Incident handler's journal

Date: 3/12/2025	**Entry:** 1
Description	Documenting a cybersecurity incident This incident occurred in the two phases The first phase is how the organization first detected the ransomware incident.The second phase is the steps that the organization took to contain the incident.
Tool(s) used	None
The 5 W's	The event was caused by a group of unethical hackers who caused a ransomware security incident. The event occurred on Tuesday at 9:00 a.m., and it occurred because the hackers installed malware on company computers using a phishing attack that installed ransomware on company computers, encrypting important files, and leaving ransom notes on every computer system, asking for a large sum of money in exchange for the decryption key.
Additional notes	Such a drastic event should never happen to a healthcare company, better safety measures should be put in place to avoid all systems being affected in such a manner.

Date: 3/11/2025	**Entry:** 2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. Wireshark helped me capture and analyze network traffic to detect and investigate malicious activity.

The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface looked fairly simple, but when I began analyzing the capture file, there was so much on the screen, it started to feel overwhelming.

Date: 3/10/2025	**Entry:** 3
Description	Capturing my first packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that users access using the Linux command-line interface. Tcpdump in cybersecurity is that it allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	I have some experience with the command-line interface, but using it to capture and filter network traffic was a challenge. I didn't understand what most things on the screen were, but reading the help me finish the activity and capture network traffic from my packet.

Date: 3/9/2025	**Entry:** 4
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, an investigative tool that analyzes files and URLs for malicious content, including viruses, worms, and trojans. It is a valuable resource for quickly determining whether an indicator of compromise such as a website or file has been flagged as malicious by the cybersecurity community. In this case, I used VirusTotal to analyze a file hash which was identified as malicious.
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., the 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 (phishing email).
Additional notes	This incident took place during the Detection and Analysis phase. The scenario positioned me as a security analyst in a SOC investigating a suspicious file hash. After the security systems flagged the file, I conducted a deeper analysis to assess whether the alert indicated a legitimate threat.

Date: 3/13/2025	**Entry:** 5
Description	Perform a search and investigation activity in Splunk
Tool(s) used	For this activity, I used Splunk Cloud, a powerful SIEM tool that collects, processes, and indexes log data, making it searchable and analyzable. Splunk enables security analysts to perform queries, analyze logs, and detect anomalies. In this case, I used Splunk Cloud to upload and query log data related to authentication and authorization attempts on Buttercup

	Games' mail server.
The 5 W's	• **Who:** An unauthorized user attempting to access the system via SSH • **What:** Multiple failed SSH login attempts for the root account • **Where:** Buttercup Games' mail server (host: mailsv) • **When:** During the log analysis session, over 300 failed SSH login events were detected • **Why:** The repeated failed login attempts suggest a possible brute-force attack or unauthorized access attempt
Additional notes	The main objective of this activity was to explore Splunk Cloud's capabilities by: • Uploading sample log data • Searching through indexed data • Evaluating search results • Identifying different data sources • Locating failed SSH login attempts for the root account This activity took place during the Detection and Analysis phase. The scenario positioned me as a security analyst investigating authentication logs. After successfully uploading and indexing the log data, I conducted queries to filter and analyze failed SSH login attempts. The search results revealed over 300 failed login events originating from the mail server, indicating a potential security threat requiring further analysis.

Reflections/Notes:

1. **Were there any specific activities that were challenging for you? Why or why not?**

I really found using tcpdump a bit challenging. Simply because it seemed like there was a lot of information being displayed on the screen, but I believe that's what happens when one is learning.

2. **Has your understanding of incident detection and response changed after taking this course?**

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.

3. **Was there a specific tool or concept that you enjoyed the most? Why?**

I really enjoyed using splunk and VirusTotal because of how simple their GUI was and how uncomplicated was to navigate.