COMPTIA SECURITY+

Security Goals and Controls

Overview
- Confidentiality, integrity, availability and non-repudiation
- Authentication, authorization and accounting (AAA)
- Control Types

CIA Triad
- Stands for confidentiality, availability and integrity

Confidentiality
- Measures an attacker's ability to get unauthorized access to data or information from an application or system
- Involves using techniques, cryptography, to allow only approved subjects with the ability to view information
- Includes preserving authorized restrictions on information access and disclosure (data in transit, data at rest, data in use)

Confidentiality
- Means for protecting personal privacy and proprietary information
- Confidential information can include passwords, cryptographic keys, personally identifiable information (PII), personal health information (PHI), intellectual property (IP), or other sensitive information.
- Examples of confidentiality:
    - Using an IPsec virtual private network (VPN)
    - Leveraging mutual transport layer security (TLS) between a web browser and web server or controller
    - Storing sensitive data or credentials in a Mobile device partition or secure enclave
    - Implementing AES encryption on data at rest in storage (file, block, object, databases, etc.)

Integrity
- Involves safeguarding against improper information modification or destruction
- It is a property that data or information have not been altered or damaged in an unauthorized way
- Integrity is the quality of an IT system that reflects
    - The logical correctness and reliability of the operating system
    - The logical completeness of the hardware and software that implements the protection mechanisms
    - The consistency of the data structures and occurrence of the stored data
- Examples of Integrity
    - An operating system performs a mathematical checksum when a file is moved or copied from one volume to another
    - A frame check sequence conducted on a Ethernet frame when sent from one MAC address to another
    - A hashed message authentication code applied to advertisements sent between neighbor systems such as routers or gateways
    - Implementing a mandatory access model technique such as Biba or Clark-Wilson

Availability

- Process of ensuring timely and reliable access to and use of information
- Property of data, information applications, systems, or services that are accessible and usable upon demand by an authorized subject
- "High availability" is a failover feature to ensure availability during device or component interruptions both, planned and unplanned.
- Examples of Availability
    - Implementing security controls that protect systems and services from spoofing, flooding, denial-of-service (DDoS), poisoning, and other attacks that negatively affect the ability to deliver data, content, or services
        - Vulnerability that impact availability can affect hardware, software, and network resources, such as flooding network bandwidth, consuming large amounts of memory, CPU cycles, or unnecessary power consumption
    - Assuming that technical controls such as firewalls, IPS sensors, anti-virus and endpoint protection are always reliable and deployed in a failover group or cluster
    - Determining the best disaster recovery site solution for every scenario or situation for an organization.

Non-Repudiation

- Opposite of repudiation
- Enforcing the inability of a subject or a principle to deny that they participated in a digital transaction, agreement, contract, or communication such as an email
- Critical in world wide web when transactions were carried out
- Non-repudiation is the property of agreeing to adhere to an obligation and not repudiating that at a later data
- The inability to refute responsibility
- For example, if you take a pen and sign a legal contract, your signature is a non-repudiation device
- In IT, non-repudiation is usually accomplished with a public/private key pair cryptosystem and digitally signed certificates between the sending and receiving parties. This happens all the time when you use your web browser on the internet

Repudiation of origin

- Sender cannot say they did not send that transfer, because their private key was used to sign the cryptographic hash of the transaction and only they have their cryptographic hash.

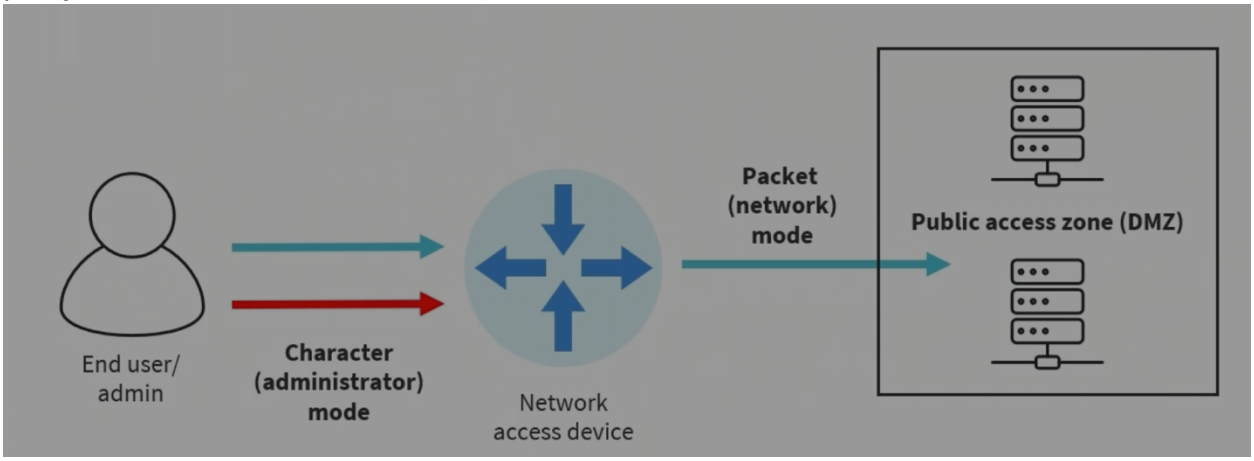
Authentication, Authorization and Accounting (AAA)

- If you want to verify when certain subjects like users, application and systems access resource objects that is called AAA.
- Authentication is the process of validating that an entity (user, application, or system) is who or what they claim to be. Fundamentally we call that origin authentication
- Authorization is the process of granting an authenticated entity permission to access a resource or perform a specific function
- Accounting is basically, when did the entity begin, when did it end, and how long did they do it

Character Mode vs Packet Mode

- When looking at AAA services it's important to know the difference between character mode and packet mode

- Character Mode sends keystrokes and commands (characters) to a network admission device (perimeter router, server, firewall) for the purpose of configuration or administration on that same device
- Packet (or network) mode occurs when the network admission device serves as an authentication proxy on behalf of services of services in other networks, VLANS, FTP servers, DNS servers.



- The end user wants to get a webpage from a web server from the public access zone. The network access device (perimeter router/firewall) will do packet mode AAA. They will receive the packet, perform authentication, authorization, accounting (locally) or send it back to authentication server. Once authenticated and authorized, they send the packet to the zone, vlan or network. If the end user is an admin and wants to manage the network access device e.g. reconfigure, then the AAA service will use character or admin mode.

Authentication

- Authenticating subjects is technically mandatory, even if using open or anonymous techniques. For example, open authentication, anonymous FTP.
- Historically, clients would initiate a TCP three-way communication handshake before the authentication process
- This is now considered sub-optimal and a violation of zero trust principles. In that the authentication authorization that occurs first before connection is set up.

Authorization

- Authorization is technically optional for authenticated entities and is mandatory from a practical policy standpoint
- In modern security deployments, it is desirable to implement session-based (tokens) and robust attribute-based authorization mechanisms.

Accounting

- Accounting is generally implemented for two use cases:
    - Monitoring, visibility, and reporting
    - Billing, chargeback, and reporting
- RADIUS is one of the most popular IETF-based AAA services, and it is known for exceptional accounting capabilities.
- DIAMETER is the next generation of RADIUS

Authenticating People

- Authenticating a person entity means confirming that they are who they claim to be. Associated with identity

- This confirms only those with authorized credentials gain access to secure systems
- Usernames/webmail/email and a password is still the most common factor for authenticating people
- There should always be another robust factor added to a simple credential today

Common ways to authenticate people
- Password, pin, passphrase they know (memorized not written)
- Smart card token or fob that they possess
- A digital certificate they present
- Biometric attribute
- QR code they present on a device

Authenticating Devices and Systems
- There are many different types of entities or principals that can be authenticated other than people
- These subjects are often called non-person entities (NPEs)
    - Laptops and pads
    - Mobile devices
    - Gateways and load balances
    - IoT Devices

Endpoint Authentication
- Endpoint (or device) authentication is a security technique designed to ensure that only authorized devices can connect to a given network, site, or service
- Endpoint security management is rapidly emerging as an important area in machine-to-machine (M2M) communications and the Internet of Things (IoT)
- Endpoint fingerprinting is one way to enable authentication of non-traditional network endpoints such as smart card readers, HVAC systems, medical equipment, and IP-enabled door locks

Common Device (Endpoint) Authentication Methods
- A shared secret key stored on the endpoints (wireless) or infrastructure devices
- An X.509 v3 device certificate stored in a software application
- A cryptographic key, certificate, or other credential stored at the hardware level in a trusted platform module
- A key stored in a hardware security module (HSM)
- A protected access file (PAC) in a Cisco infrastructure

Authorization Models: DAC
- Discretionary access control (DAC): DAC grants access control decisions to the resource owners and custodians
- Each resource typically has an owner who determines the access permissions and shares. Resources could be endpoint devices, provision devices, data
- The owner can grant or revoke access rights for other users or groups
- DAC offers flexibility and allows resource owners to have fine-granted control over access, but it can also result in inconsistent access control decisions without proper visibility, automation and orchestration
- DAC is the most prone to privilege creep

Authorization Models: RBAC

- Role-based access control (RBAC) grants access based on predefined roles or job titles
- Users are assigned roles, and access rights are associated with these roles (job title in organization chart)
- Instead of directly assigning permissions to individual users, permissions are assigned to roles, and users inherit the access rights associated with their assigned roles, for example:
    - Various roles in a hospital or medical center (doctor, nurse)
    - Built-in roles in a database management system (admin, backup, restore – operators)
- RBAC streamlines access control administration by grouping users with similar job functions and offering a scalable approach to access management.
- Don't have to use these models exclusively, can be in an environment (active directory (DAC) and another database system that uses (RBAC). No one size fits all.

Authorization Models: MAC

- A mandatory access control (MAC) is a strict mathematical model where access to resources is determined by the system based on predefined security labels and rules.
- Principles are assigned security clearances or classification levels (top secret, secret, confidential, etc.)
- Resource objects are labeled with sensitivity levels
- Access is granted or denied by comparing these labels and rules, ensuring strict control and preventing unauthorized access
- A MAC model is a non-discretionary model. Subjects in resource objects cannot change or grant themselves permissions at their discretion. There is no owner, everything is done by committee.

Authorization Models: ABAC

- Attribute-based access control (ABAC) grants access based on a combination of characteristics associated with users, resources, and environmental conditions
- Can use elements of role based or discretionary for example attributes can include user attributes (e.g. job title, department), resource attributes (e.g. sensitivity level, classification), and environmental attributes (e.g. time of access, location) or method used (VPN, no VPN).
- Authorization policies are defined using these combinations, and decisions are made based on evaluating the attributes against the defined policies

Authorization Models: ABDAC

- Attribute-based dynamic access control (ABDAC) combines the principles of attribute-based access control (ABAC) with dynamic access control (DAC)
- It considers dynamic factors such as risk assessment (qualitative model, 1-10), user attributes, resource attributes, and contextual information to make access control decisions (decision tree) in real time
- ABDAC provides more fine-grained and context-aware access control needed in "zero trust" environments when compared to traditional static access control models.
    - May include dynamic machine learning techniques such as user behavioral analytics (UBA) in next-generation environments

Authorization Models: Rule-based

- Rule-based access control (RBAC): RBAC uses rules to determine access
- Access control rules define conditions or criteria that must be met for access to be granted
- These rules can be based on several factors, such as user attribute, resource attributes, time of access, and more.
- Generally based on location, IP address and other elements such as service and port numbers

- Access decisions are made by comparing these rules against the context of the access request – usually IP transport and network layer header metadata

Security Control Categories
- Technical, Managerial, Operational, Physical

Technical Controls
- Are security mechanisms that the specific systems run on – either manually or, more often, automated and orchestrated
- These controls deliver confidentiality, integrity, authenticity, and availability protections
- They defend against unauthorized access or misuse
- They also facilitate the detection of security violations and support security requirements for applications and data

Common Technical Controls
- Infrastructure security and device hardening
- Identity and access (IAM) management engines
- Cryptographic key management and hardware security modules (HSMs)
- Cloud-based threat modeling tools
- SIEM and SOAR systems

Managerial Controls
- Managerial (also administrative) controls define policies, procedures, best practices, and guidelines and governance
- They are usually more logical in nature
- Should be published or printed definition of policies
    - No piggybacking (tailgating)
    - Acceptable use policies (e.g. social media on a corporate device)
    - Best practices and guidelines (awareness of common phishing attacks)
    - Password policies
    - Screening, hiring and termination procedures
    - Mandatory vacations
    - Training and awareness programs

Operational Controls
- Support the ongoing maintenance, dur care and continual improvement
    - Optimizing the change and configuration management database or shifting from a relational to a no sequel database
    - Performing tested patch management
    - Conducting awareness and training
    - Monitoring physical and environmental controls
    - Incident response and disaster planning testing and drills
    - Performing software assurance initiatives
    - Ongoing mobile device and mobile application management

Physical Controls
- Introduced to protect the campus, facility, environment and people
    - Various physical barriers
    - Guards and security teams

    - Cameras and surveillance equipment
    - Different types of sensors and alarms
    - Locking mechanisms
    - Secure safes, cabinets, cages and areas
    - Mantraps and faraday cages
    - Fire detection and suppressions systems
    - Environmental controls

Security Control Types

- Preventive, Deterrent, Detective, Corrective, Compensating, Directive

Preventative

- Stops an attacker from successfully conducting an exploit or advanced persistent threat
- Example is fences, gates, locking mechanisms. Practically speaking these can be overcome they are preventative

Deterrent

- Discourages an attacker from initiating or continuing an attack. For example, this could be a sign, sticker on a window or presence of security guide

Detective

- Identifies an attack that is occurring as well as the steps of the kill chain. Other words the steps that an attacker takes against a system. Intrusion detection system (IDS – technical) or camera (physical)

Corrective

- Restores a system to state before the negative event occurred (recovery point/objective); can simply rectify or correct an identified problem. For example, after a ransomware attack, can reimage a machine and recover the data from a backup.

Compensating

- Aids controls that are already in place or provides a temporary stopgap solution. For example, can be a next generation endpoint detection system, stopgap measure put in place until you have a budget for comprehensive.

Directive

- Mandatory policies and regulations that are in place to maintain consistency and compliance. For example, a directive that states how an end user can use their mobile device or company car or truck

Fundamental Security Concepts

Gap Analysis

- Difference between an initial state and another subsequent state.
- Context: Security
- In order to know where you are and where you need to go as a secure organization, you must conduct gap analysis.
- This technique will be applied to several security projects, plans, programs and initiatives throughout an entire security practitioner career.
- Information security gap analysis is a comprehensive appraisal that helps organizations determine the difference between the current state of their information security to specific industry requirements guidance and best practices, otherwise known as guidelines.
- When performing a security gap analysis, one will better understand the status of the cybersecurity risks and vulnerabilities in the organization.
- This type of risk assessment indicates where the technical, physical, managerial, and continuing operation controls need to be deployed.
- It involves knowing what the residual risks are and what further physical and logical safeguards (if any) need to be acquired and implemented.

Common Security Gaps

- Weak and/or shared credentials
- Lack of tested patch management
- Violation of the least privilege principle
- Having no/unenforced acceptable use policies
- Poor physical security
- Configuration and deployment errors due to lack of change and configuration management
- Poor visibility and lack of proper auditing

Zero Trust Control Plane

Zero Trust

- Zero trust (ZT) is the term for an evolving set of cybersecurity initiatives that move defenses from static, network-based perimeters (e.g. VLAN, subnet, IP Address) to focus on users, assets, and resources as the perimeter.
- ZT assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership. Moved from a trust and verify mentality.
- Authentication and authorization (both subject and object) are discrete functions performed before a session to an enterprise resource is established (with TCP/TLS)
- ZT embraces the principle of least privilege consistently across all resource classes and locations both physical and logical.
- Segregation (separation) of duties and high visibility (SIEM/SOAR) are also emphasized. ZTNA.

Zero Trust Adaptive Identity

- Adaptive identity is another key ZT component
    - It is also called adaptive authentication or risk-based authentication
- It is a method of access to data that matches user credentials with the risk of the requested authorization. For example, are the accessing sensitive data as opposed to readily available information

- It delivers support for multiple classes of consumers and participants, whose roles and identity may evolve to meet rapidly evolving ecosystems and environments
- Offers ease of maintenance and operation while being agile and easy to modify

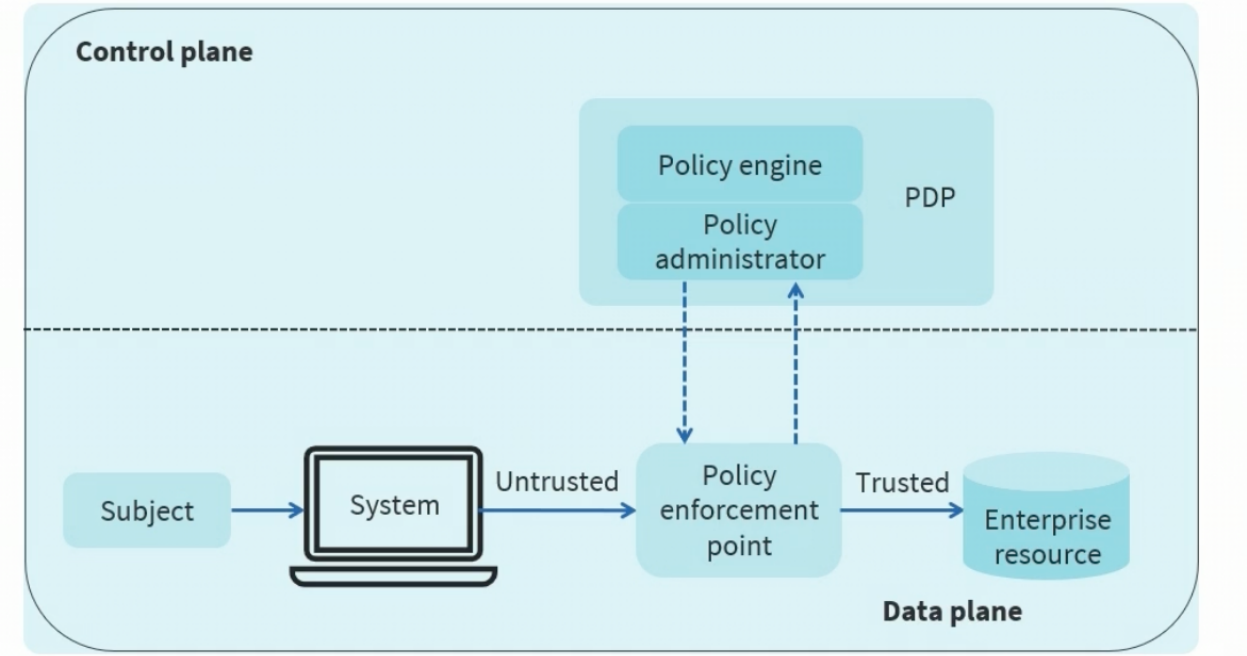
Zero Trust Threat Scope Reduction

- Another main goal of ZT is threat scope reduction and risk avoidance
    - Reduced scope of threats to support agility and support complex environments
    - Increased complexity and number of communication patterns, increasing difficulty of addressing through a data and asset-centric approach

Zero Trust Control Plane

- The ZT control plane is separate from the data plane and contains the policy decision point (PDP), which includes:
    - The policy engine (PE), which uses the enterprise policy-driven access control (as well as input from external sources) to grant, deny, or revoke access to resource objects.
    - The policy administrator (PA), which enables and/or shuts down the communication path between a subject and a resource via commands to associated policy enforcement points (PEPs)
    - The PA communicates with the PEP when creating the communication path via the control plane.

ZT Architecture



-
- Subject is a User/Person who is untrusted until PEP redirects to policy engine and administrator. Once authenticated and authorized it can access enterprise resource.

Zero Trust Data Plane

- The zero trust data plane is defined by explicit trust zones, which could include
    - Data centers
    - DMZs (public access zones)
    - The public Internet
    - Cloud computing subnets such as private or VPN-only
    - Honeynets

Policy Enforcement Points (PEP)

- Two types: Network and Application PEPs
- Network PEP Examples:
    - Edge routers
    - Edge firewall appliances
    - SDP access gateways
    - Network L2/ML switches
    - Authentication proxy servers
- Application PEP Examples:
    - API gateways (accept web socket and restful API)
    - Resource groups
    - Network VLANs
    - Code repositories
    - Cloud services

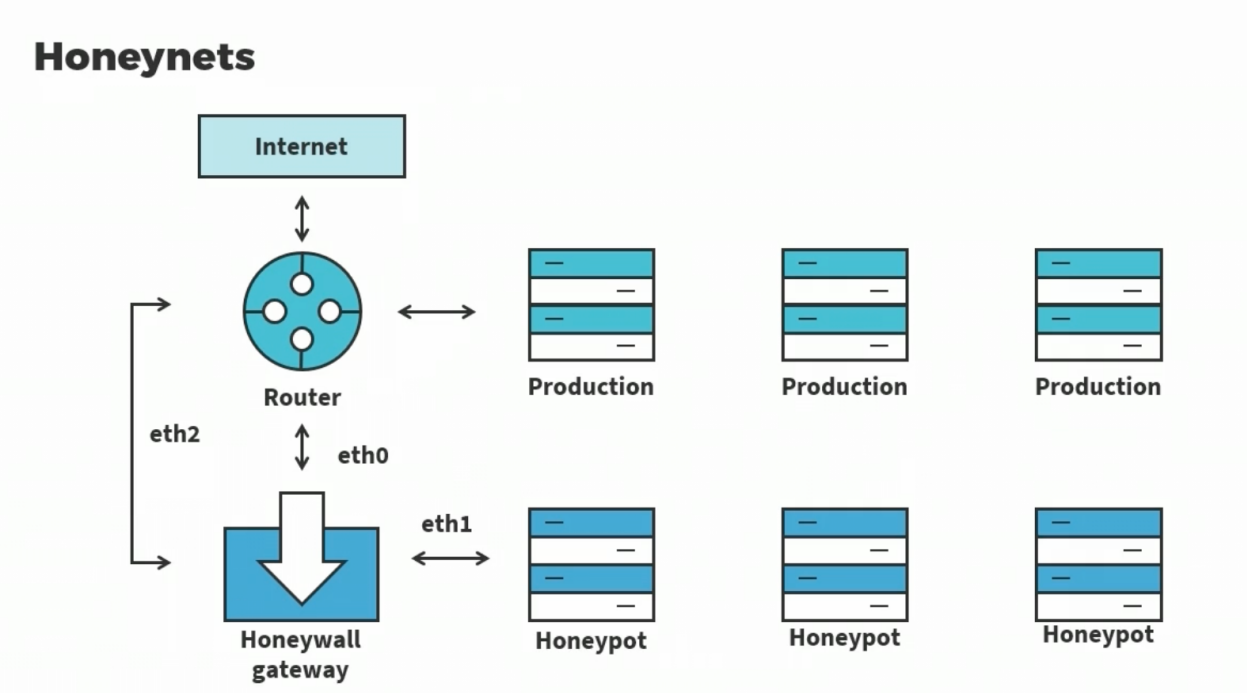
Deception Technologies: Honeypot

- A honeypot is a (single) system (e.g. a web server) or resource (e.g. a file on a server) that is designed to be attractive to potential attackers and intruders, like honey is eye-catching to bears
- Modern systems are often running as a virtual machine in a type 1 hypervisor such as a VMware solution. Typically placed behind customer premise equipment such as edge router or firewall appliance
- They are strategically placed in parallel to public access or demilitarized zones where public-facing servers are typically placed

Honeynets

- A honeynet can simply be considered a “network of honeypots”
- It is also set up with intentional vulnerabilities hosted on decoy servers and services to attract or redirect attackers
- The primary purpose is to test network security by inviting attack patterns and “kill chains” by threat agents
    - This helps security teams analyze an actual attackers activities and methods to improve network security

-



Honey Files and Honey Tokens

- The compromised privileged insider is the number one internal structured threat for most organizations
- Honey files and tokens are strategically placed artifacts and files meant to allure the suspect into exposing themselves as part of an internal investigation
- They are also valuable in the discovery of attackers who are deep into the kill chain phases. For example, enumeration and lateral movement.
- Common examples are access keys and credentials to valuable cloud-based assets and database entry points

Presentative Physical Security Controls

- Before security professionals can focus on technical and operational countermeasures, they must be certain that these are deployed in a physically secured property, facility, and environment
- Although detective and deterrent controls are important, prevention is critical for protecting all types of assets

Fence Barriers

- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- Fences can be of varying heights and barbed depending on the locale
- Electrified fences and signage are also common for high security properties and facilities (e.g. airports, prisons, military installations)

Gates

- Fences are often combined with entry/exit gates of varying strength and guarding
- Barricade gates and tire shredders are common
- Types of gates in the U.S. include
    - Class I: Residential gate operation

    - Class II: Commercial, such as a parking lot or garage
    - Class III: Industrial/limited access (e.g. warehouses, factories, docks)
    - Class IV: Restricted access operation requiring supervisory control

Bollards
- Bollards are strategically placed pylons meant to redirect pedestrian traffic or prohibit vehicles from entering certain areas, such as the foyer of an office building
- They can be permanent or temporary pillars
- They are typically made of concrete or strong metal
- High-tech bollards can be mechanical and include cameras and sensors

Access Control Vestibules
- Access control vestibules are typically areas that are fortified with forced entry-resistant and bullet-resistant security glazing
- These fortified entryways serve as formidable barriers to unauthorized access that go beyond traditional security measures
- Access control vestibules are also known as security or mantrap vestibules and are a highly effective means of hardening commercial security, typically through a series of interlocking doors

Mantraps
- There is an entry and exit door but only one door can be open at a time
- One person at a time – no piggybacking (tailgating):
    - Person can be identified and authenticated
    - Provide credentials and license or passport
    - Can include biometric readers
    - CCTV and intercom systems are often used
    - Security guard behind bullet-proof glass
    - Person is eventually allowed in through a strong door with electronic locks

Access Badges and Cards
- Access badges and cards represent another “something you have” authentication factor
- Many organizations will have all guests register at a reception area security desk:
    - Collect and input identification information in a visitor log
    - Distribute temporary access cards or badges
    - Have a camera station for pictures for a temporary badge
- There should be a “no tailgating (piggybacking)” policy at all access points regardless on the status of the person (i.e. contractor, janitor, worker)

Common Access Card (CAC)
- Expiration date
- Federal identifier
- Affiliation
- Service/agency
- Color indicator
- Pay grade
- Rank
- Integrated circuit chip

Security Guards

- Security guards are typically 24/7, but could just be present during business or non-business hours
- They are a security control of multiple types:
    - Detective
    - Deterrent
    - Preventative
- They can provide rapid security response if an intrusion or incident occurs
- Robot sentries are rapidly replacing humans in certain scenarios

Security Guard Considerations
- Are they hired, contracted, or freelance?
- Do they need to be certified/licensed?
- Will they be armed or unarmed?
- What is the impact on insurance policies? (If they carry weapons -> higher premiums)
- Is the organization directly involved with screening and background checks?
- Where are they stationed on the campus/facility?
- Who provides the ongoing training?

Detective Physical Security Controls

Video Surveillance
- Cameras and video surveillance provide a way to monitor and record the property perimeter for intruders and potential attackers
- They are considered detective physical controls, but the mere presence may also be a deterrent
- Video surveillance offers a way to record intruders in action with recordings
- Alerts should be triggered when a camera is disabled

Video Surveillance Considerations
- They systems will be indoor and outdoor webcams or CCTV systems
- May be closed-circuit to a security operations center (SOC)/linked to a third-party vendor
- It is imperative to transfer media to a safe and secure location
- Industrial camouflage involves cameras and surveillance devices hidden in landscaping elements, statues, and tall trees
- It should be combined with various lighting solutions, both of which can have “dead spots”

Lighting
- Lighting can enhance other security controls such as cameras, security guards, and sensors
    - They should start at the perimeter and be used in every defense-in-depth mechanism
- Some modes of lighting can be mercury vapor, sodium vapor, quartz, and LEDs

Security Lighting
- Continuous lighting is the most familiar form of outdoor security lighting and can provide greater projection and control
    - The glare of continuous (barrier) lighting originated in prisons and correctional institutes and is still in use today
- Stand-by lighting systems are designed for reserve or stand-by use or to supplement continuous systems
    - These systems are engaged either automatically or manually when the continuous system is inoperative or when there is a need for extra light

Security Lighting

- Moveable lighting hardware is manually operated and typically is made up of moveable search or flood lights located in chosen places, which require temporary lighting
    - The moveable system is also used to supplement continuous or stand-by lighting and is often used at construction sites
- Emergency lights are used in times of power failure or other emergencies when other systems are inoperative – often gas-powered generators or batteries

Types of Sensors

- Photoelectric – a break in a light beam
- Passive infrared – detecting infrared light
- Vibration – a change in the level of vibration
- Acoustical – noise detection of a change in sound waves
- Microwave – a change in high-frequency radio waves
- Electro-mechanical – a break in electrical circuit
- Electrostatic – a change in an electrostatic field
- Moisture and temperature detection – for server rooms and data center environmental control

Sensors Trigger Alarms

- A static or flashing light on the display panel in the security room or operations center
- Bells ringing or horns blaring
- Sending a text notification to an interested party
- Sending an email message
- A silent alarm to a security firm or local law enforcement
- A telephone or cellular call to a software program or live attendant

Change Management Business Processes

Change Management

- Change management is the methodical approach to handling the transition or modification of an organization's goals, processes, operations, configurations or technologies
- The purpose is to implement strategies for carrying out change, controlling transformation or various migrations, and assisting individuals in adapting to change
- Change management is also referred to as the change control practice
- Typically, configuration management occurs first to establish a baseline before standard, normal, and emergency changes occur

Change Management Lifecycle

1. Submitting (Iterative between 1 and 2 before 3 occurs)
2. Approving
3. Documenting
4. Testing
5. Implementing
6. Reporting

Change Control Business Processes

- The approval process should be a flexible and highly iterative phase of the lifecycle

- Ownership of the physical or logical asset must be considered and is driven by the access control model
- All stakeholders should be either involved based on the RACI model
    - Responsible, accountable, consulted, informed
    - Always at least 1 responsible, consulted involves two way communication, informed is notification, only 1 accountable
- A change impact analysis compares two states (the current and future state) of a change to identify what is changing, who is impacted by the change, and what needs to be communicated to the impacted. Also referred to as gap analysis
    - The process involves identifying and categorizing who and what will be affected, assessing the degree of change occurring within these areas, and describing the change
        - This last activity folds into stakeholder analysis, communication analysis, and strategies
- A change backout or fallback plan is a recovery point, and it must be in place during both the testing plan and implementation phase
    - Make small individual changes instead of several impactful changes
- Maintenance windows are typically used to show times during which changes should be scheduled
- A standard operating procedure (SOP) offers precise directions and detailed instructions needed to perform a specific task or operation consistently and proficiently. More orchestrated a SOP the more successful it will be in the long run

Change Management Technical Implications

- Allow/deny lists are used with change control in line with the access control model to dictate which subjects are allowed to make changes or not
    - An allow list is a permissive control
    - A deny list is a restrictive control
- By implementing least privilege and separation of duties, certain activities and areas will be restricted

Change Management Technical Implications

- Downtime relates to high availability, which is an aspect of resiliency
- Availability consists of planned and unplanned downtime (e.g. an outage) and must be considered with technical change management when making modifications or performing migrations
- Other considerations are a service restart, application restart (ensuring state machine is stable – is not affected), legacy applications, and all dependencies

Documentation and Version Control

- Organizations must document using a well-established tagging and labeling schema that maps to a configuration management database (CMDB), such as ServiceNow
- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
    - Relational databases have been used historically
    - NoSQL/document databases are emerging as a common solution
    - You could leverage a CSP service, such as Amazon Redshift data warehousing or DynamoDB

Documenting with a CMDB

- A configuration management database is not a typical data warehouse – it's a special use case often a software as a service solution
- It plays a critical role in several IT management initiatives, like IT service management (ITSM) and IT asset management (ITAM)
- It helps various IT services to better align with business needs by providing current and accurate data for
    - Change and patch management
    - Incident and problem management
    - Availability management
    - Release and deployment management

Version Control

- Version control and change management procedures are important to both the operations team and the security team
- Version control applies to
    - Operating system builds
    - Application updates
    - Device drivers
    - Licensing updates
    - Various upgrades and patches
    - Container packages, microservices and code in general
    - Firmware updates
    - Trusted platform modules
    - Component updates

Practical Cryptography

Symmetric Cryptography

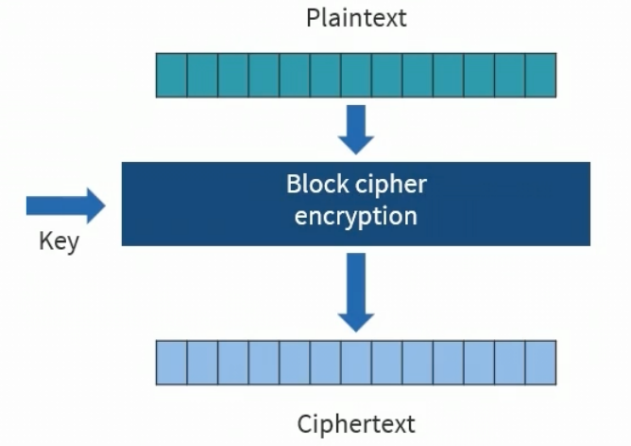
Cryptographic Services

- Confidentiality
  - (e.g. Using encryption to) hiding the data at rest, in transit, and/or in use from unauthorized principles
  - It typically involves a system or algorithm that converts plaintext data into ciphertext
- Integrity
  - Ensures the data has not been altered while at rest or in transit
- Non-repudiation
  - Ensures the original sender cannot deny sending data or engaging in a digital transaction

Symmetric Key Cryptosystems

- This historic form (e.g. Caesar cipher) uses the same key to encrypt and decrypt
- Efficient, fast, and handles high data rates of throughput
- Computationally inexpensive
- Deploys shorter key lengths (40 to 512 bits)
- Primarily used to protect data at rest
- Key management is more complex unless using hardware security modules (HSMs) or cloud key management services
- There is no built-in origin authentication
- Symmetric systems do not scale well unless a cloud key management service is used
- Most popular algorithms are AES-CBC-128/256 and AES-GCM-128/256
- Symmetric key algorithms function as a block cipher or stream cipher

Block Ciphers



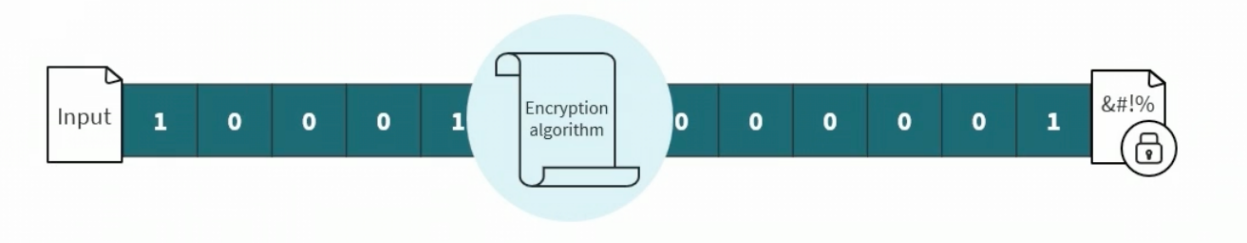
-
- Operates on fixed blocks of data (bits) based on key size
- 64, 128, and 256-bit keyspaces are common
- Messages bigger than the key size are broken into blocks the size of the key and must include padding
- Common block ciphers:
  - DES (deprecated)
  - 3DES-EDE (deprecated)
  - AES-CBC
  - AES-GCM

- Blowfish

Stream Ciphers

- Operate on a continuous stream of plaintext data by encrypting one bit or byte at a time
- Plaintext bits are typically XORed with keystream bits
- Keystream = random bits, bytes, numbers, characters
- Faster and less complex than block ciphers
- Modern ciphers can work in a block or stream mode or both:
  - FISH
  - CryptMT
  - Scream
  - Cryptographic hashing

Stream Cipher Example



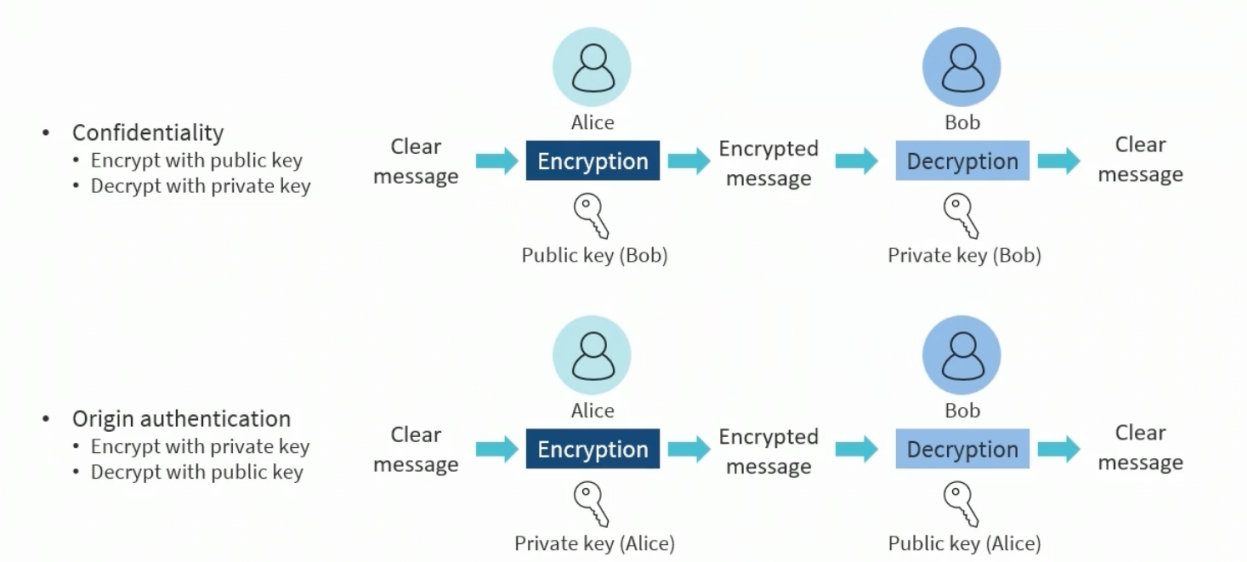
-
- Alice wants to use a stream cipher to encrypt the letter “A”
- In ASCII, the letter “A” has the value of 65 = 1000001
- The first cipher stream bits are 0101100
- We perform an XOR function (Modulo 2 addition)
  - 1000001 = A XOR 0101100 -> 1101101 is the result
- The letter “A” becomes ciphertext “m” (ASCII value 109)

Asymmetric Cryptography

Asymmetric Key Cryptosystems

- Uses a mathematically related pair of a public and private key
  - If one is used to encrypt, the other is used to decrypt
- Public key infrastructure (PKI) enables efficient key management and scalability
- Often used for digital signatures and key exchange
- Employs longer key lengths than symmetric (up to 4096)
- Slow and more computationally expensive

Example Asymmetric Key Cryptosystems



-
- Alice wants to use a asymmetric key cryptosystem to send a message to bob and him have a high degree of confidence to employ confidentiality. If she wants to send this confidential message to bob or encrypted message she will get bobs public key. She can do that in a handshake protocol or out of band or in a digital certificate. She will encrypt the message with bobs public key and he will use his related key pair – private key to decrypt the message.
- If Alice wants to send a message to bob and show that the message has an authentic origin being Alice she will encrypt the message with her private key. Then she will get bob her related public key either in a certificate or a handshake protocol or some type of out of band method. When bob gets the encrypted message that was encrypted with Alices private key he can use her public key to decrypt it. All bob really knows here is that Alices private key was used to encrypt the message. This is a fundamental basic form of origin authentication. Bob is not 100% certain that it was Alice that used her own private key. We have to use more robust identity methods and multiple factors to give bob a higher degree of assurance that it was actually Alice that used the private key. Often Alice and bob would rely on a trusted third party. For example, a PKI (public key infrastructure certificate authority)

Popular Asymmetric (Public Key) Algorithms

- RSA – the most widely used algorithm for securing communication and data encryption
- Diffie-Hellman key exchange – a protocol for securely exchanging cryptographic keys over an untrusted network
    - RSA can also exchange keys but often we will use RSA for security aspect and DH for key exchange. In more modern implementations (mobile devices) will use Elliptic Curve
- Elliptic Curve Cryptography (ECC) – an algorithm based on the algebraic structure of elliptic curves over finite fields
- Digital Signature Algorithm (DSA) – a standard based on the mathematical concept of modular exponentiation and discrete logarithm problem.
    - Can combine both ECC and DSA

Encryption Levels

Full Disk Encryption (FDE)

- Full Disk encryption is the process of encoding all user data on a device using an encrypted key
- Also called whole disk encryption – the master boot record (MBR) (or comparable) that includes code that loads the operating system is not encrypted

- Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk

Partition Encryption
- Encryption partitions are disk partitions that are protected with encryption keys to prevent unauthorized access to the data on the drive
- One advantage of encrypting only a partition instead of the whole drive is that you can encrypt/decrypt the partition while using the system for other tasks
- If one only encrypts a data partition, however, sensitive data can remain in temporary files or swap files in a non-encryption partition – this is often called data remanence

File Encryption
- File-level encryption enables the protection of individual files by encrypting them
- This technique is often utilized when there are specific files that need an extra degree of security or contain very sensitive information
- Encrypting individual files offers more control over access and assures that even if one file is cracked, the others will still be safe

Volume (Block) Encryption
- Volume encryption targets a section of the physical drive, which is defined as a separate partition or "volume"
- It provides a choice to encrypt different volumes, whereas with disk encryption, you can only encrypt everything
    - Volume encryption can help save time and provide greater flexibility
- If a single volume occupies the entire hard drive, then volume encryption will function the same way as full disk encryption

Database and Record Encryption
- Database encryption is the process of using an algorithm to transform data stored in a database into unreadable ciphertext. This could involve one key or more
- The purpose is to protect the data stored in various platforms from being accessed by external attackers or even compromised privileged insiders
- When using a cloud database service, key management services are often used
- Record encryption will encrypt and decrypt the individual records in a database systems

Hashing, Salting, and HMACs

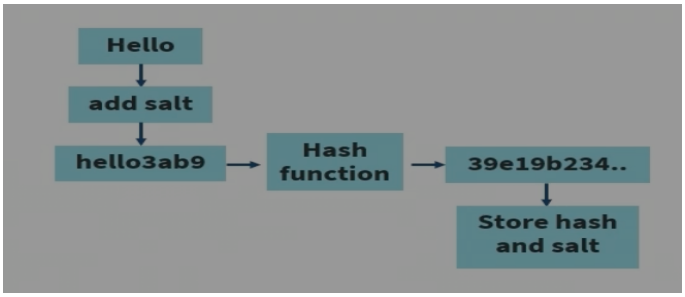
Cryptographic Hashing
- A one-way mathematical function that produces a digest of 128 to 512 bit
- Converts data of any input size to a fixed-length string called a hash value, message digest, or fingerprint
- An advanced version of a simple checksum (operating system when moving a file e.g.)
- Birthday paradox and avalanche effect
    - Birthday paradox -> a cryptographic hash is only as strong as half its bit size (512/2 -> 256 bits strong)
    - Avalanche effect -> if one bit is flipped or wrong in origin data then fixed length hash will be completely different
- Used in authentication, data integrity, non-repudiation, fingerprinting, password storage, database indexing

- Must be collision resistant (no MD5)
    - Two different inputs must not create the same fixed length hash or digest

Common Hash Functions

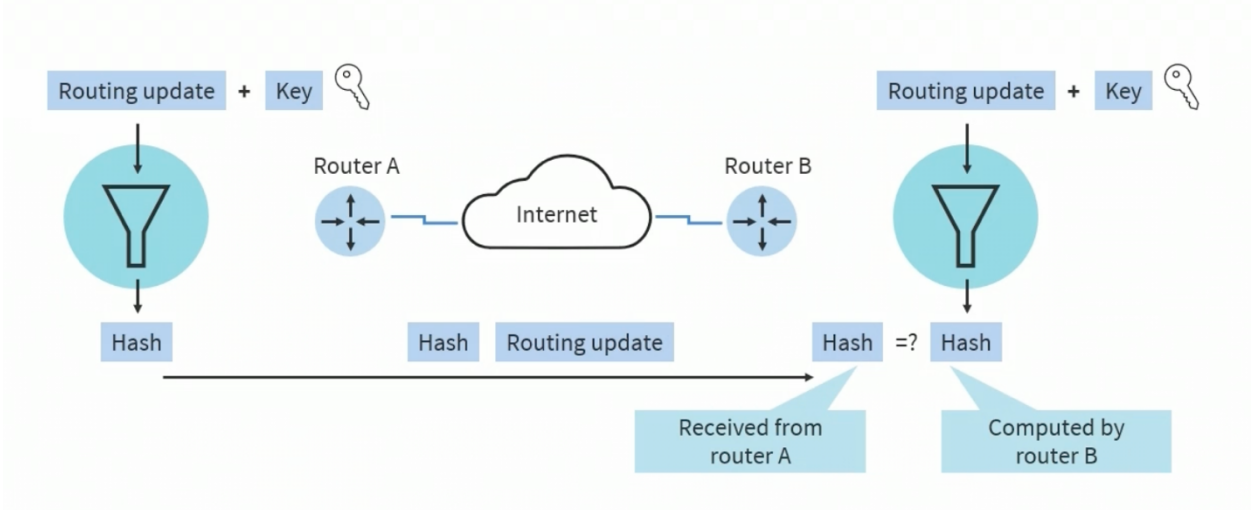
- RIPEMD (128, 160, 256 and 320-bit versions)
- SHA-1 (160-bit digest is produced)
- SHA-2 (SHA256 or SHA512)
- SHA-3 (224-512)
- Whirlpool (a modification of AES algorithm)

Salting

- 

- Salting is the technique of adding pseudorandom data to a cryptographic hash function
- The goal is to make it less deterministic for cracking tools
    - When an attacker can access a database of password hashes, they can use either hash tables or rainbow tables to look up matching hashes, which they can use to discover the passwords or other hashed data
- Two weaknesses are salts that are too short or if they aren't unique for each password

Hash-based Message Authentication Codes (HMACs) for Integrity and Origin Authentication

- 

- An HMAC is simply a hash function with a shared secret key or shared often in numeric string. This hash many applications but in this example we will look at two different routers who are sending route updates to each other. They are neighbors in a dynamic routing protocol. Make sure that only the proper updates are sent between the routers, in other words authenticating the origin of the routing update and maintaining integrity. In this example the routing update information which is varying length is added to a key and the data and the key go through the hash function. The result is appended to the routing update and the receiving router using the same cryptographic hash and the same key can trust that integrity was maintained and that the origin router was authentic.

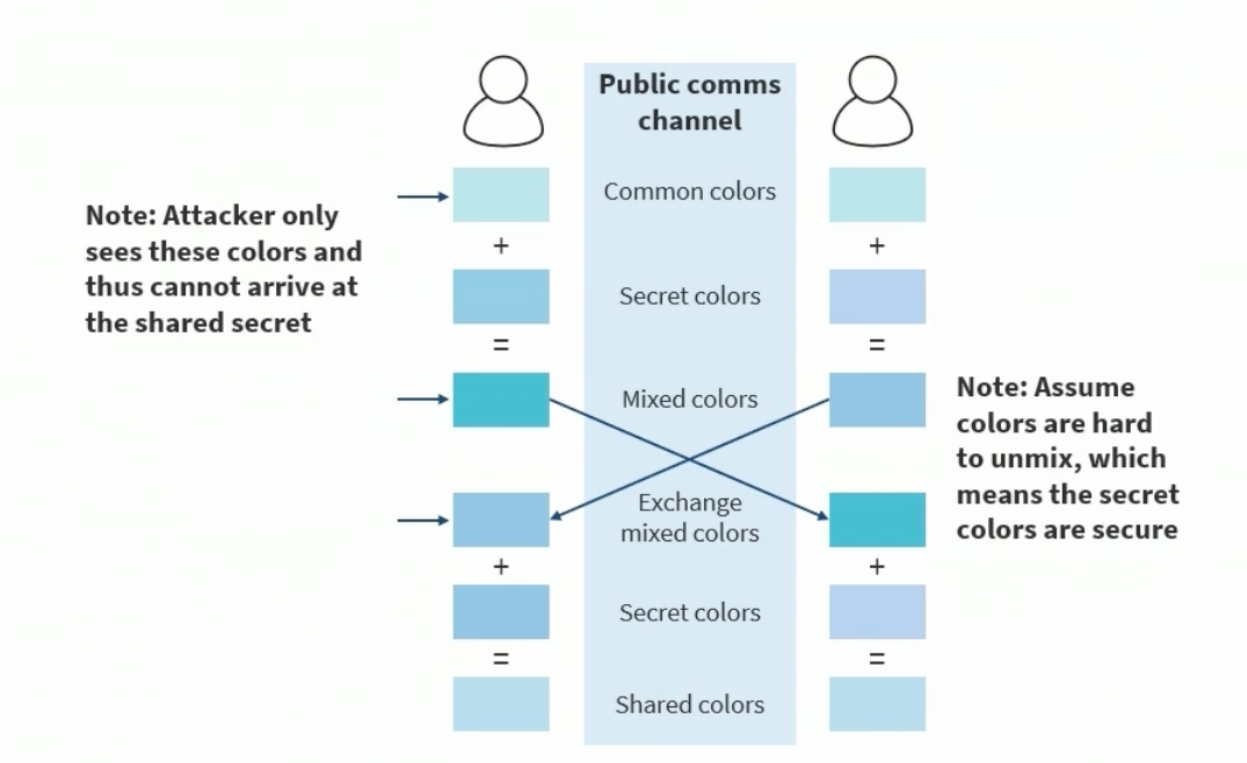
Key Exchange

- Biggest challenge with cryptosystems is managing keys especially key exchange. This is applicable with symmetric keys.
- There are several ways for parties to exchange keys:
    - Phone or text
    - Secured email
    - Couriers
    - Diplomatic bags
- Alternatively, a more effective method is using an asymmetric key exchange algorithm, such as:
    - RSA key exchange
    - Diffie-Hellman key exchange
    - Elliptic Curve Diffie-Hellman
    - Elliptic Curve Diffie-Hellman Ephemeral

Diffie-Hellman Key Exchange

- Diffie-Hellman key exchange (DHKE) and RSA key transport are original protocols created for establishing secret keys between two parties over an unsecure channel
- Diffie-Hellman is a widely used asymmetric cryptosystem found in SSH2, TLS, and IPsec
- It represents an impressive application of the discrete logarithm problem
- The RSA algorithm can sign public-key certificates, whereas the Diffie-Hellman key exchange cannot

Basic Concept of DHKE



-
- The basic concept of DHKE is at the bottom. Generating a shared color between two parties over a untrusted network that a third party or a meet in the middle or ongoing path attacker cannot determine. In this exchange here using colors the attacker only sees the common colors and cannot arrive at the shared secret color.

Diffie-Hellman Modes

- DH (Diffie-Hellman)
    - The same shared secret is used all the time between parties. Rarely used today.
- DHE/EDH (Ephemeral Diffie-Hellman)
    - A different shared secret is used each time between parties. This is also using a principle called perfect forward secrecy
- ECDH (Elliptic Curve Diffie-Hellman)
    - Uses EC public/private key pair
    - The same shared secret is used all the time between parties
- ECDHE/ECEDH (Elliptic Curve Ephemeral Diffie-Hellman)
    - Uses EC public/private key pair
    - A different shared secret is used each time or for each session

ECDHE/ECEDH (Elliptic Curve Diffie-Hellman Ephemeral)

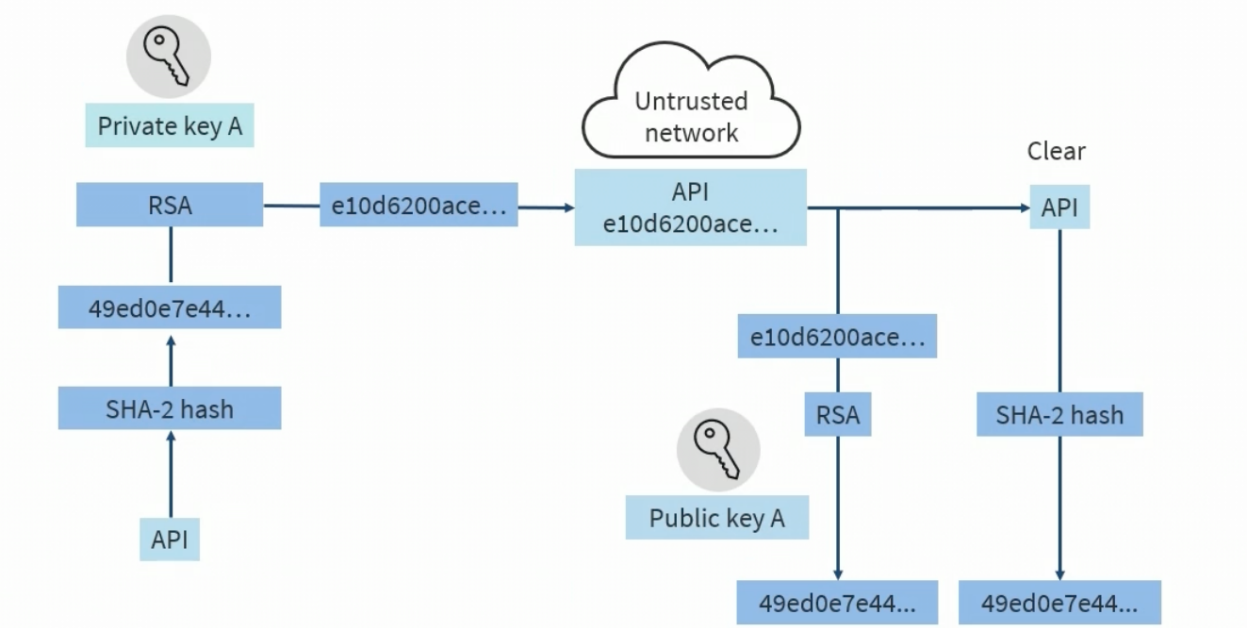
- Based on rich math functions of values plotted on an elliptic curve
- Uses smaller key spaces while offering superior strength
- 256-bit elliptic key = 3072-bit standard key
- Excellent for mobile devices and IoT with limited memory and processing power
- Common use cases:
    - Key exchange
    - IPsec and TLS
    - Digital Signatures

Digital Signatures and Certificates

Digital Signatures

- These are a scalable mechanism for providing authenticity, integrity, and non-repudiation using random public/private key pairs
    - Does not offer confidentiality
- Digital signatures are legally equivalent to a handwritten signature in many countries
- SHA1/2/3 hash algorithms are commonly used
- Signing algorithms:
    - Rivest-Shamir-Adelman (RSA)
    - Digital Signature Algorithm (DSA)
    - Elliptic Curve Digital Signature Algorithm (ECDSA)

Digitally Signing an API Call



-
- In this example the API is going to go through a SHA 2 hash which will result in a fingerprint or a digest regardless of how big the API is. Then the sender whose generated a private and public key pair will use their private key which in this case is RSA to encrypt the digital hash. The encrypted digital hash is then appended to the API and sent over the untrusted network. Again, we are getting integrity, we are getting origin authentication (because of the private key) and non-repudiation. The sender cannot come back at a later time and repudiate that they didn't send the API because there private key was used to sign the hash or encrypt the hash and it's their responsibility to protect that private key. If they can't, they must rely on a trusted third party, for example, a public certificate authority. The recipient who has the corresponding public key of the sender also knows the hash function that was used and the protocol that generated the public and private key RSA. They can then unpackage and view the API.

Digital Certificates

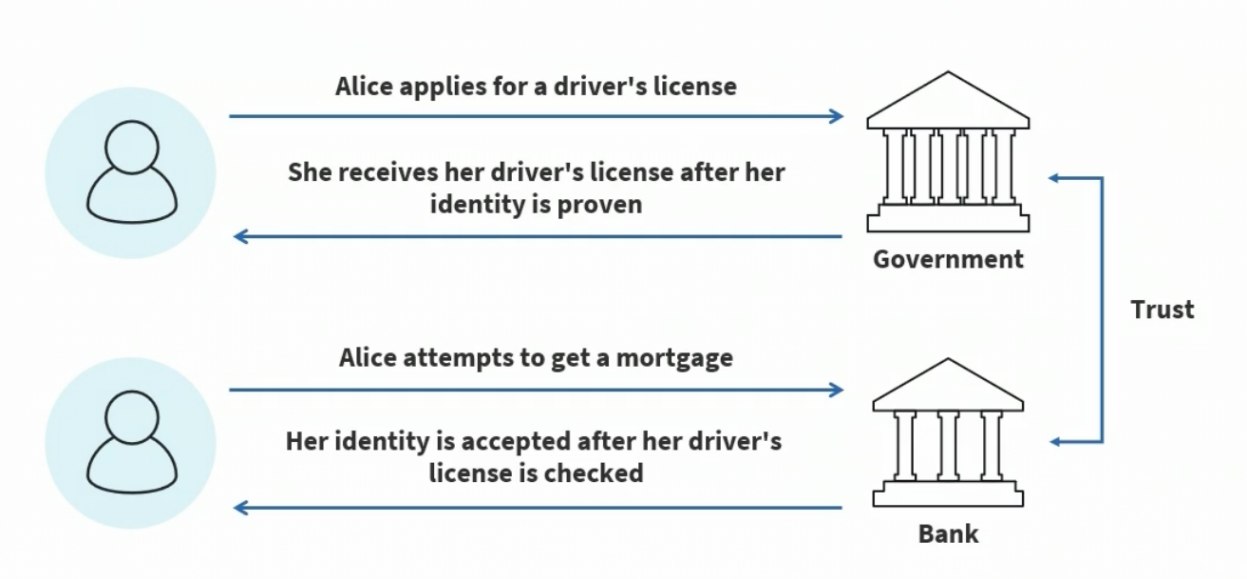
- A digital certificate is a form of file used to bind cryptographic key pairs to entities such as individuals, websites, devices, or organizations
- If validity affirmation and/or public trust is needed, then a trusted certificate authority (CA) will assume the role of a third party to validate, identify, and associate them with cryptographic pairs using the digital certificates
- The key pair consists of a public key and a private key
- The public key is included in the certificate, while the private key is stored in a secure fashion
- The owner of the private key can then use it to sign documents, and the public key can be used to verify the validity of those signatures
- A common format for digital certificates is based on the X.509 standard

X.509v3 Digital Certificates

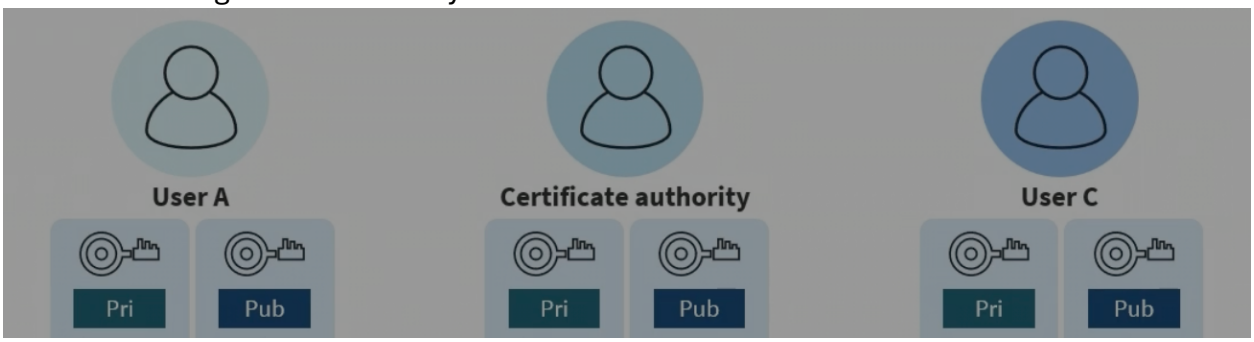
- Certificate of fields of metadata about the entity that has the public key
- Fields:
    - Version number (v3)
    - Serial number (really large pseudo random number)
    - Signature algorithm ID (what was used to digitally sign the certificate – CA)
    - Issuer name
    - Validity period (valid from a certain time to a certain time)

- Not before
- Not after
- Subject name (not really used – comptia.org)
- Subject alternative name (used because it supports IPv6 addresses – modern)
- Subject public key info
- Public key algorithm
- Subject public key
- Issuer unique identifier
- Subject unique identifier
- Extensions (used to add functionality and better security to digital certificates)
- Certificate signature algorithm
- Certificate signature

Public Key Infrastructure (PKI)

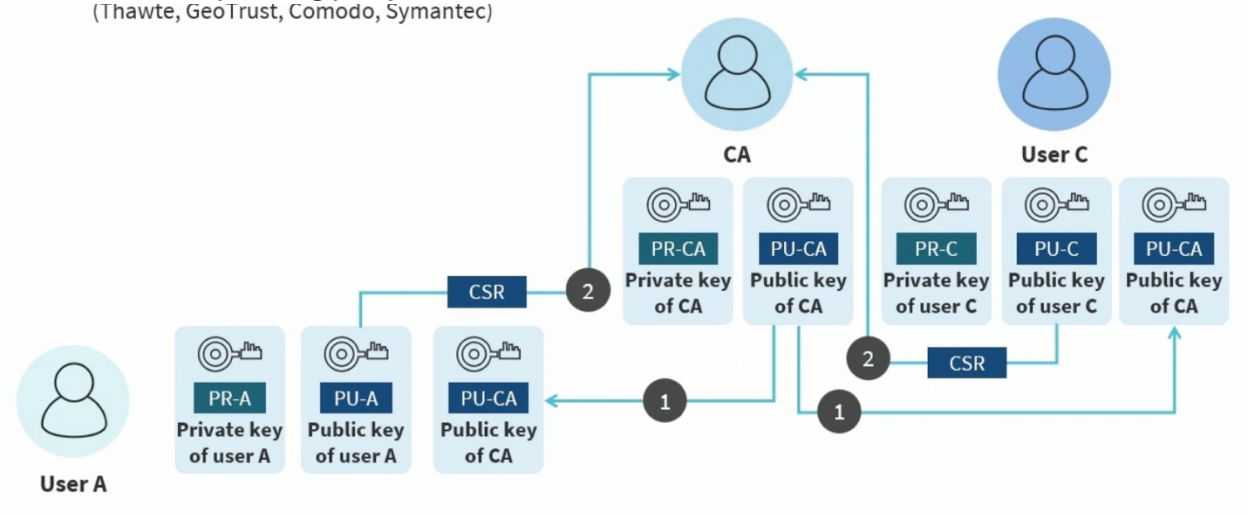


-
- One thing that makes a asymmetric key cryptosystem actually work and be scalable is having a trusted third party. For example, Alice applying for a driver's license from a government agency. When she receives the license she can use it to prove her identity in a wide variety of use cases. For example, when she tries to get a mortgage. Her identity is accepted in the mortgage application after her driver license is checked by the bank against the trusted third party which in this case is the government entity that issued her driver license.



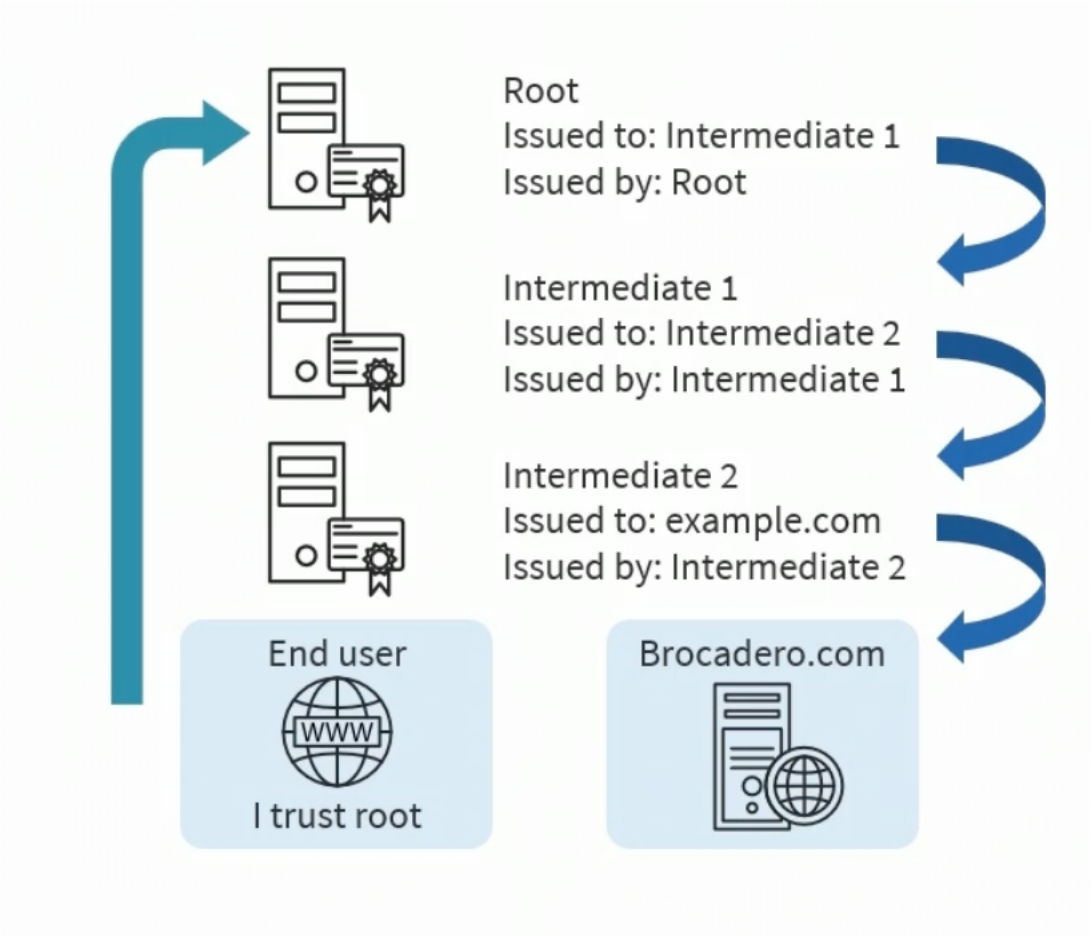
-
- The public key infrastructure is really taking this concept of a trusted third party to a potentially global scale.
- PKI is a scalable binding of a public key with an entity identity
  - A person, system, or organization

- In this example we have two users who want to communicate and perform transactions. They want integrity, origin authentication and non-repudiation. In this example user A and user C happen to use the same certificate authority (CA). Either the user A or on their behalf the certificate authority will generate a public private key pair. And the same thing goes for user C. Now the certificate authority they also have a public private key pair as well. Digital certificates are registered and issued by the certificate authority. This can be automated through an enrollment protocol or done manually or automated. The CA may also generate the key pair (e.g. RSA 248) on behalf of the requesting party and include that in the certificate.



