CompTIA Security+ Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

CompTIA Security+ is one of the most respected **cybersecurity certifications** available today and provides a strong foundation for professionals pursuing a career in **information security**.

This intensive five-day training program is designed to prepare participants for the official **CompTIA Security+ SY0-701 exam**, which is included with the course.

Throughout the program, attendees will gain practical knowledge in **network security**, **application security**, **device protection**, and **enterprise security operations**. The course also covers essential areas such as **threat analysis**, **risk mitigation**, **incident response**, and **security compliance**.

Why Earn CompTIA Security+?

The **CompTIA Security+ certification** validates the essential skills required to:

- Protect enterprise networks
- Detect and analyze threats
- Secure critical data
- Respond to security incidents

As one of the leading **cybersecurity certifications**, Security+ helps professionals build credibility, expand career opportunities, and establish a strong foundation for advanced security roles.

Prerequisites

Participants should have familiarity with:

- Basic **networking concepts**
- **Windows** operating systems
- **Linux** operating systems
- General IT infrastructure fundamentals

CompTIA Security+ Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

This course is ideal for:

- **Security Administrators**
- **Security Specialists**
- **Systems Administrators**
- **Help Desk Analysts**
- **Security Engineers**
- **Security Analysts**
- Infrastructure professionals
- IT professionals transitioning into **cybersecurity**

What You Will Learn

By completing this course, participants will be able to:

- Evaluate the **security posture** of enterprise environments
- Recommend and implement appropriate **security solutions**
- Secure **cloud**, **mobile**, **IoT**, and **operational technology** environments
- Apply principles of **governance**, **risk management**, and **compliance**
- Identify and respond to **security incidents**
- Implement **identity and access management** controls

Outline

1. General Security Concepts (12%)

This module introduces the core principles of **cyber security**.

Topics include:

- Security controls
- Security fundamentals
- Change management
- Security impacts of organizational changes
- **Cryptographic solutions**
- Security best practices

2. Threats, Vulnerabilities & Mitigations (22%)

Participants explore common cyber threats and defense strategies.

Topics include:

- Threat actors and motivations
- Attack vectors
- Attack surfaces

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Vulnerabilities
- Indicators of malicious activity
- Enterprise protection strategies
- Mitigation techniques

3. Security Architecture (18%)

Learn how to design and secure modern enterprise environments.

Topics include:

- **Security architecture models**
- Infrastructure protection
- Data security strategies
- Security principles
- Business continuity
- Resilience and recovery planning

4. Security Operations (28%)

This section focuses on day-to-day **security operations**.

Topics include:

- Securing computing resources
- Asset management
- Hardware and software security
- **Vulnerability Management**
- Security monitoring tools
- Alerting systems
- **Identity and Access Management (IAM)**
- Incident response
- Security investigations
- Automation and orchestration

5. Security Program Management & Oversight (20%)

Participants learn how to manage enterprise security programs effectively.

Topics include:

- **Security Governance**
- **Risk Management**
- Third-party risk assessments
- Compliance frameworks
- Audits and assessments
- Security awareness programs
- Organizational security policies