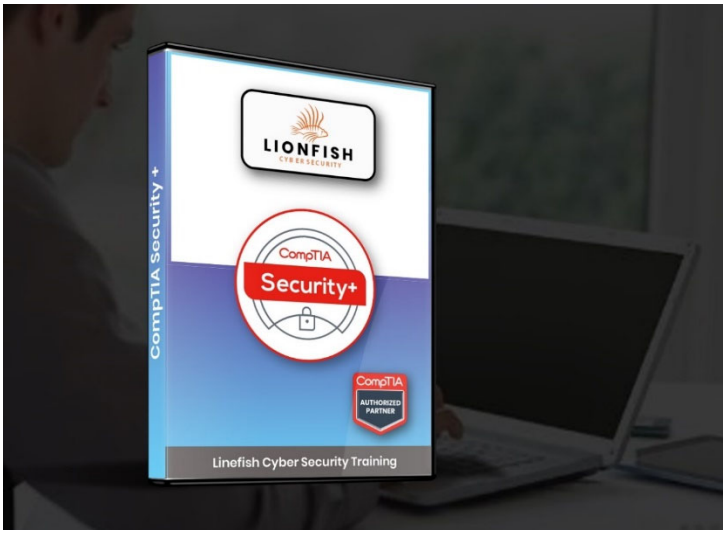
Lionfish Cyber Security Course Syllabus:

CompTIA Security+

- 40+ hours of virtual training, practice exams, and study.
- Receive a Certificate of completion
- Virtual class, self-paced
- 12 Months Access *(Unless indicated otherwise)*



DESCRIPTION

CompTIA Security+ focuses in on the latest trends in risk management, risk mitigation, threat management, and intrusion detection. This certification will allow you to demonstrate your cybersecurity skills and abilities to employers.

CURRICULUM

Overview

CompTIA Security+ is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important steppingstone of an IT security career.

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them. Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Objectives

- Provide operational, information, application and infrastructure level security
- Secure the network to maintain availability, integrity, and confidentiality of critical information
- Operate within a set of rules, policies, and regulations wherever applicable
- Comprehend Risk identification and mitigation

Prerequisites

IT security professionals with a minimum of two years' experience in IT administration with a focus on security; users with basic day-to-day technical information security experience; those interested in gaining a broader and deeper knowledge of security concerns and implementation; and learners preparing for the Security+ exam

Target Audience

- The series is intended for aspiring IT security professionals entering into security.
- The professionals who are Systems Administrator Network Administrator Security Administrator Junior IT Auditor/Penetration Tester

CURRICULUM Syllabus

See appendix A

See appendix B

Overview

Prepare for the CompTIA Security+ exam with the excellent practice tests. Enabling you to practice on test questions and assess your skill and knowledge of the material. Get certified the best way

- Applies to the current SY0-501 exam
- Includes many practices questions
- Requires Windows, macOS, Chrome OS, or Linux (iOS and Android not supported)
- Single-user license

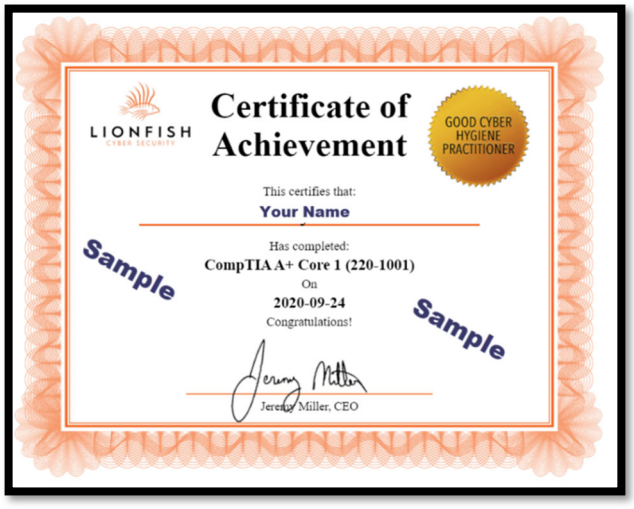
Learn includes:

- **Interactive learning with flashcards and performance-based questions.**
- **Videos that demonstrate key concepts and processes.**
- **Customizable learning plan.**
- **Easy self-assessments.**
- **Learning progress analytics and reporting.**

LIONFISH CYBER SECURITY™

Training Center

Sample Certificate upon completions of each course



To learn more, contact us at 877-732-6772 or info@lionfishcybersecurity.com

www.LionfishCyberSecurity.com

LIONFISH CYBER SECURITY™

Training Center

101 West Ohio Street, Suite 2000, Indianapolis, In 46204

This institution is regulated by the Office for Career and Technical Schools - 10 N Senate Avenue, Suite SE 308, Indianapolis 46204 - OCTS@dwd.in.gov
http://www.in.gov/dwd/2731.htm

CMMC-AB Registered Provider Organization™

Appendix B

Mapping Course Content to Time Security+® Core 2 (Exam 220-1102)

Achieving CompTIA Security+ certification requires candidates to pass Exams SYO-601. This table describes where the exam objectives for Exam SYO-601 covered in this course.

Leason and Instruction

Getting Started with CertMaster Learn | 1 Task | 7 Knowledge Points

Getting Started with CertMaster Learn

. 7 knowledge points. Estimated time to complete: Less Than 15 Minutes.7 Knowledge Points | Less Than 15 Minutes

_

Lesson 1: Comparing Security Roles and Security Controls | 6 Tasks | 72 Knowledge Points

Topic 1A: Compare and Contrast Information Security Roles

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Review Activity: Information Security Roles

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

Topic 1B: Compare and Contrast Security Control And Framework

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Review Activity: Security Control and Framework

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

PBQ 1B: Compare and Contrast Security Control and Framework Types

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Lesson 1: Practice Questions

. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

_

Lesson 2: Explaining Threat Actors and Threat Intelligence | 5 Tasks | 65 Knowledge Points

Topic 2A: Explain Threat Actor Types and Attack Vectors

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Review Activity: Threat Actor Types and Attack Vectors

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Topic 2B: Explain Threat Intelligence Sources

. 17 knowledge points. Estimated time to complete: 15-30 Minutes.17 Knowledge Points | 15-30 Minutes

Review Activity: Threat Intelligence Sources

. 6 knowledge points. Estimated time to complete: Less Than 15 Minutes.6 Knowledge Points | Less Than 15 Minutes

Lesson 2: Practice Questions

. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

_

Lesson 3: Performing Security Assessments | 14 Tasks | 227 Knowledge Points

Topic 3A: Assess Organizational Security with Network

. 37 knowledge points. Estimated time to complete: 30-60 Minutes.37 Knowledge Points | 30-60 Minutes

Review Activity: Organizational Security with Network Reconnaissance Tools

. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes

Assisted Lab: Exploring the Lab Environment

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Assisted Lab: Scanning and Identifying Network Nodes
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
PBQ 3A: Assess Organizational Security with Network Reconnaissance Tools
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Topic 3B: Explain Security Concerns with General Vulnerability Types
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Review Activity: Security Concerns with General Vulnerability Types
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Topic 3C: Summarize Vulnerability Scanning Techniques
. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes
Review Activity: Vulnerability Scanning Techniques
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 3D: Explain Penetration Testing Concepts
. 13 knowledge points. Estimated time to complete: Less Than 15 Minutes.13 Knowledge Points | Less Than 15 Minutes
Review Activity: Penetration Testing Concepts
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Lesson 3: Practice Questions
. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Lesson 4: Identifying Social Engineering and Malware | 9 Tasks | 142 Knowledge Points

Topic 4A: Compare and Contrast Social Engineering Techniques
. 18 knowledge points. Estimated time to complete: 15-30 Minutes.18 Knowledge Points | 15-30 Minutes
Review Activity: Social Engineering Techniques
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
PBQ 4A: Compare and Contrast Social Engineering Techniques
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Topic 4B: Analyze Indicators of Malware-Based Attacks
. 19 knowledge points. Estimated time to complete: 15-30 Minutes.19 Knowledge Points | 15-30 Minutes
Review Activity: Indicators of Malware-Based Attacks
. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes
PBQ 4B: Analyze Indicators of Malware-Based Attacks
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Lesson 4: Practice Questions
. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes
APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Lesson 5: Summarizing Basic Cryptographic Concepts | 10 Tasks | 127 Knowledge Points

Topic 5A: Compare and Contrast Cryptographic Ciphers
. 26 knowledge points. Estimated time to complete: 15-30 Minutes.26 Knowledge Points | 15-30 Minutes
Review Activity: Cryptographic Ciphers
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
Topic 5B: Summarize Cryptographic Modes of Operation
. 7 knowledge points. Estimated time to complete: Less Than 15 Minutes.7 Knowledge Points | Less Than 15 Minutes
Review Activity: Cryptographic Modes of Operation
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
PBQ 5B: Summarize Cryptographic Modes of Operation
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
. 13 knowledge points. Estimated time to complete: Less Than 15 Minutes.13 Knowledge Points | Less Than 15 Minutes
Review Activity: Cryptographic Use Cases and Weaknesses
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Topic 5D: Summarize Other Cryptographic Technologies
. 4 knowledge points. Estimated time to complete: Less Than 15 Minutes.4 Knowledge Points | Less Than 15 Minutes
Review Activity: Other Cryptographic Technologies
. 4 knowledge points. Estimated time to complete: Less Than 15 Minutes.4 Knowledge Points | Less Than 15 Minutes
Lesson 5: Practice Questions
. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Lesson 6: Implementing Public Key Infrastructure | 8 Tasks | 105 Knowledge Points

Topic 6A: Implement Certificates and Certificate Authorities
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Review Activity: Certificates and Certificate Authorities
. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes
PBQ 6A: Implement Certificates and Certificate Authorities
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Managing the Life Cycle of a Certificate
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 6B: Implement PKI Management
. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes
Review Activity: PKI Management
. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Managing Certificates with OpenSSL
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Lesson 6: Practice Questions
. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

_

Lesson 7: Implementing Authentication Controls | 12 Tasks | 163 Knowledge Points

Topic 7A: Summarize Authentication Design Concepts
. 9 knowledge points. Estimated time to complete: Less Than 15 Minutes.9 Knowledge Points | Less Than 15 Minutes
Review Activity: Authentication Design Concepts
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
Topic 7B: Implement Knowledge-Based Authentication
. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes
Review Activity: Knowledge-Based Authentication
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
PBQ 7B: Implement Knowledge-Based Authentication
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Auditing Passwords with a Password Cracking Utility
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 7C: Implement Authentication Technologies
. 18 knowledge points. Estimated time to complete: 15-30 Minutes.18 Knowledge Points | 15-30 Minutes
Review Activity: Authentication Technologies
. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Managing Centralized Authentication
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 7D: Summarize Biometrics Authentication Concepts
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Review Activity: Biometrics Authentication Concepts
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
Lesson 7: Practice Questions
. 38 knowledge points. Estimated time to complete: 30-60 Minutes.38 Knowledge Points | 30-60 Minutes

_

Lesson 8: Implementing Identity and Account Management Controls | 15 Tasks | 234 Knowledge Points

Topic 8A: Implement Identity and Account Types

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Review Activity: Identity and Account Types

. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes

Topic 8B: Implement Account Policies

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Review Activity: Account Policies

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

PBQ 8B: Implement Account Policies

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Managing Access Controls in Windows Server

