* Security Operations

**4.1 Security Techniques**

* **Secure baselines**
  + Establish
  + Deploy
  + Maintain
* **Hardening targets** 
  + Mobile devices
  + Workstations
  + Switches
  + Routers
  + Cloud infrastructure
  + Servers
  + ICS/SCADA
  + Embedded systems
  + RTOS
  + IoT devices
* **Wireless devices** 
  + Installation considerations
  + Site surveys
  + Heat maps
* **Mobile solutions** 
  + Mobile device management (MDM)
  + Deployment models
  + Bring your own device (BYOD)
  + Corporate-owned, personally enabled (COPE)
  + Choose your own device (CYOD)
  + Connection methods o Cellular
  + Wi-Fi o Bluetooth
* **Wireless security settings** 
  + Wi-Fi Protected Access 3 (WPA3)
  + AAA/Remote Authentication Dial-In User Service (RADIUS)
  + Cryptographic protocols
  + Authentication protocols
* **Application security** 
  + Input validation
  + Secure cookies
  + Static code analysis
  + Code signing
* **Sandboxing**
* **Monitoring**

Secure Baselines

* A secure baseline is a predefined configuration of a system.
* It is a benchmark for security settings. The minimum that should be maintained to protect the system.
* Minimum: Windows 11 OS, Debian servers, Cisco firewalls.
* For baselines to be effective:
  + Establish: Create a standard set of configurations for consistency.
  + Deploy: Implement the baselines across the organization.
  + Maintain: Regularly update and audit the baselines.

Hardening Targets

* Implementing measures to strengthen the security of systems.
* What are the targets? How can we harden (protect) them?
* **Mobile Devices**: Device encryption, Strong passwords, Mobile Device Management (MDM).
* **Workstation**s: Disable unnecessary services, enable firewalls and antivirus.
* **Switches**: Disable unused ports, use port security, implement VLANs for network segmentation.
* **Routers**: Change default credentials, implement subnets and VLANs, enable encryption.
* **Cloud**: Apply security groups, logging and monitoring.
* **Servers**: Secure configurations, Regular patches, Intrusion Detection/Prevention Systems (IDS/IPS).
* **ICS/SCADA**: Air gaps, Isolate from corporate networks, Use firewalls and VPNs, Implement strict access controls.
* **Embedded Systems**: Ensure secure firmware updates.
* **RTOS**: Secure communication channels, Apply security patches, Limit access to critical functions.
* **loT Devices**: Change default passwords, disable unused features, use network segmentation.

Installation Considerations

* Before installing a wireless network, perform a **site survey**. Check existing frequencies, install routers to minimize interference.
* Use **heat maps** to identify wireless signal strengths. It shows where the largest signal strengths are.

Mobile Device Solutions

* **MDM (Mobile Device Management):** Centralized management of mobile devices to enforce security and configurations.
* Deployment Models:
  + **BYOD (Bring Your Own Device)** is a policy that allows employees to use their personal devices to access work-related data.
  + **COPE (Corporate-Owned, Personally Enabled):** The company provides devices that employees can use for personal tasks, allowing better control over security.
  + **CYOD (Choose Your Own Device):** Employees select from a list of approved devices, balancing user preference with security.

Connection Methods

* **Cellular:** Use of mobile networks for data transmission.
* **Wi-Fi:** Wireless local networks.
* **Bluetooth:** Short-range wireless communication.

Wireless Security

* Configurations to protect wireless networks from unauthorized access.
* Includes encryption methods like WPA3.
* **WPA3**: Wi-Fi security protocol providing encryption.
* **RADIUS**: Central authentication for users connecting to the network.
  + **RADIUS** (Remote Authentication Dial-in User Service) **centralizes** authentication for different kinds of systems.
  + Remote access to a central server.
* **Cryptographic Protocols**: Use of secure protocols like AES to protect data at rest or TLS to protect data in transit.
* **Authentication Protocols**: Methods such as EAP (Extensible Authentication Protocol) to verify user identities.
  + **EAP** (Extensible Authentication Protocol) provides a method for two systems to authenticate.
  + EAP prevents access to the network until authentication is successful.

