CompTIA Security+ (SY0-701) Day 7

Multifactor Authentication

Using two or more factors in combination to authenticate.

- **Knowledge** – Something you know
  - Password, Passphrase, PIN, Graphical Password
- **Possession** – Something you have
  - Smart Cards, Security Key, SMS Text, Cell Phone App
- **Biometric** – Something you are
  - Fingerprint Scanner, Gait Analysis, Retinal Scanner, Iris Scanner, Facial Recognition, Voice Recognition
- **Location** – Somewhere you are
  - Involves tracking your location by IP or GPS

Password Concepts and Privileged Access Management Tools

- **Password Best Practices**
  - Length
  - Complexity
  - Reuse
  - Expiration / Age
- **Password Managers**
  - Software tools that help users create, store, and manage their passwords for various online accounts.
  - Allow very complex passwords for every site without memorization.
    - **Cloud**
      - Pros: Synced to all devices
      - Cons: Less secure
      - Example: Apple's iCloud Keychain

        - **On-Device**
            - Pros: More secure, more control
            - Cons: Risk of losing everything if something happens to the device
            - Example: KeePass
- **Passwordless Authentication** – Utilizes user identity verification methods other than passwords.
    - **Biometric** – Fingerprints, facial recognition, iris scans (e.g., Apple Face ID, Windows Hello)
    - **Push Notifications** – Login approval requests sent to a trusted device (e.g., Duo Security, Microsoft Authenticator)
- **Privileged Access Management Tools (PAM)** – Security solutions that help organizations manage and monitor privileged accounts and access.
    - Key functions of PAM tools:
        - Centralized Management
        - Monitoring and Auditing
        - Access Control
    - **Just-in-Time Permissions** – Grants access when needed, revoked after use.
        - Temporary admin tasks reduce standing privileges.
        - Minimizes risk of access abuse.
    - **Password Vaulting** – Secure storage for credentials.
        - Component of a password manager
        - Prevents password reuse
        - Encourages adoption of longer, more complex passwords
    - **Ephemeral Credentials** – Temporary authentication tokens or keys generated dynamically and valid only for a short time.
        - Automatically expire after use or after a preset duration

Section 4.7: Explain the Importance of Automation and Orchestration Related to Secure Operations

Automation and Orchestration Benefits

- **Efficiency / Time Saving** – Automation significantly reduces the time required to perform routine tasks and respond to security incidents.
- **Enforcing Baselines** – Ensures consistent application of security policies and configurations across the infrastructure.
- **Standard Infrastructure Configurations** – Helps maintain secure configurations across systems and applications, reducing the risk of errors.
- **Scaling Securely** – Enables organizations to scale operations securely without proportionally increasing risk or workload.
- **Employee Retention** – Reduces repetitive tasks for staff, allowing focus on strategic initiatives, improving job satisfaction and retention.
- **Reaction Time** – Improves response speed to security incidents and operational issues.
- **Workforce Multiplier** – Allows a smaller team to manage large infrastructures effectively.

Use Cases of Automation and Scripting

- **User Provisioning** – Automatically creating user accounts and assigning roles/permissions based on predefined rules.
- **Resource Provisioning** – Automating setup of servers, applications, and network resources with secure, consistent configurations.
- **Guardrails** – Implementing automated checks and controls to prevent violations of security policies.
- **Security Groups** – Automating management of group memberships to ensure only authorized access.
- **Ticket Creation** – Automatically generating tickets for security events or operational issues.
- **Escalation** – Automatically escalating issues based on severity or criteria for prompt attention.
- **Enabling/Disabling Services and Access** – Automatically managing access based on policies or incident response.
- **Continuous Integration and Testing** – Automated testing and integration to prevent introduction of vulnerabilities.

- **Integration and APIs** – Managing integrations and API connections through automation to ensure security and functionality.

