**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:** 7/24/2023 | **Entry:** 1 |
| Description | Ransomware attack occurred on a small U.S. health care clinic. Targeted phishing emails were used to deploy malicious malware onto machines, escalate privilege, and encrypt critical patient files. |
| Tool(s) used | None. |
| The 5 W's | * **Who**: An organized group of unethical hackers who target organizations in healthcare and transportation industries. * **What**: A ransomware attack was conducted on critical patient files, causing business operations to shut down. * **When**: Incident occurred on Tuesday at 9:00 a.m. * **Where**: Incident occurred at a small U.S. health clinic specializing in delivering primary-care services. * **Why**: The incident occurred because the organized group of unethical hackers were able to gain privileged access by conducting a campaign of targeting phishing emails on employees. Once the employees ran the malicious program in the email, the hackers were able to escalate their privileges to view and encrypt patient files, rendering the business inoperable. The attacker’s goal was to profit as the ransom note demanded a large sum of money and in return, they will provide the decryption key for the files. |
| Additional notes | 1. **Note:** Deploy security awareness training for all emails. Email phishing campaigns can appear legitimate but often times they can be flagged with common sense. 2. **Question:** Can some organizations reverse the encryption and decrypt themselves? Drawbackl of this would be time and money expended but maybe there are some scenarios (like a good tool or team) where this is feasible. 3. **Question:** They must pay the ransom or report it to law enforcement, correct? Then maybe law enforcement can expend their resources to help? |

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

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