CYBERSECURITY INTERVIEW REVISION (SCENARIO-BASED & SIMULATIONS)

BY IZZMIER IZZUDDIN

SET 1

1. INCIDENT RESPONSE SCENARIOS

SCENARIO 1: RANSOMWARE ATTACK

Situation:

Your SIEM alerts you to unusual file modifications on a critical file server. A user reports that files have been renamed with a .locked extension and a ransom note appears on the desktop.

Questions

1. What are the first three steps you take in response?
2. How would you determine the attack vector (e.g., phishing email, RDP compromise)?
3. What logs would you check to track the attacker's movement?
4. If you find an infected endpoint, what containment measures do you apply?
5. How do you handle communication with stakeholders and law enforcement?

SCENARIO 2: DATA EXFILTRATION DETECTED

Situation:

An alert is triggered for a high volume of outbound traffic from a finance department workstation to an unknown IP address.

Questions

1. What tools and logs would you use to investigate this anomaly?
2. How can you determine whether this is legitimate or malicious activity?
3. If confirmed as malicious, how would you stop the data exfiltration?
4. What recommendations would you make to prevent this from happening again?

SCENARIO 3: PHISHING CAMPAIGN TARGETING EMPLOYEES

Situation:

Your company’s helpdesk receives multiple complaints from employees who clicked on a suspicious email link. Some employees reported entering their credentials.

Questions

1. How do you identify the scope of this phishing attack?
2. What logs would you analyse to check for credential theft?
3. What immediate actions would you take to mitigate the risk?
4. What long-term strategies can prevent future phishing attacks?

2. SIEM INVESTIGATION SIMULATIONS

SIMULATION 1: UNUSUAL LOGIN ATTEMPTS

Data Given:

- SIEM logs show repeated login failures from a foreign country on an executive's account.
- The executive is currently on leave and not traveling.
- The login attempts use a correct username but incorrect passwords.

Questions

1. How do you determine if this is a brute-force attack or a credential stuffing attempt?
2. What actions should you take if the account gets compromised?
3. What security measures can prevent such login attempts?

SIMULATION 2: SUSPICIOUS POWERSHELL EXECUTION

Data Given:

- A host executes an encoded PowerShell command.
- The command contacts an external domain and downloads a file.
- The file is flagged as a Trojan by VirusTotal.

Questions

1. How do you decode the PowerShell command?
2. What logs should you analyse to trace the attacker's steps?
3. How do you determine the impact of the malware?
4. What mitigation steps should be taken?

3. THREAT HUNTING CHALLENGES

CHALLENGE 1: FINDING SIGNS OF LATERAL MOVEMENT

Hint: Use Windows Event Logs, Sysmon, and network logs to track lateral movement in an environment.

Questions

1. What indicators in event logs (Event ID 4624, 4672, etc.) suggest lateral movement?
2. How do you detect Pass-the-Hash or Pass-the-Ticket attacks?
3. What tools would you use to correlate logs across multiple systems?

CHALLENGE 2: DETECTING A HIDDEN BACKDOOR

A newly hired IT admin has installed a remote access tool that allows unrestricted access to company servers.

Questions

1. How do you detect unauthorised remote access tools?
2. What security controls can prevent unauthorised installations?
3. How do you ensure an insider threat does not exploit such access?

4. MALWARE ANALYSIS SCENARIOS

SCENARIO 1: WORD DOCUMENT WITH MACRO MALWARE

A user reports that opening a Word document resulted in system slowness. Network logs show connections to a suspicious IP.

Questions

1. How do you analyse the macro in the document?
2. How do you determine if the document dropped additional malware?
3. What steps should be taken to block further exploitation?

SCENARIO 2: SUSPICIOUS EXE DOWNLOAD

A user downloads a program from an unknown website. Your antivirus alerts you to a "Suspicious File Behavior" detection.

Questions

1. What are the steps for static and dynamic analysis of this file?
2. How do you determine if the file is a Remote Access Trojan (RAT)?
3. If the malware creates persistence, how do you remove it?

5. LOG ANALYSIS CHALLENGES

CHALLENGE 1: ANALYSING WEB SERVER LOGS

You receive a report that an external IP has been trying to access the admin panel of a web application.

Questions

1. What log files do you review for authentication attempts?
2. How do you detect SQL injection or XSS attempts?
3. What firewall rules can prevent further attacks?

CHALLENGE 2: SUSPICIOUS OUTBOUND DNS REQUESTS

Your firewall logs show a workstation making thousands of DNS queries to random domains.

Questions

1. How do you identify if this is a Command & Control (C2) beaconing?
2. What response actions should be taken?
3. How can you prevent DNS tunneling attacks?

6. SOC WORKFLOW & PLAYBOOK QUESTIONS

General SOC Questions:

1. What are the key phases in an incident response process?
2. How do you categorise alert severity in an MSSP?
3. How do you communicate an ongoing incident to stakeholders?
4. What KPIs should a SOC team track to measure efficiency?

Playbook Development Questions:

1. How do you standardise response actions for different threat types?
2. What elements should a phishing playbook include?
3. How do you ensure continuous improvement in incident handling?

7. CYBERSECURITY FRAMEWORKS & COMPLIANCE

SCENARIO: YOUR COMPANY IS AUDITED FOR COMPLIANCE

An external auditor requests evidence that your company follows security best practices.

Questions

1. How do you align your security operations with NIST, ISO 27001, or CIS benchmarks?
2. What logs and reports do you provide to prove compliance?
3. How do you handle security policy violations discovered during the audit?

8. MISCELLANEOUS TECHNICAL QUESTIONS

1. Explain the difference between symmetric and asymmetric encryption.
2. What are the different types of firewalls, and how do they work?
3. How does TLS ensure secure communication?
4. What is a zero-day vulnerability, and how do companies mitigate it?

SET 2

1. ADVANCED INCIDENT RESPONSE SCENARIOS

SCENARIO 4: INSIDER THREAT – DATA THEFT BY AN EMPLOYEE

Situation:

A departing employee downloads a large amount of confidential files from the internal file server onto a USB drive before resigning.

