



# 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> 03.05.2024	<b>Entry: 01</b>
Description	Security breach due to phishing scam via email
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> <p>The incident was due to an employee falling for a phishing scam. The employee then proceeded to click on the malicious attachment, which infected the computer and allowed the attackers access into the internal network. This was a ransomware attack, demanding for a large payment in order for the decryption key. The attackers had encrypted critical data, like medical records, blocking staff from performing their job function. The attack happened in a small U.S. health care clinic specializing in delivering primary-care services. The</p>

	incident likely happened as staff have not been properly trained on how to spot phishing scams and the appropriate measures when one is identified. A malicious attachment was hastily clicked and caused a serious event for the business.
Additional notes	To stop this from happening again, proper and quarterly employee training is needed in security awareness. Covering common phishing and social engineering attacks, as well as strong password practices etc.

---

<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	<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.

## 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.
---