DECISION-MAKING PROCESSES OF INCIDENT RESPONSE WITH EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

Table of Contents

BREAKDOWN OF THE DECISION-MAKING PROCESS

Stage 1: Initial Alert

- **Action**: Receive an alert from monitoring tools (e.g., SIEM) indicating a potential security incident.
- **Decision Point**: Determine the nature and severity of the alert.
  - **High Severity**: If the alert indicates a significant threat (e.g., unusual activity, malware detection), escalate immediately.
  - **Low Severity**: If the alert is less critical, continue monitoring or conduct a preliminary investigation.

Stage 2: Investigation

- **Action**: Collect and analyse data related to the alert (e.g., logs, network traffic, system behavior).
- **Decision Point**: Assess whether the suspicious activity is part of a security incident.
  - **Confirmed Incident**: If evidence suggests a security breach, escalate to containment.
  - **False Positive**: If the activity is deemed benign or non-threatening, document findings and close the alert.

Stage 3: Containment

- **Action**: Take immediate steps to contain the incident and prevent it from spreading.
- **Decision Point**: Choose the appropriate containment strategy.
  - **Isolate Affected Systems**: Disconnect compromised systems from the network to halt further damage.
  - **Partial Containment**: Apply temporary fixes or restrictions to limit the impact while keeping systems operational.

Stage 4: Eradication

- **Action**: Identify and eliminate the root cause of the incident (e.g., remove malware, close vulnerabilities).
- **Decision Point**: Determine the scope of eradication efforts.
  - **Full Eradication**: Conduct thorough scans and cleanup across all affected systems.
  - **Targeted Eradication**: Focus only on systems confirmed to be compromised.

Stage 5: Recovery

- **Action**: Restore and validate systems to return to normal operations.
- **Decision Point**: Decide on the recovery approach.

    - **Restore from Backups**: Use clean backups to recover affected systems if significant damage occurred.
    - **System Repair**: Apply patches, update configurations, or reinstall software to restore functionality.

Stage 6: Post-Incident Review

- **Action**: Conduct a comprehensive review of the incident and the response actions taken.
- **Decision Point**: Determine whether to update policies and procedures based on lessons learned.
    - **Update Playbook**: Incorporate new insights and improve the incident response process.
    - **No Changes Needed**: If the existing procedures were effective, document the incident and maintain current practices.

EXAMPLES AND SIMULATIONS

Scenario 1: Ransomware Outbreak

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the SIEM indicating unusual file encryption activity on multiple workstations within the network. The files on these workstations are being rapidly renamed with a ".locked" extension, and employees report that their files are inaccessible.

Question: Is this activity consistent with ransomware behaviour?

- **Options:**
  - **Yes:** The rapid encryption and ".locked" extension suggest a ransomware attack.
  - **No:** It might be a legitimate software update or a misconfigured backup process.

If "Yes" is selected:

Question: Should the SOC escalate this to a critical incident immediately?

- **Options:**
  - **Yes:** The scope and nature of the activity warrant immediate escalation to prevent further damage.
  - **No:** Continue monitoring to gather more information before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins to assess the scope of the outbreak.

Question: Should the affected systems be isolated from the network immediately?

- **Options:**
  - **Yes:** Isolating the systems can prevent the ransomware from spreading further across the network.
  - **No:** Isolation might disrupt critical business operations; proceed with caution.

If "Yes" is selected:

Question: Should all potentially affected endpoints be scanned for signs of encryption and the presence of the ransomware executable?

- **Options:**
  - **Yes:** Conducting a full scan can help identify all compromised machines and the ransomware variant.
  - **No:** Focus on the machines already showing symptoms to avoid overloading resources.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team isolates the affected systems and begins scanning all endpoints for encryption activity and ransomware executables.

Question: Should we disable file-sharing services and network drives to prevent further encryption?

- **Options:**
  - **Yes:** Disabling these services can stop the ransomware from spreading to shared resources.
  - **No:** Disabling these services might disrupt critical workflows; assess the impact first.

If "Yes" is selected:

Question: Should we communicate the incident to all employees and instruct them to disconnect from the network immediately?

- **Options:**
  - **Yes:** Early communication can help prevent more devices from getting infected.
  - **No:** Hold off until we have more information to avoid causing unnecessary panic.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team disables file-sharing services, network drives, and communicates with employees to disconnect from the network.

Question: Should we attempt to identify the ransomware variant using the IOCs (Indicators of Compromise) from the encrypted files and executables?

- **Options:**
  - **Yes:** Identifying the ransomware variant can help determine the best course of action for removal and recovery.
  - **No:** Focus on containment and eradication first, then identify the variant later.

If "Yes" is selected:

Question: Should we attempt to remove the ransomware from infected systems, or should we prepare to restore from backups?

- **Options:**
    - **Remove the ransomware:** Attempting to remove the ransomware might recover some systems without needing a full restore.
    - **Restore from backups:** If the ransomware has deeply compromised systems, restoring from backups might be faster and more reliable.

If "Restore from backups" is selected:

Stage 5: Recovery

- **Action:** The IR team prepares to restore affected systems from the latest clean backups. They also conduct a thorough review to ensure no ransomware traces remain.

Question: Should we verify the integrity of the backups before restoring them?

- **Options:**
    - **Yes:** Verifying backups ensures they are clean and free from any ransomware infection.
    - **No:** Restore immediately to minimise downtime.

If "Yes" is selected:

Question: Should we prioritise the restoration of critical systems and services first?

- **Options:**
    - **Yes:** Critical systems should be restored first to minimise the impact on business operations.
    - **No:** Restore systems in the order they were compromised.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team verifies the integrity of backups, restores critical systems first, and then completes the restoration of all affected systems.

Question: Should we conduct a full post-incident review to understand how the ransomware breached the network?

- **Options:**
    - **Yes:** A thorough review can uncover vulnerabilities and gaps in security controls.

    - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

Question: Should we update the incident response playbook based on the findings?

- **Options:**
    - **Yes:** Updating the playbook ensures that the response to future incidents is more effective.
    - **No:** The current playbook is sufficient; no changes are necessary.

Scenario 2: Data Exfiltration Attempt

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the DLP (Data Loss Prevention) system indicating unusual large data transfers from a critical database server to an external IP address. The transfer volume is abnormally high, and the data includes sensitive customer information.
- **Question:** Is this activity consistent with a potential data exfiltration attempt?
    - **Options:**
        - **Yes:** The large transfer of sensitive data to an external IP address suggests a data exfiltration attempt.
        - **No:** It might be a legitimate data transfer, such as a backup or scheduled data replication.

If "Yes" is selected:

- **Question:** Should the SOC escalate this to a critical incident immediately?
    - **Options:**
        - **Yes:** The potential data exfiltration of sensitive customer information warrants immediate escalation to mitigate the risk of data loss.
        - **No:** Continue monitoring to confirm if this activity is malicious before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins assessing the scope of the data transfer.
- **Question:** Should the suspicious data transfer be immediately blocked or throttled to prevent further exfiltration?
    - **Options:**
        - **Yes:** Blocking or throttling the transfer can immediately prevent further data from being exfiltrated.
        - **No:** Blocking the transfer might alert the attacker; continue monitoring stealthily.

If "Yes" is selected:

- **Question:** Should we perform an immediate investigation to identify the source of the transfer and how the data was accessed?
    - **Options:**
        - **Yes:** Investigating the source of the transfer can help identify compromised accounts or systems.
        - **No:** Focus on blocking the transfer first, and investigate the source later.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team blocks the suspicious transfer and begins an investigation into the source and scope of the data exfiltration.
- **Question:** Should we isolate the compromised database server to prevent further unauthorised access?
  - **Options:**
    - **Yes:** Isolating the server can prevent the attacker from accessing more data.
    - **No:** Isolation might disrupt critical business operations; proceed with caution.

