Business Email Compromise

**Incident Response Playbook Template**

**Suitable for all (private and public) organizations**

**Developed by: Olumuyiwa Olufunmilola Agunbiade, CISSP, CISA, CEH, CCNA, MSc**

Introduction to Business Email Compromised Playbook

In the dynamic landscape of cybersecurity, organizations face a multitude of threats, and among them, Business Email Compromise (BEC) stands out as a pervasive and highly sophisticated attack vector. In response to the escalating threat posed by BEC incidents, I have developed a comprehensive BEC Playbook attached to this post. This playbook serves as a strategic guide to equip different organizations around the world with the knowledge and tools needed to detect, respond to, and mitigate the risks associated with BEC attacks.

This document has been designed and developed by drawing insights from various regulatory standards, including but not limited to the ISO 27000 series, NIST standards, PCI DSS, and several others.

Importance of the BEC Playbook

1. Rising Threat Landscape:

The frequency and sophistication of BEC attacks have surged in recent times, making them a significant concern for organizations globally. This BEC Playbook is a proactive measure to counteract the evolving tactics employed by cyber adversaries.

2. Financial Implications:

BEC attacks often target financial transactions, leading to substantial financial losses for organizations. This playbook addresses the financial risk associated with BEC by providing guidance on identifying fraudulent activities, securing financial transactions, and implementing controls to prevent unauthorized fund transfers.

3. Operational Continuity:

BEC incidents can disrupt normal business operations, causing delays and potentially compromising sensitive information. This playbook outlines strategies to ensure operational continuity, even in the face of a BEC attack, by promptly detecting and containing threats.

4. Protection of Sensitive Information:

BEC attacks frequently involve the compromise of sensitive business information, including financial data, intellectual property, and confidential communications. This playbook emphasizes the protection of such information through effective incident response measures, thereby safeguarding the organization's integrity and reputation.

5. Regulatory Compliance:

Adherence to regulatory standards is critical for organizations, especially when dealing with sensitive data. This BEC Playbook aligns with regulatory requirements, offering guidance on incident reporting, data breach notifications, and other compliance-related aspects to ensure legal obligations are met.

6. Enhanced Employee Awareness:

BEC attacks often exploit human vulnerabilities, relying on social engineering tactics to deceive employees. This playbook includes educational resources to enhance employee awareness and promote a culture of cybersecurity vigilance within the organization.

7. Cross-Functional Collaboration:

BEC incidents necessitate collaboration across various departments, including IT, finance, legal, and executive leadership. This playbook establishes a framework for cross-functional cooperation, ensuring a unified response to mitigate the impact of BEC attacks.

8. Continuous Improvement:

Cyber threats are dynamic, requiring a playbook that evolves with the changing landscape. This BEC Playbook is a living document that undergoes regular updates to incorporate emerging threat intelligence, industry best practices, and lessons learned from previous incidents, ensuring continuous improvement in response capabilities.

In conclusion, this BEC Playbook is a strategic asset designed to fortify organizations against the multifaceted challenges posed by BEC attacks. By adopting a proactive and comprehensive approach outlined in the playbook, organizations will be able to bolster their cybersecurity defenses, fostering trust and confidence among stakeholders in today's interconnected digital landscape and ecosystem.

Version history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Update Date | Updated By | Reason for Update |
| 1.0 | 11/12/2023 | Olumuyiwa Agunbiade | Initial Draft (Template) |
|  |  |  |  |

Purpose

To guide <ORGANIZATION Name> in responding to a Business Email Compromise incident.

How to Use This Playbook

The procedures and steps outlined in this playbook are designed to be executed in sequence when applicable. Given the multiple steps within Containment, Eradication, and Recovery, it is anticipated that some steps may overlap.

Preparation

Note: Preparation steps are intended to be primarily executed and completed before the occurrence of an event or incident.

1. Identify and determine the members of the Cybersecurity Incident Response Team (CSIRT) if applicable.
   1. The essential CSIRT members should consist of individuals dedicated solely to cybersecurity.
      1. This may involve certain Information Technology roles, depending on the organization's size.
      2. The compact size of the core CSIRT aims to maintain confidentiality and operational efficiency.
      3. The core CSIRT might frequently be activated to probe security events, whether or not they escalate into incidents.
   2. Assign specific roles and responsibilities to each member.
      1. Summary of roles and responsibilities for <ORGANIZATION Name> CSIRT team
2. Determine extended CSIRT members.
   1. This may include Executive Leadership, Compliance, Legal, and Public Relations.
   2. Summary of roles and responsibilities for extended CSIRT team
3. Define and establish escalation paths.
   1. Incidents may initially manifest as events or have a lower impact/severity, evolving as more information is gathered. Defining an escalation path is crucial for success.
   2. Provide an example of an escalation path, including thresholds for escalation.
4. Ensure logging levels for email system components are set to appropriate levels.
   1. Ensure a minimum retention period of 90 days.
   2. Elaborate on what logging levels for email system components entail and provide guidance on checking and adjusting them if necessary.
   3. Demonstrate how to perform these actions on platforms like Google and Outlook.
5. Ensure that logs for email system components are securely stored, preferably on a secondary system like a Security Information and Event Management (SIEM).
   1. Define SIEM
   2. Give examples of good and reputable SIEM solutions

Identification

1. Utilize evidence leading to the notification of compromise for determining subsequent actions or next steps based on the method of compromise. **(Please note: Certain steps may not be applicable depending on the method of compromise.)**
   1. Example of evidence: emails from an external client saying they received a phishing email or malware, a fraudulent funds transfer, email rules that were not created by the user, etc.
   2. Examples of method of compromise: brute forced password attacks, attached malware, credential harvesting phish attacks, etc.
2. Identify and determine the initial method of account compromise.
   1. Conduct an interview with the affected user to collect details on potential points of compromise.
      1. Example questions:
         1. Did you recently download and install any new software?
         2. Did you receive a suspicious email?
         3. Did you recently receive any unexpected documents via email?
         4. Did you enter your email credentials after clicking a link, or on a website that seemed to not accept them?
   2. Search for phishing emails i.e search for emails containing links to credential harvesting sites
      1. Provide details on identifying phishing emails.
   3. Search for emails containing links to credential harvesting sites.
      1. Examples of credential harvesting sites and methods of identification.
   4. Search and identify potential malware on the user's workstation.
      1. Use credential harvesters like Mimikatz.
         1. Describe how to locate on the workstation.
         2. Explain what a credential harvester is.
      2. Recognize keystroke recording software.
         1. Explain how to find on the workstation.
         2. Explain Elaborate on what keystroke recording software is.
      3. Detect clipboard scraping malware.
         1. Explain what clipboard scraping malware is.
         2. Describe how to find on the workstation.
3. Once the initial compromise method is determined, use gathered Indicators of Compromise (IoCs) to search for other victims in the environment.
   1. Detail where users should search and the tools to use.
   2. Possible query inputs include the email subject name, document name, document hash, URL from email, and other relevant details.
4. Review the logs in the email system, looking for any anomalies or irregularities in user activity, login patterns, or other indicators that may suggest a security incident.
   1. Examine login activity from unusual locations, systems, or browser fingerprints.
   2. Analyze and compare any login anomalies by comparing them with other logins that share similar characteristics, such as:
      1. Originating IP address – explain how to find and provide screenshots.

**To locate the originating IP address in your email system logs, follow these steps:**

**Step 1:**

**Access Email System Logs:**

* Log in to your email system's administrative console or backend.
* Navigate to the section related to audit logs or security logs.

