CYBERSECURITY DAILY OPERATIONS: REAL-WORLD Q&A SCENARIOS

VAISHALI SHISHODIA

SOC Analyst Daily Operations: Real-World Q&A Scenarios

---

1. Incident Detection and Response:

- **Q:** You notice a sudden spike in inbound traffic to a particular server, accompanied by multiple failed login attempts. What steps would you take to investigate this incident?
- **A:** First, I would gather information about the server in question (e.g., IP addresses, service ports). Then, I'd check logs for any unusual login attempts, including failed and successful logins, to assess if it could be a brute-force attack. I'd also look at the pattern of the traffic increase to determine if it's an anomaly, check for any signs of a DDoS attack, and correlate it with other data sources (IDS, firewall logs). Finally, I would escalate if necessary or begin containment steps based on the severity of the issue (e.g., blocking IPs, isolating affected assets).

2. Phishing Email Alert:

- **Q:** A user has reported receiving a suspicious email with a link that leads to a fake login page. How do you handle this alert?
- **A:** First, I'd confirm the legitimacy of the report and then analyze the email's metadata, including the sender's IP and domain, to identify any suspicious patterns. I would also investigate the URL using a threat intelligence tool to see if it's already flagged. After that, I'd inform the user not to click on the link and advise them to change their password if they interacted with it. If needed, I'd block the malicious domain and update the email filter rules. Additionally, I'd perform a scan of the network for any indicators of compromise (IoC) related to this phishing attempt.

3. Malware Detection:

- **Q:** During a routine scan, you identify a piece of malware on an endpoint that is actively communicating with an external IP address. What actions should you take immediately?
- **A:** I would isolate the affected endpoint from the network to prevent further spread. Then, I would conduct a full malware analysis, including checking the process and file system for any abnormal activity or persistence mechanisms. I would also gather details about the external IP address to see if it's related to known threat actors or malicious activities. Following that, I would work with the incident response team to determine containment and eradication procedures and ensure the endpoint is fully cleaned. Finally, I would review other endpoints for potential compromise.

4. Alert Triage:

- **Q:** You're receiving multiple alerts from your SIEM platform about potential data exfiltration, but they appear to be false positives. How do you prioritize these alerts?
- **A:** I would start by reviewing the alert context and severity level. I would check if the triggers are related to known activity (e.g., routine backups or software updates). If they are false positives, I'd fine-tune the alert rules to reduce future noise. However, I'd escalate any alert that shows patterns of behavior that could indicate a more serious threat, such as unusually large file transfers to external IPs, which might require deeper investigation. Communication

with relevant stakeholders (e.g., network teams) is key to clarifying if any authorized data transfers are taking place.

5. Vulnerability Scanning and Patching:

- **Q:** You've just been alerted to a critical vulnerability in a commonly used software version across your organization. How do you handle patch management for this vulnerability?
- **A:** I would first confirm the scope of the vulnerability and ensure that the software version is indeed present on critical assets within the organization. I would work with the system administrators to prioritize patch deployment, making sure that any systems exposed to the internet or containing sensitive data are patched first. I would also communicate with the teams to assess if there are any dependencies that need to be tested before patching. Once the patch is deployed, I'd verify its successful implementation and check for any unusual behavior after the update.

6. Log Analysis:

- **Q:** You've been asked to analyze a large volume of logs to identify any potential breach indicators. How would you begin your investigation?
- **A:** I would begin by filtering the logs based on the timeframe of interest and then narrowing down key events, such as failed logins, unusual account activity, or network anomalies. I'd look for signs of lateral movement or privilege escalation, which might suggest an ongoing attack. Using correlation rules or threat intelligence, I'd try to link these logs to known attack patterns or IoCs. Depending on the findings, I would escalate the incident or take containment actions as necessary.

7. Incident Escalation:

- **Q:** After escalating an alert regarding potential insider threat behavior, your supervisor instructs you to continue monitoring. What additional steps would you take to ensure thorough monitoring of this potential threat?
- **A:** I would set up detailed monitoring of the user's activity across the network, focusing on unusual access patterns (e.g., accessing sensitive files at odd hours, transferring large volumes of data). Additionally, I would review any recent changes to their account (e.g., privilege changes) and correlate with other indicators (e.g., related IP addresses or devices). I would also continue to check for any alerts related to that user's activity in the SIEM and keep a detailed log of any findings to inform further escalation if needed.

