



# 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.

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> Tuesday 0900
<b>Description</b>	Phishing email with ransomware was opened in the previous hours on on eo the workstations in the clinic, leading to loss of access to critical data
<b>Tool(s) used</b>	N/A
<b>The 5 W's</b>	<ul style="list-style-type: none"><li>• Who: malicious hackers</li><li>• What: phishing email with ransomware was opened internally, leading to loss of access to various files</li><li>• When: prior to Tuesday 9AM (presumably, day before?)</li><li>• Where: Clinic's computer network</li><li>• Why: malicious hackers wanted ransom to restore the files</li></ul>
<b>Additional notes</b>	Email scanner? No segmentation / Least privilege? Lack of malware awareness? Decryptor publicly available?

---

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> 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. <ul style="list-style-type: none"> <li>• <b>Who</b> caused the incident?</li> <li>• <b>What</b> happened?</li> <li>• <b>When</b> did the incident occur?</li> <li>• <b>Where</b> did the incident happen?</li> <li>• <b>Why</b> did the incident happen?</li> </ul>
Additional notes	Include any additional thoughts, questions, or findings.

---

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> <li>• <b>Who</b> caused the incident?</li> <li>• <b>What</b> happened?</li> <li>• <b>When</b> did the incident occur?</li> <li>• <b>Where</b> did the incident happen?</li> <li>• <b>Why</b> did the incident happen?</li> </ul>
Additional notes	Include any additional thoughts, questions, or findings.

---

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> <li>• <b>Who</b> caused the incident?</li> <li>• <b>What</b> happened?</li> <li>• <b>When</b> did the incident occur?</li> <li>• <b>Where</b> did the incident happen?</li> <li>• <b>Why</b> did the incident happen?</li> </ul>
Additional notes	Include any additional thoughts, questions, or findings.

---

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> 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. <ul style="list-style-type: none"><li>• <b>Who</b> caused the incident?</li><li>• <b>What</b> happened?</li><li>• <b>When</b> did the incident occur?</li><li>• <b>Where</b> did the incident happen?</li><li>• <b>Why</b> did the incident happen?</li></ul>
Additional notes	Include any additional thoughts, questions, or findings.

---

<b>Date:</b> Record the date of the journal entry.	<b>Entry:</b> 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> <li>• <b>Who</b> caused the incident?</li> <li>• <b>What</b> happened?</li> <li>• <b>When</b> did the incident occur?</li> <li>• <b>Where</b> did the incident happen?</li> <li>• <b>Why</b> did the incident happen?</li> </ul>
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.

---

<p>Reflections/Notes: Record additional notes.</p>
--