CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-701

TEST DETAILS

Required exam	SY0-701
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	A minimum of 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	General Security Concepts	12%
2.0	Threats, Vulnerabilities, and Mitigations	22%
3.0	Security Architecture	18%
4.0	Security Operations	28%
5.0	Security Program Management and Oversight	20%
Total		**100%**

1.0 General Security Concepts

1.1 Compare and contrast various types of security controls.

- **Categories**
  - Technical
  - Managerial
  - Operational
  - Physical
- **Control types**
  - Preventive
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive

1.2 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
    - Adaptive identity
    - Threat scope reduction
    - Policy-driven access control
    - Policy Administrator
    - Policy Engine
  - Data Plane
    - Implicit trust zones
    - Subject/System
    - Policy Enforcement Point
- **Physical security**
  - Bollards
  - Access control vestibule
  - Fencing
  - Video surveillance
  - Security guard
  - Access badge
  - Lighting
  - Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic
- **Deception and disruption technology**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

1.3 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**
  - Allow lists/deny lists
  - Restricted activities
  - Downtime
  - Service restart
  - Application restart
  - Legacy applications
  - Dependencies
- **Documentation**
  - Updating diagrams
  - Updating policies/procedures
- **Version control**

1.4 Explain the importance of using appropriate cryptographic solutions.

- **Public key infrastructure (PKI)**
  - Public key
  - Private key
  - Key escrow
- **Encryption**
  - Level
    - Full-disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  - Transport/communication
  - Asymmetric
  - Symmetric
  - Key exchange
  - Algorithms
  - Key length
- **Tools**
  - Trusted Platform Module (TPM)
  - Hardware security module (HSM)
  - 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

2.0 Threats, Vulnerabilities, and Mitigations

2.1 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
  - Resources/funding
  - Level of sophistication/capability
- **Motivations**
  - Data exfiltration
  - Espionage
  - Service disruption
  - Blackmail
  - Financial gain
  - Philosophical/political beliefs
  - Ethical
  - Revenge
  - Disruption/chaos
  - War

2.2 Explain common threat vectors and attack surfaces.

- **Message-based**
  - o Email
  - o Short Message Service (SMS)
  - o Instant messaging (IM)
- **Image-based**
- **File-based**
- **Voice call**
- **Removable device**
- **Vulnerable software**
  - o Client-based vs. agentless
- **Unsupported systems and applications**
- **Unsecure networks**
  - Wireless
  - Wired
  - Bluetooth
- **Open service ports**
- **Default credentials**
- **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

2.3 Explain various types of vulnerabilities.

- **Application**
  - Memory injection
  - Buffer overflow
  - Race conditions
    - Time-of-check (TOC)
    - 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
  - Resource reuse
- **Cloud-specific**
- **Supply chain**
  - Service provider
  - Hardware provider
  - Software provider
- **Cryptographic**
- **Misconfiguration**
- **Mobile device**
  - Side loading
  - Jailbreaking
- **Zero-day**

2.4 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)
    - Amplified
    - Reflected
  - Domain Name System (DNS) attacks
  - Wireless
  - On-path
  - 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

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- **Segmentation**
- **Access control**
  - Access control list (ACL)
  - Permissions
- **Application allow list**
- **Isolation**
- **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

3.0 Security Architecture

3.1 Compare and contrast security implications of different architecture models.

- **Architecture and infrastructure concepts**
  - Cloud
    - Responsibility matrix
    - Hybrid considerations
    - Third-party vendors
  - Infrastructure as code (IaC)
  - Serverless
  - Microservices
  - Network infrastructure
    - Physical isolation
      - Air-gapped
    - Logical segmentation
    - Software-defined networking (SDN)
  - On-premises
  - Centralized vs. decentralized
  - Containerization
  - Virtualization
  - IoT
  - Industrial control systems (ICS)/ supervisory control 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

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

- **Infrastructure considerations**
  - Device placement
  - Security zones
  - Attack surface
  - Connectivity
  - Failure modes
    - Fail-open
    - Fail-closed
  - Device attribute
    - Active vs. passive
    - Inline vs. tap/monitor
  - Network appliances
    - Jump server
    - Proxy server
    - Intrusion prevention system (IPS)/intrusion detection system (IDS)
    - Load balancer
    - Sensors
  - Port security
    - 802.1X
    - Extensible Authentication Protocol (EAP)
  - Firewall types
    - Web application firewall (WAF)
    - Unified threat management (UTM)
    - Next-generation firewall (NGFW)
    - Layer 4/Layer 7
- **Secure communication/access**
  - Virtual private network (VPN)
  - Remote access
  - Tunneling
    - Transport Layer Security (TLS)
    - Internet protocol security (IPSec)
  - Software-defined wide area network (SD-WAN)
  - Secure access service edge (SASE)
- **Selection of effective controls**

