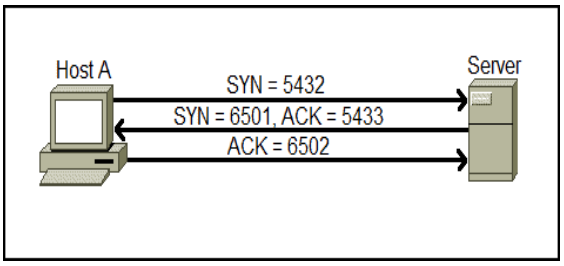
Commonly Asked Top 50 Questions and Answers in SOC Interviews

Q1: Explain 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

Q2: Explain 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.



Q3: 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.

Q.4 What is 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 enter a domain name in your web browser, your computer initiates a request to a DNS Server (resolver) to find the corresponding IP address. If the DNS server successfully locates the IP address, it returns the information to you. If not, the following process unfolds.

- The DNS Server (resolver) then sequentially queries a set of DNS servers, commencing with the root servers, which possess information about Top-Level Domains (TLDs). Each TLD shares the IP address of the authoritative DNS server for that specific domain name.

- The authoritative DNS server (Second-Level Domain - SLD) is tasked with maintaining the DNS records for the domain, including the IP address of the web server. Once the authoritative DNS server is identified, the DNS resolver stores the IP address in its cache and provides it to your web browser.

- Subsequently, the client computer utilizes the obtained IP address to establish a connection with the designated website or domain.

Q.5 What is Firewall? What is Stateful Inspection in Firewall

A firewall serves as a network security mechanism, overseeing and regulating both incoming and outgoing network traffic according to a predefined set of security rules. Positioned as a barrier between an internal network and external networks, such as the Internet, its primary function is to thwart unauthorized access to or from the network.

Stateful inspection represents a firewall technology that actively monitors and administers network connections by maintaining awareness of the state of each connection. It selectively permits traffic that aligns with established connections, contributing to a more refined control mechanism.

Compared to traditional packet filtering firewalls, stateful inspection firewalls offer heightened security. This is attributed to their capability to recognize and obstruct various types of attacks, providing a more comprehensive defense against potential threats.

Q.6 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.

Q.7 Protocols and Port Number

Protocol	Description	Port num
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

Q.8 Explain 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.

Q.9) What is 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.

Q.10) What is 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

Q.11) 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.

Q.12) 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 malwares:

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.

Q.13 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	Example: The Zeus Trojan (Zbot) is a well-known example that targeted online banking users, capturing their login credentials and financial information.

Q.14 What is Threat, Vulnerability and Risk

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

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 damage to a system or organization

Q.15) 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

Q.16) 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

Q.17) 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.

Q.18) Explain DOS and DDOS Attacks

DoS (Denial-of-Service) attack in which single system 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.

Q.19) 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.

Q.20) Explain 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

Q.21) Explain SQL Injection and how we Mitigate?

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.

Q.22) Explain 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

Q.23) What is TTP

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).

Q.24) Explain 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.

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

Q.25) Explain 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.

26) Explain Incident response and 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.

27) Common 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.

28) What is Threat Hunting, and why is it important

Threat Hunting in Simple Terms:

Threat hunting is like a proactive cybersecurity detective work. Instead of waiting for alarms, it involves actively searching for signs of hidden threats in computer systems to stop them before they cause harm.

Why Threat Hunting is Important:

Proactive Defense: It allows for actively seeking and neutralizing threats before they trigger alerts.

Unknown Threats: Finds new or sophisticated threats that may be missed by traditional security measures.

Reducing Dwell Time: Shortens the time threats go undetected, minimizing potential damage.

Understanding the Environment: Deepens knowledge of an organization's digital environment, making anomalies easier to spot.

Continuous Improvement: Drives ongoing improvement by learning from each hunt, enhancing overall cybersecurity.

29) Can you tell me what you understand Threat Intelligence

- 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.

