Computer Network and Network Security

OSI layers

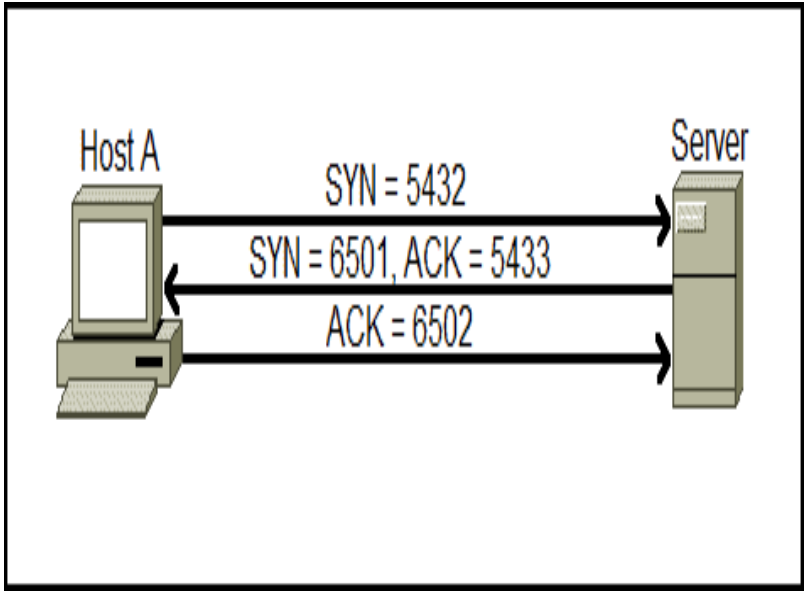
Layer	Function
Application Layer	Providing interface between user and Computer. **Example Protocols**: HTTPS,SMTP,FTP etc..
Presentation Layer	Gets the data from Application layer and perform Translation(ASCII to HEX) ,Data Compression, Encoding/Decoding and Encryption/Decryption. **Protocols: SSL/TLS,JPEG,MPEG**
Session layer	Responsible for establishing, maintaining, and terminating communication sessions between devices. **Protocols**: RPC, NetBIOS
Transportation Layer	Responsible for the end-to-end delivery of data between devices. It provides reliable data transfer, flow control, and error recovery. Protocols: TCP/UDP
Network layer	Responsible for delivery of data between devices on different networks. Routing data packets between networks, and managing congestion. Routers and Firewalls uses are the devices used in this layer
Data Link Layer	Responsible for host to host delivery of data. Dividing the data into frames, adding error detection and correction codes. Switch uses in this Layer
Physical layer	Responsible for physical transmission of data between devices

TCP 3-Way handshake

- Step 1: The client sends a SYN (synchronize) packet to the server with an initial sequence number (ISN). The SYN packet informs the server that the client wants to establish a connection

- Step 2: The server receives the SYN packet and responds with a SYN-ACK (synchronize-acknowledge) packet. Which means server is willing to establish a connection. The same Packet Contain Server own SYN packet.

- Step 3: The client receives the SYN-ACK packet and sends an ACK (acknowledge) packet to the server SYN packet and completes the three-way handshake.



TCP header

Important Fields in TCP Header:

Source Port
Destination Port
Sequence Number
Acknowledgment Number
Window Size

Control Flags (6 bits):

SYN (Synchronize): This flag is used to initiate a connection between two devices

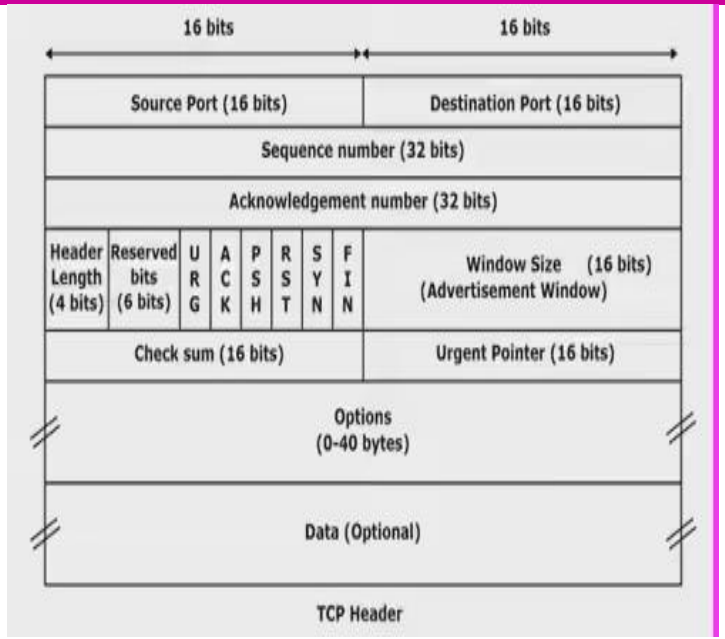
ACK (Acknowledgment): This flag is used to acknowledge the receipt of a packet

FIN (Finish): This flag is used to terminate a connection between two devices.

RST (Reset): This flag is used to reset a connection that has been terminated abruptly.

URG (Urgent): This flag is used to indicate that the data in the packet is urgent and should be processed immediately.

PSH (Push): This flag is used to indicate that the data in the packet should be pushed to the receiving application immediately



Explain IP header

Important Fields in IP Header:

Version (4 bits): The version field specifies the version of the IP protocol being used

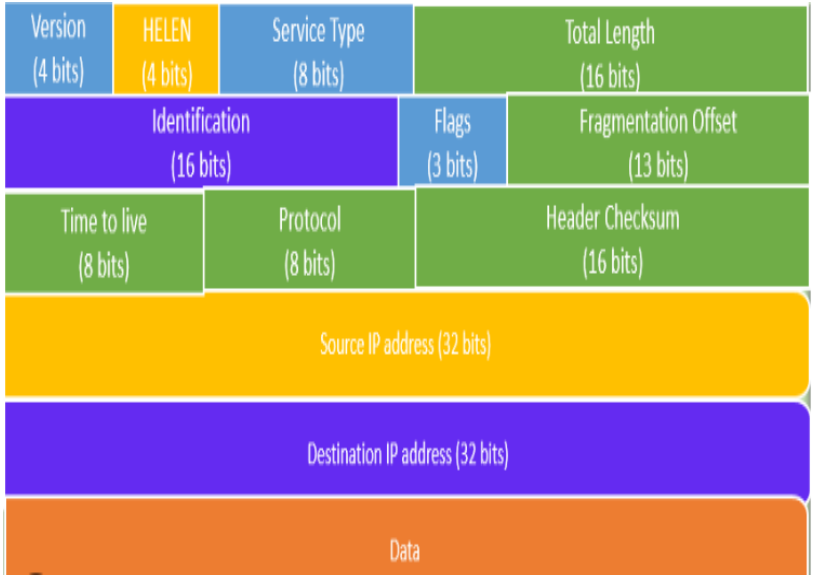
Time-to-Live : The time-to-live field is used to limit the lifetime of the IP datagram

Protocol: Indicates the protocol used in the data portion of the datagram, such as TCP, UDP, ICMP, or IGMP.

Header Checksum (16 bits): The header checksum field is used to ensure the integrity of the IP header.

Source IP Address (32 bits): The source IP address field identifies the sending device's IP address.

Destination IP Address (32 bits): The destination IP address field identifies the receiving device's IP address.



Can you explain Difference between TCP and UDP

TCP	UDP
TCP is a connection-oriented protocol. (Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.)	UDP is Connection less (This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission)
TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP
TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
An acknowledgment segment is present.	No acknowledgment segment.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Classes of IP address

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.

Class D IP Address Range: This range IP addresses are not allocated to hosts and are used for multicasting
Class E IP addresses: This Range IP address are reserved for research purposes

Private IP address range

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

DHCP and How it works

DHCP (Dynamic Host Configuration Protocol) used to automatically assign IP addresses and other network configuration **parameters (subnet masks, default gateways)** to devices on a network**.**

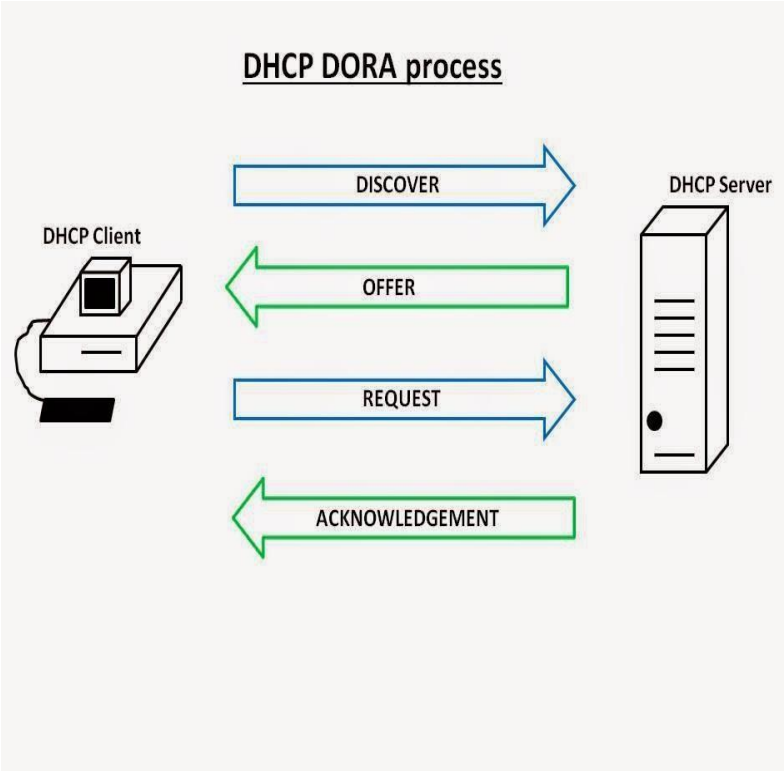
DHCP works on process called DORA

When a device connects to the network, it sends a DHCP Discover Message to the DHCP server

DHCP Server responds with a DHCP offer containing the available IP address, subnet mask, default gateway, and other configuration parameters.

If the device accepts the DHCP offer, it sends a DHCP request to the DHCP server to confirm the assignment of the IP address and other network settings

The DHCP server then sends a DHCP acknowledgement to the device, which confirms the assignment of the IP address and other network settings.

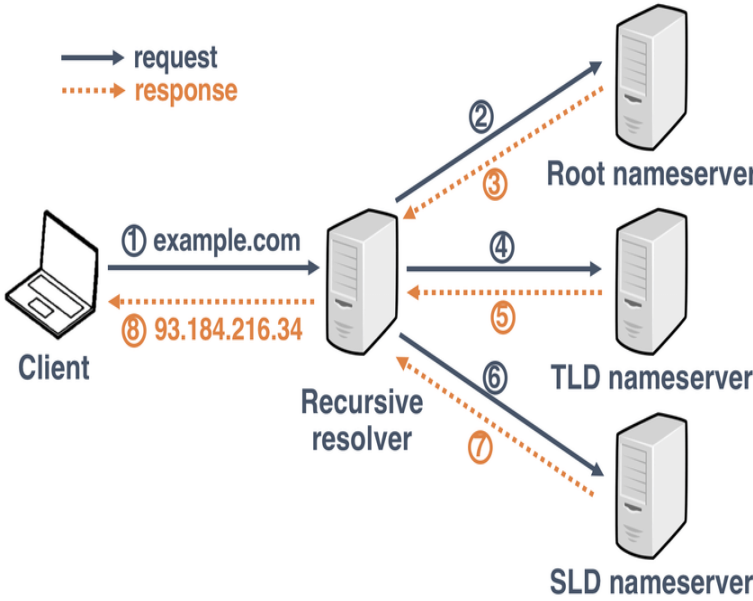


DNS Server and How it works?

A DNS (Domain Name System) server that translates domain names **(e.g. www.example.com)** into IP addresses (e.g. 192.0.2.1)

- When you type a domain name into your web browser, your computer sends a request to a DNS Server(resolver) to look up the IP address associated with that domain name. If DNS server finds IP address it return to you. if not Following Process happens.

- The DNS Server (resolver) then queries a series of DNS servers, starting with the root servers. Root servers have the Top level domains (TLD's) information.
- Top level domain (TLD) shares IP address of authoritative DNS server for that domain name.
- The authoritative DNS server(SLD) is responsible for maintaining the DNS records for the domain, which include the IP address of the web server.
- Once the authoritative DNS server is located, the DNS resolver caches the IP address and returns it to your web browser.
- Now the client Computer uses the IP address to establish a connection with website or domain.

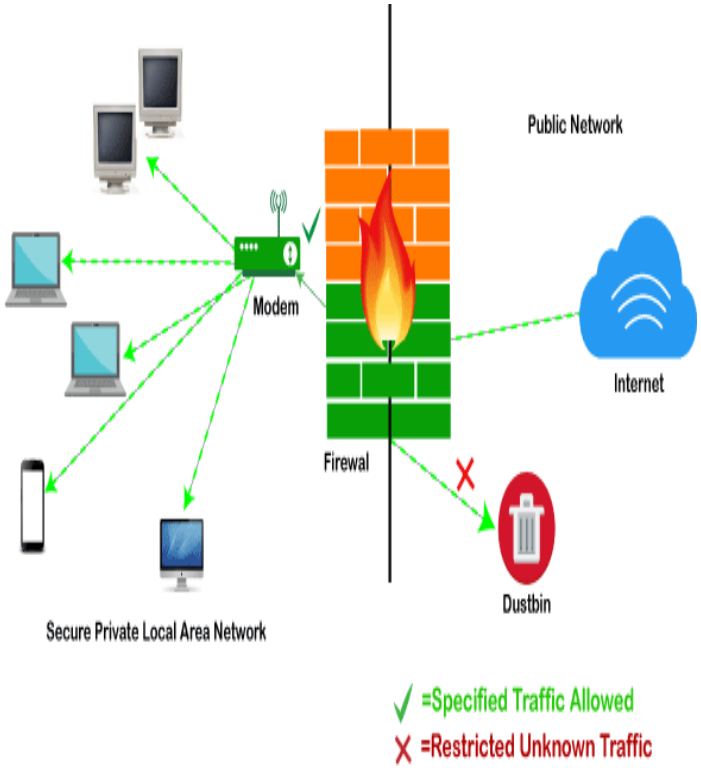


What is Firewall? What is Stateful Inspection in Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on a set of predefined security rules. It acts as a barrier between an internal network and the Internet or other external networks to prevent unauthorized access to or from the network.

Stateful inspection is a firewall technology that monitors and manages network connections by keeping track of the state of each connection and only allowing traffic that is part of an established connection.

Stateful inspection firewalls provide enhanced security compared to traditional packet filtering firewalls, as they can identify and block various types of attacks.



Difference Between Traditional Firewall VS Next generation Firewall

Traditional Firewall:

Traditional firewalls operate at the network layer (Layer 3) and transport layer (Layer 4) of the OSI model

They are designed to block or allow traffic based on IP addresses, port numbers, and protocols.

Less sophisticated than next-generation firewalls (NGFWs) and lack advanced features such as application control, intrusion prevention, and deep packet inspection.

Next generation Firewall:

NGFW operates at multiple layers of the OSI model, including the application layer (Layer 7).

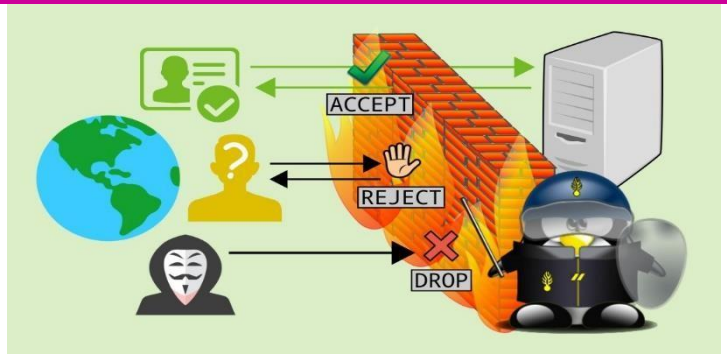
NGFWs are more sophisticated than traditional firewalls and are better able to detect and prevent advanced threats such as malware, zero-day exploits, and targeted attacks.

What is Difference between Firewall Deny and Drop

Firewall Deny: When a firewall is configured to "deny“ (Reject) traffic, it sends a response to the sender indicating that the traffic is not allowed and should be blocked

Firewall Drop:

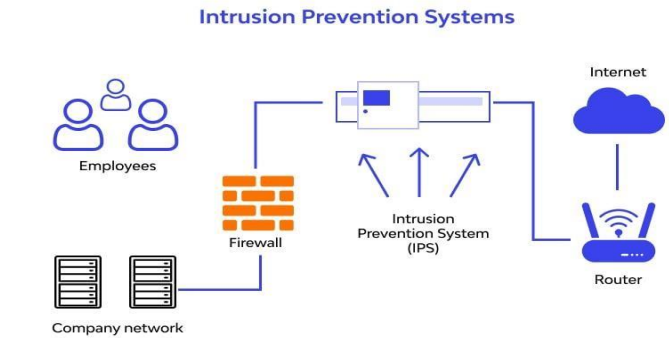
when a firewall is configured to "drop" traffic, it silently discards the traffic without sending any response to the sender.



Q13: What is IDS/IPS

IDS stands for Intrusion Detection System. An IDS monitors network traffic based on Signatures for signs of suspicious activity or attacks. When it detects suspicious activity, it generates an alert.

IPS stands for Intrusion Prevention System. An IPS also monitors network traffic for suspicious activity and actively blocking any traffic that is deemed to be malicious or unauthorized.



What is HIPS and NIPS and Difference Between Them

HIPS:

HIPS stands for Host-based Intrusion Prevention System.

HIPS runs on individual computers or servers and monitors their behavior for signs of malicious activity.

HIPS can detect and block malware, unauthorized access attempts, and other types of attacks on hosts.

NIPS:

NIPS stands for Network-based Intrusion Prevention System.

NIPS monitors network traffic for signs of malicious activity

NIPS can detect and block attacks such as distributed denial of service (DDoS) attacks or attempts to exploit vulnerabilities

Difference between Firewall and IPS

Firewall:

A firewall is a network security device that is used to monitor and control incoming and outgoing network traffic.

Firewalls can be hardware or software-based, and they are typically used to protect against known network attacks, such as denial-of-service (DoS) attacks, malware, and unauthorized access attempts.

IPS:

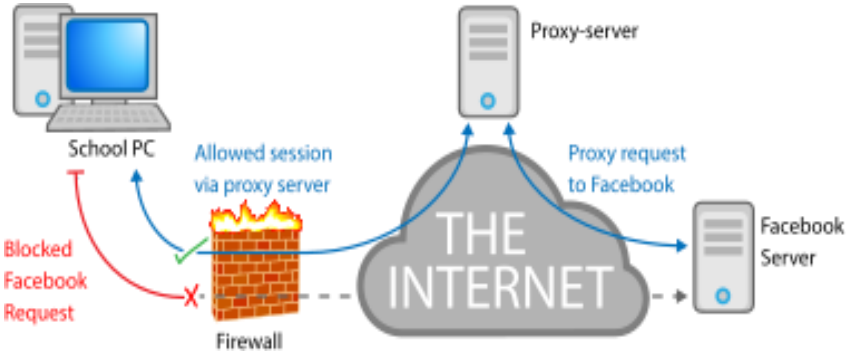
IPS system is a security measure that actively monitors network traffic for potential threats, and it has the capability to prevent those threats from succeeding.

