THINQTANK® LEARNING

COMPTIA SECURITY+

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 95% success
- Course specific thinQtank® Learning publications to promote a fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by expert security professionals

Course Duration

- Five days of instructor-led training
- 70% lecture, 30% demonstration labs

Prerequisites

- CompTIA A+ and Network+ certifications, or equivalent knowledge
- Six to nine months experience in networking including configuring security parameters

Target Audience

- Information Technology (IT) professionals who have networking and administrative responsibilities
- Anyone who wants to further their career in IT by acquiring foundational knowledge of security topics

Exam Information

- SY0-701 – Security+ Exam

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Toolkit and Pen Test Kit

- Penetration testing kit
- Kali Linux Video Course
- Security+ Video Course
- Custom Linux build for penetration testing

Course Overview

thinQtank® Learning is offering an industry unique five-day training camp in which students can receive the CompTIA Security+ certification. As with all of our CompTIA Training Experiences, exams are delivered in the classroom.

CompTIA® Security+ is the primary training course you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. 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. Students will benefit most from this course if they intend to take the CompTIA Security + SY0-701 exam. The CompTIA Security+ certification is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

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

Course Objectives

- Security+ reading plan
- Security+ review guide
- Security+ certification practice exam

Primary course objectives:

- Identify the fundamental concepts of computer security
- Identify security threats and vulnerabilities
- Manage data, application, and host security
- Implement network security
- Identify and implement access control and account management security measures
- Manage certificates
- Identify and implement compliance and operational security measures
- Manage risk
- Troubleshoot and manage security incidents
- Plan for business continuity and disaster recovery

COMPTIA SECURITY+

Course Modules

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

2 Analyzing Risk
- Topic A: Analyze Organizational Risk
- Topic B: Analyze the Business Impact of Risk

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

4 Conducting Security Assessments
- Topic A: Identify Vulnerabilities
- Topic B: Assess Vulnerabilities
- Topic C: Implement Penetration Testing

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

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

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

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

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

10 Addressing Security Incidents
- Topic A: Troubleshoot Common Security Issues
- Topic B: Respond to Security Incidents
- Topic C: Investigate Security Incidents

11 Ensuring Business Continuity
- Topic A: Select Business Continuity and Disaster Recovery Processes
- Topic B: Develop a Business Continuity Plan

A
- 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

COMPTIA SECURITY+

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com