Introduction to SOC Operations & Fundamentals

Section A: Fundamentals of Cybersecurity

1. **Define the term "Security Operations Center (SOC)" and explain its primary purpose in an organization.**

A security operations center (SOC) improves an organization's threat detection, response and prevention capabilities by unifying and coordinating all cybersecurity technologies and operations. The primary purpose of SOC is to protect the company's data, ensuring the safety by regularly monitoring (24x7). If any threat is occurred then the incident team should report to the authority through the security alarms and should ensure the measures to prevent the attack. They are responsible for the organization's safety

2. **List and explain any three common cyber threats monitored in a SOC.**

There are different types of attack that a company faces during the run, SOC is the team who regularly monitors and reports the attack and ensures the safety of the, organization.
The main , comon attack includes:

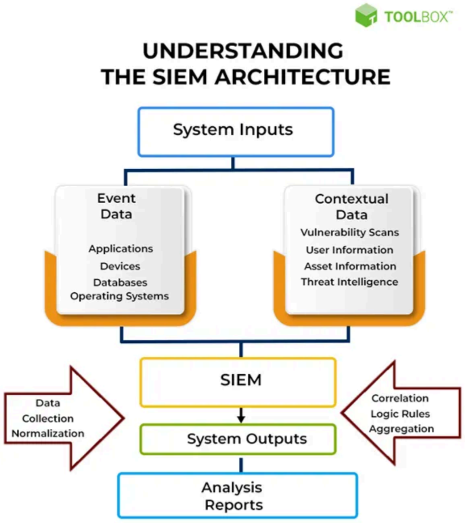
- **Phishing Attack**: These are the very common attack that are faced by a company, the attacker uses fake sites and link that are forwarded to the employee to get a vulnerability, but is any unauthorized access is being reported, the company will make sudden plan to overcome that situation, otherwise the data will be stolen.

- **Data Exfiltration**: These are the condition were the data of the organization is being transferred to another system without any access from the present organization, can be referred as the unauthorized transfer of data out of the company.

- **Credential Stealing**: These are the scenarios where the weak passwords are cracked by the attackers and try to enter into the organization. They target the system which is less secured and make a vulnerability in that particular system. SOC should find these kind of expoiltaion and make sure that no data is being stealed.

3. **Describe the role of SIEM (Security Information and Event Management) in a SOC.**

SEIM - Security information and Event Management, is a technology solution that collects, aggregates, and analyzes security-related data from various sources across an organization's IT infrastructure. The role of SEIM is in the definition that, they collect the data including the log details from server, end user systems, networking equipment, applications, and security devices, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).



Reference: spiceworks.com

4. **Explain the difference between proactive monitoring and reactive monitoring in a SOC environment.**

Proactive Monitoring

- Proactive monitoring simply means constantly attempting to identify potential issues before they create major challenges for your business.
- Proactive monitoring anticipates issues, you can address these issues before an application crashes or performance degradation sets in.

Reactive Monitoring

- Reactive monitoring in a SOC involves waiting for security incidents to occur and then responding to them after they have been detected.
- This approach relies on traditional alerting systems, such as intrusion detection systems (IDS), security information and event management (SIEM) systems, and incident response teams.

5. **Outline the basic steps involved in incident detection and response in a SOC.**