**Step 2:**

**Locate Login or Access Logs:**

* Look for logs that record user login or access activities.

**Step 3:**

**Identify Originating IP Address:**

* Within the relevant logs, find the entry corresponding to the specific user account in question.
* The originating IP address will typically be listed alongside the log entry.

**Step 4:**

**Screenshot Guidance:**

* Capture a screenshot of the log entry displaying the originating IP address.
* Ensure the screenshot includes relevant details, such as timestamps and user account information.

**Remember,** the exact steps may vary based on your specific email system. Consult the system's documentation or support resources for further assistance.

* + 1. Originating IP address: Explain how to find provide screenshots.

**To identify concurrent logins and compare anomalies, follow these steps:**

**Step 1:**

**Access Email System Logs:**

* Log in to your email system's administrative console or backend.
* Navigate to the section related to audit logs or security logs.

**Step 2:**

**Locate Login or Access Logs:**

* Look for logs that record user login or access activities.

**Step 3:**

**Identify Concurrent Logins:**

* Within the relevant logs, find the entries corresponding to the specific user account.
* Look for multiple entries with the same user account accessing the system concurrently.

**Step 4:**

**Capture Screenshots:**

* Take screenshots of the log entries displaying concurrent logins.
* Ensure the screenshots include timestamps, user account details, and the concurrent login information.

**Step 5:**

**Compare Anomalies:**

* Compare the concurrent login entries to the user's typical login patterns.
* Look for anomalies such as logins from unusual locations or simultaneous logins from different devices.

**Remember,** the steps might vary based on your specific email system. Consult the system's documentation or support resources for detailed guidance.

* + 1. Browser fingerprint: Explain how to find and provide screenshots.

**To find and compare browser fingerprints in email system logs, follow these steps:**

**Step 1:**

**Access Email System Logs:**

* Log in to your email system's administrative console or backend.
* Navigate to the section related to audit logs or security logs.

**Step 2:**

**Locate Browser Fingerprint Information:**

* Look for logs that contain details about user sessions or access activities.
* Identify the entries related to the specific user account.

**Step 3:**

**Find Browser Fingerprint Data:**

* Within the log entries, search for fields or information related to browser fingerprints.
* Browser fingerprint data may include details such as user-agent strings, device information, and browser configurations.

**Step 4:**

**Capture Screenshots:**

* Take screenshots of the log entries displaying browser fingerprint information.
* Ensure the screenshots include timestamps, user account details, and the relevant browser fingerprint data.

**Step 5:**

**Compare Anomalies:**

**Compare the browser fingerprint entries to the user's typical fingerprint.**

**Look for anomalies such as different user-agent strings, unusual device details, or unexpected changes in browser configurations.**

**Step 6:**

**Note Inconsistencies:**

* Document any inconsistencies or variations in browser fingerprints that deviate from the user's normal patterns.
* Always refer to your specific email system's documentation or support resources for precise details on accessing and interpreting logs.

1. Assess victim email accounts to determine if sensitive information may be contained in them.

**To assess victim email accounts for sensitive information, follow these steps:**

**Step 1:**

**Access the Email Account:**

* Log in to the victim's email account using appropriate administrative credentials.

**Step 2:**

**Review Inbox and Folders:**

* Navigate through the inbox, sent items, and other folders to understand the content.
* Pay special attention to emails containing sensitive information such as financial data, passwords, or personal details.

**Step 3:**

**Search for Specific Keywords:**

* Use the search functionality to look for specific keywords associated with sensitive information.
* Examples include terms like "password," "SSN," "credit card," etc.

**Step 4:**

**Examine Attachments:**

* Review attachments in emails to identify any documents or files containing sensitive data.
* Check for file types commonly used for sensitive information (e.g., PDFs, spreadsheets).

**Step 5:**

**Check Shared Folders or Drives:**

* If applicable, check shared folders, cloud drives (e.g., OneDrive, Google Drive), or network drives associated with the email account.
* Look for sensitive documents or data shared within the organization.

**Step 6:**

**Document Findings:**

* Document any sensitive information found during the assessment.
* Include details such as email subjects, sender information, and attachment names.

**Step 7:**

**Consult Legal Counsel (if needed):**

* If sensitive information is discovered, consult legal counsel to determine appropriate next steps.
* Legal advice may be necessary for handling and mitigating potential legal consequences.

**Step 8:**

**Prepare a Summary Report:**

* Create a summary report outlining the findings of the assessment.
* Include details on any sensitive information discovered and actions taken.
* Always ensure that the assessment is conducted in compliance with legal and privacy regulations, and follow organizational policies and procedures.
  1. This may need to be extended to other sources these users and/or accounts have access to such as OneDrive, Google Drive, SharePoint, shared mailboxes, fileservers, etc.
  2. If sensitive information is a possibility, consult legal counsel for next steps.
     1. Give examples of sensitive info

1. Search impacted systems for newly created users.

**To search impacted systems for newly created users, perform the following steps:**

**Step 1:**

**Access System Logs:**

* Ensure that all recently created users are accounted for.
* Log in to the affected systems using appropriate administrative credentials.

**Step 2:**

**Check Event Logs:**

* Navigate to the event logs or system logs on the affected systems.
* Look for events related to user creation or account modifications.

**Step 3:**

**Filter by Relevant Timeframe:**

* Specify the timeframe during which the incident occurred or when the compromise is suspected.
* Narrowing the search timeframe will help identify recently created users.

**Step 4:**

**Review User Account Changes:**

* Look for events indicating the creation of new user accounts or modifications to existing accounts.
* Check for information such as account creation date, username, and associated details.

**Step 5:**

**Use PowerShell or Command Line:**

* Utilize PowerShell or command-line tools to query user account information.
* Commands like Get-LocalUser (Windows) or awk/grep (Unix/Linux) can provide user details.

**Step 6:**

**Cross-Verify with User Management Tools:**

* If applicable, use user management tools or Active Directory to cross-verify the list of users.
* Ensure that all recently created users are accounted for and legitimate.

**Step 7:**

**Document Findings:**

* Document details of any newly created users, including usernames, creation dates, and associated systems.
* Note any discrepancies or suspicious accounts.

**Step 8:**

**Investigate Anomalies:**

* Investigate any anomalies or accounts that raise suspicion.
* Check for signs of unauthorized access or malicious activities associated with these users.

**Step 9:**

**Take Remedial Actions:**

* If unauthorized or suspicious users are identified, take appropriate remedial actions.
* This may involve disabling or removing unauthorized accounts and securing affected systems.

**Step 10:**

**Prepare Incident Report:**

* Compile a detailed incident report outlining the findings related to newly created users.
* Include information on actions taken and recommendations for further investigation.
* Always adhere to organizational policies, legal requirements, and privacy considerations when conducting investigations and taking remedial actions. Documenting the process thoroughly is crucial for incident response and subsequent analysis.

Containment

1. Reset all passwords associated with all identified victims.

**To reset all passwords associated with identified victims, follow these steps:**

**Step 1:**

**Access User Account Management:**

* Start with email account passwords, but all accounts associated with the user should have their passwords reset or disabled.
* Log in to the relevant user account management system or directory service with administrative credentials.

**Step 2:**

**Identify Affected User Accounts:**

* Refer to the list of identified victims or compromised accounts from the incident investigation.
* Ensure that you have a comprehensive and accurate list of affected users.