30) What is Pyramid of Pain

- Pyramid of Pain is a Visual Representation of Six different sorts of attack indications, Grouped in Escalating order of Threat actor and Security analyst work.
- Pyramid Represents different types of attack indicators you might use to detect adversary’s activities and is broken up by how much pain it will cause Attacker when you are able to deny those indicators to them

31) 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.

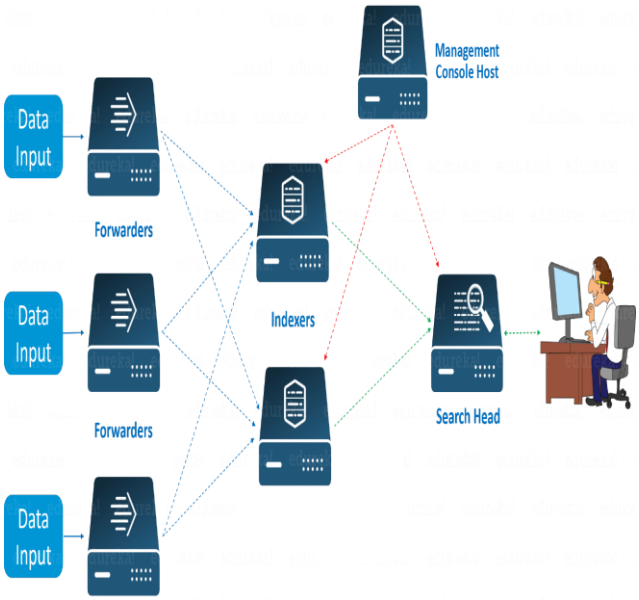
- **Heavy Forwarders** : Heavy forwarders can perform additional data processing and filtering before sending data to indexers. They are optional and used when you need more control over data before indexing

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.



Q. 32) What is 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.

Q.33) What is 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.

Q.34) What is 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 Event1
- Event 3: An outbound connection from the same IP address to a known malicious domain.

Q.35) What is 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

Q.36) 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

Q.37) Could you list some key Splunk search commands that are frequently used for data analysis?

1. search: The fundamental command to search and retrieve data from your indexed events.
2. stats: Used for statistical analysis, aggregation, and calculations on search results.
3. eval: Allows you to create calculated fields or modify existing fields in search results.
4. table: Used to format search results as a table, making it easier to view and analyze data.
5. timechart: Creates time-based charts and graphs to visualize data trends over time.
6. rex: Helps extract fields from raw event data using regular expressions.
7. dedup: Removes duplicate events from search results based on specified fields.
8. top: Identifies and displays the top values in a field, useful for finding patterns or outliers.
9. where: Filters search results based on specified conditions or criteria.
10. sort: Sorts search results based on one or more fields, either in ascending or descending order.
11. join: Allows you to combine results from multiple subsearches or sources using common fields.
12. lookup: Enables the use of external lookup tables to add additional information to your search results.
13. transaction: Groups related events together based on specified criteria, which is useful for working with event sequences.

14. spath: Extracts fields from structured data formats like JSON and XML.
15. geostats: Generates geospatial statistics and visualizations for location-based data.

Q.38) What do 'Buckets' refer to, and can you describe the lifecycle of Splunk Buckets?

Buckets in Splunk are essentially directories used to store indexed data, each corresponding to a specific time period. The lifecycle of Splunk Buckets involves several stages:

1. Hot: Hot buckets are where newly indexed data is stored, and they remain open for writing and new additions. An index can have one or more hot buckets simultaneously.
2. Warm: Warm buckets contain data that has been rolled out from hot buckets. This stage represents data that is no longer actively receiving new entries.
3. Cold: Cold buckets store data that has been rolled out from warm buckets. This stage signifies older data that is less frequently accessed.
4. Frozen: Frozen buckets hold data that has been rolled out from cold buckets. By default, the Splunk Indexer deletes the data in frozen buckets. However, there is an option to archive this data. It's essential to note that frozen data is not searchable.

Q.39) What is the impact when the Splunk cluster master goes down in a cluster?

