CompTIA Security+ Study Guide

Exam Number: SY0-701

Chloe Stogsdill

Table of Contents

Topic 1: General Security Concepts

Topic 2: Threats, Vulnerabilities, and Mitigations

Topic 3: Security Architecture

Topic 4: Security Operations

Topic 5: Security Program Management and Oversight

All topics are sourced from the CompTIA Security+ Certification Exam Objectives

EXAM NUMBER: SY0-701

Topic 1: General Security Concepts

1.1 Compare and contrast various types of security controls.

Background Knowledge:

- What are security controls?
    - Security controls are measures put in place to protect businesses and data from attacks. Often, these controls can be categorized as multiple types depending on the context of the situation.

Types of Security Controls:

- Categories
    - Technical
        - Technical controls, also known as logical controls, are hardware- and software-based solutions, such as firewalls and IDS. They focus on protecting businesses and data through the use of technology.
    - Managerial
        - Managerial controls, also known as administrative controls, are policies and procedures put in place, such as risk assessments and DRP, that guide employees on proper safety procedures.
    - Operational
        - Operation controls are security measures carried out by people, not machines or policies, such as guards and user training, to protect the day-to-day operations of a business.
    - Physical
        - Physical controls are measures put in place that protect physical access to the building, along with systems and data, such as locked doors and surveillance cameras.
- Control Types
    - Preventive
        - Preventative measures aim to stop attacks before they occur through prohibiting access and blocking malicious activities, such as firewalls and antiviruses.
    - Deterrent
        - Deterrent measures aim to discourage attackers from attacking through making an attack’s consequences clear or perceivably difficult, such as warning signs and surveillance cameras.
    - Detective
        - Detective measures aim to identify attacks as they occur or in progress, such as IDS and SIEMs.

- Corrective
    - Corrective measures aim to repair and restore attacked systems after an incident, such as patch management and IRPs.
- Compensating
    - Compensating measures are alternative solutions for when primary measures are insufficient in protecting a system, such as increasing monitoring, UPSs, and increasing on-site guards.
- Directive
    - Directive measures provide guidelines and directions on secure behavior, such as security policies and SOPs.

Categories	Preventative	Deterrent	Detective	Corrective	Compensating	Directive
Technical	Firewalls	Splash screen/ Login banner	System logs	Restore backups	Firewalls to block	Store sensitive info in folders
Managerial	Onboarding policies	Demotion	Employee reviewing logs	Policies to report issues	Separation of duties	Compliance policies
Operational	ID checks, guard shack	Reception desk	Guard patrol	Contact authorities	Simultaneous guard duty	Train users
Physical	Door locks, gates	Trespassing signs	Motion detectors	Fire extinguisher	Power generator	Authorized personnel only

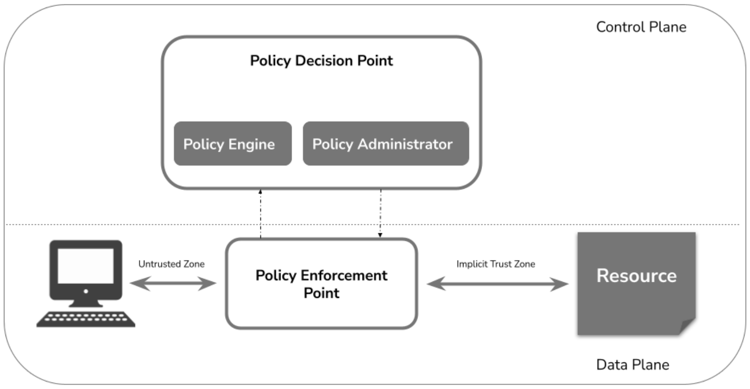
1.2 Summarize fundamental security concepts.

Security Concepts:

- Confidentiality, Integrity, and Availability (CIA)
    - The CIA triad is a foundational concept in cybersecurity
    - **Confidentiality** makes sure sensitive information is securely stored and accessible only to those who are authorized to view it. You are the only person that should have access to your information.
    - **Integrity** makes sure that data remains unaltered and trustworthy. When you send a message, you want it to remain unedited or modified, and any modification to be identified.
    - **Availability** makes sure information and resources are available to users when requested. If you need to access your data, you want the system that accesses it to be operating.

- Non-Repudiation
    - Non-repudiation is a concept that means that the person that sent a message cannot deny the authenticity or origin of their digital signature on the message itself. Through digital signatures and encryption, we provide non-repudiation when sending a message by invoking proof of origin and proof of integrity, preventing a user from denying involvement in a transaction.
    - Proof of Integrity implies that the data did not change from when the message was sent to when it was received, and is achieved using hashing.
    - Proof or Origin/Authentication implies that the message that was received came from the person it says it did, and is achieved by digitally signing a message with your private key before sending- of which is verified using your public key.
- Authentication, Authorization, and Accounting (AAA)
    - **Authenticating** people
        - Authenticating is the process of verifying the identity of people before allowing them access to a system, ensuring they are who they claim to be. This authentication is commonly done using multiple methods of identification, known as a Multi-Factor Authentication (MFA).
    - **Authorization** systems
        - Authorization is the process of verifying the identity of devices before allowing them into a network, ensuring they are trusted. An organization has a dedicated Certificate Authority that maintains digital certificates, signed by the CA, for each device used to authenticate a user.
    - **Accounting** models
        - Accounting is the process of defining permissions and access levels of a user or device. An organization might have Role-Based Access Control, where access is based on the user's role within the organization, or Attribute-Based Access Control, where access is granted based on the attributes of a user such as time or location they are logging in.
- Gap Analysis
    - A gap analysis is an assessment of the current security posture of an organization. It identifies the differences between the current state of security and the desired state or requirements. This report includes where the security is compared to where the goal is, along with how we bridge the gap.
    - The "gap" between where we are and where we want to be.

- Zero Trust
    - Zero trust is a security architecture in which every entity is not trusted by default.
    - Control Plane
        - Adaptive Identity
            - An adaptive identity is how the architecture changes the method of authentication of a user based upon contextual factors like their behavior, location, and risk level.
        - Threat Scope Reduction
            - Threat scope reduction is the process of minimizing attackable points in a network based on where a user is or what they are doing. For example, a company might have a policy that a resource is only available to an employee when they are physically in the company building, minimizing the threat of the resource being misused or displaced.
        - Policy-Driven Access Control
            - Policy-driven access control identifies which authentication process should be used to authenticate a user based on the policies of the organization.
        - Policy Administrator
            - The policy administrator is in charge of establishing and halting communications with a user based on the decisions of the policy engine.
        - Policy Engine
            - The policy engine takes user access requests and compares them against existing security policies to make decisions about granting or denying access.
        - Policy Decision Point
            - The policy decision point acts as the decision maker, using the information gathered by the PEP. This is a combination of the Policy Administrator and the Policy Engine.



        - Data Plane
            - Implicit Trust Zones and Security Zones
                - Security zones look at where you are coming from and where you are attempting to go and will either accept or deny access based on if you are in a trusted or untrusted zone. An untrusted zone trying to access a trusted zone may be enough to completely deny access, while a trusted zone accessing an untrusted zone may need closer analysis to determine. Security zones allow for implicit trust zones, meaning if a trusted zone is trying to access an internal zone, like a database, the connection may be automatically accepted.
            - Subject/System
                - Subjects and systems refer to the users and devices involved in data plane operations, such as an employee (subject) using their laptop (system) to access a resource.
            - Policy Enforcement Point
                - The policy enforcement point is the point in which any device attempting to connect to part of the network will need to be verified. This point enforces the decisions made in the control plane and acts as a gatekeeper for all traffic.
- Physical Security
    - Bollards
        - Bollards are posts that prevent vehicles from crashing into or entering restricted areas, often used around building perimeters.
    - Access Control Vestibule
        - Access control vestibules, known also as “security mantraps,” are secure rooms with two sets of locking doors. They require people attempting to enter a building to be authenticated, and prevents attacks like tailgating by only allowing in a single person at a time.
    - Fencing
        - Fencing is a physical barrier placed around the perimeter of a building or property to prevent and deter unauthorized access to the area.
    - Video Surveillance
        - Cameras and recording systems are used to monitor activity in and around a company.
    - Security Guard
        - Security guards are trained at monitoring, patrolling, and responding to incidents, along with acting as a deterrent to in-person attacks.

    - Access Badge
        - Access badges are cards or devices that allow employees and other authorized people to enter into secured areas, using technology such as RFID.
    - Lighting
        - Lighting allows for threats to be more easily identified, viewed on camera, and by guards.
    - Sensors
        - Infrared
            - Infrared sensors detect motion and heat signatures.
        - Pressure
            - Pressure sensors detect change in pressure on a surface, such as a floor mat.
        - Microwave
            - Microwave sensors detect moving objects and can penetrate non-metallic objects, making them useful for detecting metallic movement such as cars.
        - Ultrasonic
            - Ultrasonic sensors measure the time it takes for echos to return after being bounced off an object, effectively detecting changes in the environment.
- Deception and Disruption Technology
    - Honeypot
        - A honeypot is a decoy system that is set up to purposefully attract and monitor malicious activities by acting as a vulnerable and valuable target.
    - Honeynet
        - A honeynet is a network of honeypots set up to act as a real network in order to attract and monitor attacks with more detail of the attacker's behavior and techniques.
    - Honeyfile
        - A honeyfile is a decoy file, seemingly valuable, that is intentionally left unguarded to lure attackers into accessing it.
    - Honeytoken
        - A honeytoken is a piece of data designed to detect and track malicious activity.

1.3 Explain the importance of change management processes and the impact to security.

Change Management Processes:

- Business Processes Impacting Security Operation
    - Approval Process
        - An approval process is a procedure for authorizing potential changes in an organization. The process makes sure any change is reviewed and approved after verifying the change aligns with policies and does not introduce unnecessary risk.
    - Ownership
        - Ownership is the assignment of responsibility over every part of an organization, such as devices, systems, and processes. Owners are responsible for overseeing and ensuring security compliance with every part of the organization their ownership falls under.
    - Stakeholders
        - Stakeholders are individuals or groups, such as employees, management, and customers, that have a stake in security operations. Stakeholders should be consulted before a change occurs to make sure that all of their concerns are addressed.
    - Impact Analysis
        - An impact analysis is an overview of the potential risks and consequences of a change. Understanding the impacts a change might have, both good and bad, allows for proper planning and mitigation of risks.
    - Test Results
        - The test results of a change, such as vulnerability assessments or penetration tests, give insight into the effectiveness or potential weak points in a change. These allow for changes to be safely implemented in a controlled environment before the change is made throughout the company.
    - Backout Plan
        - A backout plan is a pre-made strategy detailing how to revert or backout from a change if an unexpected issue occurs or the change does not work as expected.
    - Maintenance Window
        - A maintenance window is a scheduled period for performing a change, usually done outside of work hours or during holidays to minimize disruption.

    - Standard Operating Procedure
        - SOPs are detailed instructions on how to carry out a routine operation to ensure consistency and minimize risk.
- Technical Implications
    - Allow Lists/Deny Lists
        - Allow lists/deny lists are used to control access on a network by blocking things such as IP addresses, applications, and users so only authorized interactions with systems can occur. These can be further restricted during an active change to prevent any disruption.
    - Restricted Activities
        - Restricted activities, as part of the change management process, mean you are restricted to changing only what has been approved and only during the period that is listed. You are not authorized to make any changes to any other applications or services; however, you are not limited to the changes listed in the change control document as long as the changes contribute specifically to the primary goal and are in the scope of the restricted activities you are authorized to do.
    - Downtime
        - Downtime is planned or unplanned periods where a system or service is unavailable due to a change.
    - Service Restart
        - Restarting a service may be a part of change. Planning and communicating these restarts makes sure they have minimal impact.
    - Application Restart
        - Restarting an application may be a part of change. Planning and communicating these restarts makes sure they have minimal impact.
    - Legacy Applications
        - Legacy applications are older pieces of software that are no longer supported or updated by the manufacturer. These applications may cause difficulties and introduce vulnerabilities during the change management process, as they often couple with fear of the unknown: What do we do without this system?
    - Dependencies
        - Dependencies are interconnected parts of a company that rely, or depend, on each other to operate correctly. When changing something that has a dependency, it is important to ensure the change does not negatively affect the component.

- Documentation
    - Updating Diagrams
        - Updating diagrams occurs after a change and is important in understanding and representing the current state of a company and its internal systems. It also ensures future changes can be accurately assessed based on the most current blueprint of an organization.
    - Updating Policies/Procedures
        - Updating policies and procedures make sure changes are properly documented and guidelines, policies, and SOPs are current.
    - Version Control
        - Version control involves tracking and documenting each change so that changes are stored and can be audited, reverted, or otherwise referenced.

1.4 Explain the importance of using appropriate cryptographic solutions.

Cryptographic Solutions:

- Public Key Infrastructure (PKI)
    - PKI is a security framework that uses encryption and authentication to communicate over the network using public and private keys. PKI is used to create, store, and manage keys and digital certificates.
    - Public Key
        - A public key is a key that is shared openly. It can be used to encrypt data or verify digital signatures, and often works in a pair with a private key.
    - Private Key
        - A private key is a key that is kept secret. It can be used to decrypt data or digitally sign messages, and often is important when ensuring confidentiality and integrity during communications. Private keys, due to the math involved, are underivable from their public key pairs.
    - Key Escrow
        - A key escrow is a third party that securely holds keys for authorized users to access and protects against the possibility that keys are lost.
- Encryption
    - Level
        - A level, in encryption, refers to the scope of encryption that is being applied to protect data.
        - Full-Disk Encryption (FDE)
            - FDE encrypts an entire storage device at the disk level and makes sure if the device is stolen the data on it remains confidential.

        - Partition
            - Partition encryption encrypts a specific section of a storage device meant to selectively encrypt specific portions of data.
        - File
            - File encryption encrypts a file or folder.
        - Volume
            - Volume encryption encrypts logical volumes or containers that hold data.
        - Database
            - Database encryption encrypts the data in a database.
        - Record
            - Record encryption encrypts individual rows of a database.
- Transport/Communication Encryption
    - Transport/communication encryption is the practice of encrypting data when transmitting it over a network to prevent unauthorized access to the data. This can be done by TLS, HTTPS, VPNs, etc.
- Asymmetric
    - Asymmetric key encryption, also known as public key cryptography, uses a public and private key pair to encrypt and decrypt data. Everyone has access to your public key and can use it to encrypt a message, but, as you have the private key pair, you are the only one capable of decrypting that message.
- Symmetric
    - Symmetric key encryption uses one key, meaning the key to encrypt a message is the same key to decrypt the message. This key is referred to as a "shared secret". The more people have the key, the more insecure the key becomes, meaning algorithms that use symmetric encryption do not scale well. However, as there is less overhead, it is often faster to use than asymmetric encryption.
- Key Exchange
    - Key exchange refers to the secure sharing or keys between communicating parties. These exchanges could be physical and in-person, an Out-of-Band key exchange, but internet exchanges are much faster. An In-Band key exchange is on the network and provides the keys with additional encryption and fast security. For example: sharing a symmetric key using asymmetric encryption.

- Algorithms
    - Algorithms are the mathematical procedure used to encrypt and decrypt data. Both parties in a communication agree to an algorithm before a data transfer, of which may be chosen for its speed, security, complexity of implementation, etc. Algorithms are well known and often are public. The only unknown entity in these algorithms is the key itself, which determines encrypted data, hash value, and digital signature.
- Key Length
    - Key length refers to the length of the key used to encrypt or decrypt messages. The longer the key the more secure it is against attacks, but the more computation power encryption and decryption will require.

- Tools
    - Trusted Platform Module (TPM)
        - A TPM is a chip residing in a device that provides hardware security. It can generate random numbers and keys, can securely store and manage keys, and provides unique keys often burnt into the TPM during manufacturing.
    - Hardware Security Module (HSM)
        - A HSM is a dedicated hardware device designed to generate, store, and manage cryptographic keys securely in large environments.
    - Key Management System
        - A key management system manages keys throughout their lifecycle, from generating to distributing to storing to revocation.
    - Secure Enclave
        - A secure enclave is a secure environment within a device's CPU or SoC that is quarantined from the main OS and memory, allowing for a trusted environment for sensitive operations such as key management. This means that if physical access to the device is procured by the attacker, the device will not give you access to the data on a connected device, like a phone paired to a laptop.
- Obfuscation
    - Steganography
        - Stenography is the practice of hiding information within other, unrelated data such as images or audio files, called the "covertext," to prevent detection.

    - Tokenization
        - Tokenization is the practice of replacing data with a unique identifier called a “token.” These tokens have no meaning or value outside of the context of the tokenization system, but, within the system, they are functional and connect to the original piece of data. Temporary tokens are created during credit card transfers so an attacker cannot capture credit card numbers later, as the token and data are not related.
    - Data Masking
        - Data masking is the practice of hiding information by replacing it with fictional values, such as asterisks. A credit card might be displayed on a receipt as: ****-****-1234.
- Hashing
    - Hashing transforms inputted data into a fixed-length, irreversible hash through a hashing algorithm. Hashing is most often used to verify integrity and securely store passwords.
- Salting
    - Salting is a technique in which a random value, the “salt,” is added to a password before hashing to make the hashed unique even for identical passwords. This prevents attackers from creating rainbow tables.
- Digital Signatures
    - Digital signatures use public key cryptography as a way to provide integrity and authentication. The signer will use their private key to generate the signature, which can be verified by anyone with access to the corresponding public key.
- Key Stretching
    - Key stretching, also known as key strengthening, is a way to make shorter, more insecure keys stronger by repeatedly hashing the key with a hash function. This makes the key more difficult and resource-intensive to brute force, as attackers would have to reverse every hash, even if the key was originally short or weak.
- Blockchain
    - Blockchain is a decentralized, public ledger that records transactions in a way that makes them impossible to modify or tamper. Each transaction “block” links to the previous block, forming a chain, and ensures integrity in a trustless environment. The concept and implementation of blockchain is still evolving.
- Open Public Ledger
    - An open public ledger is a completely transparent and publicly accessible record of transactions. It allows anyone to view and verify these transactions.

