Incident handler's journal

Date: 5th November 2023	**Entry:** 1
Description	Received a report of a critical security incident at a small U.S. health care clinic specializing in primary-care services. Employees reported a widespread inability to access files, including medical records, and a ransom note demanding payment for file decryption. The incident seems to have originated from a phishing attack that led to the deployment of ransomware, causing severe disruptions in business operations.
Tool(s) used	None
The 5 W's	● **Who caused the incident?** ● An organized group of unethical hackers, as indicated in the ransom note. Further investigation needed to identify specific individuals or entities. ● **What happened?** ● A phishing attack targeted employees with a malicious attachment, leading to the deployment of ransomware that encrypted critical files. The attackers demanded a ransom for the decryption key. ● **When did the incident occur?** ● Tuesday morning at approximately 9:00 a.m. Further details on the timeline of the attack and the duration of the disruption are needed. ● **Where did the incident happen?** ● At a small U.S. health care clinic specializing in primary-care services. The specific location of the clinic needs to be documented for further investigation.

	● **Why did the incident happen?** ● The incident occurred due to the successful execution of a phishing attack. The attackers gained access to the organization's network, deployed ransomware, and demanded a ransom. Motivations behind the attack, whether financial or otherwise, are yet to be determined.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? 3. What immediate actions should be taken to contain the incident and minimize further damage? Prioritize a comprehensive analysis of the phishing attack vectors and the ransomware deployed. Initiate containment measures to prevent further spread and damage. Establish communication protocols with relevant stakeholders, including affected employees and authorities. Coordinate with law enforcement and cybersecurity experts to trace the attackers and assess the viability of paying the ransom.

Date: 6th of November 2023	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a GUI. Wireshark allows security professionals to capture and analyze network traffic. This is one of the steps of detecting and

	investigating malicious activity.
The 5 W's	Capture the 5 W's of an incident. ● **Who** N/A ● **What** N/A ● **When** N/A ● **Where** N/A ● **Why** N/A
Additional notes	This is the first time I used Wireshark and my first attempt at analyzing a packet capture file.

Date: 7th of November 2023	**Entry:** #3
Description	First Packet Capture
Tool(s) used	Tcpdump - a network protocol analyzer that's accessed using the CLI. Very similar to Wireshark, although Wireshark provides a GUI, the value of tcpdump in CS is that it allows security professionals to capture, filter and analyze network traffic.
The 5 W's	Capture the 5 W's of an incident. ● **Who** N/A ● **What** N/A ● **When** N/A ● **Where** N/A ● **Why** N/A

Additional notes	Using the CLI will have a learning curve although I am already feeling more confident with simple tasks. Using it to capture and filter network traffic just showed me how powerful the CLI can be.

Date: 8th of November 2023	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal, an investigative tool that analyzes files and URL's for malicious content such as viruses, worms, trojans, etc. It was my first experience with VT but it will definitely become a part of my day to day not only professionally but personally as well. I analyzed a hash file and it was reported as malicious. This incident occurred in the Detection and Analysis phase. The scenario put me in the place of a SA at a SOC investigating a suspicious file hash. I had to perform a deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	Capture the 5 W's of an incident. ● **Who:** Unknown malicious actor ● **What:** An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **When**: At 1:20pm, an alert was sent to the organization's SOC after the intrusion detection system detected the file. ● **Where**: An employee's computer at a financial services company

	- **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?

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.