CompTIA Advanced Security Practitioner Certification (CASP+) (Exam CAS-004)

Summary

Length: 40 hours Level: Advanced

This course is for students who are preparing for the CompTIA Advanced Security Practitioner (CASP+) certification exam CAS-003. In this course, students will expand their knowledge of information security to apply more advanced principles. Students will apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies; translate business needs into security requirements; support IT governance and risk management; architect security for hosts, networks, and software; respond to security incidents; and more.

Learning Objectives

In this course students will gain knowledge in:

Supporting IT Governance and Risk Management
Leveraging Collaboration to Support Security
Using Research and Analysis to Secure the Enterprise
Integrating Advanced Authentication and Authorization Techniques
Implementing Cryptographic Techniques
Implementing Security Controls for Hosts
Implementing Security Controls for Mobile Devices
Implementing Network Security
Implementing Security in the Systems and Software Development Lifecycle
Integrating Assets in a Secure Enterprise Architecture
Conducting Security Assessments
Responding to and Recovering from Incidents

Course Outline

1. Perform Risk Management Activities

   Topic 1A Explain Risk Assessment Methods Exam objectives covered 4.1 Given a set of requirements, apply the appropriate risk strategies
   Topic 1B Summarize the Risk Lifecycle Exam objectives covered 4.1 Given a set of requirements, apply the appropriate risk strategies
   Topic 1C Assess & Mitigate Vendor Risk Exam objectives covered 4.2 Explain the importance of managing and mitigating vendor risk.

2. Summarizing Governance & Compliance Strategies

   Topic 2A Meet Cloud Identifying Critical Data Assets Exam objectives covered 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.
   Topic 2B Design Compare and Contrast Regulation, Accreditation, and Standards Exam objectives covered 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.
   Topic 2C Explain Legal Considerations & Contract Types Exam objectives covered 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.

3. Implementing Business Continuity & Disaster Recovery

   Topic 3A Explain the Role of Business Impact Analysis Exam objectives covered- 4.4 Explain the importance of business continuity and disaster recovery concepts.
   Topic 3B Assess Disaster Recovery Plans Exam objectives covered 4.4 Explain the importance of business continuity and disaster recovery concepts.

Topic 3C Explain Testing and Readiness Activities Exam objectives covered 4.4 Explain the importance of business continuity and disaster recovery concepts.

4. Identifying Infrastructure Services

Topic 4A Explain Critical Network Services Exam objectives covered 1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
Topic 4B Explain Defensible Network Design Exam objectives covered 1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
Topic 4C Implement Durable Infrastructures Exam objectives covered 1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.

5. Performing Software Integration

Topic 5A Explain Secure Integration Activities Exam objectives covered 1.3 Given a scenario, integrate software applications securely into an enterprise architecture.
Topic 5B Assess Software Development Activities Exam objectives covered 1.3 Given a scenario, integrate software applications securely into an enterprise architecture
Topic 5C Analyze Access Control Models & Best Practices Exam objectives covered 1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.
Topic 5D Analyze Development Models & Best Practices Exam objectives covered 1.4 Given a scenario, implement data security techniques for securing enterprise architecture.

6. Explain Virtualization, Cloud, and Emerging Technology

Topic 6A Explain Virtualization and Cloud Technology Exam objectives covered 1.6 Given a set of requirements, implement secure cloud and virtualization solutions
Topic 6B Explain Emerging Technologies Exam objectives covered 1.8 Explain the impact of emerging technologies on enterprise security and privacy.

7. Exploring Secure Configurations and System Hardening

Topic 7A Analyze Enterprise Mobility Protections Exam objectives covered 3.1 Given a scenario, apply secure configurations to enterprise mobility
Topic 7B Implement Endpoint Protection Exam objectives covered 3.2 Given a scenario, configure and implement endpoint security controls.

8. Understanding Security Considerations of Cloud and Specialized Platforms

Topic 8A Understand Impacts of Cloud Technology Adoption Exam objectives covered 3.4 Explain how cloud technology adoption impacts organizational security.
Topic 8B Explain Security Concerns for Sector-Specific Technologies Exam objectives covered 3.3 Explain security considerations impacting specific sectors and operational technologies.

9. Implementing Cryptography

Topic 9A Implementing Hashing and Symmetric Algorithms Exam objectives covered 3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.
Topic 9B Implementing Appropriate Asymmetric Algorithms and Protocols Exam objectives covered
3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.

10. Implementing Public Key Infrastructure (PKI)

Topic 10A Analyze Objectives of Cryptography and Public Key Infrastructure (PKI) Exam objectives covered 1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.
Topic 10B Implementing Appropriate PKI Solutions Exam objectives covered 3.5 Given a business requirement, implement the appropriate PKI solution. 3.7 Given a scenario, troubleshoot issues with cryptographic implementations.

11. Understanding Threat and Vulnerability Management Activities

Topic 11A Explore Threat and Vulnerability Management Concepts Exam objectives covered
2.1 Given a scenario, perform threat management activities. 2.3 Given a scenario, perform vulnerability management activities.
Topic 11B Explain Vulnerability and Penetration Test Methods Exam objectives covered 2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.
Topic 11C Explain Technologies Designed to Reduce Risk Exam objectives covered 2.6 Given a scenario, use processes to reduce risk

12. Developing Incident Response Capabilities

Topic 12A Analyzing and Mitigating Vulnerabilities
Exam objectives covered 2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations.
Topic 12B Identifying and Responding to Indicators of Compromise Exam objectives covered 2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response. 2.7 Given an incident, implement the appropriate response.
Topic 12C Exploring Digital Forensic Concepts Exam objectives covered 2.8 Explain the importance of forensic concepts. 2.9 Given a scenario, use forensic analysis tools.

Audience

This course is for top CASP+ Job Roles such as Security Architect, Senior Security Engineer, SOC Manager, Security Analyst, IT Cybersecurity Specialist/INFOSEC Specialist, and Cyber Risk Analyst.

Prerequisites

While there are no prerequisites for this course, please ensure you have the right level of experience to be successful in this training.