EDUSUM

#1 Online Certification Guide

COMPTIA SY0-701

CompTIA Security Plus Certification Questions & Answers

Exam Summary – Syllabus –Questions

SY0-701

CompTIA Security+

90 Questions Exam – 750 / 900 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your SY0-701 Certification Well:

The SY0-701 is best suitable for candidates who want to gain knowledge in the CompTIA Core. Before you start your SY0-701 preparation you may struggle to get all the crucial Security Plus materials like SY0-701 syllabus, sample questions, study guide.

But don't worry the SY0-701 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the SY0-701 syllabus?
- How many questions are there in the SY0-701 exam?
- Which Practice test would help me to pass the SY0-701 exam at the first attempt?

Passing the SY0-701 exam makes you CompTIA Security+. Having the Security Plus certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA SY0-701 Security Plus Certification Details:

Exam Name	CompTIA Security+
Exam Code	SY0-701
Exam Price	$392 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	**Pearson VUE**
Sample Questions	**CompTIA Security+ Sample Questions**
Practice Exam	**CompTIA SY0-701 Certification Practice Exam**

SY0-701 Syllabus:

Topic	Details
General Security Concepts - 12%	
Compare and contrast various types of security controls.	- Categories • Technical • Managerial • Operational • Physical - Control types • Preventive • Deterrent • Detective • Corrective • Compensating • Directive
Summarize fundamental security concepts.	- Confidentiality, Integrity, and Availability (CIA) - Non-repudiation - Authentication, Authorization, and Accounting (AAA) • Authenticating people • Authenticating systems • Authorization models - Gap analysis - Zero Trust • Control Plane 1. Adaptive identity 2. Threat scope reduction 3. Policy-driven access control 4. Policy Administrator 5. Policy Engine • Data Plane 1. Implicit trust zones

Topic	Details
	2. Subject/System 3. Policy Enforcement Point - Physical security • Bollards • Access control vestibule • Fencing • Video surveillance • Security guard • Access badge • Lighting • Sensors 1. Infrared 2. Pressure 3. Microwave 4. Ultrasonic - Deception and disruption technology • Honeypot • Honeynet • Honeyfile • Honeytoken
Explain the importance of change management processes and the impact to security.	- Business processes impacting security operation • Approval process • Ownership • Stakeholders • Impact analysis • Test results • Backout plan • Maintenance window • Standard operating procedure - Technical implications

Topic	Details
	• Allow lists/deny lists • Restricted activities • Downtime • Service restart • Application restart • Legacy applications • Dependencies - Documentation • Updating diagrams • Updating policies/procedures - Version control
• Explain the importance of using appropriate cryptographic solutions.	• - Public key infrastructure (PKI) • Public key • Private key • Key escrow • - Encryption • Level 1. Full-disk 2. Partition 3. File 4. Volume 5. Database 6. Record • Transport/communication • Asymmetric • Symmetric • Key exchange • Algorithms • Key length • - Tools • Trusted Platform Module (TPM) • Hardware security module (HSM)

Topic	Details
	• Key management system • Secure enclave • - Obfuscation • Steganography • Tokenization • Data masking • - Hashing - Salting - Digital signatures - Key stretching - Blockchain - Open public ledger - Certificates • Certificate authorities • Certificate revocation lists (CRLs) • Online Certificate Status Protocol (OCSP) • Self-signed • Third-party • Root of trust • Certificate signing request (CSR) generation • Wildcard
Threats, Vulnerabilities, and Mitigations - 22%	
Compare and contrast common threat actors and motivations.	- Threat actors • Nation-state • Unskilled attacker • Hacktivist • Insider threat • Organized crime • Shadow IT - Attributes of actors • Internal/external

Topic	Details
	• Resources/funding • Level of sophistication/capability - Motivations • Data exfiltration • Espionage • Service disruption • Blackmail • Financial gain • Philosophical/political beliefs • Ethical • Revenge • Disruption/chaos • War
Explain common threat vectors and attack surfaces.	- Message-based • Email • Short Message Service (SMS) • Instant messaging (IM) - Image-based - File-based - Voice call - Removable device - Vulnerable software • Client-based vs. agentless - Unsupported systems and applications - Unsecure networks • Wireless • Wired • Bluetooth - Open service ports - Default credentials

