COMPTIA SECURITY+ SY0-701 TRAINING CONTENT

Cyber Xperts

Instructor: Rajendra N

Website: https://cyberxperts.pro/

Email: rajendra.n@cyberxperts.pro

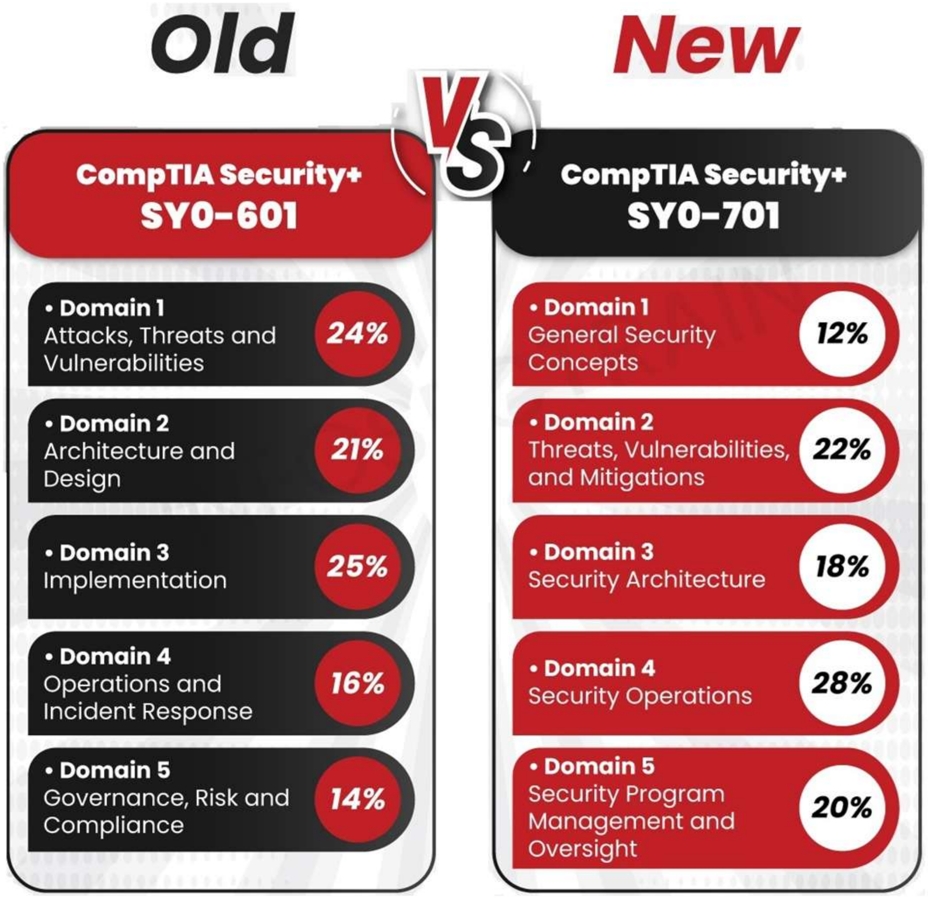
Phone: +44 7436906066

LinkedIn: https://www.linkedin.com/in/rajendra-n-75999348/

Location: Newbury Park, Essex, UK, IG27HR

Institute: Cyber Xperts

Cyber Xperts



CompTIA Security+ SY0-601		CompTIA Security+ SY0-701	
• **Domain 1** Attacks, Threats and Vulnerabilities	24%	• **Domain 1** General Security Concepts	12%
• **Domain 2** Architecture and Design	21%	• **Domain 2** Threats, Vulnerabilities, and Mitigations	22%
• **Domain 3** Implementation	25%	• **Domain 3** Security Architecture	18%
• **Domain 4** Operations and Incident Response	16%	• **Domain 4** Security Operations	28%
• **Domain 5** Governance, Risk and Compliance	14%	• **Domain 5** Security Program Management and Oversight	20%

CompTIA Security+ Training

- Prepares individuals for the certification exam by covering core cybersecurity skills like network security, risk management, threat and vulnerability management, and security operations.

