CompTIA Security+¬ Training

Course: **00068**
Filter: **Beginner**
Duration: **4 days**
Category:: **Gouvernance, Risk and Compliance**
Price: **3895,00 €**

About Course

Looking to advance your career in information security? Look no further than CompTIA Security+ Training. This comprehensive course covers everything you need to know to pass the CompTIA Security+ SY0-601 certification exam and become an information system security best practices expert. Gain a deep understanding of systems and network security, network infrastructure, access control, assessments and audits, cryptography, and organizational security. You'll also receive a CompTIA Security+ exam voucher, study guide, and practice questions to help you prepare. With on-demand, online, and in-person training options, you can choose the delivery method that works best for you. And if you're looking for even more in-depth training, the Premium Blended Training and On-Demand Training Bundles offer annual access to a wealth of additional content and resources. So don't wait any longer to take your career to the next level - enroll in CompTIA Security+ Training today.

What you'll learn

- Receive a Security+ exam voucher, study guide, and practice questions.
- Confidently explain and define security vulnerabilities.
- Navigate the complexities of secure systems and network design
- Explore defensive measures like PKI, firewalls, and IDS.
- Implement robust identity management and access control.
- Gain access to an exclusive LinkedIn group for community support.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

Pre-requisites

- Before taking this course, you should know about networking and have a background in information assurance.

Curriculum

Module 1: Introduction to the CompTIA Security+ Exam

- In this module, you will learn about:
- The five domains of knowledge
- Expected level of expertise
- Assessing initial readiness

Module 2: Threats, Attacks, and Vulnerabilities

- In this module, you will:
- Compare and contrast types of attacks
- Explore threat actor types and vectors
- Explain penetration testing and vulnerability scanning concepts
- Identify key attack indicators

Module 3: Architecture and Design

- In this module, you will learn how to:
- Deploy secure application designs across an enterprise
- Develop and deploy secure applications with trusted frameworks
- Defend embedded systems, cloud assets, and virtualized servers
- Analyze confidentiality and nonrepudiation cryptography requirements

Module 4: Implementation

- In this module, you will learn how to:
- Install and configure network protocols

- Identify effective host and application security solutions
- Implement authentication and authorization solutions with PKI
- Secure wireless and mobile communications against breaches

Module 5: Operations and Incident Response

- In this module, you will learn how to:
- Respond to alerts and alarms to identify and mitigate threats
- Design and enact effective policies, processes, and procedures
- Utilize tools and data sources to support incident investigations
- Identify key elements of an incident to conduct a forensic investigation

Module 6: Governance, Risk, and Compliance

- In this module, you will learn how to:
- Explain the importance of policies, plans, and procedures
- Summarize regulations, standards, and frameworks to enhance security
- Explore risk management for a more robust security posture
- Carry out best practices for data security and privacy compliance

Module 7: Preparing for the Examination

- In this module, you will learn how to:
- Get ready for the exam
- Handle difficult questions
- Utilize additional study guides
- Go over a final review and assessment
- Take a complete practice exam