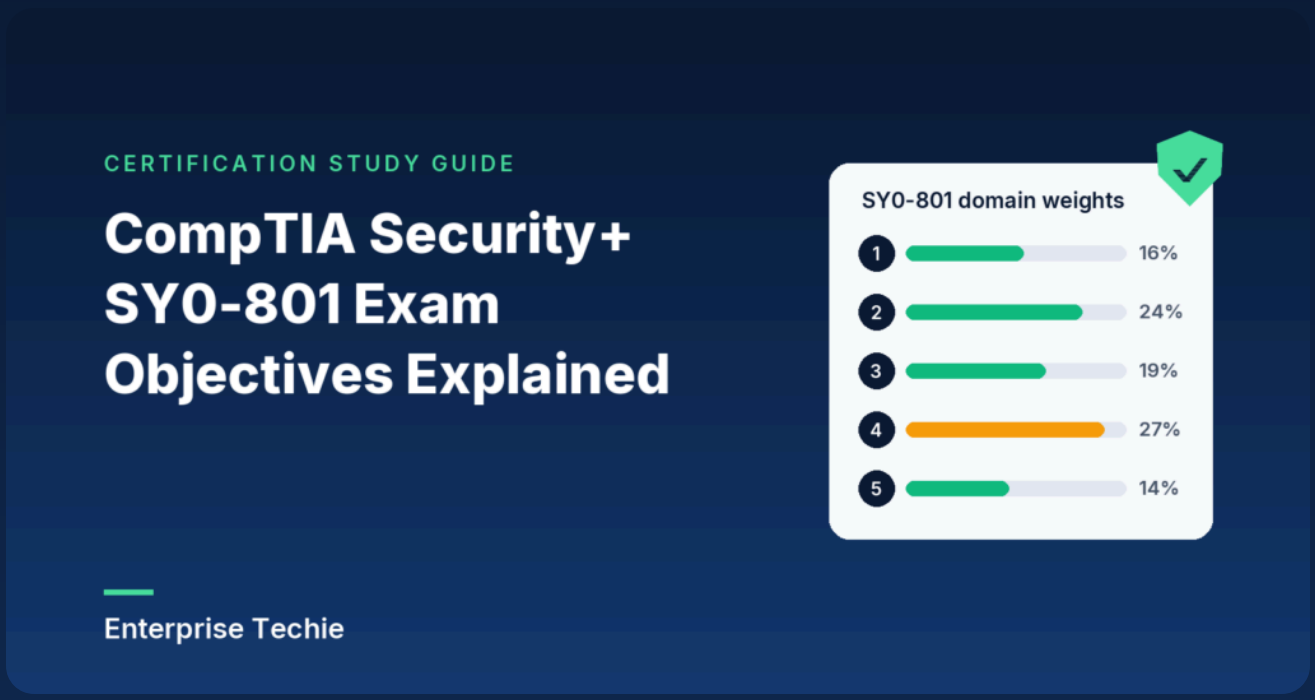


FREE STUDY GUIDE · PDF EDITION

CompTIA Security+ SY0-801 Exam Objectives Explained

The five domains and 27 objectives, in plain English.

Enterprise Techie · enterprisetechie.com/certs/ · November 2026
Online version: enterprisetechie.com/certs/comptia-security-plus-exam-objectives/

CompTIA publishes an exam objectives document for every certification, and for Security+ it is the closest thing to a syllabus that exists. CompTIA builds the SY0-801 exam from the 27 objectives it lists there. This guide walks through that document in plain English: the test details, the five domains and how much each one counts, what each objective covers, and how to turn the list into a study plan.

SY0-801 is the exam code for Security+ V8, which CompTIA expects to launch on or around November 17, 2026. Unless another source is named, every fact below comes from CompTIA's Security+ SY0-801 V8 exam objectives (document version 2.0).

In this guide

- SY0-801 at a glance
- The five domains and their weights
- How to read an objective
- Domain 1: General Security Concepts
- Domain 2: Threats, Vulnerabilities, and Attacks
- Domain 3: Security Architecture
- Domain 4: Security Operations
- Domain 5: Security Program Management and Oversight
- Where AI shows up
- How to study the objectives
- Frequently asked questions

SY0-801 at a glance

Exam code	SY0-801 (Security+ V8)
Number of questions	Maximum of 90
Question types	Multiple-choice and performance-based
Time	90 minutes
Passing score	750 on a scale of 100 to 900
Recommended experience	Two years of hands-on experience as a security administrator
Launch date	Expected on or around November 17, 2026

The previous version, SY0-701 (V7), stays available in English until June 11, 2027, according to CompTIA's Security+ V7 page. That gives the two versions an overlap of roughly seven months, so anyone booking an exam in that window should check which code the voucher and the study material are for.

