Incident handler's journal

Date: 06/16/2023	**Entry:** #1
Description	This cybersecurity analysis project involved two critical phases: Detection and Analysis: The project commenced with the organization detecting a ransomware incident. The scenario elaborates on the initial detection process employed by the organization. To conduct a comprehensive analysis, the organization reached out to multiple external entities, seeking their technical expertise and assistance. Containment, Eradication, and Recovery: Following the detection phase, the scenario delineates the organization's efforts to contain the incident. As a proactive measure, the company swiftly shut down their computer systems to prevent further spread of the ransomware. However, recognizing the complexity of eradicating the threat and recovering from its impact, the organization sought support from various external organizations to aid them in these crucial tasks.
Tool(s) used	None
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: A health care company • **When**: Tuesday (06/13/2023), 9:00 a.m. • **Why**: Unethical hackers exploited a phishing attack to breach the company's systems, enabling them to deploy ransomware and encrypt vital files. Their clear financial motive was evident from the ransom note demanding a substantial sum for the decryption key.
Additional notes	1. All employees at the company should be trained in detecting and appropriately handling human engineering attempts to avoid future incidents. 2. The company will need to weigh their options in regards to paying the ransom as there is no guarantee of file recovery whether paid or not.

Date: 06/16/2023	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	In this project, I utilized Wireshark, a graphical network protocol analyzer, to examine a packet capture file. Wireshark's significance in cybersecurity lies in its ability to capture and analyze network traffic, enabling security analysts to identify and investigate potential threats and malicious behavior.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	Using Wireshark for the first time, while intimidating at first, quickly became a very intuitive and convenient tool. It's clearly a great tool for analyzing packet capture files.

Date: 06/17/2023	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	In this exercise, I utilized tcpdump, a command-line network protocol analyzer, to capture and analyze network traffic. Similar to Wireshark, tcpdump holds significant value in the field of cybersecurity as it empowers security analysts to capture, filter, and thoroughly examine network traffic data.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	Though I was new to the command-line interface, capturing and filtering network traffic quickly became a fun and exciting challenge.

Date: 06/18/2023	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	During this cybersecurity analysis project, I utilized VirusTotal, an investigative tool designed to scrutinize files and URLs for potentially harmful content, such as viruses, worms, trojans, and more. VirusTotal proved to be an invaluable resource for promptly verifying whether an indicator of compromise, such as a website or file, had been flagged as malicious by other experts within the cybersecurity community. In this particular project, I leveraged VirusTotal to conduct an analysis on a file hash, which was identified as malicious. The incident took place within the Detection and Analysis phase, wherein I assumed the role of a security analyst stationed at a Security Operations Center (SOC). Tasked with investigating a suspicious file hash, my responsibilities involved conducting comprehensive analysis and thorough investigation to determine the validity of the alert and ascertain the presence of an actual threat.
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 of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: An employee's computer at a financial services company • **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file • **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	Every employee of the company needs to receive basic training in detecting and appropriately reporting/responding to human engineering techniques. The company needs to maintain ay