Security+ Study Guide:
Security Controls

By: Krystal Ballew

Security Controls

- **Security Control Types**
  - Preventative: Designed to be implemented prior to a threat event and reduce and/or avoid the likelihood and potential impact of a successful threat event.
    - Policies, standards, processes, procedures, encryption, firewalls, and physical barriers.
  - Detective: Designed to detect, log, and alert after an event has occurred.
    - Intrusion Detection System (IDS) and motion detectors.
  - Corrective: Used to remediate or mitigate the effect of a security incident and prevent the same security incident from recurrence.
    - Account lockout or sprinkler system coming on after detecting smoke.
  - Deterrent: Administrative mechanisms that are used to guide the execution of security within an organization.
    - Policies, procedures, standards, guidelines, laws, and regulations
  - Mitigating/ Compensating: Measures taken to address any weaknesses of existing controls or to compensate for the inability to meet specific security requirements due to various different constraints.
    - Multi-factor Authentication (MFA), patches, and firewalls.
  - Physical: The component put in place to protect a physical building, perimeter, database center, or server room.
    - Data center perimeter fencing, locks, guards, access control cards, biometric access control systems, surveillance cameras, and intrusion detection sensors.
  - Technical/Logical: The hardware and software components that protect a system against cyberattack.
    - Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.
  - Administrative: A set of security rules, policies, procedures, or guidelines specified by the management to control access and usage of confidential information.
    - Includes all the levels of employees in the organization and determines the privileged access to the resources to access data.
  - Managerial: The security controls that focus on the management of risk and the management of information system security.
    - Includes vulnerability management, change management, asset management and standardized penetration testing.
  - Procedural: Establish a framework for validating and maintaining the computer system and for ensuring that users understand how to use the system.
    - Take the form of standard operating procedures (SOPs) and user manuals.
  - Operational: The security controls that are primarily implemented and executed by people, as opposed to systems.
    - Security controls for day-to-day operations.

- **Physical Facility/ Data Center Security Controls**
  - Perimeter Security
    - Fencing/ Razor wire
    - Bollards

        - Good lighting
        - CCTV cameras
        - Signage
        - Drones
            - Easily monitor large areas
            - Site surveys
            - Damage assessments
        - Crime Prevention Through Environmental Design (CPTED)
            - Water features/ Architectural obstacles
        - Industrial Camouflage
            - Blend into the environment
            - No visible signs: “Security through Obscurity”
        - Fire Suppression and Detection Systems: Dupont FM-200
        - Air Gap: Physical space between facilities, server rooms, and networks.
    - Alarms and Sensors
        - Circuit-based
        - Motion/ Noise Detectors
        - Duress button
    - Door Access
        - Deadbolt/ lock and key
        - ID Badges/ Logical Visitor Logs
        - Employee key card/key fob
        - Biometrics /pin
        - Access Control Vestibule/ Mantrap
    - Security Guards
        - Access lists/ physical visitor log
        - Robot Sentries: Replace human guards with robot(s)
    - Vaults/ Safes

- **Physical Risk Mitigations for Server Rooms and Facilities**
    - Secure areas for live and backup data
    - Temperature sensors
        - Hot and cold isles in data centers and server rooms
        - Cooling systems
    - Moisture detection
    - Fire Suppression and Detection Systems: Dupont FM-200
    - Protected Distribution System (PDS): Metal cable/fiber protectors
    - Separate data centers in different geographic regions (In case of natural disaster)
    - Redundant ISP’s, hardware, and power supplies: Remove *single points of failure.*
    - Backup Power Supplies
        - Backup Gas Powered-Generator
        - Uninterruptible Power Supply (UPS)
        - Power Distribution Units (PDU): Power strip connected to ethernet for better control and monitoring of power usage across the network.
        - Dual Power Supplies
        - Power Conditioner
    - Redundant Data Storage
        - Redundancy: Remove *single points of failure* and create *fault tolerance.*
        - Redundant Array of Independent Disks (RAID)

Storage Area Network (SAN)	A network of storage devices that can be accessed by multiple servers or computers, providing a shared pool of storage space.
RAID 0	Striping. Splits data into blocks that get written across all drives in an array. Uses all storage capacity with no overhead. NOT redundant. Loss of any disk will cause complete data loss.
RAID 1	Mirroring. Two drives that contain the exact same data. Slower write speed, but provides redundancy if one drive fails.
RAID 5	Striping with parity across drives. Requires at least three drives. If a drive fails, data is pieced together using parity information on other drives. Loses storage space, but more cost effective than RAID 1.
RAID 6	Striping with dual parity across drives. Similar to RAID 5 but parity data is written to two drives. Requires at least four drives and can withstand two drives failing simultaneously. Good for a standard web server.
RAID 10	Mirroring and striping. Requires at least four drives. Provides speed of RAID 0 and redundancy of RAID 1. Most expensive way to provide redundancy.

Network Security

- **Physical Controls**
  - Port Security: Disable unused physical ports on network devices.
  - Hardware and vendor diversity: Fewer *attack surfaces* and *single points of failure.*
  - Redundancy: Remove *single points of failure* and create *fault tolerance.*
  - Use a *Defense-in-Depth* or *layered security* posture.
  - Replace legacy/deprecated systems at End of Life (EOL)/ End of Service Life (EOSL).

- **Technical/ Logical Controls**
  - Change all default usernames and passwords.
  - Disable unused logical ports/ use private ports.
    - Disable Telnet (Preferred) and use SSH.
    - Password Protect Telnet (if not disabled) and SSH
    - Disable remote login when not needed.
    - Use secure and updated versions of all protocols.
  - Network Segmentation
    - Physical Segmentation
      - System isolation/ Air Gap
      - Micro-segmentation: A network security approach that enables security architects to construct network security zone boundaries per machine in data centers and cloud deployments in order to segregate and secure workloads independently.
    - Virtual/ Logical Segmentation
      - VLANS
        - Collision domains: Data collisions may occur
        - Broadcast domains: Broadcasts are forwarded
      - Screened Subnet: Previously called Demilitarized Zone (DMZ)

        - Dual Firewalls (DMZ): This implementation uses two firewalls to create a DMZ.
        - Bastion Hosts: Dedicated server that lets authorized users access a private network from an external network.
        - Three-homed firewall: A network architecture where a single firewall is used with three network interfaces.
    - Subnets
        - Extranet: A private network for partners and suppliers
        - Intranet: Only available internally
        - IPv4 versus IPv6
            - Network Address Translation (NAT)
    - Virtual Wire Firewall
        - A firewall that is transparently installed on a network segment by binding two firewall ports (interfaces) together.
- Switch Security
    - Virtual Local Area Network (VLAN)s
        - Any broadcast domain that is partitioned and isolated in a computer network at the data link layer.
    - ARP Inspection
        - A security feature that protects Address Resolution Protocol (ARP) which is vulnerable to an attack like ARP poisoning.
        - Checks all ARP packets on untrusted interfaces and compares the information in the ARP packet with the DHCP snooping database and/or an ARP access-list.
    - Spanning Tree Protocol (STP)/ Rapid Spanning Tree Protocol (RSTP)
        - Prevents broadcast storms, unstable mac tables, loops, and collisions.
        - Blocking, Listening, Learning, Forwarding
        - Loop Protection: Prevents loops from forming on unmanaged switches.
        - Bridge Protocol Data Unit (BPDU) Guard: Disables a port if unwanted/ unsanctioned BPDU's are sent to it (when it's not supposed to receive any)
        - Root Protection: A port cannot be selected as the root port and is assigned an "alternate" port role and enters a blocking state.
    - DHCP Snooping
        - Excludes rogue DHCP servers and remove malicious or malformed DHCP traffic.
    - Mac Filtering
        - Prevents physical connections from neighboring MAC addresses.
        - *Security through obscurity:* More of an administrative tool than a security tool.
    - Broadcast Storm Control
        - The switch intentionally ceases to forward all broadcast traffic if the bandwidth consumed by incoming broadcast frames exceeds a designated threshold.
    - Flood Guard
        - Can limit the number of devices that can communicate through any particular switch interface.
        - Protects against Denial of Service (DoS) attacks and SYN flood attacks.
    - MacSec Encryption
        - A security protocol that guards against network data breaches by encrypting data traffic between Ethernet-connected devices.
- Router Security

- Disable Dynamic Trunking Protocol (DPT)
- Disable old, insecure routing protocols like RIPv1.
- Routing Protocols
    - Routing Information Protocol (RIP)
        - One of the oldest distance-vector routing protocols which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
            - RIPv1: Deprecated. Do not use.
            - RIPv2: An enhanced version of RIP that includes support for important routing features such as class-less addressing and variable-length subnet masks.
            - RIPng: (RIP next generation) is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol.
    - Interior Gateway Routing Protocol (IGRP)
        - A type of routing protocol used for exchanging routing table information between gateways within an autonomous system (AS).
        - This routing information can then be used to route network-layer protocols like IP.
    - Enhanced Interior Gateway Routing Protocol (EIGRP)
        - Advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration.
        - The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers.
    - Open Shortest Path First (OSPF)
        - An Interior Gateway Protocol (IGP) for the Internet. Used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network. More prone to cyberattacks.
    - Intermediate System to Intermediate System (IS-IS)
        - Designed to move information efficiently within a computer network by determining the best route for data through a packet switching network. Less prone to cyberattacks.
    - Exterior Gateway Protocol (EGP)
        - A routing protocol used to connect different autonomous systems (AS) on the Internet from the mid-1980s until the mid-1990s, when it was replaced by Border Gateway Protocol (BGP). Deprecated. Not used.
    - Border Gateway Protocol (BGP)
        - A standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems on the Internet. Mostly used for large autonomous systems (AS) by Internet Service Providers (ISP).
- Mac Address Filtering
    - Block, allow or filter traffic through router based on the hardware mac-address of the device.