-
- The CA is the central trusted introducer but they are also responsible for letting participants of the infrastructure know if for some reason that public private key pair and or certificate can no longer be trusted.
- The CA can store, issue, and digitally sign certificates of customers all over the world.
- Everyone has the public key of the CA (or a trusted CA) in a browser or O/S store
- A certificate signing request (CSR) is used by the enrolling party to be granted a certificate by a CA

CA Trust Models



-
- Single CA:
    - Responsible for directly providing certificates to everyone (enterprise PKI)
    - Must always be online
- Hierarchical CA:
    - Combination of root CA and intermediate CAs
    - Root sends certificates to intermediates
    - Intermediate CAs provide certificates and the “chain” to users or other intermediate CAs
    - Root can be online or offline
- Online – connected to the network and issues certificates over the network
- Offline – not connected to the network and issues certificates on removable media

Certificate Revocation and Suspension

- CA that is using PKI has two main purposes: global distribute public keys and certificates and revoke certificates
- Certificates are stamped with non-deterministic serial numbers and validity dates
- For security reasons, all keys must have a finite life due to brute-force attacks
- Certificate can be
    - Revoked (permanent) – never used again
    - Suspended/held (temporary) – can be reactivated
- The certificate revocation list (CRL) is the original method for revoking certificates
- Online Certificate Status Protocol (OCSP) is an Internet- enabled transactional database that CA’s and web servers utilize for suspension and revocation

Cryptographic Tools

Trusted Platform Modules (TPM)

- When an endpoint or device is using a X509v3 certificate it is stored in a TPM
- A TPM is used to improve the security of various systems, such as servers and PCs
- Microsoft uses services like BitLocker Drive Encryption, Windows Hello, and others to securely create and store cryptographic keys
- It is often a separate chip on the motherboard (TPM 2.0) that allows manufacturers to build the capability into their chipsets rather than requiring a separate chip
- Google employees store X.509v3 certificates in TPMs in devices as part of zero trust

Hardware Security Modules (HSMs)

- These are hardened, tamper-resistant dedicated appliances or integrated modules in a PC/server
    - HSMs can be physical or virtualized
- A Smartcard-HSM is a lightweight hardware security module in a smart card, MicroSD, or USB form factor providing a remotely manageable secure RSA and ECC keys
- Responsibilities include:
    - Managing, processing, generating, and storing keys
    - Verifying digital certificates
    - SSL/TLS connection accelerator
    - Encrypting sensitive data
    - Verifying the integrity of stored data

Key Management Services

- A cloud-based key management service (such as AWS KMS) is a managed service that enables the creation and control of customer-managed symmetric and asymmetric cryptographic keys to protect various types of data at rest and in some cases data in transit
- These key services integrate with many other cloud services, such as block storage, object (blob) storage, applications, and databases to facilitate the encryption of critical data

Key Stretching

- Tools such as PBKDF2 apply a pseudorandom function, such as an HMAC, to the input password or passphrase along with a salt value
- PBKDF2 then repeats the process many times (1000 iterations) to produce a derived key, which can then be used as a cryptographic key in further operations
- The stretching process makes password cracking much more difficult
- Today, programs will use hundreds of thousands of iterations due to fast processors

Secure Enclaves

- A secure enclave delivers CPU hardware-level isolation and memory encryption on a server, workstation, or mobile device by isolating application code and data from anyone with privileges and encrypting its memory
- With additional software, Secure Enclaves enable the encryption of both storage and network data for simple full-stack security
- Secure enclave hardware support is built into all new CPUs from Intel and AMD
- The Secure Enclave is a hardware feature of most versions of iPhone, iPad, Mac, Apply TV, and Apple Watch

Steganography

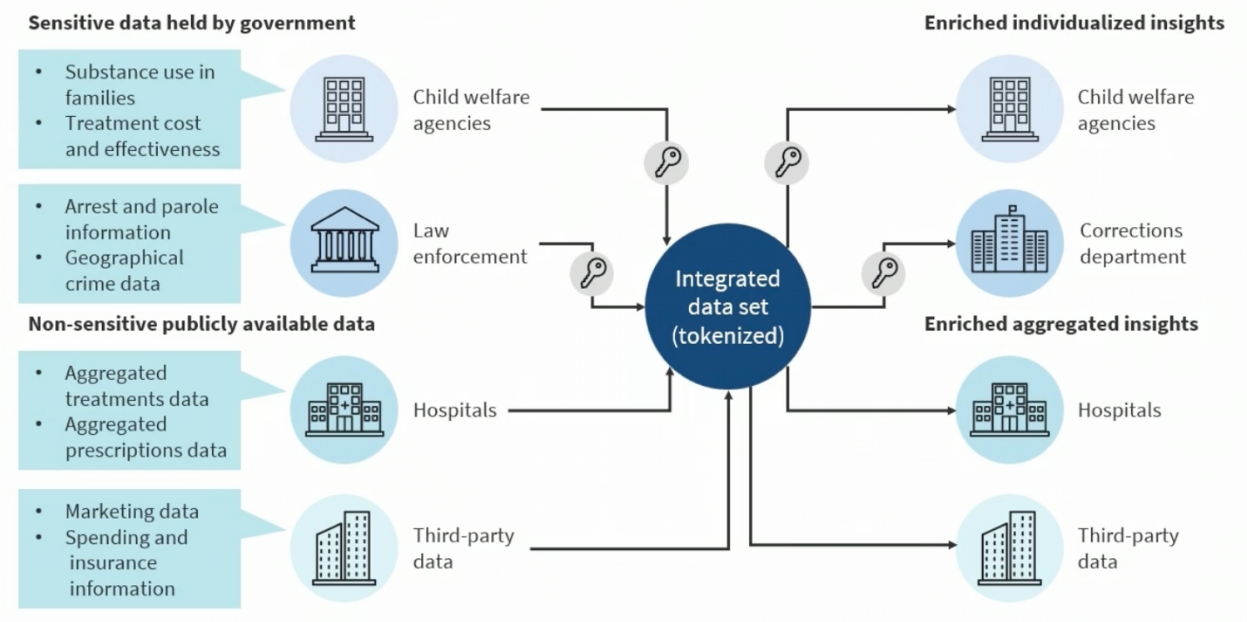
- Steganography is the process of hiding a secret message inside of (or even on top of) something that is not secret

- Tools like Steghide often involve embedding a secret piece of text inside of a picture or hiding a secret message or script inside of a Word, Excel, or PDF document
- It is a form of covert communication but not a form of cryptography because it doesn't involve scrambling data or using a key
- Steganography is a practice that enables secrecy and deceit

Data Masking

- Masking often involves using characters like "X" to hide some or all data
- For example, only displaying the last four digits of:
    - Social Security numbers
    - Credit card numbers
    - National ID numbers
    - Bank account numbers
    - Usernames or email addresses
- Methods to obfuscate data should prevent inference, and therefore, masking is suboptimal when compared to other methods like tokenization

Tokenization

- Tokenization involves sending sensitive data through an API call (or batch file) to a provider that replaces the data with non-sensitive placeholders called tokens
- The practice involves two distinct databases:
    - One with the actual sensitive data
    - One with tokens mapped to each chunk of data
- Unlike encrypted data, tokenized data is irreversible and unintelligible
- 

Blockchain Technology

- A blockchain is a distributed database that leverages a constantly growing list of ordered records called blocks
- These blocks are linked using cryptographic mechanisms
- Each block stores a cryptographic hash of the previous block, a timestamp, and transaction data
- Blockchain may be deployed as a public ledger (or private smart contract) consisting of a digital "chain of blocks" storing information

- Data can be read or written to the chain but not modified (immutability) – changes must be made to a subsequent block in the chain representing a pointer back to the original data
- Transaction data such as data, time, and amount is verified with a consensus mechanism (proof of work – POW, proof of stake – POS, etc.)
- The transaction participant's identities are based on digital signatures
- Unique cryptographic hashes are used to distinguish the blocks from each other

Blockchain Use Cases

- Cryptocurrencies and tokens
- Money and asset transfer ledgers
- Smart contracts
- Non-fungible tokens (NFTs)
- Government services
- Insurance claims (fraud prevention)
- Securities (stocks, bonds)
- Healthcare

Threat Actors and Vectors

Threat Actor Types and Attributes

Threat Actors (Agents)

- Without a threat actor or agent there is actually no threat
- Threat agents (or actors) are the persons, methods, operations, techniques, systems, or entities that act (or have the potential to act) with intent to initiate, transport, carry out, or in any way support a particular threat or exploit.
- Threats are not realized without an agent or catalyst
- Can be comprised of an individual or a group
- The attacks can also be totally automated (bots)

Some attacks are structured some are unstructured
Structured attacks

- Planned
- Organized
- Persistent
- Multi-phased/staged
- Can be internal or external
- Exploit kits, zero-days, modules, ransomware

Unstructured attacks (Can be internal or external – usually internal)

- Accidental
- Non-malicious
- Drive-by web surfing
- No acceptable use policy (AUP)
- Email and Webmail
- USBs and personal electronics

Unskilled Attackers (Script Kiddies)

- These originate from the combination of inexperienced crackers using script viruses and prepackaged malicious code (exploit kits and Malware as a Service (MaaS) campaign).
- Should be included in (every) risk analysis assessment
- The most common script viruses are spread via email attachments using preformed scripts and modules from exploit kits
- Newer techniques are often learned on YouTube and other social media sites in the dark web through ToR browsing
- These represent the lowest level of attacker sophistication and capability levels

Hacktivists

- Hacktivism unofficially began in the late 1980s when viruses and worms spread messages of protest (e.g. “Worms Against Nuclear Killers”)
- The term “hacktivism” was coined by the Cult of the Dead Cow, which also gave birth to “Hacktivism,” “a group of international crackers protesting human rights abuses
- They are responsible for DoS, DDoS, ransomware, hijacking and defacing websites, and other cyber-attacks to raise awareness

Organized Crime Syndicates

- Organized cybercrime is a well-funded, multi-billion-dollar-a-year industry that affects all sectors of government and the economy
- They are the main contributors to advanced persistent threats (APTs)
- They perform cost-benefit analysis and other research before carefully choosing targets
- The campaigns may last months or years
- Example: The ALPHV/BlackCat ransomware operation

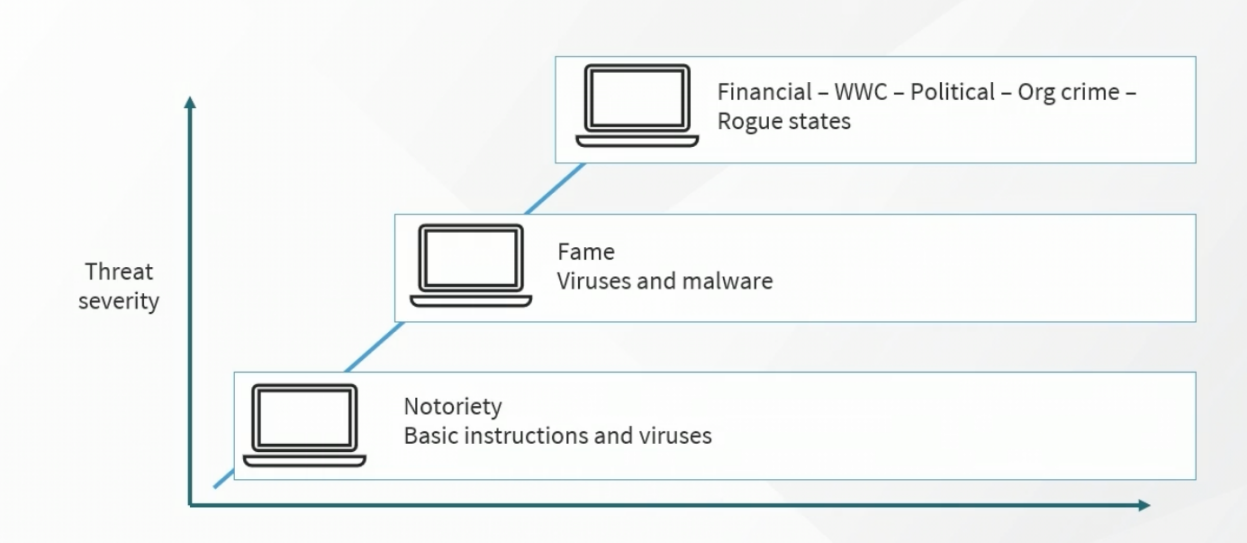
State-based Attacks

- Many security industry analysts and experts contend that the world has already entered a third world war in the form of a cyber war known as WWC (World War Cyber)
- The nation-state actor has a "license to hack" since they work for a government or military to disrupt or compromise target governments, organizations, or individuals to gain access to valuable data or intelligence
    - They might be part of a semi-hidden "cyber army" or "password crackers for hire" for companies that are aligned with the aims of a government or dictatorship
- They can create incidents and false flag operations that have international significance
- The nation-state actor has developed (along with criminals) many zero-day malware exploits that are waiting to be activated (e.g. a logic bomb)

Compromised Privileged Insiders

- These existing and recently released employees or contractors should be considered "public enemy number one"
- They can often have unfettered and elevated access and are the most likely to leave backdoors and other covert channels upon exit from the organization
- The term "compromised" is more accurate than "disgruntled" since there are several factors that can put an employee in a compromised position without being dissatisfied with the organization or other personnel

Intent and Motivation



-
- 80s and 90s – hackers and attackers conducted threats to get notoriety. Malware attacked basic instructions and viruses to attach executables. Based on popularity of attacks, with more elaborate malware and higher targets. Attacks became highly financial. Payloads got more valuable – threat severity went up – number of occurrence went up.

Threat Actor Motivations

- Data exfiltration for financial gain
- State-based or corporate espionage
- Service disruption
- Blackmail and extortion
- Political activism or ethical issues
- Revenge or act of war

Human Vectors and Social Engineering

The Dark Web
- The dark web is the veiled collective of Internet sites that are not indexed and are only accessible by a specialized web browser such as ToR, Freenet, or Subgraph OS
- It is considered a part of the deep web
- It is a vast repository of Malware as a Service (MaaS) campaigns and resources
- It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications
- While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity, such as purchases of contraband and child pornography

Phishing Attacks
- Email phishing attacks or hoaxes are one of the most common exploit vectors available to crackers
- Phishing is a cyber-attack that uses disguised email and webmail as a vector
- The goal is to trick the recipient into believing that the message is legitimate so they will click a link or download an attachment
- Common indicators are vague salutations, suspicious domains, wrong paths or hypertext, awkward grammar, urgency, lack of contact info, and spoofed headers/logos

Phishing Variants
- Spear Phishing is a select, targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. Often done to low level employees that are not trained well to identify malicious intent of the phishing attack
- Whaling is a spear phishing attack against high-level and highly privileged employees
- Smishing is using various text messaging formats (i.e. SMS) as a vector
- Vishing uses a voice over IP or telephony as the hoax vector

Business Email Compromise (BEC)
- Business email compromise (BEC) is a form of attack that targets companies that outsource, conduct wire transfers, and process invoices, often abroad
- It is often an elaborate advanced persistent hoax that targets corporate email accounts of high-level employees
- They are either spoofed or compromised through keyloggers or phishing attacks, often to perform fraudulent wire and cyber currency transfers
- Some attackers have successfully spoofed large vendors and customers, lawyers, CPAs, and even government officials (e.g. IRS)

Social Engineering
- Macro Term
- Eliciting information and reconnaissance

    - Shoulder surfing
    - Dumpster diving
        - Credential harvesting
    - Hoaxes and impersonation
    - Identity fraud and invoice scams
        - Pretexting using a fabricated story, or pretext to gain a victim's trust; brand impersonation
    - Disinformation and influence campaigns
    - Watering hole attacks – web based attack that goes against the low hanging fruit of a website (basic website – provided information, use it to attack website

Reasons for Social Engineering Effectiveness
- Lack of proper social and awareness training
- No buy-in from management and employees for prevention measures
- Outdated antivirus, DLP, and mobile device and application management tools
- Inadequate acceptable use policy (AUP)
- No enforcement of policies – no carrot and no stick
- Poor perimeter security controls for email, messaging, telephony, and web activities

Common Attack Surfaces
- Removable devices (e.g. USB)
- Vulnerable software (e.g. software downloaded or drive by websites or click through sites)
- Unpatched client-based and agentless services
- Default credentials (e.g. default passwords)
- Unsupported systems and applications (e.g. usb drive, type 2 hypervisor environment)
- Messaging and chat (e.g. phishing attacks)
- Social media (e.g. disinformation)
- Insecure network perimeters)
- Over-privileged users
- Open service ports

Supply Chain Vulnerabilities
- Software supply chain security continues to be a growing risk for organizations
- Experts predict this will only continue to rise, and damages could exceed 15% growth year-over-year for the foreseeable future
- Many organizations allow third-party organizations to have access to their networks and systems
- When an attacker exploits a vendor or partner, they can leverage this trust relationship to gain access to the organization's infrastructure
- Zero trust initiatives are a powerful countermeasure to supply chain vulnerabilities
- Could be
    - Managed service providers
    - Vendors
    - Suppliers
    - Service providers (ISPs, CSPs, SaaS)
    - Hardware providers
    - Software providers

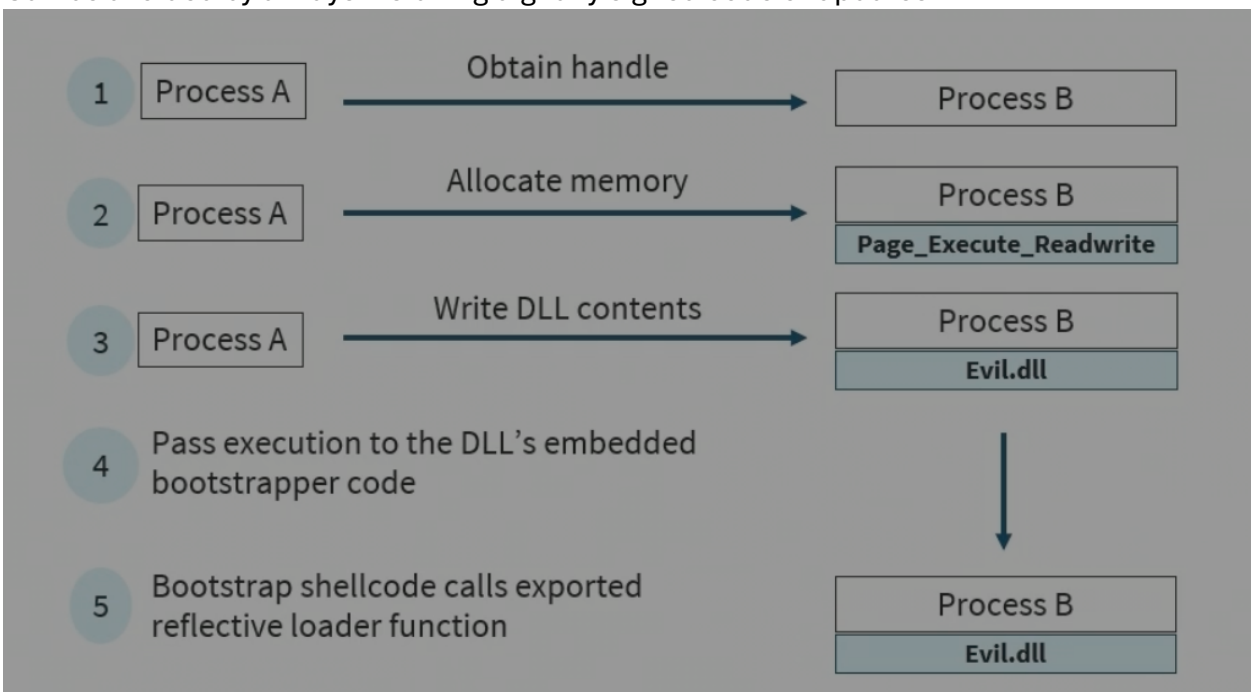
Application Vulnerabilities: Memory Injection
- Shellcodes are a small stub of code used as a payload – malware or memory attacks

- A DLL is a shared library of functions that multiple programs can access
- A process is an instance of a program being executed
- A threat is a small sequence of instructions or a component of a process
- Windows API protocols allow interaction with the Windows OS
    - VirtualAllocEx reserves or changes a region of memory
    - WriteProcessMemory writes data to an area of memory in a specified process
    - CreateRemoteThread creates a thread in the address space of another process

Application Vulnerabilities: Examples of Memory Injection

- Shellcode injects malicious code into a running application of PowerShell, which is regularly used in attempts to execute in-memory attacks
- Process hollowing starts a legitimate process whose sole purpose is to be a container for malicious code – it delivers the process in a "suspended" state, then rewrites the content with the required code in memory, and continues to execution
- Reflective DLL injection is where contents of a rogue DLL are loaded into memory

Reflective DLL Injection

- Can be avoided by always installing digitally signed code or updates
- 

Buffer Overflows

- In a buffer overflow attack, the attacker sends a larger-than-expected input
- For instance, when a front-end web server accepts it and writes it to memory areas
- Associated buffers are filled, and the adjacent memory is overwritten as a result
- This "overwrite" may contain malicious instructions or code that crash the server or runs a persistent remote access trojan

OS-based and Web-based Vulnerabilities

- One of the most prevalent misconfiguration habits is leaving debugging features enabled in production environments – operating systems and web based applications
- It is critical to make sure that debugging functionality is disabled or properly secured in production environments

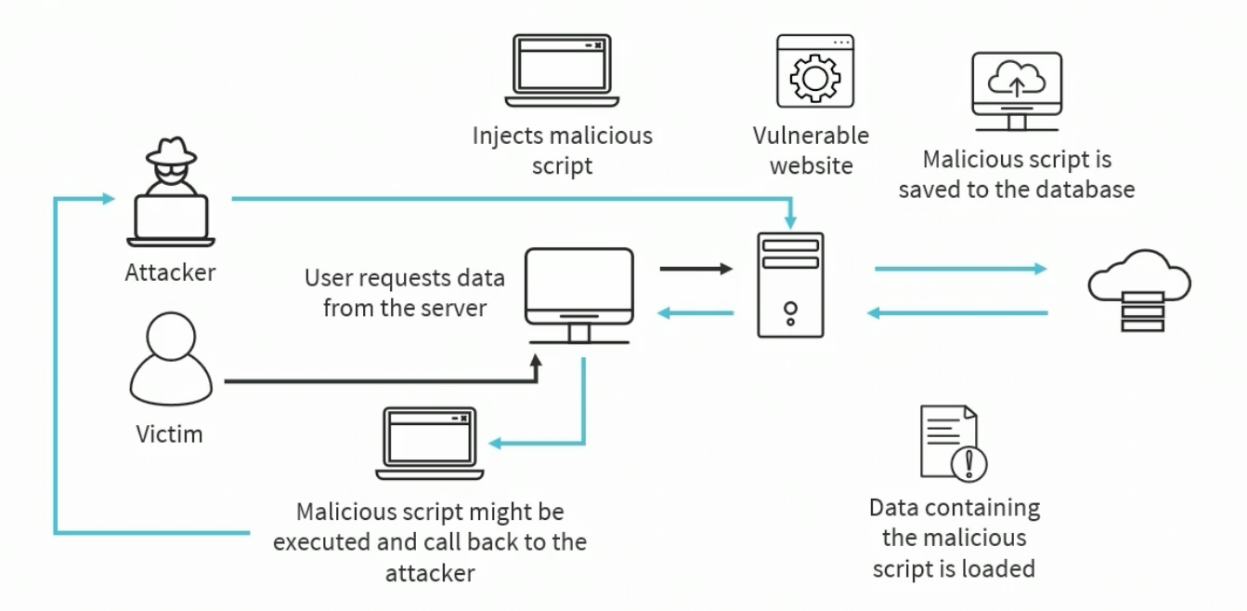
- Another common misconfiguration comes from the use of default or weak credentials for various system components such as operating systems, databases, network devices, or application interfaces
- All systems should use tested patch management

SQL Injection (SQLi)

- This common attack has been run against front-end services like web servers and Microsoft SharePoint that use SQL as a database repository
- It involves inserting a SQL query through input data from client-to-server applications:
    - Read sensitive database data (SELECT FROM)
    - Change database data (INSERT, UPDATE, DELETE)
    - Execute administrative functions (e.g. shut down DBMS)
    - Get the contents of files on a database management system (DBMS)
    - Run commands on an operating system

Cross-site Scripting (XSS)

- Flaws in pages rendered by web servers and not the web server code itself (i.e. Apache, IIS) where malicious scripts or code are injected into trusted or innocent website pages
- Malicious scripts can steal cookies, session tokens, or other sensitive data stored by the browser and used with the site
- Attacker typically sends browser-side scripts to end user
- Can occur anytime a web program uses user input within the output it generates without validating or encoding



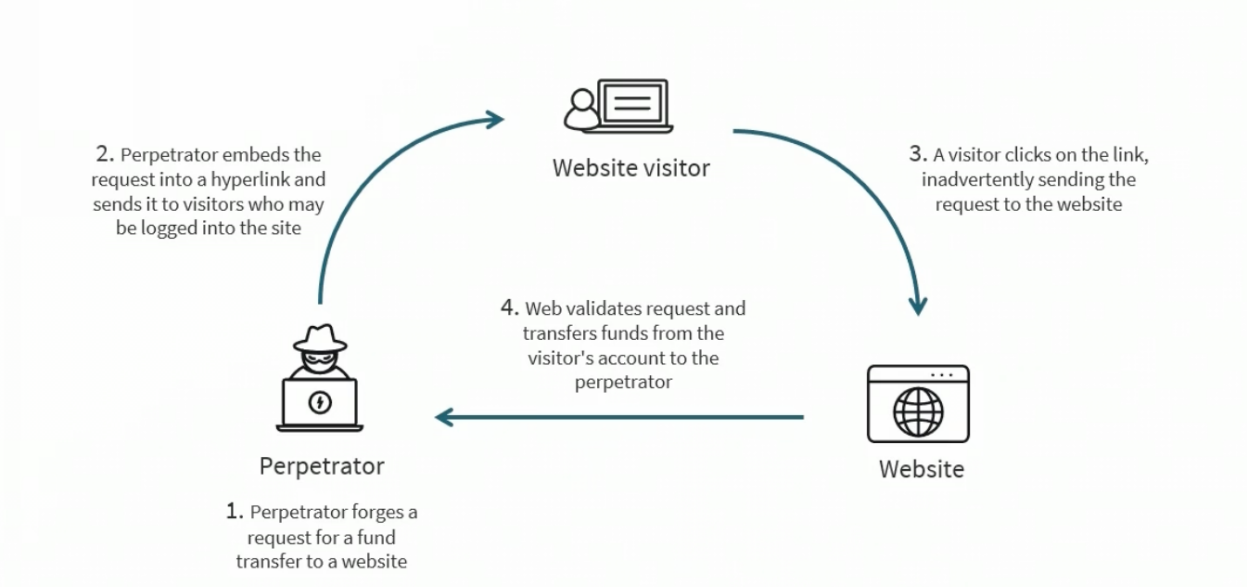
-
- Attacker injects the script onto pages rendered by the vulnerable website/application. If persistent the script is saved to database, then when the user requests data from the server the data is loaded and script is loaded and is then called back to the attacker or sent to the victim which is sent to the attacker.

XSS Variants

- DOM-based is also called local XSS or type 0
    - It does not involve vulnerable web servers but rather insecurely written HTML pages on the end user's system or local gadgets and widgets (Widgets – Apple, Nokia, Yahoo; Gadgets – Microsoft and Google

- Reflected XSS (Nonpersistent or Type 1)
    - This is a classic input trust vulnerability where the application is expecting some input (i.e. a query string), and the attacker sends something the developer did not expect
- Stored XSS (Persistent or Type 2)
    - This is a variant of type 1 where, rather than reflecting the input, the web server persists the input
    - The difference is an intermediate phase where the untrusted input is stored in a file or a database before unloading on the victim – often found in blogs and review/feedback web application

Cross-site Request Forgery (CSRF/XSRF)

- Attacks force an end user to perform undesirable actions in a web application in which they are authenticated
- An effective CSRF/XSRF attack can force users to perform state-changing requests
    - Transferring funds
    - Changing their email address
    - Changing their password
    - If the victim is an administrative account, the CSRF attack can compromise the entire web application
- 

Hardware and Virtualization Vulnerabilities

Hardware Vulnerabilities

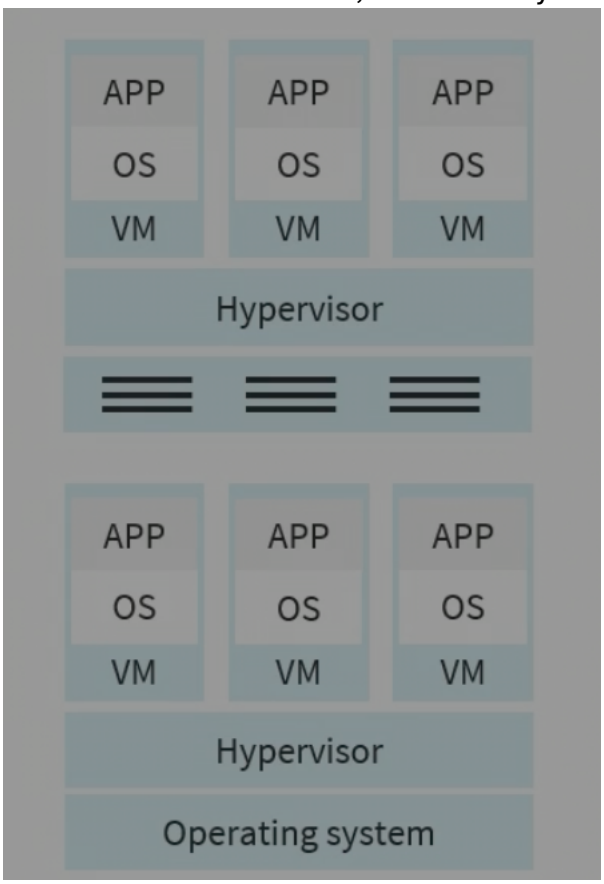
- Some of the dominant factors that contribute to vulnerabilities and flaws in hardware are
    - Vendors going out of business
    - Original equipment manufacturers (OEMs) cutting corners
    - Product becoming end-of-support and/or end-of-life with few or no alternatives
    - The usage of outdated and legacy systems
    - Unsecure and unsigned device drivers

Firmware Vulnerabilities

- Firmware is software that is embedded within hardware devices and provides low-level control and functionality

- Some firmware can be remotely reprogrammed and may be accessed by attackers through remote code execution (RCE)
- Common firmware exploits are authentication bypass, buffer overflows, and injection flaws
- The rapid emergence of the internet of things (IoT) and smart devices has introduced more security vulnerabilities

Hypervisors

- Common hardware and software solution
- The virtual machine manager software system that runs and controls virtual machines
- It allocates and shifts resources as well as manages the interaction between the VMs and the hardware
- Type 1 – bare metal or native
    - Runs directly on the underlying hardware
    - XenServer, KVM, Hyper-V, ESXI
- Type 2 – hosted
    - Runs on the OS installed on the hardware
    - Oracle VirtualBox6, VMWare Player/Workstation, UTM
- 

Hypervisor Vulnerabilities

- VM sprawl – involves having no centralized control of hypervisors and virtual machines
- VM hopping – when administrators do not enforce the partitioning of guests from each other
- VM escape – a flaw in the hypervisor that allows a guest to access the underlying hypervisor or even the hardware that it runs on
- Hyperjacking – a scenario where a privileged insider installs malware, such as a rootkit, on the hypervisor to conduct unauthorized activities

The Cloud Security Alliance (CSA) Treacherous 12

- The Treacherous 12 – Cloud Computing Top Threats report plays a vital role in the CSA research ecosystem
- The goal of the report is to offer organizations an up-to-date, expert-informed understanding of cloud security issues so that educated risk management decisions can be made concerning cloud adoption strategies
- The report reflects the current consensus among security experts in the CSA community about the most significant security issues in the cloud

The CSA Treacherous 12

1. Data breaches
2. Weak identity, credential, and access management
3. Insecure APIs
4. System and application vulnerabilities
5. Account hijacking
6. Malicious insiders
7. Advanced persistent threats (APTs)
8. Data Loss
9. Insufficient due diligence
10. Abuse and nefarious use of cloud services
11. (Distributed) Denial of service
12. Shared technology vulnerabilities

Mobile Device Vulnerabilities

- There are several classic vulnerabilities with mobile devices – most of which have been addressed with vendor updates
- Side loading, in the context of smartphones, involving installing a compatible app for an Android or iOS device that is not available, approved, or at least monitored and maintained by your device platform's official app store
- Jailbreaking is the act of exploiting the flaws of a locked-down electronic device (iPhone) to install software other than what the manufacturer has made available for that device
    - It allows the device owner to gain full access to the root of the operating system and access all the features
- Rooting is the process of unlocking usually an Android smartphone or tablet
    - A rooted device gives the user much more freedom to customize the device and achieve more administrative control

Enterprise Mobility Management (EMM)

- Organizations should employ the most robust authentication mechanisms feasible (biometrics, QR codes, trusted platform modules)
- This is accomplished through enterprise mobility management initiatives
    - Mobile device management (MDM)
    - Mobile application management (MAM)

Survey of Malicious Activities

Malware Attacks

- All security incidents can be considered an exploit, but not all exploits involve the usage of delivery of a malicious software (malware) payload
- A malware attack is a common cyberattack where malware (typically malicious software) executes unauthorized actions on the victim's system
- The malicious software (AKA virus or worm) encompasses many different types of attacks such as ransomware, spyware, command and control, and more
- Like other types of cyber-attacks, some malware attacks end up with mainstream news coverage due to their severity
- An example of famous malware is the WannaCry ransomware attack

Ransomware

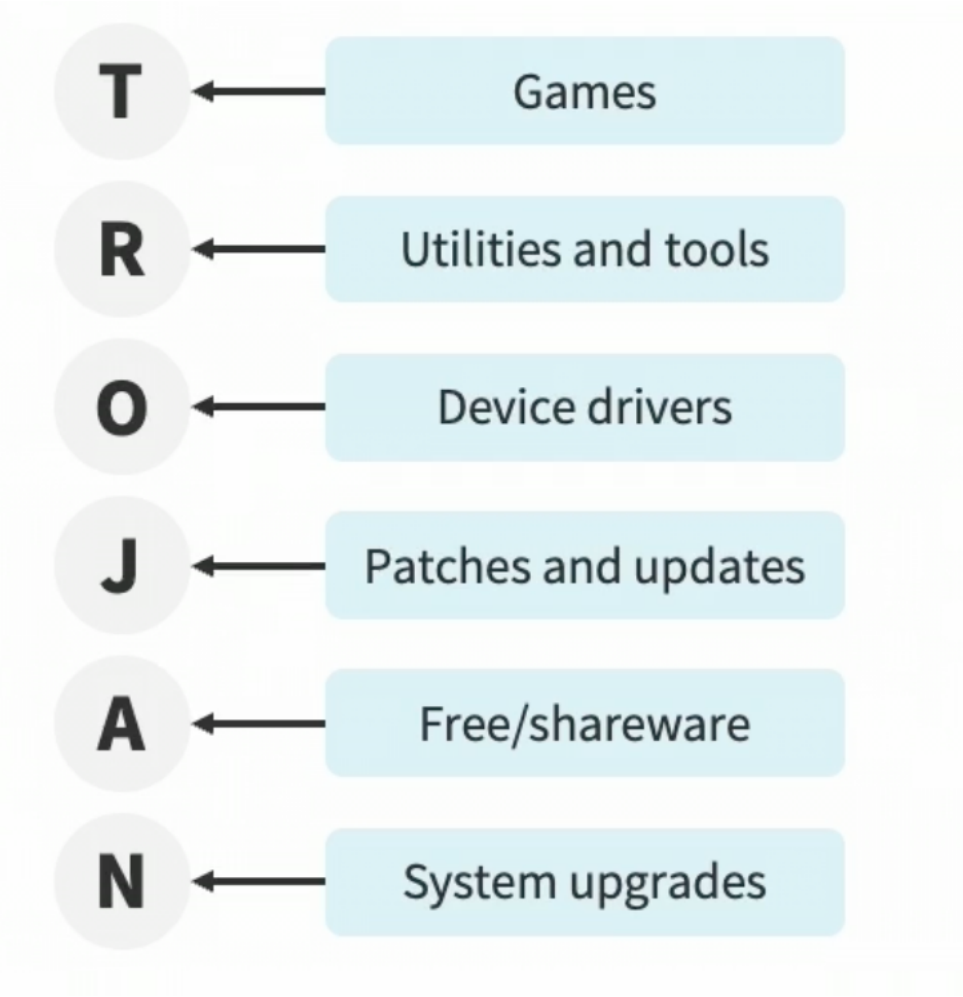
- This is a popular form of malware that encrypts key files and holds them for "ransom"
- Usually committed for cryptocurrencies such as Bitcoin (over 90%) or Monero
- Ransomware evolved from misleading "fix" apps to fake AV tools and bogus "fine" websites
- The average ransom demand has more than doubled since 2020
- Over 30% of victims are in the U.S
- The newest trend is Ransomware as a Service (RaaS) on the dark net, which is a subset of Malware as a Service (MaaS)

Ransomware Campaign

1. Installation (Crypto-ransomware installs itself after boot up (email, drive by website, trojan, USB))
2. Contacting headquarters (Malware Contacts a server belonging to an attacker or group)
3. Handshake and keys (The ransomware client and server "handshake" and the server generates two cryptographic keys)
4. Encryption (The ransomware starts encrypting every file it finds with common file extensions – documents folder example)
5. Extortion (A screen displays, giving a time limit to pay up before the criminals destroy the key and decrypt the files)

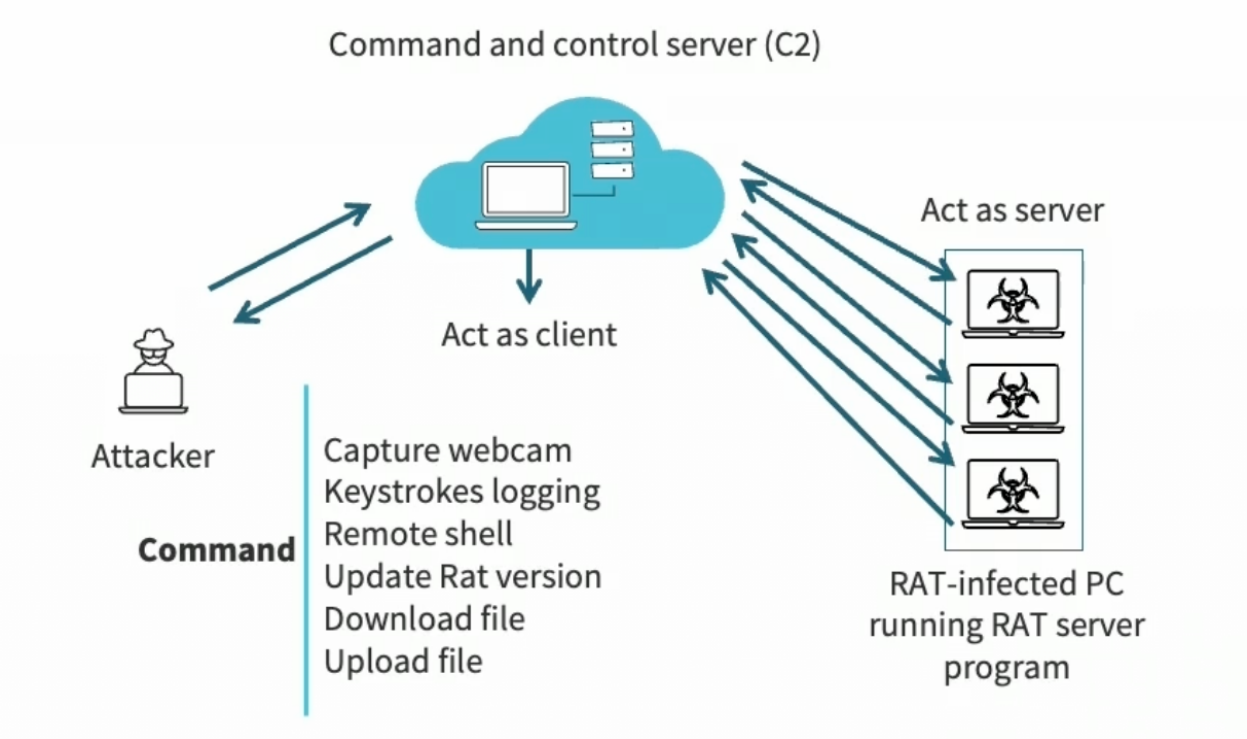
Trojans

- Trojans are malicious code and programs that masquerade as legitimate applications or are embedded in real programs
- Trojan horses have no replicating abilities like viruses or worms
- They can either be a re-named benign program or the trojan code can exist in an operable application
- Trojans can also be part of a more elaborate distributed denial-of-service or botnet attack

- 

Remote Access Trojans (RATs)

- Remote access trojans (RATs) are a variant of trojan malware engineered to permit an attacker to remotely control an infected computer
- Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response
- The server can be command and control server that is part of an automated botnet



-

Viruses

- A computer virus is a type of malware that spreads between computers and causes damage to data and software
- Viruses are distinctive in that they typically attach to executable files to disrupt systems, cause major operational issues, and result in data loss and leakage
- The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments

Worms

- Worms are a special form of self-replicating virus (malware) that generally spreads without user action
- They distribute complete copies (possibly modified) of themselves across networks
- A worm can consume resources, infiltrate data, or simply cause the CPU on the system to waste cycles, resulting in a computer becoming unresponsive

Spyware and Bloatware

- Spyware is often defined as malware intended to penetrate a device, collect personal data, and then send it to a third party without permission
- Spyware can also refer to legitimate software that monitors data for commercial purposes like advertising
- Technically speaking, practically all smart devices and IoT components are spyware
- Bloatware is unwanted and potentially harmful software preloaded onto new devices
- It is preinstalled by vendors, manufacturers, or carriers as a form of marketing to put services directly in front of customers

Keyloggers

- Keystroke logging is typically done by malicious code that records keystrokes and sends data back to command and control (C2C/C&C) servers
- Spyware uses keyloggers to capture passwords, credit card information, or other PII

- Software can also be used to track employees or family members to adhere to acceptable uses
- Keylogger detectors are special mitigation tools
- Examples: PAL KeyLogger Pro and KeyGhost

Rootkits

- Rootkits are a type of malware that can give a threat actor control of systems user consent or knowledge
- “Root”, “Admin”, “Superuser”, or “System Admin” are all interchangeable terms
- They are dangerous because they are designed to hide their presence
- A threat actor who has placed a rootkit onto a machine (often via phishing email) can remotely access and control it to deactivate the antivirus software, spy on activities, steal sensitive data, or execute other malware. Examples of this is hijacking a hypervisor in a data center

Logic Bombs are Triggered by Events

- Mouse movement or code execution
- Data/time of a major event
- File access
- Number of times code is run
- A national holiday

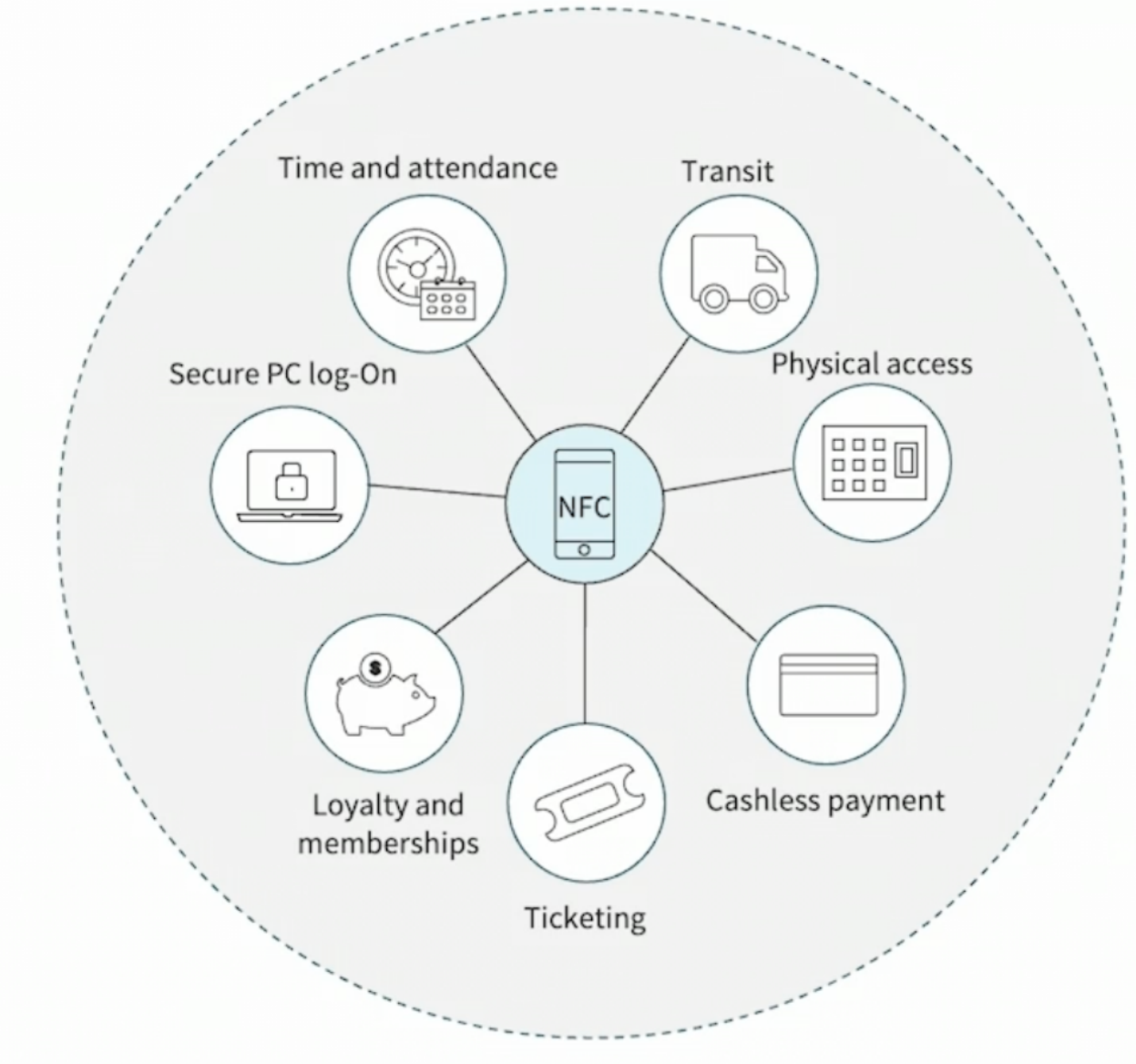
Physical Attacks

- Safes and other containers are rated based on the amount of time a tool would take to penetrate with brute force
- Doors and windows of all types are also common targets of brute force attacks
- Although considered a preventative mechanism, locks are a delay component since all could be overcome by brute force

RFID Cloning

- RFID (Radio frequency identification) and NFC (Near field communication) devices are vulnerable to a variety of physical attacks
- Crackers can clone credit and debit cards by stealing the name, account number, expiration date, and 3-digit code
- Data stored on RFID chips can be stolen, skimmed, and scanned by anyone with easily obtained RFID readers
- Skimming uses devices that overlay an ATM or point-of-sale scanner to steal the information from the victim

-



Environmental Attacks

- Any environmental system that is not air-gapped can be compromised
- Many systems and sensors are “smart” or remotely accessible with IP
- They can be hacked to shut down systems, overload them, and hijack to change temperature or humidity
- If the environmental system connects to other networks, they can represent potential backdoors
- There should be a zero trust policy and high visibility when considering these critical systems

Denial-of-Service Attacks (DoS)

- A denial-of-service (DoS) attack happens when a malicious cyber threat actor prevents legitimate subjects from accessing information systems, infrastructure devices, or other network resources
- Affected services include email/webmail, websites, personal cloud storage, online accounts (e.g. banking), or other services that depend on a server or network
- A denial-of-service condition is accomplished by flooding the targeted host or network with traffic (i.e. ICMP, TCP, UDP) until the target cannot respond or simply crashes, preventing access for legitimate users

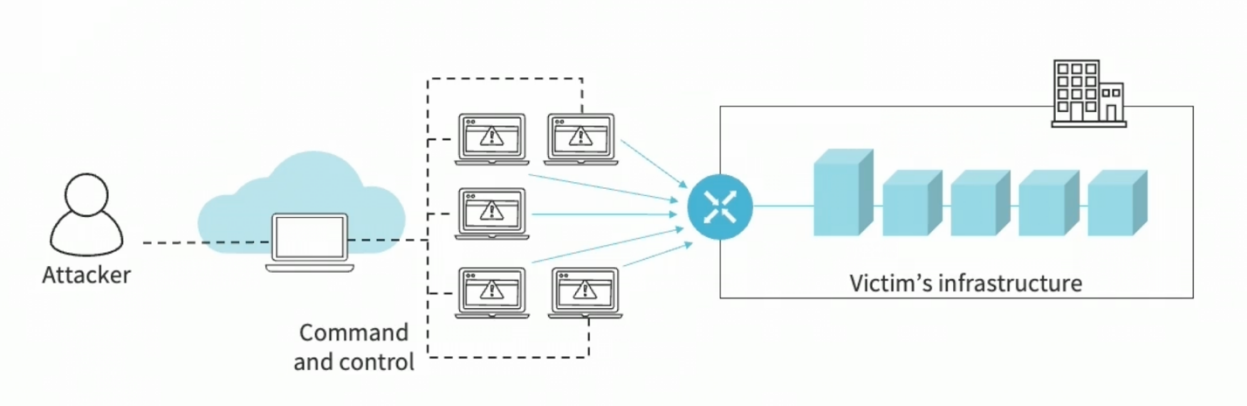
Distributed Denial-of-Service (DDoS)

- DDoS floods a server with internet or internal traffic to prevent users from accessing connected online services and sites
- Some attacks are launched by hacktivists overloading an organization's servers to make a statement or express displeasure
- Other DDoSs are financially motivated by competitors or involve extortion, in which perpetrators attack a company and install ransomware on their servers
- The most common form of DDoS attack is robot networks (botnets)

Botnets

- The most common form of distributed denial-of-service (DDoS) attack today
- The robot network (botnet) consists of a zombie computer and a master command and control server to remotely control victims, and many victims are unaware
- The communication often occurs over Internet Relay Chat (IRC), encrypted channels, bot-centric peer-to-peer networks, and even social media
- Bots can exfil data, log keystrokes, scan memory, force a system to participate in mining cyber currency, and more

DDOS Botnets



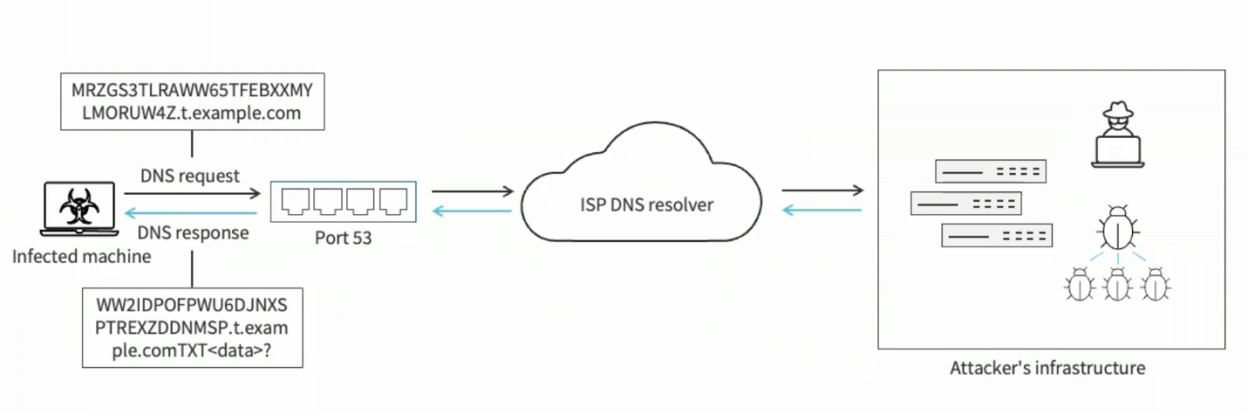
-
- Attacker is penetrated victim infrastructure (e.g. captured VPN connection). Zombie devices are the targets and they can communicate directly to command and control centre or intermediary bots on DDoS botnet

DNS Attacks

- More of the unsecure services or protocols of layer 7 in the TCP Stack
- DoS and DDoS
    - Attacker targets the root or down-level DNS servers to overwhelm the systems with a large amount of UDP queries
- Cache Poisoning
    - Attacker attempts to modify the DNS cache in the wrong way so that all DNS requests return an incorrect response
- DNS hijacking
    - Similar to poisoning the attacker often sets up a cloned site to redirect hijacked users to steal data or deliver malware.
    - If the DNS hijack sinks into a website it is also called pharming
- DNS spoofing
    - An attacker will represent a domain name and IP mapping to trick users or poison caches
- NXDOMAIN attack

    - Attempts to make servers disappear from the Internet by flooding the DNS server with requests for invalid or nonexistent records
- DNS flooding
    - This is considered a variant of the UDP flood attack, since DNS servers rely on the UDP protocol for name resolution
- Amplification attack
    - A reflection-based DDoS attack in which an attacker leverages the functionality of open DNS resolvers to overwhelm a target server or network with an amplified amount of traffic
- DNS tunneling
    - Exploits the DNS protocol to tunnel malware and other data by registering a domain server that points to the attacker's server, where a tunneling malware program is installed

DNS Tunneling



-
- Attackers infrastructure (command and control server). Have their own ISP DNS resolver and they infect machines with malicious DNS req and res on port 53. The information is tunneled within the request and response.

Wireless Attacks

- Attacks can be conducted on wireless networks but there are specific wireless attacks. Wireless has four MAC addresses and three types of packets (data, management and control)
- Rogue access points and evil twins spoof real wireless LAN devices. The difference between rogue and twin is twin access point is masquerading as the same platform and operating system as the access points being used (attacker done recon, and deploying same exact access point).
- DHCP starvation uses up real leases so that a rogue server can be introduced
- Attacks target management and control frames (disassociation or de-authentication) used for roaming devices
- On-path attacks used to be called man-in-the-middle, where rogue devices inject into TCP connections and other communications
- Jamming is a form of denial-of-service attack towards access points (Aps) and wireless controllers

Credential Replay

- A credential replay attack (whether wired or wireless) involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of generating an unauthorized effect or gaining unauthorized access. This is easier for an attacker in a wireless network.
- Attackers will also perform other reconnaissance attacks, dumpster diving, and various social engineering to harvest the internal usernames of an organization

SQL Injection (SQLi)

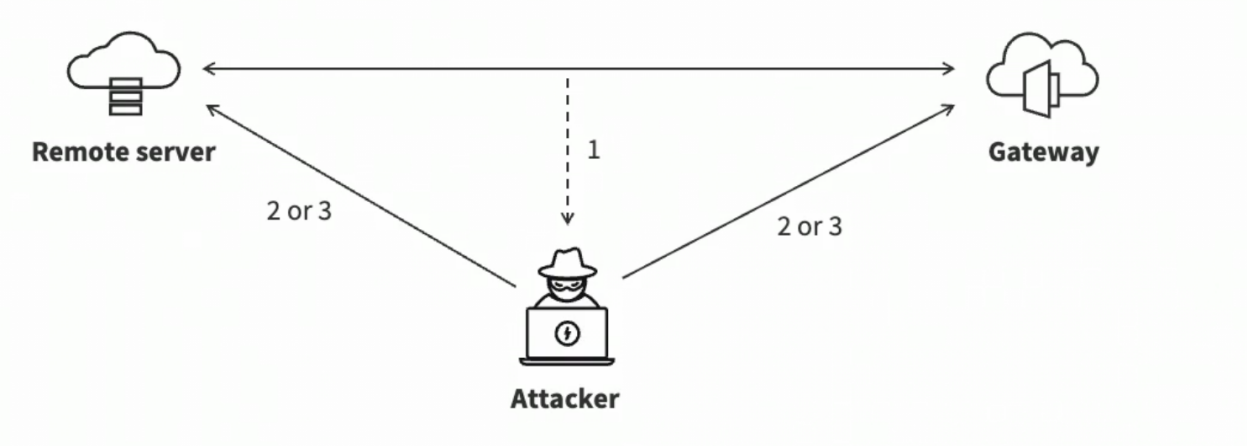
- Involves inserting a SQL query through input data from client to server application and can allow for several exploits
    - Read sensitive database data (SELECT FROM)
    - Change database data (INSERT, UPDATE, DELETE)
    - Execute administrative functions (e.g. shutdown DBMS)
    - Get the contents of files on a database management system (DBMS)
    - Run commands on the operating system

Buffer Overflows

- The buffer overflow attacker manipulates coding errors to compromise affected applications running on critical servers (e.g. email servers)
- It changes the program's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data
- It usually involves violating programming languages and overwriting the bounds of the buffers they exist on when code:
    - Is reliant on external data to control its behavior
    - Is dependent on data properties that are enforced beyond its immediate scope
    - Is so complex that programmers are not able to predict its behavior accurately

Replay Attacks

- This was possible before the introduction of modern firewalls
- A replay attack happens when an attacker snoops/sniffs on a secure network communication, intercepts it, and then deceptively delays or resends it to misdirect the receiver into doing what the cracker wants
- The added challenge of replay attacks is that a script kiddie does not need advanced skills to decrypt a message after capturing it from the network
- The attack could be successful simply by resending the entire communication



-
- Attacker places itself between the gateway and remote server or service
    1. Attacker sniffs the packets exchanged between the gateway and the remote server
    2. Attacker replays sniffed packets at a different time interval or based on the window size -> can be launched at the remote server or gateway
    3. Attacker modifies and sends sniffed packets or forges new packets

Privilege Escalation

- Attackers exploit human misconfiguration, design flaws, or omissions in web applications

- This is closely related to lateral movement – tactics by which an attacker moves deeper into a network looking for sensitive assets
    - The result is an internal or external user with unauthorized system privileges
- Depending on the extent of the attack, bad actors can do minor or major damage
- It might be a simple unauthorized email or a ransomware attack on vast amounts of data

Forgery and Directory Traversal Attacks

- Cross-site request forgery (CSRF) is an attack that tricks authenticated users into inputting a request to a web application
- CSRF attacks exploit the trust a web application has in an authenticated user
- It exploits a vulnerability in a web application if it cannot differentiate between a request generated by an end user and a request generated by a user without their consent. The higher the user's privilege is the more damage that can be done
- Directory (or path) traversal (or climbing) is a type of HTTP exploit where the attacker leverages the web server software to access data in a directory other than the server's root directory
- The threat agent, usually a browser, can view restricted files or execute commands on the server
- Any server that fails to validate input data from web browsers is vulnerable to a directory traversal attack

Cryptographic Downgrade Attack

- In a downgrade attack, the attacker attempts to force two hosts on a network (typically a browser and web server) to use an insecure or weakly protected data transmission protocol
- The downgrade is often HTTP instead of HTTPS or SSL instead of TLS
- If a downgrade attack is successful, the attacker can exploit connection vulnerabilities to intercept and read transmitted data
- It is considered a type of on-path

Collision Attacks

- To be considered trustworthy, a cryptographic hashing mechanism must be "collision-resistant"
- This means that two different inputs should never produce the same fingerprint or digest
- This collision can then be exploited by any application that compares two hashes together, such as password hashes, file integrity checks, and others
- MD5 is no longer considered collision-resistant

Cryptographic Brute Force Attacks

- A brute force attack, also known as an exhaustive search, is a cryptographic hack that depends on guessing all possible combinations of a targeted password until discovered
    - If the password is weak, it could take mere seconds with hardly any effort
- A brute force attack is time and processor-intensive and may be impossible or absurd from a physics standpoint
- It can also relate to trying all possibilities in a cryptosystem keyspace, which is why the larger bit size or modulus is preferred

Side Channel Attacks

- A side channel attack is enabled by leakage of information from a physical cryptosystem such as a smart card or cryptoprocessor
- Attributes that can be exploited in a side-channel attack, including timing, power consumption, and electromagnetic and acoustic emissions
- Wireless WPA3 had an early side-channel vulnerability in its Dragonfly protocol

Types of Password Attacks

- Dictionary Attack
    - Most people use weak and common passwords, Taking a list of words and adding a few permutations (e.g. substituting $ for s) which enables a password cracker to learn a lot of passwords very quickly
- Brute-force guessing attack
    - There are only so many potential passwords of a given length. While slow, a brute-force attack (trying all possible password combinations) guarantees that an attacker will crack the password eventually
- Hybrid attack
    - A hybrid attack mixes these two techniques. It starts by checking to see if a password can be cracked using a dictionary attack, then moves on to a brute-force attack if it is unsuccessful
- Password Spraying Attack
    - Type of brute force attack. In this attack, an attacker will brute force logins based on a list of usernames with default passwords on the application. For example, an attacker will use on password (e.g. Secure@123) against many different accounts on the application to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. Credential harvesting (for the users) then spraying with common passwords/credentials

Password Cracking Tools – Examples

- Hashcat
- John the Ripper
- Brutus
- Wfuzz
- THC Hydra
- Medusa
- RainbowCrack
- OphCrack
- Aircrack-ng (Wireless password cracker

Indicators of Compromise (IoCs)

- These a network or host-based cyber observables
- Forensic artifacts of an incursion or disturbance
- A measurable event or stateful property in the cyber domain
- Registry entries, files on disk and in-memory, etc.

Indicators of Compromise

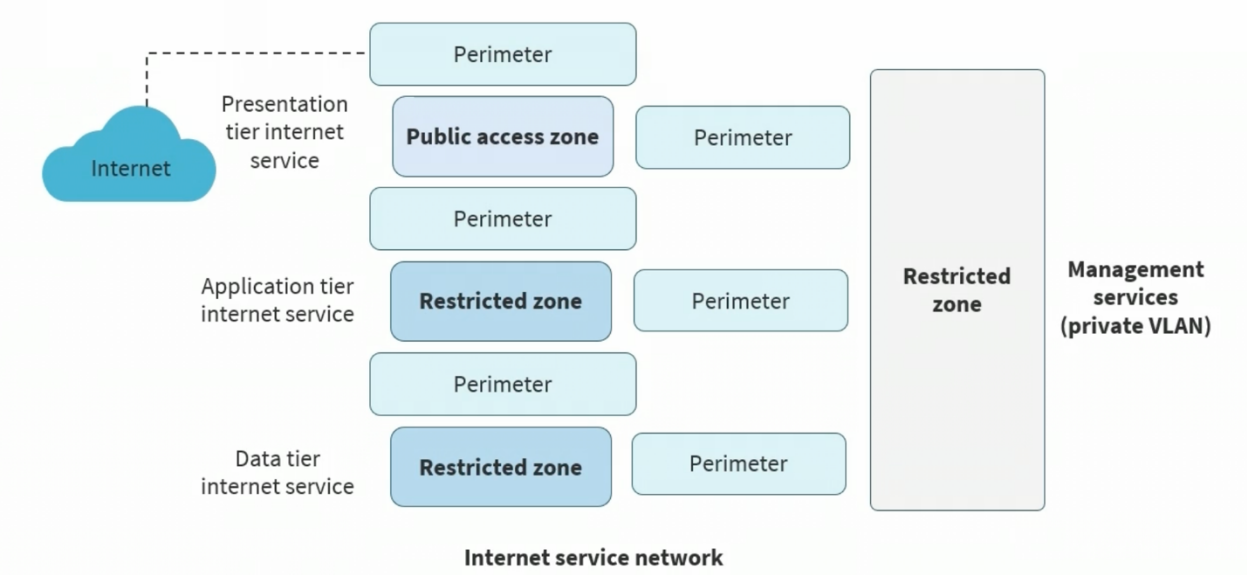
- Account lockout
- Concurrent session usage
- Blocked content
- Impossible travel
- Resource consumption
- Out-of-cyber logging
- Missing logs

Mitigation Techniques

Segmentation and Isolation

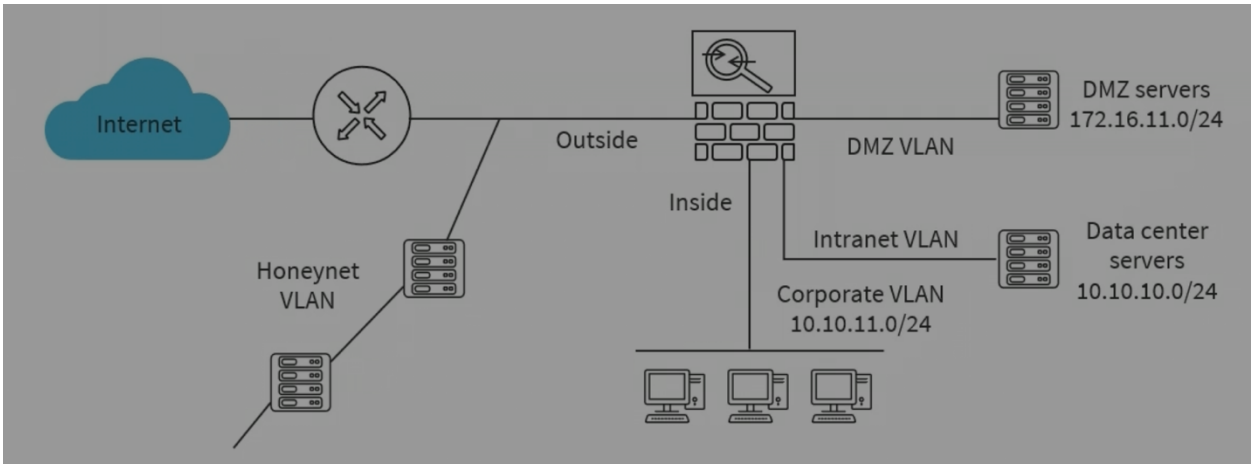
- Segmentation divides a computer network or any other system into smaller parts
- The purpose is to improve network performance and security
- Other terms that often mean the same thing are network segregation, network partitioning, and network isolation
- Segmentation and isolation are logically and physically accomplished in network infrastructures using zoning
- Zoning (segmentation) is a logical design approach used to control and restrict access
- Each zone has fundamental characteristics defined by the security:
    - Every zone contains one or more separate, routable networks
    - Every separate, routable network is contained within a single zone
    - Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs)
    - The only zone that may connect to the public zone (other works ISP or ITSP (internet and voice over IP in WAN or LAN)) is the public access zone (PAZ) (DMZ)

Logical Zoning



- Here we see a public access zone connecting through a perimeter to the internet via a ISP. The zone interface point will be a router (highly available – two or a cluster). The presentation tier which is a public access zone. If it connects to a management VLAN it will have its own perimeter and zone interface point. Zone interface point can be between two zones (firewall that has a interface in the restricted VLAN zone). In this design it has a application and data tier. Its just segmented

Physical/Logical Zoning



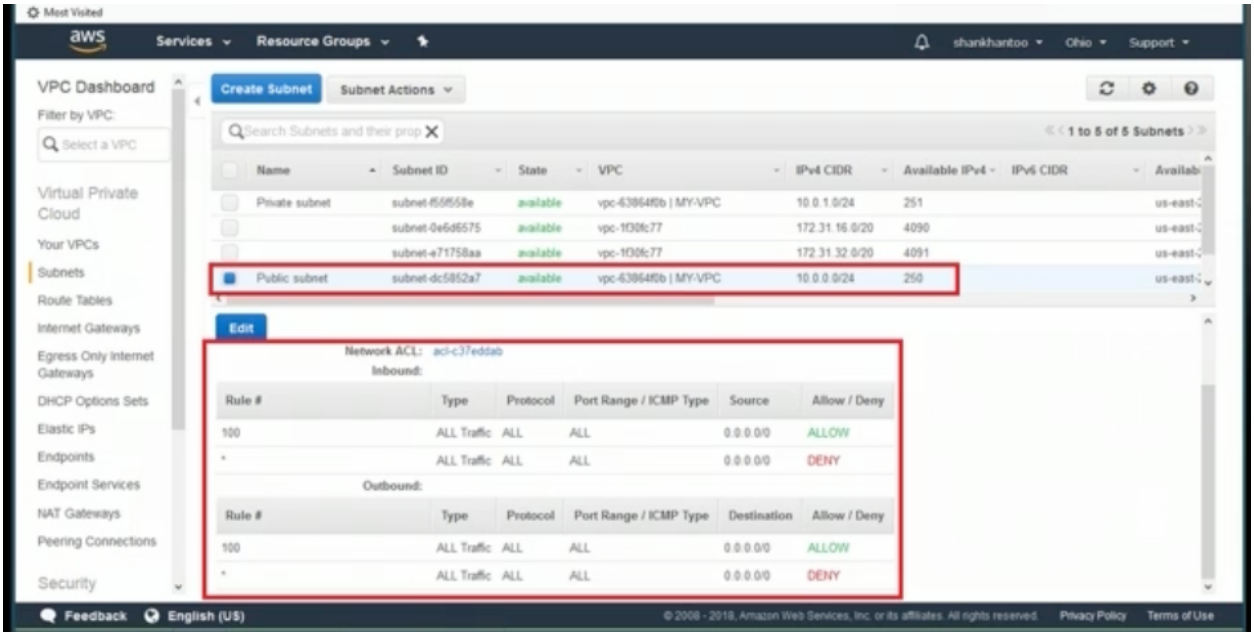
-
- Have the internet (ISP or Cloud provider) then customer premise equipment (high end router or firewall appliance). Common to deploy honeynet VLAN (between perimeter device and firewall). Intrusion prevention system (IPS) should be behind the firewall either physically or logically. The IPS sensor only acts on traffic that has gone through the firewall that has been allowed, it is meant to catch it. Have DMZ, intranet and corporate VLAN. The DMZ VLAN is serving the outside untrusted internet.