Questions

1. What logs would you analyse to confirm this data theft?
2. How do you determine if the data was exfiltrated to an external cloud service?
3. What security controls could have prevented this incident?
4. If the data was leaked, what are the legal and compliance implications?

SCENARIO 5: SUPPLY CHAIN ATTACK – COMPROMISED SOFTWARE UPDATE

Situation:

Your organisation installs a security patch from a trusted vendor. A few days later, multiple endpoints report unusual PowerShell activity contacting an external domain.

Questions

1. How do you verify if this patch is legitimate or compromised?
2. What logs would help track the execution of the malicious code?
3. What is your containment and eradication strategy?
4. What policies should be implemented to prevent supply chain attacks?

SCENARIO 6: BUSINESS EMAIL COMPROMISE (BEC) ATTACK

Situation:

A finance employee receives an email from the "CEO" requesting an urgent wire transfer of RM500,000 to a new vendor. The email is well-crafted with no obvious red flags.

Questions

1. How do you verify if this email is legitimate?
2. What logs can help determine if the CEO’s email was spoofed or compromised?
3. If the transfer was made, how would you attempt to recover the funds?

4. What long-term email security measures should be implemented?

2. COMPLEX SIEM INVESTIGATION SIMULATIONS

SIMULATION 3: BEACONING MALWARE – PERSISTENT C2 TRAFFIC

Data Given:

- SIEM detects periodic outbound connections every 30 minutes to an unknown domain.
- The traffic originates from a workstation assigned to the HR department.
- The domain resolves to an IP address in Russia.

Questions

1. How do you confirm whether this is a Command & Control (C2) server?
2. What tools can help decode the beaconing traffic?
3. How do you isolate and remediate the affected workstation?
4. What YARA rules can be created to detect similar threats in the future?

SIMULATION 4: EXPLOITATION OF A WEB SERVER

Data Given:

- SIEM flags a series of HTTP requests with SQL injection payloads targeting the company's customer portal.
- The attacker successfully executes a payload that extracts database records.

Questions

1. How do you analyse the attack to determine the exploited vulnerability?
2. What logs would help identify the full impact of the breach?
3. How do you mitigate the SQL injection vulnerability?
4. What Web Application Firewall (WAF) rules should be implemented?

3. ADVANCED THREAT HUNTING CHALLENGES

CHALLENGE 3: FILELESS MALWARE DETECTION

Attackers have deployed a fileless malware attack using PowerShell to execute malicious scripts directly in memory.

Questions

1. How do you detect fileless malware when no traditional malware files exist?
2. What Windows Event IDs are useful for detecting PowerShell exploitation?
3. How do you create Sigma rules to hunt for similar activities?

CHALLENGE 4: IDENTIFYING CREDENTIAL DUMPING ATTEMPTS

A security alert indicates that LSASS.exe was accessed by an unknown process on a domain controller.

Questions

1. What are the common techniques used for credential dumping?
2. How do you determine if Mimikatz or similar tools were used?
3. What mitigation strategies can prevent credential dumping?

4. MALWARE ANALYSIS & REVERSE ENGINEERING SCENARIOS

SCENARIO 3: ANDROID MALWARE INVESTIGATION

Situation:

A user downloads a "free VPN app" that starts collecting excessive device permissions and sending SMS messages without consent.

Questions

1. How do you analyse the APK file to determine if it's malware?
2. What tools (e.g., MobSF, JADX, APKTool) can be used for static and dynamic analysis?
3. What signs indicate spyware or banking trojans?
4. How do you mitigate and report such Android malware?

SCENARIO 4: WINDOWS PE MALWARE ANALYSIS

Situation:

A suspicious executable is flagged by EDR but has no known signatures on VirusTotal.

Questions

1. What are the steps for static analysis of this PE file?
2. How do you safely execute and monitor its behavior in a sandbox?
3. How do you extract Indicators of Compromise (IOCs) from the malware?
4. What YARA rules can you create to detect similar samples?

5. CLOUD SECURITY SCENARIOS

SCENARIO 1: MISCONFIGURED AWS S3 BUCKET LEAK

Situation:

Your company's AWS S3 storage is publicly accessible, and sensitive customer data has been exposed.

Questions

1. How do you verify which data has been leaked?
2. What AWS logs would you check to determine who accessed the data?
3. How do you properly secure an S3 bucket against such misconfigurations?
4. What IAM policies should be implemented to enforce least privilege access?

SCENARIO 2: UNAUTHORISED ACCESS TO AZURE AD

Situation:

An attacker logs in to an executive's Microsoft 365 account from an unusual location without triggering MFA.

Questions

1. How do you investigate how the attacker bypassed MFA?
2. What Azure AD logs can help track lateral movement?
3. What security controls can be implemented to detect and prevent similar attacks?

6. RED TEAM VS. BLUE TEAM CHALLENGE

SCENARIO: DETECTING & MITIGATING AN ACTIVE RED TEAM ATTACK

Situation:

Your internal red team conducts a stealthy attack simulation. They use tools like Cobalt Strike to establish persistence in your network.

Questions

1. What are the most effective detection methods for Cobalt Strike beacons?
2. How do you identify and remove persistence mechanisms?
3. What proactive threat-hunting techniques can detect advanced adversaries?
4. How do you refine your detection engineering strategies?

7. SOC WORKFLOW & CRISIS MANAGEMENT

SCENARIO: RANSOMWARE ATTACK HITS PRODUCTION SERVERS

Your organisation is hit with ransomware, and critical business operations are down.

Questions

1. How do you determine the ransomware variant and attack vector?
2. Should you negotiate with the attackers or restore from backups?
3. How do you ensure a clean recovery without reinfection?
4. What security policies should be changed post-incident?