Topic	Details
	- Supply chain • Managed service providers (MSPs) • Vendors • Suppliers - Human vectors/social engineering • Phishing • Vishing • Smishing • Misinformation/disinformation • Impersonation • Business email compromise • Pretexting • Watering hole • Brand impersonation • Typosquatting
• Explain various types of vulnerabilities.	• - Application • Memory injection • Buffer overflow • Race conditions 1. Time-of-check (TOC) 2. Time-of-use (TOU) • Malicious update • - Operating system (OS)-based - Web-based • Structured Query Language injection (SQLi) • Cross-site scripting (XSS) • - Hardware • Firmware • End-of-life • Legacy • - Virtualization • Virtual machine (VM) escape

Topic	Details
	• Resource reuse • - Cloud-specific - Supply chain • Service provider • Hardware provider • Software provider • - Cryptographic - Misconfiguration - Mobile device • Side loading • Jailbreaking • - Zero-day
• Given a scenario, analyze indicators of malicious activity.	• - Malware attacks • Ransomware • Trojan • Worm • Spyware • Bloatware • Virus • Keylogger • Logic bomb • Rootkit • - Physical attacks • Brute force • Radio frequency identification (RFID) cloning • Environmental • - Network attacks • Distributed denial-of-service (DDoS) 1. Amplified 2. Reflected • Domain Name System (DNS) attacks • Wireless • On-path

Topic	Details
	• Credential replay • Malicious code • - Application attacks • Injection • Buffer overflow • Replay • Privilege escalation • Forgery • Directory traversal • - Cryptographic attacks • Downgrade • Collision • Birthday • - Password attacks • Spraying • Brute force • - Indicators • Account lockout • Concurrent session usage • Blocked content • Impossible travel • Resource consumption • Resource inaccessibility • Out-of-cycle logging • Published/documented • Missing logs
Explain the purpose of mitigation techniques used to secure the enterprise.	- Segmentation - Access control • Access control list (ACL) • Permissions - Application allow list - Isolation

Topic	Details
	- Patching - Encryption - Monitoring - Least privilege - Configuration enforcement - Decommissioning - Hardening techniques • Encryption • Installation of endpoint protection • Host-based firewall • Host-based intrusion prevention system (HIPS) • Disabling ports/protocols • Default password changes • Removal of unnecessary software
Security Architecture - 18%	
• Compare and contrast security implications of different architecture models.	• - Architecture and infrastructure concepts • Cloud 1. Responsibility matrix 2. Hybrid considerations 3. Third-party vendors • Infrastructure as code (IaC) • Serverless • Microservices • Network infrastructure 1. Physical isolation - Air-gapped 2. Logical segmentation 3. Software-defined networking (SDN) • On-premises • Centralized vs. decentralized • Containerization • Virtualization • IoT • Industrial control systems (ICS)/supervisory control

Topic	Details
	and data acquisition (SCADA) • Real-time operating system (RTOS) • Embedded systems • High availability • - Considerations • Availability • Resilience • Cost • Responsiveness • Scalability • Ease of deployment • Risk transference • Ease of recovery • Patch availability • Inability to patch • Power • Compute
• Given a scenario, apply security principles to secure enterprise infrastructure.	• - Infrastructure considerations • Device placement • Security zones • Attack surface • Connectivity • Failure modes 1. Fail-open 2. Fail-closed • Device attribute 1. Active vs. passive 2. Inline vs. tap/monitor • Network appliances 1. Jump server 2. Proxy server 3. Intrusion prevention system (IPS)/intrusion detection system (IDS) 4. Load balancer

Topic	Details
	5. Sensors • Port security 1. 802.1X 2. Extensible Authentication Protocol (EAP) • Firewall types 1. Web application firewall (WAF) 2. Unified threat management (UTM) 3. Next-generation firewall (NGFW) 4. Layer 4/Layer 7 • - Secure communication/access • Virtual private network (VPN) • Remote access • Tunneling 1. Transport Layer Security (TLS) 2. Internet protocol security (IPSec) • Software-defined wide area network (SD-WAN) • Secure access service edge (SASE) • - Selection of effective controls
Compare and contrast concepts and strategies to protect data.	- Data types • Regulated • Trade secret • Intellectual property • Legal information • Financial information • Human- and non-human-readable - Data classifications • Sensitive • Confidential • Public • Restricted • Private • Critical

