VPWEB.DEV · STUDY PLAN

CompTIA Security+

Exam SY0-701

Security+ is the most career-defining of the core CompTIA certs: it satisfies the U.S. DoD 8140 baseline and opens the door to analyst and SOC roles. It is one exam (SY0-701) and leans heavily on scenarios — knowing definitions is not enough; you must know when and why a control applies. Everything hangs off the CIA triad.

Exam at a glance

EXAM	One — SY0-701
PASSING SCORE	750 / 900 (scale 100–900)
LENGTH	Up to 90 questions, 90 minutes
QUESTION TYPES	Multiple choice + performance-based (PBQs)
COST (APPROX.)	·$404 USD voucher — check CompTIA for current pricing
VALIDITY	Good for 3 years; renew with CE
RECOGNITION	Meets U.S. DoD 8140 / 8570 baseline for many cyber roles
BEST FOR	Security analyst, SOC analyst, junior security engineer

Every domain, in depth

DOMAIN 1 — 12%

General Security Concepts

The foundation everything else builds on — controls, principles, change, crypto.

- Control categories: technical, managerial, operational, physical
- Control types: preventive, deterrent, detective, corrective, compensating, directive
- Fundamentals: CIA triad, AAA, non-repudiation, zero trust, defense in depth
- Physical security and deception/disruption (honeypots, honeytokens)
- Change management: process, approvals, backout plans, documentation
- Cryptography: symmetric vs asymmetric, hashing, digital signatures, PKI, certificates

DOMAIN 2 — 22%

Threats, Vulnerabilities & Mitigations

Know your enemy: actors, attack surfaces, weaknesses, and how to mitigate.

- Threat actors & motivations: nation-state, insider, hacktivist, organized crime, script kiddie
- Attack vectors & surfaces: message-based, supply chain, removable media, default credentials
- Vulnerabilities: application (buffer overflow, race condition), web (XSS, SQLi), OS, cloud, zero-day
- Malicious activity & indicators: malware types, DoS, on-path, password attacks, IoCs
- Mitigation: segmentation, access control, patching, hardening, isolation, least privilege

DOMAIN 3

18%

Security Architecture

Designing secure systems and protecting data across environments.

- Architecture models: cloud, serverless, microservices, IaC, on-prem, virtualization, IoT/ICS/SCADA
- Enterprise infrastructure: secure design, device placement, firewalls, IDS/IPS, network appliances
- Data protection: classification, states (at rest / in transit / in use), encryption, DLP, tokenization
- Resilience & recovery: backups, redundancy, high availability, capacity planning, testing

DOMAIN 4

28%

Security Operations

The heaviest domain — the day-to-day work of defending an organization.

- Secure baselines & hardening across devices, mobile, cloud, and apps
- Asset & vulnerability management: scanning, CVSS, remediation, validation
- Monitoring & alerting: SIEM, SNMP, NetFlow, log aggregation, SCAP
- Enterprise capabilities: firewalls, IDS/IPS, web/DNS filtering, email security, EDR
- Identity & access management: provisioning, MFA, SSO, federation, privileged access
- Automation & orchestration (SOAR); incident response lifecycle; digital forensics

DOMAIN 5

20%

Security Program Management & Oversight

Governance, risk, compliance, and the human element.

- Governance: policies, standards, procedures, roles, regulatory frameworks
- Risk management: identification, assessment (qualitative/quantitative), appetite, treatment
- Third-party / vendor risk: assessments, SLAs, right-to-audit, supply chain
- Compliance & privacy: GDPR, PCI DSS, audits, attestations, consequences
- Security awareness: training, phishing simulations, reporting, anomalous behavior

Week-by-week study plan

Week 1 General security concepts	• CIA triad, AAA, zero trust • Control categories and types (memorize both) • Change management process
Week 2 Threats & vulnerabilities	• Threat actors and motivations • Attack types and vectors • Vulnerability classes and indicators
Week 3 Cryptography	• Symmetric vs asymmetric vs hashing • PKI, certificates, digital signatures • Where each is used (TLS, signing, storage)
Week 4 Security architecture	• Cloud, IaC, microservices, IoT/ICS • Data classification and states • Resilience, redundancy, recovery
Week 5 Security operations	• Hardening, vuln management, SIEM/monitoring • IAM, MFA, SSO, federation • Incident response lifecycle + forensics

Weeks 6–7
Governance & exam

- Risk management, compliance, vendor risk
- Scenario-based PBQ practice
- Practice exams to ≥ 90%, then book SY0-701

Cheat sheets

CORE PRINCIPLES

CIA triad	Confidentiality · Integrity · Availability
AAA	Authentication · Authorization · Accounting
Non-repudiation	Proof an action occurred and who did it
Zero trust	Never trust, always verify — every request authenticated

CONTROL CATEGORIES & TYPES

Categories	Technical · Managerial · Operational · Physical
Types	Preventive · Deterrent · Detective · Corrective · Compensating · Directive

CRYPTOGRAPHY

Symmetric	One shared key — fast, bulk data (AES, ChaCha20, 3DES)
Asymmetric	Public/private key pair (RSA, ECC, Diffie-Hellman)
Hashing	One-way integrity check (SHA-256, SHA-3; avoid MD5/SHA-1)
PKI	CA, certificates, digital signatures, key escrow, OCSP/CRL

COMMON ATTACKS

ATTACK	WHAT IT IS
Phishing	Fraudulent message to steal data/credentials
On-path	Attacker intercepts traffic between two parties
SQL injection	Malicious SQL via input fields
XSS	Injecting scripts into trusted web pages
DDoS	Overwhelming a service from many sources
Privilege escalation	Gaining higher access than authorized

INCIDENT RESPONSE LIFECYCLE

1. Preparation
2. Detection & analysis (identification)
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

Acronyms to know

CIA
Confidentiality, Integrity, Availability

AAA
Authentication, Authorization, Accounting

PKI
Public Key Infrastructure

CA
Certificate Authority

MFA
Multi-Factor Authentication

SSO
Single Sign-On

IAM
Identity and Access Management

SIEM
Security Information and Event Management

SOAR
Security Orchestration, Automation and Response

EDR
Endpoint Detection and Response

DLP
Data Loss Prevention

IDS/IPS
Intrusion Detection / Prevention System

CVSS
Common Vulnerability Scoring System

IoC
Indicator of Compromise

RTO
Recovery Time Objective

RPO
Recovery Point Objective

GDPR
General Data Protection Regulation

PCI DSS
Payment Card Industry Data Security Standard

SCADA
Supervisory Control and Data Acquisition

TLS
Transport Layer Security

Recommended resources

- **Professor Messer** — free, complete video course covering every objective. Start here.

- **Practice exams** — the one paid resource worth buying; drill to a consistent 90% on fresh questions before booking (Jason Dion's are a community favorite).
- **Official CompTIA objectives PDF** — the literal exam blueprint; use it as your master checklist.
- **Hands-on labs** — VMs, a home lab, and real devices make concepts stick far better than reading alone.
- **Flashcards (Anki)** — for ports, acronyms, commands, and definitions via active recall.

The winning formula: follow the objectives top to bottom, get hands-on, and don't book the exam until you're consistently scoring 90%+ on fresh practice tests. For the full written walkthrough and career guidance, visit **vpweb.dev/blog**.