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

COURSE DETAILS

Course Code:	CompTIA CASP+
Delivery Type:	Instructor-Led
Duration:	5 Days

COURSE CONTENT

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 guide, 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 in this guide can help you develop the skill set you need to confidently perform your duties as an advanced security practitioner.

COURSE PREREQUISITES

To be fit for this advanced guide, 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 training for CompTIA® Security+ (SY0-501) or by demonstrating this level of knowledge by passing the exam.

COURSE OBJECTIVES

In this guide, 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.

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

- 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.

COURSE OUTLINE

- 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

WHO SHOULD ATTEND

This guide is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. You should have real-world experience with the technical administration of these enterprise environments.
This guide is also designed for learners 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.