CompTIA Security+
SY0-501
Course Syllabus
26 Hours

Course Description
CompTIA Security+ is an industry certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management. CompTIA Security+ certification covers network security, compliance and operation security, threats and vulnerabilities as well as application, data and host security. Also included are access control, identity management, and cryptography. This course covers the objectives for the certification exam:

- **CompTIA Security+ SY0-501**

Learning Objectives
Upon completion of the course, students will understand:

- Control fundamentals and the CIA triad, along with the types of malware that can affect computer systems and the mechanisms and applications that can be used to combat this malware
- Common network protocols, the fundamentals and dangers of network attacks, implementation of network security, and available tools and devices used to secure networks
- Router and switch configurations, firewall types and configurations, how IDS and IPS are used to secure a network environment; security mechanisms such as proxy servers, all-in-one security devices, flood guards, and unified security management; layered security, Defense in depth, subnetting, DMZ, and NAT
- Penetration testing methods and technologies; vulnerability assessment technologies and tools; account management, risk reduction, and LDAP; best practices, mitigation techniques, and strategies to reduce overall risk
- Various environmental, data, and physical controls used to secure an environment; various methods used to harden operating systems
- Remote authentication services and mobile security implementation; how to secure a wireless network and how to prevent wireless security attacks
- How cryptography is used to secure information, the algorithms that are employed, and how public key infrastructures and digital signatures are used to secure information
- Communication standards and protocols that are used in the web server environment, along with ways to harden web servers and web browsers; different types of attacks web-based applications can face, as well as cloud computing options, and network virtualization
- Business continuity strategies and methods, along with risk assessment methodologies and management techniques, and disaster recovery preparedness; ways to create security training for users and computer forensic methodologies

Course Format
CompTIA Security+ is a self-paced, online course delivered through the learning management system Skillsoft. The site to access the coursework is su.skillport.com. Login credentials will be provided to you on the cohort launch date. If you do not receive them by the launch date, please check your Spam/Junk folder of your email and/or contact your advisor or O2O program coordinator. Once you have logged into your account, you can locate the coursework by selecting “View My Learning Plan.”

Coursework is delivered through videos, tutorials, and tests. No textbooks are required for the course; however, students are encouraged to utilize additional resources to assist with certification preparation. Resource Guides with

lists of supplemental study materials for each certification are available at http://libguide.get-vet.syr.edu/curriculum/.

Course Completion Requirements

CompTIA Security+ coursework is due within 90 days from the assignment date. The course hours listed at the top of the syllabus reflect the time it would take to click through the slides and do not account for taking notes or the end of module tests. You must complete all ten modules listed within Topic 1. Successful completion of a module is marked after you review the lesson videos and score 80% or higher on the end of module tests.

At the beginning of a module, you will be asked to take a pre-test. Scoring 80% or higher on the pre-test signifies competence in the information that will be covered; you will therefore be waived from completing the module. A non-credit certificate of completion will be awarded for successful completion of the coursework.

Industry Certification Requirements

In order for the program to fund your CompTIA Security+ certification exam you will need to meet the Security+ practice exam requirements. Your advisor or O2O program coordinator will provide you with access to the practice exam as well as completion instructions once you have finished the coursework.

Support

- For technical support, please contact Skillsoft Support at support.skillsoft.com
- For course content support, please utilize Skillsoft's "Ask My Mentor" tool, located in the left-hand Menu within the module course player
- For program support or questions, please contact your advisor or O2O program coordinator

Course Outline

Topic 1: Security Fundamentals

1.1 CompTIA Security+ SY0-501: The Present Threat Landscape

1.2 CompTIA Security+ SY0-501: Types of Malware

1.3 CompTIA Security+ SY0-501: Social Engineering and Related Attacks

1.4 CompTIA Security+ SY0-501: Application and Service Attacks

1.5 CompTIA Security+ SY0-501: Cryptographic and Wireless Attacks

1.6 CompTIA Security+ SY0-501: Penetration Testing and Vulnerability Scanning

1.7 CompTIA Security+ SY0-501: Impacts from Vulnerability Types

1.8 CompTIA Security+ SY0-501: Components Supporting Organizational Security

1.9 CompTIA Security+ SY0-501: Security Assessment Using Software Tools

1.10 CompTIA Security+ SY0-501: Cryptography

1.11 CompTIA Security+ SY0-501: Public Key Infrastructure

1.12 CompTIA Security+ SY0-501: Wireless Security Settings

1.13 CompTIA Security+ SY0-501: Analyzing Output from Security Technologies

1.14 CompTIA Security+ SY0-501: Deploying Mobile Devices Securely

1.15 CompTIA Security+ SY0-501: Implementing Secure Protocols

1.16 CompTIA Security+ SY0-501: Troubleshooting Common Security Issues

1.17 CompTIA Security+ SY0-501: Identity Concepts and Access Services

1.18 CompTIA Security+ SY0-501: Identity and Access Management Controls

1.19 CompTIA Security+ SY0-501: Common Account Management Practices

1.20 CompTIA Security+ SY0-501: Frameworks, Guidelines, and Physical Security

1.21 CompTIA Security+ SY0-501: Implement Secure Network Architecture Concepts

1.22 CompTIA Security+ SY0-501: Secure System and Application Design and Deployment

1.23 CompTIA Security+ SY0-501: Cloud, Virtualization, and Resiliency Concepts

1.24 CompTIA Security+ SY0-501: Policies, Plans, and Procedures

1.25 CompTIA Security+ SY0-501: Business Impact Analysis and Risk Management

1.26 CompTIA Security+ SY0-501: Incident Response, Forensics, and Disaster Recovery