**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry: 1**  06/26/2023 |
| Description | A small U.S. health care clinic experienced a security incident that has severely disrupted their business operations. This appears to be a ransomware attack from an experienced group of unethical hackers as several employees have reported their files to be encrypted and new ransom notes appearing on their devices. |
| Tool(s) used | * Email filters * Firewall filters and network port filtering * File recovery and backup tools * SEIM tools * Network protocol analyzers |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   + An organized group of unethical hackers who are known to target healthcare and transportation companies * **What** happened?   + The attackers sent several targeted phishing emails which contained a malicious file attachment that installed malware on the employee’s device when downloaded. This led to employees reporting that they were unable to use their computers to access files like medical records. Business operations were then shut down because employees were not able to access files or software needed to complete their jobs. There were reports of ransom notes being displayed on employee’s computers demanding payment in exchange for decryption keys. * **When** did the incident occur?   + Tuesday, approximately 9:00 a.m. * **Where** did the incident happen?   + A small U.S. health care clinic specializing in delivering primary-care services * **Why** did the incident happen?   + The attackers were able to bypass the current security controls in place to filter emails and validate attachments being sent through email |
| Additional notes | Include any additional thoughts, questions, or findings. |
|  | The phishing attacks were reported to be targeted, meaning that they were personalized for the intended receiver. The organization may need to review and update its policies on employee social media usage related to business operations. |

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