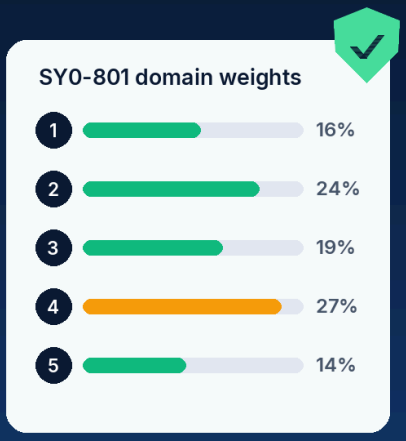
CERTIFICATION STUDY GUIDE

CompTIA Security+ Study Guide: SY0-801, Domain by Domain



Enterprise Techie

FREE STUDY GUIDE · PDF EDITION

CompTIA Security+ SY0-801 Study Guide

All five domains and 27 objectives, explained in plain English.

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

This CompTIA Security+ study guide covers SY0-801, the exam code for Security+ V8, which CompTIA expects to launch on or around November 17, 2026. It follows CompTIA's official exam objectives domain by domain and objective by objective, in CompTIA's own order, and teaches each topic in plain English with comparison tables and exam tips. It is free to read.

The test details, domain weights and objective list come from CompTIA's Security+ V8 page and its exam objectives document (version 2.0). Retirement dates for the previous exam come from CompTIA's Security+ V7 page. Technical facts in the domain sections link to the bodies that define them, such as NIST, the IETF, MITRE, CISA, FIRST and Microsoft, and every source is listed at the end.

In this guide

- Security+ SY0-801 at a glance
- How to use this guide
- 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
- A study plan
- Practice questions
- Frequently asked questions
- Sources

Security+ SY0-801 at a glance

Exam code	SY0-801 (Security+ V8)
Launch date	Expected on or around November 17, 2026
Number of questions	Maximum of 90, 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
Language	English
Expected retirement	Estimated three years after launch
Accreditation	ISO 17024, through ANAB
Objectives	27, across five domains
Previous version	SY0-701 (V7), English exam retires June 11, 2027

The objective count is taken from the objectives document, and the other rows from CompTIA's V8 and V7 pages. The V7 page lists June 11, 2027 for the English SY0-701 and August 13, 2027 for its Japanese, Portuguese, Spanish and Thai versions, so anyone booking during the overlap should check that the voucher, exam code and study material match. This guide covers SY0-801 only.

How to use this guide

Each domain gets a section, and each of the 27 objectives gets a heading numbered the way CompTIA numbers it. Sections are sized roughly in proportion to the domain weights. Objectives that CompTIA phrases as "Given a scenario" are marked (scenario): they ask candidates to apply the material to a situation.

Domain	Share of exam	Objectives	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

For a one-page overview of every objective, read Security+ SY0-801 exam objectives explained. To test each domain as it is finished, the Security+ practice test app follows the same five domains. If networking basics are new, the Network+ study guide is a useful first step.

Domain 1: General Security Concepts (16%)

The vocabulary the rest of the exam builds on: security goals, how controls are classified, change management and cryptography.

1.1 Core security concepts and how controls are classified

NIST defines confidentiality as preserving authorized restrictions on access to and disclosure of information, integrity as guarding against improper modification or destruction of information, and availability as timely and reliable access to information. Together they are the CIA triad. A leaked customer list breaks confidentiality, a tampered invoice breaks integrity, and ransomware on a file server breaks availability.

AAA covers access. Authentication proves identity, authorization sets what that identity may do, and accounting records what it did. Non-repudiation, which FIPS 186-5 describes as assurance of the integrity and origin of data, comes from digital signatures, since a signer cannot easily deny one later.

NIST SP 800-207 says Zero Trust assumes no implicit trust is granted to assets or user accounts, and that it protects resources rather than network segments. Each session is authenticated and authorized before it starts. A policy decision point, made of a policy engine that decides and a policy administrator that acts on the decision, instructs a policy enforcement point that opens, monitors and closes connections. Those decisions travel on a control plane, while application traffic uses the data plane.

Least privilege limits users, and processes acting for them, to the minimum access their tasks need. Defense in depth layers people, technology and operations so that an attack missed by one layer can be caught by another.

Every control can be labeled two ways: by category (what kind of control it is) and by type (what it is meant to do).

Category	Examples
Technical (logical)	Firewall rules, encryption, MFA
Managerial (administrative)	Risk assessments, security policies
Operational	Log reviews, awareness training, carried out by people
Physical (environmental)	Locks, fences, fire suppression

Type	Purpose	Example
Preventive	Stops an incident	Door lock, firewall deny rule
Deterrent	Discourages an attempt	Login warning banner
Detective	Finds an incident	IDS alert, log review
Corrective	Limits damage and restores	Restore from backup, patch
Compensating	Stands in for a control that is not possible	Extra monitoring on a system that cannot be patched
Directive	Tells people what to do	Acceptable use policy

Exam tip: a single control has both a category and a type. A login warning banner is technical and deterrent; an acceptable use policy is managerial and directive.

1.2 How change management protects security (scenario)

Unplanned change causes outages and security gaps, so changes go through a formal process. A change advisory board (CAB) approves or rejects requests. Each change has an accountable owner, stakeholders it affects, an impact analysis of what it touches, and test results from a non-production environment.

A backout plan returns systems to the last known-good state if a change fails. Fail forward pushes ahead with a fix instead, which suits cases where rolling back is riskier than correcting. Work happens in an agreed maintenance window, and standard operating procedures (SOPs) keep routine changes repeatable.

Technical side effects include updates to allow or deny lists, restricted activities during the work, downtime, and service or application restarts. Legacy applications and hidden dependencies are where surprises come from. Afterward, diagrams, policies and procedures are updated, and version control keeps a history so earlier states can be restored.

Exam tip: a backout plan reverses a failed change, while fail forward fixes it in place. When rolling back would do more harm than fixing, fail forward is the better fit.