Additional Considerations

- **Complexity** – Implementing automation and orchestration can be complex, requiring significant expertise and planning.
- **Cost** – Setup and ongoing maintenance can be costly, though often offset by efficiency and security gains.
- **Single Point of Failure** – Over-reliance on automated systems can create risks if those systems fail or are compromised.
- **Technical Debt** – Poorly implemented automation can create future challenges and risks.
- **Ongoing Supportability** – Automated systems require continuous support to remain effective and secure.

Section 4.8: Explain Appropriate Incident Response Activities

Incident Response Process - Steps: Preparation, Detection, Analysis, Containment, Eradication, Recovery, Lessons Learned - **"Please Don't Assume Cats Eat Really Loudly"**

1. **Preparation**
    a. Purpose - Ensure the organization is ready to respond to security incidents, including tools, processes, policies, and training.
    b. Example - Develop an incident response plan, conduct security training for employees, and set up communication channels and defined roles.
    c. Training - Enhance awareness and skills, familiarize with response procedures, test and refine plans, ensure compliance, build a security culture, and adapt to evolving threats.

2. **Detection**
    a. Purpose - Identify potential security incidents promptly via monitoring systems and networks.
    b. Example - Use intrusion detection systems (IDS) and SIEM tools to detect malicious activity.
    c. Training - Train employees to recognize signs of security incidents.
3. **Analysis**
    a. Purpose - Confirm if an incident is genuine and understand its scope and impact.
    b. Example - Examine logs, system changes, and unusual activity to determine source and method.
    c. Training - Train the incident response team in forensic analysis and threat assessment.
4. **Containment**
    a. Purpose - Limit the impact of the incident and prevent further damage.
    b. Example - Isolate affected systems, block malicious IPs, or disable compromised accounts.
    c. Training - Train staff in rapid response techniques and containment strategies.
5. **Eradication**
    a. Purpose - Remove the threat and address root causes.
    b. Example - Remove malware, apply patches, and reset compromised credentials.
    c. Training - Procedures for threat removal and system security hardening.
6. **Recovery**
    a. Purpose - Restore systems to normal operation safely.
    b. Example - Rebuild systems, restore backups, and gradually reintegrate into production.
    c. Training - Follow proper restoration procedures to ensure clean reintegration.
7. **Lessons Learned**
    a. Purpose - Review response effectiveness and identify improvements.
    b. Example - Conduct post-incident review, document findings, and update plans.
    c. Training - Apply lessons learned and feedback for continuous improvement.

Incident Response Testing, Analysis, and Digital Forensics

Incident Response Testing

- Validates plans and procedures.
- Identifies weaknesses and gaps.
- Enhances training, coordination, and compliance.

- Builds confidence in response processes.

Tabletop Exercises

- Role-play potential disaster or emergency scenarios.
- Test incident response plans and involve key personnel.
- Identify procedural gaps.

Simulation

- Mimics real-world scenarios for testing responses to network breaches, business continuity events, or system failures.

Root Cause Analysis

- Identify the fundamental cause of issues to prevent recurrence.
- Steps:
    - Identify the Problem
    - Collect Data
    - Analyze the Problem (using methods like 5 Whys, Fishbone Diagram)
    - Uncover Root Cause
    - Develop Corrective Actions
    - Implement Solutions
    - Monitor Effectiveness

Threat Hunting

- Actively search for hidden threats within the network.
- Detect anomalies before they cause harm.
- **Exam Note:** Threat hunting is proactive and focuses on identifying unknown threats inside an environment, whereas penetration testing (pen testing) is typically scheduled and simulates an attack to find vulnerabilities that could be exploited. Threat hunting continuously monitors real activity; pen testing is point-in-time and controlled.

Digital Forensics

- Investigate digital devices for legal evidence and security incidents.
- **Legal Hold** - Preserve relevant evidence.
- **Chain of Custody** - Document and track evidence handling (Collection -> Transport -> Storage -> Analysis -> Transfer).
- Acquisition - Securely collect evidence, using physical write blockers where possible for reliability.
- **Reporting** - Document and present forensic findings.
- **Preservation** - Protect evidence from tampering.
    - **Faraday cage** - Blocks external electric fields to prevent remote access or tampering.
    - Maintain detailed evidence records.
- **eDiscovery** - Identify, preserve, collect, and process electronic data for legal matters.