- Certificates
    - X.509
        - X.509 is the standard format for digital web certificates. Each X.509 certificate contains a serial number, version, signature algorithm, issuer, name of certification holder, public key, etc.
    - Certificate Authorities (CA)
        - Certificate authorities are trusted entities that create, issue, and verify digital certificates.
    - Certificate Revocation Lists (CRLs)
        - CRLS are lists, maintained by CAs, that store information on the revocation or invalidation status of digital certificates, allowing systems to check if a certificate is no longer valid.
    - Online Certificate Status Protocol (OCSP)
        - OCSP is used to check the status of a digital certificate, allowing systems to verify a certificate's validity in real-time. Having a CA verify every OCSP request it receives leads to scalability issues, so OCSP stapling was created as a way for the certificate holder to verify their own status by storing it on the server. The OCSP is "stapled" into the TLS/SSL handshake and digitally signed by the CA.
    - Self-Signed
        - A self-signed certificate is a certificate that is not signed by a CA or other trusted entity, and is instead signed by the party responsible for the website the certificate has been created for. These certificates lack third-party verification and trust.
    - Third-Party Certificates
        - A third-party certificate is a certificate that has been signed and issued by a trusted third-party, such as a CA. This provides external verification of the website and is widely accepted in secure communications.
    - Root of Trust
        - The root of trust is an entity that a system bases the trust it has for other entities on, such as a CA or HSM. Since our system inherently trusts the entity, and the entity trusts another component, our system can trust the other component.
    - Certificate Signing Request (CSR) Generation
        - A CSR is generated to obtain a digital certificate by a CA. The CSR will include the entity's public key and relevant information, allowing the certificate authority to issue a signed certificate.

- Wildcard
    - A wildcard certificate is a type of digital certificate that can secure multiple subdomains under a single domain. It uses a wildcard character (*) in the domain name, for example: *exam.com secures www.exam.com, mail.exam.com, …

Important Acronyms in Unit 1:

AAA - Authentication, Authorization, Accounting
CA - Certificate Authority
CIA - Confidentiality, Integrity, Authority
CRL - Certificate revocation list
CSR - Certificate signing request
FDE - Full Disk Encryption
HSM - Hardware Security Module
IPsec - Internet Protocol Securityused commonly in VPNs
MFA - Multi-Factor Authentication
OCSP - Online Certificate Status Protocol
PKI - Public Key Infrastructure
RFID - Radio Frequency Identification
SIEM - Security Information and Event Management
SoC - System on Chip
SSL - Secure Sockets Layer
TLS - Transport Layer Security
TPM - Trusted Platform Module
VPN - Virtual Private Network

Topic 2: Threats, Vulnerabilities, and Mitigations

2.1 Compare and contrast common threat actors and motivations.

Background Knowledge:

- What are threat actors?
    - Threat actors are the individuals responsible for an attack on an organization.

Threat Actors and Motivations:

- Attributes of actors
    - Internal/External
        - Internal actors are individuals or groups that attack from within the organization that is being attacked, such as employees or contractors.
        - External actors are individuals or groups that attack from outside of an organization that is being attacked, such as a competitor.
    - Resources/Funding
        - The resources and funding an actor has refers to how many financial, technological, human, or informational means are available to them.
    - Level of Sophistication/Capability
        - The level of sophistication and capability an actor has refers to the degree of technical expertise an attacker has.
- Motivations
    - Data Exfiltration: leaking or otherwise stealing data.
    - Espionage: gathering intelligence.
    - Service Disruption: disrupting the continuity and availability of a service.
    - Blackmail: extorting victims or gathering potentially intimidating information.
    - Financial Gain: achieving financial profit.
    - Philosophical/Political Beliefs : advancing philosophical or political ideologies.
    - Ethical: adhering to or imposing ethical principles
    - Revenge: seeking retribution
    - Disruption/Chaos: creating disorder
    - War: engaging in acts of war
- Threat Actors
    - Nation-State
        - Nation-States are external entities such as a government or national security branch. These entities may have a multitude of different reasons to want to attack an organization and extremely high sophistication and funding. They are commonly known as an Advanced Persistent Threat (APT).

- Unskilled Attacker
    - An unskilled attacker refers to anyone, external or internal, running pre-made scripts without any deep knowledge of how they work or what is happening. They are motivated by data exfiltration and disruption. The level of sophistication and resources of unskilled attackers are low.
- Hacktivist
    - Hacktivist are often external hackers with a purpose, such as philosophical beliefs, revenge, disruption, etc. Hacktivists are often extremely sophisticated, but have limited resources available to them.
- Insider Threat
    - Insider threats are internal threats motivated by revenge or financial gain with all of the resources of the company and a medium level of sophistication. These attackers excel at knowing exactly which places of the organization are vulnerable or most lucrative to hit and exploit.
- Organized Crime
    - Organized crime is a group of professional criminals motivated by monetary gain. They are almost always external threats and have a very high level of sophistication, resources, and structure.
- Shadow IT
    - Shadow IT is a group that is working around the internal IT department, motivated by philosophical beliefs or revenge. They will use their own money and have a medium level of sophistication, as they know the workings of the company but have a lesser understanding of IT.

Categories	Location	Resources	Sophistication	Motivations
Nation State	External	Very High	Very High	Data exfiltration, war, revenge, philosophical beliefs, disruption
Unskilled	External	Low	Low	Data exfiltration, disruption, (sometimes) philosophical beliefs
Hacktivist	External	Low-Medium	High	Philosophical beliefs, revenge, disruption
Insider Threat	Internal	High	Medium	Revenge, financial gain
Organized Crime	External	Very High	Very high	Financial gain
Shadow IT	Internal	High	Low-Medium	Philosophical beliefs, revenge

2.2 Explain common threat vectors and attack surfaces.

Background Knowledge:

- What is a threat vector?
    - The method an attacker uses to gain access to a system or to otherwise carry out an attack.
- What is an attack surface?
    - The entry points an attacker can exploit to attack or gain access to a system.

Threat Vectors and Attack Surfaces:

- Message-Based
    - Email
        - Threat Vector: phishing emails with malicious attachments, spam with malware, email spoofing, social engineering attacks.
        - Attack Surface: unprotected email accounts, weak passwords.
    - Short Message Service (SMS)
        - Threat Vector: texts with malicious links.
        - Attack Surface: weak securing on mobile devices, lack of awareness.
    - Instant messaging (IM)
        - Threat Vector: malicious links sent in chats, social engineering attacks.
        - Attack Surface: unencrypted IM platforms, weak user access controls.
- Image-Based
    - Threat Vector: Image formats, such as XML, that can have injected HTML or Javascript, stenography, phishing attacks.
    - Attack Surface: downloaded images from untrusted sources, opening image attachments.
- File-Based
    - Threat Vector: Malware contained within other files, such as PDFs, ZIPS, or RARS, zero-days exploited through file attachments.
    - Attack Surface: downloaded files from untrusted sources, outdated software
- Voice Call
    - Threat Vector: vishing attacks, spam over IP, war dialing, call tampering.
    - Attack Surface: lack of awareness, weak user authentication policies.
- Removable Device
    - Threat Vector: malware spread through USB devices or external hard drives.
    - Attack Surface: unrestricted use of USBs, lack of device scanning.

- Vulnerable Software
    - Client-Based
        - Software installed on a client's computer.
        - Threat Vector: unpatched software, outdated applications.
        - Attack Surface: outdated OS and applications, lack of automated software updates.
    - Agentless
        - Software that is not installed, but is accessed through a service.
        - Threat Vector: exploiting vulnerabilities in the main software.
        - Attack Surface: limited patching, increased reliance on vendors.
- Unsupported Systems and Applications
    - Threat Vector: attackers exploiting known vulnerabilities with no working patches.
    - Attack Surface: using outdated or unsupported software, applications, or OS.
- Unsecure Networks
    - Wireless
        - Threat Vector: On-path attacks on unencrypted W-Fi networks, network eavesdropping.
        - Attack Surface: connecting to public Wi-Fi without a VPN, using weak encryption protocols.
    - Wired
        - Threat Vector: physical access to a network, malware spreading through the network.
        - Attack Surface: Weak network segmentation or physical security.
    - Bluetooth
        - Threat Vector: bluetooth hijacking for data theft or malware.
        - Attack Surface: insecure bluetooth connections, leaving bluetooth enabled.
- Open Service Ports
    - Threat Vector: exploiting vulnerabilities in services running on specific ports.
    - Attack Surface: running unnecessary services, not disabling unused ports, lack of NAC.
- Default Credentials
    - Threat Vector: brute force to guess default credentials for network access.
    - Attack Surface: leaving factory default credentials, weak password policies.

- Supply Chain
    - Managed Service Providers (MSPs)
        - Managed service providers are third parties you rely on to manage your service and inform you of any updates or changes you need to make.
    - Vendors
        - Vendors provide products and services that integrate into an organization's infrastructure.
    - Suppliers
        - Suppliers are part of the broader supply chain and provide materials and components.
    - Threat Vector: compromised systems or software leading to attacks on clients.
    - Attack Surface: lack of risk management, limited visibility into third-party security practices.
- Human Vectors/Social Engineering
    - Phishing
        - Phishing is commonly used to deceive users into clicking malicious links or divulging personal information through an email or IM.
    - Vishing
        - Vishing (voice-phishing) is commonly used to deceive users into divulging personal information or making fraudulent transactions over the phone.
    - Smishing
        - Smishing (sms-phishing) is commonly used to deceive users into clicking malicious links or divulging personal information through text messages.
    - Misinformation/Disinformation
        - Misinformation (false information spread without harmful intent) and disinformation (deliberate false information spread to intentionally deceive) can be used to manipulate individuals or organizations.
    - Impersonation
        - Impersonation is the act of pretending to be someone else, typically with the intent to get access to information, systems, or physical locations.
    - Business Email Compromise
        - Business email compromise occurs when an attack infiltrates or spoofs a company email to deceive employees, customers, or partners.
    - Pretexting
        - Pretexting is when an attack creates a fake scenario, or "pretext," typically to deceive or manipulate someone into performing fraudulent transactions.

        - Watering Hole
            - A watering hole attack occurs when an attacker compromising a website that is frequently visited by the target group in order to exploit them or deliver malware indirectly, instead of directly attacking the target group.
        - Brand Impersonation
            - Brand impersonation occurs when an attacker mimics a company in an attempt to deceive and manipulate users.
        - Typosquatting
            - Typosquatting is an attack where attackers register for domain names that have slightly different variations or spellings, "typos," compared to legitimate websites.

2.3 Explain various types of vulnerabilities.

Background Knowledge:

- What are vulnerabilities, threats, exploits and attacks?
    - Vulnerabilities are weaknesses in a system that can be exploited by attackers.
    - Threats are a potential event that could occur.
    - Exploits are a method or tool that is used to take advantage of a vulnerability.
    - Attacks are the attempt that is made to take advantage of a vulnerability.

Vulnerabilities:

- Application
    - Memory Injection
        - Memory injection occurs when malicious code is inserted into a running application's memory space. Once done, an attacker can insert malicious code and can have access to the same rights, permissions, and data that has been given to the trusted process.
    - Buffer Overflow
        - A buffer overflow occurs when an application does not validate user input and more data can be written to a buffer than it can hold, causing adjacent memory to be overwritten.
    - Race Conditions
        - Race conditions occur when software is dependent on the timing of uncontrollable events, such as the concurrent execution of processes.
        - Time-Of-Check (TOC)
            - The time at which you check and validate a value
        - Time-Of-Use (TOU)
            - The time at which you use the value

    - TOCTOU Attack
      - TOCTOU vulnerabilities occur when an application checks a resource then acts on it, assuming the resource is unchanged from when it originally checked. If an attacker can alter the resource between the check and the use, they can exploit the gap.
  - Malicious Update
    - Malicious updates occur when attackers inject malicious code or software into a released update or fake update notifications. .
- Operating System (OS)-Based
  - OS-based vulnerabilities occur due to security flaws within an OS, and include default configurations, misconfiguration, privilege escalation, and zero-days.
- Web-Based
  - Structured Query Language Injection (SQLi)
    - SQL injection occurs when an attacker enters malicious SQL statements into an input field lacking input validation, allowing the attacker access to the underlying database.
  - Cross-Site Scripting (XSS)
    - XSS occurs when a malicious script is injected into an otherwise trusted web page viewed by end users. This compromises the trust a user has for the web application.
- Hardware
  - Firmware
    - Firmware is the software inside the hardware. Firmware attacks occur when the update process is compromised or through malicious downloads, and will affect the boot-up process of your computer.
  - End-Of-Life
    - End-of-life refers to devices that are no longer supported by the manufacturer, but still have enough lifespan to reliably use to find a replacement.
  - Legacy
    - Legacy hardware is hardware that is no longer supported by the vendors. These devices are outdated and lack patch management and consistent updates.
- Virtualization
  - Virtualization is the process of dividing a physical server into multiple unique and isolated virtual servers through use of a hypervisor.

    - Virtual Machine (VM) Escape
        - VM escape occurs when an attacker gains access to a VM, allowing them to attack the host server, hypervisor, or other VMs.
    - Resource Reuse
        - Resource reuse occurs when VM environments improperly clear, isolate, or allocate reused resources such as memory and storage, allowing attackers to possibly recover sensitive data.
- Cloud-Specific
    - An attack to a CSP can affect all of its customers, meaning cloud-specific vulnerabilities carry a large risk. Common vulnerabilities include data breaches, misconfiguration, weak security architecture, and weak access management.
- Supply Chain
    - Service Provider
        - Attacks on service providers can directly or indirectly affect customers. Access to a MSP can lead to access to customers' networks.
    - Hardware Provider
        - Attacks to hardware providers can compromise the physical infrastructure of a company. If an attacker gets access to physical hardware, backdoors and malware can be installed.
    - Software Provider
        - Software providers can be just as dangerous as attackers through weak coding practices and testing procedures that lead to software with easily exploitable vulnerabilities.
- Cryptographic
    - Cryptographic vulnerabilities involve weaknesses in cryptographic systems, such as weak encryption, improper key management, and inadequate randomness.
- Misconfiguration
    - Misconfiguration vulnerabilities are a result of configuration mistakes, such as open ports, default credentials, and insecure protocols.
- Mobile Device
    - Side Loading
        - Side loading occurs when applications are installed onto a mobile device from unofficial or untrusted sources on the web outside of the app store.
    - Jailbreaking (Rooting)
        - Jailbreaking occurs when vendor restrictions have been removed from a mobile device, allowing a user to run unauthorized software.
- Zero-Day
    - A zero day vulnerability is a vulnerability that is discovered by attackers before developers are aware of it.

2.4 Given a scenario, analyze indicators of malicious activity.

Indicators:

- Malware Attacks
    - Ransomware
        - Ransomware encrypts a target's file, rendering them inaccessible. The attacker then demands payment in exchange for the decryption of the files.
        - Indicators: account lockout, blocked content, resource consumption, missing logs.
    - Trojan
        - A trojan is malware that appears as a legitimate program but, once executed, performs malicious activities on the system and network.
        - Indicators: resource consumption, network inaccessibility, out-of-cycle logging, published/documented.
    - Worm
        - A worm is a self-replicating program that spreads independently across networks and systems without the need of a host program.
        - Indicators: account lockout, blocked content, resource consumption, missing logs.
    - Spyware
        - Spyware is software that secretly monitors and steals user information and activities without their knowledge.
        - Indicators: account lockout, blocked content, resource consumption, missing logs.
    - Bloatware
        - Bloatware is unnecessary software that is pre-installed on a device, consuming resources and slowing performance.
        - Indicators: resource consumption, missing logs.
    - Virus
        - A virus is a program that alters the normal operations of a computer and spreads itself throughout a network.
        - Indicators: blocked content, resource consumption, missing logs.
    - Keylogger
        - A keylogger is software that records every keystroke on a computer in an attempt to capture sensitive information, such as passwords.
        - Indicators: resource consumption, missing logs.
    - Logic Bomb
        - Logic bombs are code designed to trigger a malicious action when a predefined event occurs.
        - Indicators: resource consumption and inaccessibility, missing logs.

    - Rootkit
        - A rootkit is malware designed to stealthy give attackers administer, or "root," access to a system.
        - Indicators: resource consumption and inaccessibility, missing logs.
- Physical Attacks
    - Brute Force
        - Physical brute force attacks occur when attackers physically break into the building through breaking locks, gates, windows, etc.
        - Indicators: resource inaccessibility, out-of-cycle logging, missing logs.
    - Radio Frequency Identification (RFID) Cloning
        - RFID uses radio waves for identification on RFID tags. Cloning these tags gives an attacker the same resources unlocked by the original RFID tag.
        - Indicators: impossible travel, missing logs.
    - Environmental
        - Environmental attacks occur when physical tampering to the environment, including HVAC and power supply systems, cause the compromised security of a building.
        - Indicators: resource inaccessibility, out-of-cycle logging, missing logs.
- Network Attacks
    - Distributed Denial-of-Service (DDoS)
        - DDoS attacks involve compromising multiple computer systems to disrupt services.
        - Reflected
            - Reflected DDoS occurs when the attacker reflects their requests off of a third party with a spoofed IP address, so the response goes to the IP of the system the attacker is targeting.
        - Amplified
            - Amplified DDoS uses reflection to turn a small request, such as a DNS request, into a much larger amount of data, reflected onto the target system.
        - Indicators: resource inaccessibility, resource consumption, out-of-cycling logging, published/documented.
    - Domain Name System (DNS) Attacks
        - DNS poisoning occurs when an attacker changes the IP address a domain name is connected to, redirecting user traffic to malicious and unwanted IP addresses and websites.
        - DNS spoofing occurs when an attacker sends a false DNS reply to a system before the DNS server, linking a false IP to a requested domain name and redirecting users to malicious websites.

