MASTER SECURITY+ KEY:

* 802.1AE (MACsec) – Secure Layer 2 communication (rare, but seen on higher-end questions)
* 802.1AE (MACsec) – A Layer 2 encryption protocol used to secure Ethernet traffic on wired networks. Primarily used in high-security enterprise environments to provide data confidentiality and integrity.
* 802.1X
* AAA (Authentication, Authorization, and Accounting) - a security framework that ensures only authorized individuals are able to access resources.
* AAA (Authentication, Authorization & Accounting)
* ABAC (Attribute Based Access Control) - evaluates attributes to determine the access.
* Acceptable use policy (AUP)
* Access badge
* Access control list (ACL)
* Access control models – Mandatory, Discretionary, Role-based, Rule-based, Attribute-based, Time-of-day
* Access control vestibule
* Account lockout / impossible travel
* ACL (Access Control List) - list of rules that specifies which users or systems are granted or denied access to a particular object or system resource.
* Acquisition (forensics)
* Active vs. passive devices
* Adaptive identity (Zero Trust)
* Adaptive identity – Identity that considers device health, location, time, and behavioral traits
* Add every bullet above to your existing Acronym/Term bank.
* Advanced Encryption Standard (AES, AES-256)
* Advanced persistent threat (APT)
* AES (Advanced Encryption Standard) - a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.
* Agent / agent-less monitoring
* Air-gapped network
* Air-gapped systems – physically isolated networks
* AIS (Automated Indicator Sharing) - service provided by CISA that enables real-time exchange of machine-readable cyber threat indicators and defensive measures between public and private sector organizations.
* AIS (Automated Indicator Sharing) – CISA-supported intel sharing system
* ALE / ARO / SLE
* Allow-list / deny-list
* Amplified & reflected DDoS
* Analyzing
* Anomalous-behaviour recognition – Risky, Unexpected, Unintentional
* API (Application Programming Interface) security & integrations
* Application allow list, Isolation (quarantine VLAN), Decommissioning (as mitigations)
* Approaching the task carefully
* Approval process (change management)
* APT (Advanced Persistent Threat) - a type of cyber attack in which an unauthorized user gains access to a system or network and remains undetected for an extended period of time.
* Architecture models not in key – Serverless, Infrastructure-as-Code (IaC), Software-Defined Networking (SDN), Centralized vs Decentralized, Microservices, High-availability
* ARP (Address Resolution Protocol) - a protocol used to map an IP address to a physical MAC address.
* ASLR (Address Space Layout Randomization) - a technique used to prevent attackers from exploiting vulnerabilities in software by randomizing the location of key data areas in memory.
* Attack surface
* Attestation & acknowledgement
* Attestation – used to verify software/hardware state, especially in TPM/Secure Enclave systems
* Audit committee & right-to-audit clause
* Authentication header (AH)
* Authorization models (ABAC, RBAC, DAC, MAC)
* Automated Indicator Sharing (AIS)
* Automated Indicator Sharing (AIS) – DHS/CISA framework for sharing threat intel
* Automation caveats – Single point of failure, Technical debt, Ongoing supportability
* Availability, confidentiality, integrity (CIA triad)
* Backup types – onsite, offsite, frequency, snapshots, journaling, replication
* Backup-specific – Snapshots, Journaling, Replication
* BCP (Business Continuity Planning) - detailed strategy and set of systems for ensuring an organization’s ability to prevent or rapidly recover from a significant disruption to its operations. The plan is essentially a playbook for how any type of organization—such as a private-sector company, a government agency or a school will continue its day-to-day business during a disaster scenario or otherwise abnormal conditions.
* BDPU Guard (Bridge Protocol Data Units) - BDPU guard is a feature that defends the layer 2 STP topology against BDPU-related threats.
* Below is a “gap-list”—every Security+ SY0-701 term, acronym, protocol, concept or idea that appears in the official CompTIA Exam Objectives but does not appear anywhere in the uploaded Acronym Key.docx.  
  The items are grouped roughly the way the objectives are laid out so you can paste them into your own notes or flash-card app.
* BIA (Business Impact Analysis) - the BIA should identify the operational and financial impacts resulting from the disruption of business functions and processes.
* BIOS (Basic Input/Output System) - BIOS, or Basic Input/Output System, is software stored on a small memory chip, also known as firmware. BIOS is found on the motherboard. BIOS instructs the computer on how to perform basic functions like booting and keyboard control; it is also used to identify and configure the hardware in a computer such as the hard drive, CPU, memory, and related equipment. Finally, it manages data flow between the computer's operating system (OS) and attached devices.
* BLOB (Binary Large Object Storage) - used by cloud providers as a database for large amounts of text or binary data.
* Block rule (web / DNS / email)
* Blockchain / open public ledger
* Boards / Committees / Government-entities as governance structures
* Bollards, fencing, lighting, sensors (infra-, pressure, microwave, ultrasonic)
* Botnet / command-and-control (C2)
* BPA (Business Partnership Agreement) - agreement between 2 companies that are doing business together in which it is confirmed how much each company should contribute as well as their responsibility and how the profit will be split.
* Brand impersonation
* Breaking down the task
* Brute-force & password-spray attacks
* Bug bounty / responsible disclosure – in ethical hacking/vuln management
* Business continuity & continuity-of-operations (COOP)
* Business email compromise (BEC)
* Business impact analysis (BIA)
* Business Email Compromise (BEC)
* BYOD (Bring Your Own Device) - a policy that allows employees to use their personal devices, such as smartphones or laptops, to access company resources.
* CA (Certificate Authority) - trusted entity that issues digital certificates used to verify the identities of individuals, organizations, websites or devices.
* CAC (Common Access Card) - smart card about the size of a credit card. It is the standard identification for Active Duty United States Defense personnel.
