Security+ SY0-701 Cram Sheet

Control Types:

	Description	Example
Preventive Controls	Proactive measures implemented to thwart potential security threats or breaches	Complex passwords and frequent changes act as gatekeepers.
Deterrent Controls	Discourage potential attackers by making the effort seem less appealing or more challenging	Security cameras watch every move, making mischief less tempting.
Detective Controls	Monitor and alert organizations to malicious activities as they occur or shortly thereafter	Logs show events, revealing suspicious activities.
Corrective Controls	Mitigate any potential damage and restore our systems to their normal state	Incident response plans spring into action, minimizing the fallout.
Compensating Controls	Alternative measures that are implemented when primary security controls are not feasible or effective	Air-gapping an EOL system that can't be replaced, to minimize its attack surface.
Directive Controls	Guide, inform, or mandate actions	Company policies set the guardrails, shaping secure behavior.

Zero Trust:

Feature	Control Plane	Data Plane
Function	Decides who can access what and under what conditions	Performs actual access checks based on decisions
Roles	• Adaptive Identity: Manages user access based on risk and context • Threat Scope Reduction: Limits access to minimize attack surfaces • Policy-Driven Access Control: Sets centralized rules for authorization • Secured Zones: Isolates sensitive data and resources	• Subject/System: Represents the entity requesting access (user, device) • Policy Engine: Evaluates access requests against defined policies • Policy Administrator: Creates and manages access policies • Policy Enforcement Point: Implements access control at designated points

Data Encryption Levels:

Full-Disk Encryption (FDE)	Encrypts the entire hard drive to protect all the data being stored on it
Partition Encryption	Similar to full-disk encryption but it is only applied to a specific partition on the storage device
Volume Encryption	Used to encrypt a set space on the storage medium
Record	Encrypts individual records or rows within a database

Public key infrastructure (PKI):

- *Involves generating, validating, and managing public and private key pairs that are used in the encryption and decryption process*
- **Asymmetric Encryption**
  - Uses two separate keys for encryption and decryption
    - Public key and private key
  - No need for shared secret keys
  - Slower compared to symmetric encryption but solves key distribution challenges

Root of Trust	Highest level of trust in certificate validation
Certificate Authority (CA)	Trusted third party that issues digital certificates
Registration Authority (RA)	Requests identifying information from the user and forwards certificate request up to the CA to create a digital certificate
Certificate Signing Request (CSR)	A block of encoded text with information about the entity requesting the certificate
Certificate Revocation List (CRL)	List of all digital certificates that the certificate authority has already revoked
Online Certificate Status Protocol (OCSP)	Determines certificate revocation status or any digital certificate using the certificate's serial number
Key Escrow	Storage of cryptographic keys in a secure, third-party location (escrow). Enables key retrieval in cases of key loss or for legal investigations

Sorted by security then speed

Symmetric Encryption Algorithms	Asymmetric Encryption Algorithms
AES	ECC (Elliptic Curve Cryptography)
Blowfish	RSA
Triple DES	Diffie-Hellman
DES	DSA

Digital Certificates:

Wildcard Certificate	Allows multiple subdomains to use the same certificate
Self-Signed Certificates	Digital certificate that is signed by the same entity whose identity it certifies
Third-Party Certificates	Digital certificate issued and signed by trusted certificate authorities (CAs)
Single-Sided and Dual-Sided Certificates	**Single-sided**: Only requires the server to be validated **Dual-sided**: Both server and user validate each other

Cryptographic Attacks:

- **Downgrade Attack:** Forces a system or communication channel to abandon a more secure protocol or algorithm in favor of an older, less secure one.
- **Collision Attack**: Aims to find two different inputs to a cryptographic hash function that produce the same output (hash value).
- **Birthday Attack:** Exploits the mathematics of probability to increase the chances of finding a collision within a cryptographic hash function, thus undermining its security.

