COMPTIA SY0-601

CompTIA Security Plus Certification Questions & Answers

SY0-601

CompTIA Security+

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

Table of Contents:

Discover More about the SY0-601 Certification

Are you interested in passing the CompTIA SY0-601 exam? First discover, who benefits from the SY0-601 certification. The SY0-601 is suitable for a candidate if he wants to learn about Core. Passing the SY0-601 exam earns you the CompTIA Security+ title.

While preparing for the SY0-601 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SY0-601 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SY0-601 study materials just at one click**.

CompTIA SY0-601 Security Plus Certification Details:

Exam Name	CompTIA Security+
Exam Code	SY0-601
Exam Price	$392 (USD)
Duration	90 mins
Number of Questions	90
Passing Score	750 / 900
Schedule Exam	**CompTIA Marketplace** **Pearson VUE**
Sample Questions	**CompTIA Security+ Sample Questions**
Practice Exam	**CompTIA SY0-601 Certification Practice Exam**

SY0-601 Syllabus:

Topic	**Details**
Threats, Attacks, and Vulnerabilities - 24%	
Compare and contrast different types of social engineering techniques.	1. Phishing 2. Smishing 3. Vishing 4. Spam 5. Spam over instant messaging (SPIM)

Topic	Details
	6. Spear phishing 7. Dumpster diving 8. Shoulder surfing 9. Pharming 10. Tailgating 11. Eliciting information 12. Whaling 13. Prepending 14. Identity fraud 15. Invoice scams 16. Credential harvesting 17. Reconnaissance 18. Hoax 19. Impersonation 20. Watering hole attack 21. Typosquatting 22. Pretexting 23. Influence campaigns • Hybrid warfare • Social media 24. Principles (reasons for effectiveness) • Authority • Intimidation • Consensus • Scarcity • Familiarity • Trust • Urgency
Given a scenario, analyze potential indicators to determine the type of attack.	1. Malware • Ransomware • Trojans • Worms

Topic	Details
	- Potentially unwanted programs (PUPs) - Fileless virus - Command and control - Bots - Cryptomalware - Logic bombs - Spyware - Keyloggers - Remote access Trojan (RAT) - Rootkit - Backdoor 2. Password attacks - Spraying - Dictionary - Brute force - Offline - Online - Rainbow table - Plaintext/unencrypted 3. Physical attacks - Malicious Universal Serial Bus (USB) cable - Malicious flash drive - Card cloning - Skimming 4. Adversarial artificial intelligence (AI) - Tainted training data for machine learning (ML) - Security of machine learning algorithms 5. Supply-chain attacks 6. Cloud-based vs. on-premises attacks 7. Cryptographic attacks

Topic	Details
	- Birthday - Collision - Downgrade
Given a scenario, analyze potential indicators associated with application attacks.	1. Privilege escalation 2. Cross-site scripting 3. Injections - Structured query language (SQL) - Dynamic-link library (DLL) - Lightweight Director Access Protocol (LDAP) - Extensible Markup Language (XML) 4. Pointer/object dereference 5. Directory traversal 6. Buffer overflows 7. Race conditions - Time of check/time of use 8. Error handling 9. Improper input handling 10. Replay attack - Session replays 11. Integer overflow 12. Request forgeries - Server-side - Cross-site 13. Application programming interface (API) attacks 14. Resource exhaustion 15. Memory leak 16. Secure Sockets Layer (SSL) stripping 17. Driver manipulation - Shimming - Refactoring

Topic	Details
	18. Pass the hash
Given a scenario, analyze potential indicators associated with network attacks.	1. Wireless • Evil twin • Rogue access point • Bluesnarfing • Bluejacking • Disassociation • Jamming • Radio frequency identification (RFID) • Near-field communication (NFC) • Initialization vector (IV) 2. On-path attack (previously known as man-in-the-middle attack/man-in-the-browser attack) 3. Layer 2 attacks • Address Resolution Protocol (ARP) poisoning • Media access control (MAC) flooding • MAC cloning 4. Domain name system (DNS) • Domain hijacking • DNS poisoning • Uniform Resource Locator (URL) redirection • Domain reputation 5. Distributed denial-of-service (DDoS) • Network • Application • Operational technology (OT) 6. Malicious code or script execution • PowerShell • Python