IPS systems can detect and block attacks in real-time, using a combination of signature-based and behavior-based analysis

IPS systems are more adaptive and can respond to new and emerging threats in real-time.

What is Proxy server and Types

A proxy server is an intermediary server between a client (such as a web browser) and a server (such as a website or application server). When a client makes a request for information, the request is first sent to the proxy server, which then forwards the request to the server on behalf of the client.



Types of Proxy servers

1. Forward proxy: A forward proxy is used by clients to access websites or services on the Internet.
2. Reverse proxy: A reverse proxy is used by servers to receive requests from clients on the Internet and forward them to backend servers.
3. Transparent proxy: A transparent proxy intercepts and forwards traffic without requiring any configuration changes on the client side.

Protocols and Port Number

Protocol	Description	Port number
FTP(data)	File Transfer Protocol (Data transfer)	20
FTP(Control)	File Transfer Protocol (Control Connection)	21
SSH	Secure Shell	22
Telnet	Telnet protocol—unencrypted text communications	23
SMTP	Simple Mail Transfer Protocol	25
DNS	Domain Name System	53
DHCP	Hypertext Transfer Protocol (HTTP)	67,68
HTTP	Hypertext Transfer Protocol (HTTP)	80
POP3	Post Office Protocol	110
NTP	Network time protocol	123
NetBIOS	NetBIOS name service and Session Service	135-139
IMAP	Internet Message Access Protocol (IMAP)	**143**
SNMP	Simple Network management Protocols	161,162
LDAP	Lightweight Directory Access Protocol	389
RDP,HTTPS	Remote desktop Protocol, Hypertext Transfer Protocol Secure (HTTPS)	3389,443

Windows and Linux commands

1. **Ping**: A command to check if a computer or server is online and can be reached.

```
ping <hostname or IP address>
```

For example:

```
ping google.com
```

2. **Traceroute (tracert on Windows):** Determines the path that network packets take from the source to the destination. It helps identify intermediate hops and possible points of failure.

```
tracert google.com
```

```
Tracing route to google.com [172.217.168.174]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    10 ms     8 ms     9 ms  10.10.10.1
  3    10 ms     9 ms    11 ms  203.0.113.1
  4    14 ms    15 ms    13 ms  203.0.113.254
  5    13 ms    14 ms    13 ms  72.14.198.202
  6    15 ms    16 ms    16 ms  108.170.253.177
  7    20 ms    21 ms    20 ms  108.170.253.178
  8    17 ms    17 ms    16 ms  209.85.245.94
  9    16 ms    16 ms    17 ms  216.239.43.237
 10    17 ms    17 ms    17 ms  209.85.243.203
 11    16 ms    17 ms    16 ms  172.217.168.174

Trace complete.
```

https://t.m

Windows and Linux commands

nslookup (Windows) / dig (Linux): Both commands are used to query DNS (Domain Name System) servers to look up DNS records like A, CNAME, MX, etc., for a given domain or hostname.

```
nslookup google.com
```

```
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  172.217.167.78
          2607:f8b0:4004:815::200e
```

netstat: Displays network statistics and active ports, established connections, and listening services on a system.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    192.168.1.10:49714     151.101.1.69:443       ESTABLISHED
  TCP    192.168.1.10:49715     172.217.167.132:443    ESTABLISHED
  TCP    [::]:80                [::]:0                 LISTENING
```

arp: Helps find the physic work (arp -a (Windows) and arp -n (Linux))

```
Interface: 192.168.1.10 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c4-6e-1f-54-a2-95     dynamic
  192.168.1.100         00-1f-29-4b-52-87     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Windows and Linux commands

ifconfig (Linux) / ipconfig (Windows): Used to view and configure network interfaces, including IP addresses, netmasks, and gateways.

- **Type in Windows CMD – ipconfig** -Example Output

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : example.com
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

in Linux:

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe41:6557  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:41:65:57  txqueuelen 1000  (Ethernet)
        RX packets 35018  bytes 26038056 (24.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3980  bytes 284450 (277.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

SSH: Secure Shell protocol used for remote access to systems securely.

```
$ ssh john@192.168.1.100
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be establishe
ECDSA key fingerprint is SHA256:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.100' (ECDSA) to the list of known host
john@192.168.1.100's password: ********
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

[... MOTD and system information ...]
```

Q17: Protocols and Port Number

ls: Lists the contents of a directory, showing files and directories in the specified location.

df: Displays information about disk space usage on the file system.

chmod: Changes file permissions, allowing you to control who can read, write, or execute files.

find: Searches for files and directories in a directory hierarchy based on various criteria such as name, type, size, etc.

cat: Concatenates and displays the contents of a file. It is often used to view log files or text-based configurations,

grep: A command used for pattern searching within files or command output. It is helpful for filtering information and searching for specific strings.

ps: Displays information about running processes, including their Process ID (PID), CPU and memory usage, and other details.

CIA Triad

CIA triad is a widely recognized model for information security, consisting of three core principles: confidentiality, integrity, and availability.

Confidentiality:

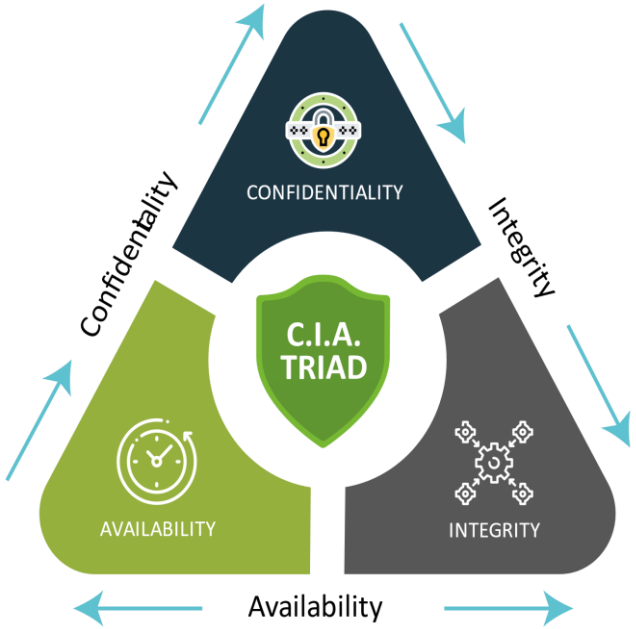
- Confidentiality ensures that only authorized individuals or systems can access sensitive information.
- Confidentiality achieved through the use of access controls, encryption, and other security measures.

Integrity:

- Data integrity ensures that information is not modified or tampered with in an unauthorized manner.
- Integrity achieved through the use of checksums, digital signatures, and other security measures.

Availability:

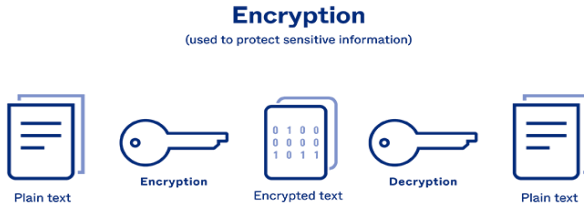
- Availability ensures that information and systems are accessible and functional when required.
- Availability achieved through redundancy, fault tolerance, and other resilience measures.



Encryption& Decryption? Types of it

Encryption : Encryption is the process of converting plaintext (unencrypted data) into ciphertext

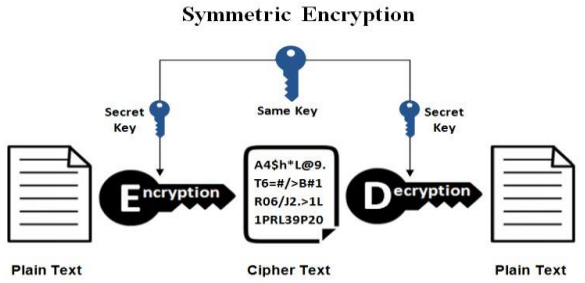
Decryption: Decryption is the process of converting ciphertext (encrypted data) back into plaintext (unencrypted data) using a decryption key



Types:

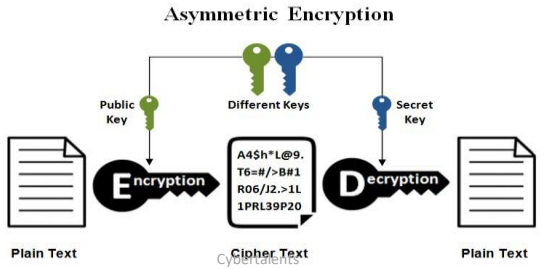
Symmetric encryption:

- In symmetric encryption, the same key is used to both encrypt and decrypt data.
- Examples of symmetric encryption algorithms include Advanced Encryption Standard (AES),
- Blowfish, and DES.



Asymmetric encryption:

- In asymmetric encryption, also known as public-key encryption, two keys are used – a public key and a private key (Secret key)
- The public key is used to encrypt the data, while the private key is used to decrypt it.



What is Hashing

Hashing:

- Converts plaintext data of any length into a fixed-length string of characters, called a hash value or message digest
- To ensure the integrity of data, the hash value of the data is calculated and compared to a known hash value. If the hash values match, it can be assumed that the data has not been tampered with. If the hash values do not match, it indicates that the data has been modified, and the integrity of the data has been compromised.
- Some common hashing algorithms include MD5, SHA-1, SHA-2, and SHA-3 and SHA-256

Types of Hackers

1. **White hat hackers**: Also known as ethical hackers, they are hired by organizations to identify and fix security vulnerabilities in their systems.

2. **Black hat hackers:** They are hackers who exploit security vulnerabilities in systems for their own gain, usually for financial or personal reasons.

3. **Grey hat hackers**: They are hackers who use their skills to find vulnerabilities in systems but do not intend to cause any harm. They may notify the system owner of the vulnerability, but they may also use it to gain unauthorized access.

4. **Hacktivists**: They are hackers who use their skills to promote a social or political cause. They often target organizations or government agencies to raise awareness or to protest against their policies.

5. **Script kiddies**: They are individuals who use pre-packaged tools and scripts to launch attacks without necessarily understanding the underlying technology.

6. **State-sponsored hackers**: They are hackers who work for or on behalf of a government or a state agency to carry out cyber espionage or other malicious activities.

Difference between Encoding, Encryption and Hashing

Encryption	Encoding	Hashing
Encryption is a security technique used to protect data confidentiality by converting plaintext (readable data) into ciphertext (unreadable data) using an encryption algorithm and a secret key.	Encoding is a process used to convert data from one format to another for the purpose of data integrity and transmission.	Hashing is a one-way cryptographic technique used to generate a fixed-length string of characters (hash value or digest) from any input data of arbitrary size
The primary goal of encryption is to ensure that only authorized parties can decrypt and access the original data..	It is not primarily a security measure but rather a method to represent data in a different, more suitable format for storage or transmission (e.g., converting special characters to their HTML entities in web pages).	The primary purpose of hashing is data integrity verification and fast data retrieval, such as in data indexing
Appropriate Keys are used in the Encryption.	No Keys are used in Encoding.	No Keys are used in Hashing.
Encryption can be reversed back to its original form by using appropriate keys.	Encoding can be reversed back to its original form.	The hashed one cannot be reversed back to its original form.
Example: AES Algorithm, RSA Algorithm, Diffie Hellman	**Example:** BASE64, UNICODE, ASCII, URL Encoding.	**Example:** MD5, SHA256, SHA – 3.

What is Malware and Types

Malware, short for "malicious software," refers to any software designed to cause harm or damage to a computer system or network. Malware can be created for various purposes, including stealing sensitive data, gaining unauthorized access, and disrupting normal computer operations.

Here are some common types of malware:

1. Virus: A virus is a program that can replicate itself and spread from one computer to another by attaching itself to a host file.
2. Trojan: A Trojan is a program that appears to be legitimate but actually contains malicious code that can be used to steal data or gain unauthorized access.
3. Worm: A worm is a self-replicating program that can spread through a network, often consuming large amounts of bandwidth and causing damage to the network.
4. Ransomware: Ransomware is a type of malware that encrypts files on a system, making them unusable, and demands payment in exchange for the decryption key.
5. Adware: Adware is a type of malware that displays unwanted advertisements on a user's computer, often in the form of pop-ups or browser redirects.
6. Spyware: Spyware is a type of malware that can track a user's online activity, steal sensitive data, and transmit it back to a third party.
7. Rootkit: A rootkit is a type of malware that can hide its presence on a system by modifying the operating system or other software components.

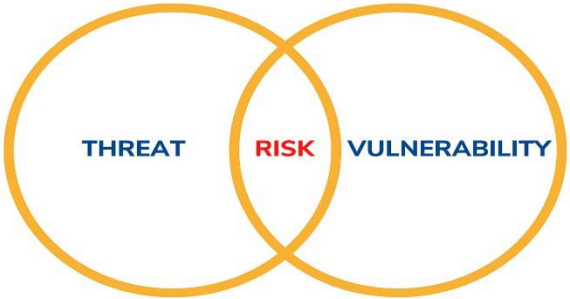
What is Threat, Vulnerability and Risk

Threat: A potential danger or risk to a system or organization.

Examples: Malwares..

Vulnerability: A weakness in a system that can be exploited by a threat actor.

Risk: A risk is the likelihood of a threat exploiting a vulnerability and causing harm or damag to a system or organization



What is Zero-day Attack

Zero day: A vulnerability that is unknown to the software vendor or security community, and for which no patch or mitigation strategy is available

What is Exploit and payload

Exploit: A piece of software or code that takes advantage of a vulnerability to gain unauthorized access to a system or data.

Payload :A payload is software used by an attacker to reach the attack objectives. Depending on the attack objectives, the payload contain malicious software that would allow the attacker to access sensitive data or cause harm to the organization.

Difference Between Virus, Worm &Trojan

VIRUS	WORM	Trojan Horse
Behavior: A virus is a type of malware that attaches itself to a legitimate program or file and replicates by infecting other programs or files..	Behavior: A worm is a self-replicating malware that spreads across networks and systems without needing human intervention	Behavior: A Trojan is a type of malware that disguises itself as a legitimate program or file to deceive users. Once installed or executed, it may perform malicious actions on the victim's system without their knowledge.
Infection Method: Viruses rely on users executing infected files or programs to spread. They can also spread through infected email attachments, removable media (e.g., USB drives), or infected downloads.	They can spread rapidly through the internet or local networks without any human intervention.	Infection Method: Trojans typically do not self-replicate like viruses or worms. Instead, they rely on social engineering to trick users into installing them, often through fake software downloads or email attachments.
Payload: Viruses often have a harmful payload that can damage or alter the infected system or files. Their primary goal is to replicate and spread.	Payload: Worms may or may not have a destructive payload. Their primary objective is to spread and infect as many systems as possible.	Payload: Trojans can have a wide range of payloads, including stealing data, providing remote access to an attacker, and more. Their primary goal is to remain hidden while carrying out malicious activities.
Example: The "ILOVEYOU" virus is a famous example of a computer virus that spread through email attachaments and caused extensive damage.	Example: The "Blaster" worm (also known as MSBlast or MS32.Blaster) targeted a Windows vulnerability and spread quickly through the internet in 2003. T https://t.me/learningnets	Example: The Zeus Trojan (Zbot) is a well-known example that targeted online banking users, capturing their login credentials and financial information.

What is Event, Alert and Incident

Event: Event refers to Activity that takes place in a system, network, or application that can be logged or detected by security monitoring tools.

Event Example :

A user logs into a system with valid credentials. This is a normal and benign event that is logged for auditing purposes.

Event Example:

A user attempts to log into a system with invalid credentials multiple times. This event may trigger an alert, as it could indicate a brute-force attack or a credential-stuffing attack

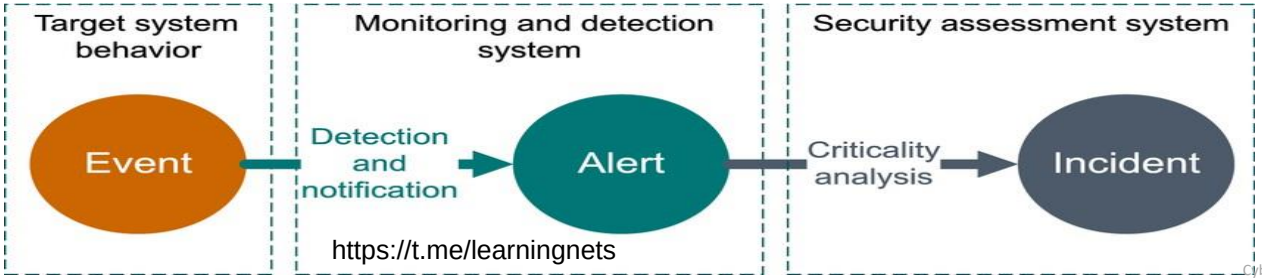
Alert: Alert is generated when the event is appears to suspicious or anomalous.

Alert Example: A security monitoring tool detects a suspicious network connection from an IP address in a high-risk country.

Incident: An incident is a confirmed or suspected security breach or threat that has been identified and requires immediate response and remediation

Example: A user's account is compromised, and sensitive data is stolen. This is a confirmed security breach that requires immediate response and remediation

Example: A ransomware attack encrypts critical files on a company's network. This is a confirmed security incident that requires immediate response and remediation



What is TP, FP,TN and FN

True Positive (TP):

when an alert or event is correctly identified as a security incident or threat.

For example, if an intrusion detection system alerts the SOC to an attempted breach, and the alert is confirmed as a genuine attack, this is a True Positive.

False Positive (FP):

when an alert or event is triggered, but it is not actually a security incident or threat.

For example, if a security system identifies an authorized user as an attacker and generates an alert, this would be a False Positive.

True Negative (TN):

when an event or activity is correctly identified as benign and not a security incident or threat.

For example, if a security system logs a legitimate user accessing a system with valid credentials, and no threat or attack is detected, this is a True Negative.

False Negative (FN):

When a security incident or threat goes undetected or unreported.

For example, if an attacker successfully compromises a system or network, and the security system does not generate an alert or event, this would be a False Negative.

Note : In summary, True Positives and True Negatives in a SOC indicate effective threat detection and response, while False Positives and False Negatives indicate room for improvement in the security systems or processes

What is IOC and IOA ?

IOC:

IOC stands for "Indicators of Compromise."

IOCs are pieces of evidence that suggest a security breach has occurred or is currently ongoing.

IOCs can include IP addresses, domain names, file hashes, URLs, and other forensic artifacts that indicate malicious activity.

IOA:

IOA stands for "Indicators of Attack."

IOAs are patterns of activity that suggest an attacker is attempting to compromise a system or network.

Unlike IOCs, which are specific pieces of evidence, IOAs are more abstract and focus on identifying malicious behavior or actions.

Example of an IOA:

Scanning for vulnerable web servers using tools like Nmap or Shodan.

