



COMPTIA

Security+ SY0-701 — CompTIA

Security+

Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

BEGINNER

40 HOURS

5 DAYS

At a glance

COURSE	Security+ SY0-701 — CompTIA Security+
TRACK	CompTIA
DOMAIN	Cyber Security
LEVEL	Beginner
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a beginner course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Five domains, mapped one-for-one to the CompTIA Security+ SY0-701 exam objectives and taught in the same order, so nothing on the exam is left uncovered.

SY0-701 is the current version. It launched on 7 November 2023 and has not been superseded — CompTIA has it scheduled to retire in English on 11 June 2027, and in Japanese, Portuguese, Spanish and Thai on 13 August 2027. Anything you are taught here is examinable until those dates.

What SY0-701 changed was the centre of gravity. Security Operations is now the biggest domain by a distance, and Security Program Management and Oversight gives governance, risk and third-party management real weight for the first time. Each domain below carries its published weighting, and we give it classroom time in proportion.

Roughly half the classroom time is hands-on, because part of the exam is not multiple-choice. Performance-based questions put you in a simulated console and score what you do, so we practise in one. CompTIA does not publish how many of the questions are performance-based, so prepare for both throughout.

Domain 01 — General Security Concepts

The vocabulary and the mental model everything else in the exam is built on. 12% of the exam.

- Categories and types of security control: technical, managerial, operational and physical
- Control functions — preventive, deterrent, detective, corrective, compensating and directive — and matching one to a stated risk
- Confidentiality, integrity and availability, and the trade-offs between them
- Non-repudiation, and authentication, authorisation and accounting as three separate things
- Zero trust: control plane and data plane, policy engines, and the adaptive identity idea behind it
- Physical security controls, and deception and disruption technology such as honeypots and honeytokens
- Change management: approval, ownership, testing, backout planning, maintenance windows and version control
- Technical implications of change — allow lists, restricted activities, downtime, restarts and dependencies
- Public key infrastructure, key management and the difference between public and private key use
- Encryption at each level, obfuscation, steganography, tokenisation, hashing, salting, digital signatures and certificates

Domain 02 — Threats, Vulnerabilities, and Mitigations

Who attacks you, how they get in, what they exploit, and what you do about it. 22% of the exam.

- Threat actor types: nation-state, unskilled attacker, hacktivist, insider threat, organised crime and shadow IT
- Actor attributes and motivations, from financial gain and espionage to disruption, revenge and war
- Threat vectors: message-based, image and file-based, voice call, removable device, and vulnerable software
- Unsecure networks, open service ports, default credentials and supply chain vectors through vendors and MSPs
- Human vectors — phishing, vishing, smishing, pretexting, business email compromise, watering hole, typosquatting
- Vulnerability classes: application, operating system, web-based, hardware, virtualisation, cloud-specific and supply chain
- Mobile device vulnerabilities including sideloading and jailbreaking, and zero-day exposure

- Malicious activity: malware families, physical attacks, network attacks, application attacks and cryptographic attacks
- Password attacks, and indicators that a given attack type is under way
- Mitigation techniques: segmentation, access control, isolation, patching, encryption, monitoring, hardening and decommissioning

Domain 03 — Security Architecture

Designing an estate so that the controls are structural rather than bolted on afterwards. 18% of the exam.

- Architecture models compared: on-premises, cloud, hybrid, virtualisation, containerisation and serverless
- Infrastructure as code, microservices, IoT, ICS and SCADA, embedded systems and real-time operating systems
- Architecture considerations: availability, cost, responsiveness, scalability, patch availability and compute requirements
- Infrastructure design decisions — device placement, security zones, attack surface, failure modes and device attributes
- Secure communication and access: VPN, remote access, tunnelling, software-defined wide area networking and secure access service edge
- Selecting infrastructure controls: firewalls, IDS and IPS, web filtering, operating system security, and secure protocols
- Data types and classifications, and the regulated, intellectual property and financial categories that attract obligations
- Data states, sovereignty, geolocation, and the methods that secure each — encryption, hashing, masking, tokenisation, segmentation, permissions
- High availability, load balancing and clustering, site considerations, and platform diversity
- Backup strategy, replication, journalling, power resilience, and testing continuity plans rather than filing them

Domain 04 — Security Operations

The largest domain, and the one closest to the job most candidates will actually be doing. 28% of the exam.

