

CompTIA Security+ (SY0-601) Quick Summary

Fast 3-5 minute refresh for the controls, comparisons, and traps that appeared most often.

Best for Ultra-fast memory refresh	Focus Controls, incident flow, and key comparisons	Use with Use with cheat sheet for deeper review
--	--	---

1. Ultra-fast refresh

MFA	One of the highest-value controls for many attack paths.
Least privilege	Applies to users, services, devices, and network paths.
Patch + backup	Two of the most exam-relevant operational controls.
Segmentation	Improves both security and containment.

2. Must-know comparisons

SSH vs Telnet	Encrypted vs plaintext remote administration.
HTTPS vs HTTP	TLS-protected web traffic vs cleartext.
SAML vs OAuth vs OpenID Connect	Federation, delegated authorization, and identity layer differences.
Symmetric vs asymmetric	Fast shared-key encryption versus public/private-key scenarios.

3. Incident shortcuts

Identify	Confirm the event and scope.
Contain	Limit spread and preserve evidence.
Eradicate	Remove persistence and root cause.
Recover	Restore service and monitor.

4. Exam traps

Hash vs encryption	Hashes verify integrity; encryption protects confidentiality.
Risk reduction vs elimination	Most controls reduce risk; very few eliminate it.
Policy vs procedure	Direction versus step-by-step action.
Vulnerability vs exploit	Weakness versus code/technique that abuses it.