

CompTIA Security+ 30-Day Study Plan (SY0-701)

A focused 30-day roadmap to pass CompTIA Security+ — built around the five SY0-701 domains, weighted so your hours go where the exam puts its points, and finished with full timed mocks.

90 MAX QUESTIONS	90 min TIME LIMIT	750 PASSING SCORE (100-900)	5 EXAM DOMAINS
----------------------------	-----------------------------	---------------------------------------	--------------------------

Days 1-5

FOUNDATION

General Security Concepts (12%)

Lock in the vocabulary everything else builds on: security controls, the CIA triad, AAA, zero trust, physical security, change management, and the cryptography basics behind PKI.

- Learn control categories and types (technical, managerial, operational, physical)
- Compare symmetric vs asymmetric encryption, hashing, salting and digital signatures
- Take the domain mini-exam and review every miss

Days 6-11

KNOW THE ENEMY

Threats, Vulnerabilities & Mitigations (22%)

Recognise threat actors and their motivations, attack vectors, malware types, and network, application and password attacks — then match each one to the right mitigation.

- Build a one-page cheat sheet of attack types and their indicators
- Practise scenario questions that ask for the BEST mitigation
- Drill social engineering and application attacks (injection, XSS, overflow)

Days 12-16

DESIGN

Security Architecture (18%)

Understand how architecture choices change risk: cloud and on-prem models, network segmentation and secure infrastructure, data protection, and resilience and recovery.

- Compare cloud models and their shared-responsibility splits
- Review data states, classification, and protection methods
- Know backup types, site resilience, and RTO / RPO

Days 17-23

BIGGEST DOMAIN

Security Operations (28%)

The largest share of the exam: hardening, asset and vulnerability management, monitoring and alerting, identity and access management, automation, incident response, and investigations.

- Walk through the incident response process in order
- Practise reading log and alert scenarios
- Review IAM: MFA, SSO, federation, and least privilege

Days 24-27

OVERSIGHT

Security Program Management & Oversight (20%)

Cover governance, risk management, third-party risk, compliance, audits and assessments, and security awareness — the questions that reward reading the scenario carefully.

- Learn the risk terms: appetite, tolerance, register, and the risk-handling options
- Review vendor assessment and agreement types (SLA, MOU, MSA, NDA)
- Take a mixed-domain timed quiz

Days 28-30

EXAM READY

Full Mocks & Weak-Area Review

Sit full-length timed mocks under real conditions (up to 90 questions including performance-based items, 90 minutes). Review every wrong answer and re-drill your weakest domain until you clear 750 with room to spare.

- Two full timed mock exams
- Re-take your weakest domain mini-exam
- Light review the day before — then rest

Adjust the pace to your schedule — the key is consistent daily practice and reviewing every question you miss. Practise free at <https://www.examgrit.com/comptia-security-plus/practice-test>