, 492–493
- dd command, 492–493, 660
- DDoS (distributed denial-of-service)
 - attacks, 337, 472
- debugging, 332, 457, 493–494, 660, 678
- decompiling, 457, 661
- decomposition, 328, 661
- dedicated security mode (MAC), 228
- deep packet inspection, 60
- Deepviz Malware Analyzer, 393
- default configurations, vulnerabilities in, 167–168
- degrading functionality, 62, 539
- deidentification, 517, 661
- DEK (data encryption key), 308
- Deleaker, 332, 494
- delivery, continuous, 428, 659
- demilitarized zone (DMZ), 61, 181, 661
- Deming’s Plan-D-Check-Act cycle, 413–414
- denial-of-service (DoS) attacks, 183, 337, 472, 661
- Department of Homeland Security (DHS), 8
- deployment
 - cloud deployment models, 126
 - continuous, 428, 659
 - diagrams of, 186–192
- dereferencing, 163, 661
- design, software, 267–268
- destruction of data, 461, 661
- detection and analysis, 34, 454–458
 - data correlation, 458, 660
 - data integrity, 456
 - downtime and recovery time, 455–456
 - economic impact, 456–457
 - improvement of, 413–414
 - reverse engineering, 457
 - scope, 455
 - security level classification, 455
 - system process criticality, 457
- detective controls, 572, 661
- deterrent controls, 571, 572, 661
- Detux Sandbox, 393
- development/rule writing, 392
- Device Manager (Android), 257
- devices, mobile. *See* mobile devices
- DevOps, 270–272
- DevSecOps, 270–272, 661
- dex2jar, 328
- DGA (domain generation algorithm), 343, 662
- DHCP (Dynamic Host Configuration Protocol) snooping, 154, 661
- DHS (Department of Homeland Security), 8

- diagrams, network, 186–192
- Diamond Model of Intrusion Analysis, 22–23, 661
- Diffie-Hellman algorithm, 198, 236
- digital certificates, 284–285
- digital forensics
 - carving, 500, 657
 - cloud-based scanning, 495–496
 - data acquisition, 501
 - endpoint, 490–493
 - FTK (Forensic Toolkit), 491, 664
 - Helix3, 491, 666
 - imaging utilities, 492–493
 - password-cracking utilities, 491–492
 - hashing, 499–500
 - legal holds, 497, 669
 - memory, 493–494
 - mobile, 494
 - network, 488–490
 - tcpdump, 490, 683
 - Wireshark, 488–490
 - procedures, 497–499
 - EnCase Forensic, 498
 - forensic investigation suites, 498–499, 664
 - Sysinternals, 498
 - virtualization, 497
- Digital Millennium Copyright Act (DMCA), 517, 685
- digital rights management. *See* DRM (digital rights management)
- Digital Security Algorithm (DSA), 246, 371
- Digital Signature Standard (DSS), 246, 371
- digital signatures, 245–246, 371, 661
- digital watermarking, 521, 661
- directive controls, 571, 572, 661
- directory traversal, 151–152, 661
- disassemblers/disassembly, 328, 457
- disclosure of information, 435
- discovery scans, 54
- disks. *See* hard drives
- disposal, secure, 460–461
- dissassembly, 661
- dissemination, 14, 662
- diStorm3, 329
- distributed denial-of-service (DDoS)
 - attacks, 337, 472
- Distributed Network Protocol 3 (DNP3), 117, 662
- distribution of critical assets, 412
- DKIM (DomainKeys Identified Mail), 368, 662
- DLP (data loss prevention), 386–387, 516, 660
- DMARC (Domain-based Message Authentication, Reporting, and Conformance), 369, 662
- DMCA (Digital Millennium Copyright Act), 685
- DMCA (Digital Millennium Copyright Act), 517
- DMZ (demilitarized zone), 61, 181, 661
- DNP3 (Distributed Network Protocol 3), 117, 662
- DNS (Domain Name System) analysis, 342–343
- DNSSEC (Domain Name System Security Extensions), 302
- document DRM (digital rights management), 520
- document object model (DOM) XSS, 162, 662
- documentation, 305, 453–454, 543
- documented compensating controls, 541–542
- DOM (document object model) XSS, 162, 662
- domain bridging, 103–104, 662
- domain generation algorithm (DGA), 343, 662
- Domain Name System (DNS) analysis, 342–343

- Domain Name System Security Extensions (DNSSEC), 302
 - Domain Reputation Center, 24
 - Domain-based Message Authentication, Reporting, and Conformance (DMARC), 369, 662
 - DomainKeys Identified Mail (DKIM), 368, 662
 - DoS (denial-of-service) attacks, 183, 337, 472, 661
 - double tagging, 157
 - downtime, 455–456, 531
 - DPAPI (Data Protection API), 131, 660
 - drive capacity consumption, 477
 - drive-by compromise, 22
 - DRM (digital rights management), 517–521
 - definition of, 661
 - document, 520
 - e-book, 521
 - movie, 520
 - music, 520
 - video game, 520
 - watermarking, 521, 661
 - drones, 113
 - Dropbox, 99
 - DSA (Digital Security Algorithm), 236, 246, 371
 - DShield, 247
 - DSS (Digital Signature Standard), 246, 371
 - DTP (Dynamic Trunking Protocol), 156, 475
 - dual-homed firewalls, 61, 189–190, 662
 - dual-key cryptography, 236
 - dumping, memory, 332, 670
 - dumpster diving, 336
 - dynamic analysis, 74, 286, 662
 - Dynamic ARP Inspection (DAI), 154, 662
 - Dynamic Host Configuration Protocol (DHCP) snooping, 661
 - dynamic packet filtering, 60
 - dynamic passwords, 565
 - Dynamic Trunking Protocol (DTP), 156, 475
- ## E
- EAP (Extensible Authentication Protocol), 279–281, 389–391
 - Early Launch Anti-Malware driver, 310
 - e-book DRM (digital rights management), 521
 - ECC (Elliptical Curve Cryptography), 236
 - ECDSA (Elliptic Curve DSA), 246, 371
 - Economic Espionage Act, 513, 662
 - economic impact analysis, 456–457
 - ECPA (Electronic Communications Privacy Act), 512, 662
 - edb-debugger, 329
 - EDR (endpoint detection and response), 387, 663
 - education. *See* training/education
 - EEPROM (electrically erasable PROM), 266
 - EF (exposure factor), 534, 663
 - eFuse, 303, 662
 - EK (endorsement key), 300
 - El Gamal, 236
 - electrically erasable programmable read-only memory (EPROM), 309
 - electrically erasable PROM (EEPROM), 266
 - Electronic Communications Privacy Act (ECPA), 512, 662
 - Electronic Security Directive (EU), 514, 663
 - Elliptic Curve DSA (ECDSA), 246, 371
 - Elliptical Curve Cryptography (ECC), 236
 - e-mail analysis, 367–372
 - digital signatures, 371
 - DKIM (DomainKeys Identified Mail), 368, 662

- DMARC (Domain-based Message Authentication, Reporting, and Conformance), 369, 662
- e-mail review, 74, 274
- e-mail signature blocks, 372, 662
- e-mail spoofing, 368
- embedded links, 372, 663
- forwarding, 370, 664
- impersonation, 372
- malicious payloads, 368
- phishing/pharming, 335, 369–370
- spam, 370
- SPF (Sender Policy Framework), 369, 680
- viruses, 324
- emanations, 337, 663
- embedded links, 372, 663
- embedded systems, 105–265, 663
- employee privacy issues, 513, 663
- Encapsulating Security Payload (ESP), 197, 663
- EnCase Forensic, 498, 663
- encoding, 276, 672
- encryption, 232–242, 510
 - AES 128/256-bit, 99
 - asymmetric algorithms, 236
 - bus, 311, 656
 - certificate management, 242–246
 - CA (certificate authority), 243, 258, 285, 371, 657
 - CRLs (certificate revocation lists), 244, 657
 - cross-certification, 245
 - digital signatures, 245–246, 661
 - OSCP (Online Certificate Status Protocol), 244, 672
 - PKI (public key infrastructure), 198, 245, 284–285
 - RA (registration authority), 243, 677
 - Verisign, 244
 - X.509 certificates, 243–244
 - cryptoperiod, 660
 - data privacy and, 516
 - dual-key cryptography, 236
 - hashing, 238–240, 665
 - MD (Message Digest) Algorithm, 239–240
 - message digests, 238
 - one-way, 238–239
 - SHA (Secure Hash Algorithm), 240
 - hybrid, 236–237
 - key management, 132–134
 - key escrow, 133
 - key stretching, 134
 - principles of, 132–133
 - security services provided by, 232–233
 - self-encrypting drives, 308
 - SHA (Secure Hash Algorithm), 499
 - symmetric algorithms, 233–236
 - block ciphers, 235–236, 656
 - stream-based ciphers, 234–235, 682
 - tools for, 499
 - transport, 240–242
- endorsement key (EK), 300
- endpoint detection and response (EDR), 663
- endpoint security, 321–341
 - definition of, 321
 - digital forensics, 490–493
 - FTK (Forensic Toolkit), 491, 664
 - Helix3, 491, 666
 - imaging utilities, 492–493
 - password-cracking utilities, 491–492
 - DLP (data loss prevention), 386
 - EDR (endpoint detection and response), 387, 663
 - malware, 323–329
 - automated malware signature creation, 424, 655
 - botnets, 325, 473–474, 656
 - commodity malware, 14, 658
 - logic bombs, 325, 669
 - ransomware, 326, 676

- reverse engineering, 75, 327–329, 457
- rootkits, 326
- signatures, 391–392
- spyware/adware, 325
- Trojan horses, 325, 684
- viruses, 115, 323–324, 686
- worms, 324, 687
- memory, 329–332
 - dumping, 332
 - protection of, 329–330
 - runtime data integrity check, 330, 678
 - runtime debugging, 332, 660, 678
 - secured, 330
- NIST SP 800–128, 322–323
- rogue endpoints, 336
- system and application behavior, 333–339
 - anomalous behavior, 334–335
 - exploit techniques, 335–339
 - known-good behavior, 333–334
- UEBA (user and entity behavior analytics), 24, 341
- ENISA (European Union Agency for Network and Information Security), 15
- enrollment time, 282
- enumeration, 44, 76–82, 427
 - active versus passive, 82, 653, 673
 - definition of, 76
 - host scanning, 79, 666
 - hping, 80–82
 - Nmap, 76–79, 671
 - Responder, 82, 677
- environmental threats, 10
- EPROM (electrically erasable programmable read-only memory), 266, 309
- eradication, 459–462
 - capability and service restoration, 462
 - log verification, 462
 - patching, 461
 - permissions restoration, 461
 - reconstruction/reimaging, 460
 - resource reconstitution, 462
 - sanitization, 460, 679
 - secure disposal, 460–461
- erasable programmable read-only memory (EPROM), 266
- error handling
 - input validation errors, 149
 - vulnerabilities in, 163
- escalation lists, 454, 657
- escape, VM, 203
- escrow, key, 133
- ESP (Encapsulating Security Payload), 197, 663
- /etc/passwd file, 567
- /etc/shadow file, 567
- ethics, code of, 563, 658
- EU (European Union)
 - Data Protection Directive, 514, 663
 - Electronic Security Directive, 514, 663
 - ENISA (European Union Agency for Network and Information Security), 15
 - GDPR (General Data Protection Regulation), 425
 - privacy laws in, 514
- event logs, 346–350
- evidence retention, 463
- exam preparation process, 579
 - exam information, 579–580
 - exam updates, 651–652
 - online testing, 580
 - tips and guidelines for, 580–581
 - tools for
 - chapter-ending review tools, 582–583
 - final review/study, 583
 - memory tables, 582
 - Pearson Test Prep practice test software, 582