Data Sources to Support an Investigation

Log Data

- **Firewall logs** - Record network traffic data filtered by a firewall.
    - Details of allowed and blocked access attempts.
    - Used to identify:
        - Unauthorized access attempts.
        - Unusual traffic patterns.

- **Application logs** - Records of events specific to a software application.
    - Document the application's operations and errors.
    - Helps pinpoint issues within a specific application:
        - Identifying errors, unauthorized access, and unusual activities.
- **Endpoint logs** - Capture events and activities occurring on the endpoint.
    - Include security events, system changes, and user activities.
    - Crucial for tracking user activity, detecting malicious actions, and monitoring policy violations.
- **OS-specific security logs** - Records of activities and events specific to an operating system.
    - Examples: login attempts, policy changes, and system alerts.
    - Used to monitor and review events related to the operating system's security.

IPS/IDS Log - Document network activities.

- Provide insights into network security threats, attempted attacks, and successful breaches.

Network log - Track activities and events on a network.

- Provides information about traffic flow, device status, and network errors.
    - Used to: Analyze overall network health and activity. Identify anomalies or patterns indicative of malicious activities.

Metadata - Captures data about other data rather than the content of the data itself

- Like file access times and user information
- Provides contextual information about data or activities.

Data Sources

- **Automated reports** - Consolidate **snapshot** view; highlight key metrics and anomalies.
- **Dashboard** - Visual representation of **real-time** data; easy to export.
- **Vulnerability Scans** - Process used to identify and evaluate security weaknesses in a network system or software.
- **Packet Captures** - Method of intercepting and logging traffic that passes over a network. Create and analyze PCAP files.

- **Wireshark** - GUI and **TCPDUMP** - CMD

Domain 5.0: Security Program Management and Oversight

Section 5.1 Summarize Elements of Effective Security Governance

Security Governance - An essential aspect of an organization's overall governance framework.

- Establishes the strategies, objectives, and policies to manage and protect information assets.
- Ensures that security efforts are aligned with business objectives and are consistent with laws, regulations, and internal policies.
    - **Security Policies** - High-level documents. Typically, very vague. Just states this must be done.
        - Outlines an organization's rules for maintaining **CIA (Confidentiality, Integrity, Availability)**
        - Sets the foundation for an organization's information security program.
        - Establishes: Principles, frameworks, and responsibilities.

    - **Security Standard** - More detailed and specific than policies.
        - Defines the specific requirements that must be achieved to meet the policies
        - Specific requirements or rules designed to implement and operationalize the principles and policies
        - Specifies the technical and procedural details.
    - **Security Procedures** - Detailed, step-by-step instructions. Very specific.
        - Designed to implement the security policies and standards of an organization
        - Practical and specific, ensuring consistent execution of tasks.
    - **Security Guidelines** - Recommended practices and advice; not mandatory.
        - Best practices that can be adapted to a specific situation
        - Fill in gaps
        - Discretion based on circumstances.

Policies

- **Acceptable use policy (AUP)** - A set of rules applied by the owner/manager of a system that restricts how that system may be used.
    - Helps protect both the organization and its users by outlining acceptable behavior and use of IT resources.
    - It must be well-communicated, understood, and enforced across the organization.
    - Regular training and acknowledgment by employees are critical for ensuring that the policy is integrated into the organization's culture.
- **Information Security Policy** - Outlines the rules, procedures, and guidelines that govern the protection of the organization's information assets.
    - Assets include data in various forms, such as electronic, paper-based, intellectual property, company secrets, data on devices, and in the Cloud.
    - Establishes the standards and procedures for employees and systems to prevent, detect, and respond to potential security threats and vulnerabilities.
- **Business Continuity Plan (BCP)** - Outlines how the organization will continue to operate in the face of disruptive events such as natural disasters, cyberattacks, technological failures, or any other incidents that could interrupt normal business processes.
- **Disaster Recovery Plan (DRP)** - A documented set of procedures and protocols designed to protect and recover an organization's IT infrastructure and systems in the event of a disaster.