Attempting to upload a web shell or other malicious code to the target system.

What is Data Leakage ?

Data leakage means the unauthorized transmission of data from an organization to an external recipient.
This can occur through intentional or unintentional means, such as:

Accidental leakage: The authorized entity sends data to an unauthorized entity accidentally.
Malicious insiders: The authorized entity intentionally sends data to an unauthorized entity.
Electronic communication: Hackers make use of hacking tools to intrude the system.
Social engineering: Attackers may use social engineering tactics, such as phishing or pretexting, to trick employees into revealing sensitive data or granting access to systems or networks.

What is BOT and BOTNET ?

BOT:
Bot (short for "robot") refers to a software program that is designed to perform automated tasks on the internet.

Bots can be used for legitimate purposes, such as web crawling and data analysis.
Bots can also be used for malicious activities such as DDoS attacks.

BOTNET:
Botnet is a network of compromised computers, also known as "zombies," that are under the control of a remote attacker.
Attacker can use this BOTNET to carry out a variety of malicious activities which includes DDoS attacks, Cryptocurrency mining etc..

SSL/TLS handshake

Client

Server

3. The Client verifies the SSL certificate information

1. Client Sends Hello, Cipher Suite, & Client Random
2. Server respond back by sending the server random & SSL certificate (Private Key)
4. Pre-master key generated using the Public Key
6. Pre-master key decrypted using the Private key
7. A Master Key or Master-secret is in place now
8. This master key is used for encryption & decryption

SSL

Server

5. The server verifies client certificate (if required)

SSL Handshake Process

DOS and DDOS Attacks

DoS (Denial-of-Service) attack in which attacker floods a target server or website with a large amount of traffic or requests, overwhelming its resources and causing it to become unavailable.

In a DDoS attack, the attacker uses a botnet to flood the target server or website with traffic, often from multiple geographic locations, making it more difficult to identify and block the attack.

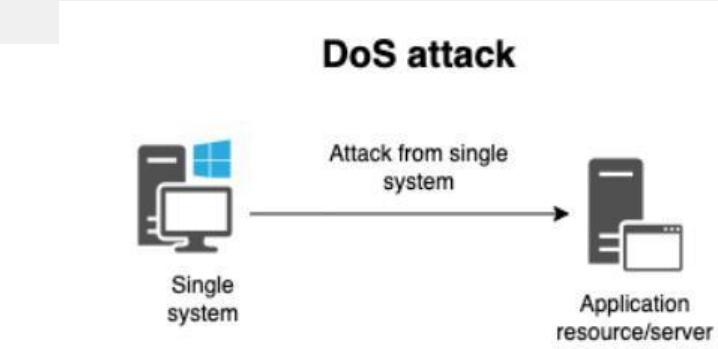
Purpose : The purpose of a DoS or DDoS attack is to disrupt the normal operation of a website, server, or network, rendering it inaccessible to legitimate users. These attacks can be used for various reasons, such as extortion, revenge, or to cause damage to a competitor's business.

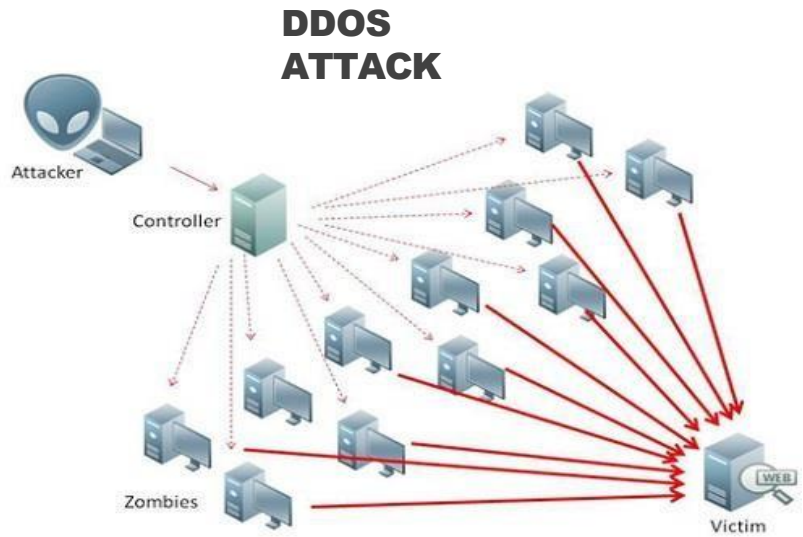
How do you defend/Prevent DOS and DDOS attack:

To defend against DoS and DDoS attacks, organizations can implement various measures such as firewalls, intrusion detection and prevention systems, and load balancers to distribute traffic across multiple servers.

Using Anti-DDOS Technology.

It is also important to keep software and security systems up to date and to monitor network traffic for signs of an attack.





What is Phishing and Types of Phishing attacks

Phishing is a type of cyber attack where an attacker tries to trick a victim into sharing sensitive information, such as login credentials or financial data.

Types of phishing:

Spear phishing: This is a targeted type of phishing attack, where the attacker sends personalized messages to a specific individual or group. The messages may appear to come from someone the victim knows or trusts, such as a coworker or a friend.

Vishing: This is a type of phishing attack that uses voice calls to trick victims into sharing sensitive information. The attacker may impersonate a bank or other financial institution and ask the victim to provide their account information.

Whaling: This is a type of spear phishing attack that targets high-level executives or other important individuals in an organization. The goal is to obtain sensitive information or access to the organization's systems.

Smishing: This is a type of phishing attack that uses SMS messages to trick victims into clicking on a link or providing sensitive information.

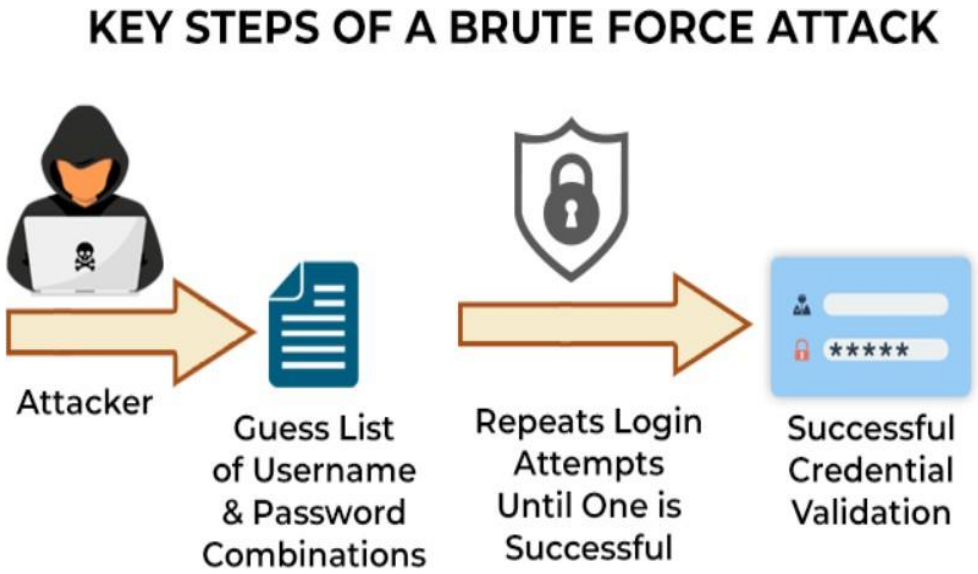
Email phishing: This is the most common type of phishing attack, where the attacker sends an email that appears to be from a legitimate source. The email may contain a link to a fake login page or a malicious attachment.

Brute force attack how you Mitigate

In brute force attack, attacker tries to gain access to a system or account by repeatedly guessing passwords or other authentication credentials.

Mitigation :

- Use strong passwords
- Implement account lockout policies
- Use multi-factor authentication
- Using Captcha



Password Spray attack how you Mitigate

In password spray attack, the attacker tries one or a few passwords against many user accounts, hoping to gain access to at least one account.

Mitigation :

- Enforce strong password policies:
- Implement multi-factor authentication
- Monitor for suspicious login activity
- Educate users

Dictionary attack and Mitigation

Dictionary attack is type of brute force attack where an intruder attempts to crack a password-protected security system with a “dictionary list” of common words and phrases used by businesses and individuals.

Mitigation :

- Enforce strong password policies:
- Implement multi-factor authentication
- Monitor for suspicious login activity
- Educate users
- Limit login attempts
- Monitor for unusual activity

Credential Stuffing Attack & Mitigation

Credential stuffing is a type of cyber attack in which an attacker tries to gain unauthorized access to user accounts by using usernames and passwords that have been previously leaked or stolen from other sources.

Mitigation :

- Enforce strong password policies:
- Implement multi-factor authentication
- Educate users
- Limit login attempts
- Use CAPTCHA or other bot detection techniques

Rainbow Table Attacks & Mitigation

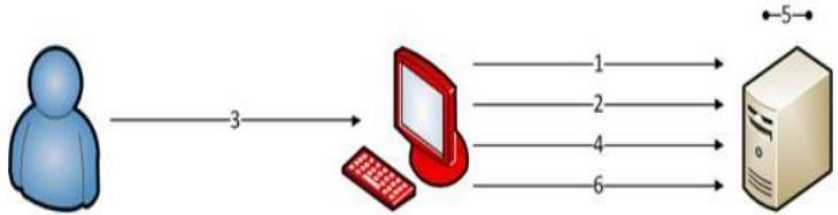
Rainbow table attacks are a type of password cracking attack in which an attacker uses a precomputed table of hashed passwords to quickly guess the plaintext password for a given hash.

Mitigation:

- Use strong hashing algorithms.
- Add salt to passwords: Adding a random string of characters, known as a salt, to each password before hashing it can make it more difficult for attackers to generate precomputed rainbow tables.
- Use key stretching techniques.

Pass the hash attack

- Pass-the-hash (PtH) is a type of cyber attack in which an attacker obtains the hash of a user's password and uses it to authenticate to a target system without knowing the actual password.
- The attacker can use various tools to capture the password hash and then replay it on other systems where the same user has administrative privileges.



1. User Attempts to Access Resource
2. Server Sends Authentication Challenge
3. User Supplies Username and Stolen Hash
4. Hash is Sent to Server
5. Server Checks Hash Value Against Expected Value
6. Access Granted to Resource

Mitigation :

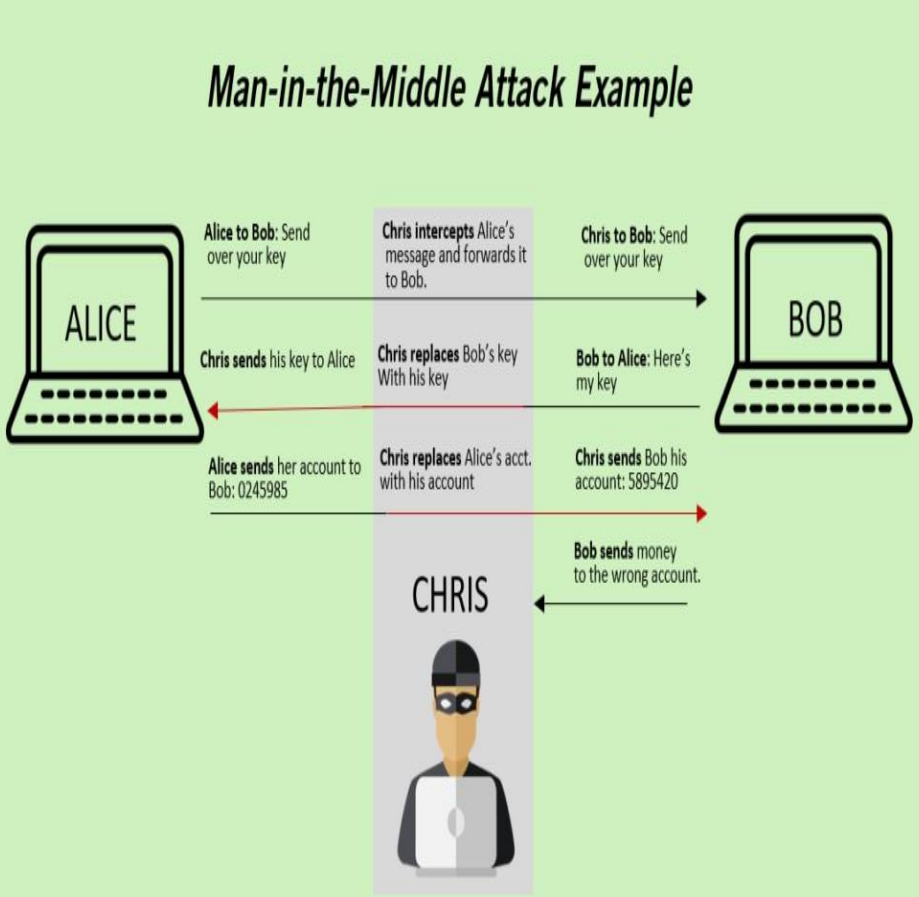
- Use strong encryption: Implementing strong encryption protocols, such as TLS, can prevent attackers from capturing the password hash in transit. This can help prevent Pass-the-hash attacks that rely on network sniffing to capture hashes.
- Use Credential Guard or similar security features: Credential Guard is a Windows security feature that helps protect against Pass-the-hash attacks by storing password hashes in a secure, isolated environment
- Restrict administrative privileges: Restricting administrative privileges can limit the impact of Pass-the-hash attacks by limiting the systems that an attacker can access using stolen credentials.

MAN-IN-THE-MIDDLE Attack

- A Man-in-the-middle (MitM) attack is a type of cyber attack in which an attacker intercepts communication between two parties, such as a user and a website or two devices communicating over a network.
- The attacker is then able to monitor and potentially manipulate the communication without either party being aware.

Mitigations:

- Use secure communication protocols: communication between devices or between a user and a website is encrypted using secure protocols such as SSL/TLS.
- Be cautious on public networks: Avoid using public Wi-Fi networks or other unsecured networks for sensitive communication.
- Verify digital certificates: Before providing any sensitive information, ensure that the website's digital certificate is valid and has not been tampered with.
- Use strong passwords:Strong passwords that are difficult to guess can help prevent attackers from being able to gain access to accounts even if they are able to intercept login credentials.



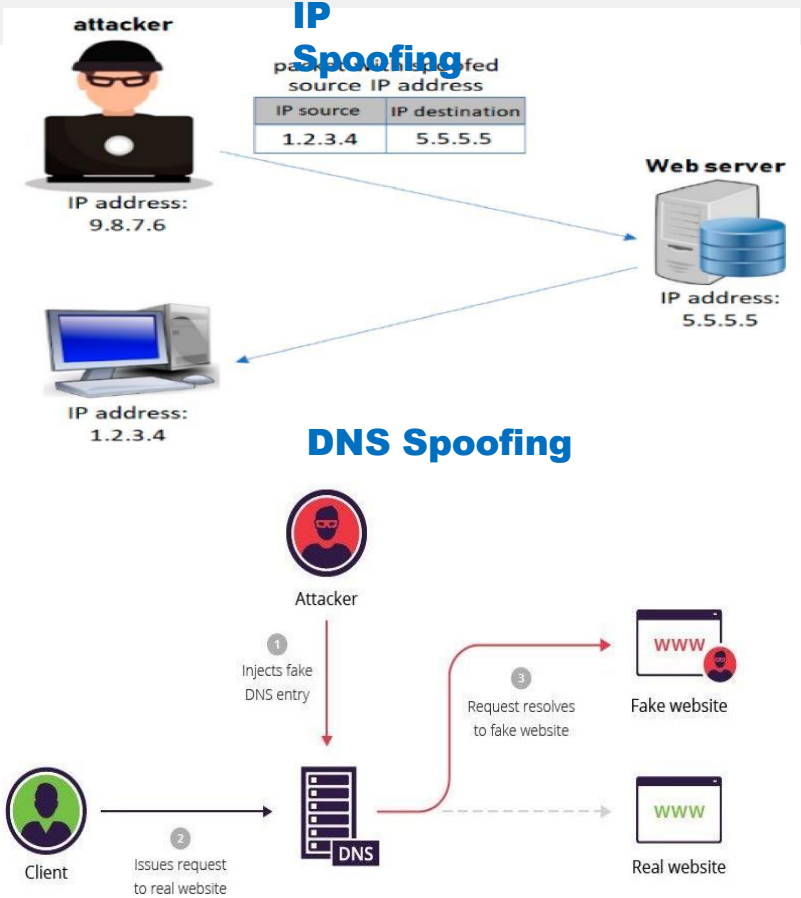
Spoofing Attacks and types

Spoofing is a type of cyber attack where an attacker Masking their identity or manipulates data to impersonate someone or something else.

Impotent types:

IP spoofing: IP spoofing is a type of cyber attack where an attacker manipulates the source IP address in a network packet to make it appear as if it is coming from a trusted source or a different location.

DNS Spoofing: In DNS spoofing, an attacker manipulates the Domain Name System (DNS) to redirect traffic to a malicious website. This can be used to steal sensitive information or spread malware.



OWASP and list top 10 vulnerabilities

OWASP stands for the Open Web Application Security Project.

OWASP is best known for its Top 10 project, which is a list of the top 10 most critical web application security risks. The OWASP Top 10 project is updated every few years to reflect changes in the threat landscape and new security risks.

The current version of the OWASP Top 10 (2021) includes the following vulnerabilities:

- Injection
- Broken Authentication and Session Management
- Insufficient Logging and Monitoring
- Insecure Design
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insufficient Attack Protection
- Insecure Communications
- Broken Access Controls
- Server-Side Request Forgery (SSRF)

SQL Injection and Mitigations

SQL Injection: It is a type of security vulnerability that occurs when an attacker injects malicious code into a SQL statement that is executed by a database.

The vulnerability arises when an application takes user input and incorporates it directly into a SQL query without properly sanitizing or validating it

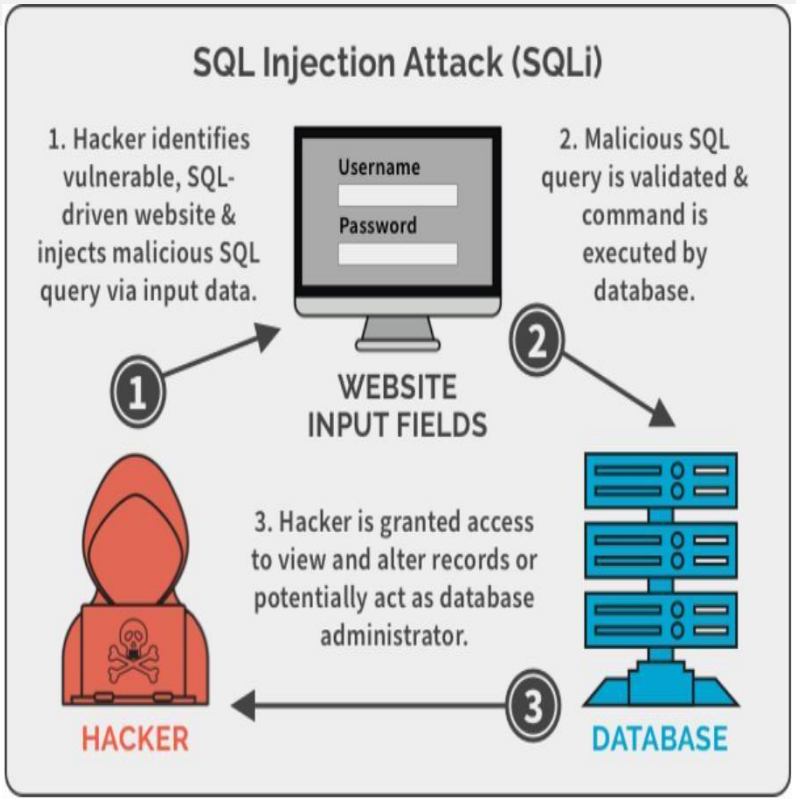
Impact: This type of attack can give the attacker unauthorized access to sensitive information, modify or delete data, and even take control of the entire database.