- executable process analysis, 407–408, 663
 - exfiltration of data, 479, 660
 - exploit techniques, 335–339
 - file system, 339–341
 - rogue access points, 336, 678
 - rogue endpoints, 336
 - servers, 337–338
 - services, 338–339
 - social engineering, 335–336
 - exposure factor (EF), 534, 663
 - Extensible Access Control Markup Language (XACML), 143–144, 220, 663
 - Extensible Authentication Protocol (EAP), 279–281, 389–391
 - Extensible Markup Language (XML) attacks, 143–144, 663
 - external scans, 53, 663
 - external stakeholders, 437
 - external threat actors, 29–30
 - extranets, 181, 663
- F**
- FaaS (Function as a Service), 128–129, 200, 665
 - facility access control, 107–109
 - false acceptance rate (FAR), 283
 - false negatives, 45, 664
 - false positives, 44, 664
 - false rejection rate (FRR), 283
 - FATKit, 332, 493, 664
 - fault tolerance, 532, 664
 - FBI (Federal Bureau of Investigation), threat actor categories, 12–13
 - feature extraction, 282
 - Federal Information Security Management Act (FISMA), 513, 664
 - Federal Intelligence Surveillance Act (FISA), 512, 664
 - Federal Privacy Act, 512, 664
 - federation, 219–224
 - models for, 219–220
 - OpenID, 222–223, 672
 - SAML (Security Assertion Markup Language), 221–222, 287, 680
 - Shibboleth, 224, 681
 - SPML (Service Provisioning Markup Language), 220
 - XACML (Extensible Access Control Markup Language), 220
 - feedback, 14
 - feeds, vulnerability, 49
 - FEMA ICS (Incident Command System), 114
 - FGPA (field programmable gate array), 105–106
 - field programmable gate array (FPGA), 664
 - file infectors, 324
 - file systems
 - changes or anomalies in, 479–480
 - exploit techniques for, 339–340
 - Hadoop Distributed File System, 136
 - monitoring, 340–341
 - file/data analysis tools, 393
 - FIN flag, 76
 - FIN scans, 78, 664
 - financial information, 441–442
 - financial sector, data sharing in, 15
 - Financial Services Information Sharing and Analysis Center (FS-ISAC), 15, 166
 - Financial Services Modernization Act, 15
 - Find My iPhone, 257
 - fingerprinting, 327
 - FireEye, 9, 387
 - firewalls, 59–62
 - architecture of, 61–62
 - comparison of, 385
 - definition of, 383, 664
 - logs, 353–355
 - Cisco Check Point, 353–355

- WAF (web application firewall), 355–356
- Windows Defender, 353
- multihomed, 671
- personal, 322
- types of, 59–61, 383–385
 - application-level proxies, 60, 385
 - bastion hosts, 188–189
 - circuit-level proxies, 60, 385
 - dual-homed, 189–190
 - host-based, 384–385, 666
 - kernel proxy firewalls, 385
 - multihomed, 190–191, 671
 - NGFWs (next-generation firewalls), 383–384, 671
 - packet-filtering firewalls, 59, 385
 - screened host, 192, 679
- WAF (web application firewall), 686
- firmware, 266, 308–309
- FISA (Federal Intelligence Surveillance Act), 512, 664
- FISMA (Federal Information Security Management Act), 513, 664
- Flash memory, 309
- flashing the BIOS, 309
- flow analysis, 345, 664
- Fluke Networks AirMagnet Enterprise, 475
- Forensic Explorer, 500
- forensic investigation suites, 498–499, 664
- Forensic Toolkit (FTK), 491, 664
- formal code review, 73, 286–287
- formal review, 273
- forwarding e-mail, 370, 664
- FPGA (field programmable gate array), 664
- frameworks, 552–562
 - definition of, 665
 - prescriptive, 555–562
 - ISO 27000 Series, 556–559
 - ITIL, 561, 668
 - maturity models, 561–562, 670

- NIST Cybersecurity Framework version 1.1, 555–556
- SABSA, 559–560, 679
- risk-based, 552–554
 - COBIT, 553, 657
 - NIST SP 800–55 Rev 1, 552–553
- TOGAF (The Open Group Architecture Framework), 554
- FreeMeter Bandwidth Monitor, 472
- FRR (false rejection rate), 283
- FS-ISAC (Financial Services Information Sharing and Analysis Center), 15, 166
- FTK (Forensic Toolkit), 491, 664
- Function as a Service (FaaS), 128–129, 200, 665
- functions, vulnerabilities in, 168. *See also* commands
- fuzzing, 75–76, 665

G

- GDPR (General Data Protection Regulation), 425, 514
- general-purpose computing on graphics processing units (GPGPU), 86
- generation-based fuzzing, 75
- geofencing, 180, 521, 665
- geographic access requirements, 521
- geolocation, 179
- geotagging, 100–101, 179, 665
- GLBA (Gramm-Leach-Bliley Act), 15, 55, 511, 665
- glossary, 653–687
- Google Cloud Platform, 87
- Google Pay, 101, 102
- governance, organizational, 62, 672
- government agencies
 - classifications in, 412
 - data sharing among, 15
- GPG (GNU Privacy Guard), 134
- GPGPU (general-purpose computing on graphics processing units), 86

- GPS (Global Positioning System), 179, 521
 - GPT (GUID partition table), 303
 - Gramm-Leach-Bliley Act (GLBA), 15, 55, 511, 665
 - graphical passwords, 565, 665
 - gray hats, 406
 - gray-box testing, 274–275
 - Greenbone console, 71
 - grep command, 366
 - Group Policy, 45, 184, 381, 570
 - GUID partition table (GPT), 303
 - Guidance Software EnCase Endpoint Security, 387
- H**
- hacking, 405, 665
 - hacking gear, 475
 - hacktivists, 12
 - Hadoop, 136
 - hard drives
 - digital forensics for, 491–492
 - disk space consumption, 477
 - self-encrypting, 308
 - hardening, 46–47, 410, 665, 683
 - hardware assurance
 - anti-tamper technology, 308, 654
 - bus encryption, 311, 656
 - eFuse, 303, 662
 - RoTs (Roots of Trust), 298–299
 - HSM (hardware security module), 302, 665
 - microSD HSM (hardware security module), 302–303, 670
 - TPM (Trusted Platform Module), 299–300, 684
 - VTPM (virtual Trusted Platform Module), 300–301
 - secure processing
 - atomic execution, 307
 - definition of, 305, 679
 - processor security extensions, 307, 675
 - secure enclave, 307, 679
 - TE (Trusted Execution), 305
 - self-encrypting drives, 308
 - trusted firmware updates, 308–309
 - attestation, 300, 310–311, 655
 - IMA (Integrity Measurement Architecture), 311
 - measured boot, 310–311, 670
 - measured launch, 311
 - Trusted Foundry program, 304–305, 544
 - UEFI (Unified Extensible Firmware Interface), 303–304, 685
 - hardware security module (HSM), 302, 665
 - hardware source authenticity, 544
 - hardware/embedded device analysis, 264–265
 - Hash-based Message Authentication Code (HMAC), 131
 - hashing, 238–240, 327, 499–500, 665
 - MD (Message Digest) Algorithm, 239–240
 - message digests, 238
 - one-way, 238–239
 - SHA (Secure Hash Algorithm), 240
 - Health and Human Services, Department of, 55, 511
 - Health Care and Education Reconciliation Act, 513, 665
 - Health Information Sharing and Analysis Center (H-ISAC), 15
 - Health Insurance Portability and Accountability Act (HIPAA), 15, 55, 436, 511, 666
 - healthcare sector, data sharing in, 15
 - heap overflow, 150, 665
 - heating, ventilation, and air conditioning (HVAC) systems, 111
 - Helix3, 491, 666

- heuristics, 25, 320, 666
 - HHS (Health and Human Services), Department of, 55, 511
 - HIDS (host-based IDS), 58
 - high value assets, 441
 - HIPAA (Health Insurance Portability and Accountability Act), 15, 55, 436, 511, 666
 - HIPS (host-based IPS), 360
 - H-ISAC (Health Information Sharing and Analysis Center), 15
 - HMAC (Hash-based Message Authentication Code), 131
 - honeypots, 230, 666
 - horizontal privilege escalation, 152
 - host scanning, 79, 666
 - host-based firewalls, 384–385, 666
 - host-based IDS, 58
 - host-based IPS, 360
 - hosted VDI model, 207
 - hostile threat actors, 30
 - host-related IOCs (indicators of compromise), 477–480
 - abnormal OS process behavior, 479
 - data exfiltration, 479, 660
 - drive capacity consumption, 477
 - file system changes or anomalies, 479–480
 - malicious processes, 478
 - memory consumption, 477
 - processor consumption, 477
 - unauthorized changes, 479
 - unauthorized privileges, 479
 - unauthorized scheduled tasks, 480
 - unauthorized software, 477–478
 - HP
 - Mobility Security IDS/IPS, 475
 - RFProtect, 475
 - hping, 80–82
 - hping3, 80–82
 - HSM (hardware security module), 302, 665
 - HTMLEncode, 261
 - HTTP (Hypertext Transfer Protocol), 241–242
 - HTTPS (HTTP Secure), 241–242
 - hub and spoke model, 9
 - human resources, response coordination by, 437
 - human threat actors, 9
 - Hunt Project, 158
 - hunt teaming, 247, 406, 666
 - HVAC controllers, 111
 - hybrid cloud, 126, 666
 - hybrid encryption, 236–237
 - Hypertext Transfer Protocol (HTTP), 241–242
 - Hyper-V, 203
 - hypervisors, 202–203
 - hypotheses, 404–405
 - HyTrust, 311
- I**
- I (Integrity) metric, 28, 667
 - IaaS (Infrastructure as a Service), 127, 667
 - IaC (Infrastructure as Code), 130, 667
 - ICMP (Internet Control Message Protocol) sweeps, 476
 - ICSSs (incident command systems), 666
 - ICSSs (industrial control systems), 107–117
 - IDEA, 235
 - identity and access management, 209–229
 - ABAC (attribute-based access control), 143, 225–227
 - access controls, 521, 569
 - ACLs (access control lists), 12, 47, 182, 458, 510
 - AD (Active Directory), 217–218, 653
 - federation, 219–224
 - models for, 219–220
 - OpenID, 222–223, 672

