CompTIA Security+ SY0-701 Bootcamp Syllabus

The CompTIA Security+ certification 5-day live bootcamp will prepare the successful candidate to have the knowledge and skills necessary to:

- Pass the most recent SY0-701 Security+ exam
- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions
- Monitor and secure hybrid environments, including cloud, mobile, and Internet of Things (IoT)
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance
- Identify, analyze, and respond to security events and incidents

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

Domains and Percentage of Coverage

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%

COURSE OUTLINE

Day 1

Course 1: Security Goals and Controls

- Confidentiality, Integrity, and Availability (CIA)
- Non-repudiation
- Authentication, Authorization, and Accounting (AAA)
- Authenticating people
- Authenticating systems
- Authorization models
- Categories (Technical, Managerial, Operational, and Physical)

- Control types (Preventive, Deterrent, Detective, Corrective, Compensating, and Directive)

Course 2: Fundamental Security Concepts

- Gap Analysis
- Zero Trust – Control Plane (adaptive identity, threat scope reduction, policy-driven access control, Policy Administrator
- Zero Trust – Data Plane (implicit trust zones, subject/system, Policy Enforcement Points)
- Deception Technologies (Honeypots, Honeynets, Honeyfiles, Honeytokens
- Preventative Physical Security (bollards, access control vestibule, access badges/cards, fencing, gates, mantraps, security guards
- Detective Physical Security (Video surveillance, lighting, sensors <Infrared, Pressure, Microwave, Ultrasonic
- Change Management Business Processes (Approval process, Ownership, Stakeholders, Impact analysis, Test results, Backout plan, Maintenance window, Standard operating procedure
- Change Management Technical Implications (Allow lists/deny lists, Restricted activities, Downtime, Service restart, Application restart, Legacy applications, Dependencies)
- Documentation and Version Control

Course 3: Practical Cryptography

- Symmetric cryptography
- Asymmetric cryptography
- Encryption Levels (Full-disk, Partition, File, Volume, Database, Record)
- Hashing, Salting and HMACs
- Key Exchange
- Digital Signatures and certificates
- Public key infrastructure (PKI) including CA's, Certificate signing request (CSR) generation, Certificate revocation lists (CRLs), Online Certificate Status Protocol (OCSP), Self-signed, Third-party, Wildcard, Root of trust
- Cryptographic tools (Trusted Platform Module (TPM), Hardware security module (HSM), Key management systems, Secure enclaves, key stretching, obfuscation with steganography, tokenization, and data masking)
- Blockchain technology

Course 4: Threat Actors and Vectors

- Threat actor types and attributes (Nation-state, Unskilled attacker, Hacktivist, Insider threat, Organized crime, Shadow IT); Attributes of actors (Internal/external, Resources/funding, Level of sophistication/capability
- Threat Actor Motivations (Data exfiltration, Espionage, Service disruption, Blackmail, Financial gain, Philosophical/political beliefs, Ethical, Revenge, Disruption/chaos, War)
- Human vectors and social engineering (Phishing, Business email compromise, Vishing, Smishing, misinformation/disinformation, Impersonation and hoaxing, Pretexting, Brand impersonation, typosquatting, and watering hole

- Common Attack Surfaces (removable devices, vulnerable software, client-based vs. agentless, unsupported systems and applications, unsecure networks <Wireless, Wired, Bluetooth>, open service ports, default credentials)
- Supply Chain Vulnerabilities (Managed service providers (MSPs), Vendors, Suppliers, Service providers, Hardware providers, Software providers)
- Application Vulnerabilities (Memory injection, Buffer overflow, Race conditions, Time-of-check (TOC)/Time-of-use (TOU), malicious updates, zero days)
- O/S Based and Web based vulnerabilities (misconfiguration <need IaC>, unpatched, outdated, SQLi, Cross-site scripting (XSS), request forgeries
- Hardware and Virtualization vulnerabilities (Firmware - End-of-life – Legacy; Virtualization - Virtual machine (VM) escape, sprawl- Resource reuse)
- Cloud Vulnerabilities
- Mobile device vulnerabilities (Side loading, Jailbreaking, rooting)

