

CompTIA Security+ Flashcards — 60 High-Yield Cards

Printable flashcard deck: 60 cards, generated from the TemplateForge concept list for this guide.

HOW TO PRINT:

1. Print this file double-sided on Letter, flip on SHORT edge.
2. Front pages show the Terms; each back page shows that same page's answers in the identical grid layout.
3. Cut along the grid lines. The card number in the top-right corner matches each front to its back.

STUDY TIP: quiz yourself with the Anki deck (import the CSV into Anki — it's free — note type Basic, fields by comma). Review daily; space your reviews instead of cramming.

Source: TemplateForge study guide concept list. Facts are the guide's own verified content — always confirm exam details at the official testing organization's website.

CIA triad

#1

Confidentiality

#2

Integrity

#3

Availability

#4

Non-repudiation

#5

AAA framework

#6

#1

CIA triad

Confidentiality (only authorized people see data), Integrity (data is accurate and unmodified), Availability (data is accessible when needed).

Tip: Match the missing letter to the control: encryption shows confidentiality, hashing shows integrity, redundancy shows availability.

Example: A login prompt protects confidentiality; a checksum protects integrity; a standby server protects availability.

#2

Confidentiality

The property that data is readable only by authorized parties.

Tip: Encryption, access controls, and least privilege serve confidentiality.

Example: Payment details are encrypted at rest so a database leak stays unreadable.

#3

Integrity

The property that data is accurate and has not been tampered with.

Tip: Hashing detects changes; digital signatures prove origin too.

Example: A file's SHA-256 hash changes when malware injects code into it.

#4

Availability

The property that systems and data are accessible to authorized users when needed.

Tip: Redundancy, backups, and DDoS protection serve availability.

Example: A failover cluster keeps the storefront up during a server outage.

#5

Non-repudiation

The inability to deny an action; proof of origin and delivery.

Tip: Digital signatures and audit logs provide non-repudiation.

Example: A signed contract email proves the sender cannot deny sending it.

#6

AAA framework

Authentication (prove identity), Authorization (what you may do), Accounting (tracking what you did).

Tip: Questions about access usually hinge on the A that fits: prove, permit, or record.

Example: The user logs in (authentication), opens only their folder (authorization), and logs are kept (accounting).

Least privilege

#7

Virus

#8

Worm

#9

Trojan

#10

Ransomware

#11

Spyware

#12

#7

Least privilege

Users and processes get only the access required to do their jobs, nothing more.

Tip: Privilege creep is the exam villain; remove stale rights on role change.

Example: A support agent has read access to tickets but cannot edit billing records.

#8

Virus

Malware that attaches to a host file or program and spreads when the host runs.

Tip: A virus needs a host and a user action to spread.

Example: An infected document macro launches the virus when opened.

#9

Worm

Self-replicating malware that spreads over networks without user action.

Tip: Worms spread automatically; patching and segmentation stop them.

Example: A worm hops between unpatched servers using a known SMB flaw.

#10

Trojan

Malware disguised as legitimate software; does not self-replicate.

Tip: Trojans arrive as gifts; delivery is via phishing or fake apps.

Example: A fake video player installs a keylogger on the user's machine.

#11

Ransomware

Malware that encrypts files or systems and demands payment for decryption.

Tip: Mitigation is back up, isolate, and restore; never pay as a policy.

Example: A hospital's files are encrypted; the team restores from isolated backups.

#12

Spyware

Malware that secretly gathers information about the user.

Tip: Spyware reports out; network egress monitoring catches it.

Example: Background software logs keystrokes and browser history.

Adware

#13

Rootkit

#14

Keylogger

#15

Botnet

#16

Logic bomb

#17

Fileless malware

#18

#13

Adware

Software that displays unwanted advertisements, often bundled with free apps.

Tip: Adware is nuisance plus data collection; remove and block.

Example: Pop-ups appear after installing a free downloader.

#14

Rootkit

Malware that hides itself and its activity, often at the kernel level.

Tip: Rootkits hide deep; reimaging beats cleaning.

Example: A kernel rootkit conceals its process from the task manager.

#15

Keylogger

Malware or hardware that records keystrokes to capture credentials.

Tip: Credential theft via typing; MFA blunts the value.

Example: A USB dongle records the password typed at a shared kiosk.

#16

Botnet

A network of compromised devices (bots) controlled by a command-and-control server.

Tip: Bots are rented for DDoS and spam; C2 traffic is the tell.

Example: A thousand infected IoT cameras flood a site with DDoS traffic.

#17

Logic bomb

Malicious code that triggers on a specific condition, such as a date or event.

Tip: The payload waits; audit code and watch for insider threats.

Example: A disgruntled admin's script deletes backups on their termination date.

#18

Fileless malware

Malware that runs in memory without writing files to disk.

Tip: Memory-resident attacks evade antivirus; EDR and memory scans catch them.

Example: PowerShell runs a script directly in memory; nothing lands on disk.

