Unit 1.0: General Security Concepts:

- **Compare and Contrast Various Types of Security Controls**
  - **Security Control:** Counter measures that reduce the chances that a vulnerability will be exploited. This is also known as Risk Mitigation.
    - Often done using Defense-In-Depth Strategy: combining controls into multiple layers of security, so that if one layer fails to counteract a threat, the other layers will prevent a breach
  - **Categories:**
    - **Technical:** Aka Logical Security Control; Using technology to reduce vulnerabilities in hardware and software; Executed by computer systems and not people (i.e. Firewalls, Encryption, Antimalware Software, Intrusion Detection Systems (IDS))
      - Access Control Lists (ACL): Network Traffic Filters that can control ingoing and outgoing traffic
      - Configuration Rules: Instructional code that guide the execution of the system
    - **Managerial:** Aka administrative controls; policies, procedures, and guidelines established by an organization to reduce risk of incident and support its security goal
      - Security Training Programs, Employee Onboarding, Compliance Audits
    - **Operational:** Controls implemented and executed by people to manage day-to-day security operations; ensures equipment continues to work as specified
      - Security Awareness Training, User Access Reviews, Incident Response Procedures, Monitoring of Security Events, Data Backups, Configuration Management, Patching
    - **Physical:** Using physical security to prevent/detect access to sensitive data (i.e. surveillance cameras, Security guards, ID scanners, doors)
  - **Control Types:**
    - **Preventive:** prevent an incident from occurring
      - Security Guards, Security Awareness Training, Hardening, Encryption, AV (antivirus) software
    - **Deterrent:** discourage individuals from causing an incident
      - Cable Locks, Guards, Warning Signs, LIGHTING, Fencing
    - **Detective:** detects incidents after they have occurred

            - Log monitoring, Video Surveillance, Trend Analysis, SIEM (Security Information and Event Management), IDS, Vulnerability Scanning
        - **Corrective:** attempts to reverse the impact of an incident
            - IPS (detects anomalies in traffic flow and then drops packets or resets connections to prevent malicious activity), Backups and System Recovery, IRP, DRPs, Forensic Analysis
        - **Compensating:** alternative controls used when a primary control is not possible
            - Time-Based One Time-Password, Encryption, Temporary Service Disablement, MFA, Sandboxing, Temporary Port Blocking
        - **Directive:** measures designed to guide and dictate the actions and behaviors of personnel within an organization to ensure compliance with security policies
            - Security Newsletters, IRP (Incident Response Plan), AUP (Acceptable Use Policy)

- **Summarize Fundamental Security Concepts**
    - **The Tenets of Information Systems Security (CIA)**
        - **Confidentiality:** Limits access or places restrictions on data
        - **Integrity:** Ensures data and associated systems are only accessible and modified by authorized users
            - Ensures data accuracy, maintains trust, ensures system operability
            - Five Methods to Ensure Integrity:
                - **Hashing:** Process of converting data into a fix-size value
                - **Digital Signatures**
                - **Checksums:** Summary information appended to a message to ensure that the values of the message have not changed
                - **Access Controls:** regulating who or what can view/use a resource
                - **Regular Audits:** Identify vulnerabilities and ensure compliance with regulations
        - **Availability:** Ensures information is ready for use and at the required performance level & prevents data loss and destruction
            - **Redundancy:** duplication of critical components to enhance reliability
                - **Server Redundancy:** using multiple servers in a load balanced configuration so that if one overloads or fails, the other servers can take over the load to continue supporting your end users
                - **Data Redundancy:** storing data in multiple places

            - **Network Redundancy:** ensures that if one network path fails, the data can travel through another place
            - **Power Redundancy:** Involves using backup power sources, like generators and UPS systems

- **Non-Repudiation:** describes the inability to deny responsibility for performing a specific action. In the context of data security, non-repudiation ensures data confidentiality, provides proof of data integrity, and proof of data origin
    - Confirms authenticity of digital transactions, ensures integrity of communication, provides accountability in digital processes
    - **Digital Certificate:** When sending a message, a digital signature is made using a private key, which is then verified by the recipient using the sender's public key, establishing a message was sent
        - *Shared Account* violates non-repudiation
- **Authentication, Authorization, and Accounting (AAA):**
    - **Identification:** Who is asking for access?
    - **Authentication:** Verifying the identity of a user or system
        - **Authenticating People:** Username/Password, Biometrics, Hardware tokens, MFA
        - **Authenticating Devices:** Digital Certificates, IP addresses, MAC addresses
        - **Multi-Factor Authentication (MFA):** Security process that requires users to provide multiple methods of identification to verify their identity
    - **Authorization:** Determining the allowed actions/resources a user can access
        - User Permission settings
        - **Role-Based Access Control (RBAC):** Assign permissions to roles and then assign individuals to roles
        - **Attribute-Based Access Control (ABAC):** dynamic rather than static roles, roles expressed in business terms making them more understandable
    - **Accounting:** Tracing actions to an individual to ensure the person who makes data or system changes can be identified
        - **Syslog Servers**: aggregate logs from various network devices so that system administrators can analyze them to detect patterns or anomalies
        - **Network Analysis Tools:** used to capture and analyze network traffic so network admins can get insight on data moving within a network
        - **Security Information and Event Management Systems (SIEM)**

- **Gap Analysis:** procedure which assess how well a business' current level of information security compares to a particular standard
    - **Technical Gap Analysis:** involves evaluating an organization's current technical infrastructure, identifying any areas where it falls short
    - **Business Gap Analysis:** Involves evaluating an organization's current business procedures
    - Gap Analysis Report Contains: requirements of the selected standard, what controls are in place, information on whether existing controls can be adapted to the desired standards, resources to aid certification, time estimation of how long it will take to reach standard, cost estimate, expected difficulties
    - **Plan of Action and Milestones (POA&M)**
        - Outlines the specific measures to address each vulnerability, what resources need to be used, and established timeline for each remediation task that is needed
- **Zero Trust Model:**
    - A "trust nothing, verify everything" design. A network security which assumes there is no trust boundary, i.e. a network perimeter where users are automatically trusted once they have crossed that boundary. ZTA (Zero Trust Architecture) is split into two functional planes of operation, control and data plane.
    - **Control Plane:** Where the policies and rules for the network are set; consists of the ZTA core and communicates among ZTA components on how to maintain, configure, and control the rest of the network
        - **Adaptive Identity:** Applies security controls based on different factors and risk indicators in real-time to authenticate users. "High Risk" analysis can increase the number of authentication requirements needed for a user to access information
            - Device configuration, User Behavior, Location, IP, Address, Time of Day
        - **Threat Scope Reduction:** Reduces the possible ways a threat might occur
            - Decreasing the number of entry points to the network, segmenting network on the inside and enforcing principles of least privilege so users only have permissions to do what is minimally necessary
        - **Policy Driven Access Control:** Access to the network & resources is driven by predefined policies

      - Once information about a person is gained through Adaptive Identity process, use these policies to determine if access should be granted
    - **Policy Administrator:** A part of the Policy Decision Point. Responsible for establishing or ending communication path between the subject and the requested resource.
    - **Policy Engine:** A part of the Policy Decision Point. Responsible for making and logging the final decision to grant or deny each request from a subject using the information given to it. Once a decision is made, it is logged by the PE, and then sent to the Policy Admin to be executed.
  - **Data Plane:** where an organization's critical data resides and is accessed by systems, applications, and users
    - **Implicit Trust Zones:** Located between the Policy Enforcement Point and the resource, where the user is briefly implicitly trusted to allow them to reach the resource
    - **Subject/System:** Refers to the individual or entity attempting to gain access.
    - **Policy Enforcement Point:** A gatekeeper for all subjects that attempt to access the network, which gathers all information about the subject, their request, sends it to the Policy Decision Point, which then gives a go-ahead to deny or permit the request

- **Physical Security**
  - **Bollards:** Short, sturdy vertical posts that prevent accidental and intentional attacks involving large vehicles

  - **Access Control Vestibule:** double door system; prevents piggybacking and tailgating
    - **Piggybacking:** involves two people working together with one person who has legitimate access intentionally allows another person in with them
    - **Tailgating:** an unauthorized person follows someone through the access control vestibule who has legitimate access without their knowledge or consent
  - **Door Locks:** traditional padlocks, basic door locks, electronic locks

  - Cipher locks: mechanical locks with numbered push buttons
  - Authentication Methods (for electronic locks): identification numbers, wireless signals, biometrics
    - Challenges with Biometrics:
      - **False Acceptance Rate (FAR):** System erroneously authenticates unauthorized user
      - **False Rejection Rate:** Denies access to authorized user
      - **Crossover Error Rate (CER):** A balance between FAR and FRR for optimal authentication effectiveness
- **Fencing:** barrier, railing, etc. that encloses an area of ground to control access
- **Video Surveillance:**
  - **Pan-Tilt-Zoom (PTZ) System:** Can move the camera or its angle to better detect issues during an intrusion
- **Security Guard**
- **Access Badge:** Using RFID card or Magnetic Stripe that stores unique data that is swiped
  - **Access Badge Cloning:** copying data from Radio Frequency Identification Cards and Near Field Communication card onto another
- **Lighting:** Well lit areas are less likely to be attacked. Motion based lighting helps identify where people are active and can alert security to a presence that is not where it's supposed to be
- **Sensors**
  - **Infrared:** Detects infrared radiation emitted by all objects and living beings. Commonly used in motion detection systems & automatic lights. Can also be used as night vision cameras.
  - **Pressure:** Detects changes in pressure or force applied to their surface. This can detect unauthorized access or tampering with doors, windows, etc.. There might be pressure-sensitive mats to detect footsteps or weight changes. Can also be put along fences to detect if someone climbed over a fence or attempted to breach a barrier.
  - **Microwave:** Emit microwave signals to detect time taken for signals to return to the sensor. When a change in time occurs, it is declared that there has been movement; has a longer range than infrared, higher sensitivity, and does not need a direct line of sight

        - **Ultrasonic:** Transmit sound waves above audible range for humans. Can detect motion by detecting change in time reflected
- **Detection and Disruption Technology:** Technology intended to deceive attackers
    - **Tactics, Techniques, and Procedures (TTPs):** Methods and patterns of activities associated with a particular threat actor or group
    - **Honeypot:** Systems setup with intentional vulnerabilities to attract attacks. While an attacker takes the bait, security teams gain insight into attack patterns, techniques, and commands
    - **Honeynet:** Multiple honeypots combined to make a more realistic bait network, with multiple intentional vulnerabilities
    - **Honeyfiles:** Bait files placed within honeypots or honeynets but can also be placed within real networks to act as an Intrusion Detection System (i.e. “passwords.txt”) and serve as a trap so that when opened by the attacker, it will set off an alarm. Usually gives the illusion of being correct
    - **Honeytoken:** Similar to Honeyfiles, but are pieces of fake data that are intended to be attractive while allowing security professionals to track the data and therefore track the attacker
- **Attacking with Brute Force**
    - **Brute Force:** trying to gain access by trying all possibilities until you break through
        - Forcible Entry
        - Tampering with Security Devices
        - Confronting Security Personnel
        - Ramming barriers with vehicles
- **Bypassing Surveillance Systems**
    - Visual Obstruction: blocking the camera’s line of sight with sprays, tape, or objects
        - Blinding Sensors or cameras with a sudden burst of light to render it ineffective for a limited period of time
    - Interference with Acoustics: playing loud music to disrupt microphone’s functionality
    - Interfering with Electromagnetic: jamming the signals the surveillance system uses to monitor environment
    - Attacking the physical environment: physical tampering (cutting wires)

➔ **Explain the Importance of Change Management Processes and the Impact to Security**

- **Change Management:** structured approach to transitioning individuals, teams, and organizations from a current state to a future state, while ensuring the security, confidentiality, integrity, and availability of information