- Secure baselines, and hardening targets across servers, workstations, switches, routers, mobile devices, IoT, ICS and embedded systems
- Mobile deployment models and device management, and wireless security: WPA3, AAA and RADIUS, authentication protocols and site surveys
- Application security, sandboxing and monitoring, including input validation, code signing and secure cookies
- Asset management across the lifecycle — acquisition, ownership, classification, tracking, sanitisation and disposal — and vulnerability management from discovery through remediation, validation and reporting
- Alerting and monitoring: log aggregation, SIEM, SNMP traps, NetFlow, alert tuning and quarantine
- Enterprise security capabilities: firewall rules and screened subnets, IDS and IPS tuning, web and DNS filtering, email security, DLP, NAC, EDR and XDR
- Identity and access management: provisioning and deprovisioning, federation, single sign-on, SAML, OAuth, LDAP, and multifactor factors and attributes
- Privileged access management, password policy, just-in-time permissions, and automation and orchestration with the single-point-of-failure risk it introduces
- Incident response end to end: preparation, detection, analysis, containment, eradication, recovery, lessons learned and root cause analysis

- Threat hunting, digital forensics, legal hold and chain of custody, and investigating with firewall, application, endpoint and network log data

Domain 05 — Security Program Management and Oversight

The management half of the exam: governance, risk, third parties, compliance and audit. 20% of the exam.

- Security governance: guidelines, policies, standards and procedures, and the acceptable use, incident response, continuity, change management and SDLC documents that carry them
- Governance structures — boards, committees, government entities — and centralised against decentralised decision-making
- Roles and responsibilities: owners, controllers, processors, custodians and stewards
- Risk identification and assessment, qualitative and quantitative analysis, the risk register, and appetite and tolerance
- The four treatment strategies — transfer, accept, avoid and mitigate — and choosing between them
- Risk reporting, business impact analysis, and the recovery time and recovery point objectives that come out of it
- Third-party risk: vendor assessment and selection, due diligence, audit and penetration testing rights, agreement types such as SLA, MOU, MSA and NDA, and ongoing monitoring
- Compliance reporting, attestation and the consequences of non-compliance, and privacy obligations by jurisdiction including data subject rights and retention
- Audits and assessments: internal and external audit, regulatory examination, and penetration testing types and reconnaissance
- Security awareness: phishing campaigns, recognising anomalous behaviour, user guidance, reporting culture, and measuring the programme

Who should take this

Help desk and IT support staff moving into security, junior SOC analysts, system and network administrators who have picked up security duties, and anyone who needs a broad, vendor-neutral credential recognised by employers and by public sector procurement.

CompTIA recommends around two years of experience in a security or systems administration role, and suggests holding Network+ first. These are recommendations, not requirements — there is nothing preventing you from booking the exam without them. In practice, you will find the course much easier if you are already comfortable with TCP/IP, subnetting, and administering Windows and Linux.

The exam

The Security+ is set and awarded by CompTIA, and delivered at a Pearson VUE test centre or by online proctor.

- A maximum of 90 questions, 90 minutes
- Multiple-choice and performance-based questions, the latter scored on what you do in a simulated environment
- A scaled score of 750 out of 100 to 900 is required to pass
- Available in English, Japanese, Portuguese, Spanish and Thai

The exam voucher is purchased separately from CompTIA. We arrange it on your behalf and send you the code, and you book your own exam date. The certification is valid for three years and is renewed through CompTIA's continuing education programme.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Roughly half the time is hands-on, with dedicated practice at performance-based question formats so the simulation on exam day is not the first one you have seen. Domain checkpoints each day, and a full-length timed mock under exam conditions on the final afternoon.

Mapped to the CompTIA Security+ SY0-701 exam objectives. Taught from Hacky Security's own curriculum and lab estate by instructors who also work our security operations centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/security-plus/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.