



# 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: 12.3.2025	Entry: #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	<ul style="list-style-type: none"><li>● <b>Who</b> caused the incident? An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries.</li><li>● <b>What</b> happened? A ransomware security incident.</li><li>● <b>When</b> did the incident occur? On Tuesday at 9 am.</li><li>● <b>Where</b> did the incident happen? At a small U.S. health care clinic.</li><li>● <b>Why</b> did the incident happen? The incident happened because phishing email was sent to several employees of the company, which contained a malicious attachment. Once it was downloaded, the attackers managed to get access to the organization's computer files, and encrypting them will demanding for a ransom. This is a type of ransomware and their motivation is financial gain, because they demanded a large sum of money in exchange for decryption key.</li></ul>

Additional notes	<ul style="list-style-type: none"> <li>• How can the organization prevent security incident like this from happening again in the future?</li> <li>• Should the organization pay the ransom in exchange for the data, or is there any better solution?</li> </ul>
------------------	---

---

<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	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	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> </ul>

	<ul style="list-style-type: none"> <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.
<b>Description</b>	Provide a brief description about the journal entry.
<b>Tool(s) used</b>	List any cybersecurity tools that were used.
<b>The 5 W's</b>	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>
<b>Additional notes</b>	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.