Topic	Details
	• Bash • Macros • Visual Basic for Applications (VBA)
Explain different threat actors, vectors, and intelligence sources.	1. Actors and threats • Advanced persistent threat (APT) • Insider threats • State actors • Hacktivists • Script kiddies • Criminal syndicates • Hackers - Authorized - Unauthorized - Semi-authorized • Shadow IT • Competitors 2. Attributes of actors • Internal/external • Level of sophistication/capability • Resources/funding • Intent/motivation 3. Vectors • Direct access • Wireless • Email • Supply chain • Social media • Removable media • Cloud 4. Threat intelligence sources

Topic	Details
	- Open-source intelligence (OSINT) - Closed/proprietary - Vulnerability databases - Public/private information-sharing centers - Dark web - Indicators of compromise - Automated Indicator Sharing (AIS) - Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII) - Predictive analysis - Threat maps - File/code repositories 5. Research sources - Vendor websites - Vulnerability feeds - Conferences - Academic journals - Request for comments (RFC) - Local industry groups - Social media - Threat feeds - Adversary tactics, techniques, and procedures (TTP)
Explain the security concerns associated with various types of vulnerabilities.	1. Cloud-based vs. on-premises vulnerabilities 2. Zero-day 3. Weak configurations - Open permissions - Unsecure root accounts - Errors - Weak encryption - Unsecure protocols

Topic	Details
	• Default settings • Open ports and services 4. Third-party risks • Vendor management - System integration - Lack of vendor support • Supply chain • Outsourced code development • Data storage 5. Improper or weak patch management • Firmware • Operating system (OS) • Applications 6. Legacy platforms 7. Impacts • Data loss • Data breaches • Data exfiltration • Identity theft • Financial • Reputation • Availability loss
Summarize the techniques used in security assessments.	1. Threat hunting • Intelligence fusion • Threat feeds • Advisories and bulletins • Maneuver 2. Vulnerability scans • False positives

Topic	Details
	- False negatives - Log reviews - Credentialed vs. non-credentialed - Intrusive vs. non-intrusive - Application - Web application - Network - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS) - Configuration review 3. Syslog/Security information and event management (SIEM) - Review reports - Packet capture - Data inputs - User behavior analysis - Sentiment analysis - Security monitoring - Log aggregation - Log collectors 4. Security orchestration, automation, and response (SOAR)
Explain the techniques used in penetration testing.	1. Penetration testing - Known environment - Unknown environment - Partially known environment - Rules of engagement - Lateral movement - Privilege escalation - Persistence

Topic	Details
	- Cleanup - Bug bounty - Pivoting 2. Passive and active reconnaissance - Drones - War flying - War driving - Footprinting - OSINT 3. Exercise types - Red-team - Blue-team - White-team - Purple-team
Architecture and Design - 21%	
Explain the importance of security concepts in an enterprise environment.	1. Configuration management - Diagrams - Baseline configuration - Standard naming conventions - Internet protocol (IP) schema 2. Data sovereignty 3. Data protection - Data loss prevention (DLP) - Masking - Encryption - At rest - In transit/motion - In processing - Tokenization

Topic	Details
	• Rights management 4. Geographical considerations 5. Response and recovery controls 6. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection 7. Hashing 8. API considerations 9. Site resiliency • Hot site • Cold site • Warm site 10. Deception and disruption • Honeypots • Honeyfiles • Honeynets • Fake telemetry • DNS sinkhole
Summarize virtualization and cloud computing concepts.	1. Cloud models • Infrastructure as a service (IaaS) • Platform as a service (PaaS) • Software as a service (SaaS) • Anything as a service (XaaS) • Public • Community • Private • Hybrid 2. Cloud service providers 3. Managed service provider (MSP)/managed security service provider (MSSP) 4. On-premises vs. off-premises 5. Fog computing 6. Edge computing 7. Thin client

