



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: 11-May-2025	Entry: 1
Description	Ransomware attack
Tool(s) used	
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">● Who caused the incident?● Unethical hacker group● What happened?● Security incident performing a ransomware attack● When did the incident occur?● Incident Reported on Tuesday 9>00 am● Where did the incident happen?● Into the company's network● Why did the incident happen?● Because an employee opened apishing email that downloaded malware when clicking on a malicious link.
Additional notes	After recovery and contention stage end, cibersecurity team should direct conferences with employees teaching about how to act to identify and prevent phishing theats.

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. <ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● Who caused the incident? ● What happened? ● When did the incident occur? ● Where did the incident happen?

	<ul style="list-style-type: none"> ● 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. <ul style="list-style-type: none"> ● 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> ● 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	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"> ● 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.