Access Control Lists (ACLs)

- Allow stateless (static) traffic filtering and management of IPv4 and IPv6 traffic to and from a network interface or virtual local area network (VLAN)
- Contain ordered rules or access control entries (ACEs) to permit (allow) or deny (block) based on Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) services and ports, as well as Internet Control Message Protocol (ICMP) messages and codes
- Function as additional infrastructure defense-in-depth mechanisms
- Have an implicit deny-all as the last entry applied if nothing matches

Network Access Control Lists (NACLs)

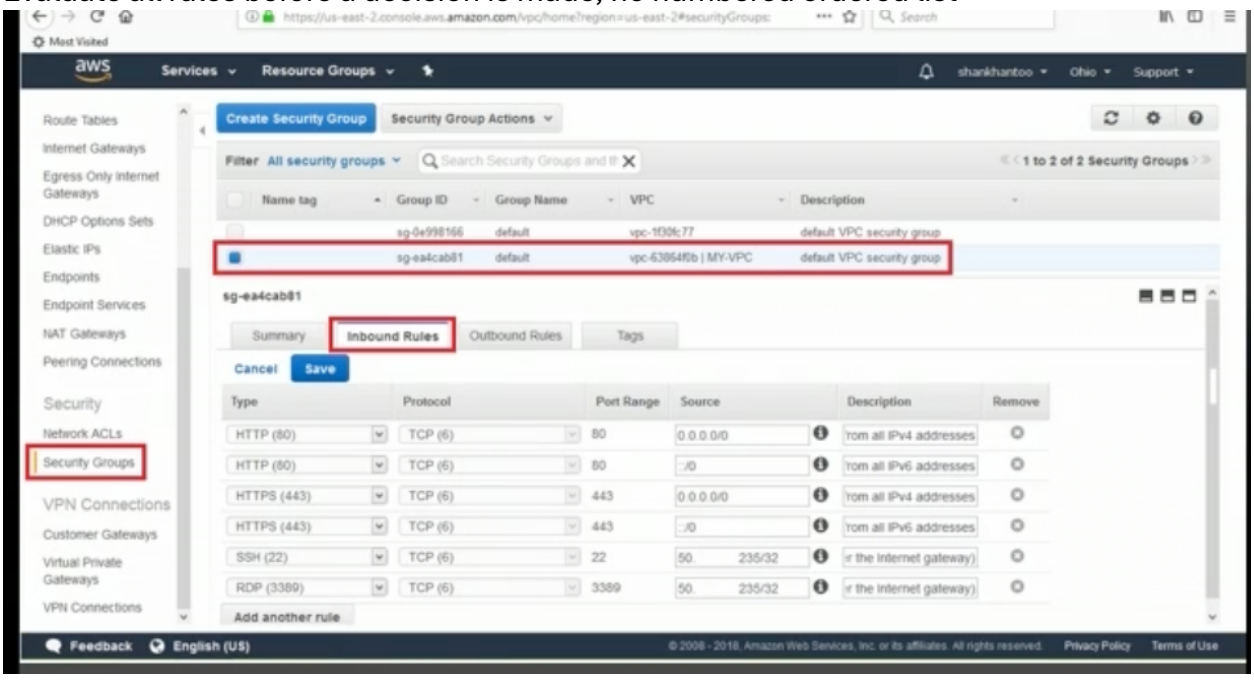
- Used by Cloud Services
- Are most often static inbound or outbound access lists applied to virtual networks or virtual private clouds
- Apply to all instances, containers, appliances, etc. in the virtual network (VNet)
- Are typically configured with the same techniques as traditional access lists



- In this screenshot all traffic and ICMP, TCP, UDP type is allowed. NOT GOOD
- To activate this access control list you would replace the top 100 line with traffic allowance that will allow certain traffic only and at the end deny all (*).

Security Groups

- Are commonly stateful “allow-list” firewalls that apply to layer to layer 3 and layer 4 network traffic
- Can be applied to a virtual load balancer and instance virtual interface:
    - These operate at the hypervisor level attached to the virtual elastic network interfaces (eth0)
- Are called network security groups (NSGs) if applied to an entire virtual network
- Have no explicit deny rules like NACLs, but rather have an implicit deny if nothing matches the “allow-list”
- Evaluate all rules before a decision is made, no numbered ordered list



- Security groups allowing rules. No numbers. No allow or deny column. Everything in the allow list is allowed with an implicit deny. Since no ordering everything is considered before decisions are made

Permissions

- Permissions that principals have can be dictated and enforced by the network operating file system (Linux or Windows) or using a directory service as in:
    - Read (r) permission to access the file's contents
    - Write (w) permission to modify or change the contents of a file
    - Execute (x) permission to execute the contents of a file
- One can change a Linux file and directory permissions with the chmod command, which stands for "change mode"

Configuration Management

- The goal of configuration management (CM) is to ensure that accurate and meaningful information is readily available regarding the configuration of applications and services along with the configuration items (CI) that support them
- It includes all relationships and dependencies between the Cis:
    - Objects include hardware, software, networks, sites, vendors, suppliers, and people
- CM is a governance and systems life cycle process for ensuring consistency among all assets (configuration items) in an operational environment:
    - Classifies and tracks individual Cis
    - Documents functional capabilities and interdependencies
    - Verifies the effect a change to one configuration item has on other systems
- CM practices offer the required data about assets and their configurations including their interactions with other assets, which assists administrators and managers with
    - Problem resolution
    - Incident response
    - Network component deployment
    - Strategy formulation
    - Budgetary forecasting
    - Overall decision-making

Replace with Something Similar

- A configuration management system (CMS) is a set of data, tools, utilities, and processes used to support configuration management
- All information should be tagged and labeled with a common unified schema, preferably using key-value pairs
- This data will populate the configuration management database (CMDB)
- Relational databases have been used historically
- NoSQL/document databases are emerging as a common solution
- A communication service provider (CSP) service such as AWS DynamoDB could be leveraged

Patch Management

- Patch management is the process of applying (hopefully fully tested) updates to software, drivers, and firmware to protect against vulnerabilities
- Effective patch management helps ensure the best operating performance of systems, boosting productivity
- All systems need to be secured with patches, if possible
- The risks of disregarding patch management can cause exposure of business to leaks and breaches, loss of productivity, and loss of reputation

Patch Management Benefits

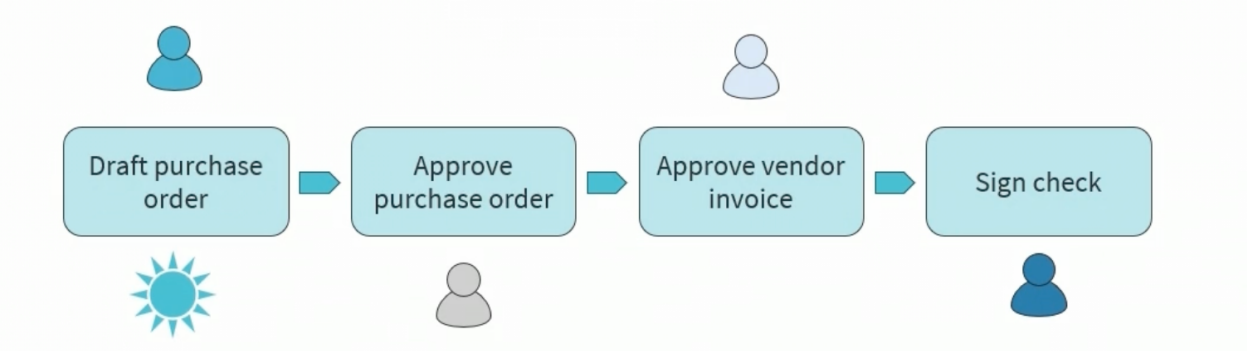
- Protects all endpoints from attackers
- Keeps all systems running in an optimized fashion
- Promotes productivity within the organization
- Helps lower the cost of device life cycle maintenance and repair
- Supports laws, regulations, and compliance standards

Least Privilege

- Is the principle that users and programs should only have the necessary privileges to complete their tasks, according to the National Institute of Standards and Technology (NIST)
- Is also referred to as "need to know" or staying within one's "pay grade" or classification level
- Is an aspect of authentications, authorization, and accounting (AAA) and identity and access management (IAM) where the subject has just the proper level or number of permissions and rights to perform the job role or responsibility and nothing more:
    - It should be built into all access control architectures
- Any deviation (escalation or elevation), if allowed, should go through an established change control IT service or service desk implementation

Separation of Duties

- Separation (also segregation) of duties (SoD) refers to the principle that no user should be given enough privileges to misuse the system on their own:
    - For example, the person authorizing a paycheck should not also be the one who can prepare them
- SoD can be enforced either statically (by defining conflicting roles) or dynamically (by enforcing the control at access time)
- An example of dynamic separation of duty is the two-person rule:
    - The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first



- Separate people approving separate shit for separate tasks

SoD

- SoD may also involve dual operator principles where two or more subjects are needed to modify or approve:
    - Example: Two signatures or cryptographic keys are required for certain actions
- Rotation of duties is also a related principle:
    - Example: Mandatory time off or forced vacations

Encryption in Access Control

- Encryption helps protect private information or sensitive data and can enhance the security of communication between client apps and servers

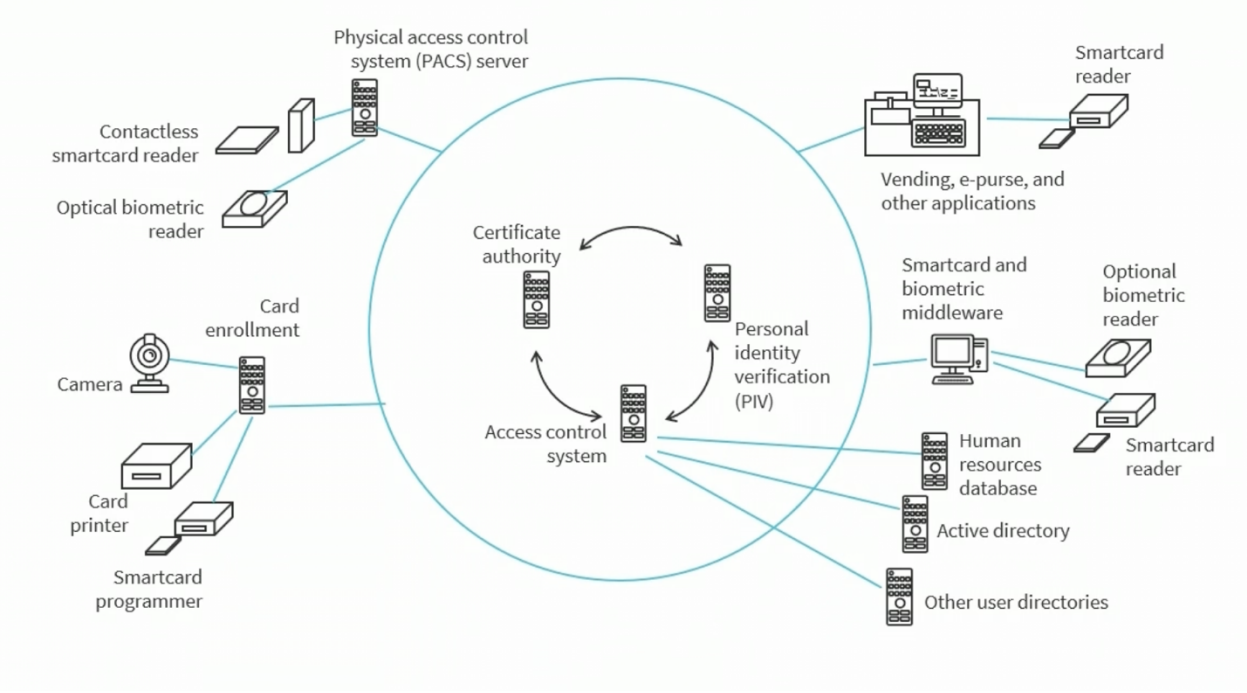
- In essence, when data is encrypted, even if an unauthorized person or entity gains access to it, they will not be able to read it
- Origin authentication uses symmetric and asymmetric encryption keys in a variety of systems, including digital signatures
- For example, encryption technologies are involved in shielding private and secret information from unauthorized users, thus safeguarding confidentiality
- This is done by enciphering information in such a way that only authorized users – users with the right key – are able to access the decrypted data

Monitoring and Visibility of Access Controls

- Access controls will determine which subjects have read access or visibility into critical access, such as sensitive data
- This visibility is vital for data in transit over remote channels and data sorted at third-party locations like code repositories (Git), personal cloud storage, and cloud-based block, object, and file storage systems
- Access control mechanisms also must be completely visible and always monitored

Access Control Visibility

- It is becoming more common to automate monitoring visibility and sending feeds to locations such as security operations centers (SOC) or cloud security information and event management (SIEM)/security orchestration, automation, and response (SOAR) systems like Azure Sentinel
- Audits should be performed regularly to discover gaps or "privilege creep" that can occur with poorly maintained access control and inventory systems
- Other tools that can be used are compliance scanners, PowerShell scanners, vulnerability scanning, and penetration testing



-

Decommissioning and Offboarding

- Outgoing employees pose major security risks to organizations
- Security practitioners should make offboarding strategies more resilient
- Without secure off-boarding processes, enterprises expose themselves to a variety of risks, from the harmlessly accidental to the maliciously purposeful

- Risks include data theft, disgruntled leavers, shadow (ghost) IT, unauthorized Software as a Service (SaaS) usage, IT and HR siloed and out-of-sync, access not removed promptly

Decommissioning and Offboarding Best Practices

- Generate solid onboarding policies and processes
- Encourage proactive, interdepartmental collaboration with stakeholders
- Secure corporate assets, devices, and associated credentials
- Make sure there is complete visibility of employees' SaaS, cloud, and third-party access, usage, and permissions
- Monitor for uncommon or even risky behavior of outgoing staff members
- Although all outgoing staff members or leavers will go into the risk database as potential threat actors, SHOULD handle all leavers respectfully and transparently

Hardening Systems

- Classic methods of hardening systems involve shutting down TCP and UDP ports and services (that need not be open/used), including ICMP messages and codes
- Only necessary secured protocols should be used, for example, Secure Shell (SSHv2) instead of teletype network (telnet) -> SSHv2 > SSHv1 > Telnet
- Continual patch management initiatives must be implemented for all systems and applications
- Strict least privilege access controls should be used for all administrative users
- Ongoing monitoring and visibility must be instigated
- Data, systems, and applications in zero-trust models can be hardened using symmetric and asymmetric cryptosystems, including data at rest, in transit, and in use
- Endpoints are secured and hardened using trusted platform modules and endpoint detection and response tools:
    - Modern solutions such as Palo Alto Cortex XDR are considered next-generation endpoint detection and host-based intrusion detection and protection

Hardening Techniques

- Other hardening best practices involve the following tasks:
    - Disabling all auto-configure features if a system requests it
    - Replacing all default passwords with strong credentials
    - Implementing strict password policies or passwordless solutions
    - Removing all unnecessary and unauthorized software (personal cloud storage, type 2 hypervisors, exploit kits, etc.)

Architecture and Infrastructure Concepts

Resilience

- Resilience is the ability of a system to continue to:
    - Operate under adverse conditions or stress, even if in a degraded or debilitated state
    - Maintain essential operational capabilities
    - Recover to an effective operational posture in a time frame consistent with mission needs
- Resilience is the ability of a workload to recover from infrastructure or service disruptions
- Administrators should be able to dynamically obtain computing resources to meet demand and mitigate disruptions
    - Disruptions can be misconfigurations or transient network issues

High Availability

- Availability is an aspect of resiliency expressed as a percentage of planned and unplanned downtime over an annual period (99.5, 99.9, 99.95, 99.99)
- High availability entails a system, component, or application operating at high capacity, continuously, without intervention, for a defined period of time
- A high-available infrastructure is designed to deliver quality performance and handle different loads and failures with minimal or zero downtime
- Reliability is a measure of percentage uptime, considering the downtime due only to faults, whereas Availability is a measure of the percentage uptime, considering the downtime due to faults and other causes such as planned maintenance
    - For two different systems, it is possible for one system to be more reliable but less available than the other

Availability vs. Durability

- Availability has historically been achieved through hardware redundancy so that if any component fails, access to data will remain
- Durability, on the other hand, refers to long-term data protection (i.e. the stored data does not suffer from bit rot, degradation, or other corruption)
    - Durability is concerned with data redundancy so that data is never lost or compromised
- Example: AWS S3 and Google Cloud are designed for 99.999999999% (11 nines) durability per object and 99.99% availability per year

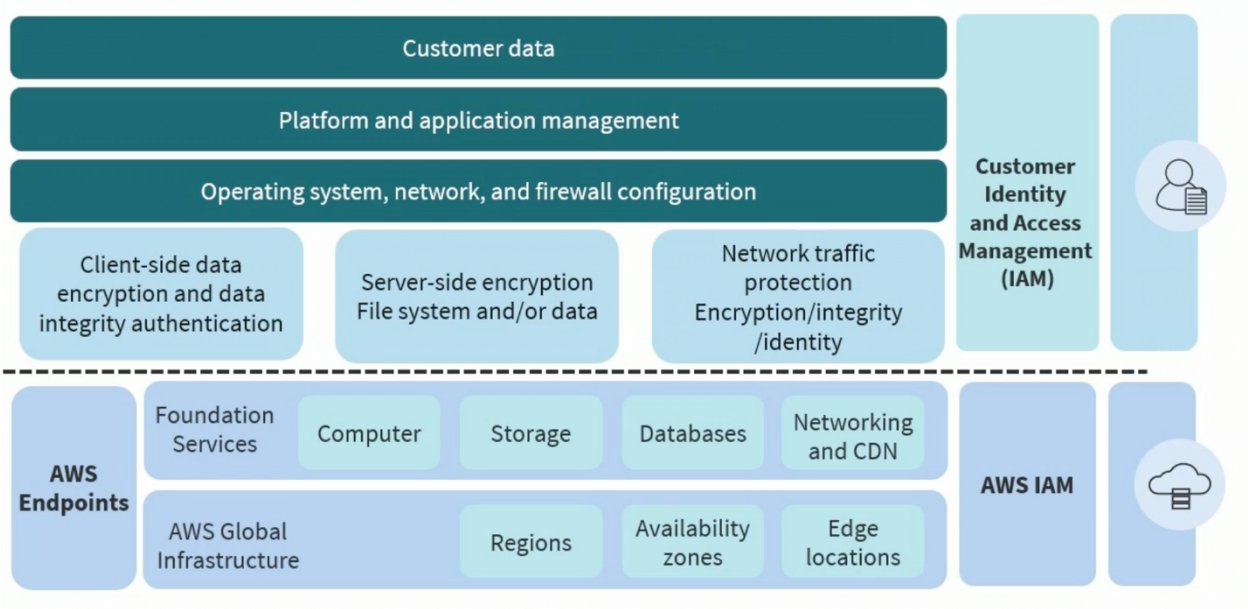
Other Architectural Considerations

- Cost
- Responsiveness
    - Low latency and performance
- Scalability
    - Scaling out adds physical and virtual instances
    - Scaling up adds compute processor, memory capacity
- Ease of deployment
    - Infrastructure as Code (IaC)
    - Patching automation
- Risk transference
    - Cloud, insurance, shared disaster sites
- Power

Cloud Computing: Infrastructure as a Service (IaaS) According to NIST

- Infrastructure as a Service is where the “capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, including operating systems and applications
- The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).”

Infrastructure as a Service at AWS

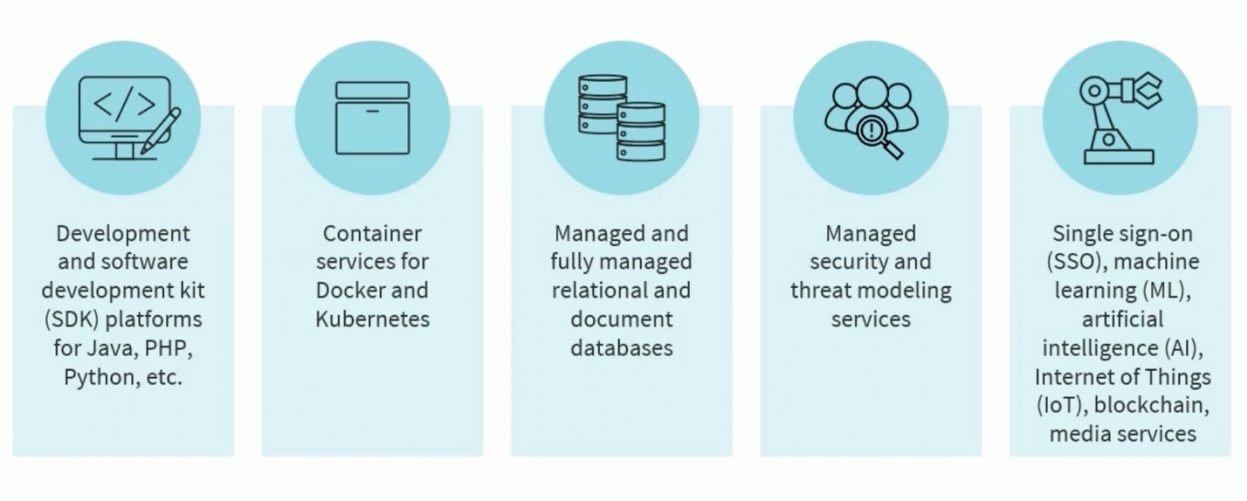


-
- Everything below the line is the responsibility of AWS
- Everything above is the responsibility of the buyer or customer
- With IaaS with the shared responsibility model the customer has the most responsibility and the provider has the least

Cloud Computing: Platform as a Service (PaaS) According to NIST

- Platform as a Service is the when the “capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly applications hosting environment configurations”. With PaaS the shared responsibility model is reliant on the service portfolio – how managed is the service. Which service type has the most variance

Platform as a Service



-

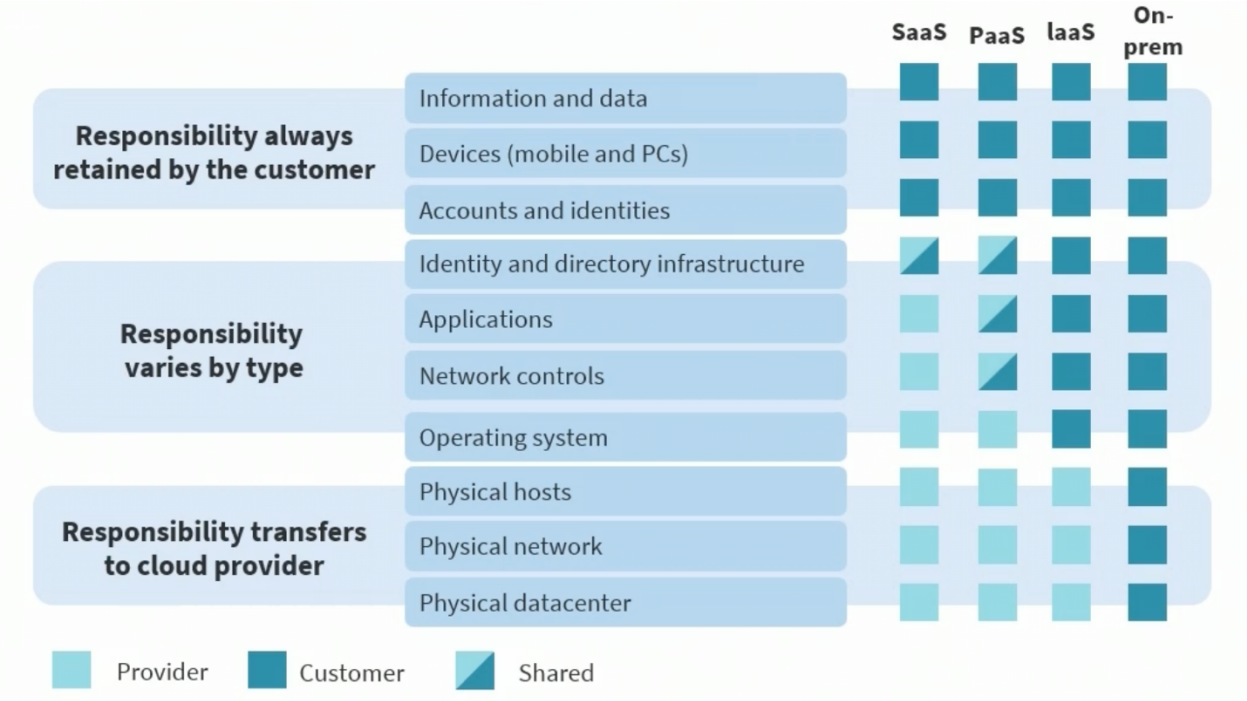
Cloud Computing: Software as a Service (SaaS) According to NIST

- Software as a Service is when the “capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings”

Software as a Service Offerings

- Customer relationship management (CRM)
- Enterprise resource management (ERM)
- Human resources and workplace tools
- Finance, sales, and marketing services
- Payroll services
- Email, collaboration, and cloud storage
- Help desk and service desk
- Virtual call center
- Business analytics

Azure Cloud Responsibility Matrix



-
- PaaS has more flexibility and most difficult to secure because it has a lot of options

Cloud Deployment Models

- Public Cloud: The organization runs an initiative (DevOps, DB) entirely at the cloud service provider (CSP) or has public customers for its deployed resources (web, e-commerce)
- Private Cloud: A cloud scenario that supports a single organization and its internal customers either in the CSP or on-premises
- Community Cloud: A consortium that uses a cloud environment for a particular use case, i.e. gaming community, metaverse, financial, healthcare, etc.
- Hybrid Cloud: A combination of the other three options or an edge computing environment – where a company is running the same hardware and software on premise (e.g. backup and restore, disaster recovery) often bursting up during peak seasons

Hybrid Cloud Considerations

- Hybrid cloud can also be a method for connecting infrastructure and applications between cloud-based resources and other resources that are not placed in the cloud
- The most common type of hybrid deployment is between the provider's public cloud and a standing on-premises enterprise private cloud
- Can be used to migrate, expand, or grow an organization's infrastructure into a cloud solution while linking internal systems to cloud resources
- Often used by organizations to "burst up" to the cloud during peak demand times or special situations

On-premises (Private) Cloud

- Involves installing resources on-premises using virtualization and resource management tools, often called private cloud
- On-premises deployment does not provide many of the benefits of cloud computing but is often chosen for its ability to provide dedicated resources
- In most scenarios, this deployment model is the same as legacy IT infrastructure while using application management and virtualization technologies to try and increase resource utilization

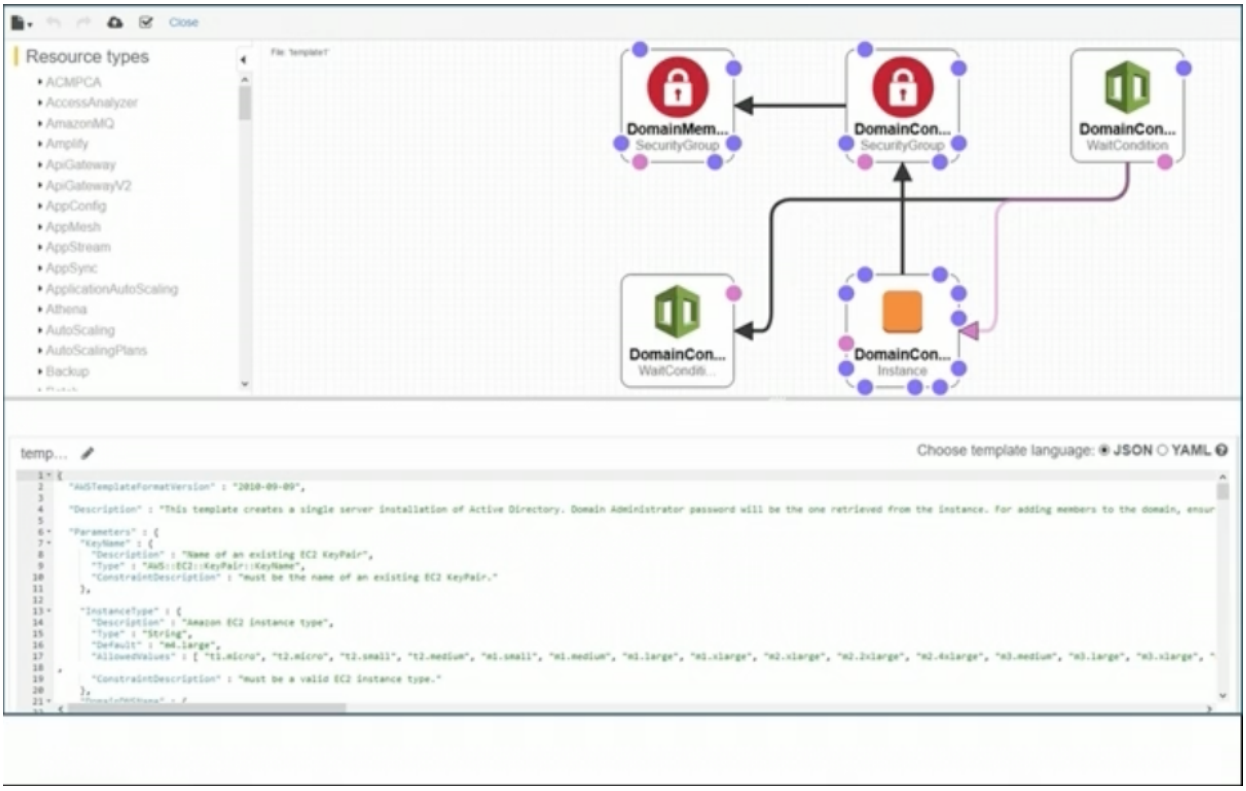
Third-party Cloud Vendors

- Brokers – local municipal partners, edge location, reciprocal partners
- Auditors – often CSA or SOC certified internal and external auditors
- MSSP – managed security service providers such as Fortinet offering cloud-based services (NGFW, NGIPS, EDR, visibility, SIEM+SOAR)
- CASB – assisting with SaaS providers for compliance, data loss prevention, and single sign-on
- Direct Connection – partners like Direct Connect, Interconnect, and ExpressRoute

Infrastructure as Code

- IaC is the provisioning and operations of infrastructure using code or templates (JSON, YAML) instead of by manual processes
- Configuration files are created that contain the infrastructure specifications, which makes it easier to edit and distribute configurations (Virtual networks, virtual machines, applications)
- It also ensures that admins provision the same environment every time by creating a single source of truth
- IaC assists configuration management and helps to avoid undocumented, ad-hoc (needed) configuration changes
- Version control is also an important part of IaC, and all configuration files should be under source control just like any other software source code files
- Deploying with IAC also means that architects can divide their infrastructure into modular components that can then be combined in different ways using automation and orchestration
- This is referred to a generating a “single source of truth” or “terraforming the environment”
- Automating with IaC also means that developers do not need to manually provision and manage servers, operating systems, containers, or microservices each time they develop or deploy an application
- Codifying the infrastructure offers a template to follow for provisioning
- An automation tool, such as Red Hat Ansible Automation Platform is a common IaC solution
- Cloud services such as AWS CloudFormation empower customers to model, deploy, and manage AWS and third-party resources by handling the Infrastructure as Code
- The cloud template language comes in either JSON or YAML formats
- Customers can automate, test, and deploy infrastructure templates with continuous integration and delivery (CI/CD) automations
- Templates can also be used to set up lab environments for learning the cloud

Infrastructure as Code: AWS

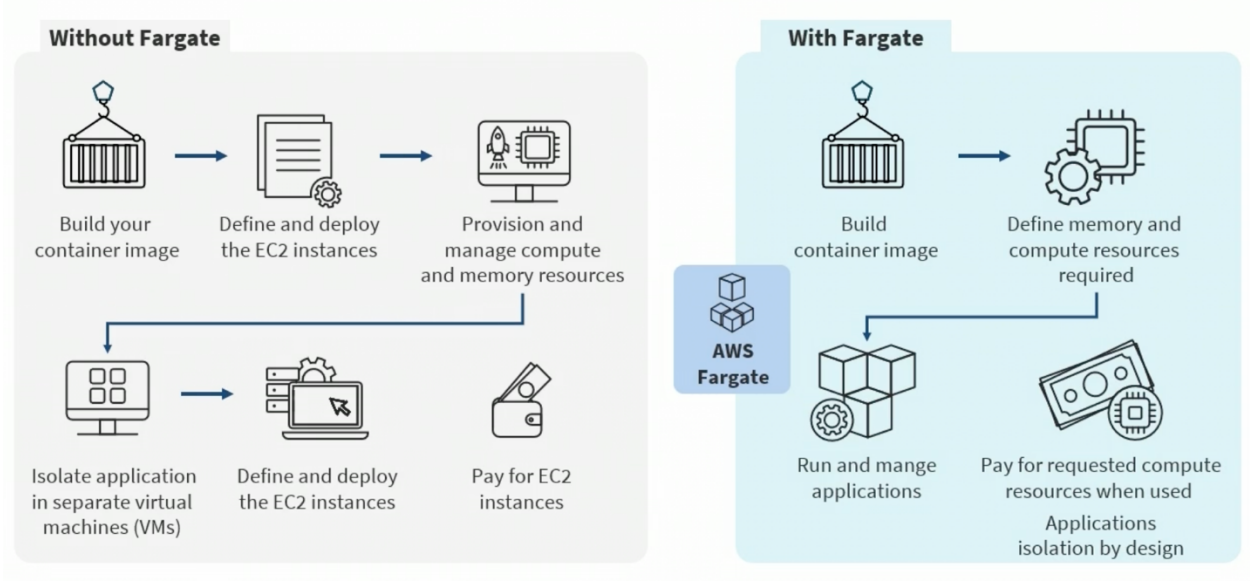


-
- AWS Cloud formation – see single source of truth or JSON file representing topology. Can use JSON or YAML for template language

Serverless Technologies

- Modern serverless solutions leverage modern cloud infrastructures to emulate the network operating system (NOS) environment without the need for a Windows or Linux-based servers
- These are technologies for running code, managing data, and integrating applications, all without managing servers
- They feature automatic scaling, built-in high availability, and a pay-for-use billing model to increase agility and optimize costs
- Functions, containers, and databases are common serverless solutions

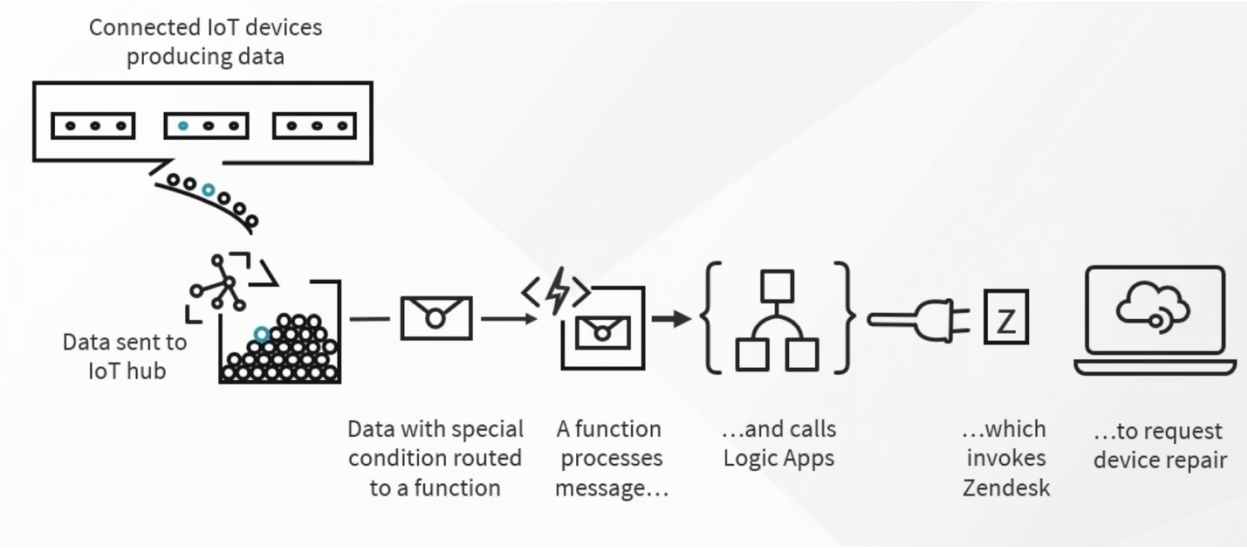
Case Study: AWS Fargate Serverless Containers



-

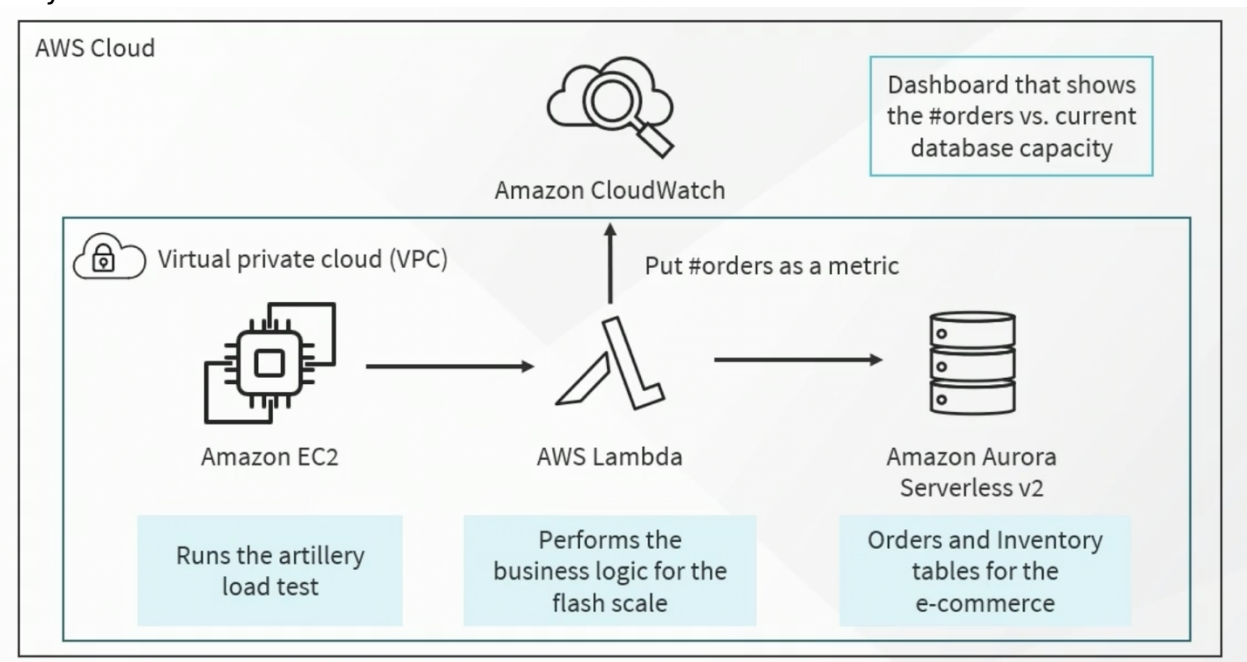
- Left (without fargate) build container image (using docker) then you define/deploy virtual instances in the EC2 environment. Provision manage and compute memory resources, isolate applications and virtual machines, then define and deploy instances and then you run.
- Fargate -> build container image, define memory and compute resources and then run and manage applications and then pay for the request resources. The applications are isolated by design

Case Study: Azure Serverless Functions



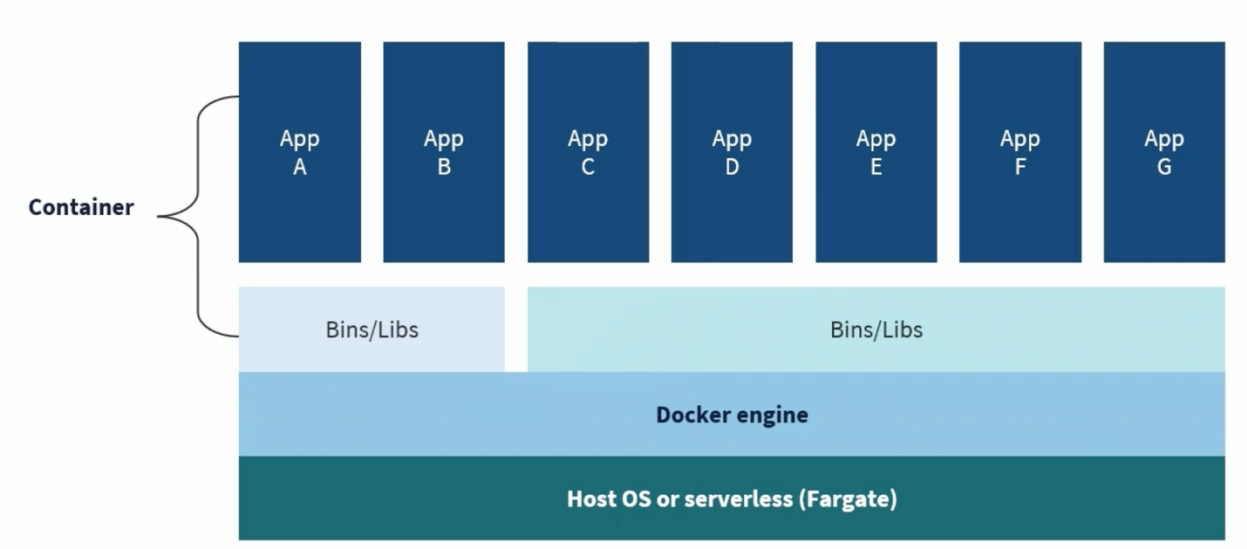
-
- Connect IoT devices that produce telemetry data. The data is sent to a IoT hub perhaps special conditions that are routed to a Azure function. The function processes the message and calls Logic Apps that calls Zendesk then you can make a request to repair the IoT device (e.g. a sensor in a firm, a tractor)

Case Study: AWS Serverless Database with Aurora



-
- Serverless databases with AWS Aurora. Can run a Amazon EC2 artillery load test to AWS Lambda which performs business logic (e.g. put orders as a metric) which simultaneously sends information to Amazon CloudWatch (or dashboard) and then a lambda function can trigger to Amazon Aurora Serverless which stores orders and inventory tables for the e-commerce solution.

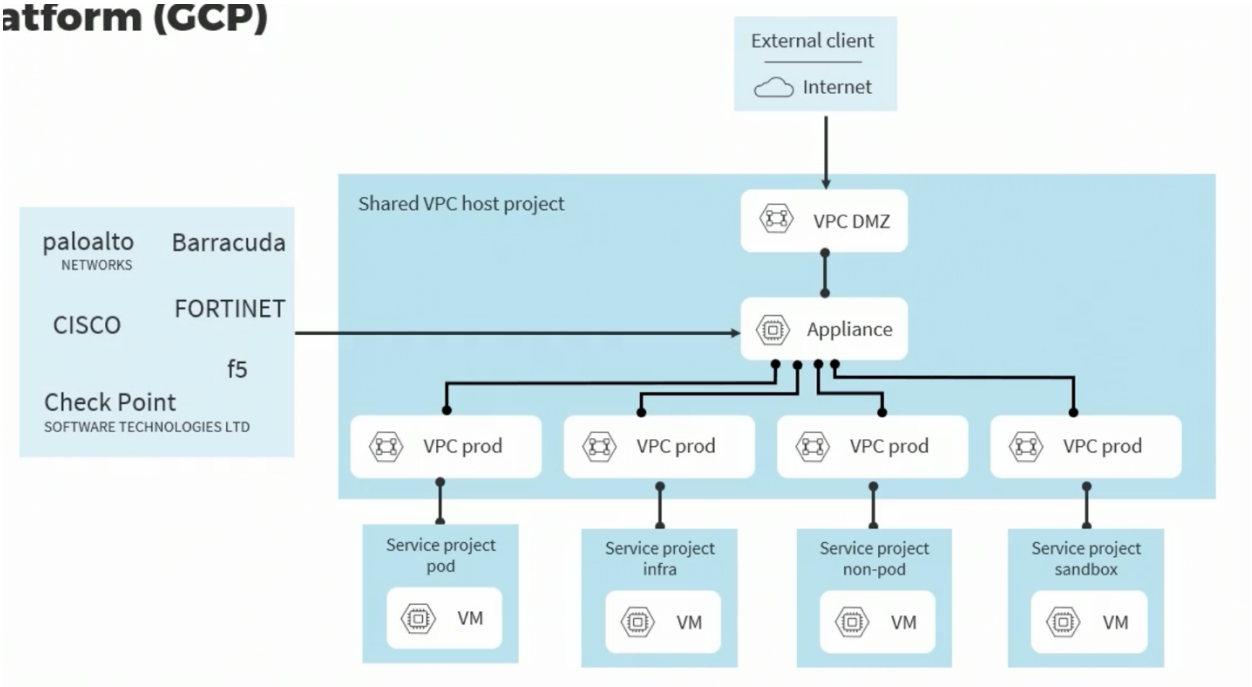
Containers

- A container is a discrete environment within an operating system (or a serverless architecture) where one or more applications can run and that is typically assigned all the resources and dependencies needed to function
- It is a modular and portable environment that includes the application binaries, software dependencies, and hardware requirements wrapped up into an independent, self-contained unit
- Containers are commonly used for processes and workflows in which there are important requirements for security, reliability, and scalability
- All cloud providers offer managed container development, automation, and orchestration services
- Containers can be server-based or serverless (AWS Fargate)
- 

Microservices

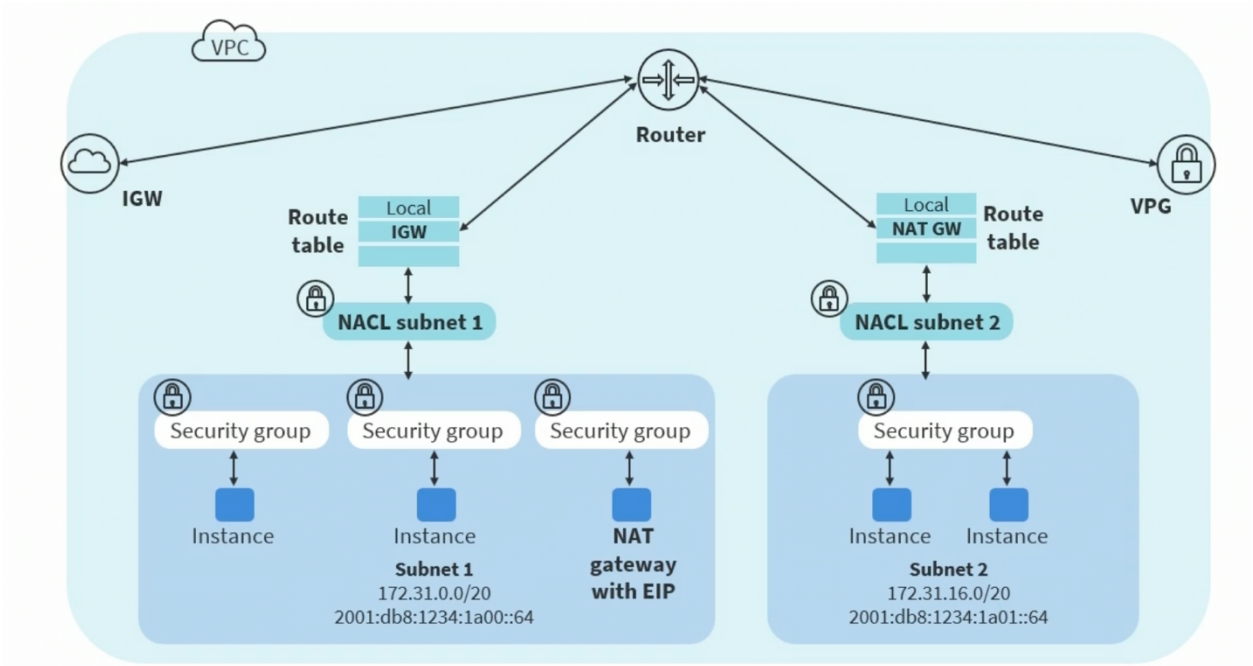
- Closely related to containers
- Microservices are specific service-oriented application components made up of small independent services that communicate over well-defined APIs for notification and process queueing
- They make applications and apps faster to develop and easier to scale by small, self-contained teams of developers
    - Microservices are about the design of software
    - Containers are about packaging software for deployment

Cloud Customer Network Infrastructure: Google Cloud Platform (GCP)



-
- All external clients coming through the internet are going to go through a DMZ VPC. The VPC is what google calls their virtual network. External clients go through the VPC DMZ and then connect to various autoscaling client solutions (e.g. palo alto, cisco). The autoscaling virtual appliances then send traffic to various production VPC or production virtual networks (those contain virtual machines). For example service project sandbox(private subnet in a VPC.

Cloud Customer Network Infrastructure: AWS



-
- Cloud customer network infrastructure at AWS. Far left, all public customers go through an internet gateway (IGW). On the right, any side to side VPN connections go through the VPG. In this VPC or virtual network we have two subnets. The left subnet is a public subnet because its routing table has a internet gateway in it. On the right, that's a private subnet and its routing table is a NAT gateway. Any instances middle tier and backend database servers that want to communicate with the internet (e.g., windows update service) they will router traffic to the NAT gateway in the left hand public subnet number 1 using an elastic Ip address, public ip address and it will go out the

gateway to the public internet. If a subnet at AWS doesn't have a internet gateway in its route table nor does it have a virtual private gateway in its route table it is a private subnet. There is only three types of subnets at aws -> public, private and VPN only. Also see a couple different firewalls, NACL subnet (stateless static firewall) and security group firewalls which are applied directly to the interfaces, EC interfaces of the instances.

Software-defined Networking (SDN)

- Most modern datacenters and cloud datacenters use SDN
- Software-defined networking is a framework intended to make a network more flexible and easier to manage, especially with disparate hardware and graphical overlays
- SDN centralizes management by abstracting the control plane from the data forwarding function in the different networking devices

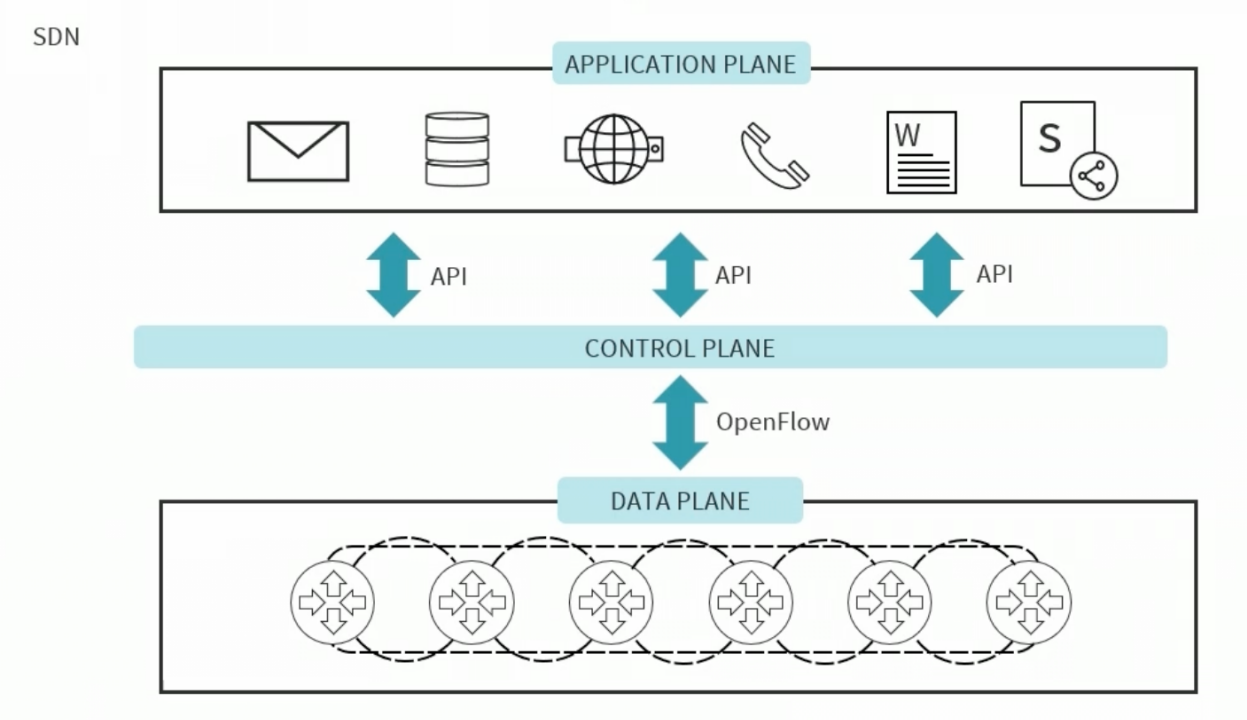
SDN

- An SDN architecture offers a centralized, programmable network consisting of the following:
    - The controller is the essential element of an SDN architecture that assists centralized management and control, automation, and policy enforcement across physical and virtual environments
    - Southbound application programming interfaces (APIs) relay information between the controller and the individual network devices
    - Northbound APIs transmit information between the controller and the applications and policy engines, to which an SDN looks like a single logical network device

SDN Characteristics

- Based on open flow technology
- Directly programmable (templates, stacks, infrastructure as code JSON, YAML)
- Agile (quick changes, scale out and up, many of the components are virtual)
- Centrally managed (done from a controller special software running on a server)
- Programmatically configured (IAC, using API calls)
- Open standards-based and vendor-neutral

Software-defined Networking

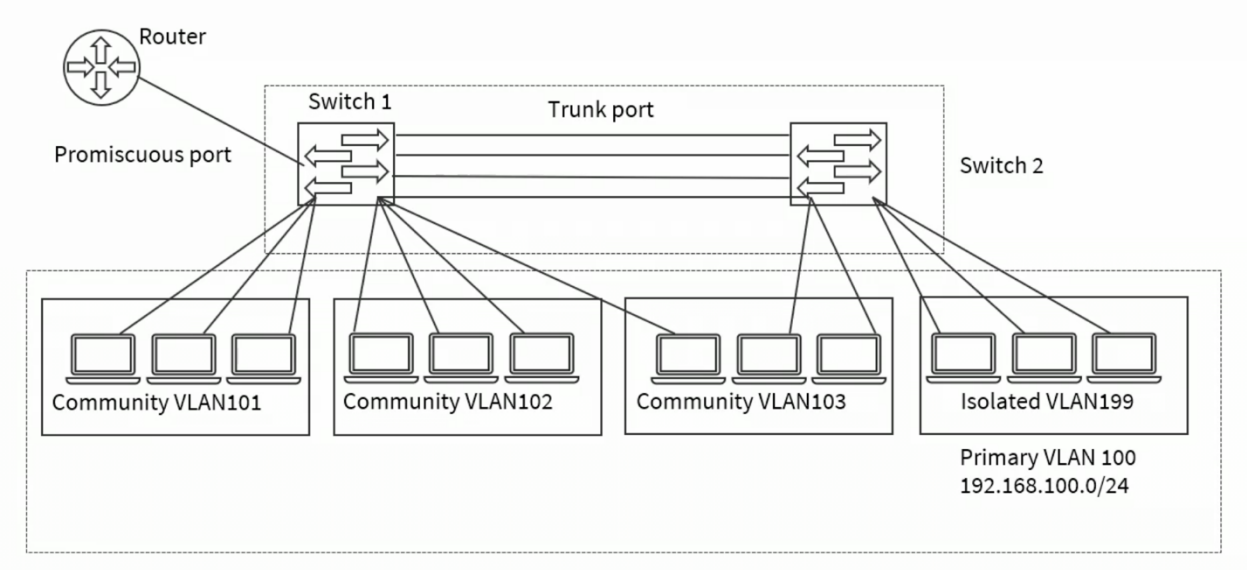


-
- Have total separation of the control and data plane. The control plane is managed through the aforementioned controllers. Administrators and engineers log onto the controls (in a zero trust environment, biometric) and then send API calls to the application plane, digitally signed, and API calls to the data plane which is where the physical and virtual layer 2 and layer 3 servers and routers reside.

Other Network Infrastructure Concepts

- Physical Isolation (e.g. storage area network should be on a separate network than your production network – corporate network should be on a separate network to your HMAC system – SDN should be on a physically isolated network)
- Air-gapped (e.g. certificate servers should be offline and off the network and only brought online for brief periods of time to down level immediate servers – hardware security modules should be air gapped) – total airgapped system is off in any network but in some environments air gapped means that it should be kept off the internet
- Logical segmentation (e.g. common way to segregate networks was accomplished with private VLANs, this is still done in virtual hypervisor environments, but can still logical segment on mobile devices)

Logical Segmentation



-
- Have a router or multi-layer switch that connects to two access switches. Those switches a trunked together. In the initial VLAN (100) has been segmented logically into private VLANs. The communities (101, 102, 103) will only send traffic to other members of the community and northbound to the switch on the promiscuous port to the router or multi-layer switch, they will not send frames to any other community or isolated device in VLAN 199. The three servers in VLAN199 will not send traffic to each other, any other community they will only respond to send traffic back to the switches and then on the promiscuous port to the router or multi-layer switch.

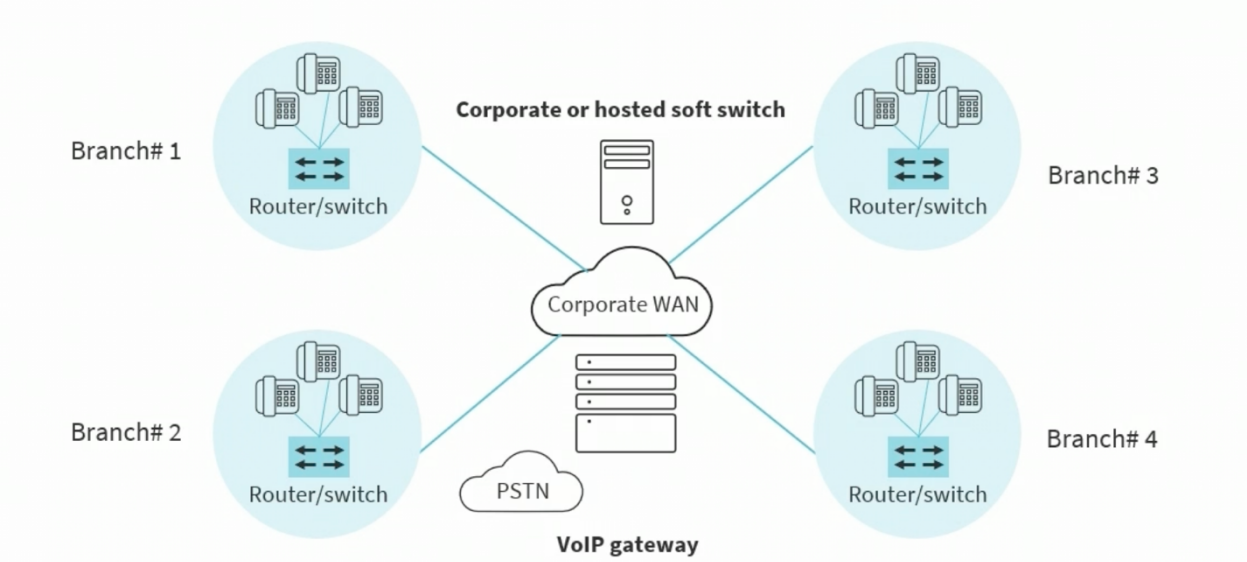
Centralized Design

- Centralized systems typically deploy a client/server architecture where one or more client node communicates directly (or through a proxy otherwise known as mediated access like a access gateway) with a central server either physically or logically
- This is the most common type of system in many organizations where a client sends a request to a corporate intranet and receives a response

Common Centralized Attributes

- Presence of a global clock: all client nodes sync up with the main clock of the central node (often using NTPv3)
- There is one highly available central node that coordinates all the other nodes in the system
- Central node failure causes the entire system to fail because if the server is down, no other entity is there to send/receive responses/requests
- Centralized servers can, in many cases, leverage a hierarchy of intermediate down-level servers, e.g. domain name system, hierarchical certificate authorities

Centralized Wide Area Network (WAN)



-
- The corporate WAN will have a central headend that connects to four different branch offices over a wide area. Each branch will have a customer premise equipment usually a router or multi layer switch or a firewall appliance

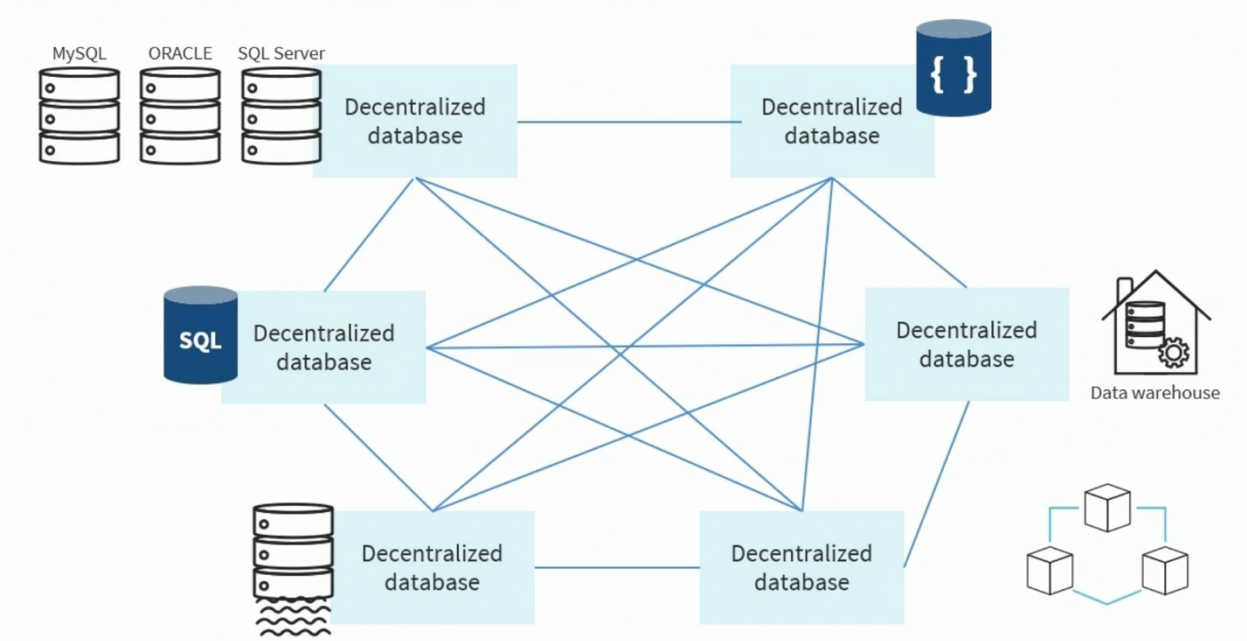
Decentralized Design

- In a decentralized system, every node makes its own decision
- The final behavior of the system is the aggregate of the decisions of each individual node or host
- There is no single entity that receives and responds to the request
- The requests are broadcasted or multi casted to the decentralized architecture

Common Decentralized Attributes

- There is no global clock as each node is independent of each other, and therefore have different clocks that they run and follow, however if all of the devices in the centralized environment connect to an atomic clock they can still have a centralized time
- Decentralized systems have multiple or shifting nodes and more than one unit which can listen for connections from other nodes
- One central node failure causes a part of the system to fail; not the whole system

Decentralized Database Network



-
- Decentralized database network, upper right hand side we have a decentralized database and a full mesh connection to a decentralized data warehouse a database cluster a SQL database or data-lake (top left)

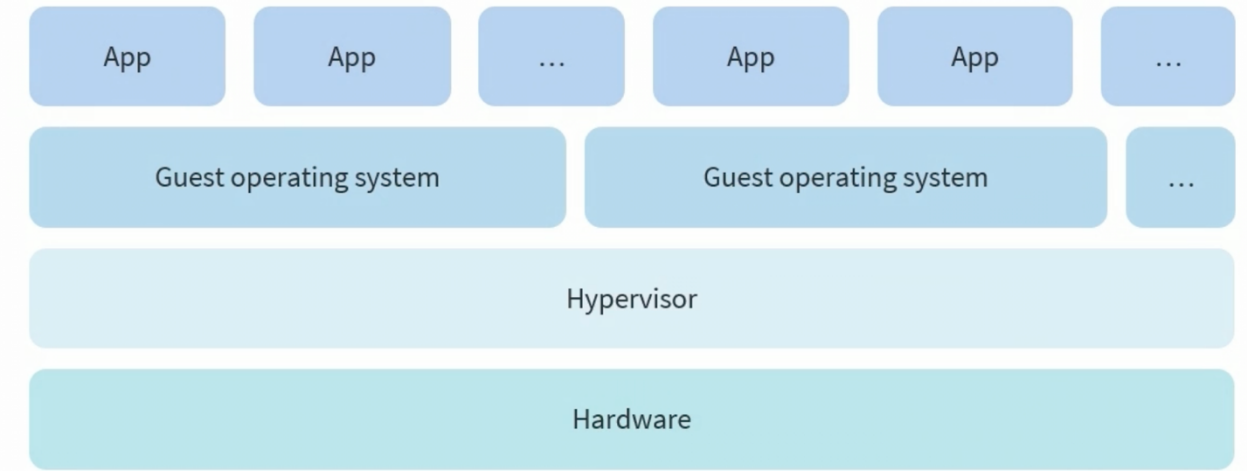
Virtualization

- Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the underlying hardware server
- It most often refers to running multiple operating systems on a computer system simultaneously
- To the applications running on top of the virtualized machine, it can seem as if they are on their own dedicated operating system with libraries, dynamic link libraries (DLLs), and associated programs

Hypervisors

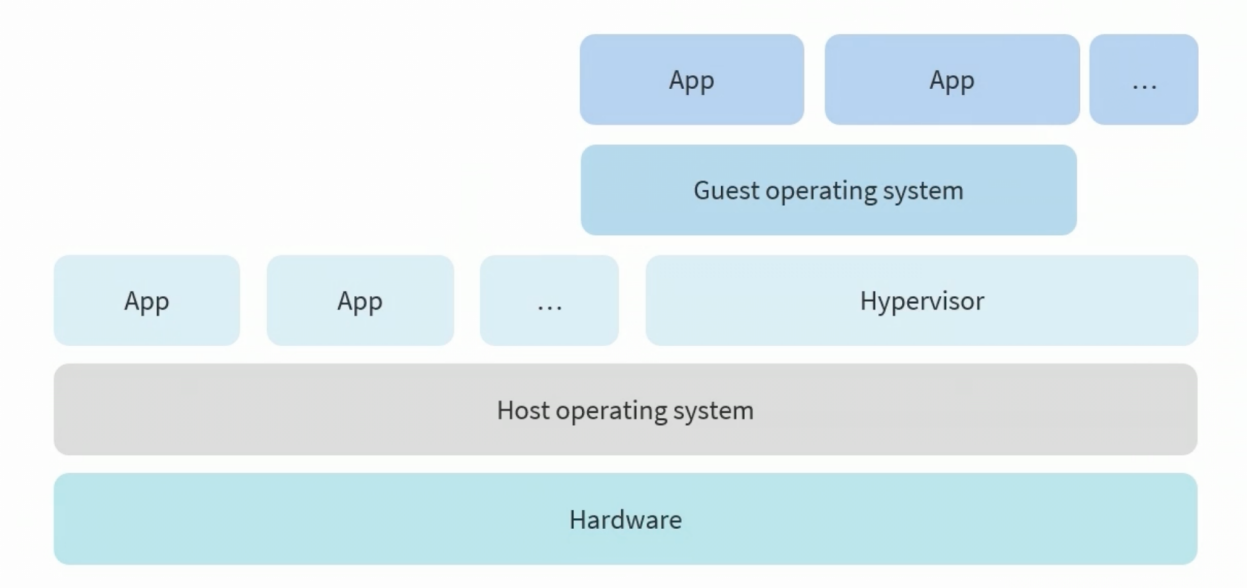
- These are the virtual machine manager system and software that run one or more virtual machines
- It controls the interaction between the VMs and the underlying hardware
- Type 1 – bare metal or native
    - Runs directly on the underlying hardware
    - XenServer, KVM, Hyper-V, ESXi
- Type 2 – hosted
    - Runs on the OS installed on the hardware
    - Oracle VirtualBox 6, VMWare Player/Workstation

Type 1 Hypervisor



-
- The underlying hardware in the data center (CISCO SERVER) will have the hypervisor directly installed onto it. Then the GOS and applications will run within the hypervisor, the VM manager running directly on the hardware. In this diagram we see what is native or bare metal

