CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-801 V8

CompTIA Security+ SY0-801 V8 Certification Exam
Exam Objectives Document Version 1.1

CompTIA

About the Exam

The CompTIA Security+ SY0-801 V8 certification exam will certify the successful candidate has the knowledge and skills required to:

- Identify, interpret, and support activities as part of the incident response process.
- Assess the security posture of an environment and recommend and implement appropriate security solutions.
- Manage and monitor modern operating environments, including cloud, mobile, and hybrid.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Understand and apply mitigation techniques pertaining to threats, vulnerabilities, and attacks.

The target audience consists of security administrators with two years of hands-on experience.

These content examples are meant to clarify the exam objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM ACCREDITATION

The CompTIA Security+ exam is accredited by the ANSI National Accreditation Board (ANAB) to show compliance with the International Organization for Standardization (ISO) 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in Bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	Security+ SY0-801 V8
Number of questions	TBD
Types of questions	Multiple-choice and performance-based
Length of test	TBD
Recommended experience	Security administrator with two years of hands-on experience.

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	16%
2.0	Threats, Vulnerabilities, and Attacks	24%
3.0	Security Architecture	19%
4.0	Security Operations	27%
5.0	Security Program Management and Oversight	14%
Total		**100%**

1.0 General Security Concepts

1.1 Explain security concepts and controls.

- Defense in depth
- Confidentiality, integrity, and availability (CIA)
- Authentication, authorization, accounting (AAA)
- Non-repudiation
- Zero Trust principles
- Least privilege
- Control categories
  - Technical/logical
  - Managerial/administrative
  - Physical/environmental
  - Operational
- Control types
  - Preventive
  - Deterring
  - Corrective
  - Detective
  - Compensating
  - Mitigating
  - Directive

1.2 Given a scenario, demonstrate the impact of change management processes on security.

- Business processes impacting security operations
  - Change advisory board (CAB)
    - Approval process
  - Ownership
  - Stakeholders
  - Impact analysis
  - Test results
  - Backout planning
  - Fail forward
  - Maintenance window
  - Standard operating procedures (SOPs)
- Technical implications
  - Allow lists/deny lists
  - Restricted activities
  - Downtime
  - Service restart
  - Application restart
  - Legacy applications
  - Dependencies
- Documentation
  - Updating diagrams
  - Updating policies/procedures
- Version control

1.3 Explain the importance of using appropriate cryptographic solutions.

- Public key infrastructure (PKI)
  - Public key
  - Private key
  - Key escrow
- 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
- Encryption
  - Protocols
  - Symmetric
  - Asymmetric
  - Level
    - Full disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  - Transport/communication
  - Key exchange
  - Algorithms
  - Key length
- Digital signatures
- Salting
- Tools
- Obfuscation
- Hashing algorithms

2.0 Threats, Vulnerabilities, and Attacks

2.1 Explain characteristics of threats and vulnerabilities.

- Threats
  - Threat feeds
  - Likelihood
  - Impact
  - Intelligence sources
  - Life cycle
- Vulnerabilities
  - Scoring
    - Common Vulnerability Scoring System (CVSS)
    - National Vulnerability Database (NVD)
  - Prioritization
  - Vulnerability types
  - Common Vulnerabilities and Exposures (CVE)

2.2 Describe common threat actors and motivations.

- Threat actors
  - Advanced persistent threat (APT)
  - Crime syndicate/organized crime
  - Terrorist
  - Unskilled attacker
  - Hacktivist
  - Insider
  - Accidental/unintentional
  - Competitor
  - State-sponsored
- Motivations
  - Financial
  - Influence
  - Intellectual property
  - Notoriety
  - Espionage
  - Fear/chaos
  - Extortion
  - General curiosity
  - Revenge
  - Ideological
  - Political
  - Ethical
  - War
- Attributes of actors
  - Internal/external
  - Resources/funding
  - Level of sophistication/capability

