



# 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> Jan 25, 2025	<b>Entry:</b> #1
Description	Documenting a cybersecurity incident
Tool(s) used	None. Microsoft word for writing journal
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"><li>• <b>Who</b> : Organized criminal hackers</li><li>• <b>What</b> happened? A ransomware incident.</li><li>• <b>When</b> did the incident occur? Tuesday morning around 9:00 Am</li><li>• <b>Where</b> did the incident happen? A small U.S. health care clinic</li><li>• <b>Why</b> did the incident happen? The incident occurred because organized criminal hackers used a phishing attack to gain access to the company's system. After gaining access, the attackers installed ransomware and encrypted critical files. Their demand was financial, as indicated by a ransom note requesting a large sum of money in exchange for the decryption key.</li></ul>
Additional notes	<p>How could the health care company prevent an incident like this in the future?</p> <p>Should the clinic pay the ransom?</p> <p>How could they restore the client data if they decide not paying the ransom?</p>

---

<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	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.

## 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.
---