Application Security

* Measures taken to protect applications from threats.
* **Input Validation**: Ensuring that user input is checked for validity to prevent injection attacks.
* **Secure Cookies**: Setting cookie attributes to protect user sessions.
* **Static Code Analysis**: Analyzing source code for vulnerabilities.
* **Code Signing**: Using digital signatures to verify the authenticity and integrity of software.

SandBoxing

* Running apps in isolated (secure) environments to prevent them from affecting the rest of the system.
* Allows safe testing of untrusted software.
* Limits the potential damage from malicious software.
* Virtual Machines are commonly used as sandboxes.

**4.2 Asset Management**

* **Acquisition/procurement process**
* **Assignment/accounting** 
  + Ownership
  + Classification
* **Monitoring/asset tracking** 
  + Inventory
  + Enumeration
* **Disposal/decommissioning** 
  + Sanitization
  + Destruction
  + Certification
  + Data retention

Acquisition

* Ensure that hardware and software are sourced from reputable vendors.
* Conduct vendor assessments and security reviews.
* Specify security certifications and compliance requirements.

Assignment

* Ownership helps ensure accountability for assets.
* Owners are responsible for implementing security measures.
* Classification helps determine the level of security controls needed.
* Sensitive and critical assets require more protection.
* Classify assets based on their sensitivity, criticality and value.

Monitoring

* Maintain an up-to-date inventory to track all assets and ensure that none are unaccounted for.
* Facilitates the identification of shadow IT (unauthorized or rogue devices).
* Ensure tracking of all assets. Helps in identifying assets that may be vulnerable or outdated.

Disposal

* **Sanitization**: Ensures that data is erased from devices. Prevents unauthorized access to sensitive data.
* **Destruction**: Physical destruction of storage media ensures that data cannot be recovered.
* **Certification**: Provides formal assurance that data sanitization and destruction procedures have been properly carried out.
* **Retention**: Ensures that data is retained only as long as necessary.

Data Disposal Concepts

* **Shredding**: Passes papers through a shredder
* **Burning**: Placing in an incinerator
* **Pulping**: Reduces shredded paper to mash
* **Degaussin**: Makes data on a tape unreadable
* **Pulverizing**: Physically destroying media

**4.3 Vulnerability**

* **Identification methods**
  + Vulnerability scan
  + Application security
    - Static analysis
    - Dynamic analysis
    - Package monitoring
  + Threat feed
    - Open-source intelligence (OSINT)
    - Proprietary/third-party
    - Information-sharing organization
    - Dark web
  + Penetration testing
  + Responsible disclosure program
    - Bug bounty program
  + System/process audit
* **Analysis** 
  + Confirmation
    - False positive
    - False negative
  + Prioritize
  + Common Vulnerability Scoring System (CVSS)
  + Common Vulnerability Enumeration (CVE)
  + Vulnerability classification
  + Exposure factor
  + Environmental variables
  + Industry/organizational impact
  + Risk tolerance
* **Vulnerability response and remediation** 
  + Patching
  + Insurance
  + Segmentation
  + Compensating controls
  + Exceptions and exemptions
* **Validation of remediation** 
  + Rescanning
  + Audit
  + Verification
* **Reporting**

What is a Vulnerability?

* It is a weakness in a system.
* These weaknesses can be exploited by attackers to cause damage.
* Vulnerabilities can arise from software bugs, misconfigurations, or more sources.
* It is important to keep systems updated to protect from vulnerabilities.

Valnerability Management Process

* **Identify**
  + The first step is to identify vulnerabilities in systems. This can be done by scanning with software.
* **Assess**
  + Once they are identified. they need to be assessed to determine their severity.
* **Remediate**
  + This involves patching, updating settings, or adding more security controls.
* **Report**
  + Generate reports on the progress, and security posture.
* **Monitor**
  + Monitor the systems to ensure that problems do not re-emerge.

