CompTIA Advanced Security Practitioner (CASP+)

Overview

This course provides the knowledge needed to implement security solutions within an enterprise policy framework, using a vendor-neutral format. This includes GRC and vulnerability management programs, applied cryptography, system and network security, identity management, secure development, and incident response. This course maps to the CompTIA CASP+ certification exam.

Course 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

Duration

5 Days

Who Should Attend

- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst
- IT Cybersecurity Specialist/INFOSEC Specialist
- Cyber Risk Analyst

Prerequisites

This course assumes that you have some applied knowledge of computers, TCP/IP networks, and cybersecurity principles. Knowledge equivalent to the CompTIA Security+ or CySA+ certification is helpful.

CompTIA Advanced Security Practitioner (CASP+)

Course Topics

Module 1	**Governance and compliance** • Security governance • Regulatory compliance • Standards and frameworks
Module 2	**Security policies** • Policy design • Controls and procedures • Training and coordination
Module 3	**Risk management** • Risk assessment • Risk management strategies
Module 4	**Enterprise resilience** • BCDR planning • Module B: Resilient architecture
Module 5	**Threat management** • Threats and vulnerabilities • Module B: Threat intelligence sources • Module C: Applied intelligence
Module 6	**Cryptographic techniques** • Cryptographic principles • Module B: Ciphers and hashes
Module 7	**Applied cryptography** • Public key infrastructure • Module B: Cryptographic protocols
Module 8	**Authentication and authorization** • Access control components • Module B: Authentication technologies

CompTIA Advanced Security Practitioner (CASP+)

Module 9	**Network security architecture** • Network vulnerabilities • Module B: Network security infrastructure • Module C: Secure network configuration
Module 10	**Protecting hosts and data** • Host security • Module B: Data security
Module 11	**Threat detection and response** • Threat detection systems • Module B: Network sensors • Module C: Data analysis
Module 12	**Specialized system security** • Mobile device security • Module B: Operational technologies •
Module 13	**Virtual and cloud infrastructure** • Virtual and cloud systems • Module B: Secure cloud infrastructure
Module 14	**Secure applications** • Software assurance • Module B: Application vulnerabilities
Module 15	**Security assessment and testing** • Security testing programs • Module B: Vulnerability assessments • Module C: Vulnerability and patch management
Module 16	**Incident response** • Incident response planning • Module B: Incident response procedures • Module C: Digital forensics