COMPTIA SECURITY + EXAM OBJECTIVES SUMMARY

01	General Security Concepts (12%)
02	Threats, Vulnerabilities, and Mitigations (22%)
03	Security Architecture (18%)
04	Security Operations (28%)
05	Security Program Management & Oversight (20%)

01 - General Security Concepts (12%)

Security Controls	Types: Technical, preventive, managerial, deterrent, operational, detective, physical, corrective, compensating, directive. Purpose: Each control type addresses different aspects of risk management, from preventing incidents to detecting and correcting them.
Fundamental Concepts	CIA Triad: Confidentiality, Integrity, Availability—core principles of information security. Non-repudiation: Ensures actions or transactions cannot be denied. AAA: Authentication, Authorization, Accounting—managing user identities and access. Zero Trust: Security model assuming no implicit trust; verifies every access. Deception/Disruption Technology: Tools and techniques to mislead attackers or disrupt malicious activities.
Change Management	Business Processes: How changes are proposed, approved, and implemented. Technical Implications: Impact on systems, security, and operations. Documentation & Version Control: Tracking changes for accountability and rollback.

Cryptographic Solutions	PKI: Public Key Infrastructure for secure communications. Encryption, Obfuscation, Hashing: Protecting data confidentiality and integrity. Digital Signatures: Verifying authenticity and integrity. Blockchain: Distributed ledger technology for secure transactions.
Fundamental Concepts	CIA Triad: Confidentiality, Integrity, Availability—core principles of information security. Non-repudiation: Ensures actions or transactions cannot be denied. AAA: Authentication, Authorization, Accounting—managing user identities and access. Zero Trust: Security model assuming no implicit trust; verifies every access. Deception/Disruption Technology: Tools and techniques to mislead attackers or disrupt malicious activities.

01 - GENERAL SECURITY CONCEPTS (12%)

2. Threats, Vulnerabilities, and Mitigations (22%)

Threat Actors & Motivations	Types: Nation-states, unskilled attackers, hacktivists, insiders, organized crime, shadow IT. Motivations: Data theft, espionage, financial gain.
Threat Vectors & Attack Surfaces	Examples: Message-based, unsecure networks, social engineering, file-based, voice call, supply chain, vulnerable software.
Vulnerabilities	Areas: Application, hardware, mobile, virtualization, OS, cloud, web, supply chain.
Malicious Activity	Types: Malware, password attacks, application attacks, physical attacks, network attacks, cryptographic attacks.
Mitigation Techniques	Methods: Segmentation, access control, configuration enforcement, hardening, isolation, patching.

3. Security Architecture (18%)

Architecture Models	Comparisons: On-premises, cloud, virtualization, IoT, ICS, Infrastructure as Code (IaC).
Enterprise Infrastructure	Principles: Secure design, control selection, secure communication/access.
Data Protection	Methods: Data classification, anonymization, securing different data types.
Resilience & Recovery	Topics: High availability, site considerations, testing, backups, continuity planning.

4. Security Operations (28%)

Computing Resources Practices	Practices: Secure baselines, mobile/wireless/app security, sandboxing, monitoring.
Asset Management	Lifecycle: Acquisition, disposal, assignment, tracking of assets.
Vulnerability Management	Process: Identification, analysis, remediation, validation, reporting.
Alerting & Monitoring	Tools: SIEM, monitoring endpoints, automation/orchestration.
Enterprise Security	Controls: Firewalls, IDS/IPS, DNS filtering, DLP, NAC, EDR/XDR
Identity & Access Management	Techniques: Provisioning, SSO, MFA, privileged access.
Automation & Orchestration	Benefits: Efficiency, consistency, reduced human error.
Incident Response	Steps: Preparation, detection, containment, eradication, recovery, post-incident analysis.
Data Sources	Usage: Log data and other sources for investigations.

5. Security Program Management & Oversight (20%)

Security Governance	Elements: Guidelines, policies, standards, procedures, governance structures, roles.
Risk Management	Process: Identification, assessment, analysis, register, tolerance, appetite, strategies, reporting, BIA.
Third-Party Risk	Management: Vendor assessment, selection, agreements, monitoring.
Security Compliance	Reporting: Compliance monitoring, consequences, privacy.
Audits & Assessments	Types: Attestation, internal/external audits, penetration testing.
Security Awareness	Training: Phishing, anomalous behaviour, user guidance, reporting.

