Security+ SY0-701 Quick Summary

Fast 3-5 minute refresh of the terms and choices that show up most often.

BEST FOR	FOCUS	USE WITH
Rapid memory reset right before question sets	Exam traps, control mapping, and response order	Cheat Sheet + Commands Sheet

1. Memorize these pairs

RBAC / ABAC / DAC / MAC - Role / attributes / owner discretion / mandatory labels.
Hashing / Encryption / Signing - Integrity / confidentiality / authenticity + integrity.
MTTR / MTTF / MTBF - Repair / failure / reliability between failures.
RTO / RPO - Recovery time target / acceptable data loss window.
Hot / Warm / Cold site - Fastest and costliest / balanced / slowest and cheapest.

2. Scenario shortcuts

Lateral movement - Think segmentation, NAC, least privilege, and EDR visibility.
Credential theft - Think MFA, password managers, disable reuse, and conditional access.
Public web app risk - Think WAF, patching, secure coding, and input validation.
Ransomware - Think isolation, immutable backups, restore testing, and containment first.
Insider risk - Think logging, separation of duties, DLP, and rapid offboarding.

3. Protocol picks

22 SSH - Remote shell, encrypted administration.
389 vs 636 - LDAP is cleartext-capable; LDAPS adds TLS.
80 vs 443 - HTTP is cleartext; HTTPS adds TLS.
49 vs 1812/1813 - TACACS+ separates auth model; RADIUS commonly handles AAA.
53 TCP vs UDP - UDP for most lookups; TCP for zone transfer and larger responses.

4. Order matters

Incident handling - Contain first when damage is active, then eradicate and recover.
Change control - Assess impact, approve, test, implement, document, review.
Vuln remediation - Validate finding, prioritize by risk, patch or compensate, then verify.
Forensics - Preserve chain of custody and volatile data before altering evidence.
Recovery - Bring back critical services first, then validate integrity and monitoring.