8. FINAL BOSS-LEVEL QUESTIONS

1. **APT Hunting**: How do you track an Advanced Persistent Threat (APT) in a large enterprise?
2. **SIEM Fine-Tuning**: How do you reduce false positives without missing real threats?
3. **Cyber Threat Intelligence (CTI)**: How do you integrate threat intelligence feeds into SOC workflows?
4. **AI in Cybersecurity**: How can AI/ML improve SOC detection and response?

SET 3

1. ADVANCED INCIDENT RESPONSE SCENARIOS

SCENARIO 7: ZERO-DAY EXPLOIT IN YOUR ORGANISATION

Situation:

A threat intelligence feed reports that a newly discovered zero-day vulnerability is being actively exploited in the wild. Your company uses the affected software in production.

Questions

1. How do you confirm if your environment has been compromised?
2. What logs or indicators would you search for?
3. If no patch is available, what mitigation steps should you take?
4. How do you prepare an internal advisory for security teams?

SCENARIO 8: PRIVILEGE ESCALATION IN AN ENTERPRISE NETWORK

Situation:

A junior employee account, which should have low privileges, was found executing commands with SYSTEM-level access on a critical server.

Questions

1. How do you determine how this user escalated privileges?
2. What security misconfigurations could allow this?
3. What logs would you check for lateral movement?
4. How do you prevent future privilege escalation attacks?

SCENARIO 9: ADVANCED RANSOMWARE ATTACK WITH WORM-LIKE BEHAVIOUR

Situation:

A ransomware variant is rapidly encrypting files and spreading laterally across multiple departments. The attacker demands payment in cryptocurrency.

Questions

1. What is the first action you take to contain the infection?
2. How do you identify the initial infection vector?
3. What forensic techniques can help recover encrypted data?

4. What long-term security improvements should be implemented?

2. COMPLEX SIEM INVESTIGATION SIMULATIONS

SIMULATION 5: UNUSUAL DNS TRAFFIC – POSSIBLE DATA EXFILTRATION

Data Given:

- SIEM detects large volumes of DNS requests to an uncommon domain.
- The DNS queries are base64-encoded and contain sensitive-looking strings.

Questions

1. How do you confirm if data is being exfiltrated over DNS?
2. What tools can help decode and analyse the DNS payloads?
3. How do you block and prevent DNS tunneling attacks?
4. What SIEM correlation rules can detect similar threats in the future?

SIMULATION 6: ROGUE ADMINISTRATOR ACCOUNT CREATED IN ACTIVE DIRECTORY

Data Given:

- An unexpected administrator account was created without an official request.
- The account was used to access multiple high-value servers.

Questions

1. How do you determine if this account was created maliciously or due to an insider threat?
2. What logs in Windows Event Viewer help track account creation?
3. How do you immediately contain this threat?
4. What security policies prevent unauthorised admin account creation?

3. ADVANCED THREAT HUNTING CHALLENGES

CHALLENGE 5: FILELESS MALWARE EXECUTING FROM WMI

Attackers have embedded a fileless malware payload within Windows Management Instrumentation (WMI) to achieve persistence.

Questions

1. How do you detect and analyse malicious WMI persistence?
2. What PowerShell commands can help investigate WMI-based attacks?

3. How do you remove and prevent WMI persistence mechanisms?
4. What are the differences between file-based and fileless malware detection?

CHALLENGE 6: LIVING OFF THE LAND (LOTL) ATTACK DETECTION

Attackers use native Windows utilities (LOLBins) like certutil.exe, mshta.exe, and rundll32.exe to execute malicious scripts.

Questions

1. How do you differentiate between legitimate and malicious use of these tools?
2. What SIEM alerts or behavioral analysis techniques help detect LOLBins?
3. How do you create detection rules for these tactics?
4. What security hardening techniques prevent LOTL attacks?

4. MALWARE ANALYSIS & REVERSE ENGINEERING SCENARIOS

SCENARIO 5: MACRO-BASED MALWARE IN OFFICE DOCUMENTS

Situation:

A user receives an email with an attached .docm file. When opened, the document asks to "Enable Macros," after which unusual network traffic starts.

Questions

1. How do you analyse the macro without executing it?
2. What tools (e.g., oletools, VBA editor) help extract the macro code?
3. How do you track the malware's network communication?
4. How do you protect users from similar threats?

SCENARIO 6: PE FILE CONTAINING ROOTKIT CAPABILITIES

Situation:

A suspicious .exe file is reported by an EDR system. The file uses direct kernel object manipulation (DKOM) to hide processes.

Questions

1. How do you analyse if the file contains rootkit behavior?
2. What debugging tools (WinDbg, Volatility) can inspect hidden processes?
3. How do you extract and analyse the malware’s kernel hooks?
4. How do you prevent kernel-mode rootkits from being installed?

5. CLOUD SECURITY SCENARIOS

SCENARIO 3: UNAUTHORISED API KEY EXPOSURE IN GITHUB

Situation:

A developer accidentally pushes an AWS API key to a public GitHub repository.

Questions

1. How do you quickly determine if the key has been used maliciously?
2. What steps do you take to revoke and rotate the key?
3. What security policies prevent API key leaks in the future?
4. What cloud monitoring tools help detect and alert on such leaks?

SCENARIO 4: CLOUD CRYPTOJACKING ATTACK

Situation:

Your cloud billing unexpectedly spikes, and logs show high CPU usage from unknown processes in your Kubernetes cluster.

Questions

1. How do you confirm if cryptojacking malware is running in your cloud environment?
2. What forensic steps help determine the attack entry point?
3. How do you immediately contain and eradicate the malicious containers?
4. What cloud security best practices prevent cryptojacking?

6. ADVANCED SOC OPERATIONS & CRISIS MANAGEMENT

SCENARIO: TARGETED ATTACK ON CEO'S PERSONAL DEVICES

An executive's personal laptop and mobile phone have been compromised by an advanced persistent threat (APT) group while traveling overseas.

Questions

1. How do you determine if the compromise affects corporate data?
2. What immediate incident response steps should be taken?
3. How do you prevent future executive-level cyber espionage attempts?
4. What role does cyber threat intelligence play in mitigating such attacks?