Topic	Details
	8. Containers 9. Microservices/API 10. Infrastructure as code • Software-defined networking (SDN) • Software-defined visibility (SDV) 11. Serverless architecture 12. Services integration 13. Resource policies 14. Transit gateway 15. Virtualization • Virtual machine (VM) sprawl avoidance • VM escape protection
Summarize secure application development, deployment, and automation concepts.	1. Environment • Development • Test • Staging • Production • Quality assurance (QA) 2. Provisioning and deprovisioning 3. Integrity measurement 4. Secure coding techniques • Normalization • Stored procedures • Obfuscation/camouflage • Code reuse/dead code • Server-side vs. client-side execution and validation • Memory management • Use of third-party libraries and software development kits (SDKs) • Data exposure

Topic	Details
	5. Open Web Application Security Project (OWASP) 6. Software diversity • Compiler • Binary 7. Automation/scripting • Automated courses of action • Continuous monitoring • Continuous validation • Continuous integration • Continuous delivery • Continuous deployment 8. Elasticity 9. Scalability 10. Version control
Summarize authentication and authorization design concepts.	1. Authentication methods • Directory services • Federation • Attestation • Technologies - Time-based one-time password (TOTP) - HMAC-based one-time password (HOTP) - Short message service (SMS) - Token key - Static codes - Authentication applications - Push notifications - Phone call • Smart card authentication 2. Biometrics • Fingerprint • Retina

Topic	Details
	- Iris - Facial - Voice - Vein - Gait analysis - Efficacy rates - False acceptance - False rejection - Crossover error rate 3. Multifactor authentication (MFA) factors and attributes - Factors - Something you know - Something you have - Something you are - Attributes - Somewhere you are - Something you can do - Something you exhibit - Someone you know 4. Authentication, authorization and accounting (AAA) 5. Cloud vs. on-premises requirements
Given a scenario, implement cybersecurity resilience.	1. Redundancy - Geographic dispersal - Disk - Redundant array of inexpensive disks (RAID) levels - Multipath - Network - Load balancers - Network interface card (NIC) teaming - Power - Uninterruptible power supply (UPS) - Generator

Topic	Details
	- Dual supply - Managed power distribution units (PDUs) 2. Replication • Storage area network • VM 3. On-premises vs. cloud 4. Backup types • Full • Incremental • Snapshot • Differential • Tape • Disk • Copy • Network-attached storage (NAS) • Storage area network • Cloud • Image • Online vs. offline • Offsite storage - Distance considerations 5. Non-persistence • Revert to known state • Last known-good configuration • Live boot media 6. High availability • Scalability 7. Restoration order 8. Diversity • Technologies

Topic	Details
	- Vendors - Crypto - Controls
Explain the security implications of embedded and specialized systems.	1. Embedded systems - Raspberry Pi - Field-programmable gate array (FPGA) - Arduino 2. Supervisory control and data acquisition (SCADA)/industrial control system (ICS) - Facilities - Industrial - Manufacturing - Energy - Logistics 3. Internet of Things (IoT) - Sensors - Smart devices - Wearables - Facility automation - Weak defaults 4. Specialized - Medical systems - Vehicles - Aircraft - Smart meters 5. Voice over IP (VoIP) 6. Heating, ventilation, air conditioning (HVAC) 7. Drones 8. Multifunction printer (MFP) 9. Real-time operating system (RTOS) 10. Surveillance systems

Topic	Details
	11. System on chip (SoC) 12. Communication considerations • 5G • Narrow-band • Baseband radio • Subscriber identity module (SIM) cards • Zigbee 13. Constraints • Power • Compute • Network • Crypto • Inability to patch • Authentication • Range • Cost • Implied trust
Explain the importance of physical security controls.	1. Bollards/barricades 2. Access control vestibules 3. Badges 4. Alarms 5. Signage 6. Cameras • Motion recognition • Object detection 7. Closed-circuit television (CCTV) 8. Industrial camouflage 9. Personnel • Guards • Robot sentries • Reception

