

Security Controls
Security+ 701 Study Guide
By: Krystal Ballew

Data Center Security

- **Physical Controls**

- **Perimeter Security:** Deter or prevent a perimeter breach at the physical site of a network or data center.
 - **Fencing/Electrical Fencing/Razor Wire:** Deter and prevent a perimeter breach. Fencing may have sensors, and/or contain electrical current.
 - **Bollards:** Cement architectural obstacles that prevent vehicle entry and direct the flow of traffic. Large cement planters outside of buildings are often disguised *bollards*.
 - **Good Lighting:** Avoid shadow and glare. Deter casual and opportunistic adversaries.
 - **One-Way Glass:** Highly reflective. See out, without allowing others to see in.
 - **CCTV Cameras:** Deter unauthorized entry, keep a digital record of access, and identify adversaries.
 - **Visible Signage:** Used to deter unauthorized access, control foot traffic, and for human safety.
 - **Drones:** Easily monitor large areas, assess damage, or conduct *Site Surveys*.
 - **Crime Prevention Through Environmental Design (CPTED):** Directing the flow of people through passive techniques, such as water features or architectural obstacles.
 - **Industrial Camouflage:** Blend into the environment. No visible signs. *"Security Through Obscurity."*
 - **Air Gap:** A network where the devices are physically separate from one another and don't share any components to communicate. Physical space between facilities, server rooms, and networks. Great for security but must be mindful of removable media.
 - **Alarms and Sensors:** On doors, windows, gates, and turnstiles. Strain-sensitive cables or other vibration sensors can detect if someone attempts to scale a fence.
 - **Object Detection:** Can detect missing objects, foreign objects and human/animal targets. May include facial recognition.
 - **Motion Detectors:** Detect unexpected access or physical presence in a restricted area.
 - **Noise Detectors:** An electronic device that measures sound levels or noise signals.
 - **Pressure Sensors:** Measures the force of pressure on a surface and converts the information into an electrical signal. The signal is used to monitor or regulate the pressure of a space.
 - **Environmental Temperature Sensors:** Monitor and detect unusual heat, cold, and humidity.
 - *Heating, Ventilation, Air Flow, and Cooling (HVAC).*
 - Moisture Detection and Humidity Control.
 - *Hot and Cold Isles* in data centers and server rooms.
 - **Fire Suppression and Detection Systems:** *Dupont FM-200.*
 - **Fire Extinguisher Classes**

Class A	Most flammable solids, such as paper, cloth, wood, or plastic. Class A extinguishers typically use pressurized water or multipurpose dry chemical.
Class B	Flammable liquids, such as oils, solvents, or gasoline. Class B extinguishers typically use CO ₂ or dry chemical mixes and work by depriving the fire of oxygen.
Class C	Fires involving active electrical current, either in electrical equipment or other materials in contact with exposed wiring. Class C extinguishers generally use CO ₂ or dry chemicals.
Class D	Combustible metals such as magnesium or sodium. Such metal fires can use water or CO ₂ as an oxidizer just like oxygen, so they must be put out using specialized dry powder extinguishers.
Class K	Cooking oils and fats. Functionally, Class K extinguishers are more or less the same as Class B but are specialized for kitchen use.

- **Door, Entryway and Window Access:** First line of defense, access control and perimeter security.
 - **Sealed and Locked Doors and Windows:** Use deadbolts, locks and keys.
 - **PINs, Passwords, Passphrases:** *Something You Know.*
 - **Employee ID Badges, Proximity Cards, Key Cards, and Key Fobs:** *Something You Have.*
 - **Biometrics:** *Something You Are.*
 - **Access Control Vestibule/Mantrap/Airlock:** Prevents *Piggybacking* and *Tailgating*.
- **Security Guards:** A physical deterrent and sometimes *preventative* security measure.
 - **Access Lists and Physical Visitor Log:** Logical or physical access lists and records.
 - **Robot Sentries:** Replaces human guards with robots and drones.
 - **Guard Dogs:** A physical deterrent for most opportunistic and casual adversaries.
- **Vaults/ Safes:** Physical protection for the most valuable assets. Vulnerable to *insider threats*.
 - **Duress/ Panic Button:** Alert the authorities and seal specific doors, vaults or safes.

Network Security

• Physical Controls

- **Physical Redundancy and Backups:** Remove *single points of failure* and create *fault tolerance*.
 - **Power Distribution Units (PDU):** A power strip connected to ethernet for better control and monitoring of power usage across the network.
 - **Power Conditioner:** Improves the quality of power that is delivered to electrical equipment.
 - **Backup Power Supplies:** Provides *fault tolerance* in the event of an electrical outage. Useful for data center, operations, and network security.
 - **Backup Gas Powered-Generator:** Also known as a *natural gas generator*. A portable piece of equipment that converts fuel into electricity. Used for backups and in natural disasters.
 - **Dual Power Supplies:** Can be used as a backup power supply for mission-critical equipment.
 - **Uninterruptible Power Supply (UPS):** A type of continual power system that provides automated backup electric power when the input power source fails.
 - **Protected Distribution System (PDS):** Metal cable and fiber protectors that prevent cable and fiber taps or cuts. All data flows through physically secured conduits. Requires periodic visual inspection.
 - **Electromagnetic Shielding:** A method of using conductive or magnetic materials to create a barrier around electronics and cables to protect them from *Electromagnetic Frequencies (EMF)*.
 - **Electrostatic Discharge (ESD):** A sudden and momentary flow of electric current between two differently charged objects when brought close together.
 - **Electromagnetic Interference (EMI):** A disturbance generated by an external source that affects a circuit by *electromagnetic induction, electrostatic coupling, or conduction*.
 - **Radio Frequency Interference (RFI):** An electrical disturbance within the radio frequency spectrum.
 - **Electromagnetic Pulse (EMP):** Also called a *Transient Electromagnetic Disturbance (TED)*, it is a brief burst of electromagnetic energy or pulse.
 - **Anti-Static Wrist Strap:** Used when troubleshooting hardware, replacing parts, or taking apart a device, to provide *grounding*. This protects the technician from shock and preserves the components of the device, and data on them.
 - **Personal Protective Equipment (PPE):** Insulated clothing or rubber gloves to prevent shock.
 - **Faraday Cage:** Used in electronic labs, where stray EM fields must be kept out. This is important in the testing of sensitive wireless receiving equipment. Also good to prevent signals from being sent to mobile devices during a forensic investigation.
- **Physical Network Segmentation:** Minimizing the attack surface of a network through physical means such as port security and isolation. Making it more difficult for a successful attack of one component or computer to spread throughout the network.

- **Hardware and Vendor Diversity:** Choosing hardware and appliances from more than one vendor provides fewer *attack surfaces* and eliminates *single points of failure*.
- **Port Security:** Disable unused physical ports on network devices/appliances (especially *switches*).
- **Air Gap:** A security measure that involves isolating a computer or network and preventing it from establishing an external connection. A network where the devices are physically separate from one another and don't share any components to communicate. Also describes the physical space between facilities, server rooms, and networks.
- **System Isolation/ Containment:** A security measure taken in the event of attack, to prevent the spread of malware, or other malicious action. Involves physically disconnecting the system from the rest of the LAN, and disabling wired, and wireless connectivity.

- **Logical Controls**

- **Logical Network Segmentation:** Also known as *Virtual Network Segmentation*. Dividing a network into smaller, more manageable sections using software. This can be done through *subnetting*, *Virtual Local Area Networks (VLANs)*, or network addressing schemes.
 - **Security Zones:** Internal security topology based on *network segmentation* and *access control*. Different *zones* for different levels of trust and access control requirements.
 - **Micro-Segmentation:** A network security approach that constructs security zone boundaries per machine in data centers and cloud deployments, to segregate and secure workloads independently. Allows an organization to limit which business functions, units, offices, or departments can communicate with each other, and enforce the concept of *least privilege*.
 - **De-Perimeterization:** Focuses on protecting specific assets instead of network boundaries. Essential due to the prevalence of cloud, remote work, mobile devices, outsourcing, and wireless networks.
 - **Virtual Local Area Networks (VLANs):** Using *switches* to create software-based LAN segments, which can segregate or consolidate traffic across multiple switch ports. Devices that share a VLAN communicate through switches as if they were on the same *Layer 2* network. *Broadcast* traffic is limited to the VLAN, reducing congestion, and reducing the effectiveness of some attacks.
 - **Screened Subnet:** Previously called a *Demilitarized Zone (DMZ)* or *Perimeter Network*. Refers to the use of one or more routers as a firewalls to define three separate subnets: An external router, that separates the *external network* from a *perimeter network*, and an internal router that separates the *perimeter network* from the *internal network*. Acts as a neutral zone between an organization's internal network and the Internet. Separates public-facing servers from sensitive internal resources. Hosts web, E-mail, DNS or FTP services accessible from the Internet but isolated from internal systems to limit damage from breaches. Firewalls control traffic to and from the *Screen Subnet*, providing an additional layer of protection.
 - **Dual Firewalls (DMZ):** This implementation uses two firewalls to create a DMZ.
 - **Intranet:** Only available internally.
 - **Extranet:** Accessed by trusted business partners or others who need access to hosted data or services but who should not get access to the entire private network. It is commonly accessed through a VPN.
 - **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, creating segmentation.
 - **Jump Server:** Also called the *Jump Box* or *Secure Admin Workstation (SAW)*. A highly secured steppingstone from one zone to another. From a workstation in a corporate network, log into a *jump server*. Access the DMZ without directly exposing the workstation to the DMZ.
 - **Out-of-Band Management:** Ensure a separate network for administrative access. Enhances security by limiting direct access to administrative interfaces.
 - **Subnets:** A logical subdivision of an IP network. The practice of dividing a network into two or more networks is called *subnetting*.

- **Network Address Translation (NAT):** A logical measure to map multiple *private IP addresses* inside a local network to a single *public IP address* before transferring the information onto the Internet. Saves IPv4 address space.
- **Port Address Translation (PAT):** Similar to *Network Address Translation (NAT)*. It permits multiple devices on a LAN to be mapped to a single *public IP address* to save address space. Found on a router or virtual switch, primarily in SOHO networks.
- **Source Network Address Translation (SNAT):** Used when most traffic comes from internal systems, such as internal client workstations connecting to Internet servers. It helps security by making it harder for outside attackers to contact internal hosts, but it also makes it harder to run server applications.
- **Destination Network Address Translation (DNAT):** Used when traffic is generally initiated by external systems, such as intranet clients connecting to local servers. It requires pre-configured address assignments for internal servers.
- **Common Address Redundancy Protocol (CARP):** Allows multiple hosts on the same network segment to share an IP address.
- **Network Appliances (Hardware-Based)**
 - **Port Mirrors:** Copies network packets from one switch port to another switch port's network monitoring connection. It's also known as *Switched Port Analyzer (SPAN)* or *traffic mirroring*. Limited functionality but can work for light traffic.
 - **Network Taps:** A hardware device that performs *Port-Mirroring*. Sends a copy of network packets from one switch port (or an entire VLAN) to a network monitoring connection on another port.
 - **Sensors:** Monitors data in different locations on the network and sends that data to a central location (like a SIEM) for storage, viewing, and analysis. Can be hardware or software and can be a component of a different network appliance, such as a switch, firewall or router. Place on the inside of a firewall, or close to a critical server to detect malicious traffic.
 - **Collectors:** Hardware or software that receives, stores, and preprocesses network monitoring data, especially in the context of *NetFlow* analysis. Works with data from proprietary consoles, SIEM consoles, syslog servers, *Intrusion Prevention Systems (IPSs)*, and firewalls.
 - **Correlation Engines:** Compares and corresponds data collected from the sensors to determine if an attack is present. Often built into a SIEM.
 - **Wrappers:** A hardware, software, or network appliance that intercepts all communications meant for a legacy or deprecated device and handles security for it. Comparable to adding a complete Firewall/Antivirus/IDS solution to a system that cannot otherwise run them.
 - **Switches:** A hardware or virtual component that connects devices on a network, allowing them to communicate and share resources.
 - **Virtual Local Area Network (VLANs):** Switches can create software-based LAN segments, which can segregate or consolidate traffic across multiple *switch ports*. Devices that share a VLAN communicate as if they were on the same *Layer 2* network. *Broadcast* traffic is limited to the VLAN, reducing congestion, and reducing the effectiveness of some attacks. VLANs can be configured based on switch port, IP subnet, MAC address, and protocols. VLAN IDs (2- 4,094) are assigned, enabling different ports on the same switch to belong to different VLANs. Routers are required for VLANs to communicate
 - **Security Concerns**
 - **Collision Domains:** Data *collisions* may occur.
 - **Broadcast Domains:** All *broadcasts* are forwarded.
 - **VLAN Hopping:** Attacks where a host on one VLAN can gain access to traffic in another, that would normally not be accessible.
 - **Security Features**
 - **ARP Inspection:** A security feature for *Address Resolution Protocol (ARP)*. Checks all ARP packets on untrusted interfaces and compares them to 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*.
 - **STP States**
 - **Blocking:** Preventing a *loop*.
 - **Listening:** STP determines whether the port should participate in frame forwarding or not.
 - **Learning:** Learns MAC addresses before entering a *forwarding* state.
 - **Forwarding:** The interface will forward Ethernet frames, enabling data transmission.
 - **Loop Protection/ Loop Guard:** Prevents loops from forming on unmanaged switches.
 - **Bridge Protocol Data Unit (BPDU) Guard:** Disables ports if unwarranted BPDUs are sent.
 - **Root Guard:** A port cannot be selected as the *root port*. It is assigned an *alternate port* role and enters a *blocking state*.
- **Port Security:** Tracks device MAC addresses connected to each port on a switch and can allow or deny traffic based on MAC address. Can prevent unauthorized devices from joining the network, or block attacks that rely on *MAC spoofing*.
- **MAC Filtering:** Prevents physical connections from neighboring MAC addresses. *Security Through Obscurity*.
- **DHCP Snooping:** Excludes rogue DHCP servers and blocks malicious or malformed DHCP traffic.
- **Broadcast Storm Control:** The switch intentionally stops *broadcast* traffic if the bandwidth consumed exceeds a designated threshold.
- **Flood Guard:** Limits the devices that can communicate through a switch interface. Protects against *Denial of Service (DoS)* and *SYN Flood* attacks.
- **MACsec Encryption:** A security protocol that guards against network data breaches by encrypting traffic between Ethernet-connected devices.
- **Routers:** A device that connects networks and allows devices to share an Internet connection. Usually connected to a modem and acts as a central *hub*, directing data packets to their intended destinations. Can also provide network security features and allow wireless setup.
 - **MAC Address Filtering:** Block, allow, or filter traffic through the router based on the hardware MAC address of the device.
 - **Access Control Lists (ACLs):** Protect against *spoofing* by blocking *Martian Packets* with unusual source addresses and/or packets arriving on invalid interfaces.
- **Firewalls:** Hardware or software devices. Rules 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 (ACLs):** Firewalls are based on an *implicit deny* rule and must specify which traffic should be *allowed*. Rules are processed top to bottom with the most specific rule first. *Implicit deny* is the default rule, often listed at the bottom, even if not specified.
 - **Whitelists/ Blacklists:** *Allow List/ Block List*. Can explicitly block or allow a range of IP addresses on the network. Any rules listed will create a log.
 - **Firewall-Based Content Filter:** Controlling the Internet content users can access.
 - **Port Filtering:** A feature in which packets that are *ingressed* through a certain source port can be blocked from *egressing* on a specific set of ports.
 - Block all unnecessary *Ports* and *Protocols*.
 - Use *Private Ports* where possible.
 - Use secure versions of *Protocols*.
 - Block Port 23 for *Telnet*.

- **Dynamic Packet Filtering:** A *Screen* that sits between the client and a server, that examines each data packet as it arrives. Based on information in the packet, the state retained from previous events, and security policy rules, the *Screen* will either pass the data packet forward, or block and drop it.
- **North/South Traffic:** Network traffic flowing into (South) and out of (North) a data center.
 - **Ingress:** Refers to traffic that originates from outside a network. Devices and tools that offer logging and alerting opportunities for *Ingress Monitoring* are:
 - *Firewalls.*
 - *Gateways.*
 - *Remote Authentication Servers.*
 - *IDS/IPS Tools.*
 - *SIEM Solutions.*
 - *Anti-Malware Solutions.*
 - **Egress:** Data shared externally via a network's *outbound* traffic. *Egress Monitoring* is used in conjunction with *Data Loss Prevention (DLP)* and *Data Leak Protection*. These solutions inspect all data leaving the organization, including E-mail contents and attachments, copy to portable media, *File Transfer Protocol (FTP)*, posting to web pages/websites, applications, and *Application Programming Interfaces (APIs)*.
- **East/West Traffic:** Network traffic among devices within a specific data center. Requires a different *security posture* than *North/South* traffic.

