**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:**  10/21/2023 | **Entry:**  001 |
| Description | Initial incident documentation for healthcare clinic ransomware attack. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *Unethical hackers through targeted phishing emails.* * **What** happened? *Ransomware attack leading to the encryption of critical files, disrupting business operations.* * **When** did the incident occur? *Tuesday morning at approximately 9:00 a.m.* * **Where** did the incident happen? *U.S. healthcare clinic specializing in primary care services.* * **Why** did the incident happen? *Attackers gained access through phishing emails with malicious attachments.* |
| Additional notes | What measures could the healthcare organization take to avoid a recurrence of such an event?  Is it advisable for the company to make the ransom payment in exchange for the decryption key? |

|  |  |
| --- | --- |
| **Date:**  10/29/2023 | **Entry:**  002 |
| Description | Analysis of a suspicious file using VirusTotal and identification of related IoCs. |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? *Unknown attackers delivered the malicious file via email.* * **What** happened? *An employee received and executed a malicious file, resulting in the creation of unauthorized executable files.* * **When** did the incident occur? *The incident happened at 1:15 p.m. When unauthorized executable files were created on the employee's computer.* * **Where** did the incident happen? *The incident occurred on the employee's computer.* * **Why** did the incident happen? *The incident happened because the employee opened a password-protected spreadsheet file from an email that contained a malicious payload.* |
| Additional notes | The VirusTotal report on the SHA256 file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) strongly indicates the file is malicious based on a high vendors' ratio, a negative community score, and multiple vendors flagging it as malicious. Additionally, the report provided various IoCs, including a SHA1 hash (e7d9cf0c6dd65f7393c15c31fca28f7ed9e7f67a), an IP address (185.53.178.7), and a domain name (mypc.com) associated with the malware. |

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