Incident Handler's journal

Instructions

Record your findings after completing an activity or take notes on what you've learned about like 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.

Date: 3/13/2024	**Entry:** 1
Description	Initial incident journal entry for the security incident at the U.S. healthcare clinic.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? **-** An organized group of unethical hackers targeted the health care clinic. • **What** happened? - The clinic's computer systems were infected with ransomware, encrypting critical files and disrupting business operations. • **When** did the incident occur? - The incident occurred on a Tuesday at 9:00 a.m. • **Where** did the incident happen? - The incident happened at a small U.S. healthcare clinic specializing in primary-care services. • **Why** did the incident happen? - The incident occurred due to employees downloading a malicious attachment from phishing emails sent by the hackers.
Additional notes	1. Did the clinic have a response plan in place for such incidents, and if so,

	how was it executed? 2. How could the healthcare company prevent an incident like this from occurring again? 3. Should the company pay the ransom to retrieve the decryption key? 4. What steps can be taken to improve employee awareness and training regarding phishing attacks? 5. Are there legal and regulatory implications for the clinic regarding patient data privacy and ransomware payments?

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: 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.