* CAC / PIV / smart-card
* Capacity planning
* Capacity planning (people, tech, infra)
* CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) - a challenge-response test used to distinguish between human and automated users.
* CASB (Cloud Access Security Broker) - software/hardware that sits between users and their cloud service to enforce security policies.
* CASB (Cloud Access Security Broker)
* CBC (Cipher Block Chaining) - a mode of operation for a block cipher -- one in which a sequence of bits are encrypted as a single unit, or block, with a cipher key applied to the entire block. Cipher block chaining uses what is known as an initialization vector (IV) of a certain length. By using this along with a single encryption key, organizations and individuals can safely encrypt and decrypt large amounts of plaintext.
* CCMP – Encryption protocol used in WPA2.
* CER (Certificate) - security files provided and generated by an Certificate Authority. These files help a browser to verify if a website is secure and save to enter, verifying its authenticity. These CER security certificates are usually installed on a web server.
* CER (Crossover Error Rate) - point where FAR and FRR are equal.
* Certificate authorities, chain & root of trust
* Certificate revocation (CRL, OCSP, OCSP-stapling)
* Certificate signing request (CSR)
* Change control artefacts – impact analysis, maintenance window, test results, back-out plan, approvals, version control
* Change-management artefacts – Approval process, Impact analysis, Test results, Back-out plan, Maintenance window, Version control, Stakeholders, Standard operating procedure
* CHAP (Challenge Handshake Authentication Protocol) - challenge-response identity authentication protocol. It depends on a combination of CHAP security credentials and a “shared secret” between the requestor (client) and the authenticator (server), and it does not expose a password.
* Choose-your-own device (CYOD)
* CIA (Confidentiality, Integrity, and Availability) - the three core principles of information security.
* CIRT (Computer Incident Response Team) - a team responsible for responding to and mitigating cyber security incidents.
* Cloud models – IaaS, PaaS, SaaS, public, private, hybrid, multi-cloud, serverless, micro-services, containerisation, virtualization
* Collision Resistance – A property of hash functions.
* Collision & birthday attacks
* Command and Control (C2) – Server used by attackers to control compromised systems.
* Compensating / corrective / detective / deterrent / directive / preventive controls
* Compliance consequences – fines, sanctions, licence loss, reputational damage
* Compliance concepts – Attestation and Acknowledgement, Due-diligence automation, Consequences (fines, sanctions, reputation loss), Right to be forgotten
* Concurrent session usage, Impossible travel, Out-of-cycle logging, Resource inaccessibility, Missing logs (indicators of compromise)
* Confidential vs. sensitive vs. public vs. restricted vs. private vs. critical data
* Configuration enforcement / secure baseline / hardening targets (workstations, servers, switches, routers, IoT, RTOS, SCADA)
* Connection methods – Cellular, Bluetooth (for MDM considerations)
* Container security & backups
* Continuity-of-operations (COOP)
* Control-plane vs. data-plane (Zero Trust)
* Control-plane components – Policy Administrator, Policy Engine, Adaptive Identity, Threat-scope Reduction, Policy-driven Access Control
* Control plane vs data plane – in Zero Trust and SDN
* Cookies – secure, SameSite
* COPE (Corporate-Owned, Personally-Enabled) - a policy that allows employees to use company-owned devices for personal use.
* COPE (Corporate-owned, personally-enabled)
* CRC (Cyclic Redundancy Check) - a mathematical algorithm used to detect errors in data transmission.
* Creating exhaustive list
* CRL (Certificate Revocation List) - first phase of checking if certificate is valid.
* CRL (Certificate Revocation List) – A list of revoked certificates.
* CRL vs. OCSP status checking
* Cryptographic attacks – downgrade, collision, birthday
* CSA (Cloud Security Alliance) - non-profit organization that provides different resources to help Cloud Security Providers (CSPs).
* CSO (Chief Security Officer) - a senior-level executive responsible for overseeing an organization's security program.
* CSP (cloud service provider) - is a third-party company that provides scalable computing resources that businesses can access on demand over a network, including cloud-based compute, storage, platform, and application services.
* CSR (Certificate Signing Request) - a request made by a user or device to a certificate authority for a digital certificate.
* CSR (Certificate Signing Request) – A request sent to a CA for certificate issuance.
* CSRF (Cross-Site Request Forgery) - is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.
* CSRF (Cross Site Request Forgery) - attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.
* CSV (Comma Separated Values) - a file format used to store data in a table-like format, with each row separated by a comma.
* CVE (Common Vulnerabilities and Exposure) - list of vulnerabilities created by MITRE.
* CVSS (Common Vulnerabilities Scoring System) - ranking of vulnerabilities and their severity.
* CVSS / CVE – Scoring and enumeration systems for vulnerabilities
* Cyber-insurance (risk transfer)
* CYOD (Choose Your Own Device) - company has set of devices that employees can choose to use for work.
* DAC (Discretionary Access Control) - restricting access to objects based on the identity of subject.
* DANE / DNSSEC (DNS security extensions)
* DANE (DNS-Based Authentication of Named Entities) – Uses DNSSEC to bind TLS certificates to DNS names
* DANE (DNS-based Authentication of Named Entities) – A method that uses DNSSEC to bind X.509 certificates to DNS names, allowing clients to validate TLS certificates without a CA.
* Data States – Data at rest, in transit, in use.
* Data inventory, retention & right-to-be-forgotten
* Data in rest / transit / use
* Data loss prevention (DLP)
* Data masking, tokenisation, obfuscation, steganography
* Data sovereignty & geo-location restrictions
* Data-plane components – Policy Enforcement Point (PEP), Implicit Trust Zone, Subject/System
* Data sovereignty & Geolocation
* Data states explicitly – Data at rest, Data in transit, Data in use
* DDoS (Distributed Denial of Service) - a type of cyber attack in which multiple systems are used to flood a target server or network with traffic, causing it to become unavailable.