7. BONUS – RED TEAM VS. BLUE TEAM CHALLENGE

SCENARIO: ACTIVE RED TEAM EXERCISE IN YOUR ORGANISATION

Situation:

Your internal red team executes a **covert penetration test** and gains **domain admin** privileges without triggering SIEM alerts.

Questions

1. How do you retrospectively analyse their attack path?
2. What advanced detection techniques (e.g., deception, honeypots) help identify Red Team activities?
3. How do you harden Active Directory against stealthy attacks?
4. How do you conduct a post-mortem to improve blue team defenses?

ANSWERS

SET 1

1. INCIDENT RESPONSE SCENARIOS

SCENARIO 1: RANSOMWARE ATTACK

Questions:

1. **What are the first three steps you take in response?**
    - **Step 1:** Isolate the infected system from the network to prevent further spread.
    - **Step 2:** Identify the scope of the infection by checking other systems for similar activity.
    - **Step 3:** Preserve evidence by taking snapshots of logs, memory, and the ransom note for forensic analysis.
2. **How would you determine the attack vector (e.g., phishing email, RDP compromise)?**
    - Check email logs for phishing attempts, review RDP logs for unauthorised access, and analyse firewall logs for unusual inbound/outbound traffic.
3. **What logs would you check to track the attacker's movement?**
    - Windows Event Logs (e.g., Event ID 4624 for logins), SIEM logs, firewall logs, and antivirus logs.
4. **If you find an infected endpoint, what containment measures do you apply?**
    - Disconnect the endpoint from the network, disable user accounts associated with the infection, and apply network segmentation to limit lateral movement.
5. **How do you handle communication with stakeholders and law enforcement?**
    - Notify internal stakeholders (e.g., IT, legal, management) and report the incident to law enforcement (e.g., FBI, local cybercrime units). Provide regular updates on the incident response progress.

SCENARIO 2: DATA EXFILTRATION DETECTED

Questions:

1. **What tools and logs would you use to investigate this anomaly?**
    - Use network monitoring tools (e.g., Wireshark, NetFlow) and review firewall logs, proxy logs, and endpoint logs.
2. **How can you determine whether this is legitimate or malicious activity?**

    - Check if the traffic aligns with normal business operations, verify the destination IP, and analyse the type of data being transmitted.
3. **If confirmed as malicious, how would you stop the data exfiltration?**
    - Block the destination IP at the firewall, disconnect the affected workstation, and revoke user credentials.
4. **What recommendations would you make to prevent this from happening again?**
    - Implement Data Loss Prevention (DLP) tools, enforce strict access controls, and conduct regular employee training on data security.

SCENARIO 3: PHISHING CAMPAIGN TARGETING EMPLOYEES

Questions:

1. **How do you identify the scope of this phishing attack?**
    - Check email logs to identify all recipients of the phishing email and monitor for any unusual login activity.
2. **What logs would you analyse to check for credential theft?**
    - Review authentication logs (e.g., Active Directory, VPN logs) and SIEM alerts for suspicious login attempts.
3. **What immediate actions would you take to mitigate the risk?**
    - Reset compromised passwords, enable Multi-Factor Authentication (MFA), and block the phishing domain.
4. **What long-term strategies can prevent future phishing attacks?**
    - Conduct regular phishing simulations, implement email filtering solutions, and provide ongoing security awareness training.

2. SIEM INVESTIGATION SIMULATIONS

SIMULATION 1: UNUSUAL LOGIN ATTEMPTS

Questions:

1. **How do you determine if this is a brute-force attack or a credential stuffing attempt?**
    - Check if the username is associated with known data breaches (credential stuffing) or if the attacker is systematically trying different passwords (brute-force).
2. **What actions should you take if the account gets compromised?**
    - Immediately reset the account password, enable MFA, and investigate for any unauthorised access.
3. **What security measures can prevent such login attempts?**

- Implement account lockout policies, use MFA, and monitor for unusual login patterns.

SIMULATION 2: SUSPICIOUS POWERSHELL EXECUTION

Questions:

1. **How do you decode the PowerShell command?**
   - Use tools like PowerShell Decoder or manually decode the Base64-encoded command.
2. **What logs should you analyse to trace the attacker's steps?**
   - Review PowerShell logs, Windows Event Logs, and network logs for suspicious activity.
3. **How do you determine the impact of the malware?**
   - Analyse the malware's behavior in a sandbox, check for persistence mechanisms, and review affected files.
4. **What mitigation steps should be taken?**
   - Isolate the infected host, remove the malware, and patch vulnerabilities that were exploited.

3. THREAT HUNTING CHALLENGES

CHALLENGE 1: FINDING SIGNS OF LATERAL MOVEMENT

Questions:

1. **What indicators in event logs (Event ID 4624, 4672, etc.) suggest lateral movement?**
   - Look for logins from unusual IPs, use of privileged accounts, and access to sensitive resources.
2. **How do you detect Pass-the-Hash or Pass-the-Ticket attacks?**
   - Monitor for unusual use of NTLM or Kerberos authentication and check for abnormal login patterns.
3. **What tools would you use to correlate logs across multiple systems?**
   - Use SIEM tools like Splunk or ELK Stack to correlate logs from different systems.

CHALLENGE 2: DETECTING A HIDDEN BACKDOOR

Questions:

1. **How do you detect unauthorised remote access tools?**

    - Use endpoint detection tools to scan for unauthorised software and monitor network traffic for unusual connections.
2. **What security controls can prevent unauthorised installations?**
    - Implement application whitelisting, restrict admin privileges, and enforce strict change management processes.
3. **How do you ensure an insider threat does not exploit such access?**
    - Conduct regular audits, monitor user activity, and implement least privilege access controls.