    - Domain hijacking exploits the DNS server and allows attackers access to the settings of different domains.
    - Indicators: resource inaccessibility, resource consumption, out-of-cycling logging, published/documented, missing logs.
- Wireless
    - Bluejacking occurs when attackers send unsolicited messages or images to nearby Bluetooth connections in an attempt to annoy or irritate.
    - Bluesnarfing occurs when attackers steal data through bluetooth connections by attacking Bluetooth connections that are open to discovery.
    - Bluebugging occurs when attackers create a backdoor for themselves through Bluetooth, allowing them full control of the device.
    - An evil twin is a fake access point set up by an attacker that appears to be a trusted network for users in the area to connect to.
    - Rogue access points are unregistered access points added to the network, allowing attackers a point of entry to the network.
    - Indicators: blocked content, concurrent session usage, out-of-cycle logging, missing logs.
- On-Path (Man-in-the-Middle)
    - On-path attacks occur when an attacker sits in between two parties, intercepting and capturing traffic, potentially changing information.
    - ARP poisoning attacks occur when an attacker sends fake ARP messages that link their MAC addresses to the IP address of other devices, allowing them to intercept traffic.
    - On-path browser attacks occur when malicious software intercepts a user and their web browser, allowing the software to manipulate web traffic.
    - Indicators: blocked content, missing logs.
- Credential Replay
    - Credential replay attacks occur when attackers capture login credentials and reuse them to gain unauthorized access to an account.
    - Indicators: impossible travel, account lockout, concurrent session usage.
- Malicious Code
    - Malicious code attacks target communication channels and exploit the vulnerabilities of the network instead of individual devices.
    - Indicators: impossible travel, account lockout, concurrent session usage, out-of-cycle logging.

- Application Attacks
    - Injection
        - Injection attacks, like SQLi, occur when attackers insert malicious commands into an input field that does not have sufficient input validation to access the underlying behavior or database in the system.
        - Indicators: resource consumption, out-of-cycle logging, resource inaccessibility, published/documented, missing logs.
    - Buffer Overflow
        - Buffer overflow attacks occur when an application does not validate user input and more data can be written to a buffer than it can hold, causing adjacent memory to be overwritten.
        - Indicators: resource consumption, out-of-cycle logging, resource inaccessibility, published/documented, missing logs.
    - Replay
        - Replay attacks occur when an attacker intercepts legitimate session tokens and retransmits, or "replays," them to gain unauthorized access to an account or system.
        - Indicators: concurrent session usage, impossible travel, out-of-cycle logging.
    - Privilege Escalation
        - Privilege escalation attacks occur when an attacker gains access to higher levels of privileges than originally authorized, allowing them to access sensitive data or to install malware.
        - Indicators: account lockout, concurrent session usage, resource consumption, out-of-cycle logging, missing logs.
    - Cross-Site Request Forgery (CSRF)
        - CSRF attacks occur when users are tricked into performing malicious actions on a website they are logged into, exploiting the trust the browser has for users.
        - Indicators: blocked content, out-of-cycle logging, published/documented.
    - Directory Traversal
        - Directory traversal attacks occur when an attacker gains access to restricted directories due to insufficient input validation.
        - Indicators: resource consumption, out-of-cycle logging, resource inaccessibility, published/documented, missing logs.

- Cryptographic Attacks
    - Downgrade
        - Downgrade attacks occur when an attacker forces a downgrade from a stronger protocol or algorithm to a more exploitable protocol or algorithm.
        - Indicators: out-of-cycle logging, published/documented.
    - Collision
        - Collision attacks occur when attackers attempt to find hash function inputs that produce the same output hash.
        - Indicators: resource consumption, published/documented.
    - Birthday
        - Birthday attacks occur when an attacker exploits the probability of a collision.
        - Indicators: resource consumption, published/documented.
- Password Attacks
    - Spraying
        - Password spraying attacks occur when an attacker tries a small number of commonly used passwords against multiple usernames in an attempt to gain access to accounts while avoiding account lockouts.
        - Indicators: account lockout, resource consumption, out-of-cycle logging, published/documented.
    - Brute Force
        - Brute force password attacks occur when attackers try every combination of characters until a correct password is discovered.
        - Online vs. Offline
            - **Online** brute force attacks occur in real-time, where each attempt is made directly against a target system
            - **Offline** brute force attacks involve precomputing and testing large sets of potential combinations offline, typically against encrypted data.
        - Indicators: account lockout, resource consumption, out-of-cycle logging, published/documented.
- Indicators Of Compromise (IOC)
    - Account Lockout
        - Account lockouts occur when a user account has repeated failed login attempts, indicating a brute force or leaked passwords attack.
    - Concurrent Session Usage
        - Concurrent session usages occur when a user is logged in on multiple devices from physically impossible locations, indicating account compromise.

    - Blocked Content
        - Blocked content refers to frequent attempts to access blocked content, such as malicious websites, and can indicate malware.
    - Impossible Travel
        - Impossible travel occurs when a user logs in from one location, then logs in again from a geographically distant location that would be impossible for them to have traveled to between login times, indicating account compromise.
    - Resource Consumption
        - Resource consumption refers to a sudden and unusual spike in resource usage, such as CPU or network bandwidth, that may indicate malware running or a hacker attempting to exploit system vulnerabilities.
    - Resource Inaccessibility
        - Resource inaccessibility refers to resources being suddenly inaccessible to authorized users, indicating DoS attacks or malware.
    - Out-of-Cycle Logging
        - Out-of-cycle logging refers to unexpected or irregular logging activity, indicating log tampering to cover an attacker's tracks.
    - Published/Documented
        - Published or documented refers to the publication of information on systems, services, or vulnerabilities that were previously confidential.
    - Missing Logs
        - Missing logs refer to the absence of log entries in a system, indicating log tampering, manipulation, or deletion to hide or cover up an attack.

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

What are mitigation techniques?

- Techniques that reduce the seriousness and consequences of a risk, focused on minimizing the impact of a risk over eliminating the risk.

Mitigation Techniques:

- Segmentation
    - Segmentation involves dividing the network into physically or logically divided segments to boost performance or enhance security.
- Access Control
    - Access Control List (ACL)
        - ACLs define which systems and resources a user is allowed access to, along with the operations that are allowed on those resources.

    - Permissions
        - Permissions define what actions users are allowed to perform on files, directories, and other resources. Common permissions include read, write, and execute rights.
- Application Allow List
    - Application allow lists explicitly define which applications are permitted to run on a system.
- Isolation
    - Isolating endpoints completely blocks access from outside systems, applications, and networks ro prevent the spread of malicious activities or potential threats.
- Patching
    - Patching is the regular testing, approval, and deployment of software to fix vulnerabilities and security flaws.
- Encryption
    - Encryption converts data into a format readable by only authorized parties. Encryption protects data at rest through the use of full disk encryption (FDE), which is built into an OS to use, called the encrypting file system (EFS) in Windows devices, or self-encrypting drives (SED) which are built into the hardware of a device and automatically encrypts stored data.
- Monitoring
    - Monitoring involves continuously watching systems and networks for signs of compromise. A security information and event manager (SIEM) consolidates logs from all around the network and creates reports for easy monitoring. A security orchestration and automation response (SOAR) automatically alerts and responds to threats.
- Least Privilege
    - The principle of least privilege encourages the apportionment of the most minimal amount of access necessary to individuals while ensuring they can still perform their functions.
- Configuration Enforcement
    - Configuration enforcement is the process of maintaining strict configurations on every system and device, requiring all users that login to meet security expectations.
- Decommissioning
    - Decommissioning is the process of safely disposing of outdated or retired systems, including data wiping, disabling accounts, and removing access. Crypto-shredding is a specific decommissioning practice that involves securely disposing of cryptographic keys and encrypted data.

- Hardening Techniques
    - Encryption
        - Encryption protects data in transit and at rest, ensuring data remains confidential and protected.
    - Installation of Endpoint Protection
        - Endpoint protection protects individual devices from threats using tools such as antivirus, anti-malware, and endpoint detection and response (EDR) tools.
    - Host-Based Firewall
        - Host-based firewalls are built into the OS of a device and allow for the monitoring and control of network traffic from the device itself, preventing unauthorized access to the host.
    - Host-Based Intrusion Prevention System (HIPS)
        - HIPS actively detect and prevent malicious activities from the host device through monitoring and blocking suspicious actions in real-time.
    - Disabling Ports/Protocols
        - Unused ports and insecure protocols should be disabled to reduce the attack surface and entry points an attacker could exploit.
    - Default Password Changes
        - Default passwords are often widely available. Changing these passwords are important in preventing easy unauthorized access and exploitation.
    - Removal of Unnecessary Software
        - Removing unnecessary software allows for decrease in potential vulnerabilities and attack vectors, reducing security risks.

Important Acronyms in Unit 2:

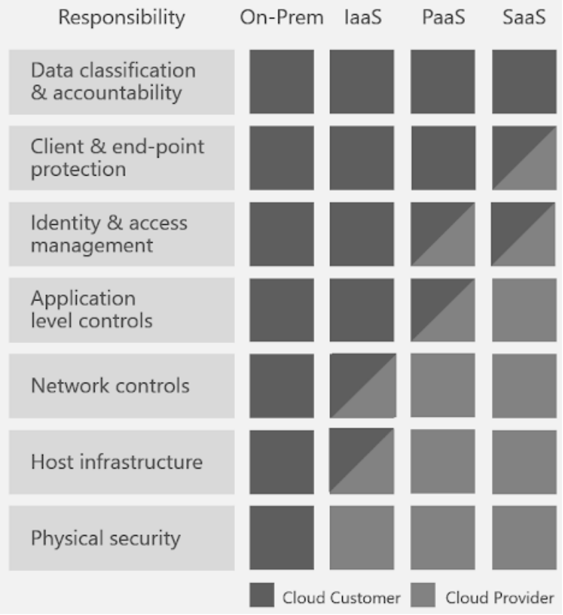
ACL - Access Control List
API - Application Programming Interface
DDoS - Distributed Denial of Service
DNS - Domain Name System
DoS - Denial of Service
EDR - Endpoint Detection and Response
EFS - Encrypting File System
HIPS - Host-based Intrusion Prevention System
HTML - HyperText Markup Language
IM - Instant Messaging
IoC - Indicators of Compromise
IP - Internet Protocol
MSP - Managed Service Providers
OS - Operating System
RFID - Radio Frequency Identification
SED - Self-Encrypting Drives
SMS - Short Message Service
SQL - Structured Query Language
SQLi - Structured Query Language injection
TCP - Transmission Control Protocol
TOC - Time-Of-Check
TOU - Time-Of-Use
UDP - User Datagram Protocol
URL - Universal Resource Locator
USB - Universal Service Bus
VLAN - Virtual Local Area Network
VM - Virtual Machine
XXS - Cross Site Scripting

Topic 3: Security Architecture

3.1 Compare and contrast security implications of different architecture models.

Architecture Models:

- Architecture and Infrastructure Concepts
    - Cloud
        - Responsibility Matrix
            - A responsibility matrix outlines the security responsibilities between a cloud service provider and a customer for the different provided services, such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service).

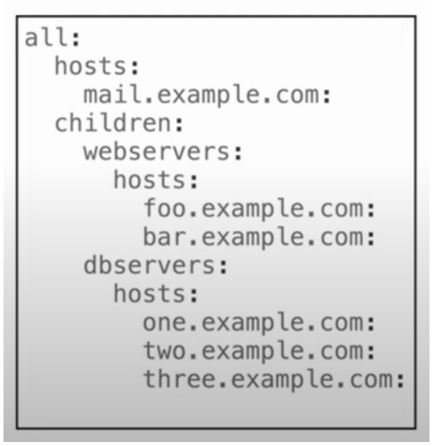


Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	■	■	■	■
Client & end-point protection	■	■	■	◩
Identity & access management	■	■	◩	◩
Application level controls	■	■	◩	▨
Network controls	■	◩	▨	▨
Host infrastructure	■	◩	▨	▨
Physical security	■	▨	▨	▨

■ Cloud Customer ▨ Cloud Provider

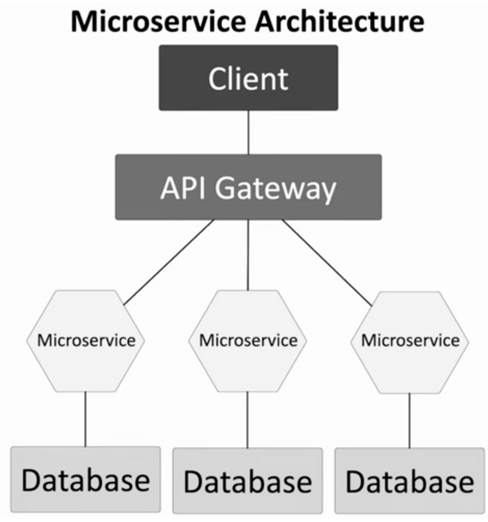
        - Hybrid Considerations
            - Hybrid clouds combine public and private clouds to enhance flexibility, but can also add additional complexity when managing across multiple providers. The systems each provider uses may work in different ways, meaning it may be necessary to manually configure the security settings for each, and, since logs are diverse and cloud-specific, monitoring may be difficult.
        - Third-Party Vendors
            - Third party vendors can provide applications and services on the cloud. It is important to conduct vendor assessments and vendor risk management to ensure third parties are trustworthy and safe.

- Infrastructure as Code (IaC)
    - IaC manages and creates infrastructure through coded scripts rather than physical hardware configuration or configuration tools. IaC automates infrastructure setups and makes scaling and consistency easier to maintain.

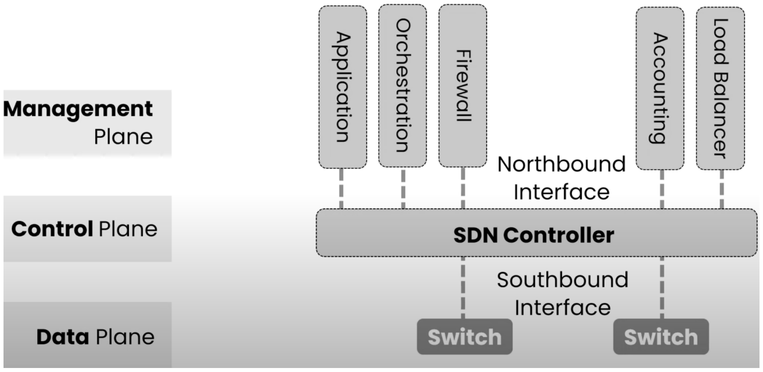


```
all:
  hosts:
    mail.example.com:
  children:
    webservers:
      hosts:
        foo.example.com:
        bar.example.com:
    dbservers:
      hosts:
        one.example.com:
        two.example.com:
        three.example.com:
```

- Serverless
    - Serverless is a cloud computing model where the CSP manages the allocation of servers to the client, while the client's developers focus on writing and deploying code devoid of server management or scaling concerns. Serverless computing, while not actually serverless, involves functions as a service (FaaS), where bigger applications are broken down into smaller unilaterally focused programs.
- Microservices
    - Microservices are well-defined services designed to perform one action. Microservices "talk" to each other using APIs, of which allow different components, like microservices, to communicate and interact with each other.

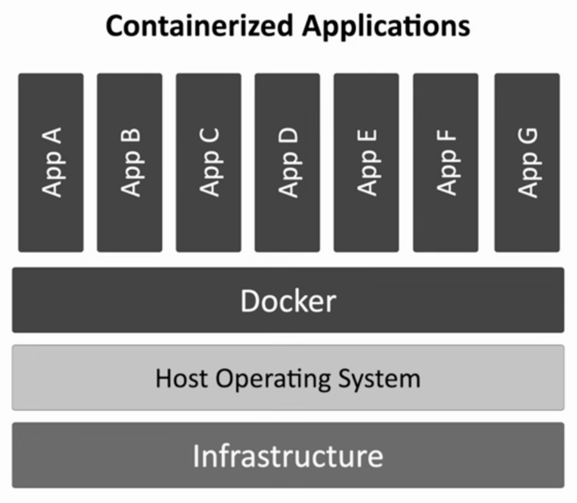


- Network Infrastructure
    - Physical Isolation
        - Physical isolation is the separation of physical devices to segment the network.
        - Air-Gapped
            - An air-gapped network is a physically isolated network that has been completely disconnected from any external network and is incapable of connecting wirelessly or physically with other computers or network devices.
    - Logical Segmentation
        - Logical segmentation is the separation of a network using software and configuration tools, often done with VLANs (Virtual Local Area Networks), which allow administrators to segment devices into separate networks regardless of their physical location.
    - Software-Defined Networking (SDN)
        - SDN is a network management approach that directs traffic based on a data, control, and management plane to control networks centrally. The data plane manages forwarding data, processing network packets, and encryption. The control plane manages what actions occur in the data plane such as routing tables and session tables. The management plane manages the configuration of devices, such as the browser and ssh.

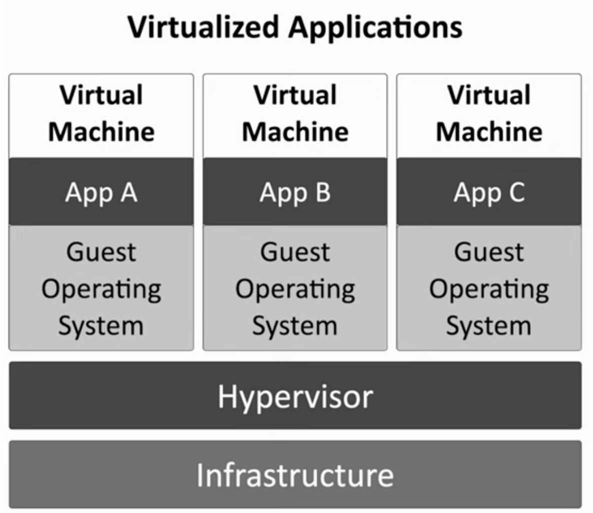


- On-Premises
    - On-premises refers to an infrastructure that is all located and managed at the physical location of an organization, allowing for complete control over hardware, software, and security but requires larger staffing, resources, and management.