Mitigation: Input validation: Developers should validate user input to ensure that it matches the expected format and length.

Least privilege principle: Developers should implement the least privilege principle, which means that applications should only be granted the minimum level of privileges needed to perform their functions.

Use of Web Application Firewalls: Web Application Firewalls can be used to filter and block malicious inputs from reaching the application.

Regular security testing: Regular security testing, such as penetration testing, can help identify vulnerabilities and ensure that they are addressed before attackers can exploit them.



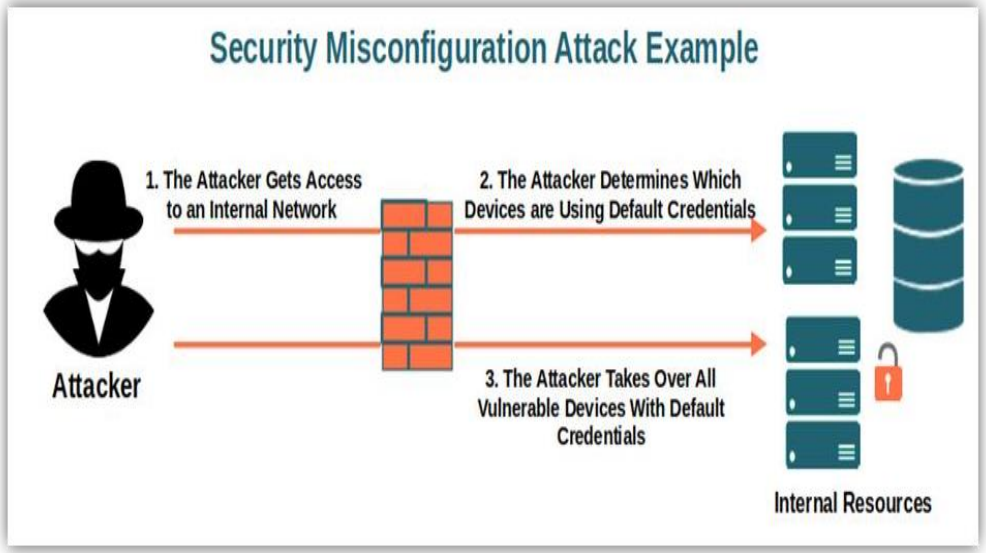
Security Misconfiguration and Mitigation

- Security misconfiguration refers to the improper configuration or setup of an application or system that can lead to vulnerabilities and potential security breaches.
- This could be caused by a variety of factors, such as weak passwords, unpatched software, default configurations, or insecure protocols.

Mitigation:

This includes

- security updates and patches,
- Using strong passwords,
- disabling unnecessary features and services,
- limiting user privileges.



Cross-Site Scripting (XSS) and Mitigation

Cross-Site Scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page viewed by other users.

There are three types of XSS attacks:

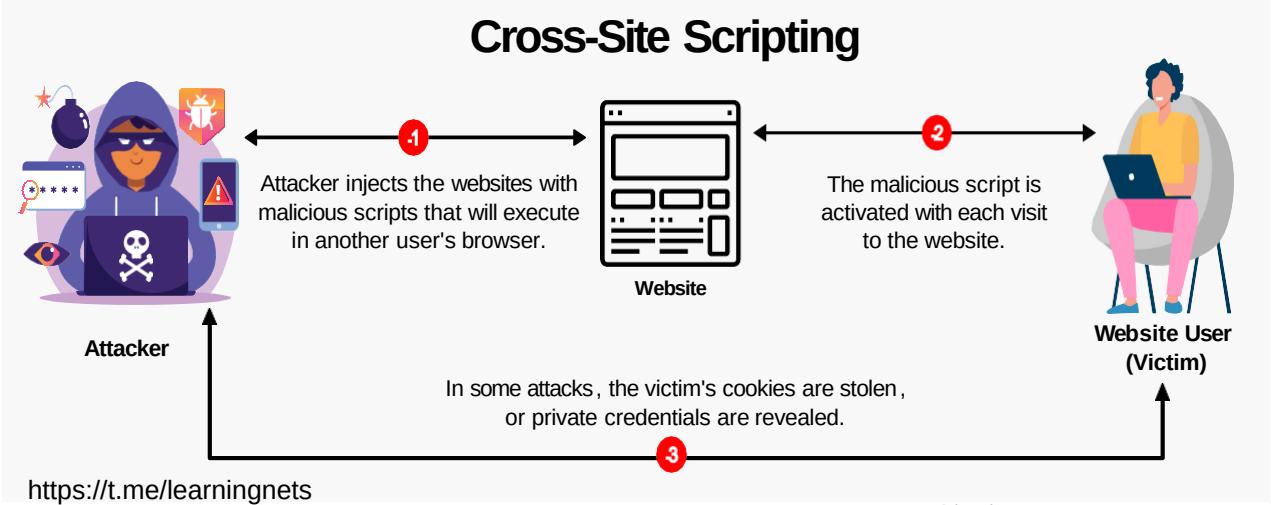
Reflected XSS: In this type of attack, the malicious script is injected into the victim's browser and reflected back to the web application. This often occurs through a URL or search query.

Stored XSS: In this type of attack, the malicious script is permanently stored on the web server and executed whenever the user visits the affected page.

DOM-based XSS: In this type of attack, the malicious script is executed at the client-side and modifies the Document Object Model (DOM) of the web page.

Mitigation:

- Input Validation
- Content Security Policy (CSP)
- Use HTTPS
- Regularly Update Software

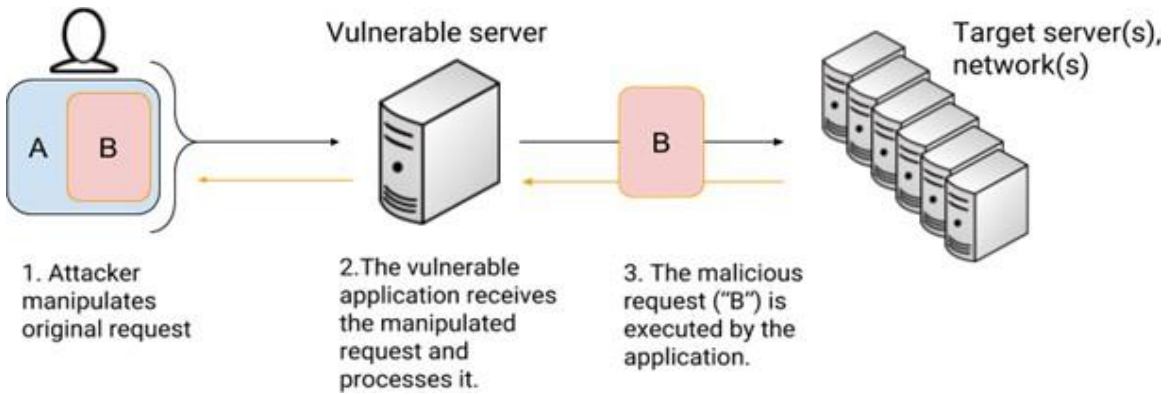


Server-Side Request Forgery (SSRF) and Mitigation c

Its type of web application vulnerability where an attacker can manipulate the web application to make it perform unintended network requests. This can result in the attacker being able to access internal network resources, steal sensitive information, or even execute arbitrary code on the server.

Mitigate SSRF attacks:

- Input Validation
- Whitelisting
- Use a Reverse Proxy
- Use Authentication and Authorization
- Regularly Update Software



Cyber kill chain

The Cyber Kill Chain consists of the following stages:

1. **Reconnaissance**: In this stage, the attacker gathers information about the target network or system, such as IP addresses, domain names, and employee names.
2. **Weaponization**: In this stage, the attacker creates a weapon, such as a virus or Trojan horse, to exploit a vulnerability in the target system.
3. **Delivery**: In this stage, the attacker delivers the weapon to the target system, typically by sending an email with a malicious attachment or by exploiting a vulnerability in a website.
4. **Exploitation**: In this stage, the weapon is used to exploit a vulnerability in the target system, allowing the attacker to gain access to the system.
5. **Installation**: In this stage, the attacker installs a backdoor or other malware on the target system, giving them persistent access to the system.
6. **Command and control**: In this stage, the attacker establishes a connection with the compromised system, allowing them to issue commands and control the system.
7. **Actions on objectives**: In this final stage, the attacker achieves their ultimate goal, which could be stealing sensitive data, disrupting operations, or causing other harm to the target system.

Incident response and phases

Incident response is the process of identifying, containing, investigating, and remediating security incidents within an organization.
The incident response process typically consists of the following phases:

Preparation: In this phase, an organization prepares for potential security incidents by developing incident response plans, implementing security controls such as IPS, firewalls etc. and establish communication protocols,

Identification: In this phase, an organization detects and identifies a security incident. This can be done through automated alerts from security systems or by manual detection by security personnel.

Containment: In this phase, an organization works to contain the incident to prevent further damage. This can involve isolating affected systems or devices from the network, disabling user accounts to prevent the spread of the incident.

Investigation: In this phase, an organization investigates the incident to determine the scope and severity of the incident, the cause of the incident, and the extent of the damage.

Remediation: In this phase, an organization takes steps to remediate the incident, such as removing malware, patching vulnerabilities, or restoring affected systems or data.

Recovery: In this phase, an organization returns to normal operations and restores systems and data to their pre-incident state.

Lessons Learned: In this final phase, an organization conducts a review of the incident response process to identify areas for improvement, update incident response plans and policies, and provide training to staff on best practices.

Windows AD and windows logs

What is Active directory

In Windows, AD stands for Active Directory, which is a directory service that stores and manages information about network resources, such as users, groups, computers, and printers. Active Directory is a centralized database that enables administrators to manage and control access to resources within a Windows domain.

Features:

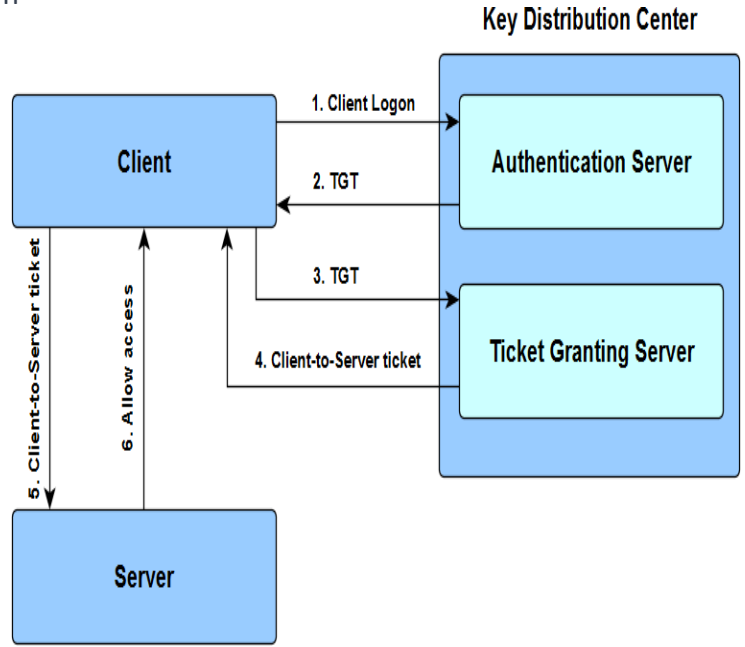
- Authentication and authorization
- Domain Services
- Group Policy
- DNS Services
- Directory replication

What is Kerberos and how Kerberos Authentication works?

Kerberos is a network authentication protocol that is used to provide secure authenticatio n between clients and servers over an insecure network, such as the Internet.

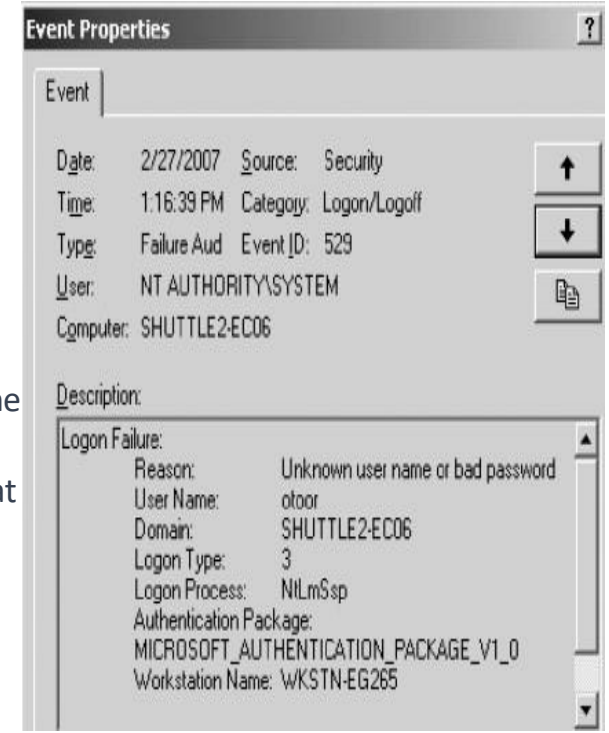
Kerberos authentication process:

1. **User requests authentication**: A user requests authentication to access a network resource, such as a file share or printer.
2. **Ticket-granting ticket request**: The user's computer sends a request to the KDC for a ticket-granting ticket (TGT).
3. **TGT delivery**: If the user's credentials are valid, the KDC delivers a TGT to the user's computer. The TGT contains a session key that is used to encrypt and decrypt subsequent communications between the user's computer and the network resource.
4. **Resource request**: The user's computer sends a request for access to the network resource to the resource server.
5. **Ticket request**: The resource server sends a request to the KDC for a service ticket, which contains the user's identity and a session key that is encrypted with the TGT.
6. **Service ticket delivery**: If the user is authorized to access the resource, the KDC delivers a service ticket to the resource server.
7. Resource access: The resource server grants access to the requested resource.



common fields in Windows event logs

1. **Date and Time**: - This shows the date and time of the event.
2. **Event ID**: This is a unique identifier assigned to the event.
3. **Source: Security** - this is the name of the software component that generated the event.
4. **Level**: Information - this is the severity level assigned to the event.
5. **User**: This is the user account involved in the event. In this example, the event was initiated by the system account.
6. **Computer**: This is the name of the computer where the event occurred.
7. **Description**: An account was successfully logged on. - this is a text description of the event.
8. **Keywords**: Audit Success - this is a keyword that describes the event, indicating that it was a successful audit event.
9. **Category**: Logon - this is a numeric value assigned to the event that indicates its category. In this example, the event is related to a user logon.
10. **Event Data**: Subject: Security ID: S-1-5-18 Account Name: DC1$ Account Domain: Example Logon ID: 0x3E7



Impotent Windows event ID’s

Here are some common Windows event IDs:

1. 4624 - An account was successfully logged on.
2. 4625 - An account failed to log on.
3. 4634 - An account was logged off.
4. 4720- New user account has been created.
5. 4726- a user account has been deleted
6. 4740 -user account has been locked out
7- 4798 - A user's local group membership was enumerated.
8. 7034 - A service was stopped.
9. 1102 - The audit log was cleared.

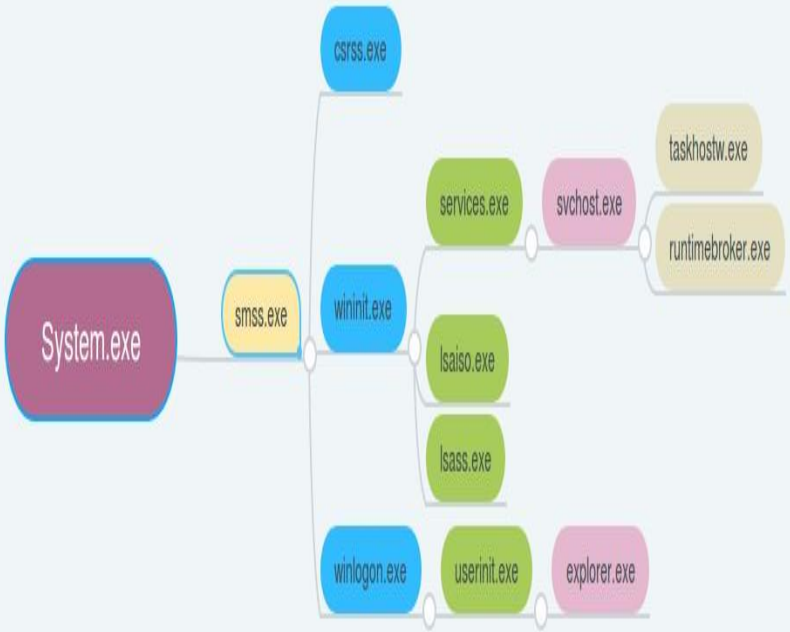
Windows logon Types

There are 10 different logon types in Windows, which are as follows:

1. **Interactive (logon at the console)**
2. **Network (logon over the network)**
3. **Batch (scheduled task)**
4. **Service**
5. **Proxy**
6. **Unlock**
7. **NetworkCleartext**
8. **NewCredentials**
9. **RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)**
10. **CachedInteractive (logon with cached credentials)**

Windows Core Process

1. **System**: This process is responsible for managing system resources such as memory, threads, and processes.
2. **Session Manager Subsystem (smss.exe):** SMSS is responsible for managing sessions and starting system services during system startup.
3. **Local Security Authority Subsystem Service (LSASS):** LSASS is responsible for authentication and enforcing security policies on the system.
4. **Windows Management Instrumentation (WMI**): WMI is used to manage and monitor system resources and events.
5. **Services**: The Services process manages Windows services, which are programs that run in the background and provide system functions such as network connectivity and printing.
6. **Windows Explorer**: This process provides the user interface for the desktop, start menu, and other graphical elements of the system.
7. **Task Manager**: The Task Manager process provides a tool for managing and monitoring system processes and resources.
8. **Winlogon**: Winlogon is responsible for managing the logon process and user authentication.
9. **Client Server Runtime Process (csrss.exe):** CSRSS is responsible for managing the Windows user interface and console windows.



Difference between a user account and a service account in Windows?

User account is a type of account that is created for individual users to log in to a computer or a network. User accounts are associated with a user profile, which contains personal settings, preferences, and data for the user

A service account, on the other hand, is a type of account that is used to run a service or a process on a computer or a network.