* Deception Technology – Includes honeypots, honeyfiles, honeynets, honeytokens.
* Deception & disruption tech – honeypot, honeyfile, honeynet, honeytoken
* Deception / disruption tech – Honeypot, Honeynet, Honeyfile, Honeytoken
* Default credentials threat
* Delegated administration / privileged access management (PAM, just-in-time, password vaulting)
* Denial-of-Service (DoS / DDoS)
* Dependent service discovery & legacy constraint identification
* DES (Data Encryption Standard) - is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) that was widely used in the past but is now considered insecure.
* Device-placement terms – Fail-open, Fail-closed, Inline vs Tap/Monitor
* DevSecOps: CI/CD, guard-rails, IaC templates
* DHCP (Dynamic Host Configuration Protocol) - a protocol used to automatically assign IP addresses and other network settings to devices on a network.
* Digital Signature – Verifies authenticity and integrity using asymmetric encryption.
* Digital certificate types – wildcard, self-signed, third-party, EV
* Digital signature (integrity, non-repudiation)
* Directory traversal / injection attacks
* Disaster recovery sites – hot, cold, warm, geographically dispersed
* DKIM, SPF, DMARC email records
* DMZ (Demilitarized Zone) - a network segment that is isolated from the internal network and is used to provide public-facing services, such as web servers or email servers.
* DNS (Domain Name System) - a system that translates domain names into IP addresses.
* DNS attacks – poisoning, tunnelling, cache-snooping
* DNSSEC – DNS security extension to protect integrity of DNS records
* DoS (Denial of Service) - a type of cyber attack in which a server or network is overwhelmed with traffic, causing it to become unavailable.
* Downgrade Attack – Forces use of older, insecure protocol versions.
* Downtime, fail-open vs. fail-closed
* DPO (Data Protection Officer) - DPO makes sure that the organization is correctly protecting individuals personal data according to current legislation.
* DRP (Disaster Recovery Plan) - preparing for any type of disaster that could occur.
* Due diligence vs Due care
* EAP (Extensible Authentication Protocol) - architectural framework that provides extensibility for authentication methods for commonly used protected network access technologies such as IEEE 802.1X-based wireless access, IEEE 802.1X-based wired access and Point-to-Point Protocol (PPP).
* EAP methods (PEAP, EAP-TLS)
* Eavesdropping & on-path / MITM / SSL-stripping
* ECDHE / ECDSA – Used in modern key exchange and digital signatures.
* ECDSA / ECDHE – modern elliptic curve crypto for signing and key exchange
* EFS (Encrypting File System) - a feature in Windows that allows files and folders to be encrypted using a user's public key. Windows' EFS feature allows you to easily encrypt and decrypt files on your Windows NTFS drives. Once you’ve encrypted files with this tool, other people won’t be able to access them unless they have your password.
* Embedded & IoT security (firmware, supply-chain, end-of-life)
* EMI (Electromagnetic Interference) - interference caused by electromagnetic waves, which can disrupt the functioning of electronic devices.
* EMP (Electromagnetic Pulse) - a burst of electromagnetic radiation that can cause damage to electronic devices.
* Encryption levels – full-disk, partition, volume, database, record, transport
* Encryption levels not listed – Partition-level, File-level, Volume-level, Database-level, Transport/Communication-level
* Endpoint detection & response (EDR/XDR)
* Enumeration (asset management)
* Ephemeral credentials and session keys
* Escalation (automated ticketing)
* ESP (Encapsulating Security Payload) - is security payload is an individual protocol in IPSec. ESP is responsible for the CIA triad of security (Confidentiality, Integrity, Availability), which is considered significant only when encryption is carried along with them. Securing all payload/ packets/ content in IPv4 and IPv6 is the responsibility of ESP.
* ESP / AH (Encapsulated Security Payload / Authentication Header) – IPsec components.
* Even if not acronyms, these terms are heavily tested:
* Explicit key length / key-exchange algorithm (exam may ask about choosing correct size or DH/ECDH)
* Exposure factor & CVSS/CVE scoring
* Exposure factor – used in ALE formulas
* Exposure factor – Proportion of asset loss when a threat is realized
* Fail-over testing & simulation / tabletop exercise
* False Positive / False Negative – terms in vulnerability scanning
* FAR (False Acceptance Rate) - metric used to measure the likelihood of granting access to an unauthorized user.
* FDE (Full Disk Encryption) - security technique that encrypts all data stored on a disk or storage device, including the operating system, applications, and user data.
* Federation (SAML, OAuth/OIDC, Kerberos)
* File-integrity monitoring (FIM)
* File integrity monitoring (FIM) – Compares system files to known good baselines
* Firewall types – NGFW, UTM, layer 4/7, WAF, screened subnet rules
* FISMA (Federal Information Security Management Act) - FISMA requires federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
* Forensics phases – legal hold, acquisition, preservation, chain-of-custody, reporting
* FQDN (Fully Qualified Domain Name)
* FQDN (Fully Qualified Domain Name) – A complete domain name that specifies an exact location in the DNS hierarchy, including the hostname and domain (e.g., mail.example.com).
* FRR (False Rejection Rate) - metric used to measure the likelihood of denying access to an authorized user.
* FTP (File Transfer Protocol) - a protocol used to transfer files between computers over a network. Port 21.
* Gap analysis
* Gateway email filtering & secure web gateway
* GBAC (Group Based Access Control) - gives access to a group of individuals to the resources that they need.
* GCM (Galois Counter Mode) – Encryption mode used in TLS.