3.3 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
- **General data considerations**
  - Data states
    - Data at rest
    - Data in transit
    - Data in use
  - Data sovereignty
  - Geolocation
- **Methods to secure data**
  - Geographic restrictions
  - Encryption
  - Hashing
  - Masking
  - Tokenization
  - Obfuscation
  - Segmentation
  - Permission restrictions

3.4 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
- **Testing**
  - Tabletop exercises
  - Fail over
  - Simulation
  - Parallel processing
- **Backups**
  - Onsite/offsite
  - Frequency
  - Encryption
  - Snapshots
  - Recovery
  - Replication
  - Journaling
- **Power**
  - Generators
  - Uninterruptible power supply (UPS)

4.0 Security Operations

4.1 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
  - ICS/SCADA
  - Embedded systems
  - RTOS
  - IoT devices
- **Wireless devices**
  - Installation considerations
    - Site surveys
    - Heat maps
- **Mobile solutions**
  - Mobile device management (MDM)
  - Deployment models
    - Bring your own device (BYOD)
    - Corporate-owned, personally enabled (COPE)
    - Choose your own device (CYOD)
  - Connection methods
    - Cellular
    - Wi-Fi
    - 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**

4.2 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

4.3 Explain various activities associated with vulnerability management.

- **Identification methods**
  - Vulnerability scan
  - Application security
    - Static analysis
    - Dynamic analysis
    - Package monitoring
  - Threat feed
    - Open-source intelligence (OSINT)
    - Proprietary/third-party
    - Information-sharing organization
    - Dark web
  - Penetration testing
  - Responsible disclosure program
    - Bug bounty program
  - System/process audit
- **Analysis**
  - Confirmation
    - False positive
    - False negative
  - 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**

4.4 Explain security alerting and monitoring concepts and tools.

- **Monitoring computing resources**
  - Systems
  - Applications
  - Infrastructure
- **Activities**
  - Log aggregation
  - Alerting
  - Scanning
  - Reporting
  - Archiving
  - Alert response and remediation/validation
    - Quarantine
    - 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

4.5 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**
  - 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**

4.6 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
  - Discretionary
  - Role-based
  - Rule-based
  - Attribute-based
  - Time-of-day restrictions
  - Least privilege
- **Multifactor authentication**
  - Implementations
    - Biometrics
    - Hard/soft authentication tokens
    - Security keys
  - Factors
    - Something you know
    - Something you have
    - Something you are
    - Somewhere you are
- **Password concepts**
  - Password best practices
    - Length
    - Complexity
    - Reuse
    - Expiration
    - Age
  - Password managers
  - Passwordless
- **Privileged access management tools**
  - Just-in-time permissions
  - Password vaulting
  - Ephemeral credentials

4.7 Explain the importance of automation and orchestration related to secure operations.

- **Use cases of automation and scripting**
  - User provisioning
  - Resource provisioning
  - 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

4.8 Explain appropriate incident response activities.

- **Process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- **Training**
- **Testing**
  - Tabletop exercise
  - Simulation
- **Root cause analysis**
- **Threat hunting**
- **Digital forensics**
  - Legal hold
  - Chain of custody
  - Acquisition
  - Reporting
  - Preservation
  - E-discovery

4.9 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

5.0 Security Program Management and Oversight

5.1 Summarize elements of effective security governance.

- **Guidelines**
- **Policies**
  - Acceptable use policy (AUP)
  - Information security policies
  - 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
  - Controllers
  - Processors
  - Custodians/stewards

5.2 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**
  - Transfer
  - Accept
    - Exemption
    - 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)

5.3 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**
- **Questionnaires**
- **Rules of engagement**

5.4 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
    - Local/regional
    - National
    - Global
  - Data subject
  - Controller vs. processor
  - Ownership
  - Data inventory and retention
  - Right to be forgotten

5.5 Explain types and purposes of audits and assessments.

- **Attestation**
- **Internal**
  - Compliance
  - 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
    - Passive
    - Active

5.6 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
  - Insider threat
  - Password management
  - Removable media and cables
  - Social engineering
  - Operational security
  - Hybrid/remote work environments
- **Reporting and monitoring**
  - Initial
  - Recurring
- **Development**
- **Execution**