Type 2 Hypervisor



-
- On the hardware you install a host operating system (UBUNTU) then you list all the type 2 hypervisor into the host operating system and that will run simultaneously with other applications and services on the host operating system. Then within the type 2 hypervisor you can run one or two more guests with applications. Without virtualization there is no cloud computing

Supervisory Control and Data Acquisition (SCADA)

- Supervisory Control and Data Acquisition (SCADA) systems represent the software used to collect and send data to throughout facility systems and to cloud services
- Programmable logic controllers (PLCs) and other embedded systems are common hardware components
- Systems that are not air-gapped introduce various threats

Industrial Control Systems (ICS)

- Subcategory of Scada

- Industrial control system (ICS) is a combined term that represents varied forms of control systems and related instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial and mechanical processes
- Each ICS typically functions differently and is built to electronically manage tasks efficiently
- Modern devices and protocols used in ICS are used in nearly every industrial sector and critical infrastructure

SCADA AND ICS Systems

- Facility and manufacturing control and management systems
- Water management systems
- Electric/nuclear power grid, solar, and wind farms
- Traffic signals and mass transit systems
- Environmental and manufacturing control systems

Internet of Things

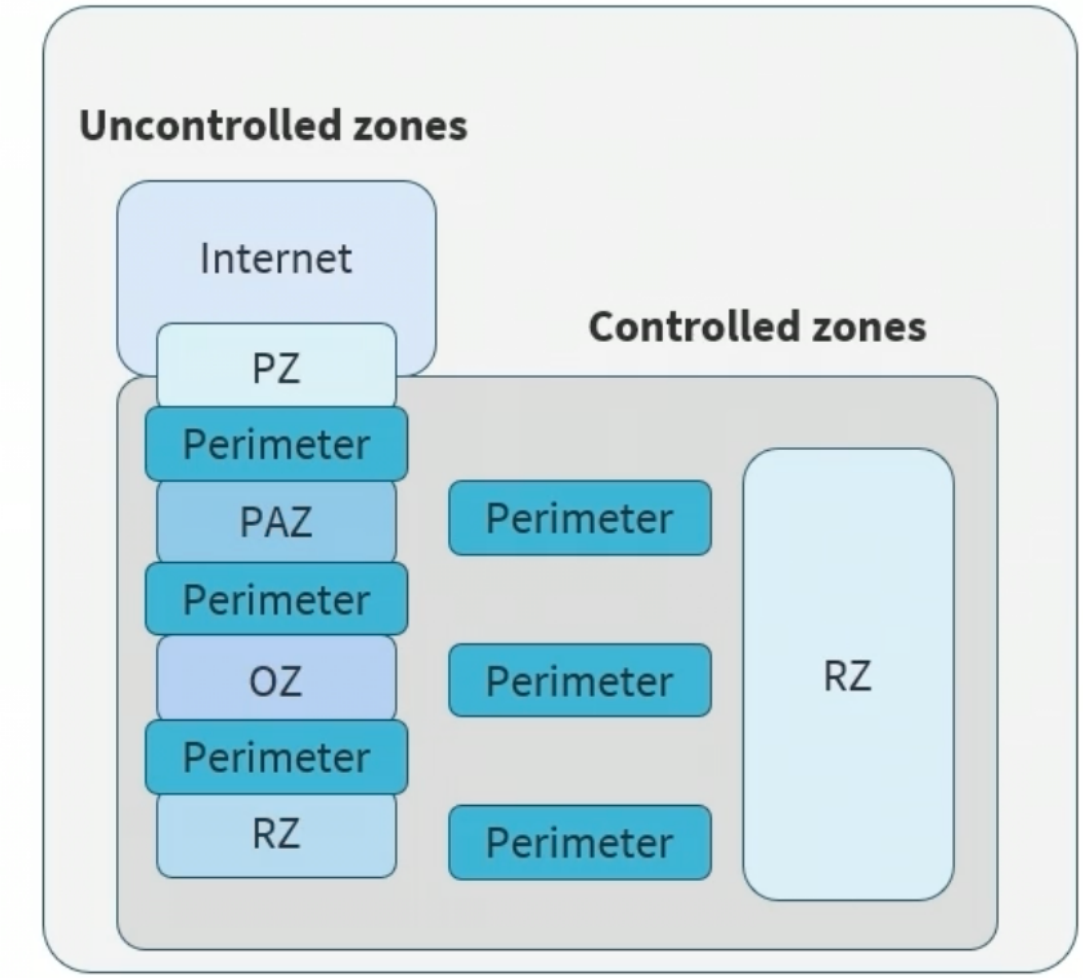
- The term IoT refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves
- With the advent of inexpensive computer chips and high bandwidth networking, there are now billions of devices connected to the Internet using IPv4 and IPv6
- Everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users

Examples of IoT

- Mobile devices
- Cameras
- Farm and ranch equipment
- Sensors
- Smart appliances
- Facility automation
- Medical devices and systems
- Vehicles and aircraft (drones)
- Smart meters
- Embedded devices and real-time operating systems (RTOS)

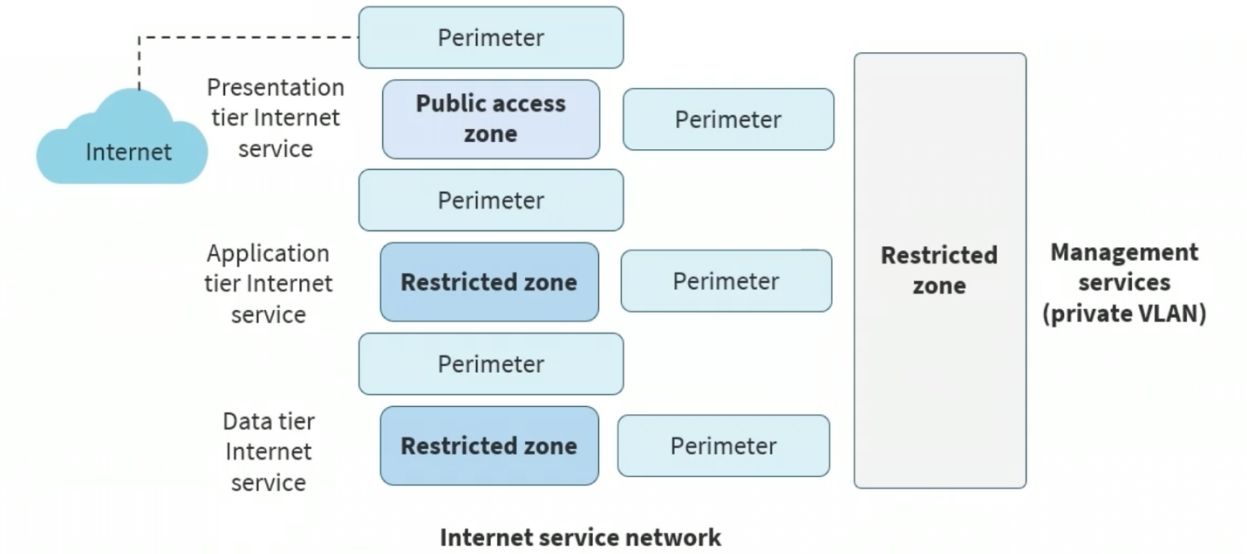
Enterprise Infrastructure Security Principles

Security Zones



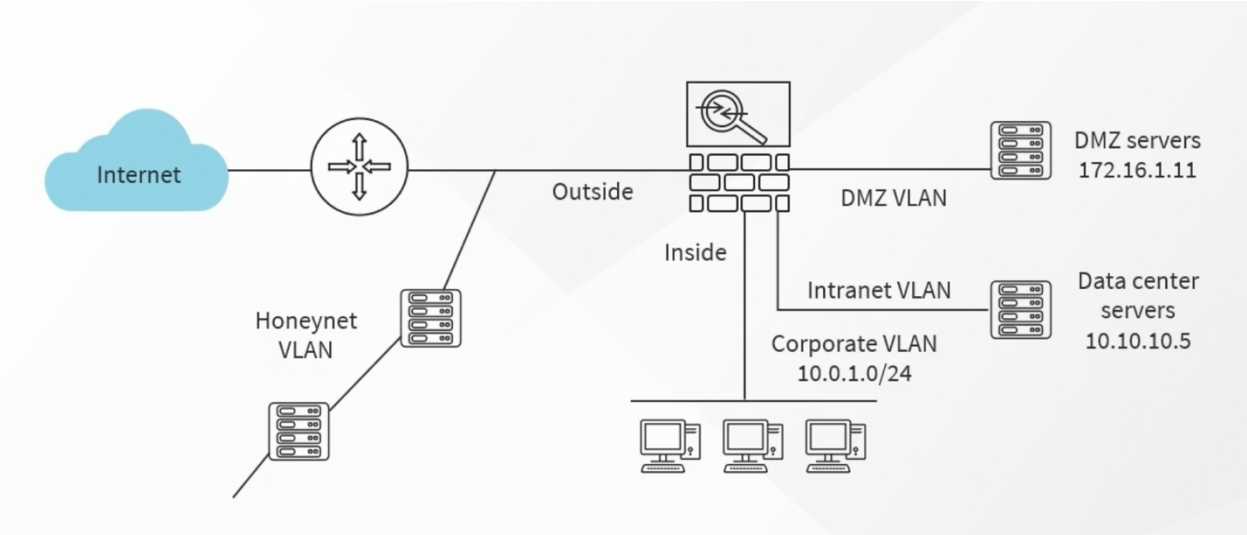
-
- Zoning is a logical design approach used to mitigate the risk of an open network by segmenting infrastructure services
- Each zone has fundamental characteristics, defined by the security policy:
    - Every zone contains one or more separate, routable networks
    - Every separate, routable network is contained within a single zone it cannot transcend more than one zone
    - Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs), usually a multi-layer switch or a firewall
    - The only zone that may connect to the public zone is the public access zone (PAZ), or DMZ

Segmentation and Zoning



-
- Restricted zones that have no access to the internet, for example a management private VLAN or a datacenter or middle tier application services. A zone interface point is between each zone it can be a firewall with the interface in each zone or each zone can have its own firewall or multi layer security switch. Again in the public access zone this is the only zone that connects to the internet tier hosting public facing servers or services. This logical segmentation is critical as a defense in depth mechanism

Zones and Virtual Local Area Networks (VLANs)



-
- Several zones. Outside zone of a firewall which has customer premise equipment including router. Have a honeynet vlan zone, corporate vlan zone, a intranet vlan zone and a dmz/public access zone. These zones could be partitioned logically or physically or they might not be. For example, the intranet vlan and honeynet vlan could actually be in the same physical location but in different logical zones

Attack Surface

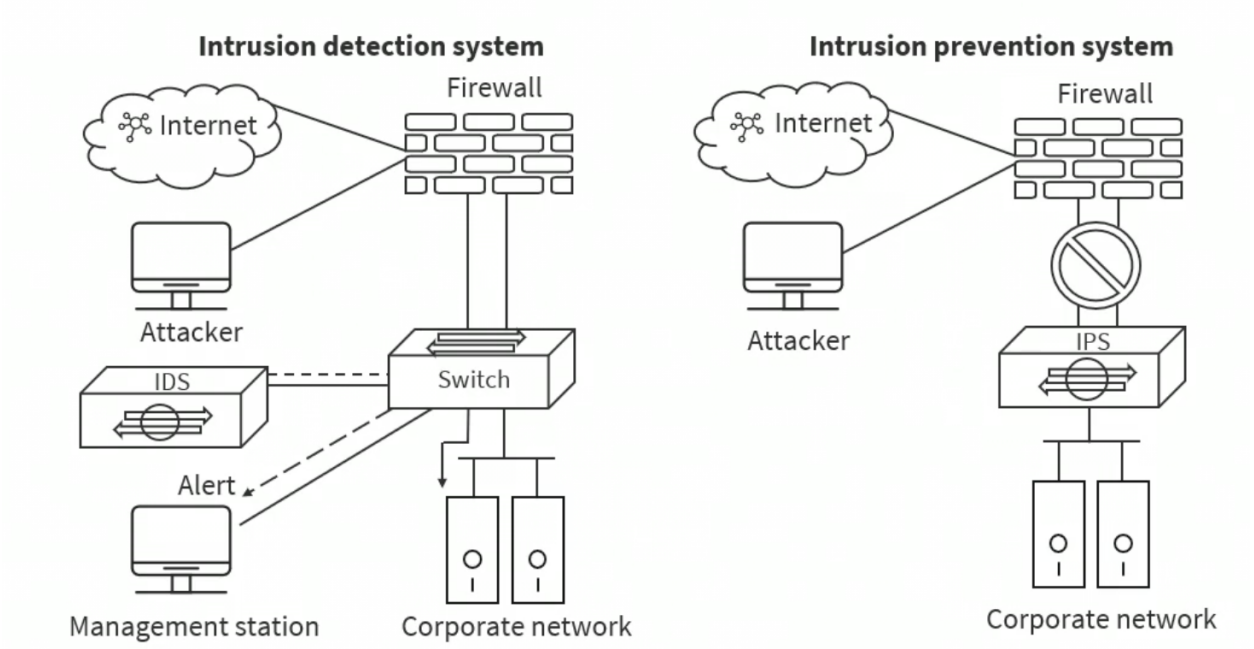
- The attack surface consists of all possible attack vectors that a threat actor can use to access a system and extract data
- It represents the targets of the cyber kill chain
- The smaller the attack surface, the easier it is to counter/mitigate with various controls
- The attack surface is split into two categories: digital/logical and physical

- Enterprises must continuously monitor their attack surface to recognize, expose, and block potential threats as quickly as possible
- They must also endeavor to minimize the attack surface area to reduce the risk of successful attacks or attacks that can effect a lot of endpoints
- Attack surface reduction becomes more difficult as organizations expand their digital footprint and leverage new technologies

Failure Modes
- Certain security infrastructure devices such as firewalls and IPS sensors can be deployed in "fail-open" or "fail-closed" modes
- Fail-open means that even if there is a system or component failure on the device IP traffic should continue to flow to zones on the outbound interfaces
- In fail-closed mode the device will stop processing packets
    - Example: One of the failover interfaces to the standby device shuts down or fails

Network Appliances: IDS/IPS
- An intrusion prevention system (IPS) is a network security hardware or software solution that continuously monitors a zone for malicious activity
- It then proactively takes action to prevent it in the line of traffic -> called an in-line solution
- It is more advanced than an intrusion detection system (IDS), which reactively detects malicious activity
- IPS systems are often integrated into security appliances or part of a next-generation firewall (NGFW) or unified threat management (UTM) solution

Intrusion Detection vs. Prevention



-
- On the left, we have a IDS sensor – this can be integrated into a firewall or a multi-layer switch or even a router, in this case it is connected to a port on a layer 3 switch, this switch is using a protocol called SPAN to send copies of frames to the IDS sensor, the IDS sensor is not in line – its basically comparing its signatures, anomaly knowledge based, heuristic rules to the copies of the frames. Therefore if there is an attack against servers or systems on the corporate network they will deliver the payload. The IDS can only react to things it has detected as it sends information or alerts to the management station

- On the right hand side we have a intrusion prevention system, this can be integrated into a router or firewall or a stand alone solution. The IPS sensor is in line behind the firewall, it only acts when the traffic it is permitted from the firewall but it is inline so it can block or drop traffic that is malicious before it gets to the corporate network. Most systems today are IPS systems which are initially deployed in a IDS mode in other words a passive or monitored mode, so you can reduce the false positives and tune in and then put it into in-line mode

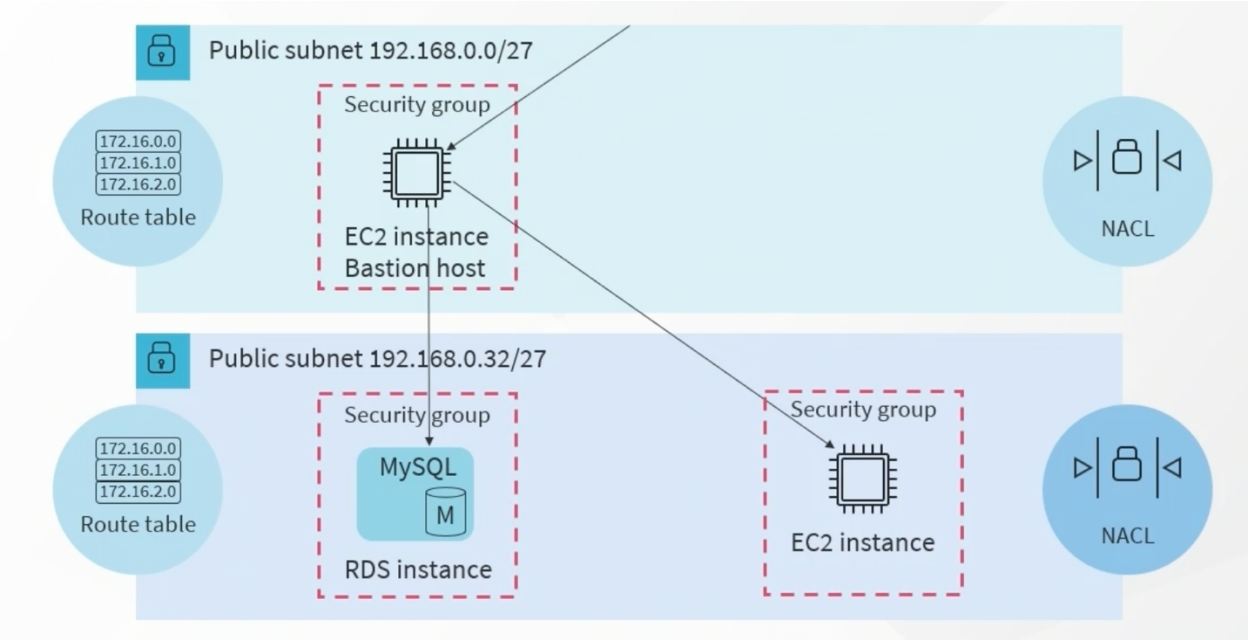
IPS Actions

- Alerts and alarms (to a SIM system e.g.)
- Verbose dumps (dumps the contents of the packet)
- Transmission Control Protocol (TCP) resets
- Drop packets or addresses
- Blocking (shun) on firewalls and routers
- Simple Network Management Protocol (SNMP) traps
- Logging to Syslog and security information and event management (SIEM) systems
- Flows to NetFlow collectors
- IPS can do everything on this list however a IPS system cannot drop packets or block addresses inline. They can still take aggressive action, like sending a TCP reset to the sender and receiver or a block or a shun on a upstream or downstream firewall or router

Intrusion Detection vs. Prevention

- You have to tune your IDS and IPS systems
- True Positive -> True (accurate) + positive (action taken)
- True Negative -> True (accurate) + negative (action not taken), e.g. identify but not take action
- False Positive -> False (error) + positive (action taken), e.g. password changes (mistype)
- False Negative -> False (error) + negative (action not take), e.g. error when an action wasn't taken, payload was delivered and IDS or IPS did not detect it or prevent it.

Jump Boxes and Bastion Servers



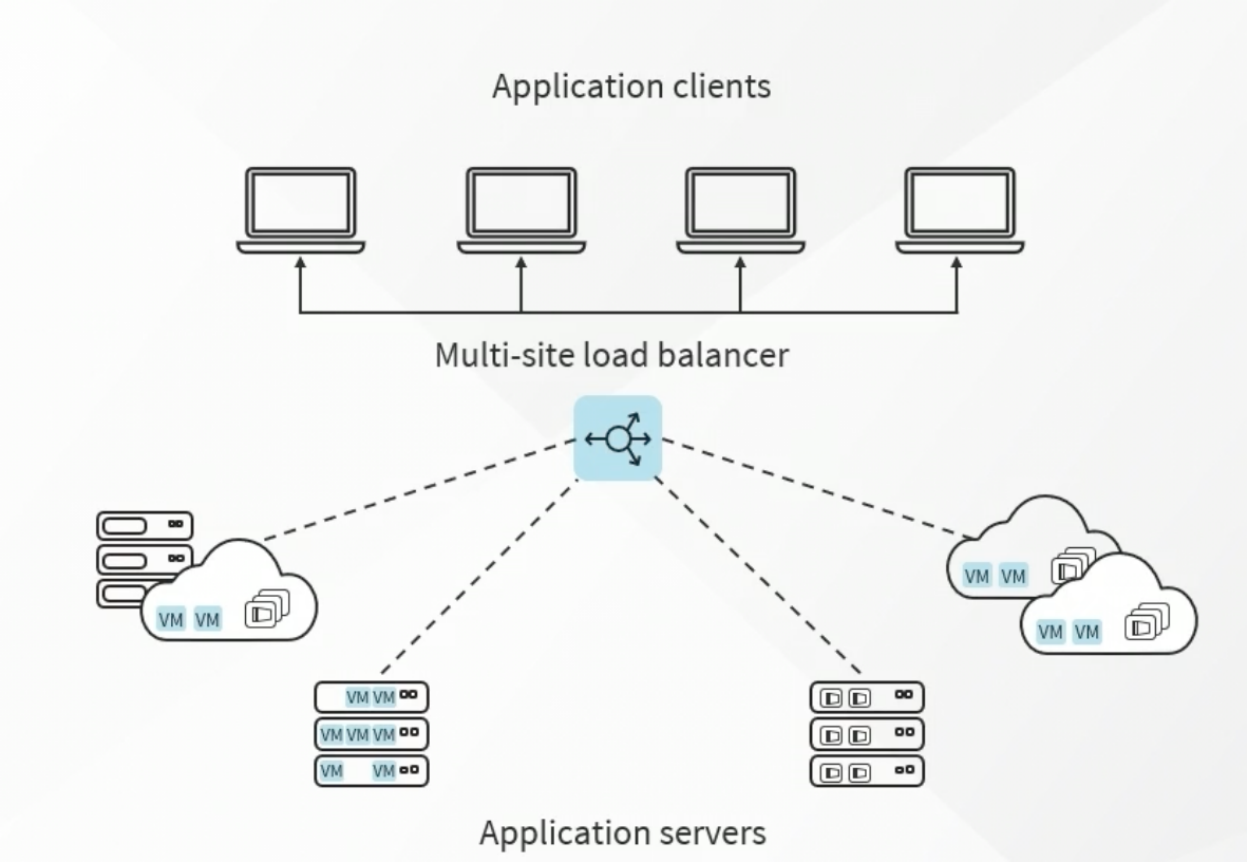
-
- When admins use secure shell 1 or 2 or RDP to Microsoft systems, instead of directly connecting to those devices they will connect to a jump box or what is known as a bastion server. We have a cloud environment (AWS) the remote admin wont connect directly to the MySQL instance or

another EC2 instance, they will deploy a virtual machine, for example UBUNTU or WINDOWS SERVER in a public subnet. They authenticate and authorize to that jump post or that jump box and from there they will administer and manage virtual machines and services in the backend subnet.

Proxy Servers (Mediated Access)

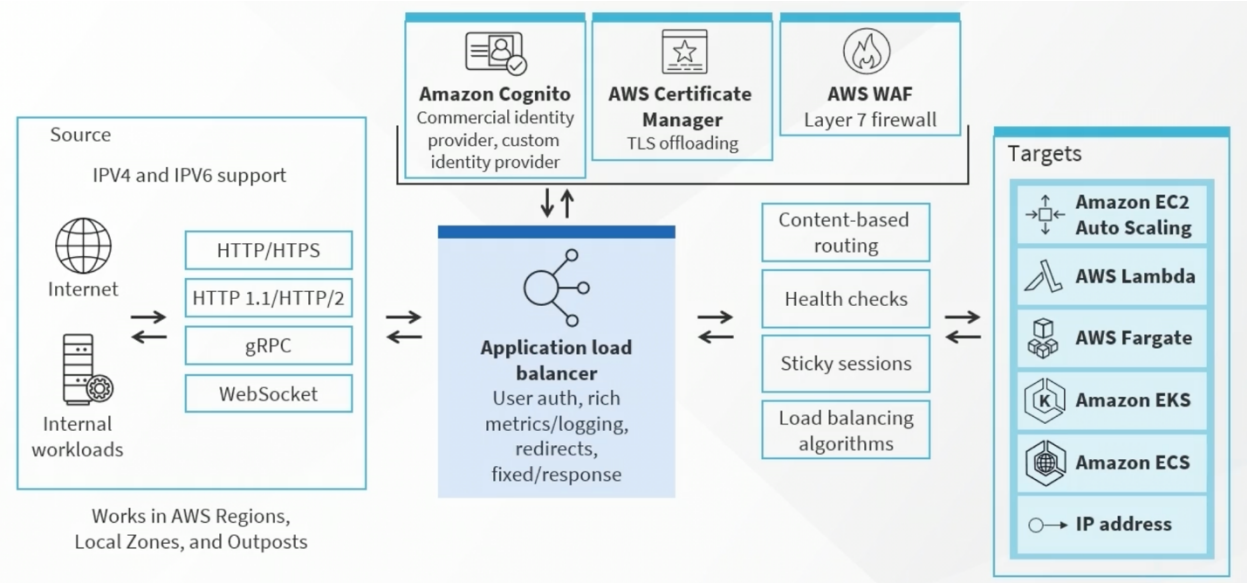
- Jump boxes and jump posts are one example of proxy servers or mediated access
- Authentication (interactive or transparent)
    - If they are interactive they will present the user with a login screen
    - If they are transparent they will authenticate and authorize on behalf of the client and server
- Translation services – Network Address Translation (NAT)
- Bastion (jump) servers and cloud service provider (CSP) managed services
- Web proxies for content storage and security
- URL filtering
- Managed security service providers (MSSP)
- Cloud access security brokers (CASB)

Load Balancers



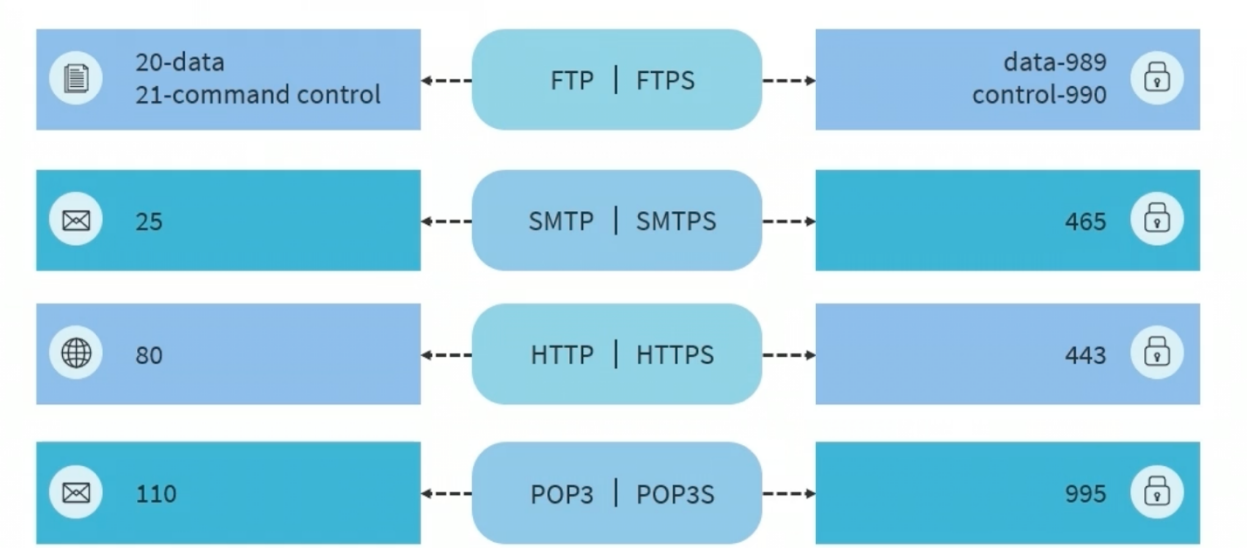
- In your intranet the load balancer is often used to improve the experience for the application clients. Can be a single site or multi site load balancer, where the traffic to and from the services is being load balanced across active clusters of application servers. Provides reliability, provides fault tolerance, and improves the delivery of audio, video, voice over IP for the application clients

Cloud Load Balancers

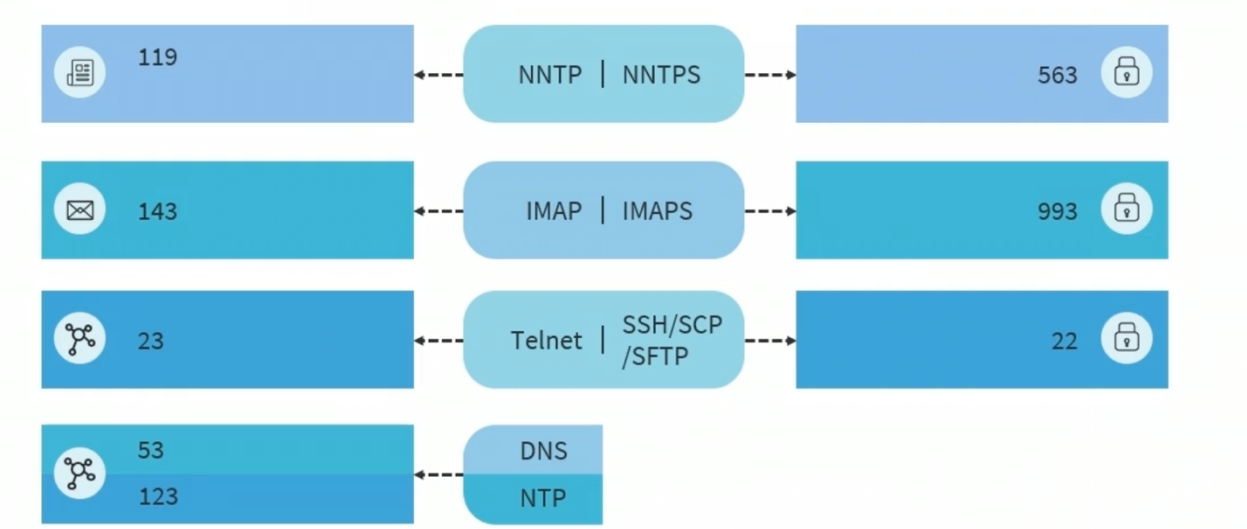


-
- Load balancers are extremely popular in the cloud. When you use your web browser it is the common places you go to when you click on the hyperlink or put in the domain name of a website. Cloud load balancers can support IPv4 and IPv6 by using transport layer security and web socket APIs. The load balancer will often run a certificate server or a TLS offloading service so it can decrypt the traffic for the layer 7 web application firewall. The cloud load balancer produces flow logs for active defense, health checks against backend targets. For example auto scaling groups of instances or appliances (FaaS, CaaS, IP addresses)

Common Port Numbers



-
- Left hand sign, FTP uses two different ports (20 for the actual data, 21 for command control). If your using FTP over SSL/TLS then the ports will be 989 for data and 990 for control. For SMPT (sends email to mail exchanges) uses TCP port 25 or for SMTP over SSL/TLS it uses 465. HTTP uses port 80 and over SSL/TLS it uses 442. POP3 uses port 110 and over SSL/TLS it uses 995. All of these services use TCP



-
- NNTP (network new protocol) is a older protocol that uses 119 and over TLS/SSL 563. Client for email is IMAP which uses TCP port 143 and over SSL/TLS it uses 993. Telnet is not used anymore but it used 23, but SSH/SCP and SFTP all use 22. DNS can use TCP or UDP port 53 and NTP (network time protocol) uses port 123. All of these services other than DNS when performing a query are going to be using TCP.

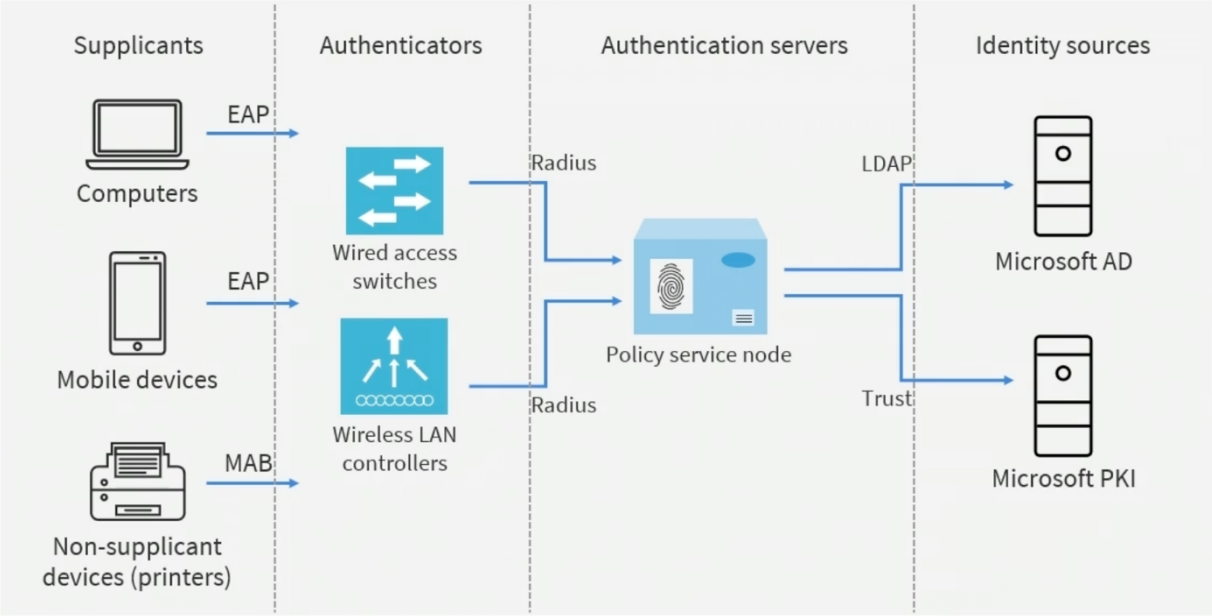
802.1X Port-based Network Access Control (PNAC)

- IEEE 802.1X authentication is also referred to as port-based network access control, or PNAC
- It involves making sure something interfacing with the system is what it claims to be
- When someone wants to gain access to an Ethernet or 802.11 wireless network, it verifies the entity connecting is who they say they are in flexible ways

802.1X Capabilities

- Pre-admission control to block unauthenticated messages
- Identify users and devices with predefined credentials or machine IDs
- Conduct both authentication and authorization. Uses radius for its authentication service
- Onboarding and provisioning devices in a Zero Trust environment
- Supporting Attribute-based Access Control (ABAC)

IEEE 802.1X



-
- The devices that want to get on the network are called supplicants. Devices are called Supplicants but also they are often running a agent, either a native agent to the operating system or something like a client. .1x will also identify certain ports like ethernet ports to be reserved for non-supplicant devices like printers. The .1x supplicants will send EAP messages to authenticators. This can be wired-access switches, access gateways or servers, or wireless access points managed by wireless LAN controllers. They will communicate the credentials back to the authentication servers, that will be radius or the new version diameter. The identity source could be on the radius server, but more often than not they will communicate back to the identity provider such as Microsoft active directory or some PKI cert authority. Then if they are allowed they will send the authentication and authorization information back to the authenticators and they can make a decision to either put the supplicants on a restricted or guest VLAN or deny them altogether. Because it supports ABAC it can have authorization policies for a wide range of attributes and characteristics of the supplements

Extensible Authentication Protocol (EAP)

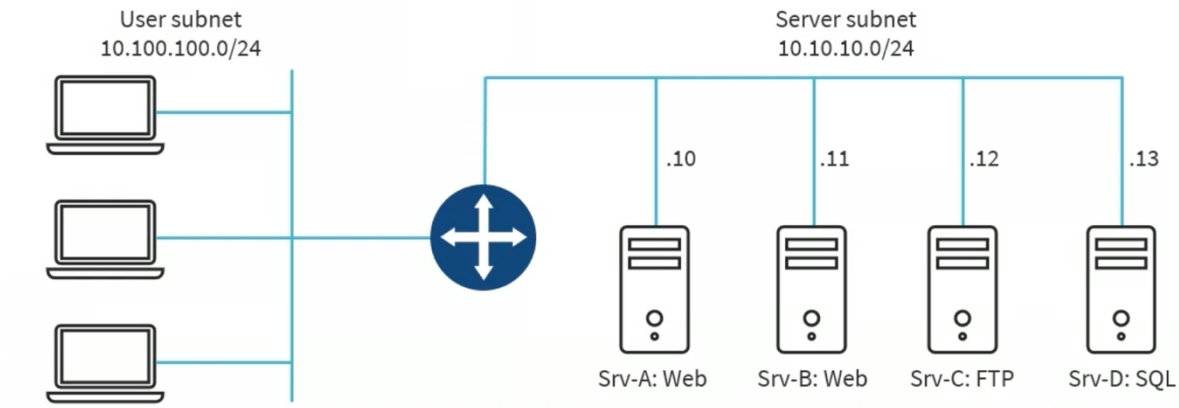
- Extensible Authentication Protocol (EAP) is an authentication framework as opposed to a specific authentication mechanism
- It has evolved over the years from the original Point-to-Point Protocol (PPP)
- It is often used in 802.1X wireless networks and point-to-point connections
- It offers some basic functions and negotiation of authentication methods called EAP methods
- There is typically an original EAP over LAN (EAPOL) exchange before the higher methods are implemented

Extensible Authentication Protocol

802.1X EAP Types Feature/Benefit	MDS ---- Message Digest 5	TLS ---- Transport Level Security	TTLS ---- Tunneled Transport Level Security	PEAP ---- Protected Transport Level Security	FAST ---- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	Yes	Yes	No (PAC)
Wired Equivalent Privacy (WEP) key Management	No	Yes	Yes	Yes	Yes
Rogue Ap detection	No	No	No	No	Yes
Provider	MS	MS	Funk	MS	Cisco
Authentication attributes	One way	Mutual	Mutual	Mutual	Mutual
Deployment difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

-
- Table of the higher methods. Don't use MD5 anymore, the most secure environment would be EAP TLS which uses X509v3 certificates and performs client side and server side certificates. This has the most difficult deployment because of having to introduce a public key infrastructure or enterprise certificate authorities. With tunneled TLS you don't need to have a client side certificate just a server side certificate. Protected EAP is very common in Microsoft environments, they actually invented it, and EAP FAST is a secure option cisco solution. For cisco environments that don't want to use EAP TLS with x590v3 certificates. Instead it will use a PAC file on the client and the server.

Access Control Lists (ACLs)

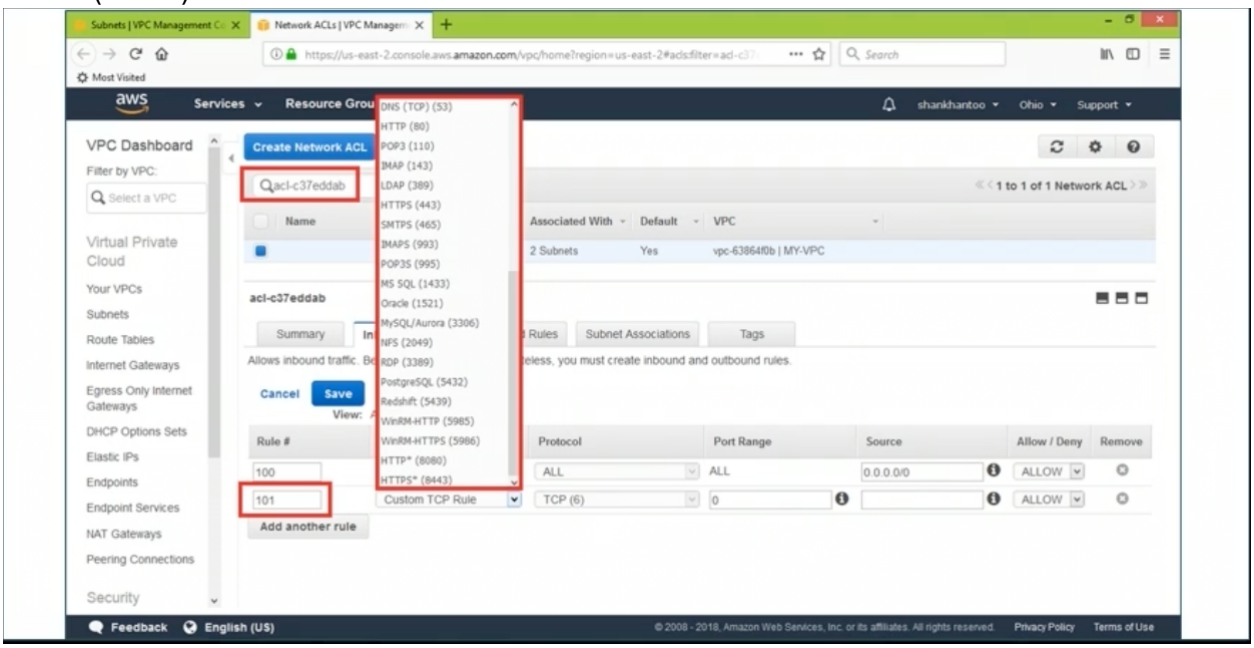



```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data
Access-list 100 deny ip any log
```

-
- Simply a list of access control entries that permit or allow and deny traffic based on the headers of IP and TCP or IP and UDP or IP and ICMP. Access control lists are ordered list, so they start with the first entry and process all the way down. They are matching on different protocols and services, and different ports and port numbers. and the final entry is an explicit deny so that if nothing matches it will send a log to a SNMP server or a SIM system. This entry is not necessary unless you want to log because ACLs have an implicit deny at the end so if nothing matches it will

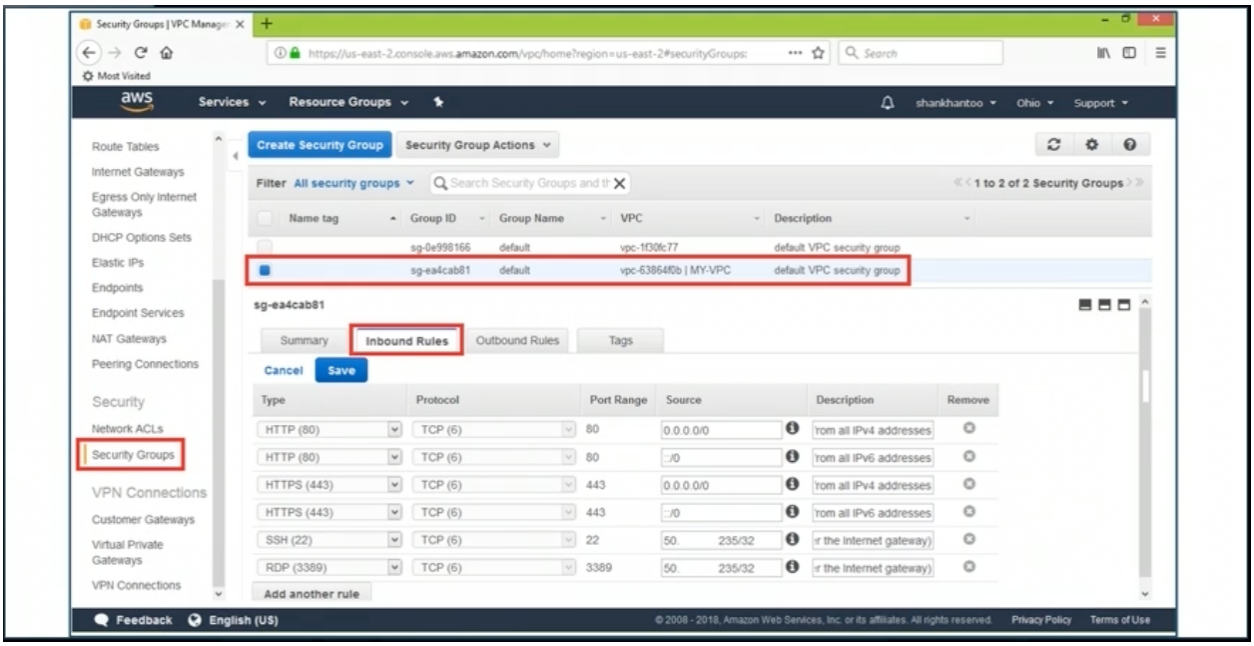
deny the traffic. www can actually represent as a token to a number of different ports -> can have HTTP on port 80 or port 80000, whatever you want that placeholder to represent. Using ftp and ftp-data (20 and 21). Important to understand how to construct and interpret access control lists

Network ACL (NACL)

- 

- AWS. Has rule numbers (starting with 100). Matching on different services and ports and protocols for UDP, TCP, ICMP. Allowing and denying based on src address. Sidr means any source (0.0.0.0/0). If using network ACL in the cloud it has a implicit deny at the end (no match, no traffic). ACL are static or stateless -> have no idea if the traffic is part of a existing TCP connection etc. Just looks at traffic one at a time and provides an allow or deny

Stateful Cloud-based Firewall

- 

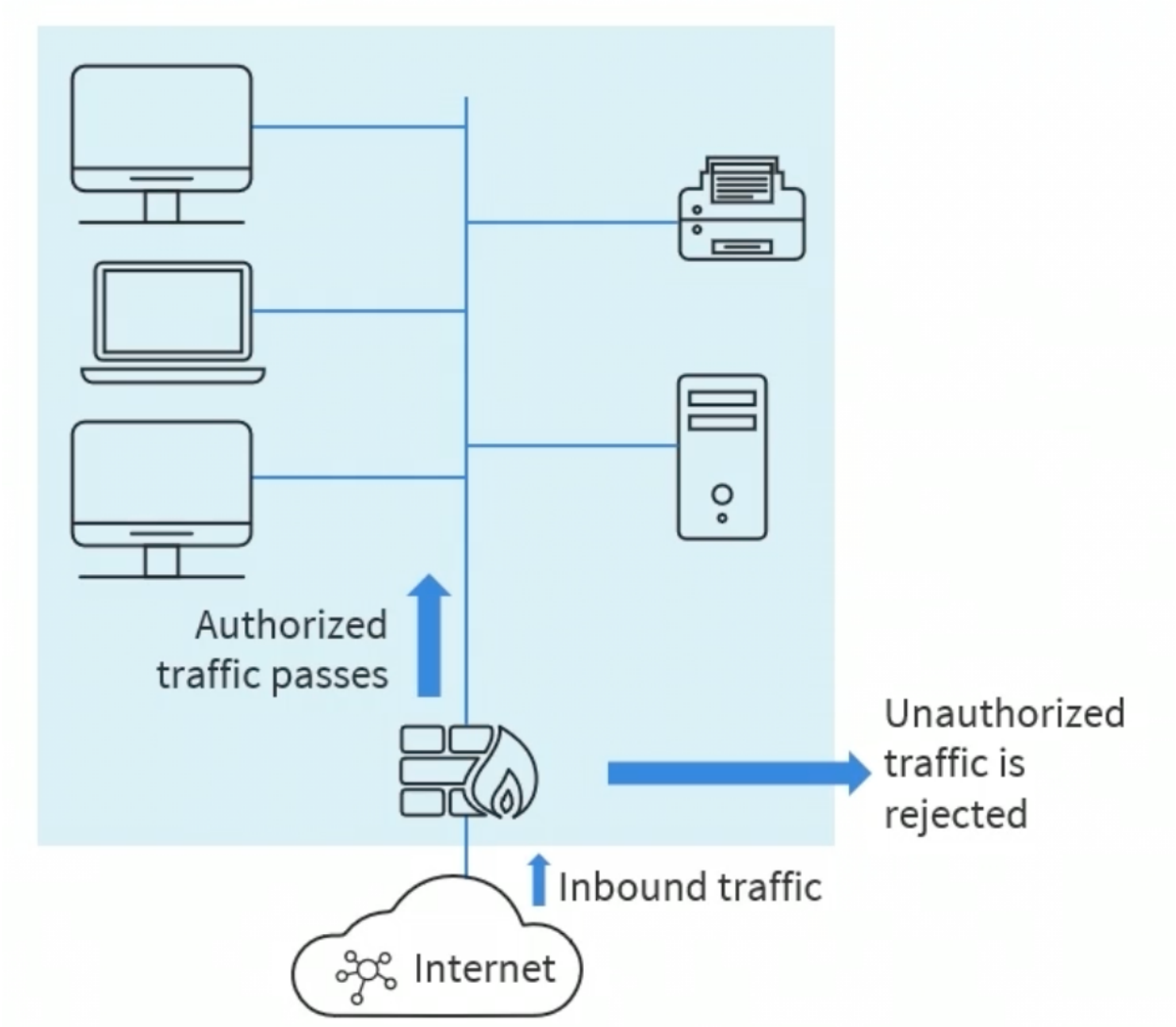
- Stateful cloud based firewall. These firewalls are called allow lists. Has inbound and outbound rules but they are placed on a specific instance so technically they are applied to the ETH0 of the windows or Linux or macOS virtual machine instance. Here in this allow list we are allowed HTTP, HTTPS, SSH, and RDP traffic to this front-end web server on both IPv4,v6. When it compares these

rules to the packet or datagram if there is not a matched then it is not allowed. Everything on the list is processed before the decision is made, there is no numbers, there is no allow or permit or deny capability, this is an allow list you cannot have explicit deny entries – use an access control list

Next-generation Firewalls

- Whether they are deployed on premise, or virtual cisco, juniper firewall in the cloud, they have common characteristics
- Firewall is not to prevent a fire from starting we use anti-virus, anti-malware and other use policies to prevent a fire from starting
- A firewall is a metaphor representing software and/or hardware controls that can limit the damage spreading from one subnet, virtual local area networks (VLAN), zone, or domain to another
- It is typically deployed as a barrier (zone interface point) between an internal (trusted) network and an external (untrusted) network
- They are integrated systems of threat defense functioning at layers 2-7 and can be categorized as network or application firewalls

Next-generation Firewalls



-
- Layer 5-7 policies (deep packet inspection) -> can permit or deny based on the behavior of the application and packet.

- Authentication proxy (interactive or transparent)
- Identity services for ABAC and advanced identity management
- Integrated IDS/IPS (also cloud-based)
- Content security with URL filtering and data loss prevention (DLP)
- Cloud correlation and integration for advanced malware protection including ML and AI engines
- Botnet filtering for advanced distributed denial-of-service (DDoS) protection
- Unified threat management

Unified Threat Management
- Most modern networks transmit more than just basic data transit and email traffic
- UTM typically provides multiple security features and services on a single network device
- It can protect email, webmail, fax, voice, conferencing, streaming, peer-to-peer file transfer services, and more
- UTM could be considered the first huge step to evolve into modern-next-generation firewall solutions

Web Application Firewall (WAF)
- Also called a web security gateway (WSG), it is usually an appliance (physical or virtual), server plugin, or virtual firewall running in a hypervisor or cloud deployment
- It protects HTTP and HTTPS (TLS) traffic at layers 5 through 7 of the OSI reference model
- Typically, these rules cover common web attacks, such as cross-site scripting (XSS), request forgeries, and SQL injection
- Typically deployed as dynamically configured WebACLs and Anti-DDoS engines with other threat management services
- The AWS WAF is commonly deployed on an elastic application load balancer, CDN distribution, or API gateway

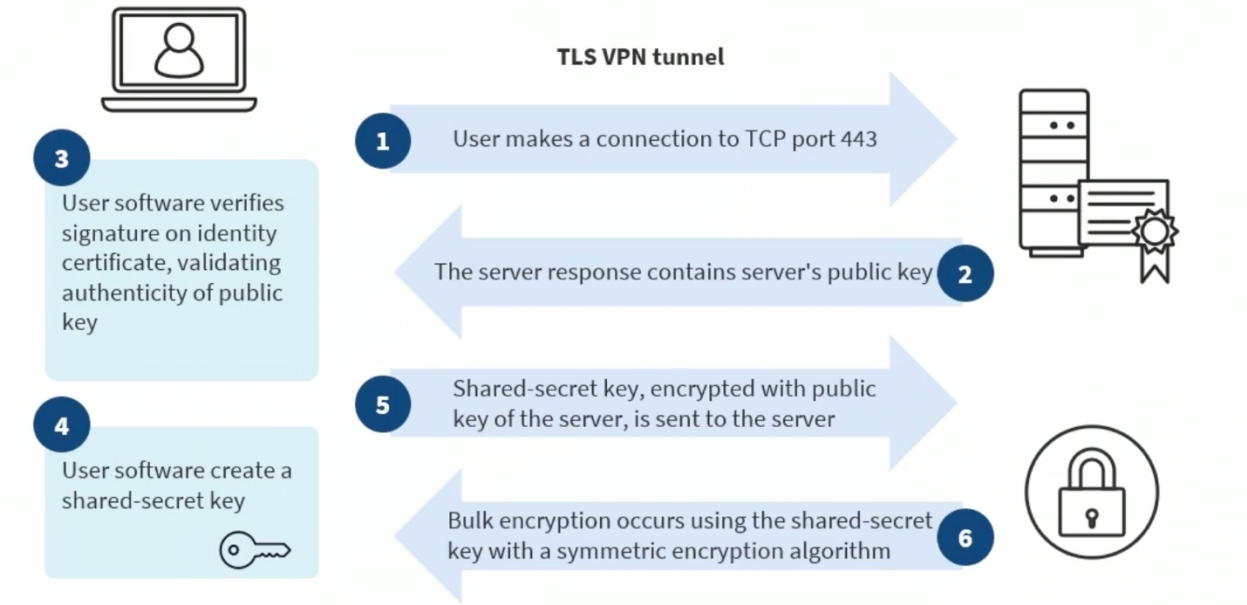
Examining Virtual Private Networks (VPNs)
- Site-to-site VPN is made up of two components
    - Customer gateway (1. Name it, 2. dynamic routing protocol (boarding gateway protocol, 3. How do we identify the device on the other side of the VPN tunnel e.g. regional office of business, 4. Certificate manager (x509.v3 certificate for that particular device), 5. Add tags (configuration management), 6. Create)
    - Virtual private gateway (1. Name it, 2. Add autonomous system number, 3. Add tags, 4. Create.
    - Create VPN connection (1. Name it, 2. Select virtual private gateway, 3. Select customer gateway, 4. Use dynamic routing with boarder gateway protocol, 5. Have options for IPv4 for the network (customer side, or regional office side), 6. Cloud side IPv4 (use in VPN subnet of cloud provider), 7. Tunnel options (using IPsec you have two tunnels that are logical and the tunnels need IPv4 addressing, we can use the cloud provider and they will provide it (e.g. 169.254.0.0) then we can see things like logic and activity log. 8. Can edit tunnel 1 options if needed

Examining IP Security (IPsec)
- With IPsec you have two options, can use ikev1 (old, deprecated) which has two phases. phase 1 is a pairing session between two endpoints (e.g. virtual private gateway and customer gateway). Generally going to use ikev2 (phase 2) which will be more robust and support a newer security suite and algorithms. With IPsec both sides have to come with an agreement with what they will use for encryption, HMAC (for integrity and authentication), what DH group they will use to create

the shared secret keys over this untrusted network. On the provider side, at the cloud provider, they will offer everything (from older less secure of SHA to deprecated DH numbers) but also up to the more robust solutions. On the customer side I will be offering up a combination (policy or suite) to this virtual private gateway with the more secure options, so regardless of what we use it will match. A general concept between the client and the server (e.g. customer gateway, and virtual private gateway) we will want to use the most robust options that both sides support. Both sides have to support these newer algorithms. Lifetime it doesn't have to match. On the virtual private gateway side it will do 12 hours (28,800 seconds). Don't have to match but when the security association is set up the tunnel is set up it will use the lowest lifetime between the two because that is more secure. with IPsec if we are using the encapsulated security payload protocol which we always use over the internet not authentication header we will have encryption. Have to match on the encryption algorithms, integrity HMAC you will use and the DH numbers.

Transport Layer Security (TLS)

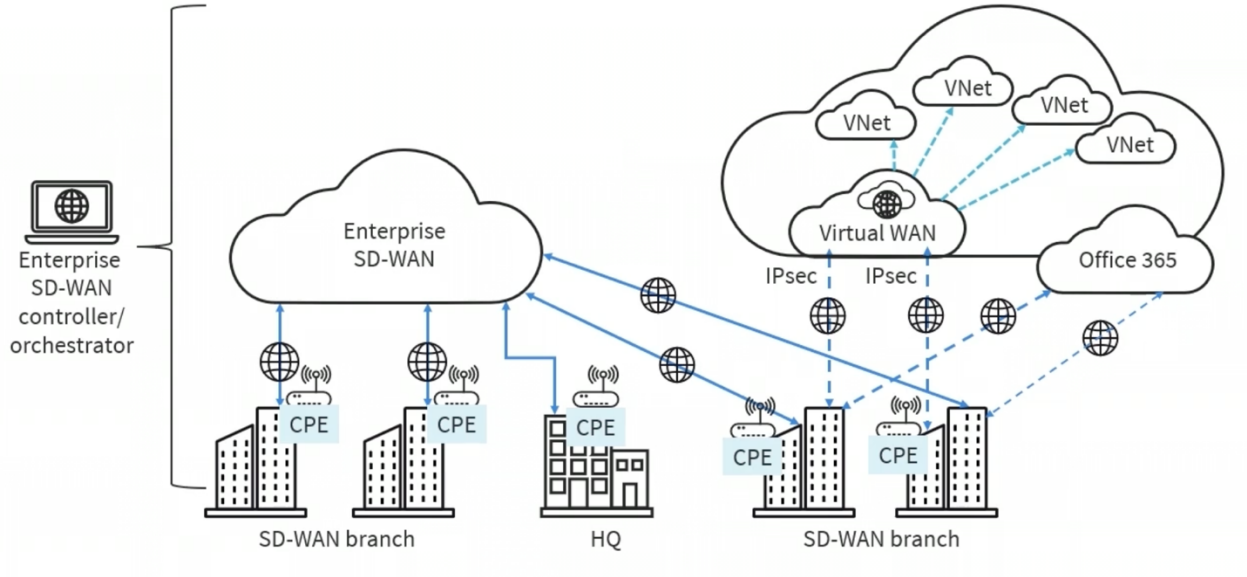
- Transport Layer Security (TLS) is the latest iteration of SSL
- TLS is the most ubiquitous certificate-based peer authentication in use on the internet (HTTPS)
- TLS 1.3 is the most recent published version and should always be used unless the client only supports version 1.2
- It includes a record protocol and a highly extensible handshake protocol
- It is also used with SMTP, Lightweight Directory Access Protocol (LDAP), and Post Office Protocol 3 (POP3)
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures
- Although TCP-based, most servers perform single-packet authentication and mutual TLS instead



-
- TLS used TCP therefore in step 1 when single packet authentication and TLS are not used the user will make a TCP connection to port 443, the server response will contains the servers public key. Then the user software verifies the signature on the identity certificate validating the authenticity of the public key. The user software then generates a shared secret or session key. The shared secret session key encrypted with the public key of the server is sent back to the web server. Then bulk encryption occurs using the shared secret key with the symmetric encryption algorithm (AES-128.256).

SD-WAN

- Software-defined wide area network (SD-WAN) is a software-defined networking (SDN) approach that raises network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- SD-WAN incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management
- It is also called SD-MAN for a metropolitan area network fiber deployment

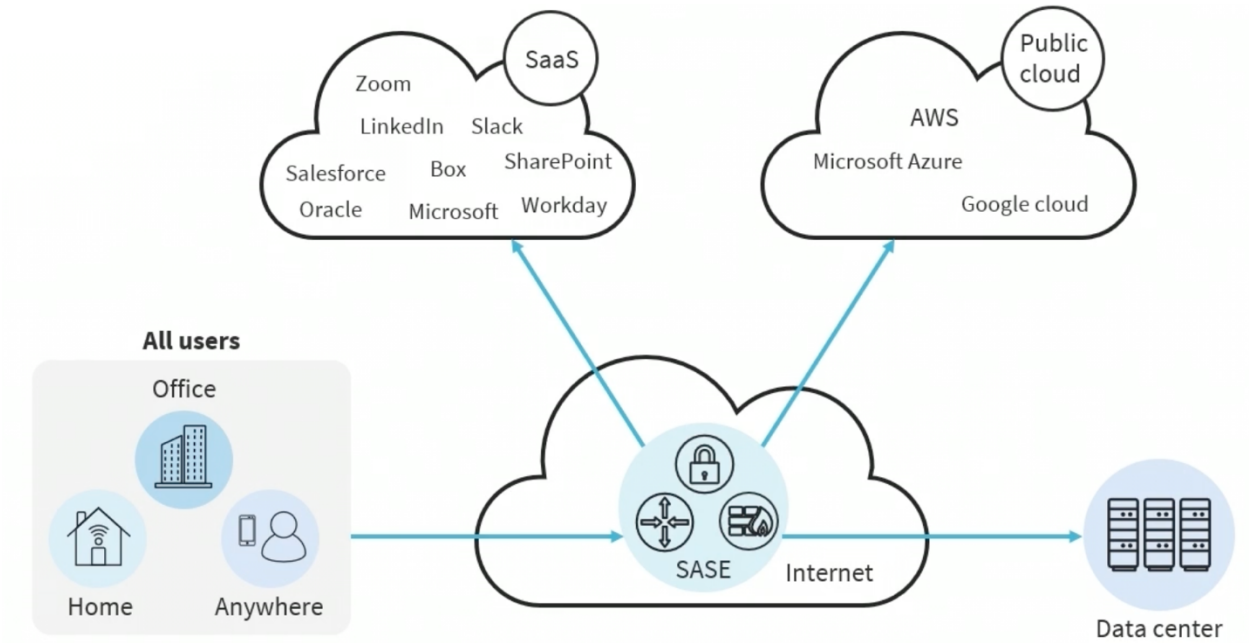


-
- SD-WAN with Microsoft Azure. Have a virtual WAN component running in the Azure cloud. Behind that virtual WAN controller you have multiple virtual networks and enterprise control to automate and orchestrate the various remote offices (e.g. headquarters). All of the sites are being managed through API calls to their customer premises equipment, automated and orchestrated from enterprise SD-WAN controllers running in the Azure cloud. Then you can make connections over the wide area network with IPsecv2 or transport layer security. Can also have federated access or single sign on access to SaaS solutions (e.g. Office365).

Secure Access Service Edge (SASE)

- Secure access service edge (SASE) is an architecture that delivers converged network and Security as a Service (SaaS) capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access (ZTNA)
- These functions are delivered from the cloud and provided as a service by the SASE vendor such as Cisco systems or Fortinet

SASE



-
- All users regardless of where they are (e.g. home, hotel) get secure access through controllers to a wide variety of SASE solutions, to the public cloud of AWS, google cloud as well as limited access to services or data running on the onsite or on premise data center running on the internet.

Data Protection Concepts and Strategies

Data States: At Rest

- Data at rest is data that has arrived at a destination in a file system, database, or object storage (disk, tape) and is not being accessed or used, for example over a network or in RAM memory
- It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory or Redis cache waiting to be read or updated
- Data at rest is data that is not dynamically moving from device to device or network to network

Data States: In Transit

- Data in transit is being packet forwarded or switched over a wireless or wired network in a unicast, broadcast, multicast, or anycast fashion
- Examples include:
    - Wired Ethernet
    - Cable (DOCSIS)
    - Fiber optic
    - 802.11 wireless
    - Cellular
    - Satellite
    - Personal area networking using RFID, Bluetooth, Infrared, Zigbee, and more

Data States: In Use

- This is active data undergoing processing, translation, analysis, change, or other manipulation
- Examples include:
    - Data in system RAM memory
    - CPU registers
    - Caches and buffers
    - Data in Memcached or Redis clusters
    - Database transactions
    - Cloud-based file or code being modified in real-time by one or more users

Data Classifications

- In early phases of data lifecycle it is important to classify data if it is pertinent to your environment or access control models

Data Classifications: Government and Military

- Sensitivity is based upon a calculation of the damage to privacy and security that an exposure of the information would cause
- The US has three levels of classification: Confidential, Secret, and Top Secret
- If one holds a Top Secret security clearance, they are allowed to handle information up to the level of Top Secret, including Secret and Confidential information
- If one holds a Secret clearance, they may only handle Secret and Confidential classified information – not Top Secret

Data Classifications: Public and Commercial

- There are five common categories used for data classification in various business and commercial sectors:
    - Public data

        - May be important, but it is accessible to the public. Since this data is openly shared, it is the lowest level
    - Private data
        - Requires a greater level of security than public data. It should not be available for public access and is often protected through common security measures such as passwords
    - Internal data
        - Is usually limited to employees only and often has different security requirements that affect who can access it and how it can be used
    - Confidential data
        - Information should only be accessed by a limited audience that has obtained proper authorization using strict identity management or access control environments
    - Restricted data
        - Classification is reserved for an organization's most sensitive information. Access to this data is strictly controlled to prevent its unauthorized use

Data Types

- Regulated data
    - Information that its use and protection is dictated by a government agency or third-party agreements
- Trade secrets
    - Any practice or process of a company that is generally not known outside of the company
- Intellectual property
    - Creations of the mind, such as inventions, literary and artistic works, designs and symbols, names and images used in commerce
- Personal health information (PHI)
    - The demographic information medical histories, test and lab results, mental health conditions, insurance information and other data
- Personally identifiable information (PII)
    - Any representation of data that allows the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means
- Legal information
    - Involves the careful reading about specific clauses or stipulations that does not constitute "advice"
- Financial data
    - Quantitative information used by organizations to make financial decisions and data concerning a company's financial health and performance
- Human and non-human readable
    - Some human-readable formats, such as PDF, are not machine-readable as they are not structured or semi-structured (JSON/YAML) data

The Data Life Cycle

- 

The Create Phase

- Create phase is one of the mandatory phase of the lifecycle. The concept of data minimization should be applied, don't create data, don't generate it, don't purchase it, unless it has utility, unless you want the data to become information and the information become knowledge
- Data is either generated from scratch, inputted, acquired, purchased, or modified into another format
- The data owner, stewards, and custodians (if applicable) are identified in this earliest phase
- Other key activities of phase one include:
    - Data discovery
    - Data categorization
    - Data classification
    - Data mapping
    - Data labeling (tagging)

The Store Phase

- Optional phase
- The data is put onto a volume (block), object (blob), or file storage system or into one of several types of database systems
- This phase relates to the optional transactional, near-term usage data as opposed to long-term cold data storage
- Activities of this phase can also occur simultaneously when the data is generated in phase one

- Protection of data at rest and data in transit will often occur in this phase unless default encryption is implemented in the create phase

The Use Phase
- Second mandatory phase
- In this mandatory phase, data is utilized by people, applications, services, and tools as well as being changed from the original state
- This is where raw data becomes information, then knowledge, then wisdom
- If data is used remotely then protection mechanisms must be in place (virtual private network (VPN), secure endpoints, digitally signed application protocol interface (API) calls)
- The systems that "use" the data must be secured as well; for example, endpoint detection and response (EDR) or host-based intrusion prevention system (IPS) agents (Palo Alto Cortex XDR)

The Share Phase
- Optional Phase
- In this optional phase, data is visible, analyzed, and apportioned among users, systems, and applications
- Data can be shared in a client-server, peer-to-peer, or distributed manner
    - Global collaboration and sharing of data introduces obvious risks and lack of control
- Most of the control used in the previous phases will be implemented here in phase four (such as information rights management (IRM) and data loss prevention (DLP) services)
- Stringent Identity and Access Management (IAM) and/or Identity Management (IdM) should be used to enforce the least privilege

The Archive Phase
- Optional phase
- In this optional phase, data is stored for the long-term and removed from active usage
- Archiving is based on regulations, governance policies, and/or best practices
- Stringent cryptography will be introduced for data at rest – as in AES-GCM-256 AEAD solutions
    - AEAD stands for authenticated encrypter associated data. When using AES-GCM you don't have to have a separate HMAC it has its own integrated GMAC
- Archiving is often automated and based on Intelligent Tiering or Storage Gateway management over a high-speed connection to cloud providers
- Costs are based on retrieval options

The Destroy Phase
- Data is no longer accessible or usable based on lifetime, utility, policy, governance, and/or regulations
- The organization should have their own established methods for disposal of data and media, often using military grade programs or physical destruction such as crushers and furnaces
- Although data can be disposed of using a variety of methods, when storing data at a cloud provider, crypto-shredding (cryptographic erasure) is the only practical and comprehensive solution

Securing Data: Geographic and Cultural Restrictions
- A major value proposition of cloud computing and content distribution is the ability to store and share data to edge locations all over the world
- When storing or sharing data and content, all local laws and regulations must be considered and obeyed

- Attention must be paid to the right of privacy in different countries, as well as the presence or absence of a data protection law
    - There may be import/export laws or mandates such as the EU General Data Protection Regulation (GDPR) data privacy in play
- It is a best practice though choose a safe country where the government is politically stable when distributing data or content
- A data center should not be deployed in a location that has the potential for instability
- Data analysts and architects should consider the potential lower costs of raw materials, labor, energy costs, and taxation
- Cultural and religious norms and sensitivities must also be considered for the storage of data and the dissemination of content

Securing Data: Cryptographic Hashing

- By hashing the data before storing it in a database, one can prevent unauthorized parties from reading or changing it without knowing the original data or the hashing algorithm
- It is common for systems like directory services to hash the passwords of users so that they can be verified without exposing the plain text
- Examples of trustworthy hashing algorithms for securing sensitive data in a database include SHA-256, SHA-512, bcrypt, scrypt, and PBKDF2
- Choose a hashing algorithm that meets all policy requirements and that is supported by tools and utilities
- Generate a salt for each data input that is hashed with a built-in function or library
- Hash the data input and salt with the chosen algorithm
    - It is essential to use the same hashing algorithm and salt for the same data input every time it is hashed
- Employ a secure connection to the data storage or database to offer protection of data-in-transit

Securing Data: Encryption

- Encryption at rest is encryption that is used to help protect data that is stored on a disk (including solid-state drives) or backup media
- All data that is stored by an organization, whether on-premises or in the cloud, should be encrypted at the storage layer using the Advanced Encryption Standard (AES) algorithm, AES-256

Securing Data: Encryption

- The separation of duties and least privilege principles should be applied to all subjects who are authorized to administer encryption policies and key management
- It is critical to remember that many drives that store data are removable and portable
    - Data at rest can also reside on removeable memory cards
- A common solution for many organizations is to employ hardware security modules (HSMs), CloudHSM, and micro HSM on memory cards

Securing Data: Obfuscation

- Obfuscation is a generic term that applies to any mechanism that makes data less decipherable
- The goal is to render data unreadable or to hide aspects of personally identifiable, personal health, or corporate intellectual property information
    - “Obscuring” is a concept where static or dynamic techniques are used on the original data or a representational data set
    - “Shuffling” is a term that describes utilizing characters from the same data set to further present the data

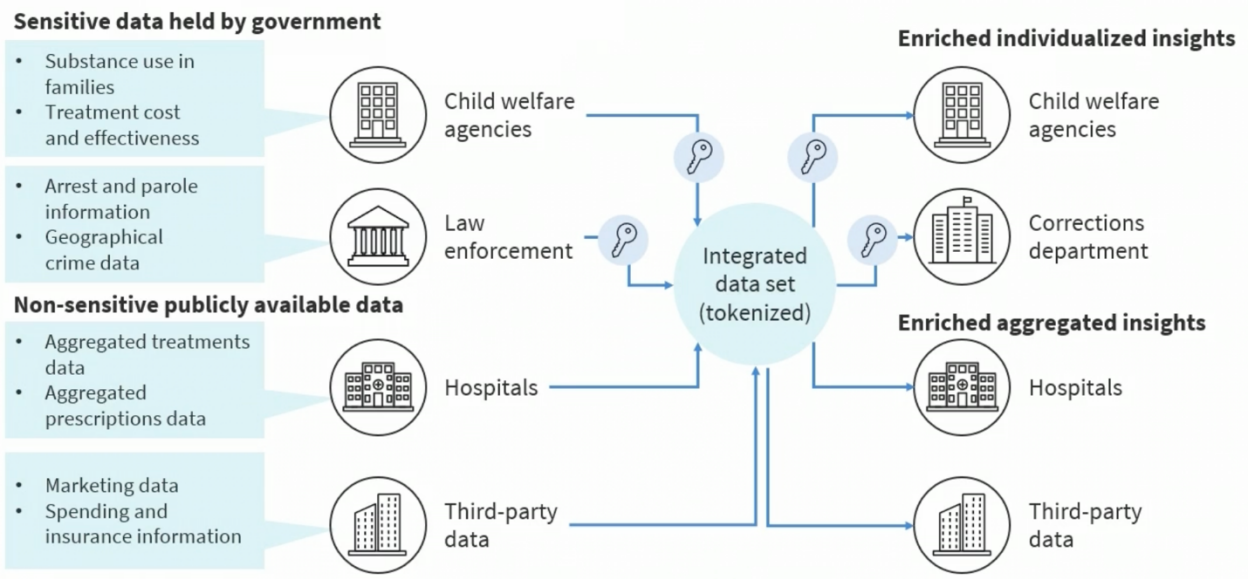
- “Randomization” is when all or some of the data is replaced with indiscriminate characters

Securing Data: Masking

- Data masking often involves using characters like “X” to hide some or all data
- Example is to only display the last four digits of:
  - Social security number
  - Credit card number
  - National ID number
  - Bank account number
  - Username or email address
- Masking is considered a suboptimal data obfuscation method since it is subject to inference

Securing Data: Tokenization

- Tokenization involves sending sensitive data through an API call (or batch file) to a system or cloud provider service that replaces the data with non-sensitive, pseudorandom placeholders called tokens
- Unlike encrypted data, the tokenized data is irreversible and unintelligible
- The practice involves two distinct databases
  - One with the actual sensitive data
  - One with tokens mapped to each chunk of data



-
- Many entities that want to use information about the minors for a wide variety of use cases; child welfare agencies, correctional departments etc. However in order to do those things with the data it must be obfuscated aka tokenized. A form of digital redaction. When the data goes through the integrated dataset and gets tokenized (at cloud provider) is everything tokenized, no, just the sensitive information. Most of it will be in the clear so it can be used by third parties, like hospitals and agencies.