1.3 Choosing the right cryptographic solution

A symmetric algorithm uses secret keying material shared between the parties, so it is fast and suits bulk data. AES (FIPS 197) transforms data in 128-bit blocks, and the number in AES-128, AES-192 and AES-256 is the key length in bits. Asymmetric cryptography uses two keys, one to encrypt or sign and the other to decrypt or verify; the public key is shared and the private key stays secret. FIPS 186-5 specifies RSA, ECDSA and EdDSA signatures and no longer approves DSA for generating them.

A hash function produces a fixed-length output and is designed to be one-way and collision resistant. The SHA-2 family in FIPS 180-4 includes SHA-256, SHA-384 and SHA-512, and FIPS 202 adds SHA-3. RFC 6151 says MD5 is no longer acceptable where collision resistance is required, and NIST says SHA-1 should be phased out by December 31, 2030. A salt is a non-secret value added to a computation, such as password hashing, so its results cannot be reused by an attacker.

A digital signature starts with a message digest that the signer signs with a private key; FIPS 186-5 says signatures detect unauthorized changes to data and authenticate the signer. Key exchange agrees on a symmetric key over an untrusted network. In TLS 1.3 (RFC 8446), every public-key-based key exchange provides forward secrecy: a long-term key compromised after the handshake does not expose the session key, as long as the session key itself was erased. RFC 8996 formally deprecated TLS 1.0 and 1.1 in March 2021.

PKI term	What it means
Certificate authority (CA)	Issues and signs certificates. A certificate from a third-party CA is trusted wherever that CA's root is trusted; a self-signed certificate is signed with its own key and trusted only where installed by hand.
Certificate signing request (CSR)	A distinguished name and public key, signed by the requester (RFC 2986)
Root of trust	Highly reliable hardware, firmware and software components that perform critical security functions (NIST)
Wildcard	The asterisk may only be the whole left-most label and matches one label (RFC 9525), so *.example.com covers www.example.com but not a.b.example.com
CRL	A time-stamped list of revoked certificates signed by a CA or CRL issuer (RFC 5280)
OCSP	Checks the current status of one certificate without a CRL; answers are good, revoked or unknown (RFC 6960)
Key escrow	Retaining the private key of an encryption key pair for recovery (CNSSI 4009)

Encryption can cover a full disk, a partition or volume, a file, a database or a single record. Full-disk encryption protects a stolen laptop, but only file or record encryption stays with data that is copied elsewhere. A trusted platform module (TPM) is a tamper-resistant chip on some motherboards that performs cryptographic operations and protects keys. Obfuscation makes code or data harder to understand without making it secret.

Exam tip: encryption is reversible with the key, and hashing is one-way. If the original data must come back, use encryption; if the need is to prove data has not changed, use hashing.

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. Objective 2.5 is the scenario objective, and 2.6 covers AI.

2.1 Threats, vulnerabilities and how they are scored

FIPS 200 defines a threat as any circumstance or event that could harm an organization's operations, assets or people through unauthorized access, destruction, disclosure, modification of information or denial of service. A vulnerability is the weakness a threat exploits. Likelihood is how probable an event is, and impact is how much harm it would do.

Threat intelligence comes from open sources, commercial feeds, sharing groups and government advisories. Feeds deliver indicators such as malicious IP addresses, domains and file hashes in machine-readable form so tools can act on them, and they need regular review because attackers change infrastructure.

Each CVE entry carries an identification number, a description and at least one public reference for a publicly known vulnerability, and the list feeds NIST's National Vulnerability Database. The Common Vulnerability Scoring System, published by FIRST, scores a vulnerability's severity relative to others. CVSS v4.0 has four metric groups (Base, Threat, Environmental and Supplemental) and these ratings:

Rating	None	Low	Medium	High	Critical
CVSS v4.0 score	0.0	0.1 to 3.9	4.0 to 6.9	7.0 to 8.9	9.0 to 10.0

Severity is only one input. The CVSS specification describes Environmental scores as a fuller input to an organization's own risk assessment, and CISA says to use its Known Exploited Vulnerabilities catalog, which lists flaws exploited in the wild, as an input to prioritization.

Exam tip: a CVE identifies a specific vulnerability, and a CVSS score rates its severity. One names the problem; the other measures it.

2.2 Threat actors and what drives them

Actor	Common motivations	Resources and capability
Unskilled attacker	Notoriety, curiosity	Low; uses tools written by others
Hacktivist	Ideological or political causes	Varies; often public actions such as defacement or leaks
Insider	Revenge, money, or none when the harm is accidental	Already holds legitimate access
Organized crime	Money, through ransomware, fraud and extortion	High; run like a business
Competitor	Intellectual property, market advantage	Varies
State-sponsored	Espionage, influence, disruption	Very high; patient and well funded
Terrorist	Fear and chaos for an ideology	Varies

NIST describes an advanced persistent threat (APT) as an adversary with sophisticated expertise and significant resources that builds a lasting foothold and pursues its goals over a long period. Sort any actor by whether it is internal or external, its resources and funding, and its sophistication. An accidental insider has no motive at all and can still cause a serious breach.

Exam tip: match the motive before the method. Money usually points to organized crime, while patient intelligence gathering points to a state-sponsored group.

2.3 Threat vectors: how attacks get in

A threat vector is the path an attack takes to its target.

Vector group	Examples
Message-based	Email, SMS, RCS, instant messaging, collaboration tools
Image-based	QR codes, which hide their destination until scanned; embedded content; CAPTCHA pages
Attachments	Documents with macros, RTF files, PDFs
Browser-based	Extensions, JavaScript, password managers, and cookies or session tokens, which let an attacker skip the login
Network-based	Routers and other infrastructure devices, virtual appliances, session keys
Remote access	Remote desktop, VNC, VPN
Endpoint-based	Workstations, servers, phones and tablets, trusted devices, built-in tools
Supply chain	Managed service providers, SaaS providers, logistics firms, other third parties
External media	Malicious USB drives and cables
Human-based	Impersonation, contractors, visitors, biometric spoofing, watering holes
IoT and OT	Cameras, sensors, printers, industrial control systems
Physical	Locks and keys, access vestibules, access passes
Signal-based	Bluetooth, RF, NFC

Living off the land means attacking with legitimate tools already on a system instead of bringing in malware. Joint guidance from CISA, NSA, FBI and international partners (February 2024) notes it stays effective with little or no investment in tooling, so detection depends on knowing what normal administration looks like.

