**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: 3/13/2024** | **Entry: 01** | | |
| --- | --- | --- | --- |
| Description | This entry details a ransomware attack on Tuesday at 9:00 A.M. at a small U.S. health care clinic. | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **A group of unethical hackers** * **The attachment ran a ransomware program that encrypted all of the clinic’s files.** * **3/12/24 Tuesday @ 9am** * **On site at the clinic** * **This incident happened because the staff were not aware of the malicious attachment on the email.** | | |
| Additional notes | Perhaps training on how to spot phishing emails could be beneficial for preventing futre phishing attacks. | | |

| **Date:**  03/28/2024 | **Entry:02**  Record the journal entry number. | | |
| --- | --- | --- | --- |
| Description | This entry details a phishing alert and the use of a playbook to respond to the alert | | |
| Tool(s) used | Phishing incident response playbook | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: A malicious individual * **What:** A questionable email with a file attachment was sent to HR * **When** Wednesday, July 20, 2022 09:30:14 AM * **Where:** On site * **Why:** The HR department was tricked as to the legitimacy of the email. | | |
| Additional notes | The phishing attempt I think is legitimate because the attached file has a .exe extension rather than a .doc extension indicating that it is a program that is to be ran. | | |

| **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. |
| --- |