

CompTIA Security+ (SYO-501)

Length: 5 Days

Summary: The CompTIA Security+ course is designed to help you prepare for the SYO-501 exam. Students will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

Who Should Attend: 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.

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 CONTENT

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

- 5: 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
- 6: Implementing Access Control, Authentication, and Account Management**
 - Access Control and Authentication Services
 - Implement Account Management Security Controls
- 7: 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
- 8: Implementing Compliance and Operational Security**
 - Physical Security
 - Legal Compliance
 - Security Awareness and Training
 - Integrate Systems and Data with Third Parties
- 9: Risk Management**
 - Risk Analysis
 - Implement Vulnerability Assessment Tools and Techniques
 - Scan for Vulnerabilities
 - Mitigation and Deterrent Techniques
- 10: Troubleshooting and Managing Security Incidents**
 - Respond to Security Incidents
 - Recover from a Security Incident
- 11: Business Continuity and Disaster Recovery Planning**
 - Business Continuity
 - Plan for Disaster Recovery
 - Execute Disaster Recovery Plans and Procedures