- Network Access Control (NAC)
    - When someone connects to a network on a Bring-Your-Own-Device (BYOD) environment, NAC performs a security posture/ health assessment to determine whether it is safe to connect.
        - Persistent Agents: Software installed on local device.

- Dissolvable Agents: Software runs but does not stay installed on the machine.
- Agentless: Checks are made during log in and log off.
- Quarantine Network: Built for devices that don't pass the health check.

- Network Security Appliances/ Devices (Hardware-Based)
  - Firewalls
    - Firewalls can be hardware or software appliances.
    - Firewall rules frequently consist of a source address, source port, destination address, destination port, and an action that determines whether to *Allow* or *Deny* the packet.
    - Access Control Lists/ ACL's
      - Whitelists/ Blacklists
        - Allow List/ Block List: Can block a range of IP addresses that are not allowed in the network.
          - Explicit/Implicit Allow and Explicit/Implicit Deny
          - Explicit Allow: Rule specifically designed to add to the Whitelist.
          - Implicit Allow: Rules don't specifically deny traffic.
          - Explicit Deny: Rule specifically designed to add to a Blacklist.
          - Implicit Deny: Rules don't specifically allow traffic.
      - Subject, Object, Rule (Active, Passive, Rule-Definer)
        - Put the most specific rules on the top of the rule base so that it is not approved based on some generic, less important rule.
        - If you get to the bottom of the rule base and nothing matches, the traffic is denied.
        - Any rules listed will create a log.
      - Port Filtering
        - Use private ports.
        - Use secure versions of protocols.
        - Block port 23 for telnet.
      - Firewall-Based Content Filter
        - Controlling the content users within a network can access over the Internet.
    - Dynamic Packet Filtering
      - Enables a Screen, which sits between the client and server, to examine each data packet as it arrives.
      - Based on information in the packet, state retained from previous events, and a set of security policy rules, the Screen either passes the data packet, or blocks and drops it.
    - Stateless Firewalls
      - Older and does not keep track of traffic flows. Needs more rules because it doesn't remember active sessions.
    - Stateful Firewalls
      - Remembers sessions and traffic flows & needs fewer rules. Rules might only allow inbound traffic initiated from the inside.
    - North/South Traffic: Network traffic flowing into (South) and out of (North) a data center.
      - Ingress: Data ingress refers to traffic that comes from outside an organization's network and is transferred into it

        - Egress: The process of data being shared externally via a network's outbound traffic
        - Different security posture than East/West
- East/ West Traffic: Network traffic among devices within a specific data center.
- Types of Firewalls
    - Network-Based Firewalls
        - Layer 3 Firewall
            - Routed Firewall Mode
                - The firewall is considered to be a L3 device in the network. It supports multiple interfaces with each interface on a different subnet and can perform network address translation (NAT) between connected networks.
            - Transparent Firewall Mode
                - The firewall acts as a L2 device, not an L3 or routed hop.
        - Network Firewall Deployments
            - Zero Trust
                - No one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.
                - This added layer of security has been shown to prevent data breaches.
            - Virtual Wire Firewall
                - A firewall transparently installed on a network segment by binding two firewall ports (interfaces) together.
            - Three-Homed Firewall
                - A network architecture where a single firewall is used with three network interfaces.
            - Dual firewalls (DMZ)
                - This implementation uses two firewalls to create a DMZ.
                - The first firewall (also called the "front-end" firewall) must be configured to allow traffic destined for the DMZ only.
                - The second firewall (also called "back-end" firewall) allows only traffic from the DMZ to the internal network.
    - Web Application Firewalls (WAF)/ Application Layer Firewalls
        - A specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service.
        - Allow or deny traffic based on input into that application.
        - Deep Packet Inspection: Inspects in detail the data being sent over a computer network, and may take actions such as alerting, blocking, re-routing, or logging it.
    - Next Gen Firewalls (NGFW)
        - Also called: Application Layer Gateway, Stateful Multilayer Inspection, or Deep Packet Inspection

        - Deep Packet Inspection: A type of data processing that inspects in detail the data being sent over a computer network, and may take actions such as alerting, blocking, re-routing, or logging it.
        - Can contain Intrusion Prevention Systems (IPS) and Content Filtering.
- Load Balancer
    - Distributes a set of tasks over a set of resources, with the aim of making their overall processing more efficient.
    - Can optimize the response time and avoid unevenly overloading some compute nodes while other compute nodes are left idle.
    - Load Balancing Modes:

Round Robin	Client requests are forwarded to each server in turn going down the list of servers in a group.
Weighted Round Robin	Each server in a pool is given a fixed numerical weight so client requests are forwarded in a particular order.
Dynamic Round Robin	The numerical weight assigned to servers in a pool is assigned dynamically based on the server's current load and idle capacity
Active Load Balancing	Spreads out the workload traffic among multiple nodes based on availability
Affinity	Directs all requests from a particular end user to a specific server, which preserves information about the user session that might otherwise be lost.

- Network Intrusion Detection System (NIDS)
    - Passive Monitoring: Examines a copy of traffic via port mirror or network tap.
    - Out-of-Band Response: IDS sends RESET frames to stop subsequent frames but cannot block the first frame.
- Network Intrusion Prevention System (NIPS)
    - In-Line Monitoring: All traffic must flow through the appliance.
    - In-Band Response: Can monitor and block traffic on the spot.
        - Can examine traffic for signatures, anomalies compared to the baseline, behaviors, or heuristics (machine learning)
- Network Detection and Response (NDR) Solution
    - Looks for Behavioral Heuristics. Uses machine learning and data analytics to compare baselines and known good behavior to anomalous behavior. Unusual behaviors generate a report/ alert.
- Unified Threat Management (UTM)
    - A single hardware or software installation provides multiple security functions, including antivirus, content filtering, email and web filtering, anti-spam, and more.
- Proxy Servers
    - Sits between users and external network. Receives the user's request and sends the request on their behalf. Also receives the response, evaluates the response, and sends result back to user. Can control much of the traffic flow.
        - Application Proxy

                - Receives requests intended for another server and acts as the proxy of the client to obtain the requested service. You often use an application proxy server when the client and the server are incompatible for direct connection.
            - Forward Proxy
                - Internal proxy, used to protect and control internal users' access to the internet.
            - Reverse Proxy
                - Inbound traffic from the internet to your internal servers.
            - Open Proxy
                - Security concern. Uncontrolled proxy, available to anyone, usually used to circumvent security protocols.
        - Content Distribution Network (CDN)
            - Geographically distributed network of proxy servers and their data centers.
            - The goal is to provide high availability and performance by distributing the service spatially relative to end users.
            - Can come with DDoS mitigation tools.
- Network Security Appliances (Software-Based)
    - Security Information and Event Management (SIEM) Tool/ Log Analysis
        - Combines event, threat, and risk data into a single system to improve the detection and remediation of security issues and provide an extra layer of in-depth defense.
    - Security Orchestration Automation and Response (SOAR)
        - A group of cybersecurity technologies that allow organizations to respond to some incidents automatically.
    - Network Access Control(ler) (NAC)
        - An approach to computer security that attempts to unify endpoint security technology, user or system authentication and network security enforcement.
    - Software Defined Networking (SDN)
        - An approach to network management that enables dynamic, programmatically efficient network configuration to improve network performance and monitoring.
    - Software-Defined Visibility (SDV)
        - Visibility refers to being aware of everything within and moving through your network with the help of network visibility tools. SDV combines the pervasive reach of visibility with an automation framework.
    - NIC Teaming/ Load Balancing Fail-Over (LBFO)
        - The process of combining multiple network cards together for performance, load balancing, and redundancy reasons. Use NIC teaming to group two or more physical NICs into a single logical network device called a bond.
    - Web Security Gateway
        - A device, cloud service, or application that is deployed at the boundaries of a network to monitor and stop malicious traffic from entering the organization, and to block users from accessing malicious or suspicious web resources.
        - Includes URL filtering, spam filtering, malware inspection, routing and switching, IDS/IPS, firewall, bandwidth sharing, and VPN endpoints.
        - Next Gen Firewalls perform all these functions as well.
    - Content Filter/ Web Filter/ URL Filter

