



## CompTIA Advanced Security Practitioner (CASP)

Duration 5 Days



### COURSE 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.

### 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.

### 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.

### PREREQUISITES

- CompTIA Network+ Certification
- CompTIA Security+ Certification
- CompTIA A+ Certification

To be fit for this advanced course, you should have at least a foundational knowledge of information security. You can obtain this level of knowledge by taking the CompTIA® Security+ (SY0-401) course. You may also demonstrate this level of knowledge by passing the Security+ (SY0-401) exam.

Although not required, we suggest that you either take the following courses or possess the equivalent knowledge in the areas of computer networking and computer maintenance:

- CompTIA® Network+® (N10-005) or CompTIA® Network+® (N10-006)
- CompTIA® A+®: A Comprehensive Approach (Exams 220-801 and 220-802)

**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