**Step 3:**

**Initiate Password Reset:**

* For each affected user account, initiate a password reset process.
* Depending on the system, this may involve using administrative tools, user management consoles, or command-line interfaces.

**Step 4:**

**Use Strong Passwords:**

* Generate or assign strong, complex passwords for each user.
* Follow best practices for password complexity, including a mix of uppercase and lowercase letters, numbers, and special characters.

**Step 5:**

**Notify Users:**

* Communicate the password reset to affected users promptly.
* Provide clear instructions on how to log in with the new credentials.

**Step 6:**

**Encourage Two-Factor Authentication (2FA):**

* Encourage users to enable two-factor authentication (2FA) if available.
* 2FA adds an additional layer of security to user accounts.

**Step 7:**

**Monitor Login Activity:**

* Monitor login activity for the reset accounts to identify any unusual or suspicious behavior.
* Implement logging and alerting mechanisms to detect potential security incidents.

**Step 8:**

**Document Changes:**

* Document the password reset process for each affected user, including the date and time of the reset.
* Maintain records for audit and incident response purposes.

**Step 9:**

**Verify Account Accessibility:**

* Verify that users can successfully log in with their new credentials.
* Address any issues promptly and provide support as needed.

**Step 10:**

**Review and Update Policies:**

* Review password reset policies and update them if necessary.
* Consider conducting user awareness training on password security.

**Step 11:**

**Conduct Post-Incident Analysis:**

* After the password reset, conduct a post-incident analysis to understand the root cause of the compromise and identify preventive measures.
* Always ensure that password reset processes align with organizational security policies and comply with relevant regulations. Additionally, communicate transparently with affected users to maintain trust and enhance cybersecurity awareness.

1. Revoke authentication tokens for all identified victim accounts.
   1. Define authentication tokens + how to revoke them

**Define Authentication Tokens:**

Authentication tokens, often referred to as auth tokens or access tokens, are cryptographic strings generated by an authentication server after a user successfully authenticates their identity. These tokens serve as proof of the user's authentication and are used to access protected resources or services without the need to re-enter credentials for each request.

**How to Revoke Authentication Tokens:**

Revoking authentication tokens is a crucial security practice to terminate access in case of compromised credentials, unauthorized access, or when a user logs out. The process involves invalidating the existing tokens and preventing their further use. Here's how to revoke authentication tokens:

**Step 1:**

**Identify Token Revocation Mechanism:**

* Determine the mechanism or API provided by the authentication server or identity provider for token revocation.
* Common protocols like OAuth 2.0 provide token revocation endpoints.

**Step 2:**

**Use Token Revocation Endpoint:**

* Utilize the token revocation endpoint to revoke specific tokens associated with a user.
* Include the token(s) to be revoked in the request.

**Step 3:**

**Send a POST Request:**

* Send a POST request to the token revocation endpoint with the necessary parameters.
* Parameters may include the token itself, client credentials, and other required information.

**Step 4:**

**Handle Token Revocation Response:**

* Process the response from the token revocation endpoint.
* A successful response indicates that the tokens have been successfully revoked.

**Step 5:**

**Update User Session:**

* If applicable, update the user's session on the client side to reflect the revoked tokens.
* Ensure that the user is logged out or prompted to re-authenticate.

**Step 6:**

**Implement Token Expiry Policies:**

* Enforce token expiry policies to automatically invalidate tokens after a certain period.
* Short-lived tokens enhance security by reducing the window of potential misuse.

**Step 7:**

**Communicate Revocation to Users:**

* Communicate token revocation events to users.
* Provide clear information on why the revocation occurred and instruct users on any necessary actions.

**Step 8:**

**Monitor and Audit Revocation Events:**

* Implement monitoring and auditing mechanisms to track token revocation events.
* Maintain logs for compliance, incident response, and analysis.

**Step 9:**

**Consider Token Refresh:**

* If applicable, consider implementing token refresh mechanisms to issue new tokens without requiring user credentials.

**Step 10:**

**Review and Update Policies:**

* Regularly review and update token revocation policies based on security requirements and industry best practices.
* Effective token revocation mechanisms are essential for maintaining the security of user accounts and protecting sensitive resources. Always follow secure coding practices and adhere to relevant security standards when implementing token revocation processes.
* This should cover the email system and any other accounts that are associated with the impacted users.

1. If an external organization is identified during the investigation, notify the organization of any compromises or concerns.
   1. Work with legal counsel to determine this process.

**Work with Legal Counsel to Determine This Process:**

Collaborating with legal counsel is a crucial step in the incident response process, especially when dealing with potential legal implications or sensitive matters. Legal professionals play a key role in ensuring that actions taken align with applicable laws, regulations, and organizational policies. Here's a guide on how to work with legal counsel to determine processes related to incident response:

**Step 1:**

**Establish Communication:**

* Initiate timely communication with the legal counsel to inform them of the incident.
* Provide a comprehensive overview of the situation, including potential legal considerations.

**Step 2:**

**Define Objectives:**

* Clearly outline the objectives of involving legal counsel in the incident response process.
* Identify specific legal aspects, such as compliance requirements, privacy laws, or potential legal actions.

**Step 3:**

**Legal Consultation:**

* Schedule a consultation session with legal counsel to discuss the incident in detail.
* Share relevant information, evidence, and context to enable legal professionals to assess the situation accurately.

**Step 4:**

**Legal Risk Assessment:**

* Collaborate with legal counsel to conduct a risk assessment related to the incident.
* Evaluate potential legal consequences, liabilities, and risks associated with different courses of action.

**Step 5:**

**Legal Compliance:**

* Ensure that all incident response actions align with applicable legal frameworks.
* Address any legal compliance requirements, industry regulations, or data protection laws.

**Step 6:**

**Documentation and Privilege:**

* Work with legal counsel to establish attorney-client privilege for sensitive communications and documentation.
* Document discussions, legal advice, and decisions made in collaboration with legal professionals.

**Step 7:**

**Legal Strategy Development:**

* Develop a legal strategy tailored to the specific incident and its implications.
* Determine whether legal actions, notifications, or other legal measures are necessary.

**Step 8:**

**Communication with Stakeholders:**

* Coordinate with legal counsel on communications with internal and external stakeholders.
* Ensure that messages are crafted in a way that minimizes legal risks and adheres to legal guidance.

**Step 9:**

**Legal Reporting:**

* Collaborate on preparing any required legal reports or notifications.
* Comply with legal obligations related to incident reporting, if applicable.

**Step 10:**

**Ongoing Collaboration:**

* Maintain ongoing collaboration with legal counsel throughout the incident response process.
* Keep legal professionals informed of developments and seek guidance as needed.

**Step 11:**

**Post-Incident Review:**

* Conduct a post-incident review with legal counsel to assess the effectiveness of legal strategies.
* Identify lessons learned and areas for improvement in future incident response efforts.

By working closely with legal counsel, organizations can navigate complex legal considerations during incident response and ensure that actions taken are legally sound and compliant with relevant regulations.

* 1. This will help prevent the organization’s users from being targeted again from the same compromised source.

1. If an external organization is identified during the investigation, block their related domains from sending email to your organization.

Blocking domains associated with external organizations is a strategic step to enhance the security posture of your organization during an incident response. This action helps mitigate potential threats and prevents further exposure to malicious activities. Here's a guide on how to block domains of external organizations:

**Step 1:**

**Identify Suspicious External Organizations:**

* Analyze the findings of the investigation to identify external organizations that pose a potential threat.
* Look for evidence or indicators of compromise related to these external entities.

