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: Aug 13, 2024	**Entry:** 1
Description	Ransomware attack on a small U.S. healthcare clinic resulting in the encryption of critical patient data and disruption of business operations.
Tool(s) used	None mentioned in the scenario
The 5 W's	Capture the 5 W's of an incident. • **Who** An organized group of unethical hackers known to target healthcare and transportation industries. • **What** A ransomware attack that encrypted the company's files and demanded a ransom for the decryption key. • **When** Tuesday morning at approximately 9:00 a.m. • **Where** A small U.S. healthcare clinic. • **Why** The attackers gained access through a phishing email with a malicious attachment, aiming for financial gain.
Additional notes	Highlights the vulnerability of healthcare organizations to cyberattacks, particularly ransomware. Emphasizes the importance of employee security awareness training and robust email security measures.

	Underscores the need for a well-defined incident response plan and backup procedures. Questions: • What specific technical controls could have prevented or mitigated this attack (e.g., email filtering, endpoint protection)? • Did the company have a data backup and recovery plan? If so, was it effective in restoring operations? • What communication strategies were used to inform patients and stakeholders about the incident and its impact on their data and services?

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.