Service accounts are typically used for system-level services such as database services, web servers, and other types of application servers

One of the **main differences** between user accounts and service accounts is that user accounts are associated with a user profile and are designed for interactive use, whereas service accounts are designed for running services or processes in the background.

Log in failures specific error codes

1. Error code 0xc00006**d**: This error code indicates that the user account is locked out.
2. Error code 0xc0000**72**: This error code indicates that the user's password has expired and needs to be changed.
3. Error code 0xc00006**a**: This error code indicates that the user attempted to log on with an incorrect username or password.
4. Error code 0xc00006**e**: This error code indicates that the user attempted to log on outside of their allowed logon hours
5. .
6. Error code 0xc0000**70**: This error code indicates that the user attempted to log on to a workstation that does not have the required network authentication.
7. Error code 0xc000019**3**: This error code indicates that the user attempted to log on to a workstation that has too many concurrent connections.
8. Error code 0xc00007**b**: This error code indicates that the user attempted to log on to a workstation that has a mismatched trust relationship with the domain.

Log fields from various security devices for Log analysis

Common log types SOC team collect Across infrastructure

1. **Network logs**: These logs capture information about network traffic, such as IP addresses, ports, protocols, and packet payloads.
2. **Server logs:** These logs capture information about server activity, such as user login/logout events, application usage, and system performance metrics.
3. **Application logs:** These logs capture information about specific application activity, such as user actions, error messages, or system events.
4. **Security logs**: These logs capture information about security-related events, such as firewall rule violations, intrusion detection alerts, or system access attempts.
5. **Audit logs**: These logs capture information about system changes or configuration modifications, such as user account creation/deletion, policy changes, or system updates.

Important fields in Firewalls for analysis

1. **Source IP Address**: This field identifies the IP address of the computer or device that is attempting to access the network
2. **Destination IP Address**: This field identifies the IP address of the computer or device that is being accessed.
3. **Source Port**: This field identifies the port number used by the source device to send the traffic.
4. **Destination Port**: This field identifies the port number used by the destination device to receive the traffic.
5. **Protocol**: This field identifies the protocol used by the traffic, such as TCP, UDP, or ICMP.
6. **Timestamp**: This field indicates the date and time when the traffic was logged.
7. **Event Type**: This field identifies the type of event being logged, such as "allowed" or "blocked".
8. **Source Country**: This field identifies the country of origin of the traffic, which can be useful in identifying potential threats.
9. **Destination Country**: This field identifies the country of the destination of the traffic.
10. **Bytes Sent**: This field indicates the number of bytes sent in the traffic.
11. **Bytes Received**: This field indicates the number of bytes received in the traffic.
12. **Protocol**: This field identifies the protocol used by the traffic, such as TCP or UDP.
13. **Action Taken**: This field indicates the action taken by the firewall, such as "allowed" or "blocked".

Explain Important fields in IPS (intrusion Prevention system)

1. **Timestamp**: This field indicates the date and time when the threat was detected.
2. **Event Type**: This field identifies the type of event being logged, such as "detected" or "blocked".
3. **Source IP Address**: This field identifies the IP address of the computer or device that is the source of the threat.
4. **Destination IP Address**: This field identifies the IP address of the computer or device that is the target of the threat.
5. **Source Port**: This field identifies the port number used by the source device to send the traffic.
6. **Destination Port**: This field identifies the port number used by the destination device to receive the traffic.
7. **Signature ID**: This field identifies the unique identifier of the signature that triggered the IPS to take action.
8. **Signature Name**: This field provides a descriptive name for the signature that triggered the IPS to take action.
9. **Severity:** This field indicates the severity of the threat, which can range from low to critical.
10. **Action Taken:** This field indicates the action taken by the IPS, such as "blocked" or "logged".
11. **Alert Type**: This field identifies the type of alert being generated, such as "intrusion detected" or "virus detected".
12. **Attack Method:** This field provides information about the method used by the attacker to carry out the attack.
13. **Attack Target:** This field provides information about the target of the attack, such as a specific application or protocol.
14. **Attack Type:** This field provides information about the type of attack, such as a denial of service (DoS) attack or a buffer overflow attack.

Important fields in EDR

1. **Timestamp**: This field indicates the date and time when the event was logged.
2. **Event Type**: This field identifies the type of event being logged, such as "process execution" or "file modification".
3. **Process Name**: This field identifies the name of the process or application that is being executed or modified.
4. **Process ID**: This field provides a unique identifier for the process or application.
5. **User**: This field identifies the user account that is associated with the process or application.
6. **Source IP Address**: This field identifies the IP address of the computer or device that is the source of the event.
7. **Destination IP Address**: This field identifies the IP address of the computer or device that is the target of the event.
8. **File Name**: This field identifies the name of the file that is being modified or executed.
9. **File Path**: This field identifies the path to the file that is being modified or executed.
10. **Hash Value**: This field provides a unique identifier for the file based on its cryptographic hash value.
11. **Action Taken**: This field indicates the action taken by the EDR system in response to the event, such as "blocked" or "quarantined".
12. **Threat Type**: This field identifies the type of threat that is associated with the event, such as malware or a suspicious process.
13. **Threat Name**: This field provides a descriptive name for the threat that is associated with the event.
14. **Detection Method**: This field identifies the method used by the EDR system to detect the threat, such as behavior monitoring or signature-based detection.
15. **Severity**: This field indicates the severity of the event, which can range from low to critical.

Important fields in Email gateway

1. **Date/time stamp**: Records the date and time the email was sent, received or processed.
2. **Sender and recipient addresses**: Provides information about the email's origin and destination.
1. **Message ID**: Unique identifier for each email message.
2. **Status cocdes**: Indicates the status of an email delivery attempt.
3. **Subject line**: Provides information about the content of the email.
4. **Message size**: Records the size of the email message in bytes.
5. **SMTP logs**: Records the details of the email delivery process, including SMTP commands, response codes, and any errors or warnings.

Important fields in Proxy device

1. **Timestamp**: The time and date the request was made to the proxy.
2. **Client IP**: The IP address of the device that made the request to the proxy.
3. **Request URL**: The URL of the website or resource requested by the client.
4. **Destination IP**: The IP address of the server hosting the website or resource requested by the client.
5. **User Agent**: The user agent string identifies the device and web browser used by the client.
6. **HTTP Response Code**: The HTTP status code returned by the server in response to the request.
7. **Bytes transferred**: The number of bytes transferred in the request and response.
8. **Content Type**: The type of content returned by the server, such as text/html, image/jpeg, etc.
9. **Referrer**: The URL of the website that referred the client to the requested resource.
10. **Category**: The category of the website or resource, as determined by the proxy device's content filtering policies.
11. **Action**: The action taken by the proxy device in response to the request, such as allow, block, or log.

What logs SOC team collect from AWS Cloud for analysis

1. CloudTrail logs (for API calls),
2. VPC Flow Logs (for network traffic),
3. AWS Config Logs (for resource configuration),
4. CloudWatch Logs (for monitoring and logging),
5. GuardDuty Logs (for detecting potential security threats).

What logs SOC team collect from Azure Cloud for analysis

1. Azure Activity Logs (for auditing management operations)
2. Azure defender for cloud Logs (for security event and vulnerability detection),
3. Azure Network Watcher Logs (for network monitoring and diagnostics),
4. Azure Application Gateway Logs (for performance and security of web traffic load balancing),
5. Azure Sentinel Logs (for a holistic view of security events).

What logs SOC team collect from Google Cloud for analysis

1. Google Cloud Audit Logs
2. Google Cloud VPC Flow Logs
3. Google Cloud Firewall Rules Logs
4. Google Cloud Storage Logs
5. Google Cloud DNS Logs

What are logging levels in network devices

Level	Level Name	Explanation
0	Emergency	The system may be unusable.
1	Alert	Immediate action may be required.
2	Critical	A critical event took place.
3	Error	The router experienced an error.
4	Warning	A condition might warrant attention.
5	Notification	A normal but significant condition occurred.
6	Informational	A normal event occurred.
7	Debugging	The output is a result of a debug command.

warning logging level in Network device

The warning logging level in a network device is used to log events or conditions that may indicate a potential problem or error in the system

For example, you might use the warning logging level to log events such as:

- A network interface that is experiencing high utilization or congestion
- A system process that is using a significant amount of CPU or memory resources

purpose of the informational logging level?

The informational logging level in a network device provides useful system information for troubleshooting and maintenance purposes, such as system startup messages, network protocol statistics, and user activity.

It helps network administrators monitor the performance of the system and identify potential issues.

Difference between the emergency, alert, and critical logging levels?

1. The emergency logging level in a network device is used to log critical system failures that require immediate attention.
2. Alert level is used for events that require immediate action but are not critical system failures.
3. Critical level is used for events that could cause significant problems if not addressed quickly.

Example: Emergency: System crashes, hardware failures, or network outages that impact critical services or applications.

Alert: Security breaches, software errors, or service disruptions that require immediate action to prevent further damage or data loss.

Critical: Network congestion or performance degradation, configuration errors, or system component failures that could cause significant problems if not addressed quickly.

Cyber Threat Intelligence

Can you tell me what you understand Threat Intilegence

- Threat Intelligence is all about analysis of information related to adversaries who have the intent, Opportunity and capability to harm you
- Threat Intelligence is data that is Collected, Processed and Analyzed to understand a Threat actors Motives, Targets and Attack Behaviors.
- It Enables us to make Faster, More informed, Data backed security Decisions and change their behavior from Reactive to Proactive in the Fight against Threat actor.

Q. Why Threat Intelligence is important today

- It enables Cyber security Stockholders by disclosing Attackers Motivations and Approaches, Tactics and Process (TTP's)

- Helps Security Professionals understand the decision-making process of Threat Actor.

Q: Who Get Most Benefit from Threat Intelligence

- Security operations center
- Senior Management
- IT Analyst
- Vulnerability Management Experts

Can you explain about Pyramid of Pain

- Pyramid of Pain is a Visual Represenation of Six differen sorts of attack indications,Grouped in Eslating oder of Threat actor and Security analyst work.

- Pyramid Represents different types of attack indicators you might use to detect anavdresary's activities and is broken up by how much pain it will cause Attacker when you are able to deny those indicators to them

What is difference between DATA vs INFORMATION Vs INTELLIGENCE

- Data is made up of distinct facts and Statistics that are acqurid as the foundation of Subsequent Research.
- Information is collection of data pieces used to Answer certain inquires.
- Intelligence examines data and information to discover patterns and Stories that may used to make decision.

What is Threat Intelligence Feed ?

- Threat Intelligence feeds are real times Streams of data that Provide information on Potential Cyber Threats and risks

- Each Threat Intelligence feed may collect data from Several Resources.

- Include the Following
  - Open source data
  - Customer telemetry information from Security companies
  - Crawling the internet to search for exploits and attacks

What are the different types of Threat Intelligence?

1. **Strategic Threat Intelligence:** It focuses on understanding the broader threat landscape, including emerging trends, geopolitical factors, and industry-specific risks.

1. **Tactical Threat Intelligence:** It concentrates on details such as malware indicators, attack techniques, and vulnerabilities being actively exploited.

1. **Operational Threat Intelligence:** It includes information on specific attack campaigns, tactics, techniques, and procedures (TTPs) used by threat actors.

While Reviewing Threat feeds what are the factors we need to verify?

1. **Source Credibility:** Ensure the source is reputable.
2. **Timeliness:** Confirm the data is current.
3. **Accuracy:** Check for reliable and accurate information.
4. **Relevance:** Assess if threats are pertinent to your organization.
5. **Completeness:** Ensure all necessary details are provided.
6. **Context:** Understand the threat context for effective response.
7. **Actionability:** Determine if the data enables meaningful actions.
8. **Integration:** Ensure compatibility with existing security tools and processes.

What are the Different Phases of Threat Inteligence?

1. **Planning and Direction:**
    1. Defining objectives and priorities for threat intelligence efforts.
    2. Identifying the scope of intelligence collection and analysis.
2. **Collection:**
    1. Gathering raw data and information from various sources, including open-source intelligence (OSINT), closed sources, and internal logs.
    2. Data collection methods may include passive DNS monitoring, honeypots, and subscribing to threat feeds.
3. **Processing:**
    1. Organizing and normalizing collected data for analysis.
    2. Transforming raw data into a structured format for further investigation.
4. **Analysis:**
    1. Evaluating the processed data to identify potential threats and vulnerabilities.
    2. Determining the nature, severity, and implications of identified threats.
    3. Assessing the tactics, techniques, and procedures (TTPs) used by threat actors.
5. **Production:**
    1. Creating actionable threat intelligence reports and alerts.
    2. Tailoring intelligence for different stakeholders, such as security teams, executives, or incident response teams.
6. **Dissemination:**
    1. Sharing threat intelligence with relevant parties both within and outside the organization.
    2. Ensuring that information reaches the right people in a timely manner.
7. **Utilization:**
    1. Applying threat intelligence to enhance security measures, such as configuring firewalls, updating intrusion detection systems, or patching vulnerabilities.
    2. Integrating intelligence into incident response plans and processes.
8. **Feedback:**
    1. Gathering feedback on the effectiveness of threat intelligence in mitigating threats and improving security posture.
    2. Continuously refining intelligence processes based on lessons learned.

How can threat intelligence be integrated into a SIEM system for proactive threat detection??

1. **Select Relevant Threat Feeds:** Choose threat intelligence sources aligned with your organization's needs.
2. **Integrate Data:** Configure your SIEM to ingest threat data regularly.
3. **Normalize and Enrich:** Standardize and enhance data for consistency and context.
4. **Create Correlation Rules:** Develop rules to trigger alerts based on threat indicators.
5. **Prioritize Alerts:** Establish a ranking system for threat-based alerts.
6. **Automate Responses:** Set up automated actions for specific alerts.
7. **Analyze Historically:** Review historical data to uncover past incidents.

Describe a specific instance where you used threat intelligence to mitigate a cyber threat. What was the outcome?

We received threat intelligence indicating the presence of a new strain of ransomware actively targeting organizations in our industry. The intelligence included file hashes associated with this malware.

Here's how we used threat intelligence to mitigate the cyber threat:

1. **Data Ingestion:** We integrated the threat intelligence feed into our security systems, ensuring that we received real-time updates regarding the malware indicators.
2. **Alert Configuration:** We configured our endpoint security solution to trigger alerts whenever it detected files with the specific file hashes provided in the threat intelligence feed.
3. **Detection and Isolation:** When an alert was triggered, our security team immediately quarantined the affected endpoint to prevent further spread of the malware within our network.

Outcome:

1. **By leveraging threat intelligence and implementing a swift response, we achieved several outcomes:**
2. **We contained the ransomware quickly, limiting its impact on our organization.**
3. **Our forensic analysis provided insights into the malware's tactics, helping us improve our defenses against similar threats.**
4. **We successfully recovered affected systems without paying a ransom.**
5. **Our proactive use of threat intelligence and rapid response demonstrated our organization's resilience in the face of emerging malware threats.**

Threat Hunting

What is Threat Hunting, and why is it important

- Threat hunting is a proactive cybersecurity practice focused on actively searching for signs of malicious activities or security threats within an organization's network or systems. Unlike traditional security measures that rely on automated tools and predefined rules, threat hunting involves skilled cybersecurity professionals actively seeking out anomalies and potential threats that may go undetected by automated systems.

Why is Threat Hunting Important?

- Proactive Detection: Threat hunting allows organizations to detect and respond to threats before they escalate. It shifts the cybersecurity approach from a reactive stance to a proactive one, actively seeking and mitigating potential risks.
- Unknown Threats: Automated security tools are effective in detecting known threats, but threat hunting is essential for identifying unknown or advanced threats that may not have established signatures.
- Contextual Understanding: Threat hunting provides a deeper understanding of the organization's security landscape. Analysts can contextualize data, understand normal behaviors, and identify deviations that may indicate a security issue.
- Reduced Dwell Time: By actively seeking and mitigating threats, threat hunting helps in reducing the dwell time—the duration a threat remains undetected within the network. Quick identification and response minimize the potential impact of a security incident.
- Continuous Improvement: Threat hunting is an iterative process that involves learning from each investigation. It contributes to continuous improvement in security measures, enhancing the organization's overall cybersecurity posture.

Can you explain the difference between Threat Detection and Threat Hunting

- **Threat Detection:** Think of Threat Detection as the automated surveillance system in a cybersecurity environment. It relies on predefined rules and patterns to identify known threats or malicious activities. These rules are often based on signatures, anomalies, or known attack patterns. Once the system detects a match, it triggers an alert or an automated response. In essence, Threat Detection is reactive, responding to known threats in real-time without requiring constant human intervention.

- **Threat Hunting:** On the other hand, Threat Hunting is a proactive and hands-on approach. It involves cybersecurity professionals actively exploring networks and systems to uncover hidden or unknown threats. Instead of relying solely on predefined patterns, threat hunters use their expertise and contextual understanding to identify anomalies that may indicate potential security issues. Threat Hunting is like a continuous investigation, seeking out both known and unknown threats that might evade automated systems. It's about staying one step ahead by actively looking for signs of compromise that automated tools might miss.

In summary, while Threat Detection is automated and reactive, relying on predefined rules, Threat Hunting is proactive, involving skilled human analysts in a continuous exploration for potential threats, including those that may not have a 'signature' in existing databases."

Can you explain the difference between proactive and reactive threat hunting?

Proactive Threat Hunting:

Proactive threat hunting involves a continuous and anticipatory approach to cybersecurity. Here, cybersecurity professionals take the initiative to actively search for potential threats, vulnerabilities, or signs of compromise before they manifest as security incidents. Key characteristics of proactive threat hunting include:

1. **Continuous Exploration:** Proactive threat hunting is an ongoing, iterative process that doesn't wait for alerts or predefined patterns. Security professionals actively explore networks, systems, and data to uncover hidden threats.
2. **Use of Expertise:** Human expertise plays a crucial role in proactive threat hunting. Cybersecurity analysts leverage their knowledge, experience, and contextual understanding of the organization's environment to identify anomalies and potential security issues.
3. **No Dependency on Known Patterns:** Proactive hunters are not solely reliant on predefined rules or signatures. They actively seek out both known and unknown threats, understanding that sophisticated threats might not conform to existing patterns.
4. **Hypothesis-Driven:** Proactive threat hunting often involves developing hypotheses about potential threats based on intelligence, trends, or previous incidents. Analysts then actively investigate to validate or refute these hypotheses.

Reactive Threat Hunting:

Reactive threat hunting, in contrast, involves responding to specific triggers, events, or alerts after they've been detected by automated systems or predefined rules. Key characteristics of reactive threat hunting include:

1. **Triggered by Events:** Reactive threat hunting is initiated in response to specific events or alerts. These events might include the detection of anomalies, unusual patterns, or known malicious activities.
2. **Automation and Predefined Rules:** Reactive hunting often relies on automated systems and predefined rules or signatures. When a match occurs, analysts investigate further to understand the nature and extent of the threat.
3. **Incident-Driven:** Reactive threat hunting is incident-driven. Analysts respond to incidents that have already been identified, focusing on containment, eradication, and post-incident analysis.
4. **Utilizes Historical Data:** While reacting to a specific incident, analysts may refer to historical data and logs to understand the timeline of events and the impact of the threat.