Exam tip: phishing goes to the victim. A watering hole attack waits for the victim to visit a site the attacker has already compromised.

2.4 Vulnerabilities and attack surfaces

NIST defines the attack surface as the points on a system's boundary where an attacker can try to enter, cause an effect or extract data. Every unneeded open port, unused service, stale account or forgotten device makes it larger.

Four states of neglect are easy to confuse. Unpatched systems have a fix that was not applied. Unsupported products no longer get vendor fixes. Obsolete systems are past their useful life. Unmanaged systems are not tracked at all. A zero-day attack exploits a previously unknown hardware, firmware or software vulnerability, so no fix exists yet.

In applications, a race condition is a timing flaw; CWE-367 describes the time-of-check to time-of-use (TOCTOU) form, where a resource's state changes between being checked and being used. A malicious update abuses trust in an update channel. Hardcoded credentials (CWE-798) put passwords or keys in code, and unsafe exception handling can leak internal details.

Misconfiguration, secrets in public repositories and publicly readable object storage expose data with no exploit at all. Shadow IT is technology used without IT's approval, rogue devices are unauthorized hardware, and unmanaged credentials stay valid until someone removes them. Identity providers are prime targets because one compromise reaches every connected application. Weak cryptography, wireless and low-power links, mobile devices, virtualization, operating systems and large language models (see 2.6) complete the list.

Exam tip: unpatched means a fix exists but was not applied; zero-day means no fix exists yet; unsupported means no fix will come.

2.5 Recognizing indicators of malicious activity (scenario)

This objective is about reading evidence: given an alert, a log excerpt or a user report, name what is happening.

Malware	What it is
Ransomware	Malware designed to encrypt files on a device, making them and dependent systems unusable (CISA)
Trojan	A program that appears useful but hides a malicious function (NIST)
Worm	A self-contained program that spreads itself across systems and networks (CNSSI 4009)
Virus	Spreads by modifying other programs to include a copy of itself (CNSSI 4009)
Spyware	Secretly installed to gather information about people (NIST)
Adware	Pushes unwanted advertising
Rootkit	Tools that hide an attacker's activity after root-level access (CNSSI 4009)
Keylogger	Records keystrokes to capture passwords and other input
Logic bomb	Code planted to trigger a malicious function when set conditions are met (CNSSI 4009)
Fileless malware	Runs in memory or through legitimate tools, leaving little on disk

A denial of service prevents authorized access to resources or delays time-critical operations, and a distributed denial of service (DDoS) does it from many sources. Sniffing captures traffic, spoofing forges an identity such as an address, and an on-path attacker sits between two parties. A protocol downgrade forces a weaker version, which is why TLS 1.3 embeds downgrade protection in the server's random value. DNS cache poisoning plants false records in a resolver; DNSSEC adds origin authentication and integrity to DNS, but not confidentiality (RFC 4033). A rogue access point is another network-level sign.

Phishing uses fraudulent messages, spear phishing targets a specific person or group, and whaling targets executives. Smishing arrives by SMS, vishing by voice, and quishing through a QR code. Deepfakes, which NIST describes as highly realistic synthetic audiovisual content and photorealistic images (NIST AI 600-1), make impersonation far more convincing.

In SQL injection (CWE-89), input is interpreted as part of a database command. A buffer overflow copies input without checking its size (CWE-120). Directory traversal uses crafted paths to reach files outside a restricted folder (CWE-22). Cross-site request forgery exploits an application that cannot tell whether the user intended a request (CWE-352), and server-side request forgery makes a server fetch a URL without checking its destination (CWE-918). Replay resends captured messages, and privilege escalation gains rights beyond those granted.

Brute force tries many passwords against one account. Password spraying reverses that, trying one or a few common passwords against many accounts. User enumeration finds which usernames exist. MFA bypass includes MFA request generation, where an attacker who has the password floods the user with push prompts until one is approved.

Indicator	What it can suggest
Account lockouts	Brute force
Impossible travel	Sign-ins from places too far apart for the time between them
Concurrent sessions	One account active in two places at once
Excessive resource consumption	Cryptomining, a worm or a denial of service
Log manipulation or gaps	An attacker covering tracks
Known-bad hashes, IP addresses, domains	Matches with threat intelligence
Malicious processes, file system artifacts, odd timestamps, plaintext strings	Malware running, dropped files, altered data, embedded commands or credentials

Exam tip: many failed logins on one account suggest brute force. One or two failures on each of many accounts suggest password spraying.

2.6 Threats and vulnerabilities that come with AI

NIST's adversarial machine learning taxonomy, NIST AI 100-2 E2025 (March 2025), is the best primary reference here.

Attack	Stage	What happens, per NIST
Data poisoning	Training	The adversary controls part of the training data
Model poisoning	Training or supply chain	The adversary controls the model and its parameters
Evasion	Deployment	Modified inputs (adversarial examples) change the model's predictions
Privacy attacks	Deployment	Inferring whether data was in the training set, or extracting model information
Direct prompt injection	Use	User instructions appended to higher-trust ones such as the system prompt
Indirect prompt injection	Use	Instructions planted in resources the model reads, such as web pages
Jailbreak	Use	A direct prompting attack to get around restrictions on outputs

Prompt injection works because generative models combine data and instructions in one channel, so text the model reads can act as a command. Model manipulation is the broader idea of changing behavior through training data, parameters or inputs. Hallucinations are what NIST AI 600-1 calls confabulation, confidently stated but false content, and they become a security problem when people or tools act on them unchecked.

Data loss happens when sensitive data goes into AI tools or leaks out in responses, and privacy covers both training data and what users share. A model that cannot explain its decisions is hard to audit, and a biased one produces unfair results at scale, which is an ethical concern too. When AI agents use tools, two classic risks return: session hijacking and code execution triggered by injected instructions.