Threat Actors:

Type	Description	Sophistication and Capability
Nation-state actor and Advanced Persistent Threats	Highly skilled attackers sponsored by governments for cyber espionage or warfare	High sophistication and high capability
Unskilled attacker	Limited technical expertise, use readily available tools. Also known as a "script kiddie"	Low sophistication and low capability
Hacktivist	Driven by political, social, or environmental ideologies	Medium sophistication and medium capability
Insider threat	Security threats originating from within the organization	High to low sophistication but high capability
Organized crime	Execute cyberattacks for financial gain (e.g., ransomware, identity theft)	High sophistication and high capability
Shadow IT	IT systems, devices, software, or services managed without explicit organizational approval	Varies

Bluetooth Attacks:

Bluejacking	This is a relatively harmless attack that involves sending unsolicited messages to nearby Bluetooth devices
Bluesnarfing	This is a more serious attack that involves stealing data from another Bluetooth device, such as contact lists, emails, or photos
Bluebugging	This is an even more advanced attack that allows the attacker to take complete control of another Bluetooth device

Threat Vectors:

Message-Based	Email Short Message Service (SMS) Instant Messaging (IM)
Image-Based	Hidden malware in images, steganography hiding secrets, manipulated photos for misinformation campaigns.
File-Based	Infected downloads, trojan horse attachments, malicious macros in documents can install malware or steal data.
Voice Call	Vishing scams impersonating trusted entities, voice phishing to capture sensitive information during calls.
Removable Device	Lost or stolen USB drives, compromised external hard drives can leak data or introduce malware
Vulnerable Software	Unpatched applications with known security holes leave systems open to exploits and attacks.
Unsupported Systems and Applications	Outdated software lacking security updates creates critical vulnerabilities for attackers.
Unsecure Networks	Public Wi-Fi, weak encryption, and lack of authentication exposes sensitive data to eavesdropping and manipulation.

Malware Types:

Ransomware	Encrypts files and demands ransom for decryption
Trojan	Disguises itself as legitimate software to gain access
Worm	Replicates itself and spreads within a network
Virus	Self-replicating malicious code that damages systems but does not necessarily spread itself across a network like a worm. (Usually limited to a single system)
Spyware	Steals sensitive information without your knowledge
Bloatware	Unnecessary software that consumes resources
Keylogger	Records keystrokes for password theft
Logic Bomb	Triggers malicious actions when specific conditions are met
Rootkit	Grants attackers hidden access and control

Race Conditions:

- **Time-of-check and Time-of-use (TOC & TOU)**
  - Attackers manipulate a resource's state after it is checked but before it is used
  - For example, overdrawing a bank account due to a time delay between checking and transferring funds

Supply Chain Attacks:

- An attack that targets a weaker link in the supply chain to gain access to a primary target
- Exploit vulnerabilities in suppliers or service providers to access more secure systems

Types of Phishing Attacks

Spear Phishing	A more targeted form of phishing
Whaling	Form of spear phishing that targets high-profile individuals, like CEOs or CFOs
Business Email Compromise	Taking over a legitimate business email. accounts through social engineering or cyber intrusion techniques to conduct unauthorized actions

Mobile Device:

- **Side Loading:** Installing apps from untrusted sources outside official app stores
- **Jailbreaking:** Bypassing security restrictions on mobile devices, increasing vulnerability

Network Attacks:

Distributed denial-of-service (DDoS)

- Overwhelms a system with traffic, making it unavailable
- **Amplified**
  - Attackers send small DNS requests with the victim's IP address as the source. The DNS server responds with large records to the victim's IP, amplifying the traffic
- **Reflected**
  - The attacker sends many requests to the reflector with the victim's IP address spoofed as the source. The reflector, unaware of the spoofing, sends responses directly to the victim, reflecting the attack traffic

Application Attacks:

Injection	Introduces malicious code into an application (e.g., SQL injection)
Buffer Overflow	Overwrites memory with malicious code to gain control (e.g., entering a value of 128 when a certain text field can only hold values up to 127, causing the resulting value to be incorrect)
Replay	Intercepts and reuses legitimate actions for unauthorized access
Privilege Escalation	Expands an attacker's access rights within a system
Forgery	Creates fake data to deceive users or systems
Directory Traversal	Exploits directory structures to access unauthorized files Example: https://google.com/../../../etc/ssh/sshd_config If google.com was insecure, this link would display sensitive operating system files
XSRF/CSRF	An exploit that targets a victim's browser session, causing it to perform unauthorized actions on a trusted website, often exploiting the victim's existing logged-in session
XSS	Malicious scripts are injected into a website, allowing the attacker to steal sensitive information from visitors who interact with the website