8. DDoS Attack Alert:

- **Q:** The network team reports significant slowdowns, and your monitoring tools have triggered DDoS-related alerts. What immediate actions would you take to verify the attack and mitigate it?
- **A:** First, I would confirm the DDoS attack by reviewing network traffic patterns to see if they match typical DDoS signatures (e.g., a flood of requests from a large number of IP addresses). I would then escalate the issue to the appropriate network team to implement DDoS mitigation measures such as rate limiting, blackholing, or re-routing traffic. In parallel, I'd update firewall rules and review other network defenses to ensure we're blocking malicious traffic. Once mitigated, I'd continue monitoring to ensure the attack subsides.

9. Access Control Violation:

- **Q:** A user reports being unable to access their workstation after hours, and logs indicate that their account was locked after multiple failed login attempts. What would you do next?
- **A:** I would check the reason for the failed login attempts, looking for any signs of a brute-force attack or unauthorized access attempts. I'd also review any recent changes to the user's access control settings or permissions to ensure there hasn't been a misconfiguration. If the user's account was potentially compromised, I'd initiate a password reset and ensure that the workstation is free from any malware. I'd also review logs for lateral movement or further attempts to escalate privileges.

10. Zero-Day Exploit:

- **Q:** A zero-day exploit is discovered in a piece of software used by your organization. How would you manage the situation, given there is no immediate patch available?
- **A:** First, I would assess the risk associated with the vulnerability and identify which systems are most at risk. I'd work with the IT and network teams to implement workarounds or mitigations (e.g., blocking certain ports or disabling vulnerable features) until a patch is available. Additionally, I would increase monitoring on the systems using this software for any signs of exploitation. Once a patch is released, I would prioritize deployment and confirm that it's applied successfully across the organization.

11. Unusual Account Activity:

- **Q:** You receive an alert indicating an unusual login attempt from an unfamiliar geographic location. What steps do you take to investigate this potential account compromise?
- **A:** First, I'd verify if the location is indeed unusual by cross-referencing the user's typical login patterns and geographical regions. If the login is unusual but not impossible, I would look into the authentication method used (e.g., was it a VPN, SSO, or traditional login?). I'd also check if the user has any active sessions and verify that no unauthorized actions have been performed (e.g., privilege escalation or access to sensitive resources). I would consider resetting the user's password, forcing MFA authentication, and notify the user for additional checks. If necessary, I would escalate to investigate further if any IoC are tied to this login.

12. Insider Threat Behavior:

- **Q:** A user has been observed downloading large amounts of sensitive data over the last few days, and they have no legitimate reason to access the files. How do you handle this situation?
- **A:** I would first confirm the user's actions through file access logs, determining the scope and sensitivity of the data accessed. Then, I'd determine whether this behavior is out of character for the user or if it could be part of their regular duties. I'd also check if there were any signs of privilege escalation or misuse of access. If the activity seems suspicious, I would escalate the case, monitor the user's activity in real-time, and involve HR or legal if necessary. Depending on the severity, I may restrict the user's access until further investigation is completed.

13. Ransomware Alert:

- **Q:** A computer in the organization is flagged as potentially infected with ransomware. What is your immediate course of action?
- **A:** I would immediately isolate the infected system to prevent the spread of ransomware to other devices. Next, I would analyze the processes running on the affected system to identify any encryption or file-locking behaviors. I'd check if any files have been modified or encrypted and search for known ransomware signatures. I'd then inform the incident response team to follow containment, eradication, and recovery procedures. I would also initiate backups to restore data (if available) and ensure no further damage is done to critical assets.

14. Exfiltration of Sensitive Data:

- **Q:** You notice an alert indicating that a large amount of sensitive data is being uploaded to an external server. How would you proceed with the investigation?
- **A:** I would immediately review the traffic patterns to confirm if this behavior is legitimate or if it represents a breach. I would analyze the external IP address to determine whether it is associated with known threat actors or domains. I would also check the user or system initiating the upload to understand their access level and whether the data involved is authorized. If it's unauthorized, I'd attempt to block the data transfer and work with the network team to stop further exfiltration. At the same time, I'd start an investigation into the source of the exfiltration and look for any signs of compromise or misconfigurations. After containment, I'd report findings to management.

