CompTIA Security+

Duration 5 Days

COURSE OVERVIEW

In this course, students will implement, monitor, and troubleshoot infrastructure, application, information, and operational security. Students will prepare for the CompTIA Security+ certification examination (SY0-501).

COURSE OBJECTIVES

In this course, you will implement information security across a variety of different contexts.

You will:

- Identify the fundamental components of information security.
- Analyze risk.
- Identify various threats to information security.
- Conduct security assessments to detect vulnerabilities.
- Implement security for hosts and software.
- Implement security for networks.
- Manage identity and access.
- Implement cryptographic solutions in the organization.
- Implement security at the operational level.
- Address security incidents.
- Ensure the continuity of business operations in the event of an incident.

TARGET AUDIENCE

This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix, or Linux; and who wants to further a career in IT by acquiring foundational knowledge of security topics; preparing for the CompTIA Security+ certification examination; or using Security+ as the foundation for advanced security certifications or career roles.

PREREQUISITES

- CompTIA Network+ Certification
- CompTIA A+ Certification
- Using Microsoft Windows 8.1
- Microsoft Windows 8.1: Transition from Windows 7

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

COURSE OUTLINE

1 - IDENTIFYING SECURITY FUNDAMENTALS

- Identify Information Security Concepts
- Identify Basic Security Controls
- Identify Basic Authentication and Authorization Concepts
- Identify Basic Cryptography Concepts

2 - ANALYZING RISK

- Analyze Organizational Risk
- Analyze the Business Impact of Risk

3 - IDENTIFYING SECURITY THREATS

- Identify Types of Attackers
- Identify Social Engineering Attacks
- Identify Malware
- Identify Software-Based Threats
- Identify Network-Based Threats
- Identify Wireless Threats
- Identify Physical Threats

4 - CONDUCTING SECURITY ASSESSMENTS

- Identify Vulnerabilities
- Assess Vulnerabilities
- Implement Penetration Testing

5 - IMPLEMENTING HOST AND SOFTWARE SECURITY

- Implement Host Security
- Implement Cloud and Virtualization Security
- Implement Mobile Device Security
- Incorporate Security in the Software Development Lifecycle

6 - IMPLEMENTING NETWORK SECURITY

- Configure Network Security Technologies
- Secure Network Design Elements
- Implement Secure Networking Protocols and Services
- Secure Wireless Traffic

7 - MANAGING IDENTITY AND ACCESS

- Implement Identity and Access Management
- Configure Directory Services
- Configure Access Services
- Manage Accounts

8 - IMPLEMENTING CRYPTOGRAPHY

- Identify Advanced Cryptography Concepts
- Select Cryptographic Algorithms
- Configure a Public Key Infrastructure
- Enroll Certificates
- Back Up and Restore Certificates and Private Keys
- Revoke Certificates

9 - IMPLEMENTING OPERATIONAL SECURITY

- Evaluate Security Frameworks and Guidelines
- Incorporate Documentation in Operational Security
- Implement Security Strategies
- Manage Data Security Processes
- Implement Physical Controls

10 - ADDRESSING SECURITY INCIDENTS

- Troubleshoot Common Security Issues
- Respond to Security Incidents
- Investigate Security Incidents

11 - ENSURING BUSINESS CONTINUITY

- Select Business Continuity and Disaster Recovery Processes
- Develop a Business Continuity Plan

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