Security+ SY0-701 Cheat Sheet

High-yield Security+ review for the last pass before practice tests.

BEST FOR	FOCUS	USE WITH
Last review before mini test or exam session	Core concepts, common controls, ports, and incident flow	Quick Summary + Ports Sheet

1. Core security concepts

CIA + AAA - Confidentiality, integrity, availability; pair with authentication, authorization, and accounting.
Zero Trust - Verify explicitly, least privilege, assume breach; trust is never granted by network location alone.
Control types - Preventive, detective, corrective, deterrent, compensating, and directive are common exam pairings.
Change management - Approval, testing, rollback, documentation, and versioning reduce operational risk.
PKI basics - Certificates bind identities to public keys; understand CA, intermediate CA, CRL, and OCSP.

2. Threats and attack patterns

Phishing variants - Know phishing, spear phishing, whaling, smishing, and vishing by delivery channel and targeting.
Common malware - Ransomware, trojans, worms, spyware, and rootkits differ by spread, stealth, and impact.
Password attacks - Brute force, dictionary, spraying, stuffing, and rainbow table attacks have different indicators.
Web attacks - SQL injection, XSS, CSRF, directory traversal, and SSRF appear often in scenario questions.
Supply chain risk - Third-party compromise can enter through vendors, signed software, libraries, or managed services.

3. Network and system defense

Segmentation - Use VLANs, subnets, ACLs, and internal firewalls to reduce lateral movement.
Secure protocols - Prefer SSH, HTTPS, SFTP, SNMPv3, LDAPS, and IPsec over legacy cleartext options.
Wireless - WPA3 is strongest; enterprise mode uses 802.1X and a RADIUS-backed identity flow.
Hardening - Disable unused services, patch quickly, enforce baselines, and turn on logging.
Vulnerability management - Scan, validate, prioritize by risk, remediate, then rescan.

4. Identity, response, and recovery

MFA factors - Something you know, have, are, or do; avoid confusing location as a factor category.
Access models - RBAC maps to job role, ABAC to attributes, DAC to owner choice, MAC to classification rules.
Incident flow - Preparation, detection, analysis, containment, eradication, recovery, and lessons learned.
Backups - Offline or immutable copies reduce ransomware impact; test restore, not just backup success.
BCP vs DRP - BCP keeps business running; DRP restores systems and data after disruption.