Securing Data: Segmentation

- Data segmentation is a process of dividing and organizing data and information into defined groups to enable:
  - Handling
  - Labeling
  - Sorting
  - Viewing

    - Securing
- Segmented data offers a team or group with segregated, clear, actionable information
- Data segmentation involves grouping data into at least two subsets, although more separations may be necessary on a large network with sensitive data.
    - Maybe a multi-national company doing data dispersion or segmentation across multiple cloud providers.
- Data should be grouped based on:
    - Use cases
    - Types of information
    - Sensitivity levels
    - Separation of duties policies
    - Level of authority for access to that type of information

Securing Data: Compartmentalization

- Compartmentalization is regarded as a very powerful way to protect personal information
- It involves limiting access to information to only those people or organizations who need it to perform a certain task
- Originating in the military with classified information, the concept can be further understood with another military term: “managing the blast radius”
- Compartmentalization is equally about:
    - Spreading the risk so if there is any impact (breach), the damage is limited
    - Lowering the effect of recovery efforts

Resilience and Recovery

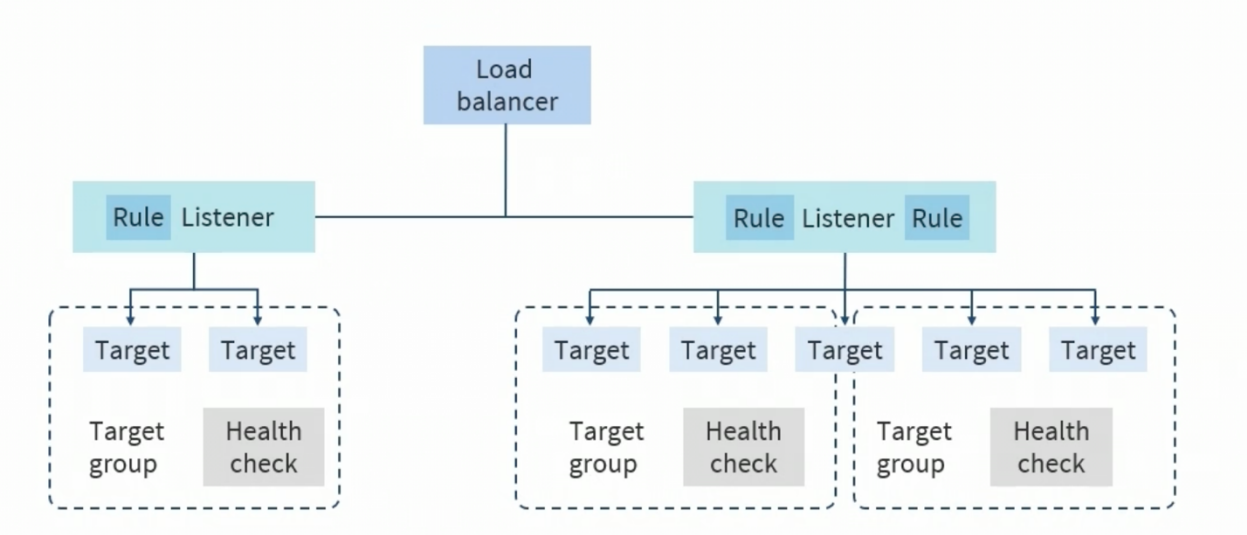
Load Balancing

- Load balancing devices and services are popular due to the usage of data and network intensive applications and services
- They can optimize application availability and performance
- They distribute Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Hypertext Transfer Protocol (HTTP), and Transport Layer Security (TLS) traffic across multiple servers to efficiently allocate resources and offer failover solutions
- Dedicated load balancing appliances and modules have become a standard component in physical and virtual networks
- All major network equipment vendors offer load balancing solutions to basically "put traffic in its place"
- These systems can optimize application availability and performance, distribute traffic across multiple servers, and offer (cluster) failover solutions. The endpoint (client) has a virtual IP address that is represented as a load balancer, which is load balancing on behalf of backend servers or services. For example load balancing across front end services in your intranet.

Load Balancing at Cloud Providers

- Network or application load balancing
- Often represents virtual network to the public based on IP address or public domain name
- Performs health checks on back-end instances and containers
- Produces flow logs for other threat management services
- Runs the TLS listener to decrypt traffic
- Can also have layer ¾ and web application firewall (web access control list (ACL))

Cloud Load Balancers



-
- Accepting requests from public internet (HTTPS, TLS). The load balancer has different firewall rules, stateful firewalls and a listener, possibly a certificate service representing traffic in target groups. The target groups are autoscaling or scaled out groups of virtual machines, like APACHE front end web services, or containers running on network operating systems. In the cloud you could consider that target group as a form of autoscaling clusters of virtual machines or clusters.

Clustering

- A primary target of modern load balancers is a cluster

- Clustering is intended to improve performance and availability of a complex physical or virtual system
- Clusters are designed to be a redundant set of service functionalities based on active-standby or active-active deployments
- Cluster deployments are often measured by:
    - Reliability – the ability to successfully provide responses on each incoming request
    - Availability – the uptime of the server (usually measured as % of annual uptime)
    - Performance – measured by the average of the time spent by the service to provide responses or by the throughput
    - Scalability – the ability to handle a growing amount of work in a capable manner without degradation in the quality of service

Clustering vs. Load Balancing

- Server clustering combines multiple servers and containers to operate as a single physical and/or virtual entity
- Load balancing distributes a workload across multiple servers to improve performance
- Both load balancing and server clustering technologies are often used together to coordinate multiple servers to handle a larger workload
- Server clusters typically require identical hardware and versioning to function optimally
- Load balancers can be used to distribute workload to different types of servers and can be more easily integrated into existing architecture
- These solutions have several common attributes:
    - To external devices, both technologies typically appear to be a single system that manages all requests
    - Both technologies often integrate reverse-proxy techniques that allow for a single IP address to redirect traffic to different IP or MAC addresses
    - Both were developed for managing a data center's physical servers but have been extended to applications, virtual servers, cloud servers, and containers

Clustering Techniques

- High availability clusters prioritize resilience over other advantages and can be implemented in either Active-Passive (standby device is on and running but not processing traffic) or Active-Active (where two or more are actively processing traffic) architecture
- Load balancing. Clusters highlight balancing the jobs among all of the servers in the cluster and incorporate load balancing software in the controller node
- High-performance clusters use multiple servers to execute a specific task very quickly and support data-intensive projects such as live-streaming and real-time data processing
- Storage clusters offer massive storage arrays, sometimes in support of high-performance clusters, but always in a support role for other servers or clusters such as storage area networking or hypervisor cluster data stores

Full Backups

- The process backs up everything regardless of whether the archive bit is set or not
    - Clears the archive bit once the backup completes
- This method takes the longest to back up and the time depends on how much must be backed up
- A full backup is quickest to restore as only the most recent full backup is required
- A full backup should be scheduled automated, and tested although it is common to perform this manually

Incremental Backups

- This method backs up any new file or any file that has changed since
    - The last full backup
    - The last incremental backup
- Subsequent backups only store changes that were made since the previous backup
- An incremental backup clears the archive bit once the backup completes
- The process of restoring lost data from an incremental backup is longer, but the backup process is much quicker
- It is not recommended to perform incremental backups manually

Differential Backups

- This method backs up any file that has the archive bit set
- Backs up any new file or any file that has changed since the last full backup
- A differential back up DOES NOT clear the archive bit when the backup completes
- It is slow to back up but quick to restore
- The last full backup and the most recent differential backup are needed for restoration
- It is not recommended to perform differential backups manually

Snapshots

- Snapshots are immediate point-in-time virtual copies of the source data. Could be data, entire elastic block store volume or machine image or virtual hard disk
- Offers easier and faster backups and restores
- Should be replicated to another medium or cloud storage to be considered a backup
- Time to back up does not increase with amount of data
- Improved Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Restores are fast
- Less data is lost with an outage
- Can easily be encrypted and decrypted

Backup Frequency

- Backup frequency is often based on the business impact analysis metric known as recovery point objective (RPO)
    - RPO is the maximum amount of data loss that you can tolerate in case of a disaster
    - The lower the RPO, the more frequently you need to back up you data
- The type of database management system (DBMS), data volume, data change rate, and performance needs all contribute to deciding the best backup strategy
- Commonly, full backups are conducted automatically or manually at least once a week, or more frequently depending on the criticality or latency of the data
- Differential backups should be done daily if the RPO is low or the data changes regularly
- Incremental backups should be done hourly if the RPO is very low or the data changes very rapidly
- Snapshots are common techniques for virtual data and should also be automated and scheduled based on various recovery points and time objectives

Journaling

- Journaling is also referred to as journal-based backup
- Journaling is the simultaneous (real-time_ logging of all data-file updates
- This log offers an audit trail and is used to reconstruct the database if the original file is damaged or destroyed

- Can also be used in e-discovery or forensic investigations or to track the kill chain of the advanced persistent threat actor
- Journal-based backup is an alternate method of backup that uses a change journal maintained by a hardware or software storage manager or server administrator

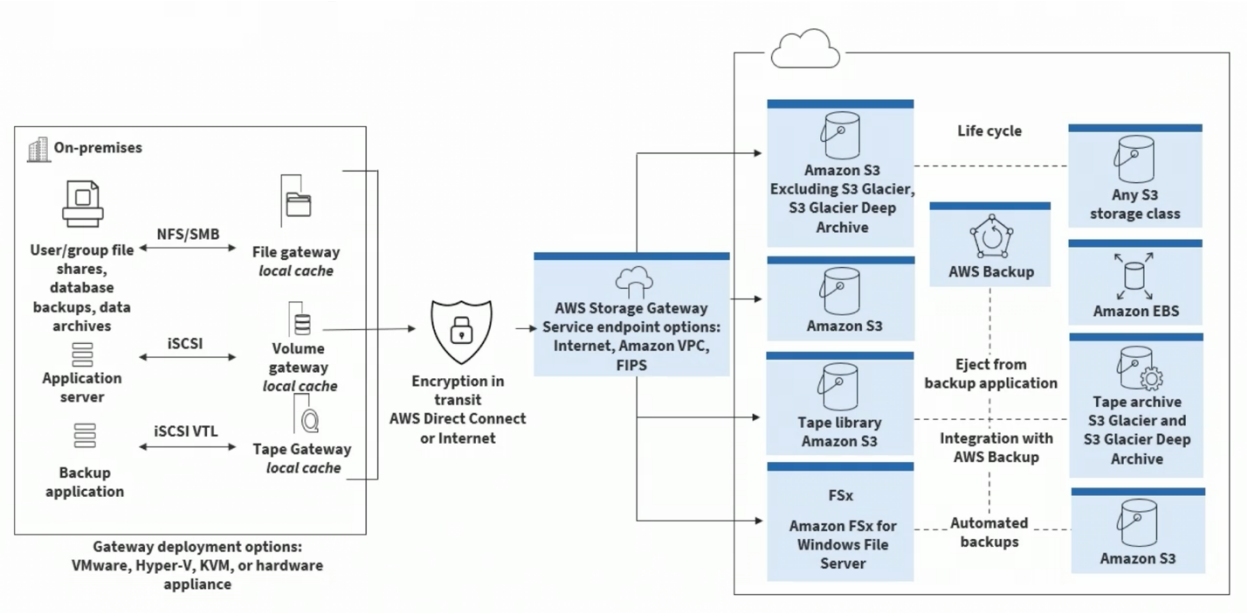
Encrypting Backup Data

- Encrypting the database and other data backups helps secure the data
- All DBMS systems offer the option to encrypt the backup data while creating a backup
- Encryption can also be used for databases that are encrypted using transparent data encryption (TDE) so that the database engine forces the creation of a new transaction log, which will be encrypted by a database encryption key
- Most scenarios include various encryption algorithms up to AES-256 bit in either CBC or GCM mode commonly
- Administrators can also integrate encryption keys with extensible key management (EKM) providers and cloud-based key management services (KMS)

Onsite vs. Offsite Backup Strategies

- Accessibility
    - Offsite backup is not as reliable to access physically as the data is stored in different geographical locations
- Cost
    - For entities with a lot of data, cloud-based backup solutions can be quite cost-efficient in the long run using Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)
- Security
    - Onsite may be as secure as offsite if a large resource commitment is made for administrative, physical, and technical security controls
- Scalability
    - Scalability is one of the huge advantages of offsite data backup where the cloud service provider (CSP) is responsible for providing the storage
- Support and Maintenance
    - With on-premises solutions, the organization has the most control with their own support team responsible for data backup
- Reliability
    - Offsite data backup is more reliable because the data is not stored in the same place as the original data

Cloud-based Replication



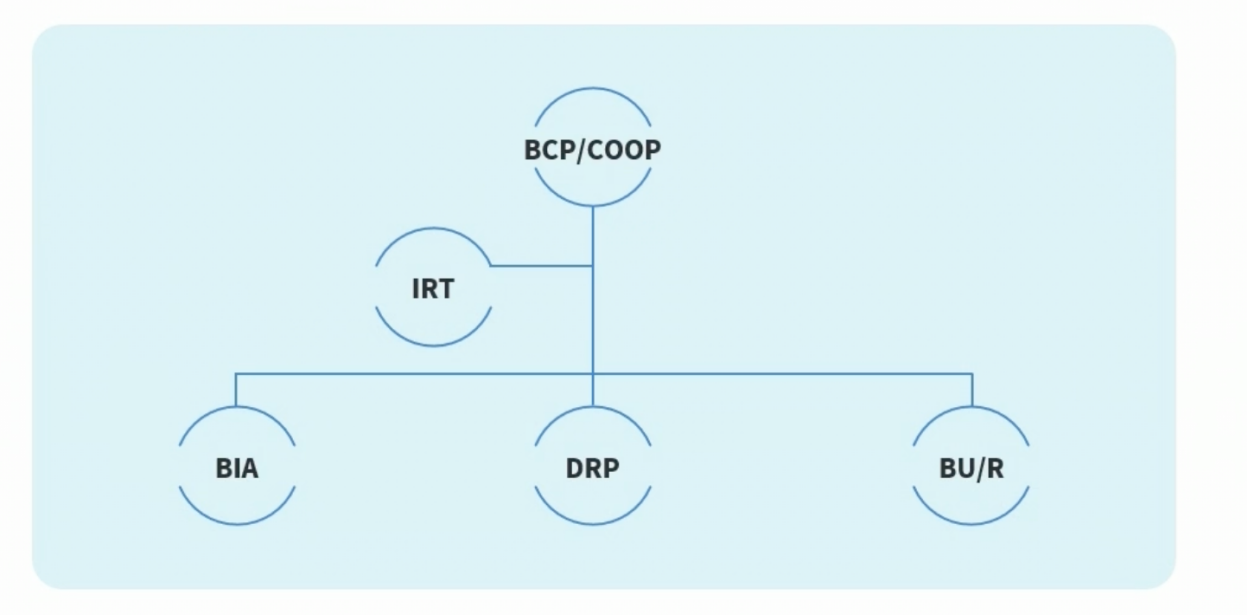
-
- Gateway can be a hardware device or a hypervisor. Then you have various types of caches and file system protocols that are supported with file gateway caches etc. often going over a direct connection to a partner (AWS direct connect, google interconnect).

Recovery and Restoration

- Without a comprehensive well-tested recovery and restoration practice there is no real backup strategy
- Many organizations have relied on regular automated backups when suffering a ransomware attack only to find out there were configuration errors or gaps that were not discovered through ongoing recovery testing
- The team that performs recovery is often different that the backup operators due to “Separation of Duties”

Continuity of Operations

- Macro term of Business continuity plan
- Continuity of operations plan (COOP) or business continuity plan (BCP) helps to ensure that the entity remains operational at a pre-determined level when disaster strikes
- These are plans and documents approved by executive management
    - Outlines risk to business
    - Populates risk register/ledger
    - Requirements to mitigate incidents
    - Identifies procedures needed to recover from a disaster
- What is an acceptable amount of time?
- How to reduce the impact of the disaster if it happens again?



-
- BIA (business impact analysis), DRP (disaster recovery planning), BU/R(backup and restore policy). IRT (incident response team) because an incident can quickly escalate or elevate into a category of a disaster so a lot of things that are done will be leveraged by the disaster recovery plan

BCP from NIST SP 800-34, Revision 1

1. Develop a continuity planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventative controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Generate after-action report (AAR)
8. Lessons learned and plan maintenance

Business Impact Analysis (BIA)

- Recovery time objective (RTO)
  - The target amount of time within which a process must be restored after disruption
- Maximum tolerable downtime (MTD)
  - Absolute maximum amount of time that a resource, service, or function can be unavailable
- Recovery point objective (RPO)
  - The maximum targeted period in which an asset or data may be lost from an IT service due to a major event
- Mean time to repair (MTTR)
  - The average time needed to repair or replace a failed system or module
- Mean time between failures (MTBF)
  - The number of failures per million hours for a product
- The Recovery time objective must be less than or equal to the maximum tolerable downtime MTD. Also even though RPO does have a time element to it, the recovery point is when something was done (snapshot, last known configuration) and the closer the RPO is to the event the better it is. The MTTR is one of the most updated metrics due to supply chain disruptions. The MTBF is information usually retrieved from the original equipment manufacturer or third-party consumer report.

Disaster Recovery Planning (DRP)

- Outlines the technical aspects involved for restoration
    - Order of restoration (most critical to least critical)
    - Backups, snapshots, and restores
    - Contact information
    - Communication plans
    - Chain of authority
    - Step-by-step instructions
    - Locations of documents, software, and keys
    - Recovery sites: Hot, warm, cold, mobile, cloud, shared

Multicloud

- Large organizations use multicloud for ultra-availability, and business continuity
- A cloud computing model where an enterprise leverages a combination of clouds (two or more public clouds, two or more private clouds, or a combination of public, private, and edge clouds)
- It enables the distribution of data, applications and services to accelerate app transformation and the delivery of new apps
- Supports disaster recovery by leveraging more than one provider for enhanced high-availability and durability

Disaster Recovery Sites

Recovery strategy	Recovery time	Advantages	Disadvantages	Comments
Commercial hot site	24 to 48 Hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high • Term of the agreement can limit the duration of use • If you are not the "most important customer" you could be bumped	Often the most cost-effective strategy for data center recovery strategies. Clear contract terms need to be defined which meets the enterprise service objectives. Consideration should be made for disasters that impact entire regions such as hurricanes and earthquakes.
Internal hot site	1 to 12 Hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high	If costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
Warm site	24 to 48 Hours	• Moderately priced • Basic infrastructure is in place to support recovery operations • Ability to pre-stage delivery and implementing of the necessary hardware, application software, OS software, data, and communications	• Not easy to test • Recovery time is longer than with hot site and is controlled by the time to locate and restore application • Facility equipment may not be exactly what is required – Once the recovery begins delays may occur because of equipment, software, or staffing shortfalls	If costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.

-
- The best solution to support your ongoing operations the best recovery time easiest to implement is the internal hot site solution where you can recover often between a hour to 12 hours. The commercial hot site is also a good solution to support ongoing operations but it is more expensive because it is a commercial solution and you are paying another company (business continuity consultant). The warm site is going to be anywhere between the internal hot site and what we call a cold site.

Recovery strategy	Recovery time	Advantages	Disadvantages	Comments
Mobile site	24 to 48 Hours	• Moderately priced • Typically, can be in place for 36 to 72 hours • Can be placed in the "parking lot" adjacent to you impacted facility	• Recovery time typically is at least 2 to 5 days longer than a hot site. • Access to your impacted facility may be hindered because of the event • A trailer may not be configured exactly as you need it	This approach avoids employee travel issues but has limitations on equipment availability and outbound bandwidth if small aperture satellite terminal (VSAT) links must be used for communication. If the disaster profile includes events such as hurricanes, floods or toxic spills, these solutions may not be appropriate.
Cold site	72 plus Hours	• Lowest cost solution • Basic infrastructure power, air, and communication are in place • Can rent the facility for a longer term at lower cost	• Longest recovery time • All equipment must be ordered, delivered, installed and made operational • Worst solution for supporting on-going operations	"Environmentally appropriate" space can be either provisioned internally or contracted form a commercial facilities service provider. Cold-site strategies are usually based on "quick-ship" delivery agreements to allow server, storage, and communications hardware and network service providers to quickly build out the data center and/or client workspace infrastructure.
Reciprocal agreement	12 to 48 Hours	• Least costly solution • Better than no strategy	• Seldom works • Typically, in the same geographic area and a wide range disaster like an earthquake renders it of no use • No easy way to test	This is typically a formal agreement between two trusted, non-competing partners in different industries in which each provides secure sites for the other. This option is the least favorable and has the greatest risk associated with it.
Cloud	0 to 24 Hours	• Data and applications available immediately • Location independent • Easy to test	• Security • May no allow enough time for a daily cycle processing window	Data should be in place so activation would only be limited by connectivity and network addressing (DNS propagation)

-
- A warm site is hard to define because it depends on your organization, it is something between he cold site and the hot site. The cold site looks like the lowest cost solution but it is not really true. There is a lower cost solution which is a reciprocal agreement cold site which seldom works its difficult to test and it's a formal agreement but it can bring in some legal complications (sub-optimal), a particular event would not effect both companies is naïve. The emerging solution that is much more popular for companies to stage in certain regions of the world is the cloud solution, where your recovery time can often be less than a hour (0-24) so the fastest solutions would be the internal hot site and the cloud solution. With the cloud solution you will save money because you a leveraging their infrastructure.

Geographic Dispersion

- Disaster recovery solution
- Distance between systems, or geographic dispersion, has benefits but also has physical and practical limitations
- For a disaster recovery solution, typically, the greater the distance between the systems, the greater the protection you will have from area-wide disasters
- However, this distance will come with application environment impacts
    - When distance is added to a data replication solution, latency is introduced
    - Latency is the added time it takes for data to reach the target system
- The further systems are apart, the more latency (time) is added to the data transmission
- Using cloud service providers and managed security service providers for high availability multi-zone and multi-regional data recovery and replication is a huge value proposition
- Many organizations are migrating from internal and commercial warm/hot site recovery solutions to cloud-based disaster recovery
- This is made more feasible and cost-efficient by the rapid proliferation of edge and hybrid cloud solutions

Capacity Planning

- Capacity planning is a technique for analyzing how much production capacity organizations need to meet consumer demand
- It is widely used in data center, manufacturing, and cloud services industries
- Capacity planning assists organizations to govern whether they have enough raw materials, people, technology, and infrastructure to deliver the value proposition

Types of Capacity Planning

- Product capacity planning -> Do I have enough product?
- Workforce capacity planning -> Do I have the right mix of employees?
- Tool capacity planning -> Do I have enough equipment and am I utilizing it effectively?
- Production capacity planning -> What's the maximum amount that I can produce at peak efficiency?

Capacity Planning

1. Identify all existing and new projects and tasks
2. Determine a strategy
3. Generate a realistic resource schedule
4. Discover any minute details, tasks and planning gaps

Testing Disaster Recovery Plans

- A disaster is a escalated or elevated incident
- Read-through (plan review)
    - is where the business continuity plan owner and business continuity team discuss the business continuity plan
    - Look for missing elements and inconsistencies within the plan or with the organization
    - A type of checklist test useful to train new members of a team, including the business function owner
- Tabletop testing
    - Is where participants gather in a room to execute documented plan activities in a stress-free environment
    - Can use blueprints, topological diagrams, or computer models to effectively demonstrate whether team members know their duties in an emergency and if they need training
    - Documentation errors, missing information, and inconsistencies across business continuity plans can be identified
- Walkthrough testing
    - Is a planned rehearsal of a possible incident designed to evaluate an organization's capability to manage that incident
    - Provides an opportunity to improve the organization's future responses and enhance the relevant competences of those involved
    - Often done on a limited basis or by scheduling each department or building separately for fire and active shooter drills
- Simulation testing
    - Determines if business continuity management procedures and resources work in a realistic situation
    - May be the most elaborate test most entities ever conduct
    - Uses established business continuity resources, such as the recovery site, backup equipment, services from recovery vendors, and transportation
    - Can require sending teams to alternate sites to restart technology as well as business functions
- Parallel test
    - Involves bringing the recovery site to a state of operational readiness, but maintaining operations at the primary site

    - Staff are relocated, backup tapes are transferred, and operational readiness established in accordance with the disaster recovery plan while operations at the primary site continue normally
    - May be the most comprehensive test most entities ever conduct
- Full-Interruption test
    - Least common test
    - Operations are completely shut down at the primary site to fully emulate the disaster
    - Enterprise transfers to the recovery site in accordance with the disaster recovery plan
    - A very thorough test, which is also expensive (may be cost-prohibitive)
    - Has the capacity to cause a major disruption of operations if the test fails

Types of Power Outages

- A blackout is a complete loss of power to an area
    - This is the most severe type of power outage, typically affecting large numbers of people over potentially large areas
- Brownouts typically occur if there is a drop in electrical voltage or a drop in the overall electrical power supply
    - While brownouts do not cause a complete loss of power, they can cause poor performance from some equipment and some devices
- A permanent fault is a sudden loss of power typically caused by a power line fault
    - These are simple and easy to deal with: once the fault is removed or repaired, power is automatically restored
- Rolling blackouts are different from the other three as they are planned power outages
    - These are usually implemented in areas with unstable grids or with infrastructure that cannot handle the population it serves
    - Rolling blackouts can also be caused if there's not enough fuel to run power at full capacity, whether for the short term or long term

Uninterruptible Power Supply

- An uninterruptible power supply (UPS) is an electrical component that delivers emergency power to a load when the main power source (typically utility power) fails
- It conditions incoming power to ensure clean and uninterrupted power, protects devices from power problems and enables seamless system shutdown during complete outages
- A UPS system is particularly beneficial for networking equipment and other devices that can lose data when power is suddenly lost
- The UPS is a critical investment to thwart damage, data loss, and downtime caused by power issues

Generators

- A backup generator is a failover power solution that provides power to business operations and homes
- They are typically stationary and require a concrete pad used as a foundation usually situated outside a facility or site
- Standby generators are a robust solution that can offer power for days during extended power outages, depending on the fuel type and configuration of the generator
- Many sites employ prime or continuous generators for disaster recovery site solutions
- According to the Uptime Institute, all tiers should have at least 12 hours of fuel (i.e. diesel) for the backup generators

Multiple Power Sources

- Electricity companies can operate in the same area because they can compete to provide electricity to consumers
- While the power may come from the same grid or transmission lines, different companies can generate and supply electricity to the grid
- These companies then compete based on factors such as pricing, customer service, and renewable energy offerings
- It is like how different phone carriers can operate using the same cell towers and infrastructure

Computing Resources Security Techniques

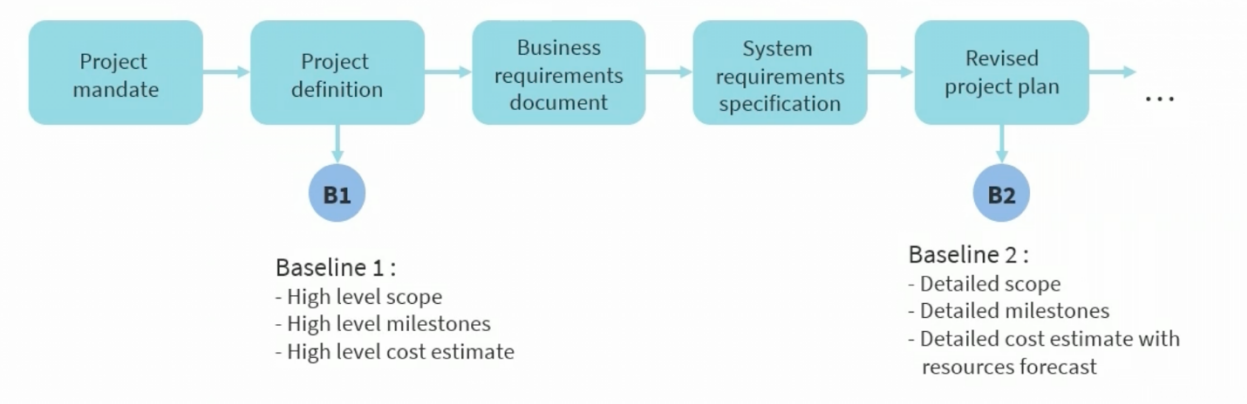
Secure Baselines

- A security baseline is defined as the minimum amount of security controls needed for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection
- For vendors such as Microsoft or Cisco, the baselines would be a group of recommended configuration settings that describe their security implications
- The settings are based on feedback from security engineering teams, product groups, partners, and customers

Center for Internet Security (CIS) Benchmarks

- The CIS Benchmarks are strict configuration recommendations for more than 25 vendor product families
- They represent a consensus-based initiative by cybersecurity experts globally to help organizations protect their systems against threats more effectively and confidently
- The CIS Benchmarks are community-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks, both internal and external
- They are mapped to the CIS Critical Security Controls (CIS Controls)
- Benchmarks elevate the security defenses for cloud provider platforms and cloud services, containers, databases, desktop software, server software, mobile devices, network devices, and operating systems

Baseline Process



-
- First you have the Project mandate (budgeting, project managers and timelines). Then Project Definition. Next business requirements document(strategic approach) then the system requirements (technical and tactical). Then Revised Project Plan(all based on the business and system requirement specifications). All a iterative process.

Hardening Defined

- This generic term is also called server hardening, security hardening, and operation systems (OS) hardening
- System hardening is a combination of methods, tools, and best practices used to reduce vulnerability (or lower the risk) in servers and computers (physical, virtual, on premise, and cloud)
- The goal of hardening is to lessen network and IT security risks by shutting down ports and channels used by unnecessary services and applications
- It also includes removing default and automatic configuration settings and activating built-in security features

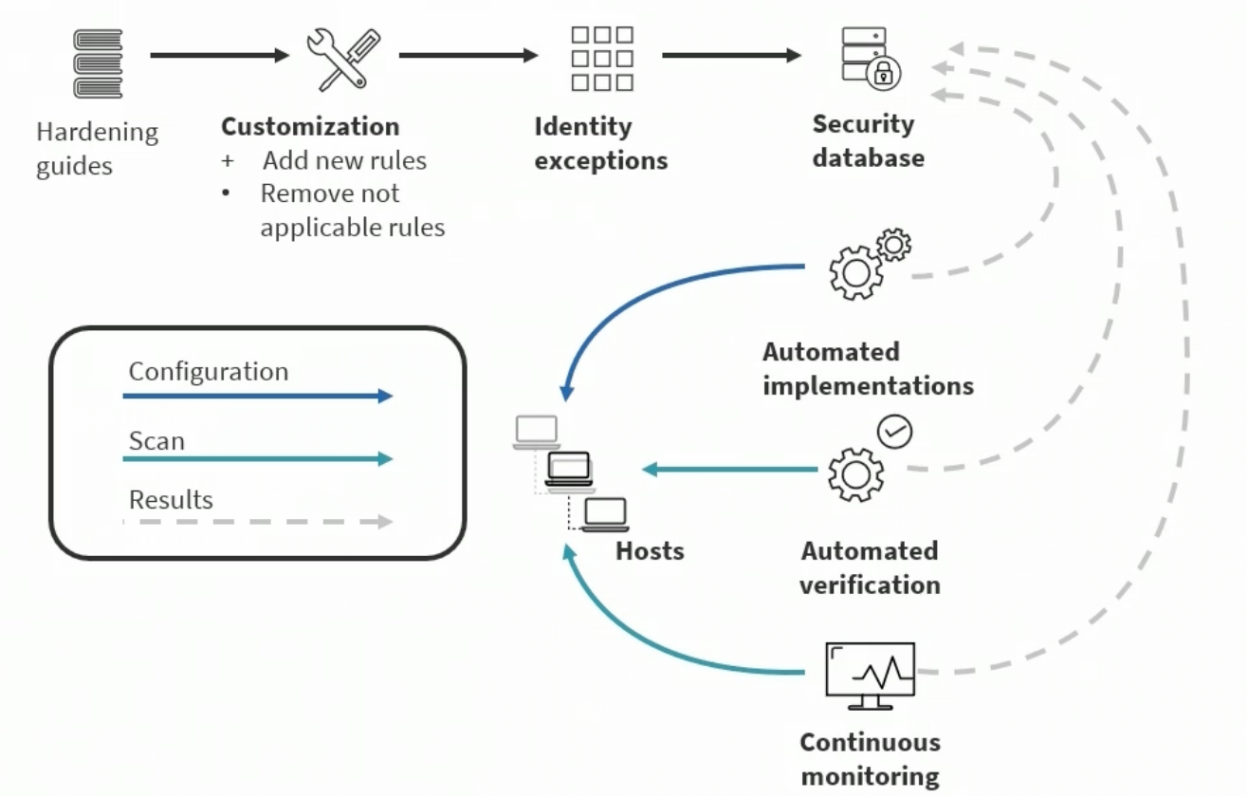
Hardening Targets

- Operating systems (Linux, Unix, MacOS)
- Wired and wireless networks
- Database Systems (relational, NoSQL, document, graph)
- Applications and containers
- Industrial control system (ICS)/Supervisory Control and Data Acquisition (SCADA), embedded systems, real-time operating system (RTOS), and Internet of Things (IoT) devices

Challenges to Hardening Embedded/IoT Systems

- Dependability – many critical aspects such as utility grids, transportation infrastructure, and communication systems are controlled by difficult to patch embedded systems
- Uneven security updates – most of the embedded and specialty systems are not upgraded regularly for security updates
- Attack replication – since embedded devices are mass produced, the same version of components have the same design and build as other devices in the lot
- Industrial protocols – embedded systems (e.g. raspberry pi) often follow a set of custom procedures that are not protected or recognized by enterprise security tools (may have their own industrial protocols and communication channels)
- Device life cycles – specialty IoT devices typically have a much longer lifespan than PCs
- Remote deployments – many embedded devices are deployed in the field, outside the enterprise security perimeter; therefore, they may be directly connected to the Internet without the security layers provided in the industrial environment

Automating System Hardening



-

Wireless Device Installation Issues

- Compared to Ethernet and Fiber wired networks, there are a wide array of wireless protocols and technologies
- Wireless networks are often the “low-hanging fruit” of network security and are a common starting point for attacks and penetration tests
- Wireless signals are more affected by physical obstacles, electromagnetic noise, or other wireless devices, resulting in lower quality or loss of connection
- This introduces wireless device installation issues like site surveys, wireless analysis, and produce heat maps. For proper implementation, for example, power outputs, designing heatmaps, if there are a overlap for devices that are roaming.

Wireless Site Surveys

- The first phase of a wireless site survey is to identify all the wireless deployment requirements
- Question to ask in the initiation phase are:
    - What is the desired speed and bandwidth?
    - How many client devices will be accessing the network at once?
    - How much transmit power will they have?
    - Which generation of the 802.11 Wi-Fi standard will the site be using? (.11n, .11ac, or .11ax)
- Next the surveyor should get a diagram of the area the network will cover, preferably with building blueprints
    - Perform a walkthrough and document the infrastructure evaluation
- The next step is to look out for places where wireless access points can be mounted, such as ceilings and pillars
- After this, determine the areas to be covered
    - Don’t forget utility rooms that may house wireless equipment
    - Indicate areas on the floor plan
- Determine the tentative access point locations
    - Make sure to check the coverage range of your access points
    - Build in some overlap between neighboring access points to guarantee seamless roaming, dynamic load balancing, and network resiliency

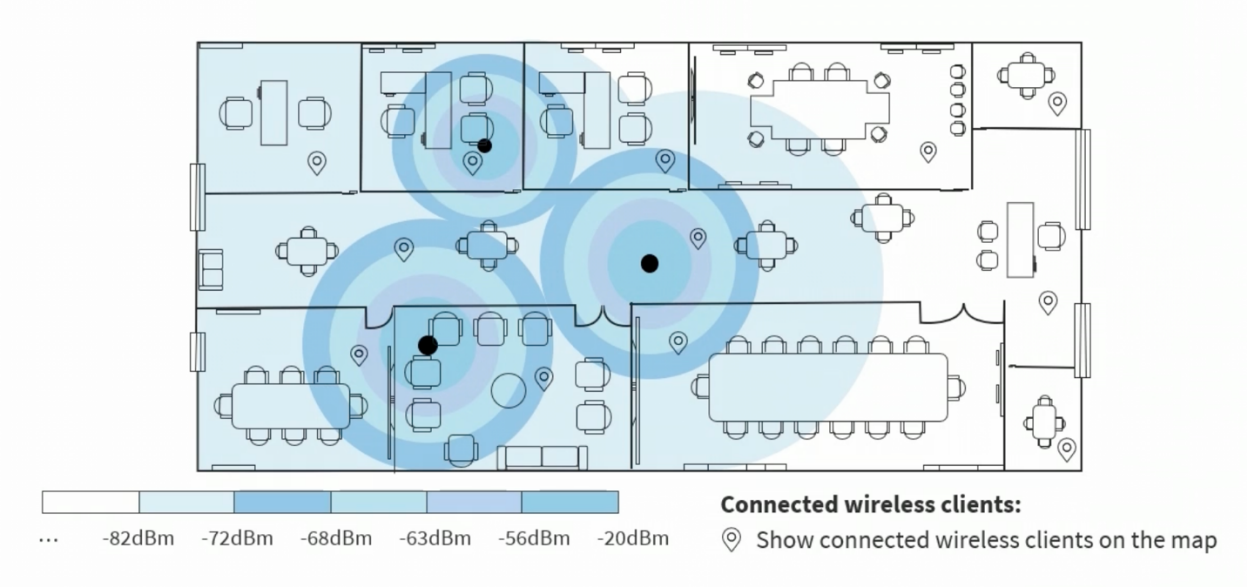
Wireless Analysis

- The initial decision should be to acquire an industry leading wireless analysis and spectrum analysis toolkit
- A Wi-Fi analyzer is a useful software application that can report many things about the wireless network and the networks around you, helping you optimize your Wi-Fi for best performance
- This will assure that the decisions made in the site survey are as optimized as possible

Heat Maps

- A Wi-Fi heatmap tool generates a color-coded graphical representation of different wireless metrics such as signal strength, signal-to-noise (SNR) ratio levels, and interference in different areas
- By leveraging the power of data visualization, Wi-Fi heatmaps empower network engineers to make educated decisions when optimizing a network, enhancing performance, or addressing potential issues

Wireless Heat Map



-
- From wireless heatmap software

Mobile Deployment Models: Bring Your Own Device (BYOD)

- Employees are permitted to use their personal mobile devices to access enterprise data and systems
- There are four basic options:
    - Unlimited access for personal devices
    - Access only to non-sensitive systems and data
    - Access with IT control over personal devices, apps, and stored data
    - Access while preventing local storage of data

Mobile Deployment Models: Corporate-owned, Personally-enabled (COPE)

- Company gives the employees or contractors mobile devices that are provisioned from vendors and cellular providers without end user input
- The users can handle as if they were their own
- This model prevents the need for two smartphones
- COPE programs should use containerization tools and extensive mobile device management and mobile application management

Mobile Deployment Models: Choose Your Own Device (CYOD)

- Much like BYOD, it lets employees work from anywhere using a mobile device
- CYOD devices must be approved by the organization, unlike BYOD
- Users often select from a list of approved devices, which are usually smartphones
- These networks offer more stability, security, and simplified IT for most businesses
- Also demands device management

Mobile Device Solutions

- Organizations must securely configure and implement each layer of the mobile technology stack, including hardware, firmware, o/S, management agent, provider agreements, and apps used for business
- The solutions should reduce risk while enabling employees to access applications and necessary data from nearly any location, over any network, using a wide variety of mobile devices in some cases

- Enterprise mobility management (EMM) = mobile device management (MDM) = mobile application management (MAM)

Mobile Device Solutions
- There are three basic core competencies that all organizations need from an EMM solution:
    - Visibility – understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
    - Secure access – providing the ability for mobile users to securely authenticate and authorize access to apps and data
    - Data protection – offering dynamic antimalware and data loss prevention (DLP) capabilities to help limit the risk of attacks and data breaches

Sandboxing
- Sandboxing is also referred to as partitioning or compartmentalization
- These techniques involve orchestrating the packaging, isolation, and encapsulation of apps and work data in a separate segmented user space within the device
- Storage sandboxing (segmentation) comprises partitioning various types of data on devices to protect IP, personally identifiable information (PII), and Protected Health Information (PHI) and support DLP initiatives
- The iPhone has a separate secure enclave for security and privacy

Common MDM Solutions
- Onboarding, offboarding, and installing certificates (e.g. installing x509v3 certificates)
- Implementing touch ID authentication and screen locking
- Configuring personal identification numbers (PINs) and push notifications for user devices
- Deploying and managing full device encryption
- Finding lost devices and remote wiping (geofencing and geotagging)

Modern EMM Attributes
- BYOD and MAM security capabilities
- Flexible bundles for different use cases (e.g. different policies for the CEO compared to the sales team)
- Unified endpoint management and enterprise integration
- End-to-end Zero Trust security and identity management (IdM)
- Productivity applications without writing code
- User behavior analytics (UBA)

Other Mobile Solutions
- Cellular
    - Multiple access technology where multiple voice or data connections are placed into a single radio channel (5G)
- Wi-Fi
    - Various IEEE standards that employ different aspects of the radio frequency (RF) spectrum and modulation schemes to transmit data wirelessly
- Bluetooth
    - An IEEE radio-frequency Personal Area Network (PAN) standard in the 2.4 to 2.485 GHz ISM and an agreement protocol

WPA2

- Wi-Fi Protected Access 2 (WPA2) was the replacement for WPA (2004)
- It has been widely used for over almost 20 years and is still a common solution
- All devices required testing and certification from Wi-Fi Alliance (2006)
- It uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for security
- WPA2 supports pre-shared key (PSK) and enterprise authentication (using 802.1x)
- Management Frame Protection (MFP) was optional but highly recommended and universally deployed to protect the management frames of wireless
- Three types of frames; data, control and management (most vulnerable)

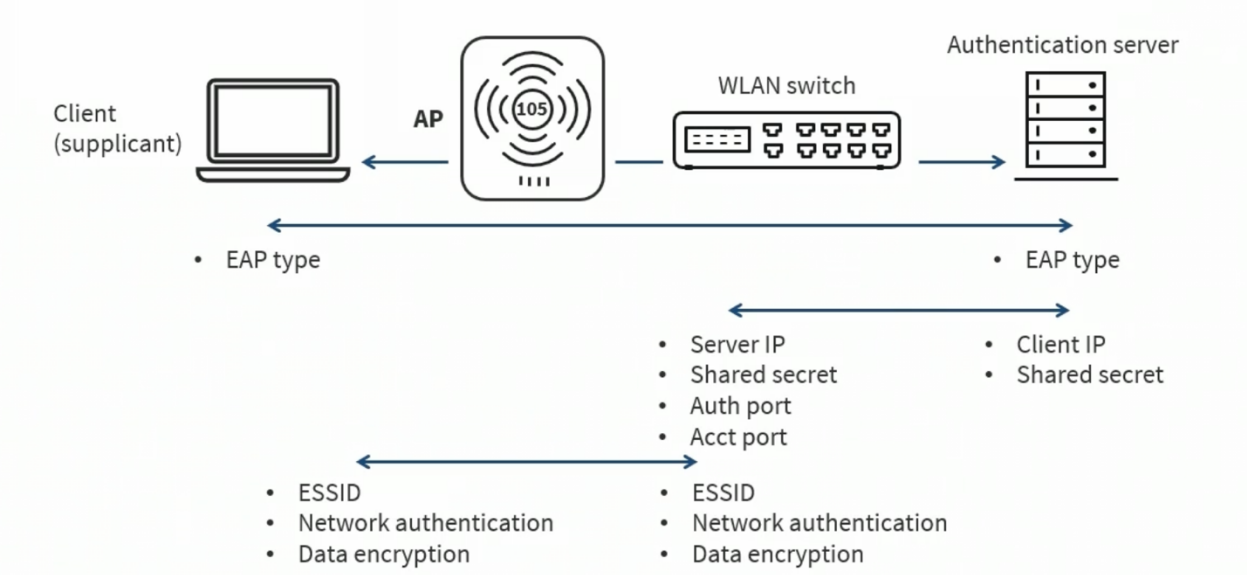
WPA3

- The Wi-Fi Alliance announced this new security protocol in 2018, with WPA3 support becoming mandatory for all routers carrying the Wi-Fi Certified label since July 2020
- All WPA3 networks use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF)
    - PMF enhances privacy protections already in place for data frames with mechanisms to improve the resiliency of mission-critical networks

WPA3 Cryptographic Mechanisms

- Authenticated encryption – GCMP-256
- Key derivation and confirmation – 384-bit HMAC with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication – ECDH exchange and ECDSA using a 384-bit elliptic curve
- Robust management frame protection – 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

Wireless 802.1X Networks



-
- Since WPA, organizations have had the option to use pre-shared key mode or 802.x enterprise mode, where the supplicant sends initial EAPLL frames to a access point. On the back-end of a wireless Lan switch or a module in a router using an authentication server (radius or diameter on the front end), but can use a wide variety of solutions as your identity provider on the back end (e.g. active directory). After the initial EAPLL exchange, then they will agree on which EAP type to use. E.g. EAPTLS, protected EAP, EAPTTLS, tunneledTLS or in cisco environments EAP fast. The client and server will establish a shared secret key, agree upon authentication ports and accounting ports, network authentication, and finally encrypt the data sent over the RS spectrum.

Application Security: Validation Testing

- Validation testing is the process of ensuring that the tested and developed software application or mobile app fulfills the needs of the customer, functional and non-functional. Functional being what it does, non-functional being how it does it.
    - The business requirement logic or use cases must be tested in full detail
    - All the critical functionalities of an application must be tested here
- It is critical to know how to verify the business logic that is provided
    - A common technique is input validation which ensures only properly formed data is entering the workflow in an information system

Functionality Testing

- Design Qualification (DQ) -> Defines the functional and operational specification of the instrument and details the conscious decision in the selection of the supplier
- Installation Qualification (IQ) -> Establishes that the instrument is received as designed and specified, that it is properly installed in the selected environment, and that this environment is suitable for the operation of the instrument
- Operational Qualification (OQ) -> The process of demonstrating that an instrument will function according to the operational specification in the selected environment
- Performance Qualification (PQ) -> The process of demonstrating that an instrument performs according to a specification appropriate for its routine use

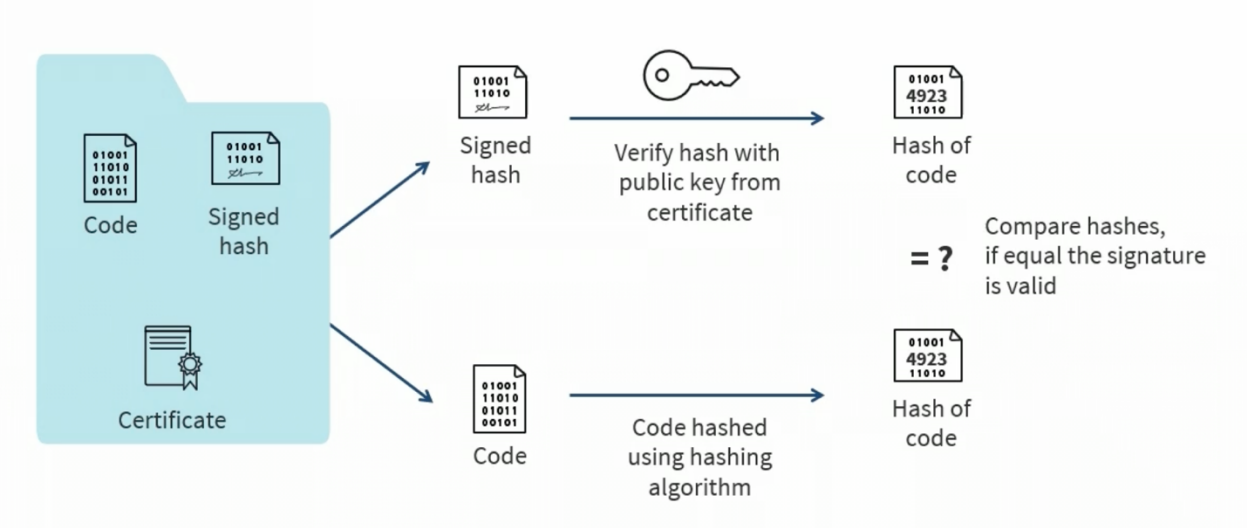
Application Security: Secure Cookies

- HTTP cookies are small packets of data stored in a browser client
- This data may contain sensitive data like passwords or use information and is therefore vulnerable for attacks
- To limit vulnerability developers can enhance cookie security by adding specific attributes to the set cookies, making it difficult for attackers to manipulate

Methods for Securing Cookies

- Really Simple Secure Sockets Layer (SSL) uses the HTTP Only, secure and use_only_cookies parameters to make cookies more secure
    - The HttpOnly flag will tell the browser that this cookie can only be accessed by the server
    - The secure parameter will make sure cookies are only sent over a secure SSL connection
    - The use_only_cookies parameter will tell your website to use only cookies to store session data

Application Security: Code Signing



-
- We see our original code, the code goes through a cryptographic hash function that can be verified by a X509v3 certificate. The code is hashed using a hashing algorithm (SHA384). On the receiving end the recipient compares hashes to see if the signature is valid. It is important today that you use digitally signed code.

SAST vs. DAST

- Static Application Security Testing (SAST)
  - Is commonly defined as a white-box test, where an analysis of the application source code, byte code, and binaries is carried out by the application test without executing the code
  - It is used to find coding errors and omissions that are symptomatic of security vulnerabilities
  - SAST is often used as a test method when the tool is under development – earlier in the development life cycle
  - It can be used to find SQL injection attacks, cross-site scripting errors, buffer overflows, unhandled error conditions, and probable back doors into the application
- Dynamic Application Security Testing (DAST)
  - Is considered a black-box test, where the tool must find distinct execution paths in the application being analyzed
  - Unlike SAST, which analyzes code that is not running, DAST is used against applications in their running state
  - It is primarily considered effective when testing exposed HTTP and HTML interfaces of web applications
  - Static and dynamic application tests work in concert to improve the reliability of applications being built and bought by organizations

Asset Management: Acquisition/Procurement

- The Acquisition/procurement process involves possible assignment of ownership, custodians, and/or stewards
- The labeling or tagging schema will be applied (e.g. QR codes)
- Classification and sensitivity levels are attacked (e.g. mandatory access control – public, private, military)
- The accounting methodology will be implemented which may include:
  - RADIUS/DIAMETER/LDAPS
  - Automated and integrated inventory engines

    - Integration with directory services, configuration management database, human resources, legal

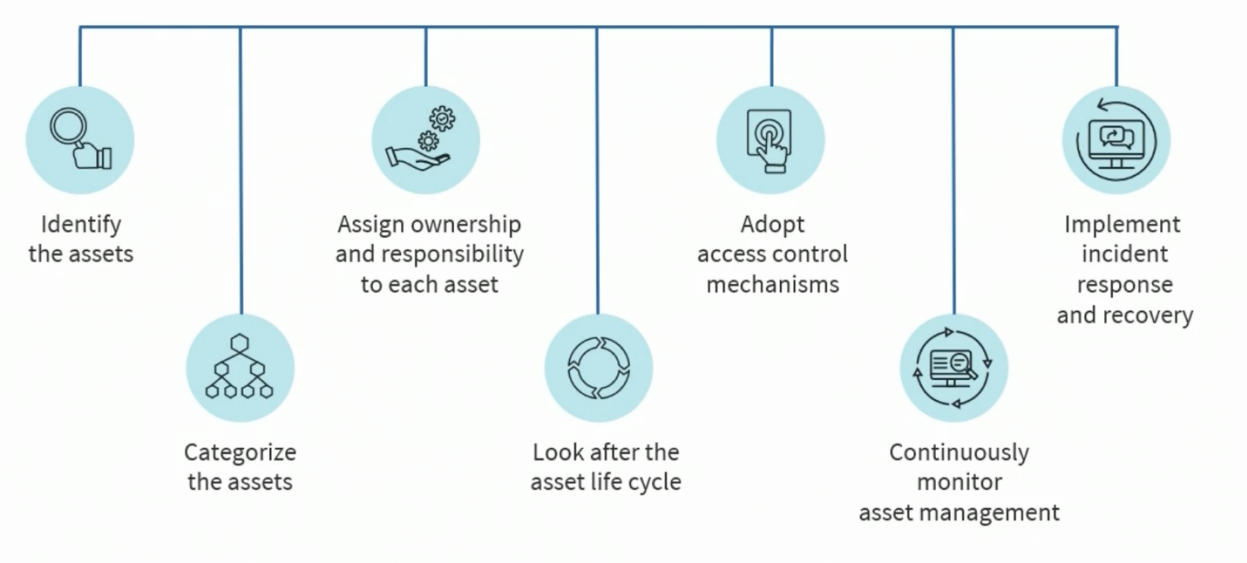
Asset Management: Monitoring/Tracking

- This initiative will involve the ongoing enumeration and tracking of all physical and logical assets
- The monitoring process may involve the implementation for security information and even management (SIEM) and security orchestration, automation, and response (SOAR) systems with cloud-based analysis for resource planning and optimization
- Continual improvement is a key aspect of this area of asset management
    - This phase also involves the ongoing search for "shadow assets" and/or "ghost IT"
- Some organizations have dedicated digital asset managers to control information/digital rights management initiatives

Asset Management: Disposal/Decommissioning

- Sanitization (e.g. cryptographic shredding)
- Certification (e.g. properly dispose physical and logical assets)
- Retention (e.g. governance, policy, best practices or government regulations (tax information, customer data)
- Destruction (e.g. final phase of asset lifecycles)

Basic Asset Management Life Cycle



-

Vulnerability Management

Exploring Threat Feeds and Resources

- Open source intelligence
- OSINT
- Maltego -> is a tool to do open source intelligence (like Kali). Express graphically what your finding on the internet. Way to visualize this information and generate reports. Intelligence and analysis tool.
- NIST (national vulnerability database) -> vulnerabilities database. Shows zero-day threats and occurrences.
- CVE stands for common vulnerability enumeration -> have the CVE followed by the year identified and then a unique identifier. Then when it was published
- CVSS is a score -> 9 is critical, 5 medium. CVSS stands for common vulnerability scoring system.
- SANS.org -> resources, web casts, newsletter, security awareness training. Who you would go through once you get security+. Security policy templates.
- MITRE -> attack matrix for enterprise. Categories that have different areas (recon, initial access, execution) that goes into phishing and attack change categories, debugger invasion. Things you don't want to be vulnerable too.

Dark Web

- Not some private island it is an overlay network or a dark net
- Also called overlay networks or darknets
- Deep web not indexed by search engines
- "Anything goes" peer-to-peer networking
- Use Tor, Freenet, I2P, and Riffle browsers

Dark Web Offerings

- Botnets (distributed denial of service attack)
- Marketplaces (e.g. silk road)
- Malware as a Service (MaaS)
- Illegal pornography
- Fraud and hoaxing services
- Phishing, ransomware, and scam campaigns
- Zero-day malware
- Niche social media
- Terrorism

Application Vulnerability Assessment

- An application vulnerability assessment is a testing methodology used to recognize and assign severity levels to as many security defects as possible in a timeframe
- This process typically involves manual and automated techniques with varying degrees of precision with an emphasis on comprehensive coverage
- It is often part of a larger software assurance initiative such as OWASP Software Assurance Maturity Model (SAMM)

Static Application Security Testing (SAST)

- SAST tools are also known as code analyzers that conduct a direct white-box analysis of the application source code

- The analysis runs on a static view of code, in that the code is not running at the time of the assessment
- SAST security tools are mainstream and are widely adopted throughout the software industry
- They have broad programming language support and use concepts that are relatively easy to comprehend
- SAST code analyzers have no visibility of the execution flow, can be slow, inaccurate, and outdated, and often need additional customization and/or tuning

Dynamic Application Security Testing (DAST)
- DAST tools are most often web scanners like OWASP ZAP and Burp Suite (vulnerability scanners)
- They perform know-nothing in that they do not have access to the code or the implementation specifics
- A DAST tool will not only inspect the system's responses to a series of tests designed to highlight vulnerabilities
- They function independently of the underlying application platform and offer solid support for manual penetration testing

Package Monitoring
- Processes and tools that troubleshoot application performance issues in Dev, QA, and production environments with:
    - Code-level insights
    - Distributed transaction tracing
    - Application service maps, and more
- They usually support Java, .NET, .NET core, Node.js, Python, PHP and Ruby applications
- Container monitoring empowers DevOps teams to stay on top of outages and pinpoint server issues with root cause analysis capabilities
    - Proactively monitor and optimize the performance of Docker, Kubernetes and Red Hat OpenShift containers and applications

Vulnerability Scanning
- Vulnerability scanning is the process of identifying known and unknown weaknesses in systems, applications, services, and policies using tools
- Vulnerability scanning is an easier and often more focused process looking for unpatched systems, misconfigurations, code, and open ports
- It is typically automated and done on a routine basis (weekly, quarterly), taking at most a few hours
- Vulnerability scanners include Nessus, OpenVAS, Core Impact, Nexpose, GFI LanGuard, OWASP ZAP, Burp Suite

Network Scanners
- Network scanners can be used to scan IP addresses, ports, and device locations (wireless and wired) presented in a customized graphical XML view
- Most provide network monitoring and management capabilities to detect, diagnose, and resolve network issues and outages
- Active malware worms are also considered network scanners

Web Vulnerability Scanning
- This most common vulnerability scanners will test web applications and services to look for:
    - Cross-site scripting and request forgery

    - SQL and other command injection
    - Broken authentication and session management
    - Insecure direct object references
    - Insecure server configuration (XML, PHP, etc.)
    - Exposing sensitive data

Compliance Scanning

- Different from performing a vulnerability scan, although there can be some overlap, compliance scanning will use vulnerability scanning tools
- Compliance audit decides if a system is configured in agreement with a recognized governance policy whereas a vulnerability scan determines if the system is exposed to known vulnerabilities
- Sometimes compliance involves auditing more sensitive data and systems
- Typically, the compliance requirements are minimal baselines that can be taken differently depending on the goals of the organization
- Compliance requirements must be in line with the business goals to ensure that risks are correctly recognized and alleviated. Risk handling and business impact analysis

Accuracy Confirmation

- Whenever performing vulnerability or compliance scanning or any other vulnerability testing, you must take the same approach as you would with a intrusion prevention or intrusion detection system. In other words how accurate is the test -> you want true positives(accurate + action taken) or true negatives(accurate + action not taken)
- A false positive (error + action taken) error state when a action was taken, how the system reacts. Or false negative (error + action not taken). Can apply this to endpoint detection and response, anti malware. Other systems that send alarms and alerts just apply to these to check if they work and whatever.