2.3 Describe threat vectors and sources.

- Message-based
  - Email
  - Short Message Service (SMS)
  - Rich Communication Services (RCS)
  - Instant messaging
  - Collaboration tools
- Image-based
  - Quick response (QR) codes
  - Embedded content
  - Completely Automated Public Turing test to tell Computers and Humans Apart(CAPTCHA)
- Attachment-based
  - Embedded macros
  - Rich Text Format (RTF) documents
  - Portable Document Formats (PDFs)
- Browser-based
  - Extensions
  - JavaScript
  - Password managers
  - Cookies
  - Session tokens
- Network-based
  - Infrastructure devices
  - Virtualized devices
  - Session keys
- Remote access
  - Remote desktop
  - Virtual Network Computing (VNC)
  - Virtual private network (VPN)
- Endpoint-based
  - Mobile devices
  - Workstations
  - Servers
  - Tablets
  - Trusted devices
  - Built-in tools
  - Living-off-the-land tools
- Supply chain-based
  - Third-party providers
  - Managed service providers
  - Logistic providers
  - Software as a service (SaaS) providers
- External media-based
  - Malicious Universal Serial Bus (USB)
- Human-based
  - Impersonation
  - Contractor
  - Visitor
  - Biometric
  - Watering hole
- Internet of Things (IoT)-based
  - Cameras
  - Sensors
  - Printers
- Operational technology (OT)-based
- Physical-based
  - Lock and key
  - Access vestibule
  - Access passes
- Signal-based
  - Bluetooth
  - Radio frequency (RF)
- Near-field communications (NFC)

2.4 Explain types of vulnerabilities and attack surfaces.

- Unsupported products
- Unpatched systems
- Obsolete systems
- Unmanaged systems
- Ports and services
- Applications
  - Race conditions
    - Time-of-check (TOC)
    - Time-of-use (TOU)
  - Malicious update
- Code
  - Hardcoded secrets
  - Unsafe exception handling
- Operating system (OS)-based
- Virtualization
- Zero-day
- Cryptographic vulnerabilities
- Unmanaged/stale credentials
- Rogue devices
- Shadow IT
- Wireless and low-powered communications
- Large language models (LLMs)
- Identity providers
- Mobile devices
- Misconfiguration
- Public repositories
- Public object storage

2.5 Given a scenario, analyze indicators of malicious activity.

- Malware attacks
  - Ransomware
  - Trojan
  - Worm
  - Spyware
  - Adware
  - Virus
  - Rootkit
  - Keylogger
  - Logic bomb
  - Fileless malware
- Physical attacks
  - Tailgating
  - Shoulder surfing
  - Skimming
  - Forced entry
- Network attacks
  - Distributed denial of service (DDoS)
  - Protocol downgrade
  - Rogue
  - Sniffing
  - Spoofing
  - On-path
  - Domain Name System (DNS) attacks
  - Cache poisoning
- Social engineering attacks
  - Smishing
  - Vishing
  - Phishing
  - Whaling
  - Spear phishing
  - Quishing
  - Impersonation
  - Deepfake
- Indicators of compromise
  - Hash
  - Internet Protocol (IP) address
  - Domain
  - Malicious processes
  - File system artifacts
  - Timestamp
  - Log manipulation
  - Excessive resource consumption
  - Plaintext strings
  - Account lockout
  - Impossible travel
  - Concurrent sessions
- Application attacks
  - Injection
  - Buffer overflow
  - Replay
  - Privilege escalation
  - Forgery
  - Directory traversal
- Credential attacks
  - Password spraying
  - Brute force
  - User enumeration
  - Replay
  - Multifactor authentication (MFA) bypass

2.6 Summarize threats and vulnerabilities associated with artificial intelligence (AI) usage.

- Model manipulation
- Poisoning
- Prompt injection
- Data loss
- Bias
- Explainability
- Hallucinations
- Jailbreaking
- Evasion
- Privacy
- Ethical considerations
- Session hijacking
- Code execution

3.0 Security Architecture

3.1 Compare and contrast security implications of different architecture models.

- Architecture and infrastructure concepts
  - Cloud
    - Serverless
    - Multicloud
    - Deployment models
      - Hybrid
      - Private
      - Public
      - Community
    - Infrastructure as Code (IaC)
  - OT
  - On-premises infrastructure
  - Air-gapped network
  - Microservices
  - Logical segmentation
  - Physical segmentation
- Technical considerations
  - Availability
  - Resilience
  - Proprietary vs. open source
  - Usability
  - Responsibility
  - Compute
  - Power requirements
  - Ease of recovery
- Business considerations
  - Data sovereignty
  - Data classification
  - Cost
  - Ownership
  - Environmental requirements
  - Scalability
  - Risk