Day 2

Course 5: Survey of Malicious Activities

- Malware attacks (Ransomware, Trojan, RATs, Worms, Viruses, Spyware and Bloatware, Keyloggers, Logic bombs, Rootkits
- Physical attacks (Brute force, Radio frequency identification (RFID) cloning, Environmental)
- Network attacks (DoS/Distributed denial-of-service (DDoS) both amplified and 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, brute force, side-channel)
- Password attacks (Spraying, Brute force, wordlists)
- Indicators of compromise (Account lockout, Concurrent session usage, Blocked content, impossible travel, Resource consumption and inaccessibility, Out-of-cycle logging, Published/documented, Missing logs

Course 6: Mitigation Techniques

- Segmentation and Isolation
- Access Control (ACL, NACL, Permissions, Allow-list, CSP security group)
- Configuration and Patch Management
- Least privilege and separation of duties
- Encryption
- Monitoring and visibility
- Decommissioning and offboarding
- Hardening techniques (Encryption, installation of endpoint protection (EDR and host-based firewalls/Host-based intrusion prevention system (HIPS), Disabling ports/protocols, Default password changes, Removal of unnecessary software

Course 7: Architecture and Infrastructure Concepts

- Architectural Considerations (Availability, high availability, durability, resilience, Ease of recovery, Cost, Responsiveness, Scalability, Ease of deployment, Risk transference, Patch availability or inability to patch, Power, Compute)
- Cloud Computing (Cloud Responsibility matrix, Hybrid considerations, Third-party vendors, on-premises cloud)
- Infrastructure-as-Code
- Serverless technologies
- Containers and microservices
- Network infrastructure (Physical isolation, Air-gapped, Logical segmentation, Software-defined networking)
- Centralized vs. Decentralized Design
- Virtualization
- Industrial control systems (ICS)/ supervisory control and data acquisition (SCADA)
- Internet of Things (IoT) (embedded systems, RTOS, smart systems)

Course 8: Enterprise Infrastructure Security Principles

- Infrastructure considerations (Device placement, Security zones, Attack surface, Connectivity, Failure modes [Fail-open/Fail-closed], Device attributes [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 (Static Access Control List (ACL), Unified threat management (UTM), Next-generation firewall (NGFW), Layer 4/Layer 7, Web application firewall (WAF)
- Virtual Private Networks (VPN)
- IP Security (IPsec)
- Transport Layer Security (TLS)
- SD-WAN and SASE (Software-defined wide area network (SD-WAN) and Secure access service edge (SASE)

Day 3

Course 9: Data Protection Concepts and Strategies

- Data States (Data at rest, Data in transit, Data in use)
- Data Classifications (Sensitive, Confidential, Public, Restricted, Private, Critical)
- Data Types (Regulated, Trade secrets, Intellectual property, PHI, PII, Legal information, financial information, Human- and non-human readable)
- Data Lifecycle (Create, Store, Use, Share, Archive, Destroy)
- Securing Data: Geographic and Cultural Restrictions
- Securing Data: Encryption and Hashing
- Securing Data: Masking, Obfuscation, Tokenization
- Securing Data: Segmentation and compartmentalization

Course 10: Resilience and Recovery

- Load Balancing vs. Clustering
- Backup Strategies (Onsite/offsite, Frequency, Encryption, Snapshots, Recovery, Replication, Journaling)
- Continuity of Operations and Multi-Cloud
- Disaster Recovery Sites (Hot, Cold, Warm, Cloud, Geographic dispersion)
- Capacity Planning (People, Technology, Infrastructure)
- Testing (Tabletop exercises, Fail over, Simulation, Parallel processing)
- Power Considerations (Generators, Uninterruptible power supply (UPS)