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Assisted Lab: Configuring a System for Auditing Policies

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 8C: Implement Authorization Solutions

. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

Review Activity: Authorization Solutions

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Managing Access Controls in Linux

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 8D: Explain the Importance of Personnel Policies

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Review Activity: Importance of Personnel Policies

. 6 knowledge points. Estimated time to complete: Less Than 15 Minutes.6 Knowledge Points | Less Than 15 Minutes

Lesson 8: Practice Questions

. 42 knowledge points. Estimated time to complete: 30-60 Minutes.42 Knowledge Points | 30-60 Minutes

Lesson 8 PBQ: Implement Identity, Account Types, and Account Policies

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

APPLIED LAB: Configuring Identity and Access Management Controls

. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Lesson 9: Implementing Secure Network Designs | 12 Tasks | 181 Knowledge Points

Topic 9A: Implement Secure Network Designs

. 18 knowledge points. Estimated time to complete: 15-30 Minutes.18 Knowledge Points | 15-30 Minutes

Review Activity: Secure Network Designs

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Topic 9B: Implement Secure Switching and Routing

. 18 knowledge points. Estimated time to complete: 15-30 Minutes.18 Knowledge Points | 15-30 Minutes

Review Activity: Secure Switching and Routing

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

PBQ 9B: Implement Secure Switching and Routing

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Implementing a Secure Network Design

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 9C: Implement Secure Wireless Infrastructure

. 25 knowledge points. Estimated time to complete: 15-30 Minutes.25 Knowledge Points | 15-30 Minutes

Review Activity: Secure Wireless Infrastructure

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

PBQ 9C: Implement Secure Wireless Infrastructure

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 9D: Implement Load Balancers

. 13 knowledge points. Estimated time to complete: Less Than 15 Minutes.13 Knowledge Points | Less Than 15 Minutes

Review Activity: Load Balancers

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Lesson 9: Practice Questions

. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Lesson 10: Implementing Network Security Appliances | 10 Tasks | 138 Knowledge Points

Topic 10A: Implement Firewalls and Proxy Servers

. 23 knowledge points. Estimated time to complete: 15-30 Minutes.23 Knowledge Points | 15-30 Minutes

Review Activity: Firewalls and Proxy Servers

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

PBQ 10A: Implement Firewalls and Proxy Servers

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Configuring a Firewall

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 10B: Implement Network Security Monitoring

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Review Activity: Network Security Monitoring

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Configuring an Intrusion Detection System

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 10C: Summarize the Use of SIEM

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Review Activity: Use of SIEM

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Lesson 10: Practice Questions

. 28 knowledge points. Estimated time to complete: 15-30 Minutes.28 Knowledge Points | 15-30 Minutes

_

Lesson 11: Implementing Secure Network Protocols | 12 Tasks | 181 Knowledge Points

Topic 11A: Implement Secure Network Operations Protocols

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Review Activity: Secure Network Operations Protocols

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Implementing Secure Network Addressing Services

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 11B: Implement Secure Application Protocols

. 23 knowledge points. Estimated time to complete: 15-30 Minutes.23 Knowledge Points | 15-30 Minutes

Review Activity: Secure Application Protocols

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

PBQ 11B: Implement Secure Application Protocols

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 11C: Implement Secure Remote Access Protocols

. 21 knowledge points. Estimated time to complete: 15-30 Minutes.21 Knowledge Points | 15-30 Minutes

Review Activity: Secure Remote Access Protocols

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

PBQ 11C: Implement Secure Remote Access Protocols

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Implementing a Virtual Private Network

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Assisted Lab: Implementing a Secure SSH Server

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Lesson 11: Practice Questions

. 30 knowledge points. Estimated time to complete: 30-60 Minutes.30 Knowledge Points | 30-60 Minutes

_

Lesson 12: Implementing Host Security Solutions | 9 Tasks | 138 Knowledge Points

Topic 12A: Implement Secure Firmware

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Review Activity: Secure Firmware

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes
Topic 12B: Implement Endpoint Security
. 13 knowledge points. Estimated time to complete: Less Than 15 Minutes.13 Knowledge Points | Less Than 15 Minutes
Review Activity: Endpoint Security
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Implementing Endpoint Protection
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 12C: Explain Embedded System Security Implications
. 19 knowledge points. Estimated time to complete: 15-30 Minutes.19 Knowledge Points | 15-30 Minutes
Review Activity: Embedded System Security Implications
. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes
Lesson 12: Practice Questions
. 30 knowledge points. Estimated time to complete: 30-60 Minutes.30 Knowledge Points | 30-60 Minutes
APPLIED LAB: Securing the Network Infrastructure
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

_

Lesson 13: Implementing Secure Mobile Solutions | 6 Tasks | 76 Knowledge Points

Topic 13A: Implement Mobile Device Management
. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes
Review Activity: Mobile Device Management
. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes
PBQ 13A: Implement Mobile Device Management
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Topic 13B: Implement Secure Mobile Device Connections
. 11 knowledge points. Estimated time to complete: Less Than 15 Minutes.11 Knowledge Points | Less Than 15 Minutes
Review Activity: Secure Mobile Device Connections
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
Lesson 13: Practice Questions
. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

_

Lesson 14: Summarizing Secure Application Concepts | 16 Tasks | 237 Knowledge Points

Topic 14A: Analyze Indicators of Application Attacks
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
Review Activity: Indicators of Application Attacks
. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Identifying Application Attack Indicators
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 14B: Analyze Indicators of Web Application Attacks
. 24 knowledge points. Estimated time to complete: 15-30 Minutes.24 Knowledge Points | 15-30 Minutes
Review Activity: Indicators of Web Application Attacks
. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Identifying a Browser Attack
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes
Topic 14C: Summarize Secure Coding Practices
. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes
Review Activity: Secure Coding Practices
. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes
Topic 14D: Implement Secure Script Environments
. 11 knowledge points. Estimated time to complete: Less Than 15 Minutes.11 Knowledge Points | Less Than 15 Minutes
Review Activity: Secure Script Environments
. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes
PBQ 14D: Implement Secure Script Environments
. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes
Assisted Lab: Implementing PowerShell Security
. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Assisted Lab: Identifying Malicious Code

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 14E: Summarize Deployment and Automation Concepts

. 7 knowledge points. Estimated time to complete: Less Than 15 Minutes.7 Knowledge Points | Less Than 15 Minutes

Review Activity: Deployment and Automation Concepts

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

Lesson 14: Practice Questions

. 52 knowledge points. Estimated time to complete: 30-60 Minutes.52 Knowledge Points | 30-60 Minutes

_

Lesson 15: Implementing Secure Cloud Solutions | 8 Tasks | 120 Knowledge Points

Topic 15A: Summarize Secure Cloud and Virtualization Services

. 17 knowledge points. Estimated time to complete: 15-30 Minutes.17 Knowledge Points | 15-30 Minutes

Review Activity: Secure Cloud and Virtualization Services

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Topic 15B: Apply Cloud Security Solutions

. 25 knowledge points. Estimated time to complete: 15-30 Minutes.25 Knowledge Points | 15-30 Minutes

Review Activity: Cloud Security Solutions

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

PBQ 15B: Apply Cloud Security Solutions

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 15C: Summarize Infrastructure as Code Concepts

. 9 knowledge points. Estimated time to complete: Less Than 15 Minutes.9 Knowledge Points | Less Than 15 Minutes

Review Activity: Infrastructure as Code

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Lesson 15: Practice Questions

. 30 knowledge points. Estimated time to complete: 30-60 Minutes.30 Knowledge Points | 30-60 Minutes

_

Lesson 16: Explaining Data Privacy and Protection Concepts | 7 Tasks | 112 Knowledge Points

Topic 16A: Explain Privacy and Data Sensitivity Concepts

. 17 knowledge points. Estimated time to complete: 15-30 Minutes.17 Knowledge Points | 15-30 Minutes

Review Activity: Privacy and Data Sensitivity Concepts

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

PBQ 16A: Explain Privacy and Data Sensitivity Concepts

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 16B: Explain Privacy and Data Protection Controls

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Review Activity: Privacy and Data Protection Controls

. 6 knowledge points. Estimated time to complete: Less Than 15 Minutes.6 Knowledge Points | Less Than 15 Minutes

Lesson 16: Practice Questions

. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

APPLIED LAB: Identifying Application Attacks

. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Lesson 17: Performing Incident Response | 10 Tasks | 156 Knowledge Points

Topic 17A: Summarize Incident Response Procedures

. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes

Review Activity: Incident Response Procedures

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

PBQ 17A: Summarize Incident Response Procedures

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 17B: Utilize Appropriate Data Sources for Incident Response

. 24 knowledge points. Estimated time to complete: 15-30 Minutes.24 Knowledge Points | 15-30 Minutes

Review Activity: Appropriate Data Sources for Incident Response

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Managing Data Sources for Incident Response

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 17C: Apply Mitigation Controls

. 17 knowledge points. Estimated time to complete: 15-30 Minutes.17 Knowledge Points | 15-30 Minutes

Review Activity: Mitigation Controls

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Assisted Lab Configuring Mitigation Controls

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Lesson 17: Practice Questions

. 30 knowledge points. Estimated time to complete: 30-60 Minutes.30 Knowledge Points | 30-60 Minutes

_

Lesson 18: Explaining Digital Forensics | 6 Tasks | 74 Knowledge Points

Topic 18A: Explain Key Aspects of Digital Forensics Documentation

. 7 knowledge points. Estimated time to complete: Less Than 15 Minutes.7 Knowledge Points | Less Than 15 Minutes

Review Activity: Digital Forensics Documentation

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

. 16 knowledge points. Estimated time to complete: 15-30 Minutes.16 Knowledge Points | 15-30 Minutes

Review Activity: Digital Forensics Evidence Acquisition

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Acquiring Digital Forensics Evidence

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Lesson 18: Practice Questions

. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

_

Lesson 19: Summarizing Risk Management Concepts | 6 Tasks | 75 Knowledge Points

Topic 19A: Explain Risk Management Processes and Concepts

. 17 knowledge points. Estimated time to complete: 15-30 Minutes.17 Knowledge Points | 15-30 Minutes

Review Activity: Risk Management Processes and Concepts

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

PBQ 19A: Explain Risk Management Processes and Concepts

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 19B: Explain Business Impact Analysis Concepts

. 11 knowledge points. Estimated time to complete: Less Than 15 Minutes.11 Knowledge Points | Less Than 15 Minutes

Review Activity: Business Impact Analysis Concepts

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Lesson 19: Practice Questions

. 18 knowledge points. Estimated time to complete: 15-30 Minutes.18 Knowledge Points | 15-30 Minutes

_

Lesson 20: Implementing Cybersecurity Resilience | 9 Tasks | 115 Knowledge Points

Topic 20A: Implement Redundancy Strategies

. 14 knowledge points. Estimated time to complete: Less Than 15 Minutes.14 Knowledge Points | Less Than 15 Minutes

Review Activity: Redundancy Strategies

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

PBQ 20A: Implement Redundancy Strategies

. 5 knowledge points. Estimated time to complete: Less Than 15 Minutes.5 Knowledge Points | Less Than 15 Minutes

Topic 20B: Implement Backup Strategies

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

Review Activity: Backup Strategies

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Assisted Lab: Backing Up and Restoring Data in Windows and Linux