        - Controlling the content users within a network can access over the Internet.
        - Can be hardware, software or on a firewall.
    - Domain Name Service Security Extensions (DNSSEC)
        - A suite of extensions that improve Domain Name System (DNS) security by verifying that DNS results have not been tampered with.
        - Validates DNS responses with origin authentication and data integrity.
    - DNS Filter
        - Restrict Web Content
    - Data Loss Prevention (DLP) Software
        - Prevents the sharing or transmitting sensitive data through e-mail, cloud, physical/USB, or other means.
        - Pattern-matching and Watermarking
- Other Network Appliances
    - Hardware Security Model (HSM)
        - High-end cryptographic hardware to store encryption and decryption keys, and offload CPU overhead for cryptographic processing from other devices.
    - Jump Server/ Jump Box
        - A highly secure, hardened device that you can "jump" to and then "jump" to other servers after
    - Sensor/ Collector
        - Aggregate information from network, and sends it to a collector for correlation, and comparing. Sensor could be found on IPS device, for example.
    - Traffic Shaping Device
        - Defends against bandwidth-abusing Distributed Denial-of- Service (DDoS) attacks while ensuring quality of service (QoS).
        - Regulates abusive users, safeguards applications and networks against traffic spikes, and stops network attacks from overwhelming network resources.
        - Quality of Service (QoS): Creates an *undesired* list, giving priority over certain kinds of traffic over others, such as giving VoIP traffic a higher priority than web browsing.
- Network Infrastructure Hardening
    - Change default passwords for more secure configuration (hardening)
    - Enable usernames/ passwords (or just simple shared passwords) on user, enable and config modes.
    - Configure authentication on switches, routers, firewalls, IPS's etc.
    - Security patches with manufacturer
    - Replace legacy or deprecated systems that have reached End of Life (EOL) or End of Service Life (EOSL).
    - Disable old, unsecure routing protocols like RIPv1.
    - Disable unneeded protocols of hosts and firewalls.
    - Use Network Address Translation (NAT) and/or IPv6 addresses.
    - Review MITRE's CVE list and National Vulnerability Database (NVD)
    - Use Baselines for Trend Analysis and Integrity Measures Check
        - Use and performance baselines.
        - Security baselines
        - Configuration and network design baselines
    - Keep physical and logical network maps up to date with device names and IP address naming schemas.
        - Network diagrams help identify single points of failure.

        - Conduct frequent audits.
    - Use Site Surveys, Port Scanners (with operating system ID turned on), and Heatmaps/ Signal Strength Measures to look for rogue access points or evil twins.
    - Monitor and management potential breaches in supply chain security.

- **Proactive Network Security Concepts and Controls**

Honeypot	Single service or computer configured to act as a decoy, attracting attackers.
Honeynet	Network of honeypots used to lure in attackers and study their activities.
Honey Files	Seemingly important files located on a honeypot.
Fake Telemetry	Similar to honey files. Contains decoy or faked telemetry data that can be used to entice attackers while capturing data on and about the attack
Darknet	The dark web is an encrypted part of the internet not indexed by search engines and needs specific authorization to access.
DNS Sinkhole	Used to redirect all traffic for a given domain name to a specific monitored server.

- **Administrative Controls**
    - Identity and Access Management (IAM)
        - A framework of policies and technologies to ensure that the right users have the appropriate access to technology resources. Includes Account Life Cycle Maintenance.
            - Groups and Permissions
                - Put users into groups and grant privileges and permissions based on job function.
                - Read, write, execute permissions.
                - Manual and automated reviews of identities/ access
        - Directories
            - Lightweight Directory Access Protocol (LDAP)
            - Microsoft Active Directory (AD)
    - Authentication
        - The act of proving the identity of a computer system or user.
        - Passwords/ Keys/ Tokens
        - Password Vault: A password manager that allows users to store/manage their pw's.
        - Knowledge-Based Authentication (KBA)
            - Static: Pre-configured shared secrets to recovery password such as "the street you grew up on."
            - Dynamic: Questions based on identity verification, such as "which of these addresses look familiar to you."
        - Context-Based Authentication
            - Geofencing: A virtual perimeter for a real-world geographic area.
            - Time of day, physical location, behavior-based and risk-based Authentication
        - Authentication Factors
            - Something You Know: Password or PIN.
            - Something You Have: Cryptographic identification device or token.
            - Something You Are: Fingerprint, voice, or facial recognition.
            - Something You Do: Actions or gestures.
            - Somewhere You Are: Current location.
        - Examples of Multifactor Authentication (MFA)
            - Time-based, One-Time Password (TOTP)
                - Uses randomly generated code as an additional authentication token.

        - HMAC-Based, One-Time Password (HOTP)
            - HMAC stands for Hash-based Message Authentication Code.
            - The moving factor for the one-time password is based on a counter that increments each time a code is requested.
        - Smart Card
            - Chip card or integrated circuit card is a physical electronic authentication device.
        - Hardware Token
            - Contains the security credentials for a login session and identifies the user, the user's groups, the user's privileges, and, in some cases, a particular application.
        - Biometrics
            - Body measurements and calculations related to human characteristics.
        - Static Codes
            - PINs that stay the same until they are changed.
        - SMS/ Phone Call
            - Verifies phones numbers and phone access as a method of authentication.
        - Push Notifications
            - Enables user authentication by sending a push notification directly to a secure application on the user's device.
        - Authenticator Applications
            - Provides an extra layer of security to your online accounts by generating time-based one-time passwords (TOTPs)
        - Attestation
            - A mechanism for software to prove its identity. Requires companies to confirm via documentation that they have protected their network in a variety of ways, including through the use of MFA.
    - Authentication Protocols
        - Password Authentication Protocol (PAP)
            - No encryption. Passwords sent in cleartext unless the application itself provides the encryption.
        - Challenge Handshake Authentication Protocol (CHAP)
            - Encrypted challenge sent over the network.
            - 3-way Handshake
                - After the link is established, the server sends the challenge message. The client responds with the password hash calculated from the challenge and the password.
                - Server compares the received hash with the stored hash.
                - No password is being sent in the clear, unlike PAP.
                - Challenge response continues periodically during the connection.
        - Extensible Authentication Protocol (EAP)
            - Provides a secure way to send identifying information across a wireless network.
    - Authentication, Authorization and Accounting (AAA):
        - Controls access to computer resources, enforces policies, and audits usage.
            - Authentication: Proof that the user is who they claim to be.

        - Authorization: Proof that the user is granted permission to access data.
        - Accounting: Logging and Audit methods
    - AAA Servers (May use more than one type of AAA server for different resources).
        - Remote Authentication Dial-In User Service (RADIUS)
            - Centralized authentication for users logging in to routers, switches, firewalls, VPNs, servers, and 802.1x
            - Available for any server operating system
        - Terminal Access Controller Access-Control System (TACACS)
            - TACACS+: More recent version. Supports more authentication requests and response codes.
            - XTACACS (Extended TACACS): CISCO proprietary tools that has additional support for accounting and auditing.
        - DIAMETER:
            - Next-generation industry-standard protocol used to exchange authentication, authorization, and accounting (AAA) information in Long-Term Evolution (LTE) and IP Multimedia Systems (IMS) networks.
            - Evolution of RADIUS
        - Kerberos
            - Single Sign-On (SSO) with Kerberos: Authentication through a cryptographic ticket granting service. Authenticate once, trusted by the system.
            - Mutual authentication, the client, and the server, protects against on-path or replay attacks. More secure option.
        - IEEE 802.1X: Port-Based Network Access Control (NAC)
            - Centralized authentication, as opposed to PSK and same passwords for everyone. Enterprise versus personal.
            - Often integrated with Extensible Authentication Protocol (EAP)
            - Works alongside RADIUS, LDAP, and TACACS+
- Security Assertion Markup Language (SAML)
    - Open standard for authentication and authorization for users to access third party resources.
    - Doesn't work well for mobile application.
- Single Sign-On (SSO)
    - OAuth:
        - Authorization framework, not an authentication protocol
        - Determines which types of data are accessible to the user.
        - Works with Open ID Connect, which provides authentication.
    - OpenID:
        - An open standard and decentralized authentication protocol promoted by the non-profit OpenID Foundation.
    - Open ID Connect: Handles single sign-on authentication.
        - Establishes trust between one of your accounts (google, for example) and a third-party account, where you decide how much access the third-party account will have to your google account.
        - Links between accounts can be removed at any time.
        - Example: Facebook Connect
- Federated Identities
    - Can log in with credentials you have with other sites, such as google or Facebook.
    - Provides authentication for partners, suppliers, customers (not just employees)

- Certificates
  - The Certificate Authority (CA)
    - Digital certificates bind a public key with a digital signature and other details about the key holder.
    - A Certificate Revocation List (CLR) is a list of digital certificates that have been revoked by the CA before their scheduled expiration date.
  - Commercial Certificate Authorities
    - Built into your browser. Creates a key pair and sends the public key to the CA to be signed.
    - Purchase a web site certificate from a CA that will be trusted by everyone's browser.
  - Private Certificate Authority (Self-Signed)
    - Medium-large organizations can create an in-house CA. All devices must trust the internal CA.
      - Single CA: The single CA is both a root CA and an issuing CA.
      - Hierarchical CA: Several CA's share the load.
        - Limits damage if any CA becomes compromised.
        - Requires a Chain of Trust: Lists all the certs between the server and the root CA.
    - Web of Trust
      - Adds other users who vouch for and self-sign each other's certificates.
    - Mesh
      - Cross Certifying CA's. Doesn't scale well.
    - Mutual Authentication
      - Server and Client mutually authenticate to each other.
    - Self-Signed CA Programs
      - Windows Certificate Services
      - Linux or other operating systems use OpenCA.
    - Other Certificates
      - Web server SSL certificate
      - Code-signing certificate
      - Root certificate
      - Machine and computer certificates
      - Email certificates
      - User certificates
  - Public Key Infrastructure (PKI)
    - Policies, procedures, software, hardware, and employees needed to create, distribute, manage, store and revoke certificates.
      - Refers to the binding of public keys to people or devices.
    - Key Management Life Cycle
      - Key Generation: Create a key with strength, using the proper cipher.
      - Certificate Generation: Allocate a key to a user.
      - Distribution: Make the key available to the user.
      - Storage: Securely store and protect against unauthorized use.
      - Revocation: Manage keys that have been compromised.
      - Expirations: Monitoring the certificates shelf life.
    - Certificate Management
      - Prevent expired certificates.
      - Registration Authority (RA).

