CompTIA Security+ (SY0-701)

Duration 5 Days

COURSE DESCRIPTION

CompTIA Security+ Certification is an excellent entry point for a career in information security. CompTIA Security plus SY0-701 exam expands coverage of cybersecurity threats, risk management, and IoT threats.

CompTIA Security+ course equips teams with the knowledge and skills required to assess the security posture of an enterprise environment, 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; identity, analyze, and respond to security events and incidents.

CompTIA Security+ training course is designed to provide learners with the knowledge and skills necessary to pass the exam and earn the certification. CompTIA Security+ prep course is an intensive program that includes instructor-led training, hands-on exercises, and practice exams. Our experienced instructors will guide you through the material and provide personalized attention to help you succeed.

What you will learn:

- Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts
- Implement secure network architecture concepts and systems design
- Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- Install and configure identity and access services, as well as management controls
- Implement and summarize risk management best practices and the business impact
- Install and configure wireless security settings and implement public key infrastructure

COURSE OBJECTIVES

- Understand and compare various types of security controls and fundamental security principles.
- Analyze and respond to indicators of malicious activity and implement appropriate security solutions.
- Apply security principles to secure enterprise infrastructure and protect data.
- Understand the security implications of different architecture models and resilience strategies.
- Manage hardware, software, and data assets effectively to enhance security.
- Conduct vulnerability management activities and understand security alerting and monitoring tools.
- Implement and maintain identity and access management controls.
- Operate within applicable regulations and policies, understanding governance, risk, and compliance principles.

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

- Respond appropriately to security events and incidents using data sources to support investigations.

COURSE OUTLINE

Module 1: General Security Concepts

- Compare and contrast various types of security controls.
- Summarize fundamental security concepts.
- Explain the importance of change management processes and the impact to security.
- Explain the importance of using appropriate cryptographic solutions.

Module 2: Security Operations

- Given a scenario, apply common security techniques to computing resources.
- Explain the security implications of proper hardware, software, and data asset management.
- Explain various activities associated with vulnerability management.
- Explain security alerting and monitoring concepts and tools.
- Given a scenario, modify enterprise capabilities to enhance security.
- Given a scenario, implement and maintain identity and access management.
- Explain the importance of automation and orchestration related to secure operations.
- Explain appropriate incident response activities.
- Given a scenario, use data sources to support an investigation.

Module 3: Security Architecture

- Compare and contrast security implications of different architecture models.
- Given a scenario, apply security principles to secure enterprise infrastructure.
- Compare and contrast concepts and strategies to protect data.
- Explain the importance of resilience and recovery in security architecture.

Module 4: Threats, Vulnerabilities, and Mitigations

- Compare and contrast common threat actors and motivations.
- Explain common threat vectors and attack surfaces.
- Explain various types of vulnerabilities.
- Given a scenario, analyze indicators of malicious activity.
- Explain the purpose of mitigation techniques used to secure the enterprise.

Module 5: Security Program Management and Oversight

- Summarize elements of effective security governance.
- Explain elements of the risk management process
- Explain the processes associated with third-party risk assessment and management.
- Summarize elements of effective security compliance.
- Explain types and purposes of audits and assessments.
- Given a scenario, implement security awareness practices.

TARGET AUDIENCE

Designed for a broad audience, The CompTIA Security+ SY0-701 course targets individuals ranging from the early stages of their cybersecurity careers to seasoned IT professionals looking to specialize further or validate their skills. It's ideal for those aspiring to roles such as security specialists, systems administrators, or security administrators. Additionally, IT professionals transitioning from other areas into security-focused positions will find this certification particularly beneficial.

The course also caters to current cybersecurity professionals aiming to keep their skills sharp and credentials updated. The globally recognized nature of this certification makes it appealing to anyone looking to position themselves competitively in the IT security job market, whether they're entering the field or seeking to ascend to higher, more specialized roles.

- Security Administrator
- Network Administrator
- Security Consultant

PREREQUISITES

- Basic understanding of computer networks and systems, including familiarity with the internet, devices, and technology.
- Knowledge of foundational IT skills will be helpful, preferably backed by experience or prior certifications (e.g., CompTIA Network+ or equivalent).
- A grasp of basic security concepts or experience in IT support roles with exposure to security tasks.
- Commitment to continuous learning and staying updated on new cybersecurity threats and technologies.