CompTIA Advanced Security Practitioner (CASP)

Duration 5 Days

COURSE OVERVIEW

This course is for students who are preparing for the CompTIA Advanced Security Practitioner (CASP+) certification exam CAS-003. In this course, students will expand their knowledge of information security to apply more advanced principles. Students will 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:

- 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

COURSE OUTLINE

Perform Risk Management Activities

- Explain Risk Assessment Methods Exam objectives covered 4.1 Given a set of requirements, apply the appropriate risk strategies
- Summarize the Risk Lifecycle Exam objectives covered 4.1 Given a set of requirements, apply the appropriate risk strategies
- Assess & Mitigate Vendor Risk Exam objectives covered 4.2 Explain the importance of managing and mitigating vendor risk.

Summarizing Governance & Compliance Strategies

- Meet Cloud Identifying Critical Data Assets Exam objectives covered 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.
- Design Compare and Contrast Regulation, Accreditation, and Standards Exam objectives covered 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- Explain Legal Considerations & Contract Types Exam objectives covered 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.

Implementing Business Continuity & Disaster Recovery

- Explain the Role of Business Impact Analysis Exam objectives covered: 4.4 Explain the importance of business continuity and disaster recovery concepts.
- Assess Disaster Recovery Plans Exam objectives covered 4.4 Explain the importance of business continuity and disaster recovery concepts.
- Explain Testing and Readiness Activities Exam objectives covered 4.4 Explain the importance of business continuity and disaster recovery concepts.

Identifying Infrastructure Services

- Explain Critical Network Services Exam objectives covered 1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
- Explain Defensible Network Design Exam objectives covered 1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.
- Implement Durable Infrastructures Exam objectives covered 1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.

Performing Software Integration

- Explain Secure Integration Activities Exam objectives covered 1.3 Given a scenario, integrate software applications securely into an enterprise architecture.
- Assess Software Development Activities Exam objectives covered 1.3 Given a scenario, integrate software applications securely into an enterprise architecture
- Analyze Access Control Models & Best Practices Exam objectives covered 1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.
- Analyze Development Models & Best Practices Exam objectives covered 1.4 Given a scenario, implement data security techniques for securing enterprise architecture.

Explain Virtualization, Cloud, And Emerging Technology

- Explain Virtualization and Cloud Technology Exam objectives covered 1.6 Given a set of requirements, implement secure cloud and virtualization solutions
- Explain Emerging Technologies Exam objectives covered 1.8 Explain the impact of emerging technologies on enterprise security and privacy.

Exploring Secure Configurations and System Hardening

- Analyze Enterprise Mobility Protections Exam objectives covered 3.1 Given a scenario, apply secure configurations to enterprise mobility
- Implement Endpoint Protection Exam objectives covered 3.2 Given a scenario, configure and implement endpoint security controls.

Understanding Security Considerations of Cloud and Specialized Platforms

- Topic Understand Impacts of Cloud Technology Adoption Exam objectives covered 3.4 Explain how cloud technology adoption impacts organizational security.
- Topic Explain Security Concerns for Sector-Specific Technologies Exam objectives covered 3.3 Explain security considerations impacting specific sectors and operational technologies.

Implementing Cryptography

- Topic Implementing Hashing and Symmetric Algorithms Exam objectives covered 3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.
- Topic Implementing Appropriate Asymmetric Algorithms and Protocols Exam objectives covered
- 3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms.

Implementing Public Key Infrastructure (PKI)

- Analyze Objectives of Cryptography and Public Key Infrastructure (PKI) Exam objectives covered 1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.
- Implementing Appropriate PKI Solutions Exam objectives covered 3.5 Given a business requirement, implement the appropriate PKI solution. 3.7 Given a scenario, troubleshoot issues with cryptographic implementations.

Understanding Threat and Vulnerability Management Activities

- Explore Threat and Vulnerability Management Concepts Exam objectives covered
- Given a scenario, perform threat management activities. 2.3 Given a scenario, perform vulnerability management activities.
- Explain Vulnerability and Penetration Test Methods Exam objectives covered 2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.
- Explain Technologies Designed to Reduce Risk Exam objectives covered 2.6 Given a scenario, use processes to reduce risk

Developing Incident Response Capabilities

- Analyzing and Mitigating Vulnerabilities
- Exam objectives covered 2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations.
- Identifying and Responding to Indicators of Compromise Exam objectives covered 2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response. 2.7 Given an incident, implement the appropriate response.
- Exploring Digital Forensic Concepts Exam objectives covered 2.8 Explain the importance of forensic concepts. 2.9 Given a scenario, use forensic analysis tools.

TARGET AUDIENCE

- Top CASP+ Job Roles
- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst
- IT Cybersecurity Specialist/INFOSEC Specialist
- Cyber Risk Analyst

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th