Current Technologies
Computer Learning Centers

CompTIA

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Security+

This course provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format; this includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security.

How you'll benefit

This class will help you:

- **More choose Security+** - chosen by more corporations and defense organizations than any other certification on the market to validate baseline security skills and for fulfilling the DoD 8570 compliance.
- **Security+ proves hands-on skills** – the only baseline cybersecurity certification emphasizing hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of today's complex issues.
- **More job roles turn to Security+ to supplement skills** – baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software and hardware.
- **Security+ is aligned to the latest trends and techniques** – covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Current Technologies Computer Learning Centers

CompTIA

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Security+

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Compare Security Roles and Security Controls
- Explain Threat Actors and Threat Intelligence
- Perform Security Assessments
- Identify Social Engineering and Malware
- Summarize Basic Cryptographic Concepts
- Implement Public Key Infrastructure
- Implement Authentication Controls
- Implement Identity and Account Management Controls
- Implement Secure Network Designs
- Implement Network Security Appliances
- Implement Secure Network Protocols
- Implement Host Security Solutions
- Implement Secure Mobile Solutions
- Summarize Secure Application Concepts
- Implement Secure Cloud Solutions
- Explain Data Privacy and Protection Concepts
- Perform Incident Response
- Explain Digital Forensics
- Summarize Risk Management Concepts
- Implement Cybersecurity Resilience
- Explain Physical Security

Course Duration

5 day

Course Price

$2,895.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

SY0-601

Who Should Attend

The job roles best suited to the material in this course are:

- IT professionals preparing for the Security+ Exam SY0-601
- Network Administrators
- Cybersecurity Associates
- IT personnel interested in pursuing a career in cybersecurity

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Security+

Perquisites

To fully benefit from this course, you should have the following knowledge:

- This course assumes that you have basic knowledge of using and configuring individual workstations and simple networks.
- CompTIA A+ certified (or have equivalent experience) and CompTIA Network+ certified (or have equivalent experience) with 2-3 years networking experience.

Outline

Module 0: Introduction

- Course setup

Module 1: Security fundamentals

- Security concepts
- Enterprise security strategy
- Security program components

Module 2: Risk management

- Understanding threats
- Risk management programs
- Security assessments

Module 3: Cryptography

- Cryptography concepts
- Public key infrastructure

Module 4: Network connectivity

- Network attacks
- Packet flow

Module 5: Network security technologies

- Network security components
- Monitoring tools

CompTIA Security+

Module 6: Secure network configuration

- Secure network protocols
- Hardening networks

Module 7: Authentication

- Authentication factors
- Authentication protocols

Module 8: Access control

- Access control principles
- Account management

Module 9: Securing hosts and data

- Malware
- Securing data
- Securing hosts

Module 10: Securing specialized systems

- Mobile security
- Embedded and specialized systems

Module 11: Application security

- Application attacks
- Securing applications

Module 12: Cloud security

- Virtual and cloud systems
- Securing cloud services

Module 13: Organizational security

- Social engineering

- Security policies
- User roles and training
- Physical security and safety

Module 14: Disaster planning and recovery

- Business continuity
- Resilient systems
- Incident response procedures