- **Dectection & Monitoring:**
  - There are tools like SEIM that monitors the network and applications, Intrusion Dectection Sytems and the Intrusion PRevention Systems and also the endpoint protection solution. If any suspicious activity is beem identified they are reported.
- **Triage:**
  - Once threat is being dectected, we analyze the scope and the impact of the attack, there are so many steps included like filtering out the false infomrations, categorizing the incidents and prioritizing the threat according to the imapct that they will cost.
- **Investigation:**
  - This is the phase where we continuously evaluate the threat which includes the identifciation of how the threat evloves, what was the root cause, attack vendors and the compromised assets.
- **Containment:**
  - To minimize damage, the SOC team takes immediate steps to contain the incident. This could involve isolating affected systems, blocking malicious IP addresses or domains, disabling compromised accounts, or implementing temporary network segmentation. Containment ensures that the threat cannot spread further.
- **Eradication:**
  - Once the threat is contained, the focus shifts to removing it completely from the environment. This may include deleting malware, patching vulnerabilities, closing exploited ports, or reconfiguring security controls.
- **Recovery:**
  - After eradication, affected systems and services are restored to normal operations. This step involves verifying that all systems are clean, data integrity is maintained, and functionality is fully restored.
- **Lessons Learned:**
  - After an incident, a debriefing or lessons learned meeting is crucial to review what happened, what worked well, and areas for improvement. The response team and stakeholders should communicate to refine processes, complete any pending documentation, and analyze how the incident was managed and resolved.
- **Documentation & Reporting:**
  - The final step involves documenting the entire incident lifecycle, from detection to resolution. This report includes the nature of the incident, the steps taken to address it, and recommendations to prevent recurrence. Reports are shared with stakeholders to improve awareness and refine security policies.

Section B: Tools and Techniques

6. Research and list any two popular SOC tools and describe their purpose in monitoring and incident handling.

SEIM

- Security information and Event Management, is a technology solution that collects, aggregates, and analyzes security-related data from various sources across an organization’s IT infrastructure. The role of SEIM is in the definition that, they collect the data including the log details from server, end user systems, networking equipment, applications, and security devices, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Network Analysis Tools

- These tools allow analysts to monitor traffic and identity anomalous activities. This helps in identifying potential threats and responding to them in a timely manner.

Example - FireEye

- **FireEye**
    - FireEye, now part of Trellix, is a key tool for SOC teams to detect, investigate, and respond to advanced cyber threats like ransomware, APTs, and zero-day attacks.
    - Some of the benefits are -
        - Provides actionable insights into attacker behavior.
        - Combines behavior analytics and machine learning for better threat visibility.
        - Tools to quickly contain and mitigate incidents.
        - Works seamlessly with existing SOC workflows to enhance efficiency

Endpoint Dectection and Response (EDR)

- These tools are also essential for SOC as they are used to monitor endpoints, such as desktops, laptop, and server for any signs of malicious activity. This allows analysts to detect and respond to the threat at the end level.

Example - Cylance, CarbonBlack

- **Cylance**
    - Cylance, now part of BlackBerry, is a leading cybersecurity solution focused on **AI-driven threat prevention**. It’s widely used by SOC teams to prevent, detect, and respond to threats with minimal impact on resources.
- Some of the benefits are:
    - Cylance tools integrate easily into SOC workflows and existing security infrastructures.
    - CylanceOPTICS enhances visibility into endpoint activity without requiring heavy system resources.
    - Automated threat response saves time for SOC analysts, enabling faster remediation.

7. Explain how a firewall log can be used in detecting unauthorized access attempts

- ### What is a Firewall?

A firewall is a security system designed to prevent unauthorized access into or out of a computer network. Firewalls are often used to make sure internet users without access are not able to interface with private networks, or intranets, connected to the internet.

- ### Purpose of a Firewall

Firewalls protect your computer or network from unwanted traffic coming in or going out. Firewalls can also inspect and authenticate all data packets in network traffic before they are allowed to move to a more secure environment.

- ### Detecting the unauthorize access

- These are usually the most important logs used for unauthorized access detection in order to capture the details of traffic flowing through the firewall. SOC teams can monitor and analyze such information concerning **IP addresses, port numbers, protocols, and timestamps that define traffic patterns**.
For example, repeated access attempts from an IP address during unusual hours can be an indication of a brute-force attack or something similar.

- Logs also report blocked traffic that is breaking the rules or policies set up by the firewall. A repeated pattern of blocked attempts from unknown or suspicious IP addresses can identify probing activities where the attacker tries to test for weaknesses in the system.

- Firewall logs is in identifying unauthorized protocols. Protocols that are not common or are unauthorized to appear in the logs may indicate attempts to bypass standard security measures.

