

## Course Training

### CompTIA Security+

#### Course Content

Advances in information and communication technology, as well as social networks, play a significant role in the daily lives of today's people. At the same time, it was found that cybersecurity problems have become increasingly intense and severe. Cyber threats have an impact on both the national and organizational levels. Therefore, organizations must develop their workforce to have the knowledge and ability to protect their organizations from various forms of cyber threats. The CompTIA Security+ course, which is an international certification, covers various forms of cyber threats, designing secure corporate information technology systems, handling cyber incidents (Incident Response), and is the starting point for professional IT security skills.

#### Course Objectives

By the end of the course, you should be able to meet the following objectives:

- To provide trainees with an understanding of the principles of information technology security
- To provide trainees with the knowledge to prepare for the CompTIA Security+ international certification exam

#### Who should attend

- Network Design Engineers
- Sales Engineers
- System Engineers
- 

#### Course Outline

- Security Roles and Security Controls
- Threat Actors and Threat Intelligence
- Security Assessments
- Social Engineering and Malware
- Basic Cryptographic Concepts
- Implement Public Key Infrastructure
- Implement Authentication Controls
- Implement Identity and Account Management Controls
- Implement Secure Network Designs
- Implement Network Security Appliances
- Implement Secure Network Protocols
- Implement Host Security Solutions
- Implement Secure Mobile Solutions
- Secure Application Concepts

- Implement Secure Cloud Solutions
- Data Privacy and Protection Concepts
- Perform Incident Response
- Digital Forensics
- Risk Management Concepts
- Implement Cybersecurity Resilience
- Physical Security