4. MALWARE ANALYSIS SCENARIOS

SCENARIO 1: WORD DOCUMENT WITH MACRO MALWARE

Questions:

1. **How do you analyse the macro in the document?**
    - Use tools like olevba or oletools to extract and analyse the macro code.
2. **How do you determine if the document dropped additional malware?**
    - Analyse network traffic for additional connections and check the system for newly created files or processes.
3. **What steps should be taken to block further exploitation?**
    - Disable macros by default, update antivirus signatures, and block the suspicious IP.

SCENARIO 2: SUSPICIOUS EXE DOWNLOAD

Questions:

1. **What are the steps for static and dynamic analysis of this file?**
    - **Static Analysis:** Use tools like PEiD or IDA Pro to examine the file without executing it.
    - **Dynamic Analysis:** Execute the file in a sandbox and monitor its behavior.
2. **How do you determine if the file is a Remote Access Trojan (RAT)?**
    - Check for behaviors like creating network connections, modifying registry keys, and attempting to hide its presence.
3. **If the malware creates persistence, how do you remove it?**
    - Identify and delete persistence mechanisms (e.g., registry keys, scheduled tasks) and remove the malicious file.

5. LOG ANALYSIS CHALLENGES

CHALLENGE 1: ANALYSING WEB SERVER LOGS

Questions:

1. **What log files do you review for authentication attempts?**
    - Review web server logs (e.g., Apache, IIS) and application logs for failed login attempts.
2. **How do you detect SQL injection or XSS attempts?**
    - Look for unusual query strings or payloads in the logs that match known attack patterns.
3. **What firewall rules can prevent further attacks?**
    - Implement IP blocking rules, rate limiting, and Web Application Firewall (WAF) rules to block malicious traffic.

CHALLENGE 2: SUSPICIOUS OUTBOUND DNS REQUESTS

Questions:

1. **How do you identify if this is a Command & Control (C2) beaconing?**
    - Check for patterns in the DNS queries, such as high frequency, random subdomains, or unusual TLDs.
2. **What response actions should be taken?**
    - Isolate the affected workstation, block the suspicious domains, and investigate for malware.
3. **How can you prevent DNS tunneling attacks?**
    - Implement DNS filtering, monitor for unusual DNS traffic, and enforce strict DNS policies.

6. SOC WORKFLOW & PLAYBOOK QUESTIONS

General SOC Questions:

1. **What are the key phases in an incident response process?**
    - Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
2. **How do you categorise alert severity in an MSSP?**
    - Based on impact (e.g., high, medium, low) and urgency (e.g., critical, major, minor).
3. **How do you communicate an ongoing incident to stakeholders?**
    - Provide regular updates, use clear and concise language, and escalate as needed.
4. **What KPIs should a SOC team track to measure efficiency?**
    - Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and number of incidents resolved.

Playbook Development Questions:

1. **How do you standardise response actions for different threat types?**
    - Create playbooks with step-by-step instructions for each type of threat (e.g., ransomware, phishing).
2. **What elements should a phishing playbook include?**
    - Steps for identifying phishing emails, resetting compromised accounts, and blocking malicious domains.
3. **How do you ensure continuous improvement in incident handling?**
    - Conduct post-incident reviews, update playbooks based on lessons learned, and provide ongoing training.

7. CYBERSECURITY FRAMEWORKS & COMPLIANCE

SCENARIO: YOUR COMPANY IS AUDITED FOR COMPLIANCE

Questions:

1. **How do you align your security operations with NIST, ISO 27001, or CIS benchmarks?**
    - Implement controls and processes that meet the requirements of these frameworks and document evidence of compliance.
2. **What logs and reports do you provide to prove compliance?**
    - Provide logs of access controls, incident response activities, and security training records.
3. **How do you handle security policy violations discovered during the audit?**
    - Investigate the violations, take corrective actions, and update policies to prevent future violations.

8. MISCELLANEOUS TECHNICAL QUESTIONS

1. **Explain the difference between symmetric and asymmetric encryption.**
    - **Symmetric Encryption:** Uses the same key for encryption and decryption (e.g., AES).
    - **Asymmetric Encryption:** Uses a public key for encryption and a private key for decryption (e.g., RSA).
2. **What are the different types of firewalls, and how do they work?**
    - **Packet Filtering Firewall:** Filters traffic based on IP addresses and ports.
    - **Stateful Inspection Firewall:** Tracks the state of active connections.
    - **Proxy Firewall:** Acts as an intermediary between users and the internet.
    - **Next-Generation Firewall (NGFW):** Includes advanced features like intrusion prevention and application control.

3. **How does TLS ensure secure communication?**
    - TLS uses encryption to protect data in transit, ensuring confidentiality, integrity, and authentication.
4. **What is a zero-day vulnerability, and how do companies mitigate it?**
    - A zero-day vulnerability is an unknown security flaw exploited by attackers. Mitigation includes patch management, intrusion detection systems, and threat intelligence.

SET 2

1. ADVANCED INCIDENT RESPONSE SCENARIOS

SCENARIO 4: INSIDER THREAT -- DATA THEFT BY AN EMPLOYEE

Questions:

1. **What logs would you analyse to confirm this data theft?**
    - Review file server access logs, USB device logs, and user activity logs.
2. **How do you determine if the data was exfiltrated to an external cloud service?**
    - Check network logs for uploads to cloud services and review the employee's browsing history.
3. **What security controls could have prevented this incident?**
    - Implement Data Loss Prevention (DLP) tools, restrict USB usage, and enforce strict access controls.
4. **If the data was leaked, what are the legal and compliance implications?**
    - Notify affected parties, report the breach to regulatory authorities, and conduct a forensic investigation.

SCENARIO 5: SUPPLY CHAIN ATTACK -- COMPROMISED SOFTWARE UPDATE

Questions:

1. **How do you verify if this patch is legitimate or compromised?**
    - Check the patch's digital signature, compare its hash with the vendor's official release, and contact the vendor for confirmation.
2. **What logs would help track the execution of the malicious code?**
    - Review PowerShell logs, Windows Event Logs, and network logs for suspicious activity.
3. **What is your containment and eradication strategy?**
    - Isolate affected systems, remove the malicious patch, and apply a clean update from the vendor.
4. **What policies should be implemented to prevent supply chain attacks?**

- Verify software integrity before installation, monitor for unusual activity post-update, and maintain a secure software supply chain.