. 15 knowledge points. Estimated time to complete: 15-30 Minutes.15 Knowledge Points | 15-30 Minutes

Topic 20C: Implement Cybersecurity Resiliency Strategies

. 11 knowledge points. Estimated time to complete: Less Than 15 Minutes.11 Knowledge Points | Less Than 15 Minutes

Review Activity: Cybersecurity Resiliency Strategies

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Lesson 20: Practice Questions

. 32 knowledge points. Estimated time to complete: 30-60 Minutes.32 Knowledge Points | 30-60 Minutes

_

Lesson 21: Explaining Physical Security | 6 Tasks | 103 Knowledge Points

Topic 21A: Explain the Importance of Physical Site Security Controls

. 13 knowledge points. Estimated time to complete: Less Than 15 Minutes.13 Knowledge Points | Less Than 15 Minutes

Review Activity: Physical Site Security Controls

. 8 knowledge points. Estimated time to complete: Less Than 15 Minutes.8 Knowledge Points | Less Than 15 Minutes

Topic 21B: Explain the Importance of Physical Host Security Controls

. 10 knowledge points. Estimated time to complete: Less Than 15 Minutes.10 Knowledge Points | Less Than 15 Minutes

Review Activity: Physical Host Security Controls

. 12 knowledge points. Estimated time to complete: Less Than 15 Minutes.12 Knowledge Points | Less Than 15 Minutes

Lesson 21: Practice Questions

. 20 knowledge points. Estimated time to complete: 15-30 Minutes.20 Knowledge Points | 15-30 Minutes

APPLIED LAB: Managing Incident Response, Mitigation and Recovery

. 40 knowledge points. Estimated time to complete: 30-60 Minutes.40 Knowledge Points | 30-60 Minutes

_

Final Assessment | 1 Task | 90 Knowledge Points

Final Assessment

. 90 knowledge points. Estimated time to complete: 60+ Minutes.90 Knowledge Points | 60+ Minutes

_

Next Steps: Become a CompTIA Security+ Certified Professional! | 1 Task | 2 Knowledge Points

Next Steps: Become a CompTIA Security+ Certified Professional!

. 2 knowledge points. Estimated time to complete: Less Than 15 Minutes.2 Knowledge Points | Less Than 15 Minutes

Appendix A

Mapping Course Content to CompTIA Security+ (Exam SY0-601)

Achieving CompTIA Security+ certification requires candidates to pass Exam SY0-601. This table describes where the exam objectives for Exam SY0-601 are covered in this course.

Domain and Objective	Covered in
1.0 Attacks, Threats, and Vulnerabilities	Lesson 4, Topic A
1.1 Compare and contrast different types of social engineering techniques	Lesson 4, Topic A
Phishing	Lesson 4, Topic A
Smishing	Lesson 4, Topic A
Vishing	Lesson 4, Topic A
Spam	Lesson 4, Topic A
Spam over Internet messaging (SPIM)	Lesson 4, Topic A
Spear phishing	Lesson 4, Topic A
Dumpster diving	Lesson 4, Topic A
Shoulder surfing	Lesson 4, Topic A
Pharming	Lesson 4, Topic A
Tailgating	Lesson 4, Topic A
Eliciting information	Lesson 4, Topic A
Whaling	Lesson 4, Topic A
Prepending	Lesson 4, Topic A
Identity fraud	Lesson 4, Topic A
Invoice scams	Lesson 4, Topic A
Credential harvesting	Lesson 4, Topic A
Reconnaissance	Lesson 4, Topic A
Hoax	Lesson 4, Topic A
Impersonation	Lesson 4, Topic A
Watering hole attack	Lesson 4, Topic A
Typo squatting	Lesson 4, Topic A
Pretexting	Lesson 4, Topic A
Influence campaigns	Lesson 4, Topic A
Hybrid warfare	Lesson 4, Topic A
Social media	Lesson 4, Topic A

Domain and Objective	Covered in
Principles (reasons for effectiveness)	Lesson 4, Topic A
Authority	Lesson 4, Topic A
Intimidation	Lesson 4, Topic A
Consensus	Lesson 4, Topic A
Scarcity	Lesson 4, Topic A
Familiarity	Lesson 4, Topic A
Trust	Lesson 4, Topic A
Urgency	Lesson 4, Topic A
1.2 Given a scenario, analyze potential indicators to determine the type of attack	Lesson 4, Topic B Lesson 5, Topic C Lesson 7, Topic B Lesson 12, Topic A Lesson 15, Topic B Lesson 17, Topic C Lesson 21, Topic A
Malware	Lesson 4, Topic B
Ransomware	Lesson 4, Topic B
Trojans	Lesson 4, Topic B
Worms	Lesson 4, Topic B
Potentially unwanted programs (PUPs)	Lesson 4, Topic B
Fileless virus	Lesson 4, Topic B
Command and control	Lesson 4, Topic B
Bots	Lesson 4, Topic B
Cryptomalware	Lesson 4, Topic B
Logic bombs	Lesson 4, Topic B
Spyware	Lesson 4, Topic B
Keyloggers	Lesson 4, Topic B
Remote access Trojan (RAT)	Lesson 4, Topic B
Rootkit	Lesson 4, Topic B
Backdoor	Lesson 4, Topic B
Password attacks	Lesson 7, Topic B
Spraying	Lesson 7, Topic B
Dictionary	Lesson 7, Topic B
Brute force	Lesson 7, Topic B
Offline	Lesson 7, Topic B
Online	Lesson 7, Topic B
Rainbow tables	Lesson 7, Topic B
Plaintext/unencrypted	Lesson 7, Topic B
Physical attacks	Lesson 12, Topic A Lesson 21, Topic A
Malicious universal serial bus (USB) cable	Lesson 12, Topic A
Malicious flash drive	Lesson 12, Topic A

Domain and Objective	Covered in
Card cloning	Lesson 21, Topic A
Skimming	Lesson 21, Topic A
Adversarial artificial intelligence (AI)	Lesson 17, Topic C
Tainted training data for machine learning (ML)	Lesson 17, Topic C
Security of machine learning algorithms	Lesson 17, Topic C
Supply-chain attacks	Lesson 12, Topic A
Cloud-based vs. on-premises attacks	Lesson 15, Topic B
Cryptographic attacks	Lesson 5, Topic C
Birthday	Lesson 5, Topic C
Collision	Lesson 5, Topic C
Downgrade	Lesson 5, Topic C
1.3 Given a scenario, analyze potential indicators associated with application attacks	Lesson 14, Topic A Lesson 14, Topic B
Privilege escalation	Lesson 14, Topic A
Cross-site scripting	Lesson 14, Topic B
Injections	Lesson 14, Topic B Lesson 14, Topic A
Structured query language (SQL)	Lesson 14, Topic B
Dynamic link library (DLL)	Lesson 14, Topic A
Lightweight directory access protocol (LDAP)	Lesson 14, Topic B
Extensible markup language (XML)	Lesson 14, Topic B
Pointer/object dereference	Lesson 14, Topic A
Directory traversal	Lesson 14, Topic B
Buffer overflows	Lesson 14, Topic A
Race conditions	Lesson 14, Topic A
Time of check/time of use	Lesson 14, Topic A
Error handling	Lesson 14, Topic A
Improper input handling	Lesson 14, Topic A
Replay attack	Lesson 14, Topic B
Session replays	Lesson 14, Topic B
Integer overflow	Lesson 14, Topic A
Request forgeries	Lesson 14, Topic B
Server-side	Lesson 14, Topic B
Cross-site	Lesson 14, Topic B
Application programming interface (API) attacks	Lesson 14, Topic B
Resource exhaustion	Lesson 14, Topic A
Memory leak	Lesson 14, Topic A
Secure sockets layer (SSL) stripping	Lesson 14, Topic B
Driver manipulation	Lesson 14, Topic A
Shimming	Lesson 14, Topic A
Refactoring	Lesson 14, Topic A
Pass the hash	Lesson 14, Topic A

Domain and Objective	Covered in
1.4 Given a scenario, analyze potential indicators associated with network attacks	Lesson 9, Topic B Lesson 9, Topic C Lesson 9, Topic D Lesson 11, Topic A Lesson 13, Topic B Lesson 14, Topic D
Wireless	Lesson 9, Topic C Lesson 13, Topic B
Evil twin	Lesson 9, Topic C
Rogue access point	Lesson 9, Topic C
Bluesnarfing	Lesson 13, Topic B
Bluejacking	Lesson 13, Topic B
Disassociation	Lesson 9, Topic C
Jamming	Lesson 9, Topic C
Radio frequency identifier (RFID)	Lesson 13, Topic B
Near-field communication (NFC)	Lesson 13, Topic B
Initialization vector (IV)	Lesson 9, Topic C
On-path attack (previously known as man-in-the-middle attack/man-in-the-browser attack)	Lesson 9, Topic B Lesson 14, Topic D
Layer 2 attacks	Lesson 9, Topic B
Address resolution protocol (ARP) poisoning	Lesson 9, Topic B
Media access control (MAC) flooding	Lesson 9, Topic B
MAC cloning	Lesson 9, Topic B
Domain name system (DNS)	Lesson 11, Topic A
Domain hijacking	Lesson 11, Topic A
DNS poisoning	Lesson 11, Topic A
Universal resource locator (URL) redirection	Lesson 11, Topic A
Domain reputation	Lesson 11, Topic A
Distributed denial-of-service (DDoS)	Lesson 9, Topic D
Network	Lesson 9, Topic D
Application	Lesson 9, Topic D
Operational technology (OT)	Lesson 9, Topic D
Malicious code or script execution	Lesson 14, Topic D
PowerShell	Lesson 14, Topic D
Python	Lesson 14, Topic D
Bash	Lesson 14, Topic D
Macros	Lesson 14, Topic D
Visual Basic for Applications (VBA)	Lesson 14, Topic D
1.5 Explain different threat actors, vectors, and intelligence sources	Lesson 2, Topic A Lesson 2, Topic B
Actors and threats	Lesson 2, Topic A
Advanced persistent threat (APT)	Lesson 2, Topic A
Insider threats	Lesson 2, Topic A

Domain and Objective	Covered in
State actors	Lesson 2, Topic A
Hacktivists	Lesson 2, Topic A
Script kiddies	Lesson 2, Topic A
Criminal syndicates	Lesson 2, Topic A
Hackers	Lesson 2, Topic A
Authorized	Lesson 2, Topic A
Unauthorized	Lesson 2, Topic A
Semi-authorized	Lesson 2, Topic A
Shadow IT	Lesson 2, Topic A
Competitors	Lesson 2, Topic A
Attributes of actors	Lesson 2, Topic A
Internal/external	Lesson 2, Topic A
Level of sophistication/capability	Lesson 2, Topic A
Resources/funding	Lesson 2, Topic A
Intent/motivation	Lesson 2, Topic A
Vectors	Lesson 2, Topic A
Direct access	Lesson 2, Topic A
Wireless	Lesson 2, Topic A
Email	Lesson 2, Topic A
Supply chain	Lesson 2, Topic A
Social media	Lesson 2, Topic A
Removable media	Lesson 2, Topic A
Cloud	Lesson 2, Topic A
Threat intelligence sources	Lesson 2, Topic B
Open source intelligence (OSINT)	Lesson 2, Topic B
Closed/proprietary	Lesson 2, Topic B
Vulnerability databases	Lesson 2, Topic B
Public/private information-sharing centers	Lesson 2, Topic B
Dark web	Lesson 2, Topic B
Indicators of compromise	Lesson 2, Topic B
Automated indicator sharing (AIS)	Lesson 2, Topic B
Structured Threat Information eXpression (STIX)/ Trusted Automated eXchange of Indicator Information (TAXII)	Lesson 2, Topic B
Predictive analysis	Lesson 2, Topic B
Threat maps	Lesson 2, Topic B
File/code repositories	Lesson 2, Topic B
Research sources	Lesson 2, Topic B
Vendor websites	Lesson 2, Topic B
Vulnerability feeds	Lesson 2, Topic B
Conferences	Lesson 2, Topic B

