

SECURITY+

DURATION: 5 DAYS

COURSE OVERVIEW

The *Security+ Certification Prep 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. This course maps to the CompTIA Security+ certification exam (SY0-501). Objective coverage is marked throughout the course.

Our Security+ courseware has received the CompTIA Approved Quality Content (CAQC) validation, assuring that all test objectives are covered in the training material.

What is Security+ Certification?

The Security+ certification is considered to be the minimum level of certification for all IT security positions beyond entry-level. This course delivers the core knowledge required to pass the exam and the skills necessary to advance to an intermediate-level security job.

Students will benefit most from this course if they intend to take the CompTIA Security+ SY0-501 exam. Read our white paper titled "New Topics on the New Security+ SY0-501 Exam."

This course supports a certification that is a DoD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

TARGET AUDIENCE

1. Network Administrators
2. Cybersecurity Associates
3. IT personnel interested in pursuing a career in cybersecurity

COURSE OBJECTIVES

In the Security+ Certification Prep Course, you will learn to:

1. Proactively implement sound security protocols to mitigate security risks
2. Quickly respond to security issues
3. Retroactively identify where security breaches may have occurred
4. Design a network, on-site or in the cloud, with security in mind

COURSE CONTENT

Chapter 1: Security Fundamentals

Module A: Security concepts

Module B: Risk management

Module C: Vulnerability assessment

Chapter 2: Understanding attacks

Module A: Understanding attackers

Module B: Social engineering

Module C: Malware

Module D: Network attacks

Module E: Application attacks

Chapter 3: Cryptography

Module A: Cryptography concepts

Module B: Public key infrastructure

Chapter 4: Network fundamentals

Module A: Network components

Module B: Network addressing

Module C: Network ports and applications

Chapter 5: Securing networks

Module A: Network security components

Module B: Transport encryption

Module C: Hardening networks

Module D: Monitoring and detection

Chapter 6: Securing hosts and data

Module A: Securing hosts

Module B: Securing data

Module C: Mobile device security

Chapter 7: Securing network services

Module A: Securing applications

Module B: Virtual and cloud systems

Chapter 8: Authentication

Module A: Authentication factors

Module B: Authentication protocols

Chapter 9: Access control

Module A: Access control principles

Module B: Account management

Chapter 10: Organizational security

Module A: Security policies

Module B: User training

Module C: Physical security and safety

Chapter 11: Disaster planning and recovery

Module A: Business continuity

Module B: Fault tolerance and recovery

Module C: Incident response

Glossary

LABS

Chapter 2: Understanding Attacks

Examining Phishing Attacks

Examining Malware

Probing a Site

Simulating a DOS Attack

Cracking Passwords

Simulating an Eavesdropping Attack

Exploring Application Vulnerabilities

Examining SQL Injection Attacks

Examining Client-side Attacks

Chapter 3: Cryptography

Symmetric Encryption

Asymmetric Encryption

Creating File Hashes

Installing a Certificate Authority

Chapter 4: Network Fundamentals

Using TCP/IP Tools

Chapter 5: Securing the Network

Configuring a Firewall

Examining Website Certificates

Securing a WAP

Viewing Event Logs

Scanning the Network

Chapter 6: Securing Hosts and Data

Enabling BitLocker

Chapter 7: Securing Network Services

Finding Vulnerable Code

Chapter 8: Authentication

Installing a RADIUS Server

Examining Active Directory

Chapter 9: Access Control

Managing NTFS Permissions

Managing Active Directory Objects

Using Group Policy Objects

Creating a Security Template

Chapter 11: Disaster planning and recovery

Using Windows Server Backup

COURSE PREREQUISITES

This course assumes basic knowledge of using and maintaining individual workstations.

Attendees should be CompTIA A+ certified (or have equivalent experience) and CompTIA Network+ certified (or have equivalent experience) with 2-3 years networking experience.

CompTIA A+ Certification Prep

TEST CERTIFICATION

This course prepares you for the Security+ certification exam based on the 2017 objectives (exam SY0-501).

The SY0-501 exam is included in the approved list of certifications that meet DoD Directive 8570.1 requirements.

Our Security+ courseware has received the CompTIA Approved Quality Content (CAQC) validation, assuring that all test objectives are covered in the training material.

CompTIA Security+ Certification

FOLLOW ON COURSES

CySA+ - Cyber security Analyst+ Prep Course

CND - Certified Network Defender

Cybersecurity Specialization: Architecture and Policy

Cybersecurity Specialization: Governance, Risk, and Compliance