



COURSE CURRICULUM · CYBERSECURITY · COMPTIA

SY0-701: CompTIA Security+

Build a solid, practical cybersecurity foundation and prepare for the CompTIA Security+ SY0-701 exam with hands-on labs.

DURATION

5 days · 40 hours

LEVEL

Intermediate

CURRICULUM

15 modules · 7 labs

DELIVERY

Live online, Classroom,
Onsite, Corporate

Course overview

Security+ is often the first certification employers look for in security and infrastructure roles, because it shows you understand how attacks work and how organisations defend against them. This five-day course builds that understanding through explanation, discussion and regular hands-on practice, so the concepts hold up in an interview or on the job, not just in the exam.

The course follows the five SY0-701 domains. Day one introduces general security concepts: security controls, the CIA triad, authentication and authorisation, change management and cryptography. Day two covers threats, vulnerabilities and mitigations, from threat actors and social engineering to malware, application and network attacks. Day three addresses security architecture: secure network design, cloud and virtualisation models, infrastructure hardening and data protection.

Day four is about security operations — hardening, vulnerability management, monitoring, identity and access management, automation and incident response — and day five covers security programme management and oversight, including governance, risk, third-party management, compliance and awareness, followed by a full exam-readiness session.

Labs use virtual machines and common tools to configure firewalls, analyse logs, inspect packets, apply encryption and respond to simulated incidents, which also prepares you for the performance-based questions. This course is aligned to the SY0-701 exam and prepares you for it. CompTIA has announced a successor version, so check the CompTIA website for the current exam before booking.

Highlights

- 40 hours of live, trainer-led sessions over five days
- Hands-on labs for every SY0-701 domain
- Performance-based question practice
- Security operations and incident response basics
- Weekday and weekend batches in IST and Gulf Time

What's included

- Coverage of all five SY0-701 domains
- Hands-on labs in a virtual lab environment
- Performance-based question walkthroughs
- Log analysis and packet inspection exercises
- Incident response tabletop exercise
- Full-length practice test with review
- Course completion certificate from Ace Skills Consulting
- Post-training doubt support while you prepare

Who this course is for

Who should attend

- System and network administrators
- IT support professionals moving into security
- Junior security analysts
- Developers who want security fundamentals
- Graduates starting a cybersecurity career

Prerequisites

- Basic networking knowledge (Network+ level recommended)
- Familiarity with Windows and Linux operating systems
- Some IT administration or support experience helps

Detailed curriculum — 5 days, 40 hours, 15 modules, 7 hands-on labs

Day 1 General Security Concepts

8 hours

1.1 Security fundamentals

- Confidentiality, integrity and availability
- Zero trust concepts
- Deception technologies
- Categories and types of security controls
- Physical security

1.2 Identity and change

- Authentication, authorisation and accounting
- Gap analysis
- Change management processes

1.3 Cryptography

- Symmetric and asymmetric encryption
- Public key infrastructure and certificates
- Hashing and digital signatures
- Blockchain and obfuscation concepts

LAB Create certificates and verify file integrity with hashes · 45 min

Day 2 Threats, Vulnerabilities & Mitigations

8 hours

2.1 Threat actors and vectors

- Threat actors and motivations
- Supply chain and message-based vectors
- Social engineering and phishing

LAB Analyse a phishing email and its headers · 30 min

2.2 Vulnerabilities and attacks

- Application vulnerabilities
- Network and password attacks
- Malware types and indicators
- Cloud, mobile and virtualisation vulnerabilities

LAB Identify indicators of malicious activity in logs · 45 min

2.3 Mitigation techniques

- Segmentation and access control
- Allow lists and isolation
- Patching and hardening

Day 3 Security Architecture

8 hours

3.1 Architecture models

- On-premises, cloud and hybrid considerations
- IoT, ICS and embedded systems
- Virtualisation and containers
- Infrastructure as code security

3.2 Securing enterprise infrastructure

- Firewalls, IDS and IPS
- Network access control
- VPNs and secure remote access
- Secure protocols

LAB Configure firewall rules and test them with a port scan · 50 min

3.3 Data protection and resilience

- Data classification and states
- Backups, high availability and site resilience
- Encryption and tokenisation

Day 4 Security Operations

8 hours

4.1 Hardening and vulnerability management

- Secure baselines
- Asset management
- Vulnerability scanning and CVSS
- Wireless and mobile security

LAB Run a vulnerability scan and prioritise the findings · 45 min

4.2 Monitoring and identity

- SIEM, log aggregation and alerting
- Multifactor authentication and SSO
- Identity and access management
- Privileged access management

LAB Investigate alerts in a SIEM · 40 min

4.3 Incident response

- Incident response process
- Automation and orchestration
- Digital forensics basics

LAB Incident response tabletop: ransomware scenario · 45 min

Day 5 Programme Management, Oversight & Exam Readiness

8 hours

5.1 Governance and risk

- Policies, standards and procedures
- Business impact analysis
- Risk identification, analysis and treatment
- Third-party risk management

5.2 Compliance and awareness

- Compliance monitoring and reporting
- Audits and assessments
- Privacy and data protection obligations
- Security awareness programmes

5.3 Exam readiness

- Performance-based question strategy
- Domain-by-domain review
- Full-length practice test

Skills and tools

Skills you will build

Security controls

Cryptography & PKI

Threat analysis

Vulnerability management

Network security

Identity and access management

SIEM monitoring

Incident response

Risk management

Security governance

Tools used in class

Wireshark

Nmap

OpenSSL

Kali Linux

Windows Defender Firewall

Wazuh

OpenVAS

Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	CompTIA Security+
Exam code	SY0-701
Questions	Maximum 90
Duration	90 minutes
Passing score	750 (on a scale of 100–900)
Format	Multiple choice, Multiple response, Performance-based / lab
Delivery	Online proctored, Test centre
Validity	3 years (renewable through CompTIA continuing education)
Official page	https://www.comptia.org/certifications/security

Exam skill areas covered

Security Architecture and Mitigations
Security Operations Management and Oversight

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Is a new version of Security+ coming?

Yes. CompTIA expects to launch SY0-801 around 17 November 2026, and the English SY0-701 exam is scheduled to retire on 11 June 2027. If you plan to test before then, SY0-701 remains a valid choice; we will update the course for SY0-801.

What are performance-based questions?

They are short simulations or drag-and-drop tasks that test practical skills. Our labs and walkthroughs are designed to prepare you for them.

Do I need Network+ first?

It is not required, but networking knowledge at that level makes the course much easier to follow.

How long is Security+ valid?

Three years, and you can renew it through CompTIA's continuing education programme.

Can you train our IT team?

Yes. Corporate batches can be scheduled privately and aligned with your security policies.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/sy0-701-comptia-security-plus · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur

New Delhi 110092

Office: 98180 12523

CompTIA, A+, Network+, Security+, CySA+, PenTest+, SecurityX, Cloud+ and Linux+ are trademarks of CompTIA, Inc. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.