**Step 2:**

**Gather Information on Identified Domains:**

* Collect comprehensive information about the domains associated with the external organizations.
* Obtain domain names, IP addresses, and any other relevant details.

**Step 3:**

**Access Email Security Settings:**

* Log in to the email security administration console or platform used by your organization.
* Navigate to the settings related to email filtering, blocking, or security.

**Step 4:**

**Domain Blocking Configuration:**

* Locate the section for domain blocking or filtering within the email security settings.
* Access the configuration options for adding or blocking domains.

**Step 5:**

**Add Identified Domains to Blocklist:**

* Input the domain names of the identified external organizations into the blocklist.
* Ensure accurate entry of domain names to prevent unintended consequences.

**Step 6:**

**Verify and Confirm Blocking Rules:**

* Review the configured rules to block the identified domains.
* Confirm that the blocking rules are properly implemented and active.

**Step 7:**

**Monitor Blocked Domains:**

* Set up monitoring mechanisms to track and log activities related to the blocked domains.
* Regularly review logs and reports for any attempts or activities associated with the blocked domains.

**Step 8:**

**Adjust Blocking Rules as Needed:**

* Stay agile in response to evolving threats.
* If additional information or threats emerge, adjust the blocking rules accordingly.

**Step 9:**

**Communicate Internally:**

* Inform relevant internal stakeholders, including IT teams and employees, about the domain blocking measures.
* Provide guidance on recognizing and reporting any further suspicious activities.

**Step 10:**

**Document Blocking Actions:**

* Document the specifics of the domain blocking actions taken during the incident response.
* Keep a record of the rationale, domains blocked, and any relevant contextual information.

**Step 11:**

**Collaborate with Security Teams:**

* Collaborate with internal and external security teams to share information on the identified external organizations.
* Participate in threat intelligence sharing initiatives, if applicable.

**Step 12:**

**Continuous Monitoring:**

* Implement continuous monitoring of inbound emails for any signs of persistence or new threats.
* Regularly reassess the effectiveness of the domain blocking measures.

By proactively blocking domains associated with external organizations identified during an incident, your organization strengthens its defenses and minimizes the risk of ongoing or future threats originating from those sources.

1. If malware is discovered during the investigation:
   1. Preserve a sample of the malware.
      1. Why you should do so
      2. How to do so safely

**Preserving a Sample of Malware:**

Preserving a sample of malware is a critical step in incident response for further analysis, investigation, and potential collaboration with cybersecurity experts. Here's a guide on how to preserve a sample of malware:

**Step 1:**

**Isolate the Infected System:**

* Immediately isolate the system or device that is suspected to be infected with malware.
* Disconnect the system from the network to prevent further spread.

**Step 2:**

**Document Relevant Information:**

* Document any relevant information about the infected system, such as system details, observed symptoms, and user activities leading to the suspicion.

**Step 3:**

**Identify Suspicious Files or Behavior:**

* Identify the files or processes on the infected system that are suspected to be malicious.
* Note any unusual or suspicious behavior exhibited by the system.

**Step 4:**

**Use a Trusted Malware Analysis Environment:**

* Set up a dedicated and isolated malware analysis environment or leverage an existing one.
* Ensure that the analysis environment is not connected to the organization's production network.

**Step 5:**

**Capture and Preserve the Malware:**

* Use a reliable malware analysis tool or platform to capture and preserve the suspected malware.
* Create a forensic image or snapshot of the system for further analysis.

**Step 6:**

**Hashing and Integrity Verification:**

* Generate cryptographic hash values (MD5, SHA-256, etc.) of the preserved malware sample.
* Verify the integrity of the preserved sample by comparing hash values.

**Step 7:**

**Secure Storage:**

* Store the preserved malware sample in a secure and encrypted location.
* Limit access to authorized personnel involved in the incident response process.

**Step 8:**

**Labeling and Documentation:**

* Clearly label the preserved malware sample with relevant details, including date, time, and source.
* Maintain detailed documentation on the characteristics and observed behavior of the malware.

**Step 9:**

**Chain of Custody:**

* Establish a chain of custody for the preserved malware sample.
* Record the names and roles of individuals handling the sample, along with timestamps.

**Step 10:**

**Consider Legal and Ethical Considerations:**

* Ensure that the process of preserving and analyzing malware complies with legal and ethical considerations.
* Consult legal counsel if necessary, especially if sharing the sample with external entities.

**Step 11:**

**Notify Relevant Stakeholders:**

* Notify relevant stakeholders, such as IT security teams, incident response teams, or external cybersecurity experts, about the preserved malware sample.

**Step 12:**

**Share Indicators of Compromise (IoCs):**

* Share identified indicators of compromise (IoCs) with relevant cybersecurity communities or threat intelligence platforms to contribute to collective defense efforts.

Preserving a sample of malware in a systematic and secure manner enables thorough analysis, enhances understanding of the threat landscape, and supports the development of effective countermeasures. It also facilitates collaboration with the broader cybersecurity community to strengthen defenses against similar threats.

* 1. Analyze the malware with any tools available.
     1. Does analyzing the malware involve more than gathering the file hash? If so please explain more.
     2. Gather file hash using PowerShell “Get-Filehash” cmdlet.

**Gathering File Hash using PowerShell:**

**To gather file hash using PowerShell's Get-FileHash cmdlet, follow these steps:**

**Step 1:**

**Open PowerShell:**

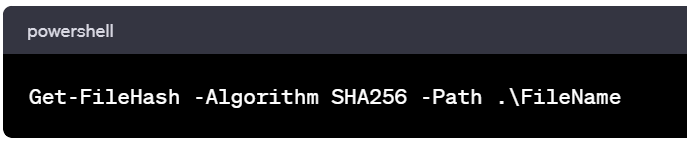
* Open PowerShell on the system where the file is located. You can do this by searching for "PowerShell" in the Start menu and selecting the application.

**Step 2:**

**Navigate to the File Directory:**

Use the ‘cd’ command to navigate to the directory where the file is located. For example:

**Code:** C:\Path\To\Directory

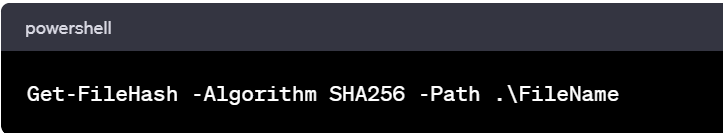


**Step 3:**

**Run the Get-FileHash Cmdlet:**

* Use the “Get-FileHash” cmdlet to generate the hash value for the file. Replace “FileName” with the actual name of the file you want to hash.

**Code:** Get-FileHash -Algorithm SHA256 -Path .\FileName



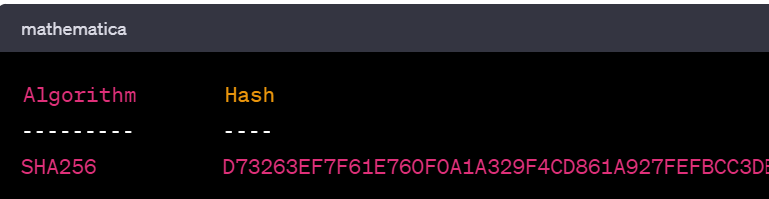
* Algorithm: Specify the hashing algorithm (e.g., SHA256).
* Path: Provide the path to the file.

**Step 4:**

**Review the Hash Output:**

* The cmdlet will generate a hash output, typically including the hash algorithm, hash value, and file path.

Example Output:



* The hash value is the string of characters following the "SHA256" label.