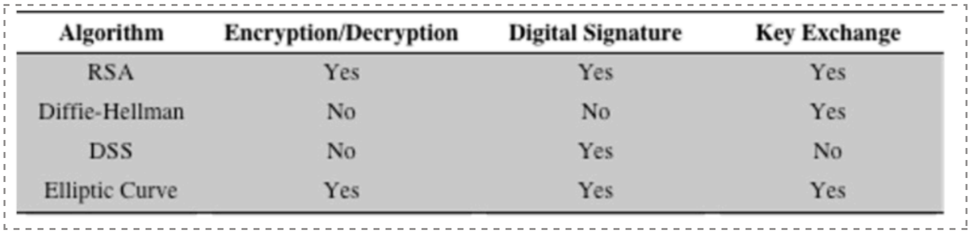
  - **Change Advisory Board (CAB):** Responsible for Evaluating, prioritizing, and sanctioning these changes. It begins with the approval process, and then the clear clarification of ownership to engaging stakeholders, conducting impact analysis, assessing test results, devising backout plans, orchestrating maintenance windows, and adhering to standard operating procedures
  - **Change Management Processes:** Offers blueprint to orchestrate modifications while security remains intact, utilizing CAB to supervise proposed changes
  - **Chief Information Security Officer (CISO):** ensures security tasks are carried out effectively and there is accountability
- Business Processes Impacting Security Operations
  - **Approval Processes:** ensures that any changes are reviewed and approved by authorized personnel before implementation
  - **Ownership:** A person within a department who has asked for a change and will be responsible for ensuring it is carried out effectively
  - **Stakeholders:** anyone who may be affected by the change or has influence in the process (IT Staff, Security Teams, Management, Users)
  - **Impact Analysis:** Before implementing a change, analyzing its potential impact to attempt to foresee security risks and addressing them before they become real problems
  - **Test Results:** Testing changes in a controlled environment before full implementation, to identify any unforeseen security issues and provide confidence that security actions will protect organization as expected
  - **Backout Plan:** contingency plan that can be activated if unacceptable risks or issues are caused by changes which outlines the steps to revert the systems to the state before the change
  - **Maintenance Window:** Predefined period when changes are implemented, during a time where it would impact the least amount of people, minimizing disruptions
  - **Standard Operating Procedures (SOP):** Detailed instructions to achieve uniformity in the implementation of change management
- **Technical Implication:** the direct effects that changes in an IT environment can have on system security, functionality, and performance
  - **Allow Lists/Deny Lists:** A list of entities that are allowed/disallowed to access a system or resource. Incorrect changes can lead to vulnerabilities or unintended access restrictions.
  - **Restricted Activities:** Prevent actions that could potentially lead to vulnerabilities or disruptions

  - **Downtime:** Organization's systems taken offline because of a system failure/maintenance. Has an adverse effect on the loss of revenue, and thus there should be plans to prevent it.
  - **Service Restart:** Shutting down or rebooting systems disrupts user access to computing resources and hinder incident response and recovery efforts. Attackers might time their actions to coincide with Service Restarts to exploit gaps in security
  - **Application restart:** Improper restart procedures can cause data inconsistencies or corruption
  - **Legacy Applications:** An application that has been used for a long time and thus tends to have outdated security measures and lack of vendor support. They might not be compatible with new security systems, creating security gaps.
  - **Dependencies:** Interconnection of services and system drivers; A change in one component can affect other dependent systems
- **Documentation:** Thorough documentation of changes ensures transparency and accountability of changes being made and makes it easier to track modifications. This ensures unauthorized or unaccounted for alterations can be caught.
  - **Updating Diagrams:** Changes in the IT infrastructure needs to be accurately reflected in network and system diagrams
  - **Updating Policies/Procedures:** Any change in the IT environment might require updates to security policies & must be documented (Change Management Process)
- **Version Control:** Tracking changes, maintaining older versions, and ensuring the integrity of software and system configurations
  - **Audit Trail:** chronological records of actions

- **Explain the Importance of Using Appropriate Cryptographic Solutions:** Keeps information secret from unauthorized users (Confidentiality), Ensures that no one, even the sender, changes information after transmitting it (Integrity), Confirms the identity of an entity (Authentication), Enables you to prevent a party from denying a previous statement or action (Nonrepudiation)
  - **Public Key Infrastructure (PKI):** Framework managing digital keys and certificates for secure data transfer
    - **Key:** A string of numbers or characters used to encrypt and/or decrypt information
    - Public Key: encrypts data
    - Private Key: decrypts data
    - Key Escrow: Method of storing cryptographic keys using 3rd party repository, which ensures encrypted information can be accessed by authorized entities

- **Encryption:** Converting plaintext to ciphertext. Provides data protection at rest, in transit, and in use
    - **Level:** The granularity at which encryption is applied
        - Full-Disk
            - **Full Disk Encryption (FDE):** Protects data on a device in the event it is lost or stolen. Requires unauthorized users to have physical access to your device as well as the password in order to decrypt the data on your device.
                - Once device is unlocked, all data is accessible
        - **Partition:** Encrypts a section of a disk, which is useful for separating sensitive data from general data, and can allow different encryption settings for different partitions
        - **File:** Encrypting individual files, allowing for granular level of control over which files are protected. However, it involves managing encryption keys for all the files.
        - **Volume:** Encrypts a logical volume, which can be multiple partitions or disks. Helpful for protecting a group of files that are treated as a single unit.
        - **Database:** Encrypts within a database, often at the column or table level.
        - **Record:** Encrypts individual records (rows) within a database, providing fine-grained control over which records are protected
    - **Transport/Communication:** A method of sending data over the internet where the data is encrypted but the original IP address information is not
    - **Asymmetric:** aka "Public Key Cryptography"; Slower compared to symmetric encryption
        - Public Key: Used for Encryption
        - Private Key: Used for Decryption
        - Examples: Diffie-Hellman, RSA, Elliptic Curve Cryptographic
            - Diffie-Hellman: Used for key exchange and distribution. Vulnerable to man in the middle attacks.
            - RSA: Used for key exchange, encryption, and digital signatures
            - Elliptical Curve Cryptography (ECC): Efficient and secure, uses algebraic structures of elliptical curves. Better than RSA for security.
                - Multiple Variants: ECDH, ECDHE, ECDSA
    - **Symmetric:** aka "Private Key Cryptographic"; Offers confidentiality but lacks non-repudiation; Uses same key for encryption and decryption; fast, scalability issues

        - **Symmetric Block Encryption Algorithms:**
            - Block Cipher: processes plaintext input in fixed sized blocks and produces a block of ciphertext of equal size for each plaintext block
            - **DES:** Data Encryption Standard
            - **AES:** Advanced Encryption Standard
    - **Key Exchange:** A method in which cryptographic keys are exchanged between two parties
        - **Diffie-Hellman-Merkle Key Exchange Algorithm**



Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic Curve	Yes	Yes	Yes

    - **Algorithms:** A repeatable process that produces the same result when it receives the same input
    - **Key Length:** proportional to security
- Tools
    - **Trusted Platform Module (TPM):** dedicated microcontroller [computer chip] that store sensitive information using cryptography; adds an extra layer of security against software attacks
    - **Hardware Security Module (HSM):** Physical device for safeguarding and managing digital keys
    - **Key Management System:** Manages, stores, distributes, and retires cryptographic keys; centralized mechanism for key lifecycle management; automates key management in complex environments
    - **Secure Enclave:** Coprocessor integrated into the main processor of some devices, isolated from main processor for secure data processing and storage, enhancing device security by preventing unauthorized access
- Obfuscation:
    - **Stenography:** Conceals a message within another to hide its existence (i.e. an image) to prevent suspicion of hidden data
    - **Tokenization:** substitutes sensitive data with non-sensitive tokens to reduce exposure of sensitive data during transaction; vaults data in a lookup table
    - **Data Masking:** Disguises original data to protect sensitive information; an access based control where data will only be visible to those with appropriate permissions
- **Hashing:** Converts data into fixed-size string (digest) using hash functions

  - Hashing Algorithms:
    - MD5: Message Digest 5 – 32 bit string
    - SHA512: Secure Hashing Algorithm – 512 bit
- **Salting:** adds random data (salt) before hashing, to ensure distinct hash outputs for same passwords due to different salts
  - Inhibits dictionary attacks, brute-force attacks, and rainbow tables
- **Digital Signatures**: Bind the identity of an entity to a particular message or piece of information to ensure the integrity of a message and verify who wrote it. Requires asymmetric key cryptographic.
- **Key Stretching:** Making a weak key stronger by sending it through multiple hashes, slowing down the process of brute-force attacks even for weak passwords
- **Blockchain:** A distributed ledger that keeps track of transactions
  - **Blockchain Process:** A transaction is requested and a copy is sent to every computer in a decentralized network to be verified. The verified transaction is added to a new block of data containing other recently verified transactions. A secure hash is calculated from the previous blocks of transaction data in the blockchain.
  - **Smart Contracts:** Self executing contracts with code defined terms. Execute actions automatically when conditions are met. Transparent, tamper-proof, trust-enhancing
- **Open Public Ledger:** A ledger that anyone can view but only those with designated private keys can authorize transactions
- Certificates
  - **Certificate Authorities:** a trusted organization that issues digital certificates for websites and other entities
  - **Certificate Revocation Lists (CRLs):** A list of digital certificates that have been revoked by the issuing certificate authority before their actual assigned expiration dates
  - **Online Certificate Status Protocol (OCSP):** Queries an OSCP responder hosted by the CA to check if a certificate is still valid
    - Client Request: When a client connects to a server, it sends an OCSP request to the CA's OCSP responder to check the status of a server's certificate
    - OCSP Responder: The OCSP responder checks its records and sends back a signed response if the certificate is good, revoked, or unknown
    - Client Verification: Client verifies the OCSP response and proceeds accordingly
  - **Self-Signed:** a certificate signed not by a CA, but by the developer or company that is responsible for the website; not trusted by browsers

- **Third-Party:** Issued and signed by trusted certificates authorities; trusted by browsers
- **Root of Trust:** A source that can always be trusted within a cryptographic system
  - Components are immutable, minimalist, and hardware-based
- **Certificate Signing Request (CSR) Generation:** a message sent from an applicant to a Certificate Authority (CA) in order to apply for a digital certificate. The CSR contains information that will be included in the certificate, such as the applicant's public key, and is digitally signed with the applicant's private key to prove that the applicant owns the key pair.
- **Wildcard Certificate:** A single certificate with * in the domain name, allowing the certificate to secure multiple subdomain names pertaining to the same base domain

Unit 2.0: Threats, Vulnerabilities, and Mitigations

- ➔ **Compare and Contrast Common Threat Actors and Motivation:**
  - ◆ **Threat Actors:** a individual, group, or entity that carries out malicious activities with the intent of causing harm, exploiting vulnerabilities, or gaining unauthorized access
    - **Nation-State:** Government backed entities that conduct cyber espionage, sabotage or other offensive activities to advance their nation's interests
    - **Unskilled Attacker:** "script kiddies"; commonly use DDOS; inexperienced individuals who use existing hacking tools without deep understanding; may engage in cyberattacks for fun or for recognition
    - **Hacktivist:** motivated by philosophical or political beliefs; usually fairly sophisticated
      - Website Defacement
      - DDoS (Distributed Denial of Service)
      - DoS (Denial of Service)
      - Doxing
      - Leaking of Sensitive Data
    - **Insider Threat:** Individuals within a business which use their close access to systems for their personal gain, espionage, or sabotage
    - **Organized Crime:** Criminal organizations using cyberattacks as a part of their broader criminal activities

      - Custom Malware, Ransomware, Phishing Campaigns, Data breaches, Identity theft, Online Fraud,
    - **Shadow IT:** using IT systems without the knowledge of the IT department
      - **Bring Your Own Devices (BYOD):** using personal device for work
  - **DOS (Denial of Service) Attack:** Overwhelming systems or networks so they cannot be utilized by legitimate users
  - **False Flag Attack:** Attack that is orchestrated in such a way that it appears to originate from a different source or group than the actual perpetrators
  - **Advanced Persistent Threat:** prolonged cyberattack in which intruder tries to remain undetected
  - **Attributes of Actors:**
    - Internal/External: Individuals within an organization vs individuals outside an organization breaching cybersecurity defenses
    - Resources/Funding
    - Level of Sophistication/Capability
  - **Motivations**
    - **Data Exfiltration:** Unauthorized transfer of data from a computer
    - **Espionage:** spying to gather sensitive or classified information
      - Nation-State
    - **Blackmail:** The attacker obtains sensitive or compromising information about an individual or an organization and threatens to release this information to the public unless certain demands are met
    - **Financial Gain:** Achieved through various means, such as ransomware attacks, or through banking trojans that allow them to steal financial information in order to gain unauthorized access into the victims' bank accounts
      - Organized Crime
    - **Philosophical/Political beliefs & Ethical:**
      - Hacktivism
    - **Revenge**
    - **Disruption/chaos:** creating and spreading malware
      - Organized crime
    - **War:** Cyber warfare used to disrupt a country’s infrastructure or compromise national security/economy
      - Nation-state
- **Common Threat Vectors and Attack Surfaces**
  - **Threat Vector:** Means or pathway by which an attacker can gain unauthorized access to a computer or network to deliver malicious payload or unwanted action (How An Attack Happens)