* GCM / CCMP – encryption modes used in TLS/WPA2
* GDPR (General Data Protection Regulation) - regulation in European Union (EU) law on data protection and privacy for individuals within the EU and the European Economic Area (EEA). It came into effect on May 25, 2018 and is enforced by the EU Data Protection Authorities.
* Geofencing / GPS restrictions
* Governance structures – board, committee, ISO/IEC, NIST, GDPR, HIPAA etc.
* GPG (Gnu Privacy Guard) – Free implementation of OpenPGP standard.
* GPS (Global Positioning System) - a system of satellites used to determine the location of a device.
* GRE (Generic Routing Encapsulation) - a protocol used to encapsulate one type of packet within another.
* Guard-rails (automation)
* Guard rails (automation), Continuous integration & testing, API integrations
* Hardening techniques not in key – Endpoint protection, Host-based IPS (HIPS), Disabling ports/protocols, Removal of unnecessary software
* Hash functions (SHA-2/3, RIPEMD, HMAC) & key stretching (bcrypt, PBKDF2, scrypt)
* Hashing vs. Encryption – Hashing is one-way, encryption is reversible (with key).
* HIDS (Host Intrusion Detection System) - HIDS stands for host-based intrusion detection system and represents an application that is monitoring a computer or network for suspicious activities.
* HIDS / HIPS vs. NIDS / NIPS
* High-availability & load-balancing / clustering
* HIPAA (Health Insurance Portability And Accountability Act) - federal law that was enacted in 1996 to protect the privacy and security of patients' personal health information (PHI).
* HMAC (Hash-based Message Authentication Code) - is a cryptographic authentication technique that uses a hash function and a secret key. With HMAC, you can achieve authentication and verify that data is correct and authentic with shared secrets, as opposed to approaches that use signatures and asymmetric cryptography.
* Honey-token deception artefacts
* Host-based firewall rules
* HOTP (HMAC-based One-Time Password) - algorithm used to generate one-time passwords that are used for authentication purposes.
* How to use this list
* HSM (Hardware Security Module) - type of specialized hardware device designed to securely store and manage digital keys and perform cryptographic operations. It can be used to store encryption keys, digital certificates, and other sensitive data.
* HSTS (HTTP Strict Transport Security) - web security policy mechanism used to protect against protocol downgrade attacks and cookie hijacking.
* HTML (Hypertext Markup Language) - is the standard markup language for creating Web pages.
* HTTP (Hypertext Transfer Protocol) - HTTP is the foundation of the World Wide Web, and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message. HTTP uses port 80.
* HTTPS (Hypertext Transfer Protocol Secure) - a secure version of HTTP that uses encryption to protect data in transit. HTTPS uses port 443.
* Hybrid-cloud considerations (network-protection mismatches, third-party vendors, responsibility matrix)
* IaaS (Infrastructure as a Service) - a cloud computing model in which infrastructure resources, such as servers and storage, are provided by a third-party provider.
* IAM (Identity and Access Management) - a cybersecurity practice that enables IT administrators to restrict access to organizational resources so that only the people who need access have access.
* ICMP (Internet Control Message Protocol) - a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.
* ICS / SCADA segmentation & jump-servers
* Identity proofing & adaptive MFA (something you know/have/are/are-doing/where-you-are)
* Identity proofing & Attestation
* IDS (Intrusion Detection System) - a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.
* IEEE (Institute of Electrical and Electronics Engineers) - The IEEE describes itself as the world's largest technical professional society -- promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members.
* IKE (Internet Key Exchange) - a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN).
* IKE (Internet Key Exchange) – Used in IPsec VPNs.
* IMAP (Internet Message Access Protocol) - an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. IMAP uses port 143.
* Independent third-party assessment
* Indicators of Compromise (IOCs) – Signs like “impossible travel,” blocked content, beaconing, etc.
* Indicators of compromise – resource consumption, missing logs, concurrent sessions etc.
* Infrastructure-as-Code security (templating, drift detection)
* Infrastructure-as-Code (IaC) – Templates and scripts used to provision and secure environments
* Insurance vs. mitigation vs. avoidance vs. acceptance strategies
* Integrity verification (hash, digital sig, code-signing)
* Interpreting the user's request
* IoT (Internet Of Things Devices) - physical devices that are connected to the internet and that can exchange data with each other.
* IP (Internet Protocol) - a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
* IPS (Intrusion Prevention System) - a network security technology that goes beyond the capabilities of an IDS (Intrusion Detection System) by actively preventing identified threats from being carried out. An IPS monitors network traffic, just like an IDS, but it can also take action to prevent attacks.
* IPS/IDS signature & anomaly detection
* IPv4 (Internet Protocol version 4) - an IPv4 address is a 32-bit address that is usually represented in dotted decimal notation, with a decimal value representing each of the four octets (bytes) that make up the address.
* IPv6 (Internet Protocol version 6) - a network protocol that serves as the successor to IPv4. The purpose of IPv6 is to provide a larger address space for the internet as the number of connected devices continues to grow. One of the main differences between IPv6 and IPv4 is the size of the address space. IPv4 uses 32-bit addresses, allowing for approximately 4.3 billion unique addresses. In contrast, IPv6 uses 128-bit addresses, which allows for an almost unlimited number of unique addresses.
* ISA (Interconnection Security Agreement) - a document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities.
* ISO (International Organization for Standardization) - an international standard-setting organization.
* ISP (Internet Service Provider) - a company that provides Internet access to customers.
* IV (Initialization Vector) – A random or pseudo-random value used with a secret key to encrypt data. Ensures uniqueness and randomness in encryption blocks.
* Jail-breaking / side-loading mobile threats
* JIT (Just-in-time access) – temporary privilege escalation
* Journaling (database resilience)
* JSON (JavaScript Object Notation) - a lightweight data interchange format.
