**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

|  |  |
| --- | --- |
| **Date:**  06-29-2024 | **Entry:**  2024-001 |
| Description | This journal entry documents a ransomeware incident at a small U.S. healthcare clinic. The incident, triggered by a phishing attack, resulted in the encryption of critical files, rendering them inaccessible and causing significant disruption to business operations. The attackers demanded a ransom in exchange for the decryption key. |
| Tool(s) used | * **SIEM (Security Information and Event Management):** To monitor and analyze security alerts in real-time. * **IDS (Intrusion Detection System):** To detect malicious activities and anomalies in the network. * **Malware Analysis Tools:** To dissect malicious activities and anomalies in the network. * **Malware Analysis Tools:** To dissect and understand the behavior of the ransomware. * **Backup and Recovery Tools:** To restore encrypted files if backups are available. * **Email Filtering Solutions:** To prevent phishing emails from reaching employees. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An organized group of unethical hackers, known for targeting healthcare and transportation sectors, orchestrated the attack.   * **What** happened?   Employees reported being unable to access critical files and software needed for their tasks. A ransom note appeared on their screens, stating that the company’s files were encrypted and demanding a substantial sum of money for the decryption key. This led to a complete shutdown of business operations.   * **When** did the incident occur?   The incident occurred on a Tuesday at approximately 9:00 a.m.   * **Where** did the incident happen?   The incident took place at a small primary-care healthcare clinic in the U.S.   * **Why** did the incident happen?   The incident was triggered by targeted phishing emails sent to multiple employees. These emails contained a malicious attachment which, when downloaded, installed ransomware that encrypted the clinic’s critical files. |
| Additional notes | * Investigate why the employees failed to recognize the phishing emails. Determine if there is a lack of or inadequate cybersecurity awareness training within the organization. Identify the specific employee(s) who downloaded the attachment and assess if they are new hires or lack sufficient training. * Conduct a detailed analysis of the malware in a controlled laboratory environment to understand its behavior and develop mitigation strategies. * Review recent security audits to identify and overlooked vulnerabilities or areas needing improvement. * Implement or enhance a comprehensive cybersecurity awareness training program for all employees to prevent future incidents. This should include phishing simulations and regular updates on emerging threats. * Ensure the organization has a robust incident response plan and regularly test it through drills and simulations. * Consider implementing multi-factor authentication (MFA) to add an extra layer of security. * Evaluate the current backup strategy and ensure that backups are regularly performed and stored securely offsite. |

|  |  |
| --- | --- |
| **Date:**  06-30-2024. | **Entry:**  2024-002 |
| Description | Initial analysis and response to suspicious file download incident. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An employee who received and opened a suspicious email attachment.   * **What** happened?   Malicious payload executed on the employee’s computer upon opening the password-protected spreadsheet file.   * **When** did the incident occur?   Timeline:  **1:11 p.m**.: Email with attachment received.  **1:13 p.m**.: File downloaded and opened by the employee.  **1:15 p.m**.: Unauthorized executables created on the employee’s computer.  **1:20 p.m**.: Intrusion detection system alerted the SOC.   * **Where** did the incident happen?   On the employee’s computer within the corporate network.   * **Why** did the incident happen?   Due to the employee opening a malicious file attachment, leading to unauthorized code execution. |
| Additional notes | The incident underscores the importance of email security awareness and proper handling of suspicious attachments.  Use of VirusTotal to further investigate IoCs associated with the malicious file hash.  <update this> |

|  |  |
| --- | --- |
| **Date:**  06-30-2024 | **Entry:**  2024-003 |
| Description | A phishing attempt was detected involving a malicious email with an attached executable file named “bfsvc.exe”. The file, once downloaded was identified as a known malicious malware called Flagpro, used by the BlackTech group. The phishing email was sent to the HR department of Inergy. |
| Tool(s) used | Virus Total |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? The phishing email was sent by an unknown attacker using the alias "Def Communications" from the IP address 114.114.114.114. * **What** happened? An employee received a phishing email claiming to be from a job applicant. The email contained an attached executable file, "bfsvc.exe," which was password-protected. The attachment was identified as malicious and known as Flagpro malware. * **When** did the incident occur?   The phishing email was sent on Wednesday, July 20, 2022, at 09:30:14 AM. The alert and investigation were conducted on 06-30-2024.   * **Where** did the incident happen? The incident involved an email sent to the HR department at Inergy, with the targeted employee being the recipient. * **Why** did the incident happen? The phishing attempt aimed to deliver the Flagpro malware, potentially to compromise the target's system and exfiltrate sensitive information or disrupt operations. |
| Additional notes | * The attachment "bfsvc.exe" was identified using its SHA256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * The email content appeared legitimate but contained several grammatical errors, which could be a red flag for phishing attempts. * The malware Flagpro has been used by the BlackTech group since at least October 2020, indicating a persistent threat actor. * Immediate action includes isolating the affected machine, scanning for further malicious activities, and educating the recipient on phishing email detection. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

### Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

|  |
| --- |
| Reflections/Notes: Record additional notes. |