Hewlett Packard Enterprise

Course Datasheet

CompTIA Security+ Certification — Video Instructor Self-Paced e-Learning

Education Services course product number – IT Security Library
Course length – 17 hours
Delivery mode – VISPEL

This course will prepare students to pass the current CompTIA Security+ SY0-401 certification exam.
After taking this course, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

Prerequisites

- It is recommended that CompTIA Security+ candidates have at least two years of technical networking experience, with an emphasis on security.
- The CompTIA Network+ certification is also recommended.

Benefits to you

- Students will have access to comprehensive training content delivered by an instructor in a video classroom environment, hands-on Lab Simulations, Printable courseware and 24x7 Learning Zone Live Mentor Support.

Detailed course outline

- Security Fundamentals
  - The Information Security Cycle
  - Information Security Controls
  - Authentication Methods
  - Cryptography Fundamentals
  - Security Policy Fundamentals
- Identifying Security Threats and Vulnerabilities
  - Social Engineering
  - Malware
  - Software-Based Threats

c04681306, Created May 2015; Updated January 2016, Rev. 1
IT Security Library A.00

  - Network-Based Threats
  - Wireless Threats and Vulnerabilities
  - Physical Threats and Vulnerabilities

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

- 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

- Implementing Access Control, Authentication, and Account Management
  - Access Control and Authentication Services
  - Implement Account Management Security Controls

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

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

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

- Troubleshooting and Managing Security Incidents
  - Respond to Security Incidents
  - Recover from a Security Incident

- Business Continuity and Disaster Recovery Planning
  - Business Continuity
  - Plan for Disaster Recovery
  - Execute DRPs and Procedures

c04681306, Created May 2015; Updated January 2016, Rev. 1
IT Security Library A.00