* Just-in-time permissions, Ephemeral credentials (PAM)
* Keep the Exam Objectives PDF handy—CompTIA may still introduce minor tweaks, but with the union of your current Acronym Key and the list above you now have 100 % coverage of every named concept CompTIA publishes for the SY0-701 test.
* Key Security+ Acronyms and Definitions
* Key Escrow – A third-party holds a copy of the encryption key for recovery purposes.
* Key Stretching – Techniques like bcrypt, scrypt, and PBKDF2 that make brute force attacks harder by increasing hashing workload.
* Key Exchange – The process of securely sharing cryptographic keys, often via Diffie-Hellman.
* Key escrow / key management systems / HSM / TPM / secure enclave
* Key-management system (KMS)
* Key Risk Indicators (KRIs), Risk threshold
* Key wrapping – Encrypting one key with another, often used in key exchange or transport
* Key Wrapping – The process of encrypting one encryption key with another. Often used during key exchange or in secure key storage mechanisms.
* KMS (Key Management System) – Centralized service for generating, storing, and rotating encryption keys
* KPI & key-risk-indicator tracking (risk register)
* LDAP (Lightweight Directory Access Protocol) - is a software protocol for enabling anyone to locate data about organizations, individuals and other resources such as files and devices in a network -- whether on the public internet or a corporate intranet. LDAP is a "lightweight" version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is considered lightweight because it uses a smaller amount of code than other protocols.
* Least privilege & Zero Standing Privilege
* Legal hold, Chain of custody, Acquisition, Preservation, E-discovery (digital-forensics steps)
* Legal hold – preserve data for legal/forensic purposes
* Legal hold – Process of preserving data for legal or regulatory investigation
* Lighting & CCTV placement (physical security)
* Load balancer – inline vs. passive tap
* Load-balancing vs Clustering (high availability)
* Logic bomb / time-of-check-time-of-use race conditions
* MAC (Media Access Control) - a unique identifier assigned to a network interface controller (NIC).
* MAC (Mandatory Access Control) - limiting access to resources based on the sensitivity of information.
* Malicious code types – virus, worm, trojan, ransomware, rootkit, spyware, keylogger, bloatware
* Master Security+ (SY0-701) Term List
* MCSP (Managed Cloud Service Provider) - provides managed cloud services to customers. Managed cloud services are a type of cloud computing service in which a third-party provider manages and delivers cloud computing resources and services to customers over the internet.
* Mean time between failures (MTBF) / to repair (MTTR) / to detect (MTTD)
* Memory injection & ASLR mitigation
* MFA (Multi-Factor Authentication) - a security feature that requires multiple forms of authentication to access a resource.
* Micro-segmentation & software-defined networking (SDN)
* Microservices – Application architecture broken into modular services with API communication
* Misinformation / Disinformation
* MITB (Man In The Browser) - an MITB attack injects malicious software (malware) into a victim's web browser. The malware typically exploits vulnerabilities in the browser or its plugins to intercept and manipulate data exchanged between the browser and the websites the user visits.
* MITM (Man-in-the-Middle) - a type of cyber attack in which an attacker intercepts communications between two parties in order to either steal or change the data in transit.
* Mobile connection methods – cellular, Wi-Fi, Bluetooth, NFC
* Monitoring activities – aggregation, alerting, scanning, reporting, archiving
* MSSP (Managed Security Service Provider) - provides managed security services to customers, typically on a subscription basis.
* MTA / MDA / MUA – Mail transfer/ delivery/ user agents (used in email security questions)
* MTBF (Mean Time Between Failures) - average amount of time between system failure which shows how reliable a system is.
* MTTD (Mean Time To Detect) - average time it takes for an organization to detect a security incident or breach after it occurs.
* MTTR (Mean Time To Repair) - average time that it takes to fix a system.
* Multi-cloud resilience & risk transference
* Multifactor authentication factors & hardware keys (FIDO/U2F)
* NAC (Network Access Control) - a system used to control access to a network based on the identity of the user or device.
* NAC (posture check, quarantined VLAN)
* NAT (Network Address Translation) - a technique used to map private IP addresses to public IP addresses.
* NDA (Non Disclosure Agreement) - contract that prevents any side of the business to give away the secrets to others.
* Network address translation (source, destination, static, dynamic)
* Network appliances – proxy, jump-server, sensors
* NFC (Near Field Communication) - short-range wireless communication technology that enables data exchange between devices that are within close proximity to each other, typically within a few centimeters.
* NIDS (Network Intrusion Detection System) - a system used to detect unauthorized activity on a network.
* NIPS (Network Intrusion Prevention System) - type of security system that is used to detect and prevent unauthorized access, attacks, and other malicious activity on a network.
* NIST (National Institute of Standards and Technology) - a U.S. government agency that develops standards for technology and engineering.
* Non-repudiation requirements
* Non-repudiation
* NTFS (New Technology File System) - a file system used in Windows operating systems.
* OAuth (Open Authorization) - open standard protocol that is used for authorization and authentication between applications or services. It allows users to grant access to their private resources stored on one website to another website or application, without sharing their credentials, such as passwords.
* OAuth scopes, SSO flow & IdP/SP roles
* OAuth/OIDC – modern federated identity/authentication frameworks
* Obfuscation – Hiding real data or intent (includes steganography, tokenization, data masking).
* Obsolete / end-of-life hardware risk
* OCSP (Online Certificate Status Protocol) - a protocol used to check the validity of a digital certificate.
* OCSP (Online Certificate Status Protocol) – Checks digital certificate status in real-time.
* Online vs. offline password cracking prevention
* Open-source intelligence (OSINT) & threat feeds (STIX/TAXII, AIS)
* Open public ledger / blockchain (concept)
* Open permissions (cloud misconfiguration)
* Operational-security (OPSEC) for hybrid / remote work
* OSI (Open Systems Interconnection) - conceptual framework that is used to standardize and describe the communication functions of a telecommunication or computing system. The OSI model is divided into seven layers, each with a specific function, that define the communication process between two devices in a network.
