What is Security+?

CompTIA **Security+** is a globally trusted, vendor-neutral certification that demonstrates competency in network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control, identity management, and cryptography.

Security+ Certification right for me?

The **Security+** certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career.

What is the format of the Security+ exam?

The current **Security+** SYO-401 exam is a mix of 90 multiple choice and performance-based questions. You have 90 minutes to complete this exam, with a passing score of 750 (on a scale of 100-900).

What is the average salary for someone with Security+ ?

Certified IT professionals will remain in high demand from private sector & U.S. government cybersecurity teams. According to the Bureau of Labor Statistics, Security Specialists, Administrators and Managers earn over $86,000 per year.

Is Security+ a recognized certification?

CompTIA **Security+** is a globally recognized credential that meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

How long is my Security+ vaild for?

Your CompTIA **Security+** certification is good for three years from the day of your exam. The CompTIA CE program allows you to extend your certification in three-year intervals through activities and training that relate to the content of your certification.

Security+ Course Outline & Objectives

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.

Testing

- Once the training is complete and the student feels confident in passing the exam. A student may test at Pueblo Community College in the Testing Center. There is a fee for the testing voucher.