- SAML (Security Assertion Markup Language), 221–222, 287, 680
- Shibboleth, 224, 681
- SPML (Service Provisioning Markup Language), 220
- XACML (Extensible Access Control Markup Language), 220
- MAC (mandatory access control), 228–229
- manual review, 229
- MFA (multifactor authentication), 211–214
 - authentication factors, 212
 - characteristic factors, 212, 214, 657
 - definition of, 670
 - identification versus authentication, 211–212
 - knowledge factors, 212, 213, 669
 - ownership factors, 212, 213, 672
- privilege management, 211
- RBAC (role-based access control), 224–225, 678
- relationship identification, 210–211
- resource identification, 210
- rogue access points, 336, 475
- SESAME, 219, 679
- SSO (single sign-on), 214–217
 - advantages and disadvantages of, 214–215
 - definition of, 681
 - Kerberos, 215–217
 - user identification, 210
- identity theft, 336
- Identity Theft Enforcement and Restitution Act, 511
- ID-FF (Liberty Identity Federation Framework), 221
- IDSs (intrusion detection systems), 10, 322
 - definition of, 668
- HIPS (host-based IPS), 360
- log review, 357–360
- Snort, 359
- Zeek, 360
- IDSs (intrusion prevention systems), 57–58
- IEC (International Electrotechnical Commission), 556–559
- IEEE (Institute of Electrical and Electronics Engineers), 75, 281–282
- IIC (Integrated Intelligence Center), 413
- IKEv2 (Internet Key Exchange), 198, 667
- IMA (Integrity Measurement Architecture), 310–311
- imaging utilities, 393, 492–493, 498, 666
- impact analysis, 361
 - definition of, 666
 - immediate versus total impact, 361
 - impact modeling, 32
 - organization versus localized impact, 361
- Impact metric group (CVSS), 27–28
- impersonation, 154, 372, 666
- improvement, continuous, 413–414
- Incident Command System (ICS), 114
- incident command systems (ICSs), 666
- incident forms, 454, 666
- incident response process
 - communication plans, 435–436
 - containment, 458–459
 - isolation, 459, 668, 683
 - segmentation, 458–459
 - definition of, 666
 - detection and analysis, 454–458
 - data correlation, 458, 660
 - data integrity, 456
 - downtime and recovery time, 455–456
 - economic impact, 456–457
 - reverse engineering, 457
 - scope, 455
 - security level classification, 455
 - system process criticality, 457

- eradication and recovery, 459–462
 - capability and service restoration, 462
 - log verification, 462
 - patching, 461
 - permissions restoration, 461
 - reconstruction/reimaging, 460
 - resource reconstitution, 462
 - sanitization, 460, 679
 - secure disposal, 460–461
- factors contributing to data criticality, 439–445
 - corporate information, 444–445
 - financial information, 441–442
 - high value assets, 441
 - intellectual property, 442–444, 667
 - PHI (protected health information), 55, 436, 440–441, 674
 - PII (personally identifiable information), 55, 436, 439–440, 674
 - SPI (sensitive personal information), 441, 680
- overview of, 33
- post-incident activities, 463–465
 - change control process, 464
 - evidence retention, 463
 - incident response plan updates, 464
 - incident summary reports, 464–465, 666
 - IOCs (indicators of compromise), 465
 - lessons learned reports, 463
 - monitoring, 465
- preparation, 452–454
 - documentation of procedures, 453–454
 - testing, 453
 - training, 452–453
- response coordination, 436–438
 - human resources, 437
 - internal versus external, 437
 - law enforcement, 437–438
 - legal, 436–437
 - public relations, 437
 - regulatory bodies, 438
 - senior leadership, 438
- incident summary reports, 464–465, 666
- indicator management, 666
- indicators of compromise. *See* IOCs (indicators of compromise)
- inductance-enabled mobile payment, 102
- industrial control systems (ICSs), 107–117
- inference, 339, 667
- information security continuous monitoring (ISCM), 232
- information security management system. *See* ISMS (information security management system)
- information sharing and analysis communities, 15
- Infrastructure as a Service (IaaS), 127, 667
- Infrastructure as Code (IaC), 130, 667
- infrastructure management, 242–246
 - access. *See* identity and access management
 - active defense, 246–247, 653
 - asset management, 178–180
 - asset tagging, 178
 - critical assets, 42–43, 411–412, 456, 531
 - device-tracking technologies, 178–179
 - high value assets, 441
 - object-tracking and object-containment technologies, 179–180
 - CASB (cloud access security broker), 229, 657
 - certificate management, 242–246
 - CA (certificate authority), 243, 258, 285, 371

- CAs (certificate authorities), 258, 285, 371
- certificate-based authentication, 284–285
- CRLs (certificate revocation lists), 244
- cross-certification, 245
- digital signatures, 245–246
- OSCP (Online Certificate Status Protocol), 244
- PKI (public key infrastructure), 198, 245, 284–285
- RA (registration authority), 243
- Verisign, 244
- X.509 certificates, 243–244
- change management, 201–208, 464
- cloud. *See* cloud computing
- containerization, 208–209, 256
- encryption. *See* encryption
- honeypots, 230, 666
- logging. *See* log review
- network architecture, 185–200
 - physical, 186–192
 - SDN (software-defined networking), 193–194, 681
 - serverless, 200
 - VPC (virtual private cloud), 195
 - VPNs (virtual private networks), 196–199
- segmentation, 180–185, 458–459
 - definition of, 680
 - jumpboxes, 183–184, 668
 - physical, 180–181
 - scans, 56
 - system isolation, 184–185
 - virtual, 182–183
- virtualization
 - advantages and disadvantages of, 201–202
 - application streaming, 208
 - attacks and vulnerabilities, 203–206
 - digital forensics for, 497
 - hypervisors, 202–203
 - management interface, 205
 - terminal services, 208
 - VDI (virtual desktop infrastructure), 207
 - virtual networks, 205
 - VMs (virtual machines), 201–204, 497
- infrastructure vulnerability scanner, 71–496
- inhibitors to remediation, 62–63
- initialization vectors (IVs), 236
- injection, SQL, 145–146, 682
- input validation, 149, 275–276, 382, 667
- insecure components, 165–166
- insecure object reference, 163, 667
- insider threats
 - definition of, 12
 - intentional, 13
 - unintentional, 13
- Institute of Electrical and Electronics Engineers (IEEE), 75, 281–282
- integer overflow, 149–150, 667
- integrated circuit cards (ICCs), 213
- integrated intelligence, 413, 667
- Integrated Intelligence Center (IIC), 413
- Integrity (I) metric, 28
- integrity, data, 233, 298, 456, 510, 667
- Integrity Measurement Architecture (IMA), 310–311
- Intel Software Guard Extensions (Intel SGX), 131, 307
- Intel Trusted Execution Technology (Intel TXT), 305, 311
- intellectual property, 442–444
 - copyright, 444, 659
 - definition of, 667
 - patents, 442–443, 673
 - security for, 444
 - trade secrets, 443, 684
 - trademarks, 443, 684
- intelligence. *See* threat intelligence

- intelligence cycle, 13–14
- intentional insider threats, 13
- internal scans, 53, 667
- internal stakeholders, 437
- internal threat actors, 29–30
- International Electrotechnical Commission (IEC), 556–559
- International Organization for Standardization. *See* ISO (International Organization for Standardization)
- Internet Control Message Protocol (ICMP) sweeps, 476
- Internet Key Exchange (IKEv2), 198, 667
- Internet of Things (IoT), 103–104, 131, 668
- Internet Security Association and Key Management Protocol (ISAKMP), 197, 668
- intranets, 181
- intrusion detection systems. *See* IDSs (intrusion detection systems)
- intrusion prevention systems. *See* IPSs (intrusion prevention systems)
- IOCs (indicators of compromise), 465
 - application-related, 480–481
 - anomalous activity, 480
 - Application log, 481, 654
 - introduction of new accounts, 480
 - service interruption, 481
 - unexpected outbound communication, 481
 - unexpected output, 480
 - definition of, 7, 25, 469, 667
 - host-related, 477–480
 - abnormal OS process behavior, 479
 - data exfiltration, 479
 - drive capacity consumption, 477
 - file system changes or anomalies, 479–480
 - malicious processes, 478
 - memory consumption, 477
 - processor consumption, 477
 - unauthorized changes, 479
 - unauthorized privileges, 479
 - unauthorized scheduled tasks, 480
 - unauthorized software, 477–478
- indicator management, 7–9
 - OpenIOC (Open Indicators of Compromise), 9, 672
 - STIX (Structured Threat Information eXpression), 8, 682
 - TAXII (Trusted Automated eXchange of Indicator Information), 8–9, 684
- network-related, 472–476
 - bandwidth consumption, 472
 - beaconing, 473, 656
 - common protocol over non-standard port, 476
 - peer-to-peer (P2P) communication, 473–474
 - rogue devices on network, 475, 678
 - scans/sweeps, 476
 - traffic spikes, 476
- IoT (Internet of Things), 103–104, 131, 668
- IP (Internet Protocol)
 - IPsec, 197–199, 242
 - known-bad IP, 363
 - video systems, 109–111
- iPhone, Find My iPhone, 257
- IPSs (intrusion prevention systems), 57–58, 322
 - definition of, 668
 - log review, 357–360
 - rules, 386
 - Sourcefire, 358
- IriusRisk, 406
- ISAKMP (Internet Security Association and Key Management Protocol), 197, 668
- ISCM (information security continuous monitoring), 232

ISMS (information security management system), 539
ISO (International Organization for Standardization), 556–559, 668
 ISO/IEC 27001 standard, 539–541, 562, 668
 ISO/IEC 27002 standard, 541
isolation, 459, 668, 683
ITIL framework, 561, 668
IVs (initialization vectors), 236

J

Jad Debugger, 329
jailbreaking, 100, 678
Java vulnerabilities, 323, 337
JavaScript Object Notation (JSON), 131, 288
JavaScript vulnerabilities, 323, 337
Javasnoop, 329
John the Ripper, 491, 668
JSON (JavaScript Object Notation), 131, 288
Juggernaut, 158
jumpboxes, 183–184, 668

K

Kaspersky, 102
KDC (key distribution center), 215–217
Kennedy-Kassebaum Act. *See* HIPAA (Health Insurance Portability and Accountability Act)
kernel debugger, 457, 668
kernel proxy firewalls, 61, 385
key distribution center (KDC), 215–217
key management, 132–134, 233, 371.
 See also IKEv2 (Internet Key Exchange)
 DEK (data encryption key), 308
 Kerberos, 215–217
 key escrow, 133, 668
 key stretching, 134, 669

PKI (public key infrastructure), 198, 236, 245, 284–285, 371, 675
 principles of, 132–133
 session keys, 234
 storage, 300
 wireless key loggers, 475, 687
keywords, sticky, 394
kill chain, 23, 669
Kindle, 521
Kiwi Syslog Server, 352
Knapsack, 236
knowledge factor authentication, 212, 213, 669
known threats, 10, 669
known-bad Internet Protocol, 363
known-good behavior, 333–334
KnTTools, 332, 493, 669

L

L2TP (Layer 2 Tunneling Protocol), 197, 669
languages, scripting, 423
LANs (local-area networks), 181
launch, measured, 311
law enforcement, response coordination by, 437–438
Layer 2 Tunneling Protocol (L2TP), 197, 669
LDAP (Lightweight Directory Access Protocol), 217
leadership, response coordination by, 438
least privilege, principle of, 338
legacy systems, 62, 669
legal department, response coordination by, 436–437
legal holds, 497, 669
less command, 367
lessons learned reports, 463–464, 669
lexical analysis, 73
Liberty Identity Federation Framework (ID-FF), 221
lightweight code review, 74, 273