Topic	Details
	• Two-person integrity/control 10. Locks • Biometrics • Electronic • Physical • Cable locks 10. USB data blocker 11. Lighting 12. Fencing 13. Fire suppression 14. Sensors • Motion detection • Noise detection • Proximity reader • Moisture detection • Cards • Temperature 15. Drones 16. Visitor logs 17. Faraday cages 18. Air gap 19. Screened subnet (previously known as demilitarized zone) 20. Protected cable distribution 21. Secure areas • Air gap • Vault • Safe • Hot aisle • Cold aisle 22. Secure data destruction • Burning

Topic	Details
	- Shredding - Pulping - Pulverizing - Degaussing - Third-party solutions
Summarize the basics of cryptographic concepts.	1. Digital signatures 2. Key length 3. Key stretching 4. Salting 5. Hashing 6. Key exchange 7. Elliptic-curve cryptography 8. Perfect forward secrecy 9. Quantum - Communications - Computing 10. Post-quantum 11. Ephemeral 12. Modes of operation - Authenticated - Unauthenticated - Counter 13. Blockchain - Public ledgers 14. Cipher suites - Stream - Block 15. Symmetric vs. asymmetric 16. Lightweight cryptography 17. Steganography

Topic	Details
	• Audio • Video • Image 18. Homomorphic encryption 19. Common use cases • Low power devices • Low latency • High resiliency • Supporting confidentiality • Supporting integrity • Supporting obfuscation • Supporting authentication • Supporting non-repudiation 20. Limitations • Speed • Size • Weak keys • Time • Longevity • Predictability • Reuse • Entropy • Computational overheads • Resource vs. security constraints
Implementation - 25%	
Given a scenario, implement secure protocols.	1. Protocols • Domain Name System Security Extensions (DNSSEC) • SSH

Topic	Details
	• Secure/Multipurpose Internet Mail Extensions (S/MIME) • Secure Real-time Transport Protocol (SRTP) • Lightweight Directory Access Protocol Over SSL (LDAPS) • File Transfer Protocol, Secure (FTPS) • SSH File Transfer Protocol (SFTP) • Simple Network Management Protocol, version 3 (SNMPv3 • Hypertext transfer protocol over SSL/TLS (HTTPS) • IPSec - Authentication header (AH)/Encapsulating Security Payloads (ESP) - Tunnel/transport • Post Office Protocol (POP)/Internet Message Access Protocol (IMAP) 2. Use cases • Voice and video • Time synchronization • Email and web • File transfer • Directory services • Remote access • Domain name resolution • Routing and switching • Network address allocation • Subscription services
Given a scenario, implement host or application security solutions.	1. Endpoint protection • Antivirus • Anti-malware • Endpoint detection and response (EDR) • DLP

Topic	Details
	• Next-generation firewall (NGFW) • Host-based intrusion prevention system (HIPS) • Host-based intrusion detection system (HIDS) • Host-based firewall 2. Boot integrity • Boot security/Unified Extensible Firmware Interface (UEFI) • Measured boot • Boot attestation 3. Database • Tokenization • Salting • Hashing 4. Application security • Input validations • Secure cookies • Hypertext Transfer Protocol (HTTP) headers • Code signing • Allow list • Block list/deny list • Secure coding practices • Static code analysis - Manual code review • Dynamic code analysis • Fuzzing 5. Hardening • Open ports and services • Registry • Disk encryption • OS

Topic	Details
	• Patch management - Third-party updates - Auto-update 6. Self-encrypting drive (SED)/full-disk encryption (FDE) • Opal 7. Hardware root of trust 8. Trusted Platform Module (TPM) 9. Sandboxing
Given a scenario, implement secure network designs.	1. Load balancing • Active/active • Active/passive • Scheduling • Virtual IP • Persistence 2. Network segmentation • Virtual local area network (VLAN) • Screened subnet (previously known as demilitarized zone) • East-west traffic • Extranet • Intranet • Zero Trust 3. Virtual private network (VPN) • Always-on • Split tunnel vs. full tunnel • Remote access vs. site-to-site • IPSec • SSL/TLS • HTML5 • Layer 2 tunneling protocol (L2TP)

