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: July 23, 2024	**Entry:** #1
Description	Documenting cybersecurity incident in healthcare company
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: A group of hackers. ● **What**: A ransomware attack. ● **When**: Tuesday 9:00 a.m. ● **Where**: health care company ● **Why**: A group of hackers used a phishing attack to get access to employees' workstations. Next they encrypted the files in the company's systems using ransomware. In exchange for the decryption key, they want money.
Additional notes	1. How can they prevent the attack in the future? 2. What to do now? Pay the ransom?

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.

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:	**Entry:**

Record the date of the journal 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.

You might have multiple entries in your incident handler's journal. If your journal contains missing or incomplete entries, go back and review any previous sections of this course to add additional log entries to your journal. Here's a list of the course activities you can revisit to complete your journal:

- **Activity: Document an incident with an incident handler's journal**
- **Activity: Analyze your first packet**
- **Activity: Capture your first packet**

- Activity: Investigate a suspicious file hash
- Activity: Use a playbook to respond to an attack
- Activity: Review a final report
- Activity: Explore signatures and logs with Suricata
- Activity: Perform a query with Splunk
- Activity: Perform a query with Chronicle

At minimum, you should have the following entries in your incident handler's journal:

- *At least* 4 dated and numbered journal entries, including:
  - 2 journal entries documenting an incident investigation using the 5 W's
  - 2 journal entries describing the use of a cybersecurity tool

Review your incident handler's journal and make any necessary changes. Here are some things to consider during your review:

- Errors in grammar, punctuation, and spelling
- Missing, inaccurate, or incomplete journal entries