Virtualization and Containerization:

- **Virtualization:** Creates virtual machines (VMs) running multiple operating systems on a single physical server
  - **VM Escape:** When a program on a virtual machine breaks free and accesses the underlying computer system.
- **Containerization:** Packages applications with dependencies, enabling isolated and portable deployments

Serverless Application Development: Enables application development and deployment without managing servers, utilizing cloud resources on-demand

Microservices: Breaks down applications into smaller, independent services for easier development, scaling, and deployment

Software-defined networking (SDN):

- Programmatically manages and controls networks, offering flexibility and agility
- **Software Defined Wide Area Networking (SD-WAN)**
  - Software-defined approach to managing wide area networks primarily through the cloud
- **Secure Access Service Edge (SASE)**
  - Converges network and security functions for simpler, cloud-based access control

SD-WAN	SASE
Simply a WAN built for the cloud	Considered a "next generation" VPN
No central point of communication	Security technologies are in the cloud
Manage the network connectivity to the cloud	Securely connect from different locations
Does not adequately address security concerns	A complete network and security solution
Managed in the cloud	Requires planning and implementation

SD-WAN can be considered a component of SASE, but SASE goes beyond traditional SD-WAN capabilities by incorporating comprehensive security features.

Network Appliances:

- **Jump server:** Secure access point for managing internal systems
- **Proxy server:** Intermediary for network requests, improving security and performance: protects internal IP addresses
- **IPS/IDS:** Systems that detect and prevent/alert malicious network activity
- **Load balancer:** Distributes traffic across multiple servers for scalability and redundancy
- **Sensors:** Devices that collect and analyze security-related data from various sources (e.g. IDS, IPS, XDR)

Port Security:

- **802.1X:** Framework for port authentication
  - Network access control based on device authentication
- **EAP:** Authentication protocol used by 802.1X for various methods for port authentication (e.g. w/ MFA)

Firewall Types:

- **Web application firewall (WAF):** Protects web applications from specific attacks
- **Unified threat management (UTM):** Combines multiple security functions in one device
- **Next-generation firewall (NGFW)**
  - Advanced firewalls with deeper inspection at application level and threat analysis capabilities
- **Layer 4/Layer 7**
  - Refers to the network layer (transport/application) the firewall operates on
  - NGFW and WAF operates on Layer 7, while a traditional firewall would operate on Layer 4

Data Security:

Data Ownership Roles:

Role	Key Responsibility	Focus
Data Owner	Decides on data strategy, determines access & controls, ensures value & governance	Business-level data decisions: strategy and governance
Data Controller	Makes decisions on data collection, storage, usage, and legality	Legality & compliance of data management
Data Processor	Acts on behalf of the controller to process data according to instructions	Technical implementation of data processing
Data Custodian	Manages data storage systems, enforcing access controls & security	Secure and reliable data storage & access
Data Steward	Ensures data quality & accuracy, manages metadata, promotes data understanding	Data quality, consistency, and usability

FIM (File Integrity Monitoring):

- Monitors files and directories for unauthorized changes, detecting potential tampering or intrusion attempts

Data Protection Techniques:

Technique	Description	Encryption?	Use Cases
Encryption	Converts data into unreadable format using a key.	Yes	Securing data at rest and in transit, protecting sensitive information like passwords and financial data.
Hashing	Creates a unique fingerprint of data using a one-way algorithm.	No	Verifying data integrity, detecting unauthorized modifications, password storage (hashed, not stored as plain text).
Masking	Obscures sensitive data while maintaining functionality.	No	Protecting displayed data like partial credit card numbers, social security numbers (e.g., showing only last digits).
Tokenization	Replaces sensitive data with a unique, non-sensitive token.	No	Facilitating secure transactions without storing full data (e.g., credit card tokens for online payments).
Obfuscation	Makes data harder to understand by scrambling or encoding.	No	Adding obscurity to data to deter casual inspection, but not fully secure against determined attackers.