Career & Certification

Introduction

Comprehensive, globally recognized cybersecurity training for real-world defense, mapped to the latest CompTIA Security+ SY0 701) objectives.

How to Advance Your Career

Get Certified: Security+ certification is globally recognized and valued in cybersecurity roles.

Training & Bundles: Explore official training, practice exams, and bundled offers to prepare effectively.

About the Security+ Exam

Exam Code: SY0 701

Format: 90 minutes, multiple-choice & performance-based Max Questions: 90

Passing Score: 750/900

Experience: 2 years in IT admin recommended

Course Content

1. The Security+ Exam

- The Security+ exam
- Careers in information security
- The value of certification
- Stackable certifications   Study resources

2. Inside the Security+ Exam

- In-person exam environment
- At-home testing
- Security+ question types
- Passing the Security+ exam

3. Preparing for the Exam

- Exam tips
- Practice tests
- Continuing education requirements

Course Content

4. Domain 1: General Security Concepts

- General security concepts

5. Fundamental Security Concepts

- The goals of information security
- Authentication, authorization, and accounting AAA
- Categorizing security controls
- Conducting a gap analysis Zero Trust
- Physical access control
- Physical security personnel Deception technologies
- Change management

6. Preparing for the Exam

- Exam tips
- Practice tests
- Continuing education requirements

Course Content

7. Symmetric Cryptography

- Data Encryption Standard DES
- 3DES
- AES, Blowfish, and Twofish
- Steganography

8. Asymmetric Cryptography

- Rivest, Shamir, Adleman RSA
- PGP and GnuPG
- Elliptic-curve and quantum cryptography
- Tor and perfect forward secrecy

9. Key Management

- Key exchange
- Diffie-Hellman
- Key escrow
- Key stretching
- Hardware security modules

Course Content

10. Public Key Infrastructure

- Trust models
- PKI and digital certificates
- Hash functions
- Digital signatures
- Digital signature standard
- Creating and revoking digital certificates
- Certificate stapling
- Certificate authorities
- Certificate subjects, types, and formats

11. Cryptographic Applications

- TLS and SSL
- Blockchain

12. Domain 2: Threats, Vulnerabilities, and Mitigations

- Threats, vulnerabilities, and mitigations

Course Content

13. Understanding Vulnerability Types

- Vulnerability impact
- Supply chain, configuration, and architectural vulnerabilities

14. Malware

- Comparing viruses, worms, and trojans
- Malware payloads
- Understanding backdoors and logic bombs
- Advanced malware
- Botnets
- Malicious script execution

15. Understanding Attackers

- Cybersecurity adversaries
- Attacker motivations
- Preventing insider threats
- Attack vectors
- Zero-day attacks

Course Content

16. Social Engineering Attacks

- Social engineering
- Impersonation attacks Identity fraud and pretexting
- Watering hole attacks
- Physical social engineering
- Business email compromise
- Misinformation and disinformation

17. Password Attacks

- Password attacks
- Password spraying and credential stuffing

18. Application Attacks

- Preventing SQL injection
- Understanding cross-site scripting
- Request forgery
- Overflow attacks
- Cookies and attachments Session hijacking
- Code execution attacks Privilege escalation
- OWASP Top Ten
- Application security
- Directory traversal defense
- Race condition vulnerabilities

Course Content

19. Cryptanalytic Attack

- Brute force
- Knowledge-based attacks
- Encryption limitations

20. Network Attacks

- Denial-of-service
- Eavesdropping, DNS, wireless, and propagation attacks
- Rogue/evil twins
- Disassociation, Bluetooth, and RFID security

21. Attack Indicators

- Attack indicators

Course Content

22. Domain 3: Security Architecture

- Security architecture fundamentals

23. Cloud Computing

- Cloud basics
- roles
- multi-tenancy and security service providers

24. Virtualization

- Server, desktop, and app virtualization

Course Content

25. Cloud Building Blocks

- Computer, storage, networking, databases, orchestration, containers, SOA, microservices