SCENARIO 6: BUSINESS EMAIL COMPROMISE (BEC) ATTACK

Questions:

1. **How do you verify if this email is legitimate?**
   - Contact the CEO directly through a verified communication channel (e.g., phone) to confirm the request.
2. **What logs can help determine if the CEO's email was spoofed or compromised?**
   - Review email headers, check for unusual login activity on the CEO's account, and analyse SMTP logs.
3. **If the transfer was made, how would you attempt to recover the funds?**
   - Contact the bank immediately to reverse the transaction and report the incident to law enforcement.
4. **What long-term email security measures should be implemented?**
   - Implement email authentication (e.g., DMARC, SPF), conduct regular phishing training, and enforce multi-factor authentication.

2. COMPLEX SIEM INVESTIGATION SIMULATIONS

SIMULATION 3: BEACONING MALWARE -- PERSISTENT C2 TRAFFIC

Questions:

1. **How do you confirm whether this is a Command & Control (C2) server?**
   - Analyse the traffic patterns, check for known malicious IPs, and use threat intelligence feeds.
2. **What tools can help decode the beaconing traffic?**
   - Use tools like Wireshark, Bro/Seek, or a SIEM with advanced analytics.
3. **How do you isolate and remediate the affected workstation?**
   - Disconnect the workstation from the network, remove the malware, and patch vulnerabilities.
4. **What YARA rules can be created to detect similar threats in the future?**
   - Create rules based on the malware's behavior, such as specific strings, IPs, or domains.

SIMULATION 4: EXPLOITATION OF A WEB SERVER

Questions:

1. **How do you analyse the attack to determine the exploited vulnerability?**

    - Review the SQL injection payload, check for vulnerable code in the web application, and analyse database logs.
2. **What logs would help identify the full impact of the breach?**
    - Review web server logs, database logs, and network logs for unauthorised access.
3. **How do you mitigate the SQL injection vulnerability?**
    - Patch the vulnerable code, implement input validation, and use parameterised queries.
4. **What Web Application Firewall (WAF) rules should be implemented?**
    - Implement rules to block SQL injection attempts, monitor for unusual traffic, and enforce strict input validation.

3. ADVANCED THREAT HUNTING CHALLENGES

CHALLENGE 3: FILELESS MALWARE DETECTION

Questions:

1. **How do you detect fileless malware when no traditional malware files exist?**
    - Monitor PowerShell logs for unusual commands, analyse memory for malicious scripts, and use endpoint detection tools.
2. **What Windows Event IDs are useful for detecting PowerShell exploitation?**
    - Event ID 4104 (PowerShell script block logging) and Event ID 4688 (process creation).
3. **How do you create Sigma rules to hunt for similar activities?**
    - Create rules based on known fileless malware behaviors, such as unusual PowerShell commands or memory execution.

CHALLENGE 4: IDENTIFYING CREDENTIAL DUMPING ATTEMPTS

Questions:

1. **What are the common techniques used for credential dumping?**
    - Tools like Mimikatz, Procdump, and PowerShell scripts are commonly used.
2. **How do you determine if Mimikatz or similar tools were used?**
    - Check for unusual process creations, analyse memory dumps, and review PowerShell logs.
3. **What mitigation strategies can prevent credential dumping?**
    - Enable Credential Guard, restrict access to LSASS, and monitor for unusual process behavior.

4. MALWARE ANALYSIS & REVERSE ENGINEERING SCENARIOS

SCENARIO 3: ANDROID MALWARE INVESTIGATION

Questions:

1. **How do you analyse the APK file to determine if it's malware?**
    - Use tools like MobSF, JADX, or APKTool to decompile and analyse the APK.
2. **What tools (e.g., MobSF, JADX, APKTool) can be used for static and dynamic analysis?**
    - **Static Analysis:** MobSF, JADX.
    - **Dynamic Analysis:** Android emulator, Frida.
3. **What signs indicate spyware or banking trojans?**
    - Excessive permissions, unusual network traffic, and attempts to access sensitive data.
4. **How do you mitigate and report such Android malware?**
    - Remove the app, revoke its permissions, and report it to Google Play Protect.

SCENARIO 4: WINDOWS PE MALWARE ANALYSIS

Questions:

1. **What are the steps for static analysis of this PE file?**
    - Use tools like PEiD, IDA Pro, or Ghidra to analyse the file's structure and code.
2. **How do you safely execute and monitor its behavior in a sandbox?**
    - Use a sandbox like Cuckoo or Joe Sandbox to execute the file and monitor its behavior.
3. **How do you extract Indicators of Compromise (IOCs) from the malware?**
    - Extract IPs, domains, file hashes, and registry keys used by the malware.
4. **What YARA rules can you create to detect similar samples?**
    - Create rules based on the malware's unique strings, behaviors, or code patterns.

5. CLOUD SECURITY SCENARIOS

SCENARIO 1: MISCONFIGURED AWS S3 BUCKET LEAK

Questions:

1. **How do you verify which data has been leaked?**
    - Review S3 access logs and check for unauthorised access to sensitive files.
2. **What AWS logs would you check to determine who accessed the data?**
    - Check CloudTrail logs for access events and S3 server access logs.

3. **How do you properly secure an S3 bucket against such misconfigurations?**
    - Set bucket policies to restrict public access, enable versioning, and use IAM roles.
4. **What IAM policies should be implemented to enforce least privilege access?**
    - Implement policies that grant only the necessary permissions to users and roles.

SCENARIO 2: UNAUTHORISED ACCESS TO AZURE AD

Questions:

1. **How do you investigate how the attacker bypassed MFA?**
    - Review Azure AD sign-in logs, check for compromised credentials, and analyse conditional access policies.
2. **What Azure AD logs can help track lateral movement?**
    - Review sign-in logs, audit logs, and security logs for unusual activity.
3. **What security controls can be implemented to detect and prevent similar attacks?**
    - Enable MFA, implement conditional access policies, and monitor for unusual sign-ins.