15. Network Traffic Anomalies:

- **Q:** Your SIEM tool has flagged unusual outbound traffic patterns, with an increase in encrypted traffic at odd hours. What actions would you take to investigate this anomaly?
- **A:** I would start by examining the affected traffic in more detail, including the destination and the volume of encrypted traffic. I'd check if this could be legitimate traffic (e.g., scheduled backups, cloud-based services, etc.), or if it might indicate the use of covert channels by an attacker (e.g., data exfiltration or a C2 server). I'd work with network monitoring tools to see if there's any correlation with known IoC or suspicious traffic signatures. If the traffic is indeed suspicious, I would attempt to block or throttle the communication while conducting further analysis. I'd also ensure the endpoint involved is investigated for signs of compromise.

16. Multiple Failed Login Attempts (Brute Force Attack):

- **Q:** You've been alerted to multiple failed login attempts from the same IP address, targeting several user accounts. What would you do to mitigate the risk?
- **A:** First, I'd verify the scope of the attack by analyzing the logins in greater detail, checking which accounts were targeted, and how many failed attempts were made. I would then temporarily block the IP address or introduce rate limiting to prevent further attempts. I'd also verify if there's any evidence of successful login attempts or lateral movement within the network. I would check whether the accounts involved are using weak passwords and recommend a password reset or enforce multi-factor authentication (MFA) for enhanced security. Depending on the severity, I would escalate the issue for a deeper investigation.

17. Vulnerability Exploit Attempt:

- **Q:** An attempt has been made to exploit a known vulnerability in an old version of a web server running in your organization. What is your immediate response?
- **A:** I would immediately isolate the affected system to prevent further exploitation. Next, I'd verify the vulnerability and check for any active indicators of compromise (e.g., abnormal network traffic, new processes). I'd prioritize patching or upgrading the vulnerable system to a more secure version. After that, I would review the logs to check if there's been any unauthorized access or data exfiltration due to this exploit. I'd also ensure that any other similar systems are up-to-date and check for any other vulnerabilities in the environment. If necessary, I would notify relevant stakeholders and initiate remediation and recovery procedures.

18. Social Engineering Attack (Impersonation):

- **Q:** A user reports receiving a phone call from someone claiming to be IT support, asking for their password to resolve a "system issue." How would you handle this report?
- **A:** I'd first advise the user not to provide any sensitive information and to hang up immediately. Then, I'd verify if there have been any other similar reports across the organization to determine if it's part of a larger social engineering campaign. I'd check if any actual support staff were involved or if the impersonator had any knowledge of internal systems that could indicate a breach. After gathering more context, I'd work with HR or management to issue a security awareness reminder to staff, reminding them of phishing/social engineering risks. Additionally, I'd investigate any indicators of potential system compromise or data leak tied to this incident.

19. SIEM Alert Fatigue:

- **Q:** The SIEM system is generating a large number of alerts, many of which appear to be false positives or low-severity issues. How do you handle alert fatigue while ensuring that critical threats are not overlooked?
- **A:** First, I would review the current alert rules and thresholds to identify and eliminate any known sources of false positives. I'd work with the team to fine-tune the rules and prioritize more meaningful alerts, focusing on high-risk events and patterns. I'd also establish an effective triage process to filter out low-priority alerts and focus on critical ones. Regular review of alert settings and continuous improvement of detection mechanisms would be necessary to ensure that the most relevant alerts are prioritized. If needed, I'd propose additional resources or automation to assist in managing the workload.

20. Security Patching Delay:

- **Q:** You notice that a critical patch for a known vulnerability in a widely used software package has been delayed. How do you address this gap in security coverage?
- **A:** I'd first assess the potential risk and exploitability of the vulnerability based on the organization's environment and the likelihood of an attack. If the patch is delayed, I would work with the appropriate teams to explore temporary mitigations (e.g., blocking ports, disabling vulnerable features, or applying workarounds). I'd escalate the issue to

management if there is a significant risk, ensuring they're aware of the gap and that it's prioritized. I would also increase monitoring for any indicators of exploitation targeting the vulnerable software until the patch is applied.