Identification

* Identifying vulnerabilities allows organizations to address security risks before they can be exploited by attackers.
* Methods for identifying vulnerabilities include:
* **Scanning with an app** -Automated software to scan systems (e.g Nessus).
* **Static Analysis** - Reviewing code without running the program. Identifying poor coding techniques or potential flaws in the program.
* **Dynamic Analysis**-Analyzing software while it is running. Detect live issues and responses.
* **Package Monitoring** - Monitors 3rd-party packages Tor security.
* **Open-source intelligence (OSINT)** - Using publicly available information to identify vulnerabilities.
* **Proprietary/third-party**- Provides detailed and specialized threat information.
* **Information-sharing organization** - They share threat information.
* **Dark web** - Monitors dark web forums for intel.
* **Penetration Testing** - Simulate real-world attacks to find vulnerabilities.
* **Bug Bounty Program** - Offer rewards for finding and reporting vulnerabilities.
* **System Audit** - Reviews of systems and processes.

Challenges

* False positives and false negatives relate to the effectiveness of vulnerability management.
* **False positives** occur when a vulnerability scanner reports a vulnerability that is not actually present in the system.
* **False negatives** occur when a vulnerability scanner fails to detect an actual vulnerability that exists in the system. It misses a real security issue.

Analysis (Assessment)

* Assess the severity of each identified vulnerability. This step often involves assigning a score or severity level.
* Prioritize them based on their level of risk and potential impact. The most critical vulnerabilities should be addressed first.
* A system called is **CVSS** used to provide a numerical score to vulnerabilities.
  + **CVE (Common Vulnerability and Exposures)**
  + A system for identifying vulnerabilities. Each vulnerability is assigned a unique identifier.
  + It creates a common language that allows professionals to refer to vulnerabilities.
* This helps organizations prioritize and respond effectively.
* **0.0-3.9**: Low severity
* **4.0-6.9**: Medium severity
* **7.0-10.0**: High severity
* **The Exposure Factor (EF)** is the percentage of asset value at risk.
* **Risk Tolerance** is the level of risk an organization is willing to accept.

Remediation (Mitigation)

* Vulnerability remediation (mitigation) is the process of reducing or eliminating the identified vulnerabilities in a system.
* The goal is to minimize the impact of a potential exploitation.
* Common vulnerability mitigation strategies:
  + Applying Patches and updates
  + Segmentation; Dividing networks to limit the spread of attacks.
  + Implement firewalls and Intrusion Prevention Systems (IPS)
  + Purchase insurance; Financial protection against security breaches.
  + Exemptions; justifications for not remediating certain vulnerabilities.
* **Rescanning**: Re-running vulnerability scans after remediation.
* **Audit:** Review of remediation efforts. Verifies compliance with policies.
* **Verification:** Testing to confirm the effectiveness of remediation.

Reporting

* Documenting the findings and remediation efforts.
* Provides transparency and supports decision-making.
* **Remediation Actions**: Steps taken to address vulnerabilities.
* **Validation Results**: Outcomes of rescanning, auditing, and verification.
* **Recommendations**: Suggestions for future improvements

**4.4 Security Alerting and Monitoring**

* **Monitoring computing resources**
  + Systems
  + Applications
  + Infrastructure
* **Activities**
  + Log aggregation
  + Alerting
  + Scanning
  + Reporting
  + Archiving
  + Alert response and remediation/validation
  + Quarantine o Alert tuning
* **Tools** 
  + Security Content Automation Protocol (SCAP)
  + Benchmarks
  + Agents/agentless
  + Security information and event management (SIEM)
  + Antivirus
  + Data loss prevention (DLP)
  + Simple Network Management Protocol (SNMP) traps
  + NetFlow
  + Vulnerability scanners

Computer Resources

* **Systems** — Continuous surveillance of OS, servers, and other systems.
* **Applications** — Track the performance and security of apps.
* **Infrastructure** — Observing network and hardware components.