- **Firewall Types**

- **Stateless Firewalls:** Older and does not keep track of traffic flows. Needs more rules because it doesn't remember active sessions.
 - **Packet Filtering Firewall:** The earliest network firewall configured using ACL rules. It is *Stateless* in that it does not preserve information about network sessions. Each packet is analyzed independently. Vulnerable to attacks spread over multiple packets. Can introduce traffic flow problems, especially with *load balancing* or *dynamically assigned ports*. Considered deprecated.
 - **Transparent Firewall Mode:** The firewall acts as an L2 device, not an L3.
- **Stateful Firewalls:** Tracks information about established sessions between hosts. Incorporates *stateful inspection* capabilities by storing session data in a *state table*. Checks incoming packets against existing connections in the state table. Once a connection is allowed, traffic usually passes unmonitored to conserve processing effort. Remembers sessions and traffic flows and needs fewer rules.
 - **Layer 3 Firewall:** A type of firewall that operates on Layer 3 of the *Open Systems Interconnection (OSI) model*.
 - **Routed Firewall Mode:** Considered a L3 device. It supports multiple interfaces with each interface on a different *subnet*. It can perform *Network Address Translation (NAT)* between connected networks.
 - **Layer 4 Firewall:** Examines the *TCP 3-Way Handshake* to distinguish new connections from established connections. Can track UDP traffic and detect IP headers and ICMP anomalies, such as a SYN without an ACK.
 - **Layer 7 Firewall/Web Application Firewalls (WAF):** Also known as an *Application Layer Firewall*, an *Application-Aware Firewall* or *Deep Packet Inspection*. A specific firewall that filters, monitors, and blocks HTTP traffic to and from a web service. Verifies that the application protocol matches the expected port. External traffic is filtered by a traditional or *Next Generation Firewall (NGFW)* first. Designed to protect web servers and back-end databases from *Code Injection* and *Denial of Service (DoS)* attacks. Can apply rules to API communication to help prevent *API injection*. Can be deployed as an appliance or plug-in software.

- **Next-Generation Firewall (NGFW):** Also called *Application Layer Gateway*, *Stateful Multilayer Inspection*, or *Deep Packet Inspection*. Third-generation firewall technology, combining a conventional firewall with other network device filtering functions. Can contain *Intrusion Detection System (IDS)*, *Intrusion Prevention Systems (IPS)*, *Content Filtering*, *Web Proxy*, *Anti-Bot*, *Anti-Malware*, *Virtual Private Network (VPN)*, and *Identity and Access Management (IAM)* functionality.
 - **Deep Packet Inspection:** A type of data processing that inspects the data being sent over a computer network in detail, and may take actions such as *alerting*, *blocking*, *re-routing*, or simply *logging* it.
- **Other Firewall Deployments**
 - **Zero Trust:** By default, no one is trusted from inside or outside the network. Verification is required from everyone trying to gain access to resources. This added layer of security has been shown to prevent *data breaches*.
 - **Virtual Wire Firewall:** A firewall that is transparently installed on a network segment by binding two firewall interfaces together. Can be *stateless* or *stateful*.
 - **Three-Homed Firewall:** A network architecture where a single firewall is used with three network interfaces, creating network segmentation.
 - **Dual Firewalls (DMZ):** This implementation uses two firewalls to create a DMZ. The first firewall, called the *Front-End Firewall*, must be configured to allow traffic destined for the DMZ only. The second firewall, called a *Back-End Firewall*, only allows traffic from the DMZ to the internal network.
- **Network Intrusion Detection Systems (NIDS):** Monitors and evaluates network activity to detect attacks or event anomalies. A single NIDS can monitor large networks by using remote sensors to collect data at key locations, which send data to a central management console. These sensors can monitor traffic at routers, firewalls, and switches that support *port mirroring*. NIDSs can detect the initiation of an attack or ongoing attacks, but they can't provide information about the success or effects of an attack, nor can they monitor the content of encrypted traffic.
 - **Passive Monitoring:** Examines a copy of traffic via a *port mirror* or *network tap*.
 - **Out-of-Band Response:** IDS sends RESET frames to stop subsequent frames but cannot block the first frame.
 - **Stateful Protocol Analysis:** Methods that use *Deep Packet Inspection (DPI)* to examine traffic by comparing a *profile* of how the protocol is supposed to work. Can detect many attacks *signature-based* methods won't, but it's only as good as the profiles it uses and doesn't work well with poorly documented proprietary protocols.
 - **Signature-Based:** Methods that look for behavior characteristics of known attacks. A signature list might include a specific malformed packet used by a *Telnet* attempt into a *root* account. *Signature-based* methods are excellent at stopping known attacks, but they'll miss anything that's not on the list.
 - **Anomaly-Based:** *Heuristic* methods that look for behavior that seems unusual relative to a normal *baseline*. Heuristic detection rules are challenging to design and rely on a large set of baseline data to be accurate. Their main advantage is the ability to identify dangerous *zero-day attacks* against undetected vulnerabilities.
- **Network Intrusion Prevention Systems (NIPS):** Automatically detects and blocks attacks before they reach target systems. All traffic must pass through the NIPS. Rules are based on *implicit allow* and must specify which traffic to block. It is common to see NIPS function integrated into firewalls.
 - **In-Line Monitoring:** All traffic must flow through the appliance.
 - **In-Band Response:** Can monitor and block traffic on the spot.
 - **Stateful Protocol Analysis:** Methods that use *Deep Packet Inspection (DPI)* to examine traffic by comparison to a *profile* of how its protocol is supposed to work.

- **Signature-Based:** Methods that look for behavior characteristics of known attacks.
- **Anomaly-Based:** Heuristic methods that look for unusual behavior relative to a *baseline*.
- **Network Detection and Response (NDR) Solutions:** Also called *Network Traffic Analysis (NTA)*, or *Network Analysis and Visibility (NAV)*. Analyzes *behavioral heuristics*. Uses *machine learning* and *data analytics* to compare *baselines* and *known good behavior* to anomalous behavior. Unusual behaviors generate a report or alert.
- **Proxy Servers:** Sits between users and the external network. Receives the user's request and sends the request on their behalf. Also receives the response, evaluates the response, and sends the result back to the user. Can control much of the traffic flow. Performs *Application Layer* filtering, deconstructs packets, performs analysis, and rebuilds packets according to rules.
 - **Forward Proxy:** An internal proxy, used to control internal access to the Internet.
 - **Reverse Proxy:** Protects inbound traffic from the Internet to the internal servers.
 - **Transparent Proxy:** Operates like a *Forward Proxy* but doesn't require any special client configuration. Commonly used on large enterprise networks. Sometimes called a *Forced Proxy* because the client doesn't choose whether to use them.
 - **Application Proxy:** Receives requests intended for another server and acts as the proxy to obtain the requested service. An application proxy server is often used when the client and the server are incompatible for direct communication.
 - **Anonymous Proxy:** Usually hosted on the Internet and masks the client's original IP address from the server. Security concern.
 - **Open Proxy:** Uncontrolled and available to anyone. Can circumvent security protocols.
 - **Jump Server:** Also called the *Jump Box* or *Secure Admin Workstation (SAW)*. A highly secure steppingstone from one zone to another.
 - **Content Distribution Networks (CDNs):** Geographically distributed network of proxy servers and their data centers. Provides *High Availability (HA)* and performance by distributing the service relative to end user. Can come with *Distributed Denial of Service (DDoS)* mitigation.
- **Load Balancers:** Distribute a set of tasks over a set of resources, to streamline processing. Can optimize response time and avoid unevenly overloading some compute nodes, while other compute nodes are left idle. Also increases hardware *redundancy* and *data availability*. *Load Balancers* use *heartbeat* or *health check* probes to verify the availability and the load of each node.
 - **Active/Active:** All redundant servers are always available and sharing the load. If one fails, its workload is distributed to the remaining nodes. Most *load balancers* are active/active. This utilizes maximum capacity but may degrade performance during a *failover*.
 - **Active/Passive:** In addition to any *active* nodes, there are one or more *failover* nodes that are left on *standby*. When a node fails, a new node becomes immediately activated. Ensures no performance impact during failover.
 - **Load Testing:** Validates system performance under expected or peak loads.
 - **Failover Testing:** Validate easy transition between primary and secondary infrastructure.
 - **Monitoring System Testing:** Validates effective detection and response to failures/issues.
 - **Load Balancing Modes:** A method of distributing network traffic or workloads across multiple resources, to reduce the strain on each resource and improve performance.

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 is assigned based on the server's current load and idle capacity.
Active Balancing	Divides workload among multiple nodes based on availability.
Source Affinity/ Sticky Session/ Session Persistence	Directs all requests from a particular end user to a specific server, which preserves data that might otherwise be lost.

- **Types of Load Balancers**
 - **Layer 4 Load Balancer:** Makes forwarding decisions based on IP address and TCP/UDP ports. They also conduct basic connectivity tests and health checks.
 - **Layer 7 Load Balancer/ Content Switch:** A higher layer router that uses *Network Address Translation (NAT)* to split server requests between multiple identical servers that share a single *virtual IP address*. Used to direct requests for specific types of content to targeted servers by way of *load-balancing* virtual servers. Makes forwarding decisions based on *Application-Level* data such as URLs or data types like video or audio streaming. Can test an application state when doing a health check.
- **Clustering:** *Load Balancing* distributes traffic, while *Clustering* provides *fault tolerance* by enabling multiple redundant nodes to share data and accept connections. Clustering ensures continuity of service by allowing connections to fail over to working nodes.
- **AAA Servers:** Controls access to resources, enforces policies, and audits usage. **Identification** creates unique user IDs. **Authentication** proves that the user is who they claim to be. **Authorization** proves that the user is allowed access the resource. **Accounting** includes logging and audit methods.
 - **Remote Authentication Dial-In User Service (RADIUS):** Authentication and authorization. Members of one organization can authenticate to the network of another organization using their normal credentials. Only encrypts the passwords. Centralized authentication for users logging in to routers, switches, firewalls, VPNs, servers, and 802.1x. Works well with *VPN Concentrators*. Available for any server operating system. The client is a *Network Access Server (NAS)*, which prompts a user for credentials and then relays user (*supplicant*) authentication requests to the RADIUS server, which responds with an acceptance or rejection. Uses UDP, over ports 1812 (*Authentication* and *Authorization*) and 1813 (*Accounting*). Supports protocols like PAP, CHAP, and EAP for authentication. Not as versatile as LDAP for authorization.
 - **DIAMETER:** Next-generation industry-standard protocol used to exchange *Authentication, Authorization, and Accounting (AAA)* information in *Long-Term Evolution (LTE)* and *IP Multi-Media Systems (IMS)* networks. An evolution of RADIUS.
 - **Terminal Access Controller Access-Control System (TACACS):** A family of protocols that provides remote authentication in a server environment. Each server on the network submits individual authentication requests to the centralized server, even though there's a common authentication database. Now considered obsolete, with the advent of TACACS+.
 - **TACACS+:** More recent version. Supports more authentication requests and response codes. Encrypts entire access request. Centralized logins for administrative accounts on network appliances. It offers advantages such as TCP-based communication, encryption of all data, and discrete *Authentication, Authorization, and Accounting* functions. No SSO functionality.
 - **XTACACS (Extended TACACS):** CISCO proprietary tool that has additional support for *Accounting* and *Auditing*. Now obsolete.
 - **Kerberos:** Authentication through a cryptographic *ticket-granting* service. Allows for *Single Sign-On (SSO)*. Authenticate once, and the device is trusted by the system. Users can gain access to multiple resources with one authentication. Still requires individual servers to maintain the access databases. Works well in Microsoft environments.
 - **Authentication Service/ Server (AS):** Users log in to initiate the authentication process. The AS directs the login process through multiple Kerberos servers.
 - **Key Distribution Center (KDC):** The AS passes the login request to the KDC, which issues the user a *Ticket-Granting Ticket (TGT)*. The TGT has a timestamp and time limit. The KDC encrypts the ticket to make it harder to duplicate or impersonate.
 - **Ticket Granting Service (TGS):** After the KDC issues the user ticket, the user can log on to any network server that supports Kerberos.

- **Unified Threat Management (UTM) Solutions:** A single hardware or software installation that provides multiple security functions, including anti-virus, *content filtering*, E-mail, web filtering, and anti-spam. Potential *single point of failure*, and high *latency* under a heavy load.
 - **VPN Concentrators:** A hardware device that manages VPN traffic for multiple users, allowing secure remote access a network. Can also be built into a firewall. Encrypts and decrypts communication.
 - **Hardware Security Models (HSM):** High-end cryptographic hardware that stores and generates encryption keys and offloads CPU overhead for cryptographic processing from other devices.
 - **SSL/TLS Accelerators:** Device on the edge of the 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. Useful because the *SSL handshake* is CPU-intensive, and time consuming.
 - **Distributed Denial of Service (DDoS) Mitigators:** Sits between the network and the Internet and identifies and blocks DDoS attacks in real-time.
- **Network Appliances (Software-Based)**
- **Syslog:** A standard by which network devices can send logs to a shared server for centralized compilation. The server can be configured to send alerts when notable events occur. Any network device can operate as a client, logging operational events and sending them to the *syslog* server.
 - **Severity Level:** An essential concept for event logging. *Syslog* defines eight levels ranging from *emergency* messages about severe error conditions, to detailed information on everyday activities that can be used to troubleshoot applications.

Value	Severity level	Typical description
0	Emergency	An error condition rendering the entire system unusable.
1	Alert	A severe failure of a service requiring immediate action.
2	Critical	A service failure which may become more severe without quick action.
3	Error	An unexpected error that causes a specific operation to fail, but not its underlying service.
4	Warning	An error or problem condition that is immediately harmless or correctable but might need user review.
5	Notice	Unusual events or state changes that are not errors but not routine operations.
6	Informational	Normal operational messages about routine system activities.
7	Debug	Additional information useful for advanced troubleshooting or application debugging.

- **Bandwidth Monitors:** Provides fundamental network statistics and monitors the percentage of network use over time. Helps identify issues. There are many different ways to gather this metric, such as *NetFlow*, *IPFIX*, *sFLOW*, and other software agents, such as *protocol analyzers*.
 - **NetFlow:** A standard collection method that gathers traffic statistics from all flows and shared communication between devices. Uses probes and collectors, where *probes* watch the network communication, and summary records are sent to the *collector*.
 - **IP Flow Information Export (IPFIX):** A newer *NetFlow*-based standard that evolved from *NetFlow v9*. Includes flexible data support and uses templates to describe the data.
 - **Sampled Flow (sFLOW):** Not technically a network traffic flow analyzer as it only looks at a portion of the actual network traffic. This is usually embedded in infrastructure such as switches and routers. Sampling usually occurs in hardware.
 - **Protocol Analyzers:** Gather packets on the network or in the air, sometimes built into a device. View detailed traffic information, identify unknown traffic, verify packet filtering and security controls, and view a plain language description of the application data.
- **Security Information and Event Management (SIEM) Tools:** *Aggregate* and *correlate* log data from various sources (hosts, switches, routers, firewalls, IDS sensors etc.) across the enterprise to better understand potential security concerns and apportion resources accordingly. Creates *alerts* for system administrators to respond to. 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. Configure SIEM to aggregate appropriate data sources, develop correlation rules, and display alerts, status indicators, and trend analysis, via a dashboard.

- **Detecting Threats**
 - **Rules:** Based on fixed criteria. When an event matches the rule, a specific action is taken. Rules can be written or write themselves.
 - **Correlations:** Based on more open-ended criteria using elaborate *Boolean Logic* and *wild card terms*. A correlation can recognize a broader range of incidents than a rule, but it is more likely to produce *false positives*.
 - **Models:** Evaluate events using *machine learning algorithms*, allowing advanced analytics. Useful for detecting unknown threats that rules and correlations cannot.
- **SIEM Notifications**
 - **Trend:** The aggregate result of many minor events on the network that do not need individual responses but form a meaningful pattern when taken as a whole.
 - **Alert:** A low-priority notification regarding an event that may or may not need an administrator response and isn't immediately critical.
 - **Alarm:** A high-priority notification of a critical or ongoing incident requiring a prompt response.
- **Data Sources**
 - **Network Traffic Log Files:** Monitors the flow of traffic through switches, routers, access points, VPN concentrators, and other infrastructure. Logs routing updates, authentication issues, and network security events. Includes *Intrusion Detection* data and *protocol flow statistics*.
 - **System Log Files:** OS/file information, authentication details, and security events, such as the detection of monitoring apps, *brute force* attempts, or file changes.
 - **Application Log File:** Specific to the application, such as *DNS*, web, or *VoIP*.
 - **Security Log Files:** Detailed security-related information, such as blocked and allowed traffic flows, exploit attempts, blocked URL categories, or *DNS sinkhole* traffic. Includes monitoring of security devices, such as *Intrusion Prevention Systems (IPSs)*, firewalls, and proxy servers.
 - **Web Log Files:** Detailed log of all web server access, including any access errors, exploit attempts, start-up and shut-down notices, or restart messages.
 - **DNS Log Files:** View lookup requests and other *DNS* queries. See the IP address of the request. Identify queries to known bad URLs, including malware sites, and known *Command and Control (C2)* domains. Lock or modify known bad requests at the *DNS* server. Log the results and report on malware activity.
 - **Authentication Log Files:** Know who logged in or who didn't. Identify multiple failures and potential *brute force* attacks. Correlate with other events, such as file transfers, authentications to other devices, and installed applications.
 - **Dump Log Files:** Stores all memory into a diagnostic file. Useful for developers.
 - **VoIP and Call Manager Log Files:** View inbound and outbound call information, endpoint details, gateway communication, and security information. Includes *Session Initiation Protocol (SIP)* traffic logs, such as call setup, management, and tear-down, and alerts on unusually numbered country codes.
 - **Host Log File:** Network, system, security, and vulnerability scan outputs.
- **Security Orchestration Automation and Response (SOAR):** A group of cybersecurity technologies that allow organizations to respond to certain incidents automatically. These often integrate *Cyber Threat Intelligence (CTI)* feeds and can act as the remediation and response engine to SIEM alerts. Best used for *Incident Response (IR)* and *Threat Hunting*.
 - **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 or alert. Monitors *use*, *performance*, *security*, and *trends*.

