Incident handler's journal

Date: 06/27/2025	**Entry:** 1
Description	A small U.S. health care clinic experienced a security incident on Tuesday at which severely disrupted their business operations.
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. ● **What** happened? Ransomware security incident ● **When** did the incident occur? Tuesday 9:00 A.M. ● **Where** did the incident happen? At a health care clinic ● **Why** did the incident happen? The incident occurred because an organized group of unethical hackers gained access to a healthcare clinic's systems via a phishing attack. After access was gained, the unethical hackers deployed their Ransomware onto the company's systems and encrypted sensitive / critical files. Attackers clearly motivated financially, as a ransom note was left demanding payment of a large sum of money in exchange for the decryption key.
Additional notes	Iplisting on the email server could be used to mitigate this vulnerability, how else can the healthcare clinic improve their security posture? Should the healthcare clinic pay the ransom to retrieve the decryption key? Will these attackers become an APT (Advanced Persistent Threat;) i.e. will the Hackers do this again?

Date: 7/24/2025	**Entry:** 2
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? Malicious Actor ● **What** happened? A Ransomware (data exfiltration) attack via forced browsing ● **When** did the incident occur? December 28, 2022 at 7:20 p.m., PT ● **Where** did the incident happen? On the organization's E-commerce website ● **Why** did the incident happen? The malicious actor exploited a vulnerability in the purchase confirmation page of the website whereby the malicious actor performed a forced browsing attack by modifying the order number included in the URL string of the purchase confirmation page. This allowed the actor to view, collect, and exfiltrate thousands of purchase confirmation pages that were involved with other customers' orders.
Additional notes	Recommendations: perform routine vulnerability scans and pen. Testing. Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. Ensure that only authenticated users are authorized access to content.

Date: 7/30/2025	**Entry:** 3
Description	Used Splunk Cloud to perform a search and investigation
Tool(s) used	Splunk
The 5 W's	• Upload sample log data • Search through indexed data • Evaluate search results • Identify different data sources • Locate failed SSH login(s) for the root account
Additional notes	

Date: 7/30/2025	**Entry:** 4
Description	Configure Suricata and use it to trigger alerts.
Tool(s) used	Suricata
The 5 W's	• create custom rules and run them in Suricata, • monitor traffic captured in a packet capture file, and • examine the `fast.log` and `eve.json` output.
Additional notes	

Date: 7/30/2025	**Entry:** 5
Description	Open and analyze a packet capture file using Wireshark
Tool(s) used	Wireshark
	• Open a packet capture file using Wireshark • Examine packet information • Apply display filters
Additional notes	Include any additional thoughts, questions, or findings.

Journal entry template

copy the table below and paste it into the template to use for future entries.

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.

Reflections/Notes: Record additional notes.