Monitoring Activities

* **Log Aggregation** — Collecting logs from various sources.
* Facilitates analysis and correlation of events.
* Tools: SIEM tools (Splunk is popular).
* **Alerting** — Generating notifications for events or anomalies.
* Informs security teams of issues.
* Tools: SIEM, Data Loss Prevention (DLP) protect sensitive data from leaks.
* **Scanning** — Checking systems for vulnerabilities.
* Tools: Vulnerability scanners like Nessus, Qualys.
* **Reporting** — Reports on performance and security.
* Tools: SIEM, Benchmarks (Security configuration guides).
* **Archiving** — Storing logs for future reference.
* **Quarantine** — Isolating affected systems to prevent the spread of malware/threats.
* Tools: Antiviruses, DLP systems.
* **Alert Tuning** — Adjusting alert thresholds to reduce false positives.
* Tools: Configure settings within SIEM tools.

Additional Monitoring Tool

* **Security Content Automation Protocol (SCAP)** — Automating vulnerability management and security assessments.
* **Agents** — Software installed on devices to collect data (real-time monitoring).
* **Agentless** — Collects data without installing software on devices.
* **NetFlow** — Network protocol for collecting IP traffic information. Monitors and analyzes network traffic flows.

**4.5 Firewall Configuration**

* **Firewall** 
  + Rules
  + Access lists
  + Ports/protocols
  + Screened subnets
* **IDS/IPS** 
  + Trends
  + Signatures
* **Web filter** 
  + Agent-based
  + Centralized proxy
  + Universal Resource Locator (URL) scanning
  + Content categorization
  + Block rules
  + Reputation
* **Operating system security** 
  + Group Policy
  + SELinux
* **Implementation of secure protocols** 
  + Protocol selection
  + Port selection
  + Transport method
* **DNS filtering**
* **Email security** 
  + Domain-based Message Authentication Reporting and Conformance (DMARC)
  + DomainKeys Identified Mail (DKIM)
  + Sender Policy Framework (SPF)
  + Gateway
* **File integrity monitoring**
* **DLP**
* **Network access control (NAC)**
* **Endpoint detection and response (EDR)/extended detection and response (XDR)**
* **User behavior analytics**

What is a Firewall?

* it is a network security device that monitors and controls incoming and outgoing network traffic.
* It protects networks from unauthorized access.
* It is like a gatekeeper that sits between your network and the outside world.
* Fireware can be software or hardware. Software firewalls are installed on individual computers, while hardware firewalls are standalone devices.

Firewalls

* Firewalls work by using a set of rules to determine whether to allow or block connections. These rules are called **access control lists (ACLs)**.
* They are relatively easy to manage. Once the rules have been configured, they can be set and forget.

Protocols & Ports

* A protocol is a set of rules that govern how digital communication should take place.
* A **port** is an entry point into an application. Each port is associated with a specific service.
* Protocols are represented with port numbers.
* There are **65535** ports, the **first 1024 are reserved** for specific apps.

**Most Common Protocols**

* FTP - File Transfer - Port# 20/21
* SSH - Secure connection to a computer - Port# 22
* SMTP - Email - Port# 25
* HTTP - Unsecure web browsing - Port# 80
* HTTPS - Secure web browsing - Port# 443
* POP - Email Management - Port# 110
* IMAP - Email Management - Port# 143

Screened Subnet

**DMZ (Demilitarized Zone)**

* A DMZ is a layer of security between an internal network and the publi
* The goal is to protect the internal network from exposure to general internet users.
* The DMZ is isolated from the private network by firewalls.
* Most of the websites you connect to are their DMZs.

IPS/IDS (Intrusion Prevention Systems/Intrusion Detection Systems)

* IDS and IPS watch network traffic and take action based on events.
* IPS **blocks (prevents)** attacks before it reaches the target.
* IDS **detects attacks** and **alerts users** but doesn't block the attack.
* **Trends**: Monitor network traffic patterns to identify **unusual activity**.
* **Signatures**: Use **predefined patterns** to detect known threats.