Penetration Testing

- Penetration testing is security testing in which assessors simulate real-world attacks to identify methods for evading the security features of an application, system, or network
- Often involves launching real attacks on systems and data that use tools and techniques commonly used by attackers
- Penetration testing can also be useful for determining:
    - How well the system tolerates real world-style attack patterns
    - The likely level of sophistication an attacker needs to successfully compromise the system
    - Additional countermeasures that could mitigate threats against the system
    - The defenders' ability to detect attacks and respond appropriately

Penetration Testing Terms

- Pre-engagement meetings determine a variety of elements:
    - Scoping (are you going to look into the wireless network first) and restrictions (is the CEO's laptop off-limits)
    - Pricing and cost structure
    - Know-all, know-nothing (clear/opaque or viewed/hidden or visible/invisible)
    - Credentialed vs. non-credentialed
    - Bug bounties
    - Intrusive vs. non-intrusive

Penetration Testing Life Cycle

1. Information gathering/reconnaissance -> the less you know the more lengthy the first phase will be
2. Threat modeling -> using data flow diagrams against applications, determining the vectors to be used, vectors and malware
3. Vulnerability analysis and scanning tools -> vulnerability scans are part of a pen test
4. Exploitation -> determine the vector and the payload
5. Post exploitation -> attempt to move laterally, escalate or elevate privileges or cover their tracks by deleting logging or logging files, placing malware in RAM or encrypted or compressed files low in the file system
6. Reporting -> after action report shows recommendations and weaknesses and controls to decrease risk and vulnerability to different kinds of attacks

Vulnerability Response and Remediation

- Additional control implementation
    - Categories (Administrative, Technical, Physical)
    - Types (Detective, Preventative, Deterrent, Compensating, Corrective)
- Patch management (tested)
    - The initiative of applying updates to software, drivers, and firmware to protect against vulnerabilities
    - Effective patch management also assists in choosing the optimal performance and productivity of applications, services, and systems
- Exceptions and exemptions

Remediation Validation and Reporting

- Implementing controls in response to vulnerability scanning and testing must be followed with security control assessment and evaluation
- Next steps involve tuning to address false positives and false negatives
- This will lead to rescanning as well as any new configuration changes or updates/versioning
- Official internal and external audits should follow to assess compliance, maturity, assurance, certification, and accreditation
- The assurance testing process concludes with validation and robust reporting

Robust Reporting

- Reports should have as much information as necessary but not a “data overload”
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)
- Understand components of visual communications
    - Avoid three-dimensional representation
    - Use a palette of sequential colors
    - Avoid pie charts in favor of scatterplots, bars and bubble charts, histograms, density plots, and boxplots

Security Monitoring and Alerting

Monitoring Computing Resources

- Monitoring and visibility is a critical aspect of hardened security and zero trust initiatives
- The more automated the monitoring solution, the more accurate the results will be as human error and configuration error is minimized
- All types of systems must be monitored including:
    - Corporate LAN endpoint devices
    - Web, email, productivity, and other application servers (i.e. SharePoint)
    - Voice over Internet Protocol (VoIP), messaging and conferencing services
    - Databases and storage area networks
    - Infrastructure devices
    - Customer premises edge

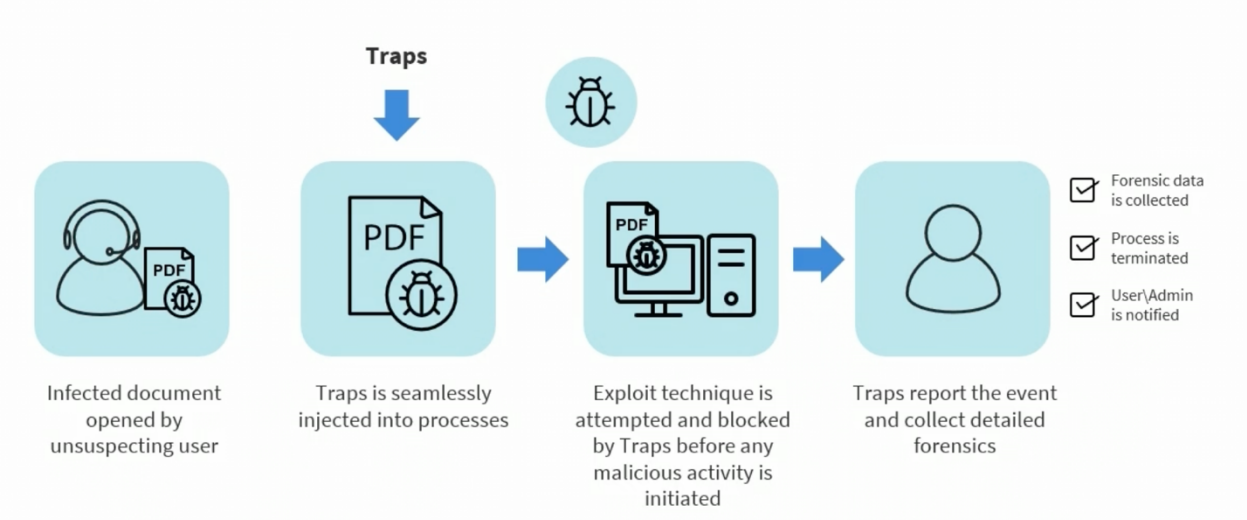
Monitoring and Visibility

- Network monitoring tools enhance visibility into system health by offering real-time information about various wired, wireless, and cloud-based components
- This suite of tools utilizes two techniques to capture performance metrics from assorted infrastructure and security devices – both physical and virtual:
    - Agent-based monitoring -> leverages lightweight software, known as monitoring agent, on the devices or virtual machine to track the uptime and performance
    - Agentless monitoring uses special application programming interfaces (APIs) or integrated code to track the health of the devices

Agent-based Monitoring

- A prototypical example of agent-based monitoring is using Simple Network Management Protocol version 2c and the more secure version 3 agents on infrastructure devices to send traps and informs to SNMP management stations
- In cloud computing environments, special agents can be embedded into virtual machine instances or installed on instantiated virtual servers to perform various system management activities

Case Study: Palo Alto Networks Traps



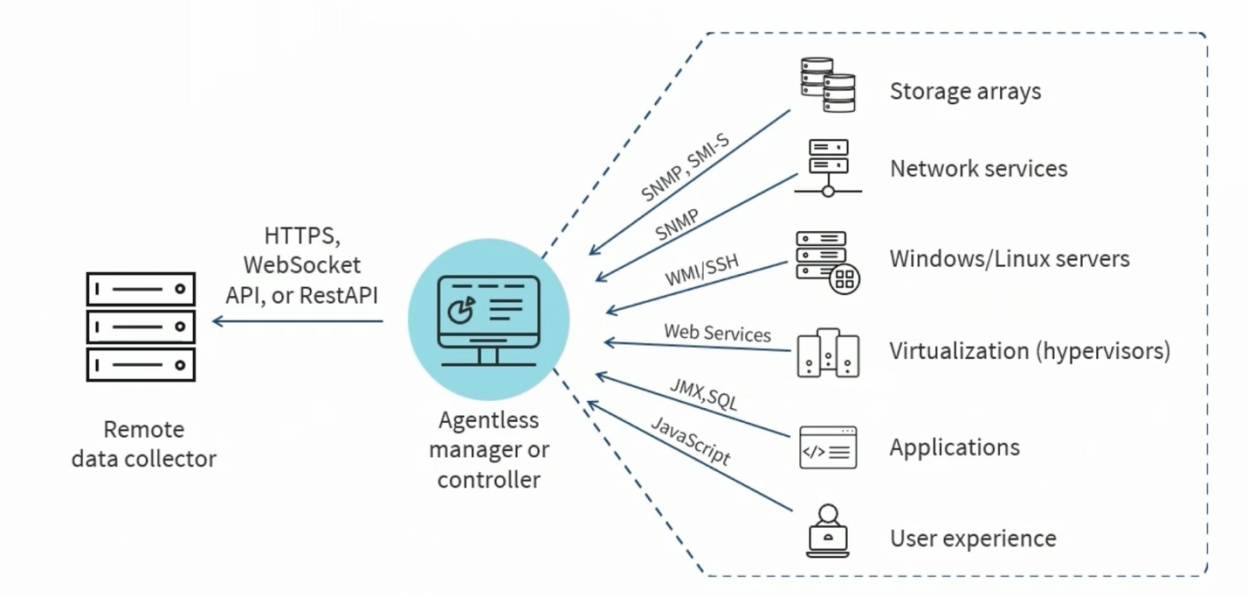
-
- The end user working at a call center accidently downloads a infected document (pdf) and open it in a unsuspecting way. Palo alto traps is seamlessly injected into the processes. A exploit

technique is attempted but is blocked by traps before any malicious activity is initiated. The palo alto will report the attempt and collect detailed forensic or e-discovery data. Forensic data is collected, the process is collected and the user/admin is notified

Agentless Monitoring

- Agentless monitoring is a less intrusive way to achieve visibility
- It typically utilizes application-specific APIs and different network protocols (such as SNMP and Windows Management Interface – WMI) to discern the overall performance of on-site and cloud-based assets, such as servers and applications
- This monitoring method does not involve the overhead of installing, tuning, and updating dedicated or third-party monitoring agents on every component
- This may be considered easier than the traditional agent-based approach

Agentless Monitoring



-
- On the right hand side we see a wide variety of devices that are sending information. E.g. storage arrays sending SNMPv3 which is a storage management initiative specification. Network devices sending SNMP traps or informs. Windows or Linux servers sending WMI. All to a agentless management or controller (often in the cloud), and then using transport layer security or web socket apis or restful apis to the remote data collector

Log Aggregation

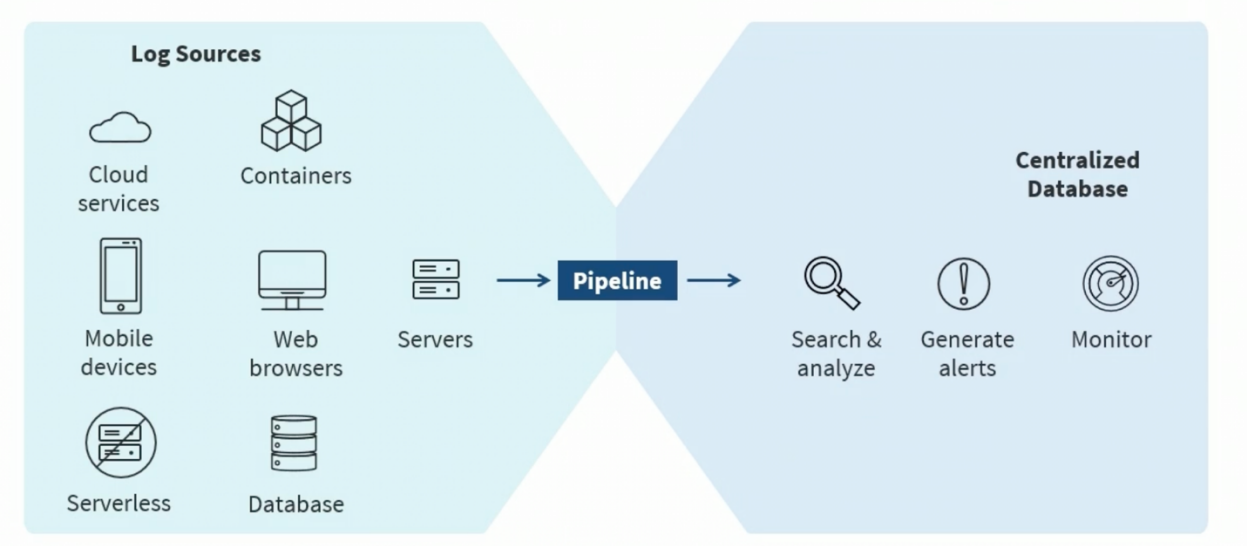
- Log aggregation is the process of accumulating, categorizing, standardizing, and consolidating log data from across an IT infrastructure to enable and enhance streamlined log analysis
- Without log aggregating, administrators and engineers would have to manually organize, deduplicate, and search through log data from various sources to generate meaningful metrics and information

Log Aggregation Goals

- Replicating log files to a centralized location
- Collecting Syslog, audited, and other traps
- Supporting automated pipelines and workflows
- Parsing key-value pairs

- Performing more complex transformations such as multiline log aggregation, tokenization, scrubbing, or masking sensitive data

Log Aggregation Pipelines



-
- Log sources are fed into a pipeline targeting a centralized database to search and analyze, generate alerts and monitor often with machine learning/ai tools

Alerting

- An alerting system delivers metrics and alrms from various tools and systems to admins and security operators for informational/event notifications, incident management, and optimization of the wider ecosystem
- These platforms help to ensure that event responses are quick and efficient so that the odds of overlooked actions are reduced, in other words false negatives
- As systems grow larger and more complex, alerting systems are more automated and orchestrated with specialty platforms and services (server-based and serverless)

Alerting Best Practices

- Choose quality over quantity
- Produce actionable results
- Consider broadcasting for mass notifications
- Have a well-designed service desk and escalation processes
- Prioritize alerts send by people
- Automate whenever feasible

Scanning Tools

- Also sends alerts and other outputs to systems
- Examples of scanners:
    - Wired and wireless IP scanners
    - Port scanners
    - Vulnerability scanners (Nessus)
    - Compliance scanning

Scanning and Alerting Life Cycle

- Planning or information gathering
- Implementation

- Testing and validation of the scans and alerts (removing false positives and tuning
- Response (security orchestration and automation response systems, fully automation, semi-automated and manual runbooks/playbooks)
- Remediation (quarantine, compartmentalization, file disposition, deletion)
- Archiving and reporting

Security Content Automation Protocol (SCAP)

- According to NIST: "The security content automation protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures that broadest possible range of use cases is reflected in SCAP functionality

Importance of SCAP

1. Improves cybersecurity posture -> improving security hygiene
2. Streamline vulnerability evaluation, assessment and analysis
3. Simplifies compliance -> compliance to best practices, policies, regulation, governance
4. Makes software deployments easy
5. Boosts cybersecurity collaboration -> between stakeholders, skillsets, processes

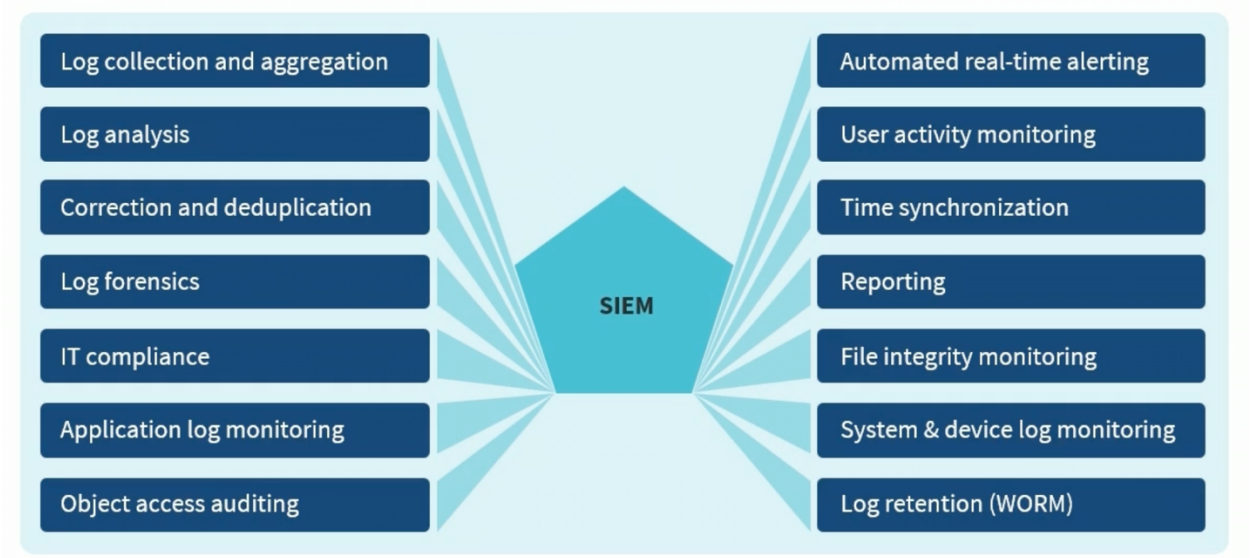
SCAP Specifications

- Asset Identification plays an important role in an organization's ability to quickly correlate different sets of information about assets
- The Asset Reporting Format (ARF) is a data model to express the transport format of information about assets, and the relationships between assets and reports
- Common Platform Enumeration (CPE) is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets
- Open Vulnerability Assessment Language (OVAL) is an information security community effort to standardize how to assess and report upon the machine state of computer systems
- The Open Checklist Interactive Language (OCIL) defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions
- Trust Model for Security Automation Data (TMSAD) describes a common trust model that can be applied to specifications within the security automation domain, such as SCAP
- The Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents
- Software Identification (SWID) Tagging allows for the proper management of software inventories of managed devices in support of higher-level business, information technology, and cybersecurity functions

Security Information and Event Management (SIEM)

- Security information and event management is a solution that helps enterprises detect, analyze, and respond to security threats before they affect business operations
- SIEM is a combination of security information management (SIM) and security event management (SEM) into a unified security management system
- SIEM technology gathers event log data from a range of sources and recognizes activity that diverges from the norm in real-time

SIEM



-
- Can pick and choose what features you want in your SIEM system. Its ability to collect information from a wide variety of devices, applications and services, aggregate it, correct it, normalize it, deduplicate it. Can do real time alerting, object access reporting, forensics, file integrity monitoring, or send the output to a SOAR system or a wide variety of services on the cloud

Benefits of SIEM Systems

- A centralized look at potential threats
- Real-time threat identification and response
- Advanced threat intelligence
- Regulatory compliance auditing and reporting
- Enhancing transparency into users, applications, and devices

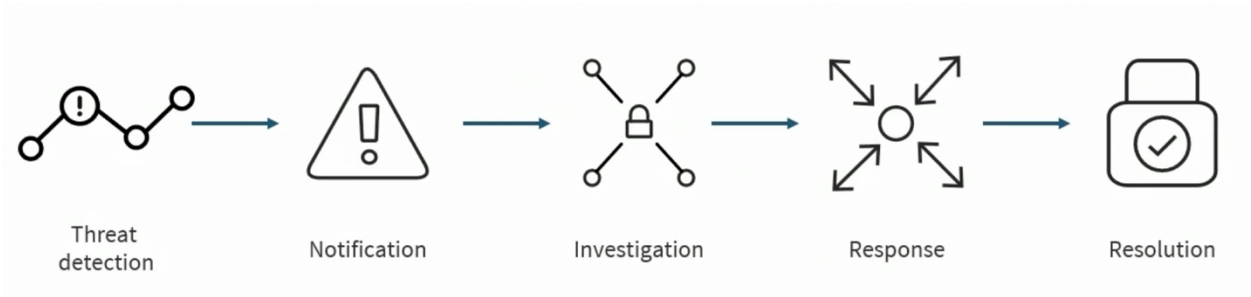
Security Orchestration and Automation and Response (SOAR)

- Security orchestration, automation, and response is an assortment of software services and tools that allow organizations to simplify and aggregate security operations in three core areas
    - Threat and vulnerability management
    - Incident response
    - Security operations automation

Security Orchestration and Automation and Response

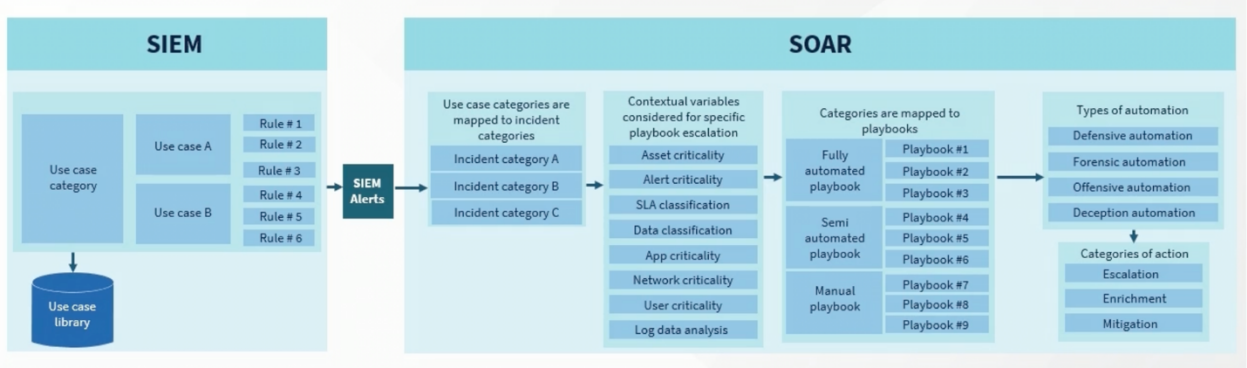
- Security automation involves performing security related tasks without the need for human intervention, or reduces the need for human intervention.
- Can be defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing
- You should automate if the process is routine, monotonous, and time-intensive

SOAR Cycle



-

SIEM + SOAR



-
- The SIEM system sends out alerts based on a wide variety of different rules, use cases. The alerts are then mapped to incident categories within the SOAR system, and then contextual variables are considered, such as the criticality of the assets (1-10). The playbooks will be fully automated, semi automated, or manual to then automate for defensive, forensic, offensive or deception. A SIEM system can run separate from a SOAR system. Can run independently of each other or together. Together is the more optimal option

Antivirus Systems

- Antivirus software is intended to protect computers and mobile devices from exploits, malware, crackers, and cybercriminals
- The systems examine data on hard drives, memory, and incoming packets from the Internet (websites, email messages, attachments, and applications) to recognize, block, and offer ongoing protection against malicious software, infected links, and other threats and suspicious activity
- Antivirus software functions by regularly scanning all devices to discover and block known worms and viruses as well as new and emerging malware variants
- If a device gets injected, antivirus software will also quarantine and eradicate it
- Many systems employ a heuristic detection method to examine code for suspicious architecture and behavior rather than a specific static signature
- To offer the best possible protection, these systems use several forms of detection:
    - Signature detection
    - Heuristic detection of files
    - Multicriteria analysis (MCA) – uses the data from other detection methods to flag a file as possibly dangerous
    - Sandbox and cloud analysis
    - Intrusion prevention via host intrusion prevention system (HIPS)
    - Anti-spam
    - Ransomware protection

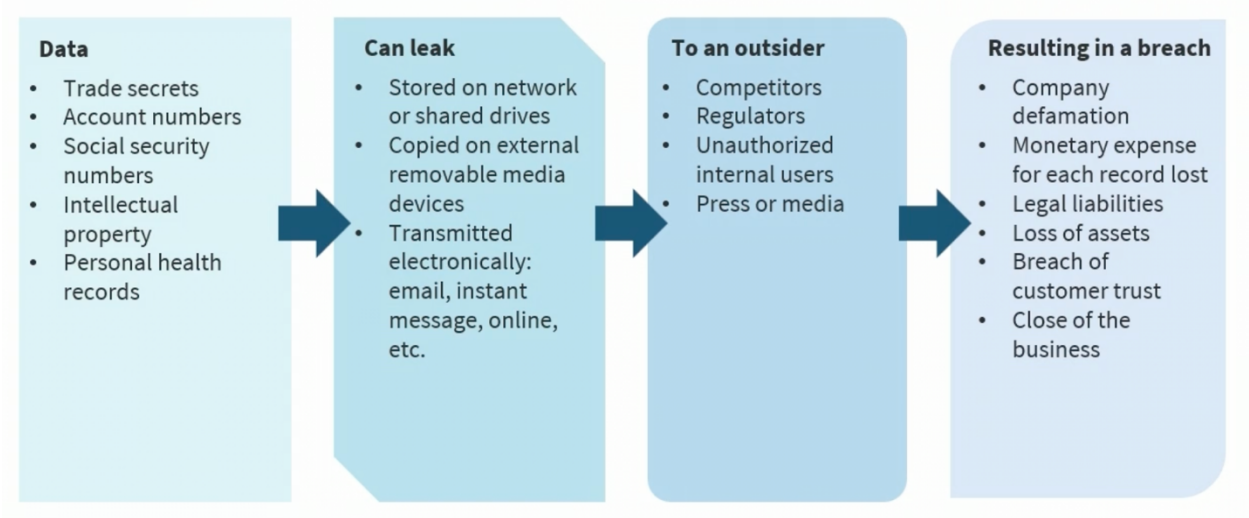
Antivirus Systems Features

- Signature detection to look for specific code from known viruses
- Heuristic detection to find suspicious architecture and behavior in code
- Cloud and sandbox analysis to run suspicious programs inside a contained and secure system to see what they do
- HIPS to bridge firewalls and other security systems for added protection

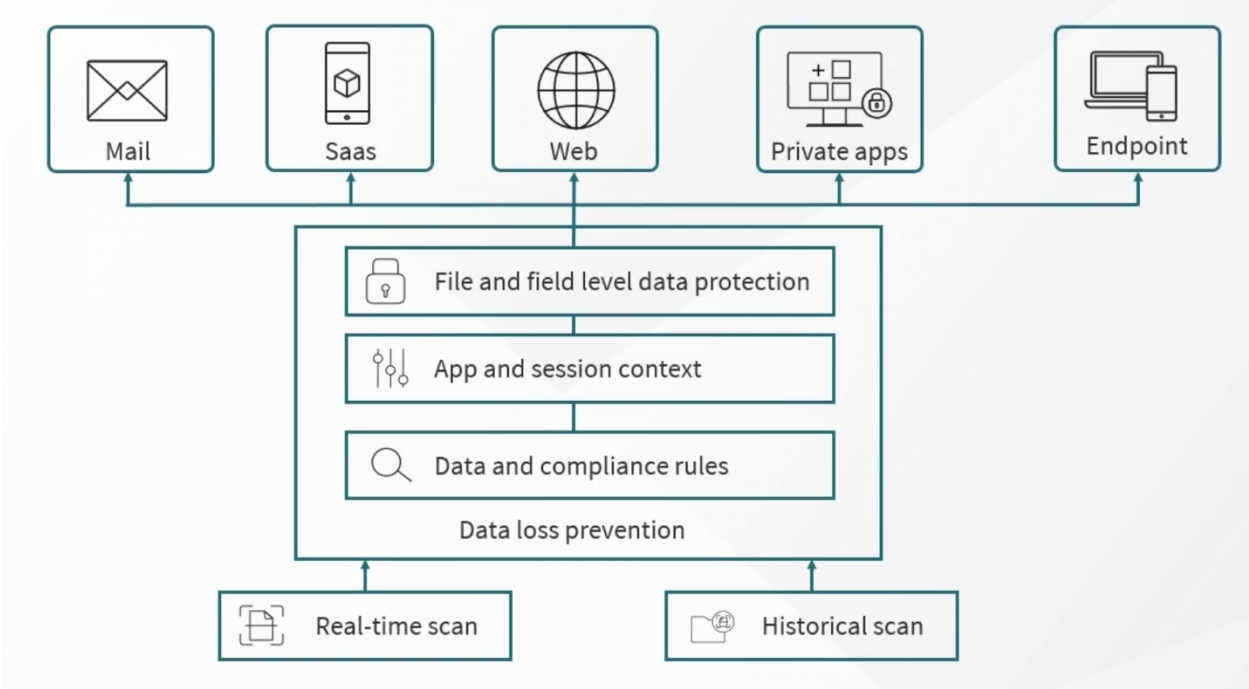
Data Loss Prevention (DLP)

- Data loss prevention is a security initiative that recognizes and mitigates unsafe or unauthorized sharing, transfer, or use of sensitive data such as personally identifiable information (PII) and protected health information (PHI)
- DLP engines and services can help organizations with monitoring and protection of sensitive information across on-premises systems, cloud-based locations, and endpoint devices
- It also assists with compliance for regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR)

Data Loss Prevention



-
- All different types of data (e.g. trade secrets, account numbers) can leak by being stored on network or shared drives, copied on external media devices, to a wide variety of various outsiders (e.g. competitors, regulators, press/media), resulting in primary and secondary loss (e.g. company definition, assets, customer trust, close of business)

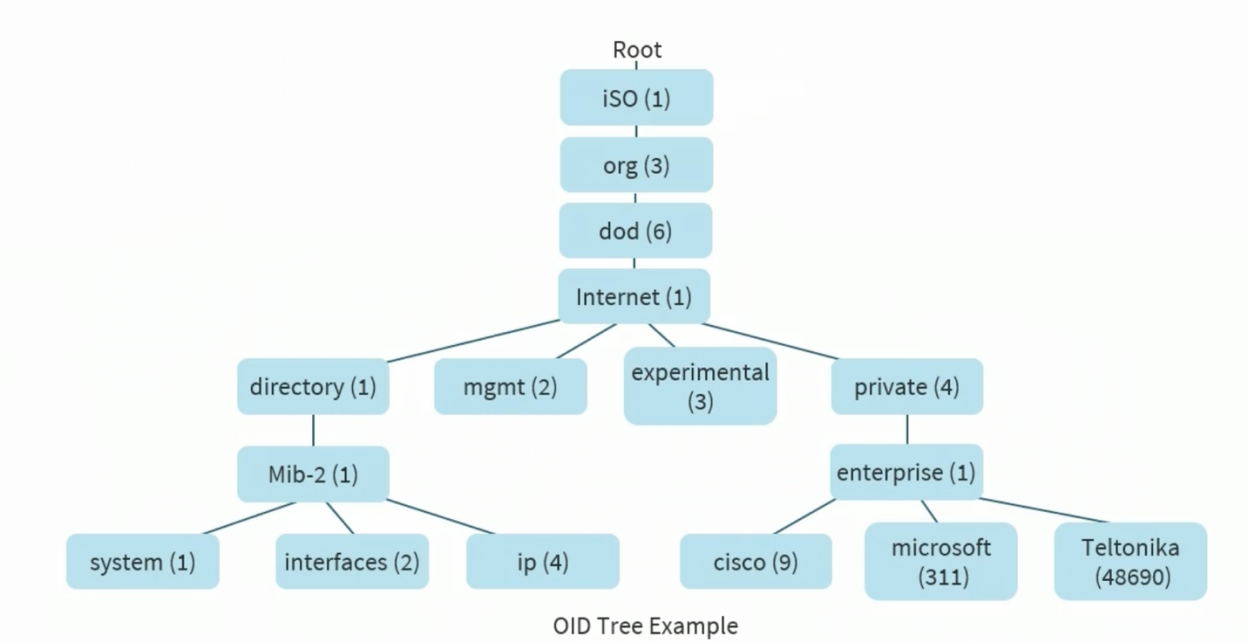


-
- Data loss prevention engine doing real time scanning, historical scanning of stored logs and files. DLP engine provides file and field level data protection, app and session context, data and compliance rules for email, SaaS, web, private apps and a wide variety of end points

Simple Network Management Protocol

- Simple Network Management Protocol is a powerful protocol and toolset that facilitates the sharing of information among various devices on a network, regardless of their hardware or software
- Although there are many emerging replacements for SNMP, it is still widely deployed in enterprises globally
- SNMP uses a basic client-server architecture using:
    - Managers collect and process information about devices on the network
    - Clients, called agents, are any type of device or device components connected to the network

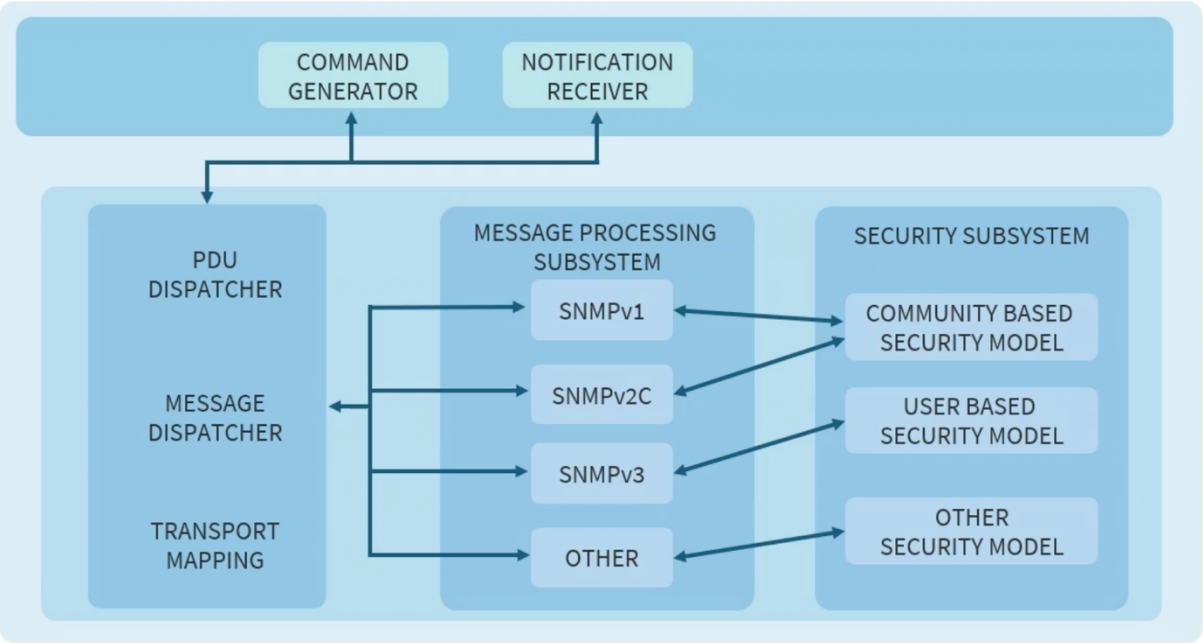
SNMP Tree Architecture



OID Tree Example

- SNMP uses a inverted tree architecture. At the top we have the root (ISO organization) and to identify a configuration item you identify it based on the path it takes from the root. E.g. if it is a CISCO device configuration item the identifier will be 1.3.6.1.4.1.9. Here we just see three vendors but SNMP is supported by many different vendors, all which have their own configuration items.

SNMP v3 Architecture



-
- Newest version of SNMP is v3. V3 is still a client server solution. Have a command generator and a notification receiver. Older versions of SNMP (v1, v2c) use a community based security model (shared password, community string) which is writable string so you can change a configuration item or read only. V3 went to a user based security model, going away from the community string, and also adding security algorithms and mechanisms, for confidentiality, origin authentication and integrity.

SNMP Version 2c vs. SNMP Version 3

	SNMPv2	SNMPv3
Primary standards	RFC- 1901	RFC- 3412, RFC- 3414, RFC- 3415, RFC- 3417,
Allowed operations	Get, GetNext, Set, Trap, GetBulk, Inform, Response	Get, GetNext, Set, Trap, GetBulk, Inform, Response with PDU message format
Authentication	Community based	User and group based
Plain text community strings	Yes	No
Data encryption	None	DES/SHA/MDS/AES
Device identification	Request/response protocol	EngineID uniquely identifies each SNMP entity
MIB	Defines general framework for definition and construction of MIB	Configures permissions based on user for differing levels of MIB access
Default/known passwords	Yes	No
Data tampering protection	No	Yes
Eavesdropping protection	No	Yes
Unauthorized access protection	Limited based on locally defined ACLs	Yes

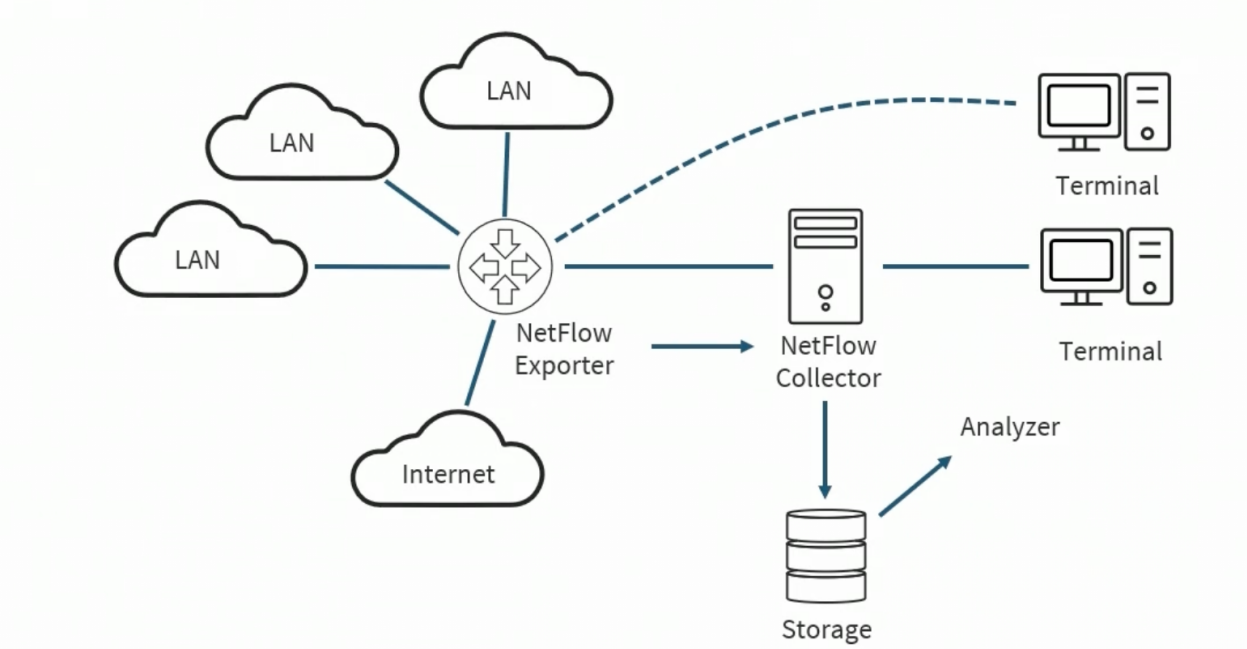
-
- Couple differences. In v3 it involved several more RFC's for request for comments. Authentication is no longer based on community string it is user and group based. V3 has no plain text community strings anymore and it supports several mechanisms for data encryption (AES being preferred). V3 has no default or pre known passwords.

NetFlow

- NetFlow is a network monitoring protocol, developed by Cisco, invented to capture metrics about the volume and types of traffic traversing a network device
- Technically, a flow is defined by its 5-tuple, a collection of five data points:
    - The source and destination IP addresses exchange information
    - The source and destination ports, if any (ICMP, for example doesn't use ports, it uses message types and codes)
    - The protocol (e.g. file transfer protocol, hyper text transport protocol (HTTP))

NetFlow 9

- By collecting and analyzing this flow data, engineers can learn details about how the network is being used for troubleshooting network issues, identifying bandwidth hogs, and tacking which external IPs or countries one is exchanging data with
- NetFlow was first implemented in Cisco devices in 1995
- It has followed a curious evolution over the years, starting as a static protocol with a fixed set of statistics collected for all flows
- In version 9, the latest version from 2021, network professionals can choose which statistics to enable, and vendors can implement extensions (extensible) to attach proprietary metadata to flow entries

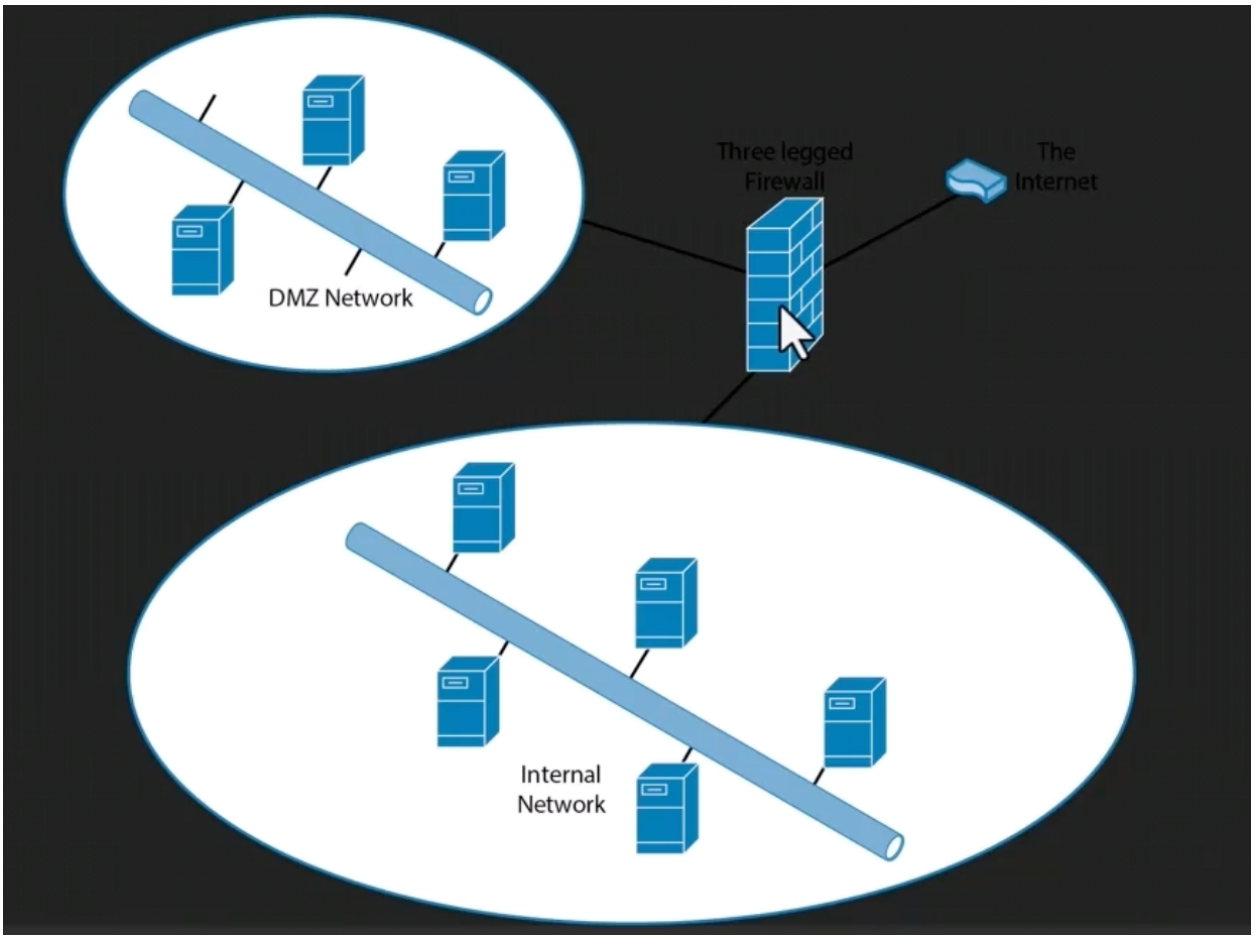


- In the architecture the NetFlow exporter will be a multilayer switch or a customer premise equipment router or a firewall appliance (CISCO ASA). The software and hardware combination its receiving a flows (records) is called the NetFlow collector (e.g. solar winds). The data is stored traditionally in relational databases and then analyzed often in the cloud with the results sent to terminals or dashboards in the security operations center. Can also be sent to a SOAR system for automation and orchestration.

Enterprise Security Capabilities

Exploring Firewall Implementations

- Static/stateless firewall (access control list). Inbound and outbound rules applies to everything in the network or the subnet. Access control list will affect all packets going in and out. There is an implicit deny all. Normally increment by 5-10 so you don't have to renumber them all. Has all common services and protocols. Having the first entry allowing everything and allow everything to only come in if you need to do deny entries if under attack from a certain IP address and port they are attacking on.
- Security group is an allow list or a stateful firewall. Security group (stateful firewall) in aws. In a security group there is no numbers, it is essentially a white-list or allow list of things that are allowed to happen. Also no permit or deny. Security group is applied directly to the instance. Technically applied to the virtual network interface that has a virtual mac address of the server. If it's a network security group, then it's a stateful firewall storing information about the TCP connection, UDP flow, in the cloud in the hypervisor or firewall appliance security gateway. If it's a security group it can be applied to the instance, if it's a network security group it will apply to everything in the network or the subnet.
- Screened subnet:



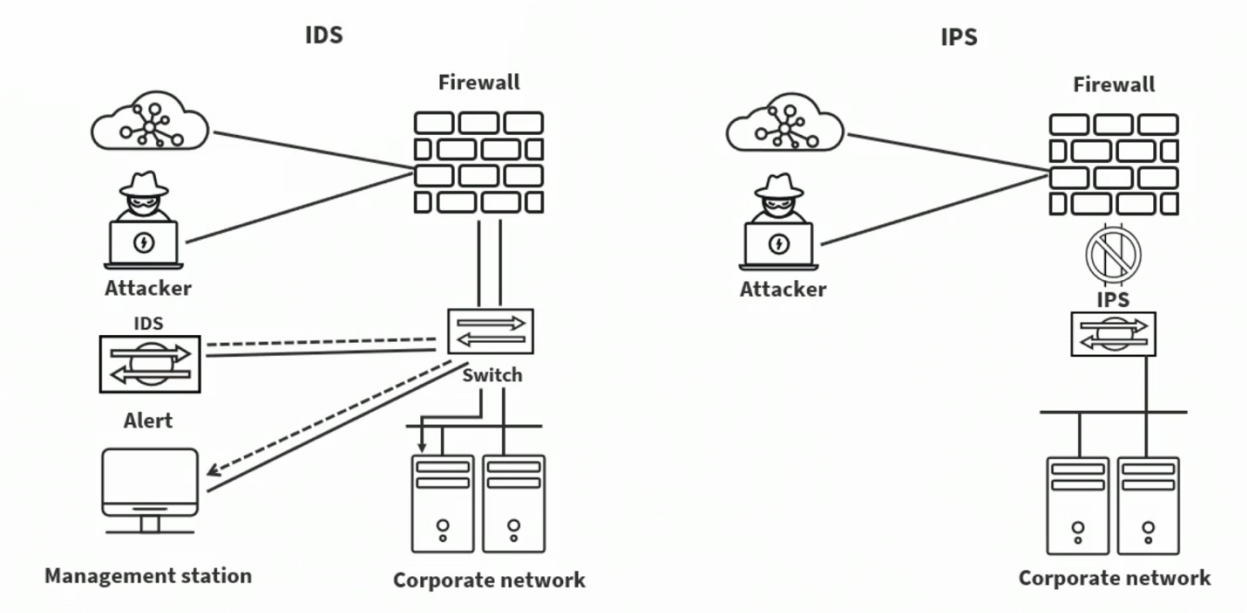
  - Fancy term for a three-legged or three armed firewall. Can be a firewall router, appliance, etc. and its got three interfaces going to three different zones. This screened subnet is basically a three armed firewall, one interface going to the public internet (upstream router or upstream customer premise equipment, etc.) public zone. Have a dmz or public access zone (all public facing servers) anyone on the internet that wants to get something from you must put those servers on the DMZ network (ftp servers, dns servers, etc.) only the things

you make available to the public go in that DMZ network. Then have a inside internal network.

Intrusion Detection and Prevention Systems (IDS and IPS)

- IDS and IPS is a combination of hardware and/or software to allow visibility and mitigation of existing exploits and malware on the network or individual hosts.
    - Today, its usually IPS and its network based, since host based IPS is often reserved for endpoint detection and response and other next generation endpoint solutions
- Snort IDS running on Unix machines was the original intrusion detection daemon
- Original serves were highly static signature-based solutions with anomaly detection introduced in later models
- These have evolved into advanced next-generation artificial intelligence (AI)/machine learning (ML) solutions

IDS vs. IPS



-
- IDS sensor was a stand alone appliance or a daemon running on a Unix or linux box. The layer 2 switch would isolate certain ports using a protocol (SPAN) to send copies of the frames to the IDS sensor. Then if the packet matched a signature it would send an alert or an alarm to the management station. The IDS was actually reactive so its possible that an attacker delivered the malware or the exploit to the target on the corporate network. The IDS sensor was not inline so it could not take aggressive actions such as dropping packets inline or denying attackers based on their IP address
- IPS is an inline solution. Could be a standalone IPS sensor running behind the firewall or a service or a module in the firewall. Either way it is physically or logically behind the firewall but is inline so it can actually aggressively drop packets or deny attackers before it reaches the corporate network. This would be a proactive solution. Most solutions today are IPS and they are initially deployed in a IDS mode or a passive or monitor mode so they can tune them to reduce false positives and put them into inline mode.

IPS Characteristics

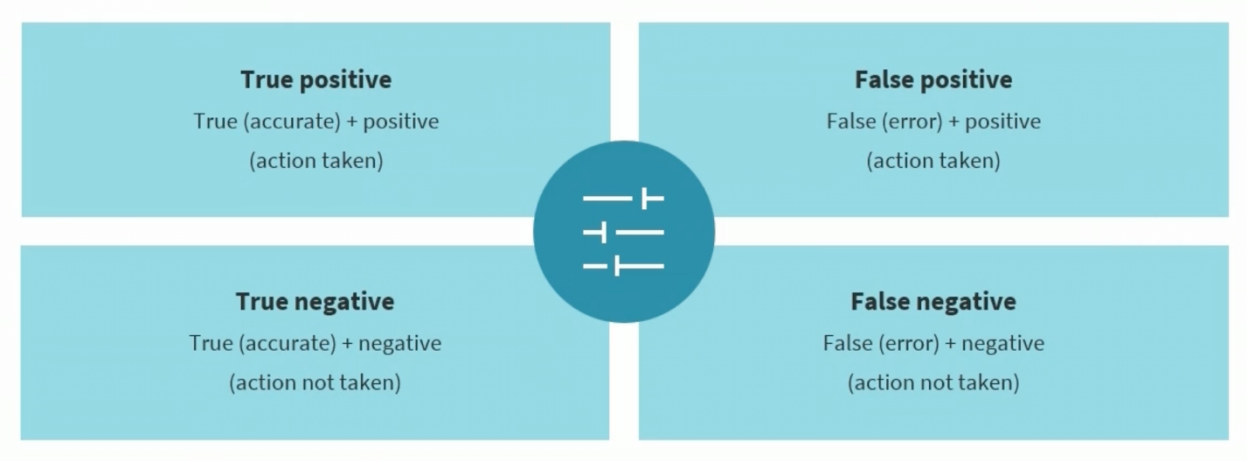
- Inline IPS or monitor (passive mode, OR initial monitor. E.g. passive mode in a honeynet for active defense)
- In-band vs. out-of-band (OOB): e.g. inline = in-band, detective or passive mode = out-band

- Signature-based and anomaly-based
- Heuristic-based
- Machine learning and AI-driven (leverage cloud and machine learning engines)
- Cloud-based correlation and integration

IPS Actions

- Alerts/alarms and verbose dumps
- Transmission Control Protocol (TCP) resets, blocks, and shuns
- Block attackers inline and drop packets
- Syslog, Simple Network Management Protocol (SNP), and NetFlow outputs
- Integrate with security information and event management (SIEM) and security orchestration automation, and response (SOAR) systems

IPS Tuning

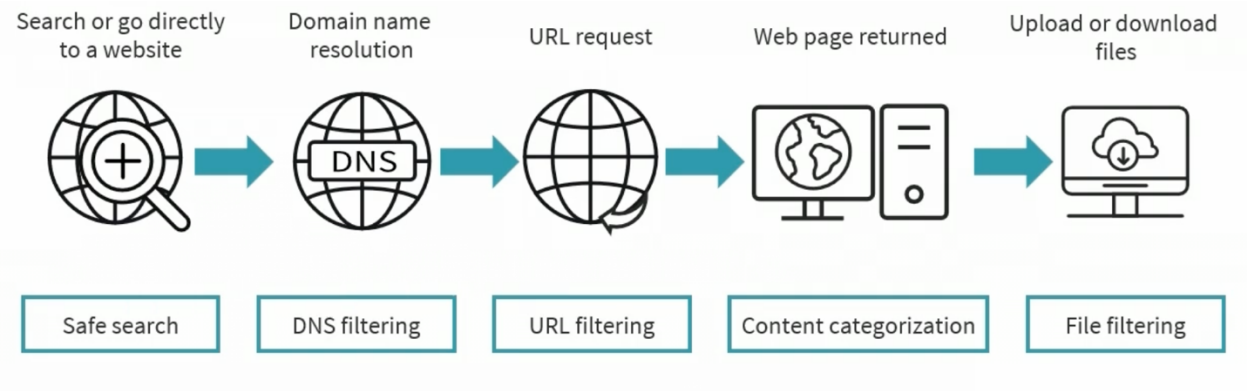


-
- When it comes to tuning IDS and IPS what we want are true positives and true negatives. A true positive is when a sensor actively takes an action. A true negative is when a sensor actively does not take an action (benign traffic). Early on in the process you want to fine tune to reduce false positives (blocked benign traffic). False negative is when you did not take action when necessary. IPS tuning involves reducing false positives and false negatives

Web Filters

- A web filter is an application layer gateway server or service (physical or virtual dedicated to analysis and control of HTTP and HTTPS traffic
- Agent-based web filters require the deployment of lightweight software packages on network devices, whereas agentless filters can be instantly deployed in Random Access Memory (RAM) or persistently without any manual configuration
- Many filtering solutions are deployed on the customer premises equipment as a centralized proxy to process all web traffic from layer 3 through layer 7

Web Filtering



-

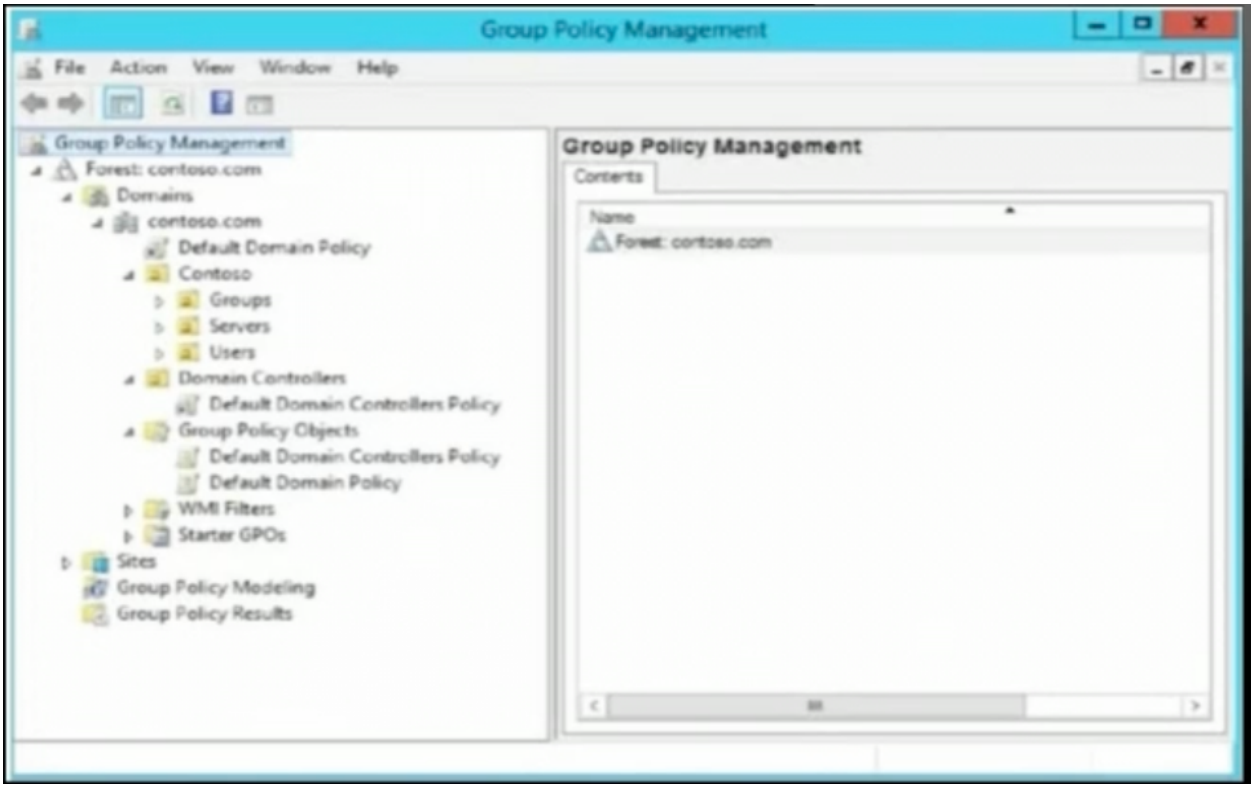
Reputation Filtering

- Web reputation services accuracy is typically determined by the breadth, depth, and variety of the data being used
- The algorithms used to analyze the relationships between Internet objects and web reputations must be persistently trained by experienced human analysts and artificial intelligence tools
- With an accurate web reputation source fueling associated URL filters, firewall solutions, or other specialty appliances, one can produce a resilient, proactive cybersecurity posture
    - Finally, when using cloud correlation or reputation, vendors and cloud service providers can distribute this information all over the world, often notifying their customers within minutes of a zero day attack, by a bad actor, domain or its IP address.

O/S Security: Group Policy

- Group Policy (GP) is a Microsoft Windows service that enabled IT administrators to centrally manage and configure the settings on Windows operating systems
- Group Policy can manage operating system settings, applications, browsers, and user settings
- GP is used in Active Directory (AD) environments with domain-joined computers as well as Microsoft Azure (Microsoft service provider) hybrid joined devices
- Some Group Policy examples include:
    - Password Policy
    - Screen Lock
    - Power Settings
    - Map Network Drives
    - Install printers, software, desktop shortcuts, etc.
    - Software restrictions (blocking access to programs)
- Group Policy Objects (GPOs) are collections of policy settings that apply to the domain (or OU) to manage users, computers, or the entire domain

Group Policy Management Console (GPMC)

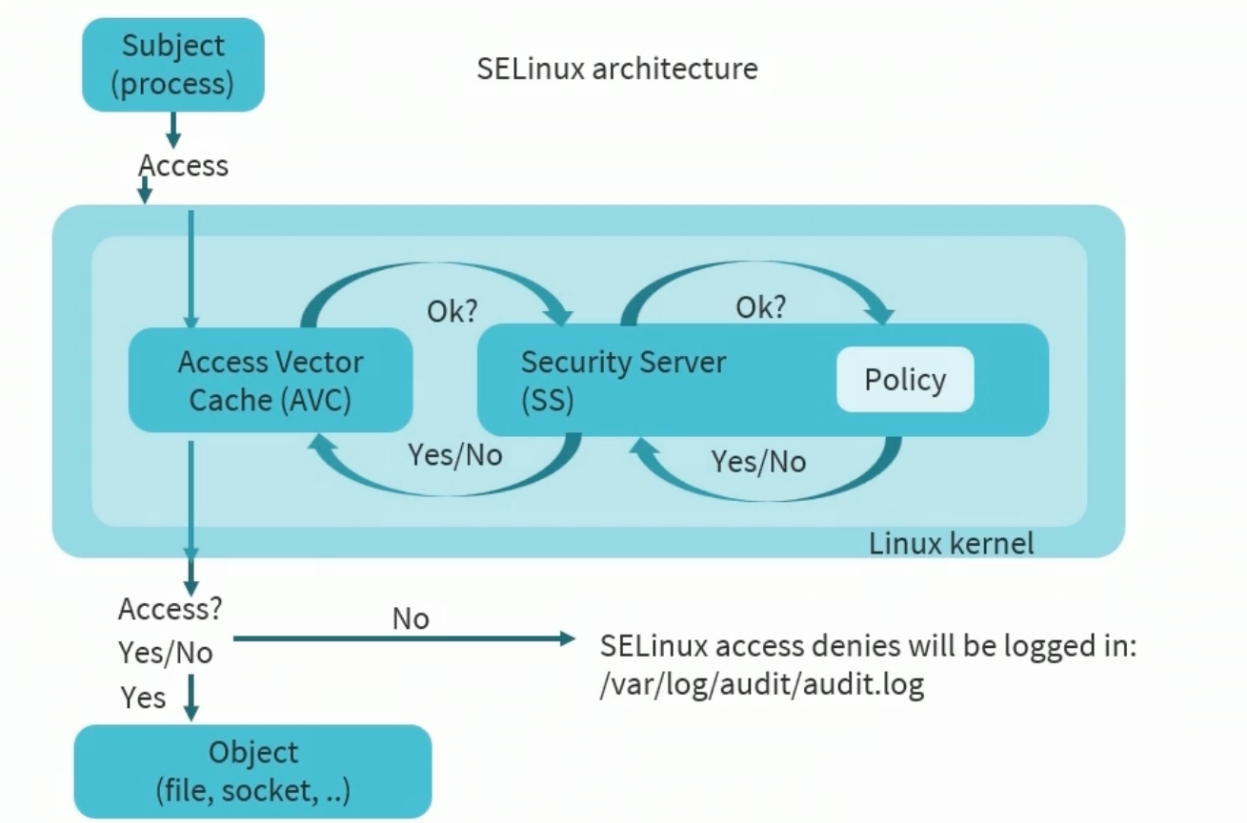
- 

O/S Security: Security Enhanced Linux

- Security Enhanced Linux (SELinux) is an access control system built into the Linux kernel
- It is used to enforce the resource policies that define what level of access users, programs, and services have on a system
- In its default enforcement mode, SELinux will deny and log any unauthorized attempts to access any resource
- This enforces the principle of least privilege, in that explicit permission must be given to a user or program to access files, directories, sockets, and other services

SELinux

- There are several ways to configure SELinux to protect a system
- The most common are targeted policy or multi-level security (MLS)
    - Targeted policy is the default option and covers a range of processes, tasks, and services
    - MLS can be very complicated and is typically only used by government organizations
- The /etc/sysconfig/selinux file has a section that shows you whether SELinux is in permissive mode, enforcing mode, or disabled, and which policy is supposed to be loaded



-
- When the subject or process wants to get access to a file or a socket or a process it goes through the access vector cache (AVC). The security server determines if that's okay, if no it gets sent back to the cache and SELinux will deny access. If it's allowed then the security server applies the policy. SELinux operates down at the Linux kernel level (very low level) and only explicit access is given through the security server policy to the object.

Internet Protocols Are Unsecure by Design

Number	Name	Description
7	Application	HTTP, FTP, SMTP, DNS, TELNET, LDAP, POP, IMAP
6	Presentation	ASCII, PNG, MPEG, AVI, MIDI
5	Session	SSL/TLS, SQL, RPC, NFS
4	Transport	TCP, UDP, SPX, AppleTalk
3	Network (or Internetwork)	IP, IPX, ICMP, ARP, BGP, OSPF
2	Link	PPP/SLIP, Ethernet, Frame Relay, ATM
1	Physical	Binary transmission, encoding, bit rates, voltages

-
- Unsecure by default
- Please Link Network Transmission Sessions Pussy Ass

Security + Ports and Protocols

Layer 7 application	Port Number	Use
File Transfer Protocol (FTP)	20/21	Port 21 is the control, while port 20 is used to transfer files
Secure Shell (SSH)	22	Designed to transmit data through a remote connection
SSH File Transfer Protocol	22	A separate protocol from FTP (it is not compliant with FTP servers) that uses SSH to encrypt file transfers
TACACS+	49	Cisco proprietary protocol used for authentication, authorization, and accounting (AAA) services
Domain Name System (DNS)	53	Used to associate IP addresses with domain names
Dynamic Host Configuration Protocol (DHCP)	67/68	This network management protocol is used to assign local IP addresses to devices on a network. It is used to create multiple private IP addresses from one IPv4 address
Hypertext Transfer Protocol (HTTP)	80	Protocol used for websites and most Internet traffic
Kerberos	88	Network authentication protocol that allows for communication over a non – secure network
Post Office Protocol (POP)	110	Email protocol that allows email clients to communicate with email servers; POP providers only one-way communication
Internet Message Access Protocol (IMAP)	143,993	Email protocol used by email clients to communicate with email servers; provides two-way communication unlike POP
Simple Network Management Protocol (SNMP)	161/162	Protocol used to monitor and manage network devices on IP networks
Lightweight Directory Access Protocol (LDAP)	389	Used to manage and communicate with directories
Hypertext Transfer Protocol Secure (HTTPS)	443	Secure version of HTTP that used TLS for encryption; most websites use HTTPS instead of HTTP
Lightweight Directory Access Protocol Secure (LDAPS)	636	Secure version of LDAP that uses TLS for encryption
File Transfer Protocol Secure (FTPS)	989/990	FTPS uses TLS for encryption; it can run on ports 20/21 but is sometimes allocated to ports 989/990
Internet Message Access Protocol Secure (IMAPS)	993	Secure version of IMAP that uses TLS for encryption
Post Office Protocol 3 Secure (POP3S)	995	Secure version of POP that uses TLS for encryption
Remote Authentication Dial-In User Service (RADIUS)	1812, 1813	Used to provide AAA for network services
Diameter	3868	Developed as an upgrade to Radius
Secure Real Time Protocol (SRTP)	5004	SRTP replaced RTP and is a protocol used to stream audio and video communication using UDP

- Application layer services and protocols are unsecure natively to by default

DNS Filtering

- One of the most unsecure protocols in the TCP/IP stack on the internet
- DNS filtering is the technique of using DNS to block malicious websites and filter out damaging or unsuitable content
- This ensures that organizational data stays secure and private
- It allows the enterprise to have control over what their employees can access on company managed networks and endpoints
- DNS filtering is often part of a wider access control strategy
- All DNS queries are delivered to a DNS resolver
- Specifically configured DNS resolvers often function as filters by refusing to resolve queries for certain domains that are tracked in a blocklist or reputation list, therefore blocking users from accessing those domains servers
- DNS filtering services can also use an allowlist instead of a blocklist
- DNS filtering can blocklist web attributes based on domain name or IPv4/v6 address:
    - By domain: The DNS resolver does not resolve (or look up) the IP addresses for certain domains at all
    - By IP address: The DNS resolver attempts to resolve all domains, but if the IP address is on the blocklist, the resolver will not send it back to the requestor

DNS Security Extensions (DNSSEC)

- DNSSEC adds a layer of trust on top of DNS by providing authentication
    - This extension does not provide confidentiality
- When a DNS resolver is looking for www.skillsoft.com, the .com name servers help the resolver verify the records returned for Skillsoft, and this security extension service helps verify the records returned for site
- The root DNS name servers help verify .com, and information published by the root is vetted by a thorough security procedure, including the Root Signing Ceremony

DNSSEC

- DNSSEC allows you to sign your company's DNS records so that any system that has an authenticating DNS resolver will automatically verify if the records are valid or have been compromised by a man-in-the-middle (MiTM) attack
- To facilitate signature validation, DNSSEC adds a few new DNS record types:
    - RRSIG – contains a cryptographic signature
    - DNSKEY – contains a public signing key
    - DS – contains the hash of a DNSKEY record
    - NSEC and NSEC3 – for explicit denial-of-existence of a DNS record
    - CDNSKEY and CDS – for a child zone requesting updates to DS record(s) in the parent zone

OpenDNS

- OpenDNS is a company that offers DNS resolution services and a suite of consumer solutions with the goal of making the Internet faster, safer, and more reliable
- It is also a cloud-delivered enterprise security service that protects against threats on the Internet; OpenDNS's consumer products include parental and content filtering, web performance, and web security
- They offer business the Umbrella (as in Cisco Umbrella) service, which is designed to protect against malware, botnets, phishing, and targeted online attacks

Sender Policy Framework (SPF)

- Practically all abusive email messages carry fake sender addresses today
- The victims whose addresses are being spoofed often suffer consequences such as:
    - Reputational damage
    - Need to repudiate the abuse
    - Time lost sorting out misdirected bounce messages
- Sender address forgery is a threat to both users and companies as it undermines the email medium and erodes people's confidence
    - This is why a bank never sends direct information about an account by email and keeps making a point of that fact

Sender Policy Framework

- The Sender Policy Framework is an open standard that introduces a method to prevent sender address forgery
- More precisely, the current version of SPF – called SPFv1 or SPF Classic – protects the envelope sender address, which is used for messages delivery
- SPFv1 permits domain owners to designate their mail sending policy (e.g. which amil servers they use to send mail from their domain)
- The SPF solution requires two sides to work together:
    - 1. The domain owner publishes this information in an SPF record in the domain's DNS zone, and when someone else's mail server receives a message claiming to come from that domain…
    - 2. The receiving server can check whether the message complies with the domain's stated policy
- For example, if the message comes from an unknown server, it will be marked as fake

DomainKeys Identified Mail (DKIM)

- DKIM is an email authentication method conducted between the outbound and inbound mail server or Message Transfer Agents (MTAs)
- The authentication process happens transparently to the end user
- With DKIM, the outbound mail server appends a digital signature to the email then the inbound server verifies the signature by looking up the public key and then comparing it with the signature from the specified outgoing mail server
- With DKIM, if the public key does not match the signature, it may be because:
    - The email was not sent from the mail server designated in the email header but was sent from another (spoofed) server instead
    - The email was modified in transit to the recipient
    - For instance, an attacker could intercept an email that was sent from a valid mail server, change it and then resend it

Domain-based Message Authentication Reporting and Conformance (DMARC)

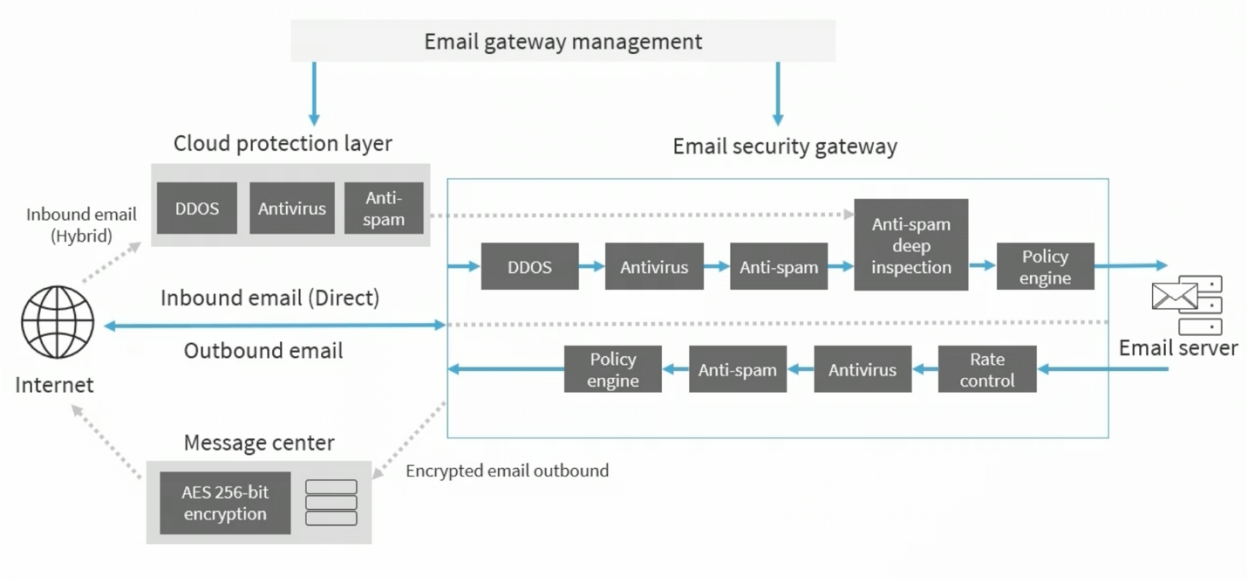
- Organizations and end users undergo a high volume of spam and phishing from the Internet
- Many modern solutions work in isolation from each other
- Each receiver makes exclusive decisions about how to evaluate the reporting results
- Legitimate domain owners rarely get any meaningful feedback
- DMARC attempts to address this by providing coordinated, tested methods for domain owners and email receivers

Domain-based Message Authentication Reporting and Conformance

- DMARC is an email authentication, policy, and reporting protocol
- It builds on the widely deployed SPF and SKIM protocols, offering:
    - Linkage to the sender (“From:”) domain name
    - Published policies for recipient handling of authentication failures
    - Reporting from receivers to senders, to enhance and monitor protection of the domain from fraudulent email

Email Security Gateways

- These special gateway appliances are dedicated email security services that work in or with MTAs to protect electronic mail
- They are also called secure email gateways (SEGs)
- This is a suite of tools that filter emails as they enter or leave the email server
- Emails are routed through the gateway service and typically require the DNS MX-records to be changed, regardless of email platform
- Many email providers today also offer a cloud-native email security solution called an Integrated Cloud Email Security (ICES), either in parallel or as a replacement for the legacy SEG



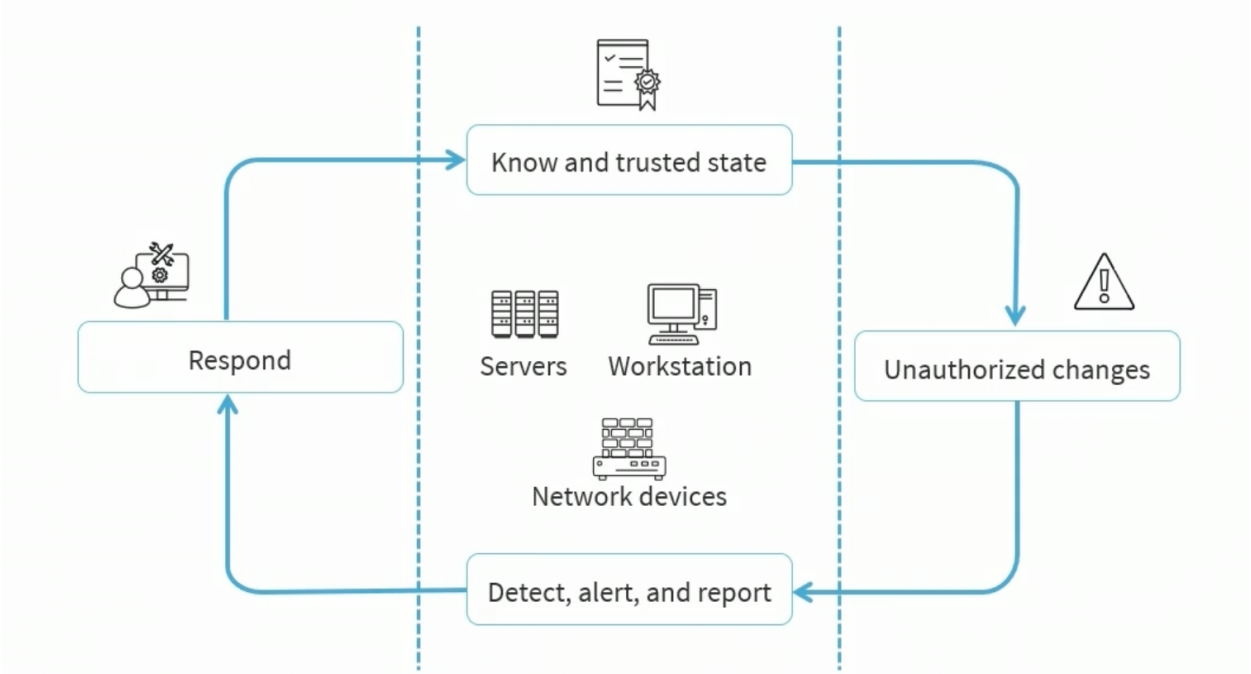
-
- Email security is accomplished by either using a cloud protection layer and/or a email security gateway. Email security gateway could be a physical highly available appliance in the datacenter or installed on a hypervisor. If we used a cloud protection layer, we will get our anti-ddos protection, virus and spam and we can optionally send that to the email security gateway or directly to the email server have we had this set up. In this diagram we have the initial cloud protection layer, and then the email that gets through that goes to the email security gateway locally for the anti-spam inspection and then our own policy engine. Then the traffic gets sent outbound through the email security gateway to do rate control, antivirus, antispam and another policy engine for outbound email. Often the policy engine for outbound is a data loss prevention engine or a cloud access security broker that can be sent back up to the cloud protection layer to go outbound. In this diagram all the outbound email is going through our own system, through our own email security gateway (potentially DLP policy engine) and then send encrypted email outbound using AES-256 or digitally signing it with SMIME

File Integrity Monitoring (FIM)

- File Integrity Monitoring examines operating system files, configuration files, registries, application software, and Linux system files for changes and indicators of compromise
- Windows FIM provides alerts about suspicious activity such as:

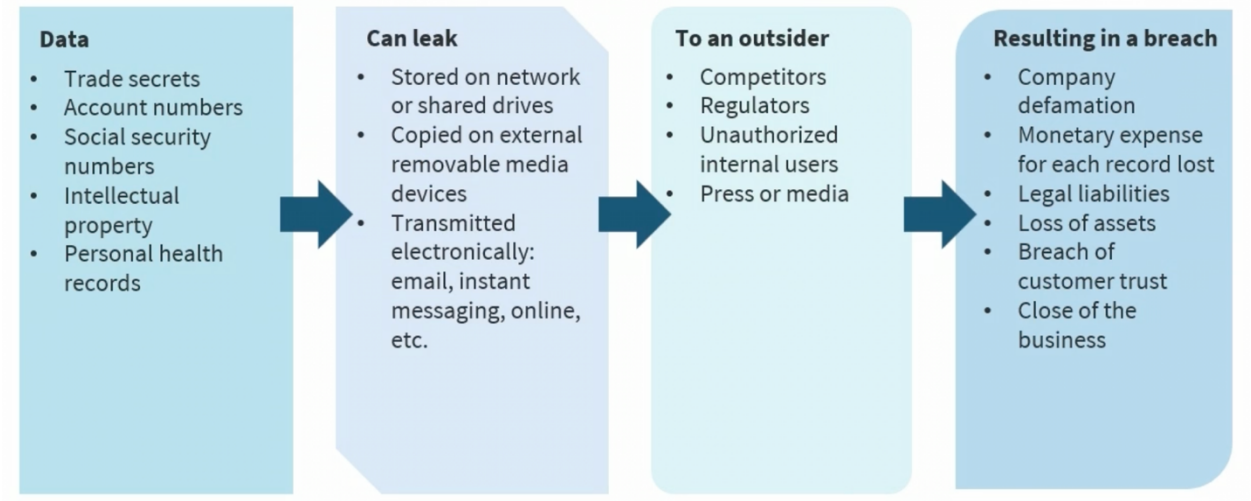
- File and registry key creation or removal
- File modifications (changes in file size, access control lists, and hash of the content)
- Registry modifications (changes in size, access control lists, type, and content)

FIM



-
- In the FIM lifecycle everything begins with the baseline. E.g. leveraging your change and configuration management principles/practices, you must have the known and trusted state, preferably its digitally signed for integrity and non-repudiation. Must have visibility systems, e.g. SIEM systems to notify you of changes or new existence of suspect files. In a zero trust environment that would involve robust and semi automated detection alert and reporting. Incident response to handle the situation, to handle the situation and get the servers, workstation, endpoint, network devices back to a known and trusted state. This is a iterative process and can be automated with robust inventory systems, SIEM and SOAR systems and highly skilled security practitioners especially on the incident response team.