If "Yes" is selected:

- **Question:** Should we review and reset credentials for all accounts with access to the compromised database?
  - **Options:**
    - **Yes:** Resetting credentials can prevent further unauthorised access using compromised accounts.
    - **No:** Hold off on resetting credentials until the full scope of the breach is understood.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team isolates the compromised server and resets credentials for all accounts with access to the database.
- **Question:** Should we perform a thorough review of all data access logs to identify other suspicious activities?
  - **Options:**
    - **Yes:** Reviewing access logs can help identify if other data has been accessed or exfiltrated.
    - **No:** Focus on containing the current incident before reviewing other logs.

If "Yes" is selected:

- **Question:** Should we begin restoring any potentially corrupted or altered data from backups?
  - **Options:**
    - **Yes:** Restoring from backups can ensure data integrity and prevent further issues.
    - **No:** Wait until the investigation is complete to ensure that the backup restoration is necessary.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team reviews access logs and begins restoring corrupted or altered data from clean backups.
- **Question:** Should we verify the integrity of the restored data before allowing it back into production?
  - **Options:**
    - **Yes:** Verifying the data ensures that it is clean and accurate before being used in operations.
    - **No:** Restore the data immediately to minimise downtime.

If "Yes" is selected:

- **Question:** Should we prioritise the restoration of data critical to customer operations?
  - **Options:**
    - **Yes:** Prioritising customer-critical data ensures that business operations can resume quickly.
    - **No:** Restore data in the order it was compromised.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team verifies the integrity of the restored data, prioritises customer-critical data, and completes the restoration process.
- **Question:** Should we conduct a full post-incident review to determine how the attacker gained access to the database?
  - **Options:**
    - **Yes:** A full review can identify vulnerabilities and security gaps.
    - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook to include lessons learned from this incident?
  - **Options:**
    - **Yes:** Updating the playbook ensures better preparedness for future incidents.
    - **No:** The current playbook is sufficient; no changes are necessary

Scenario 3: Insider Threat - Unauthorised Access to Sensitive Data

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the SIEM indicating unusual access patterns to a highly sensitive HR database containing employee personal and financial information. The access is being made from an internal user account outside of normal business hours, with multiple large queries being executed.
- **Question:** Is this activity consistent with potential insider threat behaviour?
    - **Options:**
        - **Yes:** Unusual access to sensitive data outside of normal hours suggests a potential insider threat.
        - **No:** It could be a legitimate access for maintenance or reporting purposes.

If "Yes" is selected:

- **Question:** Should the SOC escalate this to a critical incident immediately?
    - **Options:**
        - **Yes:** The potential unauthorised access to sensitive data warrants immediate escalation to prevent data leakage.
        - **No:** Continue monitoring to confirm the legitimacy of the access before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins investigating the unauthorised access.
- **Question:** Should the user account be temporarily disabled to prevent further access to sensitive data?
    - **Options:**
        - **Yes:** Disabling the account can stop any further unauthorised access.
        - **No:** Disabling the account might alert the insider; continue monitoring discreetly.

If "Yes" is selected:

- **Question:** Should we review the user's recent activity and access logs to determine the extent of the unauthorised access?
    - **Options:**
        - **Yes:** Reviewing logs can help determine what data has been accessed and if any has been exfiltrated.
        - **No:** Focus on containing the current incident before reviewing past activities.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team disables the user account and begins reviewing recent activity and access logs.
- **Question:** Should we immediately alert the HR and legal teams about the potential insider threat?
    - **Options:**
        - **Yes:** Alerting HR and legal ensures that appropriate actions are taken in line with company policy and legal requirements.
        - **No:** Hold off until the investigation confirms the insider threat to avoid false accusations.

If "Yes" is selected:

- **Question:** Should we restrict access to the sensitive HR database temporarily until the investigation is complete?
    - **Options:**
        - **Yes:** Restricting access can prevent any further unauthorised data access.
        - **No:** Restricting access might disrupt legitimate business operations; proceed with caution.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team restricts access to the HR database and alerts HR and legal teams.
- **Question:** Should we conduct interviews with the employee in question to understand the reason for the access?
    - **Options:**
        - **Yes:** Conducting interviews can provide insight into whether the access was intentional or accidental.
        - **No:** Focus on gathering evidence and understanding the full scope before engaging with the employee.

If "Yes" is selected:

- **Question:** Should we implement stricter access controls and monitoring for sensitive databases going forward?
    - **Options:**
        - **Yes:** Implementing stricter controls can help prevent similar incidents in the future.
        - **No:** The current access controls are sufficient; no changes are necessary.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team conducts interviews with the employee and begins implementing stricter access controls.
- **Question:** Should we restore normal access to the HR database once the investigation is complete?
  - **Options:**
    - **Yes:** Restoring normal access ensures that business operations can continue smoothly.
    - **No:** Keep access restricted until all potential risks are fully mitigated.

If "Yes" is selected:

- **Question:** Should we review other user accounts for any similar unauthorised access patterns?
  - **Options:**
    - **Yes:** Reviewing other accounts can help identify if the insider threat extends beyond one individual.
    - **No:** Focus on resolving the current incident before expanding the investigation.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team restores normal access to the HR database, reviews other user accounts, and completes the investigation.
- **Question:** Should we conduct a full post-incident review to understand how the insider was able to gain unauthorised access?
  - **Options:**
    - **Yes:** A thorough review can help identify gaps in access controls and security practices.
    - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook based on the findings?
  - **Options:**
    - **Yes:** Updating the playbook ensures that the response to future insider threats is more effective.
    - **No:** The current playbook is sufficient; no changes are necessary.

Scenario 4: Distributed Denial of Service (DDoS) Attack

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from network monitoring tools indicating a sudden spike in incoming traffic to the company's public-facing web servers. The traffic volume is significantly higher than normal and is causing slowdowns and accessibility issues for legitimate users.
- **Question:** Is this activity consistent with a potential DDoS attack?
    - **Options:**
        - **Yes:** The sudden surge in traffic, leading to server slowdowns, suggests a potential DDoS attack.
        - **No:** It might be a legitimate traffic increase due to a marketing campaign or other planned activity.

If "Yes" is selected:

- **Question:** Should the SOC escalate this to a critical incident immediately?
    - **Options:**
        - **Yes:** The impact on service availability warrants immediate escalation to prevent further disruption.
        - **No:** Continue monitoring to confirm if the traffic spike is malicious before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins assessing the scope and impact of the traffic spike.
- **Question:** Should traffic to the affected servers be rerouted through a DDoS mitigation service immediately?
    - **Options:**
        - **Yes:** Rerouting traffic through a mitigation service can filter out malicious traffic and restore service availability.
        - **No:** Assess the traffic patterns first to ensure rerouting is necessary and effective.

If "Yes" is selected:

- **Question:** Should we identify the source IP addresses of the traffic and block them at the firewall level?
    - **Options:**
        - **Yes:** Blocking the source IPs can immediately reduce the load on the servers and mitigate the attack.
        - **No:** Hold off on blocking until a more comprehensive analysis of the traffic is conducted.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team reroutes traffic through a DDoS mitigation service and begins blocking malicious IP addresses.
- **Question:** Should we implement rate limiting on the affected servers to reduce the impact of the attack?
  - **Options:**
    - **Yes:** Rate limiting can prevent individual IPs from overwhelming the servers with requests.
    - **No:** Rate limiting might impact legitimate users; assess the impact before implementing.