Web Filters

* **Agent-Based**: Software installed on user devices to filter web content.
* **Centralized Proxy**: A server that filters web traffic for multiple users.
* **URL Scanning**: Checks web addresses for malicious or inappropriate content.
* **Block Rules**: Rules that specify which content to block.
* **Reputation**: Uses reputation scores to block or allow web traffic.

Security Enhancement

* **Operating System Security**
* **Group Policy**: Managing the security and configuration settings of Windows OS.
* **SELinux**: A set of kernel modifications and user-space tools for enhanced security.
* **Secure Protocols**
* **Transport Method**: Determining how data will be securely transported over the network (e.g., VPN).

DNS (Domain Name System)

* Do you know the phone numbers of all your contacts? But you know to whom each name refers to, right? Same principle!
* The **DNS** is the phonebook of the Internet. It translates readable names like **www.amazon.com** to IP addresses.
* It allows us to retain names like **espn.com** instead of retaining IP addresses like 192.118.24.10
* **DNS Filtering**: Filters DNS queries to block access malicious websites.

Email Security

* **DMARC** - Email system designed to detect and prevent spoofing.
* **DKIM**: Adds a digital signature to emails to verify the sender's domain.
* **Sender Policy Framework (SPF):** Validates that emails come from authorized servers.
* **Gateway:** Email security gateways filter emails for spam, phishing, malware.

Security Enhancement

* **File Integrity Monitoring**: Monitors files for unauthorized changes. Used to detect tampering.
* **Data Loss Prevention (DLP):** Tools used to detect the unauthorized transmission of sensitive data.
* **Network Access Control (NAC):** Controls access to the network based on device compliance.
* **Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR)**
  + **EDR:** Tools responding to threats on endpoint devices.
  + **XDR:** Expands EDR to include threat detection and response across multiple security layers (network, endpoint, server, email, etc.).
* **User Behavior Analytics (UEBA):** Monitors and analyzes user behavior to detect anomalies and insider threats.

**4.6 Identity & Access Management (IAM)**

* **Provisioning/de-provisioning user accounts**
* **Permission assignments and implications**
* **Identity proofing**
* **Federation**
* **Single sign-on (SSO)** 
  + Lightweight Directory Access Protocol (LDAP)
  + Open authorization (OAuth)
  + Security Assertions Markup Language (SAML)
* **Interoperability**
* **Attestation**
* **Access controls**
  + Mandatory
  + Discretionary
  + Role-based
  + Rule-based
  + Attribute-based
  + Time-of-day restrictions
  + Least privilege
* **Multifactor authentication** 
  + Implementations
  + Biometrics
  + Hard/soft authentication tokens
  + Security keys
  + Factors
  + Something you know
  + Something you have
  + Something you are
  + Somewhere you are
* **Password concepts** 
  + Password best practices
  + Length
  + Complexity
  + Reuse
  + Expiration
  + Age
  + Password managers
  + Passwordless
* **Privileged access management tools** 
  + Just-in-time permissions
  + Password vaulting
  + Ephemeral credentials

IAM

* IAM is a set technologies that organizations use to control access to their apps, data, and more.
* IAM ensures that only authorized entities can access the resources they need.
* IAM is essential for maintaining the security and integrity of an organization's resources. It helps prevent unauthorized access.

Authentication

* Authentication is the process of determining whether someone is who they say they are.
* Users are typically identified with a user ID, and authentication occurs when the user provides credentials such as a password.
* Authentication keeps networks secure by allowing only authenticated users to gain access to protected resources.