- **Attack Surface:** all the various points where a user can try to enter data or extract data from an environment (Where An Attack Happens)
- Message-Based: embedding malicious code in messages
    - Phishing
        - Email
        - SMS
        - IM
- Image-Based
- File-Based
- Voice Call:
    - Vishing: using voice calls to trick victims into revealing sensitive information
- Removable Device
    - Baiting: leaving a malware infected USB drive in a public location where their target might find it
- Vulnerable Software
    - Client-Based: require installation of software agents or clients on each endpoint device or system
    - Agentless: operate without installing additional software, utilizing existing protocols to collect information remotely
- Unsupported Systems and Applications: no longer receive security updates from their vendors
- Unsecure Networks
    - Wireless
    - Wired
    - Bluetooth
        - **BlueBorne:** set of vulnerabilities in Bluetooth technology that allows an attacker to take or devices, spread malware, or establish an on-path attack to intercept communications without any user interaction
        - **Bluesmack:** Type of DoS that attacks bluetooth devices by sending a crafted Logical LInk Control and Adaptation Protocol packet to a target device
- Open Service Ports: A network port on a system that is configured to accept incoming network connections for a particular service or application
- Default Credentials
- Supply Chain
    - Managed Service Providers (MSPs)
    - Vendors
    - Suppliers

- Human Vectors/Social Engineering
    - Phishing: sending fraudulent messages
        - **Spear Phishing:** phishing attack that targets specific individuals or organizations
            - **Whaling:** type of spear fishing attack that is aimed exclusively at a high-level executive
        - **Vishing:** fraudulent phone calls
        - **Smishing:** fraudulent SMS
        - **Business Email Compromise:** A sophisticated phishing that targets businesses by using one of their internal email accounts to get other employees to perform some kind of malicious action on behalf of the attacker
    - **Influence Campaigns:** Coordinated efforts to affect public perception or behavior towards a particular cause, individual, or group.
        - **Misinformation:** false/inaccurate information shared WITHOUT harmful intent
        - **Disinformation:** involves the deliberate creation and sharing of false information with the intent to deceive or mislead
    - **Impersonation**: Pretending to be someone else
        - **Typosquatting:** hackers registering domains with deliberately misspelled names of well-known websites
        - **Brand Impersonation**: Pretending to represent a legitimate company or brand
        - **Watering Hole:** targets users by infecting websites they commonly visit
    - **Pretexting:** a made-up scenario developed by the threat actor for the purpose of stealing a victim's personal data
    - Frauds and Scams: Deceptive practices to deceive people into parting with money or valuable information. Identifying and training against frauds and scams.
    - Other:
        - Dumpster Diving, Eavesdropping, Shoulder Surfing, Hoaxes, Diversion Theft
    - **Motivation Triggers:**
        - Authority: coming from position in power
        - Intimidation: something bad will happen
        - Consensus and Social Proof: peer pressure
        - Scarcity: limited supply
        - Familiarity and Likeability
        - Trust:

        - Urgency: time-sensitive action

- **Explain Various Types of Vulnerabilities**
    - **Vulnerability:** A weakness in a system that can be exploited
    - **Application**
        - **Memory Injection:** inserting malicious code into a program's memory
        - **Buffer Overflow:** data that is meant to be stored in a buffer exceeds storage capacity, causing adjacent memory locations to be overwritten. This can cause code to crash, become unstable, return information that was not meant to be returned, or execute malicious code
            - **Heap-Based Buffer Overflow:** less common; attacker attacks the application by flooding reserved memory space
            - **Stack-Based Buffer Overflow:** More common; "Stack Smashing", overflowing the stack – where user input is stored
            - Overflow Mitigation: Use a language w/o buffer overflow, use secure functions
        - **Race Conditions:** think about the issues with threading, and not properly lucking or unlocking
            - **Time-of-check (TOC):** exploiting a time gap between checking a condition and acting on it
            - **Time-of-use (TOU):** Exploiting a time gap between the check and use of a resource
        - **Malicious Update:** Introducing malicious updates to software
    - **Operating System (OS)-based:** Weaknesses in the OS that can be exploited to gain unauthorized access, escalate privileges, etc..
    - **Web-Based**
        - **Structured Query Language Injection:** injecting SQL queries into input fields to manipulate a database
        - **Cross-Site Scripting: (XSS)** injecting malicious scripts into web pages viewed by other users
    - **Hardware**
        - **Firmware:** weaknesses in low level software that runs on hardware devices
        - **End-of-life:** device is no longer supported by manufacturers, resulting in unpatched vulnerabilities
        - **Legacy:** older hardware that is not compatible with current security measures
    - **Virtualization**
        - **Virtual Machine (VM) escape:** an attacker escapes the isolation of a virtual machine and gains access to the underlying operating system and other VMs on the same physical machine.

    - **Resource Reuse:** Sensitive data can remain in system resources and be accessed by other processes
- **Cloud-Specific**
    - **Attack the Service (DoS)**
    - **Authentication Bypass:** take advantage of weak authentication
    - **Directory Traversal:** faulty configurations put data at risk
    - **Data Breaches:** data stored on cloud servers may be targeted by hackers
        - Cloud Services are accessed through interfaces and APIs, which if are not properly secured, can be exploited
    - **Account Hijacking:** An attacker with access to a user's cloud account can manipulate data, eavesdrop on transactions, and redirect clients to illegitimate sites
    - **Remote Code Execution:** take advantage of unpatched systems
    - **Out of Bounds Write:** write to unauthorized memory areas
- **Supply Chain:** contains many moving parts where attackers can infect at any step along the way
    - **Service Provider:** Service provider often have access to internal services, which gives the attacker an opportunity
        - Many different types – network, utility, office cleaning, cloud service
        - Example: A heating an AC firm got infected with malware through email, and they supplied Target, and they managed to infect every cash register at 1,800 stores
    - **Hardware Provider:**
        - Server, router, switch, firewall, software
    - **Software Provider:** Trust is a foundation of security; digital signature should be confirmed during installation
- **Cryptographic:**
    - **Downgrade Attacks:** Force systems to use weaker or older cryptographic standards or protocols & exploit known vulnerabilities in outdated versions
    - **Collision Attacks:** hashes are supposed to be unique, but sometimes similar hashes result in the same MD5 value
        - **Birthday:** hash collision is the same hash value for two different plaintexts, so attackers will generate multiple versions of plaintext to match the hashes
    - **Quantum Computing Threats:** Threat to traditional encryption algorithms by rapid factorization of large prime numbers
        - Post-Quantum Cryptography creates algorithms resistant to quantum attacks

- **Misconfiguration:**
    - **Open Permissions:** accidentally leaving the door open, which is increasingly common with cloud storage
        - Open Services and Ports:
            - Must manage access with firewall rulesets
    - **Unsecured Admin Accounts:**
        - The Linux Root Account: The Windows Administrator or superuser account
            - Sometimes given an intentionally easy password, making it easy to brute force
        - Good practice is to disable direct login to the root account
    - **Default Settings**
    - **Insecure Protocols:** some protocols aren't encrypted, like Telnet, FTP, SMTP, IMAP (Encrypted versions are: SSH, sFTP, IMAPS, HTTPS)
        - Verify with a packet capture over the network
- **Mobile Device:**
    - **Side loading:** installing applications downloaded from a source other than the device manufacturer's official app store
    - **Jailbreaking (Apple)/rooting (Andriod):** Gaining access by replacing phone's operating system with own; install custom firmware; gives uncontrolled access, circumventing security features, and the Mobile Device Manager become useless
- **Zero-Day:** An attack without a patch or method of mitigation, a race to exploit the vulnerability or create a patch, difficult to defend against the unknown

➔ **Given a scenario, analyze indicators of malicious activity**

- **Malware Attacks**
    - **Ransomware:** malware that blocks access to files or the system on computer in exchange for payment, usually cryptocurrency
        - Indicators: On-screen message, all files encrypted
    - **Trojan:** malware hidden in innocuous software
        - Indicators: poor pc performance, unfamiliar programs running in task manager, intrusive pop-ups and ads
    - **Worm:** self-replicating malware
        - Indicators: slow performance on multiple computers that are connected over the network, high resource usage, creating backdoors
    - **Spyware:** malware used to gather data such as browser history and access credentials
        - Indicators: Often, system performs normally

- **Bloatware:** Not-intrinsically malicious; bloatware comes pre-installed on devices and can slow performance or increase attack vectors from a lack of patching
- **Virus:** malware designed to spread from machine to machine through user intervention
  - Indicators: damaged files, poor PC performance
- **Keylogger:** software/hardware devices that capture keystrokes
  - Indicators: lag in keystrokes or mouse movement, poor computer performance
- **Logic Bomb:** malware that releases its payload only when certain conditions are met
- **Rootkit:** Malware that provides persistent admin/root access to a hacker without the authorized admin's knowledge
  - Indicators: Difficult to detect; unfamiliar programs, hidden files, unusual network activity

◆ **Physical attacks**

- **Brute force:** physically breaking into a facility to gain access to a system
  - Indicator: Damage, out-of-cycle key card logging
- **Radio frequency identification (RFID) cloning:** cloning the information from an access card
  - Indicator: out of cycle key card logging
- **Environmental:** Attacks on the facility that supports the IT technology
  - Indicator: Cut power, HVAC system down, Fire suppression system disabled

◆ **Network Attacks**

- **Distributed denial-of-service (DDoS):** system is overwhelmed by traffic or resource consumption
  - **Amplified:** sends small request to a vulnerable server designed to trigger a very large response
  - **Reflected:** the hacker spoofs the victims IP address, getting vulnerable servers to flood response packets to the victim's ip address
- **Domain Name System (DNS) attacks:** Attacks that target unencrypted domain naim service to redirect users to malicious websites
  - Cache Poisoning: modifying DNS file data on either server or host device to redirect to malicious site
  - On-Path: intercepting then altering DNS queries
  - Domain Hijacking: modifying the domain's records and pointing it to malicious site
  - URL Hijacking: directing misspelled urls to malicious copy sites

- **Wireless:** attack on wifi systems
  - War-driving: using tools to scan for wireless networks, traditionally while driving around
  - Evil Twin: unauthorized APs with similar names to legit ones
  - Wireless Deauthentication: DOS attack where users are regularly dropped
  - Sniffing: capturing and analyzing wifi traffic
  - RF Jamming: increases noise to signal ratio to prevent a good signal
- **On-Path:** intercepting the traffic between two devices
- **Credential Replay:** attackers capture credentials to reuse them
  - Techniques: Eavesdropping, packet sniffing, phishing email, pass the hash
- **Malicious Code**

◆ **Application Attacks:** attacks against software applications that either grant unauthorized access, steal data, or disrupt functionality

- **Injection:**
- **Buffer Overflow**
- **Replay**
- **Privilege Escalation:** attacker gains elevated access acquiring low-level credentials and escalating to root-admin privilege or horizontal privilege
- **Forgery:** when a user stays logged into an app, the pre-authorization can be abused
- **Directory Traversal:** an attacker leaves the directory hosting the web app and moves to others

◆ **Cryptographic Attacks**

- **Downgrade:** an attack in which the system is forced to abandon the current higher security mode of operation and fall back to implementing an older, less secure mode
- **Collision:** hash digests are SUPPOSED to be unique, but sometimes similar hashes have the same MD5 value
- **Birthday:** exploits the possibility that two passwords will create the same hash; hash collision is the same hash value for two different plaintexts; attacker will generate multiple versions of plaintext to match the hashes

◆ **Password Attacks**

- **Spraying:** trying a password on multiple accounts to see if any authorize
- **Brute force:** trying multiple passwords on one account
  - **Offline:** Attacker gains access to a system's file or database, allowing them to decipher the passwords at their leisure

            - **Rainbow table:** used in offline attacks; a precomputed table containing a vast number of potential passwords and their corresponding hash values
        - **Online:** systematically guessing passwords on actual website
- **Indicators**
    - **Account lockout**
    - **Concurrent session usage:** one authenticated user has multiple log in sessions active
    - **Blocked content:** firewall or content filters are filtering malicious content
    - **Impossible travel:** analyzing and denying a second user login attempt based on the location of the prior attempt
    - **Resource consumption:** slow system devices with unknown heavy resource usage
    - **Resource inaccessibility:** services being unavailable
    - **Out-of-cycle logging:** logs generated outside of expected time frames
    - **Published/documented:**
    - **Missing logs:** deleted logs to cover tracks of malicious activity

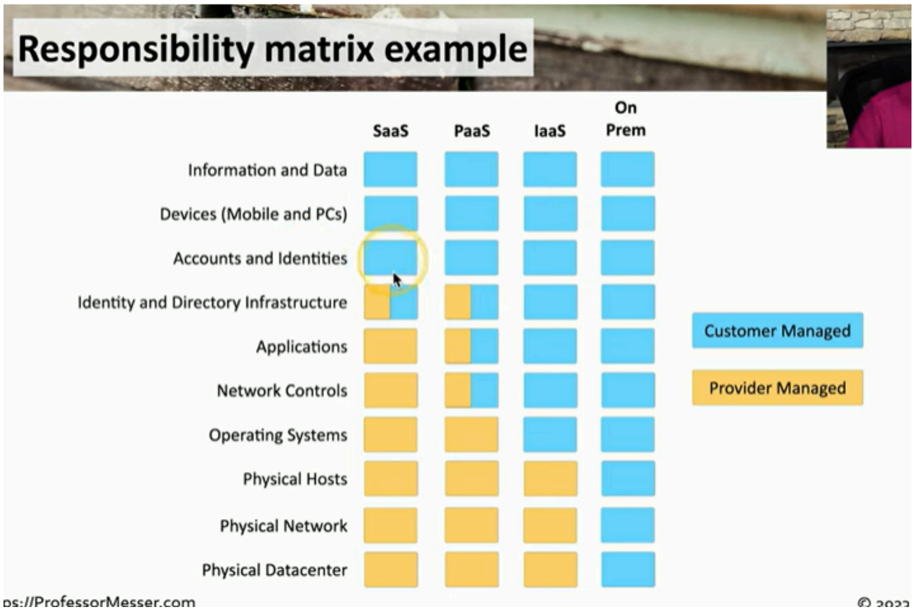
➔ **Explain the purpose of mitigation techniques used to secure the enterprise**

