EVERY EXAM PREP · CHEAT SHEET

CompTIA Security+ Cheat Sheet 2026

The night-before summary, built like the exam.

90 Questions	**1h 30m** Time limit	**750 (on a scale of 100-900)** Passing score
— Exam fee	**CompTIA** Governing body	

Exam Logistics at a Glance

Detail	Value
Exam code	SY0-701
Length of test	90 minutes
Question count	Maximum of 90 questions
Question types	Multiple-choice and performance-based questions (PBQs)
Passing score	750 on a scale of 100-900
Content domains	5 domains
Delivery	Pearson VUE test center or OnVUE online proctoring (24/7)
Languages	English, Japanese, Portuguese, Spanish, Thai
Recommended experience	2 years in IT administration with a security focus
Certification validity	Exam usually retired 3 years after launch
Renewal	50 CEUs

Content Domains (Quick List)

- 1.0 General Security Concepts — 12% of the exam
- 2.0 Threats, Vulnerabilities, and Mitigations — 22% of the exam (the heaviest domain besides Security Operations)
- 3.0 Security Architecture — 18% of the exam
- 4.0 Security Operations — 28% of the exam (the single largest domain — prioritize study time here)
- 5.0 Security Program Management and Oversight — 20% of the exam

Study-Time Allocation Tip

Since Domain 4 (28%) and Domain 2 (22%) together make up half the exam, weight your practice-question time toward operational security controls and threat/vulnerability analysis before polishing governance and architecture topics.

Key Terms and Concepts to Memorize

Domain 1 — General Security Concepts

- CIA triad: confidentiality, integrity, availability — the foundation every other concept maps back to

- Non-repudiation, AAA (authentication, authorization, accounting) framework
- Physical vs. logical vs. administrative controls, and control types (preventive, detective, corrective, deterrent, compensating)
- Zero Trust principles: never trust, always verify; control plane vs. data plane

Domain 2 — Threats, Vulnerabilities, Mitigations

- Threat actor types: nation-state, hacktivist, insider, organized crime, unskilled attacker
- Social engineering vectors: phishing, vishing, smishing, pretexting, business email compromise
- Vulnerability classes: zero-day, misconfiguration, supply chain, cryptographic weaknesses
- Malware families: ransomware, worms, trojans, rootkits, spyware, logic bombs
- Mitigation techniques: segmentation, patching, least privilege, encryption, monitoring

Domain 3 — Security Architecture

- Cloud vs. on-prem vs. hybrid architecture trade-offs, IaC (infrastructure as code)
- Network segmentation: VLANs, screened subnets (DMZ), microsegmentation, zero trust architecture
- Resilience concepts: redundancy, high availability, RTO/RPO, backup types (full, incremental, differential)
- Data protection: encryption at rest/in transit/in use, tokenization, masking, data classification

Domain 4 — Security Operations

- Hardening techniques: baselines, patch management, disabling unnecessary services/ports
- Identity and access management: SSO, federation, MFA factors, conditional access, privileged access management
- Incident response lifecycle: preparation, detection, analysis, containment, eradication, recovery, lessons learned
- Log sources and SIEM/SOAR concepts, digital forensics basics (chain of custody, order of volatility)
- Vulnerability management workflow: scanning, prioritization (CVSS), remediation, validation

Domain 5 — Security Program Management and Oversight

- Governance elements: policies, standards, procedures, guidelines
- Risk management: risk register, risk appetite/tolerance, qualitative vs. quantitative risk analysis (ALE, SLE, ARO)
- Third-party/vendor risk management, compliance frameworks, and audits
- Security awareness training and the role of a security champion program

Common Gotchas and Traps

- Questions often present two technically correct answers — pick the most secure or least disruptive option per the scenario, not just any valid control.
- Performance-based questions (PBQs) typically appear early in the exam and can consume disproportionate time — do not let them derail your pacing for the remaining multiple-choice items.
- Do not confuse similar-sounding acronyms: IPS vs. IDS, SIEM vs. SOAR, RTO vs. RPO, MTBF vs. MTTR.
- Many distractors describe a real security concept that is simply the wrong fit for the scenario's stated goal (e.g., confidentiality control offered when the question asks about availability).
- Watch for questions that test order of operations, especially in incident response and forensics (order of volatility, chain of custody).
- Zero Trust and least privilege appear across multiple domains — expect them to resurface in architecture, operations, and governance contexts, not just one section.

Night-Before Checklist

- Confirm your Pearson VUE appointment details and, if testing remotely, verify your OnVUE system check and ID requirements in advance.

- Do a final pass on the domain you're weakest in — but don't cram new material; focus on reinforcing what you already know.
- Review the CIA triad, AAA framework, incident response steps, and risk formulas (ALE = SLE × ARO) one last time — these anchor many scenario questions.
- Skim your list of confusable acronym pairs (IDS/IPS, RTO/RPO, MTBF/MTTR, SSO/federation) to avoid last-minute mix-ups.
- Get sufficient sleep — the exam is only 90 minutes but performance-based questions demand sustained focus early on.
- Prepare your government-issued photo ID and, for online testing, ensure a quiet, clear workspace that meets OnVUE proctoring requirements.
- Plan your pacing: with up to 90 questions in 90 minutes, budget roughly a minute per question and flag-and-return on anything that stalls you.

Official sources

- CompTIA — CompTIA Security+ (SY0-701) Certification Exam Objectives (Version 5.0): https://assets.ctfassets.net/82ripq7fjls2/6TYWUym0Nudqa8nGEnegjG/0f9b974d3b1837fe85ab8e6553f4d623/CompTIA-Security-Plus-SY0-701-Exam-Objectives.pdf
- CompTIA — CompTIA Security+ Certification Page: https://www.comptia.org/en-us/certifications/security/
- U.S. Bureau of Labor Statistics — Occupational Employment and Wage Statistics, May 2025 — Information Security Analysts (SOC 15-1212): https://www.bls.gov/oes/current/oes151212.htm