**Step 5:**

**Record the Hash Value:**

* Record the hash value in your documentation or incident response report. This value will be used for verification and analysis.

**Step 6:**

**Verification:**

* Optionally, you can verify the integrity of the hash value by comparing it with the hash generated from another reliable source or by re-running the Get-FileHash cmdlet at a later time.

Gathering file hashes using PowerShell provides a quick and efficient way to generate unique identifiers for files, aiding in incident response, forensic analysis, and integrity verification.

* + 1. Submit hash to community sourcesVirusTotal, Hybrid-Analysis, etc.

**Submitting Hash to Community Sources (e.g., VirusTotal, Hybrid-Analysis):**

Submitting a hash to community-driven platforms like VirusTotal and Hybrid-Analysis can provide valuable insights into the nature of the file. Follow these steps to submit a hash:

**Step 1:**

**Copy Hash Value:**

* Copy the hash value generated using PowerShell or another hashing tool.

**Step 2:**

**Visit VirusTotal:**

* Open your web browser and go to the [VirusTotal website](https://www.virustotal.com/gui/home/upload).

**Step 3:**

**Upload File or Search by Hash:**

* Paste the hash value into the search bar on the [VirusTotal website](https://www.virustotal.com/gui/home/upload) and press Enter.
* Alternatively, you can click on the "Search" tab and select "Search by hash."

**Step 4:**

**Review Results:**

* [VirusTotal](https://www.virustotal.com/gui/home/upload) will provide information about the file based on its hash.
* Analyze the results, including the detection ratio by various antivirus engines, behavioral analysis, and additional details.

**Step 5:**

**Visit Hybrid-Analysis:**

Open your web browser and go to the [Hybrid-Analysis website](https://www.hybrid-analysis.com/).

**Step 6:**

**Submit Hash:**

* Navigate to the "Search" section on Hybrid-Analysis.
* Paste the hash value into the search bar and press Enter.

**Step 7:**

**Analyze Results:**

* Hybrid-Analysis will display analysis results, including behavioral information, network activity, and more.

Submitting the hash to these community sources can help identify whether the file is associated with known threats, malware, or has been previously analyzed by security experts. Keep in mind that this process contributes to collective cybersecurity efforts by sharing threat intelligence within the community.

* + - 1. If community sources have seen the hash, note the malware characteristics.
      2. Depending on results – initiation of the [malware outbreak playbook](https://frsecure.com/malware-incident-response-playbook/) may be required.
  1. Isolate infected systems, do not power them off unless absolutely necessary.
     1. Describe how to isolate systems

**Isolating Infected Systems:**

Isolating infected systems is a crucial step to prevent the spread of malware and protect the overall network. Follow these steps to isolate an infected system:

**Step 1:**

**Network Isolation:**

* Physically disconnect the infected system from the network. Unplug the network cable or disable the wireless connection.
* Alternatively, configure network switches or firewalls to block communication to and from the infected system.

**Step 2:**

**Quarantine on the Network:**

* If possible, move the infected system to a designated quarantine network segment.
* Configure network devices to restrict the infected system's communication to essential services only.

**Step 3:**

**Endpoint Isolation:**

* Disable the infected system's network interfaces or put it in airplane mode to cut off all network connections.
* For virtual environments, suspend or isolate the virtual machine.

**Step 4:**

**Security Software:**

* Utilize endpoint security solutions to isolate the infected system. Many security tools offer features to isolate endpoints from the network.

**Step 5:**

**Firewall Rules:**

* Adjust firewall rules to block incoming and outgoing traffic from the infected system.
* Consider creating specific rules to limit communication to necessary services for analysis and remediation.

**Step 6:**

**Cloud-Based Solutions:**

* If applicable, use cloud-based security solutions to isolate and contain the infected system.

**Step 7:**

**Remote Access:**

* Disable remote access features on the infected system to prevent unauthorized connections.

**Step 8:**

**Monitor Isolation:**

* Regularly monitor the isolated system for any signs of unusual activity or attempts to reconnect to the network.

**Step 9:**

**Document Isolation Procedures:**

* Maintain documentation on the procedures for isolating infected systems to ensure a consistent and effective response.

**Step 10:**

**Coordinate with Incident Response Team:**

* If part of an incident response team, communicate the isolation status to team members for coordinated efforts.

Isolating infected systems is a critical measure to limit the impact of cybersecurity incidents and create a controlled environment for analysis, remediation, and investigation.

* + 1. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
       1. Describe how to preserve the system,

**Preserving Systems for Forensic Investigation:**

Preserving systems for forensic investigation is a crucial step in understanding the extent of a cybersecurity incident. Follow these steps to properly preserve systems for further forensic analysis:

**Step 1:**

**Document System Information:**

* Document key information about the system, including its hostname, IP address, operating system, hardware specifications, and any relevant context about its role in the network.

**Step 2:**

**Capture Memory Image:**

* Use forensic tools to capture a memory image of the system. Tools like Volatility can help create a snapshot of the system's RAM, which may contain valuable information about running processes and potential malware.

**Step 3:**

**Collect Disk Images:**

* Create forensic images of the system's disks using reliable imaging tools. This ensures that a bit-by-bit copy of the entire disk is preserved for analysis without altering the original data.

**Step 4:**

**Review Event Logs:**

* Examine system event logs for any unusual or suspicious activities. Record relevant log entries that might indicate the presence of malware or an ongoing attack.

**Step 5:**

**File System Analysis:**

* Analyze the Master File Table (MFT) and file system metadata for insights into file creation, modification, and access times. This can help identify malicious files or changes made by attackers.

**Step 6:**

**Deep Malware Scans:**

* Perform deep malware scans using reputable antivirus or anti-malware tools to identify and remove any known threats. Keep a record of detected malware and associated indicators of compromise (IoCs).

**Step 7:**

**Network Traffic Analysis:**

* Analyze captured network traffic logs to understand communication patterns, potential command and control activities, and data exfiltration attempts.

**Step 8:**

**Timeline Analysis:**

* Create a timeline of events related to the incident. Include timestamps for significant activities, such as the initial compromise, lateral movement, and data access.

**Step 9:**

**Hash Verification:**

* Verify the integrity of forensic images and collected data by calculating and comparing hash values. This ensures that the collected evidence remains unaltered.

**Step 10:**

**Secure Storage:**

* Store forensic images and evidence in a secure and tamper-evident manner. Use encrypted storage and access controls to prevent unauthorized tampering.

**Step 11:**

**Document Findings:**

* Document forensic findings, including identified artifacts, suspicious files, network connections, and any other relevant information. This documentation will be valuable for incident reports and future investigations.

Preserving systems for forensic analysis is essential for uncovering the details of a cybersecurity incident and strengthening defenses against future threats. Following a systematic and documented approach ensures the integrity and reliability of the forensic evidence.

* + - 1. Give examples of the best deep malware scanners
      2. Define MFT analysis

**Master File Table (MFT) Analysis in Forensic Investigation:**

Analyzing the Master File Table (MFT) is a crucial aspect of forensic investigation, providing insights into file system metadata and potential indicators of compromise. Here's a guide on how to use MFT analysis for further forensic investigation:

**Step 1:**

**Extract MFT Data:**

* Use forensic tools to extract the MFT data from the forensic image of the disk. Tools like The Sleuth Kit or commercial forensic suites can assist in this process.

**Step 2:**

**Understand MFT Structure:**

* Familiarize yourself with the structure of the MFT. The MFT is a database that contains records for each file and directory on an NTFS file system. Learn about attributes within MFT records, such as Standard Information, File Name, and Data attributes.