Exam tip: poisoning corrupts a model through its training; evasion fools a finished model with crafted inputs. A jailbreak targets the model's restrictions directly, while indirect prompt injection hides instructions in content the model reads.

Domain 3: Security Architecture (19%)

How the shape of an environment changes its security, how to protect data, and how to stay up through failures. Objective 3.2 is the scenario objective.

3.1 Security trade-offs of architecture models

NIST SP 800-145 (September 2011) defines the four cloud deployment models.

Model	NIST definition, in short
Public	Open use by the general public, on the provider's premises
Private	Exclusive use by a single organization, on or off premises
Community	Exclusive use by a community of organizations with shared concerns, such as compliance
Hybrid	Two or more distinct clouds bound together for data and application portability

Responsibility shifts with the service model. NIST notes that a SaaS customer does not manage the underlying infrastructure, servers, operating systems or storage, while an IaaS customer controls operating systems, storage and deployed applications. The more the customer controls, the more it must secure. AWS describes Lambda as a serverless compute service that runs code without provisioning or managing servers, with AWS handling server maintenance, scaling and patching; the customer still owns the code, its permissions and its data.

Multicloud spreads workloads across providers, adding resilience but multiplying configurations to secure. Infrastructure as code (IaC) defines infrastructure in versioned templates that can be reviewed and rebuilt consistently, though a template mistake repeats everywhere it is deployed. Microservices communicate through APIs (NIST SP 800-204), so each service is simpler but there are many endpoints to protect. Operational technology (OT) runs physical processes on equipment that is often hard to patch. An air gap is an interface where two systems are not physically connected and any data transfer is manual. Logical segmentation separates networks in software, such as VLANs, while physical segmentation uses separate hardware.

Choosing a model weighs technical factors (availability, resilience, ease of recovery, compute and power needs, usability, responsibility, open-source versus proprietary) against business factors (cost, scalability, ownership, data classification, environmental requirements, risk, and data sovereignty, meaning which country's laws apply where data is stored).

Exam tip: hybrid combines different kinds of cloud; community is one cloud shared by organizations with common concerns; multicloud means more than one provider.

3.2 Securing infrastructure through design (scenario)

Device placement decides what a device can see and protect. Security zones group systems of similar trust, such as an internet-facing screened subnet and internal server networks, with controls at each boundary. An inline device can block traffic, while a sensor on a mirrored port only watches. Shrinking the attack surface and adding diversity, meaning different vendors or technologies at different layers, keep one flaw from opening every door.

A Zero Trust architecture checks the user, the device's health and inventory status, and the application request before granting access. Microsoft's Intune documentation shows the pattern:

device compliance feeds Conditional Access, so decisions use current device posture rather than network location.

Secure access option	What it does
VPN with IPsec	Transport mode, typically host to host, or tunnel mode, applied to an IP tunnel; implementations must support ESP and may support AH (RFC 4301)
Security Service Edge (SSE)	Microsoft calls SSE an identity-aware, cloud-delivered network perimeter; its version pairs a secure web gateway and Zero Trust Network Access with a cloud access security broker (Microsoft Learn)
Out-of-band management	A separate management path that works when the production network is down or compromised
End-to-end encrypted messaging	Only the endpoints can read messages, not the servers relaying them
Secure file transfer	Encrypted transfer protocols instead of plaintext ones

Microsoft's group Managed Service Accounts (gMSAs) let Windows manage a service account's password across multiple servers, such as a load-balanced farm, so no administrator handles it. Separate least-privilege accounts keep daily work apart from admin work. Privilege creep is the build-up of rights as people change roles without losing old access, which access reviews catch.

Fail secure (fail closed) prevents loss of a secure state when a failure occurs, such as a firewall that blocks all traffic when it crashes. Fail open keeps things flowing, favoring availability, such as an exit door that releases when power fails.

Exam tip: choose fail open where life safety or availability comes first, and fail secure where protecting data comes first.

3.3 Concepts and strategies for protecting data

Structured data lives in defined fields, like a database table; unstructured data is everything else, such as documents and images. Data is at rest when stored, in transit when moving, and in use while being processed. CNSSI 4009's definition of data loss prevention covers all three states.

US government classification under Executive Order 13526 has three levels: Top Secret (exceptionally grave damage to national security), Secret (serious damage) and Confidential (damage). Commercial schemes vary and often use labels such as public, sensitive, restricted and critical. Handling rules give labels meaning: marking, which endpoints may hold the data, where it may be stored, and geofencing, which restricts actions by a device's location.

Method	What it does
Encryption	Transforms data with a key; reversible with the key
Hashing	A fixed-length, one-way digest
Masking	Conceals part of a value when displayed or printed, such as most of a card number (PCI SSC)
Tokenization	Replaces a value with a surrogate token that only the tokenization system can redeem (PCI SSC)
De-identification	Removes the link between identifying data and the person (NIST)
Transposition, filtering, obfuscation	Reorder data, strip sensitive parts, or make data harder to read

The data owner is accountable; NIST describes an information owner as an official with authority over specified information and responsibility for its controls. The custodian runs those controls day to day, a data steward enforces data policies, and an operator handles routine processing. Under the EU's GDPR, the controller determines the purposes and means of processing personal data, the processor processes it on the controller's behalf (Article 4), and a processor may bring in another processor, a subprocessor, only with the controller's written authorization (Article 28).

The data life cycle runs from creation through management, distribution and retention to disposal. Regulated categories include health, personal, financial, children's, intellectual property and legal data; PCI DSS, for example, applies to entities that store, process or transmit cardholder data.

Exam tip: masking hides part of a value on display, tokenization swaps it for a stand-in kept in a separate system, and encryption transforms the whole value and can be reversed with the key.