26. Cloud Activities

- Reference architectures, deployment models, service categories
- Privacy, security, sovereignty, and operational concerns

27. Cloud Security Controls

- Firewalls
- App security
- Provider controls

Course Content

28. TCP/IP Networking

- TCP/IP
- IP addressing
- DHCP
- DNS
- Ports
- ICMP

29. Secure Network Design

- Security zones, VLANs, segmentation, device placement, SDN

30. Network Security Devices

- Routers, switches, bridges, firewalls, WAFs, proxies, load balancers, VPNs, IDS/IPS, analyzers, UTM, failure modes

Course Content

31. Network Security Techniques

- Restricting access, NAC, router/switch security, monitoring, SNMP, isolation, zero trust, SASE

32. Embedded Systems Security

- ICS, IoT, smart device networking, embedded systems

33. Data Protection

- Data security, types, anonymization, obfuscation, classification

Course Content

34. Resilience and Recovery

- BC/DR, high availability, backups, restores, DR sites, testing, planning

35. Domain 4: Security Operations

- Security operations processes

36. Data Security Controls

- Baselines, industry standards, customization

Course Content

37. Host Security

- OS & malware prevention, application management, integrity monitoring, DLP, encryption, hardware/firmware, Linux permissions, web content filtering

38. Configuration Enforcement

- Change/configuration/asset management, disposal/decommissioning

39. Mobile Device Security

- Connections, MDM, tracking, app security, enforcement, BYOD, deployment models

Course Content

40. Wireless Networking

- Wireless theory, encryption, authentication, RADIUS, propagation, equipment

41. Code Security

- Review, software testing, fuzzing, acquisitions, monitoring

42. Threat Intelligence

- Collection, sharing, hunting

Course Content

43. Vulnerability Management

- Managing cycles, scan targets, configs, perspectives, SCAP, CVSS, analyzing/correlating/reporting/remediation

44. Penetration Testing and Exercises

- Testing, responsible disclosure, bug bounties

45. Security Alerting, Monitoring, and Automation

- Logging, SIEM, monitoring, including endpoints, automation/orchestration

Course Content

46. Secure Protocols

- TLS, SSL, IPSec, DNS/email security, gateways

47. Identification

- ID/auth/accounting, usernames, access cards, biometrics, proofing

48. Authentication

- Factors, MFA, tokens, password policy/less/auth managers, SSO/federation, Kerberos, LDAP, SAML, OAuth, OpenID, certificate auth

Course Content

49. Authorization

- Concepts, MAC, DAC, ACLs, advanced models

50. Account Management

- Privilege/account management, provisioning, deprovisioning

51. Incident Response

- Program building, identification, escalation, mitigation, containment, eradication, recovery, post-incident, training/testing

Course Content

52. Digital Forensics

- Forensics intro, system/file/chain of custody, e-discovery, data sources

53. Domain 5: Security Program Management and Oversight

- Management & oversight

54. Security Policies

- Framework, policy, standards, procedures, monitoring, revision, considerations

Course Content

55. Security Governance

- Forensics intro, system/file/chain of custody, e-discovery, data sources

56. Risk Analysis

- Assessments (quantitative/qualitative), BIA, risk treatment, visibility, reporting, updates, metrics

57. Supply Chain Risk

- Vendor relationship/agreement/information management

Course Content

58. Privacy and Compliance

- Legal/framework risks, monitoring & reporting

59. Auditing

- Audit & assessment processes

60. Conclusion

- Continuing your studies and advancing certification

COMPTIA SECURITY+ SY0-701 TRAINING CONTENT

Cyber Xperts

Instructor: Rajendra N

Website: https://www.cyberxperts.pro/

Email: rajendra.n@cyberxperts.pro

Phone: +44 7436906066

LinkedIn: https://www.linkedin.com/in/rajendra-n-75999348/

Location: Newbury Park, Essex, UK, IG27HR

Institute: Cyber Xperts