- **Segmentation:** splitting a network into multiple segments, or subnets, each functioning as a smaller, separate network
    - **VLAN:** Hardware tool used to create a network subnet
- **Access Control**
    - **Access Control List**
    - **Permissions**
- **Application Allow List**
- **Isolation:** segregating different parts of a
- **Patching**
- **Encryption**
- **Monitoring**
- **Least Privilege:** limiting access rights for users, accounts, and computing processes to only those resources.
- **Configuration Enforcement**
- **Decommissioning**
- **Hardening Techniques**
    - **Encryption**
    - **Installation of endpoint protection**
    - **Host-based firewall**
    - **Host-based intrusion prevention system (HIPS)**
    - **Disabling ports/protocols**
    - **Default password changes**

- **Removal of unnecessary software**

Unit 3.0: Security Architecture

- ➔ **Compare and contrast security implications of different architecture models**
  - ◆ **Architecture and Infrastructure concepts**
    - **Cloud**
      - ○ **Responsibility Matrix:** documentation of responsibilities for security; whether the customer or provider is responsible
        - ◆ Software as a Service
        - ◆ Platform as a Service
        - ◆ Infrastructure as a Service



Responsibility matrix example

	SaaS	PaaS	IaaS	On Prem
Information and Data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and Identities	🟦	🟦	🟦	🟦
Identity and Directory Infrastructure	🟨🟦	🟨🟦	🟦	🟦
Applications	🟨	🟨🟦	🟦	🟦
Network Controls	🟨	🟨🟦	🟦	🟦
Operating Systems	🟨	🟨	🟦	🟦
Physical Hosts	🟨	🟨	🟨	🟦
Physical Network	🟨	🟨	🟨	🟦
Physical Datacenter	🟨	🟨	🟨	🟦

🟦 Customer Managed

🟨 Provider Managed

ps://ProfessorMesser.com

© 2023

        - ◆ On-Premise

      - ○ **Hybrid Considerations:** Mixed computing environment that combines compute infrastructure from the public cloud with an organization's private cloud or on-premise data center; more difficult to manage, but easier to protect more sensitive data while not putting less sensitive data behind too many barriers
        - ◆ <u>Network protection mismatch issue:</u> authentication across platforms, firewall configurations, server settings
        - ◆ <u>Different Security Monitoring</u>**:** logs are diverse and cloud-specific
        - ◆ <u>Data Leakage</u>: data is shared across the public internet

    - **Third Party Vendors:** companies that provide cloud computing services to customers without owning or operating their own infrastructure (i.e. Google Cloud Platform)
        - Beneficial to have a vendor risk management policy and incident responses
- **Infrastructure as code (IaC):** describes servers, networks, and applications as code, which allows you to modify the infrastructure and create versions in the same way you version application code.
- **Serverless:**
    - **Function as a Service (FaaS)**: applications are separated into individual, autonomous functions, which removes the OS from the equation; allows you to run specific applications when needed, saving time and money.
    - Usually managed by 3rd-party providers
- **Microservices (and APIs)**
    - **Monolithic Applications:** one big application that does everything (User interface, business logic, data input and output)
    - **Application Programming Interfaces:** Can be considered the "glue" for microservices, which works together to combine multiple microservices for a function; *highly* scalable, resilient, and secure
- **Network Infrastructure**
    - **Physical Isolation:** physically separating the original environment and the location where copies of data are stored, making it impossible to access this off-site data through the network, because no connections exist
        - **Air-gapped:** isolating a computer or network and preventing it from establishing an external connection
        - **Physical Segmentation:** separate devices (multiple units, separate infrastructure used to keep one device from being able to access another)
    - **Logical Segmentation:** separated logically instead of physically; cannot communicate between VLANs (Virtual Local Area Network) without a Layer 3 device / router
    - **Software-defined Networking (SDN):** Network devices have different functional planes and operation
        - Data Plane: Infrastructure layer – process the network frames and packets, forwarding, trunking, encrypting, NAT
        - Control Plane: Control Layer – manages the actions of the data plan; routing tables, session protocols

            - ◆ Management Plan: Application Layer – Configure and manage the device (SSH, browser)
            - ◆ We split the functions into separate logical units
                - Extend the functionality and management of a single device (good for cloud)
- **On-Premises:** puts the security burden on the client; On-site team can manage security, but can be expensive and difficult to control
- **Centralized vs. decentralized**
    - **Centralized:** control and decision-making authority is concentrated, which can allow for greater vulnerabilities
    - **Decentralized:** control and authority spread out amongst independent nodes
- **Containerization:** Applications can be packed with their dependencies and operate in separate environments called containers thanks to a lightweight virtualization technology called containerization. Compared to virtual computers, containers are lighter because they share the host machine's OS kernel.
- **Virtualization:** t allows users to run multiple virtual machines (VMs) on a single physical server or host machine. It enables the creation of separate and isolated environments, each with its own operating system (OS) and applications, on a shared hardware infrastructure.
    - Issue: each application needs its own operating system, which adds a lot of overhead, complexity, and cost
- **IoT:** an environment where devices gather and share information, process & analyze information, and act
- **Industrial control systems (ICS)/supervisory control and data acquisition (SCADA):** System of software and hardware that allows organizations to control and monitory industrial processes by directly interfacing with plant-floor machinery and viewing real-time data
    - Using a SCADA system, we can → control industrial processes locally & remotely | monitory, gather, and process real-time data | directly interact with IoT devices | record events into log file
    - <u>Requires extensive segmentation (no access from the outside)</u>
- **Real-Time Operating System (RTOS):** an operating system with a deterministic processing schedule (no time to wait for other processes → i.e. when braking a car); extremely sensitive to security issues
- **Non-Deterministic OS:** no single process that can suddenly grab all the resources of the system and take priority

        - **Embedded Systems:** hardware and software are all created as a self-contained and purpose built device (or to operate a part of a larger system)
            - Traffic Light Controllers, Digital Watches, Medical Imaging Systems
        - **High Availability:** keeps a system constantly running even if one part of the system runs; higher cost
    - **Considerations**
        - **Availability:**
            - System uptime
            - Want resources to be available, but only to the right people
        - **Resilience:**
            - Ability to recover from unavailability
            - **MTTR:** Mean Time To Repair – the length of time it takes to replace something that isn't available with something that is
        - **Cost:** how much money is required
        - **Responsiveness:** When we send a request to a service, how long does it take to get a response?
        - **Scalability:** how easily and quickly can we increase or decrease capacity (elasticity)
        - **Ease of Deployment:** How easy is it implement various moving parts (web servers, database, caching server, firewall)
        - **Risk Transference:** minimizing the loss, through Cybersecurity insurance
        - **Ease of Recovery:** how easily can you recover?
        - **Patch availability:** Software isn't static, what is the process to install updates?
        - **Inability to patch:** If patching isn't an option (like with embedded systems)
        - **Power:** What are your power requirements; Get a backup service like a UPS or generator.
        - **Compute:** An application's heavy lifting. Use multiple CPUs across multiple clouds. Additional complexity but enhanced scalability.
- **Given a scenario, apply security principles to secure enterprise infrastructure**
    - **Infrastructure considerations:**
        - **Device Placement:** placing the device somewhere to minimize physical access by unauthorized personnel, or ensure they are protected from environmental hazards
        - **Security Zones:** Implement security zones to segment the network based on trust levels and restrict lateral movement of threats between zones

- **Attack Surface:** reduce the attack surface by minimizing unnecessary services, ports, and protocols exposed to potential threats
- **Connectivity:** implement secure connectivity mechanisms, such as encrypted communication channels, to protect data transit
- **Failure Modes:** plan for failure modes and implement appropriate fail-open or fail-closed mechanisms to ensure network continuity and security in case of device or link failures
    - **Fail-Open:** in the case of malfunction, the default state will be "open" allowing traffic or users to pass through without proper authentication
    - **Fail-closed:** in the case of malfunction, the default state will be "closed" preventing authorized individuals from accessing resources
- **Device Attribute:** specific characteristics or properties of a device, such as its hardware specifications, configuration settings, operation capabilities, or unique identifiers
    - **Active:** actively participate in network traffic by inspecting, filtering, and blocking traffic based on predefined rules
    - **Passive:** devices that operate in a non-intrusive way, analyzing traffic without modifying it (i.e. generating logs or alerts based on anomalies or suspicious behavior)
    - **Inline:** devices that sit on the direct path of network traffic and actively control data flow (i.e. inline firewalls, or Intrusion Prevention systems)
    - **Tap/Monitor:** devices that are connected to the network in a non-intrusive manner, typically through a network tap or a switch port configured for monitoring; they receive a copy of network traffic for analysis & monitoring purposes w/o disrupting data flow
- **Network Appliances:** specialized devices used to perform specific functions within a network, such as routing, switching, firewalling, or intrusion detecting
    - **Jump Server:** a computer that spans 2+ networks, letting users to connect to it from network, and then "jump" to another
    - **Proxy Server:** acts as an intermediary b/w client devices and the internet
    - **Intrusion Prevention System (IPS):** monitors network traffic for malicious activity or security violations and has automated actions to prevent or mitigate potential threats

  - **Intrusion Detection System (IDS):** detects and alerts administrators to potential issues, but does NOT take automated actions to block them
  - **Load Balancer:** distributes incoming network traffic across multiple server to ensure optimal utilization, reliability, and performance
  - **Sensors**
- **Port Security**
  - **802.1X:** an IEEE standard for network access control (NAC) that provides an authentication framework for securing wired or wireless networks. It requires users or devices to authenticate before granted access.
  - **Extensible Authentication Protocol (EAP):** authentication framework that allows various authentication methods to be used within the 802.1X framework. (i.e. password-based, certificate-based, token-based)
- **Firewall Types**
  - **Web application firewall (WAF):** protect web application from common threats
  - **Unified Threat Management (UTM):** firewall for comprehensive security features like intrusion prevention, antivirus, and content filtering
  - **Next generation firewall (NGFW):** with advanced capabilities like application awareness and threat intelligence
  - **Layer 4/Layer 7:** firewalls for granular control over network traffic based on protocols and application-layer attributes
    - Layer 4 → Transport
    - Layer 7 → Application
- **Secure Communication/access**
  - **Virtual private network (VPN):** encrypted data traversing a public network
    - **Concentrator:** decrypts traffic
  - **Remote Access:** secure remote access mechanisms with strong authentication methods like MFA
  - **Tunneling:** encrypting data and adding new headers and trailers, wrapped in an IPsec header/trailer to tell where encrypted data starts and ends
    - **Transport Layer Security:** runs on tcp/443; provides encryption while the data is still in transit

            - **Internet protocol Security (IPSec):** Centralizes network management using software, enhancing WAN performance and agility
            - **Software-Defined Wide Area Network (SD-WAN):** manage the network connectivity to the cloud, does not address security concerns
            - **Secure access service edge (SASE): i**ntegrates network security and SD-WAN functionalities into a cloud-delivered service model for comprehensive security and connectivity.
        - **Selection of Effective Controls:** identifying and implementing security measures to mitigate risks and safeguard against potential threats

- **Compare and Contrast concepts and strategies to protect data**
    - **Data Types**
        - **Regulated:** data subject to specific regulations and compliance requirements
            - Managed by third party
            - Government laws and status
        - **Trade Secret:** confidential information that provides a competitive advantage
        - **Intellectual Property**: creations that are copyrighted and trademark, but may be publicly visible
        - **Legal Information:** court records
        - **Financial Information:** payment records
        - **Human- and non-human-readable:** Data easily understood by humans vs data not easily understood (i.e. barcodes, encoded data, images)
    - **Data Classifications**
        - **Sensitive:** Information that, if accessed by unauthorized persons, can result in a loss of security or a competitive advantage (different sensitivity depending on company, like hospital data vs something else)
        - **Confidential:** Holds trade secrets, intellectual property, source code, etc., strictly accessible to internal company personnel
        - **Public/Unclassified:** No restrictions on viewing, using, or redistributing data (i.e. first names, job descriptions)
        - **Restricted:** Data that if compromised or accessed without authorization could lead to criminal charges or cause irreparable damage to the company
        - **Private:** contains internal personnel or salary information
        - **Critical:** extremely valuable and restricted information that should always be available
    - **General Data Considerations**
        - **Data States**

