CompTIA Security+ (SY0-601) Cheat Sheet

One-page cram sheet for threats, architecture, implementation, incident response, and governance.

Best for	Focus	Use with
Legacy review notes or comparison to SY0-701	Core security ideas and high-yield comparisons	Use with ports sheet and commands sheet

1. Threats, attacks, and vulnerabilities

Phishing variants	Distinguish phishing, spear phishing, whaling, vishing, and smishing by target and channel.
Malware types	Know ransomware, trojan, worm, spyware, rootkit, and fileless behavior at a high level.
Vulnerability management	Scanning finds issues; validation, prioritization, remediation, and rescanning close the loop.
Social engineering	Tailgating, shoulder surfing, dumpster diving, impersonation, and pretexting remain exam staples.

2. Architecture and design

Segmentation	Use VLANs, DMZs, ACLs, and firewalls to reduce blast radius and isolate trust zones.
Secure protocols	Prefer SSH, HTTPS, SFTP, LDAPS, and SNMPv3 over older plaintext options.
Identity services	MFA, SSO, federation, and directory services show up often in design questions.
Cloud/shared responsibility	Know what the provider secures versus what the customer still owns.

3. Implementation

PKI basics	Certificates bind identities to keys; know CA, CSR, CRL, OCSP, and certificate lifecycle basics.
Wireless security	WPA2/WPA3, enterprise auth, captive portal, guest isolation, and rogue AP detection matter.
Endpoint hardening	Disable unused services, patch regularly, encrypt storage, and enforce least privilege.
Application security	Input validation, secure coding awareness, and web protection concepts are fair game.

4. Operations and incident response

Logs and baselines	You need both to identify anomalies and investigate incidents efficiently.
Chain of custody	Preserve evidence integrity when collecting and handling incident artifacts.

Containment vs eradication	Stop spread first, remove root cause second, then recover and lessons-learn.
Backups	Recovery planning is useless without tested backups and known RPO/RTO expectations.

5. Governance, risk, and compliance

Risk types	Understand inherent, residual, control, and transfer/accept/avoid/mitigate decisions.
Policies vs standards	Policies set direction; standards define required specifics; procedures explain how.
Training	Security awareness is a control, not an afterthought.
Data handling	Classify, retain, archive, and dispose of data correctly based on sensitivity.