3.2 Given a scenario, manage the security architecture to best protect the infrastructure.

- Infrastructure considerations
  - Device placement
  - Security zones
  - Attack surface
  - Diversity
- Zero Trust architecture
  - User authentication
  - Device management
    - Health
    - Inventory
  - Application access control
- Secure communication/access
  - Virtual private network (VPN)
  - Remote access
  - Tunneling
  - User management
  - User access
    - Least privilege
  - End-to-end encrypted messaging
  - Out-of-band management
  - File transfer
  - Security Service Edge (SSE)
- Identity management
  - Group managed service accounts
  - Least privilege access accounts
  - Privilege creep
- Failure modes

3.3 Summarize concepts and strategies used to protect data.

- Data types
  - Structured
  - Unstructured
- Data states
  - Data at rest
  - Data in use
  - Data in transit
- Data classifications
  - Sensitive
  - Secret
  - Critical
  - Confidential
  - Public
  - Top secret
  - Restricted
- Methods used to secure data
  - Masking
  - Hashing
  - Filtering
  - Tokenization
  - Encryption
  - Data transpose
  - Deidentification
  - Obfuscation
- Data protection roles
  - Data owner
  - Data custodian
  - Data steward
  - Data operator
  - Data controller
  - Data subprocessor
- Data handling
  - Endpoints
  - Marking and labeling
  - Geofencing
  - Data location
  - Data placement
- Data management life cycle
  - Creation
  - Management
  - Distribution
  - Retention
  - Disposal
- Data compliance
  - Standards
  - Health data
  - Personal information
  - Financial
  - Child/minor data
  - Intellectual property
  - Legal data

3.4 Explain the importance of resilience and recovery in security architecture.

- Site considerations
  - Hot
  - Cold
  - Warm
  - Environmental
- Platform diversity
  - Vendor platform
  - Hardware
  - Virtualization
- Redundancy strategies and solutions
  - Load balancing
  - Clustering
  - Autoscaling
  - High availability
  - Multicloud systems
  - Power
    - Uninterruptible power supply (UPS)
    - Redundant power supply (RPS)
    - Power generator
    - Surge protector
- Storage
- Backups
  - Retention
  - Immutability
  - Scope
  - Restoration testing
- Testing
  - Failover
  - Simulation
  - Parallel processing
- Disaster recovery
- Business continuity
- Capacity planning
- Recovery metrics
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)

4.0 Security Operations

4.1 Given a scenario, apply mitigating controls, techniques, and solutions to secure the environment.

- Segmentation
- Access controls
- Hardening
- Sandboxing
- Deception and disruption technology
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken
  - Canary account
- Monitoring/alerting
- Mobile device management (MDM)
- Application control
  - Allow lists
  - Block lists
- Intrusion detection/prevention systems
  - Network-based intrusion detection system (NIDS)/Network-based intrusion prevention system (NIPS)
  - Host-based intrusion detection system (HIDS)/Host-based Intrusion prevention system (HIPS)
  - Wireless intrusion prevention system (WIPS)
- Firewalls
  - Rate-limiting requests
  - Web application firewall (WAF)
  - Rule-based
  - Unified threat management (UTM)
  - Layer 4/Layer 7
- Content filter
  - Data loss prevention (DLP)
  - Agent-based
  - Centralized proxy
- Endpoint security
  - Endpoint detection and response (EDR)
  - Extended direction and response (XDR)
  - Antivirus
- Network access control
  - Captive portals
  - 802.1X
  - Endpoint posture/compliance
- Repositories
  - Secrets scanning
- Application security
  - Input validation
  - Secure cookies
  - Static code analysis
  - Code signing
- Email security
  - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Sender Policy Framework (SPF)
  - DomainKeys Identified Mail (DKIM)
  - Brand Indicators for Message Identification (BIMI)
- Operating systems security
  - Group policy
  - Security-enhanced Linux (SELinux)

