Security+ (V7) exam objectives summary

General security concepts (12%)

- Security controls: comparing technical, preventive, managerial, deterrent, operational, detective, physical, corrective, compensating, and directive controls.
- Fundamental concepts: summarizing confidentiality, integrity, and availability (CIA); non-repudiation; authentication, authorization, and accounting (AAA); zero trust; and deception/disruption technology.
- Change management: explaining business processes, technical implications, documentation, and version control.
- Cryptographic solutions: using public key infrastructure (PKI), encryption, obfuscation, hashing, digital signatures, and blockchain.
- Advance your career—Buy Security+ certification exam or training today.

Threats, vulnerabilities, and mitigations (22%)

- Threat actors and motivations: comparing nation-states, unskilled attackers, hacktivists, insider threats, organized crime, shadow IT, and motivations like data exfiltration, espionage, and financial gain.
- Threat vectors and attack surfaces: explaining message-based, unsecure networks, social engineering, file-based, voice call, supply chain, and vulnerable software vectors.
- Vulnerabilities: explaining application, hardware, mobile device, virtualization, operating system (OS)-based, cloud-specific, web-based, and supply chain vulnerabilities.
- Malicious activity: analyzing malware attacks, password attacks, application attacks, physical attacks, network attacks, and cryptographic attacks.
- Mitigation techniques: using segmentation, access control, configuration enforcement, hardening, isolation, and patching.

Security architecture (18%)

- Architecture models: comparing on-premises, cloud, virtualization, Internet of Things (IoT), industrial control systems (ICS), and infrastructure as code (IaC).

- Enterprise infrastructure: applying security principles to infrastructure considerations, control selection, and secure communication/access.
- Data protection: comparing data types, securing methods, general considerations, and classifications.
- Resilience and recovery: explaining high availability, site considerations, testing, power, platform diversity, backups, and continuity of operations

Security operations (28%)

- Computing resources: applying secure baselines, mobile solutions, hardening, wireless security, application security, sandboxing, and monitoring.
- Asset management: explaining acquisition, disposal, assignment, and monitoring/tracking of hardware, software, and data assets.
- Vulnerability management: identifying, analyzing, remediating, validating, and reporting vulnerabilities.
- Alerting and monitoring: explaining monitoring tools and computing resource activities.
- Enterprise security: modifying firewalls, IDS/IPS, DNS filtering, DLP (data loss prevention), NAC (network access control), and EDR/XDR (endpoint/extended detection and response).
- Identity and access management: implementing provisioning, SSO (single sign-on), MFA (multifactor authentication), and privileged access tools.
- Automation and orchestration: explaining automation use cases, scripting benefits, and considerations.
- Incident response: implementing processes, training, testing, root cause analysis, threat hunting, and digital forensics.
- Data sources: using log data and other sources to support investigations.

Security program management and oversight (20%)

- Security governance: summarizing guidelines, policies, standards, procedures, external considerations, monitoring, governance structures, and roles/responsibilities.
- Risk management: explaining risk identification, assessment, analysis, register, tolerance, appetite, strategies, reporting, and business impact analysis (BIA).

- Third-party risk: managing vendor assessment, selection, agreements, monitoring, questionnaires, and rules of engagement.
- Security compliance: summarizing compliance reporting, consequences of non-compliance, monitoring, and privacy.
- Audits and assessments: explaining attestation, internal/external audits, and penetration testing.
- Security awareness: implementing phishing training, anomalous behavior recognition, user guidance, reporting, and monitoring.