**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** 28.11.2023 | **Entry: #1** |
| Description | Documenting a ransomware attack on a small U.S. health care clinic |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A group of unethical hackers * **What** happened? Ransomware attack * **When** did the incident occur? On Tuesday at 9am * **Where** did the incident happen? At a small U.S. health care clinic * **Why** did the incident happen? Hackers gained access to the company’s system using a phishing email and deployed ransomware which encrypted all data. The attacker’s motivation is financial gain. |
| Additional notes | What did the email they sent look like? Why did the employee not spot a phishing attack? Is it possible to decrypt the data? |

|  |  |
| --- | --- |
| **Date:** 29.11.2023 | **Entry: #2** |
| Description | Inspecting a malicious file |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Anonymous sender * **What** happened? Employee opened a malicious file from an email * **When** did the incident occur? Today at 1:11pm * **Where** did the incident happen? At a financial services company * **Why** did the incident happen? |
| Additional notes |  |

|  |  |
| --- | --- |
| **Date:** 29.11.2023 | **Entry: #3** |
| Description | Inspecting a phishing email containing an attachment |
| Tool(s) used | Phishing playbook v1.0 |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? Unknown person posing as a job seeker * **What** happened? A phishing email with a malicious file was received and opened by an employee * **When** did the incident occur? Morning of July 20 * **Where** did the incident happen? At a financial services company * **Why** did the incident happen? The attacker wanted to gain access to the system |
| Additional notes |  |

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