**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:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number.   1. **10/21/2024** |
| Description | Provide a brief description about the journal entry.  This journal entry documents the initial findings of a security incident that occurred at a small U.S. healthcare clinic. On Tuesday morning, at approximately 9:00 a.m., several employees reported being unable to access critical medical records and files due to a ransomware attack. A ransom note demanding payment in exchange for a decryption key was displayed on affected computers. The attackers likely gained access to the network through phishing emails containing malicious attachments, which deployed ransomware upon download. The clinic’s business operations were significantly impacted, and technical assistance has been requested. |
| Tool(s) used | List any cybersecurity tools that were used.  None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An organized group of unethical hackers targeted the healthcare clinic through phishing emails.   * **What** happened?   A ransomware attack was initiated after an employee downloaded a malicious attachment from a phishing email. The ransomware encrypted critical files, disrupting business operations and displaying a ransom note demanding payment.   * **When** did the incident occur?   The incident occurred on Tuesday morning at approximately 9:00 a.m.   * **Where** did the incident happen?   The incident happened at a small healthcare clinic in the United States, specifically targeting their internal network and employee computers.   * **Why** did the incident happen?   The incident occurred because an employee unknowingly downloaded a malicious attachment from a phishing email, giving the attackers access to the clinic's network and allowing them to deploy ransomware. |
| Additional notes | Include any additional thoughts, questions, or findings.   The clinic's operations were fully disrupted due to the inability to access critical patient records.   Immediate next steps should involve isolating affected systems, identifying the type of ransomware, and consulting with external cybersecurity professionals for potential decryption or mitigation strategies. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 07**/20/2022  2 |
| Description | Provide a brief description about the journal entry  This entry documents the investigation and resolution of a phishing incident involving a suspicious email with a malicious attachment. The investigation confirmed that the attachment, identified by its SHA256 hash, was indeed malicious. The incident involved suspicious sender details and indicators of a phishing attempt, including grammatical errors and a prompt to open a password-protected file. Appropriate measures were taken to contain the threat, and the incident has been documented in accordance with the organization's incident response playbook. |
| Tool(s) used | List any cybersecurity tools that were used.  None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   Unethical actors targeting the organization via phishing.   * **What** happened?   An employee received a phishing email with a malicious attachment.   * **When** did the incident occur?   July 20,2022   * **Where** did the incident happen?   Occurred on the organization's network   * **Why** did the incident happen?   Likely social engineering to gain access to sensitive information |
| Additional notes | Include any additional thoughts, questions, or findings.   **Potential Gaps in User Awareness**: The employee downloaded a suspicious attachment despite possible indicators of phishing. This highlights a need for ongoing security awareness training, emphasizing how to recognize phishing attempts and the risks of downloading unknown attachments.   **Consideration for Blocking Similar Domains**: Given the suspicious sender domain (76tguyhh6tgftrt7tg.su), consider adding similar domains to the organization’s email filtering rules to preemptively block future phishing attempts.   **Further Analysis of Malicious Hash**: It may be beneficial to submit the hash to additional threat intelligence sources to identify any related incidents or IP addresses, which could aid in future threat hunting efforts.   **Recommendation for Enhanced Monitoring**: Increased monitoring of similar phishing patterns can help detect and mitigate related incidents promptly. |

|  |  |
| --- | --- |
| **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. |

|  |  |
| --- | --- |
| **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. |