



Complete Computing, Inc.

SERVING OUR CUSTOMERS SINCE 1982

CompTIA® Security+® (Exam SY0-501)

Course length: 5 day(s)

Course Overview:

The Official CompTIA® Security+® (Exam SY0-501) course is the primary curriculum you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-501) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of computer security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your computer security skill set so that you can confidently perform your duties in any security-related role.

Target Student:

This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix, or Linux; and who wants to further a career in IT by acquiring foundational knowledge of security topics; preparing for the CompTIA Security+ certification examination; or using Security+ as the foundation for advanced security certifications or career roles.

Prerequisites:

To ensure your success in this course, you should possess:

- Basic Windows user skills and a fundamental understanding of computer and networking concepts.
- CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Course Objectives:

In this course, you will implement information security across a variety of different contexts. You will:

- Identify the fundamental components of information security.
- Analyze risk.
- Identify various threats to information security.
- Conduct security assessments to detect vulnerabilities.
- Implement security for hosts and software.
- Implement security for networks.
- Manage identity and access.
- Implement cryptographic solutions in the organization.
- Implement security at the operational level.
- Address security incidents.
- Ensure the continuity of business operations in the event of an incident.

400 WEST 7TH STREET (7TH & SPRING) LITTLE ROCK AR 72201-4288
PHONE: 501.372.3379 OR 800.880.2949 EMAIL: training@complete.com



Complete Computing, Inc.

SERVING OUR CUSTOMERS SINCE 1982

Course Content

Lesson 1: Identifying Security Fundamentals

Topic A: Identify Information Security Concepts

Topic B: Identify Basic Security Controls

Topic C: Identify Basic Authentication and Authorization Concepts

Topic D: Identify Basic Cryptography Concepts

Lesson 2: Analyzing Risk

Topic A: Analyze Organizational Risk

Topic B: Analyze the Business Impact of Risk

Lesson 3: Identifying Security Threats

Topic A: Identify Types of Attackers

Topic B: Identify Social Engineering Attacks

Topic C: Identify Malware

Topic D: Identify Software-Based Threats

Topic E: Identify Network-Based Threats

Topic F: Identify Wireless Threats

Topic G: Identify Physical Threats

Lesson 4: Conducting Security Assessments

Topic A: Identify Vulnerabilities

Topic B: Assess Vulnerabilities

Topic C: Implement Penetration Testing

Lesson 5: Implementing Host and Software Security

Topic A: Implement Host Security

Topic B: Implement Cloud and Virtualization Security

Topic C: Implement Mobile Device Security

Topic D: Incorporate Security in the Software Development Lifecycle

Lesson 6: Implementing Network Security

Topic A: Configure Network Security Technologies

Topic B: Secure Network Design Elements

Topic C: Implement Secure Networking Protocols and Services

Topic D: Secure Wireless Traffic



Complete Computing, Inc.

SERVING OUR CUSTOMERS SINCE 1982

Lesson 7: Managing Identity and Access

Topic A: Implement Identity and Access Management

Topic B: Configure Directory Services

Topic C: Configure Access Services

Topic D: Manage Accounts

Lesson 8: Implementing Cryptography

Topic A: Identify Advanced Cryptography Concepts

Topic B: Select Cryptographic Algorithms

Topic C: Configure a Public Key Infrastructure

Topic D: Enroll Certificates

Topic E: Back Up and Restore Certificates and Private Keys

Topic F: Revoke Certificates

Lesson 9: Implementing Operational Security

Topic A: Evaluate Security Frameworks and Guidelines

Topic B: Incorporate Documentation in Operational Security

Topic C: Implement Security Strategies

Topic D: Manage Data Security Processes

Topic E: Implement Physical Controls

Lesson 10: Addressing Security Incidents

Topic A: Troubleshoot Common Security Issues

Topic B: Respond to Security Incidents

Topic C: Investigate Security Incidents

Lesson 11: Ensuring Business Continuity

Topic A: Select Business Continuity and Disaster Recovery Processes

Topic B: Develop a Business Continuity Plan

Appendix A: Taking the Exams

Appendix B: Mapping Course Content to CompTIA® Security+® Exam SY0-501

Appendix C: Linux Essentials

Appendix D: Log File Essentials

Appendix E: Programming Essentials