

CompTIA Security+

Description

The CompTIA Security+ exam will certify that the successful candidate has the knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations.

Classroom Registration Price (CHF)

3800

Virtual Classroom Registration Price (CHF)

3550

Course Content

Module 1: Security Fundamentals

- Lesson 1: Security concepts
- Lesson 2: Risk management
- Lesson 3: Vulnerability assessment

Module 2: Understanding attacks

- Lesson 1: Understanding attackers
- Lesson 2: Social engineering
- Lesson 3: Malware
- Lesson 4: Network attacks
- Lesson 5: Application attacks

Module 3: Cryptography

- Lesson 1: Cryptography concepts
- Lesson 2: Public key infrastructure

Module 4: Network fundamentals

- Lesson 1: Network components
- Lesson 2: Network addressing
- Lesson 3: Network ports and applications

Module 5: Securing networks

- Lesson 1: Network security components
- Lesson 2: Transport encryption
- Lesson 3: Hardening networks
- Lesson 4: Monitoring and detection

Module 6: Securing hosts and data

- Lesson 1: Securing hosts

- Lesson 2: Securing data
- Lesson 3: Mobile device security

Module 7: Securing network services

- Lesson 1: Securing applications
- Lesson 2: Virtual and cloud systems

Module 8: Authentication

- Lesson 1: Authentication factors
- Lesson 2: Authentication protocols

Module 9: Access control

- Lesson 1: Access control principles
- Lesson 2: Account management

Module 10: Organizational security

- Lesson 1: Security policies
- Lesson 2: User training
- Lesson 3: Physical security and safety

Module 11: Disaster planning and recovery

- Lesson 1: Business continuity
- Lesson 2: Fault tolerance and recovery
- Lesson 3: Incident response

Lab / Exercises

- Official CompTIA Labs included

Documentation

- Digital courseware included

Exam

- This course prepares you to the SYO-601 exam. If you wish to take this exam, please contact our secretariat who will let you know the cost of the exam and will take care of all the necessary administrative procedures for you.

Participant profiles

- Consultants and network engineers
- Security administrators
- System administrators
- Security analysts

Prerequisites

- Having followed or the knowledge covered by the trainings: CompTIA A+ et CompTIA Network+

Objectives

- Identify network attack strategies and defences
- Understand the principles of organisational security and the elements of effective security policies
- Know the technologies and uses of cryptographic standards and products
- Identify network - and host-based security technologies and practices
- Describe how wireless and remote access security is enforced
- Describe the standard and products used to enforce security on web and communications technologies
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery

Niveau

Intermédiaire

Duration (in Days)

5

Reference

COM-03