

CompTIA Security+ Training Course

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

SEC-10B

Course Objectives

Professional, practical, & hands-on live instructor-led training


Start as a beginner and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

 Start Today


Potential Career Tracks


 Cyber Security Analyst

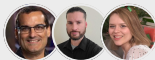
 Cloud Security Engineer

 Junior SOC Analyst

 Network Security Engineer

 Cyber Security Consultant

 Security Specialist



Taught by Industry Veterans & Qualified Instructors

Introduction to CompTIA Security+

Course Overview

Intellectual Point's comprehensive CompTIA Security+ training program is designed to not only make you proficient in cybersecurity concepts but also thoroughly prepare you for the CompTIA Security+ certification exam. Whether you're new to cybersecurity or looking to validate and deepen your existing skills, this course covers everything from foundational knowledge to advanced techniques necessary to secure networks and systems in real-world environments.

Throughout the course, you'll explore key security principles, hands-on techniques, and essential tools to safeguard sensitive information, while building your confidence for the certification exam. This training goes beyond just exam preparation, ensuring that you acquire the practical knowledge required to respond to real-life security threats and vulnerabilities with proficiency. By combining theory with practical application, this course ensures that you are not only prepared for the exam but also capable of applying your skills effectively.

Obtainable Skills

Threats and vulnerabilities

Identity and access management

Forensics

Security architecture

Cryptography and PKI

Risk management

Enterprise networks

Hybrid/cloud operations

Incident response

Course Insights

Audience Profile

This course is designed for IT professionals, network administrators, and individuals seeking to build a career in cybersecurity. It is ideal for those preparing for the CompTIA Security+ certification exam, as well as those looking to deepen their knowledge of network security, threat management, and risk mitigation.

Whether you're an entry-level professional, someone transitioning into cybersecurity, or an experienced IT professional looking to expand your skill set, this training provides a solid foundation in security principles. The course is beginner-friendly, making it accessible for those with no prior cybersecurity experience.

Course Objectives

By the end of this course, participants should:

1 Be fully prepared to take the CompTIA Security+ exam with confidence.

2 Have a deep, practical understanding of cybersecurity principles and best practices.

3 Be able to secure systems, networks, and data against a variety of threats.

4 Be equipped to handle real-world security incidents and risk management tasks.

5 Develop the ability to create effective security policies and procedures within an organization.

Module by Module Learning *Outline* 6 Modules Module 1: Introduction to Cybersecurity

Learning Objectives:

- Understand the basic principles and importance of cybersecurity.
- Identify various roles within the cybersecurity field and their functions.

 Topics Covered

Overview of Cybersecurity:

- Definition and key goals: Confidentiality, integrity, and availability.
- Importance of cybersecurity in today's digital landscape.

Cybersecurity Careers:

- Various roles in cybersecurity and their responsibilities.
- Career pathways and certifications in cybersecurity.

 Module 2: Risk Management in Cybersecurity

Learning Objectives:

- Comprehend the fundamentals of risk management and its role in cybersecurity.
- Learn to assess and mitigate risks effectively.

 Topics Covered

Risk Assessment Techniques

- Identifying and evaluating information security risks.
- Risk analysis methodologies and frameworks.

Risk Mitigation Strategies

- Approaches to risk reduction and acceptance.
- Developing and implementing risk management plans.

 Module 3: Network Security Fundamentals

Learning Objectives:

- Explore key components of network security.
- Understand secure network configurations and protocols.


 Topics Covered

Basics of Network Security:

- Network security principles and practices.
- Overview of firewalls, VPNs, and intrusion detection systems.

Securing Networks:

- Best practices for network configuration.
- Tools and techniques for enhancing network defense.

 Module 4: Threat Analysis and Response

Learning Objectives:

- Identify various types of cyber threats and vulnerabilities.
- Implement effective incident response strategies.

 Topics Covered

Cyber Threats and Vulnerabilities:

- Types of cyber threats: Malware, phishing, DDoS, etc.
- Vulnerability assessment tools and techniques.

Incident Response Protocols

- Steps in developing an incident response plan.
- Practical approaches to carrying out incident response.

 Module 5: Policy Implementation and Cybersecurity Frameworks

Learning Objectives:

- Gain insights into cybersecurity policies and frameworks.
- Develop and implement security measures within an organization.


 Topics Covered

Cybersecurity Policies:

- Importance and components of a strong cybersecurity policy.
- Processes for creating and enforcing policies.

Cybersecurity Frameworks:

- Overview of frameworks like NIST, ISO, and others.
- Implementation of best practices and controls.

 Module 6: Hands-On Lab and Certification Preparation

Learning Objectives:

- Apply theoretical knowledge in practical scenarios to reinforce learning.
- Prepare effectively for the Certified in Cybersecurity (CC) exam.

 Topics Covered

Real-World Simulations:

- Types of cyber threats: Malware, phishing, DDoS, etc.
- Vulnerability assessment tools and techniques.

Exam Preparation

- Review of key exam topics and practice questions.
- Strategies for successful exam completion and obtaining certification.