If "Yes" is selected:

- **Question:** Should we activate additional servers or use a content delivery network (CDN) to handle the increased traffic?
  - **Options:**
    - **Yes:** Activating additional servers or using a CDN can distribute the load and maintain service availability.
    - **No:** Focus on mitigating the attack first before expanding server resources.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team implements rate limiting, activates additional servers, and uses a CDN to handle the traffic.
- **Question:** Should we monitor the network for any secondary attacks or unusual activity following the DDoS attempt?
  - **Options:**
    - **Yes:** Monitoring for secondary attacks ensures that any follow-up attempts are detected early.
    - **No:** Focus on stabilising the current situation before monitoring for further attacks.

If "Yes" is selected:

- **Question:** Should we engage with the ISP or upstream providers to block malicious traffic at a higher level?
  - **Options:**
    - **Yes:** Engaging with ISPs can help block malicious traffic before it reaches the company’s network.
    - **No:** Handle the traffic internally to avoid involving external parties unless absolutely necessary.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team monitors the network for secondary attacks and engages with ISPs to block further malicious traffic.
- **Question:** Should we review the performance and effectiveness of the DDoS mitigation strategies used during the attack?
  - **Options:**
    - **Yes:** Reviewing the mitigation strategies ensures they were effective and identifies areas for improvement.
    - **No:** Resume normal operations immediately to minimise downtime.

If "Yes" is selected:

- **Question:** Should we restore any affected services that were taken offline or throttled during the attack?
  - **Options:**
    - **Yes:** Restoring services ensures that all operations return to normal.
    - **No:** Keep services restricted until there's absolute certainty that the attack is fully mitigated.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team reviews the DDoS mitigation strategies and restores affected services.
- **Question:** Should we conduct a full post-incident review to understand the origin and motivation behind the DDoS attack?
  - **Options:**
    - **Yes:** A thorough review can help uncover potential threat actors and improve future defences.
    - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook to include lessons learned from this DDoS attack?
  - **Options:**
    - **Yes:** Updating the playbook ensures better preparedness and response to future DDoS attacks.
    - **No:** The current playbook is sufficient; no changes are necessary.

Scenario 5: Phishing Attack Leading to Credential Compromise

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the email security gateway indicating that multiple employees have received emails containing links to a suspicious login page that mimics the company's internal portal. Shortly after, there are login attempts from unusual geographic locations using employee credentials.
- **Question:** Is this activity consistent with a phishing attack?
  - **Options:**
    - **Yes:** The presence of a fake login page and unusual login attempts suggests a phishing attack.
    - **No:** It might be a legitimate third-party login page or an unusual but legitimate login attempt.

If "Yes" is selected:

- **Question:** Should the SOC escalate this to a critical incident immediately?
  - **Options:**
    - **Yes:** The potential compromise of employee credentials warrants immediate escalation to prevent unauthorised access.
    - **No:** Continue monitoring to gather more information before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins investigating the extent of the credential compromise.
- **Question:** Should the affected user accounts be temporarily disabled to prevent unauthorised access?
  - **Options:**
    - **Yes:** Disabling the accounts can prevent the attacker from using the compromised credentials.
    - **No:** Disabling accounts might disrupt business operations; proceed with caution.

If "Yes" is selected:

- **Question:** Should we instruct all employees to change their passwords immediately as a precaution?
  - **Options:**
    - **Yes:** Instructing a password change can mitigate the risk of further unauthorised access.
    - **No:** Focus on identifying the compromised accounts first before instructing a widespread password change.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team disables affected accounts and instructs all employees to change their passwords.
- **Question:** Should we implement multi-factor authentication (MFA) immediately for all accounts to enhance security?
  - **Options:**
    - **Yes:** Implementing MFA can prevent unauthorised access even if credentials are compromised.
    - **No:** Assess the current situation before making significant changes to authentication processes.

If "Yes" is selected:

- **Question:** Should we block access from the unusual geographic locations where the unauthorised login attempts originated?
  - **Options:**
    - **Yes:** Blocking these locations can prevent further unauthorised access attempts.
    - **No:** Monitor the situation before implementing geo-blocking, as it might affect legitimate users.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team implements MFA, blocks access from suspicious locations, and continues monitoring the network.
- **Question:** Should we scan all company systems for signs of further compromise or malware related to the phishing attack?
  - **Options:**
    - **Yes:** Scanning can help identify if any systems were compromised as part of the phishing attack.
    - **No:** Focus on the compromised accounts first before scanning all systems.

If "Yes" is selected:

- **Question:** Should we communicate the incident to all employees, informing them of the phishing attack and the steps being taken?
  - **Options:**
    - **Yes:** Early communication can help prevent more users from falling victim to the phishing attack.
    - **No:** Hold off on communication until the full scope of the attack is understood to avoid unnecessary panic.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team scans all systems and communicates with employees about the phishing attack.
- **Question:** Should we review and update the email security policies to prevent future phishing attacks?
  - **Options:**
    - **Yes:** Updating policies can enhance the organisation's defence against phishing.
    - **No:** Focus on resolving the current incident before revisiting security policies.

If "Yes" is selected:

- **Question:** Should we restore normal access to the affected user accounts after confirming they are secure?
  - **Options:**
    - **Yes:** Restoring access ensures that employees can resume their work without disruption.
    - **No:** Keep the accounts disabled until there's absolute certainty that they are secure.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team reviews and updates email security policies and restores normal access to user accounts.
- **Question:** Should we conduct a full post-incident review to understand how the phishing attack bypassed the email security gateway?
  - **Options:**
    - **Yes:** A thorough review can help identify weaknesses in the current email security setup.
    - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

- **Question:** Should we provide additional phishing awareness training to all employees based on the findings?
  - **Options:**
    - **Yes:** Additional training can help employees recognise and avoid future phishing attempts.
    - **No:** The current training program is sufficient; no changes are necessary.

Scenario 6: Advanced Persistent Threat (APT) - Lateral Movement Detected

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the EDR (Endpoint Detection and Response) system indicating unusual PowerShell activity on a critical server. The PowerShell script executed is attempting to access and extract password hashes from the server's memory. Shortly afterward, the SOC notices unusual RDP (Remote Desktop Protocol) login attempts from this server to other sensitive systems within the network.
- **Question:** Is this activity consistent with a potential Advanced Persistent Threat (APT)?
  - **Options:**
    - **Yes:** The use of PowerShell to extract credentials and the subsequent lateral movement suggest a potential APT.
    - **No:** It might be a legitimate administrative activity or an isolated incident.

If "Yes" is selected:

- **Question:** Should the SOC escalate this to a critical incident immediately?
  - **Options:**
    - **Yes:** The combination of credential theft and lateral movement indicates a sophisticated attack, warranting immediate escalation.
    - **No:** Continue monitoring to gather more information before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins investigating the scope of the potential APT.
- **Question:** Should the compromised server be isolated from the network immediately to prevent further lateral movement?
  - **Options:**
    - **Yes:** Isolating the server can prevent the attacker from moving to other systems and stop the exfiltration of data.
    - **No:** Isolation might disrupt critical business operations; proceed with caution.

If "Yes" is selected:

- **Question:** Should we perform a thorough forensic analysis on the compromised server to identify how the attacker gained access?
  - **Options:**

        - **Yes:** A forensic analysis can provide insights into the attack vector and help identify other potentially compromised systems.
        - **No:** Focus on containing the incident first before conducting a forensic analysis.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team isolates the compromised server and begins forensic analysis.
- **Question:** Should we proactively reset all privileged account passwords across the network to prevent the attacker from using stolen credentials?
    - **Options:**
        - **Yes:** Resetting passwords can stop the attacker from leveraging stolen credentials to escalate their privileges or move laterally.
        - **No:** Focus on identifying the full scope of the breach first before taking such a broad action.