**Step 3:**

**Identify Timestamps:**

* Examine timestamps within MFT records, including the File Modified, File Accessed, and File Created timestamps. Anomalies or discrepancies in these timestamps may indicate suspicious activities.

**Step 4:**

**Analyze File Metadata:**

* Extract metadata from MFT records, including file names, sizes, and paths. Analyze this information to identify files of interest, unusual naming conventions, or hidden files.

**Step 5:**

**Spot Unusual File Attributes**:

* Look for unusual attributes within MFT records, such as alternate data streams or extended attributes. Uncommon attributes may be indicative of malicious activity or attempts to hide information.

**Step 6:**

**Identify File Relationships:**

* Explore relationships between files by analyzing parent-child associations. Determine if any files are related to known malware, unauthorized software, or tools used by attackers.

**Step 7:**

**Track File Movement:**

* Track the movement of files by analyzing MFT records. Identify instances where files were copied, moved, or deleted, as these actions may be relevant to the investigation.

**Step 8:**

**Uncover File Ownership and Permissions:**

* Examine MFT records for details about file ownership and permissions. Anomalies in ownership or unexpected changes in permissions may indicate unauthorized access or compromised accounts.

**Step 9:**

**Identify Deleted Files:**

* Use MFT analysis to identify records corresponding to deleted files. Deleted files may still leave traces in the MFT, providing valuable information about the timeline of events.

**Step 10:**

**Correlate with Other Artifacts:**

* Correlate MFT findings with other forensic artifacts, such as event logs, memory dumps, and network traffic. This holistic approach enhances the understanding of the incident and strengthens the overall investigation.

**Step 11:**

**Document Findings:**

* Document MFT analysis findings comprehensively. Include details about suspicious files, timestamps, relationships, and any other relevant information. This documentation is essential for creating a thorough forensic report.

MFT analysis is a powerful technique in forensic investigations, offering detailed insights into file system activities and aiding in the reconstruction of events leading to a cybersecurity incident. Careful examination of MFT data enhances the investigator's ability to uncover malicious activities and build a robust case for remediation and prevention.

1. Block all associated IoCs in email system components.
   1. URLs, domains, message-ID, etc. in spam filters, email based antimalware, etc.

**Blocking Associated Indicators of Compromise (IoCs) in Email System Components:**

To effectively mitigate the impact of a cybersecurity incident, blocking associated Indicators of Compromise (IoCs) in email system components is crucial. Here's a guide on how to block these IoCs to prevent further infiltration:

**Step 1:**

**Identify IoCs:**

* Based on the findings of the investigation, compile a list of identified IoCs, including but not limited to URLs, domains, and message IDs associated with the incident.

**Step 2:**

**Access Email System Components:**

* Log in to the email system components where the IoCs need to be blocked. This may include spam filters, email-based antimalware solutions, and other relevant security controls.

**Step 3:**

**Access Spam Filters:**

* Navigate to the settings or configuration panel of the spam filters in your email system. This is where you will implement rules to block specific URLs, domains, or message IDs.

**Step 4:**

**Implement Blocking Rules:**

* Create rules within the spam filters to block the identified IoCs. This involves adding entries for the URLs, domains, or message IDs associated with the incident.

**Step 5:**

**Configure Email-Based Antimalware:**

* Access the configuration settings of your email-based antimalware solution. Similar to spam filters, configure rules to block the identified IoCs, reinforcing protection against malicious activities.

**Step 6:**

**Utilize Threat Intelligence Feeds:**

* Integrate threat intelligence feeds into your email security infrastructure. Many threat intelligence platforms provide real-time updates on IoCs, enhancing your organization's ability to stay protected against emerging threats.

**Step 7:**

**Regularly Update Blocklist:**

* Stay proactive by regularly updating the blocklist within your email system components. As new IoCs emerge or threat landscapes evolve, maintaining an up-to-date blocklist is crucial for effective cybersecurity.

**Step 8:**

**Cross-Verification:**

* Cross-verify the effectiveness of the blocking rules by conducting tests or simulations. Ensure that the configured rules successfully prevent access to malicious URLs, domains, or message IDs.

**Step 9:**

**Document Configuration Changes:**

* Document all configuration changes made to block IoCs in email system components. This documentation is valuable for auditing purposes, incident response improvement, and knowledge sharing within the cybersecurity team.

**Step 10:**

**Continuous Monitoring:**

* Implement continuous monitoring of email traffic for any signs of suspicious activities. Regularly review logs and reports generated by the email security components to detect and respond to potential threats promptly.

**Step 11:**

**Collaborate with Threat Intelligence Providers:**

* Collaborate with external threat intelligence providers to enrich your IoC blocklist. Exchange information about emerging threats and IoCs to enhance your organization's overall cybersecurity posture.

By blocking associated IoCs in email system components, your organization strengthens its defenses and minimizes the risk of further incidents. This proactive approach, coupled with continuous monitoring and collaboration with threat intelligence sources, contributes to a robust cybersecurity strategy.

1. Block all associated IoCs in endpoint protection systems.

Blocking Associated Indicators of Compromise (IoCs) in Endpoint Protection Systems:

* 1. What is an endpoint protection system

An endpoint protection system, often referred to as endpoint security, is a security solution designed to safeguard individual computing devices, or endpoints, within a network. These endpoints can include desktops, laptops, mobile devices, and servers. The primary goal of an endpoint protection system is to detect, prevent, and respond to cybersecurity threats and attacks targeting these devices.

* 1. File hashes, malware identified, etc.

To effectively block associated Indicators of Compromise (IoCs) in endpoint protection systems, consider the following steps:

**Step 1:**

**Identify IoCs:**

* Compile a list of IoCs based on the findings of the incident investigation. This may include file hashes, malware signatures, registry changes, or any other indicators associated with the security incident.

**Step 2:**

**Access Endpoint Protection Console:**

* Log in to the console or management interface of your endpoint protection system. This is where you will configure rules and policies to block specific IoCs.

**Step 3:**

**Define Blocking Rules:**

* Create rules within the endpoint protection system to block the identified IoCs. Depending on the system, this could involve configuring policies to block specific file hashes, recognizing malware signatures, or preventing specific registry changes.

**Step 4:**

**Implement Real-Time Protection:**

* Ensure that real-time protection features are enabled within the endpoint protection system. Real-time protection actively monitors endpoint activities and prevents the execution of files or processes associated with known threats.

**Step 5:**

**Utilize Threat Intelligence Integration:**

* Integrate threat intelligence feeds into your endpoint protection system. This allows the system to receive updates on the latest IoCs and ensures that your organization is protected against emerging threats.

**Step 6:**

**Apply Behavioral Analysis:**

* Leverage behavioral analysis capabilities within the endpoint protection system. This enables the system to identify and block activities that deviate from normal behavior, even if specific IoCs are not explicitly known.

**Step 7:**

**Regularly Update Definitions:**

* Keep the endpoint protection system definitions up-to-date. Regularly update malware definitions, signatures, and any other components necessary for recognizing and blocking IoCs effectively.

**Step 8:**

**Conduct Periodic Scans:**

* Schedule periodic scans of endpoint devices to identify and eliminate any potential threats that might have evaded real-time protection. Ensure that these scans cover all critical areas of the endpoint.

**Step 9:**

**Monitor Quarantine and Incident Logs:**

* Monitor the quarantine and incident logs generated by the endpoint protection system. Review any actions taken by the system, such as blocking or quarantining files, and investigate further if needed.

