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: Fri. Dec. 8, 2023	**Entry:** 1
Description	At around 9:00am a health clinic in the U.S. that delivers primary-care services fell victim to a malicious-acting hacktivist group. Using targeted phishing emails, the attackers gained access to the company's network and delivered a malicious attachment which then installed malware that denied employees access from medical records and software. It was able to do this by encrypting critical files on the network. The attackers placed a ransom note for all employees to see, demanding a large sum of money in exchange for withdrawing the malware.
Tool(s) used	Encryption/Decryption key, Ransomware
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A hacktivist or unethical hacker group • **What** happened? The hacktivist group demanded a ransom from the medical care company in exchange for regaining accesses to the company's operational functions

	• **When** did the incident occur? The incident occurred at approximately 9:00am • **Where** did the incident happen? The incident occurred on the company's network and devices that had access to the network • **Why** did the incident happen? The hacktivist group targets organizations in healthcare and transportation industries, likely due to a difference in moral and political stance
Additional notes	The hacktivist group caused a major disruption of business operations in a sector involving essential services. Even after security experts recover the company's functionality, the fact that the attackers gained access to highly sensitive customer PII and potentially SPII means the customer and company information had already been compromised and likely fell into the hands of these criminals. A full disclosure procedure must be taken to ensure all patients of this healthcare organization are well informed that their information may have been compromised and the company must then find a way to apologize, since there isn't much else they can do to recover this information apart from investigation into the who these attackers really are, and to notify the authorities of the crime.

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	**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.

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.