Lightweight Directory Access Protocol (LDAP), 217

Link-Local Multicast Name Resolution (LLMNR), 82

links, embedded, 372, 663

Linux dd, 393

Linux passwords, 567

live migration, 205

LLMNR (Link-Local Multicast Name Resolution), 82

local-area networks (LANs), 181

location factor authentication, 212

lockdown, configuration, 410, 659

log review, 230–232, 345–360

- Application log, 481, 654
- audit reduction tools, 231
- cloud computing, 136
- event logs, 346–350
- firewall logs, 353–355
 - Cisco Check Point, 353–355
 - Windows Defender, 353
- IDSs (intrusion detection systems), 357–360
- IPSs (intrusion prevention systems), 357–360
- Kiwi Syslog Server, 352
- log analyzers, 394
- log management, 230–231
- log verification, 48, 462
- log viewers, 499
- logging vulnerabilities, 166
- Measured Boot, 311
- NIST SP 800–137, 232
- proxy servers, 356–357
- syslog, 350–352
- WAF (web application firewall), 355–356

logic bombs, 325, 669

logical controls, 571

logical deployment diagrams, 186–192

LonWorks/LonTalk, 117, 669

Lost Android, 257

M

MAC (mandatory access control), 228–229

MAC (media access control)

- addresses
 - limiting, 394
 - sticky MAC, 394, 682
- definition of, 669
- overflow, 155

MAC (message authentication code), 239

MacAfee, 111–112

machine learning, 426–427, 669

macro viruses, 324

magnitude, 535

maintenance, software, 269

maintenance accounts, 260

maintenance hooks, 260, 669

malware, 323–329

- automated malware signature creation, 424, 655
- botnets, 325, 473–474, 656
- commodity malware, 14, 658
- logic bombs, 325, 669
- ransomware, 326, 676
- reverse engineering, 75, 327–329, 457
 - definition of, 327, 677
 - isolation/sandboxing, 327, 668
 - software/malware, 327–328
 - tools for, 328–329
- rootkits, 326
- signatures, 391–392
- spyware/adware, 325, 681
- Trojan horses, 325, 684
- viruses, 115, 323–324, 686
- worms, 324, 687

MAM (mobile application management), 97

managed service accounts, 339

management interface, 205

management plane, 193, 669

managerial controls, 570, 669

- mandatory access control (MAC), 228–229
- Mandiant, 9
- man-in-the-middle attacks, 154–155, 205, 669
- mantraps, 108, 670
- manual review, 229
- many-to-one rules, 363
- mapping vulnerabilities, 44
- masking data, 516–517, 660
- master boot record (MBR), 303
- matrix, risk assessment, 537–538
- maturity models, 561–562
 - CMMI (Capability Maturity Model Integration), 561, 657
 - definition of, 670
 - ISO/IEC 27001, 562
- maximum tolerable downtime (MTD), 455, 670
- MBR (master boot record), 303
- McAfee, 102
- MD (Message Digest) algorithm, 239–240, 499
- MDM (mobile device management), 97, 670
- mean time between failures (MTBF), 455, 670
- mean time to repair (MTTR), 455, 670
- measured boot, 310–311, 670
- measurement, RTM (Root of Trust for Measurement), 298
- Memdump, 332, 493, 670
- memorandum of understanding (MOU), 62, 538, 670
- memory, 329–332
 - consumption of, 409, 477
 - digital forensics for, 493–494
 - dumping, 332, 670
 - EEPROM (electrically erasable PROM), 266
 - EPROM (electrically erasable programmable read-only memory), 266, 309
 - Flash, 309
 - overflows, 335
 - protection of, 329–330
 - RAM (random-access memory), 329
 - ROM (read-only memory), 309, 329
 - runtime data integrity check, 330, 678
 - runtime debugging, 332, 660, 678
 - secured, 330, 680
- memory cards, 213
- memory tables
 - GPT (GUID partition table), 303
 - how to use, 582
- Meraki, 98
- MESCM (Microsoft Endpoint Configuration Manager), 570
- message authentication code (MAC), 239
- Message Digest (MD) algorithm, 239–240, 499
- message digests, 238
- messaging, text, 103
- Metasploit, 87
- metrics, risk assessment, 533
- MFA (multifactor authentication), 211–214
 - authentication factors, 212
 - characteristic factors, 212, 214, 657
 - definition of, 670
 - identification versus authentication, 211–212
 - knowledge factors, 212, 213, 669
 - ownership factors, 212, 213, 672
- microSD HSM (hardware security module), 302–303, 670
- microservices, 288–289, 670
- Microsoft
 - Application Virtualization, 208
 - Azure, 87
 - BitLocker/BitLocker to Go, 300
 - Hyper-V, 203
 - Measured Boot, 311
 - MESCM (Microsoft Endpoint Configuration Manager), 570

- SCAP (Security Content Automation Protocol), 74, 286
- Sysinternals Autoruns, 393
- migration, VMs (virtual machines), 204, 205
- military classifications, 412
- minimization of data, 515
- mitigation. *See* remediation/mitigation
- MITRE ATT&CK, 21–22, 670
- MMS (Multimedia Messaging Service), 103
- mobile devices
 - device-tracking technologies, 178–179
 - digital forensics for, 494, 499
 - mobile code, 323, 337
 - platforms for, 256–266
 - application, content, and data management, 257
 - application wrapping, 257, 654
 - configuration profiles and payloads, 256
 - containerization, 256
 - COPE (corporate-owned, personally enabled) policy, 256, 659
 - NIST SP 800–163 Rev 1, 258–259
 - POCE (personally owned, corporate-enabled) policy, 256
 - remote wiping, 257, 677
 - SCEP (Simple Certificate Enrollment Protocol), 258, 681
 - threats and vulnerabilities, 97–103
 - Android fragmentation, 101
 - BYOD (bring your own device) policies, 97–98, 656
 - device loss/theft, 100
 - geotagging, 100–101
 - malware, 102
 - MAM (mobile application management), 97
 - MDM (mobile device management), 97, 670
 - payment technologies, 101–102
 - push notification services, 100, 675
 - rooting/jailbreaking, 100, 678
 - SMS/MMS messaging, 103
 - storage concerns, 99–100
 - system apps, 98
 - unauthorized domain bridging, 103–104
 - unsigned apps, 98
 - USB (universal serial bus), 102
- mobile hacking gear, 475
- Mobile Wallet, 102
- Mobility Security IDS/IPS, 475
- Modbus, 117, 118, 670
- models
 - maturity
 - CMMI (Capability Maturity Model Integration), 561, 657
 - ISO/IEC 27001, 562
 - threat, 29–32, 406–407
 - adversary capability, 29–30
 - attack vectors, 31–32, 412–413
 - impact, 32
 - probability, 32
 - total attack surface, 31, 684
- models, threat, 29–32, 406–407
 - adversary capability, 29–30
 - attack vectors, 31–32, 412–413
 - impact, 32
 - probability, 32
 - total attack surface, 31, 684
- Modicon, 118
- Mojo Networks AirTight WIPS, 475
- monitoring, 230–232, 465. *See also* log review
 - cloud computing, 136
 - continuous, 414, 569–570
 - file systems, 339–340
 - vulnerabilities in, 166
- MOUs (memorandum of understanding), 62, 538, 670
- movie DRM (digital rights management), 520

- MPLS (Multiprotocol Label Switching), 196
- MSAB XRY, 494
- MS-CHAP v1, 279–281
- MS-CHAP v2, 279–281
- MTBF (mean time between failures), 455, 670
- MTD (maximum tolerable downtime), 455, 670
- MTTR (mean time to repair), 455, 670
- multifactor authentication. *See* MFA (multifactor authentication)
- multihomed firewalls, 190–191, 671
- multilevel security mode (MAC), 229
- Multimedia Messaging Service (MMS), 103
- multipartite viruses, 324
- Multiprotocol Label Switching (MPLS), 196
- music DRM (digital rights management), 520
- mutation fuzzing, 75
- N**
- NAC (network access control), 387–389, 671. *See also* identity and access management
- National Institute of Standards and Technology. *See* NIST (National Institute of Standards and Technology)
- nation-state threat actors, 12
- natural threats, 10
- NBT-NS (NetBIOS Name Service), 82
- NDAs (nondisclosure agreements), 228, 436, 443, 508, 516
- near field communication (NFC), 101, 671
- Nessus Network Monitor, 43
- Nessus Professional, 43, 71, 671
- NetBIOS Name Service (NBT-NS), 82
- NetFlow, 24, 342–346, 671
- NetScanTools Pro, 43
- network access control (NAC), 387–389, 671. *See also* identity and access management
- network architecture, 185–200
 - firewalls. *See* firewalls
 - physical, 186–192
 - SDN (software-defined networking), 193–194, 681
 - segmentation
 - physical, 180–181
 - virtual, 182–183
 - serverless, 200
 - VPC (virtual private cloud), 195
 - VPNs (virtual private networks), 196–199
 - definition of, 195
 - IPsec, 197–199
 - remote-access, 196
 - site-to-site, 196
 - SSL/TLS, 199, 681
 - VPN concentrators, 196
- network authentication protocols, 279–280
- network interface cards (NICs), 58
- network security analysis, 342–345
 - DGA (domain generation algorithm), 343, 662
 - digital forensics, 488–490
 - tcpdump, 490, 683
 - Wireshark, 488–490
 - DNS (domain name system) analysis, 342–343
 - flow analysis, 345, 664
 - intelligent networks, 427
 - IOCs (indicators of compromise), 472–476
 - bandwidth consumption, 472
 - beaconing, 473, 656
 - common protocol over non-standard port, 476
 - definition of, 667

- peer-to-peer (P2P) communication, 473–474
 - rogue devices on network, 475, 678
 - scans/sweeps, 476
 - traffic spikes, 476
 - NetFlow analysis, 342–346
 - network capture tools, 394
 - network data loss prevention (DLP), 386
 - NVT (network vulnerability tests), 71
 - packet analysis, 342–343, 673
 - protocol analysis, 343, 675
 - URL (uniform resource locator) analysis, 342
 - network-based IDSs (NIDs), 58
 - never execute (XN) bit, 307
 - next-generation firewalls (NGFWs), 383–384, 671
 - NFC (near field communication), 101, 671
 - NGFWs (next-generation firewalls), 383–384, 671
 - NICs (network interface cards), 58
 - NIDSs (network-based IDSs), 58
 - Nikto, 70, 671
 - NIST (National Institute of Standards and Technology), 427, 552–553
 - NIST 800–57, 671
 - NIST 800–128, 671
 - NIST Cybersecurity Framework version 1.1, 555–556, 671
 - NIST SP 800–53, 31, 671
 - NIST SP 800–128, 322–323
 - NIST SP 800–137, 232
 - NIST SP 800–163 Rev 1, 258–259
 - Nmap, 76–79, 671
 - Node.js, 423, 671
 - no-execute (NX) bit, 307
 - nondisclosure agreements (NDAs), 228, 436, 443, 508
 - nonessential resources, 456
 - non-hostile threat actors, 30
 - nonremovable storage, 99
 - non-repudiation, 233
 - Nook, 521
 - NOP (no-operation) slide, 147–149
 - normal resources, 456
 - note-taking, 581
 - notifications, push, 100, 675
 - null scans, 77, 671
 - numeric passwords, 565, 672
 - NVT (network vulnerability tests), 71
 - NX (no-execute) bit, 307
- O**
- Oakley, 198
 - OASIS (Organization for the Advancement of Structured Information Standards), 8, 220
 - objects
 - definition of, 210
 - references to, 163, 667
 - tracking and containment technologies, 179–180
 - oclHashcat, 86, 672
 - OCR (Office of Civil Rights), 55, 511
 - OEM (original equipment manufacturer) documentation, 305, 543
 - /OFFBOOTDIR switch (SFC), 341
 - /OFFFWINDIR switch (SFC), 341
 - Office of Civil Rights (OCR), 55, 511
 - Office of Cybersecurity and Communications (CS&C), 8
 - Off-the-Record (OTR) Messaging, 435
 - OllyDbg, 329
 - Omnipeek, 394
 - one-time passwords (OTPs), 565, 672
 - one-to-many rules, 363
 - one-way hashes, 238–239
 - Online Certificate Status Protocol (OCSP), 244, 672
 - online testing, 580
 - The Open Group Architecture Framework (TOGAF), 554, 683

