



TECH VISIONS

— CONSULTING & TRAINING —



BUILDING CAPABILITY. STRENGTHENING SECURITY.

COURSE OUTLINE | EXAM SY0-701

CompTIA Security+



General Security
Concepts



Threats, Vulnerabilities
& Mitigations



Security
Architecture



Security
Operations



Program Management
& Oversight

CompTIA Security+ Certification

Exam SY0-701 | Assess, protect and respond.



COURSE OVERVIEW

CompTIA Security+ is a globally recognized certification that validates the baseline skills needed to perform core security functions and pursue an IT security career. You will be assessed on your abilities to assess the security posture of an enterprise, monitor and secure hybrid environments (cloud, mobile, IoT and operational technology), identify and respond to security events and incidents, and apply governance, risk and compliance practices. This certification prepares you for jobs in security administration, systems administration and security operations.

BENEFITS OF THE COURSE



Solid security foundations

Master the CIA triad, zero trust, security controls and cryptography, the base every security role builds on.



Threats & vulnerabilities

Recognize threat actors, attack vectors and indicators of malicious activity, and apply the right mitigations.



Secure architecture

Design and secure cloud, on-premises and hybrid infrastructure with segmentation, resilience and data protection.



Security operations

Monitor systems, manage vulnerabilities and identities, and respond to security incidents with confidence.



Governance, risk & compliance

Understand policies, risk management, third-party risk, audits and security awareness programs.



Recognized credential

Earn a vendor-neutral certification that maps to real cybersecurity and IT security job roles.

TARGET AUDIENCE



Security Administrators



Systems Administrators



Junior Security Analysts



SOC Analysts



Network Administrators



IT Support Specialists



Aspiring Cybersecurity Professionals



IT Students & Career Changers

Five domains, 28 modules

Built on the official SY0-701 exam objectives.



01

General Security Concepts

12% of exam

The foundation of every security role: the types of security controls, core security concepts, change management and the cryptographic solutions that protect data.

MODULES

- 01 Security control types & categories
- 02 Fundamental security concepts
- 03 Change management & its security impact
- 04 Cryptographic solutions

You will be able to: explain core security principles and choose the right controls and cryptography for a given scenario.



02

Threats, Vulnerabilities & Mitigations

22% of exam

Know your enemy: who attacks, how they get in, what weaknesses they exploit, how to spot the signs and which mitigations stop them.

MODULES

- 05 Threat actors & motivations
- 06 Threat vectors & attack surfaces
- 07 Types of vulnerabilities
- 08 Indicators of malicious activity
- 09 Mitigation techniques to secure the enterprise

You will be able to: identify threats and vulnerabilities, analyze indicators of compromise and apply effective mitigations.



03

Security Architecture

18% of exam

Designing secure environments: cloud, on-premises and hybrid models, secure infrastructure, data protection and resilient, recoverable systems.

MODULES

- 10 Architecture models & security implications
- 11 Securing enterprise infrastructure
- 12 Data protection concepts & strategies
- 13 Resilience & recovery in security architecture

You will be able to: apply security principles to enterprise infrastructure, protect data and plan for resilience and recovery.

Operate, then govern

Course outline continued: domains 04 and 05.



04

Security Operations

28% of exam

The heaviest domain: hardening and managing assets, vulnerability management, monitoring, identity and access management, automation and incident response.

MODULES

- 14 Security techniques for computing resources
- 15 Hardware, software & data asset management
- 16 Vulnerability management
- 17 Security alerting & monitoring tools
- 18 Modifying capabilities to enhance security
- 19 Identity & access management
- 20 Automation & orchestration
- 21 Incident response activities
- 22 Data sources for investigations

You will be able to: monitor and harden systems, manage identities and vulnerabilities, and respond to security incidents.



05

Program Mgmt & Oversight

20% of exam

Running security as a program: governance, risk management, third-party risk, compliance, audits and security awareness practices.

MODULES

- 23 Elements of security governance
- 24 The risk management process
- 25 Third-party risk assessment & management
- 26 Security compliance
- 27 Audits & assessments
- 28 Security awareness practices

You will be able to: support governance, risk and compliance programs and build a security-aware organization.

HANDS-ON LAB FOCUS



Security controls

Configure firewalls, access controls and hardening settings in lab environments.



Log & traffic analysis

Investigate events with logs, SIEM concepts, Wireshark and command-line tools.



Vulnerability scanning

Find, prioritize and remediate weaknesses using scanning and assessment tools.



PBQ-style scenarios

Solve hands-on security scenarios just like the real exam.

The Security+ exam

Everything you need to know before exam day.

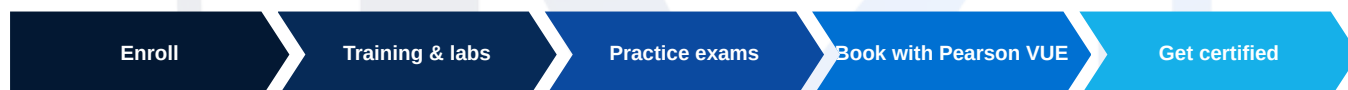


ITEM	DETAILS
Certification	CompTIA Security+
Exam code	SY0-701
Number of questions	Maximum of 90
Question types	Multiple choice and performance-based
Duration	90 minutes
Passing score	750 (on a scale of 100–900)
Exam delivery	Pearson VUE: test center or online (OnVUE)

DOMAIN WEIGHTING

12%	22%	18%	28%	20%
General Security Concepts	Threats, Vulnerabilities & Mitigations	Security Architecture	Security Operations	Program Mgmt & Oversight

YOUR PATH TO CERTIFICATION



Ready to build a rock-solid foundation in cybersecurity?

EMAIL training@thetechvisions.com
 WEB thetechvisions.com