Topic	Details
	4. DNS 5. Network access control (NAC) • Agent and agentless 6. Out-of-band management 7. Port security • Broadcast storm prevention • Bridge Protocol Data Unit (BPDU) guard • Loop prevention • Dynamic Host Configuration Protocol (DHCP) snooping • Media access control (MAC) filtering 8. Network appliances • Jump servers • Proxy servers - Forward - Reverse • Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS) - Signature-based - Heuristic/behavior - Anomaly - Inline vs. passive • HSM • Sensors • Collectors • Aggregators • Firewalls - Web application firewall (WAF) - NGFW - Stateful - Stateless - Unified threat management (UTM) - Network address translation (NAT) gateway - Content/URL filter - Open-source vs. proprietary

Topic	Details
	- Hardware vs. software - Appliance vs. host-based vs. virtual 9. Access control list (ACL) 10. Route security 11. Quality of service (QoS) 12. Implications of IPv6 13. Port spanning/port mirroring • Port taps 14. Monitoring services 15. File integrity monitors
Given a scenario, install and configure wireless security settings.	1. Cryptographic protocols • WiFi Protected Access 2 (WPA2) • WiFi Protected Access 3 (WPA3) • Counter-mode/CBC-MAC Protocol (CCMP) • Simultaneous Authentication of Equals (SAE) 2. Authentication protocols • Extensible Authentication Protocol (EAP) • Protected Extensible Authentication Protocol (PEAP) • EAP-FAST • EAP-TLS • EAP-TTLS • IEEE 802.1X • Remote Authentication Dial-in User Service (RADIUS) Federation 3. Methods • Pre-shared key (PSK) vs. Enterprise vs. Open • WiFi Protected Setup (WPS) • Captive portals 4. Installation considerations • Site surveys • Heat maps

Topic	Details
	• WiFi analyzers • Channel overlaps • Wireless access point (WAP) placement • Controller and access point security
Given a scenario, implement secure mobile solutions	1. Connection methods and receivers • Cellular • WiFi • Bluetooth • NFC • Infrared • USB • Point-to-point • Point-to-multipoint • Global Positioning System (GPS) • RFID 2. Mobile device management (MDM) • Application management • Content management • Remote wipe • Geofencing • Geolocation • Screen locks • Push notifications • Passwords and PINs • Biometrics • Context-aware authentication • Containerization • Storage segmentation • Full device encryption 3. Mobile devices

Topic	Details
	- MicroSD hardware security module (HSM) - MDM/Unified Endpoint Management (UEM) - Mobile application management (MAM) - SEAndroid 4. Enforcement and monitoring of: - Third-party application stores - Rooting/jailbreaking - Sideloading - Custom firmware - Carrier unlocking - Firmware over-the-air (OTA) updates - Camera use - SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS) - External media - USB On-The-Go (USB OTG) - Recording microphone - GPS tagging - WiFi direct/ad hoc - Tethering - Hotspot - Payment methods 5. Deployment models - Bring your own device (BYOD) - Corporate-owned personally enabled (COPE) - Choose your own device (CYOD) - Corporate-owned - Virtual desktop infrastructure (VDI)
Given a scenario, apply cybersecurity solutions to the cloud.	1. Cloud security controls - High availability across zones

Topic	Details
	• Resource policies • Secrets management • Integration and auditing • Storage - Permissions - Encryption - Replication - High availability • Network - Virtual networks - Public and private subnets - Segmentation - API inspection and integration • Compute - Security groups - Dynamic resource allocation - Instance awareness - Virtual private cloud (VPC) endpoint - Container security 2. Solutions • CASB • Application security • Next-generation secure web gateway (SWG) • Firewall considerations in a cloud environment - Cost - Need for segmentation - Open Systems Interconnection (OSI) layers 3. Cloud native controls vs. third-party solutions
Given a scenario, implement identity and account management controls.	1. Identity • Identity provider (IdP) • Attributes • Certificates • Tokens • SSH keys

