CompTIA® Advanced Security Practitioner (CASP+®)

Course Code: CASP; Duration: 5 days; Instructor-led

WHAT YOU WILL LEARN

Information security is a crucial field in the world of business. You have experience in this field, and now you're ready to take that experience to the next level. In this course, you will expand on your knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened. You'll 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.

Today's IT climate demands individuals with demonstrable skills, and the information and activities in this course can help you develop the skill set you need to confidently perform your duties as an advanced security practitioner.

AUDIENCE

This course is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. The target student should have real-world experience with the technical administration of these enterprise environments.

This course is also designed for students who are seeking the CompTIA® Advanced Security Practitioner (CASP+®) certification and who want to prepare for Exam CAS-003. Students seeking CASP+ certification should have at least 10 years of experience in IT management, with at least 5 years of hands-on technical security experience.

PREREQUISITES

To be fit for this advanced course, you should have at least a foundational knowledge of information security. This includes, but is not limited to:

- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services.
- Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI).
- Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches.
- Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs.

You can obtain this level of knowledge by taking the CompTIA® Security+® (Exam SY0-501) course or by demonstrating this level of knowledge by passing the exam

METHODOLOGY

This program will be conducted with interactive lectures, PowerPoint presentation, discussion and practical exercise.

COURSE OBJECTIVES

In this course, you will analyze and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security.

You will:

- Support IT governance in the enterprise with an emphasis on managing risk.
- Leverage collaboration tools and technology to support enterprise security.
- Use research and analysis to secure the enterprise.
- Integrate advanced authentication and authorization techniques.
- Implement cryptographic techniques.
- Implement security controls for hosts.
- Implement security controls for mobile devices.

- Implement network security.
- Implement security in the systems and software development lifecycle.
- Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture.
- Conduct security assessments.
- Respond to and recover from security incidents.

OUTLINES

Module 1: Supporting IT Governance and Risk Management

- Identify the Importance of IT Governance and Risk Management
- Assess Risk
- Mitigate Risk
- Integrate Documentation into Risk Management

Module 2: Leveraging Collaboration to Support Security

- Facilitate Collaboration across Business Units
- Secure Communications and Collaboration Solutions

Module 3: Using Research and Analysis to Secure the Enterprise

- Determine Industry Trends and Their Effects on the Enterprise
- Analyze Scenarios to Secure the Enterprise

Module 4: Integrating Advanced Authentication and Authorization Techniques

- Implement Authentication and Authorization Technologies
- Implement Advanced Identity and Access Management

Module 5: Implementing Cryptographic Techniques

- Select Cryptographic Techniques
- Implement Cryptography

Module 6: Implementing Security Controls for Hosts

- Select Host Hardware and Software
- Harden Hosts
- Virtualize Servers and Desktops
- Protect Boot Loaders

Module 7: Implementing Security Controls for Mobile Devices

- Implement Mobile Device Management
- Address Security and Privacy Concerns for Mobile Devices

Module 8: Implementing Network Security

- Plan Deployment of Network Security Components and Devices
- Plan Deployment of Network-Enabled Devices
- Implement Advanced Network Design
- Implement Network Security Controls

Module 9: Implementing Security in the Systems and Software Development Lifecycle

- Implement Security throughout the Technology Lifecycle
- Identify General Application Vulnerabilities
- Identify Web Application Vulnerabilities
- Implement Application Security Controls

Module 10: Integrating Assets in a Secure Enterprise Architecture

- Integrate Standards and Best Practices in Enterprise Security
- Select Technical Deployment Models
- Integrate Cloud-Augmented Security Services
- Secure the Design of the Enterprise Infrastructure
- Integrate Data Security in the Enterprise Architecture
- Integrate Enterprise Applications in a Secure Architecture

Module 11: Conducting Security Assessments

- Select Security Assessment Methods
- Perform Security Assessments with Appropriate Tools

Module 12: Responding to and Recovering from Incidents

- Prepare for Incident Response and Forensic Investigations
- Conduct Incident Response and Forensic Analysis

Appendix A: Taking the Exams

Appendix B: Mapping Course Content to CompTIA® Advanced Security Practitioner (CASP+®) Exam CAS-003