Data Loss Prevention (DLP)



-
- Data loss prevention involves protecting the loss and leakage of all different types of data, intellectual property, account numbers, PII, PHI and other data that must be kept private or secret.

That data can leak using a wide variety of vectors e.g. removable drives, usb, memory cards. Can leak to a wide variety of unauthorized personal e.g. competitors, regulators, unauthorized internal users. This results in primary(immediate) and secondary(subsequent) loss. Secondary could be longer and more expensive. Examples of this could be company defamation and closure of the business.

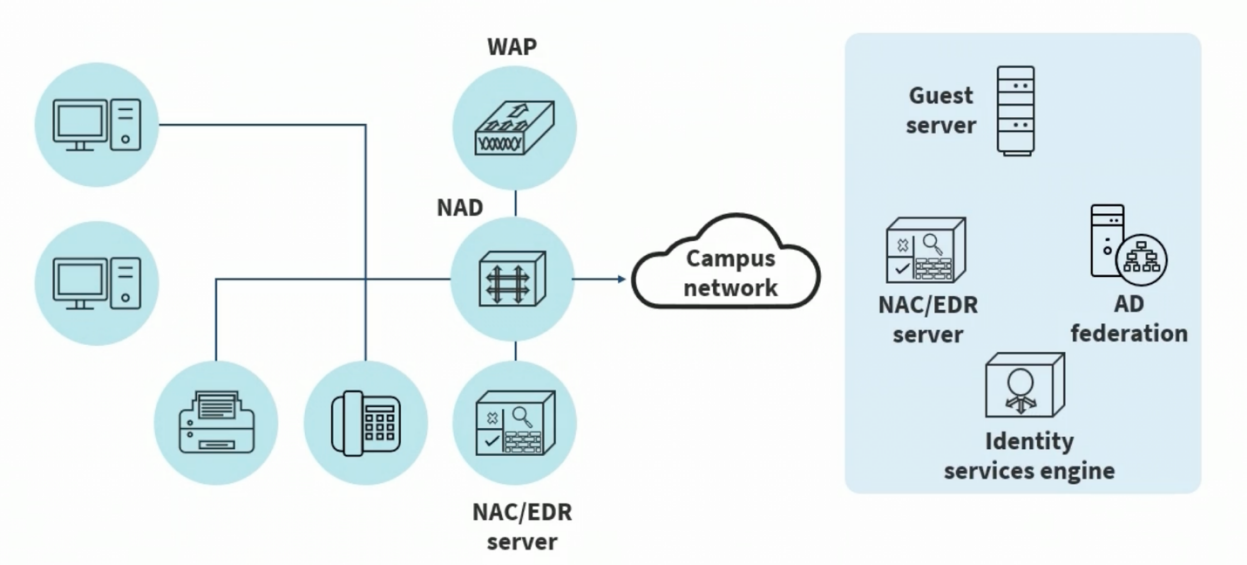
Data Loss Prevention Solutions

- There are a variety of hardware/software solutions that can mitigate data leakage and data loss:
    - Secure email gateways
    - Cloud-based email security
    - Cloud access security brokers (CASB)
    - Endpoint detection and response (EDR)
    - Database activity monitoring (DAM)

Network Access (Admission) Control (NAC)

- Network admission control (NAC) was an industry initiative sponsored by Cisco
- It typically enables 802.1X port-based network access control (PNAC) on Layer 2 and Layer 3 networks
- Does not trust anything inside or outside the perimeter without stringent authentication and verification
- Helps secure access from users and their devices, application programming interface (API) calls, Internet of Things (IoT), microservices, containers (Dockers, Kubernetes), and more

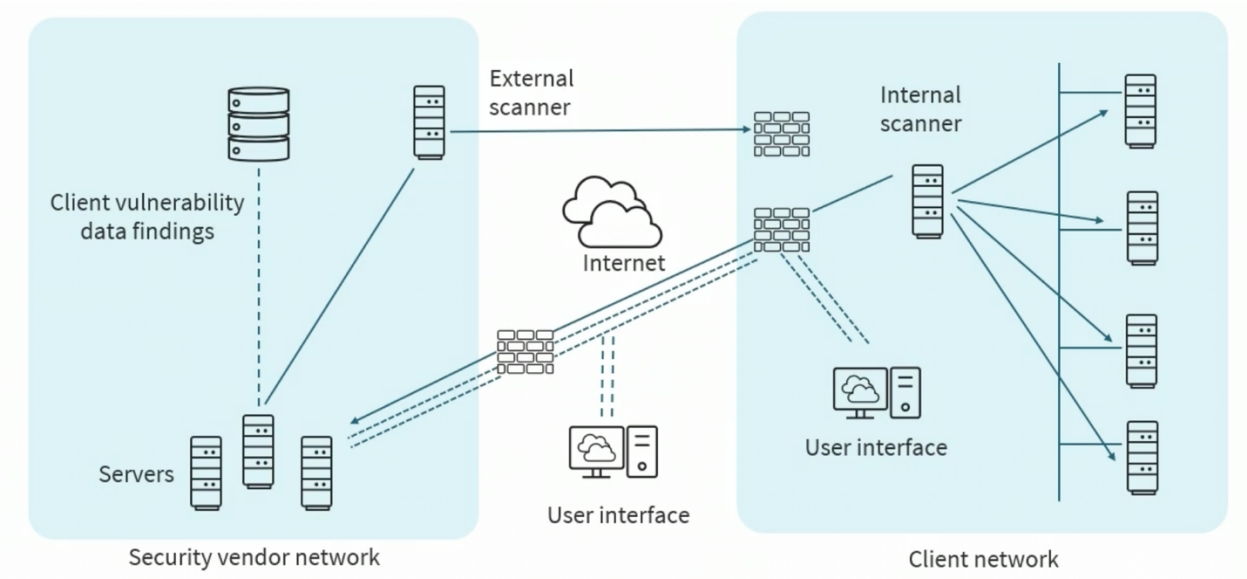
Network Admission Control



- In this diagram we see traditional network access control. Left hand side we have a wide variety of devices, these icons are outdated but we know we have laptops, pads, void devices, mobile phones etc. To get access to resources on the network they will go through a NAD (network access device) e.g. switch, multi-layer switch or a wireless access point. On the backend we have a wide variety of services, if it's a wireless access point there will be a wireless controller on the backend. We have a choice to run a NAC/EDR server directly off the NAD or they could be in a back end server or datacenter. NAC is our windows server, enterprise redhad linux server, EDR is our endpoint detection and response solution (traps, SIEM and SOAR using SPLUNK). On the backend we have a identity services engine which supports our attribute based access control and supported by an identity provider (e.g. active directory environment). Using NAD when a device

attempts to connect to the network, the NAD can either request credentials or they are provided when the device attempts to get on the network, they can then pass the credentials back to the back end and based on the credentials a NAC environment can do a variety of things e.g. refuse, restrict it in a VLAN to be remediated to then go out to the network, restrict ports, monitor, printer can only connect. Placing in restricted vlans is only one type of activity you can do in a attribute based access control environment. In cisco environments you can inject data in the outgoing frames as they go from device to device, put special rules in the NAD device to control IP connectivity. This is a popular solution (google) in zero trust environments

Cloud-based NAC/EDR



-
- Today NAC/EDR is cloud based normally (e.g. CISCO, Palo Alto XDR), where the external users are being authenticated and authorized against a controller in a software defined perimeter environment and then getting access to the internal network OR people attempting to get onto corporate network using wired or wireless are having information sent up to a cloud based solution.

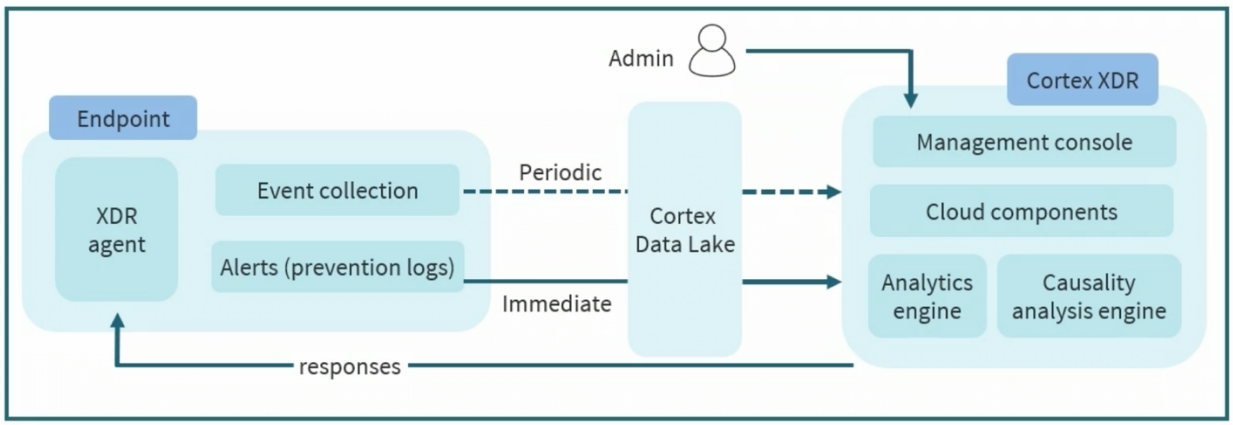
Endpoint Detection and Response Solutions

- EDR has evolved from early HIDS solutions and involves a “lighter” software agent (i.e. Palo Alto Traps) installed on the host system; this often provides the basis for event monitoring and reporting
- EDR tools focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints
- EDR monitors endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place
- Moder solutions are Extended Detection and Response (XDR) and user behavior analytics (UBA)

Extended Detection and Response

- Threat protection driving by machine learning
- Incident management
- Automated root cause analysis
- Deep forensics (e.g. e-discovery)
- Flexible response (e.g. risk based models, cloud based solution)
- Extended threat hunting (e.g. pen testers

Example: Palo Alto Cortex XDR



-
- Modern solution palo alto cortex xdr. The endpoint will run the lightweight xdr agent that is responsible for collecting events, alerts. Can be periodic through the cortex data lake or immediate through the cortex data lake. The security admin in the security operations center is running the cortex xdr console that is integrated with cloud components and palo alto networks. Includes two main engines; analytics and causality analysis engine driven by machine learning and user behavioral analytics.

Identity and Access Management

Provisioning and Deprovisioning User Accounts

- Likely going to have on-site directory service (Active directory), when you get hired you will go through an automated process of being populated as a user into a directory which will contain information about you, and will be placed into a group that will give you the permissions you have throughout the organization to resources, this is called provisioning or onboarding. Can also provision and onboard devices, so when you get hired and put into a directory you will also be provisioned laptops, pads.
- User groups (auditors, managers, production), create a user (give it a name). Scema – if using a directory service in a organization you will have a established schema, like the first initial of first name and then last name (greenthom, tgreen) and whatever schema your using it has to be unified and consistent. If your provisioning users somewhere else the best case is to use the same naming scheme. When you provision a user you want to consider separation of duties and within separation of duties, least privilege. For example, separate duties here "is this user going to use a management console or do I want this user to have programmatic access and do it that way…", shouldn't give users both programmatic access and make them console users. Can have both but its rare, has to be high level or a leader. Only want them accessing the services they have access too.
- Once you create a user you don't assign permissions or policies to that user. You put the user into a group or nested groups that give them the rights and permissions they need (e.g. auditors, managers, production) and put the user in the group. In the cloud this might be different to your own directory service. In the cloud what the groups can do are based on the policies that they have. Permissions are basically JSON documents. Cloud is normally JSON. Going to make APIs and programmatic calls and requests. When you apply some type of policy or permissions, what is the allow list, what API calls are they allowed to make. By default these policies don't have conditions in them. You have an action and effect and what resource they can access. Could put conditions in there, e.g. permissions to say they only function in a organizational unit, only allowed to run API calls at a certain time of the day.
- Provisioning is adding users generally to groups, giving them the rights and permissions to access resources, but in a wider scale provisioning also includes giving them the endpoints, hardware and devices that they can use
- Deprovisioning, delete users or delete users in groups. Identity proofing, when your hiring a new user, you go through background checks instead of them just providing their passport. Proofing goes deeper into looking into their background and that they are who they say they are so doing things like proofing is critical today than the modern enterprise. E.g. if you were to open a brokerage account, you would provide additional credentials to open up the account, however, if you want to do a elevated or escalated process, e.g. make a large withdrawal, it is likely your going to go through step up authentication or step up proofing.
- Identity proofing is a higher level of authentication and authorization.

Exploring Password Concepts

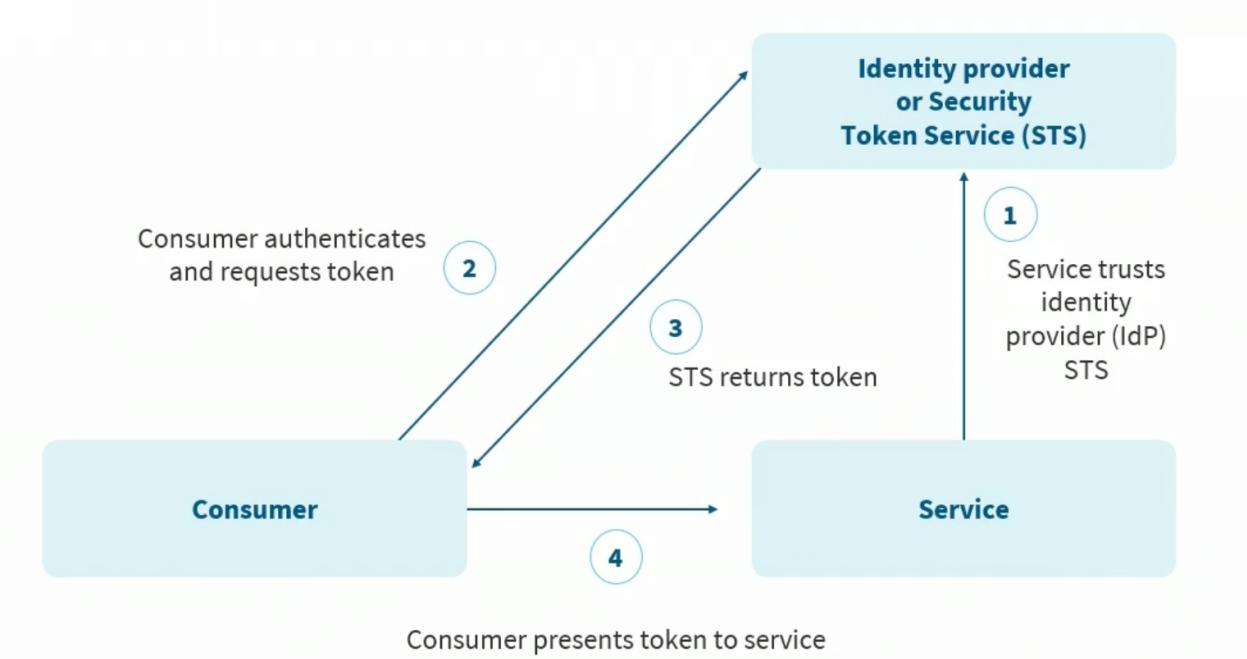
- Account settings is where password policy is. Could use active directory, LDAP… some other identity provider. Generally speaking you have different password policies. Today you want to be 10+ characters, anything less is not stringent enough. Other include uppercase, lowercase, number and non-alphanumeric character. A strict password policy would involve all 4 of those and 10+ length. Other requirements include password lifetime (e.g. 30+ days) the shorter the more secure. Password expiration requires admin reset, if the password expires and the user hasn't changed their own password, then the admin will reset it. Allowing users to change their own

password. Prevent password reuse, e.g. 12 -> using 12 unique passwords over course of 30 days, cant use same password, cant use password til next year if 30 day expiration. Passwordless solutions e.g. tokens, smartcards, qr codes, are better but passwords are widely used and a password policy is needed.

Federation and Single Sign-on (SSO)

- Federated identity management, also known as federated single sign-on, refers to the formation of a trusted relationship between separate entities and third parties, such as cloud/application vendors or partners, enabling them to share identities and authenticate users across domains and realms
- When two domains are federated, a principal can authenticate to one domain and then access resources in the other domain without needing to perform an additional login procedure
- SSO allows a user to access multiple applications using a single set of credentials
- This feature can be applied to employees often sign on to multiple business applications including messaging, email, productivity apps, various accounts, HR functions, intranet sites, financial records, etc.

Federated Access



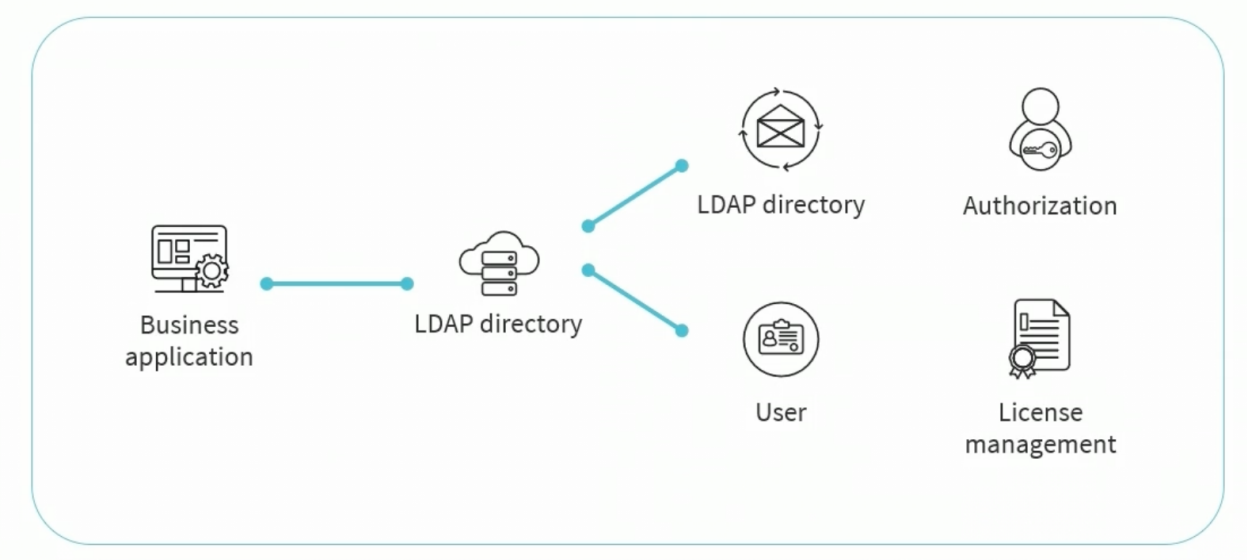
-
- Here we see the three parties of federated access. What the consumer is doing is SSO but the real federated access part is the relationship of trust and tokens between the identity provider or some token service running at a cloud provider or a vendor and various services. Services like Microsoft 365, yammer, etc. Realize when it comes to the identity provider it could be a on-premise identity provider like active directory, OpenLDAP or the identity provider or token service could be running in the cloud like AzureAD. Complex aspect is step 1 where the identity provider or trust service, creates a trust relationship with one or more services or service providers. The identity provider has a lot of information about the consumer but it only exposes certain information that is necessary and needed to authenticate that user to the service or service provider. If the consumer wants to access something like Microsoft 365, etc. it will authenticate with the identity provider either on-premise or cloud and will request a token. The providers token or assertion service will return the token or assertion to the consumer who then presents it to the service. At that point

there is a time based session where the consumer is only authorized to do what is in the token against the service or on the service.

Lightweight Directory Access Protocol (LDAP)

- LDAP was based on the X.500 directory but is a lighter, cross-platform, and standards-based solution
- LDAP servers are easy to install, maintain, and optimize, but they are without solid security of the queries, updates, and valuable information in the LDAP directory
- LDAPS (TCP 636) is LDAP over Transport Layer Security (TLS)
- Simple Authentication and Security Layer (SASL) BIND also offers authentication services using mechanisms like Kerberos, or a client certificate sent with TLS

LDAP

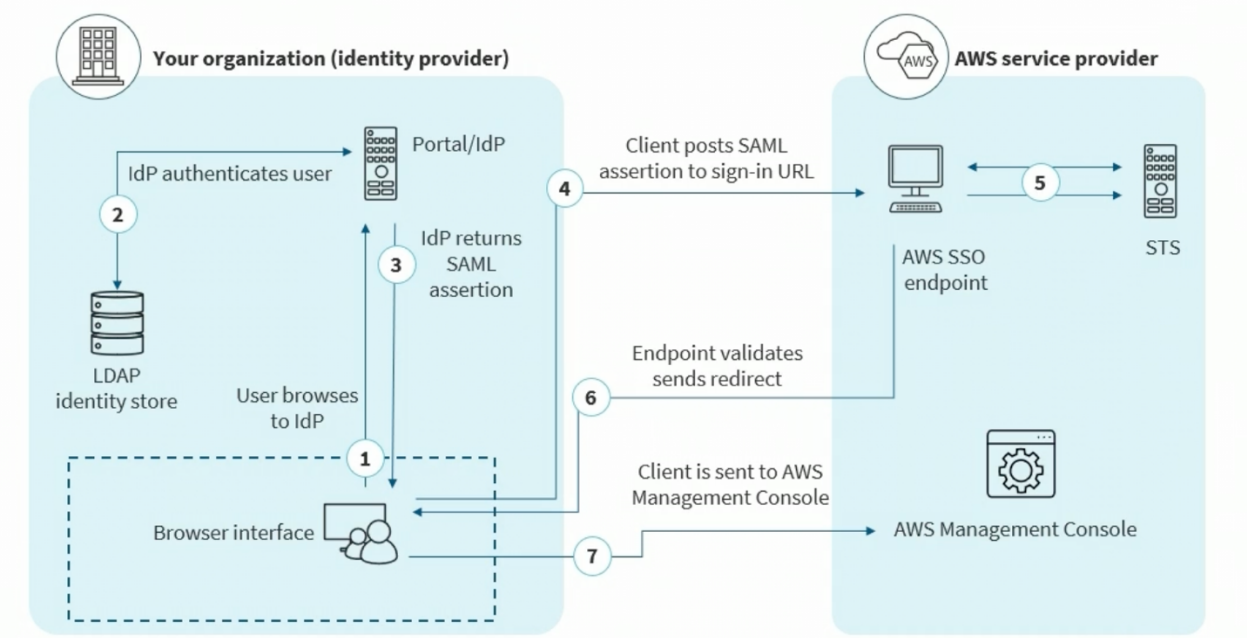


-
- The business application supports the LDAP service and directory and various users can be authenticated and authorized against the LDAP directory to get session based access to the application

Security Assertions Markup Language (SAML)

- SAML is an XML-based open-source SSO standard
- SAML is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet
- A key advantage of SAML is open-source interoperability
- Some large companies now require SAML for Internet SSO with Software as a Service (SaaS) applications and other external Internet Service Providers (ISPs)
- It is a common federated solution with cloud service providers

SAML 2.0 at Amazon Web Services (AWS)



-
- Defacto standard at AWS. In this example, your Organization has its own identity provider, its an LDAP identity store running on redhat enterprise. The browser has an interface often with a custom portal that is generated by a service provider like AWS. The users browsers requesting authentication from the identity provider or the LDAP store and this store returns a SAML assertion. The LDAP identity store and AWS have created a trust relationship by going through several steps and exchanging trust tokens. So this has already happened under the hood, once the user with the browser interface gets the SAML assertion, it will post the SAML assertion to a sign in URL which will be at amazon web services to an AWS SSO endpoint. AWS on the backend is running a STS or a security token service, this will be called a SAS (assertion service). Step 6 The SSO endpoint then validates, sends redirects, sends it back to the browser interface, the browser can now access the service using the AWS management console. Service at AWS could be different managed services at AWS or marketplace partners that present SaaS offerings.

OAUTH/OIDC

- They are not mutually exclusive, an organization or a enterprise can use both for different use cases
- OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access
- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server
- OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol
- It verifies the end-user identity using an authorization server
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients
- OpenID is extensible, as functionality can be added
- Proper implementation of OAUTH is to use OIDC or openid connect as the basic authentication and identity layer running on top of OAUTH.

Mandatory Access Control (MAC)

- "MAC is an access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system
- A subject that has been granted access to information is constrained from doing any of the following:
    - Passing the information to unauthorized subjects or objects
    - Granting its privileges to other subjects
    - Changing one or more security attributes on subjects, objects, the information system, or system components
    - Choosing the security attributes to be associated with newly-created or modified objects
    - Changing the rules governing access control

MAC

- A mandatory access control model uses a strict set of established sensitivity/classification levels and access controls for integrity and confidentiality based on classifications
- These are mathematical models used in high-security environments, like military, government agencies, and enterprises involved with sensitive data and activities
- Typically, state machine and information flow models are designed by a security team or steering committee as opposed to an administrator or asset owner

Discretionary Access Control (DAC)

- The DAC policy enforced over all entities so that a subject being granted access can:
    - Pass the information to other subjects or objects
    - Grant its privileges to other subjects
    - Change security attributes on subjects, objects, information systems, or system components
    - Choose the security attributes to be associated with newly-created or revised objects
    - Change the rules governing access control

Discretionary Access Control

- DAC models involve control and management by the owner/creator of the object
- DAC leaves a certain amount of access control to the discretion of the objects owner – or anyone else who is authorized to control the object's access
- The opposite of a MAC model in that the owner can determine who should have access rights to an object and what those rights should be

Role-based Access Control (RBAC) Models

- NIST: "Access control based on user roles (i.e. a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role)
- Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization
    - A given role may apply to a single individual or to several individuals

Rule-based Access Controls

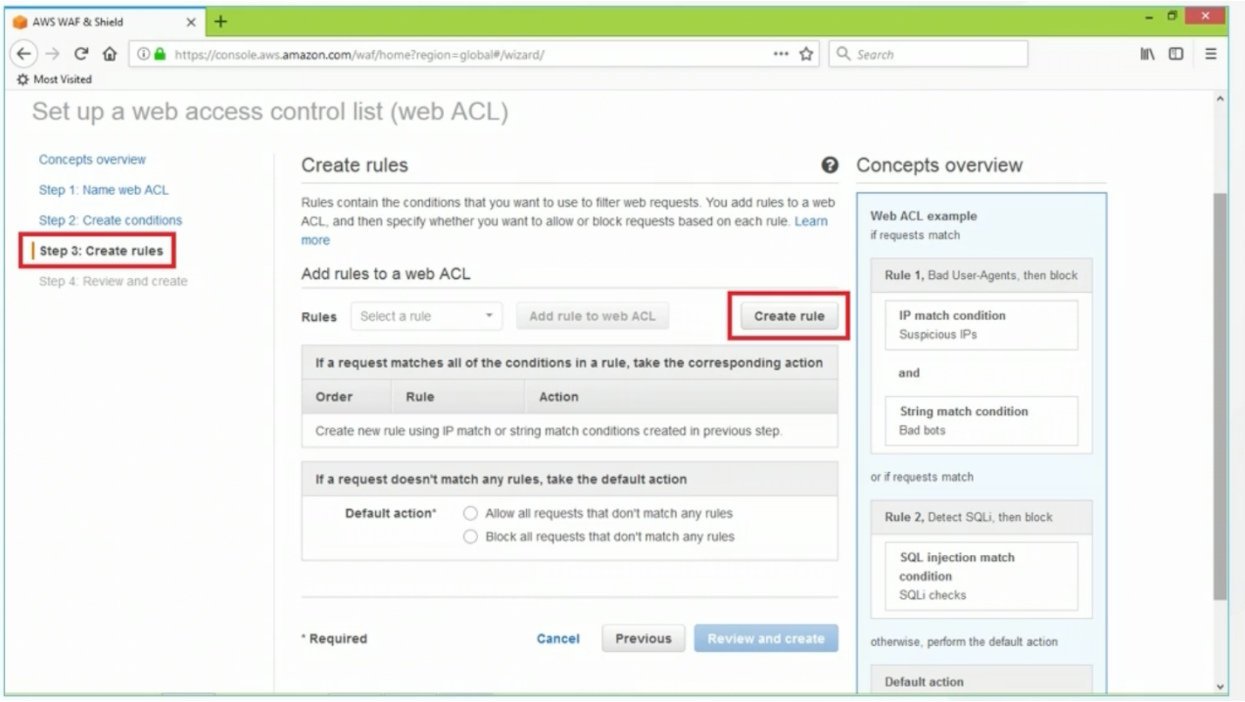
- With Rule-based (or Rules-based) Access Control, access is permitted or denied to resource objects based on a set of rules defined by a system or network administrator
- As with DAC, access properties are stored in access control lists (ACLs) associated with each resource object

- When a certain group or user account attempts to access a resource, the operating system checks the rules contained in the ACL for that object
- Examples of Rules-based Access Controls are time-based ACLs, router infrastructure ACLs, static (stateless) firewalls, and AWS network ACLs

Sample Inbound Access Rule

Protocol	Port	Source	Destination	Name	Action
UDP	53	Any	192.16.10.200	Allow DNS queries	Allow
TCP	80,443	Any	192.168.10.201	Allow HTTP and HTTPS	Allow
TCP	3,389	IT_Admin_IP_Range	Any	Allow RDP	Allow
Any	Any	Any	Any	Default	Deny

-
- Implicit Deny all at the end of the ACL



-
- Web ACL (web application firewall or web security gateways) ACL rules for HTTP and HTTPS traffic either in a virtual server in your own datacenter hypervisor environment or in this example AWS server. This list of rules can block not just on addresses but on geographic location, deep packet inspection of the HTTP req and res headers (looking for attacks like SQL injection, request forgery, xss, buffer overflow, etc.).

Multi-factor Authentication (MFA)

- Multi-factor authentication typically involves adding an additional authentication mechanism to the initial origin authentication or credential presentation
    - Something you know

    - Something you have
    - Something you are
    - Somewhere you are

Something You Know
- Password
- Personal identification number (PIN)
- Passphrase
- Secret word or phrase

Something You Have
- Hard/soft authentication tokens (YubiKey/Authy)
- Badge or smart card
- X509v3 certificates
- Security keys

Something You Are
- Fingerprint
- Ocular biometrics
- Facial recognition
- Speech patterns

Somewhere You Are
- Remote client-based and clientless virtual private network (VPN)
- Remote Software Defined Perimeter
- 802.1x wired or wireless network
- Cloud IdM management network

Fingerprint Biometrics
- This is one of the oldest and most common biometrics since they vary from person to person and do not change over time
- Integrated into mobile devices and laptop computers using hardware and/or software
- A fingerprint scanner system has two functions
- Gets an image of the finger
- Determines whether the outline of ridges and valleys in the image matches the patterns in pre-scanned images

Facial Recognition
- One of the fastest growing mechanisms pre-pandemic
- Commonly used to identify or verify an individual in still or video images
- The main applications of face recognition are in areas of security biometrics and human-to-computer interaction (including robotics)
- The primary method for modeling facial images is Principal Component Analysis (PCA)
    - This is simpler, has a high learning capability, and possesses vigorous sensitivity to small changes in the face image

Iris Scan Biometrics
- The iris is the thin, circular structure “color” part of the eye and controls the diameter and size of the pupils and therefore the amount of light reaching the retina

- Muscles attached to the iris expand or contract the pupil so the larger the pupil, the more light that can enter
- Iris scanners use camera technology to get images of the intricate and detailed structures of the iris using delicate infrared illumination

Retina Scan Biometrics
- The retina is a thin tissue composed of neural cells located in the back portion of the eye
- Due to the complex make-up of the capillaries, every person's retina is distinctive
- Scanner sends a beam of low-energy infrared light into an eye when user looks through the scanner's eyepiece
- A beam of light traces a standardized path on the retina and the pattern of variations are converted to code and stored in a database
- Retinal scanning is categorized as invasive (more than iris scanning) since the eye must be very close to the eyepiece, for a long/er period of time

Voice Recognition
- There is a difference between speaker recognition and speech recognition
- "Voice recognition" can be used for both terms
- Speaker recognition leverages the aural aspects of speech that diverge among people
- Traits include human physical structure learned social communication patterns
- Voice recognition is classified as a "behavioral biometric" which is non- invasive

IMPORTANT TO REMEMBER (FOR THE EXAM) WHICH ARE INVASIVE AND NON-INVASIVE (behavioral is better = non-invasive)

Mobile Biometrics
- Fingerprint scanning
- Facial recognition
- Ocular, voice, and swipe patterns

Biometric Measurements
- False acceptance rate (FAR) measures the probability that the biometric system will incorrectly accept an access effort by an unauthorized user
    - A system's FAR is often specified as the ratio of the number of false acceptances divided by the amount of authentication attempts
- The False rejection rate (FRR) is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template
- The Crossover error rate (CER) is the value of FAR and FRR when the sensitivity is setup so that FAR and FRR are the same
    - This is an excellent metric for quantitative comparison of differing biometrics

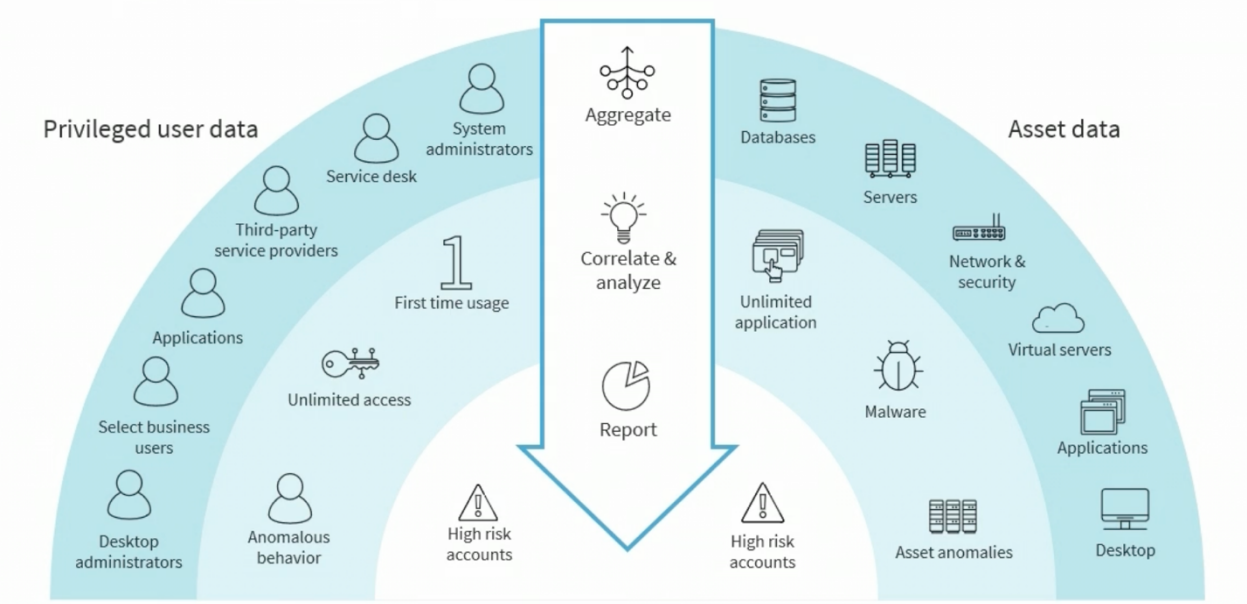
Privileged Access Management
- Privileged access management (PAM) is an identity security initiative that helps organizations counter cyberthreats by monitoring, detecting, and stopping unauthorized access to critical resources
- PAM works as a collaboration of people, processes, and technology to provide visibility into subjects using privileged accounts and what they are doing
- System security is enhanced by limiting the number of subjects that have access to administrative functions

- Additional layers of protection mitigate data breaches by threat actors

PAM Components

- Just-in-time permissions: A practice where the privilege granted to applications or systems is limited to predetermined periods of time, on an as-needed basis. Can be achieved through ACLs and attribute-based access control. Minimizes the risk of standing privileges (persistent 24/7 privileges or rights) that attackers can easily exploit
- Password vaulting: A program that securely stores credentials for multiple applications in an encrypted format. Users can access the vault via a single “master” password and the vault then presents it for the account they need to access
- Ephemeral credentials: Dynamically generated credentials that are created when needed, then discarded afterward. Like persistent credentials, these credentials offer the subject a temporary token needed to gain access

Privileged Access Management



-
- Three main goals of PAM are to aggregate based on different users and different systems and services, to correlate and analyze and then deliver reports. You’ve got privileged user data (e.g. Microsoft SharePoint, or in file servers in datacenter or AZURE cloud and asset data). One of the main goals is least privilege for system admins and high level service desk employees, business users, and to separate those with least privilege principles from other types of users. Can get visibility into anomalous behavior, users that have unlimited access, users who are doing it for the first time which could be an attack, malware, and anomalies in various assets isolating high risk accounts and getting visibility into high risk accounts and generating meaningful reports

Automation, Orchestration and Incident Response

Automation vs Orchestration

- IT automation involves generating a single task to run automatically without any human intervention
- Automation could involve sending alerts to a security information and event management (SIEM) system, dynamically triggering a serverless function at a cloud provider, or adding a record to a database when a batch job is run
- Enterprises often automate both cloud-based and on-premises tasks
- Orchestration involves managing several or many automated tasks or processes
- As opposed to focusing on one task, orchestration combines all the individual tasks
- Orchestration occurs with various technologies, applications, containers, datasets, middleware, systems, and more

Automation and Scripting Use Cases

- User and resource provisioning – Most modern enterprises have tightly integrated Joiner and Mover onboarding and provisioning processes that involve integration and automation between Human Resources, Legal, Directory Services, Identity Management (IdM), and inventory engines. Inventory are both physical and virtual assets
- Guard Rails – Cloud providers use JSON policies and Infrastructure as Code (IaC) to enforce least privilege policies and separation of duties to remove certain API calls from privileged groups and users
- Security group firewalls are layer 3/5 stateful packet filters applied to either subnets or virtual instances in hypervisors or cloud
- Ticket creation and escalation as part of a Service Desk deployment will run scripts and automated workflow
    - Software-defined networks (SD-LAN, SD-WAN, SD-MAN)
- In modern LANs and datacenters, enabling/disabling services and access controls is a common functions of scripting, automation, and IaC (JSON, YAML)
- As part of the DevOps life cycle (Agile, CI/CD) automation is leveraged for continuous integration and testing
- Any application programming interface (API) call or request can be automated (Python, Postman, etc.) to:
    - Run tests to help quality assurance (QA) continuously check a product's quality
    - Generate light orchestrations that involve several API calls to perform a particular task on a microservice backend
    - Use preformed snippets to run Functions as a Service in the cloud

Benefits of Automation

- Efficiency and productivity
    - Automated processes can finish tasks and processes faster and more effectively in a manual process. Automation increases productivity levels and when your working with a manual workforce, the production rate will increase with it.
- Time savings
    - By automating manual tasks, businesses can remove or greatly reduce a requirement or repetitive in time consuming tasks. Security tasks example; dealing administratively with layer 2 switches and routers and other infrastructure devices that have a lot of manual tasks and configuration. Will allow security force focus on critical and strategic actions in the security centre

- Enforcing baselines
    - Often standardized security images and we can get these from CIS(center for internet security) or vendors that are government and military contractors.
- Standard infrastructure configurations
    - System admins use combination of scripts and manual processes to set up infrastructure environments, e.g. wireless local area networks while automation supports infrastructure as code. This can be utilized for new physical and virtual network and datacenter environments or creating those baselines. Widely used for software development to build, test and deploy applications
- Secure scalability
    - Creating secure scalable network automation (e.g. JSON, YAML) enhances security, calibration, version control, documentation, error handling, testing, compliance, visibility, collaboration and contributes overall to ongoing maintence or due care providing more resilient environment as you scale up to more robust processes and more RAM, higher end platforms, or scale out
- Employee retention
    - Automation can free up employees from every day processes, providing them with more time and energy with more creative and meaningful tasks and projects. Also helps prevent critical errors that might jeopardize a job performance review. Also helps increase productivity, employee morale and job satisfaction
- Reaction time
    - Increase safety, operation performance, incident response security with fine tuned playbooks and runbooks.
- Force multiplier
    - A military term but for our organizations they will be tools that help amplify efforts to produce more output. E.g. when your roofing your home and using a nail gun instead of a hammer. Investing in force multiplier means you will accomplish more with the same or less effort. Automation will enhance patch management, backup and restore policies, compliance scanning, and software development lifecycles

Automation Considerations

- Developers can reduce the complexity of automation by using established toolsets and integrated solutions
- Automation and scripting can reduce costs for provisioning/onboarding users and devices reducing human interaction and potential configuration errors and troubleshooting
- In this context, a single point of failure (SPOF) is a flaw in the design, configuration, or implementation of the automation solution
    - If the automation solution is not redundant and reliable, one loses the overall benefits
- Automation systems can also be a technical debt if implemented in a rush and/or without proper testing
- Ongoing supportability of automation and orchestration is another key factor

Incident Response Process

- Ideally pre-determined actions!
- The classification of the negative event will determine action
    - Is it an event or an incident?
    - What is the immediate impact on operations?
    - What is the scope of impact?
    - How prioritized or critical is the target?

    - Can root cause analysis be performed quickly and easily?
    - Does the incident trigger disaster recovery escalation?

Goals of Incident Response

- Reduce the immediate impact
- Prevent the spread
- Protect and maintain ongoing operations
- Support forensics, e-discovery, and continuity of operations
- Provide after-action reports and lessons learned

Incident Response Life Cycle

- Preparation (1)
- Detection (2)
- Analysis and escalation (3)
- Containment (4)
- Eradication and recovery (5)
- Lessons learned (6)

Detection

- Also referred to as "identification"
- First responders or SIEM/security orchestration, automation, and response (SOAR) system must separate an event from an incident (or breach) immediately, using pre-defined metrics and experience
- Responders will implement techniques for categorizing and prioritizing the incident based on an established risk register or runbook

How Were You Alerted?

- Logs, alerts, and feeds
- Phone calls
- Text messages
- Logical and physical alarms
- Interactive monitoring in security operations center (SOC)

Analysis and Escalation

- The analysis of incidents is a combination of an art and a science
- There are important questions to answer:
    - What is the scope of the incident?
    - Does it qualify for escalation or disaster recovery?
    - Are there obvious artifacts and indicators of compromise?
    - Can you discover the actions in the kill chain?
    - Can you quickly identify the root cause?

Escalation (Elevation)

- Not a mature organization if does not have a service desk!
- A pre-established workflow for escalating the incident to a higher service desk tier must be established
- Does the incident need to be passed from a first responders to an incident response team (IRT)?
- Many organizations have a SOC and a service desk along with an emergency Change Advisory Board (CAB)

Containment

- Implement short-term processes, such as disconnecting devices from the network
- Malware can be quarantined by antivirus programs and security suites
- Leverage quarantine compartments, sandbox locations, detonation chambers, private clouds, and threat modeling environments
- Managed security service providers (MSSPs) can help maintain separation, containment, and segregation

Eradication

- Potentially unwanted programs (PUPs) can be eradicated by advanced antivirus and antimalware suites
- Some artifacts may need to be moved to detonation chambers for further analysis and machine learning
- All findings should be reported to cloud partners and added to vulnerability repositories and shared reputation databases
- Advanced wiping tools may be needed to completely remove all malware footprints and artifact remnants

Incident Response Recovery and Lessons Learned

- Full recovery is getting back to a point where the "incident never happened" but sometimes a company needs to function in a perpetual state of recovery
- Recovery involves getting back to an acceptable state to continue to deliver the value proposition
- Complete remediation may not be possible even for an extended period
- After-action reports will be generated after exercises and actual incidents
- There should be a lessons learned database
- The success of redress and recovery depends on the level of testing and exercises performed

Incident Response (IR) Training

- A prime example of IR training is the Cybersecurity Infrastructure Security Agency (CISA)
- This important entity helps organizations across the nation protect their IT enterprises and enable their cybersecurity talent
- CISA offers Incident Response training course free to government employees and contractors across federal, state, local, tribal, and territorial government, educational and critical infrastructure partners and the general public.

Testing Incident Response

- Plan Review (read-through)
    - Group discussion, plan auditing, and Delphi and brainstorming sessions with stakeholders
- Tabletop
    - Examine documented plans, diagrams, and logical and virtual walkthroughs to eliminate gaps/errors
- Walkthrough (exercise)
    - Planned rehearsals and drills
    - Performed in stages and by department/building only
    - Should find additional gaps to those found during plan review and tabletop exercises

Testing Incident Response

- This is the highest level test most organizations conduct because it will have an impact on delivering the value proposition and impact on the productivity of employees, effect customers, vendors, and partners to some degree
- Simulation
    - Focuses on specific scenarios and areas
    - Uses real business continuity plan (BCP) and disaster recovery plan (DRP) resources (recovery sites) and teams (swarm simulations)
    - Tests snapshot recovery and hot spares
    - May be the highest-level test that most organizations conduct
- Parallel
    - Real-world drill while still operating business
    - More resource-intensive than simulations
- Full interruption
    - Most elaborate
    - Cease conducting activities, organization goes dark and will go to the cold, warm or cloud site fully interrupting the delivery of the value proposition
    - Only a very well funded company could do this or an organization that has a lot of tax dollars. Other extreme to the checklist/readthrough plan that you do/get to begin with
    - Real-world drill while ceasing business activities
    - Cost-prohibitive for most organizations

Root Cause Analysis

- Root cause analysis (RCA) is a function of the Problem Management IT service practice
- A root cause is defined as a factor that introduced a non-conformance in an application, service, or system
- It is the core causative issue – the highest-level trigger – that sets in motion the entire cause-and-effect reaction that ultimately leads to the problem(s)
- RCA is defined as a collective term that describes a wide range of approaches, tools, and techniques used to uncover causes of problems

Root Cause Analysis Steps

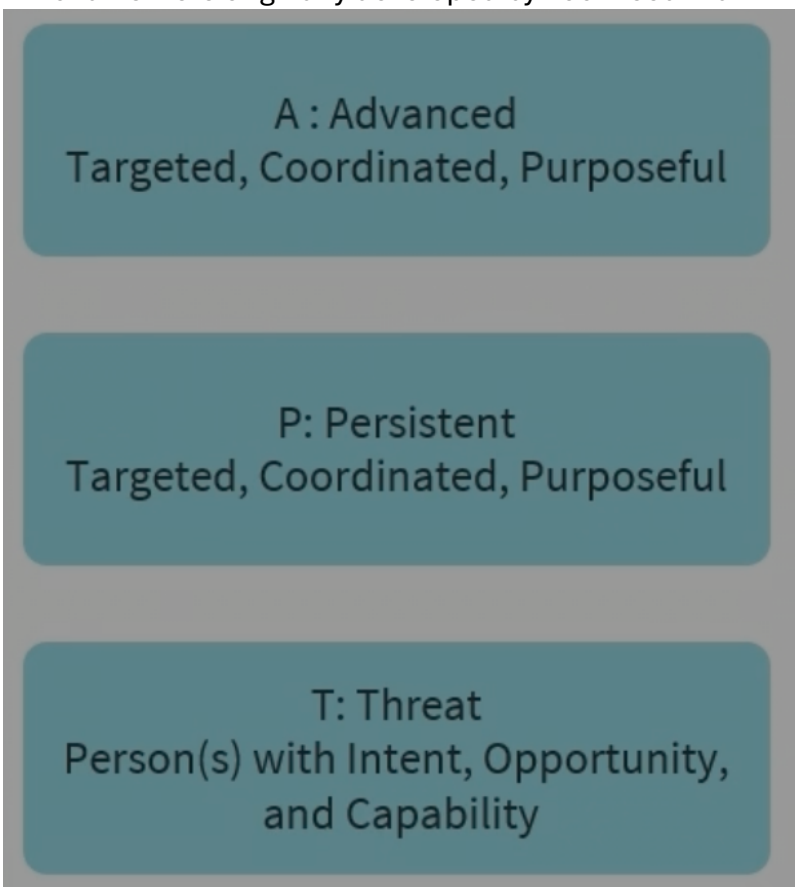
1. Define the problem: Normally obvious, e.g. notified through an alert, function, API call, phone call, on dashboard. Hopefully already categorized likely problems/issues, if not step 2 will take longer. More meaningful data and indicators collected in step 3 the easier it is to identify the cause. Root cause analysis is a combination of art and a science. So often based on the experience of the first responder or incident team they will quickly identify if not it will involve longer e-discovery.
2. Collect data
3. Identify possible causal factors
4. Identify the root cause(s)
5. Recommend and implement solutions: to reduce the likelihood of the problem occurring again

Threat Hunting

- Also called “Hunt Teams”
- Threat hunting involves groups of cyber investigators aggressively seeking out threats on a network or system
- They are often compliance or regulatory auditors
- They attempt to quickly recognize anomalies and discover historic patterns in data and Indicators of Compromise (IoC) to counter cybercriminals and mitigate threats
- Can also be Red Team vs. Blue Team exercises

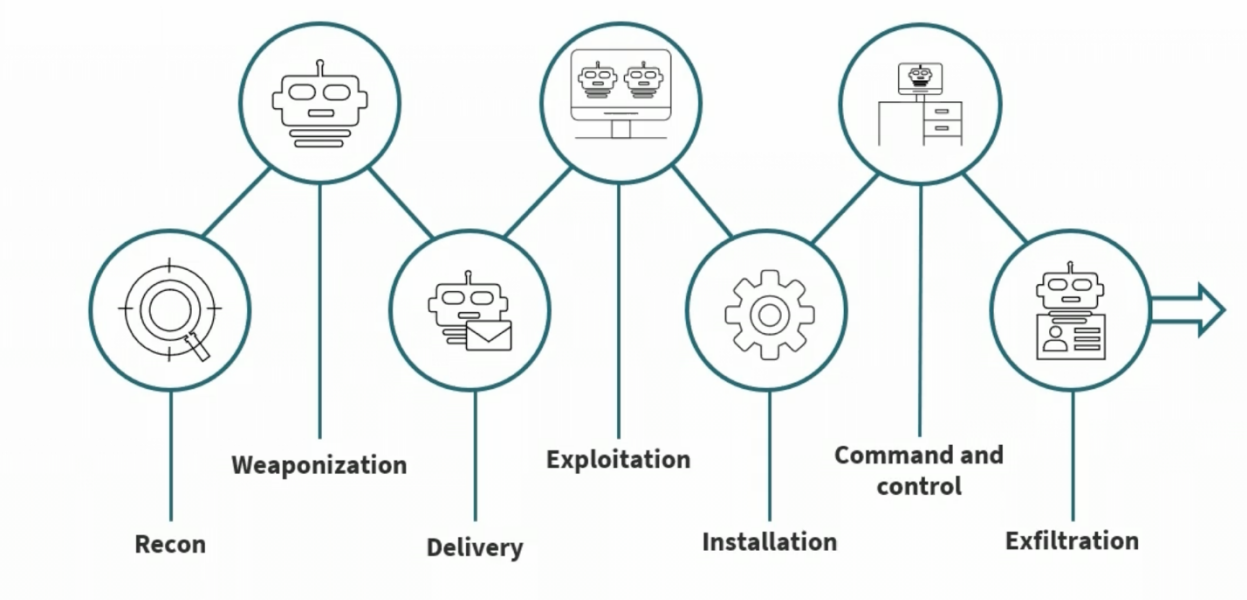
- Experts will have a solid understanding of the cyber kill chain

Cyber Kill Chain

- A kill chain is the succession of steps and phases used during a structured external or internal cyberattack
- It is used by penetration testers and threat hunting teams to better understand advanced persistent threats from exploits and malware attacks
- Kill chains were originally developed by Lockheed-Martin
- 

- Define advanced persistent threat: exploits that use a kill chain. A means its targeted, coordinated, planned ahead of time its purposeful often with cross benefit analysis and other analytics before the threat is launched. Its persistent, its repetitive, iterative, if not successful in the early phases the attacker attempts to get closer and closer to the target, involves remnants where the malware may survive the reboot of the system or hide from antivirus or antimalware tools. T is the threat, the person or persons (threat actors) have the intent, opportunity and capability.

7-Step Cyber Kill Chain



-
- First phase is recon or information gathering, if the attacker or pen testers know nothing about your organization or target this phase can take a long period of time (days, weeks, months) and the various recon tools are considered attacks (e.g. fingerprinting, posture of systems, delineate systems and versions. Weaponization is choosing the modality or malicious code or the exploit. Delivery is the vector, through email, spam, email attachments, phishing attacks, business email compromise, putting code on USB fobs and leaving them in the parking lot or foyer, penetrating firewall systems or internal compromised users introducing root kits or remote access trojans on systems and services. Exploitation is taking advantage of the weakness or vulnerability in the application service or system. Installation of the malware often involving lateral movement or escalation or elevation on the server or workstation. Command and control, e.g. often in malware there is a remote access trojan so it communicates back to a server (DDoS or botnet) in a stealthily and polymorphic advanced persistent threat. And then typically exfiltration of data is the primary goal.

Why Perform Digital Forensics?

- Laws have been violated
- Organizational policies have been violated
- Systems have been attacked, either internally or externally
- Data and identity have been breached
- Intellectual property has been exfiltrated
- Privileged insiders are suspected of crimes
- It is the next incident response phase (root cause analysis/problem management)

E-Discovery

- Cyber forensics is a main category of e-discovery
- E-discovery is innovative technology that has emerged over the last decade to lower the risks and costs associated with big data, especially in litigation and internal corporate and government investigations
- The e-discovery process includes four phases:
    1. Identifying and collecting documents
    2. Sorting through data by relevance
    3. Creating production sets
    4. Data management

Cyber Forensics Process

1. Identification of the crime
2. Collection of evidence
3. Examination of the evidence
4. Analysis of the evidence
5. Reporting on the findings of the analysis

- When talking about phases e.g. incident response lifecycle, sometimes these phases or states can happen simultaneously

Collecting and Handling Evidence

- Employ forensic kits and laptops -> typically Linux or FTK imager
- Collect network traffic and various logs (SIEM)
- Capture and hash systems images and memory dumps using write-blockers so you leave no fingerprint on the target device
- Document timeline of event sequence
- Record time offsets
- Create screenshots
- Take pictures
- Conduct interviews/depositions

Order of Volatility

1. CPU (most volatile), registers and its cache
2. Kernel statistics, tables, and caches -> of workstations, operating systems, specialty devices (controllers) infrastructure devices, server operating systems
3. Memory (RAM)
4. Temporary file systems and swap/slack space -> on a hard disk drive or solid state drive

- At this point of the incident response if you decide to turn off the system or shut down the system that has been attacked you will not have these four things they are volatile and only exist when system is running otherwise....

5. Disk drives and volumes
6. Attached removable drives or directly attached storage or USB
7. Logged data to a remote location -> e.g. cluster of SYS log servers, SIEM and SOAR system
8. Copies of data to achieved media/cloud

Processing Forensic Evidence

- Detect encrypted files and volumes and attempt to decrypt them
- Discover compressed files and folders
- Perform validation and pattern matching often using your forensic kit
- Leverage regular expressions and metacharacters in forensic kits
- Filter for suspected user data -> e.g. suspect a internal user of using corporate email in unauthorized way you want to filter just for the security identifier of that user
- Filter SIDs on shared systems for privacy reasons
- Perform discovery of hidden data in slack space
- Extract only meaningful data -> data that has utility in the forensic process
- Conduct traces and calibrated estimates to determine suspect(s)

Chain of Custody

- Integral to maintain chain of custody

- Follows evidence through entire life cycle until possible court data
- Involves strict procedures for collecting, handling, and tagging evidence
- Provides a history and timeline of evidence handling
- Maintains evidence integrity
- Provides accountability
- Prohibits tampering
- Anticipates any admissibility issues, such as legal holds

Legal Holds

- A legal holds refers to a process which an organization uses to retain all forms of pertinent data and information when it reasonably expects some type of litigation against it, or some need for future utility in a court of law
- It can be a restriction placed on a database or set of records because of existing or anticipated litigation, audit, government investigation, or other such activity that suspends the regular usage, processing, or disposition of data

Chain of Custody Labeling

Chain of custody				
Registered mail	Date/Time	Released by	Received by	Reason
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	

-
- Chain of custody involves different types of labels. Could use special types of bags that have areas to mark information or document information on the bag itself. A sticker that you attach to a box. Could also correspond information that you put into a software application designating the form of registered mail or certified mail, maybe using a delivery service, date and time stamp, who released it, who received it and a description or reason

Forensic Reporting

- Like any activity you want to have after action reporting
- Reports should have as much information as necessary but not a “data overload”
- May need to express in simpler terms or have different reports for different target audiences. For example; for the IT audience it can be more elaborate and in depth and for CO and CEO audience it can be much shorter and simpler
- Provide electronic and physical documents of all findings
- Meet with proper authorities (e.g. state, national) and possibly prepare to offer expert testimony
- Provide any needed clarification
- Identify overall impact on business and recommend any countermeasures
- Who, what, when, and how? – important for court and other proceedings

Investigation of Data Sources: Logs

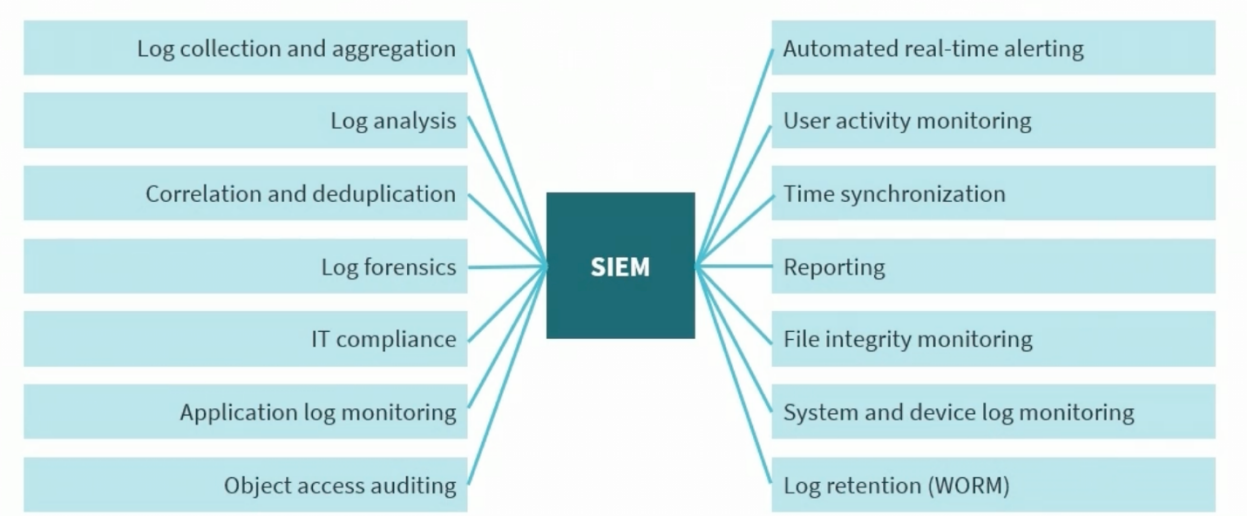
- Firewall logs can provide traffic data in layer 2 frames up to deep packet application inspection using different outputs, e.g. FTP, HTTP, DNS, SMTP
- Application logs for email, web, SharePoint, file, directory, database servers, and more
- Endpoint logs such as Palo Alto Cortex XDR, Configuration Logs, Logs showing API activity
- OS-specific security logs from Windows, UNIX, Linux, macOS, solaris
- Intrusion prevention system (IPS)/intrusion detection system (IDS) logs, alerts, dumps, traps, informs
- Network logs from infrastructure device, security, appliances, database activity monitors and more

Monitoring Source Systems and Events

- Simple Network Management Protocol (SNMPv3) traps and informs (inform is just when it gets sent the sender gets a notification it is received)
- NetFlow collections (v5 and v9) -> v5 is traditional with metadata of layer 3 and 4 ip headers and v9 which is extensible but you can create your own tags in metadata
- Syslog trap messages
- SIEM system events
- SOAR analysis output
- Cloud-based machine learning (ML) and artificial intelligence (AI) visibility/analysis
- IPS sensor dumps and alerts
- Endpoint detection and response (EDR) logs (e.g. Palo alto traps)

Security Information and Event Management

- The term SIEM is a combination of security information management (SIM) and security event management (SEM)
- The objectives:
    - Centralize the storage and analysis of logs and other security-related documentation to perform near real-time analysis
    - Send filtered data to mining, big query, and data warehousing servers in a data center or at a cloud service provider
    - Allow security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents



-
- One of the main goals of a SIEM system is to collect, aggregate, correlate and deduplicate information from a wide variety of devices. Then you can use the SIEM system for example CISCO

splunk, to perform log analysis, contribute to forensics, IT compliance, monitoring applications, auditing object access, auditing real time alerts, monitoring user activity, synchronizing time, generating reports, conducting FIM (file integrity monitoring) and storing them on the SIEM system or a database attached to the SIEM system

Security Orchestration, Automation, and Response

- SOAR is an assortment of software services and tools
    - Azure Sentinel
    - Splunk
    - Chronicle SOAR (part of the Google Cloud umbrella)
- It allows organizations to simplify and aggregate security operations in three core areas:
    - Threat and vulnerability management
    - Incident response
    - Security operations automation
    - CAN DEPLOY SOAR TO DO ONE, TWO OR ALL OF THESE ^^^
- Security automation involves performing security-related tasks without the need for human intervention
- It includes defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing

SOAR Components

- SIEM use cases, categories, and rules are mapped to incident categories
- These categories are then mapped to three types of playbooks
    - Manual playbooks (series of manual tasks)
    - Semi-automated playbooks (hybrid of automated and manual subtasks)
    - Fully-automated playbooks (completely automated)
- Four types of automation
    - Defensive automation (anything that tries to prevent the threat of risk)
    - Forensic automation (anything that tries to retrieve additional evidence)
    - Offensive automation (anything pro-active that tries to investigate an asset)
    - Deception automation (anything that retrieves or adjusts deception tools)
- Three different categories of action
    - Enrichment (adding additional configuration management database (CMDB) or environment data)
    - Escalation (email, ticket escalation, Simple Notification Service (SNS), chat/messaging communication)
    - Mitigation (the modification of device configuration)

Effective Security Governance

Security Governance Defined

- A security practitioner must align all security functions to a business's strategy, value proposition, charters, goals, mission, and objectives
- This alignment must permeate through all organizational processes including governance, steering committee charters, and corporate initiatives to name a few
- Security strategists must account for any major changes to organizational operations or activity
- The need for governance exists anytime a group of people comes together to accomplish an end
- Typically focuses on three attributes or characteristics:
    - Authority
    - Decision-making
    - Accountability
- Is focused on the structure and processes for sound decision-making, accountability, management, and conduct (in relation to security and privacy) at the top of an organization
- It directs how an organization's objectives are determined and achieved, how risk is controlled and addressed, and how the delivery of value is improved
- Security governance is broadly defined as the rules that protect the assets and continuity of an organization
- It includes mission statements, charters, declarations of value propositions, policies, standards, processes and procedures
- Guides the course and control of organizational security operations, initiatives, and activities
- The security practitioner's strategy will be derived from effective security governance

Security Governance Activities

- Creating a risk register (ledger)
- Aligning security strategy with organizational goals
- Publishing all compliance and regulatory requirements (e.g. GDPR)
- Performing a vital role in risk assessment and management
    - Offering guidance into acquiring security controls to reduce risk
- Tracking and recording all compliance and remediation initiatives (e.g. GDPR)
- Documenting stakeholder interactions and reporting related workflows

Centralized vs. Decentralized Governance Structures

- With centralized governance, the higher positions of management such as executives and/or the C-suite hold the decision-making authority
    - It relies heavily on top-down decision-making
- With decentralized, management distributes the decision-making authority throughout the organization
    - Decisions are made closer to the source of action and information
    - Used in flatter, more projectized organizations

Security Governance Boards

- Board governance refers to a security framework or architecture that provides structure to a group of decision-making stakeholders (The Board) and how it functions
- Board governance defines the roles and responsibilities of board members and executives in the form of a:
    - Working board
    - Governing board

- Advisory board

Board of Directors (BOD)

- A board of directors is the governing body of an organization or company, whose members are elected by shareholders (in the case of public companies)
- The duties include setting strategy, overseeing executive management, and protecting the interests of shareholders, bondholders, and other stakeholders
- Every public company must have a board of directors

Steering Committees

- A steering committee is a group of key organizational stakeholders that makes determinations regarding an organization's priorities or order of business, and manages its operations general counsel
- The goal of a steering committee is to oversee and support a project from the management level
- The information Security Committee exists to offer recommendations to executive management and team leads concerning security efforts undertaken
- The committee may also coordinate and communicates the direction, current state, and continual oversight and improvement of information security initiatives
    - For example: Enterprise mobility management, cloud computing adoption, Wireless WPA3, Zero trust

Security Steering Committee Responsibilities

1. Frame. View, and recommend information security policies
2. Evaluate the effectiveness of implemented policies
3. Offer clear guidance and management support for security initiatives
4. Ensure that security activities are executed in compliance with policy
5. Initiate security awareness and training programs
6. Identify and recommend non-compliance responses
7. Approve methodologies and processes for information security
8. Identify significant threat changes and vulnerabilities

Government Agencies

- Cybersecurity and Infrastructure Security Agency (CISA) – leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure
- United States Customs and Border Protection (CBP) – has the mission to keep terrorists and their weapons out of the U.S. along with securing trade and travel while enforcing regulations, including immigration and drug laws
- Office of Homeland Security Situational Awareness (OSA) – provides operations coordination, information sharing, situational awareness, common operating picture, and executes the Secretary's responsibilities across the homeland security enterprise
- Office of Intelligence and Analysis (I&A) – assists the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure and resilient

Roles and Responsibilities

- Security initiatives require a broad awareness of organizations roles and responsibilities
- Companies are organized in different ways, such as top-down, flat, or outsourced
- Directory services are often closely aligned and mapped to organizational duties and job titles
- Roles and responsibilities will often directly affect access control methodologies and sensitivity levels for mandatory access architectures

Owners

- With Role-based Access Control (RBAC), access decisions typically rely on organizational charts, roles, responsibilities, or locations in a user base
    - The role is often set based on evaluating the essential objectives and architecture of the enterprise aligned with the subject's job title and responsibilities
- Physical and logical asset owners may:
    - Determine the classification level
    - Conduct labeling and tagging
    - Grant additional shares and rights

Custodians

- Custodians are also referred to as "controllers"
- They should maintain the assets from a technical and operational perspective
- Custodians often interact directly with owner stakeholders and answer to executive managers (C-suite)
- Often responsible for ensuring confidentiality, integrity, authenticity, availability and non-repudiation of assets

Stewards

- Stewards will manage assets from a business perspective
- May interface with other departments such as legal, human resources, mobile application and digital asset managers
- They are more likely to deal directly with internal and external customers and stakeholders
- Often ensure compliance (standards and controls) and data quality

Officers

- The buck should stop here although it is not uncommon that the custodians/controllers take the hit when goals are not accomplished
- C-suite or C-team includes CEO, CIO, CISO, CPO, CTO, and other new forms of chief officers
- These are totally responsible for due diligence and adherence to security governance
- Will often answer to steering committees and various boards such as the BOD

RACI Charts

R – Responsible **A** – Accountable **C** – Consulted **I** – Informed

	GRC* Department	Legal Department	Security Team	IT Operations
Establish the provider requirements	R/A	C	C	I
Build the governance scheme	R/A	C	C	I
Assess cloud vendor	A	I	R	R
Build the architecture	I	I	A/R	R
Conduct cloud migration	I	I	C	A/R

**GRC – Governance, Risk, and Compliance*

-
- There is four different roles here; responsible, accountable, consulted, informed. In this use case we are doing a cloud migration; migrating our oracle database up to AWS relational database service for oracle. This is a streamline initiative (only 5 tasks) but doing a RACI chart realize that one and only one party which in this case 4 parties (GRC Department, legal department, security team, IT Operations), one and only one party or element is accountable. For each one of these 5 tasks we have 1 and only 1 accountable party. Responsible you will have at least 1 response party but you can have more than 1 responsible party. E.g. "Build the architecture", both the security and the IT operations team are responsible so at least 1, but notice only the security team is ultimately accountable. Consulted infers some type of 2-way relationship or when you consult the subject you expect some feedback or answer or approval. Remember consulted is a 2-way communication, e.g. when you establish the provider requirements, your going to consult the legal department and security team and you expect feedback. I or informed is simply a notification, so when you inform someone it can be a blind copy of a email, a notification service in the cloud NaaS, or a Microsoft notification in Microsoft SharePoint to a interested or informed party.