If "Yes" is selected:

- **Question:** Should we implement additional network segmentation to limit the attacker's ability to move laterally across the network?
    - **Options:**
        - **Yes:** Network segmentation can slow down or prevent further lateral movement by the attacker.
        - **No:** Focus on monitoring and containment before making significant network changes.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team resets privileged account passwords and implements additional network segmentation.
- **Question:** Should we deploy a threat-hunting team to actively search for other signs of compromise across the network?
    - **Options:**
        - **Yes:** Threat hunting can help identify other compromised systems and prevent further escalation.
        - **No:** Focus on the current known breach points before expanding the scope of the investigation.

If "Yes" is selected:

- **Question:** Should we analyse network traffic logs to identify communication with any Command and Control (C2) servers?
    - **Options:**

        - **Yes:** Analysing traffic can help identify and block communication with the attacker's C2 servers.
        - **No:** Focus on containing the incident locally before diving into network traffic analysis.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team deploys a threat-hunting team and analyses network traffic logs.
- **Question:** Should we consider re-imaging compromised systems to ensure they are clean before returning them to operation?
    - **Options:**
        - **Yes:** Re-imaging can ensure that any backdoors or persistent threats are removed.
        - **No:** Attempt to clean the systems without re-imaging to minimise downtime.

If "Yes" is selected:

- **Question:** Should we prioritise the restoration and re-imaging of critical systems before moving on to less critical ones?
    - **Options:**
        - **Yes:** Restoring critical systems first can minimise the impact on business operations.
        - **No:** Follow a standard restoration process without prioritising systems.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team re-images compromised systems and restores critical systems first.
- **Question:** Should we conduct a full post-incident review to understand the APT's tactics, techniques, and procedures (TTPs) used?
    - **Options:**
        - **Yes:** A thorough review can help improve defences and prevent future attacks using similar methods.
        - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook and security controls based on the lessons learned from this incident?
    - **Options:**

- **Yes:** Updating the playbook and controls can enhance the effectiveness of responses to future APTs.
- **No:** The current playbook and controls are sufficient; no changes are necessary.

Scenario 7: Brute-Force Attack - Unauthorised Access Attempt Detected

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the SIEM system indicating multiple failed login attempts on a critical application server within a short period. The login attempts originate from an external IP address and seem to be targeting administrative accounts.
- **Question:** Is this activity consistent with a potential brute-force attack?
  - **Options:**
    - **Yes:** The high number of failed login attempts targeting admin accounts suggests a potential brute-force attack.
    - **No:** It might be a legitimate user who has forgotten their password or a misconfigured system.

If "Yes" is selected:

- **Question:** Should the SOC initiate an immediate investigation to identify the source and potential impact?
  - **Options:**
    - **Yes:** Immediate investigation can help prevent unauthorised access if the brute-force attack succeeds.
    - **No:** Continue monitoring the situation to gather more data before taking action.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins investigating the source of the brute-force attack.
- **Question:** Should the SOC block the IP address from which the brute-force attempts are originating to prevent further access attempts?
  - **Options:**
    - **Yes:** Blocking the IP address can stop the brute-force attack and protect the system.
    - **No:** Blocking the IP might disrupt legitimate traffic; proceed with caution.

If "Yes" is selected:

- **Question:** Should we perform a detailed analysis of the logs to determine if any accounts were compromised during the attack?
  - **Options:**
    - **Yes:** Analysing the logs can help identify any successful login attempts and prevent further damage.
    - **No:** Focus on containing the attack first before conducting a detailed log analysis.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team blocks the suspicious IP address and begins analysing the logs for any signs of compromised accounts.
- **Question:** Should we enforce a mandatory password reset for all administrative accounts on the affected server?
  - **Options:**
    - **Yes:** Resetting passwords can prevent unauthorised access if any credentials were compromised.
    - **No:** Focus on monitoring the situation before enforcing a password reset.

If "Yes" is selected:

- **Question:** Should we implement multi-factor authentication (MFA) for all administrative accounts to enhance security?
  - **Options:**
    - **Yes:** Implementing MFA can significantly reduce the risk of unauthorised access even if credentials are compromised.
    - **No:** Consider other containment measures before making changes to authentication methods.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team enforces a mandatory password reset for all administrative accounts and implements MFA.
- **Question:** Should we review and strengthen the password policies across the organisation to prevent future brute-force attacks?
  - **Options:**
    - **Yes:** Strengthening password policies can reduce the likelihood of successful brute-force attacks.
    - **No:** Focus on the current incident before making organisation-wide policy changes.

If "Yes" is selected:

- **Question:** Should we update the firewall rules to automatically block IPs after a certain number of failed login attempts?
  - **Options:**
    - **Yes:** Updating firewall rules can help prevent brute-force attacks by blocking suspicious IPs in real-time.
    - **No:** Continue monitoring the situation before making changes to firewall rules.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team updates the firewall rules and reviews the password policies.
- **Question:** Should we monitor the affected server closely for any signs of further unauthorised access attempts?
    - **Options:**
        - **Yes:** Close monitoring can help detect any residual threats or further attempts to breach the server.
        - **No:** The containment measures are sufficient; resume normal operations.

If "Yes" is selected:

- **Question:** Should we consider running a full security audit on the server to ensure no other vulnerabilities exist?
    - **Options:**
        - **Yes:** A full audit can help identify and mitigate any remaining vulnerabilities.
        - **No:** Focus on addressing the specific incident rather than conducting a full audit.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team runs a full security audit and monitors the server closely for further threats.
- **Question:** Should we conduct a post-incident review to understand the attack methods and improve future defences?
    - **Options:**
        - **Yes:** A thorough review can help enhance defences and prevent similar attacks in the future.
        - **No:** Focus on resuming normal operations and conduct the review later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook and security controls based on the lessons learned from this incident?
    - **Options:**
        - **Yes:** Updating the playbook and controls can enhance the effectiveness of responses to future brute-force attacks.
        - **No:** The current playbook and controls are sufficient; no changes are necessary.

Scenario 8: DNS Tunneling Attack - Covert Communication Detected

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the Intrusion Detection System (IDS) indicating unusual DNS query patterns originating from a critical server. These queries are longer than typical DNS requests and occur at regular intervals, suggesting potential data exfiltration via DNS tunneling.
- **Question:** Is this activity consistent with a DNS tunneling attack?
  - **Options:**
    - **Yes:** The unusual DNS traffic patterns and regular intervals suggest potential DNS tunneling.
    - **No:** It might be an anomaly in DNS traffic that requires further investigation.

If "Yes" is selected:

- **Question:** Should the SOC escalate this incident for further investigation?
  - **Options:**
    - **Yes:** Escalating the incident can help quickly determine if sensitive data is being exfiltrated.
    - **No:** Continue monitoring the DNS traffic to gather more information before escalating.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins investigating the unusual DNS traffic.
- **Question:** Should the suspicious DNS traffic be blocked immediately to prevent potential data exfiltration?
  - **Options:**
    - **Yes:** Blocking the traffic can stop the exfiltration of sensitive data through DNS tunneling.
    - **No:** Blocking the traffic might disrupt legitimate DNS queries; proceed with caution.

If "Yes" is selected:

- **Question:** Should we perform a deeper analysis of the DNS logs to identify the domains involved in the suspected tunneling activity?
  - **Options:**
    - **Yes:** Analysing the DNS logs can help identify the specific domains being used for the tunneling activity.
    - **No:** Focus on containment before diving into detailed DNS log analysis.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team blocks the suspicious DNS traffic and begins analysing the DNS logs.
- **Question:** Should we isolate the affected server from the network to prevent further tunneling activity?
  - **Options:**
    - **Yes:** Isolating the server can prevent the attacker from continuing the tunneling activity.
    - **No:** Isolation might disrupt critical business functions; proceed with caution.

