**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:**  2024-09-05 | **Entry:**  **1** |
| Description | A small U.S. health care clinic experienced a security incident involving a ransomware attack. The attack began at approximately 9:00 a.m. on a Tuesday morning, disrupting business operations by encrypting the clinic's critical files. Employees were unable to access medical records and other essential systems. |
| Tool(s) used | No cybersecurity tools were directly mentioned in the scenario, but incident response tools like SIEM (Security Information and Event Management), antivirus/malware removal software, and email filtering systems could be involved in future responses. |
| The 5 W's | * **Who**: An organized group of unethical hackers, targeting the healthcare industry, caused the incident. The phishing email was directed at clinic employees. * **What**: The clinic’s computer systems were infected by ransomware via a phishing email, which led to encryption of critical files. A ransom note was left demanding payment for the decryption key. * **When**: The incident occurred on a Tuesday morning around 9:00 a.m., severely impacting business operations. * **Where**: The incident took place at a small U.S. health care clinic specializing in primary-care services. * **Why**: The incident happened due to successful phishing attacks, which allowed malware to be installed on the employees' computers. The attackers aimed to extort money by encrypting the clinic’s data and demanding a ransom in exchange for the decryption key. |
| Additional notes | This incident highlights the importance of phishing awareness and employee training, as well as the need for robust email filtering systems. A more detailed investigation will be needed to determine if there are further vulnerabilities in the network and how to prevent similar incidents in the future. |

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