**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:**  **Date:** September 22, 2025. | **Entry:**  Journal Number 1 | | |
| --- | --- | --- | --- |
| Description | This is the initial journal entry documenting a ransomware attack experienced by the clinic. The attack resulted in the encryption of critical files, disrupting business operations and preventing access to patient data. Immediate actions were taken to contain the incident and seek technical assistance. | | |
| Tool(s) used | * Email security tools (for phishing detection) * Antivirus/antimalware software (for malware detection and removal) * Incident response tools (for logging and analysis) | | |
| 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 | **The 5 W’s:**   * **Who caused the incident?**  An organized group of unethical hackers targeted the clinic using phishing emails containing malicious attachments. * **What happened?**  Ransomware was deployed via phishing emails, encrypting critical files and displaying a ransom note demanding payment for the decryption key. * **When did the incident occur?**  The security incident occurred on Tuesday at approximately 9:00 a.m. * **Where did the incident happen?**  The incident occurred at the clinic's U.S. location, affecting all computers and networked systems. * **Why did the incident happen?**  The incident occurred because employees opened a malicious attachment from a targeted phishing email, which allowed attackers to deploy ransomware on the network. | | |
| 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: **Date:** September 22, 2025  **Journal Entry Number:** 1  **Description:**  This is the initial journal entry documenting a ransomware attack experienced by the clinic. The attack resulted in the encryption of critical files, disrupting business operations and preventing access to patient data. Immediate actions were taken to contain the incident and seek technical assistance.  **Tool(s) Used:**   * Email security tools (for phishing detection) * Antivirus/antimalware software (for malware detection and removal) * Incident response tools (for logging and analysis)   **The 5 W’s:**   * **Who caused the incident?**  An organized group of unethical hackers targeted the clinic using phishing emails containing malicious attachments. * **What happened?**  Ransomware was deployed via phishing emails, encrypting critical files and displaying a ransom note demanding payment for the decryption key. * **When did the incident occur?**  The security incident occurred on Tuesday at approximately 9:00 a.m. * **Where did the incident happen?**  The incident occurred at the clinic's U.S. location, affecting all computers and networked systems. * **Why did the incident happen?**  The incident occurred because employees opened a malicious attachment from a targeted phishing email, which allowed attackers to deploy ransomware on the network. |
| --- |