Incident handler's journal

Date: 13th January 2025	**Entry: 1**
Description	A US healthcare clinic experienced a security incident which disrupted their business operations
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? This incident was caused by an organized group of unethical hackers • **What** happened? A ransomware security incident • **When** did the incident occur? The security incident occurred at approximately 9am on Tuesday • **Where** did the incident happen? At a healthcare company • **Why** did the incident happen? The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How will the company prevent future attacks like this in the future? 2. Will it be necessary to pay the organized group to restore access?

Date: 15th January 2025	**Entry: 2**
Description	A phishing email was sent
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A malicious actor ● **What** happened? An attempted phishing email was sent to an employee ● **When** did the incident occur? 20th July 2022 ● **Where** did the incident happen? Financial Services company ● **Why** did the incident happen? The incident happened as the employee downloaded a malicious file onto his pc. After investigating the email attachment file's hash it has been verified that it's malicious.
Additional notes	Training for employees post incident to watch out and detect for phishing emails

---

Date: 16th January 2025	**Entry: 3**
Description	Analyzing a packet capture file
Tool(s) used	Wireshark- A network protocol analyzer that uses a Graphical User Interface

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? **n/a** ● **What** happened? **n/a** ● **When** did the incident occur? **n/a** ● **Where** did the incident happen? **n/a** ● **Why** did the incident happen? **n/a**
Additional notes	

Date: 17th January 2025	**Entry: 4** Analyzing a packet file capture
Description	Provide a brief description about the journal entry.
Tool(s) used	TCPdump to capture and analyze network traffic. This is a network protocol analyzer that's accessed using the command-line interface. Similar to Wireshark, the value of tcpdump in cyber security is that it allows security analysts to capture, filter and analyze network traffic
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? **N/a** ● **What** happened? **N/a** ● **When** did the incident occur?

	n/a ● **Where** did the incident happen? **n/a** ● **Why** did the incident happen? **n/a**
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.