4.2 Explain the security implications of proper hardware, software, and data asset management.

- Asset management life cycle
- Planning/scoping
- Acquisition/procurement process
- Assignment/accounting
- Monitoring/asset tracking
- Disposal/decommissioning

4.3 Given a scenario, perform tasks associated with vulnerability management.

- Identification methods
  - Scanning
  - Internet Protocol Address Management (IPAM)
  - Cloud security posture management (CSPM)
  - Source code review
- Prioritization
  - Severity assessment
  - Penetration test report review
- Remediation
- Verification
- Reporting
  - Internal
  - External
    - Bounty program
    - Responsible disclosure policies

4.4 Explain security alerting and monitoring concepts and tools.

- Monitoring computing resources
  - Systems
  - Application
  - Infrastructure
- Activities
  - Log aggregation
  - Alerting
  - Scanning
  - Archiving
  - Reporting
  - Alert tuning
- Tools
  - Benchmarks
  - Agents/agentless
  - Security Information and Event Management (SIEM)
  - Antivirus
  - DLP
  - Vulnerability scanners
  - Orchestration
  - Packet analyzer
- Protocols
  - NetFlow
  - Simple Network Management Protocol (SNMP)
  - Syslog
  - Security Content Automation Protocol (SCAP)
- Automated alerts
- Port mirroring
- Dashboards
- Network management systems

4.5 Given a scenario, apply concepts related to identity and access management.

- Provisioning/deprovisioning user accounts
- Permissions assignments and implications
- Identity proofing
- Federation
- Single sign-on (SSO)
  - Security Assertions Markup Language (SAML)
  - Lightweight Directory Access Protocol (LDAP)
  - Open authorization (OAuth)
- Account types
  - User
  - Privileged
    - Global
    - Local
  - Service
  - Third-party
  - Emergency access
- MFA
  - Hard token
  - Soft token
  - Biometrics
  - One-time password (OTP)
  - Backup code
- Access control models
  - Rule-based
  - Role-based
  - Time-based
  - Mandatory
  - Discretionary
  - Just-in-time
- Access management
  - Authentication
  - Policies
    - Logical/technical
    - Administrative/business
- Access review
- Password concepts
  - Passkey
  - Password managers
  - Passwordless
  - Password best practices
    - Length
    - Complexity
    - Reuse
    - Expiration
    - Age
    - Compromised credential monitoring
    - Account auditing
    - Policy report

4.6 Given a scenario, apply automation and orchestration solutions to secure operations.

- Use cases of automation and scripting
  - User provisioning
  - Resource provisioning
  - Desired state management
  - Anomaly detection
  - Ticket management
- Considerations
  - Guardrails
  - Automation logic
  - Process engineering
  - Complexity
  - Financial
  - Process risks
  - Deployment
- AI
  - Capabilities
    - Agentic
    - Chatbot
    - Predictive analysis
    - AI-augmented baselines
- Intended outcomes
  - Efficiency/time saving
  - Enforcing baselines
  - Continuous improvements
  - Productivity improvements
  - Reduced downtime
  - Increased proactivity
- SecOps
  - Continuous integration and continuous deployment (CI/CD)
- Workflows
  - Automation
  - Integrations

4.7 Summarize concepts associated with incident response activities.

- Preparation
  - Training
  - Testing
  - Tabletop exercises
  - Playbooks
  - Simulation
  - Roles
- Identification
  - Detection
  - Internal advisory
  - External advisory
  - Threat hunting
- Investigation
  - Digital forensics
  - Chain of custody
  - E-discovery
  - Preservation
- Containment
  - Quarantine/isolation
- Negotiation
- Eradication/recovery
- Notification/external reporting
  - Stakeholders
  - Customers
  - Law enforcement
  - Mandatory
- Post-incident
  - Lessons learned
  - Root cause analysis
  - Post-incident reporting (PIR)

4.8 Given a scenario, use data, artifacts and sources to support a security investigation.

- Log and trace data types
  - Access and accounting
    - Logical
    - Physical
  - Device
  - Server
  - Application
  - Authentication
  - Communication
  - Audit
  - Endpoint
  - Network
  - Metadata
- Data sources
  - Vulnerability scans
  - Automated reports
  - NetFlow/Internet Protocol Flow Information Export (IPFIX)
  - Surveillance footage
  - Security tools
  - Dashboards
  - Packet captures
- File/log integrity
- System image
  - Memory dump
  - Bit-level copy
  - Snapshot
- Stakeholders
  - Human Resources (HR)
  - Accounts
  - Legal
- Log-parsing techniques

