1. What is the role of a SOC Analyst?

Answer:
A SOC Analyst is responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents. They use SIEM tools, analyze security alerts, investigate threats, and coordinate incident response efforts to protect an organization's IT infrastructure.

---

2. What are the different SOC tiers, and how do they function?

Answer:

- **Tier 1 (L1) - Security Monitoring:** Monitors alerts, performs initial triage, and escalates incidents.
- **Tier 2 (L2) - Incident Response:** Investigates escalated alerts, performs deep analysis, and mitigates threats.
- **Tier 3 (L3) - Threat Hunting & Forensics:** Proactively searches for advanced threats, analyzes malware, and provides strategic improvements.
- **SOC Manager:** Oversees operations, coordinates between teams, and ensures security policies are enforced.

---

3. What are SIEM tools, and why are they important?

Answer:
SIEM (Security Information and Event Management) tools collect, analyze, and correlate logs from various sources to detect security threats. Examples include **Splunk, IBM QRadar, Azure Sentinel, and ArcSight**. They help in identifying anomalies, automating alerts, and supporting compliance.

---

4. What is the difference between IDS and IPS?

Answer:

- **Intrusion Detection System (IDS):** Monitors network traffic for malicious activity and generates alerts.
- **Intrusion Prevention System (IPS):** Acts as an active security measure by blocking detected threats in real time.

---

5. How do you respond to a phishing attack?

Answer:

- Analyze the email headers and links using tools like **VirusTotal, URLScan, and IPVoid**.
- Check sender reputation and email anomalies.
- Quarantine the email and report it to security teams.
- Investigate if any user clicked the link or downloaded malicious files.
- Educate users on phishing awareness and update email security policies.

---

6. What are the steps in the Incident Response (IR) process?

Answer:

1. **Identification:** Detect and validate security incidents.
2. **Containment:** Isolate affected systems to prevent further damage.
3. **Eradication:** Remove threats and malicious files.
4. **Recovery:** Restore affected systems and resume operations.
5. **Lessons Learned:** Conduct post-incident analysis to improve defenses.

---

7. How do you differentiate between a False Positive and a False Negative?

Answer:

- **False Positive:** A benign event incorrectly flagged as a threat (e.g., a legitimate login marked as brute force).
- **False Negative:** A real threat that goes undetected (e.g., malware bypassing detection systems).
- SOC analysts fine-tune security rules and thresholds to minimize false positives/negatives.

---

8. What is Threat Intelligence, and how is it used in a SOC?

Answer:
Threat Intelligence provides insights on emerging threats, indicators of compromise (IoCs), and attack patterns. Tools like **VirusTotal, Shodan.io, Cyberchat, and THOR Scanner** help analysts identify and mitigate threats proactively.

---

9. What is the MITRE ATT&CK Framework?

Answer:
MITRE ATT&CK is a **knowledge base of adversary tactics, techniques, and procedures (TTPs)** used for threat hunting, red teaming, and security assessments. It categorizes cyber threats into **Initial Access, Execution, Persistence, Privilege Escalation, etc.**

---

10. How do you handle a ransomware attack?

Answer:

- Isolate infected machines from the network.
- Identify the ransomware strain using tools like **ID Ransomware**.
- Restore systems using backups if available.
- Block indicators of compromise (IoCs) in firewalls and EDR solutions.
- Conduct a forensic analysis and apply security patches.

---

11. What are some common Log Sources in a SOC?

Answer:

- **Network Logs:** Firewalls, IDS/IPS, VPN logs
- **Endpoint Logs:** EDR solutions (e.g., Microsoft Defender, CrowdStrike)
- **Application Logs:** Web servers, databases
- **Cloud Logs:** AWS CloudTrail, Azure Security Center
- **Authentication Logs:** Active Directory, Okta, Radius

---

12. What is a Brute Force Attack? How can you prevent it?

Answer:
A brute force attack is when an attacker repeatedly tries different username-password combinations to gain access.
Mitigation:

- Implement **Account Lockout Policies**
- Enforce **Multi-Factor Authentication (MFA)**
- Use **CAPTCHA** and rate limiting
- Monitor for multiple failed login attempts

---

13. What are Indicators of Compromise (IoCs)?

Answer:
IoCs are evidence of a security breach, such as:

- **IP addresses of known attackers**
- **Malicious file hashes (MD5, SHA256)**
- **Suspicious domain names and URLs**
- **Unusual login activities**

---

14. What is the difference between Symmetric and Asymmetric Encryption?

Answer:

- **Symmetric Encryption:** Uses a **single key** for encryption and decryption (e.g., AES, DES).
- **Asymmetric Encryption:** Uses a **key pair (public & private)** (e.g., RSA, ECC). Used in SSL/TLS communication.

---

15. What is Zero Trust Security?

Answer:
Zero Trust is a security model that follows **"Never Trust, Always Verify"**, ensuring that every request is authenticated and authorized before granting access. It involves:

- **Multi-Factor Authentication (MFA)**
- **Least Privilege Access Control**
- **Micro-segmentation**

---

16. What is a DDoS attack, and how can it be mitigated?

Answer:
A **Distributed Denial-of-Service (DDoS) attack** overwhelms a server or network with excessive traffic.
Mitigation:

- Use **Rate Limiting** and **WAF (Web Application Firewall)**
- Deploy **CDN (Content Delivery Network)** to absorb traffic
- Implement **Geo-blocking** for suspicious locations

---

17. What is the difference between Vulnerability Scanning and Penetration Testing?

Answer:

- **Vulnerability Scanning:** Identifies security weaknesses in a system using tools like **Nessus, Qualys, and Rapid7**.
- **Penetration Testing:** Actively exploits vulnerabilities to assess the system's security.

---

18. What is a Security Playbook?

Answer:
A Security Playbook is a **standardized response guide** for handling security incidents. It includes:

- Steps for detecting and analyzing threats
- Containment and mitigation procedures
- Communication and escalation protocols

---

19. What is an SQL Injection attack, and how can it be prevented?

Answer:
SQL Injection occurs when an attacker injects malicious SQL queries into an application.
Prevention:

- Use **Parameterized Queries** and **Prepared Statements**
- Implement **Input Validation**
- Limit database privileges

20. What tools have you used for security analysis and investigation?

Answer:

- **SIEM Tools:** Splunk, QRadar, Azure Sentinel
- **Endpoint Security:** Microsoft Defender 365, CrowdStrike, SentinelOne
- **Threat Intelligence:** VirusTotal, Shodan.io, Cyberchat
- **Firewall & Network Security:** Palo Alto, FortiGate, F5 WAF