Course 11: Computing Resources Security Techniques

- Secure Baselines (Establish, Deploy, Maintain)
- Hardening targets (Mobile devices, Workstations, Switches, Routers, Cloud infrastructure, Servers, ICS/SCADA, Embedded systems, RTOS, and IoT devices)
- Wireless Device Installation Issues (Site surveys, Heat maps)
- Mobile Device Solutions (Mobile device management (MDM), Sandboxing, Deployment models including bring your own device (BYOD), Corporate-owned, personally enabled (COPE), and choose your own device (CYOD); Connection methods like Cellular, Wi-Fi, and 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)
- Asset Management (Acquisition/procurement process: Assignment/accounting [Ownership, Classification]; Monitoring/asset tracking [Inventory, Enumeration; Disposal/decommissioning [Sanitization, Destruction, Certification, Data retention])

Course 12: Vulnerability Management

- Threat Feeds (Open-source intelligence (OSINT), Proprietary/third-party, Information-sharing organization, Dark web, Common Vulnerability Scoring System (CVSS), Common Vulnerability Enumeration (CVE), Vulnerability classification)
- Application Vulnerability Assessment (Static analysis, Dynamic analysis, Package monitoring)
- Vulnerability Scanning (add confirmation false positive/false negative, Exposure factor, Environmental variables, industry/organizational impact, risk tolerance)
- Penetration Testing (add Responsible disclosure program and Bug bounty program)
- Vulnerability response and remediation (Patching, Insurance, Segmentation, Compensating controls, exceptions and exemptions)
- Remediation Validation and Reporting (Rescanning, Audit, Verification)

Day 4

Course 13: Security Monitoring and Alerting

- Monitoring Computing Resources (Systems, Applications, Infrastructure agents/agentless)
- Monitoring Activities (Log aggregation, Alerting, Scanning, Reporting, Archiving, Alert response and remediation/validation [Quarantine, Alert tuning]
- Security Content Automation Protocol (SCAP)

- Security information and event management (SIEM) [revisit vulnerability scans]
- Security Orchestration and Automation and Response (SOAR)
- Antivirus and Data loss prevention (DLP) systems
- Simple Network Management Protocol (SNMP) traps
- NetFlow Records

Course 14: Enterprise Security Capabilities

- Firewalls (Rules, Access lists, Ports/protocols, Screened subnets)
- IDS and IPS (Trends, Signature)
- Web filters (Agent-based, Centralized proxy, URL scanning, Content categorization, Block rules, Reputation)
- Operating system security (Group Policy, SELinux)
- Implementing Secure Protocols (Protocol selection, Port selection, Transport method)
- DNS Filtering (DNSSEC, OpenDNS)
- Email Security (Domain-based Message Authentication Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), Gateway
- File integrity monitoring
- Data Loss Prevention (DLP)
- Network access control (NAC)
- Endpoint detection and response (EDR)/extended detection and response (XDR), User behavior analytics (UBA)

Course 15: Identity and Access Management

- Provisioning/de-provisioning User Accounts (Permission assignments and implications, Identity proofing)
- Password concepts (Password best practices, Length, Complexity, Reuse, Expiration, Age, Password managers, Passwordless solutions
- Federation and Single sign-on (SSO) (Lightweight Directory Access Protocol (LDAP), Open authorization (OAuth), Security Assertions Markup Language (SAML), Interoperability, Attestation)
- Access Control Models (Mandatory, Discretionary, Role-based, Rule-based, Attribute-based, Time-of-day restrictions, Least privilege)
- Multifactor Authentication (something you know, something you have, something you are, somewhere you are, hard/soft authentication tokens, security keys, certificates)
- Biometric Authentication
- Privileged Access Management tools (PAM, Just-in-time permissions, Password vaulting, Ephemeral credentials)