- **Runbooks:** A set of conditional steps that must be performed as part of any security process, such as log review, *vulnerability scanning*, or *Incident Response (IR)*. A set of rules that can be largely automated. While it may involve a human element, little human intervention is needed. Often used to automate features such as *Threat Response*, *Threat Intelligence Enrichment*, and other activities that the platform can orchestrate on its own. These rules are generally *condition-based*, so instead of following a step-by-step pattern, they are triggered by pre-set conditions.
- **Playbooks:** A looser workflow or checklist that is used to organize or document a security response process. Step-by-step actions that occur in the SOAR process itself. Focuses on assisting security analysts in responding to large incidents or those heavily reliant on human decision-making. These actions typically need to be performed by humans, so *playbooks* serve as a definitive guides to ensure that any documentation, required reporting, or other mandated actions that require human involvement and decision-making, occur exactly when they should.
- **Network Access Control (NAC):** A network security component, usually installed as a software agent on an endpoint. A critical component of both network and endpoint security. Unifies endpoint security, user and system authentication, and network security. When someone tried to connect on a *Bring-Your-Own-Device (BYOD)*, NAC performs a *security posture/health assessment* to determine whether it is safe to allow the connection. Factors that may influence a *posture assessment* are: Is this a trusted device? Is it running antivirus? Which one? Is it updated? Are the correct corporate applications installed? Is it a mobile device? Is the disk encrypted? NAC software can authenticate users and devices, ensure that devices comply with security policies, and regulate traffic between devices. It can also automatically scan devices for updates and schedule security patches.
 - **Persistent Agents:** Software installed on the local device.
 - **Dissolvable Agents:** Software runs but does not stay installed on the machine.
 - **Agentless:** Checks are made during login and log-off.
 - **Quarantine Network:** Built for devices that don't pass the health check.
- **Virtual Private Networks (VPNs):** A mechanism for creating secure connections between a computing device and a computer network, or between two networks, using an unsecure communication medium, such as the public Internet.
 - **VPN/Tunneling Protocols:** Communication and encryption methods for VPNs.
 - **Point-to-Point Protocol (PPP):** Connects one computer 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. Considered deprecated.
 - **Layer Two Tunneling Protocol (L2TP):** An extension of the *Point-to-Point Tunneling Protocol (PPTP)* used by Internet Service Providers (ISPs) to enable VPNs. Commonly implemented with *IPsec* for encryption.
 - **Transport Layer Security (TLS) Tunneling:** Mutual authentication using digital certificates. TLS creates an encrypted tunnel for user authentication and data transmission. Preferred for VPN access.
 - **IPSec Tunneling:** Not a cryptographic protocol, but a Layer 3 *framework*, typically at a VPN application's core. It does not enforce a particular key method or encryption algorithm. Connects sites over a *Layer 3* network as if they were connected at a *Layer 2*. It adds encryption and authentication to make the protocol more secure.
 - **Authentication Header (AH):** No encryption but does contain a hash of the IPsec packet to provide integrity, origin authentication, and *replay attack* protection. Authenticates the entire IP packet, including the IP header.
 - **Encapsulating Security Payload (ESP):** Encrypts the data and the IP packet. Provides data integrity, confidentiality and encryption, limited traffic flow

confidentiality, and *replay attack* protection. While AH authenticates the entire IP packet, including the IP header, ESP authenticates only the IP datagram portion of the IP packet.

- **Transport Mode:** Only encrypts the payload of the packet. Used for host-to-host communication.
- **Tunnel Mode:** Provides end-to-end security by encrypting the entire IP packet and adding a new IP header. Used for connecting entire networks with a *site-to-site VPN*.
- **Internet Key Exchange (IKE):** Authentication and key exchange for IPSec. Negotiates security associations and establishes a secure channel between hosts. Negotiations occur in two phases: *Key Agreement* and *Cipher Selection*. IKEv2 enhances IKE with *Extensible Authentication Protocol (EAP)* authentication and a simplified setup, providing reliability and support for *Network Address Translation (NAT)* traversal.
- **VPN Options**
 - **Host-to-Host:** Joins two computers as though they were directly wired together. Securing traffic between two computers on an untrusted private network.
 - **Host-to-Site/Remote Access VPN:** A computer joins a trusted network remotely, via a *VPN Gateway*. Software is installed on the device that needs the VPN tunnel. The encrypted tunnel is created to connect to a specific network. The VPN software connects to a *VPN Concentrator* and can be configured as *always-on*. *Always-On VPNs* establish connections automatically when detecting trusted networks. Suitable for telecommuters and field employees.
 - **Transport Layer Security (TLS)/ Secure Socket Layer (SSL) VPN:** Enables users to access a network, client-server applications, or internal network utilities and directories, without the need for specialized software. Can be run from a browser or light VPN client. Establishes a secure connection over Port 443, encrypting data and ensuring user authentication.
 - **HTML 5 VPN:** Allows users to access internal resources via pre-configured *VPN Concentrator*, using only a browser as a client.
 - **Site-to-Site:** Connects two or more private networks. This could be a corporate network where multiple offices work in conjunction with each other, or a network with a central office and multiple branch locations. Done by installing a VPN on both sides. Traffic is encrypted as it passes through the local *VPN Concentrator* and is decrypted in the concentrator on the other side.
 - **Full Tunnel:** All data goes through the concentrator, which makes the forwarding decisions.
 - **Split Tunnel:** Some information is sent through the tunnel and other information can be sent outside of the tunnel. Only traffic to the corporate network traverses the VPN tunnel. Traffic to all other sites is split from the tunnel and is not encrypted.
 - **Secure Web Gateway (SWG):** A software application, hardware device, or cloud service 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 Monitoring*, and VPN endpoints. *Next-Gen Firewalls (NGFW)* perform these functions as well.
 - **Content Filters/ Web Filters/ URL Filters:** Control the content users can access over the Internet. Can be hardware, software, or on a firewall. Issues include *over-blocking*, *under-blocking*, handling of encrypted traffic and privacy concerns.
 - **DNS Filters:** Restrict web content.

- **Data Loss Prevention (DLP):** Prevents the sharing or transmitting of sensitive data through E-mail, cloud, USB, or other means. Also includes *Pattern-Matching* and *Watermarking*. DLP solutions can inspect all data leaving the organization, including E-mail contents and attachments, copy to portable media, *File Transfer Protocol (FTP)*, posting to web pages/websites, applications, and *Application Programming Interfaces (APIs)*.
- **Software Defined Networking (SDN):** An approach to network management that enables dynamic, programmatically efficient network configuration to improve network performance and monitoring. It separates the functions of routers, switches, and related devices into two planes. Administrators can centrally manage the network through a *network controller* that separates the two planes.
 - **Data Plane:** Does the work of moving individual frames and packets through the network. It routes packets, schedules queues, and reads *routing tables* and ARP values.
 - **Control Plane:** Makes decisions about the overall flow of traffic, and encompasses the duties of routing protocols, switching protocols, *Quality of Service (QoS)* settings, and other settings that store or communicate rules through the network.
 - **Network Controller:** Communicates with upper-level SDN applications to govern the *control plane* functions and with lower-level SDN data paths to adjust settings in the *data plane*.
- **Software-Defined Visibility (SDV):** *Visibility* refers to being aware of everything within and moving through the network with the help of *network visibility* tools, such as *Next-Generation Firewalls (NGFW)*, *Web Application Firewalls (WAF)* and *Security Information and Event Management (SIEM)* solutions. SDV combines visibility with an automation framework. Gathers data from taps on the physical network and redirects it according to its logical structure. SDV collects real-time data about network traffic and host configurations for improved *anomaly detection* and *incident response*.
 - **Network Packet Brokers (NPB):** Gathers and forwards visibility traffic and performs additional tasks, such as *data deduplication*, *SSL decryption*, *data masking*, and other features to improve security and reduce network load.
- **NIC Teaming/ Load Balancing Fail-Over (LBFO):** The process of combining multiple network cards for performance, load balancing, and redundancy reasons. Group two or more physical NICs into a single logical network device, called a *bond*.
- **Traffic Shaping Devices:** Regulate abusive users, safeguard applications and networks against traffic spikes, and stop network attacks from overwhelming network resources.
- **Quality of Service (QoS):** Creates an *undesired list* and gives priority to certain kinds of traffic over others, such as giving VoIP traffic a higher priority than web browsing.
- **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. Provides authorization services when performing operations on the DNS. Must be *digitally signed*.
- **Domain-Based Message Authentication, Reporting, and Conformance (DMARC):** An E-mail security protocol that verifies E-mail senders and helps prevent spoofing.
- **Windows Registry:** Primary configuration database that monitors unwanted application changes. Backup the registry before making changes.
- **Configuration Management Systems (CMS):** Tools/databases that are used to manage IT infrastructure configuration and data for users, suppliers, locations, business units, and customers.
- **Configuration Management Database (CMDB):** A central repository for infrastructure information.
 - **CM Diagrams:** Includes *workflows*, physical and logical *network diagrams*, and *rack layouts*.
 - **Baseline Configurations:** Note any *static* allocation of IP addresses, versus DHCP. May utilize *IP Address Management (IPAM) Suites* for managing the assignment of IP addresses.
- **Asset Management Software:** Automatically discover, track, and catalog various assets, providing a centralized dashboard for management.

- **Administrative Controls**

- **Onboarding Policies**

- Hiring Qualified Candidates.

- Employee Background Check/ Clearances.
- *Social Media Analysis.*
- Code of Ethics.
- Provision Accounts/ Credentials.
- Employee Training.
 - Gamification.
 - Tabletop Exercises.
 - Hands-On/ Live Demo.
 - Audits/ Walk-Throughs.
 - *Phishing Simulations/Campaigns.*
 - *Computer-Based Training (CBT).*
 - *Capture the Flag (CTF):* Jeopardy or Attack/Defense Style.
 - Pen-Testing/ Attack Simulation.
- **Role-Based Security Awareness Policies**
 - **End Users:** Understanding threats and how to protect against them. Password security, *phishing* awareness, and physical security may also be components of end-user training.
 - **Customer-Facing Employees:** Recognizing *social engineering* and protect the company's reputation.
 - **Privileged Users:** Understanding the permissions they have been given, what responsibilities come with them, and the importance of not sharing credentials.
 - **Administrators:** Understanding technical threats, network configuration, and security solutions.
 - **Incident Response Teams:** Understanding how to respond to physical threats, malware removal, legal procedures and forensics investigations.
 - **Management:** High-level knowledge of current controls and how they could be compromised.
 - **Recertification:** Defines how frequently users must certify their need for a resource or membership.
- **Privacy/User Agreement Policies**
 - *Terms of Service/ Terms of Use/ Terms and Conditions (T&C's).*
 - *Standard Operating Procedures (SOP).*
 - *Privacy Notices/ Privacy Policy.*
 - *Acceptable Use Policies.*
 - *Non-Disclosure Agreements (NDA)/ Non-Competes.*
- **Password Policies**
 - Change all default usernames and passwords.
 - Minimum/ Maximum *Password Age.*
 - Complexity: Length/ character/ Re-use restrictions.
 - Passphrase.
- **Secure Personnel Policies**
 - **Principle of Least Privilege:** The user is given a minimum level of access needed to perform a job.
 - **Clean Desk Policy:** Requires that employees shred or contain all physical documents each time they leave a work environment. Requires all laptops and phones to be password-protected.
 - **Mandatory Vacation:** A policy that requires employees to take a set number of vacation days per year. Used to detect fraud/*malicious insiders*, as well as to prevent employee burnout.
 - **Separation/ Rotation of Duties:** Users must not be granted enough privileges to misuse a system.
 - **Two-Person/ Dual Integrity:** Prohibits individual access to certain material by requiring the presence of at least two authorized persons, each capable of detecting incorrect or unauthorized security procedures concerning the task being performed.
 - **M of N Control:** A protection measure that requires that a *minimum number of agents (M)* out of the *total number of agents (N)* work together to perform high-security tasks.
- **Time-Based Access Policies:** Disallow network access before or after business hours.
- **Location-Based Policies:** Disallow network access depending on device location.
 - **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 photographs, videos, websites, and SMS messages.
- **Impossible Travel:** Office 365 includes a security feature to detect remote hacking attempts. With each login from a new location, it calculates the travel time from the previous login location and uses it to determine whether the travel is possible.
- **Asset, Configuration, and Change Policies**
 - **Asset Management Policies:** *Asset Tracking, RFID Tagging*, and procedures for lost/stolen devices.
 - **Configuration Management (CM) Policies:** The process of maintaining systems in a desired state. CM requires inventory *baselines*, updates and patches.
 - **Change Management Policies:** Procedures for implementing a change, involving the *Request for Change (RFC)*, *Approval*, and *Regression/Rollback* processes.
- **Risk Planning Policies**
 - **Cyber Risk Assessment:** Identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.
 - **Qualitative Risk Assessment:** Quickly identify risks using numerical ratings (1-5) or colors (green, yellow, red) that rank risks based on *likelihood of occurrence* and *business impact*.
 - **Quantitative Risk Assessment:** Involves numerical values, statistical analysis, and measurable data to provide a more precise and objective measure of cybersecurity risks.
 - **Single Loss Expectancy (SLE):** The expected cost of one loss event.
 - **Annual Rate of Occurrence (ARO):** The number of loss events expected in a year.
 - **Annual Loss Expectancy (ALE)= SLE x ARO:** The total value lost over a year.
 - **Audit Risk Model:** Assesses the potential implications, risks, and costs of a data breach or cyber-attack on the organization and its stakeholders.
 - **Privacy Impact Assessment (PIA):** An analysis of how *Personally Identifiable Information (PII)* is handled to ensure compliance with regulations, determine privacy risks associated with information systems or activities, and evaluate ways to reduce risk.
 - **Risk Transference:** A risk management technique in which risk is transferred to a third party.
 - **Cybersecurity Insurance Policies:** Insurance is useful in the event of a data breach.
 - **Managed Detection and Response (MDR):** A service where a vendor monitors firewalls and other security tools to provide expertise in triaging events. Offers hosted security services.
 - **Managed Service Providers (MSPs):** Companies that manage the IT assets and cybersecurity of other companies.
 - **Security-as-a-Service (SECaaS):** A business model in which a service provider integrates their cloud-based security services into a corporate infrastructure on a subscription basis. May include authentication, anti-malware, *Intrusion Detection Systems (IDSs)*, and *Security Information and Event Management (SIEM)*.
 - **Vulnerability Management Policies:** The process of identifying, evaluating, treating, and reporting security vulnerabilities in systems and the software that runs on them. Frequently conduct assessments to find vulnerabilities and possible attack vectors, as well as to harden the system.
 - **Penetration Testing/ Ethical Hacking Policies:** An authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an *ethical hack* involves duplicating the strategies and actions of malicious attackers. Certain industries are required to conduct semi-regular *penetration tests* to stay compliant with regulations, such as PCI DSS.
- **Incident and Impact Planning Policies**
 - **Incident Response Plan (IRP):** A written document, formally approved by the senior leadership team, that helps the organization before, during, and after a security incident.
 - **Business Impact Analysis (BIA):** Predicts the consequences of a business disruption and develops recovery strategies. Potential loss scenarios should be identified during a *risk assessment*.

