**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:**  06/04/2024 | **Entry:1** | | |
| --- | --- | --- | --- |
| Description | This is the documentation of a journal entry of a cybersecurity incident at a healthcare clinic. | | |
| Tool(s) used | No tools were used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** An organized group of unethical hackers. * **What**: Ransomware security incident * **When**: Tuesday at 9:00 am * **Where**: Healthcare clinic in the USA * **Why:** The group of unethical hackers sent malicious emails to several employees of the company and were able to gain access to the company’s network. Once they gained access to the network they deployed Ransomware and encrypted the critical files. The company was unable to access critical patient data, causing major disruption in business operations. | | |
| Additional notes | What is the option for the company rather than paying ransom money?  What are the preventive measures for them to avoid such 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**: | | |
| 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 | This is a documentation of the journal entry about the security incident at the health care clinic on Tuesday at 9 am. | | |
| Tool(s) used | No tool was used. | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Organized group of Unethical Hackers. * **What**: Ransomware security incident * **When**: Tuesday At 9:00 am * **Where**: Health care clinic * **Why**: | | |
| 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. |
| --- |