#19

Cryptojacking

#20

Social engineering

#21

Firewall

#22

Next-generation firewall (NGFW)

#23

**Intrusion detection/prevention
(IDS/IPS)**

#24

DMZ

#19

Cryptojacking

Hijacking a device's computing power to mine cryptocurrency.

Tip: Watch for high CPU and unexpected mining traffic.

Example: A browser tab mines crypto at night using the office workstations.

#20

Social engineering

Manipulating people into breaking security procedures.

Tip: The target is the human; training is the defense.

Example: An attacker poses as IT support to collect a password.

#21

Firewall

Filters traffic between networks by rules: allow, deny, or drop.

Tip: Order and specificity matter; default deny is safest.

Example: The edge firewall permits only web and mail ports from the internet.

#22

Next-generation firewall (NGFW)

Firewall with application awareness, IDS/IPS, and identity features.

Tip: NGFW sees the app, not just the port.

Example: The NGFW blocks video chat traffic even on an open HTTPS port.

#23

Intrusion detection/prevention (IDS/IPS)

IDS monitors and alerts; IPS blocks inline.

Tip: Signature, anomaly, and behavioral detection feed both.

Example: The IPS drops traffic matching a known exploit signature.

#24

DMZ

A perimeter network hosting public services, isolated from the internal LAN.

Tip: Public servers live here so a breach does not reach internal hosts.

Example: The web and mail servers sit in the DMZ behind two firewalls.

#25

VLANs and subnetting

#26

Network access control (NAC)

#27

Port security and 802.1X

#28

Proxy and forward/transparent proxies

#29

Load balancing

#30

VPN and tunneling

#25

VLANs and subnetting

Logical network separation within a switch (VLAN) and IP ranges (subnets).

Tip: Segmentation limits blast radius and lateral movement.

Example: The guest Wi-Fi VLAN cannot reach the finance VLAN.

#26

Network access control (NAC)

Enforcing security posture before devices join the network.

Tip: NAC checks health: patched, AV running, compliant.

Example: An unpatched laptop is placed in a quarantine VLAN until fixed.

#27

Port security and 802.1X

Port security limits MACs per port; 802.1X authenticates devices at the port.

Tip: Physical-layer authentication stops strangers plugging in.

Example: A printer port accepts only the printer's MAC address.

#28

Proxy and forward/transparent proxies

Intermediaries that relay traffic; forward proxies serve clients, transparent ones work invisibly.

Tip: Proxies filter, cache, and log web traffic.

Example: All user web traffic exits through a filtering proxy.

#29

Load balancing

Distributing traffic across servers for availability and scale.

Tip: Balancers add health checks and TLS termination.

Example: A load balancer spreads requests across four web servers.

#30

VPN and tunneling

Secure encrypted tunnels over untrusted networks (site-to-site, remote access).

Tip: IPSec and TLS VPNs protect data in transit.

Example: A remote worker's laptop connects through an encrypted VPN tunnel.

SDN and SD-WAN

#31

Logging and log sources

#32

SIEM

#33

SOAR

#34

Host and network monitoring

#35

Baselining and anomaly detection

#36

#31

SDN and SD-WAN

Software-defined networks centralize control; SD-WAN routes WAN traffic dynamically.

Tip: Central policy and path intelligence improve security and cost.

Example: SD-WAN fails over to a second link when the primary degrades.

#32

Logging and log sources

Records from systems, apps, firewalls, and endpoints that enable detection.

Tip: Centralize logs; you cannot investigate what you never recorded.

Example: Firewall and domain logs stream to the central log server.

#33

SIEM

Security information and event management: collects, correlates, and alerts.

Tip: SIEM ties events together across sources; tune to reduce noise.

Example: The SIEM correlates a failed-login spike with a new malware signature.

#34

SOAR

Security orchestration, automation, and response: runbooks and automation.

Tip: SOAR automates the response steps SIEM detects.

Example: A phishing alert auto-quarantines the email and disables the link.

#35

Host and network monitoring

Watching endpoints (EDR) and traffic (NIDS) for signs of compromise.

Tip: Both matter; hosts see process-level, network sees lateral movement.

Example: EDR blocks a suspicious process; NIDS flags the exfiltration stream.

#36

Baselining and anomaly detection

Learning normal behavior, then flagging deviations.

Tip: Anomalies are hints, not proof; verify before acting.

Example: A server never calls out at night; tonight it dials an unknown IP.

#37

Log integrity and retention

#38

Time synchronization

#39

False positives and tuning

#40

Adversarial AI and shields

#41

Blockchain and ledgers

#42

Cloud and hybrid visibility

#37

Log integrity and retention

Protecting logs from tampering and keeping them per policy.
Tip: Append-only storage and time sync make logs trustworthy.
Example: Logs hash to remote storage, so an attacker cannot rewrite history.

#38

Time synchronization

Consistent timestamps across systems (NTP) for accurate correlation.
Tip: One shared clock makes event order provable.
Example: All devices sync to the same NTP stratum for incident timelines.