- Open Indicators of Compromise (OpenIOC), 9, 672
 - open message format, 236
 - Open Source Security Information Management (OSSIM), 365
 - Open Web Application Security Project (OWASP), 69, 136, 406
 - OpenID, 222–223, 672
 - OpenIOC (Open Indicators of Compromise), 9, 672
 - open-source intelligence (OSINT), 6, 672
 - OpenVAS, 43, 50, 71–72, 672
 - operational controls, 571, 672
 - operational threats, 10
 - Oracle Cloud Infrastructure, 87
 - Oracle VM VirtualBox, 203
 - orchestration, workflow, 422–423
 - Organization for the Advancement of Structured Information Standards (OASIS), 8, 220
 - organizational governance, 62, 539, 672
 - organized crime threat actors, 12, 405
 - original equipment manufacturer (OEM) documentation, 305, 543
 - OS (operating system)
 - digital forensics for, 499
 - process behavior, 479
 - OSCP (Online Certificate Status Protocol), 244, 672
 - OSINT (open-source intelligence), 6, 672
 - OSSIM (Open Source Security Information Management), 365
 - OTPs (one-time passwords), 565, 672
 - OTR (Off-the-Record) Messaging, 435
 - outage impact, 531
 - outbound communication, unexpected, 481
 - output
 - encoding, 276, 672
 - unexpected, 480
 - OutputDebugString Checker, 494
 - overflow attacks, 147–150, 335
 - buffer, 147–149, 656
 - definition of, 672
 - heap, 150, 665
 - integer, 149–150, 667
 - over-the-shoulder review, 74, 274
 - OWASP (Open Web Application Security Project), 69, 136, 406
 - ownership factor authentication, 212, 213, 672
 - ownership policy, 508
- P**
- P2P (peer-to-peer) communication, 9, 473–474
 - PaaS (Platform as a Service), 127, 674
 - packet analysis, 342–343, 673
 - packet-filtering firewalls, 59, 385
 - Pacu, 87–88, 673
 - pair programming, 74, 273
 - Palo Alto Networks AutoFocus threat feed, 426
 - PAP (Password Authentication Protocol), 279–281
 - parameterized queries, 285, 673
 - parasitic viruses, 324
 - parity bits, 237
 - passive enumeration, 82, 673
 - passive scans, 43–44
 - passive vulnerability scanners (PVSs), 43, 673
 - passphrase passwords, 565, 673
 - Password Authentication Protocol (PAP), 279–281
 - Password-Based Key Derivation Function 2 (PBKDF2), 134
 - passwords
 - authentication period for, 566, 655
 - CAPTCHA, 154, 565
 - complexity of, 566, 658, 673
 - history, 566, 673
 - length of, 566, 673
 - life of, 566, 673

- password-cracking utilities, 491–492, 499
- policies for, 564–567
- spraying, 152, 673
- patching, 46, 48, 461, 673
- patents, 442–443, 673
- PATRIOT Act, 438, 513
- pattern matching, 57
- payloads, 256, 368
- payment, mobile, 101–102
- Payment Card Industry Data Security Standard (PCI DSS), 55–56, 441, 673
- PayPal, 102
- PBKDF2 (Password-Based Key Derivation Function 2), 134
- PCI DSS (Payment Card Industry Data Security Standard), 55–56, 510, 673
- PCR (platform configuration register) hash, 300
- PDPs (policy decision points), 144, 674
- Pearson Test Prep practice test software, 582
- peer-to-peer (P2P) communication, 9, 473–474
- peer-to-peer botnets, 474, 673
- PEframe, 393
- PEnE (Policy Enforcement Engine), 298
- PEPs (policy enforcement points), 144, 674
- peripheral-enabled payments, 102
- Perl, 423, 673
- permissions
 - definition of, 381, 673
 - restoration of, 461
 - verification of, 48
- persistent XSS (cross-site scripting), 161, 673
- personal firewalls, 322
- personal health information (PHI), 510
- Personal Information Protection and Electronic Documents Act (PIPEDA), 512, 674
- personally identifiable information (PII), 55, 436, 439–440, 508, 509, 674
- personally owned, corporate-enabled (POCE) policy, 256
- PeStudio, 393
- PGP (Pretty Good Privacy), 134, 300
- PHI (protected health information), 55, 436, 440–441, 510, 674
- phishing/pharming, 335, 369–370, 674
- physical access control, 106–109
 - devices, 107
 - facilities, 107–109
 - systems, 106–107
- physical controls, 674
- physical network architecture, 186–192
- physical segmentation, 180–181
- physical threats, 10
- PIA (privacy impact assessment), 508
- PII (personally identifiable information), 55, 436, 439–440, 508, 509, 674
- ping sweeps, 79, 476, 674
- PIPEDA (Personal Information Protection and Electronic Documents Act), 512, 674
- pipng, 367, 674
- PKI (public key infrastructure), 198, 236, 245, 284–285, 371, 675
- planning software development, 267
- plans, communication, 435–436, 536–537.
 - See also* response coordination
- Platform as a Service (PaaS), 127, 674
- platform configuration register (PCR) hash, 300
- platforms, 256–266
 - client/server, 263
 - embedded systems, 105–265
 - firmware, 266
 - mobile, 256–266

- application, content, and data management, 257
- application wrapping, 257, 654
- configuration profiles and payloads, 256
- containerization, 256
- COPE (corporate-owned, personally enabled) policy, 256, 659
- NIST SP 800–163 Rev 1, 258–259
- POCE (personally owned, corporate-enabled) policy, 256
- remote wiping, 257, 677
- SCEP (Simple Certificate Enrollment Protocol), 258, 681
- SoC (system-on-chip), 105, 265
 - central security breach response, 265–266
 - secure booting, 265
- web application, 260–262
 - click-jacking, 262, 657
 - CSRF (cross-site request forgery), 261–262, 660
 - maintenance hooks, 260
 - time-of-check/time-of-use attacks, 260, 684
- PLCs (programmable logic controllers), 115, 675
- PLD (programmable logic device), 105
- POCE (personally owned, corporate-enabled) policy, 256
- PoE (Power over Ethernet), 109
- Point-to-Point Tunneling Protocol (PPTP), 197, 674
- policies
 - account management, 568–569
 - AUP (acceptable use policy), 563–564, 653
 - BYOD (bring your own device), 97–98, 656
 - code of conduct/ethics, 563, 658
 - continuous monitoring, 569–570
 - data classification, 411
 - data ownership, 508, 567
 - data retention, 509, 567–568
 - definition of, 562
 - Group Policy, 184
 - mobile, 256
 - password, 564–567
 - work product retention, 570, 687
- policy decision points (PDPs), 144, 674
- Policy Enforcement Engine (PEnE), 298
- policy enforcement points (PEPs), 144, 674
- polymorphic viruses, 324
- port security mac-address command, 394
- ports
 - non-standard, common protocols over, 476
 - scans of, 476, 674
 - security, 394, 674
 - enabling, 394
 - MAC addresses, limiting, 394
 - sticky MAC, 394, 682
- post-incident activities, 463–465
 - change control process, 464
 - evidence retention, 463
 - incident response plan updates, 464
 - incident summary reports, 464–465, 666
 - IOCs (indicators of compromise), 465
 - lessons learned reports, 463–464
 - monitoring, 465
- Power over Ethernet (PoE), 109
- PowerShell, 423
- PPTP (Point-to-Point Tunneling Protocol), 197, 674
- Pr (Privileges Required) metric, 27
- precise methods, 386
- premises-based scanning, 495–496
- preparation, exam. *See* exam preparation process
- preparation, in incident response process, 452–454
 - documentation of procedures, 453–454

- testing, 453
- training, 452–453
- prescriptive frameworks, 555–562
 - ISO 27000 Series, 556–559
 - ITIL, 561, 668
 - maturity models, 561–562, 670
 - CMMI (Capability Maturity Model Integration), 561, 657
 - definition of, 670
 - ISO/IEC 27001, 562
 - NIST Cybersecurity Framework version 1.1, 555–556
 - SABSA, 559–560, 679
- preshared secret, 258
- Pretty Good Privacy (PGP), 134, 300
- preventative controls, 572, 674
- Principles on Privacy (EU), 514
- prioritization of risk, 537–539
 - engineering tradeoffs, 538–539
 - ISO/IEC 27001 standard, 539–541
 - ISO/IEC 27002 standard, 541
 - risk assessment matrix, 537–538
 - security controls, 538
- privacy. *See* data privacy
- privacy impact assessment (PIA), 508
- private cloud, 126, 675
- private VLANs (PVLANS), 458
- PrivateCore, 311
- privilege management, 211
 - privilege elevation, 205
 - privilege escalation, 152
 - privileged accounts, 211
 - unauthorized privilege, 479
- Privileges Required (Pr) metric, 27
- proactive threat indicators (PTIs), 328
- probability, 32, 535
- procedures, 562. *See also* policies
 - digital forensics, 497–499
 - EnCase Forensic, 498
 - forensic investigation suites, 498–499, 664
 - Sysinternals, 498
 - documentation, 453–454
 - process behavior, abnormalities in, 479
 - Process Explorer, 408, 675
 - process isolation, 459
 - processing. *See* secure processing
 - processor consumption, 477
 - processor security extensions, 307, 675
 - profiles, mobile, 256
 - programmable logic controllers (PLCs), 115, 675
 - programmable logic device (PLD), 105
 - proprietary systems, 63, 675
 - proprietary/closed-source intelligence, 6, 675
 - protected health information (PHI), 55, 436, 440–441, 674
 - protocol analysis, 343, 675
 - protocol anomaly-based IDSs, 58
 - Prowler, 87, 675
 - proximity readers, 108, 675
 - proxy firewalls, 60
 - proxy server logs, 356–357
 - PRTG Network Monitor, 472
 - PSH flag, 76
 - PTIs (proactive threat indicators), 328
 - public cloud, 126, 675
 - Public Company Accounting Reform and Investor Protection Act. *See* SOX (Sarbanes-Oxley Act)
 - public key infrastructure (PKI), 198, 236, 245, 284–285, 371, 675
 - public relations, response coordination by, 437
 - /PURGECACHE switch (SFC), 341
 - purging data, 461, 675
 - purpose limitation, 515
 - push notification services, 100, 675
 - PVLANS (private VLANs), 458
 - PVSs (passive vulnerability scanners), 43, 673
 - Python, 423, 676