Disposal/Decommissioning of Data:

- **Sanitization**
  - Removing sensitive data from the item before disposal
- **Destruction**
  - Physically destroying the item if necessary (e.g., for security reasons)
- **Certification**
  - Obtaining documentation that the item has been disposed of properly
- **Data retention**
  - Following legal and organizational guidelines for retaining or destroying data associated with the item

Mobile Asset Deployments (Main Mobile Device Deployment Models):

- **BYOD (Bring Your Own Device)**
  - Employees use personal devices for work
  - Cost-effective for employers
  - Drawbacks include reduced control over security and device management
- **COPE (Corporate-Owned, Personally Enabled)**
  - The company provides devices for employees
  - Greater control over security and standards
  - Higher initial investment
  - Employees may have privacy concerns or need to carry two devices
- **CYOD (Choose Your Own Device)**
  - Employees select devices from a company-approved list
  - Balance between employee choice and organizational control
  - Similar drawbacks to COPE in terms of initial cost and potential privacy concerns Application security

App Security:

Static Code Analysis (SAST):

- A method of debugging an application by reviewing and examining its source code before running the program
- Identifies issues like buffer overflows, SQL injection, and XSS
- Important for proper input validation in both front-end and back-end code

Dynamic Code Analysis (DAST):

- Analyzes applications while they run
  - **Fuzzing (Fuzz Testing)**
    - Inputs random data to provoke crashes or exceptions
    - Helps uncover security flaws and weaknesses
  - **Stress Testing**
    - Evaluates system stability and reliability under extreme conditions
    - Reveals bottlenecks and assesses system recovery

Code Signing:

- Confirms the software author's identity and integrity
- Utilizes digital signatures to verify code authenticity
- Protects against code tampering but does not guarantee absence of vulnerabilities

Sandboxing:

- Isolates running programs, limiting their access to resources
- Prevents harmful actions on the host device or network
- Used to execute untrusted or untested programs securely

Security Tools:

- **Security Content Automation Protocol (SCAP)**
  - A standardized framework for vulnerability management, including defining security benchmarks and tools for scanning and compliance
- **Benchmarks**
  - Standardized configurations for systems and applications, setting baselines for secure and compliant configurations (e.g. DoD, CIS)
- **Agents/agentless**
  - **Agents**
    - Software installed on devices to collect data and transmit it to a central server
  - **Agentless**
    - Tools that monitor devices without requiring installed software, often relying on network protocols or APIs
- **Security information and event management (SIEM)**
  - Tool that aggregates logs from various sources, analyzes them for security incidents, and generates alerts
- **Security, Orchestration, Automation, and Response (SOAR)**
  - SOAR seeks to alleviate the strain on IT teams by incorporating automated responses to a variety of events.
- **Data Loss Prevention (DLP)**
  - Prevents unauthorized data exfiltration through various channels (email, USB, cloud)
- **Simple Network Management Protocol (SNMP) traps**
  - Messages sent by network devices indicating specific events for monitoring
- **Vulnerability scanners**
  - Tools that identify known vulnerabilities in systems and applications
  - Examples: Nessus, Nmap, Wireshark
    - Specific internal networks protected by the firewall
- **Endpoint Detection and Response/Extended Detection and Response (EDR/XDR)**
  - EDR monitors endpoints for malicious activity, while XDR extends monitoring to broader security events across the network
- **NAC (Network Access Control)**
  - Enforces security policies on devices trying to connect to the network

IDS/IPS:

- **Trends**
  - Analyze patterns in network traffic to identify suspicious activity
- **Signatures**
  - Predefined patterns of known malicious activity used to detect attacks
- **IDS (Intrusion Detection System)**
  - Watchman monitoring network activity, alerting you to suspicious behavior
  - Only monitors and reports threats
- **IPS (Intrusion Prevention System)**
  - Enforcer guarding your network, actively blocking potential threats
  - Actively fights threats