- Centralized vs. Decentralized
    - **Decentralized**: Physically decentralized organizations have multiple locations, systems, and third-party providers, avoiding a single point of failure but more difficult to secure.
    - **Centralized**: Physically centralized organizations have all data and networking tasks handled by a central server or data center, simplifying management but creating a single point of failure.
- Containerization
    - Containerization is a virtualization method that allows applications to run in isolated "containers" on a single OS. Each containerized application is unable to interact with any others on the OS, and must be configured to run on the host's OS.



- Virtualization
    - Virtualization is the process of dividing a physical server into multiple unique and isolated virtual servers through use of a hypervisor.



    - IoT
        - The Internet of Things (IoT) is the class of devices that connect to the internet and exchange data with systems and devices.
    - Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA)
        - ICS and SCADA systems are designed to closely monitor, control, and collect data on industrial operations. They provide the efficient, safe, and reliable operation of critical infrastructure like power plants, water treatment facilities, and manufacturing plants. These need to be highly segmented and closely monitored, as outside access to systems such as power generation and oil refinements could not only impact the company managing the system, but could have immediate and long lasting impact on consumers.
    - Real-Time Operating System (RTOS)
        - RTOS is used for applications that require high reliability and precise timing, like embedded systems in medical devices and industrial automation, where delays can lead to failures or unsafe conditions. For example, braking your car takes immediate priority in your vehicle and having a fast, real-time response to pressure on the brake pedal is crucial. These systems are typically self-contained and difficult to access, as installing firewalls and anti-malware is difficult and could result in non-immediate responses or delays.
    - Embedded Systems
        - Embedded systems are computing systems specially made to perform dedicated functions or tasks optimized for specific applications, such as apple watches, stoplights, and digital cameras.
    - High Availability (HA)
        - High availability systems are systems designed to provide continuous operation and minimal downtime, even in the event of a failure or during maintenance.
- Considerations
    - Availability
        - Availability refers to a system that remains accessible when needed.
    - Resilience
        - Resilience refers to a system that can withstand or quickly recover from attacks or disruptions without impacting availability.
    - Cost
        - Cost refers to the ongoing financial requirement to retain staff, license, hardware, software, and other expenditures.

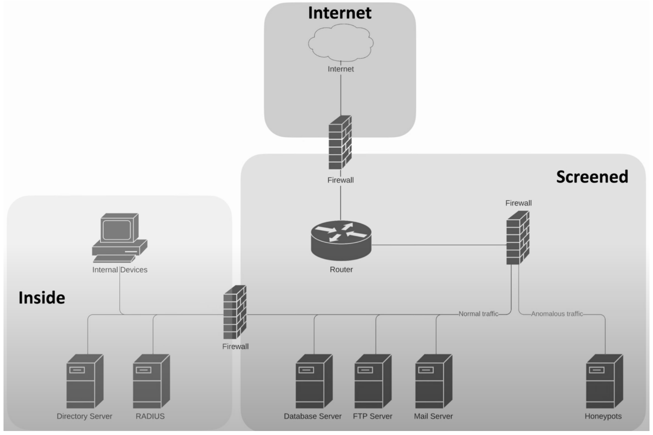
- Responsiveness
  - Responsiveness refers to a system’s ability to respond and react to user requests in a timely manner.
- Scalability
  - Scalability refers to a system’s ability to scale resources to handle increased loads and meet demands.
- Ease of Deployment
  - Ease of deployment refers to the complexity and effort it takes to implement a solution, including the initial and ongoing costs.
- Risk Transference
  - Risk transference refers to the transference of risks to a third party, often through insurance, to mitigate the impact of risks.
- Ease of Recovery
  - Ease of recovery refers to the time and effort it takes to restore a system to normal operation after a failure or disruption.
- Patch Availability
  - Patch availability refers to how timely and available updates and patches are for vulnerabilities on a system.
- Inability to Patch
  - Inability to patch refers to a system that is outdated or unable to be patched, often because of legacy software, that might need alternative security measures.
- Power
  - Power refers to power consumption low to keep costs low while still providing ongoing availability to services.
- Compute
  - Compute refers to keeping the need for computational power low to keep costs low while still handling workloads and maintaining performance levels.

3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

Security Principles:

- Infrastructure Considerations
  - Device Placement
    - Device placement involves positioning hardware components within a network to provide the most optimal performance and security possible.

- Security Zones
    - Security zones are containment zones within a network that prevent an attacker that gains access to the network to spread to the entire network. This includes: an intranet, or private network that hosts the internal information of an organization; an extranet, or the part of the network that links the intranet to the internet; and a screened subnet, or the public-facing extranet, also known as a demilitarized zone (DMZ).

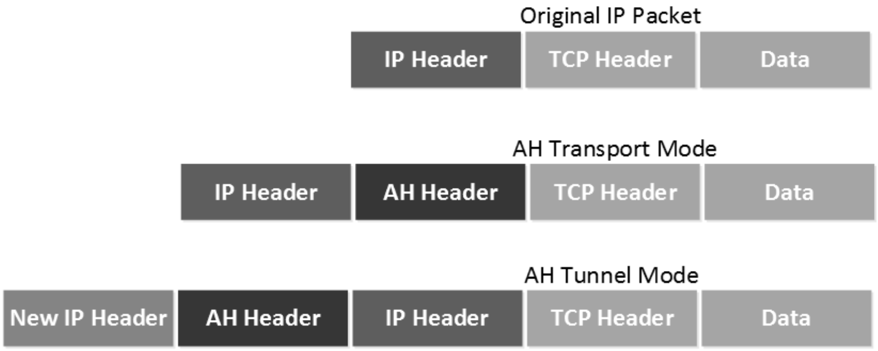


- Attack Surface
    - An attack surface is all of the entry points an attacker can exploit to attack or gain access to a system, including the ways an attacker might come after it.
- Connectivity
    - Connectivity is the ability of devices within a system to adequately communicate with each other.
- Failure Modes
    - Fail-Open
        - Fail-open is a mode where, if a failure or disruption occurs, the system defaults to allowing all data or traffic to pass through, prioritizing availability, but exposing the system to security risks as protective mechanisms are down during failure.
    - Fail-Closed
        - Fail-closed is a mode where, if a failure or disruption occurs, the system defaults to blocking all data and traffic from passing through, prioritizing security, but disrupting service.

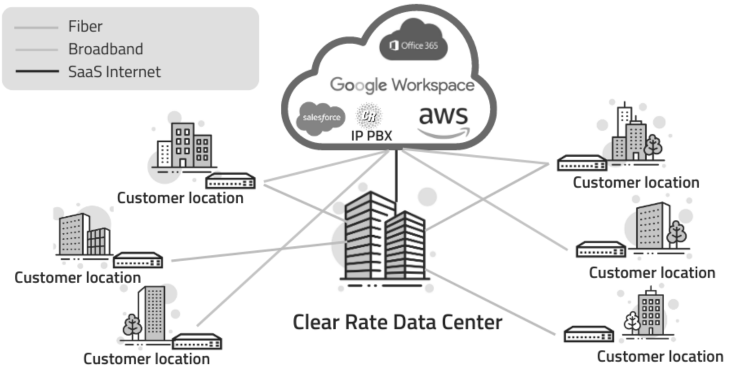
- Device Attribute
    - Active vs. Passive
        - **Active Devices**: Active devices interact directly with traffic by filtering, modifying, or forwarding it, such as a firewall or IPS.
        - **Passive Devices**: Passive devices do not interact directly with traffic; instead monitoring or analyzing it. Devices include an IDS and network taps.
    - Inline vs. Tap/Monitor
        - **Inline Devices**: Inline devices are found directly in the line of traffic and data is directly passed through them. They inspect and control traffic, like a firewall, load balancer, or IPS.
        - **Tap/Monitor Devices**: Tap/Monitor devices observe traffic without being in the direct path through tapping duplicating traffic to monitor events, like an IDS or network analyzer.
- Network Appliances
    - Jump Server
        - A jump server is used to manage devices in a separate security zone, allowing admin to connect remotely to the network.
    - Proxy Server
        - A proxy server is used to control requests from clients seeking resources on the internet or external network. It is primarily used to filter outbound web traffic.
    - Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
        - **Intrusion Detection System (IDS)**: IDS monitors network traffic for malicious or suspicious activities passively, alerting administrators in the event of a potential security incident.
        - **Intrusion Prevention System (IPS)**: IPS builds on IDS by actively rejecting the malicious packets.
    - Load Balancer
        - Load balancers distribute network traffic across multiple servers to increase server reliability and performance, making sure no single server becomes overwhelmed.
    - Sensors
        - Sensors are devices that observe and collect data on the changes in network patterns, such as network performance or security events.

- Port Security
    - 802.1X
        - 802.1X provides port-based network access control through enabling an authentication protocol for devices trying to connect to a LAN or WAN. Authentication occurs over a RADIUS server, forming a three-way authentication with the user, authenticator, and authentication server. Authentication relies on the EAP.
    - Extensible Authentication Protocol (EAP)
        - EAP is an authentication framework that allows newer authentication technologies to be compatible with older point-to-point authentication.
        - LEAP, or lightweight EAP, was the Cisco alternative to TKIP before 801.2X and WPA became the standard.
        - PEAP, or protected EAP, encompasses EAP in a TLS tunnel, providing authentication and encrypted/protected data transfers.
        - EAP-FAST is Cisco's replacement to LEAP, providing wireless point-to-point connections for session authentication.
        - EAP-TLS is a secure version of wireless authentication requiring X.509 certificates.
        - EAP-TTLS offers greater flexibility with TLS tunneling and password-based authentication.
- Firewall Types
    - Web Application Firewall (WAF)
        - WAF are designed to protect web applications through filtering HTTP/HTTPS traffic between web apps and the internet, protecting from vulnerabilities such as SQLi, XXS, and CSRF. WAF is not a primary firewall, but it is good for protecting web applications exposed to the internet.
    - Unified Threat Management (UTM)
        - UTM is an all–in-one solution to security. It combines firewall, antivirus, IDS/IPS, and filtering, etc. into one application.
    - Next-Generation Firewall (NGFW)
        - NGFW are advanced firewalls that combine traditional firewalls with WAFs. They offer deep packet inspection with the ability to process traffic from Layers 3, 4, and 7 and use that information to take action before traffic reaches the application

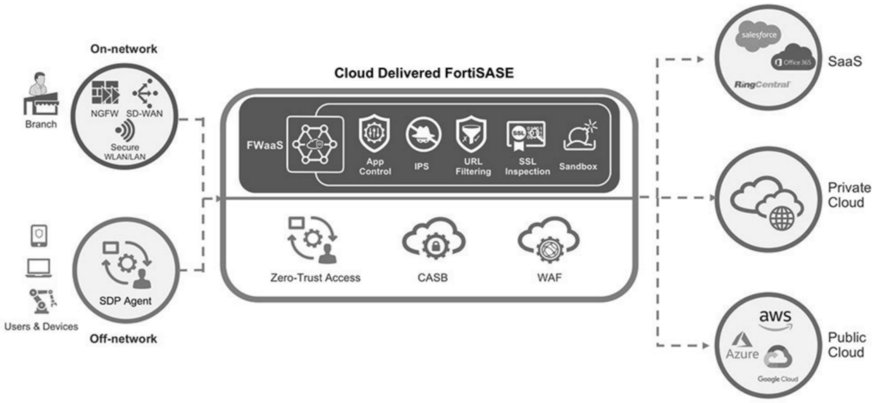
        - Layer 4/Layer 7
            - Layer 4 is the transport layer of the OSI model, containing traffic's IP addresses, port numbers, and transport protocols. This layer is used by a traditional firewall and allows for basic packet filtering.
            - Layer 7 is the application layer of the OSI model and is used to analyze the content of the traffic to understand the specific applications and services being used. This layer is used by NGFW.
- Secure Communication/Access
    - Virtual Private Network (VPN)
        - VPNs create secure, encrypted tunnels over insecure networks, like the internet. Users can send data that is protected from unauthorized access, allowing for secure access to private networks from remote locations.
    - Remote Access
        - Remote access is the ability of a computer to connect to a system or server without being physically present. Solutions include VPNs and remote desktop services.
    - Tunneling
        - Tunneling encapsulates one type of network protocol within another protocol. This allows encrypted and secure transmission of data over a network by creating a “tunnel.”
        - Transport Layer Security (TLS)
            - TLS is a cryptographic protocol that encrypts data sent over the internet for secure and private communications, commonly used in HTTPS.
        - Internet Protocol Security (IPSec)
            - IPSec is a suite of protocols used to secure IP communications. It includes an authentication header (AH) and encapsulating security payloads (ESP) protocols. AH is used to provide authentication and ESP provides confidentiality and integrity through encryption. IPSec has two modes: transport mode and tunnel mode.



  - Software-Defined Wide Area Network (SD-WAN)
    - SD-WAN enables users in remote offices to securely and remotely connect to an organization’s network, allowing the usage of many network services, such as LTE, MPLS, and broadband. It uses IPSec, VPNs, and NGFWs to provide secure connections.



  - Secure access service edge (SASE)
    - SASE combines networking, WAN, and security, delivering them as a unified cloud service using cloud architecture. It integrates SD-WAN with security functions like secure web gateways, cloud access security brokers, firewall-as-a-service, and zero-trust network access. SASE can automatically connect remote and hybrid users to nearby cloud gateways instead of routing traffic to corporate data centers.



- Selection of Effective Controls
  - Selection of effective controls takes into account the assets, vulnerabilities, impact, and threat landscape of an organization to select the best security controls to protect a company.

3.3 Compare and contrast concepts and strategies to protect data.

Data Protection Strategies:

- Data Types
  - Regulated
    - Regulated data is subject to laws and regulations governing its use, storage, and transmission, such as financial and health information.
  - Trade Secret
    - Trade secrets are intellectual property that is critical to a business and is not to be disclosed, such as formulas, processes, or proprietary techniques.
  - Intellectual Property
    - Intellectual property are creations of the mind, such as inventions, names, and artistic designs.
  - Legal Information
    - Legal information includes any data related to legal proceedings.
  - Financial Information
    - Financial information includes any financial data maintained by an organization, such as transaction records and tax information.
  - Human and Non-Human Readable
    - **Human-Readable Data**: Human readable data is formatted in a way that is easily understood by humans, such as emails and reports.
    - **Non-Human Readable Data**: Non-human readable data requires software or computing tools to be understood, such as binary or encrypted data.
- Data Classifications
  - Sensitive
    - Sensitive data is not publicly known and requires careful handling, encompassing private, confidential, and restricted data.
  - Confidential
    - Confidential data is meant to be kept secret within certain authorized groups, such as salary data and trade secrets.
  - Public
    - Public data is free and accessible information intended for the general public without restriction.
  - Restricted
    - Restricted data is subject to external regulations and legal requirements, requiring access controls and protections to prevent unauthorized access.
  - Private
    - Private data is information about an individual meant to be kept confidential, such as protected health information (PHI) and personally identifiable information (PII).

        - Critical
            - Critical data is important to the ongoing operation of an organization and would cause a significant impact to the organization if lost or tampered.
- General Data Considerations
    - Data States
        - Data at Rest
            - Data at rest is information that is currently stored– not in use or in transit. Securing this data involves encryption, access controls, and physical security so no unauthorized access can occur.
        - Data in Transit
            - Data in transit is information actively moving from one location to another, such as across the internet. Securing this data includes using TLS/SSL, VPNs, and secure communication channels so that the data remains confidential and integral.
        - Data in Use
            - Data in use is information being currently processed and actively used or accessed. Securing this data includes using strong access controls, memory protection techniques, and secure coding practices to prevent unauthorized access and tampering.
    - Data Sovereignty
        - Data sovereignty means that data is subject to the laws and regulations of the country where it was created and where it is physically stored. Data cannot be moved to another region, even as a backup.
    - Geolocation
        - Geolocation involves using a GPS in order to give the physical location of a device. This can be used for a variety of reasons, including enforcing geographic restrictions on data access.
- Methods to Secure Data
    - Geographic Restrictions
        - Geographic restrictions limit access to data based on physical location, preventing access from certain regions or countries.
    - Encryption
        - Encryption is a two-way function that converts data into a format readable by only authorized parties through the usage of decryption keys.
    - Hashing
        - Hashing transforms inputted data into a fixed-length, irreversible hash through a hashing algorithm.

- Masking
    - Data masking is the practice of hiding information by replacing it with fictional values, such as asterisks. A credit card might be displayed on a receipt as: ****-****-1234.
- Tokenization
    - Tokenization is the practice of replacing data with a unique identifier that has no value outside of the context of the tokenization system, but, within the system, they are functional and connect to the original piece of data.
- Obfuscation
    - Obfuscation is the practice of altering data to make it unclear, while retaining its functionality to protect data from being easily understood.
- Segmentation
    - Segmentation involves dividing the network into physically or logically divided segments to limit the spread of potential breaches, so that compromised data in one segment does allow access to the entire system.
- Permission Restrictions
    - Permissions define what actions users are allowed to perform on files, directories, and other resources, reducing the risk of data exposure and unauthorized actions.

3.4 Explain the importance of resilience and recovery in security architecture.

Resilience and Recovery:

- High Availability
    - High availability systems are systems designed to provide continuous operation and minimal downtime, even in the event of a failure or during maintenance.
    - Load Balancing vs. Clustering
        - **Load Balancing**: Load balancing is the practice of distributing network traffic across multiple servers to increase server reliability and performance, making sure no single server becomes overwhelmed.
        - **Clustering**: Clustering is the practice of grouping multiple servers and systems together, so that if one fails, another can take over its workload without interrupting services.
- Site Considerations
    - Hot
        - A hot site is a backup facility that has been pre-prepared to take over operations immediately in the event that the primary site fails. It has up-to-date hardware, software, network connectivity, and data, ready to immediately continue operations.