In summary, proactive threat hunting is a continuous, proactive exploration for potential threats, driven by human expertise and a hypothesis-driven approach. Reactive threat hunting, on the other hand, responds to specific triggers or incidents, often leveraging automation and predefined rules. Both approaches are essential components of a comprehensive threat hunting strategy, providing a layered defense against evolving cyber threats.

What is hypotheses in Threat hunting ?

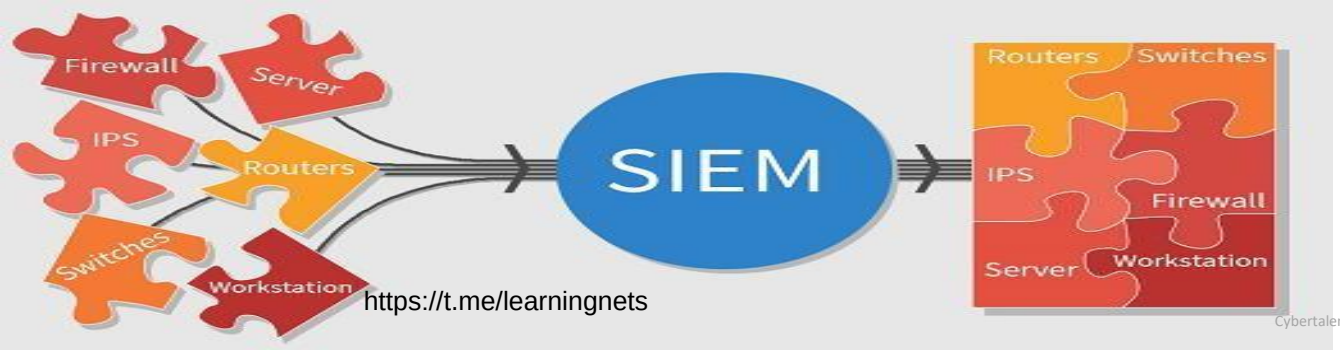
- In threat hunting, a hypothesis is a focused assumption about potential security threats. It outlines a specific threat scenario, expected indicators, and data sources to investigate.
- For example, a hypothesis might suggest monitoring network traffic for unusual patterns indicative of a specific type of attack. By formulating hypotheses, threat hunters streamline their investigations and target specific areas for proactive detection of potential threats.

Example Hypothesis: "Adversaries may be using legitimate-looking communication channels for command and control (C2) to evade detection. We hypothesize that monitoring outbound network traffic for unusual patterns, especially encrypted communication, may reveal potential C2 activity.

SIEM

Q74: What is a SIEM and Why We need SIEM?

- A SIEM (Security Information and Event Management) is a software platform that collects, correlates, and analyzes security data from multiple sources across an organization's IT infrastructure.
- It provides a centralized platform for security monitoring, analysis, and response, enabling organizations to improve their security posture and reduce the risk of security breaches.
- It enables real-time monitoring and analysis of security events, detects potential security threats, and enables timely response and remediation.
- SIEM also helps organizations comply with regulatory requirements by providing audit trails and reports on security incidents.



Normalization in SIEM

Normalization in SIEM refers to the process of transforming incoming security event data from different sources into a standardized format for easier analysis and correlation.

Example device logs:

Check Point: "14" "21Nov2016" "12:10:29" "eth-s1p4c0" "ip.of.firewall" "log" "accept" "wwwhttp" "192.0.2.0" "192.0.2.1" "tcp" "4" "1355" "" "" "" "" "" "" "" "" "" "firewall" "len 68

Cisco Router:

Nov 21 15:10:27: %SEC-6-IPACCESSLOGP: list 102 permitted tcp 192.0.2.0(1355) - > 192.0.2.1(80), 1 packet Cisco PIX: Nov 21 2016 12:10:28: %PIX-6-302001: Built inbound TCP connection 125891 for faddr 192.0.2.0/1355 gaddr 192.0.2.1/80 laddr 10.0.111.22/80

Snort: [**] [1:971:1] WEB-IIS ISAPI .printer access [**] [Classification: Attempted Information Leak] [Priority: 3] 11/21-12:10:29.100000 192.0.2.0:1355 -> 192.0.2.1:80 TCP TTL:63 TOS:0x0 ID:5752 IpLen:20 DgmLen:1234 DF ***AP*** Seq: 0xB13810DC Ack: 0xC5D2E066 Win: 0x7D78 TcpLen: 32 TCP Options (3) => NOP NOP TS: 493412860 0 [Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN2001-0241] [Xref => http://www.whitehats.com/info/IDS533]

After Normalization

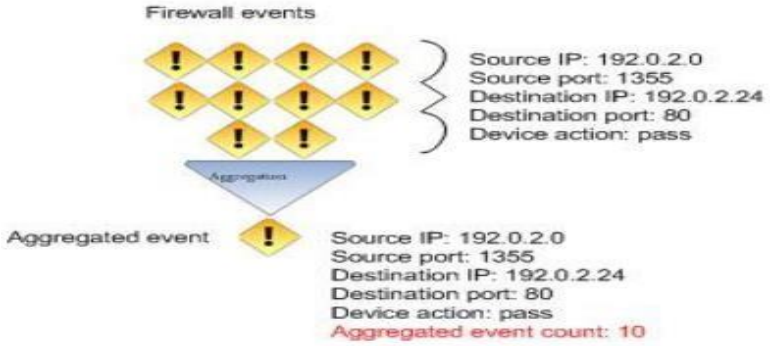
Date	Time	Event_Name	Src_IP	Src_ Port	Tgt_IP	Tgt_ Port	Device_Type
21-Nov-16	12:10:29	Accept	192.0.2.0	1355	192.0.2.1	80	CheckPoint
21-Nov-16	12:10:27	List 102 permitted tcp	192.0.2.0	1355	192.0.2.1	80	Cisco Router
21-Nov-16	12:10:29	WEB-IIS ISAPI printer access	192.0.2.0	1355	192.0.2.1	80	Snort

Aggregation in SIEM

Aggregation in SIEM (Security Information and Event Management) refers to the process of grouping related security events or log entries based on certain criteria or attributes, such as source IP addresses, event types, or timeframes.

Example:

For example, suppose the connector is configured to aggregate events with a certain source IP and port, destination IP and port, and device action if they occur 10 times in 30 seconds. If the connector receives 10 events with these matching values within that time, they are grouped into a single aggregated event with an aggregated event count of 10.



Correlation in SIEM

Correlation in the context of SIEM refers to the process of identifying relationships and connections between different security events or log entries.

In simpler terms, correlation helps in understanding how different events are related and whether they collectively form a meaningful security incident

For example, let's consider the following events:

- Event 1: Multiple failed login attempts from IP address 192.168.1.100.
- Event 2: A successful login from the same IP address 192.168.1.100 immediately after Event 1.
- Event 3: An outbound connection from the same IP address to a known malicious domain.

By correlating these events, a SIEM system can identify a potential attack scenario. The failed login attempts (Event 1) followed by a successful login (Event 2) indicate a possible brute-force attack. The subsequent outbound connection to a malicious domain (Event 3) further raises suspicion of a compromised system.

Parsing in SIEM

Parsing involves extracting relevant information from event logs and transforming it into a structured format that can be understood and processed by the SIEM system.

Example, consider a log entry from a firewall device:

Raw Log: [timestamp=2023-05-15 14:30:45] [source=192.168.1.100] [event=Blocked connection] [user=admin]

After parsing, the SIEM system will extract the relevant fields:

Parsed Fields:

- Timestamp: 2023-05-15 14:30:45
- Source IP: 192.168.1.100
- Event Type: Blocked connection
- User: admin

SIEM Components

Data sources: These are the devices and applications that generate security event data, such as firewalls, Windows, Database, intrusion detection systems etc.

Data collection agents: These agents collect security event data from the data sources and forward it to the SIEM system for analysis.

Log management system: This component is responsible for collecting, storing, and managing the logs generated by the data sources and data collection agents.

Event processing engine: This engine analyzes the security event data and identifies potential security incidents based on pre-defined rules and policies.

Correlation engine: This engine correlates the security events and incidents to provide a more comprehensive view of the security posture of the organization.

Alerting and reporting system: This component generates alerts and reports based on the identified security incidents and events, and provides real-time notification to the SOC analysts.

Analytics and threat intelligence: This component leverages advanced analytics and threat intelligence feeds to identify and respond to advanced and emerging threats.

Explain SIEM Workflow

Data Collection: The SIEM collects data from various sources such as logs from network devices, applications, endpoints, and servers.

Normalization: The collected data is processed to create a normalized format for easy analysis and correlation.

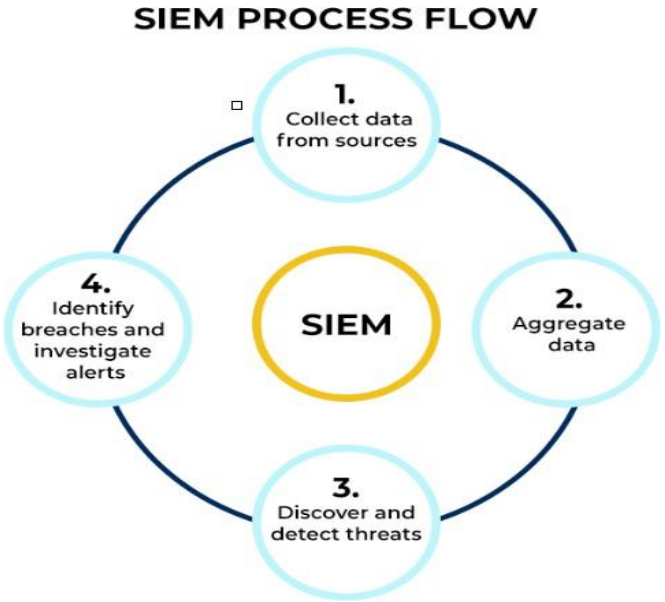
Correlation: The SIEM correlates the normalized data to identify patterns, events, and anomalies that may indicate a security threat.

Alerting: When a potential security threat is detected, the SIEM generates alerts and sends them to the security analyst for investigation.

Incident Investigation: The security analyst investigates the alert by reviewing the relevant data, such as logs and packets, to determine the root cause and scope of the incident.

Remediation: Based on the findings of the investigation, the security analyst takes appropriate actions to contain the incident, mitigate the risk, and prevent it from happening again.

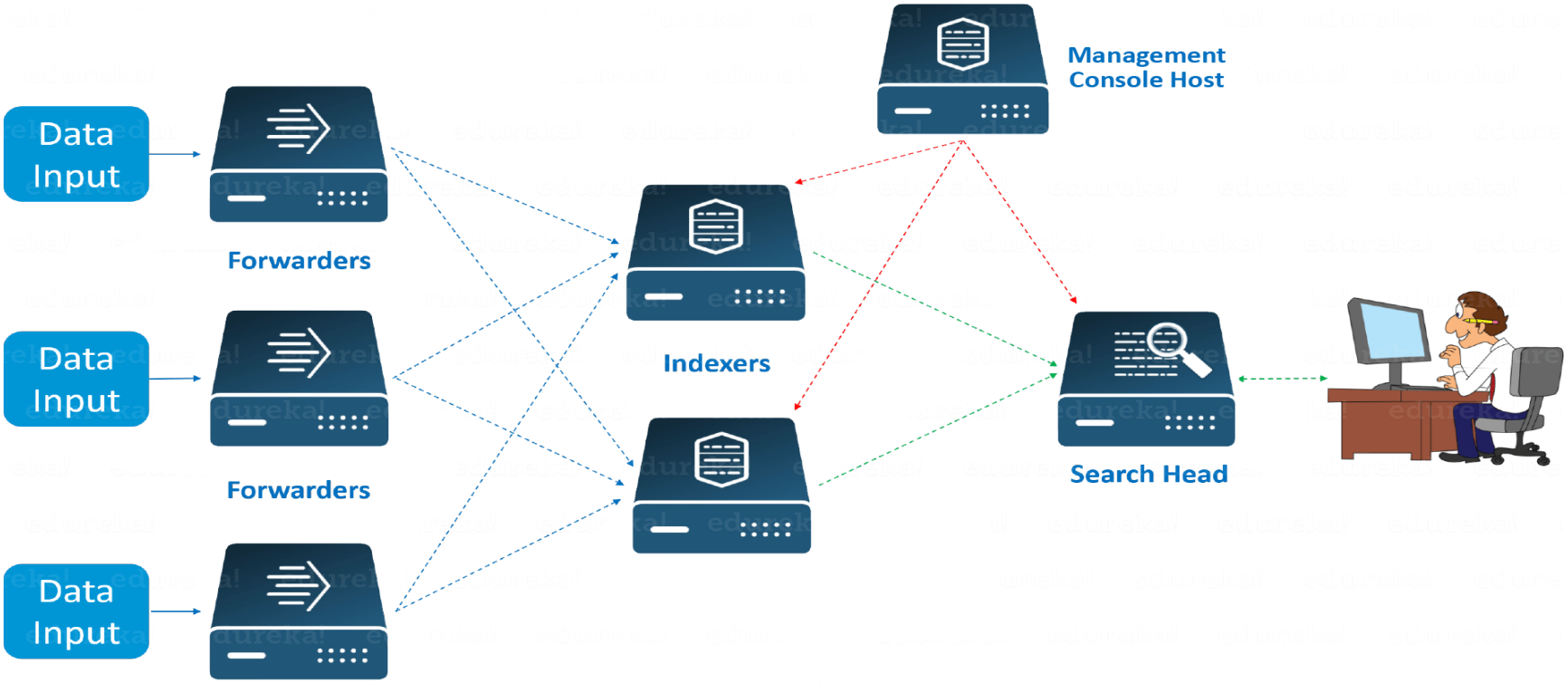
Reporting: The SIEM generates reports to provide an overview of security events, trends, and compliance status. These reports can be used for compliance audits and to improve the security posture of the organization.



Popular SIEM vendor ?

1. Splunk Enterprise Security
2. Azure Sentinal
3. IBM QRadar
4. LogRhythm
5. McAfee Enterprise Security Manager (ESM)
6. Elastic SIEM (formerly known as ELK Stack)
7. Sumologic
8. Exabeam
9. SolarWinds Security Event Manager (formerly Log & Event Manager)
10. ArcSight (Micro Focus)
11. AlienVault USM (now part of AT&T Cybersecurity)
12. RSA NetWitness Platform
13. Fortinet FortiSIEM

Splunk Architecture



Explain the Components in Splunk Architecture

Forwarders:

- Forwarders are like data collection agents.
- They are installed on various data sources like servers, workstations, or network devices.
- Forwarders collect and send log data to the Splunk indexer.

Types : **Heavy Forwarders and Universal Forwarders**

- **Universal Forwarders**:These are lightweight forwarders that are used for sending data to Splunk indexers.
- **Heavy Forwarders :**Heavy forwarders can perform additional data processing and filtering before sending data to indexers. They are optional and used when you need more control over data before indexing

Indexers: They receive data from forwarders, process it, and then index it for quick and efficient retrieval. Indexers are responsible for storing and managing the data.

Search Heads: Search Heads provide the user interface for interacting with Splunk. They allow analysts to search and visualize data, set up alerts, and create reports and dashboards.

Deployment Server: The deployment server helps manage the configuration and updates for the Splunk components.
License Master: The License Master manages licenses for all Splunk instances in your environment.

List the commonly used ports for Splunk

8000: Splunk Web Interface
8089: Management Port
9997: Data Ingestion
8088 (Optional): Indexer Replication (used for data replication in clustered environments)
9997 (Optional): Universal Forwarder (for sending data to indexers)
Splunk Index Réplications Port: 8080
514: Splunk Network port

List the different ways you can search for information in Splunk

1. **Fast Mode**:
    1. This mode is the default and quickest way to search data.
    2. It's designed for fast results and is suitable for most general searches.
2. **Smart Mode**:
    1. Smart Mode uses a combination of Fast and Verbose modes.
    2. It attempts to deliver fast results but will switch to Verbose Mode if it needs to gather more details for the search.
3. **Verbose Mode**:
    1. Verbose Mode provides more detailed search results.
    2. It's useful when you need in-depth information or troubleshooting data.

Explain QRadar architecture overview

1.Data Collection:

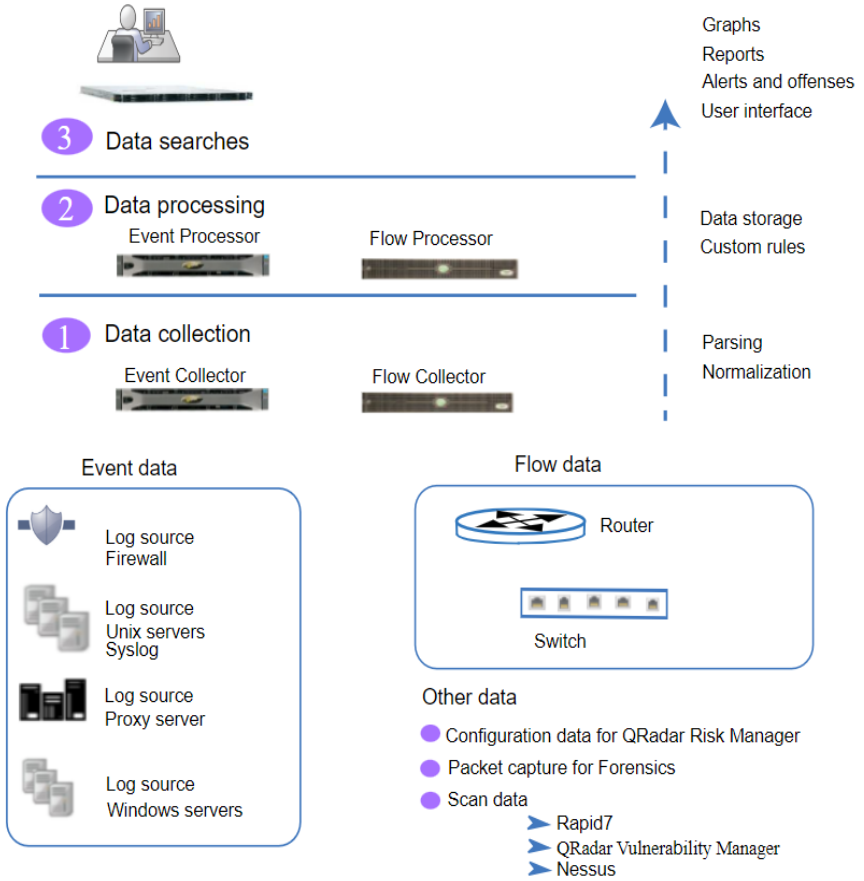
1. This initial layer involves gathering data like events or flows from the network. The All-in-One appliance or collectors such as QRadar Event Collectors and QRadar Flow Collectors can be utilized for this purpose. The collected data is parsed and normalized to ensure a structured and usable format.

2.Data Processing:

1. The second layer, or the data processing layer, runs event and flow data through the Custom Rules Engine (CRE). This process generates offenses and alerts, and the data is then written to storage. Processing can be handled by an All-in-One appliance, and additional appliances like Event Processors or Flow Processors may be added for increased capacity.