IAM in CyberSecurity

IAM helps address security challenges and contributes to the security strategy of an organization:

* **Authentication:** only authorized entities gain access to resources.
* **Multi-Factor Authentication (MFA):** adds an extra layer of security.
* **Provisioning:** Creating user accounts and granting them access to resources.
* **De-provisioning:** Removing user accounts and revoking access to resources when no longer needed.
* **Identity Proofing:** Verifying the identity of users during the account creation process.
* **Knowledge-based questions**, document verification, and biometric verification.
* **Permission Assignments:** Assigning specific permissions to users based on their roles.
* Ensuring **least privilege** by granting only the necessary permissions to perform job functions.

SSO (Single-Sign-On)

* SSO is an authentication method that enables users to authenticate with multiple apps by using one set of credentials.
* By using SSO, organizations reduce the number of passwords that users have to remember.

Federation

* Federation is the process of establishing a trust relationship between different organizations to enable access to resources without the need for separate sets of credentials.
* Federation allows users to access resources in one domain using their identities from another Facebook trusted domain.

Authentication Protocols

* Authentication protocols are standard processes used to verify the identity of a user trying to access a secure resource.
* These protocols ensure that only authorized individuals are granted access.
* The most common are:
* **Kerberos**: uses tickets to verify the identities of users.
* **SAML**: often used for SSO and federation.
* **Open ID**: provides authentication and SSO.

Authorization Protocols

* Authorization protocols define methods to grant or deny access to authenticated users.
* **OAuth** al lows users to grant third-party apps access to their resources without having to share their passwords (federation).
* Commonly used for token-based authentication.

LDAP (Lightweight Directory Access Protocol)

* LDAP is commonly used for querying and modifying directories (databases that store information about users, devices, etc.)
* LDAP is also used for authenticating users against a directory.

IAM in CyberSecurity

**InteroperabiIity:** Ensuring different IAM systems and apps can work together seamlessly.

**Attestation:** A process of verifying that a user or system meets certain security requirements.

Access Control Schemes

* The methods used to manage access to resources.
* They are essential for ensuring that only authorized individuals have the appropriate level of access to specific resources.
* There are several access control schemes commonly employed in IAM: **RBAC, MAC, Rule-BAC, ABAC, DAC.**

**Role-Base Access Control(RBAC)** is based on your role in the organization.

* The administrator determines what kind of access a user has.
* Useful for users in a department with same job functions.

**Mandatory Access Control (MAC)** uses labels to determine access.

* It is based on clearance levels. Every object gets a label, users are labelled with rights on what they can access.
* It is common in the military.

**Discretionary Access Control (DAC):** the ow of data determines access.

* Access can be modified by users. It is has weak security because it relies on the owner of the file.

**Attribute-based Access Control (ABAC)** creates relationships for authorization. Many criteria are used to determine access.

* It considers IP address, time, GPS location, etc. Policies typically use plain language.

**MFA** (Multi-Factor Authentication)

* It is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence.
* MFA requires 2 or more verification factors to access a system.
* Factors are:
  + Something you know - Password, PIN
  + Something you are - Biometrics
  + Something you have - Smart cards, tokens
  + Somewhere you are - Geolocation-based

Password Policies

* Password policies establish guidelines for creating, and using passwords for users and systems. It includes:
  + **Password Complexity**: mix of uppercase and lowercase letters, numbers, and special characters.
  + **Password Length**: Minimum character length for strong passwords.
  + **Password Expiration**: Periodic expiration of passwords to ensure regular updates.
  + **Password History (Age):** Prohibit the reuse of previous passwords.
  + **Passwordless**: Authentication methods that do not require passwords, such as biometrics.

**PAM** (Privilege Access Management)

* PAM is a set of security controls used to manage and control access to privileged accounts.
* Privileged accounts are accounts that have higher privileges, such as administrator accounts.
* These accounts can perform sensitive tasks, such as installing software or accessing sensitive data.

Least Privilege

* It is a fundamental concept that restricts access rights for users to the **minimum levels necessary to perform their job functions.**
* Giving individuals the minimum level of access or permissions they need to perform their job functions, and no more.

