CompTIA Security+ 501 Training

EMC² Education Technologies

Table of **Contents**

CompTIA Security+

CompTIA Security+ is the first security certification IT professionals earn. It is a globally trusted certification that verifies foundational-level IT security knowledge and skills. Our CompTIA Security+ course teaches baseline cybersecurity skills while emphasizing hands-on practical skills; ensuring the security professional is better prepared to problem solve a wide variety of issues such as performing threat analyses and responding with appropriate mitigation skills.

Target **Audience**

- Non-IT Professionals
- Students studying at community colleges or universities
- IT Professionals
- High school students (juniors and seniors only)

Key **Outcomes**

- Recognize threats, attacks and vulnerabilities
- Understand cyber technologies & tools to mitigate risks
- Architecture & design of network security to preserve integrity and confidentiality of critical information
- Understand cryptography and Public Key Infrastructure (PKI)

Course **Features**

- Course delivery 100% online, live classroom and self-paced learning
- 50 hours of blended learning
- 32 hours of synchronous instructor-led instruction
- 18 hours of self-paced learning
- CompTIA Security+ Certification Exam Voucher included

Additional **Resources**

- Intensive boot camp (certification exam prep)
- 2 full review exams
- Career counseling
- Resume prep workshop

Certification

Candidates must pass the SYO-501 exam administered by CompTIA. The exam has up to 90 questions and lasts 90 minutes. Candidates must score at least 750 to pass the exam.

Exam fee is included in the course fee.

https://comptia.org/certifications/security

CompTIA Security+ Training Course **Curriculum**

- **Module 1 – Threats, Attacks and Vulnerabilities**
  - Introduction
  - Malware Types & Indicator of Compromise
  - Cyber Attacks
    - Application/Service Attacks
    - Network Vulnerability – Lab
    - Cryptographic Attacks
    - Social Engineering
    - Social Engineering – Lab
    - Wireless Attacks
  - Threat Actors
  - Introduction to Penetration Testing
  - Introduction to Vulnerability Scanning
  - Vulnerability Scanning – Lab
  - SQL Injection Attack – Lab
  - Exam & Assessment

- **Module 2 – Cyber Technologies & Tools**
  - Introduction
  - Introduction to Networking
  - Networking Components
    - Firewall
    - Router
    - VPN
    - Switch
    - Proxy
    - Access Point
    - Load Balancer
    - SIEM
    - NAC
    - IPSEC
  - Security Tools
  - Mobile Security
  - Traffic Analyze – Lab
  - Exam & Assessment

- **Module 3 – Architecture & Design**
  - Introduction
  - Frameworks & Best Practices
  - Network Architecture Concept
    - Topologies
    - Zones
    - VPN
    - SDN
  - Secure System Design
    - Hardware / Firmware Security
    - Operating Systems
    - Patch Management
  - Embedded System

- Secure Application Development & Deployment
- Cloud Systems
- Physical Security
- System Resilience – Lab
- Exam & Assessment

- **Module 4 – Identity & Access Management**
  - Introduction
  - IAM Concepts
  - Install & Configure Identity & Access Services – Lab
  - IAM Models
  - Password Cracking Tools – Lab
  - Account Management Practices
  - Exam & Assessment

- **Module 5 – Risk Management**
  - Introduction
  - Policy, Plan & Procedure
  - Business Impact Analysis Concept
  - Risk Management Processes and Concepts
  - Incident Management
  - Incident Management – Lab
  - Introduction to Digital Forensics
  - Digital Forensics Types
  - Backup & Disaster Recovery
  - Backup & Disaster Recovery Planning – Lab
  - Control Types
  - Data Privacy
  - Exam & Assessment

- **Module 6 – Cryptography & PKI**
  - Introduction
  - Cryptography Basics – I
  - Cryptography Basics – II
  - Cryptography Basics – III
  - Hashing & Encryption
  - Cryptography Algorithms – I
  - Cryptography Algorithms – II
  - Cryptography Algorithms – Lab
  - Wireless Security
  - Introduction to PKI
  - PKI Concepts
  - Certificates
  - Exam & Assessment

- **Module 7 – Boot Camp**
  - Introduction
  - Thread Attack & Vulnerabilities – Brief
  - Thread Attack & Vulnerabilities – Lab
  - Exam & Assessment
  - Cyber technologies & Tools – Brief
  - Cyber technologies & Tools – Lab
  - Exam & Assessment
  - Architecture & Design – Brief
  - Architecture & Design – Lab
  - Exam & Assessment
  - Identity & Access Management – Brief
  - Identity & Access Management – Lab
  - Exam & Assessment
  - Risk Management – Brief
  - Risk Management – Lab

- Exam & Assessment
- Cryptography & PKI – Brief
- Cryptography & PKI – Lab
- Exam & Assessment
- CompTIA Security + Test Taking Tips
- Practice Certification Exam – I
- Practice Certification Exam – II
- Practice Certification Exam – III

About **Us**

EMC^2 Education Technologies is a distance learning company providing state-of-the-art IT certification programming. The mission of our company is creating opportunities for individuals and communities through digital skills training. Our company transforms lives by helping close the achievement gap and digital divide.

We partner with leading companies and industry leaders to offer carefully-designed courses to help our students achieve their professional goals. Our founders have decades of experience working with students and providing results-oriented solutions based on unique needs of each client.