**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:**  Tuesday, 9:00am | **Entry:**  001 |
| Description | Ransomware attack on US health care clinic specializing in delivering primary care services |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.  Unethical hackers known to target healthcare organizations encrypted all company files and are demanding a large sum of money for the decryption key, all employees received a ransom note and all business operations had to shut down. This incident happened on Tuesday at 9am at a US health care clinic. This incident originated from a phishing email, that was sent to several employees, that contained a malicious attachment that installed malware onto he employee’s computer once it was downloaded. |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  N/A | **Entry:**  002 |
| Description | Malicious attachment on email was downloaded onto the system by employee |
| Tool(s) used | SHA256 hashing, Virus total |
| The 5 W's | Capture the 5 W's of an incident.  The incident was caused by an employee at the financial services company who downloaded and opened a suspicious email attachment. The incident occurred when the employee received an email containing a password-protected spreadsheet file and used the provided password to open it. This action triggered the execution of a malicious payload on their computer. The incident took place on the employee’s device within the organization’s network. It happened because the employee failed to recognize the email as a phishing attempt, highlighting a gap in email security awareness or training. |
| 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. |