- **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. A well-written BCP should include *preventative*, *corrective* and *recovery* controls.
- **Disaster Recovery Plan (DRP):** Maintaining or reestablishing vital infrastructure following a natural or human-induced disaster, such as a storm or war. It employs policies, tools, and procedures.
 - **Site Resilience/ Redundancy/ Fault-Tolerance**
 - **Hot Sites:** A fully functional backup site that already has mirrored data.
 - **Warm Sites:** Contains all elements of cold sites but adds storage hardware. Still requires data to be transported, should a disaster occur.
 - **Cold Sites:** Provides power, networking, and cooling, but no other hardware.
- **Functional Recovery Plan (FRP):** A step-by-step guide from an outage to being back up and running.
- **Measurement System Analysis (MSA):** A thorough assessment of a measurement process. Includes an experiment that seeks to identify the components of variation in that measurement process.
- **Offboarding Policies**
 - Disabling Accounts and Passwords.
 - Disabling Permissions and Access to VPN, E-mail, Network, Servers, and Files.
 - Policy Enforcement, Conduct Requirements, and Discipline.
 - Exit Interviews.

Wireless Security

- **Logical Controls**
 - **Wireless Access**
 - **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 access to network resources.
 - **Wi-Fi Protected Setup (WPS):** A feature on many routers. It is designed to make the process of connecting to a wireless network easier. Connect by pushing a button on the router, by bringing the device near the router (NFC), or by entering a PIN/passphrase on the device. Best to disable this feature or opt for the more secure *Easy Connect DPP*.
 - **Easy Connect DPP:** Also known as *Wi-Fi Easy Connect* or *Device Provisioning Protocol (DPP)*. A Wi-Fi Alliance-certified standard that allows devices to be securely added to a network. It uses techniques, such as *QR Code scanning*, to simplify the process.
 - **Wireless Authentication and Encryption**
 - **Wired Equivalent Privacy (WEP):** A severely flawed security algorithm for 802.11 wireless networks.
 - **Wi-Fi Protected Access (WPA):** A stronger wireless authentication and encryption standard.
 - **WPA:** Provides more sophisticated data encryption and stronger authentication than WEP. Uses the RC4 encryption algorithm with TKIP. Was later replaced by WPA2.
 - **Temporal Key Integrity Protocol (TKIP):** Provides more secure encryption than the earlier WEP, without needing to replace existing hardware.
 - **WPA2:** WPA2 replaces *RC4* and *TKIP* with stronger encryption and authentication mechanisms: *Advanced Encryption Standard (AES)*, an encryption mechanism, and *CCMP*, an authentication mechanism. Has a *Pre-Shared Key (PSK)* brute-force problem. Since there is no *Perfect Forward Secrecy*, once an attacker has the PSK, they can easily ascertain all keys.
 - **WPA2-Personal-PSK:** *Pre-Shared Key (PSK)*. All users of a SOHO network use the same key/password to authenticate. All passwords are 8 to 63 characters long.
 - **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP):** Based on 128-bit AES. More secure than TKIP. Was advanced for its time. Provides data confidentiality and message integrity.
 - **WPA3:** Offers individualized data encryption for each device connected to the network, even in open Wi-Fi networks. Each device has a unique encryption key, enhancing privacy and security. Offers improved security with enhanced, open, updated cryptographic

protocols, key agreement, and mutual authentication. Creates a shared session key without sending that key across the network. Includes *Simultaneous Authentication of Equals (SAE)*, *Management Frame Protection (MFP)*, *Galois/Counter Mode Protocol (GCMP)*, and *Perfect Forward Secrecy (PFS)*. Eliminates the need for *four-way handshakes* and hashes. Has no *brute force* problems.

- **Simultaneous Authentication of Equals (SAE):** Also known as *Dragonfly Key Exchange*. A password-based protocol that authenticates and exchanges keys between two parties.
- **Management Frame Protection (MFP):** Also known as *Protected Management Frames (PMF)*. A security feature that protects unencrypted management messages and broadcast frames between wireless devices.
- **Galois/Counter Mode Protocol (GCMP):** An authenticated mode that combines *Counter Mode* with a hash-based authentication code. Provides data authenticity and integrity. Useful for hashes as well. Widely used.
- **Perfect Forward Secrecy (PFS):** Generates a new key each session. Prevents stolen *private keys* from decrypting all past and current connections. Increases complexity for attackers, which enhances security.

- **Administrative Controls**

- **Wireless Security Policies and Procedures:** Address how wireless networks can be used and what types of information can be transmitted. Policies should also outline procedures for installation, protection, management, and usage.
 - **Enforce Access Control:** Restrict access to the network based on the organization's security policies. For example, limit access to certain IP addresses or only allow access from certain locations.
 - **Restrict Wi-Fi Access:** Choose a router that allows change to the strength of the signal to ensure only authorized users can use the connection.
 - **Require Automatic Firmware Updates:** Keep networking equipment firmware current, as updates often contain security patches.
 - **Require Authentication:** Ensures that data or control packets come from the right source.
 - **Disable SSID Broadcasting:** Prevent unauthorized users from seeing and connecting to the network.
 - **Require VPNs:** Encrypt data to make it unreadable to eavesdroppers on public Wi-Fi networks. Look for VPNs that use industry-standard AES-256 encryption and open-source protocols.

Cloud Security

- **Logical Controls**

- **Server-Side Encryption:** The encryption of data at its destination by the application that receives it.
- **Client-Side Encryption:** Encrypting data on the sender's side before it is transmitted to a server.
- **Cloud-Related Security Appliances**
 - **Virtual/ Cloud Firewall:** A software-based security device or service that monitors and filters network traffic for *Virtual Machines (VMs)*. Also known as *cloud firewalls*, they are designed to offer the same security and inspection capabilities as a physical firewall but with additional capabilities for cloud deployment. Virtual firewalls provide valuable East/West network security.
 - **Next-Gen Firewall (NGFW):** Third-generation firewall technology, combining a conventional firewall with other network device filtering functions. Can contain *Intrusion Detection System (IDS)*, *Intrusion Prevention Systems (IPS)*, *Content Filtering*, *Web Proxy*, *Anti-Bot*, *Anti-Malware*, *Virtual Private Network (VPN)*, and *Identity and Access Management (IAM)* functionality. Also called an *Application Layer Gateway*, *Stateful Multi-Layer Inspection*, or *Deep Packet Inspection*.
 - **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-Based Intrusion Prevention System (IPS):** Any IPS is based on *implicit allow*. Its rules are designed to specify types of traffic that should be *blocked*.
 - **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, baseline deviations, anomalies, and/or behavior heuristics*.
- **Cloud Access Security Broker (CASB):** An on-premises, client-side software, physical hardware device, or cloud-based software that sits between cloud service users and cloud applications. Monitors all activity and enforces security policies. Mediates access to cloud services, provides visibility into application use and data security policy use, and enforces access controls. Other functions include verification of compliance with formal standards and the monitoring and identification of threats. Can be implemented as a *forward proxy, reverse proxy*, or API-based.
- **Service Integration and Management (SIAM):** Allows the integration of many different cloud service providers into a single management system. This simplifies the application management and deployment process when using separate cloud providers.
- **Administrative Controls**
 - **Cloud Security Policies and Procedures:** Govern network security and manage risk in the cloud.
 - **Access Control:** The process of granting or denying users or entities access to cloud resources, such as sensitive data and applications.
 - **User Education:** Training to help ensure security awareness.
 - **Password Administration:** Managing passwords.
 - **Background Checks:** A preventive administrative control.
 - **Backup and Recovery:** A policy for backing up and recovering data.
 - **Incident Response:** A policy for responding to incidents.
 - **Auditing:** A policy for auditing cloud security controls.

Endpoint Security

- **Physical Controls**
 - **Cable Locks:** Secure laptops, desktop computers, audio equipment, and other hardware from theft.
 - **Server Racks:** Organize and lock server racks. Consider *standard naming conventions* and rack layout diagrams for easier servicing.
 - **Privacy Screens:** Shields the content on a screen from everyone except the user.
 - **USB Data Blocker:** Considered *Data Loss Prevention (DLP)* and prevents *Malicious USB* attacks.
 - **Port Security:** Disable unused physical ports on routers, switches, and other network hardware.
- **Logical Controls**
 - **Power On Self-Test (POST):** A hardware check that is performed before booting an OS.
 - **Hardware Root of Trust (RoT):** A fundamental security component that provides a trusted source of function, so a device can establish strong security levels. Highly reliable hardware, firmware, and software components that perform specific, critical security functions. Often integrated as a chip and is considered inherently trusted, so it must be *secure by design*. The RoT starts a *chain of trust*, which ensures that no malicious code is present before the boot process begins. Utilizes *Trusted Platform Modules (TPMs)* which store encryption keys, hashed passwords and user identification. A secure subsystem providing *attestation*.
 - **Boot Integrity (Chain of Trust):** Assures the integrity of a platform by demonstrating that the boot process starts from a trusted combination of hardware and software and continues until the OS has fully booted and applications are running.
 - **Secure Boot:** In the BIOS EUFI, this checks the bootloader's *digital certificates* and *signature*. Password-protecting the BIOS EUFI creates an additional layer of security.
 - **Trusted Boot:** Verifies the OS Kernel and starts the *Early Launch Anti-Malware (ELAM)* process, which checks for trusted drivers and won't load untrusted ones.

- **Measured Boot:** Verifies that nothing on the computer has been changed by malicious software or other processes. Uses the TPM to check hashes of key system state data. The *attestation server* receives a boot log report signed by the TPM for analysis. Changes are monitored and managed.
 - **Remote Attestation:** A mechanism for hardware and software to prove their identity and integrity while logging on. Uses a combination of a *digital certificate* and cryptographic *hashes* of relevant software files and settings, to determine that they haven't been tampered with.
 - **File Integrity Monitoring:** Validates the integrity of operating system and application software files using a verification method between the current file state and a *known good baseline*.
 - **File Integrity Checks:** Using hash algorithms to ensure that files have not been modified.
- **(Identification), Authentication, Authorization, and Accounting (AAA):** A cybersecurity framework that controls access to computer resources and networks, enforces policies, and audits usage.
 - **Identification:** The management of identity controls. *Digital Identity* is represented by accounts managed by network administrators. Cryptography enhances identity security on public networks.
 - **Identity Proofing:** Also known as *Identity Verification*. A process that verifies and authenticates a person's identity when they try to access a service or system. The goal is to confirm that the person's identity is true and that they are the rightful owner.
 - **Authentication:** The act of proving the identity of a user/system with passwords, keys, and tokens.
 - **Authentication Protocols:** A communications or cryptographic protocol specifically designed for transfer of authentication data between two entities.
 - **Password Authentication Protocol (PAP):** No encryption. Passwords are 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 a *challenge message*. The client responds with the *password hash* calculated from the challenge and the password. The server compares the received hash with the stored hash. The *challenge-response* continues periodically during the connection. No password is sent in the clear, unlike PAP.
 - **MS-CHAPv2:** Microsoft's proprietary version of CHAP, which uses encrypted tunnels.
 - **Extensible Authentication Protocol (EAP):** An authentication framework that provides general guidance for authentication methods. Provides a secure way to send identifying information across a wireless network.
 - **Protected EAP (PEAP):** A protocol that encapsulates EAP within an encrypted and authenticated TLS tunnel. An extension of EAP that is sometimes used with 802.1x. The authentication server uses a *digital certificate*, but the client does not.
 - **Lightweight Extensible Authentication Protocol (LEAP):** A Cisco-proprietary network authentication mechanism for wireless LANs.
 - **EAP Flexible Authentication over Secure Tunneling (EAP-FAST):** A Cisco-designed replacement for LEAP. A method that enables secure communication between a client and an authentication server. Works with a RADIUS server. Supports certificates, but they are not required.
 - **EAP Transport Layer Security (EAP-TLS):** An IETF open standard that uses *public key cryptography* and *public key infrastructure* to securely identify both the client and the network. Uses certificates and TLS for mutual authentication between a client and a server. Complex to implement because it requires a *digital certificate* for the authentication server and all other devices. One of the most secure EAP standards and is widely used.
 - **EAP Tunneled Transport Layer Security (EAP-TTLS):** A framework to support authentication across several communication systems. All authentication

methods work inside the TLS tunnel. Allows for systems to use older authentication methods, such as PAP, within a TLS tunnel. Requires a *digital certificate* on the authentication server and builds a TLS tunnel using this digital certificate. It does not require digital certificates on every device.

- **IEEE 802.1x: Port-Based Network Access Control (NAC):** A hardware-based *Network Access Control (NAC)*. Centralized authentication for enterprise environments. An authentication protocol used in VPNs, wired, and wireless networks. In VPNs, it is used via a RADIUS server. Wired networks use it for port-based authentication. Wireless networks use it in *enterprise mode*. Uses a centralized server so all users can use their normal credentials to authenticate. Can be used with certificate-based authentication. Requires integration with *Extensible Authentication Protocol (EAP)* and an authentication server. Works alongside RADIUS, LDAP, and TACACS+. Can also be used as a *Network Access Server (NAS)*. No SSO functionality.
- **Single Sign-On (SSO):** An authentication scheme that allows a user to login to any of several related, yet independent, software systems, with a single ID
 - **OAuth:** *Authorization framework*, not an *authentication protocol*. Works with *Open ID Connect*, which provides authentication. Determines which data is accessible to the user. Users can allow one application to interact with another, without using a password. Facilitates sharing of resources between sites. Doesn't share password data, but instead uses authorization tokens to prove identity.
 - **OpenID:** An open standard authentication protocol. Adds authentication to *OAuth* and validates user presence.
 - **Open ID Connect:** Handles Single Sign-On (SSO) authentication over TLS. Establishes trust between one account (Google, for example) and a third-party account. Users decide how much access the third-party account will have to the original account. Doesn't contain security features, like encryption. It relies on TLS. This means it is susceptible to any attacks that bypass TLS. Links between accounts can be removed at any time. Example: *Facebook Connect*.
- **Federated Identities:** Extends network accessibility beyond employees. Allows access to trusted accounts from different networks. Users provide *attestation of identity* to service providers. Can log in with credentials from other sites, such as Google or Facebook. Provides authentication for partners, suppliers, customers, and employees.
 - **Transitive Trust:** If one party has *explicit trust* relationships with two other parties, that can form an *implied trust* relationship between those two.
 - **Identity Provider (IdP):** A system entity that creates, maintains, and manages identity information, and also provides authentication services to applications within a federated network. *Identity Providers (IdP)* offer user *Authentication-as-a-Service (AaaS)*.
 - **RADIUS Federation:** Members of one organization can authenticate to the network of another organization using their normal credentials. Uses 802.1x as the authentication method, RADIUS on the backend, and EAP to authenticate.
 - **Security Assertion Markup Language (SAML):** Open standard for authentication and authorization for users to access third-party resources. Authenticates through a third-party source to gain access. The resource is not responsible for authentication. The request is passed through a trusted third-party server. The authentication process starts with the *Principal* directly contacting the *Service Provider (SP)* and the SP asking for an *authentication token* from the *Identity Provider (IdP)*. If granted, the SP gives access. If not granted, the principal automatically negotiates with the IdP for authentication. The SP and the IdP do not need to communicate to maintain a trusting relationship. Doesn't work well for mobile applications.

- **Shibboleth:** An open-source software that uses SAML to provide a third-party *Federated, Single Sign-On (SSO)* authentication.
- **Authentication Factors:** Evidence that a person provides to verify their identity when trying to sign in to an application, online account, or other resource.
 - **Knowledge-Based Authentication (KBA) Factors:** Easy to memorize.
 - **Something You Know:** Password, PIN, or challenge question.
 - **Passphrase:** A type of password that uses a text string or sentences, with or without spaces.
 - **Static Codes:** PINs that stay the same until they are changed.
 - **Secret Questions:** Users answer at least one secret question.
 - **Static:** Pre-configured secrets to recover a password, such as *the street you grew up on*.
 - **Dynamic:** Identity verification questions, such as *which address looks familiar to you?*
 - **Possession Factors:** Digital data that a human cannot be expected to memorize.
 - **Something You Have:** Cryptographic identification device, physical key, ID badge, smartcard, or token.
 - **Smart Card:** A physical *electronic chip* or *integrated circuit* card.
 - **Common Access Card (CAC):** A verification card used by the U.S. military and the *Department of Defense (DoD)*, for identification and access to secure systems and locations.
 - **Personal Identification Verification Card (PIV):** A security standard and smart card used by federal agencies in the U.S. Used by civilians working in the federal government.
 - **Hardware Token/Token Key:** Contains the security credentials for a login session and identifies the user, the user's groups, the user's privileges, and a particular application.
 - **Authenticator Applications:** Adds an extra layer of security to online accounts via *Time-Based One-Time Passwords (TOTPs)*.
 - **HMAC-Based, One-Time Password (HOTP):** HMAC stands for *Hash-Based Message Authentication Code*. Used only once before a new code must be generated.
 - **Time-Based One-Time Password (TOTP):** Uses a randomly generated code as an additional authentication token. Provides an indicator of integrity, the current local time.
 - **SMS/Phone Call:** Verifies phone numbers and phone access.
 - **Push Notifications:** Enables user authentication by sending a *push notification* directly to a secure application on the user's device.
 - **Digital Certificates:** A file created and signed using cryptographic algorithms, which demonstrates that the person presenting the public certificate also holds its *private key*.
 - **Inherence Factors:** A unique physical or behavioral trait.
 - **Something You Are:** Body measurements and calculations for human characteristics. **Biometrics** are *Personally Identifiable Information (PII)*, and protocols must not reveal this data without consent. Fingerprints and other scans are not usually stored. Data is stored as a mathematical computation.
 - **Physiological Biometric Systems:** Measure characteristics of a person, such as a fingerprint, iris scan, retinal scan, palm scan, or venous scan. Some can check for pulse and temperature on a fingerprint scanner to detect counterfeiting.