5.0 Security Program Management and Oversight

5.1 Explain the importance of governance, risk, and compliance artifacts.

- Guidelines
  - Benchmarks
  - Advisories
  - Implementation guides
  - Reference architecture
- Standards
  - Baselines
  - Passwords
  - Physical security
  - Request for Comments (RFC)
  - Encryption
- Procedures
  - Standard operating procedure (SOP)
  - Runbooks
- Plans
  - Business continuity
  - Disaster recovery
- Policies
  - Bring your own device (BYOD)
  - Acceptable use policy (AUP)
  - Clean desk
  - Information security
  - Incident response
  - Data classification and retention
  - Access control
  - Data disposal
  - Vulnerability disclosure
  - Privacy

5.2 Explain the impact of risk management processes on the security of the organization.

- Risk identification
  - Asset identification
  - Stakeholder ownership
- Risk assessment
  - Scoring
  - Categorization
- Risk analysis
  - Impact
  - Likelihood/probability
  - Owner
  - Current mitigations
  - Qualitative vs. quantitative
- Risk register
  - Communication
  - Reviews
- Risk treatment
  - Transferring
  - Accepting
  - Avoiding
  - Mitigating
- Business-level considerations
  - Business impact analysis
  - Risk appetite
  - Residual risk
  - Stakeholder involvement
  - Management oversight
  - Regulatory
  - Legal
  - Single loss expectancy (SLE)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)

5.3 Explain the assessment and management processes associated with third-party risk.

- Vendor selection
  - Request for proposal (RFP)
  - Request for information (RFI)
  - Request for quote (RFQ)
  - Expression of interest (EOI)
  - Due diligence
  - Conflict of interest
- Agreement types
  - Service-level agreement (SLA)
  - Service-level objective (SLO)
  - Memorandum of understanding (MOU)
  - Memorandum of agreement (MOA)
  - Non-disclosure agreement (NDA)
  - Master services agreement (MSA)
  - Statement of work (SOW)
- Vendor monitoring
  - Right to audit
  - Service-level monitoring
  - Vendor registry
  - Vendor assessment
  - Compliance attestation
  - Penetration testing
- Limitations/constraints
  - Staffing limitations
  - Resource availability
  - Environment
  - Legal and regulatory factors
  - Geography/jurisdiction
  - Financial/return on investment (ROI)
  - Vendor lock-in
  - Assurance mechanisms
- Rules of engagement

5.4 Summarize elements of effective security compliance.

- Compliance training
  - Data handling
  - Anti-money laundering/counter-terrorism financing (AML/CTF)
  - Anti-bribery
- Compliance monitoring
  - Attestations
  - Acknowledgements
- Consequences of non-compliance
  - Reputational damage
  - Financial
  - Legal
  - Contractual
  - Sanctions
  - Loss of license
- Privacy
  - Right to be forgotten
  - Opt-in or opt-out
  - Data correction
  - Processing restrictions
  - Processing prevention
  - Controller vs. processor
  - Ownership
- Legal compliance
  - Legal hold
  - Legal orders
  - Data retention requirements

5.5 Explain concepts associated with audit and assessment activities.

- Data gathering
  - Sampling
  - Questionnaires/surveys
  - Interviews
  - Assertion
  - Reference sources
    - MITRE ATT&CK
    - Cyber Kill Chain
    - Diamond Model of Intrusion Analysis
- Scoping
  - Audit charter
  - Frequency
- Engagement types
  - Gap analysis
  - Internal
    - Compliance
    - Audit committee
    - Self-assessments
  - External
    - Examinations
    - Assessments
    - Regulatory
    - Independent third-party audits
  - Benchmarking
- Penetration testing
  - Known environment
  - Unknown environment
  - Partially known environment
  - Physical
  - Offensive
  - Defensive
  - Integrated
  - Reconnaissance
    - Passive
    - Active
- Frameworks and standards
  - Industry-based standards
  - International standards
  - Region-specific standards
- Functional testing
- Behavioral testing