Topic	Details
	• Smart cards 2. Account types • User account • Shared and generic accounts/credentials • Guest accounts • Service accounts 3. Account policies • Password complexity • Password history • Password reuse • Network location • Geofencing • Geotagging • Geolocation • Time-based logins • Access policies • Account permissions • Account audits • Impossible travel time/risky login • Lockout • Disablement
Given a scenario, implement authentication and authorization solutions.	1. Authentication management • Password keys • Password vaults • TPM • HSM • Knowledge-based authentication 2. Authentication/authorization • EAP

Topic	Details
	• Challenge-Handshake Authentication Protocol (CHAP) • Password Authentication Protocol (PAP) • 802.1X • RADIUS • Single sign-on (SSO) • Security Assertion Markup Language (SAML) • Terminal Access Controller Access Control System Plus (TACACS+) • OAuth • OpenID • Kerberos 3. Access control schemes • Attribute-based access control (ABAC) • Role-based access control • Rule-based access control • MAC • Discretionary access control (DAC) • Conditional access • Privileged access management • Filesystem permissions
Given a scenario, implement public key infrastructure.	1. Public key infrastructure (PKI) • Key management • Certificate authority (CA) • Intermediate CA • Registration authority (RA) • Certificate revocation list (CRL) • Certificate attributes • Online Certificate Status Protocol (OCSP) • Certificate signing request (CSR) • CN

Topic	Details
	• Subject alternative name • Expiration 2. Types of certificates • Wildcard • Subject alternative name • Code signing • Self-signed • Machine/computer • Email • User • Root • Domain validation • Extended validation 3. Certificate formats • Distinguished encoding rules (DER) • Privacy enhanced mail (PEM) • Personal information exchange (PFX) • .cer • P12 • P7B 4. Concepts • Online vs. offline CA • Stapling • Pinning • Trust model • Key escrow • Certificate chaining
Operations and Incident Response - 16%	
Given a scenario, use the appropriate tool	1. Network reconnaissance and discovery

Topic	Details
to assess organizational security.	• tracert/traceroute • nslookup/dig • ipconfig/ifconfig • nmap • ping/pathping • hping • netstat • netcat • IP scanners • arp • route • curl • theHarvester • sn1per • scanless • dnsenum • Nessus • Cuckoo 2. File manipulation • head • tail • cat • grep • chmod • logger 3. Shell and script environments • SSH • PowerShell • Python • OpenSSL

Topic	Details
	4. Packet capture and replay • Tcpreplay • Tcpdump • Wireshark 5. Forensics • dd • Memdump • WinHex • FTK imager • Autopsy 6. Exploitation frameworks 7. Password crackers 8. Data sanitization
Summarize the importance of policies, processes, and procedures for incident response.	1. Incident response plans 2. Incident response process • Preparation • Identification • Containment • Eradication • Recovery • Lessons learned 3. Exercises • Tabletop • Walkthroughs • Simulations 4. Attack frameworks • MITRE ATT&CK • The Diamond Model of Intrusion Analysis • Cyber Kill Chain

Topic	Details
	5. Stakeholder management 6. Communication plan 7. Disaster recovery plan 8. Business continuity plan 9. Continuity of operations planning (COOP) 10. Incident response team 11. Retention policies
Given an incident, utilize appropriate data sources to support an investigation.	1. Vulnerability scan output 2. SIEM dashboards • Sensor • Sensitivity • Trends • Alerts • Correlation 3. Log files • Network • System • Application • Security • Web • DNS • Authentication • Dump files • VoIP and call managers • Session Initiation Protocol (SIP) traffic 4. syslog/rsyslog/syslog-ng 5. journalctl 6. NXLog 7. Bandwidth monitors 8. Metadata • Email • Mobile