**Step 10:**

**Document Configuration Changes:**

* Document all configuration changes made to the endpoint protection system for blocking IoCs. This documentation aids in auditing, compliance, and continuous improvement of incident response capabilities.

By blocking associated IoCs in the endpoint protection system, your organization enhances its ability to thwart cybersecurity threats at the device level. This multi-layered defense strategy, coupled with continuous monitoring and threat intelligence integration, contributes to a resilient cybersecurity posture.

Eradication

1. Preserve artifacts, systems, and relevant backups according to the sensitivity and scale of the incident. These may be important for future forensics.
   1. Retain copies of malicious emails and malware.
      1. Store in a safe location, password protected.
      2. What makes a safe location
   2. If rebuilding or replacing physical systems, preserve physical hard disks, solid state drives, or forensically sound images of those storage drives.
   3. If rebuilding or replacing virtual machines, preserve a copy, full (independent) snapshot, or a backup of the system.

**Preserving Artifacts, Systems, and Relevant Backups:**

Preserving artifacts, systems, and relevant backups is a crucial step in incident response, especially for future forensics and analysis. Follow these guidelines based on the sensitivity and scale of the incident:

**Step 1:**

**Identify Critical Artifacts:**

* Determine which artifacts are critical for forensic analysis. This may include system logs, registry entries, memory dumps, network traffic captures, and any other evidence related to the incident.

**Step 2:**

**Secure Systems:**

* Isolate affected systems to prevent further compromise. Ensure that these systems are secured and disconnected from the network to contain any potential threats.

**Step 3:**

**Take System Snapshots:**

* Take snapshots or images of affected systems using forensically sound methods. Tools like Forensic Imaging Software or built-in system imaging tools can be used to create a bit-for-bit copy of the system state.

**Step 4:**

**Document System Configuration:**

* Document the configuration of affected systems before making any changes. This includes hardware specifications, installed software, running processes, and user accounts.

**Step 5:**

**Preserve Memory Dumps:**

* Capture memory dumps from affected systems. Memory analysis can provide insights into active processes, injected code, and other runtime activities during the incident.

**Step 6:**

**Backup Relevant Logs:**

* Identify and back up relevant logs from affected systems. This includes system logs, application logs, security logs, and any other logs that may contain evidence of the incident.

**Step 7:**

**Secure Network Captures:**

* If network traffic captures are part of the artifacts, secure and store them for analysis. These captures can reveal communication patterns, lateral movement, and potential indicators of compromise.

**Step 8:**

**Assess Sensitivity:**

* Assess the sensitivity of the incident and the data involved. Classify artifacts and evidence based on their sensitivity and confidentiality. Treat highly sensitive information with extra precautions.

**Step 9:**

**Encrypt Preserved Data:**

* Encrypt preserved data to ensure its confidentiality and integrity. Implement strong encryption measures to protect the stored artifacts from unauthorized access.

**Step 10:**

**Store Backups Securely:**

* Securely store relevant backups, ensuring they are not overwritten or compromised. Backups may be critical for restoring systems to a known good state for further analysis.

**Step 11:**

**Maintain Chain of Custody:**

* Establish and maintain a chain of custody for all preserved artifacts. Document who handles the evidence, when, and for what purpose. This documentation is essential for legal and investigative purposes.

**Step 12:**

**Comply with Legal Requirements:**

* Ensure that the preservation process aligns with legal requirements and regulations. Consult legal counsel to understand any specific obligations related to preserving evidence.

**Step 13:**

**Consider Forensic Experts:**

* In cases of complex incidents or legal investigations, consider involving forensic experts who specialize in preserving and analyzing digital evidence.

Preserving artifacts, systems, and relevant backups in a meticulous and secure manner is fundamental to the success of future forensic investigations. By following these guidelines, your organization enhances its ability to conduct thorough analyses, understand the scope of the incident, and take appropriate remediation measures.

**Step 14:**

**Retaining Copies of Malicious Emails and Malware:**

**Store in a Safe Location:**

* Retain copies of malicious emails and malware in a safe and secure location, ensuring that they are password-protected and encrypted to prevent unauthorized access.

**Step 15:**

**What Makes a Safe Location:**

* A safe location is one that provides controlled access and protects the stored data from unauthorized disclosure. This could be a secure server, encrypted external storage, or a designated folder with restricted access. Encryption ensures an additional layer of security.

**Step 16:**

**Preserving Physical Storage Drives:**

* If rebuilding or replacing physical systems, retain physical hard disks, solid-state drives, or forensically sound images of those storage drives. This ensures that the original state of the system can be reconstructed for forensic analysis.

**Step 17:**

**Preserving Virtual Machines:**

* If rebuilding or replacing virtual machines, preserve a copy, full (independent) snapshot, or a backup of the system. This allows for the recreation of the virtual environment in its original state for forensic examination.

Preserving these elements in a secure manner is essential for maintaining the integrity and authenticity of evidence during forensic investigations. Ensure that the retained data is not altered, and access is restricted to authorized personnel to maintain the chain of custody and uphold the forensic soundness of the investigation.

1. Preserve any volatile data that may have been collected during the identification and containment phases.
   1. What makes data volatile
   2. This may include log files, backups, malware samples, memory images, etc.

**Preserving Volatile Data:**

What Makes Data Volatile: Volatile data refers to information that is stored temporarily in a system's memory (RAM) and is typically lost when the system is powered down or restarted. This type of data is dynamic and can change rapidly. Examples include running processes, open network connections, and system logs in memory.

**Preserving Volatile Data:**

* Preserve any volatile data that may have been collected during the identification and containment phases. This includes but is not limited to:
* Log Files: Capture logs generated during the incident to understand the sequence of events.
* Backups: If any volatile backups were created, ensure they are preserved for analysis.
* Malware Samples: Retain samples of identified malware for further examination.
* Memory Images: Capture memory images for analysis, providing insights into the state of the system during the incident.

Preserving volatile data is crucial as it allows forensic investigators to analyze the state of the system at the time of the incident. This information aids in understanding the tactics, techniques, and procedures (TTPs) employed by malicious actors, contributing to a comprehensive forensic examination.

1. Once all relevant data, equipment, and/or systems have been preserved, replace or rebuild systems accordingly.

**Replacing or Rebuilding Systems:**

**How to Replace or Rebuild?**

**System Replacement:**

**Physical Systems:**

* If dealing with physical hardware, replace compromised components, ensuring they are free from any potential compromise.
* Install a fresh operating system, applications, and restore data from clean backups.
* Implement security best practices during the rebuild process, such as applying the latest security patches.

**Virtual Machines:**

* For virtual machines, deploy new instances from clean templates or images.
* Ensure that virtual machine configurations adhere to security standards.
* Reinforce security measures during the setup, including access controls and network configurations.

**Rebuilding:**

**Physical Systems:**

* If rebuilding physical systems, wipe the hard drives or solid-state drives securely to remove any remnants of compromised data.
* Install a fresh operating system and applications.
* Restore clean backups of data and configurations.

**Virtual Machines:**

* Rebuild virtual machines by resetting them to a known-good state.
* Apply security configurations and policies to prevent similar incidents in the future.
* Ensure that the virtual machine images are sourced from secure and verified repositories.

**Post-Replacement/Rebuilding Actions:**

* Security Verification: Perform thorough security checks to ensure that the replaced or rebuilt systems meet security standards.
* Monitoring: Implement continuous monitoring to detect and respond to any suspicious activities.
* Incident Documentation: Document the replacement or rebuilding process for future reference and analysis.

