
COMPTIA SECURITY PLUS (SYO-501)

Who Should Attend

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

This course is targeted toward an Information Technology (IT) professional who has networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as OS X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Why is it different?

- No other certification that assesses baseline cybersecurity skills has performance-based questions on the exam. Security+ emphasizes hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of issues.
- More choose Security+ for DoD 8570 compliance than any other certification.
- Security+ focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection.
- The new Security+ certification covers the Junior IT Auditor/Penetration Tester job role, in addition to the previous job roles for Systems Administrator, Network Administrator, and Security Administrator.

Course Objectives

Upon successful completion of this course, students will be able to:

- Identify the fundamental concepts of computer security.
- Identify security threats and vulnerabilities.
- Examine network security.
- Manage application, data and host security.
- Identify access control and account management security measures.
- Manage certificates.
- Identify compliance and operational security measures.

- Manage risk.
- Manage security incidents.
- Develop business continuity and disaster recovery plans.

Course Outline

1 - Security Fundamentals

- Information Security Cycle
- Information Security Controls
- Authentication Methods
- Cryptography Fundamentals
- Security Policy Fundamentals

2 - Identifying Security Threats and Vulnerabilities

- Social Engineering
- Malware
- Physical Threats and Vulnerabilities
- Software-Based Threats
- Network-Based Threats
- Wireless Threats and Vulnerabilities
- Physical Threats and Vulnerabilities

3 - Managing Data, Application, and Host Security

- Manage Data Security
- Manage Application Security
- Manage Device and Host Security
- Manage Mobile Security

4 - Implementing Network Security

- Configure Security Parameters on Network Devices and Technologies
- Network Design Elements and Components
- Implement Networking Protocols and Services
- Apply Secure Network Administration Principles
- Secure Wireless Traffic

5 - Implementing Access Control, Authentication, and Account Management

- Access Control and Authentication Services

- Implement Account Management Security Controls

6 - Managing Certificates

- Install a Certificate Authority (CA) Hierarchy
- Enroll Certificates
- Secure Network Traffic by Using Certificates
- Renew Certificates
- Revoke Certificates
- Back Up and Restore Certificates and Private Keys
- Restore Certificates and Private Keys

7 - Implementing Compliance and Operational Security

- Physical Security
- Legal Compliance
- Security Awareness and Training
- Integrate Systems and Data with Third Parties

8 - Risk Management

- Risk Analysis
- Implement Vulnerability Assessment Tools and Techniques
- Scan for Vulnerabilities
- Mitigation and Deterrent Techniques

9 - Troubleshooting and Managing Security Incidents

- Respond to Security Incidents
- Recover from a Security Incident

10 - Business Continuity and Disaster Recovery Planning

- Business Continuity
- Plan for Disaster Recovery
- Execute Disaster Recovery Plans and Procedures