- **Something You Can Do:** Actions, gestures, gait analysis, or signatures.
 - **Behavioral Biometric Systems:** Measures how a person acts via voice prints, gait, signature dynamics, or keystroke dynamics.
 - **Something You Exhibit:** Inherent behaviors, like personality traits or even detectable neurological activities.
 - **Evaluation Metrics for Biometric Patterns**
 - **False Rejection Rate (FRR):** Measures legitimate users not recognized.
 - **False Acceptance Rate (FAR):** Measures interlopers accepted.
 - **Crossover Error Rate (CER):** Where FRR and FAR meet, indicating *system efficiency*.
 - **Context-Aware Factors:** Time of day, physical location, behavior or risk-based authentication, or relationship to someone trusted.
 - **Somewhere You Are:** Current location.
 - **Geofencing:** A virtual perimeter for a real-world geographic area.
 - **Impossible Travel:** Detects remote hacking attempts. With each login from a new location, it calculates the travel time from the previous login location and uses it to determine whether both logins can belong to the same person.
 - **Someone You Know:** Connection to another person who is trusted via personal relationships or *chain of trust* authentication systems.
- **Two-Factor Authentication (2FA):** Requires two forms of identification to access resources.
 - **2-Step Verification:** Also known as *out-of-band mechanisms*. Sends a software token to a user-controlled resource via SMS, phone call, push notification, or E-mail. Though considered *two-factor authentication*, intercepting the code within the time frame would compromise security.
- **Multi-Factor Authentication (MFA):** A user is granted access only after successfully presenting *two or more* pieces of evidence to an authentication mechanism. Most widely used authentication option.
- **Continuous Authentication:** Monitors user activity post-login, enhancing security. Currently in the research phase.
- **Adaptive Identity:** The process of tailoring each customer authentication to the specifics of the request. It involves calibrating multiple sets of risk indicators to determine the type of authentication needed, and how strong to make it.
- **Password Vaults:** Generates random passwords and securely stores them, reducing the risk of data breaches. Risks include compromise of the *master password*, and other attacks related to vendors, the cloud, or impersonation.
 - **Windows Credential Manager:** Provides secure storage for credentials used to access Windows computers, as well as storage for certificates and passwords used for network services or websites.
 - **Keychain:** Stores passwords, certificates, and other credentials in MacOS.
 - **The Credential Management API:** Password management by web browsers and applications. Includes *federated credentials*, such as *Single Sign-On (SSO) tokens*.
 - **KeePass:** Third-party password manager that stores passwords or other credentials in an encrypted file and is protected by a central account.
 - **LastPass:** Third-party password manager that stores passwords online.
- **Digital Signatures:** Combines *public key cryptography* with *hashing* for authentication, integrity, and non-repudiation. The sender creates a hash of the message and signs it with their *private key*. The recipient verifies the signature using the sender's *public key*. Added to clear text messages. Verifies the message has not been tampered with by a MitM.

- **Authorization:** Specifying access rights and privileges for resources.
 - **Identity and Access Management (IAM):** A framework of policies and technologies to ensure that the right users have the appropriate access to technology resources. IAM encompasses four main processes: *Identification*, *Authentication*, *Authorization* and *Accounting*. *Identification* creates unique IDs, *authentication* verifies identities, *authorization* determines access rights, and *accounting* tracks authorized usage. Includes *Account Life Cycle Maintenance*.
 - **Directory Services:** Determines *authorization* by referencing a single database, or *Directory*, composed of the organization's usernames and passwords. Also contains computers, printers, and other devices. All authentication requests must reference this directory. Each user only needs one set of credentials. Access *Directory Services* via *Kerberos* or *LDAP*.
 - **Microsoft Active Directory (AD):** A *Directory Service* that uses a combination of *Kerberos* for authentication and *Single Sign-On (SSO)*, and *LDAP* for resource authorization queries.
 - **Kerberos:** Authentication through a cryptographic *ticket-granting* service. Authenticate once, and the device is trusted by the system. Users can gain access to multiple resources with one authentication. Still requires individual servers to maintain their access databases. Allows for *Single Sign-On (SSO)*. Works well in Microsoft environments.
 - **Lightweight Directory Access Protocol (LDAP):** A database that stores information about network users, systems, and services. Utilizes a *hierarchical tree database structure* to store information about both network users and resources. Network administrators can enter permissions for various network resources into the LDAP database structure. This provides centralized authorization for all servers in the network. *Secure LDAP (LDAPS)* over TSL has a large attack surface, so it is not used over the Internet. No SSO functionality.
 - **Simple Bind Authentication:** A common way to authenticate LDAP clients to a directory server. It's also known as *password-based authentication* because the client provides a password to the *Directory Proxy Server*.
 - **Privilege Management:** A combination of people, processes, and technologies that help organizations control access to critical resources.
 - **Privileged Access Management (PAM):** Also known as *Privileged Identity Management (PIM)*. Manages privileged accounts (*superuser*, *admin*, and *root* users) and their credentials. Policies, procedures, and controls to prevent the abuse of privileged accounts. Privileges are granted by request, doled out for a short time, and easily logged and audited. Privileged accounts are stored in *digital vaults*. Requires stringent authentication, mandatory logging, and frequent audits.
 - **Just-In-Time (JIT) Permissions:** Elevates privileges only when needed, for a limited duration. Implemented through *temporary elevation*, *password vaulting*, or *ephemeral credentials*. Ensures *Zero Standing Privileges (ZSP)*, a security principle that eliminates persistent, *always-on* access rights for accounts and identities.
 - **Accounting:** Account policies that enforce *privilege management*. They dictate what users can do and enforce strong credential policies. This helps manage risk from compromised accounts. Auditing and *permissions reviews* aid in detecting suspicious activity and preventing data breaches.
 - **Public Key Infrastructure (PKI):** The policies, procedures, software, hardware, and employees needed to create, distribute, manage, store, and revoke *digital keys* and *digital certificates*. Also includes the binding of *public keys* to people or devices. The user maintains control over their *private key* but can share the *public key* with any server that requires it for login. The user presents the *private key*, and the server matches it to the *public key* already stored on the server. If not managed properly, PKI can lead to critical vulnerabilities.

- **Private and Public Keys:** Sessions are encrypted with a recipient's *public key* and decrypted with the recipient's *private key*. Compromised *private keys* endanger the authentication process and therefore, data confidentiality.
 - **Static Keys:** For use in many instances of a cryptographic key establishment process, over a relatively long period of time.
 - **Ephemeral Keys:** *Session keys* created with the *symmetric* and *asymmetric keys*, generated for each execution of a key establishment process.
 - **Symmetric Keys:** A single, shared, *public key*. Also called a *private*, *secret*, or *session key*.
 - **Asymmetric Keys:** Each user has a *public key* and a *private key*. The use of the *public key* is the basis for *Public Key Infrastructure (PKI)*.
- **Key Exchange:** An encryption key is used to decrypt *ciphertext* back into *plain/clear text*. Users cannot exchange, or decrypt encrypted data without first securely exchanging keys. Keys are securely exchanged between two parties, with the help of a cryptographic algorithm.
 - **In-Band Key Exchange:** Exchanging keys in the same communication channel that is going to be encrypted. Poses a security threat.
 - **Out-of-Band Key Exchange:** Exchanging keys in a separate, more secure communication channel, such as sending a *smart card* via the mail, or communicating a password verbally. Keys are more secure, but the communication is slower and less convenient.
 - **Digital Envelopes:** Combine *symmetric* and *asymmetric encryption* to securely exchange keys and ensure message confidentiality. The process is as follows: The sender encrypts the message with the *symmetric key* to make a *session key*. The *session key* is then encrypted with the recipient's *public key* and sent along with the encrypted message (Double encryption). The recipient decrypts the *session key* with their *private key* and then decrypts the message with the *symmetric key*.
- **Key Management:** Technology, policies and procedures for protecting, storing, organizing, and distributing *public* and *private keys*. The process of managing cryptographic keys and related security parameters throughout their *lifecycle*. This includes the generation, storage, distribution, use, rotation, and destruction of keys. *Key management* also involves establishing and controlling access to keys, and ensuring that only authorized individuals can access them
 - **Key Generation:** Create a strong key, 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 *private keys* against unauthorized use (usually in a *Trusted Platform Module (TPM)*).
 - **Revocation:** Manage keys that have been compromised.
 - **Expirations:** Monitoring the certificate's shelf life.
- **Digital Certificates:** Small data files that contain identity credentials. A public assertion of *identity*, validated by a *Certificate Authority (CA)*. An electronic document assigned to a person or device, used to prove the validity of a *public key*. Binds the *digital certificate* owner to a *public* and *private key*. Also used to encrypt data or create *digital signatures*. Based on x.509 standard, certificate attributes are as follows: *Serial number*, *signature algorithm*, *issuer*, *validity dates*, *subject name*, *public key*, *extensions*, and *Certificate Authority (CA) signature*.
 - **Certificate Authority (CA):** A third-party organization that verifies the authenticity and identity of an entity, such as a website, E-mail address, or person. CAs also provide cryptographic keys for data encryption.
 - **Public/Commercial Certificate Authorities:** Built into *Browsers* and trusted across organizations and networks. Creates a *key pair* and signs the *public key*. Purchase a website certificate from a CA that will be trusted by browsers.

- **Private Certificate Authority (Self-Signed):** An in-house CA used in medium-large organizations. All devices must trust the internal CA. While useful for internal trust, *self-signed certificates* should never be used in a production environment.
 - **Single CA:** The *Single CA* is both a *root CA* and an *issuing CA*. Simple to implement, but risky, as a compromise could lead to a system collapse. Often used on private networks.
 - **Third Party/ Hierarchical CA:** Several CAs share the load. Limits damage if any CA becomes compromised. Requires a *Chain of Trust*, which lists all the certificates between the server and the *root CA*. Adds layers of security, but still vulnerable at the root level.
 - **Web of Trust:** Adds other users who vouch for and self-sign each other's certificates.
 - **Mesh:** Cross-certifying CAs. Doesn't scale well.
 - **Mutual Authentication:** A server and client mutually authenticate.
- **Offline Certificate Authority (CA):** A CA that is isolated from network access and is often kept in a powered-down state. The purpose of keeping a CA offline is to protect an organization's most valuable information by separating it from potentially malicious third parties.
- **Certificate Types**
 - **Root Certificate:** The certificate that identifies the *Root Certificate Authority (CA)*. Everything starts with this certificate. The *root certificate* issues other certificates. Access to the root certificate allows for the creation of any trusted certificate.
 - **Web Server/SSL Certificate:** A data file hosted on a website's origin server that enables websites to use HTTPS. SSL certificates make SSL/TLS encryption possible. They contain the website's *public key*, *identity*, and other related information.
 - **Subject Alternative Name (SAN) Certificates:** Allows the certificate to contain multiple names, such as multiple website domains or the names of both the website and the organization. Preferred over the *Common Name (CN)*, for specifying the identity of the certificate subject.
 - **Domain Validation (DV) Certificate:** Used to identify a DNS host or a *domain name* for TLS-protected protocols like HTTPS.
 - **Extended Validation (EV) Certificates:** A certificate backed by a stricter identity validation process than the CA's default.
 - **Wildcard Certificates:** A multi-domain certificate that can apply to any number of sub-domains within a single domain.
 - **User or Machine Certificates:** Used to identify an entity like a user or a computer. Typically issued by a *Private CA* for use within an organization, so users and devices within a corporate network trust each other.
 - **Self-Signed Certificates:** Used when PKI is too difficult or expensive. These can be deployed on machines, web servers, or programs. They are trusted within the corporate network but marked untrusted by the OS or browser. Suitable for non-critical environments like development or testing.
 - **E-mail Certificates:** Usable for sending and receiving E-mail messages. Usually only requires proof that the user owns the associated E-mail address.
 - **Code-Signing Certificates:** Used to authenticate the source and integrity of executable files.
- **Certificate Management:** The process of monitoring and controlling digital certificates to ensure network security and prevent disruption. It involves managing every step in a certificate's lifecycle, including issuing, renewing, deploying, and revoking certificates.
 - **Registration Authority (RA):** Identifies and authenticates certificate requesters, maintains certificates for current certificate holders, and prevents the use of expired

certificates. Facilitates the identity verification process and submits CSRs to the CAs. RAs do not issue certificates.

- **Certificate Signing Request (CSR):** The process for requesting certificates. The subject generates a *key pair* and submits a CSR to the CA. The CA reviews and validates the information before issuing the certificate. A *private key* is not a part of the CSR and must be securely stored by the subject.
- **Certificate Chain of Trust:** List of all the certificates between the server and the *Root Certificate*. Any certificate between the *SSL Certificate* and the *Root Certificate* is a *chain* or *intermediate certificate*. The web server needs to be configured with the proper chain, otherwise the end user will receive an error.
- **Key Escrow:** A method of storing, archiving and recovering important keys. *Escrow* involves archiving keys with a third-party for secure storage. Root CA keys require stringent access controls. Key recovery mechanisms ensure encrypted data can be accessed if keys are lost.
- **Certificate Revocation List (CRL):** A list of *digital certificates* that have been revoked by the *Certificate Authority (CA)* before their scheduled expiration date. Revoked certificates are no longer valid. Suspended certificates can be re-enabled.
- **Online Certificate Status Protocol (OCSP):** The method by which a browser can automatically check for *certificate revocation*. OCSP servers provide real-time certificate status checks. *OCSP Stapling* and *Certificate Pinning* enhance security.
 - **OCSP Stapling:** The device that holds the certificate will be the one to provide status of any revocation. *Stapling* helps maintain the privacy of the end user, as the OCSP request does not require a connection to the CRL.
 - **Certificate Pinning:** Embeds or *pins* a certificate to a service. When the application contacts the service, the service certificate will be compared to the *pinned certificate*. If the certificate matches, the application knows that it can trust the service. If the certificate doesn't match, then the application can choose to shut down, show an error message, or make the user aware of the discrepancy.
- **Certificate Troubleshooting:** Common issues include certificate expiration, misconfiguration, and trust chain problems. Ensure proper key usage settings, subject name configuration, and time/date synchronization. Regularly audit *digital certificate* infrastructure for security, compliance, and validity.
- **Host-Based Security Appliances**
 - **Antivirus/Anti-Malware:** Used to prevent, detect, and remove malware. Automated detection and removal of heuristic viruses by checking files and code that may be behaving suspiciously.
 - **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 individual hosts from malware. Firewalls are based on an *implicit deny* rule and specify which traffic should be *allowed*. This is contrary to IPSs, which are based on *implicit allow*, and specify which traffic to be *blocked*.
 - **Host-Based Intrusion Detection System (HIDS):** Monitors activity on a single computer, including process calls and information recorded in the system, application, security, and host-based firewall logs. Can pinpoint specific files compromised in an attack and also track processes employed by the attacker. It can detect anomalies on the host system that a NIDS cannot detect. For example, it can detect infections where an intruder has infiltrated a system and is controlling it remotely. HIDS are more costly to manage than NIDS because they require administrative attention on each system. HIDS cannot detect network attacks or prevent host attacks.
 - **Passive Monitoring:** Examines a copy of traffic via a *port mirror* or *network tap*.
 - **Out-of-Band Response:** Sends RESET frames to stop subsequent frames but cannot block the first frame.