Topic	Details
	- General data considerations • Data states 1. Data at rest 2. Data in transit 3. Data in use • Data sovereignty • Geolocation - Methods to secure data • Geographic restrictions • Encryption • Hashing • Masking • Tokenization • Obfuscation • Segmentation • Permission restrictions
Explain the importance of resilience and recovery in security architecture.	- High availability • Load balancing vs. clustering - Site considerations • Hot • Cold • Warm • Geographic dispersion - Platform diversity - Multi-cloud systems - Continuity of operations - Capacity planning • People • Technology • Infrastructure

Topic	Details
	- Testing • Tabletop exercises • Fail over • Simulation • Parallel processing - Backups • Onsite/offsite • Frequency • Encryption • Snapshots • Recovery • Replication • Journaling - Power • Generators • Uninterruptible power supply (UPS)
Security Operations - 28%	
Given a scenario, apply common security techniques to computing resources.	- Secure baselines • Establish • Deploy • Maintain - Hardening targets • Mobile devices • Workstations • Switches • Routers • Cloud infrastructure • Servers

Topic	Details
	• ICS/SCADA • Embedded systems • RTOS • IoT devices - Wireless devices • Installation considerations 1. Site surveys 2. Heat maps - Mobile solutions • Mobile device management (MDM) • Deployment models 1. Bring your own device (BYOD) 2. Corporate-owned, personally enabled (COPE) 3. Choose your own device (CYOD) • Connection methods 1. Cellular 2. Wi-Fi 3. Bluetooth - Wireless security settings • Wi-Fi Protected Access 3 (WPA3) • AAA/Remote Authentication Dial-In User Service (RADIUS) • Cryptographic protocols • Authentication protocols - Application security • Input validation • Secure cookies • Static code analysis • Code signing - Sandboxing - Monitoring

Topic	Details
Explain the security implications of proper hardware, software, and data asset management.	- Acquisition/procurement process - Assignment/accounting • Ownership • Classification - Monitoring/asset tracking • Inventory • Enumeration - Disposal/decommissioning • Sanitization • Destruction • Certification • Data retention
Explain various activities associated with vulnerability management.	- Identification methods • Vulnerability scan • Application security 1. Static analysis 2. Dynamic analysis 3. Package monitoring • Threat feed 1. Open-source intelligence (OSINT) 2. Proprietary/third-party 3. Information-sharing organization 4. Dark web • Penetration testing • Responsible disclosure program 1. Bug bounty program • System/process audit - Analysis • Confirmation 1. False positive 2. False negative

Topic	Details
	• Prioritize • Common Vulnerability Scoring System (CVSS) • Common Vulnerability Enumeration (CVE) • Vulnerability classification • Exposure factor • Environmental variables • Industry/organizational impact • Risk tolerance - Vulnerability response and remediation • Patching • Insurance • Segmentation • Compensating controls • Exceptions and exemptions - Validation of remediation • Rescanning • Audit • Verification - Reporting
Explain security alerting and monitoring concepts and tools.	- Monitoring computing resources • Systems • Applications • Infrastructure - Activities • Log aggregation • Alerting • Scanning • Reporting • Archiving

Topic	Details
	• Alert response and remediation/validation 1. Quarantine 2. Alert tuning - Tools • Security Content Automation Protocol (SCAP) • Benchmarks • Agents/agentless • Security information and event management (SIEM) • Antivirus • Data loss prevention (DLP) • Simple Network Management Protocol (SNMP) traps • NetFlow • Vulnerability scanners
Given a scenario, modify enterprise capabilities to enhance security.	- Firewall • Rules • Access lists • Ports/protocols • Screened subnets - IDS/IPS • Trends • Signatures - Web filter • Agent-based • Centralized proxy • Universal Resource Locator (URL) scanning • Content categorization • Block rules • Reputation - Operating system security

