**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:**  21st April, 2025 | **Entry:**  1 |
| Description | An incident occurred on Tuesday at 09:00 hours, the hospital systems were exploited by hackers encrypting files and asking for money rescue for unlocking all systems. |
| 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?   **Hackers**   * **What** happened?   information seizure and ransom payment   * **When** did the incident occur?   Tuesday at 09:00   * **Where** did the incident happen?   **Hospital systems**   * **Why** did the incident happen?   **There is not and IDS, XDR and the personnel have not trained about the risk of attachment files.** |
| Additional notes | Why there is not a IDS implement on hospital systems? |

|  |  |
| --- | --- |
| **Date:**  3 May 2025 | **Entry:**  2 |
| Description | An alert has been triggered due to an email that was sent to an employee email. The file is protected spreadsheet, and the password was provided in the email body, the malicious code was executed when the employee opens the file with the password. |
| Tool(s) used | Virutstotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   **An employee**   * **What** happened?   **A malicious code was executed**   * **When** did the incident occur?   **Business hours**   * **Where** did the incident happen?   **Employee’s computer**   * **Why** did the incident happen?   **The employees don’t have cybersecurity fundamentals** |
| Additional notes | The employees must receive cybersecurity fundamentals training.  The IPS must be updated with the most recently KB |

|  |  |
| --- | --- |
| **Date:**  3 May 2025 | **Entry:**  3 |
| Description | A phishing alert was triggered due to a suspicious file being downloaded on an employee’s computer. The hash file was reviewed on Virustotal and is known by the community. Other characteristics what confirm the analysis was going into the correct way were the grammar in the email body and subject. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   **Employee**   * **What** happened?   **Alert triggered due to suspicious file**   * **When** did the incident occur?   **Business hours**   * **Where** did the incident happen?   **Employee’s computer**   * **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. |