        - Certificate Revocation Lists with the Certificate Authority
            - Online Certificate Status Protocol (OSCP): The browser can check for certificate revocation.
    - Digital Signatures: Added to clear text messages.
        - Proves authentication and non-repudiation. Adds trust.
        - Verifies the message has not been tampered with by a MITM, because it is created with a private key and verified with the public key.
- Encryption Key Exchange
    - Symmetric Keys: A single shared key.
        - Private/Secret/ Session Key Cryptography
        - Faster but less secure.
        - Algorithms
            - Advanced Encryption Standard (AES): A symmetric block cipher chosen by the U.S. government to protect classified information.
                - AES is the symmetric algorithm of choice for most applications today and is the strongest block cipher choice. It is widely used, typically with 128 or 256-bit keys, the latter of which is considered strong enough to protect military TOP SECRET data.
            - Blowfish: A variable-length, symmetric-key, 64-bit block cipher.
            - Twofish: A symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.
            - Data Encryption Standard (DES): A symmetric-key algorithm for the encryption of digital data. Its short key length of 56 bits makes it too insecure for modern applications.
            - Triple Data Encryption Standard (3DES): a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.
    - Asymmetric Keys: Each user has a Public Key and a Private Key
        - Public Key Cryptography
        - Sessions are encrypted with the recipient's public key and decrypted with their private key.
        - Algorithms
            - Rivest, Shamir, and Adleman (RSA):
                - A type of asymmetric encryption, which uses two different but linked keys. In RSA cryptography, both the public and the private keys can encrypt a message. The opposite key from the one used to encrypt a message is used to decrypt it.
                - Most widely used asymmetric algorithm.
            - Digital Signature Algorithm (DSA)
                - A cryptographic algorithm used to generate digital signatures, authenticate the sender of a digital message, and prevent message tampering.
                - DSA works by having two keys: a private key owned by the sender and a public key held by the receiver.
            - Elliptical Curve Cryptography (ECC)
                - Uses curves instead of prime numbers. Lower CPU usage. Perfect for mobile devices.
            - Diffie-Hellman/ Diffie-Hellman (Key) Exchange (DH/DHE)
                - Allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure

channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

- ElGamal
  - An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange. It is probabilistic, meaning that a single plaintext can be encrypted to many possible ciphertexts.

- Ephemeral Keys
  - Session keys created with the symmetric and asymmetric keys, generated for each execution of a key establishment process.
- Static Keys
  - Intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establishment scheme.
- Perfect Forward Secrecy (PFS)
  - Uses DH-Ephemeral, or Elliptic Curve. Better than using traditional RSA.

- Encryption/ Cryptography
  - Protects confidentiality of data by scrambling it and making it unreadable to humans.
  - Homomorphic Encryption:
    - Conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form.
    - Uses a public key and is more secure than traditional encryption methods.
  - Encryption Key:
    - Stored in a file, which decrypts the cipher text back into plain text.
  - Protocols
    - Pretty Good Privacy (PGP)
      - A security program that enables users to communicate securely by decrypting and encrypting messages, authenticating messages through digital signatures, and encrypting files. It was one of the first freely available forms of public-key cryptography software. Perfect for lower budget cryptography needs.
    - Secure Socket Layer (SSL)/ Transport Layer Security (TLS)
      - A security protocol that provides privacy, authentication, and integrity to Internet communications. SSL eventually evolved into Transport Layer Security (TLS).Works with HTTP to route encrypted web traffic.
    - Temporal Key Integrity Protocol (TKIP)
      - A security protocol used in the IEEE 802.11 wireless networking standard. It was designed to provide more secure encryption than the earlier Wired Equivalent Privacy (WEP), without needing to replace existing hardware.
  - Ciphers/ Ciphertext
    - Stream Ciphers
      - A symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream. In a stream cipher, each plaintext digit is encrypted one at a time.
      - Examples: RC-4, Salsa, and SEAL
        - RC-4 is the most widely used stream cipher.
    - Block Cipher
      - A deterministic algorithm that operates on fixed-length groups of bits, called blocks.

        - Examples: AES, DES, 3DES, Twofish and Blowfish
            - AES is the most widely used block cipher.
    - Substitution Cipher
        - Units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key.
            - Monoalphabetic Cipher: A cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
                - Caesar: Replaces a letter with the letter 3 places after it in the Latin alphabet. A becomes D.
                - ROT13: Replaces a letter with the 13th letter after it in the Latin alphabet.
            - Polyalphabetic Cipher: A substitution cipher, using multiple substitution alphabets.
                - Vigenère Cipher: A method of encrypting alphabetic text where each letter of the plaintext is encoded with a different Caesar cipher, whose increment is determined by the corresponding letter of another text, the key.
                - One-Time Pad (OTP): An encryption system that is unbreakable providing certain conditions are met. Plaintext is paired with a random secret key that is also called a one-time pad.
    - Progressive Key Cipher
        - A primitive form of substitution encryption that uses a rolling key. Can be used with any of the above ciphers. Includes an incremental shift.
    - Transposition Ciphers
        - Scrambles the positions of characters without changing the characters themselves.
            - Rail Fence/ Zigzag: The plaintext is written downwards diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached, down again when the top rail is reached, and so on.
    - Blockchain Technology
        - An advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain.
- Cryptographic Encryption Appliances
    - Hardware Security Module (HSM)
        - High end cryptographic hardware to store encryption and decryption keys, and offload CPU overhead for cryptographic processing from other devices.
    - Trusted Platform Module (TPM)
        - Hardware component in motherboard of smaller/ mobile devices for cryptographic processing.
    - SSL/TLS Accelerator
        - Device on edge of network used to offload processor-intensive public-key encryption for Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) to a hardware accelerator.

        - Quantum Computing:
            - Performs very large calculations in a very short period.
            - Not 1's and zeros, but both 1's and zeros at the same time.
            - Renders existing cryptography useless.
            - Monitoring conversation would modify the keys, preventing verification.
            - Prevents MITM attacks.
    - Virtual Private Networks (VPNs)
        - Tunneling/ VPN Protocols
            - Point-to-Point Protocol (PPP)
                - TCP/IP protocol that is used to connect one computer system to another. Computers use PPP to communicate over the telephone network or the Internet. A PPP connection exists when two systems physically connect through a telephone line.
            - Point to Point Tunneling Protocol (PPTP)
                - A network protocol used to create VPN tunnels between public networks.
            - Layer Two Tunneling Protocol (L2TP)
                - An extension of the Point-to-Point Tunneling Protocol (PPTP) used by internet service providers (ISPs) to enable virtual private networks (VPNs).
            - IPsec:
                - Adds encryption and authentication to make the protocol more secure.
                    - Tunnel Mode: Provides end-to-end security by encrypting the entire IP packet, while. Used for connecting entire networks.
                    - Transport Mode: Only encrypts the payload of the packet. Used for host-to-host communication.
        - VPN Options
            - VPN Concentrator
                - Could be built into a firewall. Encrypts and decrypts the communication.
                    - Full Tunnel: Everything is sent to concentrator, and concentrator decides where to send.
                    - Split Tunnel: Administrator can configure that some information is sent through the tunnel and other information can be sent outside of the tunnel.
            - Site-to-Site VPN
                - A connection set up between multiple networks. This could be a corporate network where multiple offices work in conjunction with each other or a branch office network with a central office and multiple branch locations. Always-on.
            - Secure Socket Layer (SSL) VPN
                - Enables individual users to access an organization's network, client-server applications, and internal network utilities and directories without the need for specialized software.
            - HTML 5 VPN
                - Allows users from external sources to access internal resources via pre-configured connection types, using only a browser as a client.

Endpoint Security

- **Physical Controls**
  - Cable Locks
  - Privacy Screens
  - USB Data Blocker: Considered Data Loss Prevention (DLP) and prevents Malicious USB attacks.
  - Port Security: Disable unused physical ports.
  - Replace legacy or deprecated systems that have reached End of Life (EOL) and End of Service Life (EOSL).