- Configuration: You can't make changes or adapt to new data needs.
- Replication: Data availability and redundancy can be disrupted.
- Topology: Adding/removing indexers or adjusting topology becomes challenging.
- Search Head Clustering: Adding new search heads or managing existing ones becomes problematic.
- Data Routing: Efficient data routing within the cluster is hampered.
- Recovery: A plan for promoting a new cluster master is needed.
- High Availability: Redundancy, like a secondary cluster master, minimizes downtime.

Q.40) What are the consequences when all the search heads become unavailable in a 3-member cluster?

- When all search heads go down in a 3-member Splunk cluster, the immediate impact is a complete loss of search and data retrieval capabilities. Users can't execute searches, and query functionality is significantly limited. However, data ingestion continues.
- Administrative tasks can still be performed, but to address the loss of search functionality, a recovery plan is essential. High availability measures, such as deploying redundant search heads, can help minimize downtime and maintain user access to the data."

Q.41) What are the implications when the Deployment Server (Deployer) goes offline in a Splunk environment?

When the Deployment Server (Deployer) in a Splunk environment goes down:

- Centralized configuration changes and app deployments are halted.
- Consistency and compliance across the environment may be compromised.
- Monitoring and management become more challenging.
- Cluster and forwarder management can be affected.
- Security-related settings may not be updated in a timely manner.
- To mitigate this, redundancy and a recovery plan are crucial

Q.42) Scenario: An SOC analyst notices a substantial spike in inbound network traffic on a specific server in the organization's data center around 2:00 AM, even though this time typically sees minimal activity. The spike continues for about 30 minutes and then decreases. The server hosts an internal application used for file sharing among employees.

Initial Observations:

The monitoring system flags an abnormal increase in incoming traffic.

Upon further review, the traffic is primarily coming through port 22 (SSH) and port 80 (HTTP).

Identification of the Affected System:

The surge is isolated to a single server within the data center, which hosts the file-sharing application.

Traffic Analysis:

- Examination of the inbound traffic reveals an unusually high number of HTTP requests during this period. The data transfer through SSH is also spiking.
- Most of the incoming connections appear to be coming from various IP addresses, some of which are located overseas.

Source and Destination Verification:

The destination IP addresses are predominantly external and don't correspond to any known legitimate connections for this application.

There's no indication of any outgoing traffic from the server during the surge.

- Security Breach Investigation:
- Further investigation reveals the potential for unauthorized access attempts or a brute-force attack through SSH based on failed login attempts.
- The pattern of HTTP requests looks like a potential attempt to exploit the application's web interface.

Mitigation and Action:

1. The system administrator promptly implements additional security measures to reinforce SSH access.
2. Immediate action is taken to limit access from foreign IP addresses and block the suspect traffic.

Follow-up Actions:

Plans are made to update security rules, intensify monitoring on the file-sharing application, and implement patches if vulnerabilities are identification.

Q.43. Scenario A company server experiences a sudden crash, and there are indications of a DDoS (Distributed Denial of Service) attack. What steps would you take to respond to this incident?

Initial Triage:

Example: Quickly verify the server crash and check for any unusual patterns in network traffic indicating a DDoS attack. Use monitoring tools to identify the type and scale of the attack.

Isolate the Affected Server:

Example: If possible, isolate the affected server to prevent further impact on other network resources and services.

Traffic Analysis:

Example: Use network traffic analysis tools to identify the characteristics of the DDoS attack, such as the source IP addresses, patterns, and types of traffic flooding the server.

Filter Malicious Traffic:

Example: Implement traffic filtering or rate-limiting rules on network devices to block or mitigate the malicious traffic. This might involve configuring firewalls, routers, or dedicated DDoS mitigation devices.

Cloud-Based DDoS Protection:

Example: If applicable, engage cloud-based DDoS protection services that can absorb and filter out the malicious traffic, allowing legitimate traffic to reach the server.

Incident Notification:

Example: Notify key stakeholders, including IT personnel, network administrators, and relevant management, about the DDoS incident. Establish communication channels for ongoing updates.

Incident Documentation:

Example: Document the incident, including the timeline of events, actions taken, and lessons learned. This documentation is valuable for post-incident analysis and reporting.