Domain and Objective	Covered in
Academic journals	Lesson 2, Topic B
Request for comments (RFC)	Lesson 2, Topic B
Local industry groups	Lesson 2, Topic B
Social media	Lesson 2, Topic B
Threat feeds	Lesson 2, Topic B
Adversary tactics, techniques, and procedures (TTP)	Lesson 2, Topic B
1.6 Explain the security concerns associated with various types of vulnerabilities	Lesson 3, Topic B
Cloud-based vs. on-premises vulnerabilities	Lesson 3, Topic B
Zero-day	Lesson 3, Topic B
Weak configurations	Lesson 3, Topic B
Open permissions	Lesson 3, Topic B
Unsecure root accounts	Lesson 3, Topic B
Errors	Lesson 3, Topic B
Weak encryption	Lesson 3, Topic B
Unsecure protocols	Lesson 3, Topic B
Default settings	Lesson 3, Topic B
Open ports and services	Lesson 3, Topic B
Third-party risks	Lesson 3, Topic B
Vendor management	Lesson 3, Topic B
System integration	Lesson 3, Topic B
Lack of vendor support	Lesson 3, Topic B
Supply chain	Lesson 3, Topic B
Outsourced code development	Lesson 3, Topic B
Data storage	Lesson 3, Topic B
Improper or weak patch management	Lesson 3, Topic B
Firmware	Lesson 3, Topic B
Operating system (OS)	Lesson 3, Topic B
Applications	Lesson 3, Topic B
Legacy platforms	Lesson 3, Topic B
Impacts	Lesson 3, Topic B
Data loss	Lesson 3, Topic B
Data breaches	Lesson 3, Topic B
Data exfiltration	Lesson 3, Topic B
Identity theft	Lesson 3, Topic B
Financial	Lesson 3, Topic B
Reputation	Lesson 3, Topic B
Availability loss	Lesson 3, Topic B
1.7 Summarize the techniques used in security assessments	Lesson 3, Topic C Lesson 10, Topic C
Threat hunting	Lesson 3, Topic C
Intelligence fusion	Lesson 3, Topic C

Domain and Objective	Covered in
Threat feeds	Lesson 3, Topic C
Advisories and bulletins	Lesson 3, Topic C
Maneuver	Lesson 3, Topic C
Vulnerability scans	Lesson 3, Topic C
False positives	Lesson 3, Topic C
False negatives	Lesson 3, Topic C
Log reviews	Lesson 3, Topic C
Credentialed vs. non-credentialed	Lesson 3, Topic C
Intrusive vs. non-intrusive	Lesson 3, Topic C
Application	Lesson 3, Topic C
Web application	Lesson 3, Topic C
Network	Lesson 3, Topic C
Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)	Lesson 3, Topic C
Configuration review	Lesson 3, Topic C
Syslog/Security information and event management (SIEM)	Lesson 10, Topic C
Review reports	Lesson 10, Topic C
Packet capture	Lesson 10, Topic C
Data inputs	Lesson 10, Topic C
User behavior analysis	Lesson 10, Topic C
Sentiment analysis	Lesson 10, Topic C
Security monitoring	Lesson 10, Topic C
Log aggregation	Lesson 10, Topic C
Log collectors	Lesson 10, Topic C
Security orchestration, automation, and response (SOAR)	Lesson 10, Topic C
1.8 Explain the techniques used in penetration testing	Lesson 3, Topic D
Penetration testing	Lesson 3, Topic D
Known environment	Lesson 3, Topic D
Unknown environment	Lesson 3, Topic D
Partially known environment	Lesson 3, Topic D
Rules of engagement	Lesson 3, Topic D
Lateral movement	Lesson 3, Topic D
Privilege escalation	Lesson 3, Topic D
Persistence	Lesson 3, Topic D
Cleanup	Lesson 3, Topic D
Bug bounty	Lesson 3, Topic D
Pivoting	Lesson 3, Topic D
Passive and active reconnaissance	Lesson 3, Topic D
Drones	Lesson 3, Topic D
War flying	Lesson 3, Topic D
War driving	Lesson 3, Topic D

Domain and Objective	Covered in
Footprinting	Lesson 3, Topic D
OSINT	Lesson 3, Topic D
Exercise types	Lesson 3, Topic D
Red-team	Lesson 3, Topic D
Blue-team	Lesson 3, Topic D
White-team	Lesson 3, Topic D
Purple-team	Lesson 3, Topic D
2.0 Architecture and Design	
2.1 Explain the importance of security concepts in an enterprise environment	Lesson 5, Topic A Lesson 11, Topic B Lesson 16, Topic A Lesson 16, Topic B Lesson 20, Topic C
Configuration management	Lesson 20, Topic C
Diagrams	Lesson 20, Topic C
Baseline configuration	Lesson 20, Topic C
Standard naming conventions	Lesson 20, Topic C
Internet protocol (IP) schema	Lesson 20, Topic C
Data sovereignty	Lesson 16, Topic A
Data protection	Lesson 16, Topic B
Data loss prevention (DLP)	Lesson 16, Topic B
Masking	Lesson 16, Topic B
Encryption	Lesson 16, Topic B
At rest	Lesson 16, Topic B
In transit/motion	Lesson 16, Topic B
In processing	Lesson 16, Topic B
Tokenization	Lesson 16, Topic B
Rights management	Lesson 16, Topic B
Geographical considerations	Lesson 16, Topic A
Response and recovery controls	Lesson 20, Topic C
Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection	Lesson 11, Topic B
Hashing	Lesson 5, Topic A
API considerations	Lesson 11, Topic B
Site resiliency	Lesson 20, Topic C
Hot site	Lesson 20, Topic C
Cold site	Lesson 20, Topic C
Warm site	Lesson 20, Topic C
Deception and disruption	Lesson 20, Topic C
Honeypots	Lesson 20, Topic C
Honeyfiles	Lesson 20, Topic C
Honeynets	Lesson 20, Topic C

Domain and Objective	Covered in
Fake telemetry	Lesson 20, Topic C
DNS sinkhole	Lesson 20, Topic C
2.2 Summarize virtualization and cloud computing concepts	Lesson 15, Topic A Lesson 15, Topic B Lesson 15, Topic C
Cloud models	Lesson 15, Topic A
Infrastructure as a service (IaaS)	Lesson 15, Topic A
Platform as a service (PaaS)	Lesson 15, Topic A
Software as a service (SaaS)	Lesson 15, Topic A
Anything as a service (XaaS)	Lesson 15, Topic A
Public	Lesson 15, Topic A
Community	Lesson 15, Topic A
Private	Lesson 15, Topic A
Hybrid	Lesson 15, Topic A
Managed service provider (MSP)/managed security service provider (MSSP)	Lesson 15, Topic A
On-premises vs. off-premises	Lesson 15, Topic A
Fog computing	Lesson 15, Topic C
Edge computing	Lesson 15, Topic C
Thin client	Lesson 15, Topic A
Containers	Lesson 15, Topic A
Microservices/API	Lesson 15, Topic C
Infrastructure as code	Lesson 15, Topic C
Software-defined networking (SDN)	Lesson 15, Topic C
Software-defined visibility (SDV)	Lesson 15, Topic C
Serverless architecture	Lesson 15, Topic C
Services integration	Lesson 15, Topic C
Resource policies	Lesson 15, Topic B
Transit gateway	Lesson 15, Topic B
Virtualization	Lesson 15, Topic A
Virtual machine (VM) sprawl avoidance	Lesson 15, Topic A
VM escape protection	Lesson 15, Topic A
2.3 Summarize secure application development, deployment, and automation concepts	Lesson 14, Topic C Lesson 14, Topic E
Environment	Lesson 14, Topic E
Development	Lesson 14, Topic E
Test	Lesson 14, Topic E
Staging	Lesson 14, Topic E
Production	Lesson 14, Topic E
Quality assurance (QA)	Lesson 14, Topic E
Provisioning and deprovisioning	Lesson 14, Topic E
Integrity measurement	Lesson 14, Topic E

Domain and Objective	Covered in
Secure coding techniques	Lesson 14, Topic C
Normalization	Lesson 14, Topic C
Stored procedures	Lesson 14, Topic C
Obfuscation/camouflage	Lesson 14, Topic C
Code reuse/dead code	Lesson 14, Topic C
Server-side vs. client-side execution and validation	Lesson 14, Topic C
Memory management	Lesson 14, Topic C
Use of third-party libraries and software development kits (SDKs)	Lesson 14, Topic C
Data exposure	Lesson 14, Topic C
Open Web Application Security Project (OWASP)	Lesson 14, Topic C
Software diversity	Lesson 14, Topic E
Compiler	Lesson 14, Topic E
Binary	Lesson 14, Topic E
Automation/scripting	Lesson 14, Topic E
Automated courses of action	Lesson 14, Topic E
Continuous monitoring	Lesson 14, Topic E
Continuous validation	Lesson 14, Topic E
Continuous integration	Lesson 14, Topic E
Continuous delivery	Lesson 14, Topic E
Continuous deployment	Lesson 14, Topic E
Elasticity	Lesson 14, Topic E
Scalability	Lesson 14, Topic E
Version control	Lesson 14, Topic E
2.4 Summarize authentication and authorization design concepts	Lesson 7, Topic A Lesson 7, Topic C Lesson 7, Topic D
Authentication methods	Lesson 7, Topic C
Directory services	Lesson 7, Topic C
Federation	Lesson 7, Topic C
Attestation	Lesson 7, Topic C
Technologies	Lesson 7, Topic C
Time-based onetime password (TOTP)	Lesson 7, Topic C
HMAC-based one-time password (HOTP)	Lesson 7, Topic C
Short message service (SMS)	Lesson 7, Topic C
Token key	Lesson 7, Topic C
Static codes	Lesson 7, Topic C
Authentication applications	Lesson 7, Topic C
Push notifications	Lesson 7, Topic C
Phone call	Lesson 7, Topic C
Smart card authentication	Lesson 7, Topic C

