CompTIA Security+

Duration: 5 Day(s)

Course Overview:

CompTIA Security+ is a global certification that validates the baseline skills you need to perform core security functions and pursue an IT security career. 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 solve a wider variety of issues. 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 troubleshooting 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 also designed to help prepare for the SY0-501 exam.

Who Should Attend?

- Systems Administrators
- Network Administrators
- Security Administrators
- Junior IT Auditors/Penetration Testers
- Security Specialists
- Security Consultants
- Security Engineers

Course Objectives:

- 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 risks
- 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

4 - Implementing Network Security

- Configure Security Parameters on Network Devices and Technologies
- Network Design Elements and Components
- Implementing 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
- Enrol 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