- **Incident Response Plan (IRP)** - A predetermined set of guidelines and procedures for detecting, responding to, and managing the aftermath of a security breach or cyberattack.
    - The goal of this policy is to mitigate damage, reduce recovery time and costs, and manage the incident in a way that upholds the organization's legal and ethical responsibilities.
- **Software Development Lifecycle (SDLC) Policy** - Outlines the processes and methodologies to be followed during the development and maintenance of software to ensure quality and security at every phase.
    - Typically covers: Requirements analysis, Testing, Design, Deployment, Development/Coding, and Maintenance.
- **Change Management Policy** - A set of procedures and guidelines that govern how modifications to the IT systems, applications, and other critical technological infrastructure are proposed, revised, implemented, and documented.
    - Aims to ensure that changes do not compromise system integrity or security, and are made in a controlled, predictable, and reversible manner.

Standards

- **Password Standards** - A set of criteria and best practices for creating and managing passwords that are designed to protect against unauthorized access to systems and data.
    - Goal - Making passwords difficult to guess.
    - Specifies requirements for: Password complexity, Length, Expiration, Storage, and Management.
- **Access Control Standards** - Outline the processes and principles associated with granting, restricting, and managing access to systems, applications, data, and facilities.
    - Details how access rights should be assigned, reviewed, and revoked.
    - Ensures that users have appropriate access levels based on their roles and responsibilities within an organization.
- **Physical Security Standards** - Outline measures and controls that are put in place to protect an organization's building, equipment, resources, and personnel from physical threats that could lead to security breaches or harm.
    - Threats can include unauthorized access, theft, vandalism, natural disasters, as well as others.
- **Encryption Standards** - Sets of specifications and protocols for securing electronic data through the process of transforming readable data into an unreadable format, using algorithms and cryptographic keys.

Procedures

- **Change Management Procedures** - A formal process that ensures all changes to IT systems, applications, or other critical technical processes are conducted in a controlled and systematic manner.
    - Aims to minimize the potential negative impact changes could have on a system's reliability, security, and availability.
- **Onboarding/Offboarding Procedures** - Defined set of processes that detail how employees, contractors, or partners are granted access to an organization's resources when they join (onboarding) and how access is revoked when they leave (offboarding).
    - Procedures are crucial for maintaining security controls over who has access to what within the organization.
- **Playbooks Procedures** - A comprehensive set of documented procedures that provide detailed instructions on how to handle specific security incidents or events.
    - An operational guide that outlines the steps that should be taken by the security team and other stakeholders to effectively manage and mitigate security incidents.

External Consideration of Effective Security Governance

External Considerations - Any factors outside an organization that can impact its security posture and governance.

- Examples: **Regulatory, Legal, Industry, Local/Regional, National, Global**

Regulatory - Requirements set by governmental regulatory bodies that organizations must comply with.

- Such as: **GDPR (Data Protection), CCPA (Data Protection), Sarbanes-Oxley Act (Financial Reporting), HIPAA (Healthcare), FERPA (Education)**

Legal - Obligations arising from the legal system within which the organization operates, including contracts, service-level agreements (SLAs), intellectual property rights, and litigation risks.

- Examples: **Contractual Obligations, Intellectual Property Laws**

Industry - Benchmarks, standards, and best practices that are commonly accepted within an industry.

- Examples: **Payment Card Industry Data Security Standard (PCI DSS), Society for Worldwide Interbank Financial Telecommunications (SWIFT) Customer Security Controls Framework**

Local/Regional - Local and regional laws, norms, and cultural considerations that can impact an organization's operations, such as municipal privacy regulations or regional data sovereignty laws.