Domain and Objective	Covered in
Biometrics	Lesson 7, Topic D
Fingerprint	Lesson 7, Topic D
Retina	Lesson 7, Topic D
Iris	Lesson 7, Topic D
Facial	Lesson 7, Topic D
Voice	Lesson 7, Topic D
Vein	Lesson 7, Topic D
Gait analysis	Lesson 7, Topic D
Efficacy rates	Lesson 7, Topic D
False acceptance	Lesson 7, Topic D
False rejection	Lesson 7, Topic D
Crossover error rate	Lesson 7, Topic D
Multifactor authentication (MFA) factors and attributes	Lesson 7, Topic A
Factors	Lesson 7, Topic A
Something you know	Lesson 7, Topic A
Something you have	Lesson 7, Topic A
Something you are	Lesson 7, Topic A
Attributes	Lesson 7, Topic A
Somewhere you are	Lesson 7, Topic A
Something you can do	Lesson 7, Topic A
Something you exhibit	Lesson 7, Topic A
Someone you know	Lesson 7, Topic A
Authentication, authorization, and accounting (AAA)	Lesson 7, Topic A
Cloud vs. on-premises requirements	Lesson 7, Topic A
2.5 Given a scenario, implement cybersecurity resilience	Lesson 20, Topic A Lesson 20, Topic B Lesson 20, Topic C
Redundancy	Lesson 20, Topic A
Geographic dispersal	Lesson 20, Topic A
Disk	Lesson 20, Topic A
Redundant array of inexpensive disks (RAID) levels	Lesson 20, Topic A
Multipath	Lesson 20, Topic A
Network	Lesson 20, Topic A
Load balancers	Lesson 20, Topic A
Network interface card (NIC) teaming	Lesson 20, Topic A
Power	Lesson 20, Topic A
Uninterruptible power supply (UPS)	Lesson 20, Topic A
Generator	Lesson 20, Topic A
Dual supply	Lesson 20, Topic A
Managed power distribution units (PDUs)	Lesson 20, Topic A

Domain and Objective	Covered in
Replication	Lesson 20, Topic A
Storage area network	Lesson 20, Topic A
VM	Lesson 20, Topic A
On-premises vs. cloud	Lesson 20, Topic A
Backup types	Lesson 20, Topic B
Full	Lesson 20, Topic B
Incremental	Lesson 20, Topic B
Snapshot	Lesson 20, Topic B
Differential	Lesson 20, Topic B
Tape	Lesson 20, Topic B
Disk	Lesson 20, Topic B
Copy	Lesson 20, Topic B
Network-attached storage (NAS)	Lesson 20, Topic B
Storage area network	Lesson 20, Topic B
Cloud	Lesson 20, Topic B
Image	Lesson 20, Topic B
Online vs. offline	Lesson 20, Topic B
Offsite storage	Lesson 20, Topic B
Distance considerations	Lesson 20, Topic B
Non-persistence	Lesson 20, Topic B
Revert to known state	Lesson 20, Topic B
Last known-good configuration	Lesson 20, Topic B
Live boot media	Lesson 20, Topic B
High availability	Lesson 20, Topic A
Scalability	Lesson 20, Topic A
Restoration order	Lesson 20, Topic B
Diversity	Lesson 20, Topic C
Technologies	Lesson 20, Topic C
Vendors	Lesson 20, Topic C
Crypto	Lesson 20, Topic C
Controls	Lesson 20, Topic C
2.6 Explain the security implications of embedded and specialized systems	Lesson 12, Topic C
Embedded systems	Lesson 12, Topic C
Raspberry Pi	Lesson 12, Topic C
Field-programmable gate array (FPGA)	Lesson 12, Topic C
Arduino	Lesson 12, Topic C
Supervisory control and data acquisition (SCADA)/industrial control system (ICS)	Lesson 12, Topic C
Facilities	Lesson 12, Topic C
Industrial	Lesson 12, Topic C

Domain and Objective	Covered in
Manufacturing	Lesson 12, Topic C
Energy	Lesson 12, Topic C
Logistics	Lesson 12, Topic C
Internet of Things (IoT)	Lesson 12, Topic C
Sensors	Lesson 12, Topic C
Smart devices	Lesson 12, Topic C
Wearables	Lesson 12, Topic C
Facility automation	Lesson 12, Topic C
Weak defaults	Lesson 12, Topic C
Specialized	Lesson 12, Topic C
Medical systems	Lesson 12, Topic C
Vehicles	Lesson 12, Topic C
Aircraft	Lesson 12, Topic C
Smart meters	Lesson 12, Topic C
Voice over IP (VoIP)	Lesson 12, Topic C
Heating, ventilation, air conditioning (HVAC)	Lesson 12, Topic C
Drones	Lesson 12, Topic C
Multifunction printer (MFP)	Lesson 12, Topic C
Real-time operating system (RTOS)	Lesson 12, Topic C
Surveillance systems	Lesson 12, Topic C
System on chip (SoC)	Lesson 12, Topic C
Communication considerations	Lesson 12, Topic C
5G	Lesson 12, Topic C
Narrow-band	Lesson 12, Topic C
Baseband radio	Lesson 12, Topic C
Subscriber identity module (SIM) cards	Lesson 12, Topic C
Zigbee	Lesson 12, Topic C
Constraints	Lesson 12, Topic C
Power	Lesson 12, Topic C
Compute	Lesson 12, Topic C
Network	Lesson 12, Topic C
Crypto	Lesson 12, Topic C
Inability to patch	Lesson 12, Topic C
Authentication	Lesson 12, Topic C
Range	Lesson 12, Topic C
Cost	Lesson 12, Topic C
Implied trust	Lesson 12, Topic C
2.7 Explain the importance of physical security controls	Lesson 21, Topic A Lesson 21, Topic B
Bollards/barricades	Lesson 21, Topic A
Access control vestibules	Lesson 21, Topic A

Domain and Objective	Covered in
Badges	Lesson 21, Topic A
Alarms	Lesson 21, Topic A
Signage	Lesson 21, Topic A
Cameras	Lesson 21, Topic A
Motion recognition	Lesson 21, Topic A
Object detection	Lesson 21, Topic A
Closed-circuit television (CCTV)	Lesson 21, Topic A
Industrial camouflage	Lesson 21, Topic A
Personnel	Lesson 21, Topic A
Guards	Lesson 21, Topic A
Robot sentries	Lesson 21, Topic A
Reception	Lesson 21, Topic A
Two-person integrity/control	Lesson 21, Topic A
Locks	Lesson 21, Topic A
Biometrics	Lesson 21, Topic A
Electronic	Lesson 21, Topic A
Physical	Lesson 21, Topic A
Cable locks	Lesson 21, Topic A
USB data blocker	Lesson 21, Topic A
Lighting	Lesson 21, Topic A
Fencing	Lesson 21, Topic A
Fire suppression	Lesson 21, Topic B
Sensors	Lesson 21, Topic A Lesson 21, Topic B
Motion detection	Lesson 21, Topic A
Noise detection	Lesson 21, Topic A
Proximity reader	Lesson 21, Topic A
Moisture detection	Lesson 21, Topic B
Cards	Lesson 21, Topic A
Temperature	Lesson 21, Topic B
Drones	Lesson 21, Topic A
Visitor logs	Lesson 21, Topic A
Faraday cages	Lesson 21, Topic B
Air gap	Lesson 21, Topic B
Screened subnet (previously known as demilitarized zone)	Lesson 21, Topic A
Protected cable distribution	Lesson 21, Topic B
Secure areas	Lesson 21, Topic B
Air gap	Lesson 21, Topic B
Vault	Lesson 21, Topic B
Safe	Lesson 21, Topic B
Hot aisle	Lesson 21, Topic B
Cold aisle	Lesson 21, Topic B

Domain and Objective	Covered in
Secure data destruction	Lesson 21, Topic B
Burning	Lesson 21, Topic B
Shredding	Lesson 21, Topic B
Pulping	Lesson 21, Topic B
Pulverizing	Lesson 21, Topic B
Degaussing	Lesson 21, Topic B
Third-party solutions	Lesson 21, Topic B
2.8 Summarize the basics of cryptographic concepts	Lesson 5, Topic A Lesson 5, Topic B Lesson 5, Topic C Lesson 5, Topic D
Digital signatures	Lesson 5, Topic B
Key length	Lesson 5, Topic A
Key stretching	Lesson 5, Topic C
Salting	Lesson 5, Topic C
Hashing	Lesson 5, Topic A
Key exchange	Lesson 5, Topic B
Elliptic-curve cryptography	Lesson 5, Topic A
Perfect forward secrecy	Lesson 5, Topic B
Quantum	Lesson 5, Topic D
Communications	Lesson 5, Topic D
Computing	Lesson 5, Topic D
Post-quantum	Lesson 5, Topic D
Ephemeral	Lesson 5, Topic B
Modes of operation	Lesson 5, Topic B
Authenticated	Lesson 5, Topic B
Unauthenticated	Lesson 5, Topic B
Counter	Lesson 5, Topic B
Blockchain	Lesson 5, Topic D
Public ledgers	Lesson 5, Topic D
Cipher suites	Lesson 5, Topic A
Stream	Lesson 5, Topic A
Block	Lesson 5, Topic A
Symmetric vs. asymmetric	Lesson 5, Topic A
Lightweight cryptography	Lesson 5, Topic D
Steganography	Lesson 5, Topic D
Audio	Lesson 5, Topic D
Video	Lesson 5, Topic D
Image	Lesson 5, Topic D
Homomorphic encryption	Lesson 5, Topic D
Common use cases	Lesson 5, Topic C
Low power devices	Lesson 5, Topic C

Domain and Objective	Covered in
Low latency	Lesson 5, Topic C
High resiliency	Lesson 5, Topic C
Supporting confidentiality	Lesson 5, Topic C
Supporting integrity	Lesson 5, Topic C
Supporting obfuscation	Lesson 5, Topic C
Supporting authentication	Lesson 5, Topic C
Supporting non-repudiation	Lesson 5, Topic C
Limitations	Lesson 5, Topic C
Speed	Lesson 5, Topic C
Size	Lesson 5, Topic C
Weak keys	Lesson 5, Topic C
Time	Lesson 5, Topic C
Longevity	Lesson 5, Topic C
Predictability	Lesson 5, Topic C
Reuse	Lesson 5, Topic C
Entropy	Lesson 5, Topic C
Computational overheads	Lesson 5, Topic C
Resource vs. security constraints	Lesson 5, Topic C
3.0 Implementation	
3.1 Given a scenario, implement secure protocols	Lesson 9, Topic B Lesson 11, Topic A Lesson 11, Topic B Lesson 11, Topic C
Protocols	Lesson 11, Topic A Lesson 11, Topic B Lesson 11, Topic C
Domain Name System Security Extension (DNSSEC)	Lesson 11, Topic A
SSH	Lesson 11, Topic C
Secure/Multipurpose Internet Mail Extensions (S/MIME)	Lesson 11, Topic B
Secure Real-time Protocol (SRTP)	Lesson 11, Topic B
Lightweight Directory Access Protocol Over SSL (LDAPS)	Lesson 11, Topic A
File Transfer Protocol, Secure (FTPS)	Lesson 11, Topic B
SSH File Transfer Protocol (SFTP)	Lesson 11, Topic B
Simple Network Management Protocol, version 3 (SNMPv3)	Lesson 11, Topic A
Hypertext transfer protocol over SSL/TLS (HTTPS)	Lesson 11, Topic B
IPSec	Lesson 11, Topic C
Authentication Header (AH)/Encapsulated Security Payloads (ESP)	Lesson 11, Topic C
Tunnel/transport	Lesson 11, Topic C
Secure Post Office Protocol (POP)/Internet Message Access Protocol (IMAP)	Lesson 11, Topic B