- **Technical/ Logical Controls**
  - Strong Password Policies
    - Change all default usernames and passwords.
    - Minimum/ Maximum Password Age
    - Length/ character/ re-use restrictions
  - Antivirus and Anti-Malware
  - Full-Disk Encryption
  - Unified Endpoint Management (UEM)
    - Manage mobile and non-mobile devices.
    - An evolution of the Mobile Device Manager (MDM)
  - Boot Integrity (Chain of Trust)
    - Secure Boot
      - UEFI BIOS: Checks the bootloaders digital certificates and signature.
    - Trusted Boot
      - Early Launch Anti-Malware (ELAM): Checks for trusted drivers. Won't load untrusted drivers.
    - Measured Boot
      - Attestation server receives a boot report. Changes are monitored and managed.

- **Administrative Controls**
  - Strong password policies and procedures
  - Separate User Accounts
    - No shared or generic accounts
    - Restrict or disable guest accounts to avoid potential privilege escalation.
    - Only use privileged accounts when necessary
  - Account Limits
    - Users can only do what is needed for their job duties.
  - Perform routine Groups and Permissions audits
    - Correct permissions/ groups?
    - How are the resources being used?
    - Password complexity and length and prevent re-use.
      - Change passwords frequently.
      - Account lockout policy
  - Location-Based Policies
    - Network Location: Disallowing network access from certain countries
    - Geolocation: Process of determining the geographic position of an object or user.
    - Geofencing: A virtual perimeter for a real-world geographic area.

        - Geotagging: Adding geographical identification metadata to various media such as a photograph, video, websites, and SMS messages.
    - Time-based Access Rules
        - Disallowing network access before or after business hours.
    - Network Access Control (NAC)
        - Performs a security posture/ health assessment on the endpoint to determine whether it is safe to connect.

- **Endpoint/ OS Hardening**
    - Password-protect the BIOS/ EUFI
    - User Accounts: Minimum password lengths and complexity, with account limitations and password policies
    - Monitor and secure with anti-virus and anti-malware.
    - Review MITRE's CVE list and National Vulnerability Database (NVD)
    - Patches and Updates
        - Updates, service packs, security patches
        - Update firmware, apps, and OS
        - Patch Management
            - Automated and Scheduled
            - Test in isolated sandbox of VM before deploying.
            - Have a backup and rollback plan ready.
    - Disk Encryption
        - Full Disk Encryption (FDE)
            - Bitlocker
            - FileVault
        - Self-Encrypting Drive (SED)
            - Hardware-based encryption based on Opal storage standard.
    - Windows Registry
        - Primary configuration database which monitors unwanted application changes
        - Take a backup of the registry before changes.

- **Application Hardening**
    - Review MITRE's CVE list and National Vulnerability Database (NVD)
    - Limit open ports and services (logical)
    - Application and vendor diversity: Fewer attack surfaces
    - Windows User Account Control (UAC): Allows the app only the permission it needs or has been specifically allowed by the user.
    - Information Rights Management (IRM): Controls printing, editing, copying, pasting, or screenshots of documents.

- **Host-Based Security Appliances**
    - Host-Based Firewall
        - Firewall software that runs on an individual computer or device connected to a network.
        - These types of firewalls are a granular way to protect the individual hosts from viruses and malware.
    - Trusted Platform Module (TPM)
        - Hardware for individual devices that helps with cryptographic functions and isn't susceptible to dictionary attacks.

- Data Loss Prevention (DLP) Software
  - Prevents the sharing or transmitting sensitive data through e-mail, cloud, physical/USB, or other means.
- Host-Based Intrusion Detection System (HIDS)
  - Passive Monitoring: Examines a copy of traffic via port mirror or network tap.
  - Out-of-Band Response: IDS sends RESET frames to stop subsequent frames but cannot block the first frame.
- Host-Based Intrusion Prevention System (HIPS)
  - In-Line Monitoring: All traffic must flow through the appliance.
  - In-Band Response: Can monitor and block traffic on the spot.
    - Can examine traffic for signatures, anomalies compared to the baseline, behaviors, or heuristics (machine learning).
- Advanced Intrusion Detection Environment (AIDE)
  - A file and directory integrity checker, which creates a database from the regular expression rules that it finds in the config files.
  - Once this database is initialized it can be used to verify the integrity of the configuration files.
- End-Point Detection and Response (EDR) Solution
  - Machine learning and process monitoring to look for and block malicious actions instead of signatures.
  - Behavioral Heuristics
    - User and Entity Behavior Analytics (UEBA)
      - Uses machine learning and data analytics to compare Current baselines and known good behavior to anomalous behavior.
      - Unusual behaviors generate a report/ alert.
        - Use and Performance
        - Security
      - Trend Analysis

Policies and Procedures

- **Business Policies**
  - Background check
  - Social media analysis
  - User training
    - Gamification
    - Capture the Flag (CTF)
    - Tabletop Exercises
    - Phishing Simulations
    - Computer-Based Training (CBT)
    - Role-Based/ User Security Awareness Training

- **Business Documents**
  - Memorandum of Understanding (MOU)
    - A nonbinding agreement that states each party's intentions to take action, conduct a business transaction, or form a new partnership. This type of agreement may also be referred to as a letter of intent (LOI) or memorandum of agreement (MOA).
  - Memorandum of Agreement (MOA)

        - Can also be a legal document that is binding and hold the parties responsible to their commitment or just a partnership agreement.
    - Service Level Agreement (SLA)
        - A document that outlines a commitment between a service provider and a client, including details of the service, the standards the provider must adhere to, and the metrics to measure the performance.
    - Business Partnership Agreement (BPA)
        - Establishes rules for two or more parties going into business together. It's a legally binding document that outlines every detail of your business operations, ownership stakes, financials, responsibilities, and decision-making strategies.

- **Job Role-Based Policies**
    - Clean Desk Policy
    - Separation/ Rotation of Duties
        - Two-Person/ Dual Integrity
        - Mandatory Vacation
    - Principle of Least Privilege
    - Hiring/ Termination Policies
        - Onboarding/ Offboarding Policies
            - Disable employee access to VPN, e-mail, network, servers, and files.

- **Password Policies**
    - Change all default usernames and passwords.
    - Minimum/ Maximum Password Age
    - Length/ character/ re-use restrictions

- **Privacy Policies/ User Agreements**
    - Terms of Service/ Terms of Use/ Terms and Conditions (T&C's)
    - Privacy Notice/ Privacy Policy
    - Acceptable Use Policies
        - Prevent after hours login's (permissions)
        - Balance security with usability/ performance
    - Non-Disclosure Agreements (NDA)/ Non-Competes

- **Data Loss Prevention (DLP) Policies**
    - Prevents the sharing or transmitting sensitive data through e-mail, cloud, physical/USB, or other means.

- **Data Ownership Policies**
    - Data Sovereignty
        - Determines ownership of the data, and which laws apply to the governance of such data, based on geographic region.
    - Information Classification
        - Top secret, secret, confidential and unclassified
    - Access Control (Groups/ User Permissions)
        - Discretionary Access Control
            - Owner of the file controls the permissions.
        - Attribute-Based Access Control
            - A collection of attributes defines which rights to grant.

        - Rule-Based Access Control
            - A set of rules implemented by an administrator.
                - Geofencing: A virtual perimeter for a real-world geographic area.
                - Geographic access requirements/ Prohibiting after-hours log on's.
        - Role-Based Access Control
            - Roles associated with job function.
        - Mandatory Access Control (MAC)
            - Very restrictive, used in government systems.
        - Conditional Access
            - Setting conditions like location or employee status for access to cloud resources.
    - Privileged Access Management
        - Managing superuser, admin, and root users
        - Privileged accounts are stored in digital vaults.
        - Privileges are granted by request, doled out for a short time, and easily logged and audited.

- **Data Handling Policy**
    - Data Labels
        - Proprietary
        - Personally Identifiable Information (PII)
        - Protected Health Information (PHI)
    - Data Classification
        - Public/ Unclassified
        - Private/Classified/ Restricted/Internal Use Only
        - Sensitive
        - Confidential
        - Critical
    - Data Responsibilities
        - Data Owner
            - The entity that creates the data and is legally responsible and accountable for it.
        - Data Controller
            - Same as the data owner when a true data owner does not exist.
        - Data Processors
            - Any entity that works under the direction of the owner or controller, such as an IT department.
        - Data Custodian/ Data Steward
            - Any entity that handles the data daily or uses the data for business purposes.
        - Data Protection Officer (DPO)
            - Ensures that the organization processes the personal data of its staff, customers, and providers in compliance with applicable data protection rules.
    - Data Governance
        - Data Steward
            - Responsible for data classification and the application of rules
        - Data Retention Policies
            - How many years, and in which ways must the data be stored, protected, and later destroyed.
        - Sovereignty

- Determines ownership of the data, and which laws apply to the governance of such data, based on geographic region.

