Incident handler's journal

Date: March 31, 2024	**Entry: #1**
Description	Documentation of a ransomware cybersecurity incident
Tool(s) used	None
The 5 W's	**Who**: A group of organized unethical, or “black hat”, hackers. **What:** Ransomeware installed on PC’s with SPII. **When**: 09:00 Tuesday **Where**: A healthcare company **Why**: The hackers wanted monetary compensation after encrypting vital files with ransomware. They gained access to the company using a phishing email campaign.
Additional notes	The company will need to provide comprehensive cybersecurity training heavily focusing on phishing attacks to all employees. If the company does not have backups of the data they’ll have to lose it all or pay the ransom.

Date: Apr 1, 2024	**Entry: #2**.
Description	Analyzation of captured packets with Wireshark
Tool(s) used	During this activity I used Wireshark to analyze network packets. Wireshark is heavily used in cybersecurity as it provides an easy to use graphical user interface that helps the network protocol analyzer stand out. This application is

	invaluable to security teams for investigations as well.
The 5 W's	N/A
Additional notes	I can see why so many cybersecurity professionals would rely on such a tool. I could see myself quickly learning tips and tricks that could make it more valuable than I even know.

Date: Apr 1, 2024	**Entry:** #3
Description	Capturing packets with tcpdump
Tool(s) used	I used the command line interface of a Linux virtual machine to capture packets with tcpdump. It was a very powerful tool that I can see being invaluable to the day to day activities of cybersecurity experts. It can provide you with as little, or as much information as you'd like.
The 5 W's	N/A
Additional notes	I found using the CLI very appealing. While I'd say that the output can be easier to digest using Wireshark, it was pleasant and easy to type what you needed in a clear and visible way without the distraction of a graphical user interface.

Date: April 1, 2024	**Entry:** #4

Description	Suspicious file hash investigation
Tool(s) used	After a suspicious file was downloaded after a phishing email. I used the website VirusTotal, which has a repository of malicious content such as worms, viruses, bad URLs, and corrupted hash values.
The 5 W's	● Who: An unknown malicious actor ● What: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● Where: An employee's computer at a financial services company ● When: 1:20 p.m., when the SOC’s intrusion detection system detected the file ● Why: An employee was able to download and execute a malicious file attachment from a phishing email
Additional notes	The financial services company should hold periodic cybersecurity training to inform its employees of malicious actors and their methods.