External Governance Considerations

- Despite the size or the industry, every organization must adhere to specific laws and regulations
- Regulatory compliance describes the actions an organization takes to comply with those rules and policies as part of its operations
- When it comes to data, there are rules for handling sensitive information
- To be in regulatory compliance, organizations set up internal processes to keep data safe and secure – otherwise, they may be fined, sued or face criminal prosecution
- Some laws and regulations may be driven by the applicable business sector or industry for example Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act, Sarbanes-Oxley, or Payment Card Industry Data Security Standard (PCI DSS)
- The scope can be global, international (treaties), national, state/province/parish, county, or local
- Guidance such as International Electrotechnical Commission/International Organization for Standardization (ISO/IEC) or National Institute of Standards and Technology (NIST) cannot supersede or overwrite governmental laws and regulations at any level even local

Exploring Organizations for Security Standards and Best Practices

- ISO (International Organization of Standardization). Brings global experts together to find the best way to do things, covers a wide variety. Enabling trade and cooperation. Where the OSI model comes from.
- NIST (National Institute of Standards and Technology). A lot of the things we look at in terms of definitions comes from NIST. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.
- ISACA. CISM cert and Auditor cert. Focuses on audit, cybersecurity and tech
- CIS (Center for Internet Security). To improve state, local, tribal and territorial cybersecurity. Has 18 CIS Critical Security Controls. Unless you have determined, evaluated, and assessed the assets you have, so e.g. unless you have a inventory and control of your enterprise assets and software assets don't bother with the remaining 16 controls. You have to know what you have before you can deal with the risk, treat risk, have risk management and risk assessment. The top 18 is a popular set of controls from the CIS.
- For cloud based security, CSA (cloud security alliance) helps define and raise awareness of best practices to secure cloud environments. Have a STAR program, questionary of cloud SaaS providers for businesses to go look at. Certifications for cloud security. Have the Cloud Controls Matrix that is composed of 197 control objectives in 17 different domains, used as a audit tool to test the maturity of your organization. Providers use this to evaluate maturity and posture. CAIQ is the one that is put into the STAR registry.
- OWASP (open worldwide application security project). Used for securing websites. Improve security of software, web applications, mobile applications, IoT, application program interfaces. Community lead open source project. OWASP cheat sheets to secure internet gateways.
- SANS Institute is a coop for information security to empower cyber professionals with practical skills and knowledge. Security Policy Templates for security policy.
- MITRE Attack Matrix. Knowledge based of adversary techniques based on real-world attacks in different sectors. Has its own categories of attacks that can be used by blue teams, penetration testers. Repo for red team and blue team.

Best Practices and Guidelines

- Guidelines provide a list of suggestions on how one can do things more effectively
- Guidelines and practices are like standards but are more flexible and not usually mandatory
- They are used to define how standards should be developed or to guarantee adherence to general security policies or governance

Security Guidelines

- NIST Computer Security Resource Center
- National Security Agency (NSA) Security Configuration Guides: does have security config guides specifically for military, government agencies or agencies that have contracts with them
- Center for Internet Security (CIS) Top 18
- Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Best Practices: has a set of best practices
- Cloud Security Alliance (CSA) – Cloud Controls Matrix (CCM)

Standards

- Standards allow an information technology staff to be consistent and systematic
- Standards specify the use of specific technologies in a uniform way, because no one individual practitioner can know everything

- They also help to provide consistency in the enterprise, because it is unreasonable to support multiple versions of hardware and software unless necessary
- Standards are usually mandatory, and the most successful IT organizations have standards to improve efficiency and keep things as simple as possible

Policies

- Policies, specifically security policies, establish a general framework within which to work and a guiding direction to take in the future
- The function of a policy is to classify guiding principles, direct behavior, and offer stakeholder guidance and a security control implementation roadmap
- An information security policy is a directive that outlines how an enterprise plans on protecting its data, applications, and systems
- It helps ensure compliance with legal and regulatory requirements and preserve an environment that sustains security principles
- Policy documents are high-level overview publications that guide the way in which various controls and initiatives are implemented

Developing an Information Security Policy

1. Sanctioned
    - The policy has the support of executive management
    - Requires visible participation and action, ongoing communication and championing, investment, and prioritization
2. Applicable
    - The policy is applicable to the organization
    - Strategically, the information security policy must support the guiding principles and goals of the organization
    - Tactically, it must be relevant to those who must comply
3. Realistic
    - The policy can be effectively executed
    - Policies must represent the actual environment in which they will be deployed
    - Information security policies and procedures should only express what is achievable
    - If the policy is to advance the organization's guiding principles, one can also assume that a positive outcome is anticipated
    - A policy should never set up constituents for failure but instead should offer a clear track for success
4. Flexible
    - The policy can accommodate change and be adapted if necessary
    - An adaptable information security policy recognizes that information security is not a static, point-in-time endeavor, but rather an ongoing process designed to support the organizational mission
    - Must be able to adapt in change of technology, governance, compliance
5. Comprehensive
    - The policy scope includes all relevant parties – it is inclusive
    - An information security policy must consider:
        - Organizational objectives
        - International law
        - Cultural norms of its employees
        - Business partners, suppliers, and customers
        - Environmental impacts

        - Global cyber threats
6. Enforced
    - The policy is statutory and is enforced
    - Enforceable means that administrative, physical, or technical controls can be put in place to support the policy
    - Compliance can be measured and, if necessary, appropriate sanctions applied
    - Enforcement states should be well-documented:
        - Verbal reprimand
        - Written warning
        - Punitive actions
        - Temporary suspension
        - Permanent termination
        - Legal actions

Example Standards and Policies
- Password
- Access control
- Physical security
- Encryption
- Information security
- Business continuity
- Disaster recovery
- Incident response
- Software development life cycle (SDLC)
- Change management
- Acceptable Use Policy (AUP)

Acceptable Use Policies
- Considered one of the most important sections of a written security policy
- Identifies how employees are expected to use resources in the organization
- Defines rules of behavior/code of conduct:
    - Use proper and acceptable language
    - Avoid illegal activities
    - Avoid disturbing or disrupting other systems
    - Do not reveal personal information

Sample AUP Categories
- Mobile device policy
- Virtual private network (VPN)/software-defined perimeter (SDP) usage
- Operating systems and software
- Social media
- Removable media
- Augmented reality
- Personal cloud storage
- Clean desk

Procedures
- Procedures are usually required and are the lowest level of the policy chain
- Procedure documents are longer and more detailed than standards and guidelines documents

- These include implementation details with step-by-step instructions and graphics
- Established practices are very important for helping large organizations achieve the consistency of deployment necessary for a secure environment

Standard Operating Procedures (SOPs)
- Step-by-step instructions that define how workers carry out routine tasks
- Can greatly improve
    - Compliance with regulations
    - Efficiency
    - Quality
    - Performance
    - Communication

SOP Considerations
- Describe purpose and limits of procedures
- Offer all the steps needed to complete the process
- Clarify concepts and terminology
- Consider health and safety issues
- List the location of all necessary supplemental resources

Change Management Practice
- The change management practice is also called the change control practice
- The change control process reduces risk in security policy by delivering a systematic approach to assess and manage proposed and subsequent changes
    - Normal changes (e.g. changing password in active directory)
    - Standard changes (e.g. 48 months being provisioned a new mobile device or laptop)
    - Emergency changes (e.g. mobile device lost or stolen)
- It assures that changes are carefully assessed for possible impacts on project scope, schedule, and resources, allowing for informed decisions

Onboarding (Provisioning)
- Is typically much more automated than offboarding and deprovisioning process
- Provide assets, guidance, knowledge, skills, and behavior needed for associated job roles
    - Videos, printed material, computer-based training (CBT), lectures, formal and informal meetings, and mentors
- Introductions and explanation of standards and practices including SOPs
    - Clearly define roles and responsibilities
- Provisioning all devices and equipment
- Deliver security awareness and AUP expectations
- Additional Human Resources activities
    - Remove any ambiguity and uncertainty
- Offboarding or deprovisioning is the reverse process

Automating Onboarding and Other Processes
- Enterprises often deploy systems that involve self-service onboarding of personal devices
- These processes can be fully and semi-automated with runbooks and playbooks
    - Security information and event management (SIEM) and security orchestration, automation, and response (SOAR) systems are emerging solutions

- The Joiner or Mover registers a new device, and the native supplicant is automatically provisioned for that user and device and installed using a supplicant profile that is preconfigured to connect the device to the corporate network

Monitoring and Revisions

- The proper usage of various visibility tools will result in comprehensive monitoring and proper revisions and improvements
    - SIEM systems
    - Intrusion detection system (IDS)/intrusion prevention system (IPS) sensor logs
    - Application logs (system, security, application logs)
    - Firewall logs
    - Simple Network Management Protocol (SNMP) traps and informs
    - NetFlow records
    - Database activity monitor (DAM) reports
    - Software as a Service (SaaS) solutions

Risk Management

Define Risk Management

- Risk management is the continuous process of handling risks to organizational operations, including mission-critical services and functions, physical and logical assets, and people
- The results of this management might be
    - Establishing the context for risk-related activities
    - Conducting an asset and risk assessment
    - Implementing a risk mitigation strategy based on established risk treatment
    - Employing techniques and procedures for the continuous monitoring of the security state of information systems
- Inherent (total) risk:
    - The vulnerabilities and risks that the organization faces before safeguards are implemented
    - The present baseline or system/application state before a formal assessment begins
- Residual risk:
    - The vulnerability or risk that remains after the mitigating controls are introduced
- Residual = inherent risk – safeguards (controls)

Risk Identification and Assessment

- According to the Center for Internet Security (CIS) Top 18 Controls, two initiatives must be conducted before the most critical assets (data and people) can be protected:
    1. Inventory and Control of Enterprise Assets
    2. Inventory and Control of Software Assets
- These initiatives will contribute greatly to risk identification and assessment activities

Inventory and Control of Enterprise Assets

- Before the security practitioner can identify and assess risk, they must “know what they have”
- This involves actively tracking, labeling, and inventory of all enterprise assets:
    - End-user devices (stationary, portable, and mobile)
    - Network infrastructure devices
    - Security devices and appliances
    - Servers and hypervisors
    - Non-computing/Internet of Things (IoT) devices
    - Any physical component connected virtually, remotely, and to cloud environments
- The security practitioner should accurately know the entirety of assets that need to be monitored and protected within the enterprise

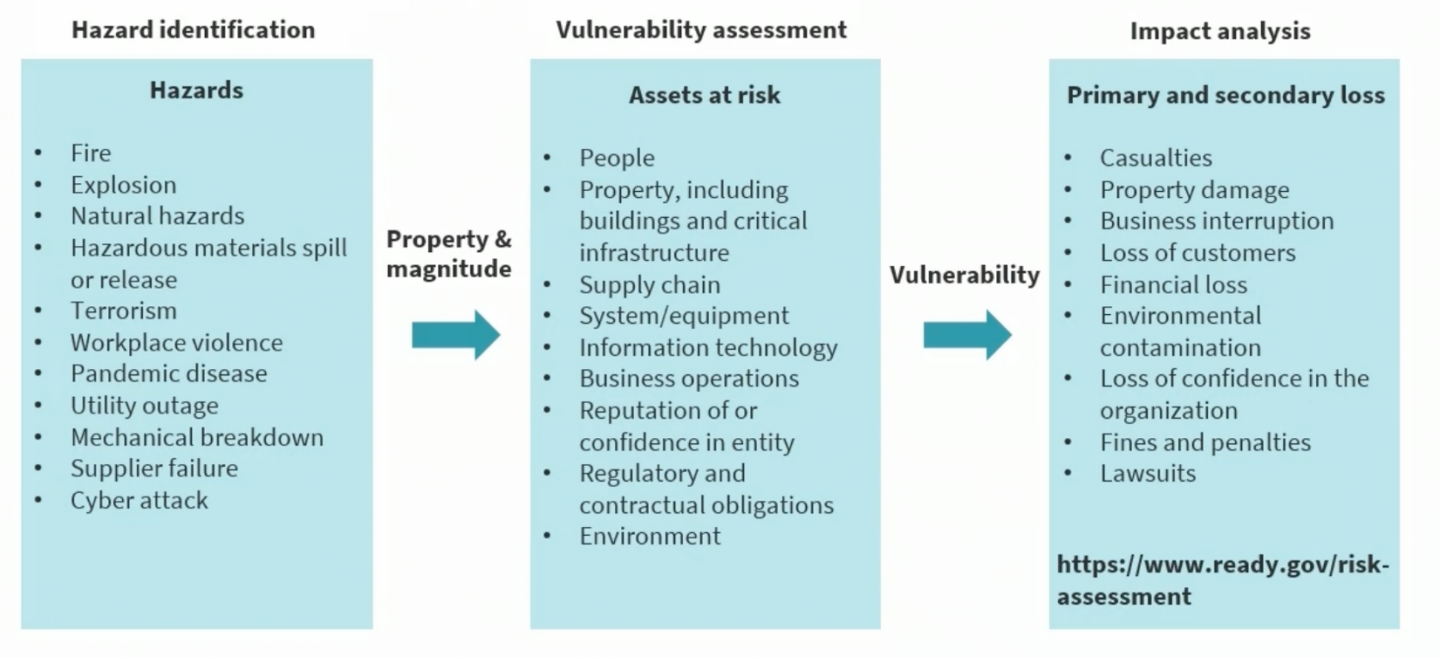
Inventory and Control of Software Assets

- The security practitioner must vigorously manage (inventory, track, and repair) all operating system software and applications on all networks (production, management, storage area, hypervisor) so that only authorized software is installed and run
- This includes virtual assets at cloud providers in infrastructure, platform, and Software as a Service deployments
- Any unauthorized and unmanaged software must be located and prevented from installation or execution (ghost or shadow IT) in accordance with policies and procedures

Risk Identification and Assessment

- Risk identification involves the qualitative (relative or on a particular scale) and/or quantitative (mathematical) evaluation of the most probable risks and threats to organizational assets

- The practitioner should determine the potential impact (magnitude) and likelihood (probability) against the mission-critical assets first
- There's four major ways to perform identification and assessment of risk:
    - Continuous -> continual due care, continuous operation maintenance, security hygiene
    - Ad hoc -> as needed basis
    - Recurring -> schedule (weekly, monthly, quarterly, bi-annual or annual, fiscal year or calendar year)
    - One-time -> risk identification and assessment, why, because so many things can change e.g. new technology, policies, regulations, competitors



-
- Wide variety of potential hazards so the organization has to decide which of these are likely or probable and realize things can change. E.g. pandemic disease (quite likely due to past 5 years) which has moved up on the list. Once identified hazards we will perform vulnerability assessment and look at the assets that are at risk. For some organizations, people are at the top of the list, but not all organizations consider people to be the most valuable asset, it may be property or infrastructure, supply chain, business operations, environmental aspects. Then once you've done that you do impact analysis. Basically primary (immediate loss e.g. casualty, property damage, business interruption, DDoS attack) and secondary loss (subsequent loss, secondary loss can be more costly than the primary loss e.g. loss of confidence, stock price, fines and penalties or civil law suites).

Five Key Elements of Risk Analysis

1. Assets or an asset class
2. Incident or scenario (e.g. web servers in a fire, CEO laptop with ransomware)
3. Timeframe (fiscal/calendar year)
4. Impact (magnitude)
5. Likelihood (probability)

Qualitative Risk Analysis

- The most common method used in risk and security
- Descriptive approach using subjective opinions, history, and scenarios to determine risk levels:
    - Expert judgement
    - Best practices

    - Experience
    - Intuition
- Often involves interviews, questionnaires, surveys (Delphi), and conducting brainstorming sessions and workshops addressing assets, known risks, known vulnerabilities, common threats, and historical impacts

Qualitative Risk Analysis Heat Maps

			Impact				
Likelihood			Negligible	Minor	Moderate	Critical	Disastrous
			1	2	3	4	5
	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

-
- Generally, qualitative analysis will generate a heat map, in this heat map lets focus on the five key elements. First this heat map will apply to an asset or an asset class e.g. hypervisors in your data center. Secondly under a certain scenario, e.g. a highly privileged user installing a root kit or a remote access trojan in the hypervisors (called hyperjacking). Third, a time frame (quarterly, semi-annual, most often – fiscal or annual year). Then the final two elements we see in the diagram, on the horizonal we have impact/magnitude, on the vertical we have likelihood or probability. Then we are going to have a scale e.g. 1-5, 1-8, 1-10. Want to use same scale typically for likelihood and impact (1-5). We have labels and if we determine that the particular risk to our hypervisors is likely and causing critical damage then we will have high (which means we will focus our resources protecting this asset based on our risk analysis). Realize that a qualitative method is effective, generally from a more macro standpoint, but it is more subjective, and there is a little bit more guess work and calibrated estimation that goes into qualitative

Quantitative Risk Analysis

- Quantitative risk analysis is a scientific/mathematical approach to getting monetary and numeric results based on:
    - Asset values (cost and depreciated)
    - Impact (magnitude) or severity of the incident
    - Probability (likelihood) of occurrence
    - Threat frequency
    - Costs and effectiveness of safeguards
- The resulting probabilities are based on percentages, mathematical formulas, and calibrated estimation
- Even a semi-quantitative approach will be preferable to a purely qualitative analysis

Classic Quantitative Analysis (Whitman)

- AV (asset value):
  - Value of the asset according to the organization
- EF (exposure factor):
  - Percentage of asset loss caused by identified threat
- SLE (single loss expectancy):
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- ARO (annualized rate of occurrence):
  - Estimated frequency the threat will occur within a single year
- ALE (annualized loss expectancy) = (SLE * ARO)
  - For a particular asset or asset class in a certain scenario

Quantitative Risk Analysis

Whitman risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15,000	100%	$15,000	0.1	$1,500
SRV_2	Fire	$20,000	100%	$20,000	0.1	$2,000
SRV_1	Flood	$15,000	100%	$15,000	0.0001	$1.5
SRV_2	Flood	$20,000	100%	$20,000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15,000	10%	$1,500	365	$547,500
SRV_1	Virus (with AV software)	$15,000	10%	$1,500	1	$1,500

-
- For example in your Whitman analysis you would generate spreadsheets or database reporting based on different assets and asset classes under different threats or scenarios. And then we have all our values here; asset value AV, exposure factor EF< single loss expectancy SLE, Annualized rate of occurrence ARO, and annualized loss expectancy ALE (goal). Based on that we will allocated resources to managing or treating the risk to our assets under various scenarios.

Risk Treatment (Handling): Accept

- Risk acceptance:
  - Do not implement any additional safeguards
  - Justification in writing is often required
  - This can also be the process of “ignoring” the risk
- Examples:
  - Only having one supplier or vendor for hardware or services relying on their uptime reputation
  - Leasing a facility in a 100-year flood zone
  - Deciding not to add a cyber security rider to your existing business insurance policy

    - Continuing with a Wi-Fi Protected Access (WPA2) – secured wireless local-area network (WLAN)

Risk Treatment (Handling): Transfer

- Risk transference is also referred to as risk sharing:
    - Passing off risk to a third-party or shared party
- Examples:
    - Purchasing an insurance policy or additional cyber insurance
    - Leveraging a shared responsibility model 9SRM) with a cloud service provider (IaaS)
    - Leasing a warm/cold disaster recovery facility with another similar business that is several miles away using a reciprocal agreement

Risk Treatment (Handling): Avoid

- Remember risk avoidance may also demand that you answer to decision makers, the steering committee or your C-suite
- Risk avoidance involves deciding not to undertake actions or engage in activities that introduce or increase risk
- Being too risk-averse can lead to missing out on opportunity or advantages
- Examples:
    - Not processing and storing credit card information of customers on-premises
    - Not using a cloud service provider for DevOps or managed data services
    - Avoiding the use of any clear-text protocols, such as HTTP, Lightweight Directory Access Protocol (LDAP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), or telnet
    - Not storing sensitive data in a personal cloud service, such as Dropbox or Google Drive

Risk Treatment (Handling): Mitigate

- Cant remove we can only reduce…there is always some type of risk, but we can mitigate the current risk to reduce
- This involves the strategic and tactical deployment of an array of technical, administrative, and physical controls to reduce risk to an acceptable level
- Enterprises will implement safeguards that will reduce risk exposure – the risk may still exist, but the impact is reduced
- Examples:
    - Implementing endpoint protection, such as Palo Alto Cortex XDR
    - Upgrading the edge firewall appliance
    - Using a cloud-based security information and event management (SIEM)/security orchestration, automation, and response (SOAR) solution like Azure Sentinel or a managed security service provider (MSSP) solution from Fortinet
    - Hiring armed security guards

Risk Treatment

- Treatment and handling may also be referred to as “risk appetite”
- Any combination of treatments can be used with risk management
- Analysts must also consider any exemptions or exceptions for certain privileged users, air gapped systems, or special use case applications

Risk Handling Approaches

- Expansionary

    - Enterprise intends to increase the number of resources to allocate to treat risk as needed on an ongoing basis
- Conservative
    - Enterprise is frugal and extremely careful to spend more money, acquire controls, add personnel
    - They would rather find compensating controls
- Neutral
    - Enterprise will take a balanced approach to risk treatment
    - The appetite is neither expansionary or conservative unless necessary

Risk Assessment Documents

- These assessments will record the processes used to identify probable threats and propose subsequent action plans if the hazard occurs
- The document will declare assets at risk (people, buildings, information technology, utility systems, machinery, raw materials, and finished goods)
- There are many templates and prototypes available online
- These documents will be used to construct risk registers and ledgers

Creating a Risk Register (Ledger)

Identified risks	Root causes	Probability and impact	Ranking	Categories	Priorities	Time and cost objectives	Potential responses	Risk owners	Assumptions

-
- Is a compilation of information related to vulnerabilities, risks, and countermeasures:
    - Repository of identified risks, impact, scenarios, and potential responses
- Populated from after-action reporting, lessons learned, case studies, and assessments
- Often represented as a table/scatter plot from a spreadsheet or database view
- May be an important tool to fulfill regulatory compliance

Risk Ledger Matrix

		Event type								
		Accidental leak	Espionage	Financial fraud	Misuse	Opportunistic data theft	Physical theft	Product alteration	Sabotage	Violence
Intent	**Nonhostile**									
	Reckless insider	X			X			X		
	Untrained/distracted insider	X			X			X		
	Outward sympathizer	X			X					
	Unknown (nonhostile or hostile)									
	Supplier	X	X	X	X	X		X		
	Partner	X	X	X	X	X		X		
	Hostile									
	Irrational individual	X			X		X		X	X
	Thief		X	X		X	X			
	Disgruntled insider	X	X	X	X	X	X	X	X	X
	Activist		X		X	X	X	X	X	
	Terrorist						X		X	X
	Organized crime		X	X		X	X	X		
	Competitor		X			X		X	X	
	Nation state		X			X		X	X	

-
- On the horizontal we have the incident or event type, in this case it is a non-physical attack (accidental leak -> data leak as opposed to a chemical leak). Then on the vertical we have different types of threat actors with various levels of intent. The one that checks off all the box is the hostile disgruntled insider. It may be preferable to refer to this insider as a compromised insider because they can be compromised for a wide variety of reasons and may not necessarily be disgruntled

Other Risk Document Concepts

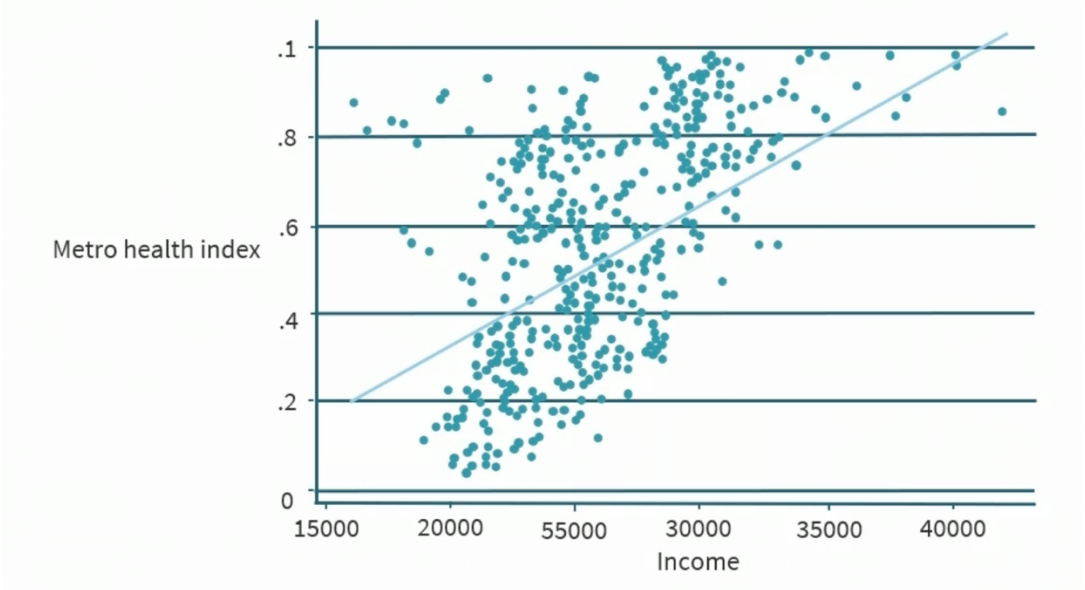
- Risk owners are persons or entities responsible for managing threats and vulnerabilities that might be exploited such as a chief information security officer (CISO), data custodian, virtual asset manager, or other technical risk stakeholder
- Key risk indicators (KRIs) are meaningful metrics for measuring the likelihood and impact of an incident and if the results exceed established risk appetite. KRIs are commonly used in quantitative risk analysis
- A risk threshold is a quantifiable level of uncertainty and impact from risk, below which an organization will accept a risk and above which an organization will not accept a risk

Risk Reporting

- Risk reports should have just as much information as necessary but not a “data overload”
- Reports should be concise and yet comprehensive:
    - Written reports and summaries
    - White papers, special publications
    - Published to an intranet
    - Live presentations (in-person or conferencing sessions)
- Analysts may need to express in simpler terms or have different reports for different target audiences:
    - Possibly include a glossary of terms
- Dashboards are very effective (Python and R programming)
- Understand the optimal aspects of visual communications:
    - Avoid three-dimensional representation
    - Use a palette of sequential colors

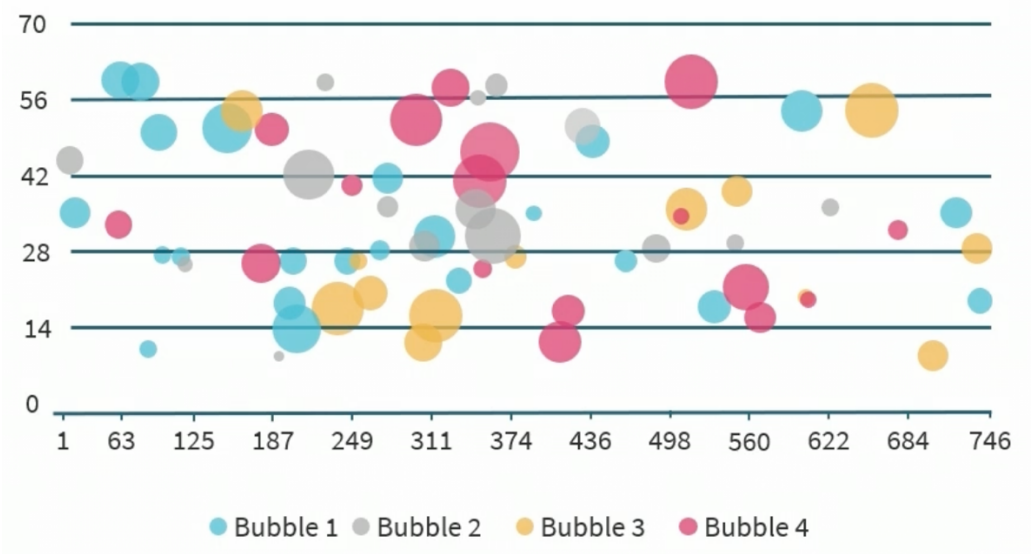
- Consider possible “color blindness” and sight-impaired audiences
- Avoid pie charts or simple histograms and consider using:
  - Scatterplots
  - Bars and bubble charts
  - Density plots
  - Boxplots

Scatterplots



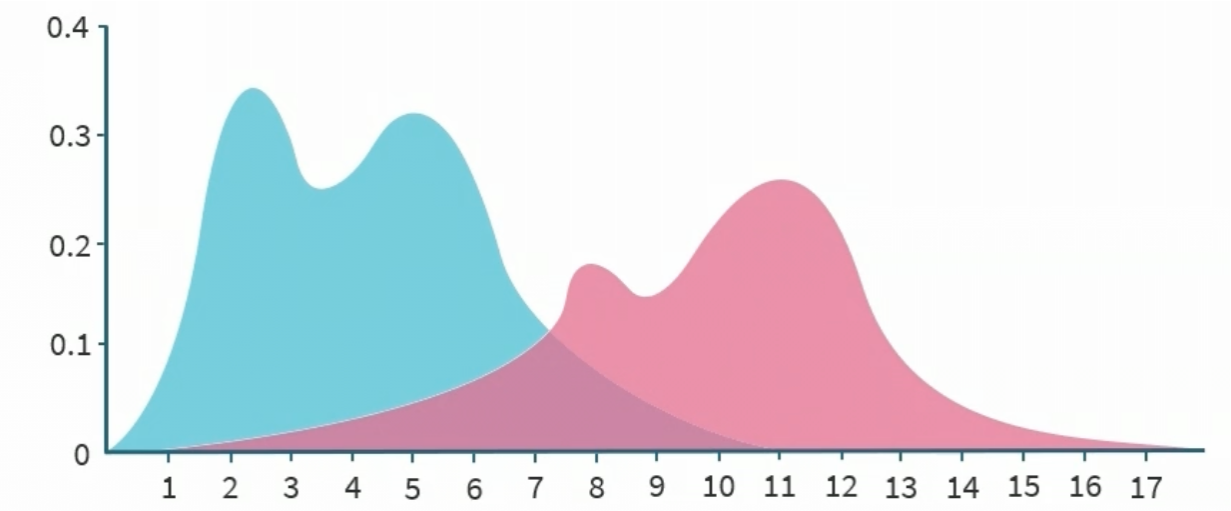
-
- A scatterplot will show the relationship between two different quantitative variables, for the same event or incident, systems or people. One of the values appears on the horizontal axis and the other variable is on the vertical axis, and each component appears as a point on the graph

Bubble Charts



-
- Basically extending the scatter plot but looking at the relationship between variables, so each dot in the bubble chart is a single data point and the variables value for each point are indicated by the horizonal position, vertical position and the dot size

Density Plots



-
- Density plots represent a distribution of a numeric value. So basically uses what's called kernel density estimates to show the probability or the likelihood of a particular variable. Consider this a more smooth representation of a histogram and it uses the same concept

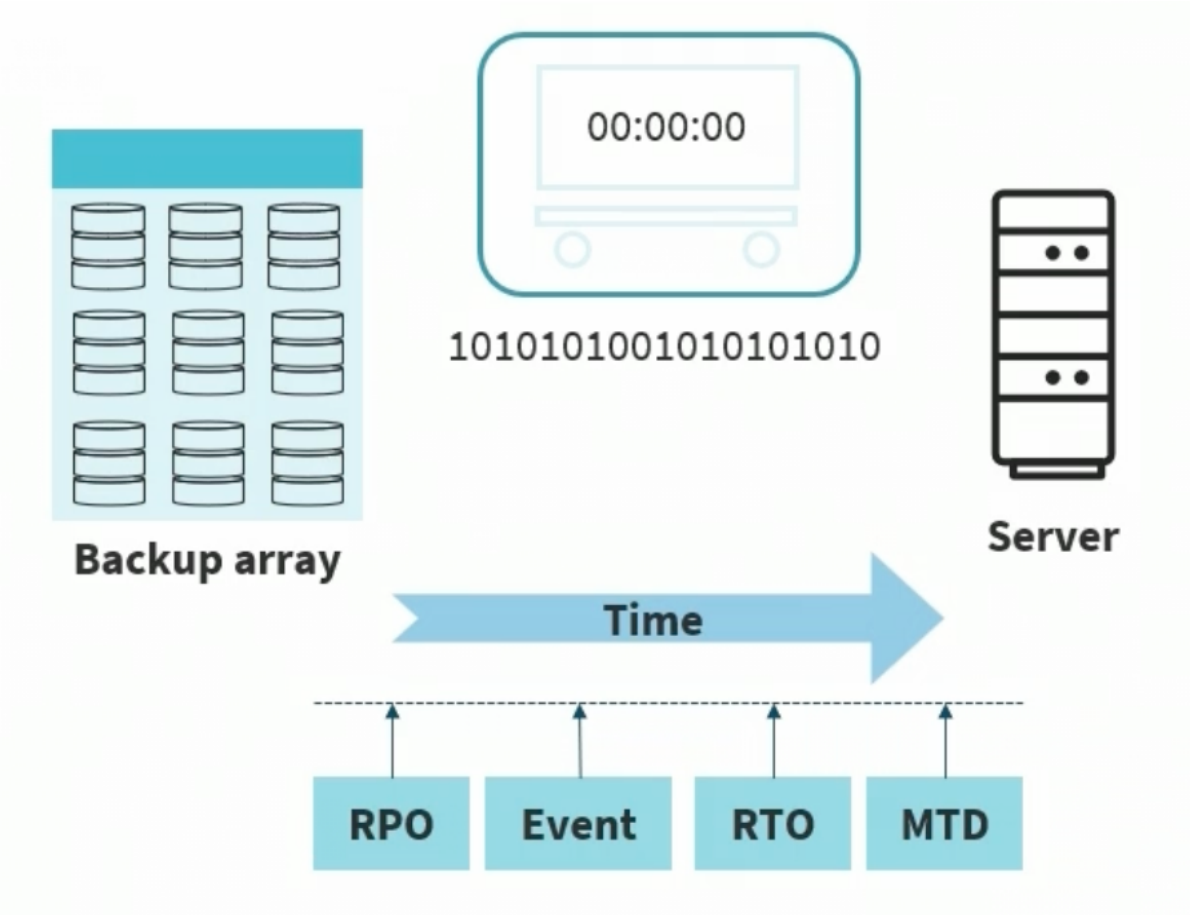
Boxplots

- Basically a graph that shows the summary of a dataset. Shape of the boxplot shows how the data is distributed, can also be represented as a candle (if doing technical analysis of stocks, commodities, crypto where the bottom of the line represents the lowest value of the trading session and the top of the line is the highest value during the trading session).

Business Impact Analysis (BIA)

- A BIA predicts the consequences of a disruption to a business and collects information needed to develop recovery strategies
- Potential loss scenarios should be identified from risk assessment
- Activities may include developing questionnaires, conducting workshops, distributing stakeholder surveys, and performing follow-ups and gap analysis

BIA Metrics: RTO -> Recovery Time Objective



-
- In this use case, our backup strategy to an array from our servers in our datacenter or server farm
- The Recovery Time Objective (RTO) is the amount of time needed to recover a resource, service, application, or function. In this example, to recover our server from our backups.
- It must be less than or equal to the maximum tolerable downtime (MTD)
- Any solutions must be completed within this time frame, or it is considered an unacceptable loss
- Ways to reduce RTO include
    - Adding physical security
    - Adding redundancy
    - Purchasing insurance
    - Investing in better generators
    - Investing in faster recovery solutions

BIA Metrics: MTD

- The maximum tolerable downtime (MTD) is also called maximum allowable downtime (MAD)
- This BIA metric represents the absolute maximum amount of time that a resource, service or function can be unavailable before the entity starts to experience a catastrophic loss. For example; what is the maximum amount of time the VOIP can be down, how long our power can be out
- When the MTD is exceeded, the disaster recovery plans (DRPs) are often triggered

BIA Metrics: RPO

- The Recovery Point Objective (RPO) is often represented as the target amount of time within which a process must be restored after disruption
- It is commonly a point when some manual or automated task occurred
- The activity point, relative to a disaster, is where the recovery process begins:

    - Last Known Good Configurations
    - Database transaction logs
    - Snapshots
    - Recovery volumes
    - State machine instances

Mean Time Between Failures (MTBF)

- MTBF is the measurement of the reliability of a hardware system (CISCO/Juniper router), component, or hot spare
- This data often comes from Original Equipment Manufacturers (OEMs), retailers/distributors, or third-party consumer reporting
- The MTBF of solid-state drives (SSDs) is usually rated in the millions of hours, so an MTBF of 1 million hours means that the average lifespan of a device is over 114 years
    - Industrial SSDs typically have ratings between 2 million hours (about 228 years) or 5 million hours of 570 years

Mean Time to Repair or Replace (MTTR)

- This meaningful metric determines how long it will take in minutes, hours, or days to repair or replace a failed system, component, application, or service
- The MTTR is often calculated for replacements and hot spares
- This BIA measurement has and is heavily affected by supply chain disruptions, backorders, and vendor(manufacturers, wholesalers, distributors) dislocation
- It is typically a mathematical average value based on experience and documentation:
    - MTTR = (Total down time)//(number of breakdowns)

Security Compliance and Third-Party Risk

Compliance

- Compliance is defined as observing a rule, such as a policy, standard, specification, or law
- Regulatory compliance outlines the goals organizations want to accomplish to certify that they understand and take actions to comply with policies, relevant laws, and regulations
    - For example, companies that provide products and services to the U.S. federal government must meet certain security directives set by NIST
- Specifically, NIST SP 800-53 and SP 800-171 are two common mandates with which companies working within the federal supply chain may need to comply

Compliance Monitoring

- Compliance monitoring is a continuous process to ensure that all organizational subjects are adhering to all polices and procedures in the published polices and procedures
- Goals of compliance monitoring include:
    - Exposing compliance risk issues in an organization's operations or functions
    - Helping organizations achieve consistent regulatory compliance and avoid areas of non-compliance
- Compliance monitoring is often considered an important part of security governance and overall cybersecurity posture
- Failure to conform with compliance requirements can result in severe fines and business disruptions

Compliance Monitoring Activities

- Monitoring for continuous certification and accreditation. You can actually use appliance vulnerability assessment tools so you can be certified or accredited the next time the governing body does it
- Publishing all compliance and regulatory requirements, both logical and physical
- Tracking and recording all compliance and remediation initiatives
- Supporting a compliance manager enforcing a Separation of Duty (SOD) or larger Zero Trust initiative
- May be an activity for one with the role of a data steward in some organizations

Due Diligence

- Due diligence relates to the act of performing thorough research before committing to a particular plan of action
- It involves proper information gathering, planning, testing, scoping, and strategizing before development, production, and deployment
    - Comprehensive background check practices for hiring
    - Investigating a cloud service provider (CSP) thoroughly before signing a memorandum of understanding (MOU)
    - Testing and evaluating nonrepudiation techniques (digital signatures) before signing contracts or using code

Due Care

- Due care refers to the degree of attention that a reasonable person takes for a particular entity
- Is the level of judgement, attention, and activity that a person would engage in under similar circumstances
- It involves all ongoing operational controls
- Many organizations with rely on an ITIL4 continual improvement framework to optimize due care to elevate them to a higher Capability Maturity Model (CMM) level

Attestation

- Compliance attestation is a formal validation document that is used to certify an organization's status to interested external parties
- According to ISO/IEC, attestation is the issue of a "statement" based on a decision that a specific requirements have been met
- SOC 2 is an attestation report that offers in depth information and assurance about an entity's availability, processing integrity, confidentiality, and privacy controls

Acknowledgement

- Compliance acknowledgement typically involves a statement affirming that an authorized enterprise understands and will adhere to their confidentiality obligations and a security and privacy mandate such as:
    - Sarbanes-Oxley (SOX)
    - Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical health (HITECH)
    - SOC1/2
    - Payment Card Industry Data Security Standard (PCI DSS)
    - General Data Protection Regulation (GDPR)
    - CSA Cloud Controls Matrix (CCM)
    - Other regulations and governance

Compliance Monitoring Automation

- Compliance processes are time-consuming, and when there is no automation involved, it quickly uses productive hours
- A manual workflow/audit can take around 150 hours, while an automated compliance tools may only need about 10-12 hours to complete
- Compliance automation tools ensure the protection of data and are governed according to the applicable regulations such as GDPR
- Tasks can include self-assessment, planning and monitoring controls, testing, and reporting
- Compliance automation tools can assist enterprises to reduce non-compliance risk, improve efficiency, and attain better visibility, which is critical aspect of the zero-trust initiative

Internal Compliance Reporting

- Internal compliance reporting allows organizations to institute internal controls (administrative, physical and technical and ongoing operation controls), to monitor employee behavior to detect potential fraud, illegal activities, misconduct, or non-compliant activities to:
    - Adhere to regulatory requirements
    - Maintain stakeholder trust
    - Mitigate risk
    - Support ethical considerations and corporate social responsibility (CSR)
    - Establish internal governance and performance monitoring

External Compliance Reporting

- External compliance refers to following the rules, laws, and standards set by a Government entity
    - The primary goal is to avoid any negative impact on the organization such as fines, penalties, and loss of corporate goodwill
    - The state or province in which the firm is incorporated (located) is concerned with defining these compliances
    - External compliance reports and audits are reviewed by regulatory bodies for determining compliance status, certification, and/or accreditation
    - These can vary as per industries, business sector, applicable regulations and geographical locations

Consequences of Non-compliance

- Specifically, non-compliance to laws, regulations, mandates
- Fines -> regulations such as GDPR (EU and businesses and any organization that does business with the EU can inflict multiple levels of fines for non-compliance, e.g. HIPA have delivered fines to

a wide variety of organizations who have not kept medical and personal information private. If a company is subject to a criminal case the result might not be jail time it will be fines or restitution)

- Sanctions -> a sanction can be placed on a organization or a business where they are unable to conduct activities for a certain period of time or area or a sanction can just be a threat of a penalty for disobeying a law or rule or mandate. A sanction isn't an official order, it places some limitation, a limitation on trade, on contact, on doing business or delivering a certain value proposition, such as a product or service, usually for a finite amount of time.
- Reputational damage -> damage to good will. Over the course of time, a commercial entity or an organization will build up a reputation, build up good will with the public, customers, vendors, strategic partners, shareholders or bondholders. If they fail to comply with laws, mandates and regulations, this could be not only temporary damage, but a permanent damage to their reputation
- Loss of licenses -> license is a permit or some certificate granted from some authority. It gives them permissions to own something or use something to conduct a particular action or activity or possibly carry on trade. A license is a permit that endorses an activity, its an official permission and there is many licenses throughout the world. If an organization is non-compliant, they can lose their license temporarily, an extended period of time or permanently.
- Contractual impacts -> e.g. going back to a vendor after non-compliance the vendor can charge more for the service, or if an entity needs to borrow money from the bank or some other lender they can be charged a higher interest rate because of their previous non-compliance. The non-compliance can be a breach of the service level agreement or the master service agreement.

Privacy Considerations

- Confidentiality and privacy are closely related, but privacy is a subset of confidentiality because it relates to information revolving around people so it is more specific.
- Legal implications
- Local/regional, national/global distinctives
- Data subjects (controller vs. processor) -> so certain data subjects like a controller will generally have more access to data than a steward, because a controller responsible for confidentiality, integrity, non-repudiation, availability. Also data processors, how do we protect private and confidential information when someone's doing data processing or running batch jobs or doing data input, so obviously there will be non-disclosure agreements or we may have to tokenize the data in certain high security environments
- Ownership -> for the asset. In a discretionary access control model you can be the owner of the spreadsheet, word doc, or the pdf file or even a database table. When it is discretionary the owner has the ability to assign permissions or views or shares of that data, does that fit into your privacy model
- Data inventory and retention and archiving -> obviously we want to protect data at rest with a cryptographic mechanism. If we are moving data (data in transit) we will use some type of IPSEC tunnel or use TLS1.2 or higher
- Right to be forgotten -> GDPR

Right to Be Forgotten

- According to the EU GDPR: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if one of a number of conditions applies"
- "Undue delay" is typically about a month

- Organizations must also take reasonable measures to validate the person requesting erasure is truly who they say they are or the data subject. We would call that step up authentication, authorization or possibly proofing
- The right to be forgotten merges with people's right to access their personal information
- The right to control one's data is meaningless if people cannot act when they are no longer consent to processing, when there are significant errors within the data, or if they believe information is being stored unnecessarily
- In these cases, an individual can request that the data be erased
- This is not an absolute right as the GDPR walks a fine line on data erasure

Vendor Assessment and Selection

- Penetration testing -> uncommon for normal vendors, if your going to choose AWS as a cloud provider you will not going to get to go and do a penetration test in one of their data centers. But if its part of a larger initiative (e.g. a merger) and your evaluating their security controls, you may be able to do some sort of penetration testing on their organization before the merger is approved
- Right-to-audit clause -> so in a business to business relationship you may be able to audit one of these vendors, specifically if they are part of a mission critical supply chain, you may be allowed to conduct the audit yourself but more likely you will rely on a third-party objective auditor. The vendor will have the audit performed and they will deliver the reports to you or accreditation or certification
- Evidence of internal audits -> they have done this. Highly objective or evidence through accreditation of a auditing firm or some other accountancy organization
- Independent assessments -> if they choose to adhere to PCI DSS because they process credit cards or use a cloud provider so they perform a questionnaire
- Supply chain analysis -> using supply chain risk management techniques and assessments to look at every link in the supply chain for both products and/or services
- Vendor selection
- Due diligence -> before choosing your vendor, doing all proper information gathering, recon, assessments, comparison, even before you enter the negotiation process for the contracts or agreements
- Conflicts of interest -> between you and the potential vendor and maybe your partners and customers.
- Questionaries and templates and surveys -> At the very least for a medium to small sized organizations, to look for missing pieces when establishing vendors
- Rules of engagement -> as you move forward, establish processes and procedures that you go through every time when in the lifecycle when choosing the vendor or supplier. Well defined processes for assessment and selction

Case Study: The CSA Cloud Controls Matrix

- The Cloud Controls Matrix is a cybersecurity control framework for cloud computing that aligns to the Cloud Security Alliance (CSA) best practices
- It is considered the de-facto standard for cloud security and privacy
- There is an accompanying questionnaire, CAIQ, that populates the "STAR" registry and offers a set of "yes or no" questions based on the security controls in the CCM

CCM Controls Matrix v4

-
- Download the CCM v4 there is also a CCM lite for smaller to medium sized organizations that don't want to use all 197 controls. Gives you 1/3 of the controls, but this isn't a spreadsheet format. Will have listing of all the controls, give best practices and guidelines for implementing those controls, guidelines for auditors (CSA also has a cert for cloud auditors so they can use those guidelines in evaluating the organization). Also maps to different things like ISO, NIST and others, and there is a consensus questionaries that the vendor can fill out which is submitted to the CSA and it gets populated into the STAR registry.

Nondisclosure agreements (NDA)

- This is also called a "confidentiality agreement"
- NDAs are legally enforceable contracts that generate a confidential/private relationship between an entity that has sensitive information and an entity who will gain access to that information
- A confidential relationship means one or both parties has a duty not to share that information
- These can be signed:
    - At the outset of a pre-engagement meeting
    - Early in the interview process
    - As part of the hiring and post-termination process
    - In anticipation of a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU)

Memorandum of Agreement

- A Memorandum of agreement is a written document describing a cooperation between two entities that want to work together on a project or an agreed-upon objective
- It serves as a legal document that describes the details of a partnership agreement and is more formal than a verbal agreement but less formal than a contract
- Organizations can use this to establish and outline shared agreements

- An MOA may be used regardless of whether currency will be exchanged as part of the agreement

Memorandum of Understanding

- A memorandum of understanding is a nonbinding agreement that declares each party's objectives in performing a business transaction or initiating a new partnership
    - This form of agreement may also be referred to as a letter of intent (LOI) or MOA
- If a business is in the beginning phases of a transaction with another party, an MOU is often the first step toward a formal agreement via a binding contract
- It openly defines how the parties will work together and what are the mutual expectations and responsibilities
- The goal is to attain a mutual understanding of the partnership so that both parties can move forward into an enforceable contract
- Companies might require a MOA and a MOU before moving into a fully pledged agreement, providing software and whatever other service they offer

Service-level Agreement (SLA)

- A provider must realize that the use of contractual agreements such as hosting/connection agreements and SLAs are used to allocate shared responsibility and risk among both providers and consumers
- An SLA defines the precise responsibilities of the provider and sets customer expectations
- It also clarifies the support system (service desk) response to problems or outages for an agreed level of service (based on support plan)
- The liability for the failure of one or more controls and the realization of risk can be appropriately documented and understood by all involved parties

Master Service Agreement (MSA)

- An SLA is also called a master service agreement
- As part of due diligence in the business continuity plan (BCP), one should confirm any/all expectations with the candidate service provider and ensure that they are documented in your MSA/SLAs
- An MSA is a contract two parties enter into during a service transaction
- This agreement details the expectations of both parties
- The goal of a master service agreement is to make the contract process faster
- It also should make future contract agreements simpler

Work Order (WO)

- A work order is a document that delivers all the information about an ongoing maintenance task and outlines a process for completing that activity
- Work orders can include details regarding:
    - Who authorized the job
    - The scope
    - Who the job/task is assigned to
    - What are all expectations (delivery time or date)

Statement of Work (SOW)

- This is an agreement that establishes the expectations for a project or program and aligning the team(s) involved
- Details should clarify price, cost, timeline, deliverables, process, expectations of requirements, invoicing schedules, and much more, depending on the scope and breadth of the project

- Basically, an SOW is a document of agreement between a client and service or agent defining the scope and details of a project
- It is among the first documents you will use to establish the framework of a project before entering the planning and execution stages

Business Partnership Agreement (BPA)

- A BPA establishes rules for two or more parties going into business agreement together
- It is a legally binding document that outlines every detail of the business operations, ownership stakes, financials, accountabilities, and decision-making approach and strategies
    - General partnerships
    - Limited partnerships
    - Limited liability partnerships
    - Limited liability limited partnerships

Audits, Assessments, & Awareness

Internal Audit and Attestation

- An internal security audit operates by attesting that all organizational information systems are adhering to a set of internal or external criteria regulating data security, network security, and infrastructure security
- Internal criteria include the company's IT policies, procedures, and security controls
- Internal audit should objectively assess the organization's overall strategy for handling emerging threats from a governance, architectural, operational, and technology standpoint

Security Audit Committees

- The audit committee is responsible for assisting independent auditors to examine the organization's security reporting system in a process independent of management by:
    - Offering critical oversight of the corporation's reporting processes, internal controls, and independent auditing
    - Providing checks and balances, for example choosing certain supervisors or security managers who audit other division or other areas of the company internally
    - Allowing a forum for discussing security concerns candidly and objectively
- An audit committee is typically appointed by the board and is composed of directors who are not part of management

Duties of Internal Audit Committees

- Risk oversight
- Ethics and compliance
- Oversight of independent auditors
- Oversight of internal audit
- Manage controls and reporting

Self-assessment Audits

- The self-assessment with independent validation (SAIV) approach is a more cost-effective assessment solution
- The organization's internal audit activities leverage a capable, independent validator who is well versed in security assessment methodology
- The goal is to deliver an independent validation of the internal audit activity's self-assessment
- In addition to reviewing the self-assessment, the validator also confirms work completed by the self-assessment team and interviews senior management

External Audit and Attestation

- Internal audit and attestation would be the best approach, least costly approach, but it isn't always the most objective approach and for many organizations they don't have a choice, they must allow external auditing and attestation in order to be accredited or certified
- In an external audit, an organization compares itself to an established standard
    - ISO 27001 is an example of a compliance audit with a certification as the result
    - CSA certifies auditors for cloud security, and they use the Cloud Controls Matrix (CCM)
- The level for audits can be further segmented based on the agreed-upon procedures that are involved in the scope

Audits vs. Assessments

- There is technically a difference between an assessment and an audit
- An assessment could be seen as an "audit plus"
- Assessments compare with both standards and industry practices, the auditor's knowledge and experience, etc.
- For example, Payment Card Industry Data Security Standard (PCI DSS) is an audit, but organizations are required to go through a penetration test as well, which is an assessment
    - Therefore, PCI DSS can also be called an assessment

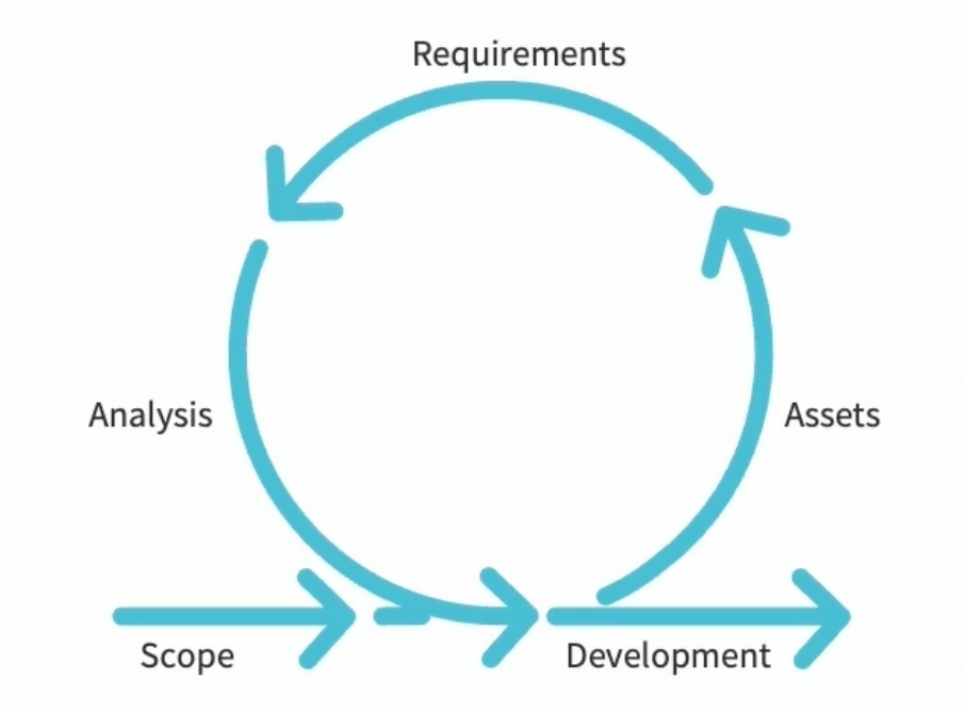
Security Examinations

- Security examinations are used to certify security professionals at various experience levels to participate in auditing and assessments
- Common examples of security examinations are:
    - CompTIA Security+
    - CompTIA Advanced Security Practitioner (CASP+)
    - Certified Information Systems Security Professional (CISSP) from ISC^2
    - Certified Information Security Manager (CISM) from ISACA

Independent Third-parties

- The audit of information security is a comprehensive assessment that evaluates, often with gap analysis, the current state of security controls in the organization, and offer solutions to those issues made aware
- It enables the planning of timely actions to raise the level of difficulty or resistance to threat agents
- When applied to DevSecOps, a third-party security audit is an exhaustive assessment of all code, documentation, and processes related to a software system by an independent security firm
- The goal of an audit is to uncover potential security risks which can then be patched by the software's developer

Independent Third-party Audit Process



-
- Once independent third-party auditor from the meeting understands the scope of the audit and assessment, it will then evaluate all the assets, understand the requirements for securing those assets and an analysis of the existing technical, physical, administrative or managerial and operational controls and then do a deep dive into the development process looking for gaps, weaknesses and vulnerabilities and then reporting back to the organization with potential countermeasures or additional controls to raise difficulty or resistance to threat actors

Penetration Testing

- Penetration testing is a process used to collect information and actively expose vulnerabilities in a system or application by conducting actual exploits and red team attacks

- Penetration testing is conducted as a known environment(white-box), partially known environment(grey-box), or unknown environment(black-box), where the tester assumes the attacker role to discover vulnerabilities and weaknesses
- Pentesting can be launched against physical, technical, and/or logical controls
- Penetration testing can also be useful for determining:
    - How well the system tolerates real-world-style attack patterns
    - The likely level of sophistication an attacker needs to successfully compromise the system
    - Additional countermeasures that could mitigate threats against the system
    - The defenders' ability to detect attacks and respond appropriately

Penetration Testing Attributes

- Known, partially known, vs. unknown environment
- Credentialed vs. non-credentialed
    - Guest user credential
    - Privileged user credential
- Offensive (red team, threat hunting) vs. defensive (blue team)
- Integrated with vulnerability assessments, incident response testing, and other decision-making initiatives
- Intrusive vs. non-intrusive
- Passive(scanning) vs. active(leaving a mark)

Penetration Test Life Cycle

1. Rules of engagement agreement -> meeting where the attackers determine the scope, areas that are off limits, exceptions, exemptions. Is there a bug bounty for a vulnerability or gap in security controls. Is it a know all, know some, know nothing. If it is a no nothing step 2 will be a lot more because unless the attacker knows or the information is in the engagement meeting the more recon and information gathering they must do
2. Reconnaissance and initial engagement
3. Step 3: Privilege escalation -> once they get access to a system, service or application they will try elevating their privileges or move laterally off other systems that have open ports or trust relationships
4. Step 4: Lateral movement and pivoting -> try to distribute throughout the VLAN, call center, corporate LAN, wireless VLAN
5. Step 5: Persistence -> install persistent code that can evade anti-virus or anti-malware tools, stealthy polymorphic code that can RAM memory or encrypt itself or compress itself and move to lower levels of a directory. Also, persistent so the threat actor will try different vectors or modes to be successful
6. Step 6: Cleanup -> during lateral movement and pivoting and persistence they are probably deleting logs, disabling services so at the end of the test they have to cleanup there mess and go back to a recovery point to leave all their systems, applications and services in a state before they began their test. This also involves making recommendations to the client or security solutions to improve their security posture and be a more mature organization so next time they will be more resistant to assessments and tests

Penetration Testing Frameworks

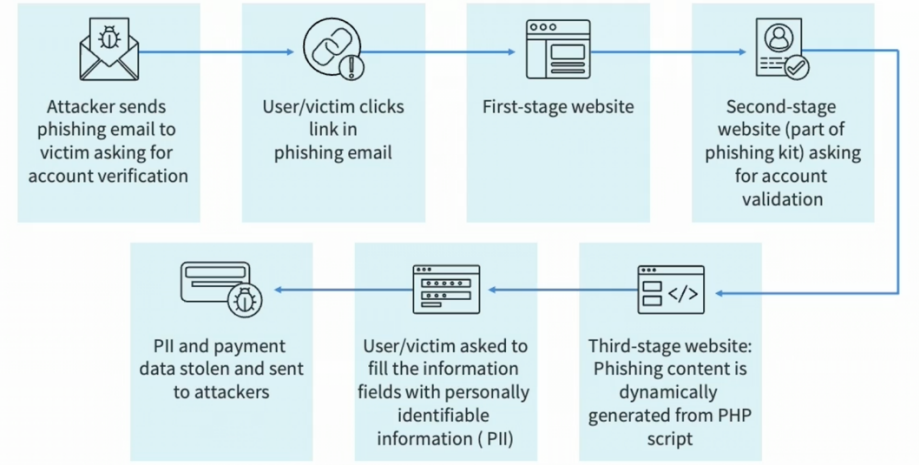
- SSAF – framework provided by Open Information Systems Security Group (OISSG); a not-for-profit organization based in London
- OSSTMM – open-source security testing created by Institute for Security and Open Methodologies (ISECOM)

- OWASP – popular methodology used widely by security professionals, created by a non-profit organization focused on advancing software security
- PTES – Penetration Testing Execution Standard (PTES) methodology was developed to cover the key parts of a penetration test
- NIST – National Institute of Standards and Technology (NIST) provides a manual that is best suited to improve the overall cybersecurity of an organization

User Guidance and Training Topics

- Password polices and self-management of passwords -> including the use of tokens and registering biometrics, often automated
- Policy documents and handbooks -> those that are published to the intranet or human resource sites or in physical format
- Situational awareness -> how to respond where you see someone on your floor without a badge or someone who is unfamiliar
- Insider threats and use of honey tokens -> reporting to security guards, security operations center, or supervisors when your aware of unauthorized use or violations of a AUP. Letting employees know that management may use honeytokens or honeyfiles as a part of data loss prevention or to expose illegal activities or violations of the AUP
  Hybrid/remote work environments -> and what are their expectations as remote workers. Giving employees the awareness that you might be using user behavioral analysis and other ML tools to monitor their activities both onsight or remote
- Anomalous behavior and social engineering -> awareness to different social engineering campaigns that might be launched e.g. mock phishing campaign
- Removable media and cables
- Operational security -> with the goal of continual improvement

Phishing Attack



-
- Most organizations might formulate a mock phishing campaign to simulate a phishing attack against their own employees to enhance and increase security awareness so in this case the attacker is actually your own security operations center or security team, it may be a penetration testing team that sends phishing email to the employees often asking them to verify their account, the corporate emails will be strategic and well crafted. They'll look just like a corporate email from someone else in the organization or one of your vendors, partners or customers. The end-user clicks on a link in the email which sends them to a first stage website. This is a mock website that you can create, in rapid 7 for example by using a wizard driven tool. The second stage will ask for

some information and the third stage will dynamically generate a PHP script (most common) then the user will fill in some information offering some PII or other intellectual property. If this were a real attacker, the information (data) will be stolen and possibly go through an intermediate bot to a command and control server or to some campaign center on the dark web

Phishing Campaigns

- A phishing campaign is an email hoax designed to replicate a real attack against employees as part of security awareness training
- This is a critical exercise since cybercriminals use phishing, the fraudulent attempt to obtain sensitive information such as intellectual property, credentials, and credit card details by spoofing a trustworthy organization or reputable partner in an email communication
- These initiatives are used to support security training for new hires and ongoing anti-phishing awareness for all stakeholders
- The goal is not to entrap and punish employees but rather raise awareness and instruct

Security Training Monitoring and Reporting

- Security training monitoring and reporting must be scoped to the specific audience to deliver different types of security training:
    - Basic security awareness training
    - Technical security training
    - Security management training
    - Compliance training

Security Training Monitoring

- Regardless of the training modality, participants should be able to answer surveys and evaluations about all aspects of the experience
- Participants should also be provided with an avenue for giving open-ended subjective feedback
- The Net Promoter Score (NPS) is considered the gold standard customer experience metric
- In this context, the NPS score measures participant loyalty by looking at their probability of recommending a given security training experience
- NPS scores are measured with a single-question survey and reported with a number ranging from -100 to +100, where a higher score is desirable

Security Training Reporting

- The NPS score evaluation would only be a part of the reporting process
- Often peer and supervisory evaluations should be performed to offer valuable critique and reinforcing feedback to the one delivering the training
- This evaluation should also include the origin content, graphical representations, test questions, and various modalities of the training
- All reporting best practices mentioned in this Security+ training should be considered