If "Yes" is selected:

- **Question:** Should we reset the DNS settings on the affected server to ensure that no unauthorised configurations remain?
  - **Options:**
    - **Yes:** Resetting the DNS settings can remove any malicious configurations that facilitated the tunneling.
    - **No:** Focus on analysing the server before making configuration changes.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team resets the DNS settings and continues analysing the server for any additional indicators of compromise.
- **Question:** Should we update the firewall and DNS filtering rules to block similar suspicious traffic in the future?
  - **Options:**
    - **Yes:** Updating the firewall and filtering rules can help prevent future DNS tunneling attempts.
    - **No:** Focus on remediating the current incident before making broader changes.

If "Yes" is selected:

- **Question:** Should we conduct a full network sweep to identify any other servers that might be compromised?
  - **Options:**
    - **Yes:** A full network sweep can help identify other potentially compromised systems.
    - **No:** Focus on the known affected server before expanding the scope of the investigation.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team updates the firewall and DNS filtering rules and conducts a network sweep for additional compromised systems.
- **Question:** Should we monitor DNS traffic more closely in the future to detect similar attacks early?
  - **Options:**
    - **Yes:** Close monitoring can help detect and respond to DNS tunneling attacks more quickly.
    - **No:** The current monitoring system is sufficient; no additional monitoring is necessary.

If "Yes" is selected:

- **Question:** Should we re-image the compromised server to ensure that no backdoors or malicious code remain?
  - **Options:**
    - **Yes:** Re-imaging can ensure that the server is clean before returning it to operation.
    - **No:** Attempt to clean the server without re-imaging to minimise downtime.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team re-images the compromised server and monitors DNS traffic more closely.
- **Question:** Should we conduct a post-incident review to understand how the DNS tunneling attack was carried out?
  - **Options:**
    - **Yes:** A thorough review can help improve defences and prevent similar attacks in the future.
    - **No:** Focus on resuming normal operations and conduct the review later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook and security controls based on the lessons learned from this incident?
  - **Options:**
    - **Yes:** Updating the playbook and controls can enhance the effectiveness of responses to future DNS tunneling attacks.
    - **No:** The current playbook and controls are sufficient; no changes are necessary.

Scenario 9: Credential Dumping - Suspicious LSASS Access Detected

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the EDR (Endpoint Detection and Response) system indicating suspicious access to the LSASS (Local Security Authority Subsystem Service) process on a critical server. The process accessing LSASS is attempting to dump memory, which could be an attempt to extract credentials.
  - **MITRE ATT&CK Technique:** T1003.001 - OS Credential Dumping: LSASS Memory
- **Question:** Is this activity consistent with credential dumping?
  - **Options:**
    - **Yes:** The attempt to access LSASS memory is a common method for credential dumping.
    - **No:** It could be legitimate software or a misconfiguration.

If "Yes" is selected:

- **Question:** Should the SOC escalate this incident as a critical security event?
  - **Options:**
    - **Yes:** Credential dumping is a serious threat that can lead to further compromise.
    - **No:** Continue monitoring to confirm if it is truly malicious activity.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC escalates the incident, and the Incident Response (IR) team begins investigating the suspicious process accessing LSASS.
- **Question:** Should the process be terminated immediately to prevent further credential dumping?
  - **Options:**
    - **Yes:** Terminating the process can stop the attacker from accessing and dumping credentials.
    - **No:** Terminating the process might disrupt legitimate activity; proceed with caution.

If "Yes" is selected:

- **Question:** Should we collect a memory dump from the compromised server for forensic analysis?
  - **Options:**
    - **Yes:** A memory dump can provide valuable information about the attack vector and any extracted credentials.
    - **No:** Focus on containing the incident first before conducting forensic analysis.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team terminates the suspicious process and collects a memory dump for analysis.
- **Question:** Should we reset all potentially compromised accounts to prevent further unauthorised access?
  - **Options:**
    - **Yes:** Resetting passwords can mitigate the risk of attackers using dumped credentials.
    - **No:** Focus on identifying the scope of the compromise before taking broad action.

If "Yes" is selected:

- **Question:** Should we deploy additional monitoring to detect any further attempts at credential dumping or lateral movement?
  - **Options:**
    - **Yes:** Enhanced monitoring can help detect and respond to any follow-up actions by the attacker.
    - **No:** Current monitoring is sufficient; no further actions are necessary.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team resets potentially compromised accounts and deploys additional monitoring.
- **Question:** Should we hunt for other indicators of compromise (IOCs) across the network to identify additional compromised systems?
  - **Options:**
    - **Yes:** Threat hunting can help identify other systems that may have been affected by the attacker.
    - **No:** Focus on the known affected server before expanding the scope of the investigation.

If "Yes" is selected:

- **Question:** Should we implement additional access controls to prevent similar attacks in the future?
  - **Options:**
    - **Yes:** Strengthening access controls can reduce the likelihood of successful credential dumping.
    - **No:** Current controls are sufficient; no additional measures are necessary.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team conducts a network-wide hunt for IOCs and implements additional access controls.
- **Question:** Should we re-image the compromised server to ensure it is free of any backdoors or persistent threats?
    - **Options:**
        - **Yes:** Re-imaging the server can eliminate any remaining malware or unauthorised changes.
        - **No:** Attempt to clean the server without re-imaging to minimise downtime.

If "Yes" is selected:

- **Question:** Should we prioritise re-imaging and restoring critical systems before moving on to less critical ones?
    - **Options:**
        - **Yes:** Prioritising critical systems can minimise the impact on business operations.
        - **No:** Follow a standard restoration process without prioritising specific systems.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team re-images the compromised server and restores critical systems first.
- **Question:** Should we conduct a post-incident review to analyse the attack and the effectiveness of our response?
    - **Options:**
        - **Yes:** A thorough review can provide insights to improve defences and incident response processes.
        - **No:** Focus on resuming normal operations and review the incident later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook and security controls based on the lessons learned from this incident?
    - **Options:**
        - **Yes:** Updating the playbook and controls can enhance future responses to credential dumping attacks.
        - **No:** The current playbook and controls are sufficient; no changes are necessary.

Scenario 10: Command and Control (C2) - Suspicious Network Traffic Detected

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the IDS/IPS (Intrusion Detection System/Intrusion Prevention System) indicating suspicious outbound network traffic from a non-standard port to an external IP address. The traffic pattern suggests a potential communication with a Command and Control (C2) server.
  - **MITRE ATT&CK Technique:** T1071 - Application Layer Protocol: Non-Standard Port
- **Question:** Is this traffic indicative of potential C2 communication?
  - **Options:**
    - **Yes:** The use of non-standard ports and external IPs is common in C2 communications.
    - **No:** It could be legitimate traffic that warrants further investigation.

If "Yes" is selected:

- **Question:** Should the SOC block the outbound connection to prevent further communication with the potential C2 server?
  - **Options:**
    - **Yes:** Blocking the connection can prevent the attacker from maintaining control over the compromised system.
    - **No:** Continue monitoring to gather more information before blocking the traffic.

If "Yes" is selected:

Stage 2: Incident Identification and Scope

- **Action:** The SOC blocks the suspicious outbound connection and alerts the Incident Response (IR) team to investigate.
- **Question:** Should the compromised system be isolated from the network to prevent further malicious activity?
  - **Options:**
    - **Yes:** Isolating the system can prevent the attacker from issuing further commands or exfiltrating data.
    - **No:** Isolation might disrupt legitimate operations; proceed with caution.

If "Yes" is selected:

- **Question:** Should we perform a deep packet inspection (DPI) on the captured traffic to understand the nature of the communication?
  - **Options:**
    - **Yes:** DPI can reveal if the traffic contains malicious commands or data exfiltration attempts.