3.4 Resilience and recovery

Site (NIST SP 800-34)	What is there	Trade-off
Hot	A fully operational offsite facility with hardware and software	Fastest, costliest
Warm	Partially equipped with systems and telecommunications	Middle ground
Cold	Power and space for a computer facility, but no computer equipment until needed	Slowest, cheapest

An alternate site exposed to the same flood or storm as the primary adds little, so environmental factors matter. Platform diversity, meaning more than one vendor, hardware type or virtualization platform, keeps one flaw from stopping everything. Load balancing spreads requests, clustering lets nodes take over for each other, and autoscaling adjusts capacity; high availability is the goal they

serve, and multicloud adds redundancy at the provider level. For power, a UPS bridges short interruptions, a generator covers long outages, a redundant power supply survives a failed unit, and surge protectors absorb spikes.

Backups need retention periods, a defined scope, immutability where possible and regular restore tests. CISA's ransomware guide recommends offline, encrypted backups of critical data, tested regularly, because many ransomware variants hunt for reachable backups. A failover test switches to standby systems for real, a simulation walks through a scenario, and parallel processing runs recovery systems alongside production. Disaster recovery restores IT systems; business continuity keeps the business running; capacity planning makes sure there are enough people, technology and infrastructure.

Metric	Meaning
RTO	How long a system can be in recovery before the delay harms the organization
RPO	The point in time to which data must be recovered, which sets how much data can be lost
MTTR	Mean time to repair a failed component
MTBF	Mean running time between failures

Exam tip: MTBF measures reliability, so higher is better. MTTR measures how fast things are fixed, so lower is better.

Domain 4: Security Operations (27%)

The largest domain, with eight objectives, five of them scenario-based: the daily work of hardening, monitoring, managing identities and vulnerabilities, automating, and responding to incidents.

4.1 Mitigating controls that secure an environment (scenario)

Segmentation limits how far an attacker can move, and access controls decide who reaches what. Hardening removes what is not needed and applies secure settings; the CIS Benchmarks are consensus-based, prescriptive configuration recommendations for many product families. Sandboxing runs untrusted code in isolation. Deception tools catch intruders: a honeypot is a system or resource designed to attract intruders, a honeynet is a network of them, and honeyfiles, honeytokens and canary accounts are decoy files, data and accounts that raise an alert when touched.

NIST SP 800-94 covers four classes of intrusion detection and prevention: network-based, wireless, network behavior analysis and host-based. An IDS alerts; an IPS sits inline and can block. NIDS and NIPS watch traffic, HIDS and HIPS watch one host, and a wireless IPS (WIPS) watches the radio environment.

As NIST SP 800-41 Rev. 1 explains, packet filters decide on addresses, ports and protocols, stateful inspection also tracks each connection in a state table, and application firewalls analyze traffic at the application layer, for example blocking a forbidden attachment type. That is the difference between a Layer 4 and a Layer 7 decision. Microsoft describes Azure WAF as centralized protection for web applications against common exploits such as SQL injection and cross-site scripting. Unified threat management (UTM) bundles several functions in one device, and rate limiting caps requests per client, slowing brute force and some denial-of-service attempts.

Antivirus is the endpoint baseline. EDR adds detection, investigation and response on the device; Microsoft describes Defender for Endpoint as a platform for preventative protection, post-breach detection, automated investigation and response. XDR widens the view: Defender XDR coordinates detection and response across endpoints, identities, email and applications. MDM manages a whole enrolled device and can wipe it, while mobile application management covers only work apps and their data (Microsoft Intune). Application control uses allow lists or block lists, and DLP and content filters inspect outbound data through endpoint agents or a central proxy.

IEEE 802.1X provides port-based network access control, restricting LAN access to authenticated, authorized devices. It carries EAP, a framework supporting multiple authentication methods directly over data link layers such as IEEE 802 (RFC 3748), and RADIUS (RFC 2865) carries authentication, authorization and configuration information to a shared authentication server. Posture checks confirm patches and settings first. A captive portal limits a device to restricted hosts until the user meets its conditions (RFC 8952).

For code, GitHub's secret scanning searches the entire Git history on all branches for hardcoded credentials. Input validation blocks malformed data (CWE-20 is its absence). The Secure cookie attribute limits a cookie to secure channels, and HttpOnly keeps it away from browser scripts (RFC 6265). Static analysis examines code without running it, and code signing applies a digital signature so changes are detectable and the publisher is authenticated.

Email control	What it does
SPF	The domain names the hosts allowed to send its mail, and receivers check (RFC 7208)
DKIM	Signs messages; verifiers fetch the public key from the signing domain's DNS (RFC 6376)
DMARC	The domain owner requests handling for mail that fails validation (none, quarantine or reject) and asks for reports (RFC 9989, which obsoletes RFC 7489)
BIMI	Shows a brand indicator next to authenticated mail and requires a DMARC policy of quarantine or reject; an Internet-Draft, not an RFC

Group Policy provides centralized management of Windows operating systems, applications and user settings, often through Group Policy Objects linked to sites, domains and organizational units. SELinux is the primary mandatory access control mechanism in a number of Linux distributions.

Exam tip: an IDS alerts and an IPS blocks. If traffic must be stopped automatically, the device has to be inline.

4.2 Managing hardware, software and data assets

An organization can only protect what it knows it has. Planning and scoping decide what is needed, procurement checks suppliers and security requirements, assignment records an owner for each asset, and tracking keeps the inventory current for patching, licensing and incident response. Disposal is where data leaks. NIST SP 800-88 Rev. 2 (September 2025) defines three sanitization methods:

Method	What it does	Media afterward
Clear	Logical techniques through the normal interface, against simple, non-invasive recovery	Reusable
Purge	Makes recovery infeasible even with state-of-the-art lab techniques; includes cryptographic erase	Potentially reusable
Destroy	Makes lab recovery infeasible and leaves the media unable to store data	Not reusable

For cloud storage, where the customer cannot reach the physical media, NIST notes that cryptographic erase may be the only viable purge option.

Exam tip: purge and destroy both defeat lab-grade recovery, but only purge can leave the device usable.