6. RED TEAM VS. BLUE TEAM CHALLENGE

SCENARIO: DETECTING & MITIGATING AN ACTIVE RED TEAM ATTACK

Questions:

1. **What are the most effective detection methods for Cobalt Strike beacons?**
    - Monitor for unusual network traffic, analyse process behavior, and use endpoint detection tools.
2. **How do you identify and remove persistence mechanisms?**
    - Check for unusual scheduled tasks, registry keys, and startup items.
3. **What proactive threat-hunting techniques can detect advanced adversaries?**
    - Use behavioral analysis, threat intelligence, and deception techniques like honeypots.
4. **How do you refine your detection engineering strategies?**
    - Continuously update detection rules based on new threats, conduct red team exercises, and analyse past incidents.

7. SOC WORKFLOW & CRISIS MANAGEMENT

SCENARIO: RANSOMWARE ATTACK HITS PRODUCTION SERVERS

Questions:

1. **How do you determine the ransomware variant and attack vector?**
    - Analyse the ransom note, check for known indicators of compromise (IOCs), and review logs for the initial infection.
2. **Should you negotiate with the attackers or restore from backups?**
    - Restore from backups if possible, as negotiating with attackers is risky and not guaranteed to succeed.
3. **How do you ensure a clean recovery without reinfection?**
    - Isolate infected systems, patch vulnerabilities, and thoroughly scan all systems before restoring.
4. **What security policies should be changed post-incident?**
    - Implement stricter access controls, improve patch management, and conduct regular security training.

8. FINAL BOSS-LEVEL QUESTIONS

1. **APT Hunting:** How do you track an Advanced Persistent Threat (APT) in a large enterprise?
    - Use threat intelligence, conduct behavioral analysis, and monitor for unusual network traffic.
2. **SIEM Fine-Tuning:** How do you reduce false positives without missing real threats?
    - Adjust correlation rules, use machine learning to filter noise, and regularly review alerts.
3. **Cyber Threat Intelligence (CTI):** How do you integrate threat intelligence feeds into SOC workflows?
    - Automate the ingestion of threat feeds, correlate IOCs with internal logs, and use threat intelligence to prioritise alerts.
4. **AI in Cybersecurity:** How can AI/ML improve SOC detection and response?
    - AI/ML can improve threat detection by analysing large datasets, identifying patterns, and automating response actions.

SET 3

1. ADVANCED INCIDENT RESPONSE SCENARIOS

SCENARIO 7: ZERO-DAY EXPLOIT IN YOUR ORGANISATION

Questions:

1. **How do you confirm if your environment has been compromised?**

    - Search for known IOCs, analyse logs for unusual activity, and use endpoint detection tools.
2. **What logs or indicators would you search for?**
    - Review application logs, network logs, and endpoint logs for signs of exploitation.
3. **If no patch is available, what mitigation steps should you take?**
    - Implement network segmentation, disable vulnerable features, and monitor for exploitation attempts.
4. **How do you prepare an internal advisory for security teams?**
    - Provide details on the vulnerability, recommended mitigations, and steps to monitor for exploitation.

SCENARIO 8: PRIVILEGE ESCALATION IN AN ENTERPRISE NETWORK

Questions:

1. **How do you determine how this user escalated privileges?**
    - Review logs for privilege escalation attempts, check for misconfigurations, and analyse user activity.
2. **What security misconfigurations could allow this?**
    - Weak password policies, excessive permissions, and lack of privilege separation.
3. **What logs would you check for lateral movement?**
    - Review Windows Event Logs, network logs, and SIEM alerts for unusual activity.
4. **How do you prevent future privilege escalation attacks?**
    - Implement least privilege access, regularly review user permissions, and monitor for unusual activity.

SCENARIO 9: ADVANCED RANSOMWARE ATTACK WITH WORM-LIKE BEHAVIOUR

Questions:

1. **What is the first action you take to contain the infection?**
    - Isolate infected systems from the network to prevent further spread.
2. **How do you identify the initial infection vector?**
    - Analyse logs for the first signs of infection, such as phishing emails or malicious downloads.
3. **What forensic techniques can help recover encrypted data?**
    - Use file recovery tools, check for shadow copies, and analyse memory dumps.
4. **What long-term security improvements should be implemented?**

- Implement network segmentation, improve patch management, and conduct regular security training.

2. COMPLEX SIEM INVESTIGATION SIMULATIONS

SIMULATION 5: UNUSUAL DNS TRAFFIC -- POSSIBLE DATA EXFILTRATION

Questions:

1. **How do you confirm if data is being exfiltrated over DNS?**
   - Decode the DNS queries, analyse the payload, and check for patterns of sensitive data.
2. **What tools can help decode and analyse the DNS payloads?**
   - Use tools like Wireshark, DNSQuerySniffer, or a SIEM with DNS analysis capabilities.
3. **How do you block and prevent DNS tunneling attacks?**
   - Implement DNS filtering, monitor for unusual DNS traffic, and enforce strict DNS policies.
4. **What SIEM correlation rules can detect similar threats in the future?**
   - Create rules to detect base64-encoded DNS queries, unusual domain patterns, and high-volume DNS traffic.

SIMULATION 6: ROGUE ADMINISTRATOR ACCOUNT CREATED IN ACTIVE DIRECTORY

Questions:

1. **How do you determine if this account was created maliciously or due to an insider threat?**
   - Review account creation logs, check for unusual activity, and investigate the user who created the account.
2. **What logs in Windows Event Viewer help track account creation?**
   - Event ID 4720 (user account created) and Event ID 4722 (user account enabled).
3. **How do you immediately contain this threat?**
   - Disable the rogue account, revoke its permissions, and investigate its activity.
4. **What security policies prevent unauthorised admin account creation?**
   - Implement strict change management processes, enforce least privilege access, and monitor for unusual account activity.