The five domains and their weights

The objectives are grouped into five domains, and CompTIA gives each domain a percentage of the exam. The two right-hand columns are counted from the objectives document itself.

Domain	Share of exam	Objectives	"Given a scenario" objectives
1.0 General Security Concepts	16%	3	1
2.0 Threats, Vulnerabilities, and Attacks	24%	6	1
3.0 Security Architecture	19%	4	1
4.0 Security Operations	27%	8	5
5.0 Security Program Management and Oversight	14%	6	1
Total	**100%**	**27**	**9**

Two things stand out. Security Operations is the heaviest domain at 27 percent, and it holds five of the nine objectives that begin with "Given a scenario". And Domains 2 and 4 together account for 51 percent of the exam, so threats and day-to-day operations make up more than half of what is tested.

How to read an objective

Each objective opens with a verb, and the verb says what kind of knowledge is expected. Most objectives ask candidates to explain, summarize, describe, or compare and contrast. Those test whether a concept is understood well enough to recognize it and say why it matters.

Nine objectives begin with "Given a scenario". They are about applying the material to a situation: picking the right control, reading an indicator, choosing the next step. Those are the objectives where hands-on practice pays off most.

Under each objective sits a list of bulleted examples. CompTIA states that the lists are not exhaustive: other technologies, processes or tasks related to an objective can appear on the exam even when they are not listed. Treat the bullets as a map of the territory, not the full inventory.

Domain 1: General Security Concepts (16%)

The vocabulary the rest of the exam assumes. Three objectives, one of them scenario-based.

- **1.1 Security concepts and controls.** Confidentiality, integrity and availability; authentication, authorization and accounting; non-repudiation; Zero Trust principles and least privilege. It also

covers how controls are classified, by category (technical, managerial, operational, physical) and by type (preventive, deterrent, detective, corrective, compensating, directive).

- **1.2 Change management (scenario).** How approval processes, change advisory boards, impact analysis, backout plans and maintenance windows protect security, along with the technical side effects of change: downtime, service and application restarts, legacy applications and dependencies. Keeping diagrams, policies and version control up to date belongs here too.
- **1.3 Cryptographic solutions.** Public key infrastructure, certificates and how they are revoked and checked (CRLs and OCSP), encryption at levels from full disk down to individual records, key exchange and key length, digital signatures, hashing, salting and obfuscation.

Study note: control categories and control types are two separate labels, and a single control carries one of each. A security camera, for example, is a physical control and a detective one. Practice labeling controls on both axes.

Domain 2: Threats, Vulnerabilities, and Attacks (24%)

Who attacks, how attacks arrive, where systems are weak, and what an attack looks like in the evidence. Six objectives, including a dedicated one on AI.

- **2.1 Threats and vulnerabilities.** Threat feeds and intelligence sources, likelihood and impact, and how vulnerabilities are scored with CVSS and catalogued as CVEs.
- **2.2 Threat actors and motivations.** Unskilled attackers, hacktivists, insiders, competitors, organized crime and state-sponsored groups, what drives them (money, espionage, revenge, ideology and more), and how their resources and sophistication differ.
- **2.3 Threat vectors.** How attacks get in: email, SMS and RCS messages, collaboration tools, QR codes, malicious attachments, browser extensions and session tokens, remote access tools, supply-chain providers including SaaS and managed service providers, USB media, IoT and OT devices, and signals such as Bluetooth, RF and NFC.
- **2.4 Vulnerabilities and attack surfaces.** Unpatched, unsupported and unmanaged systems, race conditions, hardcoded secrets, zero-days, shadow IT, rogue devices, misconfiguration, public code repositories and object storage, identity providers, and large language models.
- **2.5 Indicators of malicious activity (scenario).** Malware families, physical, network and application attacks, social engineering including QR-code phishing (quishing) and deepfakes, credential attacks such as password spraying and MFA bypass, and indicators of compromise like impossible travel, concurrent sessions and log manipulation.
- **2.6 AI threats and vulnerabilities.** Prompt injection, poisoning, model manipulation, jailbreaking, evasion and hallucinations, data loss and privacy, bias, explainability and ethics, plus the session hijacking and code execution risks that come with AI use.

Study note: 2.5 is the scenario objective in this domain. Practice reading a short alert or log excerpt and naming the attack behind it, because that is the skill the objective describes.