4.3 Running vulnerability management (scenario)

Vulnerability management is a loop: identify, prioritize, remediate, verify, report. Identification uses scanning, with credentialed scans seeing more than uncredentialed ones; IP address management, which Microsoft describes as discovering IP address infrastructure and managing it centrally; cloud security posture management, which Microsoft Defender for Cloud uses to continually assess cloud resources against security standards; and source code review.

Prioritization combines severity (CVSS, from 2.1), evidence of exploitation such as CISA's KEV catalog, the asset's exposure, and penetration test findings. Remediation means patching, reconfiguring or adding a compensating control, and verification, usually a rescan, confirms the fix. Reports go to internal owners and to outsiders through bug bounty programs and responsible disclosure policies. CISA's disclosure policy template tells researchers what is in scope and how to report, and treats good-faith research under the policy as authorized.

Exam tip: a finding is closed when verification shows the vulnerability is gone, not when the patch is deployed.

4.4 Security alerting and monitoring

Monitoring covers systems, applications and infrastructure through log aggregation, alerting, scanning, archiving, reporting and alert tuning, which keeps analysts out from under false positives. NIST describes SIEM software as providing centralized logging for many log types. Agents see more detail on the host; agentless tools query remotely and are easier to deploy. NIST describes SCAP as a suite of specifications for expressing and exchanging security configuration and vulnerability information, so tools can check systems against benchmarks consistently.

Protocol	Purpose	IANA port
NetFlow v9, IPFIX	Export flow records; a flow is a set of IP packets passing an observation point in a time interval (RFC 3954, RFC 7011)	IPFIX 4739
SNMP	Manages network devices; traps notify the manager. SNMPv3 adds message-level security with authentication and privacy (RFC 3414)	161, traps 162
syslog	Conveys event notifications, with severities from 0 (Emergency) to 7 (Debug) (RFC 5424)	514 UDP; 6514 over TLS

Port mirroring copies traffic for analysis; Cisco's SPAN sends a copy of traffic from source ports to a destination port where an analyzer listens. Packet analyzers, vulnerability scanners, DLP and antivirus feed the same picture, dashboards and network management systems summarize it, and orchestration and automated alerts act on it.

Exam tip: NetFlow shows who talked to whom, when and how much. A packet capture also shows what was said.

4.5 Identity and access management (scenario)

Provisioning creates accounts with the right permissions, and deprovisioning removes them promptly. Identity proofing establishes an identity with enough information, such as documents and credentials, before credentials are issued (FIPS 201-3).

Term	What it does
Federation	Conveys identity and authentication information across networked systems (FIPS 201-3)
SSO	One account and its authenticators reach multiple applications (SP 800-63-4)
SAML	An XML-based framework where an identity provider vouches for a user to a service provider (OASIS)
OAuth 2.0	An authorization framework giving a third-party app limited access to an HTTP service through access tokens (RFC 6749)
LDAP	Access to directory services based on X.500 models (RFC 4511); IANA port 389, and 636 for LDAPS

Account types carry different risk: user, privileged (global or local), service, third-party, and emergency access accounts kept for when normal administration fails, which are tightly controlled and monitored. MFA combines something you know, something you have and something you are (CNSSI 4009). Hard tokens are devices and soft tokens are apps; time-based one-time passwords use a default 30-second step (RFC 6238), and backup codes are single-use recovery codes.

Access model	How decisions are made
Mandatory (MAC)	A central authority decides, not the object's owner (NIST SP 800-192)
Discretionary (DAC)	The object's owner decides who gets which rights
Role-based (RBAC)	Permitted actions attach to roles, and people get roles
Rule-based	System-wide rules apply whoever the user is, as in firewall rules
Time-based	Access only within set hours or dates
Just-in-time	Temporary privileges granted when needed (Microsoft PIM)

NIST SP 800-63B-4 (July 2025) requires passwords used as the only factor to be at least 15 characters, and those used only within MFA at least 8. Verifiers should permit at least 64 characters, must not impose composition rules or periodic changes, must check new passwords against a blocklist of common, expected or compromised values, and must allow password managers and autofill. A change is still forced on evidence of compromise, which is what compromised credential monitoring looks for. The FIDO Alliance describes passkeys as phishing-resistant credentials that replace passwords with cryptographic key pairs.

Exam tip: SAML exchanges authentication assertions so a user signs in once; OAuth 2.0 grants an application limited access to resources on a user's behalf.

4.6 Automation and orchestration in security operations (scenario)

Scripts handle repeatable work: provisioning users and cloud resources, keeping systems at a desired state, flagging anomalies and managing tickets. Orchestration chains tasks across tools, such as an alert that triggers enrichment, containment and a ticket. Weigh the costs: guardrails, the quality of the logic and process being automated, complexity, money, process risk and deployment effort. A flawed process runs faster once automated.

The objective names agentic AI, chatbots, predictive analysis and AI-augmented baselines as AI capabilities. Objective 2.6 explains the risk: an agent that reads untrusted content can be steered by indirect prompt injection. The payoff is saved time, consistent baselines, continuous improvement, productivity, less downtime and a more proactive team. In SecOps, security checks run inside CI/CD pipelines, so code is tested each time it changes.

Exam tip: automation performs a task without a person; orchestration coordinates many automated tasks across systems.

4.7 Incident response activities

NIST's current guidance, SP 800-61 Rev. 3 (April 2025), places incident response inside risk management as described by Cybersecurity Framework 2.0, whose six functions are Govern, Identify, Protect, Detect, Respond and Recover (released February 26, 2024). The objective follows its own sequence:

Phase	Key activities
Preparation	Defined roles, playbooks, training, tabletop exercises, simulations
Identification	Detection, threat hunting, internal and external advisories
Investigation	Preserving evidence, forensics, chain of custody, e-discovery
Containment	Isolating or quarantining affected systems
Negotiation	Dealing with the attacker where unavoidable, with legal guidance
Eradication and recovery	Removing the cause, then restoring and monitoring
Notification	Customers, stakeholders, law enforcement, required reports
Post-incident	Root cause analysis, lessons learned, a written report

A tabletop exercise is a discussion-based exercise in which people with roles in a plan talk through a facilitator's scenario (NIST SP 800-84). Chain of custody tracks evidence through collection, safeguarding and analysis (NIST SP 800-72). Notification can be a legal duty: under the GDPR, a controller must notify the supervisory authority of a personal data breach within 72 hours of becoming aware of it, where feasible (Article 33).

