Incident handler's journal

Date: 05/16/2023	**Entry:** 1
Description	Health Clinic Ransomware Event
Tool(s) used	None
The 5 W's	• **Who:** Unethical Hackers • **What**: Employee PCs locked to ransomware • **When**: 9 AM, Tuesday • **Where**: Healthcare Clinic • **Why**: Employee clicked on phishing email link, which then provided access to the hackers to plant the ransomware.
Additional notes	The Health Clinic needs cyber security awareness training. Needs a business continuity plan

Date: 5/22/2023 Record the date of the journal entry.	**Entry:** 2
Description	Malicious File Download
Tool(s) used	VirusTotal website

The 5 W's	Capture the 5 W's of an incident. - **Who:** Employee - **What**: Employee accidentally downloaded malware from phishing email - **When**: 1 P.M, afternoon - **Where**: In the work office - **Why**: Employee was not properly trained for cyber awareness
Additional notes	Cyber Security awareness training is needed among the workforce to prevent further incidents.

Date: 5/23/2023	**Entry:** 3
Description	Monitoring Network Traffic with Suricata
Tool(s) used	Suricata
Events	Explored custom rules with Suricata. Ran created a custom rule to trigger and study output logs, and finally examined output from from eve.json log file.
Additional notes	Suricata test ran smoothly with no incidents

Date: 5/24/2023	**Entry:** 4
Description	Used Phishing Playbook in response to an alert
Tool(s) used	Phishing Playbook

The 5 W's	Capture the 5 W's of an incident. ● **Who**: Employee ● **What**: Employee downloaded suspicious file ● **When:** 10 AM ● **Where**: In Office ● **Why**: Employee accidentally click on phishing email link
Additional notes	Phishing playbook was used in incident response to determine the level of escalation, and actions to take to prevent further damage. Successfully contained the incident.