Email Security:

Technique	Description	Purpose
SPF (Sender Policy Framework)	Specify which email servers are authorized to send emails from your domain	Blocks unauthorized senders from impersonating your domain
DKIM (DomainKeys Identified Mail)	Digitally signs each email sent from your domain, allowing receivers to verify its authenticity	Helps prevent phishing attacks and builds trust with recipients
Gateway (Email Filtering System)	Acts as a frontline defense, scanning incoming emails for spam, phishing attempts, malware, and other threats	Protects users from malicious emails and keeps your inboxes clean
DMARC (Domain-based Message Authentication, Reporting & Conformance)	Acts as a policy framework, telling receivers what to do with emails claiming to be from your domain	Prevents email spoofing and protects your sender reputation

Identity Proofing, Federation, and Access Controls:

- **Identity proof**
  - Establishing and verifying someone's identity
- **Federation**
  - Collaborative approach where users can access authorized resources across different organizations using their primary login credentials
- **Single Sign-On (SSO)**
  - Accessing multiple resources with a single login
- **Lightweight Directory Access Protocol (LDAP)**
  - An open-standard protocol for accessing and managing directory information (e.g., user accounts)
- **Open authorization (OAuth)**
  - Authorization framework enabling secure access to protected resources without revealing user credentials
  - Does not provide authentication, relies on OpenID for that
- **Security Assertion Markup Language (SAML)**
  - standardized way to tell external applications and services that a user is who they say they are (e.g. Single sign on)

Digital Forensics:

- **Investigative science of collecting, analyzing, and presenting digital evidence**
- Used in incident response to gather evidence of the attack, identify attackers, and support legal action

Key Terms

- **Legal hold:** Preserving relevant data for potential legal proceedings
- **Chain of custody:** Maintaining a documented record of evidence handling to ensure its authenticity
- **Acquisition:** Collecting digital evidence in a forensically sound manner
- **Reporting:** Documenting the findings of the investigation in a clear and concise format
- **Preservation:** Ensuring the integrity and availability of digital evidence over time
- **E-discovery:** Identification, collection, and production of electronically stored information relevant to legal matters

Log Data Types:

Log Data Type	Description	Use Cases
Firewall logs	Track network traffic flow, including successful/blocked access attempts, policy violations	Monitoring network security, identifying unauthorized access, analyzing attack patterns
Application logs	Record application activity, including errors, warnings, successful actions, user interactions	Troubleshooting application issues, debugging errors, understanding user behavior
Endpoint logs	Capture activity on individual devices, including user logins, file access, software installations	Monitoring device security, detecting suspicious activity, investigating potential incidents
OS-specific security logs	System event logs related to security, like failed logins, file changes, privilege escalations	Identifying security vulnerabilities, investigating security incidents, analyzing system integrity
IPS/IDS logs	Record detections and events related to intrusion prevention/detection systems	Identifying and analyzing potential attacks, assessing system vulnerabilities, evaluating security effectiveness
Network logs	Capture overall network traffic information, including device communication, bandwidth usage, anomalies	Monitoring network performance, identifying traffic bottlenecks, detecting suspicious network activity
Metadata	Additional information associated with log data (timestamps, user IDs, source IPs)	Adds context and value to log data, facilitating analysis and investigation

Risk Assessment and Analysis:

- **Ad hoc:** Business reports or data analysis curated and created by users when needed
- **Qualitative:** Technique used to qualify risk associated with a particular hazard (e.g., High, Medium, Low severity)
- **Quantitative:** Focuses on providing a clear, numeric picture of the risk landscape
  - **Single loss expectancy (SLE):** The monetary value expected from the occurrence of a risk on an asset
  - **Annualized loss expectancy (ALE):** The product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE)
  - **Annualized rate of occurrence (ARO):** The probability that a risk will occur in a particular year

Business Impact Analysis:

- **Recovery time objective (RTO):** Maximum acceptable time for restoring a network or regaining access to data after an unexpected disruption
- **Recovery point objective (RPO):** Maximum acceptable amount of lost data after an unexpected data-loss incident
- **MTTR (Mean time to repair):** The average time it takes to repair a system
- **MTBF (Mean Time Between Failures):** The average time between two successive failures of a component or system