Exam tip: containment stops the spread, and eradication removes the cause. Isolating an infected host is containment; reimaging it is eradication and recovery.

4.8 Using data and artifacts in an investigation (scenario)

Investigations draw on access logs, both logical (sign-ins) and physical (badge readers); logs from devices, servers, applications and endpoints; authentication, audit, communication and network logs; and metadata such as timestamps or email headers. Other sources include scan results, automated reports, NetFlow or IPFIX records, surveillance footage, security tool alerts, dashboards and packet captures. Hashing files and logs at collection proves later that they were not altered.

RFC 3227 orders collection from most to least volatile: registers and cache; routing table, ARP cache, process table, kernel statistics and memory; temporary file systems; disk; remote logging and monitoring data; physical configuration and network topology; archival media. So a memory dump comes before a bit-level copy of a drive, and a snapshot captures a virtual machine at a point in time. Log parsing turns raw logs into a timeline. HR, accounts (finance) and legal are stakeholders when an employee, money or evidence handling is involved.

Exam tip: collect the most volatile evidence first. Memory disappears at power-off; a disk does not.

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

Governance, risk, compliance and people, with security awareness (5.6) as the scenario objective.

5.1 Governance, risk and compliance documents

Document	Role	Examples
Policy	Mandatory intent and rules	Acceptable use, BYOD, privacy, clean desk, data retention and classification, access control, incident response, vulnerability disclosure, data disposal
Standard	Mandatory specifics	Password, encryption and physical security standards, baselines, RFCs
Procedure	Mandatory steps	SOPs, runbooks
Guideline	Recommended practice	Benchmarks, advisories, implementation guides, reference architectures
Plan	Prepared response	Business continuity, disaster recovery

Many internet standards are published as Requests for Comments, such as TLS 1.3 in RFC 8446, so an internal standard can point to an RFC rather than restate it. A runbook gives the steps for one operational task, often scripted.

Exam tip: policies say what and why, standards set mandatory specifics, procedures give the steps, and guidelines only recommend.

5.2 Risk management and its effect on security

Risk management identifies assets and owners, then assesses and analyzes each risk by likelihood, impact and current mitigations. NIST SP 800-30 Rev. 1 separates qualitative assessment, using nonnumerical categories or levels, from quantitative assessment, using numbers. A risk register is a repository of risk information over time. The risk responses are accepting, avoiding, mitigating, sharing or transferring risk, as with insurance.

A business impact analysis analyzes operational functions and the effect a disruption might have on them. Risk appetite is the types and amount of risk an organization will accept in pursuit of value, and residual risk is what remains after security measures. NIST IR 8286A describes the single loss expectancy (SLE) as the loss for each occurrence and the annualized loss expectancy (ALE) as the total loss over a year. With the annualized rate of occurrence (ARO) as expected occurrences per year, ALE is SLE multiplied by ARO: a $5,000 event expected three times a year has an ALE of $15,000.

Exam tip: if residual risk is above the risk appetite, more treatment is needed.

5.3 Assessing and managing third-party risk

Selection starts with a request for information (RFI), proposal (RFP) or quote (RFQ), or an expression of interest (EOI), followed by due diligence on the vendor's security and finances and a check for conflicts of interest.

Agreement	Purpose
SLA	Defines the provider's responsibilities and the customer's expectations (CNSSI 4009)
SLO	One measurable target, such as an uptime figure
MOU, MOA	Defined together by NIST as a statement of intent to work together, with terms and conditions (SP 800-47 Rev. 1)
NDA, MSA, SOW	Confidentiality; general terms for future work; the specific work and deliverables of one project

Monitoring uses a right-to-audit clause, service-level monitoring, a vendor registry, assessments, attestations and penetration tests. Constraints include staffing, jurisdiction, return on investment and vendor lock-in. Rules of engagement are detailed guidelines and constraints for security testing (NIST SP 800-115).

Exam tip: an SLA is the agreement; an SLO is one target inside it.

5.4 What effective security compliance includes

Compliance training covers data handling, anti-money laundering and counter-terrorism financing (AML/CTF) and anti-bribery. Monitoring collects attestations that controls are in place and acknowledgements that people read a policy. Non-compliance can bring reputational damage, fines, legal action, contract breaches, sanctions and loss of license. GDPR rights match the objective's privacy items: erasure, or the right to be forgotten (Article 17), rectification (Article 16) and restriction of processing (Article 18). Opt-in requires agreement first; opt-out processes unless someone objects. A legal hold preserves data for a legal matter and suspends its deletion, legal orders can compel data, and retention requirements set how long records are kept.

Exam tip: a legal hold overrides the normal retention schedule for the data it covers.

5.5 Audits and assessments

Reference model	Structure
MITRE ATT&CK	Knowledge base of adversary tactics (the "why") and techniques, based on real-world observations
Cyber Kill Chain	Seven steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives
Diamond Model	Four core features of every intrusion event: adversary, infrastructure, capability, victim

Auditors gather evidence by sampling, questionnaires, interviews and assertions, scoped by an audit charter and a set frequency. Engagements range from gap analysis and internal self-assessments to external examinations, regulatory audits and independent third-party audits. Penetration testing, per NIST SP 800-53, means assessors attempt to circumvent or defeat a system's security features. Testers get full information in a known environment, none in an unknown one, and some in a partially known one. Passive reconnaissance gathers information without touching the target; active reconnaissance, such as port scanning, interacts with it.

Standards come in three scopes: industry (PCI DSS, a baseline of requirements to protect payment account data), international (ISO/IEC 27001, which specifies an information security management system, per Microsoft Learn) and regional (the EU's GDPR). Functional testing checks that a control works; behavioral testing checks what people actually do, as in a phishing simulation.

Exam tip: ATT&CK catalogs individual techniques, the Kill Chain is a sequence of stages, and the Diamond Model analyzes one event by its four features.

