



# 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> 17/05/2025	<b>Entry:</b> 1
Description	Ransomware attack on a U.S. health care clinic, causing critical disruption to business operations and file access.
Tool(s) used	Direct employee observation, Ransom note display.
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"><li>• An unknown organized group of unethical hackers (known to target healthcare and transportation sectors).</li><li>• Critical files encrypted by ransomware, leading to inability to access medical records and shutdown of business operations.</li><li>• Tuesday morning. Around 9:00 a.m.</li><li>• Small U.S. health care clinic specializing in primary-care services.</li><li>• Attackers gained access via targeted phishing emails with malicious attachments, installing malware that deployed ransomware to encrypt files for financial gain (ransom).</li></ul>
Additional notes	Major disruptions to business operations due to inability to access critical patient data. The company was forced to shut down computer systems and contacted external organizations for assistance.

---

<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> <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> <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.
---