Q

QRadar, 364
qualitative risk analysis, 534, 676
Qualys, 496, 676
quantitative risk analysis, 534, 676
queries, 366–367
 parameterized, 285, 673
 writing, 676
 piping, 367, 674
 scripts, 366, 679
 Sigma, 366
 string searches, 366, 682

R

RA (registration authority), 243, 677
race conditions, 164, 260, 676
radio frequency identification (RFID),
 180, 521, 676
RADIUS (Remote Authentication Dial-in
 User Service), 281–282, 389–391
RAM (random-access memory), 329
ransomware, 326, 676
RBAC (role-based access control), 224–
 225, 678
RC4, 235
RC5, 235
RC6, 235
read-only memory (ROM), 309, 329
real user monitoring (RUM), 69, 74, 286,
 676
real-time operating systems (RTOSs),
 105, 676
Reaver, 84–86, 676
reconstruction/reimaging, 460
recoverability, 532, 676
recovery, 459–462
 capability and service restoration, 462
 log verification, 462
 patching, 461
 permissions restoration, 461
 priorities, identification of, 531–532
 reconstruction/reimaging, 460
 resource reconstitution, 462
 sanitization, 460, 679
 secure disposal, 460–461
 time requirements, 455–456
recovery point objective (RPO), 455, 676
recovery time objective (RTO), 455, 677
red teams, 542, 677
reflective XSS (cross-site scripting), 161,
 677
registration authority (RA), 243, 677
Registry/configuration tools, 393
regulatory audits/assessments, 573–574
regulatory bodies, response coordination
 by, 438
relationships, identification of, 210–211
release, software, 269
remediation/mitigation, 45, 459–462, 538
 capability and service restoration, 462
 cloud computing, 177–178
 compensating controls, 47, 658
 configuration baseline, 45–46, 659
 hardening, 46–47, 665, 683
 inhibitors to, 62–63
 log verification, 462
 patching, 46, 48, 461, 673
 permissions restoration, 461
 reconstruction/reimaging, 460
 resource reconstitution, 462
 risk acceptance, 47, 677
 sanitization, 460, 679
 secure disposal, 460–461
 verification of, 47
Remote Authentication Dial-in User
 Service (RADIUS), 281–282,
 389–391
remote code execution, 150, 677
remote terminal units (RTUs), 115, 677
remote virtual desktops model, 207
remote wiping, 257, 677
remote-access VPNs (virtual private
 networks), 196

- removable storage, 99
- reports
 - incident summary, 464–465, 666
 - lessons learned, 463–464, 669
 - reporting requirements, 436
 - RTR (Root of Trust for Reporting), 298
 - SOC (Service Organization Control) reports, 574, 681
- REpresentational State Transfer (REST), 131, 677
- reputational scores, 24
- requirements gathering, 267
- requirements stage, intelligence life cycle, 13
- research, threat, 23–29. *See also* IOCs (indicators of compromise)
 - behavioral analysis, 24–25
 - reputational scores, 24
- resources
 - critical, 531
 - function criticality levels, 456
 - identification of, 210
 - reconstitution of, 462
 - requirements for, 531
- Responder, 82, 677
- response coordination, 436–438
 - human resources, 437
 - internal versus external, 437
 - law enforcement, 437–438
 - legal, 436–437
 - public relations, 437
 - regulatory bodies, 438
 - senior leadership, 438
- responsive controls, 677
- REST (REpresentational State Transfer), 131, 288, 677
- restoration
 - of capabilities and services, 462
 - of permissions, 461
 - of resources, 462
- retention standards, 510
- reverse engineering, 75, 327–329, 457
 - definition of, 327, 677
 - isolation/sandboxing, 327, 668
 - software/malware, 327–328
 - tools for, 328–329
- /REVERT switch (SFC), 341
- RFID (radio frequency identification), 180, 676
- RFProtect, 475
- risk, 29. *See also* threat intelligence
 - acceptance of, 47, 538, 677
 - assessment of, 532–534
 - definition of, 677
 - goals of, 532–533
 - metrics, 533
 - qualitative risk analysis, 534, 676
 - quantitative risk analysis, 534, 676
 - risk assessment matrix, 537–538
 - avoidance of, 47, 538, 678
 - BIA (business impact analysis), 530–532
 - critical processes and resources, 531
 - definition of, 657
 - outage impact and downtime, 531
 - recovery priorities, 531–532
 - resource requirements, 531
 - calculation of, 534–535
 - cloud computing, 177
 - communication of risk factors, 536–537
 - documented compensating controls, 541–542
 - mitigation of. *See* remediation/mitigation
 - overview of, 33
 - prioritization of, 537–539
 - engineering tradeoffs, 538–539
 - ISO/IEC 27001 standard, 539–541
 - ISO/IEC 27002 standard, 541
 - risk assessment matrix, 537–538
 - security controls, 538
 - of scans/sweeps, 49–62

- supply chain assessment, 543–544
 - hardware source authenticity, 544
 - vendor due diligence, 543
 - systems assessment, 539–541
 - training and exercises, 542–543
 - transfer of, 47, 538, 678
 - risk-based frameworks, 552–554
 - COBIT, 553, 657
 - NIST SP 800–55 Rev 1, 552–553
 - TOGAF (The Open Group Architecture Framework), 554
 - rogue access points, 336, 678
 - rogue devices, 475, 678
 - rogue endpoints, 336
 - role-based access control (RBAC), 224–225, 678
 - ROM (read-only memory), 309, 329
 - rooting, 100, 678
 - rootkits, 159–160, 326, 678
 - RoTs (Roots of Trust), 298–299
 - definition of, 678
 - HSM (hardware security module), 302
 - microSD HSM (hardware security module), 302–303
 - TPM (Trusted Platform Module), 299–300
 - VTPM (virtual Trusted Platform Module), 300–301
 - RPO (recovery point objective), 455, 676
 - RSA, 236, 371, 387
 - RST flag, 76
 - RTI (Root of Trust for Integrity), 298
 - RTM (Root of Trust for Measurement), 298
 - RTO (recovery time objective), 455, 677
 - RTOSs (real-time operating systems), 105, 676
 - RTR (Root of Trust for Reporting), 298
 - RTS (Root of Trust for Storage), 298
 - RTUs (remote terminal units), 115, 677
 - RTV (Root of Trust for Verification), 298
 - Ruby, 423, 678
 - rules
 - configuration of, 386
 - rule-based IDSs, 58
 - SIEM (security information and event management) system, 362–363
 - writing, 392
 - RUM (real user monitoring), 69, 74, 286, 676
 - runtime data integrity check, 330, 678
 - runtime debugging, 332, 493–494, 660, 678
- ## S
- S (Scope) metric, 27
 - SaaS (Software as a Service), 21, 71, 127, 495, 681
 - SABSA framework, 559–560, 679
 - safe harbor, 514
 - Safe Harbor Privacy Principles, 514
 - Safe Mode, 477
 - SafeBack Version 2.0, 393
 - safeguards, 47
 - SAML (Security Assertion Markup Language), 221–222, 287, 680
 - Samsung eFuse, 303
 - sandbox tools, 393
 - Sandboxie, 392
 - sandboxing, 327, 392–394, 668
 - sanitization, 460, 679
 - Sarbanes-Oxley Act (SOX), 55, 511, 679
 - SAS (Statement on Auditing Standards), 573
 - SCADA (Supervisory Control and Data Acquisition), 114–117
 - /SCANBOOT switch (SFC), 341
 - /SCANFILE switch (SFC), 341
 - /SCANNOW switch (SFC), 341
 - /SCANONCE switch (SFC), 341
 - scans/sweeps, 49–62, 476
 - active versus passing, 43–44
 - cloud-based, 495–496

- secure enclave, 307, 679
 - TE (Trusted Execution), 305
- Secure Shell (SSH), 183, 242, 679
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS), 199, 241, 681
- Secure View 4, 494
- secured memory, 330, 680
- securiCAD, 407
- Security Assertion Markup Language (SAML), 221–222, 287, 680
- security awareness training, 452–453
- Security Compliance Toolkit (SCT), 570
- Security Content Automation Protocol (SCAP), 44, 49, 426–427, 680, 682
- security controls, 538–539
- security engineering, 33, 680
- security information and event management system. *See* SIEM (security information and event management) system
- security level classification, 455
- security parameter index (SPI), 198
- security regression testing, 273, 680
- SecurStar DriveCrypt, 300
- segmentation, 180–185, 458–459
 - definition of, 680
 - jumpboxes, 183–184, 668
 - physical, 180–181
 - scans, 56
 - system isolation, 184–185
 - virtual, 182–183
- self-encrypting drives, 308
- Sender Policy Framework (SPF), 369, 680
- senior leadership, response coordination by, 438
- sensitive personal information (SPI), 441, 680
- sensitivity of data, 165, 411, 412, 439, 680
- sensors, 111, 115
- server-based application virtualization, 208
- server-based scans, 52
- serverless architecture, 128–129
- servers
 - authentication, 281, 655
 - 802.1X, 389
 - RADIUS (Remote Authentication Dial-in User Service), 389–391
 - TACACS+ (Terminal Access Controller Access Control System Plus), 389–391
 - exploit techniques, 337–338
 - proxy, 356–357
- service interruption, 481
- Service Organization Control (SOC) reports, 574
- Service Provisioning Markup Language (SPML), 220, 680
- service-level agreements (SLAs), 62, 515, 539, 680
- service-oriented architecture (SOA), 287, 680
- services
 - cloud service models, 127–128
 - exploit techniques, 338–339
 - push notification, 100
 - restoration of, 462
- SESAME, 219, 679
- session hijacking, 158, 681
- session keys, 234
- session management, 276–277
- SFC (System File Checker), 340–341, 479
- SFC command, 340–341
- SGX (Software Guard Extensions), 131
- SHA (Secure Hash Algorithm), 240, 371, 499
- “sheep dip” computers, 393
- Shibboleth, 224, 681
- Short Message Service (SMS), 103
- shoulder surfing, 336
- S-HTTP (Secure HTTP), 241–242

