**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  05/06/2025 | **Entry: 1** |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None |
| The 5 W's | * **Who** An organized group of unethical hackers * **What** A ransomware security incident * **When** Tuesday 900 a.m. * **Where** At a health care company * **Why** The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes | 1. How could the health care company prevent an incident like this from  occurring again?  2. Should the company pay the ransom to retrieve the decryption key? |

|  |  |
| --- | --- |
| **Date:**  05/06/2025 | **Entry: 2** |
| Description | Analyzing a packet capture file |
| Tool(s) used | **Wireshark** |
| The 5 W's | * **Who** N/A * **What** N/A * **When** N/A * **Where** N/A * **Why** N/A |
| Additional notes | Wireshark is new to me, but I can see how it would be a valuable tool to use to understand network traffic. |

|  |  |
| --- | --- |
| **Date:**  05/07/2025 | **Entry: 3** |
| Description | Capturing my first packet |
| Tool(s) used | TCPDump |
| The 5 W's | * **Who** N/A * **What** N/A * **When** N/A * **Where** N/A * **Why** N/A |
| Additional notes | Learning the command-line interface was interesting. I look forward to more insight into capturing network packets. |

|  |  |
| --- | --- |
| **Date:**  05/07/2025 | **Entry: 4** |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this activity, I used VirusTotal to analyze a file  hash, which was reported as malicious**.** This incident occurred in the Detection and Analysis phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat. |
| The 5 W's | * **Who** Unknown Malicious Hacker * **What** An email was sent to an employee with a file attachment with the SHA-256 file hash of “54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When** At 1:20pm * **Where** An employee's computer at a financial services company * **Why** An employee was able to download and execute a malicious fiie * attachment via e-mail. |
| Additional notes | Need to prevent future incidents by improving security awareness training |

|  |  |
| --- | --- |
| **Date:** | **Entry: 5** |
| Description | Provide a brief description of 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 of 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. |