Incident handler's journal

Date: 03/16/2025	**Entry:** 1
Description	Ransomware attack and security breach reported at small US healthcare clinic
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Known Group of unethical Hackers known to attack healthcare and transportation organizations** • **Phishing emails were sent to various employees at the healthcare clinic. A malicious program was an attachment that downloaded onto the employees computers and provided access to the hackers.** • **Tuesday at 9 am** • **On the employees computers at the healthcare clinic** • **Ransom note displayed on the employees computers. Hackers demanded a large sum of money in return for access to the healthcares DATA and network**
Additional notes	Additional Phishing training needed for employees. Furthermore, proper authorities need to be contacted.

Date: 03/18/2025.	**Entry:** 2

Description	Malware file downloaded on employees computer
Tool(s) used	SHA256, VirusTotal, IDS
The 5 W's	Capture the 5 W's of an incident. • **Who** an employee • **What** employee recieved an email with a spreadsheet attached • **When** 1:11 pm • **Where** on employees computer • **Why** malicious file was downloaded onto employees computer to gain access to employees device and network
Additional notes	VirusTotal shows file to be malware. Most current community members are students with this hash as an example . information capture utilized

---

Date: 03/18/2025.	**Entry:** 3
Description	Response and evaluation to phishing alert ticket
Tool(s) used	unknown
The 5 W's	Capture the 5 W's of an incident. • **Who** employee • **What** was sent a phishing email with attachment. An alert was created • **When** Wednesday 9:30:14 AM • **Where**On the employees computer • **Why** to gain access to employees computer and data. Data capture detected

Additional notes	Ticket and event escalated. Severity medium. MA used the concept of job hunting and a password encrypted resume to entice employee to download Malicious file

---

Date: 03/20/2025	**Entry:** 4
Description	Uploaded and searched logs on splunk
Tool(s) used	Splunk
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	Utilized filters. Need to review SPL language for future needs

---

Date: 03/20/2025	**Entry:** 5

Description	Researched log entries through suricata
Tool(s) used	Linux, suricata
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	Further practice in linux needed. Suricata utilized to filter log entries. Research jq command

---

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: Further research into command prompt languages and querying languages needed to hone log query and filtering skills. Utilized ticketing systems and event investigations. This helped me better understand more about what a day to day might be for a level 1 SOC analyst. I used multiple Security tools in this course. I have also responded to multiple practice IoCs and IoAs to better understand what data to look for in the initial discovery and how to properly respond.