#39

False positives and tuning

Alerts that are not real attacks; adjust rules and thresholds.
Tip: Over-alerting causes alert fatigue; tune, do not ignore.
Example: The rule now ignores expected backup traffic and catches the rest.

#40

Adversarial AI and shields

Attackers using AI (deepfakes, automated phishing) and AI-based defenses.
Tip: AI accelerates both sides; verify media and user identity.
Example: A deepfake CEO voice is used in a phishing attempt.

#41

Blockchain and ledgers

Distributed, tamper-evident records; useful for provenance and logs.
Tip: Ledger integrity helps where append-only truth matters.
Example: A supply-chain ledger proves each hardware part's origin.

#42

Cloud and hybrid visibility

Logs and control across on-prem and cloud workloads.
Tip: One pane of glass: unify clouds and on-prem logs.
Example: On-prem and AWS logs merge into a single SIEM view.

#43

Uptime and monitoring metrics

#44

Incident response process

#45

Preparation

#46

Detection and analysis

#47

Containment

#48

Eradication

#43

Uptime and monitoring metrics

Availability baselines, thresholds, and alerting for services.

Tip: Monitor the service, not just the box.

Example: The ERP monitor alerts when response time exceeds two seconds.

#44

Incident response process

NIST phases: preparation, detection and analysis, containment, eradication, recovery, lessons learned.

Tip: Know the phase order; each phase has its tools.

Example: After detection, the team contains the host before eradicating the malware.

#45

Preparation

Building plans, teams, tooling, and training before an incident.

Tip: The plan saves time when the alarms fire.

Example: A playbook documents roles, contacts, and evidence procedures.

#46

Detection and analysis

Recognizing an incident from alerts, logs, and indicators and determining scope.

Tip: Verify and triage; not every alert is an incident.

Example: A spike in failed logins is analyzed and confirmed as a brute force.

#47

Containment

Isolating the incident to stop spread: disconnect, quarantine, segment.

Tip: Contain first, then investigate; it limits damage.

Example: The infected laptop is pulled off the network immediately.

#48

Eradication

Removing the root cause: delete malware, patch, fix the hole.

Tip: Eradication removes the attacker's foothold.

Example: The team wipes the host and patches the exploited service.

#49

Risk assessment

#50

Qualitative risk analysis

#51

Quantitative risk analysis

#52

Risk register

#53

Risk response strategies

#54

Risk appetite and tolerance

#49

Risk assessment

Identifying, analyzing, and evaluating risks to decide responses.

Tip: Risk is likelihood times impact; quantify where possible.

Example: The team rates the data-breach risk high after a vendor exposure.

#50

Qualitative risk analysis

Rating risks by categories and judgment: high, medium, low.

Tip: Fast and subjective; use scales consistently.

Example: A tabletop rates the phishing risk as high probability, high impact.

#51

Quantitative risk analysis

Numeric analysis: SLE, ARO, ALE, and expected loss.

Tip: ALE equals SLE times ARO; show the math.

Example: ALE \$50,000 times ARO 0.2 equals \$10,000 expected annual loss.

#52

Risk register

The living list of risks: description, owner, rating, response, status.

Tip: Every risk needs an owner, a response, and a review date.

Example: The register tracks the legacy system risk with a patch plan.

#53

Risk response strategies

Accept, avoid, mitigate, transfer (and opportunity equivalents: exploit, share, enhance).

Tip: Match the verb to the situation: pool, dodge, reduce, or insure.

Example: The team buys cyber insurance to transfer residual breach cost.

#54

Risk appetite and tolerance

How much risk the organization is willing to take.

Tip: Appetite is strategic; tolerance is per-risk threshold.

Example: The board accepts high innovation risk but zero compliance risk.

#55

Risk ownership

#56

Risk and control self-assessment

#57

Supply chain risk

#58

Third-party risk management

#59

Risk management frameworks

#60

Armored and clean environments

#55

Risk ownership

Assigning a named owner responsible for each risk and its response.

Tip: Without an owner, a risk is noise.

Example: The CFO owns the payment-fraud risk and reviews it quarterly.

#56

Risk and control self-assessment

Teams self-evaluate risk and control effectiveness.

Tip: Self-assessments feed the audit and program priorities.

Example: Each department completes an annual control self-check.

#57

Supply chain risk

Vendors and partners introduce risk: software, hardware, services.

Tip: Third parties inherit your weakest link; assess before contracting.

Example: A new SaaS tool is vetted for security before sign-off.

#58

Third-party risk management

Vendor assessments, contracts, and ongoing monitoring of suppliers.

Tip: Contract the requirements; review the evidence regularly.

Example: The vendor must show a current audit report and 30-day breach notice.

#59

Risk management frameworks

NIST RMF, ISO 27001, and FAIR structure how risk is managed.

Tip: Frameworks give process; match the question to the framework name.

Example: The team follows NIST RMF: categorize, select, implement, assess, authorize, monitor.

#60

Armored and clean environments

Controlled environments for handling risky content or assets.

Tip: Use isolated analysis environments for untrusted code.

Example: Attachments open inside a disposable virtual machine.