  - **Data at Rest:** Data stored on a storage device
    - Could have encryption (whole disk encryption, database encryption, file or folder-level encryption)
  - **Data in Transit:** Data transmitted over the network also called data-in-motion
    - Not much protection as it travels
    - Could protect it with Network-based protection (firewall, IPS) or transport encryptions (Transport Layer Security or IPsec)
  - **Data in Use:** Data that is actively processing memory
    - System RAM, CPU registers and cache
    - Almost always decrypted
- **Data Sovereignty:** information is subject to laws and governance structures within the nation it is collected
  - Laws may prohibit where data is stored
    - **GDPR (General Data Protection Regulation):** data collected on EU citizens must be stored in EU
- **Geolocation:** geographical location of user & data
- **Methods to secure data**
  - **Geographic restrictions (Geofencing):** virtual boundaries to restrict data access based on location. Compliance with data sovereignty laws. Prevents unauthorized access from high-risk locations
    - Identify based on IP subnet & geolocation
  - **Encryption**
  - **Hashingl**
  - **Masking:** Replacing some or all data with a placeholder (i.e. hxxxx)
  - **Tokenization**
  - **Obfuscation:** Making data unclear or unintelligible
  - **Segmentation:** divide network into separate segments with unique security controls to limit potential damage
  - **Permission Restrictions:** define data access and actions through Access Control Lists

➔ **Explain the importance of resilience and recovery in security architecture**

- **High Availability:** ensures systems remain operational and accessible with minimal downtime
  - **Load Balancing:** distributes traffic between independent processing nods
  - **Clustering:** servers grouped together to operate as a single, unified system
- **Site Resiliency:** Recovery site is prepped where data is synchronized

- **Site considerations**
  - **Hot:** an exact replica, including hardware, of the original site
  - **Cold:** no hardware, empty building, where you will need to bring all the data to
  - **Warm:** Somewhere in between hot and cold
  - **Geographic Dispersion:** These sites should be physically different than the organization's primary location
    - Many disruptions can affect a large area (hurricane, flood)
- **Platform diversity:** every operating system contains potential security issues, which are also usually specific to just that OS, so best to use many different platform to "spread" risk
- **Multi-Cloud systems:** having multiple cloud providers in case for cloud outages and ensures that a breach with one provider would not affect the others
- **Continuity of Operations Planning (COOP):** The plan for when a disaster disrupts the norm, like using manual transactions, paper receipts, phone calls
- **Capacity Planning:** matching the supply to the demand
  - **People:** some services require human intervention (call services)
  - **Technology:** pick a technology that can scale (not all services can easily shrink and grow)
  - **Infrastructure:** the underlying framework (application servers, network services, physical devices, cloud-based devices)
- **(Recovery) Testing:** testing yourselves before an actual event
  - **Tabletop exercises:** talking through a simulator disaster
  - **Fall Over:** a test to check if the redundant systems work properly
  - **Simulation:** test with a simulated event (phishing attack)
  - **Parallel processing:** split a process through multiple CPUs
- **Backups**
  - **Onsite:** no internet link required, data is immediately available, generally less expensive than off site
  - **Offsite:** Transfer data over Internet or WAN link, data is available after a disaster, restoration can be performed from anywhere
  - **Frequency:** how often to backup (every week, day, hour?)
  - **Encryption:** protecting data through encryption, but must ensure you have all the recovery keys
  - **Snapshots:** a common recovery method for virtual machines; it takes a snapshot of an entire system
  - **Recovery:** mentioned above
  - **Replication:** ongoing, almost real-time backup (keep data synched in multiple locations)

    - **Journaling:** power goes out while writing data to storage and could lead data to be corrupted, so before writing to storage, make a journal entry. That way, if power goes out while writing the entry, the journal would be lost but data would not be corrupted

- **Power**
    - **Generators:** long-term power backup that can power an entire building
    - **Uninterruptible Power Supply:** short-term backup power for blackouts, brownouts, surges
        - Types:
            - **Offline/Standby UPS:** constantly runs on main power so when mainpower fails, it switches
            - **Line-Interactive UPS:** slowly increases voltage if you see a drop on main power line
            - **On-Line UPS:**

Unit 4.0: Security Operations

- **Given a scenario, apply common security techniques to computing resources**
  - **Secure Baselines:** foundationals et of security configurations and practices that establish a starting point for computing resources
    - **Establish:** create foundational security policies; these are often available from the manufacturer, application developer, operating system manufacturer, appliance manufacturer
    - **Deploy:** putting the baselines into action, hopefully automated
    - **Maintain:** determining best baseline in the instance something needs to be changed
  - **Hardening Targets**
    - **Mobile devices:** hardening checklists are available from manufacturers & updates help close vulnerabilities; segmentation can protect data (i.e. keeping company and user data separated)
    - **Workstations:** also have periodic updates (usually monthly patches); remove unnecessary software to limit threats
    - **Switches:** configure authentication (don't use default credentials), check with the manufacturer for security updates
    - **Routers:** configure authentication (don't use default credentials), check with the manufacturer for security updates
    - **Cloud infrastructures:** ensure we are using the least privilege principle (evaluate all services, network settings, application rights and permissions), install Configure Endpoint detection and Response, and have a backup (Cloud 2 Cloud = c2c)
    - **Servers:** Updates/Security Patches, ensure User accounts follow least privilege, and check for password complexity, limit network access, include anti-virus/anti-malware
    - **ICS/SCADA:** Supervisory Control and Data Acquisition System/Industrial Control System: PC manages equipment like power generation, refining, manufacturing, etc..; takes advantage of distributed control systems to give real-time information and have system control; Requires extensive segmentation
    - **Embedded Systems:** can be difficult to upgrade purpose-built appliances; consider putting them on their own separate network and have a firewall as well
    - **RTOS:** An operating system with a deterministic processing schedule; no time to wait for other processes (i.e. industrial equipment, automobiles, military environments); isolate the system to prevent access from other areas, and run it with the minimum necessary services

  - **IoT Devices:** change defaults
- **Wireless Devices**
  - **Installation considerations**
    - **Site Surveys:** determine existing wireless landscape, identify existing access points, and work around existing frequency
    - **Heat maps:** identify wireless signal strengths
  - **Mobile solutions**
    - **Mobile device Management (MDM):** managing company owned and user owned mobile devices; allows the system administrator to require certain application or rollout certain policies
    - **Deployment Models**
      - **Bring your own device (BYOD):** employees use personal device for work, which is more cost-effective for the employer, but then there is reduced control over security and device management
      - **Corporate-owned, personally enabled (COPE):** Company provides devices for employees, greater control
      - **Choose your own device (CYOD):** Similar to COPE, but with the user's choice of device
    - **Connection methods**
      - **Cellular:** Mobile devices ("Cell" phones / 4G, 5^)
        - Separate land into "cells", antenna coverage a cell with certain frequencies. This causes security concerns such as traffic monitoring, location tracking, and worldwide access to mobile device
      - **Wi-Fi:** same security concerns as other Wi-Fi devices; data capture risk, on-path attack risk
      - **Bluetooth:** high speed communication over short distances
        - PAN (personal area network); formal pairing prevents unauthorized access
  - **Wireless security settings**
    - **Wi-Fi Protected Access 3 (WPA3):** GCMP block cipher mode which has stronger encryption, and requires mutual authentication, creates shared session key without sending the key across the network
      - No 4-way handshake, no hashes, no brute force
      - Simultaneous authentication of equals (SAE): a diffie-hellman derived key exchange with an authentication component, everyone uses a different session key

      - **AAA/Remote Authentication Dial-In User Service (RADIUS):** Authenticates credentials: identification → authentication → authorization → accounting
      - **Cryptographic Protocols**
      - **Authentication Protocols**
    - **Application Security**
      - **Input validation:** check and correct all input (normalization)
      - **Secure cookies:** cookies are used for tracking, personalization, session management, and are not usually a security risk, but some browsers will use secure cookies and will only transfer cookies over HTTPS
        - Sensitive information is not put in cookies
      - **Static code analysis:**
        - Static Application Security Testing (SAST): searches for vulnerabilities like buffer overflows, database injections, etc
      - **Code signing:** digital signature validates the identity of the software author or publisher and verifies that the file has not been altered or tampered with since it was signed; contains identity and public key of publisher
    - **Sandboxing:** applications cannot access unrelated resources (they can only play in their own sandbox); used in many different forms (virtual machines, mobile devices, browser iframes, window user account control)
    - **Monitoring:** real-time information, view blocked attacks, audit the logs, anomaly detection
- **Explain the security implications of proper hardware, software, and data asset management**
  - **Acquisition/procurement process:** The acquisition and procurement process begins with a strategic evaluation of an organization's technological needs. Whether it involves new hardware, software, or data assets, comprehending these requirements is crucial to ensuring that all potential purchases are compatible with our existing systems and monitoring tools; also identifying deficiencies in the existing infrastructure, evaluating potential upgrades, and defining the scope of the acquisition
    - Change management, vendor selection, total cost of ownership, risk assessment, compliance alignment
  - **Assignment/accounting**
    - **Ownership:** each asset assigned to a person or group is known as an "owner"; avoids ambiguity, aids troubleshooting, upgrades, and replacements

- **Classification:** categorizing assets into critical, essential, and non-essential assets; allows us to take proper measures when it comes to securing sensitive vs non-sensitive aspects
- **Monitoring/asset tracking**
    - **Inventory:** record of all assets
    - **Enumeration:** process of assigning unique identifiers or serial numbers to assets
- **Disposal/Decommissioning**
    - **Sanitization:** throughout process to make data inaccessible and irretrievable from storage medium using traditional forensic methods
    - **Destruction:** goes beyond sanitization, ensure physical device is unusable
    - **Certification:** acts as proof that data or hardware has been securely disposed of; important for organizations with regulatory requirements; creates an audit log of sanitization, disposal, or destruction
    - **Data Retention:** deciding what to keep and for how long; data has a lifecycle from creation to disposal

➔ Explain various activities associated with vulnerability management

- **Identification methods**
    - **Vulnerability scan:** usually minimally invasive, checking if the potential for an attack exists (i.e. like a port scan which just hecks what is open and what is closed, identifying all systems, and testing from inside and outside threats, and categorize threats by severity)
    - **Application security**
        - **Static Analysis:** Static Application Security Testing – help identify security flaws, where buffer overflows can occur, database injections, etc.., but it is still necessary to verify each finding
        - **Dynamic Analysis:** also known as fuzzing; send random input to an application (fault-injecting, robustness testing, syntax testing, negative testing)
        - **Package monitoring:** some applications are distributed in a package, which could be a part of an executable or standalone; confirm the package is legitimate and does not have any embedded vulnerabilities
    - **Threat feed**
        - **Open-Source Intelligence (OSINT):** publicly available sources, internet, government data (public hearings, reports, websites, etc.), commercial data (maps, financial reports, databases)
        - **Proprietary/Third-party:** companies that has already compiled the threat information for purchase; threat intelligence services (threat analytics, correlation across different data sources)

-
  - **Information-sharing organization:**
    - public threat intelligence → often classified information
    - Private threat intelligence → private companies have extensive research
    - **Cyber Threat Alliance (CTA):** members upload specifically formatted threat intelligence, CTA scores each submission and validates across other submissions, other members can extract the validated data
  - **Dark web:** overlay network that use the Internet; requires specific software and configurations to access
    - Contains hacking groups and services (activities, tools and techniques, credit card sales, accounts and passwords)
- **Penetration Testing:** simulating an attack where we attempt to exploit vulnerabilities
  - **Rules of Engagement:** formal list of rules of the test parameters (i.e. types of tests allowed, times you are allowed to try and breach, emergency contacts, how to handle sensitive information, in-scope and out-of-scope devices or applications)
- **Responsible disclosure program:** process that allows individuals to safely report found vulnerabilities to a team, before publicly documenting them
  - **Bug bounty program:** a reward for discovering vulnerabilities, earn money for hacking a system, document the vulnerability to earn cash; a controlled information release (researcher reports vulnerability, manufacturer creates a fix, vulnerability is announces)
- **System/process audit**

- **Analysis**
  - **Confirmation**
    - **False Positive:** a vulnerability is identified that doesn't really exist
    - **False Negative:** a vulnerability is said to not exist when it does
  - **Prioritize:** not all vulnerabilities are critical or share the same priority
  - **Common Vulnerability Scoring (CVSS):** a scoring system , synchronized with the CVE list, and determines how critical a vulnerability is from 0 to 10 (most critical)
  - **Common Vulnerability Enumeration (CVE):** the vulnerabilities can be cross-referenced online
  - **Vulnerability classification:** performs a vulnerability scan that looks through vulnerabilities using signatures (application, web, and networks cans)