Q.44) A High number of failed login attempts are detected on multiple user accounts. What does the process of alert verification and what steps would you take to resolve this issue?

Alert Verification:

- Review access logs or authentication logs to identify the specific accounts experiencing multiple failed login attempts.
- Analyze the patterns of failed login attempts. Look for commonalities such as specific timeframes, IP addresses, or geographic locations to determine if it's a coordinated attack or random occurrence.
- Verify the source of the authentication attempts. Determine if they are coming from internal network sources, external IP addresses, or a combination of both.
- Investigate if there are any recent changes in the authentication system or network configurations that might be triggering false positives. Confirm that the failed login attempts are not due to system updates or legitimate changes.

Once you have verified the alert and confirmed that there is indeed a concerning pattern of failed login attempts, you can take the following measures:

Measures to Address the Issue:

Isolate Compromised Accounts:

- Temporarily disable affected accounts to prevent unauthorized access.

Account Lockout Policy:

- Implement or adjust account lockout policies to thwart brute-force attacks.

Password Reset:

- Reset passwords for compromised accounts and notify affected users.

Two-Factor Authentication (2FA):

- Strengthen security with the implementation or enhancement of 2FA.

Investigate Source IP Addresses:

- Analyze and block malicious source IP addresses.

User Education:

- Educate users on password hygiene and the importance of reporting suspicious activities.

Enhanced Monitoring:

- Intensify monitoring for real-time detection and response.

Incident Documentation:

- Document the incident for post-incident analysis and reporting.

Q.45) How Ransomware works what if a piece of ransomware has infected a department's shared drive, and it's rapidly spreading. What actions would you take to contain and mitigate this attack?

- Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money, or ransom, is paid. Here's a general overview of how ransomware works:

    1. Ransomware typically enters a system through malicious email attachments, infected websites, or vulnerabilities in software. Once executed, it encrypts files on the system, rendering them inaccessible.
    2. The ransomware encrypts files using a strong encryption algorithm, making it extremely difficult or nearly impossible to decrypt the files without the corresponding decryption key.
    3. After encrypting files, the ransomware displays a ransom note, informing the victim of the encryption and demanding payment (often in cryptocurrency) in exchange for the decryption key.
    4. Some advanced ransomware variants are capable of self-replicating and spreading across a network. This can lead to rapid infections in shared drives and connected devices.

Actions to take:

- Isolate Affected Systems:
- Notify relevant stakeholders, including IT and management, about the ransomware incident.
- Determine the specific ransomware variant to understand its behavior and potential weaknesses
- Verify the availability and integrity of recent backups for the shared drive.
- Implement network segmentation to isolate the infected shared drive and prevent lateral movement.

- Isolate affected endpoints connected to the shared drive by disconnecting them from the network.
- Identify and terminate ransomware processes on infected systems using antivirus tools.
- Conduct thorough antivirus scans on systems connected to the shared drive.
- Ensure all systems are updated with the latest security patches to address vulnerabilities.
- Review and limit user access to the shared drive to prevent unauthorized access.
- Document the incident, actions taken, and impact for future analysis and reporting.

Q.46) Tell us about some cyber-attacks happened.

- The SolarWinds cyber-attack, discovered in December 2020, stands out as a significant and highly sophisticated supply chain attack.
- The attackers compromised the SolarWinds Orion software, a widely utilized IT management tool employed by numerous organizations and government agencies.
- The adversaries ingeniously inserted a malicious code, known as Sunburst or Solorigate, into legitimate software updates distributed by SolarWinds.
- As organizations unsuspectingly downloaded and installed these compromised updates, the attackers gained unauthorized access to a multitude of networks, allowing them to conduct extensive espionage and exfiltrate sensitive information.
- The extent of the breach was substantial, impacting a wide range of sectors, including government agencies, technology firms, and major corporations.