- side-channel attacks, 106
- SIEM (security information and event management) system, 48, 166, 361–365, 426, 458
 - agent-based collection, 362
 - agentless collection, 362
 - dashboard, 363–365
 - definition of, 680
 - known-bad Internet Protocol, 363
 - rule writing, 362–363
- Sigma, 366
- signatures
 - digital, 245–246, 371, 661
 - malware, 391–392
 - signature blocks, 372
 - signature-based IDSs, 57
- Silent Runners.vbs, 393
- Simple Certificate Enrollment Protocol (SCEP), 258, 681
- Simple Object Access Protocol (SOAP), 131, 220, 287, 681
- single event rules, 363
- single loss expectancy (SLE), 534, 681
- single sign-on (SSO), 214–217
 - advantages and disadvantages of, 214–215
 - definition of, 681
 - Kerberos, 215–217
- sinkholing, 391, 681
- site accreditation. *See* accreditation
- site-to-site VPNs (virtual private networks), 196
- Skylake, 131
- SLA (service-level agreement), 62, 515, 539, 680
- SLE (single loss expectancy), 534, 681
- smart cards, 213
- smart cities, 104. *See also* IoT (Internet of Things)
- smart homes, 104. *See also* IoT (Internet of Things)
- SMS (Short Message Service), 103
- snooping, DHCP, 154, 661
- Snort, 359
- SOA (service-oriented architecture), 287, 680
- SOAP (Simple Object Access Protocol), 131, 220, 287, 681
- SOC (Service Organization Control) reports, 574, 681
- SoC (system-on-chip), 105, 265
 - central security breach response, 265–266
 - definition of, 683
 - secure booting, 265
- SOCKS firewall, 60
- Software as a Service (SaaS), 21, 71, 127, 495, 681
- software assessment methods, 72–76, 272–275
 - code review, 273–274, 275, 286–287
 - dynamic analysis, 74, 286, 662
 - fuzzing, 75–76, 665
 - reverse engineering, 75
 - SDLC (software development life cycle), 72–76
 - security regression, 273, 680
 - security testing, 274–275
 - static analysis, 73–74, 286, 682
 - stress testing, 272–273
 - user acceptance testing, 272, 685
- software assurance. *See also* software assessment methods
 - DevOps, 270–272
 - DevSecOps, 270–272
 - dynamic analysis, 286
 - microservices, 288–289, 670
 - platforms, 256–266
 - client/server, 263
 - embedded systems, 105–265
 - firmware, 266
 - mobile, 256–266
 - SoC (system-on-chip), 105, 265
 - web application, 260–262

- REST (REpresentational State Transfer), 288
- SAML (Security Assertion Markup Language), 287
- SDLC (software development life cycle), 267–270
- secure coding, 275–285
 - authentication, 277–285
 - data protection, 285
 - input validation, 275–276, 382
 - output encoding, 276
 - parameterized queries, 285
 - session management, 276–277
- SOA (service-oriented architecture), 287, 680
- SOAP (Simple Object Access Protocol), 287
 - unauthorized software, 477–478
- software development life cycle (SDLC), 72–73, 267–270, 681
- Software Guard Extensions (SGX), 131
- Software Verify, OutputDebugString Checker, 494
- software-defined networking (SDN), 193–194, 681
- software-defined storage (SDS), 194
- softwareverify, 332
- Sophos SafeGuard, 300
- Sourcefire, 358
- source/subscriber model, 9
- sovereignty, 514–515, 660
- SOX (Sarbanes-Oxley Act), 55, 511, 679
- spam, 370
- spear phishing, 22, 369
- SPF (Sender Policy Framework), 369, 680
- SPI (security parameter index), 198
- SPI (sensitive personal information), 441, 680
- Splunk, 364
- SPML (Service Provisioning Markup Language), 220, 680
- spoofing
 - ARP, 154
 - e-mail, 368
 - switch, 156–158
- sprawl, VM, 204
- spyware, 325, 681
- SQL (Structured Query Language)
 - injection, 145–146, 682
- SRK (storage root key), 300
- SSAE (Statement on Standards for Attestation Engagements), 573
- SSH (Secure Shell), 183, 242, 679
- SSL (Secure Sockets Layer)/TLS (Transport Layer Security), 199, 241, 681
- SSO (single sign-on), 214–217
 - advantages and disadvantages of, 214–215
 - definition of, 681
 - Kerberos, 215–217
- stakeholders, communication with
 - communication plans, 435–436
 - response coordination, 436–438
- standard word passwords, 564, 682
- state sponsors, 12, 405
- stateful firewalls, 59
- stateful matching, 57
- Statement on Auditing Standards (SAS), 573
- Statement on Standards for Attestation Engagements (SSAE), 573
- static analysis, 73–74, 286, 682
- static passwords, 564, 682
- statistical anomaly-based IDSs, 58
- stealth viruses, 324
- steganography, 510
- step-up authentication, 277
- sticky keyword, 394
- sticky MAC, 394, 682
- STIX (Structured Threat Information eXpression), 8, 682
- storage. *See also* cloud computing

- nonremovable, 99
 - removable, 99
 - RTS (Root of Trust for Storage), 298
 - SDS (software-defined storage), 194
 - uncontrolled, 99
 - vulnerabilities with, 99–100
 - storage keys, 300
 - storage root key (SRK), 300
 - strcpy function, 168, 682
 - stream-based ciphers, 234–235, 682
 - stress testing, 272–273, 682
 - stretching, key, 134
 - string searches, 366, 682
 - Structured Query Language (SQL)
 - injection, 145–146, 682
 - Structured Threat Information
 - eXpression (STIX), 8, 682
 - study trackers, 580
 - Stuxnet virus, 115
 - subnets, screened, 62, 679
 - sudo command, 81
 - Supervisory Control and Data Acquisition (SCADA), 114–117
 - suplicants, 281, 389, 682
 - supply chain assessment, 543–544
 - hardware source authenticity, 544
 - vendor due diligence, 543
 - Susteen Secure View 4, 494
 - swatch, 166
 - sweeps. *See* scans/sweeps
 - switches
 - rogue, 475
 - spoofing, 156–158
 - switchport mode access command, 157
 - switchport mode trunk command, 157
 - switchport port security command, 394
 - switchport port security maximum 2
 - command, 394
 - switchport port security violation restrict
 - command, 394
 - Symantec Endpoint Protection, 387
 - symmetric algorithms, 233–236, 682
 - block ciphers, 235–236, 656
 - stream-based ciphers, 234–235, 682
 - SYN flag, 76
 - SYN flood, 80, 490, 682
 - synthetic transaction monitoring, 69, 74, 286, 682
 - Sysinternals, 408, 498, 683
 - syslog, 350–352
 - Syslog Server (Kiwi), 352
 - system apps, 98
 - system behavior, 333–339
 - anomalous behavior, 334–335
 - exploit techniques, 335–339
 - file system, 339–340
 - rogue access points, 336, 678
 - rogue endpoints, 336
 - servers, 337–338
 - services, 338–339
 - social engineering, 335–336
 - known-good behavior, 333–334
 - System Center Operations Manager (SCOM), 69, 74, 286
 - System File Checker (SFC), 340–341, 479
 - system hardening, 410
 - system high security mode (MAC), 228
 - system isolation, 184–185
 - system lockdown, 410
 - system process criticality, 457
 - system-on-chip. *See* SoC (system-on-chip)
 - systems assessment, 539–541
 - Systems Manager, 98
- ## T
- tables, memory
 - GPT (GUID partition table), 303
 - how to use, 582
 - tabletop exercises, 543, 683
 - TACACS+ (Terminal Access Controller Access Control System Plus), 281–282, 389–391
 - tagging assets, 178, 654

- taint analysis, 73
- Task Manager, 407, 478
- tasks, unauthorized, 480
- TAXII (Trusted Automated eXchange of Indicator Information), 8–9, 684
- tcpdump, 490, 683
- TE (Trusted Execution), 305
- teams, hunt, 247, 666
- technical controls, 516–521, 571, 683
- technical threats, 10
- telemetry system, 115, 683
- TEMPEST, 337
- Tenable PVS, 43
- Terminal Access Controller Access Control System Plus (TACACS+), 281–282, 389–391
- terminal services, 208
- terrorist group threat actors, 12, 405
- test data method, 269
- test preparation. *See* exam preparation process
- testing, 274–275, 453
 - security regression, 273, 680
 - stress, 272–273, 682
 - test data method, 269
 - user acceptance, 272, 685
- text messaging, 103
- TGT (ticket-granting ticket), 218
- threat actors
 - categories of, 9–10, 12–13
 - definition of, 12, 683
 - hostile versus non-hostile, 30
 - identification of, 405–406
 - internal versus external, 29–30
- threat classification, 9–11
 - APTs (advanced persistent threats), 11, 653
 - known threats, 10, 669
 - unknown threats, 10, 685
 - zero-day vulnerabilities, 10–11, 687
- threat feed, 426, 683
- threat hunting. *See also* threat actors
 - attack surface area, reduction of, 409–410
 - configuration lockdown, 410, 659
 - system hardening, 410
 - attack vectors, 412–413
 - critical assets, bundling, 411–412
 - commercial business classifications, 411
 - data classification policy, 411
 - distribution of critical assets, 412
 - military and government classifications, 412
 - sensitivity and criticality, 411
 - detection capabilities, improvement of, 413–414
 - hypotheses, 404–405
 - integrated intelligence, 413, 667
 - tactics for, 406–409
 - executable process analysis, 407–408, 663
 - hunt teaming, 406
 - memory consumption, 409
 - threat models, 406–407
- threat intelligence. *See also* attacks; vulnerability management
 - attack frameworks
 - definition of, 21, 655
 - Diamond Model of Intrusion Analysis, 22–23, 661
 - kill chain, 23, 669
 - MITRE ATT&CK, 21–22, 670
 - definition of, 683
 - intelligence sources, 6–7, 683
 - accuracy of, 7
 - confidence levels for, 7, 659
 - intelligent networks, 427
 - OSINT (open-source intelligence), 6, 672
 - proprietary/closed-source intelligence, 6, 675
 - relevance of, 7
 - timeliness of, 7, 684

- sharing, 33–34
 - threat modeling, 29–32, 683
 - adversary capability, 29–30
 - attack vectors, 31–32, 412–413
 - impact, 32
 - probability, 32
 - total attack surface, 31, 684
 - threat research, 23–29. *See also* IOCs (indicators of compromise)
 - behavioral analysis, 24–25
 - CVSS (Common Vulnerability Scoring System), 25–29, 44, 412
 - reputational scores, 24
 - Threat Modeling Tool, 406
 - ThreatConnect, 426
 - ThreatModeler, 406
 - ThreatQuotient, 426
 - throughput rate, 282
 - ticket-granting ticket (TGT), 218
 - timeliness, 7, 684
 - time-of-check/time-of-use attacks, 260, 684
 - TLP (Traffic Light Protocol), 25
 - TLS (Transport Layer Security), 117, 199, 241, 681
 - TOGAF (The Open Group Architecture Framework), 554, 683
 - token devices, 213
 - tokenization, 517, 684
 - tool-assisted review, 74, 274
 - top secret data, 412
 - total attack surface, 31, 684
 - TPM (Trusted Platform Module), 299–300, 684
 - tracking rules, 363
 - trade secrets, 443, 684
 - trademarks, 443, 684
 - traditional botnets, 473, 684
 - traffic
 - spikes in, 476
 - traffic anomaly-based IDSs, 58
 - Traffic Light Protocol (TLP), 25
 - training/education, 452–453, 542–543
 - transfer of risk, 47, 538, 678
 - transitive rules, 363
 - transport encryption, 240–242
 - Transport Layer Security (TLS), 117, 199, 241, 681
 - trapdoors, 338, 656
 - trend analysis, 320, 684
 - Trend Micro Maximum Security, 300
 - trending rules, 363
 - Tripwire, 340
 - Trojan horses, 325, 684
 - true negatives, 44, 684
 - true positives, 44, 684
 - Trusted Automated eXchange of Indicator Information (TAXII), 8–9, 684
 - Trusted Execution (TE), 305
 - trusted firmware updates, 308–309
 - attestation, 300, 310–311, 655
 - IMA (Integrity Measurement Architecture), 311
 - measured boot, 310–311, 670
 - measured launch, 311
 - Trusted Foundry program, 304–305, 544
 - Trusted Platform Module (TPM), 299–300, 684
 - trusted relationships, 22
 - trusted third-party federation model, 219
 - Twofish, 235
 - Type 1 hypervisors, 203, 684
 - Type 2 hypervisors, 203, 684
- ## U
- UAT (user acceptance testing), 272
 - UEBA (user and entity behavior analytics), 24, 341, 685
 - UEFI (Unified Extensible Firmware Interface), 303–304, 685
 - UI (User Interaction) metric, 27
 - unauthorized access, 183
 - unauthorized changes, 479