Topic	Details
	- Web - File 9. Netflow/sFlow - Netflow - sFlow - IPFIX 10. Protocol analyzer output
Given an incident, apply mitigation techniques or controls to secure an environment.	1. Reconfigure endpoint security solutions - Application approved list - Application blocklist/deny list - Quarantine 2. Configuration changes - Firewall rules - MDM - DLP - Content filter/URL filter - Update or revoke certificates 3. Isolation 4. Containment 5. Segmentation 6. SOAR - Runbooks - Playbooks
Explain the key aspects of digital forensics.	1. Documentation/evidence - Legal hold - Video - Admissibility - Chain of custody

Topic	Details
	• Timelines of sequence of events - Time stamps - Time offset • Tags • Reports • Event logs • Interviews 2. Acquisition • Order of volatility • Disk • Random-access memory (RAM) • Swap/pagefile • OS • Device • Firmware • Snapshot • Cache • Network • Artifacts 3. On-premises vs. cloud • Right-to-audit clauses • Regulatory/jurisdiction • Data breach notification laws 4. Integrity • Hashing • Checksums • Provenance 5. Preservation 6. E-discovery 7. Data recovery

Topic	Details
	8. Non-repudiation 9. Strategic intelligence/counterintelligence
Governance, Risk, and Compliance - 14%	
Compare and contrast various types of controls.	1. Category • Managerial • Operational • Technical 2. Control type • Preventive • Detective • Corrective • Deterrent • Compensating • Physical
Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	1. Regulations, standards, and legislation • General Data Protection Regulation (GDPR) • National, territory, or state laws • Payment Card Industry Data Security Standard (PCI DSS) 2. Key frameworks • Center for Internet Security (CIS) • National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/Cybersecurity Framework (CSF) • International Organization for Standardization (ISO) 27001/27002/27701/31000 • SSAE SOC 2 Type I/II • Cloud security alliance • Cloud control matrix

Topic	Details
	• Reference architecture 3. Benchmarks /secure configuration guides • Platform/vendor-specific guides - Web server - OS - Application server - Network infrastructure devices
Explain the importance of policies to organizational security.	1. Personnel • Acceptable use policy • Job rotation • Mandatory vacation • Separation of duties • Least privilege • Clean desk space • Background checks • Non-disclosure agreement (NDA) • Social media analysis • Onboarding • Offboarding • User training 1. Gamification 2. Capture the flag 3. Phishing campaigns - Phishing simulations - Computer-based training (CBT) - Role-based training 2. Diversity of training techniques 3. Third-party risk management • Vendors • Supply chain • Business partners

Topic	Details
	- Service level agreement (SLA) - Memorandum of understanding (MOU) - Measurement systems analysis (MSA) - Business partnership agreement (BPA) - End of life (EOL) - End of service life (EOSL) - NDA 4. Data - Classification - Governance - Retention 5. Credential policies - Personnel - Third-party - Devices - Service accounts - Administrator/root accounts 6. Organizational policies - Change management - Change control - Asset management
Summarize risk management processes and concepts.	1. Risk types - External - Internal - Legacy systems - Multiparty - IP theft - Software compliance/licensing 2. Risk management strategies

Topic	Details
	• Acceptance • Avoidance • Transference - Cybersecurity insurance • Mitigation 3. Risk analysis • Risk register • Risk matrix/heat map • Risk control assessment • Risk control self-assessment • Risk awareness • Inherent risk • Residual risk • Control risk • Risk appetite • Regulations that affect risk posture • Risk assessment types - Qualitative - Quantitative • Likelihood of occurrence • Impact • Asset value • Single-loss expectancy (SLE) • Annualized loss expectancy (ALE) • Annualized rate of occurrence (ARO) 4. Disasters • Environmental • Person-made • Internal vs. external 5. Business impact analysis • Recovery time objective (RTO)

Topic	Details
	• Recovery point objective (RPO) • Mean time to repair (MTTR) • Mean time between failures (MTBF) • Functional recovery plans • Single point of failure • Disaster recovery plan (DRP) • Mission essential functions • Identification of critical systems • Site risk assessment
Explain privacy and sensitive data concepts in relation to security.	1. Organizational consequences of privacy and data breaches • Reputation damage • Identity theft • Fines • IP theft 2. Notifications of breaches • Escalation • Public notifications and disclosures 3. Data types • Classifications - Public - Private - Sensitive - Confidential - Critical - Proprietary • Personally identifiable information (PII) • Health information • Financial information • Government data • Customer data

