CompTIA Security+ (SY0-601)

Duration 5 Days

COURSE DESCRIPTION

In this course, students will build on their knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

COURSE OBJECTIVES

In this course, students will use fundamental security principles to install and configure cybersecurity controls and participate in incident response and risk mitigation. Students will:

- Given a scenario, analyze potential indicators to determine the type of attack.
- Given a scenario, analyze potential indicators associated with application and network attacks.
- Explain different threat actors, vectors, and intelligence sources.
- Explain the security concerns associated with various types of vulnerabilities.
- Summarize the techniques used in security assessments.
- Explain the techniques used in penetration testing.
- Explain the importance of security concepts in an enterprise environment.
- Summarize virtualization and cloud computing concepts and authentication and authorication design concepts.
- Summarize secure application development,deployment, and automation concepts.
- Given a scenario, implement cybersecurity resilience.
- Explain the security implications of embedded and specialized systems.
- Explain the importance of physical security controls.
- Summarize the basics of cryptographic concepts.
- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions and secure network designs.
- Given a scenario, install and configure wireless security settings and implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity and account management controls and authentication and authorization solutions.
- Given a scenario, implement public key infrastructure.
- Given a scenario, use the appropriate tool to assess organizational security.
- Summarize the importance of policies, processes, and procedures for incident response.
- Given an incident, utilize appropriate data sources to support an investigation.
- Given an incident, apply mitigation techniques or controls to secure an environment.
- Explain the key aspects of digital forensics.
- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, or
- frameworks that impact organizational security posture.
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts in relation to security.

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 - THREATS, ATTACKS, AND VULNERABILITIES

- Compare and contrast different types of social engineering techniques.
- Given a scenario, analyze potential indicators
- to determine the type of attack.
- Given a scenario, analyze potential indicators
- associated with application attacks.
- Given a scenario, analyze potential indicators
- associated with network attacks.
- Explain different threat actors, vectors, and intelligence sources.
- Explain the security concerns associated with
- various types of vulnerabilities.
- Summarize the techniques used in security assessments.
- Explain the techniques used in penetration testing.

2 - ARCHITECTURE AND DESIGN

- Explain the importance of security concepts
- in an enterprise environment.
- Summarize virtualization and cloud computing concepts.
- Summarize secure application development,
- deployment, and automation concepts.
- Summarize authentication and authorization design concepts.
- Given a scenario, implement cybersecurity resilience.
- Explain the security implications of embedded and specialized systems.
- Explain the importance of physical security controls.
- Summarize the basics of cryptographic concepts.

3 - IMPLEMENTATION

- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions.
- Given a scenario, implement secure network designs.
- Given a scenario, install and configure wireless security settings.
- Given a scenario, implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity and
- account management controls.
- Given a scenario, implement authentication
- and authorization solutions.
- Given a scenario, implement public key infrastructure.

4 - OPERATIONS AND INCIDENT RESPONSE

- Given a scenario, use the appropriate tool to
- assess organizational security.
- Summarize the importance of policies, processes,
- and procedures for incident response.
- Given an incident, utilize appropriate data
- sources to support an investigation.

- Given an incident, apply mitigation techniques
- or controls to secure an environment.
- Explain the key aspects of digital forensics

5 - GOVERNANCE, RISK, AND COMPLIANCE

- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, or
- frameworks that impact organizational security posture.
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts in relation to security.

TARGET AUDIENCE

This course is designed for information technology (IT) professionals who have 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 want to further a career in IT by acquiring foundational knowledge of security topics or using CompTIA Security+ as the foundation for advanced security certifications or career roles.

This course is also designed for students who are seeking the CompTIA Security+ certification and who want to prepare for the CompTIA Security+ SY0-601 Certification Exam.

PREREQUISITES

- CompTIA Network+ Certification
- CompTIA A+ Certification (Exams 220-1001 and 220-1002)
- To ensure your success in this course, you should have basic Windows user skills and a fundamental understanding of computer and networking concepts.
- CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.