Domain and Objective	Covered in
Use cases	Lesson 9, Topic B Lesson 11, Topic A Lesson 11, Topic B Lesson 11, Topic C
Voice and video	Lesson 11, Topic B
Time synchronization	Lesson 11, Topic A
Email and web	Lesson 11, Topic B
File transfer	Lesson 11, Topic B
Directory services	Lesson 11, Topic A
Remote access	Lesson 11, Topic C
Domain name resolution	Lesson 11, Topic A
Routing and switching	Lesson 9, Topic B
Network address allocation	Lesson 11, Topic A
Subscription services	Lesson 11, Topic B
3.2 Given a scenario, implement host or application security solutions	Lesson 12, Topic A Lesson 12, Topic B Lesson 14, Topic C Lesson 14, Topic D Lesson 16, Topic B
Endpoint protection	Lesson 12, Topic B
Antivirus	Lesson 12, Topic B
Anti-malware	Lesson 12, Topic B
Endpoint detection and response (EDR)	Lesson 12, Topic B
DLP	Lesson 12, Topic B
Next-generation firewall (NGFW)	Lesson 12, Topic B
Host-based intrusion prevention system (HIPS)	Lesson 12, Topic B
Host-based intrusion detection system (HIDS)	Lesson 12, Topic B
Host-based firewall	Lesson 12, Topic B
Boot integrity	Lesson 12, Topic A
Boot security/Unified Extensible Firmware Interface (UEFI)	Lesson 12, Topic A
Measured boot	Lesson 12, Topic A
Boot attestation	Lesson 12, Topic A
Database	Lesson 16, Topic B
Tokenization	Lesson 16, Topic B
Salting	Lesson 16, Topic B
Hashing	Lesson 16, Topic B
Application security	Lesson 14, Topic C Lesson 14, Topic D
Input validations	Lesson 14, Topic C
Secure cookies	Lesson 14, Topic C
Hypertext Transfer Protocol (HTTP) headers	Lesson 14, Topic C
Code signing	Lesson 14, Topic D
Allow list	Lesson 14, Topic D

Domain and Objective	Covered in
Block list/deny list	Lesson 14, Topic D
Secure coding practices	Lesson 14, Topic C
Static code analysis	Lesson 14, Topic C
Manual code review	Lesson 14, Topic C
Dynamic code analysis	Lesson 14, Topic C
Fuzzing	Lesson 14, Topic C
Hardening	Lesson 12, Topic B
Open ports and services	Lesson 12, Topic B
Registry	Lesson 12, Topic B
Disk encryption	Lesson 12, Topic B
OS	Lesson 12, Topic B
Patch management	Lesson 12, Topic B
Third-party updates	Lesson 12, Topic B
Auto-update	Lesson 12, Topic B
Self-encrypting drive (SED)/full-disk encryption (FDE)	Lesson 12, Topic A
Opal	Lesson 12, Topic A
Hardware root of trust	Lesson 12, Topic A
Trusted Platform Module (TPM)	Lesson 12, Topic A
Sandboxing	Lesson 12, Topic B
3.3 Given a scenario, implement secure network designs	Lesson 7, Topic C Lesson 9, Topic A Lesson 9, Topic B Lesson 9, Topic D Lesson 10, Topic A Lesson 10, Topic B Lesson 11, Topic C
Load balancing	Lesson 9, Topic D
Active/active	Lesson 9, Topic D
Active/passive	Lesson 9, Topic D
Scheduling	Lesson 9, Topic D
Virtual IP	Lesson 9, Topic D
Persistence	Lesson 9, Topic D
Network segmentation	Lesson 9, Topic A
Virtual local area network (VLAN)	Lesson 9, Topic A
Screened subnet (previously known as demilitarized zone)	Lesson 9, Topic A
East-west traffic	Lesson 9, Topic A
Extranet	Lesson 9, Topic A
Intranet	Lesson 9, Topic A
Zero Trust	Lesson 9, Topic A
Virtual private network (VPN)	Lesson 11, Topic C
Always-on	Lesson 11, Topic C
Split tunnel vs. full tunnel	Lesson 11, Topic C
Remote access vs. site-to-site	Lesson 11, Topic C

Domain and Objective	Covered in
IPSec	Lesson 11, Topic C
SSL/TLS	Lesson 11, Topic C
HTML5	Lesson 11, Topic C
Layer 2 tunneling protocol (L2TP)	Lesson 11, Topic C
DNS	Lesson 9, Topic A
Network access control (NAC)	Lesson 9, Topic B
Agent and agentless	Lesson 9, Topic B
Out-of-band management	Lesson 11, Topic C
Port security	Lesson 9, Topic B
Broadcast storm prevention	Lesson 9, Topic B
Bridge Protocol Data Unit (BPDU) guard	Lesson 9, Topic B
Loop prevention	Lesson 9, Topic B
Dynamic Host Configuration Protocol (DHCP) snooping	Lesson 9, Topic B
Media access control (MAC) filtering	Lesson 9, Topic B
Network appliances	Lesson 7, Topic C Lesson 10, Topic A Lesson 10, Topic B Lesson 11, Topic C
Jump servers	Lesson 11, Topic C
Proxy servers	Lesson 10, Topic A
Forward	Lesson 10, Topic A
Reverse	Lesson 10, Topic A
Network-based intrusion detection system (NIDS)/ network-based intrusion prevention system (NIPS)	Lesson 10, Topic B
Signature-based	Lesson 10, Topic B
Heuristic/behavior	Lesson 10, Topic B
Anomaly	Lesson 10, Topic B
Inline vs. passive	Lesson 10, Topic B
HSM	Lesson 7, Topic C
Sensors	Lesson 10, Topic B
Collectors	Lesson 10, Topic C
Aggregators	Lesson 10, Topic C
Firewalls	Lesson 10, Topic A Lesson 10, Topic B
Web application firewall (WAF)	Lesson 10, Topic B
NGFW	Lesson 10, Topic B
Stateful	Lesson 10, Topic A
Stateless	Lesson 10, Topic A
Unified threat management (UTM)	Lesson 10, Topic B
Network address translation (NAT) gateway	Lesson 10, Topic A
Content/URL filter	Lesson 10, Topic B
Open-source vs. proprietary	Lesson 10, Topic A

Domain and Objective	Covered in
Hardware vs. software	Lesson 10, Topic A
Appliance vs. host-based vs. virtual	Lesson 10, Topic A
Access control list (ACL)	Lesson 10, Topic A
Route security	Lesson 9, Topic B
Quality of service (QoS)	Lesson 9, Topic D
Implications of IPv6	Lesson 9, Topic A
Port spanning/port mirroring	Lesson 10, Topic B
Port taps	Lesson 10, Topic B
Monitoring services	Lesson 10, Topic C
File integrity monitors	Lesson 10, Topic B
3.4 Given a scenario, install and configure wireless security settings	Lesson 9, Topic C
Cryptographic protocols	Lesson 9, Topic C
WiFi Protected Access 2 (WPA2)	Lesson 9, Topic C
WiFi Protected Access 3 (WPA3)	Lesson 9, Topic C
Counter-mode/CBC-MAC protocol (CCMP)	Lesson 9, Topic C
Simultaneous Authentication of Equals (SAE)	Lesson 9, Topic C
Authentication protocols	Lesson 9, Topic C
Extensible Authentication Protocol (EAP)	Lesson 9, Topic C
Protected Extensible Application Protocol (PEAP)	Lesson 9, Topic C
EAP-FAST	Lesson 9, Topic C
EAP-TLS	Lesson 9, Topic C
EAP-TTLS	Lesson 9, Topic C
IEEE 802.1X	Lesson 9, Topic C
Remote Authentication Dial-in User Service (RADIUS) Federation	Lesson 9, Topic C
Methods	Lesson 9, Topic C
Pre-shared key (PSK) vs. Enterprise vs. Open	Lesson 9, Topic C
WiFi Protected Setup (WPS)	Lesson 9, Topic C
Captive portals	Lesson 9, Topic C
Installation considerations	Lesson 9, Topic C
Site surveys	Lesson 9, Topic C
Heat maps	Lesson 9, Topic C
WiFi analyzers	Lesson 9, Topic C
Channel overlaps	Lesson 9, Topic C
Wireless access point (WAP) placement	Lesson 9, Topic C
Controller and access point security	Lesson 9, Topic C
3.5 Given a scenario, implement secure mobile solutions	Lesson 13, Topic A Lesson 13, Topic B
Connection methods and receivers	Lesson 13, Topic B
Cellular	Lesson 13, Topic B
WiFi	Lesson 13, Topic B

Domain and Objective	Covered in
Bluetooth	Lesson 13, Topic B
NFC	Lesson 13, Topic B
Infrared	Lesson 13, Topic B
USB	Lesson 13, Topic B
Point-to-point	Lesson 13, Topic B
Point-to-multipoint	Lesson 13, Topic B
Global Positioning System (GPS)	Lesson 13, Topic B
RFID	Lesson 13, Topic B
Mobile device management (MDM)	Lesson 13, Topic A Lesson 13, Topic B
Application management	Lesson 13, Topic A
Content management	Lesson 13, Topic A
Remote wipe	Lesson 13, Topic A
Geofencing	Lesson 13, Topic A
Geolocation	Lesson 13, Topic A
Screen locks	Lesson 13, Topic A
Push notifications	Lesson 13, Topic B
Passwords and PINs	Lesson 13, Topic A
Biometrics	Lesson 13, Topic A
Context-aware authentication	Lesson 13, Topic A
Containerization	Lesson 13, Topic A
Storage segmentation	Lesson 13, Topic A
Full device encryption	Lesson 13, Topic A
Mobile devices	Lesson 13, Topic A
MicroSD HSM	Lesson 13, Topic A
MDM/Unified Endpoint Management (UEM)	Lesson 13, Topic A
Mobile application management (MAM)	Lesson 13, Topic A
SEAndroid	Lesson 13, Topic A
Enforcement and monitoring of:	Lesson 13, Topic A Lesson 13, Topic B
Third-party application stores	Lesson 13, Topic A
Rooting/jailbreaking	Lesson 13, Topic A
Sideloading	Lesson 13, Topic A
Custom firmware	Lesson 13, Topic A
Carrier unlocking	Lesson 13, Topic A
Firmware over-the-air (OTA) updates	Lesson 13, Topic B
Camera use	Lesson 13, Topic A
SMS/Multimedia Messaging Service (MMS)/Rich communication services (RCS)	Lesson 13, Topic B
External media	Lesson 13, Topic A
USB On-The-Go (USB OTG)	Lesson 13, Topic B
Recording microphone	Lesson 13, Topic A