  - **Exposure factor:** loss of value or business activity if the vulnerability is exploited (usually expressed as a percentage)
  - **Environmental variables:** what type of environment is associated with this vulnerability? (internal server, public cloud, test lab)
    - Prioritize based on environment, and patch frequency varies,
  - **Industry/organizational impact:** the consequences of exploits (i.e. a DDoS attack of a Power Utilities vs cafe)
  - **Risk tolerance:** the amount of risk acceptable to an organization
- **Vulnerability response and remediation**
  - **Patching:** the most common mitigation technique; usually have a schedule
    - "We know a vulnerability exists, here is a patch file to install to fix it"
  - **Insurance:** Cybersecurity insurance coverage (lost revenue, data recovery cost, money lost to phishing, privacy lawsuit costs)
    - Does NOT cover intentional acts, funds transfers, etc..
  - **Segmentation:** limit the scope of an exploit by separating devices into their own networks/VLANS
  - **Compensating controls:** optimal security method may not be available, and so we compensate by
    - Disabling the problematic service, revoke access to the application, limit external access, modify internal security controls and software firewalls
  - **Exceptions and exemptions:** Removing the vulnerability is optimal, but not everything can be patched; not all vulnerabilities share the same severity → it may be decided that patching a vulnerability is not a reasonable risk
- **Validation of remediation:** The vulnerability is patched, but has it been removed?
  - **Rescanning:** perform an extensive vulnerability scan
  - **Audit:** check remediated systems to ensure the patch was successfully deployed
  - **Verification:** manually confirm the security of the system
- **Reporting:** on-going checks are required to discover new vulnerabilities; usually managed with automation, and includes continuous reporting on
  - Number of system identified
  - Systems patched vs unpatched
  - New threat notifications
  - Errors, exceptions, and exemptions

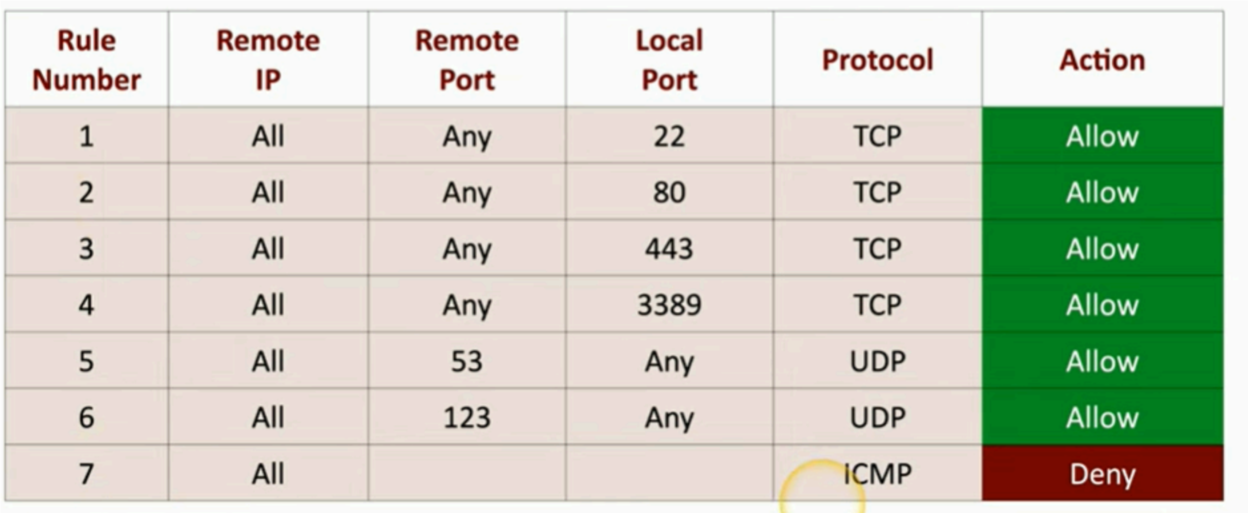
- ➔ Explain security alerting and monitoring concept and tools
  - **Monitoring computing resources**
    - **Systems:**
      - Authentication points - logins from strange places
      - Server monitoring - service activity, backups, software versions
    - **Applications:**
      - Availability - uptime and response times
      - Data transfers = increases or decreases in rates
      - Security notifications - from the developer/manufacturer
    - **Infrastructures**
      - **Remote Access Systems** - employees, vendors, guests
      - **Firewall and IPS reports -** increase or type of attack
  - **Activities**
    - **Log aggregation:** consolidates many different logs to a central database (servers, firewalls, VPN concentrators, SANs, cloud services); Allows correlation between diverse systems (view authentication and access, track application access, measure and report on data transfers)
    - **Alerting**
    - **Scanning:** constantly checking threat landscape, since new vulnerabilities always appear and systems/people are always moving; actively check OS types and versions, device driver versions, installed applications, and potential anomalies, and store it all
    - **Reporting:** analyze the collected data and create "actionable" reports, provide status information (number of devices up to date/in compliance, devices running older OS) and determine the next best steps
      - Ad-Hoc Reporting: reporting what COULD happen in the future to prepare for the unknown
    - **Archiving:** it takes an average of about 9 months to identify and contain a breach; may be mandated by state or federal law to record attacks
    - **Alert Response and remediation/validation:** real-time notification of security events and forming actionable data (keep the right people informed, enable quick response and status information) and notify relevant people
      - **Quarantine:** A foundational security response, prevent a potential issue from spreading
      - **Alert tuning:** ensure alerts are accurate, prevent false positive and false negative
    - **Tools**
      - **Security Content Automation Protocol (SCAP):** Many different security tools on the market with their own ways of evaluating

threats, so SCAP allows tools to identify and act on the same criteria

    - Maintained by NIST (National Institute Standards and Technology)

- **Benchmarks:** apply security best-practices to everything
    - Operating systems, cloud providers, mobile devices, etc.
    - The bare minimum for security settings
- **Agents/agentless:** check to see if the device is in compliance by installing a software agent onto the device or run an on-demand agentless check
    - Agents: provide more detail, but must be maintained and updated
    - Agentless: runs without a formal install, executes, and then disappears after completion; it does not require ongoing updates but will not inform or alert if not running
- **Security information and event management (SIEM):** logging of security events and information; good for log aggregation and long-term storage and for linking diverse data types and for making forensic reports
- **Data loss prevention (DLP):** looks for and blocks any type of data that you don't want running on your network (i.e. social security numbers, credit card numbers, medical records); stops the data before the attacker gets it
- **Simple Network Management Protocol (SNMP) traps:** a message sent from a network device to an SNMP management system once the trap is triggered (i.e. if the # of CRC errors increases by 5, send a trap so the monitoring station can react immediately)
    - **SNMP:** a database of data (MIB) - Management Information Base which contains OIDS - Object Identifiers; requests statistics from a device (server, firewall, workstation, switch, router, etc.)
- **NetFlow:** Standard collection method for monitoring traffic statistics from all traffic flows; contains a <u>probe</u> that watches network communication and summary records are sent to the <u>collector;</u> there is usually a separate reporting application
- **Vulnerability Scanners:** minimally invasive; port scan; identifying systems/security devices; test from the outside and inside

- Given a scenario, modify enterprise capabilities to enhance security
  - **Firewall**
    - **Network-based firewall:** sits inline your network and makes decisions whether an application should be allowed or disallowed based on its port number (traditional firewall) or by the application itself (New Generation Firewall)
      - Some firewalls may also encrypt traffic (VPN between sites)
      - Most firewalls can be layer 3 devices
      - **Next Generation Firewall:** Layer 7 Firewall (Application Layer) which recognizes the specific application being used and then makes a decision; also known as Application layer gateway/Stateful multilayer inspection/Deep packet inspection; requires some advance decodes as every packet must be analyzed, categorized, and then have a decision for it
      - **Traditional Firewalls:** made forwarding decisions based on protocol (TCP or UDP) and port number
    - **Rules:** a logical path, usually top-to-bottom (specific rules at the top of the firewall)
      - Might contain an implicit deny (any traffic that does not match a rule, automatically denies, even if you didn't explicitly put that there)
    - **Access Control Lists (ACL):** Allow or disallow traffic, groupings of categories (Source IP, Destination IP, port number, time of day, application, etc.)



Rule Number	Remote IP	Remote Port	Local Port	Protocol	Action
1	All	Any	22	TCP	Allow
2	All	Any	80	TCP	Allow
3	All	Any	443	TCP	Allow
4	All	Any	3389	TCP	Allow
5	All	53	Any	UDP	Allow
6	All	123	Any	UDP	Allow
7	All			ICMP	Deny

- **Ports/Protocols:**
  - **Web server:** tcp/80 || tcp/443

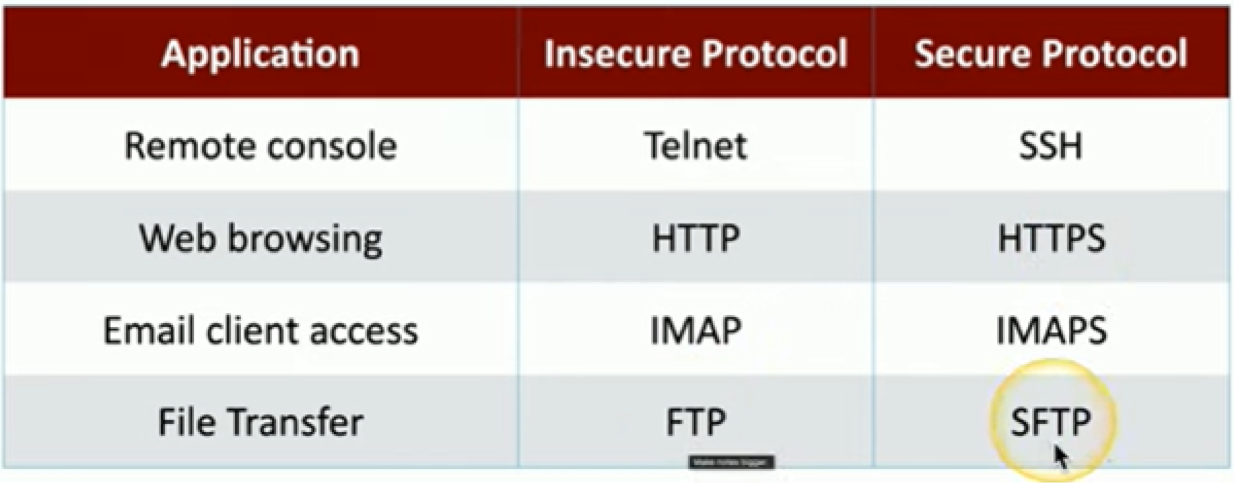
    - **SSH Server:** tcp/22
    - **Microsoft RDP:** tcp/3389
    - **DNS Query:** udp/53
    - **NTP:** udp/123
  - **Screened subnets:** an additional layer of security between you and the internet, usually put in the ingress/egress point of the internet (the point that separates the internet from the internal part of the network)
    - Ensures public access to public resource and private data remains inaccessible
- **IDS/IPS:** Intrusion Prevention System
  - **Trends:**
    - Anomaly-based: building a baseline fo what's normal, and then flag unusual traffic patterns
  - **Signatures:** looking for a perfect match of traffic, which you then have pre-defined rules for
- **Web Filter** (i.e. think about parental control, or anti-malware)
  - **Agent-based:** install client software on the user's device, usually managed from a central console; beneficial because users can be located anywhere and the local agent makes the filtering decisions
  - **Centralized proxy:** Sits between the users and the external network (internet) and receives the users requests and sends the request on their behalf. The proxy then receives the response, and determines whether or not to send it back to the user. This is very useful for caching information, access control, URL filtering, and content scanning
    - **Forward Proxy: ("internal proxy")** A proxy that is in the internal network with the organization
  - **Universal Resource Locator (URL) Scanner:** Allow or restrict based on Uniform Resource Locator (also known as URI) using an Allow list / block list
  - **Content Categorization:** filtering based on the category of a site
  - **Block Rules:** Based on specific URL, or category of site content (usually divided into over 50 different topics)
  - **Reputation:** Filter URLs based on perceived risk (Good reputation = Allowed, Bad reputation = blocked)
    - Automated Reputation: sites are scanned and assigned a reputation
    - Manual Reputation: Managers can administratively assigned a reputations
- **Operating System Security**
  - **Active Directory:** a database of everything on the network (i.e. computers, user accounts, file shares, printers, etc.). We can manage

authentication using AD credentials and can determine which users can access certain resources