PAM Best Practices

* PAM best practices helps organizations secure privileged accounts and reduce the risk of cyberattacks. Here are some key PAM best practices:
  + **Implement Least Privilege**: Limit privileges to the minimum required for users.
  + Maintain a clear separation between regular user accounts and privileged accounts.
  + **Use Strong Authentication**: Require MFA for accessing privileged accounts.
  + **Review Privileged Access**: Periodically review and audit privileged accounts.
  + **Implement Privilege Revocation**: Have a process in place to revoke privileged access when users change roles or leave the organization.
  + **Implement Anomaly Detection**: to identify unusual behavior on privileged accounts.

**4.7 Automation and Orchestration**

* **Use cases of automation and scripting** 
  + User provisioning
  + Resource provisioning
  + Guard rails
  + Security groups
  + Ticket creation
  + Escalation
  + Enabling/disabling services and access
  + Continuous integration and testing
  + Integrations and Application programming interfaces (APIs)
* **Benefits** 
  + Efficiency/time saving
  + Enforcing baselines
  + Standard infrastructure configurations
  + Scaling in a secure manner
  + Employee retention
  + Reaction time
  + Workforce multiplier
* **Other considerations** 
  + Complexity
  + Cost
  + Single point of failure
  + Technical debt
  + Ongoing supportability

Automation & Scripting

* Techniques used to enhance the efficiency and consistency of security operations.
* **Automation:** Use tools to perform tasks with minimal human intervention.
* Automation can be applied to: Incident Response, Vulnerability Management, Security Monitoring.
* **Scripting:** Write code (scripts) to automate repetitive tasks. Commonly with Python.
* Automation and Scripting are commonly seen in SIEM tools, SOAR, Patch management, Data analysis.

Use Cases

* **User Provisioning** - Automating the creation and deactivation of user accounts.
* **Resource Provisioning** - Automatically allocating IT resources as needed.
* **Security Groups** - Automating the management of security group (firewall) rules.
* **Ticket Creation** - Automatically generating tickets for security incidents or routine tasks.
* **Escalation** - Automating the escalation of incidents to appropriate personnel.
* **Enabling/Disabling Services and Access** - Automatically enabling or disabling services and access based on predefined criteria.
* **Continuous Integration and Testing** - Integrating automated security testing into the continuous integration/continuous deployment (CI/CD) pipeline.
* **Integrations and Application Programming Interfaces (APIs)** - Using APIs to integrate different security tools and automate workflows.

Benefits

* **Efficiency/Time Saving** - Reduces the manual effort required for routine tasks.
* **Enforcing Baselines** - Ensures that minimum security levels are consistently applied.
* **Standard Infrastructure Configurations** - Promotes the use of standard configurations across the organization.
* **Scaling in a Secure Manner** - Supports secure scaling of infrastructure and services.
* **Employee Retention** - Reduces repetitive manual tasks — higher job satisfaction.
* **Reaction Time** - Enables faster response to security incidents and operational changes.
* **Workforce Multiplier** - Allows teams to accomplish more with the same number of resources

Considerations

* **Complexity** - Automation can introduce complexity in system management.
* **Cost** - Implementation of automation and orchestration tools can be expensive.
* **Single Point of Failure** - Automation systems can become a single point of failure if not designed redundantly.
* **Technical Debt** - Requires regular review and maintenance.
* **Ongoing Supportability** - Automation systems require ongoing support and updates.

**4.8 Incident Response**

* **Process** 
  + Preparation
  + Detection
  + Analysis
  + Containment
  + Eradication
  + Recovery
  + Lessons learned
* **Training**
* **Testing** 
  + Tabletop exercise
  + Simulation
* **Root cause analysis**
* **Threat hunting**
* **Digital forensics** 
  + Legal hold
  + Chain of custody
  + Acquisition
  + Reporting
  + Preservation
  + E-discovery

What is a Security Incident?

* It is an event that could potentially jeopardize the security of an organization.
* Security Incidents include data breaches, ransomware attacks, insider attacks, etc.
* Impacts of an incident include financial loss, reputation damage, legal liability, etc.