- **Data Life Cycle Policies**
  - Data Minimization: Collect as little as possible.
  - Purpose Limitation: Use data for only expressed purposes.
  - Protect the confidentiality, integrity and availability of data in use, in transit, and at rest.
  - Information Life Cycle
    - Creation and Receipt
    - Distribution
    - Use
    - Maintenance
    - Disposition/ Destroy
  - Data Retention/Disposal
    - Secure Data Destruction
      - Shredder
      - Degausser
      - Drill a hole through the disk/ destroy.
      - Incinerator
      - 3RD party certificate of destruction
    - Data Sanitization
      - Purge: Destroy some of the data.
      - Wipe: Unrecoverable deletion

- **Asset Management Policies**
  - Asset Tracking
    - Asset Tagging (RFID)
    - Procedures for lost or stolen devices
  - Configuration Management (CM) Policies
    - The process of maintaining systems, such as computer hardware and software, in a desired state.
    - Also, a method of ensuring that systems perform in a manner consistent with expectations over time.
  - Change Management Policy/ Change Control Policies
    - Request for Change (RFC)
    - Approval
    - Regression/ Rollback: If something has been broken in the change/update.

- **Mobile Device Management (MDM) Policies**
  - Centralized management of mobile devices.
    - Can implement screen locks, account lockout, patch management, firmware updates and remote wipe.
  - Corporate Device Management Models
    - Corporate Owned, Business Only (COBO)
      - Owned and managed by the company. Prohibits personal use on the device.
    - Corporate Owned, Personally Enabled (COPE)
      - Devices are owned by an enterprise and issued to an employee. Both the enterprise and the employee can install applications onto the device.
    - Choose Your Own Device (CYOD)

- Organization allows people to select the mobile devices they would like to use.
- Bring Your Own Device (BYOD)
  - Containerization to separate corporate information from personal info.
  - Important for offboarding to sanitize corporate data from personal device.

- Geofencing
  - A virtual perimeter for a real-world geographic area.
- Virtual Desktop Infrastructure (VDI)/ Virtual Mobile Infrastructure (VMI)
  - Creates a virtual desktop on a central server, and remote users can access this desktop from any physical machine over the internet.
  - Apps and data are managed and stored externally from the device (cloud).
  - Minimizes risk from device loss.

- **Risk Planning Policies/ Documents**
  - Cyber Risk Assessment
    - Risk Analysis
      - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.
    - Risk Awareness
      - Forms the foundation of an organization's defense against cyber threats. It involves educating employees about potential risks, promoting best practices, and fostering a culture of vigilance so cyber pitfalls and threats are avoided.
    - Audit Risk Model
      - Assesses the potential implications, risks and costs of a data breach or cyber-attack on the organization and its stakeholders.
        - Inherent Risk: The inherent probability that a cybersecurity event may occur due to a lack of countermeasures.
        - Residual Risk: Residual risk is what remains after risk mitigation efforts and internal controls have been implemented.
        - Risk Appetite: The level of risk that an organization is prepared to take on in order to achieve its objectives.
    - Risk Management Strategies
      - Acceptance
        - Acknowledging that the potential loss from a risk is not great enough to warrant spending money to avoid it.
      - Avoidance
        - Completely eliminating any hazard that might harm the organization.
      - Transference
        - Use of insurance, disclaimers, etc. to transfer liability for expected loss.
      - Mitigation
        - Reducing impact of potential risks by implementing controls and plans.
    - Qualitative Risk Assessment
      - The primary focus when using qualitative assessments is to quickly identify risks. These use either numerical ratings (1-5) or colors (green, yellow, and red) to rank risks based on their likelihood of occurrence (frequency) and impact on the business (magnitude).
    - Quantitative Risk Assessment

- Involve numerical values, statistical analyses, and measurable data to provide a more precise and objective measure of cybersecurity risks.
    - Single Loss Expectancy (SLE)
    - Annual Rate of Occurrence (ARO)
    - Annual Loss Expectancy (ALE)= SLE x ARO
- Risk Assessment Results
    - Risk Heatmap/ Risk Matrix
        - A graphical representation of cyber risk data where the individual values contained are represented as colors that connote meaning.
        - Risk heat maps are used to present cyber risk assessment results in an easy to understand, visually attractive and concise format.
    - Risk Register
        - A document used as a risk management tool and to fulfill regulatory compliance. A repository for all risks identified and includes additional information about each risk.
        - It can be displayed as a scatterplot or as a table.

- Privacy Impact Assessment (PIA)
    - An analysis of how personally identifiable information (PII) is handled to ensure compliance with appropriate regulations, determine the privacy risks associated with information systems or activities, and evaluate ways to reduce the risks.
- Incident Response Plan (IRP)
    - A written document, formally approved by the senior leadership team, that helps your organization before, during, and after a security incident.
- Business Impact Analysis (BIA)
    - Predicts the consequences of a disruption to your business, and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment.
        - Recovery- Time Objective (RTO)
            - The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
        - Recovery Point Objective (RPO)
            - The maximum amount of data, as measured by time, that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization.
        - Mean-Time to Repair (MTTR)
            - The average time it takes to recover from a product or system failure.
        - Mean-Time Between Failures (MTBF)
            - A measure of the reliability of a system or component, representing the average time that it will operate before it fails.
- Business Continuity Plan (BCP)
    - The capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident.
- Disaster Recovery Plan (DRP)
    - Process of maintaining or reestablishing vital infrastructure and systems following a natural or human-induced disaster, such as a storm or battle. It employs policies, tools, and procedures.
    - Disasters
        - Environmental
        - Person-made/ Malicious Insiders

                - Internal vs External
            - Site Resilience/ Redundancy/ Fault-Tolerance
                - Hot Sites
                    - Fully functional backup site that already has data mirrored.
                - Cold Sites
                    - Provides power, networking capability, and cooling, but no other hardware elements.
                - Warm Sites
                    - Contains all elements of cold sites but adds storage hardware. Still require data to be transported should a disaster occur.
    - Functional Recovery Plan (FRP)
        - This is a functional recovery plan, and it's a step-by-step guide from going from an outage to being back up and running.
    - Measurement System Analysis (MSA)
        - A thorough assessment of a measurement process, and typically includes a specially designed experiment that seeks to identify the components of variation in that measurement process.
    - Cybersecurity Insurance Policies
        - Risk Transference in the event of data breaches.

- **Vulnerability Management Policies**
    - Vulnerability Assessments
        - The process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimizing their attack surface.
        - Frequently conduct vulnerability assessments to find vulnerabilities and attack vectors and harden system.
- **Penetration Testing/ Ethical Hacking**
    - An authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.
    - Certain industries are required to conduct semi-regular penetration tests to stay compliant.
        - White Team: Rule-Makers
        - Blue Team: Defensive Team
        - Red Team: Offensive Team
        - Purple Team: Blended Teams
        - White Box/ Known Environment
        - Black Box/ Unknown Environment
        - Gray Box/ Partially Known Environment
        - Passive Foot-Printing: Collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, browsing through employees' social media profiles, looking at job sites and using Whois.
        - Reconnaissance: The practice of covertly discovering and collecting information about a system. This method is often used in ethical hacking or penetration testing.

Data/ Database/ Server/ File Security

- **Data Backups**
    - Full Backup:

        - A complete copy of a business or organization's data assets in their entirety. This process requires all files to be backed up into a single version.
        - It is the best data protection option in terms of speed of recovery and simplicity.
    - Incremental Backup
        - Successive copies of the data contain only the portion that has changed since the preceding backup (of any kind) was made.
        - When a full recovery is needed, the restoration process would need the last full backup plus all the incremental backups until the point of restoration.
    - Differential Backup
        - Copies all of the files that have changed since the last FULL backup was performed.
        - This includes any data that has been created, updated, or altered in any way.

- **Encryption**
    - Encryption/ Cryptography
        - Protects confidentiality of data by scrambling it and making it unreadable to humans.
        - Homomorphic Encryption
            - Conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form.
            - Uses a public key and is more secure than traditional encryption methods.
        - Encryption Key: Stored in a file, which decrypts the cipher text back into plain text.

- **Hashing**
    - The process of transforming any given key or a string of characters into another value, which can then guarantee integrity of the data.
    - Used for data integrity, continuity, and non-repudiation.
        - Message Digest
            - A fixed size numeric representation of the contents of a message, computed by a hash function. A message digest can be encrypted, forming a digital signature.
        - Check Digit
            - One or more digits (or letters) computed by an algorithm from the other digits (or letters) in the sequence input. With a check digit, one can detect simple errors in the input.
        - Checksum
            - A digital fingerprint of a piece of data (e.g., a block of text) which can be used to check that you have an unaltered copy of that data.
        - Salt/Pepper
            - A pepper is similar to a salt, a random bit of data added to the password before it's hashed through an algorithm. But unlike a salt, it's not kept in the database along with the hash value. Instead, it's usually hardcoded into the website's source code.
        - Hash Functions
            - Message Digest (Algorithm) 5 (MD5)
                - A widely used hash function producing a 128-bit hash value. Has collisions, do not use.
            - Secure Hash Algorithm (SHA-1)
                - Produces a 160-bit digest for the same input.
            - Secure Hash Algorithm 3 (SHA-2)

        - Commonly produces a 256-bit digest. The functions range from 224 to 512-bit.
    - Secure Hash Algorithm 3 (SHA-3):
        - Six hash functions with digests (hash values) that are 128, 224, 256, 384 or 512 bits: Newer, more secure, but slower.
        - SHA3-256 is the most widely used algorithm.