Topic	Details
	• Group Policy • SELinux - Implementation of secure protocols • Protocol selection • Port selection • Transport method - DNS filtering - Email security • Domain-based Message Authentication Reporting and Conformance (DMARC) • DomainKeys Identified Mail (DKIM) • Sender Policy Framework (SPF) • Gateway - File integrity monitoring - DLP - Network access control (NAC) - Endpoint detection and response (EDR)/extended detection and response (XDR) - User behavior analytics
Given a scenario, implement and maintain identity and access management.	- Provisioning/de-provisioning user accounts - Permission assignments and implications - Identity proofing - Federation - Single sign-on (SSO) • Lightweight Directory Access Protocol (LDAP) • Open authorization (OAuth) • Security Assertions Markup Language (SAML) - Interoperability - Attestation - Access controls • Mandatory

Topic	Details
	• Discretionary • Role-based • Rule-based • Attribute-based • Time-of-day restrictions • Least privilege - Multifactor authentication • Implementations 1. Biometrics 2. Hard/soft authentication tokens 3. Security keys • Factors 1. Something you know 2. Something you have 3. Something you are 4. Somewhere you are - Password concepts • Password best practices 1. Length 2. Complexity 3. Reuse 4. Expiration 5. Age • Password managers • Passwordless - Privileged access management tools • Just-in-time permissions • Password vaulting • Ephemeral credentials
Explain the importance of automation and orchestration related	- Use cases of automation and scripting • User provisioning • Resource provisioning

Topic	Details
to secure operations.	• Guard rails • Security groups • Ticket creation • Escalation • Enabling/disabling services and access • Continuous integration and testing • Integrations and Application programming interfaces (APIs) - Benefits • Efficiency/time saving • Enforcing baselines • Standard infrastructure configurations • Scaling in a secure manner • Employee retention • Reaction time • Workforce multiplier - Other considerations • Complexity • Cost • Single point of failure • Technical debt • Ongoing supportability
• Explain appropriate incident response activities.	• - Process • Preparation • Detection • Analysis • Containment • Eradication • Recovery • Lessons learned • - Training

Topic	Details
	- Testing • Tabletop exercise • Simulation • - Root cause analysis - Threat hunting - Digital forensics • Legal hold • Chain of custody • Acquisition • Reporting • Preservation • E-discovery
Given a scenario, use data sources to support an investigation.	- Log data • Firewall logs • Application logs • Endpoint logs • OS-specific security logs • IPS/IDS logs • Network logs • Metadata - Data sources • Vulnerability scans • Automated reports • Dashboards • Packet captures
Security Program Management and Oversight - 20%	
Summarize elements of effective security governance.	- Guidelines - Policies • Acceptable use policy (AUP) • Information security policies

Topic	Details
	• Business continuity • Disaster recovery • Incident response • Software development lifecycle (SDLC) • Change management - Standards • Password • Access control • Physical security • Encryption - Procedures • Change management • Onboarding/offboarding • Playbooks - External considerations • Regulatory • Legal • Industry • Local/regional • National • Global - Monitoring and revision - Types of governance structures • Boards • Committees • Government entities • Centralized/decentralized - Roles and responsibilities for systems and data • Owners

Topic	Details
	• Controllers • Processors • Custodians/stewards
Explain elements of the risk management process.	- Risk identification - Risk assessment • Ad hoc • Recurring • One-time • Continuous - Risk analysis • Qualitative • Quantitative • Single loss expectancy (SLE) • Annualized loss expectancy (ALE) • Annualized rate of occurrence (ARO) • Probability • Likelihood • Exposure factor • Impact - Risk register • Key risk indicators • Risk owners • Risk threshold - Risk tolerance - Risk appetite • Expansionary • Conservative • Neutral - Risk management strategies

Topic	Details
	• Transfer • Accept 1. Exemption 2. Exception • Avoid • Mitigate - Risk reporting - Business impact analysis • Recovery time objective (RTO) • Recovery point objective (RPO) • Mean time to repair (MTTR) • Mean time between failures (MTBF)
Explain the processes associated with third-party risk assessment and management.	- Vendor assessment • Penetration testing • Right-to-audit clause • Evidence of internal audits • Independent assessments • Supply chain analysis - Vendor selection • Due diligence • Conflict of interest - Agreement types • Service-level agreement (SLA) • Memorandum of agreement (MOA) • Memorandum of understanding (MOU) • Master service agreement (MSA) • Work order (WO)/statement of work (SOW) • Non-disclosure agreement (NDA) • Business partners agreement (BPA) - Vendor monitoring

