CompTIA Security+ (SY0-701)

Independent Course Syllabus & Comprehensive Study Blueprint

EXAM CODE	TIME LIMIT	QUESTION COUNT	PASSING SCORE
SY0-701	90 Minutes	Maximum of 90 Questions	750 (Scale 100–900)

Recommended Prerequisites: CompTIA Network+ and 2 years hands-on experience in security/systems administration recommended.

Curriculum Blueprint & Domain Breakdown

Official Blueprint Weighted Distribution

1.0 General Security Concepts — 12%

- Compare and contrast security control types (Technical, Managerial, Operational, Physical, Detective, Preventative)
- Fundamental security concepts (CIA Triad, Non-repudiation, Authenticity, Zero Trust Architecture)
- Change management processes, cryptographic algorithms, PKI, and key management

2.0 Threats, Vulnerabilities, and Mitigations — 22%

- Threat actors, vectors, and motivations (Nation-state, Hacktivists, Insiders, Supply chain)
- Vulnerability classifications (Hardware, Software, Firmware, Misconfigurations, Zero-day)
- Indicators of malicious activity (Ransomware, Social Engineering, XSS, SQLi, Buffer Overflows)
- Mitigation strategies, vulnerability management lifecycles, and attack surface reduction

3.0 Security Architecture — 18%

- Zero Trust architecture, enterprise security models, and defense-in-depth principles
- Securing multi-cloud, hybrid, and on-premises enterprise environments
- Network segmentation, microsegmentation, SASE, and ZTNA
- Data protection: Data classification, DLP, tokenization, and encryption at rest and in transit
- High availability, disaster recovery, and resilience engineering

4.0 Security Operations — 28%

- Identity and access management (IAM), MFA, PAM, and federated identity
- Vulnerability scanning, SIEM, SOAR, EDR, and centralized logging analysis
- Incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery)
- Digital forensics investigation, chain of custody, and forensic evidence acquisition

5.0 Security Program Management and Oversight

20%

- Security governance frameworks (NIST CSF, ISO/IEC 27001, CIS Critical Security Controls)
- Risk management processes, risk scoring, risk registers, and qualitative vs quantitative analysis
- Third-party risk management and vendor assessment protocols
- Compliance requirements, legal standards, and data privacy frameworks (GDPR, HIPAA, PCI DSS)

Recommended 8–10 Week Study Milestone Plan

Structured Self-Paced Schedule

WEEKS 1–2

Domain 1.0 & 2.0: Core Security Concepts, Cryptography, Threat Actor Profiling

WEEKS 3–4

Domain 3.0: Cloud Architecture, Network Segmentation & Zero Trust Models

WEEKS 5–6

Domain 4.0: Hands-On Security Operations, SIEM/EDR Analysis & Incident Drills

WEEK 7

Domain 5.0: Governance, Compliance, Risk Management & Third-Party Oversight

WEEK 8

Full-Length Practice Simulators, Performance-Based Question (PBQ) Drills

DISCLAIMER & INDEPENDENT TRAINING NOTICE: DISCLAIMER & INDEPENDENT TRAINING NOTICE: This syllabus is an independent educational publication and study guide produced by ITCertifa (itcertifa.com). CompTIA® and CompTIA Security+® are registered trademarks of the Computing Technology Industry Association, Inc. ITCertifa is an independent training provider and is not affiliated with, endorsed by, authorized by, or sponsored by CompTIA. Official exam objectives and certification blueprints are maintained exclusively by CompTIA.