Replacing or rebuilding systems is a critical step in restoring the integrity of the environment and preventing the recurrence of security incidents. It involves creating a secure and clean computing environment that aligns with established security protocols.

Recovery

1. Remediate any vulnerabilities and gaps identified during the investigation.
2. Reset passwords for all impacted accounts and/or create replacement accounts and leave the impacted accounts disabled permanently.

**Resetting and Replacing Passwords:**

**Step 1:**

**Resetting Passwords:**

**Impacted Accounts:**

* Reset passwords for all accounts that were identified as compromised during the incident.
* Use a strong, unique password for each account to enhance security.
* Communicate the password reset to users through secure channels, avoiding potential phishing risks.

**Step 2:**

**Creating Replacement Accounts:**

**Disabled Accounts:**

* Permanently disable compromised accounts to prevent any unauthorized access.
* Create replacement accounts for affected users with new credentials.
* Ensure that replacement account credentials follow robust password policies.

**Step 3:**

**Security Considerations:**

**Multi-Factor Authentication (MFA):**

* Encourage or enforce the use of multi-factor authentication for enhanced account security.
* Configure MFA settings for both existing and replacement accounts.

**Step 4:**

**Communication:**

**User Notification:**

* Notify affected users about the password reset and account replacement.
* Provide clear instructions on how to securely access their new accounts.

**Step 5:**

**Documentation:**

**Record Keeping:**

* Maintain detailed records of the password reset process, including the date, time, and individuals involved.
* Keep a record of disabled accounts and the creation of replacement accounts.

**Step 7:**

**Post-Action Verification:**

**Account Access Review:**

* Conduct a review to ensure that only authorized users have access to the new accounts.
* Monitor account activities to detect any unusual behavior after the reset.

Resetting passwords and creating replacement accounts are crucial steps to regain control over compromised credentials and prevent unauthorized access. These actions contribute to strengthening the overall security posture of the organization.

1. Continue to monitor for malicious activity related to this incident for an extended period.
   1. Alerts should be configured to aid in quick detection and response.

**Monitoring for Malicious Activity**:

**Step 1:**

**Setting Up Alerts:**

**Configuration Steps:**

* Utilize security tools or platforms that support alert configurations.
* Access the settings menu within the chosen tool for alert management.

**Step 2:**

**Selecting Alert Criteria:**

* Identify specific criteria for triggering alerts, such as unusual login activities.
* Customize alert parameters based on the organization's security requirements.

**Step 3:**

**Thresholds and Sensitivity:**

* Set appropriate thresholds and sensitivity levels to avoid false positives.
* Adjust sensitivity based on the organization's risk tolerance and security priorities.

**Examples of Anomalous Behavior Alerts:**

**Unusual Login Locations:**

* Create alerts for login activities from locations not typical for the user.
* Specify criteria, such as geographically distant IP addresses.

**Abnormal Access Times:**

* Configure alerts for logins during non-standard hours or outside regular patterns.
* Consider time-based parameters to identify abnormal access times.

**Multiple Failed Login Attempts:**

* Implement alerts for an excessive number of failed login attempts within a defined timeframe.
* Define thresholds for recognizing potential brute-force attacks.

**Unusual File Access:**

* Extend alerts to detect anomalies in file access, especially sensitive or critical data.
* Specify criteria for identifying unexpected or unauthorized file interactions.

**Step 4:**

**Continuous Review and Adjustment:**

**Regular Alert Review:**

* Establish a routine for reviewing generated alerts.
* Investigate any alerts triggered by anomalous behavior promptly.

**Step 5:**

**Feedback Loop for Tuning:**

* Solicit feedback from security analysts regarding the relevance of alerts.
* Fine-tune alert settings based on evolving threat landscapes and incident patterns.

**Step 6:**

**Incident Response Drills:**

* Conduct simulated incident response drills to validate the effectiveness of alerting mechanisms.
* Use insights from drills to further refine alert configurations.

Setting up alerts involves configuring security tools to detect specific patterns indicative of malicious activity. By defining clear criteria and adjusting sensitivity levels, organizations can ensure timely detection and response to anomalous behavior. Regular review and adjustment of alert settings contribute to an adaptive and effective security posture.

1. If financial loss was incurred, consult cybersecurity insurance.

Lessons Learned

1. Conduct a meeting after the incident to discuss the following:
   1. What things went well during the investigation?
   2. What things did not go well during the investigation?
   3. What vulnerabilities or gaps in the organization’s security status were identified?
      1. How will these be remediated?
   4. What further steps or actions would have been helpful in preventing the incident?
   5. Do modifications need to be made to any of the following:
      1. Application security
      2. Operating System and/or Application patching procedures
      3. Employee, IT, or CSIRT training
      4. Email filtering policies
      5. Multifactor Authentication
      6. Email retention policies
      7. Sensitive information policies and procedures related to email
2. Create and distribute an incident report to relevant parties.
   1. A primary, and more technical, report should be completed for the CSIRT.
   2. An executive summary should be completed and presented to the management team.

**Post-Incident Meeting Agenda:**

**Incident Overview:**

* Briefly recap the incident, providing context on the type, scope, and impact.
* Summarize the key facts surrounding the incident.

**Timeline Review:**

* Present a detailed timeline of events leading up to and during the incident.
* Discuss the sequence of actions taken by the incident response team.

**Root Cause Analysis:**

* Conduct a thorough analysis to identify the root cause of the incident.
* Discuss any vulnerabilities or weaknesses in existing security measures.

**Response Effectiveness:**

* Evaluate the effectiveness of the response strategy and actions taken.
* Discuss areas of success and opportunities for improvement.

**Communication Assessment:**

* Review internal and external communication efforts during the incident.
* Identify strengths and weaknesses in communication protocols.

**Lessons Learned:**

* Discuss key lessons learned from the incident.
* Explore how these lessons can inform future incident response strategies.

**Documentation Review:**

* Examine the documentation generated during the incident.
* Ensure that incident details, response actions, and outcomes are well-documented.

**Feedback and Suggestions:**

* Encourage team members to provide feedback on the incident response process.
* Solicit suggestions for enhancing future incident response capabilities.

**Training and Awareness:**

* Discuss the need for additional training or awareness programs based on the incident.
* Identify areas where team members can further enhance their skills.

**Policy and Procedure Review:**

* Evaluate existing cybersecurity policies and procedures.
* Discuss any necessary updates or modifications to enhance security measures.

**Preventive Measures:**

* Brainstorm preventive measures to reduce the likelihood of similar incidents.
* Explore strategies for strengthening the organization's overall security posture.

**Post-Incident Reporting:**

* Discuss requirements and timelines for post-incident reporting.
* Ensure that all relevant stakeholders are informed of incident details.

**Recovery and Resilience:**

* Assess the organization's recovery efforts and resilience post-incident.
* Identify areas for improving recovery capabilities and minimizing future impact.

**Continuous Improvement Plan:**

* Develop an action plan for continuous improvement in incident response.
* Outline specific steps and timelines for implementing identified enhancements.

**Closure and Recognition:**

* Acknowledge the efforts of the incident response team.
* Confirm the closure of the incident and transition back to normal operations.

Conducting a post-incident meeting is crucial for learning from the incident, improving response capabilities, and fortifying the organization against future threats. The agenda should be comprehensive, covering various aspects of the incident response lifecycle

**QUESTION AND ANSWER!**