- **Host-Based Intrusion Prevention System (HIPS):** Automatically detects and blocks attacks before they affect target systems. Can examine traffic for signatures, anomalies compared to the *baseline*, behaviors, or *heuristics*. Involved *machine learning*. Any IPS is based on *implicit allow*. Its rules are designed to specify types of traffic that should be *blocked*.
 - **In-Line Monitoring:** All traffic must flow through the appliance.
 - **In-Band Response:** Can monitor and block traffic on the spot.
 - **Signature-Based:** Methods that look for behavior characteristics of known attacks.
 - **Stateful Protocol Analysis:** Methods that use *Deep Packet Inspection (DPI)* to examine traffic by comparing it to a profile of how the protocol is supposed to work.
 - **Anomaly-Based:** *Heuristic* methods that look for behavior that seems unusual relative to a normal *baseline*.
- **End-Point Detection and Response (EDR) Solution:** Also called *Endpoint Threat Detection and Response (ETDR)*, or *Endpoint Protection Platform (EPP)*. Comprehensive endpoint security software, which gathers security-related behaviors from individual network hosts, and then uses the data to investigate suspicious activities and trends. Has rule-based automated response and analysis capabilities. Data collected might include processes, configuration changes, file system activity, and network connections. *Machine learning* and *process monitoring* look for and block malicious *actions* instead of *signatures*. Provides real-time *visibility*, *continuous monitoring*, and *containment*.
 - **Behavioral Heuristics/User and Entity Behavior Analytics (UEBA):** Uses *machine learning* and *data analytics* to determine *anomalous behavior* by comparing *known good behavior baselines* to the current state. Unusual behaviors generate *use*, *performance*, or *security* alerts. Also conducts *trend analysis*.
- **Endpoint Data Loss Prevention (DLP):** Prevents the sharing or transmitting of sensitive data. DLP solutions inspect all data leaving the organization, including, E-mail contents, attachments, copy to portable media, *File Transfer Protocol (FTP)*, posting to web pages and websites, applications, and *Application Programming Interfaces (APIs)*.
- **Network Access Control (NAC):** Performs a *security posture* and *health assessment* on the endpoint to determine whether it is safe to connect. Primarily a software-based, network security component that runs on or interacts with endpoints. Can be hardware-based (*802.1x: Port-Based Network Access Control (NAC)*). Listed here because it does offer host-based security analysis.
- **Unified Endpoint Management (UEM):** Manages mobile and non-mobile endpoint devices. An evolution of the *Mobile Device Manager (MDM)*.
- **Trusted Platform Module (TPM):** Hardware for individual devices that helps with cryptographic functions. Built into the motherboard of the device. Not susceptible to *Dictionary Attacks*.

- **Administrative Controls**

- **Password Policies:** Change all default usernames and passwords. Require password complexity and prevent password re-use. Activate *account lockout* and require users to change their password frequently. Consider a *minimum/maximum password age* and length.
 - **NIST Guidance:** While strict password policies seem more secure, research shows that they encourage poor password storage and writing passwords down, which ultimately decreases security. NIST recommends allowing user-selected passwords between 8 and 64 characters and avoiding complexity rules. Aging policies should not be enforced. Users should choose when to change passwords. Password hints should not be used for account recovery.
- **Separate User Accounts:** No shared or generic accounts. Restrict or disable *guest accounts* to avoid potential *privilege escalation*. Only use *privileged accounts* when necessary. Choose usernames carefully according to a standard naming convention. A username should not be easy to guess by knowing the name of a job role or the account owner. It should be easy for users to remember their names and for help desk employees to find the account of a particular user. For auditing purposes, usernames should never be changed and should be easily filtered for reports.

- **Account Limits:** Users must only have access to what is needed to perform their job duties. Conduct frequent *Groups and Permissions* audits to verify that resources are being provisioned and used correctly.
- **Patch Management:** Establish automated and scheduled *patch management*. Update firmware, applications, and OS frequently. Consider using a *trusted OS*. Test in an isolated *sandbox* or VM before deploying. Have a backup and *rollback plan* ready.
 - **Patch:** A set of changes to a program or its supporting data, designed to update, fix, or improve it.
 - **Hotfix:** A quick-fix engineering update that is a single, cumulative package, and includes information that is used to address a problem in a software product.
 - **Service Pack:** Comprises a collection of updates, fixes, or enhancements to a software program delivered in the form of a single installable package.
 - **Upgrade:** The process of replacing a product with a newer version of the same product.
 - **Maintenance Release:** A release of a product that does not add new features or content, but may solve minor problems, typically *bugs* or security issues.
 - **Definition Update:** Updates to files that are used to identify spyware and other potentially unwanted software.
 - **Unofficial Patch:** A patch for a piece of software, created by a third party such as a user community without the involvement of the original developer.
 - **Rolling Release:** Also known as *rolling update* or *continuous delivery*. Frequently delivering updates to applications.
- **User Training/ Education:** The process of educating end users about how to avoid *social engineering* and *malware attacks*. Using guided digital learning tools is one of the most popular methods.

Virtualization Security

• Logical Controls

- **Virtual Machines (VM):** Provides the functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination of the two. A computer on which a *hypervisor* runs one or more *virtual machines* is called a *host machine*, and each virtual machine is called a *guest machine*.
 - **Hypervisors:** Type of software, firmware, or hardware that creates and runs *virtual machines*.
 - **Type 1:** Also called *bare metal hypervisors*. These hypervisors directly access underlying machine resources. They implement custom resource allocation to service the VMs.
 - **Type 2:** Also called a *hosted hypervisor*. These hypervisors negotiate resource allocation with the operating system, which makes the process slower and less efficient.
 - **Virtual Network Interface Cards (VNICs):** A software-based NIC that allows a VM to join a network. They have a MAC address, IP address, and all other functions of a real card, except instead of sending and receiving physical signals, all of its traffic passes through the *hypervisor*. Multiple VNICs can correspond to one physical NIC. VNICs allow the hypervisor to behave as a virtual switch, router, firewall or NAT. Since routers and firewalls are essentially network hosts themselves, users could install one as a VM. Many firewall and router vendors offer virtual versions of their products.
 - **Benefits of Virtualization**
 - **Snapshots:** Easily create a *snapshot* of a VM, a *read-only* copy of the disk file and configuration information, much like a *system image* or a *restore point* on a physical host. By creating a snapshot before risky activities or updates, users can quickly *roll back* if needed.
 - **Security Control Testing:** Virtual test environments are an ideal place to thoroughly test security protocols before deploying them on the real network.
 - **Patch Compatibility:** A test VM is useful for testing any operating system or application patches to make sure they don't introduce any problems.
 - **Host Availability and Elasticity:** Easily maintain *High Availability (HA)* for services hosted on a VM by transferring the VM if the physical host has problems or needs maintenance. Easily provide *elasticity* by changing the resources allocated to the VM based on its load. Copy it to create *redundant* systems for *load balancing*.

- **Sheep Dip:** The process of using a dedicated device to test inbound files on removable media for viruses before they are allowed to be used with other computers.
- **Other VM Technologies**
 - **Thin Clients:** Optimized for establishing a remote connection with a server-based computing environment. Relies on a network connection for computing and processes very little on the actual hardware. *Thin clients* connect to VMs stored on company servers. Can use VMs to provision corporate desktops, effectively replacing traditional desktop computers.
 - **Thick Clients:** Systems that connect to servers even without a network. They do not rely on server applications since they can process, store, and manage data independently.
 - **Containers:** Instead of a *bare metal* or a *hosted hypervisor*, the host operating system runs a *container service* that can host multiple containers. Like a VM, a *container* is isolated from other containers on the same computer. It can also perform relatively low-level operating system tasks, such as defining its file system. Unlike a VM, *containers* do not have a *guest operating system*. Instead, it shares the *kernel* of the host operating system. Containers are somewhat less flexible than VMs, but they consume fewer resources and can be deployed more quickly. Containers have similar security concerns as any other application deployment method, such as bugs, insufficient security controls, or misconfigurations. Use container-specific operating systems, which are minimal and designed specifically for containers. Group container types on the same host by purpose, sensitivity, and threat posture. This limits the scope of any potential intrusion.
 - **Storage Segmentation:** Separates the information on a device into partitions.
 - **Sandboxes:** Can be used as a test environment for code execution, patches, updates, rollback planning, *quarantining*, segmentation during *Incident Response*, or *reverse-engineering* malware.
 - **Virtual Desktop Infrastructure (VDI)/ Virtual Mobile Infrastructure (VMI):** A virtual desktop that allows users to access their desktop from a mobile endpoint. Applications and data are managed externally from the device, on a separate server, or in the cloud. Minimizes risk from device loss. Uses virtual machines to provision corporate desktops, replacing traditional desktop computers.
 - **Non-Persistent VDI:** The central server only stores one *master image* or *golden image* of a fully configured computer. Whenever a user logs in, the server starts a VM based on that master image, but it doesn't directly change any of its files or settings. All changes are applied to a temporary copy or file system instead. When the user logs out, all of the temporary data is deleted. When a user logs back in, or when different users log in simultaneously, they each receive a new, generic VM. Saves on storage space and also makes it easy to apply updates for configuration changes. Prevents users from making changes that will cause security risks. Works best for users that only need standard workstations without customization. They do not work very well for users who have unique configurations or software needs.
 - **Application Layering:** A given user can have a customized VM that includes all the applications assorted with their user profile, without the server needing a separate *master image* for each unique combination of installed applications.
- **VM Security**
 - **Virtual Machine Life Cycle Management (VMLM) Software:** A set of processes that help oversee the implementation, delivery, operation, and decommissioning of VMs.
 - **Virtual/ Cloud Firewall:** A software-based security device or service that monitors and filters network traffic for *Virtual Machines (VMs)* and virtualized environments. Provides valuable East/West network security.
 - **Network Segmentation:** Allows administrators to isolate network traffic and organize resources. Virtual networks use *subnets*, *security groups*, routing, and firewall rules to manage network communications within and between segments.

- **Role-Based Access Control:** Allows administrators to grant access to users based on their role, authorization, and permissions. This can help delegate administrative controls across a company, allowing different users to access different parts of the environment.
- **Just-in-Time (JIT) VM Access:** Limits inbound traffic to VMs, reducing exposure to attacks.
- **Administrative Controls**
 - **VM Policies and Procedures:** Enforced to help secure *Virtual Machines (VMs)*.
 - **Patching and Updates:** Keeping VMs current with the latest patches and updates for their operating systems and applications can help avoid vulnerabilities and exploits.
 - **Deactivate Unnecessary Functionality:** Deactivating features that are used infrequently can help minimize potential points of attack.
 - **VM Life Cycle Management:** This includes restricting storage of VM images and snapshots, using backup and failover systems, tagging VMs based on their sensitivity or risk level, and creating a formal change management process for VM images.
 - **Monitor Resource Utilization:** Deploying monitoring tools to track resource usage across VMs can help identify underutilized or overprovisioned VMs.
 - **Use Separate Management APIs:** Isolating service from infrastructure management and orchestration can help protect the network.

Mobile Security

- **Logical Controls**
 - **Carrier Locking/ Unlocking:** In the *locked* state, only the SIM card of a specific carrier will work. In the *unlocked* state, the device has no carrier restrictions, and any SIM card will work.
 - **Mobile Device Management:** A proven methodology and toolset used to provide workforce mobile productivity tools and applications, while keeping corporate data secure.
 - **Mobile Device Management (MDM):** Centralized management of mobile devices. Can implement screen locks, *account lockout*, *patch management*, *Over-the-Air (OTA)* updates, and *remote wipe*.
 - **Mobile Application Management (MAM):** Allows provisioning and access control for approved enterprise apps. Has features for app delivery, configuration management, authentication, access control, *push notifications*, and reporting. Creates an enterprise-approved application catalog to choose from. Can also *remotely wipe* application data.
 - **Mobile Content Management (MCM):** Delivers centrally hosted data and services to mobile devices, allowing device-specific formatting and security controls. Features include data encryption, secure connection to web applications, and DLP rules.
 - **Mobile Identity Management (MIM):** Centralized *Identity and Access Management (IAM)* for mobile devices. Features include *Single Sign-On (SSO)*, certificate management, and device enrollment.
 - **Enterprise Mobility Management (EMM):** An evolution of MDM, with MAM, MCM, and MIM. Popular in BYOD environments. Detects *rooted/jailbroken* devices to help protect enterprise data.
 - **Unified Endpoint Management (UEM):** A further evolution of EMM, which provides central management of all endpoints from a single platform. In addition to mobile devices, it supports desktops, printers, and IoT devices. Can detect rooted/jailbroken devices to protect enterprise data.
 - **Virtual Desktop Infrastructure (VDI)/ Virtual Mobile Infrastructure (VMI):** A virtual desktop that allows users to access their desktop from a mobile device. Apps and data are managed and stored externally from the device, in the cloud. Minimizes risk from device loss. Managed from a single platform, like a *remote desktop*. Works best for Android devices.
 - **SEAndroid:** Security enhancements for Android devices. Considered a *Trusted OS*.
 - **MicroSD HSM:** Provides security services for mobile devices, such as encryption, key generation, digital signatures, authentication, and secure storage. Works well to securely store cryptocurrency.
 - **Lightweight Cryptography:** Field of study in the pursuit of developing more powerful tools and algorithms that use less computer power and resources.

- **Elliptical Curve Cryptography (ECC):** Math based on calculating the properties of curves, instead of prime numbers. Uses a smaller key size and curve algorithms to secure data. Lower CPU usage. Stronger security with much shorter keys than other asymmetric algorithms. Perfect for mobile and portable devices.
- **Administrative Controls**
 - **Corporate Device Deployment Models**
 - *Corporate Owned, Business Only (COBO).*
 - *Corporate Owned, Personally Enabled (COPE).*
 - *Choose Your Own Device (CYOD).*
 - *Bring Your Own Device (BYOD).*
 - *Virtual Desktop Infrastructure (VDI)/ Virtual Mobile Infrastructure (VMI).*
 - **Mobile Device Management Policies:** Logical controls enforced by administrative policies.
 - **Acceptable Use Policies:** Set policies on apps, data, camera usage, etc.
 - **Application Management:** Block the use of apps that have not been expressly approved.
 - **Screen Locks:** Set policies for auto-locking mobile devices.
 - **Passcode/PIN Requirements:** Implements *Screen Locks* and PINs, as well as a *Screen Lockout* after too many failed login attempts. May require *Biometrics*, and/or *Multi-Factor Authentication (MFA)*.
 - **Authentication:** Allow or disallow the use of *Biometrics* for authentication, and manage *Context-Aware Authentication*, which takes additional factors into account, like location.
 - **Data Management:** Set policies for data backups, encryption, and *remote wipe*.
 - **Over the Air (OTA) Firmware Updates:** Push required firmware/OS updates and patches.
 - **Geolocation/ Geofencing:** A virtual perimeter for a geographic area. Can disable or enable location, geotagging, camera, microphone, and recording devices, depending on location. Helps with DLP.
 - **Data Loss Prevention (DLP):** Can disable the ability to plug-in or read external storage devices, such as flash drives, SD cards, USBs, or *USB On-the-Go* devices.

Web Security

- **Logical Controls**
 - **HTTPS:** The primary protocol for sending data between a website and a browser. HTTPS uses encryption to secure data transfer, making it important for transmitting sensitive data like login credentials, banking information, and credit card numbers. Protects users from *Eavesdropping*, *Man-in-the-Middle (MitM)*, *Domain Name System (DNS) Spoofing*, and *transaction tampering*.
 - **Captchas:** A type of challenge-response test used to determine whether the user is human, to deter bot attacks and spam.
 - **Secure Cookies:** An HTTP cookie that sets a *Secure* attribute. Limits a search to secure channels only.
 - **Web Application Firewalls (WAF)/ Application Layer Firewalls:** An *Application-Layer* firewall that filters, monitors, and blocks HTTP traffic to and from a web service. It monitors all traffic, encrypted or not, for malicious behaviors, before passing commands to a web server. External traffic is filtered by a traditional or *Next Generation Firewall (NGFW)* first. May take actions such as *alerting*, *blocking*, *re-routing*, or *logging*. Protects web servers and back-end databases from *code injection* and *Denial of Service (DoS)* attacks. Uses *application-aware* processing rules and *pattern-matching* to filter traffic and detect threats. Includes *Deep Packet Inspection*. Can be deployed as a hardware appliance or plug-in software on a host/web server. Firewalls are based on *implicit deny* and must specify which traffic will be *allowed*.
 - **Secure Web Gateways (SWG):** A software application, hardware device, or cloud service 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 Monitoring*, and VPN endpoints. *Next-Gen Firewalls (NGFW)* perform these functions as well.

- **Content Filters/Web Filters/URL Filters:** Control the content users can access over the Internet. Can be hardware, software, or on a firewall. Issues include *over-blocking*, *under-blocking*, handling of encrypted traffic and privacy concerns.
- **DNS Filters:** Restrict web content.
- **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. An example of *Zero Trust* being applied to websites.
- **Administrative Controls**
 - **Access Control Management:** Administrators manage access controls based on an organization's security policies. For example, restricting access to only approved IP addresses.
 - **Web Security Awareness Training:** Implementing an educational program to improve cybersecurity awareness and skills among all users.
 - **Information Privacy Policies:** Also known as *data privacy*, this is the ability to control how personal information is accessed, stored, and used. This includes information like names, addresses, contact information, and online behavior. It also includes the right to consent to the collection, disclosure, and use of data, and to ensure that data is accurate and current. *Information privacy* is important because it protects individuals from criminals who may use their personal data for fraud or harassment, or from entities that may sell their data to advertisers without their consent.

