+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 24/06/2025

Sign up

CompTIA Security+ Training : Certification (SY0-701)

ALL-IN-ONE : EXAM INCLUDED IN PRICE

4 days (28 hours)

Presentation

Our Comptia Security+© training course will prepare you effectively for certification. An essential qualification to prove your fundamental skills in IT security.

Our syllabus follows the main sections of the exam: threats, attacks and vulnerabilities, architecture, implementation, incident response and compliance.

Our training begins with a presentation of the different types of attack and their associated risks, followed by an introduction to the fundamental concepts of cybersecurity, including cryptography and the cloud. We'll also help you choose the right services for your organization.

Finally, we'll teach you key concepts in terms of incident response, forensic analysis, the importance of governance and compliance with security standards.

Training content

- 8 expert coaching sessions: 8 x Wednesday mornings (9am to 12:30pm) per week (28 hours)
- 1 year's self-study access to the Labs
- 1 certification exam

Objectives

- Understand general security concepts
- Identify threats, vulnerabilities and mitigation measures in given scenarios
- Understand and apply secure architectures
- Understand and apply security operations
- Manage and supervise security programs

Target audience

- System administrators
- Security engineer
- Cybersecurity analyst
- Network Administrator

Prerequisites

- Recommended experience of 2 years in system/security administration
- Solid knowledge of IT security
- Proficiency in networking and administration of Windows-based TCP/IP networks
- Knowledge of other operating systems, such as OS X, Unix or Linux
- Comptia Network+™ certification is recommended

Note: Ambient IT does not own Comptia Certifications©, this certification belongs to Comptia, Inc.

Comptia Security+™ Certification Preparation Program

Threats, attacks and vulnerabilities

- Summary of fundamental security concepts
- Comparison of threat types
- Cryptographic solutions explained
- Implementing identity and access management
- Secure enterprise network architecture
- Secure cloud network architecture
- Explanation of resilience and site security concepts
- Explanation of vulnerability management
- Assessment of network security capabilities
- End-point security assessment
- Enhancement of application security capabilities
- Analysis of malicious activity indicators
- Explanation of incident response and monitoring concepts
- Analysis of malicious activity indicators
- Summary of security governance concepts
- Explanation of risk management processes
- Summary of data protection and compliance concepts

- Mapping course content to CompTIA Security+

Architecture

- IT security concepts
- Virtualization and cloud computing
- Securing application development
- Authentication and authorization
- Understanding resilience
- Security on embedded and specialized systems
- Physical security controls
- Cryptography concepts

Implementation

- Secure protocols
- Hosting security
- Application security
- Network security
- Wireless security configuration
- Mobile security
- Protecting the cloud
- Implementing IAM
- Authentication and authorization solutions
- Setting up a public key

Operations and incident response

- Choosing the right tools
- Rules and procedures for responding to incidents
- Choosing the right data sources for investigation
- Mitigation techniques
- Understanding forensic analysis

Governance, risk and compliance

- Different types of control
- Current security standards
- The importance of security policies within an organization
- Risk management
- Concepts of confidentiality and sensitive data

Strategy and methods for passing the exam Mock

exam

FAQ - QUESTIONS / ANSWERS

What language is Comptia Security+ taught in?

The course is taught in French.

Is the exam included in the course price?

Yes, the price of the certification is included in the cost of the course ($404 for information purposes). You can take the exam at the end of the session.

How does the Comptia Security+ certification exam work?

The exam consists of a performance-based MCQ of up to **90 questions**. It is taken online at

an approved Pearson Vue test center.

The exam lasts **90 minutes**, and is available in English and French.

To pass this exam, you need to score at least 750 points, on a scale from 100 to 900 points.

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples and

and group work sessions.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.