- Firewall logs can also be cross-referenced with threat intelligence to detect known malicious actors. Indicators of compromise (IoCs) such as repeated failed login attempts, traffic to blacklisted domains, or unexpected outbound traffic spikes—possibly signaling data exfiltration—can all be derived from firewall logs. For example, if logs show hundreds of login attempts on a server from a single external IP, it may indicate a brute-force attack.

- SOC teams should review the firewall logs regularly for anomalies, use automated tools to correlate log data with threat intelligence, and set up alerts for suspicious patterns. The real-time investigation of flagged activities and blocking of malicious traffic by SOC teams can prevent unauthorized access and mitigate potential breaches.

8. Write a brief note on the significance of packet analysis in a SOC.

Packet analysis plays a vital role in the work of a Security Operations Center (SOC). It involves closely examining the data packets flowing through a network to uncover potential threats, unusual behavior, or breaches of security policies. An SOC analyzes the packet and they help the SOC in the following ways:

- **Spotting Malicious Activity:**
    - By checking the headers and payloads of the packet that are receiving, SOC could identify if ther is any vulnerability is there or not.
- **Incident Response:**
    - During any particular crisis the packet will help in identifying critical datas including that about how the attack happened, who was affected by the attack and so on.
- **Improve Network Quality:**
    - This very helpfull that is when we thoroughly watch the packet, we could identify whether there is any corruption or not, if there is any corruption the network is not efficiently working, otherwise it is efficiently working.

9. How do indicators of compromise (IoCs) help a SOC analyst in identifying potential threats?

Indicators of Compromise (IoCs) play a crucial role in helping Security Operations Center (SOC) analysts identify potential threats by providing digital forensic evidence of malicious activities. They can be helped in these ways:

- **Identifying Threats early:**
    - IoC will notice if there is any unusual network traffic or if there is any suspicious files or links, or there is any unusual Internet Protocol Address there, if there one among them there is a chance for the attack, they will dectect early and prevent the attack to the organization.

- **Act Quickly & Security Improvment:**
    - IoC will give information to the SOC like the attack which other organization have faced and they take enough mesaure the prevent those attack, these attack includes the unsual IP, Filename and the netwrok trafficwith the help of IoC we could find our faults and improve our weaker side by focusing on that area.’

- **Providing the Context of the attack:**
    - The IoC have the top to down data of how an attack have been faced ot the origin of the attack that are faced by the organization including the tools used and also the malware that are included in the attack.

10. Explain the importance of maintaining a threat intelligence database in SOC operations

Threat Intelligence Database:

A threat intelligence database is a centralized collection of information about known and emerging cybersecurity threats. It stores details like malicious IP addresses, domains, file hashes, attack techniques, and behavioral patterns of malware or attackers. This database helps security teams, especially in a SOC, to identify and respond to threats more efficiently.

Importance of Threat Intelligence:

- **Improves Threat Dectection:**
    - They contain the full history of how attack have happened and what is the pattern of the attack, we can check and compare with those files with the threat information that are faced by the organization so they can prevent those attack.

- **Proactive Security:**
    - They conatin the data of different kind of attack, by strictly monitoring the data SOC could be able to strengthen the security and prevent some attack.The attack can be dectected by Ioc.

- **Incident Response:**
    - During an attack, the database offers valuable insights to understand the nature of the threat, its behavior, and potential impact, ensuring a faster and more accurate response.

- **Collaboration:**
    - The database serves as a shared knowledge base, improving coordination within the SOC team and across organizations.