Domain 3: Security Architecture (19%)

How the shape of an environment changes its security, and how to protect data and keep services running. Four objectives, one scenario-based.

- **3.1 Architecture models.** The security trade-offs of cloud (serverless, multicloud, public, private, hybrid and community deployments, infrastructure as code), on-premises systems, operational technology, air-gapped networks and microservices, weighed on technical factors such as availability and ease of recovery and business factors such as data sovereignty, cost and risk.
- **3.2 Protecting infrastructure (scenario).** Device placement and security zones, Zero Trust architecture, secure remote access (VPN, tunneling, Security Service Edge), out-of-band management, Group Managed Service Accounts, privilege creep, and how systems should behave when they fail.
- **3.3 Data protection.** Data types and states (at rest, in transit, in use), classification levels, protection methods such as masking, tokenization, hashing and encryption, data roles from owner and custodian to controller and subprocessor, the data life cycle, and categories of regulated data such as health, financial and children's data.
- **3.4 Resilience and recovery.** Hot, warm and cold sites, redundancy through clustering, load balancing, autoscaling and backup power, backups with retention, immutability and restore testing, failover testing, and the recovery metrics RTO, RPO, MTTR and MTBF.

Study note: keep the recovery metrics straight. The recovery time objective (RTO) is how long a service can be down before recovery must be complete; the recovery point objective (RPO) is how much data, measured in time, the business can afford to lose.

Domain 4: Security Operations (27%)

The largest domain and the most hands-on: eight objectives, five of them scenario-based. This is the work a security administrator does every week.

- **4.1 Mitigating controls (scenario).** Segmentation, hardening and sandboxing, deception tools such as honeypots, honeytokens and canary accounts, intrusion detection and prevention, firewalls and web application firewalls, EDR and XDR, network access control with 802.1X, secrets scanning in code repositories, application security controls, email authentication (DMARC, SPF, DKIM, BIMI), Group Policy and SELinux.
- **4.2 Asset management.** The life cycle of hardware, software and data assets, from planning and procurement through assignment, tracking and disposal.

- **4.3 Vulnerability management (scenario).** Finding vulnerabilities (scanning, IP address management, cloud security posture management, source code review), then prioritizing, remediating, verifying and reporting them, including bug bounty programs and responsible disclosure.
- **4.4 Alerting and monitoring.** Log aggregation and alert tuning, SIEM, agents and benchmarks, vulnerability scanners and packet analyzers, the protocols NetFlow, SNMP, syslog and SCAP, port mirroring and dashboards.
- **4.5 Identity and access management (scenario).** Provisioning and deprovisioning, identity proofing, federation and single sign-on (SAML, LDAP, OAuth), account types including emergency access, MFA methods, access control models from role-based to just-in-time, access reviews, passkeys and passwordless sign-in.
- **4.6 Automation and orchestration (scenario).** Scripting for user and resource provisioning and ticketing, guardrails and process risks, CI/CD, and AI capabilities in security operations: agentic AI, chatbots, predictive analysis and AI-augmented baselines.
- **4.7 Incident response.** Preparation (training, tabletop exercises, playbooks), identification and threat hunting, investigation and chain of custody, containment, negotiation, eradication and recovery, notification and external reporting, and post-incident review with root cause analysis.
- **4.8 Investigation data (scenario).** Log and trace data types, NetFlow and IPFIX, packet captures, memory dumps, bit-level copies and snapshots, file and log integrity, and working with HR and legal during an investigation.

Study note: with 27 percent of the exam and five scenario objectives, this domain rewards time at a keyboard. Reading real logs, setting up MFA on a test account and walking through an incident response playbook all map directly to objectives here.

Domain 5: Security Program Management and Oversight (14%)

Governance, risk, compliance and people. Six objectives, one scenario-based.

- **5.1 Governance, risk and compliance artifacts.** Guidelines, standards, procedures and runbooks, business continuity and disaster recovery plans, and policies such as BYOD, acceptable use, clean desk, data retention and vulnerability disclosure.
- **5.2 Risk management.** Identifying, assessing and analyzing risk, the risk register, the four treatments (transfer, accept, avoid, mitigate), business impact analysis, risk appetite and residual risk, and the quantitative measures SLE, ALE and ARO.
- **5.3 Third-party risk.** Vendor selection (RFP, RFI, RFQ, due diligence), agreement types (SLA, SLO, MOU, MOA, NDA, MSA, SOW), vendor monitoring and the right to audit, constraints such as vendor lock-in and jurisdiction, and rules of engagement.