* PaaS (Platform as a Service) - a cloud computing model in which a third-party provider offers a platform for developing and deploying applications.
* Packet capture & NetFlow analysis
* PAM (Privileged Access Management) - type of security solution that helps organizations manage and control access to privileged accounts and systems.
* Passwordless authentication (exam buzz-word)
* Patch testing, staging, deployment & exception process
* PBKDF2 – A key stretching technique (Password-Based Key Derivation Function 2).
* PBKDF2 – key stretching function
* PCI DSS (Payment Card Industry Data Security Standard) - a set of security standards for protecting credit card data.
* Pen-test flavours – Known environment, Partially-known, Unknown, Physical, Offensive, Defensive, Integrated; Passive vs Active reconnaissance
* Perfect Forward Secrecy (PFS) – Ensures that session keys cannot be derived from a compromised long-term key.
* PGP (Pretty Good Privacy) - an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.
* Phishing, vishing, smishing, watering-hole, typosquatting, brand-impersonation
* Physical isolation vs. logical segmentation
* Physical-security items not in key – Bollards, Access-control vestibule, Infrared sensor, Pressure sensor, Microwave sensor, Ultrasonic sensor
* Platform diversity, Multi-cloud systems
* Playbooks & run-books (SOAR)
* PMF (Protected Management Frames) - security feature used in Wi-Fi networks to protect against certain types of attacks that can be carried out against wireless management frames.
* Policy engine & policy enforcement point (Zero Trust)
* Policy Engine / Enforcement Point – parts of Zero Trust enforcement
* Policy Administrator – Delivers decisions from the policy engine to the PEP
* Policy Administrator – In Zero Trust Architecture, the component responsible for delivering access decisions (from the policy engine) to the enforcement point. Acts as the messenger between logic and enforcement.
* POP3 (Post Office Protocol version 3) - a protocol used to retrieve email messages from a mail server.
* Port-based security (disabled ports, default service removal)
* Port-security/EAP flavours – EAP-TLS, EAP-TTLS, PEAP
* Power redundancy – UPS, generator, dual feeds
* PPP (Point-to-Point Protocol) - a protocol used to establish a direct connection between two devices.
* Preservation vs. acquisition – Key forensic phases prior to analysis
* Pretexting
* Privacy roles – data subject, controller, processor, owner, custodian
* Privilege escalation & pass-the-hash / replay attacks
* Proxy types – forward, reverse, transparent
* Public Key / Private Key – Used in asymmetric encryption (e.g., RSA).
* Public key infrastructure components – KDC, CA, RA
* Pulling in details to give the best answer
* Quarantine & sandbox analysis (static/dynamic)
* Race condition (TOC/TOU) vulnerabilities
* RADIUS (Remote Authentication Dial-In User Service) - networking protocol that is used to provide centralized authentication, authorization, and accounting (AAA) management for users who connect and use network services. RADIUS is commonly used in enterprise and service provider environments, such as Wi-Fi networks, virtual private networks (VPNs), and dial-up services.
* RAID (Redundant Array of Inexpensive Disks) - a technique used to increase the reliability and performance of data storage.
* RAID levels & SAN vs. NAS
* RAM (Random Access Memory) - computer's short-term memory, where the data that the processor is currently using is stored. Your computer can access RAM memory much faster than data on a hard disk, SSD, or other long-term storage device, which is why RAM capacity is critical for system performance.
* Ransomware stages: initial access, encryption, double extortion
* RAT (Remote Access Trojan) - a type of malware that allows an attacker to remotely control a victim's computer.
* RBAC (Rule Based Access Control) - high level rules that determine how, where and when employees can access spaces or resources.
* RDP (Remote Desktop Protocol) - a protocol used to remotely access and control a desktop computer.
* Recovery metrics – RPO, RTO, MTBF, MTTR
* Recovery site types – Hot, Warm, Cold, Geographic dispersion
* Remote access technologies – VPN (TLS/IPsec, L2TP, SSTP, SD-WAN), SASE
* Replay Attack – Reuse of valid data transmission to impersonate.
* Replay, reflected & forged requests
* Reporting – internal attestation, external audit, independent assessment
* Resource provisioning automation (cloud)
* Responsible disclosure / bug bounty
* REST (Representational State Transfer) - software architectural style that describes the architecture of the web.
* RFID (Radio Frequency Identification) - a technology used for tracking and identifying objects using radio waves.
* RIPEMD (RACE Integrity Primitives Evaluation Message Digest) - a cryptographic hash function.
* Risk appetite (expansionary, conservative, neutral)
* Risk-analysis math pieces missing – Single Loss Expectancy (SLE), Annualized Loss Expectancy (ALE), Annualized Rate of Occurrence (ARO), Exposure factor, Probability & Likelihood
* Risk strategies – Transfer, Avoid, Mitigate, Accept (plus Exception/Exemption)
* Root cause analysis & lessons-learned meeting
* Root of trust
* Router / switch secure baseline (SSH, SNMPv3, BPDU guard, DHCP snooping)
* RTO (Recovery Time Objective) - the maximum amount of time it takes to recover data after a disaster.
* RTOS (Real Time Operating System) - an operating system commonly found in Internet of Things Devices.
* S/MIME (Secure/Multipurpose Internet Mail Extensions) - standard for secure email messaging that provides encryption and digital signing capabilities.
* S/MIME – Used to secure email (encryption + digital signing).
* SaaS (Software as a Service) - a cloud computing model in which a third-party provider offers software applications.
* SaaS vs. on-prem cost & patch considerations
* SAE (Simultaneous Authentication of Equals) - key exchange protocol that provides stronger security and that replaced PSK in WPA2.