- **Group Policy:** Manage the computers or users with group policies, which allows us to set individual permissions for different users and individual devices. Typically run from a central console (Group Policy Management Editor)
- **SELinux: ("Security-Enhanced Linux")** Security patches for the Linux kernel; Linux traditionally uses a Discretionary Access Control (DAC) device, which means the user has their own discretion to be able to assign rights and permissions to different resources in the operating system. In many secure environments, a Mandatory Access Control (MAC) is added to implement the principle of least privilege; Open-source

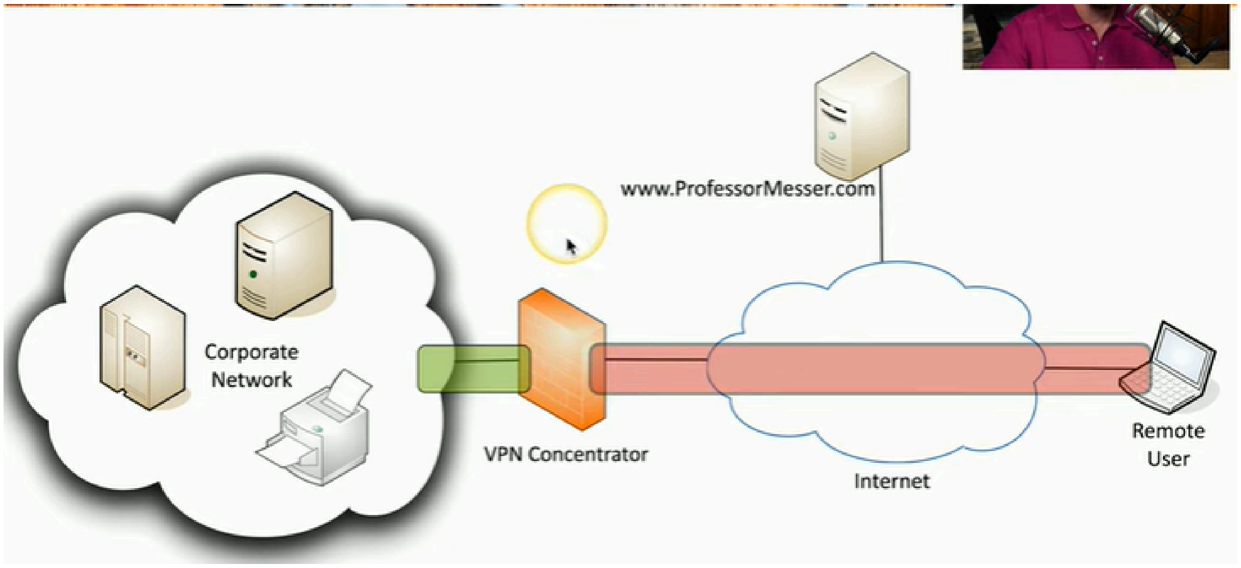
◆ **Implementation of secure protocols**

- **Protocol selection:** Since some protocols aren't encrypted (Telnet, FTP, SMTP, IMAP), use a secure application protocol (built-in encryption)



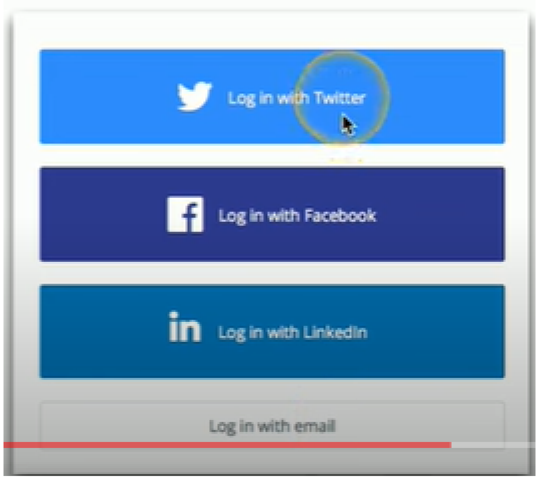
Application	Insecure Protocol	Secure Protocol
Remote console	Telnet	SSH
Web browsing	HTTP	HTTPS
Email client access	IMAP	IMAPS
File Transfer	FTP	SFTP

- **Port selection:** It's common to run secure and insecure applications on different ports (ie. HTTP/Port 80 vs HTTPS/Port 443_
- **Transport methods:** Encrypt everything over the current network transport
  - 802.11 Wireless: Open-access point – no transport level encryption vs WPA3 – all user data is encrypted
  - VPN: create an encrypted tunnel, all traffic is encrypted and protected (often requires 3rd party services)



- **DNS filtering:** Before connecting to a website, get the IP Address and then perform a DNS lookup. DNS is updated with real-time threat intelligence which are both commercially and publicly available. Harmful sites are not resolved, no IP address = no connections
- **Email security**
    - **Domain-based Message Authentication Reporting and Conformance (DMARC):** An extension of SPF and DKIM; The domain owner decides what receiving email servers should do with emails not validated using SPF and DKIM. That policy determining whether the email should be accepted, sent to spam, or rejected is then written into a DNS TXT record. Also allows us to set a destination for Compliance Reports so the domain owner can see how emails are received (how many messages are being validated properly vs spoofing)
    - **DomainKeys Identified Mail (DKM):** A mail server digitally signs all outgoing mail and the public key is in the DKIM (domain keys identified mail) TXT record; the signature is validated by the receiving mail servers and is not usually seen by the end user
    - **Sender Policy Framework (SPF):** Sender configures a list of all servers authorized to send emails for a domain; List of authorized mail servers are added to a DNS TXT record (receiving mail servers perform a check to see if incoming mail really did come from an authorized host)
    - **Gateway:** Evaluates the source of the inbound email messages, blocks it at the gateway before it reaches the user, and determines whether it is spam or not (on-site or cloud-based)
- **File Integrity Monitoring (FIM):** Monitor important operating system and application files and identify when changes occur

        - In Windows, this is done on demand using SFC (System File Checker) which scans all important OS files
        - In Linux, it is done using Tripwire
    - **DLP:** Prevent sensitive data from being transported
        - DLP on your computer: Data in use/Endpoint DLP
            - USB blocking: allow or deny certain tasks
        - DLP on your network: Data in motion
    - **Network Access Control (NAC):**
        - Control the edge (where the inside of the network meets the outside/internet) by using a firewall
        - **Endpoint:** Device used by the user
    - **Endpoint Detection and Response (EDR):** a different method of threat protection; Detects threats through behavioral analysis, machine learning, and process monitoring and runs as an agent on the endpoint. It also provides root cause analysis which helps us determine *why* a virus got onto the system. It also automates the response to the threat.
        - **XDR (Extended Detection and Response):** evolution of EDR which provides missed detections, categorizes false positives, and long investigation times
    - **User behavior analytics:** Watch users, hosts, network traffic, data repositories, etc. and creates a baseline of normal activity to easily find when abnormal events occur
- Given a scenario, implement and maintain identity and access management
    - **Provisioning/deprovisioning user accounts:** the user account creation and removal process; occurs for certain events like hiring, transfers, promotions, job separations. This is an important part of the IAM process (identity and management) to limit access
    - **Permission assignments and implications:** Each entity gets limited permissions that is just enough to do their job. In addition, storage and files can be private to that user, even if the device is shared.
    - **Identity proofing:** verifies a User's identity
        - Resolution: Who the system thinks you are
        - Validation: gathering information from a user
    - **Federation:** provide network access without using local authentication database. Third party can establish a federated network to allow authentication and authorization between the two organizations.



- **Single sign-on (SSO):** provide credentials one time to get access to all available or assigned resources
  - **Lightweight Directory Access Protocol (LDAP):** Protocol for reading and writing directories over an IP network
  - **Open authorization (OAuth):** Authorization framework that determines what resources a user will be able to access. Still requires a third party application to handle authentication.
  - **Security Assertions Markup Language (SAML):** open standard for authentication and authorization; You can authenticate through a third-party to gain access. Involves three different devices, the User device, the resource server, and the authorization server. THe client accesses resource, which sends request to the authorization server, which asks for credentials, checks for credentials, creates a SAML token for the USER, who then presents can the token to the resource server and gain access
    - Not originally designed for mobile devices
- **Interoperability:** the ability of different systems, devices, networks, etc. to securely share and use information without inconvenience to the user or security concerns
- **Attestation:** evidence or proof of being (i.e. passport)
- **Access controls**
  - **Mandatory:** The operating system limits the operation on an object based on security clearance level (Confidential, secret, top secret, etc.). The administrator decides who gets access to the what security levels, and the User cannot modify that
  - **Discretionary:** The User that creates the data has the control on who can access and modify the data (i.e. when sharing a Google doc file); Allows flexible access control, though weak security

- **Role-based:** Modifying who has access to certain rights and permissions based on your role (Manager, director, team lead, project manager)
- **Rule-Based:** access is determined through system-enforced rules (i.e. Lab network is only available from 9AM and 5PM, or that the site can only be completed through Chrome)
- **Attribute-based:** Considers many parameters (i.e. resource information, IP address, time of day, desired action, relationship to the data, etc.) to determine what kind of control the user has
- **Time-of-day restrictions:** restrict access during certain times of days of the week
- **Least privilege:** rights and permissions should be set to the bare minimum needed to complete objectives

◆ **Multi Factor Authentication:** prove who you are using more than one factor

- **Implementation**
  - **Biometric:** fingerprint, etc.
  - **Hard/Soft authentication tokens:** hard tokens = physical device; soft tokens = software
  - **Security keys:** physical device sued for MFA. combines soft token and hard token principles
- **Factors**
  - **Something you know (Knowledge):** relies on information a user can recall
  - **Something you have (Ownership):** relies on the user presenting a physical item to authenticate themselves
  - **Something you are (Characteristics):** a fingerprint, signature, or something else unique to a person as an individual
  - **Somewhere you are (Location):** relies on a user being in a certain area before access is granted
- **Password Concepts**
  - **Password best practices**
    - **Length:** longer = better
    - **Complexity:** mix upper and lower case letters, numbers, special characters to prevent brute force or guessing
    - **Expiration:** password works for a specified amount of time, and after that time, password no longer works
    - **Age:** how long since a password was last modified
  - **Password Managers:** a database to store all passwords in a single database
  - **Passwordless:** authentication without a password (i.e. facial recognition, security key)

- **Privilege Access Management tools**
  - **Just-in-time permissions:** Administrative access granted for a limited amount of time
  - **Password vaulting:** primary credentials that would allow someone access to a system are generated into a secret vault
  - **Ephemeral credentials:** temporary credentials

- **Explain the importance of using automation and orchestration related to secure operations**
  - **Use cases of automation and scripting**
    - User Provisioning: assign access to specific resources
    - Resource Provisioning: assign access to specific resources
    - Guard Rails: a set of automated validations to limit behavior and responses to reduce errors
    - Security Groups: assign (or remove) group access, constant audits without human intervention
    - Ticket creation: automatically identify issues, script email submissions into a ticket
    - Escalation: correct issues before involving (escalating the problem to) a human
    - Enabling/Disabling services and access: prevents “set and forget”
    - Continuous Integration and testing
    - Integrations and Application Programming Interfaces (APIs)
  - **Benefits**
    - Efficiency/Time saving
    - Enforcing baselines
    - Standard Infrastructure configurations: use a script to build a default router configurations, add firewall rules to a new security appliance, IP configurations, security rules, standard configuration options
    - Scaling in a secure manner
    - Employee Retention: automate the boring stuff, ease workload
    - Reacting time: reacts to problems faster than humans
    - Workforce Multiplier
  - **Other Considerations**
    - Complexity: many moving parts
    - Cost: costs money to create script and then more to implement
    - Single Point of Failure: what happens if the script stops working?
    - Technical Debt: patching problems may push the issue down the road
    - Ongoing supportability: script good for now, but maybe not for the future
- **Explain appropriate Incident Response Activities**
  - **Process**

        - **Preparation:** communication methods (phone & contact information), incident handling hardware & software, incident analysis resources, incident mitigation software, set of policies for incident handling
        - **Detection:**
        - **Analysis:** web server log, exploit announcement
        - **Containment**
        - **Eradication**
        - **Recovery**
        - **Lessons learned**
    - **Training**
    - **Testing**
        - **Tabletop Exercise**
        - **Simulation**
    - **Root Cause analysis**
    - **Threat Hunting**
    - **Digital Forensics**
        - **Legal Hold:** a legal technique to preserve relevant information
            - Custodian: request for legal hold is usually sent to the custodian, who has access to all of the data associated with this particular request
            - All data acquired is **ESI (Electronically Stored Information)**
        - **Chain of Custody:** maintains integrity by keeping track of everyone who contacts the evidence, using hashes and digital signatures to avoid tampering
        - **Acquisition:** obtaining data from Disk/RAM/Firmware/OS Files; for virtual systems, get a snapshot
        - **Reporting:** document the findings
        - **Preservation:** handling the evidence; isolate and protect the data; manage the collection process by working from copies
        - **E-Discovery:** Electronic discovery; the process of collecting, preparing, reviewing, interpreting and produce electronic documents; gathers data required by legal process and works together with digital forensics
- **Given a scenario, use data sources to support an investigation**
    - **Security log files:** displays blocked and allowed traffic flows, exploit attempts, blocked URL categories, DNS sinkhole traffic
    - **Log data**
        - **Firewall logs:** traffic flows through the firewall
            - Source/destination IP, port numbers, disposition
        - **Application logs:** specific to the application
            - Windows – Event Viewer

