

COMPTIA SECURITY+ CERTIFICATION PREP COURSE

Course Code: 3404

Prepare for the CompTIA Security+ SY0-701 certification while building your cybersecurity knowledge, skills, and abilities

Our 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 (SY0-701). Objective coverage is marked throughout the course. Exam voucher included.

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.

This course includes an exam voucher.

What You'll Learn

- Knowledge and skills to understand to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
- Monitor and secure hybrid environments, including cloud, mobile, and IoT
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents, and prepare candidates to take the CompTIA Security+ certification exam.

Who Needs to Attend

- Network Administrators
- Cybersecurity Associates
- IT personnel interested in pursuing a career in cybersecurity

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 SECURITY+ CERTIFICATION PREP COURSE

Course Code: 3404

CLASSROOM LIVE

\$2,970 USD

5 Day

Classroom Live Outline

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Classroom Live Labs

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security

- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling
- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds
- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering
- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

COMPTIA SECURITY+ CERTIFICATION PREP COURSE

Course Code: 3404

VIRTUAL CLASSROOM LIVE

\$2,970 USD

5 Day

Virtual Classroom Live Outline

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Virtual Classroom Live Labs

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security

- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling
- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds
- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering
- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

Sep 22 - 26, 2025 | 11:30 AM - 7:30 PM EDT

Sep 29 - Oct 3, 2025 | 8:30 AM - 4:30 PM EDT

Oct 20 - 24, 2025 | 8:30 AM - 4:30 PM EDT

Oct 27 - 31, 2025 | 11:30 AM - 7:30 PM EDT

Nov 3 - 7, 2025 | 11:30 AM - 7:30 PM EST

Nov 10 - 14, 2025 | 8:30 AM - 4:30 PM EST

Dec 1 - 5, 2025 | 11:30 AM - 7:30 PM EST

Dec 8 - 12, 2025 | 8:30 AM - 4:30 PM EST

Jan 12 - 16, 2026 | 8:30 AM - 4:30 PM EST

Jan 26 - 30, 2026 | 11:30 AM - 7:30 PM EST

Feb 9 - 13, 2026 | 11:30 AM - 7:30 PM EST

Feb 23 - 27, 2026 | 8:30 AM - 4:30 PM EST

Mar 2 - 6, 2026 | 11:30 AM - 7:30 PM EST

Mar 9 - 13, 2026 | 8:30 AM - 4:30 PM EDT

Apr 6 - 10, 2026 | 8:30 AM - 4:30 PM EDT

Apr 13 - 17, 2026 | 11:30 AM - 7:30 PM EDT



COMPTIA SECURITY+ CERTIFICATION PREP COURSE

Course Code: 3404

PRIVATE GROUP TRAINING

5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 8/30/2025 8:25:51 AM

Copyright © 2025 Global Knowledge Training LLC. All Rights Reserved.