  - Cold
    - A cold site is a backup facility that lacks all hardware, software, network connectivity, and data– providing only the most basic infrastructure and requiring significant time to become operational after a disaster.
  - Warm
    - A warm site is a backup facility between a hot site and a cold site, providing hardware and network connectivity, but requiring restoration before becoming fully operational.
  - Geographic Dispersion
    - Geographic dispersion involves placing backup sites and data centers in geographically different locations to prevent regional disasters affecting all sites simultaneously.
- Platform Diversity
  - Platform diversity involves using many different OS, CSPs, and vendors ro reduce the likelihood that a failure in one platform will affect all systems.
- Multi-Cloud Systems
  - Multi-cloud systems involve using multiple CSPs to distribute data and applications across to enhance redundancy and fault tolerance in the case of an outage or attack on one of the clouds.
- Continuity of Operations (CoOp)
  - COOP are the processes and procedures an organization puts in place to ensure operations can continue during and after a failure or disruption, such as backups.
- Capacity Planning
  - People
    - Capacity planning for people ensures that the workforce processes the necessary skills and is large and knowledgeable enough to handle maintaining systems and responding to incidents.
  - Technology
    - Capacity planning for technology ensures that software, hardware, and other tools are maintained correctly to ensure appropriate security and sufficiency in supporting normal operations and additional loads.
  - Infrastructure
    - Capacity planning for infrastructure ensures there are adequate resources, such as storage and network processing, to handle current and future operational demands.
- Testing
  - Tabletop Exercises
    - Tabletop exercises are discussion-based, simulated walkthroughs of emergency scenarios to identify gaps and ensure understanding.

  - Fail Over
    - Failovers are tests that physically shut down the primary site and test whether or not the backup site can handle continuing operations.
  - Simulation
    - Simulations are functional and realistic exercises done in a controlled environment to mimic the conditions of a disaster, providing a practical, hands-on way to test recovery plans, weaknesses, and staff.
  - Parallel processing
    - Parallel processing are tests that activate the backup site, without shutting down the main site, to ensure the recovery site is operational and operations can still continue at the main site, unlike failover tests.
- Backups
  - Onsite/Offsite
    - **Onsite**: Onsite backups are stored at the same location as the primary data center.
    - **Offsite**: Offsite backups are stored at a different, remote location.
  - Frequency
    - Frequency refers to how often backups are performed, such as daily or hourly. The frequency depends on the importance of data, the amount of changes that occur within a period of time, and the acceptable level of data loss in the event of a disaster.
  - Encryption
    - Encryption of backups ensures no unauthorized access to stored data.
  - Snapshots
    - Snapshots are copies of the state of data at a specific moment in time, allowing recovery to that specific state.
  - Recovery
    - Recovery is the process of restoring the data from a backup to its original location or new location following a disruption or data loss.
  - Replication
    - Replication is the process of creating duplicates of data in multiple locations for redundancy.
  - Journaling
    - Journalling is a logged record of changes made to data in a sequential log file, used to recover data by replaying logged changes.
- Power
  - Generators
    - Generators are backup power systems that provide electricity to an organization for an extended period in the event of a power outage.

- Uninterruptible Power Supply (UPS)
    - A UPS is a standby, battery-powered device that provides immediate, short-term power to critical systems when the primary power source fails.

Important Acronyms in Unit 3:

EAP - Extensible Authentication Protocol
CoOp- Continuity of Operations/Continuity of Operations Planning
HA - High Availability
IaaS - Infrastructure as a Service
IaC - Infrastructure as Code
ICS - Industrial Control Systems
IDS - Intrusion Detection System
IEEE - Institute of Electrical and Electronics Engineers
IoT - Internet of Things
IPS - Intrusion Protection System
IPSec - Internet Protocol Security
NGFW - Next Generation Firewall
PaaS - Platform as a Service
PHI - Protected Health Information
PII - Personally Identifiable Information
RPO - Recovery Point Objectives
RTO - Recovery Time Objectives
RTOS - Real Time Operating System
SaaS - Software as a Service
SASE - Secure Access Service Edge
SCADA - Supervisory Control and Data Acquisition
SDN - Software-Defined Networking
SD-WAN - Software-Defined Wide Area Network
SLA - Service-Level Agreement
TLS - Transport Layer Security
UPS - Uninterruptible Power Supply
UTM - Unified Threat Management
VPN - Virtual Private Network
WAF - Web Application Firewall

Topic 4: Security Operations

4.1 Given a scenario, apply common security techniques to computing resources.

Security Techniques:

- Secure Baselines
    - A secure baseline is a set of security configurations and best practices for the minimum security requirements that must be met to secure an organization.
    - Establish
        - Establishing refers to the process of defining and setting up the initial security configurations and policies.
    - Deploy
        - Deploying is applying the established security configurations and settings across the organization's systems, applications, and networks..
    - Maintain
        - Maintaining involves ongoing monitoring, updating, and managing the security configurations to ensure the standards adhere to the baseline.
- Hardening Targets
    - Mobile Devices
        - Hardening mobile devices involves device encryption, strong passwords, remote wipe, updating OS and apps, and disabling bloatware.
    - Workstations
        - Hardening workstations involves antivirus, security patches and updates, firewalls, restricting user privileges, and disabling unnecessary services.
    - Network Infrastructure Devices
        - Hardening network infrastructure involves configuring authentication, strong passwords, firmware updates, and ACLs.
    - Cloud Infrastructure
        - Hardening cloud infrastructure involves IAM, encryption, logging, monitoring, and secure configuration.
    - Servers
        - Hardening servers includes updating OS, patching, configuring firewalls, disabling unnecessary services, and strong authentication.
    - ICS/SCADA
        - Hardening ICS/SCADA systems involves segmentation, physical security, change management, IDS, password management, and monitoring.
    - Embedded Systems & RTOS
        - Hardening embedded systems & RTOS involves secure coding practices, firmware update, secure boot, and limited network access.

    - IoT Devices
        - Hardening IoT devices involves strong passwords, firmware updates, segmentation, and secure communication protocols..
- Wireless Devices
    - Installation Considerations
        - Site Surveys
            - Site surveys are an assessment of the presence, strength, and reach of wireless access points in relation to the physical environment.
        - Heat Maps
            - Heat maps are visual representations of wireless signal strength and coverage that visually display areas with strong, moderate, and weak signals.
- Mobile Solutions
    - Mobile Device Management (MDM)
        - MDM solves how organizations can securely manage and monitor mobile devices using passwords, geofencing, app and content management, remote wipe, screen lock, geolocation, and push notifications.
    - Deployment Models
        - Bring Your Own Device (BYOD)
            - BYOD is a policy where employees use their own mobile devices for work, requiring more detailed MDM policies to secure, such as acceptable use policy (AUP) and on/offboarding policies.
        - Corporate-Owned, Personally Enabled (COPE)
            - COPE is a policy where the employer provides devices for employees to use for both work and personal activities. Organizations have more control over the device, as IT can control security, wipes, and applications.
        - Choose Your Own Device (CYOD)
            - CYOD is a policy where employees choose from a select few pre-approved devices that employees can buy and bring to work, allowing IT to manage fewer devices while still offering options.
    - Connection Methods
        - Cellular
            - Cellular connections use mobile networks operated by carriers to provide internet and communication services to mobile devices.
        - Wi-Fi
            - Wi-Fi connections use wireless local area networks to provide internet access to mobile devices within a limited range.

        - Bluetooth
            - Bluetooth is a short-range wireless technology used for connecting mobile devices to other Bluetooth-enabled devices..
- Wireless Security Settings
    - Wi-Fi Protected Access 3 (WPA3)
        - WPA3 is the latest security protocol for Wi-Fi networks. It provides stronger encryption and more secure authentication methods compared to WPA2. WPA3 uses Simultaneous Authentication of Equals (SAE) to ensure authenticity and integrity.
        - SAE allows for the mutual authentication of devices as part of a handshake process using cryptographic tools to prevent brute force attacks. Authentication hashes a key unique to each authentication, rather than having the same key every time.
    - AAA/Remote Authentication Dial-In User Service (RADIUS)
        - RADIUS is a network protocol designed to provide AAA. RADIUS is often used to authenticate users connecting to Wi-Fi networks. User's usernames and passwords are sent to a RADIUS server to be authenticated during log-in. This is often the back-end of the 802.1X authentication.
    - Cryptographic Protocols
        - Cryptographic protocols are tools for securing wireless networks by encrypting data and preventing unauthorized access. Common cryptographic protocols used in wireless security include WPA3.
    - Authentication Protocols
        - Authentication protocols are used to verify the identity of users or devices, such as the Extensible Authentication Protocol (EAP), which supports various authentication methods and is commonly used along with 802.1X.
- Application Security
    - Input Validation
        - Input validation verifies that inputted data provided by external parties meets the expected format before being accepted and processed.
    - Secure Cookies
        - Secure cookies are used by web browsers and contain session information. Setting cookies to be secure ensures that they can only be downloaded in HTTPS sessions.
    - Static Code Analysis
        - Static code analysis is the process of examining source code without executing it to identify potential vulnerabilities or errors.

    - Code Signing
        - Code signing is the process of digitally signing software or executables to verify the authenticity and integrity of the code.
- Sandboxing
    - Sandboxing is a security process that isolates applications so that testing and patching can safely occur isolated from the network or malicious activity can be contained.
- Monitoring
    - Monitoring involves continuously watching systems and networks for signs of compromise. A SIEM consolidates logs for easy monitoring, including alerting and analyzing application activities, user actions, and system events.

4.2 Explain the security implications of proper hardware, software, and data asset management.

Security Implications:

- Acquisition/Procurement Process
    - The acquisition/procurement process includes ensuring hardware, software, and data assets are acquired from reputable sources and meet security standards.
- Assignment/Accounting
    - Ownership
        - Ownership refers to the process of clearly defining who is responsible for each asset.
    - Classification
        - Classifying is the process of categorizing assets based on their sensitivity and importance to ensure appropriate security is applied.
- Monitoring/Asset tracking
    - Inventory
        - An inventory is an up-to-date list of all hardware, software, and data assets for tracking and management in events such as new patches needing to be installed or incidents in which devices need to be quickly located.
    - Enumeration
        - Enumeration is the process of cataloging and identifying all assets of an organization or device (CPU type, memory, storage, etc.).
- Disposal/Decommissioning
    - Sanitization
        - Sanitization is the process of irretrievably removing data from a decommissioned device, preventing unauthorized access to residual data.
    - Destruction
        - Destruction is the process of destroying a device beyond recovery.

        - Certification
            - Certification is documented proof that formally verifies an asset has been sanitized or destroyed for compliance purposes.
        - Data Retention
            - Data retention policies define how long data must be stored before destruction to comply with legal and regulatory requirements.

4.3 Explain various activities associated with vulnerability management.

Vulnerability Management:

- Identification Methods
    - Vulnerability Scan
        - Vulnerability scans periodically scan the network to detect known vulnerabilities, misconfigurations, outdated software, and missing patches, helping identify weaknesses in an organization before they are exploited.
    - Application Security
        - Static Analysis
            - Static analysis is the process of examining source code without executing it to identify potential vulnerabilities or errors.
        - Dynamic Analysis
            - Dynamic analysis is the process of examining source code as it is running to identify potential vulnerabilities or errors, including improper input management, runtime errors, and memory leaks.
        - Package Monitoring
            - Package monitoring refers to tracking third-party or open-source packages and libraries used in an application for vulnerabilities.
    - Threat Feed
        - Open-Source Intelligence (OSINT)
            - OSINT are publicly available sources of information such as security blogs, social media, and government advisories, to identify potential threats and vulnerabilities.
        - Proprietary/Third-Party
            - Proprietary/third-parties are intelligence feeds that offer vendor-specific information to keep customers updated on vulnerabilities and keep attackers unalerted.
        - Information-Sharing Organization
            - These are groups where organizations share threat intelligence and best practices.

        - Dark Web
            - The dark web can provide an organization with early warnings of potential threats through underground forums and marketplaces where cybercriminals discuss and trade stolen data, exploits, and attack tools.
    - Penetration Testing
        - Pen testing, or ethical hacking, involves actively testing and probing a system in an attempt to find and exploit vulnerabilities to provide a comprehensive assessment of the organization's security posture.
    - Responsible Disclosure Program
        - Responsible disclosure is a process that allows hackers to safely report found vulnerabilities.
        - Bug Bounty Program
            - The bug bounty program is a program where organizations offer financial rewards in exchange for researchers responsibly disclosing vulnerabilities in their systems.
    - System/Process Audit
        - System/process audits are used to review and evaluate an organization's IT systems, processes, and controls to ensure they meet security standards and identify areas of non-compliance/risk.
- Analysis
    - Confirmation
        - False Positive
            - A false positive occurs when a vulnerability scan or security tool detects a vulnerability that is not present.
        - False Negative
            - A false negative happens when a vulnerability scan or security tool fails to detect a vulnerability.
    - Prioritize
        - Prioritizing vulnerabilities based on severity, exploitability, and potential impact helps address the most critical vulnerabilities first.
    - Common Vulnerability Scoring System (CVSS)
        - CVSS is a standardized framework for rating the severity of security vulnerabilities from 0 to 10.
    - Common Vulnerability Enumeration (CVE)
        - CVE is a standardized list of publicly known security vulnerabilities where each entry includes an ID, description, and relevant patches.

    - Vulnerability Classification
        - Vulnerability classification is the process of categorizing vulnerabilities based on their type, severity, or potential impact.
    - Exposure Factor
        - Exposure factor refers to the potential impact or damage to an organization if a particular vulnerability is exploited, helping in quantifying the risk associated with vulnerabilities
    - Environmental Variables
        - Environmental variables are factors of an organization's environment that can influence the severity and impact of vulnerabilities, including network architecture and system configurations.
    - Industry/Organizational Impact
        - Evaluating the industry/organizational impact involves assessing how a vulnerability could affect the specific industry or organization. Factors such as regulatory requirements, customer trust, financial impact, and reputation are considered.
    - Risk Tolerance
        - Risk tolerance is the level of risk an organization is willing to accept in pursuit of its objectives. It reflects the organization's ability to endure losses or adverse outcomes without jeopardizing its operations or goals.
- Vulnerability Response and Remediation
    - Patching
        - Patching is the regular testing, approval, and deployment of software to fix vulnerabilities and security flaws.
    - Insurance
        - Cybersecurity insurance provides financial protection against losses from cyber incidents, including those related to vulnerabilities.
    - Segmentation
        - Segmentation involves dividing the network into segments to limit the spread of potential breaches, reducing the overall impact of vulnerabilities.
    - Compensating Controls
        - Compensating controls are secondary or support measures put in place to mitigate vulnerabilities, such as firewalls or IDSs.
    - Exceptions and Exemptions
        - Exceptions and exemptions are documented and approved special cases of not remediating a vulnerability in the event that it is not possible or practical to remove a vulnerability immediately.

- Validation of Remediation
    - Rescanning
        - Rescanning involves conducting another vulnerability scan to ensure that the vulnerabilities have been successfully addressed.
    - Audit
        - Security audits are a comprehensive review and examination of systems to identify any remaining vulnerabilities or confirm that remediation measures were effective.
    - Verification
        - The verification process involves confirming that any identified vulnerabilities have been remediated through testing, reviewing logs, and conducting manual checks.
- Reporting
    - Reporting involves documenting and communicating the status of vulnerability management activities, including identified vulnerabilities, remediation actions, rescanning and audit result, and security posture.

4.4 Explain security alerting and monitoring concepts and tools.

Alerting and Monitoring Concepts & Tools:

- Monitoring Computing Resources
    - Systems
        - Systems monitoring involves tracking the performance and health of servers, desktops, and virtual machines to identify performance bottlenecks, hardware failures, and other issues.
    - Applications
        - Application monitoring involves tracking the performance and health software applications to detect and resolve issues like application crashes, slow performance, and security vulnerabilities.
    - Infrastructure
        - Infrastructure monitoring involves tracking the performance and health of hardware and network components including servers, storage devices, and network switches, routers, and cloud resources to ensure functionality.
- Activities
    - Log Aggregation
        - Log aggregation involves collecting and consolidating log data from multiple sources into a centralized report of system activities.

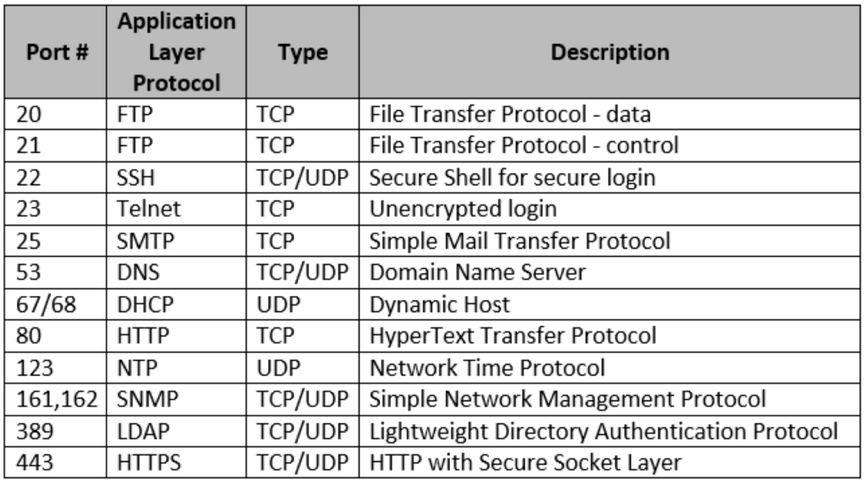
    - Alerting
        - Alerting is the process of generating notifications or alarms when suspicious activities or security events are detected through SIEMs, IDS/IPS, or monitoring tools.
    - Scanning
        - Scanning involves periodically searching the network to detect vulnerabilities, misconfigurations, outdated software, and missing patches. Types of scanning include vulnerability scanning, network scanning, and application scanning.
    - Reporting
        - Reporting is the process of creating detailed reports on security events, vulnerabilities, and compliance statuses to track security controls and support decision-making processes.
    - Archiving
        - Archiving is the long-term storage information required for regulatory compliance, forensic investigations, and historical analysis.
    - Alert Response and Remediation/Validation
        - Quarantine
            - Quarantine is the isolating of suspicious or compromised systems to prevent the spread of malware throughout a network,
        - Alert tuning
            - Alert tuning is the process of refining alerting systems to reduce false positives and false negatives.
- Tools
    - Security Content Automation Protocol (SCAP)
        - SCAP is a suite of standards used to automate vulnerability management, security measurement, and compliance evaluation to assess, measure, and report the security posture of systems.
    - Benchmarks
        - Security benchmarks are sets of best practices and guidelines to follow when securing systems and applications.
    - Agents/Agentless
        - **Agents**: Security agents are software components that send logs for systems that don't have specific log forwarding capabilities, like server and desktop endpoints.
        - **Agentless**: Agentless systems send data without the need of a local agent.