        - **No:** Focus on containing the incident first before analysing traffic in-depth.

If "Yes" is selected:

Stage 3: Containment Strategy

- **Action:** The IR team isolates the compromised system and performs deep packet inspection on the suspicious traffic.
- **Question:** Should we search for other compromised systems within the network that may also be communicating with the C2 server?
    - **Options:**
        - **Yes:** Identifying all systems in communication with the C2 server can help in containing the attack.
        - **No:** Focus on the known compromised system before expanding the scope.

If "Yes" is selected:

- **Question:** Should we implement additional network monitoring to detect any further C2 communication attempts?
    - **Options:**
        - **Yes:** Enhanced monitoring can detect any new C2 connections and prevent further compromise.
        - **No:** Current monitoring is sufficient; no further actions are necessary.

If "Yes" is selected:

Stage 4: Eradication and Remediation

- **Action:** The IR team searches for other compromised systems and implements additional network monitoring.
- **Question:** Should we terminate any identified malicious processes on compromised systems to disrupt the attacker's control?
    - **Options:**
        - **Yes:** Terminating malicious processes can stop the attacker's activities on the compromised systems.
        - **No:** Focus on identifying the full scope of the breach before taking action.

If "Yes" is selected:

- **Question:** Should we change the external IP block policy to prevent further communication with known C2 servers?
    - **Options:**
        - **Yes:** Blocking known C2 server IPs can prevent further connections from being established.

        - **No:** Focus on addressing the current incident before implementing broader changes.

If "Yes" is selected:

Stage 5: Recovery

- **Action:** The IR team terminates malicious processes and updates the external IP block policy.
- **Question:** Should we re-image compromised systems to ensure they are free of any backdoors or persistent threats before returning them to operation?
    - **Options:**
        - **Yes:** Re-imaging can ensure the removal of any remaining malware or unauthorised changes.
        - **No:** Attempt to clean the systems without re-imaging to minimise downtime.

If "Yes" is selected:

- **Question:** Should we prioritise the re-imaging and restoration of systems that were most critical to the business first?
    - **Options:**
        - **Yes:** Prioritising critical systems can minimise operational impact.
        - **No:** Follow a standard restoration process without prioritising specific systems.

If "Yes" is selected:

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team re-images compromised systems and restores critical systems first.
- **Question:** Should we conduct a post-incident review to analyse the tactics, techniques, and procedures (TTPs) used by the attacker?
    - **Options:**
        - **Yes:** A thorough review can provide insights to improve defences and incident response processes.
        - **No:** Focus on resuming normal operations, and review the incident later.

If "Yes" is selected:

- **Question:** Should we update the incident response playbook and security controls based on the lessons learned from this incident?
    - **Options:**
        - **Yes:** Updating the playbook and controls can enhance future responses to similar attacks.

- **No:** The current playbook and controls are sufficient; no changes are necessary.

Simulation 1: Data Exfiltration via DNS Tunneling

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the DNS monitoring system indicating a high volume of DNS requests from a specific workstation to an external domain. The DNS queries contain encoded data, which suggests potential DNS tunneling for data exfiltration.
  - **MITRE ATT&CK Technique:** T1071.004 - Application Layer Protocol: DNS

Step 1: Is This Traffic Indicative of Potential Data Exfiltration via DNS Tunneling?

- **Options:**
  - **Yes:** The presence of encoded data within DNS queries is a known method for covert data exfiltration.
  - **No:** It might be legitimate traffic that warrants further investigation.
- **Selection: Yes**

Step 2: Should the SOC Block Outbound DNS Requests to the Suspicious Domain?

- **Options:**
  - **Yes:** Blocking the requests can prevent further data from being exfiltrated.
  - **No:** Continue monitoring to gather more information before blocking the traffic.
- **Selection: Yes**

Stage 2: Incident Identification and Scope

- **Action:** The SOC blocks DNS requests to the suspicious domain and escalates the incident to the Incident Response (IR) team.

Step 3: Should the Compromised Workstation Be Isolated from the Network?

- **Options:**
  - **Yes:** Isolating the system can prevent further data exfiltration.
  - **No:** Isolation might disrupt legitimate operations; proceed with caution.
- **Selection: Yes**

Step 4: Should a Detailed Forensic Analysis Be Conducted on the Compromised Workstation?

- **Options:**
  - **Yes:** Forensic analysis can help identify the tools and methods used for DNS tunneling.
  - **No:** Focus on containing the incident first before conducting forensic analysis.
- **Selection: Yes**

Stage 3: Containment Strategy

- **Action:** The IR team isolates the compromised workstation and begins forensic analysis.

Step 5: Should We Search for Other Systems Exhibiting Similar DNS Tunneling Behaviour?

- **Options:**
  - **Yes:** Identifying other compromised systems can help in containing the full scope of the attack.
  - **No:** Focus on the known compromised system before expanding the scope.
- **Selection: Yes**

Step 6: Should We Implement Additional DNS Filtering and Monitoring?

- **Options:**
  - **Yes:** Enhanced DNS filtering can detect and block further DNS tunneling attempts.
  - **No:** Current monitoring is sufficient; no further actions are necessary.
- **Selection: Yes**

Stage 4: Eradication and Remediation

- **Action:** The IR team searches for other compromised systems and implements additional DNS filtering.

Step 7: Should We Terminate Any Identified Malicious Processes on the Compromised Workstation?

- **Options:**
  - **Yes:** Terminating malicious processes can stop the attacker's activities on the compromised systems.
  - **No:** Focus on identifying the full scope of the breach before taking action.
- **Selection: Yes**

Step 8: Should We Implement New Security Controls to Prevent DNS Tunneling?

- **Options:**
  - **Yes:** Updating security controls can prevent future DNS tunneling attacks.
  - **No:** Focus on addressing the current incident before implementing broader changes.
- **Selection: Yes**

Stage 5: Recovery

- **Action:** The IR team terminates malicious processes and updates security controls to prevent DNS tunneling.

Step 9: Should We Re-Image Compromised Systems to Ensure They Are Clean?

- **Options:**
  - **Yes:** Re-imaging can ensure the removal of any remaining malware or unauthorised changes.
  - **No:** Attempt to clean the systems without re-imaging to minimise downtime.
- **Selection: Yes**

Step 10: Should We Prioritise the Re-Image and Restoration of Systems That Were Most Critical to the Business?

- **Options:**
  - **Yes:** Prioritising critical systems can minimise operational impact.
  - **No:** Follow a standard restoration process without prioritising specific systems.
- **Selection: Yes**

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team re-images compromised systems and restores critical systems first.

Step 11: Should We Conduct a Post-Incident Review to Analyse the Tactics, Techniques, and Procedures (TTPs) Used by the Attacker?

- **Options:**
  - **Yes:** A thorough review can provide insights to improve defences and incident response processes.
  - **No:** Focus on resuming normal operations, and review the incident later.
- **Selection: Yes**

Step 12: Should We Update the Incident Response Playbook and Security Controls Based on the Lessons Learned from This Incident?