Section C: Practical Scenarios

11. Assume you are a SOC analyst. How would you respond to a DDoS attack detected in your organization?

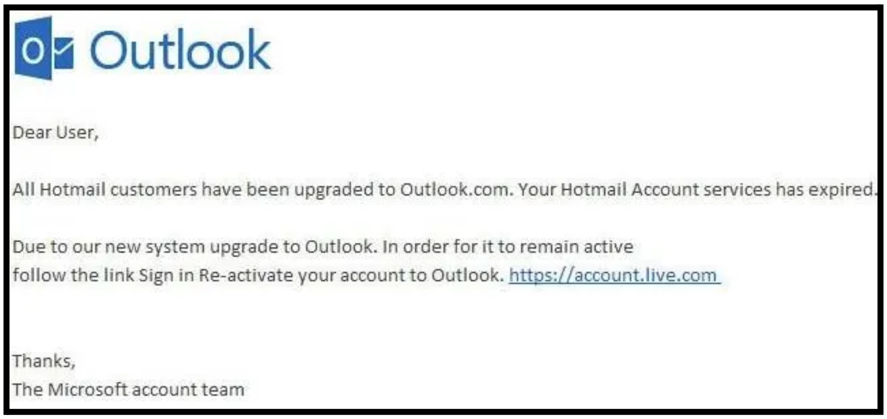
As a SOC analyst, responding to a Distributed Denial-of-Service (DDoS) attack requires a swift and structured approach. Here's how I would respond:

- **Dectect and Monitor:**
  - I use tools like SEIM to monitor the network packages, will look whether there is an unusual spikes in traffic such as a huge request in IP targeting a specific node.
  - If any threat is been live, i will verify the type of that, if the traffic consist of repetitive non legitimate req like UDP, SYN floods, its likely to be the DDoS attack
- **Implement Proper Actions:**
  - Apply rate-limiting rules on the firewall or web server To limit the number of requests a client can make within a set time Frame. This helps mitigate traffic surges from malicious sources.
  - Blocking the IP using a firewall or IDS/IPS.
- **Engage with DDoS Mitigation Services:**
  - If the attack continues to overwhelm internal defenses, I would escalate the issue to external DDoS protection services (for Example, AWS Shield), which specialize in mitigating large-scale attacks by rerouting traffic through their infrastructure
- **Communication:**
  - Notify relevant internal stakeholders (For example, network administrators, IT teams, and management) about the attack, its impact, and the ongoing mitigation efforts.
  - If the attack is affecting customers or end-users, I would coordinate with the communications team to inform them of any service interruptions and expected resolution times.
- **Post Threat Analysis:**
  - Identify the root cause of the attack , understanding how the attack happened, which vulnerabilities were targeted, and how it was mitigated
  - I would recommend improving the organization's defenses against future attacks, such as improvencing firewall rules.
- **Report & Documentation:**
  - Properly document all actions taken during the incident and generate a report for internal records or compliance requirements. The report should include the attack's duration, impact, and steps taken to mitigate it

12. Write a short procedure to handle a phishing email reported by an employee.

- **Initial Response:**
    - After receiving a phishing email report from an employee, promptly acknowledge their concern and thank them for reporting the incident.
    - Inform the employee that their report will be investigated and appropriate action will be taken.
- **Investigation:**
    - Next we have to forward the current situation to the security team of the organization
    - We have to conduct thorough examination of the email , how the vulnerabilities have been occurred.
- **Report & Tracking:**
    - Document the phishing email including the employee details and short description of the email content and the suspicious note and also the results.
- **Follow-up:**
    - Notify the employee that the investigation is complete and provide a summary of the findings.
    - Offer additional training or guidance on phishing recognition and prevention.
- **Strengthen the Security:**
    - After a vulnerability has been identified, we must prevent them on the future attacks my adding additional security measures.
    - These include giving the employees proper training and guidance also.

Sample e-mail phishing:



Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

Thanks,
The Microsoft account team

13. Analyze the following hypothetical log snippet and identify any suspicious activity:

192.168.1.1

a. Failed Login Attempt - 10 times - 192.168.1.1

A high number of failed login attempts in a short period (commonly known as a brute force attack) is a red flag. Attackers often use brute force to guess passwords and gain unauthorized access to systems.

b. IP Blocked - 192.168.2.5

The blocking of the IP suggests that the system has responded to the failed login attempts, which could indicate that the attack is being actively mitigated. However, it’s essential to check if the blocking is based on automated security tools or manual intervention.

c. Download Attempt

Downloads from internal systems or outside sources that aren't authorized could indicate malicious activity, such as an attempt to steal sensitive data or deploy malware. It’s crucial to verify whether the downloaded file is benign or malicious.

d. Suspicious File

This is a critical sign of potential malware or unauthorized data exfiltration. The file could be an indicator of a malware download, ransomware, or data exfiltration tool.