**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:** **14.08.2025** | **Entry: #1** |
| Description | Malware(ransomware) downloaded by phishing. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who:** An organized group of unethical hackers. * **What**: A ransomware encrypted organization’s files. * **When**: on Tuesday at 9.00 a.m. * **Where**: Small U.S. healthcare clinic. * **Why**: Some employees received a phishing email with an attachment that downloads a malware. When an employee installed the malware, unethical hackers gained access to their computer and deployed their ransomware encrypting critical files in the system. Their motivation seems to be financial since the ransomware left a note demanding large amount of money in exchange for decryption key. |
| Additional notes | 1. How could a company prevent an incident like this from occurring? |

|  |  |
| --- | --- |
| **Date:** **19.08.2025** | **Entry: #2** |
| Description | Malware downloaded by phishing email attachment. |
| Tool(s) used | VirusTotal, SHA256 Hashing |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Unknown malicious actor * **What**: Multiple unauthorized executable files are created on the computer. * **When**: 1:11 – 1:20 p.m. * **Where**: A financial services company * **Why**: An employee received a phishing email with an attachment. The attachment was a password-protected spreadsheet file and password was provided in the email. The employee downloaded and entered the password to open the file. After that, malicious payload was executed on the computer. |
| Additional notes | File name: bfsvc.exe  SHA-256 : 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b  Can VirusTotal make mistakes?  Can a file not have a hash value in VirusTotal? |

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