- **Options:**
  - **Yes:** Updating the playbook and controls can enhance future responses to similar attacks.
  - **No:** The current playbook and controls are sufficient; no changes are necessary.
- **Selection: Yes**

Full Analysis

1. Initial Detection:

The SOC identified abnormal DNS traffic using the following logs:

- **DNS Log Excerpt:**

  ```
  2024-08-14 10:05:23 - DNS Query: exfil.domain.com
  2024-08-14 10:05:23 - Query Type: A
  2024-08-14 10:05:23 - Query Data: xyz789examplebase64data
  2024-08-14 10:05:24 - DNS Response: 192.168.1.5
  ```

- **Network Traffic Log Excerpt:**

  ```
  2024-08-14 10:05:25 - Source IP: 10.0.0.5
  2024-08-14 10:05:25 - Destination IP: 192.168.1.5
  2024-08-14 10:05:25 - Destination Port: 53 (DNS)
  2024-08-14 10:05:25 - Protocol: UDP
  ```

- **Analysis:** The DNS queries include base64-encoded data indicative of possible data exfiltration through DNS tunneling. The domain “exfil.domain.com” was flagged as suspicious, and subsequent network traffic logs showed communication on port 53.

2. Incident Identification:

- **Forensic Analysis:**
  - **Tools Used:** Wireshark, Splunk
  - **Findings:** The Wireshark capture confirmed that the DNS queries were carrying encoded data, likely containing sensitive information. Splunk analysis showed repeated access to sensitive files on the workstation prior to the DNS queries.
- **System Logs:**

  ```
  2024-08-14 09:55:00 - User: izzmier
  2024-08-14 09:55:05 - File Accessed: /sensitive_data/financial_report.xlsx
  2024-08-14 09:55:10 - Application Used: powershell.exe
  2024-08-14 09:55:15 - Command Executed: Invoke-DNSExfil -Data financial_report.xlsx
  ```

- **Analysis:** The compromised workstation was used to execute a PowerShell script that facilitated DNS-based data exfiltration.

3. Containment Strategy:

- **Action:** The workstation was isolated, and DNS filtering was enhanced to block all traffic to the suspicious domain.

4. Eradication and Remediation:

- **Action:** Malicious processes were terminated, and the compromised workstation was re-imaged. A full audit of DNS traffic was performed across the network to ensure no other systems were compromised.

5. Recovery:

- **Action:** The re-imaged system was restored to the network with enhanced monitoring. Critical systems were prioritised to minimise operational disruption.

6. Post-Incident Review and Improvements:

- **Action:** A detailed review was conducted, leading to updates in the incident response playbook and DNS security controls to mitigate future DNS tunneling attempts.

Simulation 2: Brute Force Attack on Web Application

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the Web Application Firewall (WAF) indicating multiple failed login attempts to a web application from a specific IP address. The number of attempts exceeds the threshold for typical user behaviour, suggesting a brute force attack.
  - **MITRE ATT&CK Technique:** T1110 - Brute Force

Step 1: Is This Activity Consistent with a Potential Brute Force Attack?

- **Options:**
  - **Yes:** The high volume of failed login attempts from a single IP address suggests a brute force attempt.
  - **No:** It might be a legitimate user who has forgotten their password.
- **Selection: Yes**

Step 2: Should the SOC Block the IP Address Associated with the Failed Login Attempts?

- **Options:**
  - **Yes:** Blocking the IP can stop the brute force attempt and protect the web application.
  - **No:** Continue monitoring to gather more information before blocking the IP.
- **Selection: Yes**

Stage 2: Incident Identification and Scope

- **Action:** The SOC blocks the IP address and escalates the incident to the Incident Response (IR) team.

Step 3: Should We Investigate the Impact of This Brute Force Attempt on Other Systems?

- **Options:**
  - **Yes:** Brute force attacks often target multiple systems; investigating others can reveal additional compromised systems.
  - **No:** Focus on the current system before expanding the investigation.
- **Selection: Yes**

Step 4: Should We Check for Any Successful Login Attempts from the Suspicious IP Address?

- **Options:**
  - **Yes:** Checking for successful logins can help identify if the attacker gained access.

    - **No:** Focus on containing the current brute force attempt before checking logs.
- **Selection: Yes**

Stage 3: Containment Strategy

- **Action:** The IR team investigates the potential impact on other systems and checks for successful logins from the suspicious IP address.

Step 5: Should We Enforce Multi-Factor Authentication (MFA) on All User Accounts?

- **Options:**
    - **Yes:** Enforcing MFA can prevent attackers from using compromised credentials to gain access.
    - **No:** Focus on identifying the full scope of the breach before implementing MFA.
- **Selection: Yes**

Step 6: Should We Review and Strengthen Password Policies Across the Organisation?

- **Options:**
    - **Yes:** Strengthening password policies can reduce the risk of successful brute force attacks.
    - **No:** Current policies are sufficient; no changes are necessary.
- **Selection: Yes**

Stage 4: Eradication and Remediation

- **Action:** The IR team enforces MFA and reviews password policies.

Step 7: Should We Reset Passwords for Accounts That Were Targeted in the Brute Force Attack?

- **Options:**
    - **Yes:** Resetting passwords can ensure that compromised accounts are secure.
    - **No:** Focus on containing the incident before resetting passwords.
- **Selection: Yes**

Step 8: Should We Monitor for Any Further Brute Force Attempts from Different IP Addresses?

- **Options:**
    - **Yes:** Monitoring can help detect and prevent additional brute force attempts.
    - **No:** Current monitoring is sufficient; no further actions are necessary.
- **Selection: Yes**

Stage 5: Recovery

- **Action:** The IR team resets passwords for targeted accounts and implements enhanced monitoring.

Step 9: Should We Conduct a Review of All Access Logs to Identify Any Unusual Login Patterns?

- **Options:**
  - **Yes:** Reviewing logs can help identify any other compromised accounts or systems.
  - **No:** Focus on the known affected accounts without expanding the scope.
- **Selection: Yes**

Step 10: Should We Communicate the Incident to All Users and Educate Them on Brute Force Attacks?

- **Options:**
  - **Yes:** Educating users can help them recognise and report suspicious activity.
  - **No:** Communication is not necessary at this time.
- **Selection: Yes**

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team reviews access logs and communicates the incident to users.

Step 11: Should We Conduct a Post-Incident Review to Analyse the Tactics, Techniques, and Procedures (TTPs) Used by the Attacker?

- **Options:**
  - **Yes:** A thorough review can provide insights to improve defences and incident response processes.
  - **No:** Focus on resuming normal operations, and review the incident later.
- **Selection: Yes**

Step 12: Should We Update the Incident Response Playbook and Security Controls Based on the Lessons Learned from This Incident?

- **Options:**
  - **Yes:** Updating the playbook and controls can enhance future responses to similar attacks.
  - **No:** The current playbook and controls are sufficient; no changes are necessary.
- **Selection: Yes**

Full Analysis

1. Initial Detection:

The SOC identified suspicious login attempts using the following logs:

- **WAF Log Excerpt:**

  ```
  2024-08-14 09:30:00 - IP Address: 203.0.113.45
  2024-08-14 09:30:02 - Failed Login Attempt: user1
  2024-08-14 09:30:05 - Failed Login Attempt: user2
  2024-08-14 09:30:07 - Failed Login Attempt: user3
  ...
  2024-08-14 09:35:00 - Total Failed Attempts: 150
  ```

- **Access Log Excerpt:**

  ```
  2024-08-14 09:36:00 - Successful Login: admin - IP Address: 203.0.113.45
  2024-08-14 09:36:05 - Access to Sensitive File: /admin/dashboard
  2024-08-14 09:36:10 - Logout: admin
  ```

- **Analysis:** The WAF logs show repeated failed login attempts, indicating a brute force attack. The access logs reveal a successful login from the same IP address, suggesting the attacker successfully breached the account.

2. Incident Identification:

- **Forensic Analysis:**
  - **Tools Used:** Wireshark, Splunk
  - **Findings:** The Splunk analysis confirmed multiple failed login attempts followed by a successful login, matching the pattern of a brute force attack. Wireshark captured the network traffic, which showed a high volume of login requests from the suspicious IP address.
- **System Logs:**

  ```
  2024-08-14 09:35:59 - User: admin
  2024-08-14 09:36:01 - IP Address: 203.0.113.45
  2024-08-14 09:36:02 - Action: Successful Login
  2024-08-14 09:36:03 - Resource Accessed: /admin/dashboard
  ```

- **Analysis:** The attacker successfully gained access to the admin account using brute force techniques and accessed sensitive resources.