Re: https://cm-alliance.com/cybersecurity-blog/what-really-happened-in-the-solarwinds-cyber-attack

Q. 47) explain WannaCry ransomware attack in 2017

The WannaCry ransomware attack in 2017 was a global cyber incident that affected hundreds of thousands of computers in over 150 countries. Here's an overview of the key aspects of the WannaCry attack:

WannaCry exploited a Windows operating system vulnerability called EternalBlue, which was part of a collection of hacking tools allegedly developed by the NSA and leaked by a group known as the Shadow Brokers.

WannaCry exploited a Windows operating system vulnerability called EternalBlue, which was part of a collection of hacking tools allegedly developed by the NSA and leaked by a group known as the Shadow Brokers.

WannaCry exploited a Windows operating system vulnerability called EternalBlue, which was part of a collection of hacking tools allegedly developed by the NSA and leaked by a group known as the Shadow Brokers.

A cybersecurity researcher, Marcus Hutchins, accidentally discovered a "kill switch" in the ransomware's code. Registering a specific domain acted as a kill switch, temporarily stopping the spread.

Vulnerability Management: The incident underscored the importance of promptly applying security patches and updates to mitigate the risk of exploitation.

Global Collaboration: The widespread impact highlighted the need for international cooperation in addressing and preventing cyber threats.

Security Awareness: Organizations and individuals increased their awareness of the importance of cybersecurity practices, such as regular backups and maintaining up-to-date security measures.

Patching Practices: There was a renewed emphasis on the urgency of patching vulnerabilities to prevent similar large-scale attacks.

Q.48) How do you stay on top of cybersecurity news and developments?

- Security News Websites: Visit sites like KrebsOnSecurity.
- Blogs: Follow expert blogs (Schneier on Security, Krebs on Security).
- Threat Intel Platforms: Subscribe to platforms for emerging threat insights.
- Podcasts: Listen to cybersecurity podcasts for expert discussions.
- Social Media: Follow professionals on Twitter, LinkedIn.
- RSS Feeds: Use feeds to aggregate content from various sources.
- Forums: Engage with cybersecurity communities online.
- Training: Enroll in cybersecurity courses for ongoing learningQ.48)

Q.49) Which types of alerts have you encountered while working in a SOC?

- Malware Alerts: Indications of malicious software or code on the network or endpoints.
- Intrusion Detection System (IDS) Alerts: Alerts triggered by suspicious or anomalous network activities.
- Data Leakage Alerts: Indicators of unauthorized data exfiltration or leakage.
- Phishing Alerts: Identification of phishing emails or malicious URLs.
- Denial of Service (DoS) Alerts: Indicators of attempts to overwhelm a system or network to disrupt services.
- Authentication Anomalies: Alerts related to unusual login patterns or potential unauthorized access.
- Endpoint Security Alerts: Alerts from antivirus or endpoint protection systems.
- SIEM Alerts: Alerts generated by SIEM platforms based on correlated security events.
- Firewall Alerts: Notifications related to suspicious traffic or unauthorized access attempts.
- Anomaly Detection Alerts: Indicators of abnormal behavior that may suggest a security threat.
- Vulnerability Alerts: Notifications about identified vulnerabilities in systems or applications.
- Insider Threat Alerts: Indicators of potential malicious activities by internal users.

Q.50) What is Phishing and Types

Phishing is a form of cyber attack where attackers use deceptive tactics to trick individuals into providing sensitive information such as usernames, passwords, credit card numbers, or other personal details.

Email Phishing: This is like the classic phishing. Imagine receiving a deceitful email, looking all official, but it's just a trick to get you to spill the beans.

Spear Phishing: This one's like a personalized attack. The scammer knows more about you, making the phishing attempt look very convincing.

Vishing: Now, picture phishing but over the phone. It's like someone calling and sweet-talking you into sharing personal info.

Smishing: This is the texting version of phishing. You get a message that seems harmless but is actually a sneaky attempt to get your info.

Pharming: Think of it as a redirect scam. You type in a legit website, but the trickery sends you to a fake one, trying to steal your details.

Clone Phishing: This is like a copycat move. Scammers replicate a legitimate message, making it look real, but it's just a trap.