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: 12/05/2023	**Entry:** # 1
Description	There has been a security breach, in the incident, the hacker was able to encrypt sensitive data and is requesting a ransom in order to provide a decryption key. This was done through a phishing email that the attacker sent to several of our employees.
Tool(s) used	No tools were used, it was done through a phishing email, and he's requesting a ransom.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers • **What** happened? A group of unethical hackers was able to gain access to our sensitive files by sending a phishing email to several of our employees and now are requesting a ransom • **When** did the incident occur? Tuesday 9:00am • **Where** did the incident happen? At a U.S. health care clinic specialized in delivering primary-care services.

	• **Why** did the incident happen? Because the group of attackers wanted money they left a ransom note displayed on the employees computers requesting a huge amount of money.
Additional notes	We have to get help and see if there's a way that our company can decrypt these files or this company is going to have to pay to gain access to these files again by paying the ransom requested by these hackers and getting a decryption key, but we are not guarantee that this group of hackers won't come back for more, or give access to other groups of hackers to do the exact same thing again, Next We have to go through what we have learned as the incident response team and train all employees at this company to not click on any email and we have to keep this kind of training updated and keep updating employees to new attack strategies that are rising in the tech landscape

---

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	**Entry:** Record the journal entry number.

of 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.