Course 16: Automation. Orchestration, and Incident Response

- Automation and Scripting Use Cases (User and 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 of Automation (Efficiency/time saving, Enforcing baselines, Standard infrastructure configurations, Scaling in a secure manner, Employee retention, Reaction time, Workforce multiplier
- Automation Considerations (Complexity, Cost, Single point of failure, Technical debt, ongoing supportability)
- Incident Response Process (Preparation, Detection, Analysis, Containment, Eradication, Recovery, Lessons learned)
- Training and Testing IR (Training, Testing, Tabletop exercise, Simulation)
- Threat Hunting and Root Cause Analysis
- Digital forensics (Legal hold, Chain of custody, Acquisition, Reporting, Preservation, E-discovery)
- Investigation Data Sources (Firewall logs, Application logs, Endpoint logs, OS-specific security logs, IPS/IDS logs, network logs, metadata, vulnerability scans, automated reports, dashboards, packet captures)

Day 5

Course 17: Effective Security Governance

- Security Governance Defined
- Types of governance structures (Boards, Committees, Government entities, Centralized/decentralized)
- Roles and Responsibilities (Owners, Controllers, Processors, Custodians/stewards, officers)
- External Governance Considerations (regulatory, legal, industry, local/regional, national, global)
- Guidance and Best Practices
- Standards and Policies (Standards – Password, Access control, Physical security, Encryption; Policies - Acceptable use policy (AUP), Information security policies, Business continuity, Disaster recovery, Incident response, Software development lifecycle (SDLC), Change management
- Security Governance Procedures (Change management, Onboarding/offboarding, Playbooks, Monitoring and revision

Course 18: Risk Management

- Risk Management Defined
- Risk identification and Assessment (identification, Ad hoc, Recurring, One-time, Continuous)
- Risk Analysis (Qualitative, probability/likelihood, impact/magnitude, Quantitative – Whitman model
- Risk Treatment and Handling (Transfer, Accept, Exemption, Exception, Avoid, Mitigate); Risk appetite – Expansionary, Conservative, Neutral)
- Risk Registers and Ledgers (Key risk indicators, Risk owners, Risk threshold)
- Risk Reporting
- Business impact analysis (Recovery time objective (RTO), Recovery point objective (RPO), Mean time to repair (MTTR), Mean time between failures (MTBF)

Course 19: Security Compliance and 3rd Party Risk

- Compliance monitoring (due diligence/care, attestation and acknowledgement, Internal and external, automation

- Compliance Reporting (Internal, External)
- Consequences of non-compliance (Fines, Sanctions, Reputational damage, Loss of license, Contractual impacts)
- Privacy (Legal implications - Local/regional, National, Global; Data subject, Controller vs. processor, ownership, Data inventory and retention, right to be forgotten
- Vendor Assessment and Selection (Penetration testing, Right-to-audit clause, Evidence of internal audits, independent assessments, Supply chain analysis: vendor selection: due diligence, conflict of interest, questionnaires, rules of engagement)
- Agreement Types (Non-disclosure agreement (NDA), , Memorandum of agreement (MOA), Memorandum of understanding (MOU), Service-level agreement (SLA), Master service agreement (MSA), Work order (WO)/statement of work (SOW), Business partners agreement (BPA)

Course 20: Audits, Assessments, and Awareness

- Internal Audit and Attestation (Compliance, Audit committee, Self-assessments)
- External Audit and Attestation (Regulatory, Examinations, Assessment, Independent third-party audit)
- Penetration Testing (Known environment, partially known environment, Unknown environment, Physical, Offensive, Defensive, Integrated, Reconnaissance – Passive vs. Active)
- User guidance and training (Policy/handbooks, Situational awareness, Insider threats, Password management, Removable media and cables, social engineering, Operational security, Anomalous behavior recognition – risky, unexpected, unintentional; Hybrid/remote work environments best practices)
- Phishing Campaigns (Recognizing a phishing attempt, responding to reported suspicious messages)
- Security Training Monitoring and Reporting