* Salting – Appending random data to passwords before hashing.
* Salting & peppering passwords
* SAML – for SSO via XML, used in federated identity
* SAN (Storage Area Network) - specialized, high-speed network that provides network access to storage devices. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.
* SASE (Secure Access Service Edge) – cloud-edge security model
* SATCOM (Secure Satellite Communications) - refers to the use of satellite technology for communication purposes, including voice, data, and video transmission.
* SCADA (Supervisory Control and Data Acquisition) - a system used to control and monitor industrial processes.
* SCAP benchmarks & automated compliance scanning
* SCAP, Benchmarks, NetFlow, SNMP traps (monitoring data sources)
* SCP (Secure Copy Protocol) - a protocol used to securely transfer files between two devices.
* SD-WAN – secure, cloud-optimized WAN
* Secure Enclave – A protected area of hardware used for secure computations.
* Secure cookie / SameSite attributes
* Secure wipe / sanitization / destruction / certification
* Secure-communication technologies – Software-Defined WAN (SD-WAN), Secure Access Service Edge (SASE)
* Secure baseline – Establish / Deploy / Maintain
* Security awareness programme – initial & recurring, reporting pipeline
* Security Content Automation Protocol (SCAP)
* Security incident phases – prep, detect, analyse, contain, eradicate, recover, review
* Security-Awareness Extras
* Segmentation techniques – VLAN, VRF, ACL, air-gap
* Self-signed certificate – A certificate signed by the same entity that created it.
* Sensors (infra-red, microwave, ultrasonic, pressure) integration
* Serverless & micro-service outage considerations
* Serverless – Cloud model where functions run without managing infrastructure (think AWS Lambda)
* Service-level, master-service & business-partner agreements (SLA, MSA, BPA, MOA, MOU, NDA, SOW)
* Session hijack & credential-replay detection
* Session Key – A temporary encryption key used during a single session to encrypt data. Common in TLS and symmetric encryption for performance and confidentiality.
* SFTP (Secure File Transfer Protocol) - a protocol used to securely transfer files between two devices.
* SHA (Secure Hash Algorithm) - SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions.
* SID (Security Identifier) - a unique identifier used to identify a user or group in Windows operating systems.
* SID (Security Identifier) – Noted in logs to identify users or systems.
* SIEM (Security Information and Event Management) - type of security solution that provides real-time analysis of security alerts and events generated by network hardware and applications.
* SIEM – dashboards, correlation, tuning, SOAR playbooks
* Site surveys & wireless heat-maps
* Site-survey & heat-map (wireless planning)
* SMTP (Simple Mail Transfer Protocol) - a protocol used to send email messages between servers.
* SMTP, POP3, IMAP security (STARTTLS, S/MIME)
* Snapshot, image & gold-master creation
* SNMP (Simple Network Management Protocol) - a protocol used to manage and monitor network devices.
* SOAR (Security Orchestration, Automation and Response) - security technology that helps organizations automate and streamline their security operations and incident response processes.
* SoC (System on Chip) - integrated circuit (IC) that combines various components of a computer or electronic system into a single chip.
* Social-engineering principles – authority, urgency, intimidation, scarcity, familiarity, trust
* Software-defined perimeter (SDP) / Zero Trust Network Access
* Software-defined networking (SDN) – Network management model with centralized logic control
* Special-purpose appliances – Jump server, Sensors
* SPF & reverse-DNS validation
* Spraying vs. brute-force vs. dictionary attacks
* SQL (Structured Query Language) - a programming language used for managing and manipulating data in relational databases.
* SSH (Secure Shell) - a protocol used for secure remote access to a device. Uses Port 22.
* SSH, TLS versions & cipher-suite negotiation
* SSL (Secure Sockets Layer) - SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today. A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP".
* Static vs. dynamic code analysis, package monitoring & signing
* STIX (Structured Threat Information Exchange) - designed to support the sharing of cybersecurity threat intelligence between different organizations and cybersecurity technologies.
* STIX – standardized threat intel format
* STP (Spanning Tree Protocol) - a protocol used to prevent loops in a network topology.
* Structured Query Language injection (SQLi)
* Supply-chain threats (hardware, software, firmware, MSP)
* Suspicious-message reporting metrics
* Synchronised authentication of equals (SAE) & WPA3-Enterprise
* Tabletop vs. simulation vs. full-scope testing
* TACACS+ (Terminal Access Controller Access Control System Plus) - protocol used for providing centralized authentication, authorization, and accounting (AAA) services for network devices such as routers, switches, and firewalls.
* TAXII (Trusted Automated Exchange of Indicator Information) - application protocol for exchanging Cyber Threat Intelligence over HTTPS. It works with STIX.
* TAXII – threat intelligence exchange protocol
* TCP (Transmission Control Protocol) - a protocol used to establish a reliable connection between two devices. Uses three way handshake.
* TCP three-way handshake & SYN flood detection
* Testing methods – Fail-over test, Simulation, Parallel-processing test
* Threat hunting – hypothesis-driven, IOC/IOA driven
* Threat-scope reduction – Principle of limiting potential attack surface in Zero Trust
* Ticket creation & escalation via SOAR run-books
* Time-of-check / Time-of-use (TOC/TOU) race condition
* Tip: Use your browser’s search to jump straight to any keyword.
* Tokenisation service & vaultless tokenisation
* Tokenization – Replaces sensitive data with non-sensitive placeholders.
* Tokenization (data-obfuscation method)
* TOTP (Time Based One Time Password) - TOTP uses a timestamp and a time-based factor to generate the password. Specifically, TOTP calculates the message authentication code based on the current time and a time interval (usually 30 seconds).
* TPM (Trusted Platform Module) - chip on motherboard that can be used to store critical information such as encryption keys. TPM can be used for FDE (Full Disk Encryption).