3.Data Searches:

1. In the top layer, users access the collected and processed data for searches, analysis, reporting, and investigation through the QRadar Console. Features like QRadar Risk Manager, QRadar Vulnerability Manager, and QRadar Incident Forensics offer additional functionalities for risk management, vulnerability scanning, and forensic investigations.

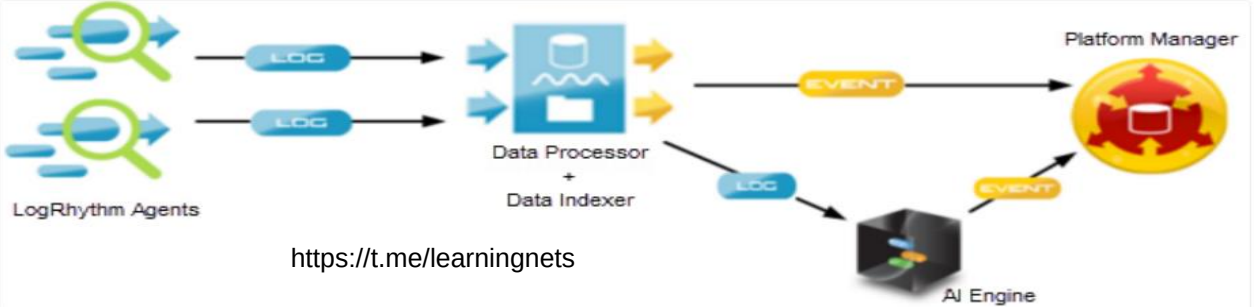


Explain LogRhythm architecture and Components

A basic LogRhythm deployment includes one each of the following components**: Platform Manager, Data Processor, Data Indexer, and System Monitor**.

For low-volume deployments, Platform Manager, Data Processor, and Data Indexer can reside on the same server, while high-volume deployments may require dedicated servers for each.

- The **System Monitor**, which collects log data and forwards it to a Data Processor
- The **Data Processor** forwards Agent log data to the Data Indexer. It is the recommended practice to deploy Data Processors and Data Indexers in a secure internal network. However, in some scenarios it may be advisable to place the Data Processor in a DMZ when Agents will be used to collect from Remote Sites.
- The **Data Processor** is a Windows server. The Data Indexer is a Windows or Linux server, and it should be protected with strict access controls placed on devices that can connect to the log repository if deployed in a DMZ or an untrusted environment
- The **Platform Manager**, containing event records and configuration data, should always be in a secure internal network.



Explain Azure Sentinel architecture and Components

1.Data Connectors:
1. Provides real-time connectivity for Microsoft products and users.
2. Out-of-the-box connectivity to the larger security ecosystem for non-Microsoft products.

2.Workbooks:
1. Monitors connected data sources through Azure monitor workbooks.
2. Allows the creation of unique or pre-built workbook templates for visualizing Sentinel data.

3.Analytics:
1. Correlates alerts using analytics rules into high-security incidents.
2. Users can create custom rules using Kusto Query Language (KQL) or use pre-built rules linked to Microsoft sources.

4.Playbooks:
1. Automates and simplifies security orchestration using Azure Logic Apps.
2. Designed for operations like data intake, enrichment, and investigation.

5.Community:
1. GitHub-powered page with threat intelligence and automation resources.
2. Offers sample hunting queries, playbooks, and workbooks.

6.Workspace:
1. Storage area for information and configuration settings.
2. Used to store data gathered from various sources.

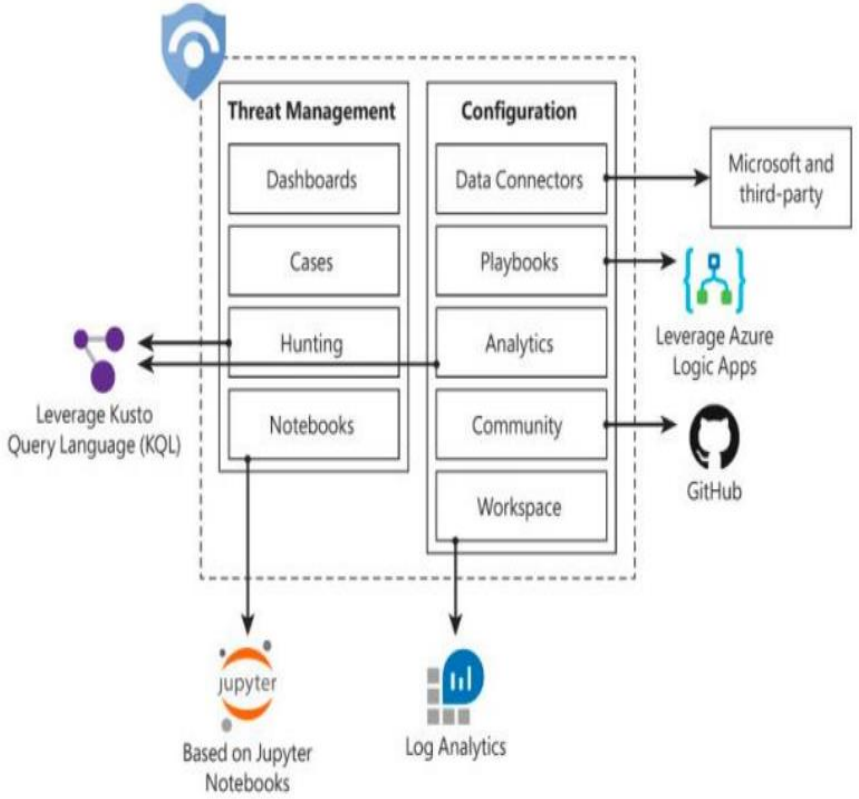
7.Dashboard:
1. Standalone dashboard for visualizing data and configuring rules in real-time.
2. Features machine learning, rule management, and resource analysis.

8.Investigation:
1. Assists in determining the scope and root cause of potential security problems.
2. Launches an investigation based on specific incidents.

9.Hunting:
1. Executes manual and proactive investigations using advanced search tools.
2. Based on the MITRE ATT&CK framework and enhanced by KQL.

10.Notebooks:
1. Supports Jupyter notebooks in Azure ML workspaces.
2. Enables machine learning, visualization, and data analysis, with integrated code

Azure Sentinel Components:



Explain ELK (Elastic search) architecture and Components

Beats are open-source data shippers that you install as agents on your systems. Beats send security events and other data to Elasticsearch.

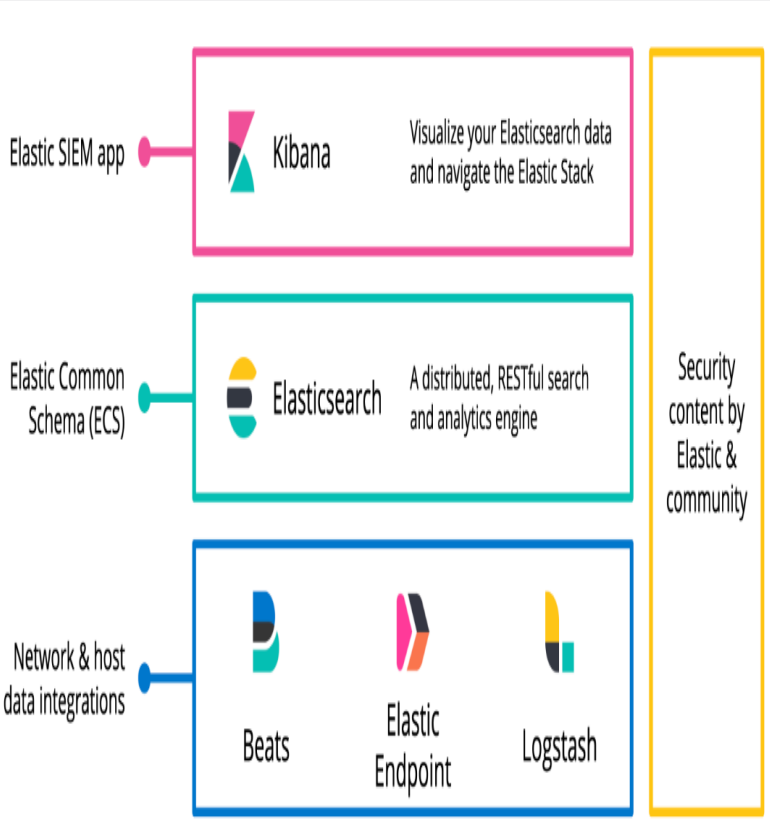
•**Logstash:** Ingests and processes log data from various sources. It can parse, filter, and transform raw logs before sending them to Elasticsearch.

•**Elasticsearch:** Serves as the core data store and search engine. It stores and indexes security-related data for fast and efficient retrieval.

•**Kibana:** Provides the user interface for visualizing and analyzing security data. It allows security analysts to create custom dashboards, conduct searches, and investigate security incidents.

Elastic Common Schema (ECS):ECS is a standardized schema for the Elasticsearch SIEM module. It provides a common framework for organizing and mapping fields within logs, facilitating correlation and analysis.

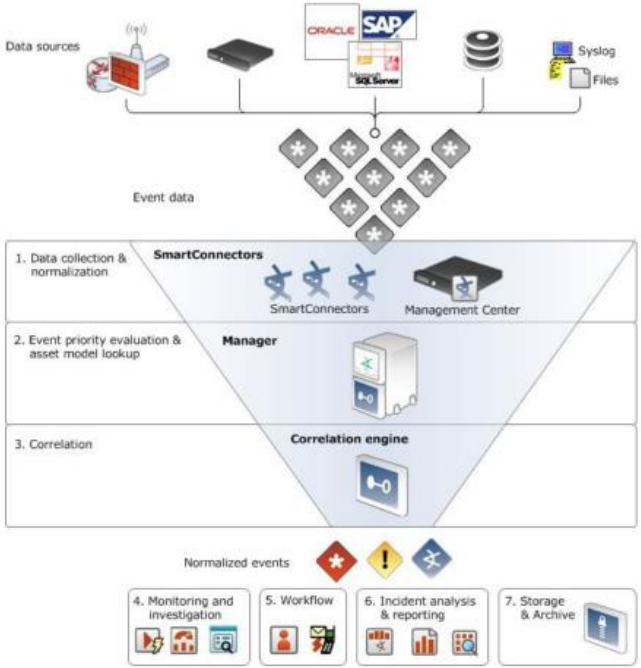
SIEM App in Kibana: The SIEM app in Kibana is a dedicated workspace for security analysts. It includes pre-built visualizations, dashboards, and tools specifically designed for threat detection and incident response.



Explain Arcsight architecture and Components

- ArcSight Enterprise Security Manager (ESM), ESM uses **Smart Connectors** to collect event data from your network. Smart Connectors convert device event data into a standardized schema that serves as the basis for correlation.
- In the **CORR-Engine, the Manager** processes and stores event data.
- Users can use the ArcSight Console or the ArcSight Command Center to monitor events, run reports, generate resources, conduct investigations, and manage the system.
- Additional ArcSight solutions that drive event flow, ease event analysis and provide security alerts and incident response are built on ESM's fundamental architecture.
- **ArcSight Logger** enables automated compliance reporting and log management and storage. It has a storage capacity of up to 42TB of log data and can search for multiple events per second across organized and unstructured data

ESM processes events in phases to identify and act upon events of interest. The graphic below provides an overview of the major steps in the life cycle of an event:



Data sources generate thousands of events. SmartConnectors, hosted individually or part of the ArcSight Management Center, parse them into the ESM event schema. Each step narrows events down to those that are more likely to be of interest.

Once the event stream is narrowed, ESM provides tools to monitor and investigate events of interest, track and escalate developing situations, and analyze and report on incidents. Event data is then stored and archived according to policies set during configuration.

This process is detailed in the following sections:

MITRE ATT&CK

TTP (Tactics, Techniques, and Procedures.)

TTPs stands for Tactics, Techniques, and Procedures.

The Tactics refer to the overall goals and objectives of the attacker, such as stealing data, gaining unauthorized access to a system, or disrupting operations.

One Example of tactics in MITRE framework is Initial access, Execution etc

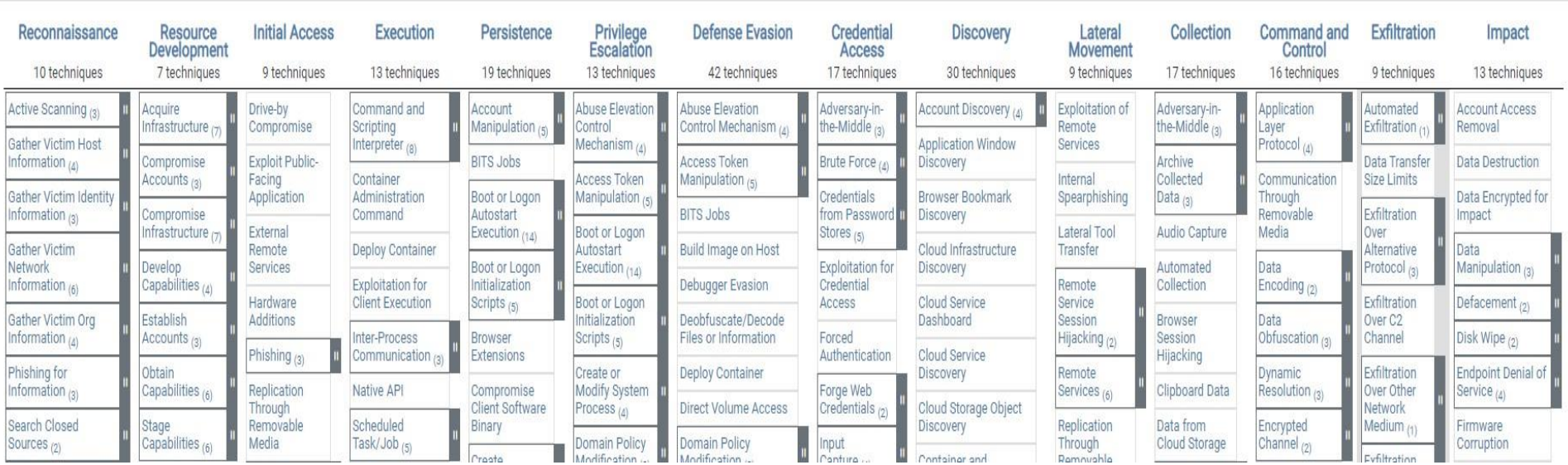
The Techniques refer to the specific methods and tools that attackers use to achieve their goals, such as exploiting a vulnerability, using malware, or social engineering.

One Example of Techniques in MITRE framework for Initial access is Phishing

The Procedures refer to the step-by-step process that attackers follow to carry out their attack, such as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives (AOO).

MITRE ATT&CK framework

MITRE ATT&CK: This framework focuses on adversary or attacker behavior and tactics, techniques, and procedures (TTPs) used in cyber attacks. It provides a comprehensive list of known TTPs and helps organizations to identify, detect, and respond to them.



Mitre framework TTP's (Phases in Mitre)

Reconnaissance: gathering information to plan future adversary operations, i.e., information about the target organization.

Resource Development: establishing resources to support operations, i.e., setting up command and control infrastructure.

Initial Access: trying to get into your network, i.e., spear phishing.

Execution: trying the run malicious code, i.e., running a remote access tool.

Persistence: trying to maintain their foothold, i.e., changing configurations.

Privilege Escalation: trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access.

Defense Evasion: trying to avoid being detected, i.e., using trusted processes to hide malware.

Credential Access: stealing accounts names and passwords, i.e., keylogging.

Mitre framework TTP's (Phases in Mitre) Cont...

Discovery: trying to figure out your environment, i.e., exploring what they can control.

Lateral Movement: moving through your environment, i.e., using legitimate credentials to pivot through multiple systems.

Collection: gathering data of interest to the adversary goal, i.e., accessing data in cloud storage.

Command and Control: communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network.

Exfiltration: stealing data, i.e., transfer data to cloud account

Impact: manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

Initial Access: How can attackers successfully gain Initial Access to a target system?

Attackers may use various methods to gain Initial access of targeted machine
such as exploiting unpatched vulnerabilities,
conducting spear-phishing campaigns,
leveraging stolen credentials.

Attackers use spear-phishing for the initial breach.
A finance employee receives a tailored email with a malicious budget spreadsheet. Opening the spreadsheet activates a payload, providing access to the attacker.
The attacker then elevates privileges for greater control, employs techniques to avoid detection, captures login credentials, navigates the network, identifies vulnerabilities, collects sensitive organizational data, and exfiltrates it, impacting the organization's security.

Execution: how attackers execute malicious code on a compromised system during the Execution phase.

Attackers may use techniques like
Running malicious scripts,
Leveraging PowerShell commands,
Exploiting software vulnerabilities…etc

•For instance, executing a payload through a Microsoft Word macro in a spear-phishing document.
In a common scenario, attackers hide malicious PowerShell commands in documents, such as Word files sent via phishing emails. When victims open these documents and enable macros, the concealed PowerShell commands run, leading to the download and execution of malware like Emotet.
This enables attackers to gain a foothold, deploy additional payloads, and potentially exfiltrate sensitive data. The versatility and evasiveness of PowerShell make it a frequent choice for code execution in the Execution phase of advanced cyber campaigns.

Persistence : how attackers establish Persistence on a compromised system.

Attackers might achieve persistence by
creating scheduled tasks
Modifying registry entries,
Installing backdoors.

For instance, creating a scheduled task to execute a malicious payload at regular intervals.

Attackers establish persistence on compromised systems by strategically creating scheduled tasks. After an initial breach through methods like phishing or exploiting vulnerabilities, they upload a backdoor or malicious script.
To maintain continuous access, they exploit the operating system's scheduled task functionality, creating a task that runs their payload at set intervals. This scheduled task serves as a persistent mechanism, allowing prolonged access without immediate detection.

Privilege escalation : How do attackers typically escalate privileges after gaining initial access?

Attackers might
Exploit vulnerabilities in the operating system or applications,
Abuse misconfigurations,
use privilege escalation tools.

For example, leveraging a zero-day vulnerability to escalate privileges on a Windows system.

Attackers often escalate privileges after gaining initial access to expand their control over a compromised system. One common method involves exploiting vulnerabilities or misconfigurations to gain higher-level permissions. For instance, an attacker may discover a system vulnerability that allows them to execute arbitrary code with low-level privileges. Once inside, they may search for and exploit additional vulnerabilities, use privilege escalation exploits, or employ techniques like abusing misconfigured permissions or weak authentication protocols to gain higher-level access. A real-world example includes exploiting a Windows privilege escalation vulnerability, such as the "Pass-the-Ticket" attack in Kerberos authentication, allowing an attacker to forge tickets and elevate their privileges on the compromised system.

Defenses Evasion : how attackers successfully evade security defenses during an attack.

Attackers can use techniques
code obfuscation,
encryption,
disabling security tools.

