CO-CASP

COMPTIA ADVANCED SECURITY PRACTITIONER

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Advanced	Cybersecurity	Instructor Led	NA

INTRODUCTION

CompTIA Advanced Security Practitioner (CASP+) is the ideal certification for technical professionals who wish to remain immersed in technology as opposed to strictly managing. CASP+ is the only hands-on technical mastery and is the ideal certification for advanced practitioners of cybersecurity who require the necessary skills to design, implement, and manage cybersecurity solutions on complex networks to skilfully build a resilient enterprise and prevent the next attack.

AUDIENCE PROFILE

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. The target audience includes the following:

- Cyber Security/IS Professionals
- Information Security Analysts
- Security Architects
- IT Specialist
- Cybersecurity Risk Managers
- Cybersecurity Risk Analysts

PREREQUISITES

Before attending this course, delegates must have achieved the following requirements:

- A minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience.
- While there is no required prerequisite, CASP+ certification is intended to follow Security+ and CySA+ or equivalent experience.

COURSE OBJECTIVES

After completing the CompTIA CASP+ course, delegates will have the skills and knowledge to:

- Enterprise Security domain expanded to include operations and architecture concepts, techniques, and requirements
- More emphasis on analyzing risk through interpreting trend data and anticipating cyber defence needs to meet business goals
- Expanding security control topics to include Mobile and small form factor devices, as well as software vulnerability
- Broader coverage of integrating cloud and virtualization technologies into a secure enterprise architecture
- Inclusion of implementing cryptographic techniques, such as Blockchain-Cryptocurrency and Mobile device encryption

COURSE CONTENT

Lesson 1: Security Architecture

- Analyze the security requirements and objectives to ensure an appropriate, secure network
- Analyze the organizational requirements to determine the proper infrastructure security design
- Integrate software applications securely into an enterprise architecture

Lesson 2: Security Operations

- Perform threat management activities
- Analyze indicators of compromise and formulate an appropriate response
- Perform vulnerability management activities
- Use the appropriate vulnerability
- Assessment and penetration testing methods and tools

Lesson 3: Security Engineering and Cryptography

- Configure and implement endpoint security controls
- Explain security considerations impacting specific sectors and operational technologies

Lesson 4: Governance, Risk, and Compliance

- Apply the appropriate risk strategies
- Explain the importance of managing and mitigating vendor risk
- Explain compliance frameworks and legal
- considerations, and their organizational impact

SKILLS AND COMPETENCIES COVERED

Risk Management 19%

- Summarize business and industry influences and associated security risks
- Compare and contrast security, privacy policies and procedures based on organizational requirements
- Given a scenario, execute risk mitigation strategies and controls
- Analyze risk metric scenarios to secure the enterprise

Enterprise Security Architecture 25%

- Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements
- Implement security controls for host, mobile and small form factor devices
- Given software vulnerability scenarios, select appropriate security controls

Enterprise Security Operations 20%

- Given a scenario, conduct a security assessment using the appropriate methods
- Analyze a scenario or output, and select the appropriate tool for a security assessment
- Given a scenario, implement incident response and recovery procedures

Technical Integration of Enterprise Security 23%

- Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture
- Integrate cloud and virtualization technologies into a secure enterprise architecture
- Troubleshoot advanced authentication technologies to support enterprise security objectives
- Given a scenario, implement cryptographic techniques

Research, Development and Collaboration 13%

- Given a scenario, apply research methods to determine industry trends and their impact to the enterprise
- Implement security activities across the technology life cycle
- Explain the importance of interaction across diverse business units to achieve security goals

ASSOCIATED CERTIFICATIONS & EXAM

This course is designed to prepare students to take the CompTIA CASP CAS-004 Exam. Successfully passing this exam will result in the achievement of the CompTIA Advanced Security Practitioner Certification.