- **Enhancing Privacy**
    - Data Minimization
        - A data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose.
    - Tokenization
        - A process by which a piece of sensitive data, such as a credit card number, is replaced by a surrogate value known as a token. The sensitive data still generally needs to be stored securely at one centralized location for subsequent reference and requires strong protections around it.
    - Data Masking****
    - Deidentification
        - Any process of removing the association between a set of identifying data and the data subject.
    - Anonymization
        - A de-identification technique that involves the complete and irreversible removal of any information from a dataset that could lead to an individual being identified.
    - Pseudo-Anonymization
        - The process of removing personal identifiers from data and replacing those identifiers with placeholder values.
    - Obfuscation
        - Creating source or machine code that is difficult for humans or computers to understand.
    - Steganography
        - Representing information within another message or physical object, in such a manner that the presence of the information is not evident to human inspection.
        - *Security through Obscurity.* Not innately secure, but harder to see.

- **Web Server Hardening**
    - Review MITRE's CVE list and National Vulnerability Database (NVD)
    - Change all default usernames and passwords.
    - Use a *Defense-in-Depth* or *layered security* posture.
    - Redundancy: Remove Single Points of Failure and create Fault Tolerance
    - Add banner info and disable directory browsing.
    - Permissions: Run from a non-privileged account and configure file permissions
    - Configure SSL to manage and install certificates.
    - Manage Log files: Monitor access and error logs.

Wireless Security

- **Types of Connectivity**
    - Point-to-Point (PtP)

        - Used to connect two locations together using directional antennas with LoS (Line of Sight). They use a combination of small, powerful, highly directional aerials, routers, and cables to set up the connection.
    - Point-to-Multi-Point
        - A one-to-many connection, providing multiple paths from a single location to multiple locations.
    - Cellular
        - Where the link to and from end nodes is wireless and the network is distributed over land areas called cells, each served by at least one fixed-location transceiver.
    - Hotspot/ Tethering
        - With tethering, you can use your existing mobile phone and data plan to share a secure internet connection with another device, typically a laptop or tablet. With true hotspots, you have access to a dedicated device, like a portable Wi-Fi hotspot, that's capable of connecting to the closest cellular tower.
            - Mobile LAN
            - Bluetooth
            - Wired device, such as USB.
    - Ad Hoc Mode/ Mobile Direct
        - When two wireless devices communicate in a peer-to-peer (P2P) manner without using APs or wireless routers. For example, a client workstation with wireless capability can be configured in ad hoc mode enabling another device to connect to it.
    - Near Field Communication (NFC)
        - A set of communication protocols that enables communication between two electronic devices over a distance of 4 cm or less. It is best known as the technology that lets consumers pay retailers and each other with their cell phones.

- **Wireless Authentication/ Authorization**
    - Captive Portals
        - Web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources.
    - Captchas
        - A type of challenge–response test used in computing to determine whether the user is human in order to deter bot attacks and spam.
    - Wi-Fi Protected Setup (WPS)
        - A feature supplied with many routers. It is designed to make the process of connecting to a secure wireless network from a computer or other device easier. Some manufactures may use the following terms instead of WPS (Push Button) to describe this function.

- **Wireless Encryption/ Authentication**
    - Wired Equivalent Privacy (WEP)
        - Wired Equivalent Privacy was a severely flawed security algorithm for 802.11 wireless networks.
    - Temporal Key Integrity Protocol (TKIP)
        - A security protocol used in the IEEE 802.11 wireless networking standard. It was designed to provide more secure encryption than the earlier Wired Equivalent Privacy (WEP), without needing to replace existing hardware.
    - Wi-Fi Protected Access (WPA)
        - WPA:

        - A security standard for computing devices equipped with wireless internet connections. WPA was developed by the Wi-Fi Alliance to provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP), the original Wi-Fi security standard.
    - WPA2
        - WPA2 replaces RC4 and TKIP with two stronger encryption and authentication mechanisms: Advanced Encryption Standard (AES), an encryption mechanism; and. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an authentication mechanism.
    - WPA3
        - Offers individualized data encryption for each device connected to the network, even in open Wi-Fi networks. This means that each device has its own encryption key, enhancing privacy and security. In WPA2, all devices connected to the same network share the same encryption key.
            - WEP and WPA are deprecated.
            - Use WPA2 or WPA3.
            - WPA3 is the best choice for encryption/ authentication of wireless networks.

- **Enhancing Wireless Security**
    - Disable SSID broadcasting.
    - Change default SSID and password.
    - Disable Wi-Fi Protected Setup (WPS). Easy to hack.
    - Use WPA 3 (Wi-Fi Protected Access 3)
        - WEP and WPA, are deprecated.

Cloud Security

- **Enhancing Cloud Security**
    - Separate Availability Zones (AZ)
        - Duplicate data and store backups in different geographic locations
        - Hot site for disaster recovery
    - Build apps to be highly available.
        - Use load balancers to provide high availability.
    - Secrets Management
        - API keys, passwords, and certificates
    - Identity and Access Management (IAM)
        - Put users into groups based on job function.
    - Assign user groups and permissions.
    - Cloud-Based Security Information and Event Manager (SIEM)
    - Block public access
    - VPN for cloud access
    - Configure Cloud-Based Virtualized Networks

- **Encrypting Data in the Cloud**
    - Server-Side Encryption
        - The encryption of data at its destination by the application or service that receives it.
    - Client-Side Encryption

        - Encrypting data on the sender's side before it is transmitted to a server such as a cloud storage service.
    - Encryption Key Management
        - The administration of policies and procedures for protecting, storing, organizing, and distributing encryption keys.

- **Security Technologies for the Cloud**
    - Web Application Firewall (WAF)/ Application Layer Firewalls
        - A specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service.
            - Allow or deny traffic based on input into that application.
            - Deep Packet Inspection: A type of data processing that inspects in detail the data being sent over a computer network, and may take actions such as alerting, blocking, re-routing, or logging it.
    - Next-Gen Firewall (NGFW)
        - Also called: Application Layer Gateway, Stateful Multilayer Inspection, or Deep Packet Inspection
            - Deep Packet Inspection: A type of data processing that inspects in detail the data being sent over a computer network, and may take actions such as alerting, blocking, re-routing, or logging it.
        - Can contain Intrusion Prevention Systems (IPS) and Content Filtering.
    - Intrusion Prevention System (IPS)
        - In-Line Monitoring
            - All traffic must flow through the appliance.
        - In-Band Response
            - Can monitor and block traffic on the spot.
            - Can examine traffic for signatures, anomalies compared to the baseline, behaviors, or heuristics (machine learning).
    - Remote Browser Isolation (RBI)
        - A web security technology that neutralizes online threats by hosting users' web browsing sessions on a remote server instead of the user's endpoint device.
        - RBI separates web content from the user's device to reduce its attack surface.
    - Next-Gen Secure Web Gateway (NG-SWG)
        - A new cloud-native solution for protecting enterprises from the growing volume of sophisticated cloud enabled threats and data risks.
        - It is the logical evolution of the traditional secure web gateway, also known as a web proxy or web filter.
    - Cloud Access Security Broker (CASB)
        - On-premises or cloud-based software that sits between cloud service users and cloud applications and monitors all activity and enforces security policies.
    - Identity Provider (IdP)
        - An Identity as a Service (IDaaS) solution that centrally manages users and groups. You can configure Cloud Identity to federate identities between Google and other identity providers, such as Active Directory and Azure Active Directory.

Virtualization Security

- **Containers/ Sandboxes**

- Can be used as a test environment for code execution, patches, updates, rollback planning or quarantining or segmentation during incident response.
- Reverse Engineering malware
  - Compiler
    - Source code to binary for computer readable format
  - De-Compiler
    - Binary back to source code

- **Thin/ Thick Clients**
  - Thin clients
    - Rely on a network connection for computing and don't do much processing on hardware.
  - Thick clients
    - Don't need a constant network connection and do much of the processing for client/server applications.

- **Virtual Desktop Infrastructure (VDI)/ Virtual Mobile Infrastructure (VMI)**
  - Apps and data are managed and stored externally from the device (cloud)
  - Minimizes risk from device loss.

- **VM Security Issues**
  - Avoid VM Sprawl
  - Protect against VM Escape Attacks

Mobile Security

- **Mobile Networks**
  - Point-to-Point (PtP)
    - Used to connect two locations together using directional antennas with LoS (Line of Sight). They use a combination of small, powerful, highly directional aerials, routers, and cables to set up the connection.
  - Point-to-Multi-Point
    - A one-to-many connection, providing multiple paths from a single location to multiple locations.
  - Cellular
    - Where the link to and from end nodes is wireless and the network is distributed over land areas called cells, each served by at least one fixed-location transceiver.