- unauthorized privilege, 479
 - unauthorized scheduled tasks, 480
 - unauthorized software, 477–478
 - unclassified data, 412
 - uncontrolled storage, 99
 - uncredentialed scans, 476, 685
 - Unicode, 276
 - Unified Extensible Firmware Interface (UEFI), 303–304, 685
 - unified threat management (UTM), 383
 - uniform resource locators. *See* URLs (uniform resource locators)
 - unintentional insider threats, 13
 - United States Federal Sentencing Guidelines, 512, 685
 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. *See* USA PATRIOT Act
 - universal serial bus (USB), 102
 - unknown threats, 10, 685
 - unsigned apps, 98
 - updates
 - exam, 651–652
 - trusted firmware, 308–309
 - URG flag, 76
 - urgent resources, 456
 - URLEncode, 261
 - URLs (uniform resource locators)
 - analysis of, 342
 - encoding of, 276
 - U.S. Government Configuration Baseline (USGCB), 323
 - USA PATRIOT Act, 438, 513, 685
 - USB (universal serial bus), 102
 - USB OTG (USB On-The-Go), 99–100, 685
 - user acceptance testing, 272, 685
 - user and entity behavior analytics (UEBA), 24, 341, 685
 - user identification, 210
 - User Interaction (UI) metric, 27
 - usermode debugger, 457, 685
- V**
- Valgrind, 329
 - VDI (virtual desktop infrastructure), 207, 686
 - vectors, attack, 31–32, 412–413
 - vehicles, 111–113
 - CAN (Controller Area Network) bus, 112, 659
 - drones, 113
 - vendor due diligence, 543
 - verification testing, 269
 - /VERIFYFILE switch (SFC), 341
 - /VERIFYONLY switch (SFC), 341
 - Verisign, 244
 - vertical privilege escalation, 152
 - Vetting the Security of Mobile Applications*, 258–259
 - video game DRM (digital rights management), 520
 - video systems, IP, 109–111
 - virtual SAN, 686
 - virtual TPM, 686
 - virtualization
 - advantages and disadvantages of, 201–202
 - application streaming, 208
 - attacks and vulnerabilities, 203–206
 - digital forensics for, 497
 - hypervisors, 202–203
 - management interface, 205
 - terminal services, 208
 - VDI (virtual desktop infrastructure), 207, 686
 - virtual private networks. *See* VPNs (virtual private networks)
 - virtual SAN, 686
 - virtual segmentation, 182–183
 - virtual TPM, 686

- VLANs (virtual LANs), 156–158, 182–183, 458
- VMs (virtual machines)
 - attacks and vulnerabilities, 201–204
 - digital forensics for, 497
- VPC (virtual private cloud), 195, 686
- VPNs (virtual private networks), 196–199
 - definition of, 195, 686
 - IPsec, 197–199
 - remote-access, 196
 - site-to-site, 196
 - SSL/TLS, 199, 681
 - VPN concentrators, 196
- VSAN (virtual storage area network), 194
- VTPM (virtual Trusted Platform Module), 300–301
- viruses, 115, 323–324, 686
- VLANs (virtual LANs), 182–183, 458
 - advantages and disadvantages of, 156
 - VLAN-based attacks, 156–158
- VMs (virtual machines)
 - attacks and vulnerabilities, 201–204
 - digital forensics for, 497
- VMware, 311
 - VMware vSphere, 203
 - VMware Workstation, 203
- volatile memory, 329
- VPC (virtual private cloud), 195, 686
- VPNs (virtual private networks), 196–199
 - definition of, 195, 686
 - IPsec, 197–199
 - remote-access, 196
 - site-to-site, 196
 - SSL/TLS, 199, 681
 - VPN concentrators, 196
- VSAN (virtual storage area network), 194
- vSphere, 203
- VTPM (virtual Trusted Platform Module), 300–301
- vulnerability assessment output. *See also* vulnerability management
 - cloud infrastructure assessment tools, 86–88
 - Pacu, 87–88, 673
 - Prowler, 87, 675
 - ScoutSuite, 87, 679
 - enumeration, 76–82
 - active versus passive, 82, 653, 673
 - definition of, 76
 - host scanning, 79, 666
 - hping, 80–82
 - Nmap, 76–79, 671
 - Responder, 82, 677
 - infrastructure vulnerability scanners, 71–496
 - software assessment tools, 72–76
 - dynamic analysis, 74, 286, 662
 - fuzzing, 75–76, 665
 - reverse engineering, 75
 - SDLC (software development life cycle), 72–73
 - static analysis, 73–74, 286, 682
 - web application scanners, 69–70
 - wireless assessment tools, 82–86
 - Aircrack-ng, 83, 654
 - oclHashcat, 86, 672
 - Reaver, 84–86, 676
- vulnerability feeds, 49, 686
- vulnerability management. *See also* data analysis
 - definition of, 686
 - firewalls. *See* firewalls
 - identification, 41–44
 - active versus passive scanning, 43–44
 - assessment goals, 41–42
 - asset criticality, 42–43, 654

- mapping and enumeration, 44
 - overview of, 33
 - remediation/mitigation, 45
 - compensating controls, 47, 658
 - configuration baseline, 45–46, 659
 - hardening, 46–47, 665, 683
 - inhibitors to, 62–63
 - patching, 46, 48, 673
 - risk acceptance, 47, 677
 - verification of, 47
 - scans/sweeps, 49–62, 476
 - cloud-based, 495–496
 - credentialed versus non-credentialed, 51, 660
 - criteria for, 53–62
 - internal versus external, 53, 663, 667
 - risks associated with, 49–62
 - scope, 49–50
 - server-based versus agent-based, 52
 - verification of, 48
 - vulnerability feeds, 49, 686
 - for specialized technology
 - automation systems, 109
 - embedded systems, 105–264, 663
 - FGPA (field programmable gate array), 105–106
 - HVAC controllers, 111
 - ICS (Incident Command System), 114
 - IoT (Internet of Things), 103–104, 668
 - IP video systems, 109–111
 - mobile devices, 97–103
 - Modbus, 117, 118, 670
 - physical access control, 106–109
 - RTOSs (real-time operating systems), 105, 676
 - SCADA (Supervisory Control and Data Acquisition), 114–117
 - sensors, 111
 - SoC (system-on-chip), 105, 265–266, 683
 - vehicles and drones, 111–113
 - workflow and process automation
 - systemsworkflow and process automation systems, 113
 - validation, 44–48
 - virtualization, 203–206
 - vulnerability assessment output
 - cloud infrastructure assessment tools, 86–88
 - enumeration, 76–82
 - infrastructure vulnerability scanner, 71–496
 - software assessment tools, 72–76
 - web application scanners, 69–70
 - wireless assessment tools, 82–86
 - vulnerability types, 163–168
 - broken authentication, 164–165
 - code reuse, 166
 - dereferencing, 163, 661
 - improper error handling, 163
 - insecure components, 165–166
 - insecure functions, 168
 - insecure object reference, 163, 667
 - insufficient logging and monitoring, 166
 - race conditions, 164, 676
 - sensitive data exposure, 165
 - weak or default configurations, 167–168
 - zero-day vulnerability, 269
 - vulnerability mitigation. *See* remediation/mitigation
- ## W
- WAF (web application firewall), 355–356, 686
 - war game exercises, 542–543
 - wash command, 85–86
 - watermarking, 521, 661
 - web application firewall (WAF), 355–356, 686
 - web application platforms, 260–262

- click-jacking, 262, 657
 - CSRF (cross-site request forgery), 261–262, 660
 - maintenance hooks, 260
 - time-of-check/time-of-use attacks, 260, 684
 - web application scanners, 69–70
 - Arachni, 70–496, 654
 - Burp Suite, 69, 656
 - Nessus Professional, 71
 - Nikto, 70, 671
 - OpenVAS, 71–72
 - OWASP Zed Attack Proxy (ZAP), 69
 - Qualys, 496, 676
 - types of, 69
 - web vulnerability scanners, 69, 686
 - whaling, 370
 - white hats, 406
 - white teams, 543, 686
 - white-box testing, 274–275
 - whitelisting, 275, 381, 687
 - Wi-Fi hacking gear, 475
 - Wi-Fi Protected Access (WPA), 134
 - Windows computers
 - DPAPI (Data Protection API), 131, 660
 - Group Policy, 45, 184, 381, 570
 - least privilege, principle of, 338
 - Measured Boot, 311
 - Process Explorer, 408, 675
 - Secure Boot, 310–311
 - SFC (System File Checker), 340
 - Task Manager, 407
 - Windows Server managed service accounts, 339
 - Windows Defender, 353
 - Windows PowerShell, 423
 - Winload (Windows Boot Loader), 310
 - wiping, remote, 257, 677
 - WIPO (World Intellectual Property Organization), 444
 - WIPS (a wireless intrusion prevention system), 475
 - WIPS (wireless intrusion prevention system), 336, 687
 - wireless assessment tools, 82–86
 - Aircrack-ng, 83, 654
 - oclHashcat, 86, 672
 - Reaver, 84–86, 676
 - wireless intrusion prevention system (WIPS), 336, 475, 687
 - wireless key loggers, 475, 687
 - Wireshark, 394, 488–490, 687
 - work product retention policy, 570, 687
 - work recovery time (WRT), 455, 687
 - workflow
 - automation systems for, 113
 - orchestration of, 422–423, 687
 - scans and, 53
 - World Intellectual Property Organization (WIPO), 444
 - worms, 324, 687
 - WPA (Wi-Fi Protected Access), 134
 - WRT (work recovery time), 455, 687
- X**
- X.509 certificates, 243–244
 - XACML (Extensible Access Control Markup Language), 143–144, 220, 663
 - XenServer, 203
 - XMAS scans, 78–79, 687
 - XML (Extensible Markup Language)
 - attacks, 143–144, 663
 - XN (never execute) bit, 307
 - XRY, 494
 - XSS (cross-site scripting), 160–162
 - definition of, 660
 - DOM (document object model), 162, 662
 - example of, 160–161

persistent, 161, 673
reflective, 161, 677

Y-Z

ZAP, 687
Zebra Technologies AirDefense, 475
Zed Attack Proxy (ZAP), 69

Zeek, 360
Zero Knowledge Proof, 236
zero-day vulnerability, 10–11, 269, 320,
687
zero-knowledge testing, 274–275
zombies, 325