- Security Information and Event Management (SIEM)
    - SIEM systems collect, aggregate, and analyze log data from various sources within an organization, providing real-time monitoring and alerts on suspicious activities.
- Antivirus (AV)
    - Antivirus software is designed to detect, prevent, and remove malware using signature-based detection to identify and mitigate threats.
- Data Loss Prevention (DLP)
    - DLP solutions are designed to prevent sensitive data from being lost, misused, or accessed by unauthorized users. DLP tools monitor, detect, and block the transfer of confidential information.
- Simple Network Management Protocol (SNMP) Traps
    - SNMP traps are alert messages sent from network devices to a management system when specific events or threshold breaches occur.
- NetFlow
    - NetFlow is a network protocol developed by Cisco for collecting and analyzing IP traffic information, providing data on network traffic patterns– including the source and destination of traffic, the type of service, and the amount of data transferred.
- Vulnerability Scanners
    - Vulnerability scanners periodically scan the network to detect known vulnerabilities, misconfigurations, outdated software, and missing patches, helping identify weaknesses in an organization before they are exploited.

4.5 Given a scenario, modify enterprise capabilities to enhance security.

Enterprise Capabilities:

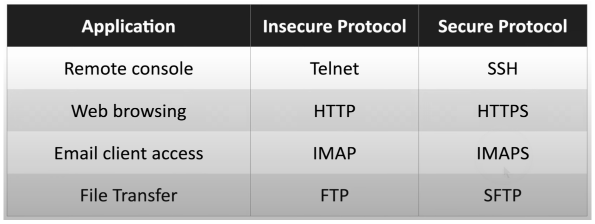
- Firewall
    - Firewalls filter traffic based on predefined security rules.
    - Rules
        - Firewall rules define the allowed and denied sources, destinations, and protocols that can pass through the network. Regularly remove outdated rules, permissions, and add new rules to address emerging threats.
    - Access Lists
        - Access lists are the collection of rules that define what traffic is allowed and what traffic is denied. The default rule should be to deny all.
    - Ports/Protocols
        - Every network connection happens over a specific port using a specific protocol. Transmission protocols include TCP, UDP, and ICMP.



Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

  - Screened Subnets
    - Screened subnets isolate and protect internal networks from external threats by placing public-facing services (e.g., web servers) in a demilitarized zone to provide an additional layer of protection.
- IDS/IPS
  - IDS and IPS detect and prevent malicious activities within the network.
  - Trends
    - Trends are unusual patterns that may indicate potential threats or anomalies.
  - Signatures
    - Signatures are predefined patterns of malicious activities used by IDS/IPS to detect known attacks or threats.
- Web Filter
  - Web filtering controls and monitors the content that users access on the internet.
  - Agent-Based
    - Agent-based web filters are installed on endpoints and enforce web access policies directly on the device, providing consistent filtering regardless of the user's location or network.
  - Centralized Proxy
    - A centralized proxy server routes all internet traffic allowing for centralized monitoring and control of web traffic.
  - Universal Resource Locator (URL) Scanning
    - URL scanning checks web addresses before allowing access to detect and block access to known malicious websites.

    - Content Categorization
        - Content categorization is used to classify websites into predefined categories (e.g., social media, gambling, news, adult content). Policies can then be applied to allow, block, or limit access based on these categories.
    - Block Rules
        - Block rules prevent access to certain types of content or known bad sites though blacklisting specific URLs, IP addresses, or keywords.
    - Reputation
        - Reputation based filtering blocks websites based on their reputations– derived from historical data, threat intelligence, and user feedback.
- Operating System Security
    - Group Policy
        - Group policy provides a policy-based, centralized control of Windows devices, allowing for remote control over all computers' user permissions, security settings, password policies, and software installations.
    - SELinux
        - For Linux environments, SELinux enforces mandatory access controls (MAC), and can confines user programs and system services to the minimum required privileges.
- Implementation of Secure Protocols
    - Secure protocols protect data in transit and ensure secure communication.
    - Protocol Selection
        - Using secure protocols ensures CIA, non-repudiation, and availability in communications. For example, use HTTPS instead of HTTP for secure browser communication.



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

    - Port Selection
        - Using the ports associated with secure protocols avoids confusion and ensures compatibility. For example, HTTP uses port 80 while HTTPS uses port 443.
    - Transport Method
        - Using secure transport methods like VPNs for remote access or WPA3 for wireless access ensures that data is encrypted during transit.

- DNS Filtering
  - DNS filtering can monitor and block requests to malicious domains, allowing for enhanced content filtering.
- Email Security
  - Domain-based Message Authentication Reporting and Conformance (DMARC)
    - DMARC controls how your domain handles emails that fail SPF or DKIM checks, providing instructions to email servers on how to deal with unauthenticated emails. DMARC uses a TXT file stored in your DNS with a tag called ‘p’. Setting p=none alerts the inbox provider to take no action, p=quarantine alerts the provider to move the email to the spam folder, and setting p=reject alerts the provider to block the message entirely.
  - Domain Keys Identified Mail (DKIM)
    - DKIM is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain. It is designed to detect forged sender addresses in email, a technique often used in phishing and email spam. In essence, DKIM allows the receiver to check that an email that claimed to have come from a specific domain was authorized by the owner of that domain by matching the digital signature the email is signed with to the domain name the email was sent using.
  - Sender Policy Framework (SPF)
    - SPF is an email authentication protocol that helps verify the sender of an email and helps to identify the mail servers that are allowed to send email for a given domain. By using SPF, ISPs can identify email from spoofers, scammers and phishers as they try to send malicious email from a domain that belongs to a company or brand. In essence, SPF allows the receiver to check that an email was not sent using a forged sender address by ensuring the IP address the email was sent from is authorized by the domain owner.
  - Gateway
    - Secure email gateways act as a checkpoint for emails moving in and out of an organization, using filters to prevent spam or other attacks. Additionally, the gateway can prevent sensitive data from leaving an organization by automatically encrypting messages containing sensitive information.
- File Integrity Monitoring (FIM)
  - FIM involves tracking changes to files to ensure that unauthorized modifications do not occur, alerting administrators to any unauthorized changes that could indicate a security breach or malicious activity.

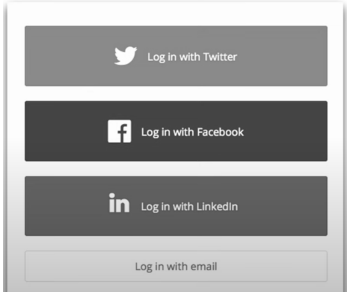
- Data Loss Prevention (DLP)
    - DLP helps protect sensitive information from leaving an organization by identifying and monitoring sensitive data and blocking, encrypting, or alerting administrators of intentional or unintentional transmission.
- Network Access Control (NAC)
    - NAC ensures only authorized and compliant devices have access to a network through authenticating, authorizing, and assessing the security posture of devices before granting network access. NAC allows for network segmentation and access controls based on user roles, device types, and security status.
- Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR)
    - EDR and XDR are advanced threat detection and response tools that protect endpoints from suspicious activities and have real-time threat detection. They have automated response capabilities such as isolating infected endpoints, blocking malicious activities, and remediating threats.
    - XDR extends EDR by integrating with other security tools and providing a holistic view of threats including networks, servers, and cloud services.
- User Behavior Analytics
    - User behavior analytics use machine learning and data analytics to detect unusual user activities. It establishes a baseline of normal user behavior patterns based on historical data and identifies deviations from the normal behavior, such as unusual login times, access to sensitive data, or large data transfers, which could indicate a security threat.

4.6 Given a scenario, implement and maintain identity and access management.

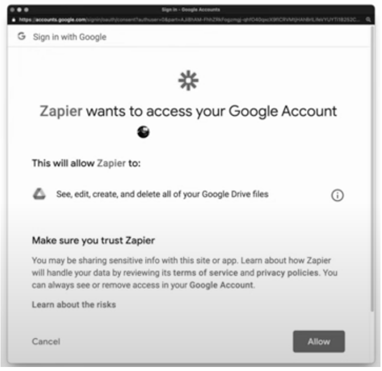
Identity Access Management (IAM):

- Provisioning/Deprovisioning User Accounts
    - Provisioning user accounts involves creating and configuring new user accounts, ensuring they have the appropriate access rights and permissions.
    - Deprovisioning involves removing or disabling accounts when they are no longer needed, which prevent unauthorized access.
- Permission Assignments and Implications
    - Permission assignments grant users rights to access systems, applications, or data based on their roles and responsibilities. Improper permission assignments can lead to data breaches, unauthorized access, and potential legal liabilities.
- Identity Proofing
    - Identity proofing, also known as identity verification, is the process of verifying that an individual is who they claim to be before granting them access to systems and resources. This involves checking identity documents, biometrics, or other credentials.

- Federation
    - Federation is the establishment of trusted relationships between organizations' IAM systems, allowing users to use their home organization's credentials to access external systems, implemented through protocols like SAML or OAuth.



- Single Sign-On (SSO)
    - SSO allows a user to log in to multiple applications using a single set of credentials. For example, your Google account allows you to access services like Gmail, Photos, Drive, etc, using the one login.
    - Lightweight Directory Access Protocol (LDAP)
        - LDAP is used to access and manage directory information over an IP network. LDAP provides a centralized repository for user credentials and access rights. For example, a user might log in to an application using their ID and password. The software sends this information to a security server, which logs into the LDAP server on the user's behalf with their ID and password. If successful, the security server can authorize the user and allow them to access the application.
    - Open authorization (OAuth)
        - OAuth allows a website or application to access resources hosted by other web apps on behalf of a user. OAuth is commonly used in SSO scenarios to grant access to user data across different applications without sharing passwords. For example, a web service might ask permission to add or modify files in your Google Drive account.



Zapier wants to access your Google Account

This will allow Zapier to:

See, edit, create, and delete all of your Google Drive files

Make sure you trust Zapier

You may be sharing sensitive info with this site or app. Learn about how Zapier will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

    - Security Assertions Markup Language (SAML)
        - SAML allows users to log into multiple applications with one set of credentials through authenticating a user once and then communicating that authentication to multiple applications. It is generally used as an authentication protocol for exchanging authentication and authorization between directories and web applications.
- Interoperability
    - Interoperability is the ability of different systems to work together and exchange information and services without compatibility issues, functioning together cohesively.
- Attestation
    - Attestation is the process of certifying a device is compliant with organizational policies and has the correct level of access rights.
- Access Controls
    - Mandatory
        - Mandatory Access Control (MAC) is a model where access rights are strictly regulated by a central authority based on levels of security. Users and resources are assigned classifications, such as “confidential,” and access rights are based on these classifications.
    - Discretionary
        - Discretionary Access Control (DAC) is a model that gives the owner of a resource full control over who can access the resource and what permissions they have.
    - Role-Based
        - Role-Based Access Control (RBAC) is a model that assigns permissions to users based on their role within an organization.
    - Rule-Based
        - Rule-Based Access Control (RBAC) is a model that uses specific organization or administrator rules to determine access permissions. These rules can be based on various conditions such as time of day, location, or type of resource.
    - Attribute-Based
        - Attribute-Based Access Control is a model where access permissions are granted based on the attributes of the user, such as user roles, resource type, or the current date and time.
    - Time-of-Day Restrictions
        - Time-of-Day Restrictions limit access to resources based on the time of day, during specified hours.

        - Least Privilege
            - The principle of least privilege encourages the apportionment of the most minimal amount of access necessary to individuals while ensuring they can still perform their functions.
    - Multi Factor Authentication (MFA)
        - MFA is a security mechanism that requires users to provide two or more forms of identification before accessing a system or application.
        - Implementations
            - Biometrics
                - Biometrics are unique physical characteristics like fingerprints or facial recognition, of which are difficult to replicate.
            - Hard/Soft Authentication Tokens
                - Authentication tokens are physical or virtual devices that generate one-time codes or tokens. Hard tokens are physical devices, while soft tokens are typically apps on smartphones.
            - Security Keys
                - Security keys are physical devices that connect to a computer or mobile device to authenticate a user.
        - Factors
            - Something you know
                - This factor involves information that only the user should know, such as a password or PIN.
            - Something you have
                - This factor refers to something physical that the user possesses, like a smartphone, smart card, or authentication token.
            - Something you are
                - This factor relates to biometric data unique to the user, such as fingerprints or facial features.
            - Somewhere you are
                - This factor considers the user's location or network environment, which can be used to verify their identity based on their typical patterns of access.
    - Password Concepts
        - Password Best Practices
            - Length
                - The longer the length of the password, the more secure.
            - Complexity
                - Complexity involves using a combination of uppercase and lowercase letters, numbers, and special characters in a password.

        - Reuse
            - Password reuse refers to using the same password across multiple accounts or systems, which can lead to multiple compromised accounts if any one account is breached.
        - Expiration
            - Password expiration requires users to change their passwords after a specified period to reduce the risk of old passwords being compromised.
        - Age
            - Password age refers to how long a password has been in use before it must be changed.
    - Password Managers
        - Password managers securely store and manage passwords for various accounts, eliminating the need for users to remember multiple passwords.
    - Passwordless
        - Passwordless authentication eliminates the need for passwords, relying on alternative methods such as biometrics, hardware tokens, or mobile-based authentication, reducing the risk of password-related attacks.
- Privileged Access Management Tools
    - Just-In-Time Permissions
        - Just-in-Time Permissions is a security practice that limits the time users have access to applications or systems to predetermined periods.
    - Password Vaulting
        - A password vault is a program that stores login credentials for multiple applications and users securely, and in an encrypted format. The vault controls who gets access to which credentials.
    - Ephemeral Credentials
        - Ephemeral Credentials are temporary tokens that give limited access to systems or resources for a set period of time. They are created when needed and then discarded, and they expire after a session, such as a just in time permission.

4.7 Explain the importance of automation and orchestration related to secure operations.

Background Knowledge:

- What is automation and orchestration?
    - Automation refers to the use of technology to perform tasks with minimal human intervention, while orchestration involves coordinating and managing automated tasks and workflows to achieve specific outcomes.

Automation And Orchestration Importance:

- Use Cases of Automation and Scripting
    - User Provisioning
        - Automation can automatically configure new user accounts, assigning roles, permissions, and access rights based on rules and policies.
    - Resource Provisioning
        - Automation can automatically allocate resources such as virtual machines, storage, and network configurations, along with deprovisioning them when no longer needed.
    - Guard Rails
        - Automation can automatically enforce security and compliance standards through guard rails, preventing actions by users that could lead to security vulnerabilities or compliance breaches.
    - Security Groups
        - Automation can dynamically manage security groups by automatically adding or removing users, adjusting permissions based on role changes, and applying access controls consistently across all systems.
    - Ticket Creation
        - Automation can automatically generate tickets for IT support, incidents, or service requests based on system alerts, user actions, or scheduled tasks.
    - Escalation
        - If automation cannot correct an issue itself, it can manage the escalation of issues by automatically forwarding unresolved tickets to higher-level support teams or triggering alerts to supervisors.
    - Enabling/Disabling Services and Access
        - Automation can enable or disable services and access rights based on user activity, roles, or specific conditions. For example, automation can automatically disable access for terminated employees.
    - Continuous Integration and Testing
        - Automation can automatically and continuously generate code builds, testing, and deployment processes, ensuring consistency and reliability.
    - Integrations and Application Programming Interfaces (APIs)
        - Automation can automatically integrate between different systems and applications using APIs, which enable data exchange and process automation across systems.
- Benefits
    - Efficiency/Time Saving
        - Automation reduces the need for employees to manually engage in repetitive tasks, such as patch management, saving time and energy.

  - Enforcing Baselines
    - Automation ensures that security baselines are applied across all systems, reducing the risk of human error and ensuring compliance.
  - Standard Infrastructure Configurations
    - Automation can automatically deploy infrastructure configurations, ensuring consistency and reducing the change of misconfigurations.
  - Scaling in a Secure Manner
    - Automation can automatically securely scale operations by configuring new applications and systems and manage the deployment of resources.
  - Employee Retention
    - By automating repetitive and mundane tasks, IT staff can focus on more challenging and rewarding work, improving job satisfaction and retention.
  - Reaction Time
    - Automation significantly improves the reaction time to security incidents through detection and response mechanisms that can identify and mitigate threats in real-time.
  - Workforce Multiplier
    - Automation acts as a multiplier for the workforce by automating routine tasks so the existing workforce can handle more significant workloads without compromising on quality or security.
- Other Considerations
  - Complexity
    - Automation can introduce complexity through the integration of various automated tools and orchestration platforms, and creating, without proper planning, convoluted systems that are difficult to manage.
  - Cost
    - Deploying automation and orchestration tools can be costly, including software licensing, hardware, and training, along with the ongoing costs of maintaining and updating systems.
  - Single Point of Failure
    - Relying heavily on automation and orchestration can create single points of failure if an automation tool or orchestration platform fails and disrupts processes and operations.
  - Technical Debt
    - Over time, the accumulation of outdated or poorly implemented automation scripts can lead to technical debt, or systems that take more time and money to understand and fix than to add upon and expand.

    - Ongoing Supportability
        - The long-term supportability of automation and orchestration solutions include the need for updates, patches, and vendor support, along with the availability of skilled personnel to manage and operate these systems.

4.8 Explain appropriate incident response activities.

Background Knowledge:

- What is an incident response?
    - Incident response is a structured and standardized approach for handling security incidents.