Application Security

- **Logical Controls**
 - **Quality Assurance (QA):** Logical controls/procedures for the secure development of applications.
 - **Dynamic Analysis:** Testing and evaluating a program, while the software is running.
 - **Fuzzing:** Also called *Fault Injection*, *Robustness Testing*, *Syntax Testing* or *Negative Testing*. Used to test for *code injection*, errors, and other exploits.
 - **Protocol Fuzzing:** Send modified, replayed, or nonstandard packets to an application.
 - **Application Fuzzing:** Tests input/output functions of the application.
 - **File Format Fuzzing:** Creates and saves randomly formatted file samples to be opened and parsed by an application.
 - **Stored Procedures:** SQL queries that execute server-side instead of on the client side of the application. The client application calls the *stored procedure* on the server. This prevents the client from making any changes to the actual SQL queries.
 - **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.
 - **Output Encoding:** Translating special characters into a different but equivalent form that is no longer dangerous to the target interpreter.
 - **Error Handling:** Creating meaningful *error messages* for the user, useful diagnostic information to the site maintainers, but no other useful information to an attacker.
 - **Escaping:** Adding a special character to avoid misinterpretation. For example, adding a \ character before a " character so that it is interpreted as text and not as closing a string.
 - **Data Execution Prevention (DEP):** Memory regions are marked as non-executable, preventing code from being executed. This protects against *memory abuse* attacks, such as *Buffer Overflows*.
 - **Static Application Security Testing (SAST):** *Static code analyzer* that identifies security flaws.
 - **Code Signing:** The process of digitally signing executables and scripts, to confirm the software author and guarantee that the code has not been altered or corrupted. The encryption is *asymmetric*, where a trusted CA signs the developer's *public key*, and the developer signs the code with their *private key*. The process also employs the use of a *cryptographic hash* to validate *authenticity* and *integrity*.

- **Web Application Firewall (WAF)/ Application Layer Firewalls:** An *Application-Layer* firewall that filters, monitors, and blocks HTTP traffic to and from a web service. Includes *Deep Packet Inspection*. May take actions such as *alerting*, *blocking*, *re-routing*, or *logging*. Uses *application-aware* processing rules and pattern-matching to filter traffic and detect threats. Can apply rules to API communication to help prevent *API Injection*. Can be deployed as an appliance or plug-in software.
- **Allow Lists and Deny Lists:** The OS allows or disallows applications from running or being installed.
- **Cryptographic Obfuscation:** Taking something that is normally understandable and making it very difficult to understand. Many developers will *obfuscate* their code to prevent others from following the logic used in the application. Protects code from *reverse engineering*. Used by *malware* to hide itself from scanners.
- **Compilers:** Source code to binary for a computer-readable format.
- **De-Compilers:** Binary back to source code.
- **Administrative Controls**
 - **Application Development Models**
 - **DevOps:** Focused on increasing the speed and quality of software development and delivery.
 - **DevSecOps:** Integrates security early and throughout the *Software Development Life Cycle*. Developers and operations teams work together.
 - **Secure Deployment Policies**
 - **Harden the Underlying Host and Network:** Ensure the host is kept updated. Disable unnecessary applications, services, and user accounts. Apply antivirus and HIDS/HIPS software on the host. Protect the network with firewalls, NIDS/NIPS, or a *Web Application Firewall (WAF)*. If the application uses multiple servers, make sure all of them are suitably hardened.
 - **Securely Configure the Application:** Choose securely coded applications using secure protocols. Make sure that the app components and users operate in a *least privilege* environment. Apply secure *client-side validation* features. Apply special protections against likely attack vectors.
 - **Thoroughly Test the Application Before Deployment:** Use a combination of human testing and *fuzzing* techniques. For critical applications, consider outside *security audits* or *penetration tests*.
 - **Maintain the Deployed Application Security Over Time:** Use rigorous patch management to update software without introducing new vulnerabilities. Conduct regular *security audits*. Educate users to prevent attacks that rely on *social engineering*. Be aware of evolving network application threats.

Data Security

- **Logical Controls**
 - **Windows Group Policy Tool:** Puts users into *groups* and grants privileges based on job function. Enforces password policies, sets firewall rules, blocks access to folders or network shares, and restricts the use of desktop features, like *task manager*. Includes manual and automated reviews of *Identities* and *Access*. Windows has two types of permissions that restrict access: *NTFS Permissions* and *Share Permissions*.
 - **NTFS Permissions:** Apply to every file and folder stored on a volume formatted with the NTFS file system. Permissions are inherited from a *Root Folder* to the files and subfolders beneath it by default, but this can be disabled.
 - **Basic Permissions:** A simpler way to set permissions. Each *basic permission* maps to one or more *advanced permissions*.
 - **Advanced Permissions:** Also known as *special permissions*. More granular settings that divide *basic permission* levels.
 - **Share Permissions:** Apply only to shared folders. Takes effect when a folder is accessed from a remote system. There are three types of *share permissions*: *Full Control*, *Change*, and *Read*.
 - **Full Control:** Allows *Users* *Read*, *Change*, and *Edit* permissions, and file *Ownership*.
 - **Change:** Allows *Users* to *Read*, *Execute*, *Write* and *Delete* folders and files within a share.
 - **Read:** Allows *Users* to *View* the folders contents, including folder and subfolder names, file data, and programs contained in the folder.

- **Linux File Permissions:** Each object in a file system has an *Access Control List (ACL)*, which contains lists of allowed accounts and permissions. **chmod:** Sets or modifies permissions using *Symbolic* or *Absolute* mode.
 - **Symbolic Mode:** Uses letters and symbols to add or remove permissions. For example, **u+x** gives the *Owner* permission to *Execute*. *Symbolic mode* is good for small modifications, like adding *Execute* permissions to files that already have *Read* permissions. Use commas to separate symbolic modes. *Read* (r), *Write* (w), and *Execute* (x) can be applied to *Owner/User* (u), *Group* (g), and *Others* (o). Also includes *No Permissions* (-). Math operators include + to *add* permissions, - to *remove* permissions, and = to give *no access*.
 - **Examples of Symbolic Permissions**
 - **u+r:** Grants the *User Read* permission.
 - **g+rw:** Grants the *Group Read* and *Write* permissions.
 - **o-rw:** Removes *Read* and *Write* permission from *Others*.
 - **rw-r--:** *Users* can *Read* and *Write*, while *Groups* and *Others* can *Read*.
 - **Absolute Mode:** Uses numeric *octal values* to represent permissions levels. For example, 6 gives *Read* and *Write*, but not *Execute* access. *Absolute mode* is good for large modifications, like removing all *World* and *Group* permissions. The sum of the values is added in a specific order: *User*, then *Group*, then *Others*.
 - **Examples of Absolute Permissions**
 - **chmod 700:** Removes all permissions for the *Group* and *World*.
 - **chmod 701:** Gives the *Owner* all permissions and *World Execute permissions*.
 - **chmod 705:** Gives the *Owner* all permissions and *World Read* and *Execute*.
 - **chmod 640:** Gives the *Owner Read* and *Write* permission, members of the *Group Read* permissions, and no permissions for anyone else.

#	Permission	r	w	x
7	Read, Write, and Execute	r	w	x
6	Read and Write	r	w	-
5	Read and Execute	r	-	x
4	Read only	r	-	-
3	Write and Execute	-	w	x
2	Write only	-	w	-
1	Execute only	-	-	x
0	none	-	-	-

- **Cryptography:** The study and practice of techniques that help secure data and communication in the presence of adversarial behavior.
 - **Cryptographic Concepts**
 - **Plaintext:** Readable text before it is *encrypted* into *ciphertext*, or after it is *decrypted*.
 - **Ciphertext:** The result of using an encryption algorithm or *cipher*, on plaintext.
 - **Confusion:** Encrypted data made to be drastically different from the *plaintext*, making the mathematical relationship between the *plaintext* and *keys* as complex as possible.
 - **Diffusion:** Changing one character of the input will cause many characters to change in the output. Breaking up patterns in the *plaintext* so they won't be at all apparent in the *ciphertext*. Known contents won't be useful in decoding the ciphertext.
 - **Cryptographic Obfuscation:** Taking something that is normally understandable and making it very difficult to understand. Many developers will *obfuscate* their code to prevent others from following the logic used in the application. Protects code from those who would try to *reverse engineer* it. Sometimes used by *malware* to hide itself from scanners.

- **Cryptographic Agility:** The capability of an organization to quickly and efficiently switch between cryptographic algorithms without disrupting existing systems. Ensures that an organization can adapt to new cryptographic standards as threats evolve or new vulnerabilities are discovered.
- **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. An example of *Security Through Obscurity*. Not innately secure, but harder to see.
- **Cryptographic 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 *asymmetrically* encrypting files. It was one of the first freely available forms of *public-key cryptography* software. Perfect for lower-budget cryptography needs. Uses a peer-to-peer, *web of trust* model for E-mail security.
 - **GNU Privacy Guard (GPG):** A free, open-source version of PGP that provides equivalent encryption and authentication services.
 - **Secure Socket Layer (SSL):** A security protocol that provides privacy, authentication, and integrity to Internet communications. Certificate-based authentication that performs a key exchange to set up symmetrically encrypted communication sessions that last until one side breaks the connection. Can also perform *two-way authentication*, where both the client and server must have a certificate to present to the other.
 - **Transport Layer Security (TLS):** SSL eventually evolved into *Transport Layer Security (TLS)*. It works with HTTP to route encrypted web traffic. TLS employs *symmetric encryption* for the data and a *public key* for confirming the system's identity. Data includes a *Message Authentication Code (MAC)* to prevent alteration during transmission or MitM attacks. In addition, TLS has restrictions that curb *replay attacks*.
 - **Datagram Transport Layer Security (DTLS):** A secure communication protocol, that is designed to employ only UDP packets. It is sometimes known as *UDP TLS*. Because UDP is a *connectionless* protocol, DTLS is faster, and it does not suffer the performance problems of other stream-based protocols. DTLS is based on SSL/TLS, and it provides similar security protections. This makes it favorable to use for VPN software.
- **Early Ciphers**
 - **Transposition Ciphers:** Scrambles the positions of characters without changing the characters themselves.
 - **Rail Fence/ Zigzag:** The plaintext is written downwards or 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.
 - **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 with 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:** Replace 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, called 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.
- **Modern Ciphers**
 - **Stream Ciphers:** A symmetric cipher where plaintext digits are combined with a pseudorandom cipher digit stream. Each plaintext digit is encrypted one at a time. Examples: **RC-4**, **Salsa**, and **SEAL**. The most widely used *stream cipher* is **RC-4**. Mainly used for *symmetric encryption*. High speed and low hardware complexity. The key is often combined with an *Initialization Vector (IV)*, so the starting state is never the same twice.
 - **Block Ciphers:** A deterministic algorithm that operates on fixed-length groups of bits, called *blocks*. Examples: **AES**, **DES**, **3DES**, **Twofish** and **Blowfish**. The most widely used *block cipher* is **AES**. While the block size is a fixed size, not all data matches the block size perfectly. Some modes require *padding* before encrypting. Each block is encrypted and decrypted independently. Mainly used for *symmetric encryption*.
 - **Block Cipher Modes:** Additional algorithms called *modes of operation* can be used to change how the key is applied to successive blocks. Defines the method of encryption. May provide a method of authentication. Available modes depend on the encryption protocol used. Helps to avoid patterns in the encryption output.
 - **Electronic CodeBook Mode (ECB):** Applies the key the same way to each block. It is sufficient for a single block but provides little security for longer messages. Simplest cipher mode and not recommended.
 - **Cipher Block Chaining Mode (CBC):** Performs an *XOR operation* on each block of plaintext using the previous block of ciphertext, then encrypts it with the key. A corrupted block will prevent the decryption of the subsequent block, but not the following blocks. Symmetric and uses an *Initialization Vector (IV)* for randomization. Encryption that is dependent on the block before it. Slower than other modes.
 - **Exclusive OR (XOR):** A mathematical operation that's a part of all symmetric operations. Done by comparing bits of plaintext and a key (same= 0, different= 1). Can be reversed to get the plaintext back.
 - **Cipher FeedBack Mode (CFB):** For each block, the key stream is modified using an XOR of the previous ciphertext, making sure it's always different. CFB makes it easy to encrypt a stream of values smaller than the standard block.
 - **Output FeedBack Mode (OFB):** Like CFB, but the keystream is generated independently of the previous ciphertext. Chaining still happens, but only after the key is applied to the plaintext. It is better able to correct errors in transmitted ciphertext, but it still can't correct for missing or added bits.
 - **Counter Mode (CTR):** A stream cipher mode where each block encryption uses a successively incremental counter. Converts blocks into streams. Uses an *Initialization Vector (IV)*. Its main benefit is performance. It has low overhead and is well suited to parallelization during encryption and decryption. Widely used.
 - **Galois Counter Mode (GCM):** An authenticated mode that combines *Counter Mode* with a hash-based *Galois* authentication code. Provides data authenticity and integrity. Used for hashes and *packetized* data as well. Minimal latency and operational overhead. Widely used.
 - **Offset Codebook Mode (OCB):** An authenticated encryption mode that applies a *Message Authentication Code (MAC)* and encryption in a single pass. OCB has very high performance and is easier to implement than GCM, but it is under patent protection, which has limitations.
- **Data Encryption:** Protects confidentiality of data by scrambling it and making it unreadable to humans. The *encryption key* is stored in a file and can decrypt the *ciphertext* back into *plaintext*.
- **Categories of Encryption**
 - **Transport Encryption:** Protect *data in transit*, such as that being sent over the network.

- **Storage Encryption:** Protects *data at rest*, on some sort of persistent storage medium.
- **Memory Encryption:** Protects *data in use*, such as RAM data or data that is being processed. *Memory Encryption* is challenging to implement without hurting performance and interoperability, but it is increasingly desirable to organizations with strict security needs.
- **Homomorphic Encryption:** Conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form. Perform research, work, or calculations on the data without viewing the data. Uses a *public key* and is more secure than traditional encryption. Decrypted data can only be viewed with the *private key*.
- **Symmetric Encryption:** Uses a single, shared key. Also called *Private/Secret/Session Key Cryptography*. Faster than *asymmetric encryption* but is considered less secure. Efficient enough to handle bulk data encryption, but not secure enough to be used for *secure key exchange*.
 - **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. It is widely used, typically with 128-bit, 192-bit or 256-bit keys, the latter of which is considered strong enough to protect *Top-Secret* military data. 128-bits is strong enough for most other uses. No known cryptographic weaknesses. This is the encryption standard used by WPA2.
 - **Twofish:** A symmetric block cipher with a 128-bit, 192-bit, or 256-bit key size. Uses a very complex key structure with 128-bit blocks. No known cryptographic weaknesses. Not limited by patents. As good as AES.
 - **Blowfish:** A variable-length, symmetric, 64-bit block cipher, with a maximum key size of 448 bits. Not limited by patents.
 - **Data Encryption Standard (DES):** A symmetric-key block cipher. Its short key length of 56-bits makes it too unsecure for modern applications. Was common until replaced by AES. The block size is 64 bit. It can be easily *brute forced*.
 - **Triple Data Encryption Standard (3DES):** A symmetric block cipher, which applies DES three times to each block. Has an optional mode where a decryption operation is applied in the middle of its procedures. Block size is 64-bit. Key sizes are 112-bit or 168-bit. Considered a secure upgrade over DES, although not widely used.
 - **RC-4:** A symmetric algorithm that was part of the original WEP standard with SSL. Removed in the next implementation. Key sizes between 40-bits and 2048-bits. Considered deprecated due to biased output.
- **Asymmetric Encryption:** Each user has a *public key* and a *private key*. Also called *Public Key Cryptography*. Sessions are encrypted with the recipient's *public key* and decrypted with their *private key*. Allows for non-repudiation of origin and delivery, access control, and data integrity. More secure than *symmetric encryption*, but slower, with more cryptographic processing overhead. It is mathematically intensive, and impractical for everyday use or encrypting large amounts of data. For that purpose, *symmetric encryption* is more efficient. *Asymmetric encryption* is more often used for *secure key exchange*, *digital certificates*, and *sharing public keys*.
 - **Algorithms**
 - **Rivest, Shamir, and Adleman (RSA):** A type of asymmetric encryption, which uses two different, but linked *keys*. In RSA, both the *public* and the *private keys* can encrypt a message. The opposite key from the one used to *encrypt* is used to *decrypt*. This was the first practical use of *public key cryptography*. It uses large prime numbers as a basis for encryption. 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 involves two keys: A *private key* owned by the sender and a *public key* held by the receiver.