- **5.4 Security compliance.** Compliance training (including anti-money laundering and anti-bribery), monitoring and attestations, the consequences of non-compliance, privacy rights such as the right to be forgotten, legal holds and data retention requirements.
- **5.5 Audits and assessments.** Evidence gathering and scoping, internal and external engagements, penetration testing in known, unknown and partially known environments, reference models such as MITRE ATT&CK, the Cyber Kill Chain and the Diamond Model, and industry, international and regional standards.
- **5.6 Security awareness (scenario).** Training types and delivery, measuring whether training works, and common topics such as social engineering, business email compromise, remote work and removable media.

Study note: the risk measures are simple arithmetic once the terms are clear. Annualized loss expectancy is the single loss expectancy multiplied by the annualized rate of occurrence, so a $10,000 loss expected twice a year carries an ALE of $20,000.

Where AI shows up in SY0-801

Artificial intelligence appears in four places across the objectives, from both the attacker's side and the defender's:

- **2.4** lists large language models as an attack surface.
- **2.5** includes deepfakes among social engineering attacks.
- **2.6** is a whole objective on threats and vulnerabilities that come with using AI, from prompt injection and poisoning to hallucinations and bias.
- **4.6** covers AI as a security operations tool: agentic AI, chatbots, predictive analysis and AI-augmented baselines.

For candidates who already work with AI tools, 2.6 is a chance to pick up points on familiar ground. For everyone else, it is worth reading the terms closely, because several of them (poisoning, evasion, jailbreaking) describe different stages of an attack on a model.

How to study the objectives

1. **Turn the document into a checklist.** Download the objectives from CompTIA's Security+ V8 page and mark each bullet as it becomes familiar. Gaps show up quickly.
2. **Split study time by weight.** Domains 2 and 4 are 51 percent of the exam, so they deserve about half the hours. Domain 5 is the smallest at 14 percent, but its vocabulary (SLA, MOU, ALE) is easy points once learned.
3. **Practice the nine scenario objectives hands-on.** 1.2, 2.5, 3.2, 4.1, 4.3, 4.5, 4.6, 4.8 and 5.6 are about applying knowledge, and a lab, a free cloud account or a home network turns those bullets

into experience.

4. **Test against the objectives, then read the explanations.** Practice questions show which objectives are solid and which are not. The explanation for a missed question usually teaches more than the question itself.

PRACTICE AGAINST THESE OBJECTIVES

Security+ Practice Test: ET for iPhone and iPad has 1,000 original SY0-801 practice questions spread across the five domains at these weights (160, 240, 190, 270 and 140 questions), with an explanation for every answer, timed mock exams and an AI tutor. It is free to start with 30 questions and needs no account.

See the Security+ app

Frequently asked questions

How many questions are on the Security+ SY0-801 exam?

A maximum of 90, a mix of multiple-choice and performance-based questions, with 90 minutes to complete them, according to CompTIA's exam objectives.

What is the passing score for Security+ SY0-801?

750 on a scale of 100 to 900.

What are the five Security+ domains?

General Security Concepts (16%), Threats, Vulnerabilities, and Attacks (24%), Security Architecture (19%), Security Operations (27%), and Security Program Management and Oversight (14%).

How many objectives does SY0-801 have?

27, spread across the five domains. Nine of them begin with "Given a scenario", which means they are about applying knowledge to a situation rather than recognizing a term.

Does Security+ SY0-801 cover AI?

Yes. Objective 2.6 is dedicated to threats and vulnerabilities associated with AI, objective 4.6 covers AI capabilities in security operations, and AI also appears in 2.4 (large language models as an attack surface) and 2.5 (deepfakes).

When does SY0-701 retire?

CompTIA lists June 11, 2027 as the retirement date for the English SY0-701 exam. SY0-801 is expected to launch on or around November 17, 2026, so both versions should be available for roughly seven months.

Is everything on the exam listed in the objectives?

Not every detail. CompTIA notes that the bulleted examples under each objective are not exhaustive, and related technologies or tasks can appear on the exam even if they are not listed.

Sources: CompTIA Security+ V8 (SY0-801) and its exam objectives, document version 2.0; CompTIA Security+ V7 (SY0-701). Question counts per domain: the Security+ Practice Test: ET question bank. CompTIA and Security+ are trademarks of CompTIA, Inc. Enterprise Techie is not affiliated with or endorsed by CompTIA.

This PDF matches the online guide as of November 2026. The online version is updated first when the exam changes: https://enterprisetechie.com/certs/comptia-security-plus-exam-objectives/