5.6 Given a scenario, apply security awareness concepts to improve organizational security.

- Types of training
  - Initial/onboarding
  - Ongoing
  - Targeted
  - Corrective
- Delivery mechanisms
  - Learning management system (LMS)
  - Self-service portals
  - One-to-one
  - One-to-many
- Reporting and monitoring of effectiveness
  - Metrics
  - Managerial reports
  - Personnel behavior risk scoring
- Common training topics
  - Social engineering
  - Emerging security topics
  - Password and credential management
  - Remote work/teleworking/hybrid
  - BYOD
  - Business email compromise (BEC)
  - Removable media and cables
  - Situational awareness
  - Operational security

CompTIA Security+ Acronym List

The following is a list of acronyms that appear on the CompTIA Security+ SY0-801 V8 certification exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
AI	Artificial Intelligence
ALE	Annualized Loss Expectancy
AML/CTF	Anti-money Laundering/Counter-terrorism Financing
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
AUP	Acceptable Use Policy
BEC	Business Email Compromise
BIMI	Brand Indicators for Message Identification
BYOD	Bring Your Own Device
CAB	Change Advisory Board
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CI/CD	Continuous Integration and Continuous Deployment
CIA	Confidentiality, Integrity, and Availability
CRL	Certificate Revocation List
CSPM	Cloud Security Posture Management
CSR	Certificate Signing Request
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
EDR	Endpoint Detection and Response
EOI	Expression of Interest
GBIC	Gigabit Interface Converter
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HR	Human Resources
IaC	Infrastructure as Code
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export

ACRONYM	DEFINITION
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
LLM	Large Language Model
LMS	Learning Management System
MDM	Mobile Device Management
MFA	Multifactor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NDA	Non-disclosure Agreement
NFC	Near-field Communication
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NVD	National Vulnerability Database
OAuth	Open Authorization
OCSP	Online Certificate Status Protocol
OS	Operating System
OT	Operational Technology
OTP	One-time Password
PDF	Portable Document Formats
PIR	Post-incident Reporting
PKI	Public Key Infrastructure
QR	Quick Response
RCS	Rich Communication Services
RF	Radio Frequency
RFC	Request for Comments
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quote
ROI	Return on Investment
RPO	Recovery Point Objective
RPS	Redundant Power Supply
RTF	Rich Text Format
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SCAP	Security Content Automation Protocol
SELinux	Security-enhanced Linux
SFP	Small Form-factor Pluggable
SIEM	Security Information and Event Management
SLE	Single Loss Expectancy

ACRONYM	DEFINITION
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SOW	Statement of Work
SPF	Sender Policy Framework
SSE	Security Service Edge
SSO	Single Sign-on
TLS	Transport Layer Security
TOC	Time-of-check
TOU	Time-of-use
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTM	Unified Threat Management
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAF	Web Application Firewall
WIPS	Wireless Intrusion Prevention System
XDR	Extended Direction and Response

CompTIA Security+ Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Security+ SY0-801 V8 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The Bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Tablet
- Laptop
- Web server
- Firewall
- Router
- Switch
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Wireless access point
- Virtual machines
- Email system
- Internet access
- Domain Name System (DNS) server
- Internet of Things (IoT) devices
- Hardware tokens
- Smartphone

SPARE PARTS/HARDWARE

- Network interface cards (NICs)
- Power supplies
- Gigabit interface converter (GBICs)
- Small Form-factor Pluggables (SFPs)
- Managed Switch
- Uninterruptible power supply (UPS)

SOFTWARE

- Windows OS
- Linux OS
- Kali Linux
- Packet capture software
- Penetration testing software
- Static and dynamic analysis tools
- Vulnerability scanner
- Network emulators
- Sample code
- Code editor
- Security information and event management (SIEM)
- Keyloggers
- Mobile device management (MDM) software
- Virtual private network (VPN)
- Dynamic Host Configuration Protocol (DHCP) service
- DNS service

TOOLS

- Wi-Fi analyzer
- Network mapper
- NetFlow analyzer

OTHER

- Access to cloud environments
- Sample network documentation/diagrams
- Sample logs