- **Elliptic Curve Digital Signature Algorithm (ECDSA):** Offers a variant of the *Digital Signature Algorithm (DSA)*, using *Elliptical-Curve Cryptography (ECC)*.
 - **Elliptical Curve Cryptography (ECC):** Uses math based on the difficulties of calculating properties of curves, instead of prime numbers. Use smaller key sizes and curve algorithms to secure data. Lower CPU usage. Stronger security with much shorter keys than other asymmetric algorithms. It is much faster than RSA and DSA. Perfect for mobile and portable devices.
 - **Diffie-Hellman (Key) Exchange (DH/DHE):** An asymmetric standard for exchanging keys. Primarily used to send *private keys* over a public, unsecured network. Allows two parties that have no prior knowledge of each other, to jointly establish a *shared secret key* over an unsecure channel.
 - **Diffie-Hellman (DH) Groups:** Determines the strength of the key used in the *key exchange* process. Higher group numbers are more secure but require additional time to compute the key.
 - **Diffie Hellman Ephemeral (DHE):** A DH *key exchange* with different keys.
 - **Elliptical Curve Diffie-Hellman Ephemeral (ECDHE):** A key agreement protocol that allows two parties, each having an *elliptical curve public-private key pair*, to establish a shared secret over an unsecure channel.
 - **ElGamal:** An asymmetric algorithm for *public-key cryptography*, based on *Diffie-Hellman key exchange*. It is probabilistic, meaning that a single plaintext can be encrypted into many possible ciphertexts.
- **Disk Encryption:** A technology that protects information by converting it into code that cannot be deciphered easily by unauthorized people or processes.
 - **Full Disk Encryption (FDE):** Encrypts the entire storage device, including metadata, via *BitLocker* or *FileVault* software. FDE keys are securely stored in the TPM or on a USB drive.
 - **Self-Encrypting Drive (SED):** Hardware-based full-disk encryption based on the *Opal Storage Standard*. Built-in encryption mitigates the performance issues of FDE.
 - **Partition-Based Encryption:** Allows selective encryption for different partitions.
 - **Master Symmetric Key:** A symmetric key that protects other keys, such as *session keys*. Also protects *Hard Disk Drive (HDD)* data when *whole drive encryption* is implemented.
 - **Recovery Agent:** In the case of file encryption, the role of the *recovery agent* is to give a copy of the recovered file back to the user in plaintext.
- **Blockchain Technology:** An advanced database mechanism that allows transparent information sharing within a network. Stores data in *blocks* that are linked together in a *chain*. Each block is linked by *hashing*.
 - **Public Ledger:** Peer-to-peer transactions are public and cannot be deleted or reversed because to do so would invalidate the hash.
- **Hashing:** The process of transforming any given key or a string of characters into another value. The hash cannot be turned back into the original data but can be compared to the data to verify its integrity and or authenticity. Also useful for generating keys from passwords created by humans.
 - **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* or piece of data that helps check for unaltered copies of that data.
 - **Salt/Pepper:** A *pepper* is similar to a *salt*, a random bit of data that is 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 hard coded into source code.
 - **Key Stretching:** An *algorithm* that increases key length through multiple iterations. Hashing a password and then hashing that hashed value protects a weak password from brute-force attacks.
 - **Bcrypt:** Protects passwords by repeating the *Blowfish cipher*.

- **Password-Based Key Derivation Function 2 (PBKDF2):** Applying the *RSA* function to passwords to create a stronger key.
- **Hash Table:** A data structure for stored hashes that allows for searching and organizing large amounts of data, such as recognizing duplicate files stored in different folders. *Identity hashing* is used for source code management systems, file-sharing networks, and image databases.
- **Password Hash Storage:** Many password databases only store the hash, not the plaintext password. When a user enters a password, it is hashed and compared to the stored hash in the database.
- **Hashing Algorithms**
 - **Message Digest (Algorithm) 5 (MD5):** A widely used hash function producing ONLY a 128-bit hash value. Has collisions. Do not use.
 - **Secure Hash Algorithm (SHA-1):** Produces ONLY 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.
 - **Hash-Based Message Authentication Code (HMAC):** A hashing algorithm combined with a symmetric key. Provides data integrity and authenticity. Faster than asymmetric encryption.
 - **RACE Integrity Primitives Evaluation Message Digest (RIPEMD):** It is based on MD. Collisions were found, but with security improvements and additional functions to produce hashes between 128-320 bits, it is more secure now. The most popular is RIPEMD-160, which is similar to SHA-1 in performance, but has fewer known flaws.
- **Redundant Data Storage:** Remove *single points of failure* and create *fault tolerance*.
 - **Multi-Pathing:** Connections allowing multiple paths between two points, so that an interruption or failure of one won't interrupt service. Most often used in *Fiber Channel SANs* and other storage solutions, which use them to increase both *reliability* and performance.
 - **Load-Balancing:** Spreads traffic load across multiple servers or databases so that a server failure won't interrupt service. Provides *fault-tolerance* and *redundancy*.
 - **Clustering:** Multiple servers in a cluster supply redundant resources, are aware of each other, and work toward a common goal. Clusters can dynamically reallocate duties when individual servers fail.
 - **Virtualization:** Virtual and cloud systems make it much easier to quickly deploy new copies of existing systems. Beyond recovery from failure, it also includes *elasticity* to meet transient surges in demand, and *scalability* to meet long-term growth.
 - **Geographic Dispersal:** Large organizations maintain multiple facilities for the sake of redundancy. If a disaster impairs or disables one site, others can pick up the slack until service is restored. Also adds *fault tolerance*.
 - **Data Replication:** Maintains exact copies of data at multiple locations, providing *redundancy* and ensuring data *availability* in the case of disasters.
 - **Synchronous Replication:** Writes data to all replicas simultaneously.
 - **Asynchronous Replication:** Copies data to replicas at scheduled intervals.
 - **Redundant Array of Independent/ Inexpensive Disks (RAID):** A data storage virtualization technology that combines multiple physical drive components into one or more logical units for data redundancy, performance improvement, or both.
 - **Striping:** The technique of segmenting logically sequential data, so that consecutive segments are stored on different physical storage devices. Striping is useful when a processing device requests data more quickly than a single storage device can provide it.
 - **Parity:** A calculated value that's used to restore data from information found on the other drives, if a drive fails.
 - **Mirroring:** The replication of logical disk volumes onto separate physical hard disks in real-time to ensure *continuous availability*.

RAID 0	Striping. Splits data into blocks that get written across all drives in an array. Uses all storage capacity with no overhead. <u>NOT redundant</u> . No <i>mirroring</i> , and no <i>parity</i> . Loss of any disk will cause complete data loss.
RAID 1	Mirroring. Two drives that contain the exact same data. No <i>striping</i> or <i>parity</i> . Slower write speed but provides redundancy if one drive fails. Uses only 50% of available disk space because saved data is duplicated on a second disk. This does not minimize disk space utilization compared to RAID 5.
RAID 5	Striping with Parity. No <i>mirroring</i> . Requires at least three drives. Rights data evenly across disks in a striped set. Error recovery information is distributed across disks, such that a failure of a single hard drive can be tolerated. If a drive fails, data is recovered using parity. Requires less storage space and is more cost effective compared to RAID 1. High read speeds and fault tolerance.
RAID 6	Striping with Dual Parity. Similar to RAID 5, but parity data is written to two drives. Requires at least four drives and can withstand two drive failures.
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.

RAID LEVEL	METHOD	HARDWARE / SOFTWARE	MINIMUM # OF DISKS	COMMON USAGE	PROS	CONS
JBOD	SPANNING		2	INCREASE CAPACITY	COST-EFFECTIVE STORAGE	NO PERFORMANCE OR SECURITY BENEFITS
0	STRIPING		2	HEAVY READ OPERATIONS	HIGH PERFORMANCE (SPEED)	DATA IS LOST IF ONE DISK FAILS
1	MIRRORING		2	STANDARD APP SERVERS	FAULT TOLERANCE, HIGH READ PERFORMANCE	LAG FOR WRITE OPS, REDUCED STORAGE (BY 1/2)
5	STRIPING & PARITY		3	NORMAL FILE STORAGE & APP SERVERS	SPEED + FAULT TOLERANCE	LAG FOR WRITE OPS, REDUCED STORAGE (BY 1/3)
6	STRIPING & DOUBLE PARITY		4	LARGE FILE STORAGE & APP SERVERS	EXTRA LEVEL OF REDUNDANCY, HIGH READ PERFORMANCE	LOW WRITE PERFORMANCE, REDUCED STORAGE (BY 2/5)
10 (1+0)	STRIPING & MIRRORING		4	HIGHLY UTILIZED DATABASE SERVERS	WRITE PERFORMANCE + STRONG FAULT TOLERANCE	REDUCED STORAGE (1/2), LIMITED SCALABILITY

○ Data Backups

- **3-2-1 Rule:** 3 copies of data, across 2 media types, with one offline and one off-site.
- **Backup Types**
 - **Online:** Instant availability, but vulnerable to *ransomware* and other attacks.
 - **Offline:** A manual connection is required. Better security, but less convenient.
 - **Full Backup:** A complete copy of data assets. 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 requires the last *full backup* plus all the *incremental backups* that took place up 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.
 - **Image:** A full backup of an entire system, allowing it to be restored to full operation from a bare metal state. Images are especially popular for freshly configured servers and workstations and are valuable for horizontal scaling and non-persistence.

- **Snapshot:** A type of backup used to quickly capture the state of a system at a given point, with limited impact on ongoing operations. Snapshots make a virtual copy of the active system and then back up that copy. The backups can be *full*, *incremental*, or *differential*. Popular for VMs or *High Availability (HA)* databases.
- **Replication:** Create redundant copies of data for availability and recovery. Enhances data protection across multiple locations and systems.
 - **Remote Journaling:** A data replication method that copies journal or transaction logs from one system to another, often to a separate location.
 - **SAN Replication:** A data protection technique that copies data from one device on a *Storage Area Network (SAN)* to another.
 - **VM Replication:** A process that creates a copy, or replica, of a VM and keeps it in sync with the original. The replicas are stored in a *powered-off* state, so they don't use compute resources. If the original VM's data is lost or corrupted, the replica can be used to restore the machine.
- **Backup Utilities**
 - **Backup and Restore:** A traditional backup utility that allows manual or scheduled backups of folders, volumes, or drive images. It does not include *continuous backups*.
 - **File History:** By default, it copies the contents of libraries and user folders to an external drive, but it can be configured to include any folder. Once configured, it operates continuously, keeping data protected. It even stores multiple versions of each file, so if a previous version is needed, it can be restored.
 - **Windows Server Backup:** Similar to *Backup and Restore* but found on *Windows Server* operating systems. It has additional options intended for use in a server environment.
 - **System Restore:** Reverts the computer to a previous state, undoing system changes and application installations. It does not copy user files, nor does it save data to external drives. It allows users to revert unwanted system changes to a *known good state*. Automatically or manually creates *restore points* before software or Windows Update installations.
 - **WinRE:** *Windows Recovery Environment (WinRE)* is available from advanced boot options or a system disk. It includes troubleshooting tools and can also attempt automated boot repair or restore data from a system image. It isn't used to create backups, but if the data is still available, it can be used to repair the system.
 - **Volume Shadow Copy Service (VSS):** A technology used by *Windows Backup* and *System Restore*, that allows Windows to take backup or replica copies of files or entire volumes, even when they're already in use and would otherwise be locked from reading.
- **Backup Media**
 - **Disk:** Small Office/Home Office (SOHO) backups. They lack enterprise-level capacity, *scalability*, and manageability.
 - **Tape:** Enterprise-level capacity, scalability, and manageability.
 - **Network Attached Storage (NAS):** A specialized hardware appliance with nothing but hard drives, a network interface, and a stripped-down operating system optimized for sharing files. Any host with appropriate permissions can access its storage. Allows file-level access.
 - **Storage Area Network (SAN):** Block-level access to storage devices. Highly configurable with mixed storage technologies to implement performance tiers. Looks and feels like a local storage device. Very efficient reading and writing. Requires a lot of bandwidth. May use an isolated network and high-speed network topologies. If one device fails, users can still work with the data. It has very fast recovery times compared to traditional backups.
 - **SAN Snapshot:** Create a data state at a point in time. Copy that state to other SANs.
 - **SAN-to-SAN Replication:** Duplicate data from one data center to another.
 - **Cloud:** Functions are distributed over multiple locations, each of which is a data center.

- **Normalization:** A technique used to design and redesign databases. It is a process or set of guidelines used to optimally design a database to reduce redundant data.
- **Database Management Systems (DBMS):** Software systems used to store, retrieve, and run queries on data. A DBMS serves as an interface between an end-user and a database, allowing users to create, read, update, and delete data in the database. The identification methods are often implemented within DBMSs
- **Content Management Systems:** A software application that manages digital content. Provides indexing, which allows for file-labeling (names, dates, and file types), and *data classifications*. Search and access content across multiple websites and mobile apps. This feature provides more flexibility in how, where, and when content files can be accessed.
- **Data Loss Prevention (DLP):** Prevents the sharing or transmitting of sensitive data. DLP solutions inspect all data leaving the organization, including E-mail contents and attachments, copy to portable media, *File Transfer Protocol (FTP)*, posting to web pages/websites, applications, and *Application Programming Interfaces (APIs)*. Also includes *Pattern-Matching* and *Watermarking*.
- **Information Rights Management (IRM):** Controls printing, editing, copying, pasting, or screenshots. Restricts file permissions and forwarding.
- **File Integrity Checks:** An application that verifies that files have not been modified, using a hash algorithm.
- **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 configuration files. Once this database is initialized it can be used to verify the integrity of the configuration files.
- **Hardware Security Module (HSM):** High-end hardware to store and generate encryption and decryption keys, and offload CPU overhead for cryptographic processing from other devices. Useful as network devices in PKI environments. Can be a plug-in device or a network appliance.
- **Trusted Platform Module (TPM):** Hardware component in the motherboard of smaller/mobile devices for cryptographic processing.
- **Quantum Computing:** Performs very large calculations in a very short period. Monitoring conversations would modify the keys, preventing verification. Prevents MitM attacks because the act of observing a conversation would alter the conversation. Just theoretical at this point but will eventually render existing cryptographic methods useless.
 - **Qubit:** The smallest unit of information.
 - **Superposition:** Zeros, ones, and any combination in between, at the same time.
 - **Quantum Key Distribution (QKD):** Create unbreakable encryption by sending a random stream of *qubits* (the key), across a quantum network channel. Both sides can verify the key. If it's identical, the key was not viewed during transmission. Any attacker eavesdropping on the communication would modify the data stream. This act would violate quantum physics.

- **Administrative Controls**

- **Data Privacy Policies**
 - **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 fulfill that purpose.
 - **K-Anonymity:** Ensures that data cannot be linked to fewer than “K” individuals, reducing re-identification risks. If identifiers for each person in a dataset are identical to at least $(k - 1)$ other people in the dataset, then the data is not unique to a certain individual and can't be used to identify them. This is achieved by hiding individual records in groups of similar records, which significantly reduces the possibility of identification.
 - **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. Requires strong protections.
 - **Data Masking:** ****
 - **De-Identification:** 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.
- **Data Governance Policies**
 - **Data Classification**
 - *Public/Unclassified.*
 - *Private/Classified.*
 - *Restricted/Internal Use Only.*
 - *Sensitive.*
 - *Confidential.*
 - *Secret.*
 - *Critical.*
 - *Top Secret.*
 - **Data Sensitivity Labels**
 - *Proprietary.*
 - *Personally Identifiable Information (PII).*
 - *Protected Health Information (PHI).*
 - **Access Control Policies**
 - **Discretionary Access Control (DAC):** The owner has full control over the resource.
 - **Attribute-Based Access Control (ABAC):** Fine-grained access control. Decisions are based on a combination of *subject*, *object*, and *context* attributes.
 - **Rule-Based Access Control (RBAC):** Access is based on pre-defined organizational rules.
 - **Role-Based Access Control (RBAC):** Access is allocated to pre-defined organizational roles.
 - **Mandatory Access Control (MAC):** Based on security *clearance* level.
 - **Conditional Access:** Suspends account or requires re-authorization based on conditions.
 - **Data Retention Policies**
 - **Data Minimization:** Collect as little data as possible.
 - **Purpose Limitation:** Use data for only expressed purposes.
 - **Data Sanitization Policies**
 - **Purge:** Destroy some of the data.
 - **Wipe:** Unrecoverable deletion.
 - **Secure Data Destruction Policies**
 - **Pulping:** Removes ink, breaks down paper, and recycles it.
 - **Shredding:** Industrial shredder is used to break documents and drives into bits.
 - **Degaussing:** Using a strong magnet to wipe the data.
 - **Destroying:** Physically drilling a hole through the device or smashing it to pieces.
 - **Incinerating:** Burning the medium.
 - **Third-Party Certificate of Destruction:** Proof that a third-party destroyed the data.