For instance, using encryption to hide malicious payload traffic from network-based detection systems
In this example, the attacker might use PowerShell, a legitimate scripting language, to execute malicious commands directly in memory, making it challenging for traditional antivirus programs to identify and block the malicious activity.
By avoiding the creation of suspicious files, the attacker can evade conventional security defenses that rely on file-based detection methods.
This illustrates the need for advanced threat detection mechanisms that can identify and respond to anomalous behavior and tactics beyond traditional signature-based approaches.

Credential access: Provide an example of how attackers obtain credentials during an attack.

Attackers may use techniques like credential dumping, keylogging, or password spraying.

Attackers often employ various methods to obtain credentials during an attack, and one common technique is phishing. In a scenario, imagine an attacker sending deceptive emails to employees within an organization, posing as a trusted entity, such as the IT department or a reputable service provider. The email may contain a seemingly legitimate link to a fake login page that mimics the organization's login portal.

Once an unsuspecting user enters their credentials on the fake page, the attacker captures the information. With these stolen credentials, the attacker gains unauthorized access to the victim's account and potentially escalates privileges within the network. This method highlights the effectiveness of social engineering in tricking individuals into divulging sensitive information, emphasizing the importance of user education and robust multi-factor authentication measures to mitigate such attacks.

Discovery: How do attackers conduct Discovery to gather information about a target environment?

Attackers use techniques
network scanning,
Querying Active Directory
using public information sources.

For example, using tools like Nmap to scan for open ports and services.

After exploiting a web server vulnerability, the attacker conducts Discovery within the compromised system, examining files, logs, and configurations. Tools like 'ipconfig'/'ifconfig' gather network data, identifying IPs and neighboring systems. 'Nmap' scans unveil open ports, potential entry points. 'Systeminfo'/'uname -a' provide OS insights;
Registry queries extract configuration details. Harvested credentials aid lateral movement, guiding post-exploitation actions. Swift security measures are crucial.

Lateral Movement: how attackers move laterally within a network after gaining initial access.

Lateral movement is a critical phase in an attacker's progression within a network. Once initial access is achieved, attackers seek to navigate horizontally, exploring different systems and domains to escalate privileges and broaden their influence.
Common techniques involve the exploitation of weaknesses in authentication protocols, leveraging compromised credentials, and exploiting vulnerabilities in unpatched systems.

For instance, an attacker may use tools like PowerShell or Mimikatz to extract credentials and move laterally, attempting to access higher-value assets.

This phase demands sophisticated detection mechanisms to identify abnormal patterns of behavior, anomalous access requests, or unusual data flows that could indicate unauthorized lateral movement. Implementing strong network segmentation, robust access controls, and continuous monitoring are essential defenses against lateral movement strategies.

Command and Control: How do attackers typically achieve Command and Control within a network?

Command and Control (C2) is a crucial phase in the Mitre ATT&CK framework where attackers establish communication channels to manage compromised systems.

Attackers often leverage various techniques, such as using custom protocols, domain fronting, or exploiting trusted communication channels like HTTP or DNS.

They may employ malware with built-in C2 capabilities or repurpose legitimate tools for unauthorized communication. Detection mechanisms need to focus on identifying abnormal network traffic patterns, unexpected data flows, or unusual communication behavior to mitigate the risks associated with Command and Control tactics.

Implementing robust network monitoring, intrusion detection systems, and endpoint protection are essential for detecting and preventing C2 activities effectively.

Exfiltrate: How do attackers exfiltrate data from a compromised environment successfully?

Attackers employ various sophisticated techniques for successful data exfiltration. Common methods include using covert channels within legitimate network protocols, encrypting stolen data to avoid detection, and disguising exfiltration as normal network traffic.

Additionally, attackers may leverage DNS tunneling, steganography, or even trusted cloud services to exfiltrate data unnoticed.

Implementing robust data loss prevention measures, monitoring for unusual data transfer patterns, and employing encryption are crucial defenses against these exfiltration tactics.

Detection relies on anomaly detection systems, network monitoring, and a comprehensive understanding of the organization's data flow to identify and prevent unauthorized data exfiltration

SOC Fundaments and Workflow

L1 SOC Analyst Key Responsibilities

Key responsibilities

- **Monitoring and investigating security incidents triggered from Various Security Controls (By Following SOP''s)**
- **Assist in incident response activities, collaborating with L2 & L3 analysts.**
- **Follow SOPs for incident containment, eradication, and recovery.**
- **Document all actions taken during incident investigation and response.**
- **Providing timely incident reports.**
- **Monitoring and Investigating user reported Phishing emails.**
- **Actively utilize security tools such as EDR, Email Gateway, Proxy, DLP, WAF, etc., for the analysis of network traffic and system logs.**
- **Give detailed shift reports for a smooth transition**

L2 SOC Analyst Key Responsibilities

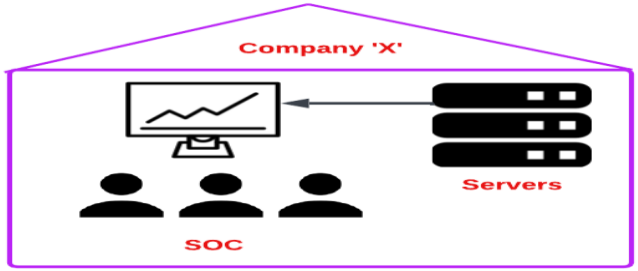
My Key responsibilities included :

- Review and triage alerts generated by the SIEM system, prioritizing them based on severity and relevance.
- Conduct in-depth investigations into alerts and anomalies to determine the root cause and potential impact on the organization's security. Apply additional context to events and alerts, correlating information from various sources to understand the broader security picture.
- Evaluate alerts to identify false positives and eliminate noise, ensuring that We focuses on genuine security threats.
- I prioritize and categorize incidents, ensuring that critical ones receive immediate attention. I escalate Those incidents with Initial analysis to L3 or higher-level teams when needed, Helping to quickly and efficiently respond.
- Fine-tune SIEM rules and configurations based on analysis and feedback to improve the accuracy and relevance of generated alerts.
- I play a central role in coordinating incident response activities, working closely with different teams to ensure a smooth and effective response to security incidents.
- Creation and documentation of SOPs and regular updates to SOPs for various security processes, including incident response, threat hunting, and log analysis
- Generate regular reports summarizing SIEM activities, incident trends, and key metrics for presentation to management, stakeholders, and regulatory bodies.
- Monitor the health and availability of the SIEM platform, ensuring that it operates optimally to support security monitoring activities.

What All Tools and Technologies you are using in SOC

What type of SOC Model you are working (Inhouse/MSSP/Hybrid SOC)

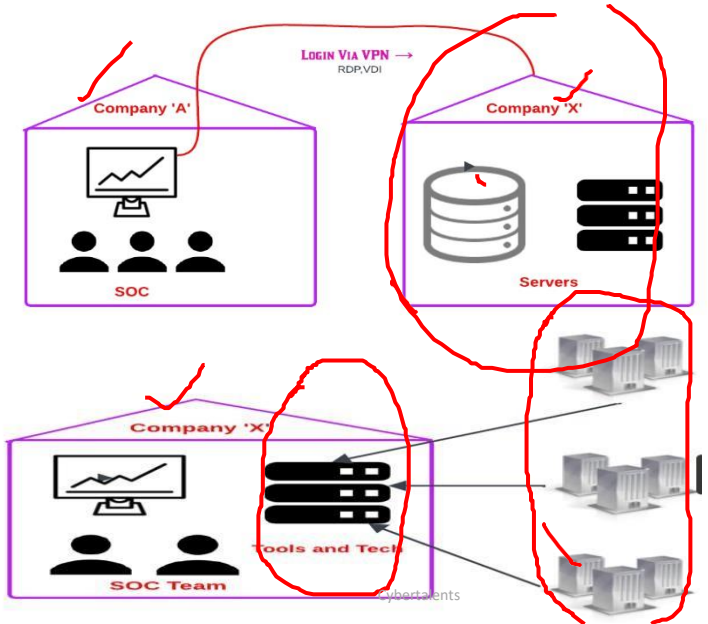
Inhouse:
I am part of an in-house SOC, which is dedicated to secure the internal assets and information of our organization. Our focus is on maintaining the security posture of the company's networks, systems, and data



MSSP (Managed Security Service Provider) SOC:

Dedicated MSSP: I work in a Dedicated MSSP SOC, where we provide cybersecurity services to multiple clients. Each client has a dedicated SOC team, and our responsibilities include monitoring and responding to security incidents on behalf of our clients. We log in to client environments via VPN and utilize security tools and technology to secure the organization.

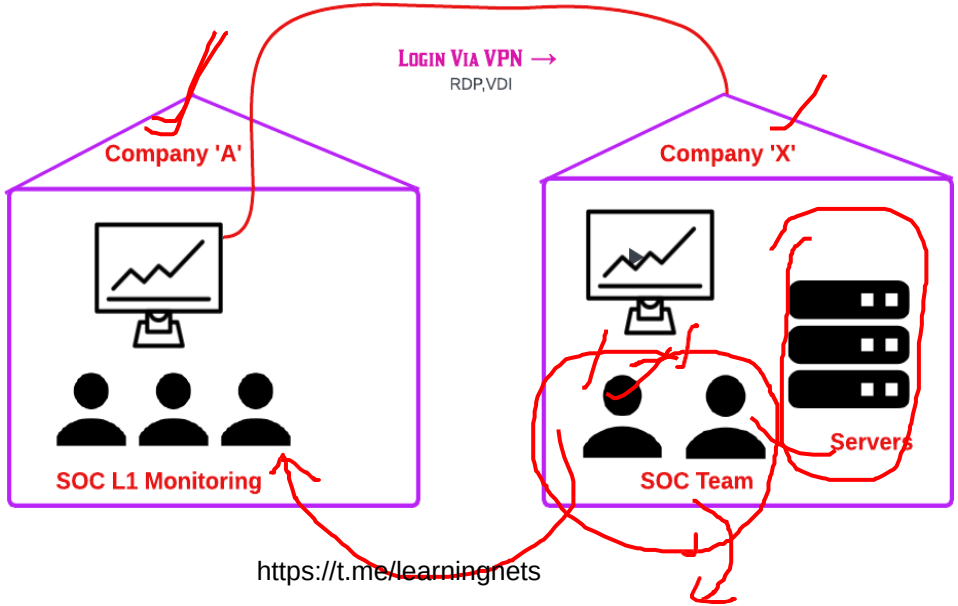
In the shared MSSP model, tools and technology are hosted within our environment (service provider). Multiple clients send logs to us for monitoring, threat detection, and analysis. In this model, responsibilities for security operations are shared between the service provider and the client



What type of SOC model you are working (Hybrid SOC)

I am a member of a **hybrid SOC**, which combines elements of both in-house and MSSP models. We manage the security of our organization's internal assets while also offering security services to external clients.

In a Hybrid SOC, we manage all higher-level security operations for our company, while L1 SOC operations are taken care of by a Service Provider.



What is your Security team size and Hierarchy

The SOC team consists of

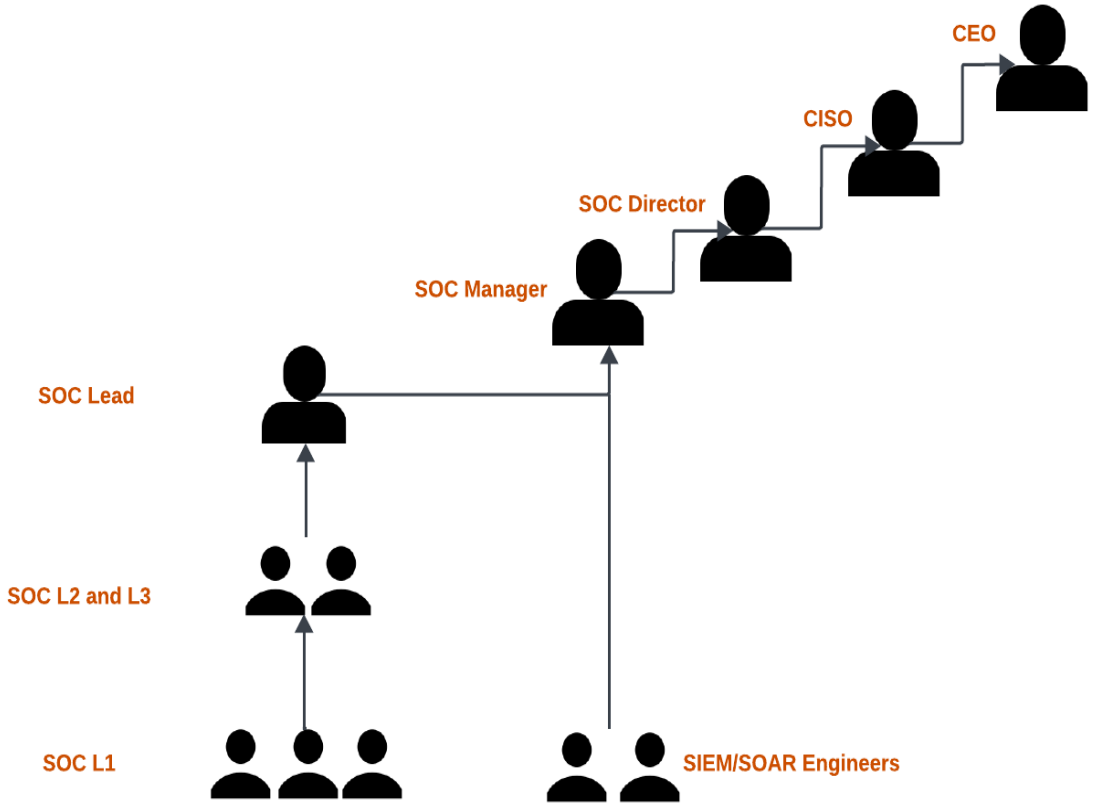
- ‘X’ SOC L1 analysts ,
- 'X' SOC L2 analysts,
- SOC L3/Lead, SOC Manager and Director

- L1,L2 reports to SOC L3/Lead or SOC Manager

- L3 report to SOC Manager/Director

- SIEM/SOAR Engineers reports SOC Lead/SOC Manager

- SOC Managers report to the Director, who, in turn, reports to the Chief Information Security Officer (CISO). The CISO reports directly to the Chief Executive Officer (CEO)."



What all Different Log sources Integrated to your Clients SIEM

Servers and Hosts:

- Antivirus and endpoint protection logs
- File integrity monitoring logs
- Linux/Unix system logs
- Application logs (e.g., web servers, database servers)
- Windows event logs

Network Devices:

- Intrusion Detection/Prevention Systems (IDS/IPS)
- Proxies
- Routers and switches
- Firewalls
- Load balancers

Security Devices:

- Data Loss Prevention (DLP) logs
- Web Application Firewalls (WAF) logs
- Intrusion Detection/Prevention Systems (IDS/IPS) logs

Endpoint Security:

1. Antivirus and endpoint protection logs
2. Host-based intrusion detection system logs
3. User and system activity logs

Applications and Databases:

- Application-specific logs (e.g., ERP systems, CRM systems)
- Database logs (e.g., MySQL, Oracle, SQL Server)
- Web server logs (e.g., Apache, Nginx, IIS)

DNS and DHCP:

- DNS server logs
- DHCP server logs

Email and Messaging:

- Email server logs
- Instant messaging logs

Authentication and Authorization:

- Authentication server logs (e.g., RADIUS, TACACS+)
- VPN logs
- Remote Desktop logs

Cloud Services:

- Cloud provider logs (e.g., AWS CloudTrail, Azure Monitor)
- Cloud application logs (e.g., AWS S3 access logs, Azure App Service logs)

Third-Party Applications:

- Logs from third-party security solutions (e.g., vulnerability scanners, security analytics
- tools) &Logs from custom-built applications

How many Alerts You received per day

I work for 24*7 rotational shifts. The number of alerts receive per day varies significantly, relying on the specific client and the type of SOC in operation. In my current role at a Dedicated MSSP, We as SOC team typically handle around 40-50 alerts daily. However, in a Shared MSSP environment, the volume can increase substantially, ranging from 200-250 alerts daily.

Describe how you categorize and prioritize incidents in your SOC

- We classify incidents according to their type, such as malware infections, phishing attempts, or unauthorized access.
- The prioritization process considers the potential impact on critical assets and the overall risk posture of the organization.
- Service Level Agreements (SLAs) are linked to the prioritization, ensuring a timely and effective response based on the severity of each incident.

Priority Level	Description	Target Response Time
P1	Critical	15 Minutes
P2	High	30 Minutes
P3	Medium	2 Hours
P4	Low	4 Hours

At the beginning of your shift as a SOC analyst, what tasks do you typically perform?

Shift Handover Review:

I review any ongoing incidents or alerts from the previous shift by checking the shift handover documentation. This helps me understand the current state of the environment and any unresolved issues.

Check Alerts and Incidents:

I examine the real-time alerts generated by our security tools and investigate any incidents that might have occurred during the previous shift. This involves looking at the severity levels and understanding the nature of each alert.

System Health Check:

I perform a quick check on the health of critical systems. including components of the SIEM and other vital log sources. This involves ensuring that all security tools are functioning properly, logs are flowing as expected, and there are no issues affecting the overall infrastructure.

Communication and Collaboration:

At the start of my shift, I talk to the SOC analyst finishing their shift to get more details about the current security issues. I also work closely with my team, sharing information and working together to respond effectively to any incidents

Update Documentation:

I make sure to update incident logs, documentation, and any important runbooks at the beginning of my shift. This helps keep our records accurate and current, ensuring we have a clear and complete view of incidents and our responses.

Prepare for Shift Briefing:

I prepare for the shift briefing by summarizing any notable incidents or observations. This information is shared with the next shift to ensure a seamless transition and awareness of the current security landscape."

Collaborative Functions within the SOC Team

SIEM Administration and Engineering:

work closely with the SIEM administration and engineering teams to ensure the optimal performance and configuration of our Security Information and Event Management (SIEM) system. This involves fine-tuning rules, creating custom dashboards, and addressing any issues related to log ingestion and correlation

Collaboration with the SOAR (Security Orchestration, Automation, and Response) team is crucial as we work together to automate and orchestrate incident response processes.

SOAR (Security Orchestration, Automation, and Response):

We work together to create and refine playbooks, automate repetitive tasks, and integrate various security tools.

By doing so, we aim to streamline and optimize our incident response workflows, ensuring a more efficient and effective response to security incidents

Threat Intelligence:

Regular interaction with the Threat Intelligence team is essential. We integrate threat feeds into our SIEM, enhancing our ability to correlate events and proactively detect known threats.

Malware Analysis:

- *Collaboration:* Close coordination with the malware analysis team is critical for identifying and mitigating advanced threats. We collaborate on analyzing suspicious files, understanding malware behavior, and implementing countermeasures to prevent and respond to malware incidents.

Endpoint Security Team:

The endpoint security team is a key partner in securing individual devices. We collaborate on endpoint protection strategies, share information on endpoint incidents detected by the SIEM, and work together to address vulnerabilities at the endpoint level.

Network Security Team:

We engage regularly, exchanging insights into network traffic patterns and collectively addressing any anomalies that impact network security. This includes proactive measures such as blocking URLs and IP addresses, ensuring a unified and responsive approach to safeguarding our network infrastructure.