3. Containment Strategy:

- **Action:** The SOC blocked the IP address, enforced MFA, and initiated a review of password policies.

4. Eradication and Remediation:

- **Action:** Passwords for targeted accounts were reset, and enhanced monitoring was implemented to detect further brute force attempts.

5. Recovery:

- **Action:** The IR team reviewed access logs, communicated the incident to users, and provided education on recognising brute force attacks.

6. Post-Incident Review and Improvements:

- **Action:** A detailed post-incident review was conducted, leading to updates in the incident response playbook and security controls to better defend against future brute force attacks.

Simulation 3: SQL Injection Attack on a Web Application

Stage 1: Initial Detection

- **Alert:** The SOC receives an alert from the Web Application Firewall (WAF) indicating an unusual spike in SQL queries from a specific IP address targeting the login page of a web application. The queries contain suspicious patterns, such as ' OR '1'='1'--.
    - **MITRE ATT&CK Technique:** T1190 - Exploit Public-Facing Application (SQL Injection)

Step 1: Is This Activity Consistent with a Potential SQL Injection Attack?

- **Options:**
    - **Yes:** The suspicious SQL queries suggest an attempt to exploit a vulnerability in the web application.
    - **No:** It might be legitimate queries from an authorised user.
- **Selection: Yes**

Step 2: Should the SOC Block the IP Address Associated with the Suspicious SQL Queries?

- **Options:**
    - **Yes:** Blocking the IP can prevent the potential SQL injection attack from succeeding.
    - **No:** Continue monitoring to gather more information before blocking the IP.
- **Selection: Yes**

Stage 2: Incident Identification and Scope

- **Action:** The SOC blocks the IP address and escalates the incident to the Incident Response (IR) team.

Step 3: Should We Investigate Other Web Application Logs to Identify Similar Suspicious Activity?

- **Options:**
    - **Yes:** Investigating other logs can help identify if the attacker attempted SQL injection on other parts of the application.
    - **No:** Focus on the current identified activity before expanding the investigation.
- **Selection: Yes**

Step 4: Should We Check for Any Successful Database Access or Data Exfiltration?

- **Options:**

  - **Yes:** Checking for successful database access can determine if the attacker retrieved sensitive data.
  - **No:** Focus on preventing further attacks before checking for data exfiltration.
- **Selection: Yes**

Stage 3: Containment Strategy

- **Action:** The IR team investigates other web application logs and checks for any successful database access or data exfiltration.

Step 5: Should We Patch Any Identified SQL Injection Vulnerabilities Immediately?

- **Options:**
  - **Yes:** Patching can prevent the attacker from exploiting the vulnerability further.
  - **No:** Focus on containment before implementing patches.
- **Selection: Yes**

Step 6: Should We Implement Web Application Hardening Measures, Such as Input Validation and Parameterised Queries?

- **Options:**
  - **Yes:** Hardening the web application can reduce the risk of future SQL injection attacks.
  - **No:** Current security measures are sufficient; no changes are necessary.
- **Selection: Yes**

Stage 4: Eradication and Remediation

- **Action:** The IR team patches the SQL injection vulnerabilities and implements web application hardening measures.

Step 7: Should We Review and Update the Web Application Firewall (WAF) Rules to Better Detect and Block SQL Injection Attempts?

- **Options:**
  - **Yes:** Updating WAF rules can improve detection and prevention of SQL injection attacks.
  - **No:** The current WAF rules are sufficient; no changes are necessary.
- **Selection: Yes**

Step 8: Should We Monitor the Web Application for Any Further Suspicious Activity Post-Patching?

- **Options:**
  - **Yes:** Monitoring can help detect any additional attempts to exploit the web application.

    - **No:** Focus on the known incident without further monitoring.
- **Selection: Yes**

Stage 5: Recovery

- **Action:** The IR team updates the WAF rules and monitors the web application for any further suspicious activity.

Step 9: Should We Conduct a Full Code Review of the Web Application to Identify and Fix Any Other Potential Vulnerabilities?

- **Options:**
    - **Yes:** A code review can help identify and remediate other vulnerabilities that might be exploited.
    - **No:** Focus on the current identified vulnerability without expanding the scope.
- **Selection: Yes**

Step 10: Should We Communicate the Incident to the Development Team and Provide Guidance on Secure Coding Practices?

- **Options:**
    - **Yes:** Communicating with the development team can help prevent similar vulnerabilities in the future.
    - **No:** No need to involve the development team at this stage.
- **Selection: Yes**

Stage 6: Post-Incident Review and Improvements

- **Action:** The IR team conducts a full code review and communicates with the development team.

Step 11: Should We Conduct a Post-Incident Review to Analyse the Tactics, Techniques, and Procedures (TTPs) Used by the Attacker?

- **Options:**
    - **Yes:** A thorough review can provide insights to improve defences and incident response processes.
    - **No:** Focus on resuming normal operations, and review the incident later.
- **Selection: Yes**

Step 12: Should We Update the Incident Response Playbook and Security Controls Based on the Lessons Learned from This Incident?

- **Options:**
    - **Yes:** Updating the playbook and controls can enhance future responses to similar attacks.

    - **No:** The current playbook and controls are sufficient; no changes are necessary.
- **Selection: Yes**

Full Analysis

1. Initial Detection:

The SOC identified suspicious SQL queries using the following logs:

- **WAF Log Excerpt:**

  ```
  2024-08-14 14:45:00 - IP Address: 192.168.1.105
  2024-08-14 14:45:05 - SQL Query: ' OR '1'='1'-- targeting /login
  2024-08-14 14:45:07 - SQL Query: ' OR '1'='1'-- targeting /login
  ...
  2024-08-14 14:50:00 - Total SQL Queries: 50
  ```

- **Access Log Excerpt:**

  ```
  2024-08-14 14:50:10 - IP Address: 192.168.1.105
  2024-08-14 14:50:12 - Database Access: SELECT * FROM users WHERE
  username='admin'
  ```

- **Analysis:** The WAF logs show repeated SQL injection attempts, indicating that the attacker tried to exploit a vulnerability in the login page. The access logs reveal that the attacker executed a query against the users table, which could lead to unauthorised access.

2. Incident Identification:

- **Forensic Analysis:**
    - **Tools Used:** Splunk, Wireshark
    - **Findings:** Splunk confirmed the SQL injection pattern by analysing the query structure. Wireshark captured the network traffic, showing a series of suspicious SQL queries from the identified IP address.
- **System Logs:**

  ```
  2024-08-14 14:50:12 - User: admin
  2024-08-14 14:50:14 - Action: Database Query Executed
  2024-08-14 14:50:16 - Resource Accessed: /users table
  ```

- **Analysis:** The attacker executed a SQL injection attack to gain unauthorised access to the database, potentially compromising user credentials.

3. Containment Strategy:

- **Action:** The SOC blocked the IP address, patched the identified SQL injection vulnerability, and implemented web application hardening measures.

4. Eradication and Remediation:

- **Action:** The IR team updated the WAF rules to detect and block future SQL injection attempts and monitored the web application for any further suspicious activity.

5. Recovery:

- **Action:** The IR team conducted a full code review to identify and fix other potential vulnerabilities and communicated secure coding practices to the development team.

6. Post-Incident Review and Improvements:

- **Action:** A detailed post-incident review was conducted, leading to updates in the incident response playbook and security controls to better defend against future SQL injection attacks.