CompTIA Advanced Security Practitioner (CASP+) Certification (Exam CAS-003)

Overview

In this course, which prepares you for the CompTIA Advanced Security Practitioner exam (CAS-003),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.

Prerequisite Comments

10 years experience in IT administration, including at least 5 years of hands-on technical security experience, are recommended, but not required

Target 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. It is recommended for students with at least 10 years of experience in IT management, with at least 5 of those years in hands-on technical security.

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, security controls for hosts and mobile devices, network security, and 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; responding to and recovering from security incidents.

Course Outline

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

2 - Leveraging Collaboration to Support Security

Facilitate Collaboration Across Business Units
Secure Communications and Collaboration Solutions

3 - Using Research and Analysis to Secure the Enterprise

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

4 - Integrating Advanced Authentication and Authorization Techniques

Implement Authentication and Authorization Technologies
Implement Advanced Identity and Access Management

5 - Implementing Cryptographic Techniques

Select Cryptographic Techniques
Implement Cryptography

6 - Implementing Security Controls for Hosts

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

7 - Implementing Security Controls for Mobile Devices

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

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

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

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

11 - Conducting Security Assessments

Select Security Assessment Methods
Perform Security Assessments with Appropriate Tools

12 - Responding to and Recovering from Incidents

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

Related Courses, Certifications, Exams

- CompTIA Cybersecurity Analyst (CySA+) Certification (Exam CS0-002)