Security+ (SY0-701) Course Introduction

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

About the certification

- **The new CompTIA Security+ (SY0-701)** represents the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk – and more.

- Once certified, you'll understand the core skills needed to succeed on the job – and employers will notice too.

https://www.comptia.org/certifications/security

About the certification (cont.)

- **The Security+ exam** verifies you have the knowledge and skills required to:
  - ✓ Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
  - ✓ Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
  - ✓ 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.

https://www.comptia.org/certifications/security

Course Prerequisites

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

- CompTIA Network+ and two years of experience working in a security/ systems administrator job role

IT Jobs Related to CompTIA Security+

- Security & System Administrator
- Junior Security Engineer
- Cybersecurity Analyst
- Incident Response Analyst
- SOC Analyst
- Penetration Tester
- Network Security Analyst
- Web App Penetration Tester

Course Domains

Domain 1: General Security Concepts **(12%)**

Domain 2: Threats, Vulnerabilities, and Mitigations **(22%)**

Domain 3: Security Architecture **(18%)**

Domain 4: Security Operations **(28%)**

Domain 5: Security Program Management and Oversight **(20%)**

Official Topics

1. Summarize Fundamental Security Concepts
2. Compare Threat Types
3. Explain Cryptographic Solutions
4. Implement Identity and Access Management
5. Secure Enterprise Network Architecture
6. Secure Cloud Network Architecture
7. Explain Resiliency and Site Security Concepts
8. Explain Vulnerability Management

CompTIA CertMaster Learn for Security+ (SY0-701) Individual License

Official Topics (cont.)

9. Evaluate Network Security Capabilities
10. Assess Endpoint Security Capabilities
11. Enhance Application Security Capabilities
12. Explain Incident Response and Monitoring Concepts
13. Analyze Indicators of Malicious Activity
14. Summarize Security Governance Concepts
15. Explain Risk Management Processes
16. Summarize Data Protection and Compliance Concepts

CompTIA CertMaster Learn for Security+ (SY0-701) Individual License

Official Labs

1. Exploring the Lab Environment
2. Perform System Configuration Gap Analysis
3. Configuring Examples of Security Control Types
4. Finding Open Service Ports
5. Using SET to Perform Social Engineering
6. Using Storage Encryption
7. Using Hashing and Salting
8. Managing Password Security

CompTIA CertMaster Labs for Security+ (SY0-701) Individual License

Official Labs (cont.)

9. Managing Permissions
10. Setting up Remote Access
11. Using TLS Tunneling
12. Using Containers
13. Using Virtualization
14. Implement Backups
15. Performing Drive Sanitization
16. Exploiting and Detecting SQLi

CompTIA CertMaster Labs for Security+ (SY0-701) Individual License

Official Labs (cont.)

17. Working with Threat Feeds
18. Performing Vulnerability Scans
19. Understanding Security Baselines
20. Implementing a Firewall
21. Using Group Policy
22. Hardening
23. Performing DNS Filtering
24. Configuring System Monitoring

CompTIA CertMaster Labs for Security+ (SY0-701) Individual License

Official Labs (cont.)

25. Incident Response: Detection
26. Performing Digital Forensics
27. Performing Root Cause Analysis
28. Detecting and Responding to Malware
29. Understanding On-Path Attacks
30. Using a Playbook
31. Implementing Allow Lists and Deny Lists
32. Performing Reconnaissance

CompTIA CertMaster Labs for Security+ (SY0-701) Individual License

Official Labs (cont.)

33. Performing Penetration Testing
34. Training and Awareness through Simulation
35. Discovering Anomalous Behavior
36. Use Cases of Automation and Scripting
37. Using Network Sniffers

CompTIA CertMaster Labs for Security+ (SY0-701) Individual License

FAQs

- Should I have **Networks** knowledge before taking this course ?
  - Yes, as recommended experience you should have finished **Network+** or **equivalent knowledge**.

- Do I need a powerful computer to implement the course's Labs ?
  - **Yes**, only If you will build your own Virtual Lab.
  - For me as an Instructor I will show you how to implement labs using **CompTIA Labs** hosted in their cloud.

    CompTIA CertMaster Labs for Security+ (SY0-701)- (paid subscription)

"LABS ARE OPTIONAL, THERE IS NO LABS IN THE EXAM"

Resources for the online & recorded course

- We will provide you with the following course materials
  - ✓PDF slides for each topic.
  - ✓HD recorded videos in .mp4 format ready for online watching.
  - ✓Lifetime access to the course contents.

- Register here for the pre-recorded course - https://netriders.academy/courses/security-new/