Incident Response

* **Incident response** is the process of handling a cybersecurity incident.
* It is an approach that helps organizations recover from incidents.
* The purpose is to minimize the damage caused by an incident, ensure business continuity, to build stakeholder trust, to comply with legal laws restore normal operations as quickly as possible.
* The incident response process happens in 7 steps:
* **Preparation** 
  + Occurs before an incident.
  + Provides guidance to personnel on how to respond.
* **Detection (Identification) & & Analysis**
  + How to identify threats. All events aren’t security incideents.
  + Use software, CCTV, IDS, humans.
  + How dangerous is the incident? What is the potential impact.
* **Containment**
  + Disconnect and contain everything.
  + Limit the ability of an attack to spread.
* **Eradication**
  + Delete components from the attack.
  + Disable affected accounts.
* **Recovery**
  + Return systems to normal operations.
  + Restore servers.
* **Lessons Learned**
  + Find out what happened.
  + What you can do differently.
  + Provide training.

Lessons Learned

* Analyze an incident to understand what happened, why it happened, and how future incidents can be prevented.
* **Root Cause Analysis**: Identifying the underlying reasons for the incident.
* **Tabletop Exercises**: Discussion-based sessions where team members walk through hypothetical incident scenarios to evaluate the effectiveness of their plans.
* Simulations are more advanced and realistic exercises that replicate real-world cyber incidents. They involve active participation from the incident response team and often include live attacks on systems.

Digital Forensics

* Digital Forensics is the process of collecting information from security incidents/events.
* The information is collected to be **legally admissible** in a court of law.
* Digital forensics is essential for incident response, risk management, and legal proceedings.
* It is a discipline in cybersecurity combining technical expertise with legal knowledge.

Digital Forensics Terminology

* **Legal Hold** is a process used to preserve relevant information. A legal hold ensures that evidence is not altered or deleted, maintaining its integrity.
* **Chain of Custody** documents transfer of evidence from the time it is collected until it is presented in court. It records every person who handled evidence, the time it was collected, changes, transfers, storage.
* **Acquisition** is collecting evidence from various devices. Creating an exact copy of the data to ensure that the original evidence remains unaltered.
* **Reporting** is documenting the findings of a forensic investigation. Methods, evidence, analysis, conclusions.
* **Preservation** is the process of protecting evidence.
* **E-Discovery** (Electronic Discovery) is the process of collecting, digital information. Emails, audio/video files, databases, social media content, digital data.

**4.9 Investigations**

* **Log data** 
  + Firewall logs
  + Application logs
  + Endpoint logs
  + OS-specific security logs
  + IPS/IDS logs
  + Network logs
  + Metadata
* **Data sources** 
  + Vulnerability scans
  + Automated reports
  + Dashboards
  + Packet captures

Log

* A log is an entry that captures specific events. It can be generated by an app, the OS, devices, etc.
* Logs a re used for monitoring, troubleshooting, etc.

Types Of Logs

* **Firewall Logs** - Record of traffic allowed or blocked by the firewall.
  + Details include Source IP, Destination IP, Ports, Protocols.
* **Application Logs** - Logs generated by apps to record events and errors.
* **Endpoint Logs** - Logs from endpoint devices (e.g., PCs, laptops, mobile devices) capturing security events and application usage.
* **OS Logs** - Security logs maintained by the operating system.
  + Login attempts, security changes, system alerts.
* **IPS/IDS Log**s - Logs from Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).
  + Potential intrusion attempts and malicious activities.
* **Network Logs** - From network devices such as routers.

MetaData

* Data that provides information about other data, such as timestamps, file size, and ownership.
* Useful for investigations.

Data Sources

* **Vulnerability Scans** - Generated from scanning tools identifying vulnerabilities in systems.
* **Automated Reports**-Regularly generated reports from systems.
* **Dashboards** - Visual representation of security metrics.
* **Packet Captures** - Data captured from network traffic.