Training: CompTIA

CompTIA Security+ Prep Course

FORM OF TRAINING	MATERIALS	PRICE	DURATION
Traditional	Digital materials	1200 EUR	5 days
Traditional	CTAB Tablet	1300 EUR	5 days
Distance learning	Digital materials	1200 EUR	5 days
Distance learning	CTAB Tablet	1200 EUR	5 days

LOCATIONS

Krakow - 5 Tatarska Street, II floor, hours: 9:00 am - 4:00 pm
Warsaw - 17 Bielska Street, hours: 9:00 am - 4:00 pm

TRANING TERMS

2019-09-09 | 5 days | Warszawa
2019-10-14 | 5 days | Kraków
2019-11-25 | 5 days | Warszawa

TRAINING GOALS:

The **CompTIA Security+ certification** is an internationally recognized validation of foundation-level security skills and knowledge, and is used by organizations and security professionals around the globe.

CompTIA Security+ Prep Course prepares you for the Security+ certification exam based on the 2014 objectives (Exam SY0-501, which is included in the approved list of certifications to meet DoD Directive 8570.1 requirements.

In this course with a particular focus on CompTIA Security+ certification exam preparation, you'll gain 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.

*Each participant in an authorized training **CompTIA Security+ Prep Course** held in Compendium EC will receive a free SY0-501 CompTIA Security+ Certification Exam voucher.*

CONSPECT:

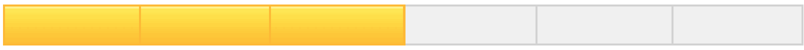
- Network Security
  - Implement security configuration parameters on network devices and other technologies
  - Given a scenario, use secure network administration principles
  - Explain network design elements and components
  - Given a scenario, implement common protocols and services
  - Given a scenario, troubleshoot security issues related to wireless networking
- Compliance and Operational Security
  - Explain the importance of risk related concepts
  - Summarize the security implications of integrating systems and data with third parties
  - Given a scenario, implement appropriate risk mitigation strategies
  - Given a scenario, implement basic forensic procedures
  - Summarize common incident response procedures
  - Explain the importance of security related awareness and training
  - Compare and contrast physical security and environmental controls
  - Summarize risk management best practices
  - Given a scenario, select the appropriate control to meet the goals of security
- Threats and Vulnerabilities
  - Explain types of malware
  - Summarize various types of attacks
  - Summarize social engineering attacks and the associated effectiveness with each attack
  - Explain types of wireless attacks
  - Explain types of application attacks
  - Analyze a scenario and select the appropriate type of mitigation and deterrent techniques
  - Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities
  - Explain the proper use of penetration testing versus vulnerability scanning
- Application, Data and Host Security
  - Explain the importance of application security controls and techniques
  - Summarize mobile security concepts and technologies
  - Given a scenario, select the appropriate solution to establish host security
  - Implement the appropriate controls to ensure data security
  - Compare and contrast alternative methods to mitigate security risks in static environments
- Access Control and Identity Management

    - Compare and contrast the function and purpose of authentication services
    - Given a scenario, select the appropriate authentication, authorization or access control
    - Install and configure security controls when performing account management, based on best practices
- Cryptography
    - Given a scenario, utilize general cryptography concepts
    - Given a scenario, use appropriate cryptographic methods
    - Given a scenario, use appropriate PKI, certificate management and associated components

REQUIREMENTS:

- A minimum of 2 years experience in IT administration with a focus on security
- Day to day technical information security experience
- Broad knowledge of security concerns and implementation including the topics in the domain list above

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the **CompTIA Security+ certification exam**, which is available through the **Pearson VUE test centers**.

Each participant in an authorized training CompTIA Security+ Prep Course held in Compendium EC will receive a free SY0-501 CompTIA Security+ Certification Exam voucher.

TRAINER:

Authorized CompTIA Trainer.