Incident Response Activities:

- Process
    - Preparation
        - Preparation is the process of establishing and maintaining incident response plans, including policies, procedures, and defining roles and responsibilities.
    - Detection
        - Detection is the process of identifying potential security incidents through monitoring systems for signs of suspicious activity or breaches.
    - Analysis
        - Analysis involves investigating incidents to understand their nature, scope, and impact– gathering information on the severity of the incident and the appropriate response.
    - Containment
        - Containment attempts limit the damage caused by an incident and prevent further compromise through isolating systems and stopping the spread of the incident.
    - Eradication
        - Eradication involves removing the cause of the incident and eliminating malicious code from the environment, ensuring the threat is eliminated.
    - Recovery
        - Recovery focuses on restoring affected systems and services to normal operations while ensuring that any lingering or exploited vulnerabilities are addressed to prevent recurrence.
    - Lessons Learned
        - Lessons learned focuses on the process of reviewing and analyzing the incident and the response to find improvements and strengthen the incident response plans.

- Training
    - Training involves educating employees and IT staff on security policies, procedures, and best practices so they are prepared for security incidents.
- Testing
    - Tabletop Exercise
        - Tabletop exercises are discussion-based, simulated walkthroughs of emergency scenarios to identify gaps and ensure understanding.
    - Simulation
        - Simulations are functional and realistic exercises done in a controlled environment to mimic the conditions of a disaster, providing a practical, hands-on way to test recovery plans, weaknesses, and staff.
- Root Cause Analysis
    - Root cause analysis attempts to identify the underlying causes of an incident to determine why it happened and how to prevent it from happening again.
- Threat Hunting
    - Threat hunting involves searching for threats before they can cause harm, using advanced techniques and tools to identify hidden or unknown threats.
- Digital Forensics
    - Legal Hold
        - A legal hold, also known as a litigation hold, is used to protect any documents relevant to a legal dispute from being altered or destroyed until they can be collected for review or until the matter is resolved.
    - Chain of Custody
        - A chain of custody is the “paper trail,” or recorded sequence, of custody over physical or electronic evidence to confirm the evidence remains admissible in court and that its integrity is preserved.
    - Acquisition
        - Acquisition is the process of collecting digital evidence in a manner that ensures it keeps its integrity and reliability.
    - Reporting
        - Reporting involves documenting the findings of a forensic investigation in a detailed and understandable manner to use for legal proceedings.
    - Preservation
        - Preservation refers to the process of maintaining and protecting digital evidence in its original state to ensure it is not altered or corrupted during the investigation.
    - E-Discovery
        - E-Discovery is the process of identifying, collecting, and producing electronic documents and information for legal cases or investigations.

4.9 Given a scenario, use data sources to support an investigation.

Data Sources:

- Log Data
    - Firewall Logs
        - Firewall logs track incoming and outgoing traffic that passes through a network, recording the source and destination IP addresses, ports, protocols, and action taken (allowed/blocked).
    - Application Logs
        - Application logs track the actions taken within specific applications, such as user activities, errors, and application-specific events.
    - Endpoint Logs
        - Endpoint logs capture specific events on end-user devices, such as system processes, user logins, file accesses, and security software actions.
    - OS-Specific Security Logs
        - OS-specific security logs are generated by operating systems and contain records of user authentication attempts, system changes, and access control events.
    - IPS/IDS Logs
        - IPS and IDS logs record detected security threats, suspicious activities, and potential intrusions or attacks on the network, including details about detected threats, signatures, and actions taken.
    - Network Logs
        - Network logs record data captured from network devices, such as traffic flow, connection attempts, and network performance metrics.
    - Metadata
        - Metadata provides additional context about files, emails, and other data objects, such as creation and modification dates, file size, and user ownership. It is not the content itself but information about the content.
- Data Sources
    - Vulnerability Scans
        - Vulnerability scans periodically scan the network to detect known vulnerabilities, misconfigurations, outdated software, and missing patches, helping identify weaknesses in an organization before they are exploited.
    - Automated Reports
        - Automated reports compile data from various security tools and systems, providing a summary of security events, alerts, and statuses.

- Dashboards
  - Dashboards provide real-time visualization of security data from multiple sources into an interactive interface, displaying performance indicators, threat alerts, and system statuses.
- Packet Captures
  - Packet captures are records of network traffic at the most baseline level, capturing the actual data transmitted over the network, providing information on network communications.

Important Acronyms in Unit 4:

AAA - Authentication, Authorization, Accounting
AES - Advanced Encryption Standard
API - Application Programming Interface
AUP - Acceptable Use Policy
AV - AntiVirus
BYOD - Bring Your Own Device
COPE - Corporate Owned, Personally Enabled
CSP - Cloud Service Provider
CSRF - Cross-Site Request Forgery
CVE - Common Vulnerabilities and Exposures
CVSS - Common Vulnerability Scoring System
CYOD - Choose Your Own Device
DAC - Discretionary Access Control
DKIM - DomainKeys Identified Mail
DLP - Data Loss Prevention
DMARC - Domain-based Message Authentication, Reporting, and Conformance
DNS - Domain Name Service
EAP - Extensible Authentication Protocol
EDR - Endpoint Detection and Response
FIM - File Integrity Monitoring
FTP - File Transfer Protocol
FTPS - File Transfer Protocol (Secure)
HTTP - HyperText Transfer Protocol
HTTPS - HyperText Transfer Protocol (Secure)
IAM - Identity and Access Management
ICS - Industrial Control Systems
IDS - Intrusion Detection System
IoT - Internet of Things
IPS - Intrusion Prevention System
IPSec - Internet Protocol Security
IMAP - Internet Message Access Protocol
LDAP - Lightweight Directory Access Protocol
MAC - Mandatory Access Control
MDM - Mobile Device Management
MFA - Multi Factor Authentication
NAC - Network Access Control

OAUTH - Open Authentication
OS - Operating System
OSINT - Open Source Intelligence
RADIUS - Remote Authentication Dial-In User Service
RBAC - Role-Based Access Control
RBAC - Rule-Based Access COntrol
RTOS - Real Time Operating System
SAE - Simultaneous Authentication of Equals
SAML - Security Assertion Markup Language
SCADA - Supervisory Control and Data Acquisition
SCAP - Security Content Automation Protocol
SELinux - Security-Enhanced Linux
SIEM - Security Information and Event Management
SNMP - Simple Network Management Protocol
SPF - Sender Policy Framework
SQL - Structured Query Language
SSH - Secure SHell
SSL - Secure Sockets Layer
SSO - Single Sign On
TLS - Transport Layer Security
URL - Universal Resource Locator
VPN - Virtual Private Network
WPA3 - Wi-Fi Protected Access 3
XDR - Extended Detection and Response
XML - eXtensible Markup Language
XXS - Cross-Site Scripting

Topic 5: Security Program Management and Oversight

5.1 Summarize elements of effective security governance

Security Governance Elements:

- Guidelines
    - Guidelines provide recommended practices for implementing security measures within an organization to help achieve compliance with policies and standards.
- Policies
    - Acceptable Use Policy (AUP)
        - The AUP defines acceptable and unacceptable behaviors when using organizational resources. It aims to protect both the organization and its employees by outlining rules and expectations.
    - Information Security Policies
        - Information security policies establish the framework for protecting an organization's information assets, including data protection, risk management, and compliance with legal and regulatory requirements.
    - Business Continuity
        - Business continuity policies ensure that critical business functions can continue during and after a disruption, involving planning and procedures for maintaining operations and minimizing downtime.
    - Disaster Recovery
        - Disaster recovery plans (DRP) focus on restoring IT systems and data after a catastrophic event, including plans for data backups, system restoration, and recovery procedures to resume operations.
    - Incident Response
        - Incident response policies provide a structured and standardized approach for handling security incidents, outlining roles, responsibilities, and procedures
    - Software Development Lifecycle (SDLC)
        - SDLC policies merge security with each phase of software development. They ensure that security considerations, vulnerabilities, and compliance requirements are addressed throughout the development process.
    - Change Management
        - Change management policies outline the process of making changes to IT systems and infrastructure, aiming to minimize the risks associated with making changes.

- Standards
    - Password
        - Password standards are requirements for creating and managing passwords, such as complexity, length, and expiration.
    - Access Control
        - Access control standards specify how access is granted and managed, such as with RBAC and least privilege principles.
    - Physical Security
        - Physical security standards outline measures to protect an organization's physical assets, such surveillance and environmental controls to prevent unauthorized access and damage.
    - Encryption
        - Encryption standards define the methods for encrypting data to protect its confidentiality and integrity, including encryption algorithms, key management practices, and usage scenarios.
- Procedures
    - Change Management
        - Change management procedures involve steps to plan, test, implement, and review changes, ensuring changes are made in a controlled manner to minimize disruptions.
    - Onboarding/Offboarding
        - Onboarding procedures ensure new employees are given appropriate access and security training. Offboarding procedures ensure departing employees have their access revoked and company assets are returned.
    - Playbooks
        - Playbooks are detailed, step-by-step instructions that outline the specific actions to take during various security incidents to ensure consistent and effective responses to threats and breaches.
- External Considerations
    - Regulatory
        - Regulatory considerations involve complying with laws and regulations relevant to data protection and privacy, such as GDPR or HIPAA. Organizations must ensure their security practices meet these regulatory requirements to avoid penalties and legal issues.
    - Legal
        - Legal considerations involve complying with the legal obligations of security practices, including data breaches and liability issues to protect against legal action and ensure lawful handling of data.

  - Industry
    - Industry considerations involve complying with the best practices and standards specific to the organization's industry, including adhering to industry-specific regulations and adopting industry-recognized security frameworks.
  - Local/Regional
    - Local/regional considerations require organizations to comply with security laws and regulations specific to their geographic location, ensuring that security practices align with local legal requirements.
  - National
    - National considerations include complying with the country’s national policies, governmental directives, cybersecurity laws, regulations, and standards.
  - Global
    - Global considerations involve managing security practices across international borders, addressing diverse regulations, standards, and threats.
- Monitoring and Revision
  - Monitoring and revision is the continuous tracking of the effectiveness of security measures, making the appropriate adjustments when revision is necessary. This process includes audits, vulnerability assessments, and updating policies to adapt to threats and compliance requirements.
- Types of Governance Structures
  - Boards
    - Boards, such as boards of directors, provide strategic oversight and direction for an organization's security governance, ensuring that security policies align with business objectives, allocating resources, and monitoring overall compliance and risk management efforts.
  - Committees
    - Committees, such as security or risk committees, are specialized groups within an organization that focus on specific parts of security governance. Their responsibilities involve developing policies, overseeing implementation, and improving security practices.
  - Government Entities
    - Government entities set regulatory standards and compliance requirements for organizations, providing guidance, support, and enforcement mechanisms to ensure adherence to security regulations and laws.

        - Centralized/Decentralized
            - Centralized governance structures have consolidated security, decision-making, and control within a single entity or team.
            - Decentralized structures distribute security responsibilities across various departments or locations, for more tailored approaches.
    - Roles and Responsibilities for Systems and Data
        - Owners
            - Owners are individuals or entities responsible for the overall management and protection of specific assets. They are responsible for access policies, classifying data, and ensuring compliance with regulations and policies.
        - Controllers
            - Controllers determine the purposes and means of processing personal data. They are responsible for ensuring that data processing activities comply with legal requirements and for implementing appropriate security measures to protect data.
        - Processors
            - Processors handle and process data on behalf of controllers. They follow the controller's instructions, maintain data security, and ensure data processing activities comply with legal and contractual obligations.
        - Custodians/Stewards
            - Custodians or stewards manage the day-to-day maintenance and protection of data. They implement and enforce security measures, manage access controls, and ensure data integrity and availability according to the policies set by data owners.

5.2 Explain elements of the risk management process.

Elements of Risk Management:

- Risk Identification
    - Risk identification involves recognizing potential threats that could impact an organization's assets, operations, or objectives.
- Risk Assessment
    - Ad hoc
        - Ad hoc risk assessments are conducted on an as-needed basis, often in response to specific incidents or emerging threats. These are not part of a regular schedule, instead they are performed when a situation emerges that demands immediate attention.

  - Recurring
    - Recurring risk assessments are performed at regular intervals, such as quarterly or annually, to ensure ongoing identification and evaluation of risks to help maintain an up-to-date awareness of potential threats and vulnerabilities.
  - One-Time
    - One-time risk assessments are conducted for a specific project, event, or change in operations. Once completed, these assessments provide a snapshot of the risks associated with that particular instance.
  - Continuous
    - Continuous risk assessments involve ongoing monitoring and evaluation of risks in real-time to quickly identify and respond to new or changing threats.
- Risk Analysis
  - Qualitative
    - Qualitative risk analysis evaluates risks based on their characteristics and impacts, using descriptive terms like high, medium, or low, without using numerical values.
  - Quantitative
    - Quantitative risk analysis involves numerical measurements of risk, using data and statistical methods to calculate precise assessments of risks in financial terms.
  - Single Loss Expectancy (SLE)
    - Single Loss Expectancy (SLE) calculates the expected monetary loss each time a risk event occurs. It is determined by multiplying the asset value by the exposure factor (percentage of loss).
  - Annualized Loss Expectancy (ALE)
    - Annualized Loss Expectancy (ALE) estimates the yearly financial impact of a risk. It is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO).
  - Annualized Rate of Occurrence (ARO)
    - The Annualized Rate of Occurrence (ARO) represents the expected frequency of a risk event occurring within a year. It helps quantify how often a specific risk is likely to happen annually.
  - Probability
    - Probability assesses the likelihood that a risk event will occur. It provides a measure of how probable it is for a particular threat to exploit a vulnerability.

  - Likelihood
    - Likelihood indicates the chance of a risk event occurring, considering factors like threat capability, vulnerability presence, and existing controls.
  - Exposure Factor
    - The exposure factor is the percentage of an asset's value that is lost when a risk event occurs. It helps determine the potential impact of a risk event on the asset.
  - Impact
    - Impact refers to the consequences or effects of a risk event, typically measured in terms of financial loss, operational disruption, or damage to reputation. It helps gauge the severity of a risk in material terms.
- Risk Register
  - A risk register is a documented record of risks, including details about their nature, assessment, and management. It is a central repository for tracking risks and their mitigation strategies.
  - Key Risk Indicators
    - Key Risk Indicators are metrics used to measure and monitor the likelihood and impact of risks, providing early warning signs of increasing risk exposure, and helping organizations take proactive measures.
  - Risk Owners
    - Risk owners are individuals or entities responsible for managing a specific risk. They implement the risk mitigation strategies and monitor the risk to ensure it remains within acceptable levels.
  - Risk Threshold
    - The risk threshold is the level of risk an organization is willing to accept before action is required. It is the clear boundary between acceptable and unacceptable risk, helping guide in decision-making and risk management.
- Risk Tolerance
  - Risk tolerance is the amount of risk an organization is willing to take on while pursuing its objectives. It reflects the organization's capacity to withstand losses or adverse outcomes without jeopardizing its operations or goals.
  - For example, police officers will tolerate you going a certain speed above the speed limit. However, these tolerances can change depending on the weather, road conditions, and traffic. How far can I deviate from the risk appetite?

- Risk Appetite
    - Risk appetite is the overall level of risk an organization is prepared to accept to achieve its strategic objectives. It defines the organization's approach to risk-taking and influences decision-making across various activities.
    - For example, the government sets a specific speed limit that they determine is an acceptable balance between safety and convenience. How much risk can I intake (my appetite) before I must take action to reduce that risk?
    - Expansionary
        - An expansionary risk appetite is a willingness to take on higher risks to achieve significant growth or aggressive strategic goals, prioritizing opportunities and potential high rewards over safety.
    - Conservative
        - A conservative risk appetite is a preference for minimizing risks, focusing on stability and the preservation of existing assets, prioritizing risk avoidance and careful risk management.
    - Neutral
        - A neutral risk appetite is a balance between expansionary and conservative, where an organization will accept moderate risks that align with the organization's strategic objectives without exposing themselves to excessive risk.
- Risk Management Strategies
    - Transfer
        - Risk transfer involves shifting the risk to a third party, such as through insurance or outsourcing. This strategy reduces the organization’s exposure factor or potential monetary loss of the risk by having a third party assume responsibility for it.
    - Accept
        - Exemption
            - Exemption is a situation where a specific risk is formally recognized and accepted, intentionally left unmitigated based on some justified decision.
        - Exception
            - Exception is the temporary or permanent acceptance of a risk that would otherwise deviate from standard policies or controls.
    - Avoid
        - Risk avoidance involves taking actions to eliminate a risk entirely, such as discontinuing certain activities or altering processes. This strategy is used when a risk is deemed to have too severe of an impact and cannot be mitigated or transferred.

    - Mitigate
        - Risk mitigation involves implementing measures to reduce the likelihood or impact of a risk, including controls, processes, or technologies designed to manage the risk within acceptable levels.
- Risk Reporting
    - Risk reporting involves regularly communicating information about risk status, assessments, and management efforts to stakeholders. This ensures that decision-makers are informed about current risks and the effectiveness of mitigation strategies.
- Business Impact Analysis (BIA)
    - A BIA evaluates the potential effects of disruptions to critical business operations, prioritizing recovery efforts and resources based on the impact of different scenarios.
    - Recovery Time Objective (RTO)
        - Recovery Time Objective (RTO) is the maximum acceptable amount of time to restore a business function or system after a disruption. It defines the target timeframe for resuming normal operations to minimize impact.
    - Recovery Point Objective (RPO)
        - Recovery Point Objective (RPO) is the maximum acceptable amount of data loss measured in time. It defines the point in time to which data must be recovered to resume operations, indicating the tolerance for data loss.
    - Mean Time To Repair (MTTR)
        - Mean Time to Repair (MTTR) is the average time required to repair a system or component and restore it to full functionality. It measures the efficiency and effectiveness of the repair process.
    - Mean Time Between Failures (MTBF)
        - Mean Time Between Failures (MTBF) is the average time between successive failures of a system or component. It provides an indication of the reliability and expected lifespan of the system or component.