3. ADVANCED THREAT HUNTING CHALLENGES

CHALLENGE 5: FILELESS MALWARE EXECUTING FROM WMI

Questions:

1. **How do you detect and analyse malicious WMI persistence?**
    - Use tools like WMI Explorer to analyse WMI objects and check for unusual scripts.
2. **What PowerShell commands can help investigate WMI-based attacks?**
    - Use Get-WmiObject to query WMI classes and check for suspicious entries.
3. **How do you remove and prevent WMI persistence mechanisms?**
    - Delete malicious WMI objects, implement WMI filtering, and monitor for unusual WMI activity.
4. **What are the differences between file-based and fileless malware detection?**
    - File-based malware can be detected through file signatures, while fileless malware requires behavioral analysis and memory forensics.

CHALLENGE 6: LIVING OFF THE LAND (LOTL) ATTACK DETECTION

Questions:

1. **How do you differentiate between legitimate and malicious use of these tools?**
    - Analyse the context of the command, check for unusual parameters, and monitor for suspicious behavior.
2. **What SIEM alerts or behavioral analysis techniques help detect LOLBins?**
    - Use behavioral analysis to detect unusual command patterns and create alerts for known LOLBin abuse.
3. **How do you create detection rules for these tactics?**
    - Create rules based on known LOLBin abuse patterns, such as unusual command-line arguments or network connections.
4. **What security hardening techniques prevent LOTL attacks?**
    - Restrict access to LOLBins, monitor for unusual command usage, and implement application whitelisting.

4. MALWARE ANALYSIS & REVERSE ENGINEERING SCENARIOS

SCENARIO 5: MACRO-BASED MALWARE IN OFFICE DOCUMENTS

Questions:

1. **How do you analyse the macro without executing it?**
    - Use tools like olevba or oletools to extract and analyse the macro code.
2. **What tools (e.g., oletools, VBA editor) help extract the macro code?**

    - Use olevba to extract the macro code and analyse it in a VBA editor.
3. **How do you track the malware's network communication?**
    - Use network monitoring tools like Wireshark to capture and analyse the traffic.
4. **How do you protect users from similar threats?**
    - Disable macros by default, provide security training, and implement email filtering.

SCENARIO 6: PE FILE CONTAINING ROOTKIT CAPABILITIES

Questions:

1. **How do you analyse if the file contains rootkit behavior?**
    - Use tools like WinDbg or Volatility to analyse the file's behavior and check for hidden processes.
2. **What debugging tools (WinDbg, Volatility) can inspect hidden processes?**
    - Use WinDbg for live system analysis and Volatility for memory forensics.
3. **How do you extract and analyse the malware's kernel hooks?**
    - Use tools like WinDbg to analyse kernel hooks and check for unusual modifications.
4. **How do you prevent kernel-mode rootkits from being installed?**
    - Implement secure boot, use endpoint protection tools, and monitor for unusual kernel activity.

5. CLOUD SECURITY SCENARIOS

SCENARIO 3: UNAUTHORISED API KEY EXPOSURE IN GITHUB

Questions:

1. **How do you quickly determine if the key has been used maliciously?**
    - Check AWS CloudTrail logs for unauthorised API calls and monitor for unusual activity.
2. **What steps do you take to revoke and rotate the key?**
    - Immediately revoke the exposed key, generate a new key, and update all systems using the old key.
3. **What security policies prevent API key leaks in the future?**
    - Implement pre-commit hooks to scan for sensitive data, enforce code reviews, and use secret management tools.
4. **What cloud monitoring tools help detect and alert on such leaks?**
    - Use tools like AWS Config, CloudTrail, and third-party solutions like GitGuardian.

SCENARIO 4: CLOUD CRYPTOJACKING ATTACK

Questions:

1. **How do you confirm if cryptojacking malware is running in your cloud environment?**
    - Analyse CPU usage, check for unknown containers, and monitor for connections to known cryptojacking domains.
2. **What forensic steps help determine the attack entry point?**
    - Review Kubernetes logs, check for misconfigured pods, and analyse network traffic.
3. **How do you immediately contain and eradicate the malicious containers?**
    - Isolate the affected pods, delete malicious containers, and patch vulnerabilities.
4. **What cloud security best practices prevent cryptojacking?**
    - Implement resource quotas, monitor for unusual CPU usage, and enforce strict access controls.

6. ADVANCED SOC OPERATIONS & CRISIS MANAGEMENT

SCENARIO: TARGETED ATTACK ON CEO'S PERSONAL DEVICES

Questions:

1. **How do you determine if the compromise affects corporate data?**
    - Check for access to corporate accounts, review email logs, and analyse device activity.
2. **What immediate incident response steps should be taken?**
    - Isolate the devices, reset credentials, and conduct a forensic analysis.
3. **How do you prevent future executive-level cyber espionage attempts?**
    - Provide secure devices, enforce MFA, and conduct regular security training.
4. **What role does cyber threat intelligence play in mitigating such attacks?**
    - Threat intelligence helps identify APT tactics, track IOCs, and improve detection capabilities.

7. BONUS -- RED TEAM VS. BLUE TEAM CHALLENGE

SCENARIO: ACTIVE RED TEAM EXERCISE IN YOUR ORGANISATION

Questions:

1. **How do you retrospectively analyse their attack path?**

    - Review logs for unusual activity, analyse the red team's tools and techniques, and conduct a post-mortem.
2. **What advanced detection techniques (e.g., deception, honeypots) help identify Red Team activities?**
    - Use deception techniques like honeypots, monitor for unusual behavior, and implement advanced threat hunting.
3. **How do you harden Active Directory against stealthy attacks?**
    - Implement least privilege access, monitor for unusual account activity, and use tools like Microsoft ATA.
4. **How do you conduct a post-mortem to improve blue team defenses?**
    - Analyse the red team's tactics, update detection rules, and implement lessons learned into security policies.