- **Mobile Device Enforcement**
  - Carrier Locking/ Unlocking
    - In the locked state, only the SIM card of a specified carrier can work, and other carriers are illegal for the device. In the unlocked state, the device has no restrictions on the carrier and the SIM card of any carrier can work.
  - Jailbreaking/ Rooting:
    - Jailbreaking refers to iPhones in particular. It means getting around Apple software restrictions so you can manage your phone at an administrator level. Rooting refers to achieving the same results on an Android.

- **Mobile Security Enhancements**

- Screen Locks
  - Always Auto-Lock mobile devices
  - Biometrics
  - Multi-Factor Authentication
- SEAndroid
  - Security enhancements for Android
- MicroSD HSM
  - Provides security services for mobile devices.
    - Encryption
    - Key generation
    - Digital Signatures
    - Authentication
    - Secure storage
- Mobile Application Management (MAM)
  - Provisions, updates, and removes apps.
  - Keeps all devices running on the correct and current app version.
- Unified Endpoint Management (UEM)
  - Manage mobile and non-mobile devices.
  - An evolution of the Mobile Device Manager (MDM)
- Virtual Desktop Infrastructure (VDI)/ Virtual Mobile Infrastructure (VMI)
  - Apps and data are managed and stored externally from the device (cloud).
  - Minimizes risk from device loss.
  - Managed from a single platform, like remote desktop.
  - Works best for Android devices.

- **Mobile Device Manager (MDM)**
  - Centralized management program for mobile devices.
    - Implement screen locks and pins.
    - Keeps firmware and OS updated and patched.
    - Geolocation/ Geofencing
      - A virtual perimeter for a real-world geographic area.
      - Can disable or reenable camera, microphone, recording devices, or other apps depending on location.
      - Helps with DLP.
    - Can disable location and prevent geotagging data from being saved.
    - Remotely control device/ Remote wipe
    - Screen Lockout: Too many failed attempts at logging in
    - Allow or disallow the use of biometrics for authentication.
    - Manage context-based authentication.
    - Disable or allow push-notifications.
    - Can enable or disable SMS features.
    - Can disable the ability to plug in or read external storage devices, such as flash drives, SD cards, USBs or USB-OTG (On-the-Go) or other storage devices.
    - Manage containerization and remote wipe corporate data from the mobile container.
    - Set policies on apps, data, camera usage etc.
      - Application Management
        - Installation of only approved apps
      - Mobile Content Management (MCM) program
        - Monitor and manage file sharing and viewing on mobile devices.

- Monitor/ prevent data sent or downloaded from devices.
  - Data Loss Prevention (DLP)
  - Can force full disk encryption.

IoT Security

- **IoT Technology Types**
  - Near Field Communication (NFC)
    - A set of communication protocols that enables communication between two electronic devices over a distance of 4 cm or less.
  - Radio Frequency Identification (RFID)
    - Uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter.
  - Bluetooth
    - Used for exchanging data between fixed and mobile devices over short distances (up to 10 meters) and building personal area networks.
  - Infrared (IR)
    - A wireless mobile technology used for device communication over short ranges. IR communication has major limitations because it requires line-of-sight, has a short transmission range and is unable to penetrate walls.
  - Zigbee
    - A wireless protocol that is used to allow Smart Devices such as light bulbs, sockets, plugs, smart locks, and motion sensors.
  - Z-wave
    - Used primarily for residential and commercial building automation.

- **Fog/Edge Computing Devices**
  - Fog Devices
    - IoT devices with limited access to internet.
  - Edge Devices
    - IoT devices that only make local decisions.

- **Enhancing IoT Security**
  - Change all default usernames and passwords.
  - Require Access Control Management
  - Require segmentation.

- **Lightweight Cryptography**
  - Field of study in the pursuit of developing more powerful tools and algorithms that use computer power and resources.

Embedded Systems Security

- **Embedded System Technology**
  - A combination of a computer processor, computer memory, and input/output peripheral devices that has a dedicated function within a larger mechanical or electronic system.
    - Raspberry Pi

            - A debit card-sized low-cost computer that connects to a computer Desktop or TV and uses a standard mouse and Keyboard. It has a dedicated processor, memory, and a graphics driver, just like a PC. It also comes with its operating system, Raspberry Pi OS, a modified version of Linux.
        - Arduino
            - A low-cost, flexible, and easy-to-use programmable open-source microcontroller board that can be integrated into a variety of electronic projects.
    - Smart TVs, Appliances, Thermostats, Printers etc.
        - Require segmentation.
        - Require Identity and Access Control Management

Application Security

- **DevOps/ DevSecOps**
    - DevOps: Primarily focused on increasing the speed and quality of software development and delivery.
    - DevSecOps: Aims to secure the software development process by integrating security early and throughout the software development life cycle. Developers and operations teams work together.

- **Quality Assurance (QA)**
    - Dynamic Analysis (Fuzzing)
        - Also called Fault Injection, Robustness Testing, Syntax Testing or Negative Testing, used to test for code injection errors and exploits.
    - Input Validation
        - The process of testing input received by the application for compliance against a standard defined within the application. It can be as simple as strictly typing a parameter and as complex as using expressions or business logic to validate input.
    - Escaping
        - Involves adding a special character before the character/string to avoid it being misinterpreted. For example, adding a \ character before a " (double quote) character so that it is interpreted as text and not as closing a string.
    - Static Application Security Testing (SAST)
        - Static code analyzer helps to identify security flaws.
    - Code Signing
        - Developer's must sign their new code.

- **Web Application Firewalls (WAF)/ Application Layer Firewalls**
    - A specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. Allow or deny traffic based on input into that application.

- **Securing Browsers**
    - Secure Cookies
    - HTTPS (Secure Headers)
    - Allow Lists and Deny lists (the OS allows or disallows certain applications to run)

- **Application Server Hardening**
    - Review MITRE's CVE list and National Vulnerability Database (NVD)

- Passwords should be stored on a server, not on the application itself.
- Redundancy: Remove *single points of failure* and create *fault tolerance*
- Use a *Defense-in-Depth* or *layered security* posture.
- Disable all unnecessary services.
- Security patches for application OS
- File permissions and access controls
- Manage Service Accounts and their permissions: A web server's permissions to access data and interact with the application, for example.

Detecting Network Attacks

- **Indicators of Compromise (IoC)**
  - Bandwidth consumption
  - Beaconing
  - Unexpected traffic according to current Baseline
  - Memory and drive capacity consumption
  - Abnormal system and process behavior
  - Scans and probes
    - Sequentially testing ports
    - Connecting to many addresses in a network
    - Repeated requests to inactive ports/ services
  - Denial of Service
  - Monitor for changes in permissions, registry, scheduled tasks, or privileges.
  - Watch for netcat!

Common Vulnerabilities and Their Mitigations

Common Vulnerabilities	Mitigations
Missing Patches	Patch
Unsupported Operating Systems/ Applications	Update to a newer version, or where not feasible, isolate and implement compensating control
Buffer Overflow Attacks	Patch
Privilege Escalation Attacks/ Rootkits	Patch, IAM and Active Directory, to ensure proper privileges and groups. To detect, monitor logs for unauthorized event and process changes
Arbitrary and Remote Code Execution-	Patch
Insecure Protocols: FPT, telnet, SSL, and http	Use encrypted protocols like SSH and newer versions that use encryption, or better encryption, like FTPS.
Visible Debug Modes for developer troubleshooting	Developers must ensure that debug modes can only be used by authenticated users on internal servers.
Missing Firmware Updates	Patch
SSL and outdated TLS use	Use a newer version of TSL to avoid susceptibility to eavesdropping attacks.
Unsecure or outdated cipher	Avoid outdated ciphers like RC4 and only use secure ciphers like AES
Certificate issues, expiration of certificate, or unknown certificate authority	Get a new certificate.
DNS attacks used in DDoS attacks	Stateful firewall can inspect entire conversations, and block large influx of packets when there is no record of initialized convo

Configuration issues that lead to IP address exposure, such as listing the address in the header of a reply to an HTTP address	Configure NAT correctly
VPN issues such as out of date or using less secure encryption ciphers	Patch and update
SQL Injection	Work with developers to fix the code- require input validation (block the use of an apostrophe) and least privilege (blocks the tables that can be accessed by a web server).
XSS	Input validation and working with developers to implement appropriate controls.
Directory traversal/ ability to navigate a directory or file path to get to a file otherwise not accessible.	Three controls developers can implement are: input validity, block file names from being used in user-manipulatable fields, and access controls on servers
Password Spraying/ Password Stuffing	Multifactor authentication, strong passwords, and avoiding reuse.
Session Hijacking	Encrypted network sessions and links
DoS and DDOS	Firewalls and IPS to block known attack traffic, purchase more bandwidth or server capacity, purchase a third-party DoS mitigation service- but shutting down, isolating, or creating too strict of firewall rules would result in denial of service as well.
MITM/ Eavesdropping	End to end encryption can prevent this, unless the attacker controls the endpoints, or have the encryption key.
Phishing	Employee training, two-factor authentication, email filtering, and reputation-based sender rules
Flash Drive Drop/ Malicious USB Cable	User Awareness Training, DLP, and USB Blockers
Malicious insiders	Employee Training, strong account policies, job rotation, mandatory vacation
SPIM attack- Spam over instant messaging	User Awareness Training