5.3 Explain the processes associated with third-party risk assessment and management.

Third-Party Processes:

- Vendor Assessment
    - Penetration Testing
        - Penetration testing involves actively testing and probing a system in an attempt to find and exploit vulnerabilities to provide a comprehensive assessment of the organization’s security posture. It helps assess a vendor’s security posture and their ability to protect sensitive data.

  - Right-to-Audit Clause
    - A right-to-audit clause grants an organization the authority to conduct audits of a vendor’s security controls and practices, ensuring transparency and compliance with agreed-upon security standards.
  - Evidence of Internal Audits
    - Requiring vendors to provide evidence of their internal audits ensures they regularly review and improve their own security measures, demonstrating both organizations’ commitment to maintaining strong security practices.
  - Independent Assessments
    - Independent assessments are evaluations conducted by third-parties to verify a vendor’s security controls and compliance, providing an unbiased review of the vendor’s security posture and risk management practices.
  - Supply Chain Analysis
    - Supply chain analysis involves assessing the security risks associated with a vendor’s supply chain, ensuring that all parties involved with delivering products or services adhere to appropriate security standards.
- Vendor Selection
  - Due Diligence
    - Due diligence and care involves conducting thorough and ongoing assessments of a vendor’s security policies and procedures to identify potential risks with a vendor. This includes reviewing their financial stability, reputation, security practices, and compliance with legal and regulatory requirements.
  - Conflict of Interest
    - Conflicts of interest are personal or financial interests that could compromise the objectivity of the vendor selection process.
- Agreement Types
  - Service-Level Agreement (SLA)
    - A Service-Level Agreement (SLA) is a contract that specifies the expected level and quality of service that is to be provided between a vendor and a client. It outlines metrics for performance, response times, uptime, and the penalties for failing to meet these standards.
  - Memorandum of Agreement (MOA)
    - A Memorandum of Agreement (MOA) is a formally agreed upon document that outlines the terms of an agreement between two or more parties. It specifies the responsibilities, objectives, and commitments of each party involved.

    - Memorandum of Understanding (MOU)
        - A Memorandum of Understanding (MOU) is a non-binding agreement that expresses the intention of two parties to cooperate. It outlines the general terms and conditions of a partnership and serves as a preliminary understanding between groups before a formal contract is established.
    - Master Service Agreement (MSA)
        - A Master Service Agreement (MSA) is a detailed contract that establishes the general terms and conditions for future transactions between parties, simplifying future agreements by providing a foundational framework for continuing services.
    - Work order (WO)/Statement of Work (SOW)
        - A Work Order (WO) or Statement of Work (SOW) is a detailed document that defines specific tasks, deliverables, timelines, and costs for a particular project or service and operates under the terms of a MSA or other agreement.
    - Non-Disclosure Agreement (NDA)
        - A Non-Disclosure Agreement (NDA) is a legal contract that protects confidential information that is shared between parties. It ensures that sensitive information is not disclosed to unauthorized individuals.
    - Business Partners Agreement (BPA)
        - A Business Partners Agreement (BPA) outlines the terms and conditions of a partnership between businesses. It includes details about roles, responsibilities, revenue sharing, and conflict resolution mechanisms.
- Vendor Monitoring
    - Vendor monitoring involves the ongoing evaluation of a vendor's performance and compliance with contractual obligations. This ensures the vendor maintains the required service levels and adheres to security and regulatory standards.
- Questionnaires
    - Questionnaires are used to collect information from vendors about their security practices, compliance, and risk management processes. They are used to assess the vendor's ability to meet the organization's requirements.
- Rules of Engagement
    - Rules of Engagement are the protocols and boundaries for interactions between the organization and vendors. They detail acceptable behavior, communication channels, and escalation procedures during collaboration.

5.4 Summarize elements of effective security compliance.

Security Compliance Elements:

- Compliance Reporting
    - Internal
        - Internal compliance reporting involves documenting and communicating the organization’s adherence to security policies, standards, and procedures within the organization.
    - External
        - External compliance reporting involves providing compliance information to external entities such as regulatory bodies, customers, and partners.
- Consequences of Non-Compliance
    - Fines
        - Fines are monetary penalties imposed for failing to comply with legal or regulatory requirements.
    - Sanctions
        - Sanctions are measures taken against an organization for non-compliance, including restrictions on business activities or operations that can severely limit an organization’s ability to function.
    - Reputational Damage
        - Reputational damage occurs when non-compliance harms an organization’s public image, leading to loss of trust and credibility.
    - Loss of License
        - Loss of license involves revoking certifications or licenses required due to non-compliance, halting license-specific operations.
    - Contractual Impacts
        - Contractual impacts refer to the negative consequences on existing business agreements, such as breaches of contract, loss of business, or termination of agreements due to non-compliance.
- Compliance Monitoring
    - Due Diligence/Care
        - Due diligence and care involves conducting thorough and ongoing assessments of security policies and procedures to identify and mitigate potential risks before they become security incidents.
    - Attestation and Acknowledgement
        - Attestation and acknowledgement require employees to formally confirm their understanding of security policies and compliance requirements to ensure everyone is aware of their responsibilities.

        - Internal and External
            - **Internal** compliance monitoring involves audits and reviews within the organization to verify compliance with internal policies and procedures.
            - **External** compliance monitoring involves reviews and audits conducted by third parties or regulatory bodies to verify compliance with external standards and regulations.
        - Automation
            - Automation in compliance monitoring allows for the continuous tracking and enforcement of compliance requirements. Automated tools reduce human error and provide real-time alerts.
    - Privacy
        - Legal Implications
            - Local/Regional
                - Local and regional legal implications involve complying with data protection laws specific to a particular area or region.
            - National
                - National legal implications involve complying with country-wide data protection regulations, such as GDPR in the European Union or CCPA in California.
            - Global
                - Global legal implications involve complying with data protection laws across multiple countries and jurisdictions.
        - Data Subject
            - A data subject is an individual whose personal data is collected, processed, and stored by an organization.
        - Controller vs. Processor
            - A controller determines why and how personal data is processed and is responsible for complying with data protection laws.
            - A processor handles data on behalf of the controller, following the controller’s instructions.
        - Ownership
            - Data ownership involves defining who owns the data and who has the authority to access, modify, and share it.
        - Data Inventory and Retention
            - Data inventory involves cataloging all personal data, including its sources, uses, and storage locations. Retention policies define how long data should legally be kept and ensure it is securely disposed when no longer needed.

  - Right to be Forgotten
    - The right to be forgotten allows users to request for the personal data to be deleted immediately or when it is no longer necessary for the purpose of why it was collected.

5.5 Explain types and purposes of audits and assessments.

Types & Purposes of Audits & Assessments:

- Attestation
  - Attestation is a formal declaration by an independent auditor that an organization adheres to the expected standards.
- Internal
  - Compliance
    - Compliance audits assess whether an organization adheres to internal policies, procedures, and external regulations, helping identify areas of non-compliance.
  - Audit Committee
    - An audit committee is a group within the organization that is responsible for overseeing the internal audit process and addressing the findings in order to maintain accountability and transparency.
  - Self-Assessments
    - Self-assessments involve internal reviews conducted by employees to evaluate their compliance with policies and procedures
- External
  - Regulatory
    - Regulatory audits are conducted by government agencies or regulatory bodies to ensure an organization complies with laws and regulations to protect the public and maintain industry standards.
  - Examinations
    - Examinations are thorough evaluations performed by external auditors to assess specific elements of an organization, providing an in-depth analysis of risks and improvement areas.
  - Assessment
    - External assessments involve evaluations by third parties to measure an organization’s compliance against established criteria, providing an unbiased view that helps validate internal processes and controls.
  - Independent Third-Party Audit
    - An independent third-party audit is conducted by an external auditor, providing an objective evaluation of an organization.

- Penetration Testing
    - Physical
        - Physical pen testing involves attempting to breach physical security controls to access a facility or sensitive areas.
    - Offensive
        - Offensive pen testing, also known as red teaming, focuses on actively seeking and exploiting vulnerabilities in systems and networks to identify weaknesses that could be exploited by attackers.
    - Defensive
        - Defensive pen testing, also known as blue teaming, involves testing an organization's defensive measures and incident response capabilities.
    - Integrated
        - Integrated pen testing, known as purple teaming, combines offensive and defensive approaches to provide a comprehensive assessment of an organization's security posture where vulnerabilities and defensive capabilities are evaluated.
    - Known Environment
        - In a known environment (or white-box) penetration test, the testers have full knowledge of the system, allowing for a thorough assessment of security controls.
    - Partially Known Environment
        - In a partially known environment (or gray-box) penetration test, the testers have limited knowledge of the system, simulating an attack from an internal employee or a privileged attacker..
    - Unknown Environment
        - In an unknown environment (or black-box) penetration test, the testers have no prior knowledge of the system, simulating an attack from someone with no insider information.
    - Reconnaissance
        - Passive
            - Passive reconnaissance involves collecting information without directly interacting with the target, including searching OSINT.
        - Active
            - Active reconnaissance involves directly interacting with the target system to gather information about it, such as scanning ports, sending queries, or probing the network.

5.6 Given a scenario, implement security awareness practices.

Security Awareness Practices:

- Phishing
    - Campaigns
        - Regularly conduct simulated phishing campaigns to test employees ability to recognize phishing emails and to reinforce training, offering additional training if needed.
    - Recognizing a Phishing Attempt
        - Educate employees on identifying phishing indicators such as suspicious sender addresses, unexpected attachments, and urgent requests for personal information.
    - Responding to Reported Suspicious Messages
        - Protocols for employees to report suspicious messages should be clear and easily accessible. The IT team should promptly respond to reports.
- Anomalous Behavior Recognition
    - Risky
        - Train employees to recognize and report risky behavior that could indicate a security threat, such as accessing data without proper authorization.
    - Unexpected
        - Implement systems to detect and alert IT staff about unexpected behaviors, such as unusual login locations or times..
    - Unintentional
        - Educate employees on common unintentional behaviors that pose security risks, like sending confidential information to the wrong recipient.
- User Guidance and Training
    - Policy/Handbooks
        - Policy handbooks outline security protocols, including AUPs, data protection guidelines, and IRPs. Ensure all employees read and understand these policies.
    - Situational Awareness
        - Situal awareness includes instructing employees to be aware of suspicious emails, unusual device behaviors, and physical security measures, such as ensuring laptops are not left unattended in public places.
    - Insider Threat
        - The dangers of insider threats, both malicious and accidental, should be presented to employees, including how to recognize suspicious activities and how to discreetly report the concerns.

    - Password Management
        - Strong password management and policies should be implemented and training on using password managers and complex passwords should be provided to employees.
    - Removable Media and Cables
        - Removable media and cables should be company-approved and all external devices should be scanned for malware before use. Employees should be informed of the risks associated with using removable media and connecting unknown cables to their devices.
    - Social Engineering
        - Social engineering training sessions involve teaching employees how to recognize and avoid attacks such as pretexting, baiting, and tailgating.
    - Operational Security
        - Operational security includes teaching employees to not discuss sensitive information in public, encrypting communications, and securely disposing of confidential documents.
    - Hybrid/Remote Work Environments
        - Hybrid/remote work environments require specific training on securing home networks, using VPNs, and protecting data outside the office.
- Reporting and Monitoring
    - Initial
        - An initial security assessment creates a baseline of logging, network activities, and incident reporting protocols. Ensure new employees are trained on how to report security incidents.
    - Recurring
        - Recurring security training sessions, simulated attack exercises, and system reviews keep security measures and employees up to date. Conduct audits regularly and continuously monitor systems to detect security vulnerabilities.
- Development
    - Develop security policies and procedures based on best practices and industry standard, including creating IRPs, security protocols, and improving the security posture through monitoring and incident reports.
- Execution
    - Executing the security measures involves enforcing policies, responding to reported incidents, and applying updates and patches regularly. Monitor threats, analyze security data, and take action to mitigate risks. Regularly test IRPs.

Important Acronyms in Unit 5:

ALE - Annualized Loss Expectancy
ARO - Annualized Rate of Occurrence
AUP - Acceptable Use Policy
BIA - Business Impact Analysis
BPA - Business Partners Agreement
DRP - Disaster Recovery Plan
MFA - Multi-Factor Authentication
MOA - Memorandum of Agreement
MOU - Memorandum of Understanding
MSA - Master Service Agreement
MTBF - Mean Time Between Failures
MTTR - Mean Time To Repair
NDA - Non-Disclosure Agreement
RPO - Recovery Point Objective
RTO - Recovery Time Objective
SDLC - Software Development LifeCycle
SLA - Service Level Agreement
SLE - Single Loss Expectancy
SOW - Statement of Work
USB - Universal Service Bus
WO - Work Order

Additional Information:

Common Ports:

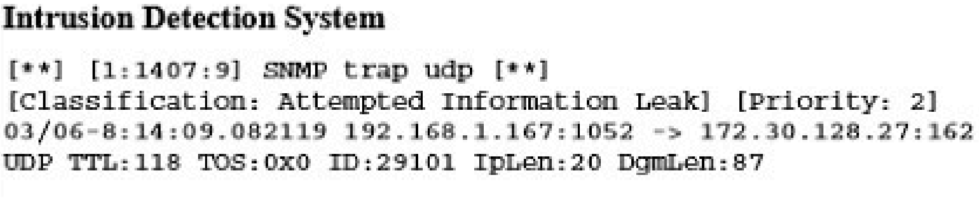
Port	Function	TCP/UDP	Port	Function	TCP/UDP
20	FTP (data)	TCP	161	SNMP	UDP
21	FTP (control)	TCP	389	LDAP	TCP
22	SSH	TCP	443	HTTPS	TCP
23	Telenet	TCP	636	LDAPS	TCP
25	SMTP	TCP	989	FTPS	TCP
53	DNS	TCP/UDP	993	IMAPS	TCP
80	HTTP	TCP	995	POP3	TCP
110	POP	TCP	1812	RADIUS	UDP
143	IMAP	TCP	3389	RDP	TCP

Configure a Firewall:

1. Block HTTP between 10.1.1.2 and 10.2.1.20.
2. Allow 10.2.1.33 to transfer files over HTTPS to 10.1.1.7
3. Allow 10.2.1.47 to use a secure terminal on 10.1.1.3

Source IP	Destination IP	Protocol	Port #	Allow/Block
10.1.1.2	10.2.1.20	TCP	80	Block
10.2.1.33	10.1.1.7	TCP	443	Allow
10.2.1.47	10.1.1.3	TCP	22	Allow

Read a Log:



Intrusion Detection System

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

This log indicates that the IDS detected a UDP packet associated with an SNMP trap, which might be part of an attempted information leak. The source IP address and port is 192.168.1.167:1052 and the destination IP address and port is 172.30.128.27:162.

Common Protocols:

HTTP: Defines how data should be formatted and transmitted between a client and a web server.
TCP: A reliable, connection-oriented protocol that ensures data is delivered correctly between applications.
IP: Delivers packets from the source host to the destination host based on their IP addresses.
UDP: A connectionless communication protocol used for fast and efficient data transmission with no error checking or guaranteed delivery.
DNS: Translates human-readable domain names into corresponding IP addresses.
FTP: A standard network protocol used for transferring files from one host to another.
SMTP: The standard protocol for sending email messages across a network.
TLS: Provides secure communication over the internet between the client and the server.
SSL: Encrypts data sent between a website and a browser.
SSH: Allows users to securely access a computer over an unsecured network.
IMAP: Allows users to access their email from multiple devices.
IPsec: Authenticates and encrypts each IP packet in a data stream.
POP: Allows users to request new messages from the email server.
LDAP: Stores and authenticates information about users and computers within a network
Telenet: Allows users to virtually access a computer, providing a two-way text-based communication channel.
SNMP: Manages and monitors network-connected devices in Internet Protocol networks.
RADIUS: Authenticated and authorized users who access a remote network.
RDP: Allows users to use a desktop computer remotely.

Cryptographic Algorithms:

Hashing:

- MD5
    - One of the first popular hashing algorithms, considered secure when it was developed. Now easily decoded and unsafe for use.
- SHA
    - A family of hash functions. SHA-256 is now the most commonly used hashing algorithm, resulting in a 256-bit hash value from an input message of any length.

Symmetric:

- DES
    - The Data Encryption Standard is a block cipher that encrypts data in 64-bit blocks. Its short key length makes it too insecure for modern applications.
- AES
    - The Advanced Encryption Standard is the most common symmetric encryption algorithm used. It was created as a replacement for DES. AES is a block cipher that commonly uses 128-bit blocks.

Asymmetric:

- RSA
    - RSA uses the factorization of the product of two prime numbers to deliver encryption of 1024-bits and up to 2048-bit key length. The length of keys make encryption and decryption incredibly slow, but the level of security is extremely high.
- Diffie-Hellman
    - Diffie-Hellman is a way of generating a shared secret between two people so that the secret can’t be seen by observing the communication. Parties are not sharing information during the key exchange, they are creating a key together mathematically. Diffie-Hellman needs to be very cautiously implemented to be secure on its own; however, it provides the basis for a variety of other, authenticated protocols.
- Elliptic Curve Cryptography
    - ECC uses a mathematical operation based on elliptic curves on a finite field, called the “Elliptic-Curve Diffie–Hellman”. The private keys created are nearly impossible to crack, as the math involved is extremely difficult to reverse. It provides fast encryption speeds along with comparable security to RSA.

Additional Resources:

CompTIA Security+ Exam SY0-701 Objectives: Objectives
CompTIA Exam Accommodation Requests: PersonVUE
CompTIA Student Discount Store: CompTIA Store
Free Exam Objective Video Series: Professor Messer, Exam Cram Series
Free Security+ Labs: 101Labs
Free Exam Practice Questions: Crucial Exams, Andrew Ramdayal, Exam Compass, Cyber James
Performance-Based Questions: InfoSec
Monthly Study Groups: Professor Messer
Cyber Security Roadmap: Roadmap