# CompTIA Security+ Certification Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Data Security | **Duration** | 5 Days |
| **Base Fee** | $1,500 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

In today’s hyper-connected digital landscape, cybersecurity is no longer optional—it's a necessity. The CompTIA Security+ Certification is a globally recognized credential that validates the baseline skills necessary to perform core security functions and pursue an IT security career. CompTIA Security+ Certification Training Course is designed to equip IT professionals with the essential knowledge to protect systems, mitigate cyber threats, and ensure data integrity in enterprise environments.

This course emphasizes hands-on training, real-world case studies, and up-to-date cybersecurity tools and practices. Through engaging content and industry-relevant examples, learners gain in-demand skills such as threat detection, incident response, and risk management. Whether you’re a beginner or looking to advance your IT security career, this course will provide the technical and strategic competencies needed for Security+ certification and beyond.

## Programme Curriculum

**CompTIA Security+ Certification Training Course**

**Introduction**

In today’s hyper-connected digital landscape, cybersecurity is no longer optional—it's a necessity. The CompTIA Security+ Certification is a globally recognized credential that validates the baseline skills necessary to perform core security functions and pursue an IT security career. CompTIA Security+ Certification Training Course is designed to equip IT professionals with the essential knowledge to protect systems, mitigate cyber threats, and ensure data integrity in enterprise environments.

This course emphasizes hands-on training, real-world case studies, and up-to-date cybersecurity tools and practices. Through engaging content and industry-relevant examples, learners gain in-demand skills such as threat detection, incident response, and risk management. Whether you're a beginner or looking to advance your IT security career, this course will provide the technical and strategic competencies needed for Security+ certification and beyond.

**Course Objectives**

1. Understand and apply cybersecurity principles to real-world scenarios.
2. Analyze and mitigate security threats, attacks, and vulnerabilities.
3. Master security architecture and design for enterprise systems.
4. Deploy secure network components and configure access control models.
5. Identify and respond to security incidents using appropriate tools and techniques.
6. Manage and protect data, devices, and infrastructure across platforms.
7. Implement identity and access management controls effectively.
8. Evaluate and apply risk management and cryptographic solutions.
9. Use SIEM tools and other logging systems for threat intelligence.
10. Explore emerging technologies like cloud security and IoT risks.
11. Align IT security measures with compliance frameworks (GDPR, HIPAA).
12. Prepare for the CompTIA Security+ SY0-601 exam with confidence.
13. Develop career-ready cybersecurity skills for job placement success.

**Target Audience**

1. IT Support Specialists
2. Network Administrators
3. Cybersecurity Enthusiasts
4. Junior Penetration Testers
5. Help Desk Technicians
6. Government and Military IT Staff
7. Recent Graduates in IT or CS
8. Professionals Preparing for a Career in Cybersecurity

**Course Duration:** 5 days

**Course Modules**

**Module 1: Threats, Attacks & Vulnerabilities**

- Types of attacks (malware, phishing, DoS, etc.)
- Threat actors and their motivations
- Penetration testing vs vulnerability scanning
- Security assessment techniques
- Social engineering threats and countermeasures
- **Case Study**: Analysis of the 2021 Colonial Pipeline ransomware attack

**Module 2: Architecture and Design**

- Secure network architecture principles
- Security implications of embedded systems
- Virtualization and cloud computing security
- Enterprise resilience and redundancy strategies
- Implementing secure system design
- **Case Study**: Securing a multi-tier cloud-based application infrastructure

**Module 3: Implementation**

- Secure protocols (HTTPS, SFTP, SNMPv3)
- Wireless security settings and best practices
- Identity and access management (IAM)
- Implementing PKI and certificates
- Host and application security measures
- **Case Study**: Implementing security controls for a remote workforce

**Module 4: Operations and Incident Response**

- Incident response process and roles
- Digital forensics basics and tools
- Detection tools: SIEM, EDR, logs
- Mitigation strategies post-breach
- Business continuity and disaster recovery plans
- **Case Study**: Responding to an advanced persistent threat (APT)

**Module 5: Governance, Risk, and Compliance**

- Risk analysis and mitigation planning
- Data privacy laws and compliance (GDPR, HIPAA)
- Security policies and procedures
- Frameworks: NIST, ISO, COBIT
- Audit processes and reporting
- **Case Study**: Navigating a compliance audit in the healthcare sector

**Module 6: Cryptography and PKI**

- Encryption algorithms (AES, RSA, ECC)
- Hashing and message integrity
- Public key infrastructure (PKI) components
- Key management and lifecycle
- Secure protocols using cryptography
- **Case Study**: Using PKI to secure an e-commerce website

**Module 7: Identity and Access Management (IAM)**

- Authentication methods (MFA, biometrics)

- Authorization models (RBAC, ABAC)
- Account management best practices
- Identity federation and SSO
- Secure credential storage
- **Case Study**: IAM implementation in a growing fintech company

**Module 8: Security+ Exam Prep and Career Guidance**

- Exam format and study tips
- Practice questions and mock tests
- Resume building for cybersecurity roles
- Interview preparation strategies
- LinkedIn optimization for job seekers
- **Case Study**: From training to job offer – the path of a successful Security+ student

**Training Methodology**

- Interactive instructor-led sessions and self-paced options
- Scenario-based hands-on labs and simulations
- Real-world case studies and group discussions
- Regular quizzes and assignments for reinforcement
- Comprehensive exam preparation with mock tests
- Personalized mentorship and career guidance

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.org or call** *+254769199797*

***Certification***

*Upon successful completion of this training, participants will be issued with a globally- recognized certificate.*

***Tailor-Made Course***

*We also offer tailor-made courses based on your needs.*

**Key Notes**

**a.** The participant must be conversant with English.

**b.** Upon completion of training the participant will be issued with an Authorized Training Certificate

**c.** Course duration is flexible and the contents can be modified to fit any number of days.

**d.** The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **21 Sep 2026** | 25 Sep 2026 | Online | $1,000 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $1,500 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |

Ready to enroll or request a customized program? Book online or contact us:

**Register Online Now**

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com