* TPM / UEFI secure-boot
* Traffic tunnelling (DNS, ICMP, HTTP)
* Trusted Platform Module (TPM) & measured boot
* UBA (User Behaviour Analysis) - checks whether user activity sticks out from their usual activity.
* UDP (User Datagram Protocol) - a protocol used for sending datagrams over a network. Connectionless.
* UEFI (Unified Extensible Firmware Interface) - modern version of BIOS. UEFI can be used for securely starting a device.
* Understanding the user's request
* Uninterruptible Power Supply (UPS) and Generators as resilience controls
* Unsecure networks – open Wi-Fi, Bluetooth, public endpoints
* URL (Uniform Resource Locator) - a unique identifier used to locate a resource on the Internet. It is also referred to as a web address.
* User behaviour analytics (UBA) & impossible travel alerts
* Vendor-management docs – Master Service Agreement (MSA), Memorandum of Understanding (MOU), Work Order/Statement of Work (WO/SOW), Right-to-audit clause, Vendor questionnaires
* Virtual-machine escape and Resource reuse (virtualization vulns)
* VLAN (Virtual Local Area Network) - a logical grouping of devices on a network that are grouped together based on factors such as function, department, or location, rather than physical location.
* VM (Virtual Machine) - a software environment that emulates a physical computer.
* VPN (Virtual Private Network) - a virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.
* VTP (VLAN Trunking Protocol) - proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (such as VLAN ID or VLAN name) with switches inside the same VTP domain.
* Vulnerability classes – application, OS, web, cloud, mobile, firmware, zero-day, misconfiguration
* Vulnerability management cycle – scan, prioritise, remediate, verify, report
* WAF (Web Application Firewall) - firewall used to protect web applications.
* WAF tuning & false-positive handling
* WAP (Wireless Access Point) - network device that receives and transmits data over WLAN.
* Waterfall vs. Agile vs. DevSecOps lifecycle governance
* Web-filter modes – agent, proxy, reputation, content category
* WEP (Wired Equivalent Privacy) - wired equivalent privacy is meant to protect Wi-Fi transmissions by encrypting the data so outsiders who are not inside the encrypted network will not be able to read the messages or data contained within. WEP is better than no security at all, and it is still used on older devices that do not support WPA or WPA2.
* WIDS (Wireless Intrusion Detection System) - a system used to detect unauthorized access to a wireless network.
* WIDS/WIPS – Wireless intrusion detection/prevention
* Wildcard Certificate – A digital certificate that secures multiple subdomains.
* Wildcard certificate
* Wireless security – WPA3-SAE, PMF, evil-twin, de-auth flood, RF jamming
* WPA (Wi-Fi Protected Access) - a security protocol used for wireless networks. There is WPA, WPA2, WPA3.
* X.509 - a standard for public key certificates used for authentication in network communication.
* X.509 – Standard for public key certificates used in SSL/TLS, VPNs, etc. (mentioned briefly, but a full entry is valuable)
* XML (Extensible Markup Language) - a markup language used for encoding documents in a format that is both human-readable and machine-readable.
* XSS (Cross-Site Scripting) - a type of attack in which an attacker injects malicious code into a web page viewed by other users. Usually this code is javascript code. There are 3 main versions of XSS: DOM Based, Stored and Reflected XSS.
* Zero Trust Architecture – Includes Policy Engine, Policy Enforcement Point (PEP), Control vs. Data Plane.
* Zero-day definition & responsible disclosure
* Zero-Trust pillars – verify everything, assume breach, least privilege, continuous evaluation
* Zero-Trust (framework)

**Possible Missing Sections:**

* Cryptography & Encryption
* IKE – Internet Key Exchange (used in IPSec VPNs)
* ESP / AH – Components of IPsec
* GCM / CCMP – Common encryption modes (TLS, WPA2)
* ECDSA / ECDHE – Modern elliptic curve crypto
* PBKDF2 – Key stretching method
* GPG – Gnu Privacy Guard
* S/MIME – Secure email standard
* Key Management System (KMS)
* Key Wrapping
* X.509 – Certificate standard
* Zero Trust & Security Architecture
* Zero Trust Components:
  + Policy Administrator
  + Policy Engine
  + Adaptive Identity
  + Threat-Scope Reduction
  + Policy Enforcement Point (PEP)
  + Control vs. Data Plane
* SD-WAN, SASE – Modern architecture components
* Serverless, IaC, Microservices – Not listed
* Vulnerability, Risk & Attack Concepts
* TOC/TOU – Race condition type
* Downgrade Attack
* Replay Attack
* Deception Tech – Honeypot, Honeynet, Honeyfile, Honeytoken
* Indicators of Compromise (IOCs) – Impossible travel, concurrent sessions, etc.
* Exposure Factor – Used in risk math
* Bug Bounty / Responsible Disclosure
* Monitoring & Logging
* SIEM Alert Logic
* File Integrity Monitoring (FIM)
* Log Artifacts – Account lockout, out-of-cycle logging, blocked content
* Governance, Risk, Compliance
* Gap Analysis
* Attestation and Acknowledgment
* Exception vs. Exemption
* Right to be Forgotten
* Email & DNS Security
* MTA / MDA / MUA – Mail components
* DNSSEC – DNS integrity validation
* MUA/MTA/MDA roles (you mention them briefly but a definition line may help)
* SASE (Secure Access Service Edge) – mentioned in objectives, not clearly defined
* SD-WAN, TLS VPN, and IKEv2 – are key VPN protocol options you should define individually
* SameSite cookies, HSTS, PFS (Perfect Forward Secrecy) – scattered but could benefit from their own concise line entries
* Quantitative vs. Qualitative Risk Analysis – mentioned under risk, but not defined separately