CompTIA Advanced Security Practitioner (CASP+)

Introduction

CompTIA Advanced Security Practitioner (CASP+) Certification is for professionals who wish to expand their knowledge of information security to apply more advanced principles. Moreover, CASP+ is the only hands-on and performance-based credential for candidates which enhances their ability to identify the cybersecurity policies and frameworks that can be implemented. Also, Candidates will get the opportunity to apply their critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security measures that help in a lot of organizational strategies.

Course Highlights

This course teaches you about core aspects such as;

- Research, Development & Collaboration
- Risk Management
- Enterprise Security Architecture
- Technical Integration of Enterprise Security
- Enterprise Security Operations

Course Outline

MODULE 1: Risk Management

- Summarize business and industry influences and associated security risks.
- Compare and contrast security, privacy policies, and procedures based on organizational requirements.
- Given a scenario, execute risk mitigation strategies and controls.
- Analyze risk metric scenarios to secure the enterprise.

MODULE 2: Enterprise Security Architecture

- Analyze a scenario and integrate network and security components, concepts, and architectures to meet security requirements.
- Analyze a scenario to integrate security controls for host devices to meet security requirements.
- Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.
- Given software vulnerability scenarios, select appropriate security controls.

MODULE 3: 3.0 Enterprise Security Operations

- Given a scenario, conduct a security assessment using the appropriate methods.
- Analyze a scenario or output, and select the appropriate tool for a security assessment.
- Given a scenario, implement incident response and recovery procedures. 3.3

MODULE 4: Technical Integration of Enterprise Security

- Given a scenario, integrate hosts, storage, networks, and applications into a secure enterprise architecture.
- Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.
- Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.
- Given a scenario, implement cryptographic techniques.
- Given a scenario, select the appropriate control to secure communications and collaboration solutions.

MODULE 5: Research, Development, and Collaboration

- Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.
- Given a scenario, implement security activities across the technology life cycle.
- Explain the importance of interaction across diverse business units to achieve security goals.

Prerequisites

- A minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience.

- A minimum of ten years of general hands-on IT experience, with at least five years of broad hands-on security experience.

Target Audience

The CASP Exam CAS-003 is ideal for the job roles of security architects, security engineer, application security engineer, and technical lead analyst.

Duration

16 hours training course