Agreement Types:

- **Service-level agreement (SLA):** Agreement between two or more parties where one is the customer, and the others are service providers
- **Memorandum of agreement (MOA):** A document written between parties to cooperatively work together on an agreed upon project or meet an agreed upon objective (formal, can be binding)
- **Memorandum of understanding (MOU):** Starting point of negotiations between multiple parties to signal the intent of doing business or coming to an agreement (non-formal, non-binding)
- **Master service agreement (MSA):** Contract outlining the relationship between two parties including the terms and conditions for their future activities and responsibilities
- **Work order (WO):** Document that provides information on a maintenance task and outlines a process for completing it
- **Statement of work (SOW):** Document that gives a description of a given project's requirements

Segmentation:

- Divide your network into smaller, isolated segments to limit the impact of a breach.

Access control:

- Control who can access what. This includes:
  - **Access Control List (ACL):** Rules defining who can access specific resources
  - **Permissions:** Granular control over user and application access rights
- **Mandatory Access Control (MAC):** The operating system limits the operation on an object based on security clearance levels: pyramid style level of access (level 1, 2, 3…)
- **Discretionary Access Control (DAC):** Used in most operating systems, the owner of an object controls who can access it
- **Role-based Access Control (RBAC):** Administrators provide access based on the role of the user: much more granular than MAC
- **Rule-based Access Control:** based on a set of predefined rules to control the system
- **Attribute-based Access Control (ABAC):** an authorization methodology that sets and enforces policies based on characteristics, such as department, location, manager, and time of day (e.g. a user cannot access a system at night)
- **Application allow list:** Only allow approved applications to run, blocking suspicious ones

Endpoint protection:

- Install software that protects devices from malware and other threats

Host-based firewall:

- Filter incoming and outgoing traffic on individual devices

Host-based intrusion prevention system (HIPS):

- Monitors system activity for suspicious behavior

Password Attacks:

- **Spraying:** Tries common passwords against many accounts
- **Brute force:** Tries all possible password combinations systematically
- **Rainbow Table:** Method of cracking encrypted passwords by using a large pre-computed table of possible passwords and their corresponding hash values.

Device Attributes:

- **Active vs. Passive**
  - Active devices process and forward data, while passive ones monitor or analyze it
- **Inline vs. Tap/monitor**
  - Inline devices handle all traffic, while tap/monitor devices capture a copy of it

Input Validation:

- Ensures that applications process well-defined, secure data
- Guards against attacks exploiting data input vulnerabilities (e.g., SQL injection, XSS, buffer overflows)
- Serves as a kind of quality control for data to ensure that every piece of information is valid, secure, and correctly formatted

Guidelines and Policies:

- **Acceptable Use Policy (AUP)**
  - List of guidelines delegating how a system may be used by the owner
- **Software Development Lifecycle (SDL)**
  - A process for creating, planning, testing, and deploying an information system
- **Change management**
  - Specifies the rules and levels of authorization needed to approve different types of changes to a system

Procedures:

- **Onboarding**
  - Integrating new hires (employees) into the organization
- **Offboarding**
  - Removing an employee from the organization through resignation, retirement, or termination
- **Playbooks**
  - Predefined steps to perform to identify an issue

Governance Structures:

- **Boards**
  - A set of principles and processes that are in the best interest of a governing board while also providing oversight and accountability
- **Committees**
  - A group of people who oversee the function and duties of the board of directors
  - **Centralized**
    - Data management and decision-making is concentrated within a single, central entity
  - **Decentralized**
    - Data management and decision-making is separated between several different subsections

Types of sites:

- **Hot Site:** A fully equipped, mirrored replica of your primary data center that's always running, allowing for near-instant failover and minimal downtime in a disaster.
- **Warm Site:** A partially equipped site with basic infrastructure and pre-installed hardware, requiring data restoration and some setup before full failover.
- **Cold Site:** A basic facility with power and space, but no pre-installed hardware or data, requiring significant setup time before becoming operational.