5.6 Applying security awareness (scenario)

Training is initial, ongoing, targeted at higher-risk roles, or corrective after a failure, delivered through a learning management system, self-service portals, one-to-one or one-to-many sessions. Effectiveness is measured with metrics, managerial reports and personnel behavior risk scoring; NIST SP 800-50 Rev. 1 (September 2024) says a learning program should encourage behavior change and suggests metrics. Topics include social engineering, deepfakes, credentials, remote work, BYOD, removable media and business email compromise, which the FBI describes as a sophisticated scam targeting people who perform legitimate transfer-of-funds requests; it reported $55,499,915,582 in exposed losses from October 2013 to December 2023.

Exam tip: corrective training follows a specific failure; targeted training goes to higher-risk roles before anything goes wrong.

A study plan

Here is an example six-week plan built from the domain weights. Treat it as a template to adjust: CompTIA's V8 page lists recommended experience but no study time, so the right pace depends on background and practice results. Domains 2 and 4 together make up 51 percent of the exam, so they get the most time.

Week	Focus	Weight
1	Domain 1	16%
2	Domain 2, objectives 2.1 to 2.4	24%
3	Objectives 2.5 and 2.6, then Domain 3 through 3.2	24% and 19%
4	Objectives 3.3 and 3.4, then Domain 4 through 4.3	19% and 27%
5	Objectives 4.4 to 4.8	27%
6	Domain 5, then timed practice exams and weak spots	14%

Give the nine scenario objectives (1.2, 2.5, 3.2, 4.1, 4.3, 4.5, 4.6, 4.8 and 5.6) hands-on time: read real logs, set up MFA on a test account, write a firewall rule. A free cloud account or a few virtual machines are enough. Test each week's objectives as they are finished, and mix all five domains under time pressure in the final week.

Practice questions

Security+ Practice Test: ET for iPhone and iPad has 1,000 original SY0-801 practice questions spread across the five domains in proportion to their weights (160, 240, 190, 270 and 140 questions), with an explanation for every answer. It is free to start with 30 sample questions and needs no account. Every question is written to the SY0-801 exam objectives and checked in a separate review against primary sources such as NIST, IETF, CISA and MITRE. 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. Candidates get 90 minutes, according to CompTIA's Security+ V8 page.

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

750 on a scale of 100 to 900, according to CompTIA.

When does SY0-801 launch and when does SY0-701 retire?

CompTIA expects to launch SY0-801 on or around November 17, 2026. The English SY0-701 exam retires on June 11, 2027, and its Japanese, Portuguese, Spanish and Thai versions on August 13, 2027, according to CompTIA's Security+ V7 page.

What are the Security+ SY0-801 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, counted from CompTIA's exam objectives document. Nine of them begin with "Given a scenario", which means they test applying knowledge to a situation rather than recognizing a term.

How much experience do you need for Security+?

CompTIA recommends two years of hands-on experience as a security administrator. Its V8 page lists that as recommended experience and gives no study time, so how long preparation takes depends on background.

Does Security+ SY0-801 cover AI?

Yes. Objective 2.6 covers threats and vulnerabilities that come with AI, and objective 4.6 covers AI capabilities in security operations. AI also appears in 2.4, which lists large language models as an attack surface, and 2.5, which lists deepfakes.

Sources

- CompTIA: Security+ V8 (SY0-801) and exam objectives document version 2.0, Security+ V7 (SY0-701)
- NIST CSRC glossary: confidentiality, integrity, availability, non-repudiation, least privilege, defense in depth, symmetric key algorithm, asymmetric cryptography, hash function, salt, roots of trust, key escrow, TPM, threat, CVE, APT, attack surface, zero day attack, trojan horse, worm, virus, spyware, rootkit, logic bomb, denial of service, jailbreak, prompt injection, air gap, fail secure, DLP, de-identification, information owner, data steward, hot site, warm site, cold site, RTO, RPO, honeypot, SIEM, identity proofing, federation, SSO, MFA, MAC, DAC, RBAC, tabletop exercise, chain of custody, qualitative and quantitative assessment, risk register, risk response, BIA, risk appetite, residual risk, SLA, MOU/A, rules of engagement, penetration testing
- NIST publications: SP 800-207, FIPS 197, FIPS 186-5, Hash Functions project, SHA-1 retirement, AI 100-2 E2025, AI 600-1, SP 800-145, SP 800-204, SP 800-94, SP 800-41 Rev. 1, SP 800-88 Rev. 2, SCAP, SP 800-63B-4, SP 800-61 Rev. 3, CSF 2.0 release, IR 8286A, SP 800-50 Rev. 1

- RFC Editor: RFC 8446, 8996, 6151, 2986, 9525, 5280, 6960, 4033, 4301, 3748, 2865, 8952, 6265, 7208, 6376, 9989, 3954, 7011, 3414, 5424, 6749, 4511, 6238, 3227; IETF BIMI Internet-Draft
- IANA port registry: ldap, snmp, syslog, ipfix
- MITRE: CWE-367, CWE-798, CWE-89, CWE-120, CWE-22, CWE-352, CWE-918, CWE-20, ATT&CK, T1110.003, T1621
- CISA: KEV catalog, living off the land guidance, ransomware guide, disclosure policy template
- Other standards bodies: FIRST CVSS v4.0, IEEE 802.1X, OASIS SAML, FIDO Alliance passkeys, CIS Benchmarks, PCI SSC PCI DSS, glossary and tokenization guidelines
- Microsoft Learn: Global Secure Access, gMSA, Intune, Azure WAF, Defender XDR, Group Policy, IPAM, CSPM, PIM, ISO/IEC 27001
- Vendor and project documentation: AWS Lambda, Cisco SPAN, GitHub secret scanning, SELinux Notebook, Lockheed Martin Cyber Kill Chain, The Diamond Model of Intrusion Analysis
- Law and government: GDPR, Executive Order 13526, FBI IC3 business email compromise announcement

Last checked: November 2026.

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-study-guide/