CO1 COMPENDIUM CENTRUM EDUKACYJNE

Training: CompTIA
CompTIA Security+ Prep Course

CompTIA. Authorized Partner | DELIVERY PARTNER

TRANING TERMS

2026-02-23 | 5 days | Kraków / Virtual Classroom
2026-03-16 | 5 days | Warszawa / Virtual Classroom
2026-03-23 | 5 days | Kraków / Virtual Classroom
2026-05-18 | 5 days | Warszawa / Virtual Classroom
2026-05-25 | 5 days | Kraków / Virtual Classroom
2026-06-22 | 5 days | Warszawa / Virtual Classroom

TRAINING GOALS:

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

The new CompTIA Security+ (SY0-701) represents the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk – and more. Once certified, you'll understand the core skills needed to succeed on the job – and employers will notice too. The Security+ exam verifies you have the knowledge and skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

CompTIA Security+ is compliant with ISO 17024 standards and approved by the U.S. DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

Each participant in an authorized training CompTIA Security+ Prep Course held in Compendium CE will receive a free SY0-701 CompTIA Security+ Certification Exam vouchers.

Jobs You Can Land With CompTIA Security+

- Cloud Penetration Tester
- Network Security Operations

CO1

- Penetration Tester
- Network Security Analyst
- Web App Penetration Tester
- Security Architect
- Cybersecurity Engineer

CONSPECT:

- General Security Concepts
    - Compare and contrast various types of security controls.
    - Summarize fundamental security concepts.
    - Explain the importance of change management processes and the impact to security.
    - Explain the importance of using appropriate cryptographic solutions.
- Threats, Vulnerabilities, and Mitigations
    - Compare and contrast common threat actors and motivations.
    - Explain common threat vectors and attack surfaces.
    - Explain various types of vulnerabilities.
    - Given a scenario, analyze indicators of malicious activity.
    - Explain the purpose of mitigation techniques used to secure the enterprise.
- Security Architecture
    - Compare and contrast security implications of different architecture models.
    - Given a scenario, apply security principles to secure enterprise infrastructure.
    - Compare and contrast concepts and strategies to protect data.
    - Explain the importance of resilience and recovery in security architecture.
- Security Operations
    - Given a scenario, apply common security techniques to computing resources.
    - Explain the security implications of proper hardware, software, and data asset management.
    - Explain various activities associated with vulnerability management.
    - Explain security alerting and monitoring concepts and tools.
    - Given a scenario, modify enterprise capabilities to enhance security.
    - Given a scenario, implement and maintain identity and access management.
    - Explain the importance of automation and orchestration related to secure operations.
    - Explain appropriate incident response activities.
    - Given a scenario, use data sources to support an investigation.
- Security Program Management and Oversight
    - Summarize elements of effective security governance.

- Explain elements of the risk management process.
- Explain the processes associated with third-party risk assessment and management.
- Summarize elements of effective security compliance.
- Explain types and purposes of audits and assessments.
- Given a scenario, implement security awareness practices.

REQUIREMENTS:

Network+ or equivalent knowledge. A minimum of 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts

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 CE will receive a free SY0-701 CompTIA Security+ Certification Exam vouchers.

TRAINER:

Authorized CompTIA Trainer.