Topic	Details
	4. Privacy enhancing technologies • Data minimization • Data masking • Tokenization • Anonymization • Pseudo-anonymization 5. Roles and responsibilities • Data owners • Data controller • Data processor • Data custodian/steward • Data protection officer (DPO) 6. Information life cycle 7. Impact assessment 8. Terms of agreement 9. Privacy notice

Broaden Your Knowledge with CompTIA SY0-601 Sample Questions:

Question: 1

An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one implementing the changes.

Which of the following describes this policy?

a) Change management
b) Job rotation
c) Separation of duties
d) Least privilege

Answer: c

Question: 2

The IT department receives a call one morning about users being unable to access files on the network shared drives. An IT technician investigates and determines the files became encrypted at 12:00 a.m.

While the files are being recovered from backups, one of the IT supervisors realizes the day is the birthday of a technician who was fired two months prior.

Which of the following describes what MOST likely occurred?

a) The fired technician placed a logic bomb.
b) The fired technician installed a rootkit on all the affected users' computers.
c) The fired technician installed ransomware on the file server.
d) The fired technician left a network worm on an old work computer.

Answer: a

Question: 3

A Chief Financial Officer (CFO) has been receiving email messages that have suspicious links embedded from unrecognized senders.

The emails ask the recipient for identity verification. The IT department has not received reports of this happening to anyone else.

Which of the following is the MOST likely explanation for this behavior?

a) The CFO is the target of a whaling attack.
b) The CFO is the target of identity fraud.
c) The CFO is receiving spam that got past the mail filters.
d) The CFO is experiencing an impersonation attack.

Answer: a

Question: 4

Joe, an employee, knows he is going to be fired in three days. Which of the following characterizations describes the employee?

a) An insider threat
b) A competitor
c) A hacktivist
d) A state actor

Answer: a

Question: 5

What is the term given to a framework or model outlining the phases of attack to help security personnel defend their systems and respond to attacks?

a) Command and control
b) Intrusion kill chain
c) Cyber-incident response
d) CIRT

Answer: b

Question: 6

Why do vendors provide MD5 values for their software patches?

a) To provide the necessary key for patch activation
b) To allow the downloader to verify the authenticity of the site providing the patch
c) To ensure that auto-updates are enabled for subsequent patch releases
d) To allow the recipient to verify the integrity of the patch prior to installation

Answer: d

Question: 7

Which of the following would be the BEST method to prevent the physical theft of staff laptops at an open-plan bank location with a high volume of customers each day?

a) Guards at the door
b) Cable locks
c) Visitor logs
d) Cameras

Answer: b

Question: 8

Which of the following disaster recovery sites would require the MOST time to get operations back online?

a) Colocation
b) Cold
c) Hot
d) Warm

Answer: b

Question: 9

You have been asked to provide a virtualized environment. Which of the following makes it possible for many instances of an operating system to be run on the same machine?

a) API
b) Virtual machine
c) Hypervisor
d) Container

Answer: c

Question: 10

A security manager needed to protect a high-security datacenter, so the manager installed an access control vestibule that can detect an employee's heartbeat, weight, and badge. Which of the following did the security manager implement?

a) A physical control
b) A corrective control
c) A compensating control
d) A managerial control

Answer: a

Avail the Study Guide to Pass CompTIA SY0-601 Security Plus Exam:

- Find out about the SY0-601 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **SY0-601 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the SY0-601 training. Joining the CompTIA provided training for SY0-601 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **SY0-601 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SY0-601 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the SY0-601 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the SY0-601 Certification

EduSum.Com is here with all the necessary details regarding the SY0-601 exam. We provide authentic practice tests for the SY0-601 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **SY0-601 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the CompTIA Security+.

Start Online Practice of SY0-601 Exam by visiting URL
https://www.edusum.com/comptia/sy0-601-comptia-security