Topic	Details
	- Questionnaires - Rules of engagement
Summarize elements of effective security compliance.	- Compliance reporting • Internal • External - Consequences of non-compliance • Fines • Sanctions • Reputational damage • Loss of license • Contractual impacts - Compliance monitoring • Due diligence/care • Attestation and acknowledgement • Internal and external • Automation - Privacy • Legal implications 1. Local/regional 2. National 3. Global • Data subject • Controller vs. processor • Ownership • Data inventory and retention • Right to be forgotten
Explain types and purposes of audits and assessments.	- Attestation - Internal • Compliance

Topic	Details
	• Audit committee • Self-assessments - External • Regulatory • Examinations • Assessment • Independent third-party audit - Penetration testing • Physical • Offensive • Defensive • Integrated • Known environment • Partially known environment • Unknown environment • Reconnaissance 1. Passive 2. Active
Given a scenario, implement security awareness practices.	- Phishing • Campaigns • Recognizing a phishing attempt • Responding to reported suspicious messages - Anomalous behavior recognition • Risky • Unexpected • Unintentional - User guidance and training • Policy/handbooks • Situational awareness

Topic	Details
	• Insider threat • Password management • Removable media and cables • Social engineering • Operational security • Hybrid/remote work environments - Reporting and monitoring • Initial • Recurring - Development - Execution

CompTIA SY0-701 Sample Questions:

Question: 1

When considering the security implications of hardware, software, and data asset management, which practices contribute to maintaining a secure environment?

(Select all that apply)

a) Regular disposal and destruction of outdated assets
b) Dynamic assignment of ownership
c) Monitoring and tracking assets throughout their lifecycle
d) Lack of classification for sensitive data

Answer: a, c

Question: 2

What is the role of a Policy Enforcement Point (PEP) in policy-driven access control?

a) Creating security policies
b) Enforcing security policies at runtime
c) Analyzing threat scope reduction
d) Allowing unrestricted access to all users

Answer: b

Question: 3

What are common characteristics of external threat actors?

a) Limited access to internal systems
b) Often motivated by financial gain
c) Typically have less sophisticated tools
d) Usually driven by political or ideological beliefs

Answer: a, b

Question: 4

Why is root cause analysis important in incident response?

a) To increase complexity
b) To understand the fundamental reasons behind an incident
c) To ignore the incident
d) To decrease reaction time

Answer: b

Question: 5

In a wartime scenario, which threat actors are most likely to be active?

a) Nation-state
b) Insider threats
c) Organized crime
d) Hacktivists

Answer: a

Question: 6

In vulnerability management, the term _____ refers to the process of determining the relative importance or urgency of addressing a particular vulnerability.

a) Rescanning
b) Analysis
c) Confirmation
d) Prioritize

Answer: d

Question: 7

How do privileged access management tools enhance security in an organization?

a) By granting all users privileged access
b) By restricting access to all resources
c) By disabling all access controls
d) By implementing just-in-time permissions and password vaulting

Answer: d

Question: 8

Which of the following agreement types is specifically focused on defining the scope of work to be performed by a vendor?

a) Memorandum of Agreement (MOA)
b) Service-Level Agreement (SLA)
c) Work Order (WO)/Statement of Work (SOW)
d) Non-Disclosure Agreement (NDA)

Answer: c

Question: 9

Who are stakeholders in the context of change management?

a) Only technical staff
b) Individuals or groups affected by or involved in a change
c) Only security personnel
d) Only upper management

Answer: b

Question: 10

How does User Behavior Analytics (UBA) contribute to enterprise security?

a) By analyzing and detecting anomalous user behavior
b) By ignoring user activities
c) By disabling user access
d) By allowing unrestricted user activities

Answer: a

Study Guide to Crack CompTIA Security Plus SY0-701 Exam:

- Getting details of the SY0-701 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SY0-701 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for SY0-701 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SY0-701 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SY0-701 practice tests is must. Continuous practice will make you an expert in all syllabus areas.