# 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:**<br>2024-06-28 | **Entry:**<br>1 |
|---|---|
| Description | Ransomware attack through phishing. |
| Tool(s) used | Ransomware |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident? Unethical hackers<br>• **What** happened? Attacker encrypted the organization's computer files.<br>• **When** did the incident occur? Tuesday at 09:00<br>• **Where** did the incident happen? Organization's computer<br>• **Why** did the incident happen? A phishing email with a malicious attachment was used. |
| Additional notes | Attacker left a note asking for money in exchange for the decryption key. |

---

| **Date:** | **Entry:** |
|---|---|

| | |
|---|---|
| 2024-06-28 | 2 |
| Description | Analyzing packets |
| Tool(s) used | Wireshark |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Analyzing a sample packet |

---

| **Date:**<br>2024-06-28 | **Entry:**<br>3 |
|---|---|
| Description | Capturing packets |
| Tool(s) used | tcpdump |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |

| | |
|---|---|
| Additional notes | Capturing a sample packet |

---

| **Date:**<br>2024-06-8 | **Entry:**<br>4 |
|---|---|
| Description | Investigating a suspicious hash file. |
| Tool(s) used | VirusTotal.com |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?An employee.<br>• **What** happened?A file attached to an email was successfully downloaded.<br>• **When** did the incident occur? From 1:11 pm to 1:20pm<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? A malicious email was opened and the file attached to it downloaded. |
| Additional notes | 61/73 security vendors flagged this file as malicious. |

---

| **Date:**<br>2024-06-28 | **Entry:**<br>5 |
|---|---|

| | |
|---|---|
| Description | Using a playbook to respond to the phishing incident. |
| Tool(s) used | Playbook |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Followed the playbook and escalated the incident. |

---

| **Date:**<br>2024-06-28 | **Entry:**<br>6 |
|---|---|
| Description | Reviewing the final report. |
| Tool(s) used | Google Doc. |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Reviewed the final report that contains all the details related to the incident. |

| **Date:**<br>2024-06-28 | **Entry:**<br>7 |
|---|---|
| Description | Exploring signatures and logs with Suricata |
| Tool(s) used | Suricata |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Examine and trigger  a custom rule, and examined eve.json output |

| **Date:**<br>2024-06-28 | **Entry:**<br>6 |
|---|---|
| Description | Reviewing the final report. |
| Tool(s) used | Google Doc. |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Reviewed the final report that contains all the details related to the incident. |

| **Date:**<br>2024-06-28 | **Entry:**<br>6 |
|---|---|
| Description | Reviewing the final report. |
| Tool(s) used | Google Doc. |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident?<br>• **What** happened?<br>• **When** did the incident occur?<br>• **Where** did the incident happen?<br>• **Why** did the incident happen? |
| Additional notes | Reviewed the final report that contains all the details related to the incident. |

## 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. |
|---|