Domain and Objective	Covered in
GPS tagging	Lesson 13, Topic A
WiFi direct/ad hoc	Lesson 13, Topic B
Tethering	Lesson 13, Topic B
Hotspot	Lesson 13, Topic B
Payment methods	Lesson 13, Topic B
Deployment models	Lesson 13, Topic A
Bring your own device (BYOD)	Lesson 13, Topic A
Corporate-owned personally enabled (COPE)	Lesson 13, Topic A
Choose your own device (CYOD)	Lesson 13, Topic A
Corporate-owned	Lesson 13, Topic A
Virtual desktop infrastructure (VDI)	Lesson 13, Topic A
3.6 Given a scenario, apply cybersecurity solutions to the cloud	Lesson 15, Topic B
Cloud security controls	Lesson 15, Topic B
High availability across zones	Lesson 15, Topic B
Resource policies	Lesson 15, Topic B
Secrets management	Lesson 15, Topic B
Integration and auditing	Lesson 15, Topic B
Storage	Lesson 15, Topic B
Permissions	Lesson 15, Topic B
Encryption	Lesson 15, Topic B
Replication	Lesson 15, Topic B
High availability	Lesson 15, Topic B
Network	Lesson 15, Topic B
Virtual networks	Lesson 15, Topic B
Public and private subnets	Lesson 15, Topic B
Segmentation	Lesson 15, Topic B
API inspection and integration	Lesson 15, Topic B
Compute	Lesson 15, Topic B
Security groups	Lesson 15, Topic B
Dynamic resource allocation	Lesson 15, Topic B
Instance awareness	Lesson 15, Topic B
Virtual private cloud (VPC) endpoint	Lesson 15, Topic B
Container security	Lesson 15, Topic B
Solutions	Lesson 15, Topic B
CASB	Lesson 15, Topic B
Application security	Lesson 15, Topic B
Next-generation Secure Web Gateway (SWG)	Lesson 15, Topic B
Firewall considerations in a cloud environment	Lesson 15, Topic B
Cost	Lesson 15, Topic B

Domain and Objective	Covered in
Need for segmentation	Lesson 15, Topic B
Open Systems Interconnection (OSI) layers	Lesson 15, Topic B
Cloud native controls vs. third-party solutions	Lesson 15, Topic B
3.7 Given a scenario, implement identity and account management controls	Lesson 8, Topic A Lesson 8, Topic B
Identity	Lesson 8, Topic A Lesson 8, Topic B
Identity provider (IdP)	Lesson 8, Topic A
Attributes	Lesson 8, Topic B
Certificates	Lesson 8, Topic A
Tokens	Lesson 8, Topic A
SSH keys	Lesson 8, Topic A
Smart cards	Lesson 8, Topic A
Account types	Lesson 8, Topic A
User account	Lesson 8, Topic A
Shared and generic accounts/credentials	Lesson 8, Topic A
Guest accounts	Lesson 8, Topic A
Service accounts	Lesson 8, Topic A
Account policies	Lesson 8, Topic B
Password complexity	Lesson 8, Topic B
Password history	Lesson 8, Topic B
Password reuse	Lesson 8, Topic B
Network location	Lesson 8, Topic B
Geofencing	Lesson 8, Topic B
Geotagging	Lesson 8, Topic B
Geolocation	Lesson 8, Topic B
Time-based logins	Lesson 8, Topic B
Access policies	Lesson 8, Topic B
Account permissions	Lesson 8, Topic B
Account audits	Lesson 8, Topic B
Impossible travel time/risky login	Lesson 8, Topic B
Lockout	Lesson 8, Topic B
Disablement	Lesson 8, Topic B
3.8 Given a scenario, implement authentication and authorization solutions	Lesson 7, Topic B Lesson 7, Topic C Lesson 8, Topic C
Authentication management	Lesson 7, Topic B Lesson 7, Topic C
Password keys	Lesson 7, Topic B
Password vaults	Lesson 7, Topic B
TPM	Lesson 7, Topic C
HSM	Lesson 7, Topic C
Knowledge-based authentication	Lesson 7, Topic B

Domain and Objective	Covered in
Authentication/authorization	Lesson 7, Topic B Lesson 7, Topic C Lesson 8, Topic C
EAP	Lesson 7, Topic C
Challenge Handshake Authentication Protocol (CHAP)	Lesson 7, Topic B
Password Authentication Protocol (PAP)	Lesson 7, Topic B
802.1X	Lesson 7, Topic C
RADIUS	Lesson 7, Topic C
Single sign-on (SSO)	Lesson 7, Topic B
Security Assertions Markup Language (SAML)	Lesson 8, Topic C
Terminal Access Controller Access Control System Plus (TACACS+)	Lesson 7, Topic C
OAuth	Lesson 8, Topic C
OpenID	Lesson 8, Topic C
Kerberos	Lesson 7, Topic B
Access control schemes	Lesson 8, Topic C
Attribute-based access control (ABAC)	Lesson 8, Topic C
Role-based access control	Lesson 8, Topic C
Rule-based access control	Lesson 8, Topic C
MAC	Lesson 8, Topic C
Discretionary access control (DAC)	Lesson 8, Topic C
Conditional access	Lesson 8, Topic C
Privilege access management	Lesson 8, Topic C
Filesystem permissions	Lesson 8, Topic C
3.9 Given a scenario, implement public key infrastructure	Lesson 6, Topic A Lesson 6, Topic B
Public key infrastructure (PKI)	Lesson 6, Topic A Lesson 6, Topic B
Key management	Lesson 6, Topic B
Certificate authority (CA)	Lesson 6, Topic A
Intermediate CA	Lesson 6, Topic A
Registration authority (RA)	Lesson 6, Topic A
Certificate revocation list (CRL)	Lesson 6, Topic B
Certificate attributes	Lesson 6, Topic A
Online Certificate Status Protocol (OCSP)	Lesson 6, Topic B
Certificate signing request (CSR)	Lesson 6, Topic A
CN	Lesson 6, Topic A
Subject alternative name	Lesson 6, Topic A
Expiration	Lesson 6, Topic B
Types of certificates	Lesson 6, Topic A
Wildcard	Lesson 6, Topic A
Subject alternative name	Lesson 6, Topic A

Domain and Objective	Covered in
Code signing	Lesson 6, Topic A
Self-signed	Lesson 6, Topic A
Machine/computer	Lesson 6, Topic A
Email	Lesson 6, Topic A
User	Lesson 6, Topic A
Root	Lesson 6, Topic A
Domain validation	Lesson 6, Topic A
Extended validation	Lesson 6, Topic A
Certificate formats	Lesson 6, Topic B
Distinguished encoding rules (DER)	Lesson 6, Topic B
Privacy enhanced mail (PEM)	Lesson 6, Topic B
Personal information exchange (PFX)	Lesson 6, Topic B
.cer	Lesson 6, Topic B
P12	Lesson 6, Topic B
P7B	Lesson 6, Topic B
Concepts	Lesson 6, Topic A Lesson 6, Topic B
Online vs. offline CA	Lesson 6, Topic A
Stapling	Lesson 6, Topic B
Pinning	Lesson 6, Topic B
Trust model	Lesson 6, Topic A
Key escrow	Lesson 6, Topic B
Certificate chaining	Lesson 6, Topic A
4.0 Operations and Incident Response	
4.1 Given a scenario, use the appropriate tool to assess organizational security	Lesson 3, Topic A Lesson 4, Topic B Lesson 6, Topic B Lesson 7, Topic B Lesson 8, Topic C Lesson 10, Topic C Lesson 11, Topic C Lesson 14, Topic D Lesson 18, Topic B Lesson 21, Topic B
Network reconnaissance and discovery	Lesson 3, Topic A Lesson 4, Topic B
tracert/traceroute	Lesson 3, Topic A
nslookup/dig	Lesson 3, Topic A
ipconfig/ifconfig	Lesson 3, Topic A
nmap	Lesson 3, Topic A
ping/pathping	Lesson 3, Topic A
hping	Lesson 3, Topic A
netstat	Lesson 3, Topic A
netcat	Lesson 3, Topic A

Domain and Objective	Covered in
IP scanners	Lesson 3, Topic A
arp	Lesson 3, Topic A
route	Lesson 3, Topic A
curl	Lesson 3, Topic A
the harvester	Lesson 3, Topic A
sn1per	Lesson 3, Topic A
scanless	Lesson 3, Topic A
dnsenum	Lesson 3, Topic A
Nessus	Lesson 3, Topic A
Cuckoo	Lesson 4, Topic B
File manipulation	Lesson 8, Topic C Lesson 10, Topic C
head	Lesson 10, Topic C
tail	Lesson 10, Topic C
cat	Lesson 10, Topic C
grep	Lesson 10, Topic C
chmod	Lesson 8, Topic C
logger	Lesson 10, Topic C
Shell and script environments	Lesson 6, Topic B Lesson 11, Topic C Lesson 14, Topic D
SSH	Lesson 11, Topic C
PowerShell	Lesson 14, Topic D
Python	Lesson 14, Topic D
OpenSSL	Lesson 6, Topic B
Packet capture and replay	Lesson 3, Topic A
Tcpreplay	Lesson 3, Topic A
Tcpdump	Lesson 3, Topic A
Wireshark	Lesson 3, Topic A
Forensics	Lesson 18, Topic B
dd	Lesson 18, Topic B
Memdump	Lesson 18, Topic B
WinHex	Lesson 18, Topic B
FTK imager	Lesson 18, Topic B
Autopsy	Lesson 18, Topic B
Exploitation frameworks	Lesson 3, Topic A
Password crackers	Lesson 7, Topic B
Data sanitization	Lesson 21, Topic B
4.2 Summarize the importance of policies, processes, and procedures for incident response	Lesson 17, Topic A
Incident response plans	Lesson 17, Topic A
Incident response process	Lesson 17, Topic A

Domain and Objective	Covered in
Preparation	Lesson 17, Topic A
Identification	Lesson 17, Topic A
Containment	Lesson 17, Topic A
Eradication	Lesson 17, Topic A
Recovery	Lesson 17, Topic A
Lessons learned	Lesson 17, Topic A
Exercises	Lesson 17, Topic A
Tabletop	Lesson 17, Topic A
Walkthroughs	Lesson 17, Topic A
Simulations	Lesson 17, Topic A
Attack frameworks	Lesson 17, Topic A
MITRE ATT&CK	Lesson 17, Topic A
The Diamond Model of Intrusion Analysis	Lesson 17, Topic A
Cyber Kill Chain	Lesson 17, Topic A
Stakeholder management	Lesson 17, Topic A
Communication plan	Lesson 17, Topic A
Disaster recovery plan	Lesson 17, Topic A
Business continuity plan	Lesson 17, Topic A
Continuity of operations planning (COOP)	Lesson 17, Topic A
Incident response team	Lesson 17, Topic A
Retention policies	Lesson 17, Topic A
4.3 Given an incident, utilize appropriate data sources to support an investigation	Lesson 17, Topic B
Vulnerability scan output	Lesson 17, Topic B
SIEM dashboards	Lesson 17, Topic B
Sensor	Lesson 17, Topic B
Sensitivity	Lesson 17, Topic B
Trends	Lesson 17, Topic B
Alerts	Lesson 17, Topic B
Correlation	Lesson 17, Topic B
Log files	Lesson 17, Topic B
Network	Lesson 17, Topic B
System	Lesson 17, Topic B
Application	Lesson 17, Topic B
Security	Lesson 17, Topic B
Web	Lesson 17, Topic B
DNS	Lesson 17, Topic B
Authentication	Lesson 17, Topic B
Dump files	Lesson 17, Topic B
VoIP and call managers	Lesson 17, Topic B
Session Initiation Protocol (SIP) traffic	Lesson 17, Topic B

