**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:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number.  *Incident Journal Entry 000 – July 30th, 2025* |
| Description | Provide a brief description about the journal entry.  *Security Incident Details about a ransomware incident at a US health care clinic that occurred via phishing* |
| Tool(s) used | List any cybersecurity tools that were used.  *According to the information given, no tools were used. There are tools in Kali Linux that maybe useful for finding a way to unencrypt the files. If the company was running in a more virtual environment, all of the computers could be booted from an earlier snapshot (after performing a ram and storage dump to analyze the malware for future prevention).* |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *A group of unethical hackers that target healthcare and transportation organizations* * **What** happened? *Attackers gained access to company’s network via a phishing email that contained a malicious attachment and installed malware.* * **When** did the incident occur? *Tuesday, July 22nd, 2025 @9:00am* * **Where** did the incident happen? *It happened at the healthcare company via targeted phishing emails which encrypted critical files when the employee(s) downloaded the file(s)* * **Why** did the incident happen? *The unethical group of hackers wants money and used the encryption of the critical files to demand ransom for their restoration (i.e. decryption and regain access)* |
| Additional notes | Network Booting and running Operating Systems in Virtual Environments such as VMware or Hyper-V or VirtualBox would allow snapshots of computers at certain regular intervals, which would allow all infected systems to be restored to a previous point where the malicious files weren’t downloaded. Depending on how far back the restore/save point is, will determine how many files or file edits will be lost |

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