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: August 26, 2025	**Entry:** #1
Description	Ransomware attack on a healthcare clinic.
Tool(s) used	None. User-reported incident.
The 5 W's	• **Who caused the incident:** An organized group of unethical hackers known for targeting the healthcare sector. • **What happened:** A ransomware attack that resulted in the encryption of critical files and a complete halt of clinic operations. • **When did the incident occur:** Tuesday, at approximately 09:00 AM. • **Where did the incident happen:** On the internal computer network of the healthcare clinic. • **Why did the incident happen:** A targeted phishing email with a malicious attachment was opened by an employee. The hackers goals is financial gain through extortion via a ransom demand
Additional notes	• Investigation: Priority is to determine the scope of the breach and identify if data was exfiltraded. • Recommendation: Do not pay the ransom as per industry best practices.

	● Next step: Activate the Incident Response Plan to begin containment, eradication, and recovery procedures. ● Long-term recommendation: Implement security awareness training, use advanced email filters and create a robust backup policy.

Date: Record the date of the journal entry.	**Entry:** 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. ● **Who** caused the incident? ● **What** happened? ● **When** did the incident occur? ● **Where** did the incident happen? ● **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of	**Entry:** Record the journal entry number.

the journal entry.	
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. ● **Who** caused the incident? ● **What** happened? ● **When** did the incident occur? ● **Where** did the incident happen? ● **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** 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. ● **Who** caused the incident? ● **What** happened? ● **When** did the incident occur? ● **Where** did the incident happen? ● **Why** did the incident happen?

Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** 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. ● **Who** caused the incident? ● **What** happened? ● **When** did the incident occur? ● **Where** did the incident happen? ● **Why** did the incident happen?
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.