      - Linux – /var/log
    - **Endpoint logs:** Logon events, policy changes, system events, processes, account management, directory services
    - **OS-Specific security logs:** Monitoring apps, brute force, file changes, authentication details
    - **IPS/IDS logs:** contains information about predefined vulnerability
    - **Network logs:** switches, routers, access points, VPN concentrators, Network changes (routing updates, authentication issues, network security issues)
    - **Metadata:** data that describes other data sources (i.e. in Emails – header details, sending servers, destination address)
  - **Data sources**
    - **Vulnerability Scans:** finding devices with lack of security controls (i.e no firewalls, no antivirus, no anti-spyware) or that are misconfigured or finding known vulnerabilities
    - **Automated Reports:** Most SIEMS include a report generator
    - **Dashboards:** real-time status information/summaries on a single screen
    - **Packet Captures**

5.0 Security Program Management and Oversight

- **Summarize elements of effective security governance**
  - **Guidelines:** What rules are you following to provide CIA?
  - **Policies:** Security policies answer "what" we are doing and "why" we are doing it
    - **Acceptable use policy (AUP):** defines what users are able to do with the technology provided to them
    - **Information security policies**
    - **Business continuity:** An alternative plan for when technology/resources used to perform business tasks cannot be used (i.e. paper receipts, manual transactions)
    - **Disaster Recovery:** The plan for natural disasters, technology or system failures, or human-created disasters (i.e. recovery location, data recovery method, app restoration)
    - **Incident Response:** How do we deal with different security incidents? (i.e. clicking on a malicious link in email, DDoS / Botnet attack, confidential information is stolen)
    - **Software Development Lifecycle (SDLC):** Many ways to get from an idea to an app
      - Waterfall: linear way to create applications [requirements, design, develop, test, deploy, maintain]
      - Agile: cyclical, faster

    - **Change Management:** how to make a change to software, firewall, etc.
- **Standards:** a formal definition for using technologies and processes
    - **Password:** what makes a good password? How to change password?
    - **Access Control:** determine which information, at what time, a user can access
    - **Physical Security:** rules and policies regarding physical security controls
    - **Encryption:** standard for encrypting and securing data
- **Procedures**
    - **Change Management:** a formal process for managing change to avoid downtime, confusion, and mistakes
    - **Onboarding/Offboarding:** bringing in someone to the team and removing someone from the team
    - **Playbooks:** conditional steps to follow in the case of a particular event (i.e. data breaches, ransomware)
        - Often integrated with a SOAR platform (Security orchestration automation and response)
- **External Considerations**
    - **Regulatory:** mandated processes
        - Sarbanes-Oxley Act (SOX): The Public Company Accounting Reform and Investor Protection Act of 2002
        - HIPAA
    - **Legal:** security team is tasked with legal responsibilities (i.e. security breaches)
    - **Industry:** Electrical power vs Medical
    - **Local/Regional**
    - **National**
    - **Global**
- **Monitoring and revision:** processes and procedures must change to take in account emerging issues
- **Types of governance structures**
    - **Boards:** a panel of specialist that set the tasks or requirements for the committee to follow
    - **Committees:** subject-matter experts, consider input from the board, determines next steps for a topic at hand, presents the results to the board
    - **Government entities:** a different kind of machine for legal concerns, administrative requirements, political issues, and are open to the public
    - **Centralized/decentralized:**
        - **Centralized:** governance is located in one group of decision makers

        - **Decentralized:** decision making process around to other individuals or locations
  - **Roles and responsibilities for systems and data**
    - **Owners:** accountable for specific data, often a senior assess (ie. VP of Sales owns the customer relationship data & treasurer owns the financial information)
    - **Controllers:** manages how the data is used
    - **Processors:** processes data on behalf of the data controller (often a 3rd party or different group)
    - **Custodians/Stewards:** responsible for data accuracy, privacy, and security; works directly with the data (gives sensitivity labels to data, ensures compliance w/ applicable laws, manages access rights to the data, implements security controls)
- **Explain elements of the risk management process**
  - **Risk Identification**
  - **Risk assessment**
    - **Ad hoc:** an assessment for one specific purpose/attack typ
    - **Recurring**
    - **One-time**
    - **Continuous**
  - **Risk Analysis**
    - **Qualitative:** Identify significant risk factors, asks opinions about the significance, display visually with traffic light grid or similar method
    - **Single Loss Expectancy (SLE):** the monetary loss if a single event occurs?
      - Asset Value (AV) x Exposure Value (EF)
    - **Annualized Rate of Occurrence (ARO):** how often a risk will occur in a single year
    - **Annual Loss Expectancy:** ARO x SLE
    - **Asset Value:** the value of the asset to the organization (includes cost of the asset, effective on company sales, potential regulatory fines)
    - **Probability:** A quantitative measurement, statistical, can be based on historical performance
    - **Likelihood:** A qualitative measurement of risk (Risk, possible, almost certain)
    - **Exposure Factor:** the percentage of the value that was lost due to that risk
    - **Impact:** Life (most important consideration), Property (risk to buildings and assets), Safety, Financial
  - **Risk Register:** identify and document the risk associated with each step, apply possible solutions, monitor results

    - **Key risk indicators:** identify risks that could impact an organization
    - **Risk owners:** each indicator is assigned someone to manage the risk
    - **Risk threshold:** the cost of mitigation is at least equal to the value gained by mitigation
  - **Risk tolerance:** an acceptable variance from the risk appetite
  - **Risk appetite:** a broad description of risk-taking deemed acceptable & the amount of accepted risk before taking any action to reduce that risk
    - **Expansionary**
    - **Conservative**
    - **Neutral**
  - **Risk management strategies**
    - **Transfer:** move risk to another party (insurance)
    - **Accept**
      - **Exemption:** a security policy or regulation cannot be followed and so an exemption is required
      - **Exception:** Internal security policies are not applied
    - **Avoid:** stop participating in high-risk activity
    - **Mitigate:** decrease the risk level
  - **Risk Reporting:** a formal document, identifies risks, detailed information for each risk
  - **Business Impact Analysis**
    - **Recovery Time Objective (RTO):** how long will it take to get up and running
    - **Recovery Point Objective (RPO):** defines how much data loss a company can tolerate after a disruptive event before it exceeds what is acceptable to the organization
    - **Mean Time to Repair (MTTR):** how long it takes to fix
    - **Mean Time Between Failures (MTBF):** time between outages, can be used to predict next courage, total uptime / number of breakdowns
- **Explain the processes associated with third-party risk assessment and management**
  - **Vendor assessment**
    - **Penetration testing:** stimulate an attack by trying to exploit vulnerabilities
    - **Right-to-audit clause:** a legal agreement to have the option to perform a security audit at any time
    - **Evidence of Internal Audits:** evaluate the effectiveness of security controls with a 3rd party
    - **Independent Assessments:** bring in someone else to evaluate security and provide recommendations

        - **Supply chain analysis:** get a product from a supplier to customer, evaluate coordination b/w groups, identify areas of improvement, assess the IT systems supporting the operation, document the business process changes
    - **Vendor Selection**
        - **Due diligence:** investigating a company before deciding to work with them
        - **Conflict of Interest:** a personal interest that could compromise judgment
    - **Agreement Types**
        - **Service-level agreement (SLA):** minimum terms for services provided, up-time, response time, commonly used b/w customers and service providers
        - **Memorandum of Agreement (MOA):** both sides conditionally agree to the objectives & can be a legal document but without legal language
        - **Memorandum of Understanding (MOU):** broad goals about what the two groups want to accomplish, may include confidentiality statements, informal letter of intent (not a signed contract)
        - **Master Service Agreement (MSA):** legal contract and agreement of terms, a broad framework to cover later transactions
        - **Work Order (WO)/Statement of Work (SOW):** specific list of items to be completed, used in conjunction with MSA, details the scope of the job, location, deliverables schedule, acceptance criteria, etc
        - **Nondisclosure agreement (NDA):** confidentiality agreement between parties
            - Unilateral: one-way NDA
            - Bilateral: both parties remain quiet
        - **Business partners agreement (BPA):** going into business together, owner stake, financial contract, who gets ot make decisions? Prepare for contingencies
    - **Vendor monitoring:** ongoing management of the vendor relationship, reviews should occur on a regular basis with both quantitative and qualitative analysis
    - **Questionnaires:** an important part of due diligence and get ongoing monitoring, ask about security related questions
    - **Rules of engagement (ROE):** defines the purpose and scope of penetration testing
- **Summarize elements of effective security compliance**
    - **Compliance reporting**
        - **Internal:** monitor and report on organizational compliance efforts, used to provide details to customers or potential investors
            - CCO (Central Compliance Officer)

    - **External:** Documentation required by external or industry regulators, may require annual or ongoing reporting, missing or invalid reporting could result in fines/sanctions
- **Consequences of non-compliance**
    - **Fines:** financial fee
    - **Sanctions:**
    - **Reputational damage**
    - **Loss of license:** significant economic sanctions, organization cannot sell products,
    - **Contractual impacts:** some business deals may require a minimum compliance level
- **Compliance Monitoring**
    - **Due diligence/care:** a duty to act honestly and in good faith
        - Due Care: internal activities
        - Due Diligence: external
    - **Attestation and acknowledgement:** someone must sign off on formal compliance document
    - **Internal and external:** monitor compliance with internal tools, provide access or information to 3rd party participants
    - **Automation:** many 3rd party systems to compile data and report
- **Privacy**
    - **Legal Implications**
        - **Local/Regional**
        - **National**
        - **Global**
            - **GDPR (General Data Protection REgulation):** data protection and privacy for individuals in the EU which allows users to decide where their data goes
    - **Data subject:** any information relating to an identified or identifiable natural person
    - **Controller vs. Processor**
        - **Controller:** manages the purposes and means by which personal data is processed
        - **Processor:** processes data on behalf of data controller; could be 3rd party
    - **Ownership**
    - **Data Inventory and retention:** listing of all managed data including owner of data, how often it is used, and the format of the data
    - **Right to be forgotten:** giving "data subjects" control of their personal data

- **Explain the types and purposes of audits and assessments**
  - **Attestation:** opinion of truth or accuracy of a company's security positioning after an audit
  - **Internal**
    - **Compliance:** is your organization complying with regulatory or industry requirements?
    - **Audit committee:** oversees risk management activities
    - **Self-assessments:** have the organization perform their own checks
  - **External**
    - **Regulatory:** an independent 3rd party may be required to perform
    - **Examinations:** hands on research of viewing records, compiling resorts, gather additional details
    - **Assessments**
    - **Independent third-party audit**
  - **Penetration testing**
    - **Physical:** operating systems security can be circumvented by physical means (can you enter a building?)
    - **Offensive:** red team; attack system and look for vulnerabilities to exploit
    - **Defensive:** blue team; identify attacks in real time and prevent any unauthorized access
    - **Integrated:** create an ongoing process (Red Team constantly attacks, then tells blue team for patching)
    - **Known Environment:** full disclosure
    - **Partially known environment:** a mix of known and unknown environment
    - **Unknown environment:** blind test
    - **Reconnaissance:** gathering a digital footprint, security posture, etc
      - **Passive:** learn as much as you can from open sources
      - **Active:** trying the doors, network traffic & logs, ping scans, port scans, DNS queries, OS Scans, OS fingerprinting, service scans
- **Given a scenario, implement security awareness practices**
  - **Phishing**
    - **Campaigns**
    - **Recognizing a phishing attempt:** spelling or grammatical errors, domain name and email inconsistencies, unusual attachments, request for personal information
    - **Responding to reported suspicious messages:**
  - **Anomalous Behavior Recognition**
    - **Risky:** modifying hosts file, replacing a core OS file, uploading sensitive file

  - **Unexpected:** someone logging in from another country, increase in data transfer
  - **Unintentional:** typing in wrong domain name, misplacing USB drives
- **User guidance and training**
  - **Policy/handbooks**
  - **Situational awareness**
  - **Insider threat**
  - **Password management**
  - **Removable media and cables**
  - **Social Engineering**
  - **Operational Security**
  - **Hybrid/Remote work environment**
- **Reporting and monitoring**
  - **Initial:** first occurrence is an opportunity for user training
  - **Recurring:** the value of long term monitoring; identify high frequency security issues
- **Development:** create as security awareness team, establish minimum awareness level
- **Execution:** create the training materials, document success measurements, identify stakeholders, deploy the training material