Domain and Objective	Covered in
syslog/rsyslog/syslog-ng	Lesson 17, Topic B
journalctl	Lesson 17, Topic B
nxlog	Lesson 17, Topic B
Bandwidth monitors	Lesson 17, Topic B
Metadata	Lesson 17, Topic B
Email	Lesson 17, Topic B
Mobile	Lesson 17, Topic B
Web	Lesson 17, Topic B
File	Lesson 17, Topic B
Netflow/sflow	Lesson 17, Topic B
Netflow	Lesson 17, Topic B
sflow	Lesson 17, Topic B
IPFIX	Lesson 17, Topic B
Protocol analyzer output	Lesson 17, Topic B
4.4 Given an incident, apply mitigation techniques or controls to secure an environment	Lesson 17, Topic C
Reconfigure endpoint security solutions	Lesson 17, Topic C
Application approved list	Lesson 17, Topic C
Application block list/deny list	Lesson 17, Topic C
Quarantine	Lesson 17, Topic C
Configuration changes	Lesson 17, Topic C
Firewall rules	Lesson 17, Topic C
MDM	Lesson 17, Topic C
DLP	Lesson 17, Topic C
Content filter/URL filter	Lesson 17, Topic C
Update or revoke certificates	Lesson 17, Topic C
Isolation	Lesson 17, Topic C
Containment	Lesson 17, Topic C
Segmentation	Lesson 17, Topic C
SOAR	Lesson 17, Topic C
Runbooks	Lesson 17, Topic C
Playbooks	Lesson 17, Topic C
4.5 Explain the key aspects of digital forensics	Lesson 18, Topic A Lesson 18, Topic B
Documentation/evidence	Lesson 18, Topic A
Legal hold	Lesson 18, Topic A
Video	Lesson 18, Topic A
Admissibility	Lesson 18, Topic A
Chain of custody	Lesson 18, Topic A
Timelines of sequence of events	Lesson 18, Topic A
Time stamps	Lesson 18, Topic A
Time offset	Lesson 18, Topic A

Domain and Objective	Covered in
Tags	Lesson 18, Topic A
Reports	Lesson 18, Topic A
Event logs	Lesson 18, Topic A
Interviews	Lesson 18, Topic A
Acquisition	Lesson 18, Topic B
Order of volatility	Lesson 18, Topic B
Disk	Lesson 18, Topic B
Random-access memory (RAM)	Lesson 18, Topic B
Swap/pagefile	Lesson 18, Topic B
OS	Lesson 18, Topic B
Device	Lesson 18, Topic B
Firmware	Lesson 18, Topic B
Snapshot	Lesson 18, Topic B
Cache	Lesson 18, Topic B
Network	Lesson 18, Topic B
Artifacts	Lesson 18, Topic B
On-premises vs. cloud	Lesson 18, Topic B
Right-to-audit clauses	Lesson 18, Topic B
Regulatory/jurisdiction	Lesson 18, Topic B
Data breach notification laws	Lesson 18, Topic B
Integrity	Lesson 18, Topic B
Hashing	Lesson 18, Topic B
Checksums	Lesson 18, Topic B
Provenance	Lesson 18, Topic B
Preservation	Lesson 18, Topic B
E-discovery	Lesson 18, Topic A
Data recovery	Lesson 18, Topic B
Non-repudiation	Lesson 18, Topic B
Strategic intelligence/counterintelligence	Lesson 18, Topic A
5.0 Governance, Risk, and Compliance	
5.1 Compare and contrast various types of controls	Lesson 1, Topic B
Category	Lesson 1, Topic B
Managerial	Lesson 1, Topic B
Operational	Lesson 1, Topic B
Technical	Lesson 1, Topic B
Control type	Lesson 1, Topic B
Preventative	Lesson 1, Topic B
Detective	Lesson 1, Topic B
Corrective	Lesson 1, Topic B
Deterrent	Lesson 1, Topic B
Compensating	Lesson 1, Topic B
Physical	Lesson 1, Topic B

Domain and Objective	Covered in
5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture	Lesson 1, Topic B
Regulations, standards, and legislation	Lesson 1, Topic B
General Data Protection Regulation (GDPR)	Lesson 1, Topic B
National, territory, or state laws	Lesson 1, Topic B
Payment Card Industry Data Security Standard (PCI DSS)	Lesson 1, Topic B
Key frameworks	Lesson 1, Topic B
Center for Internet Security (CIS)	Lesson 1, Topic B
National Institute of Standards and Technology (NIST) RMF/CSF	Lesson 1, Topic B
International Organization for Standardization (ISO) 27001/27002/27701/31000	Lesson 1, Topic B
SSAE SOC 2 Type I/II	Lesson 1, Topic B
Cloud security alliance	Lesson 1, Topic B
Cloud control matrix	Lesson 1, Topic B
Reference architecture	Lesson 1, Topic B
Benchmarks /secure configuration guides	Lesson 1, Topic B
Platform/vendor-specific guides	Lesson 1, Topic B
Web server	Lesson 1, Topic B
OS	Lesson 1, Topic B
Application server	Lesson 1, Topic B
Network infrastructure devices	Lesson 1, Topic B
5.3 Explain the importance of policies to organizational security	Lesson 8, Topic A Lesson 8, Topic D Lesson 12, Topic A Lesson 16, Topic A Lesson 20, Topic C
Personnel	Lesson 8, Topic A Lesson 8, Topic D
Acceptable use policy	Lesson 8, Topic D
Job rotation	Lesson 8, Topic A
Mandatory vacation	Lesson 8, Topic A
Separation of duties	Lesson 8, Topic A
Least privilege	Lesson 8, Topic A
Clean desk space	Lesson 8, Topic D
Background checks	Lesson 8, Topic A
Non-disclosure agreement (NDA)	Lesson 8, Topic A
Social media analysis	Lesson 8, Topic D
Onboarding	Lesson 8, Topic A
Offboarding	Lesson 8, Topic A
User training	Lesson 8, Topic D
Gamification	Lesson 8, Topic D

Domain and Objective	Covered in
Capture the flag	Lesson 8, Topic D
Phishing campaigns	Lesson 8, Topic D
Phishing simulations	Lesson 8, Topic D
Computer-based training (CBT)	Lesson 8, Topic D
Role-based training	Lesson 8, Topic D
Diversity of training techniques	Lesson 8, Topic D
Third-party risk management	Lesson 12, Topic A
Vendors	Lesson 12, Topic A
Supply chain	Lesson 12, Topic A
Business partners	Lesson 12, Topic A
Service level agreement (SLA)	Lesson 12, Topic A
Memorandum of understanding (MOU)	Lesson 12, Topic A
Master services agreement (MSA)	Lesson 12, Topic A
Business partnership agreement (BPA)	Lesson 12, Topic A
End of life (EOL)	Lesson 12, Topic A
End of service life (EOSL)	Lesson 12, Topic A
NDA	Lesson 12, Topic A
Data	Lesson 16, Topic A
Classification	Lesson 16, Topic A
Governance	Lesson 16, Topic A
Retention	Lesson 16, Topic A
Credential policies	Lesson 8, Topic A
Personnel	Lesson 8, Topic A
Third-party	Lesson 8, Topic A
Devices	Lesson 8, Topic A
Service accounts	Lesson 8, Topic A
Administrator/root accounts	Lesson 8, Topic A
Organizational policies	Lesson 20, Topic C
Change management	Lesson 20, Topic C
Change control	Lesson 20, Topic C
Asset management	Lesson 20, Topic C
5.4 Summarize risk management processes and concepts	Lesson 19, Topic A Lesson 19, Topic B
Risk types	Lesson 19, Topic A
External	Lesson 19, Topic A
Internal	Lesson 19, Topic A
Legacy systems	Lesson 19, Topic A
Multiparty	Lesson 19, Topic A
IP theft	Lesson 19, Topic A
Software compliance/licensing	Lesson 19, Topic A
Risk management strategies	Lesson 19, Topic A

Domain and Objective	Covered in
Acceptance	Lesson 19, Topic A
Avoidance	Lesson 19, Topic A
Transference	Lesson 19, Topic A
Cybersecurity insurance	Lesson 19, Topic A
Mitigation	Lesson 19, Topic A
Risk analysis	Lesson 19, Topic A
Risk register	Lesson 19, Topic A
Risk matrix/heat map	Lesson 19, Topic A
Risk control assessment	Lesson 19, Topic A
Risk control self-assessment	Lesson 19, Topic A
Risk awareness	Lesson 19, Topic A
Inherent risk	Lesson 19, Topic A
Residual risk	Lesson 19, Topic A
Control risk	Lesson 19, Topic A
Risk appetite	Lesson 19, Topic A
Regulations that affect risk posture	Lesson 19, Topic A
Risk assessment types	Lesson 19, Topic A
Qualitative	Lesson 19, Topic A
Quantitative	Lesson 19, Topic A
Likelihood of occurrence	Lesson 19, Topic A
Impact	Lesson 19, Topic A
Asset value	Lesson 19, Topic A
Single loss expectancy (SLE)	Lesson 19, Topic A
Annualized loss expectancy (ALE)	Lesson 19, Topic A
Annualized rate of occurrence (ARO)	Lesson 19, Topic A
Disasters	Lesson 19, Topic B
Environmental	Lesson 19, Topic B
Person-made	Lesson 19, Topic B
Internal vs. external	Lesson 19, Topic B
Business impact analysis	Lesson 19, Topic B
Recovery time objective (RTO)	Lesson 19, Topic B
Recovery point objective (RPO)	Lesson 19, Topic B
Mean time to repair (MTTR)	Lesson 19, Topic B
Mean time between failures (MTBF)	Lesson 19, Topic B
Functional recovery plans	Lesson 19, Topic B
Single point of failure	Lesson 19, Topic B
Disaster recovery plan (DRP)	Lesson 19, Topic B
Mission essential functions	Lesson 19, Topic B
Identification of critical systems	Lesson 19, Topic B
Site risk assessment	Lesson 19, Topic B

Domain and Objective	Covered in
5.5 Explain privacy and sensitive data concepts in relation to security	Lesson 16, Topic A Lesson 16, Topic B
Organizational consequences of privacy and data breaches	Lesson 16, Topic A
Reputation damage	Lesson 16, Topic A
Identity theft	Lesson 16, Topic A
Fines	Lesson 16, Topic A
IP theft	Lesson 16, Topic A
Notifications of breaches	Lesson 16, Topic A
Escalation	Lesson 16, Topic A
Public notifications and disclosures	Lesson 16, Topic A
Data types	Lesson 16, Topic A
Classifications	Lesson 16, Topic A
Public	Lesson 16, Topic A
Private	Lesson 16, Topic A
Sensitive	Lesson 16, Topic A
Confidential	Lesson 16, Topic A
Critical	Lesson 16, Topic A
Proprietary	Lesson 16, Topic A
Personally identifiable information (PII)	Lesson 16, Topic A
Health information	Lesson 16, Topic A
Financial information	Lesson 16, Topic A
Government data	Lesson 16, Topic A
Customer data	Lesson 16, Topic A
Privacy enhancing technologies	Lesson 16, Topic B
Data minimization	Lesson 16, Topic B
Data masking	Lesson 16, Topic B
Tokenization	Lesson 16, Topic B
Anonymization	Lesson 16, Topic B
Pseudo-anonymization	Lesson 16, Topic B
Roles and responsibilities	Lesson 16, Topic A
Data owners	Lesson 16, Topic A
Data controller	Lesson 16, Topic A
Data processor	Lesson 16, Topic A
Data custodian/steward	Lesson 16, Topic A
Data protection officer (DPO)	Lesson 16, Topic A
Information life cycle	Lesson 16, Topic A
Impact assessment	Lesson 16, Topic A
Terms of agreement	Lesson 16, Topic A
Privacy notice	Lesson 16, Topic A