CompTIA CASP+

Course Duration:40 Hours **Course code: CAS - 004**

1. Course Overview

The CompTIA Advanced Security Practitioner (CASP+) course prepares IT professionals for an advanced-level cybersecurity certification, focusing on technical skills, leadership, and practical implementation of security solutions across enterprise environments.

2. What you'll learn?

- Security architecture
- Senior security engineering in traditional, cloud, and hybrid environments
- Governance, risk, and compliance
- Cybersecurity readiness assessment
- Implementation of enterprise-wide cybersecurity solutions
- Monitoring, detection, incident response, and automation
- Security practices in cloud, on-premises, endpoint, and mobile infrastructure
- Cryptographic technologies and techniques

3. Target Audience

IT Professionals:

Individuals working in IT cybersecurity are the primary target, regardless of specific job title, and seek to deepen their understanding of advanced security practices.

Experienced Cybersecurity Professionals:

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

Professionals with a minimum of 10 years of experience in IT administration, with at least 5 years of hands-on technical security experience are ideal candidates

4. Pre-Requisites

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.

5. Course content

Lesson 1: Supporting IT Governance and Risk Management

A: Identify the Importance of IT Governance and Risk Management

B: Assess Risk

C: Mitigate Risk

D: Integrate Documentation into Risk Management

Lesson 2: Leveraging Collaboration to Support Security

A: Facilitate Collaboration across Business Units

B: Secure Communications and Collaboration Solutions

Lesson 3: Using Research and Analysis to Secure the Enterprise

A: Determine Industry Trends and Their Effects on the enterprise

B: Analyze Scenarios to Secure the Enterprise

Lesson 4: Integrating Advanced Authentication and Authorization Techniques

A: Implement Authentication and Authorization Technologies
B: Implement Advanced Identity and Access Management

Lesson 5: Implementing Cryptographic Techniques
A: Select Cryptographic Techniques
B: Implement Cryptography

Lesson 6: Implementing Security Controls for Hosts
A: Select Host Hardware and Software
B: Harden Hosts
C: Virtualize Servers and Desktops
D: Protect Boot Loaders

Lesson 7: Implementing Security Controls for Mobile Devices
A: Implement Mobile Device Management
B: Address Security and Privacy Concerns for Mobile Devices

Lesson 8: Implementing Network Security
A: Plan Deployment of Network Security Components and Devices
B: Plan Deployment of Network-Enabled Devices
C: Implement Advanced Network Design
D: Implement Network Security Controls

Lesson 9: Implementing Security in the Systems and Software Development Lifecycle
A: Implement Security throughout the Technology Lifecycle
B: Identify General Application Vulnerabilities
C: Identify Web Application Vulnerabilities
D: Implement Application Security Controls

Lesson 10: Integrating Assets in a Secure Enterprise Architecture

A: Integrate Standards and Best Practices in Enterprise Security

B: Select Technical Deployment Models

C: Integrate Cloud-Augmented Security Services

D: Secure the Design of the Enterprise Infrastructure

E: Integrate Data Security in the Enterprise Architecture

F: Integrate Enterprise Applications in a Secure Architecture

Lesson 11: Conducting Security Assessments

A: Select Security Assessment Methods

B: Perform Security Assessments with Appropriate Tools

Lesson 12: Responding to and Recovering from Incidents

A: Prepare for Incident Response and Forensic Investigations

B: Conduct Incident Response and Forensic Analysis

6. Exam Preference

Exam Code	CAS-004
Number of Questions	Max. 90
Passing Score	This test has no scaled score; it's pass/fail only.
Length Of Test	165 Minutes