BOOST
THE LEADING TRAINING PROVIDER

Information Technology

CompTIA Advanced Security Practitioner (CASP+)

Course Introduction

This training course is designed to provide participants with the fundamental concept and knowledge on information security to apply more advanced principles and keep your organization safe from threats. Today's advanced digital world demands IT professionals and individuals with a higher demonstrable skill. This course will help participants develop the skill set needed to confidently perform the tasks as an advanced security professional.

Target Audience

This training course is designed for IT professionals who want to acquire the technical knowledge and skills needed to conceptualize, engineer, integrate, and implement secure solutions across complex enterprise environments. IT professionals should have at least a minimum of 10 years of experience in IT administration and at least five years of hands-on security in an enterprise environment

Learning Objectives

- Determine and choose among different types of virtualized, distributed and shared computing
- Integrate hosts, networks, infrastructures, applications and storage into secure comprehensive solutions
- Discuss the security implications of enterprise storage
- Know the importance of application security
- Conduct security activities across the technology life cycle
- Perform relevant analysis for the purpose of securing the enterprise
- Integrate and implement secure solutions across complex environments to support a resilient enterprise

- Use monitoring, detection, incident response and automation to proactively support ongoing security operations in an enterprise environment
- Apply security practices to cloud, on-premises, endpoint and mobile infrastructure, while considering cryptographic technologies and techniques
- Consider the impact of governance, risk and compliance requirements throughout the enterprise

Course Outline

- **Day 01**

Module 1: Security Architecture

  - Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
  - Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.
  - Given a scenario, integrate software applications securely into an enterprise architecture.
  - Given a scenario, implement data security techniques for securing enterprise architecture.
  - Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls

- **Day 02**

Module 1: Security Architecture

  - Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements
  - Explain the impact of emerging technologies on enterprise security and privacy.

Module 2: Security Operations

- Given a scenario, perform threat management activities.
- Given a scenario, analyze indicators of compromise and formulate an appropriate response
- Given a scenario, perform vulnerability management activities.
- Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.

- **Day 03**

Module 2: Security Operations

- Given a scenario, analyze vulnerabilities and recommend risk mitigations.
- Given a scenario, use processes to reduce risk
- Given an incident, implement the appropriate response.
- Explain the importance of forensic concepts.
- Given a scenario, use forensic analysis tools.

- **Day 04**

Module 3: Security Engineering and Cryptography

- Given a scenario, apply secure configurations to enterprise mobility.
- Given a scenario, configure and implement endpoint security controls.
- Explain security considerations impacting specific sectors and operational technologies.
- Explain how cloud technology adoption impacts organizational security
- Given a business requirement, implement the appropriate PKI solution.
- Given a business requirement, implement the appropriate cryptographic protocols and algorithms
- Given a scenario, troubleshoot issues with cryptographic implementations.

- **Day 05**
  - **Module 4: Governance, Risk, and Compliance**
  - Given a set of requirements, apply the appropriate risk strategies
  - Explain the importance of managing and mitigating vendor risk.
  - Explain compliance frameworks and legal considerations, and their organizational impact.
  - Explain the importance of business continuity and disaster recovery concepts

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
April 14, 2025	April 18, 2025	5 days	4250.00 $	UAE - Dubai
July 21, 2025	July 25, 2025	5 days	4950.00 $	Austria - Vienna
Nov. 3, 2025	Nov. 7, 2025	5 days	4250.00 $	UAE - Dubai