DYNAMICDNA
We develop and empower

COMPTIA SECURITY+

Duration	Delivery Method	Level
5 days	Online / Instructor Led	Foundation

Introduction:

Course Code: CO-SE+

CompTIA Security+ is the first security certification a candidate should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to: - Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions - Monitor and secure hybrid environments, including cloud, mobile, and IoT - Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance - Identify, analyse, and respond to security events and incidents

Audience profile:

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+ SY0-601 certification examination; or using Security+ as the foundation for advanced security certifications or career roles.

Pre-requisites:

Before attending this course delegates should possess basic Windows user skills and a fundamental understanding of computer and networking concepts. Additionally, delegates should have:

- Either attended the CompTIA Network+ course, or have equivalent knowledge or;
- Have a minimum of two years of technical networking experience, with an emphasis on security

Course objectives:

In this course, delegates will describe the major networking technologies and systems of modern networks, and configure, manage, and troubleshoot modern networks. In addition, delegates will be able to:

- Assess attacks, threats and vulnerabilities
- Identify various threats to information security
- Conduct security assessments to detect vulnerabilities
- Implement secure cloud solutions
- Implement security for hosts and software
- Implement security for networks
- Implement cryptographic solutions in the organization
- Implement security at the operational level
- Ensure the continuity of business operations in the event of an incident
- Explain data privacy and protection concepts

Modules

Module 1: Comparing Security Roles and Security Controls

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types

Module 2: Explaining Threat Actors and Threat Intelligence

- Explain Threat Actor Types and Attack Vectors
- Explain Threat Intelligence Sources

Module 3: Performing Security Assessments

- Assess Organisational Security with Network Reconnaissance Tools

- Explain Security Concerns with General Vulnerability Types
- Summarize Vulnerability Scanning Techniques
- Explain Penetration Testing Concepts

Module 4: Identify Social Engineering and Malware

- Compare and Contrast Social Engineering Techniques
- Analyse Indicators of Malware-Based Attacks

Module 5 : Summarising Basic Cryptographic Concepts

- Compare and Contrast Cryptographic Ciphers
- Summarise Cryptographic Modes of Operation
- Summarise Cryptographic Use Cases and Weaknesses
- Summarise Other Cryptographic Technologies

Module 6: Implementing Public Key Infrastructure

- Implement Certificates and Certificate Authorities
- Implement PKI Management

Module 7: Implementation Authentication Controls

- Summarise Authentication Design Concepts
- Implement Knowledge-Based Authentication
- Implement Authentication Technologies
- Summarise Biometrics Authentication Concepts

Modules 8: Implementation Identity and Account Management Controls

- Implement Identity and Account Types
- Implement Account Policies
- Implement Authorisation Solutions
- Explain the Importance of Personnel Policies

Modules 9: Implementation Secure Network Designs

- Implement Secure Network Designs
- Implement Secure Switching & Routing
- Implement Secure Wireless Infrastructure
- Implement Load Balancers

Modules 10 : WAN Infrastructure

- Implement Firewalls and Proxy Servers
  Implement Network Security Monitoring
- Summarise the Use of SIEM

Modules 11 : WAN Infrastructure

- Implement Secure Network Operations Protocols
- Implement Secure Application Protocols
- Implement Secure Remote Access Protocols

Modules 12 : Implementing Host Security Solutions

- Implement Secure Firmware
- Implement Endpoint Security
- Explain Embedded System Security Implications

Modules 13 : Implementing Secure Mobile Solutions

- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

Associated certifications and exam:

This course will prepare delegates to write the CompTIA Security+ SY0-601 exam. Successfully passing this exam will result in the attainment of the CompTIA Security+ certification.