- Examples: **California Consumer Privacy Act (CCPA), German Federal Data Protection Act (BDSG)**

National - Country-specific laws and national security directives, including cybercrime laws, national data breach notification laws, and government-led cybersecurity initiatives.

- Examples: **Cybersecurity Information Sharing Act (CISA) in the United States, Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada**

Global - Encompasses international treaties, cross-border data transfer rules, global cybersecurity threats, and international cooperation frameworks.

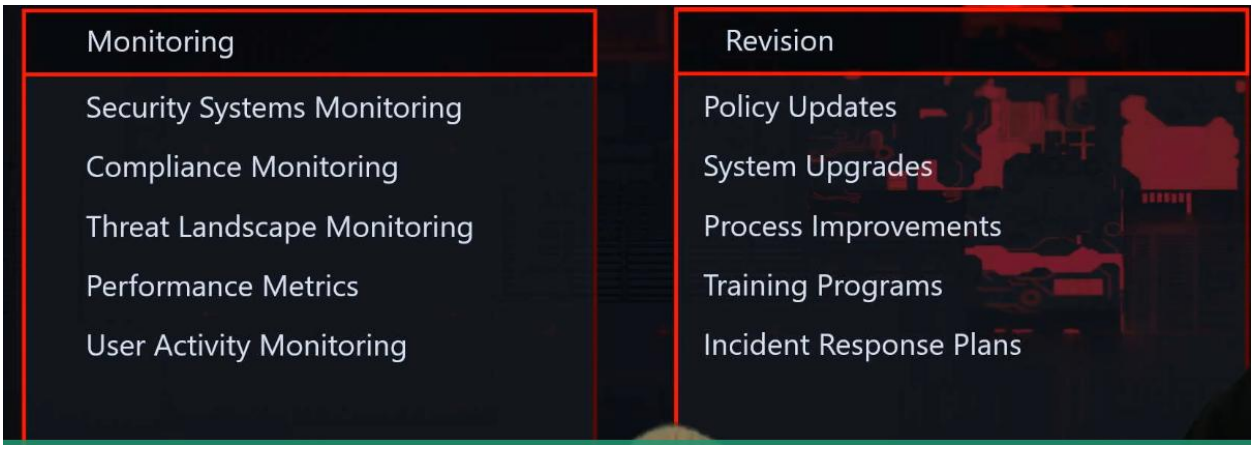
- Examples: **United Nations Guidelines for the Regulation of Computerized Personal Data Files, Convention on Cybercrime (Budapest Convention)**

Effective Integration into Security Governance

- Stay Informed
- Assess and Adapt
- Engage Experts
- Risk Management
- Document and Audit
- Communication and Training

Monitoring and Revision for Effective Security Governance

- Ensures that an organization's security posture remains strong and adaptive to changing conditions through ongoing assessments and improvements of security strategies, **policies**, and controls.
- Ensures that the organization's security strategy remains relevant and robust.



Types of Governance Structure of Effective Security Governance

Boards - Acts as governing bodies, often setting strategy and policy.

- Made up of a diverse group of stakeholders
- Provide oversight, financial governance, and high-level direction
- Ensure **Compliance**

Committees - Usually a subgroup of a larger governing body, like a board.

- Responsible for a specialized area like finance, HR, or IT
- Operate based on a defined mandate or terms of reference

Government Entities - Governmental bodies responsible for oversight at the local, regional, or national levels.

- Subject to public laws and regulations
- Roles can include funding, policy settings, and legal enforcement
- Often have the authority to audit or regulate other entities

Centralized/Decentralized

- **Centralized** - Focuses on central authority, usually in a single location
- **Decentralized** - Spreads authority across multiple units or locations

Roles and Responsibilities for Systems and Data of Effective Security Governance

- **Data Owner** - Accountable for making decisions regarding the data

- **Data Steward / Custodian** - Responsible for the day-to-day management, protection, and maintenance of data
- **Data Controller** - Manages how and why data is going to be used by the organization
- **Data Processor** - Handles the manipulation of the data as part of business processes