Incident handler's journal

Date: April 27, 2025	**Entry:** **#1**
Description	Documenting a cybersecurity incident **1. Detection and Analysis** The ransomware incident was initially detected through internal monitoring. Upon confirmation of malicious activity, the organization initiated its incident analysis procedures and engaged multiple external technical partners to assist with investigation and assessment. **2. Containment, Eradication, and Recovery** Containment measures were implemented immediately, including the shutdown of all computer systems to prevent further spread of the ransomware. Due to limited in-house capability for complete eradication and recovery, the organization coordinated with specialized external agencies to remove the threat and restore operational systems.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who** An organized group of unethical hackers ● **What** Through phishing emails, ransomware was installed ● **When** at 9am on Tuesday ● **Where** A small U.S. healthcare clinic ● **Why** The incident happened when targeted employees clicked on a malicious attachment. This installed malware and gave the unethical

	hackers the ability to encrypt critical data, and ransomware was installed. A ransom note stated to decrypt, the company must provide money. Money seems to be the motivation.
Additional notes	1. How could the healthcare company prevent an incident like this from occurring again? 2. Should the company pay the ransom to receive the decryption key?

Date: May 5, 2025	**Entry: #2**
Description	Documenting a cybersecurity incident
Tool(s) used	Email, attachment on email
The 5 W's	Capture the 5 W's of an incident. ● **This is caused by the attachment on the email, and the employee who downloaded the file.** ● **What** The employee clicked on the email, and this downloaded the flagpro trojan, which caused many executables to infect the computer. ● **When** This occured at 1:15 PM. ● **Where** In a financial services company. ● **Why** The employee clicked on the malware.
Additional notes	How can the financial services company prevent this from happening in the future? What kind of IT security training should be provided to the employees?

Date: May 6th, 2025	**Entry: #3**
Description	Documenting a cybersecurity incident
Tool(s) used	Used VirusTotal website, and notes on the email sent to the employee. VirusTotal is an investigative tool to analyze files and URLs for viruses, worms, trojans, and more.
The 5 W's	Capture the 5 W's of an incident. ● **Who** The incident caused by the employee who clicked on malware, called flagpro. ● **What** The senders email address doesn’t match the name and the sender information. There are grammatical errors and an executable included in the email. ● **When** Occured on July 20, 2022. ● **Where** This email is sent to hr at the financial institution. ● **Why** The employee clicked on the folder, and didn’t recognize the indications of malicious intent, and evidence of alarm.
Additional notes	How did the malicious actor/s know the employee’s email address? What can be done to prevent this from happening again?

Date: May 7th, 2025	**Entry: #4**.

Description	Investigation of major security incident
Tool(s) used	Forced browsing attack, changed the URL string of a purchase confirmation page, required for retail company to pay to not release customer data.
The 5 W's	Capture the 5 W's of an incident. ● **Who** An unknown unethical hacker. ● **What** The hacker found a vulnerability in the web-site, and injected a modifying the order number in the URL string ● **When** Started on December 28th 2022, through December 31, 2022. ● **Where** In the e-commerce web application ● **Why** The vulnerability in the web application.
Additional notes	How can this be prevented in the future? What additional training should be provided to employees that receive emails that are similar?

Date: May 17th, 2025	**Entry: #5**
Description	Analyzing a packet capture file
Tool(s) used	Network protocol analyzer Wireshark that uses a graphical user interface to analyze a packet capture file.
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	I was so excited to begin this exercise and analyze the packet capture file, since I am gaining experience. At first it was overwhelming, but as I learned about what each part of the captured file meant I understood what was being shown.

Date: May 22, 2025	**Entry: #6**
Description	A Denial-of-Service (Dos) attack, specifically a SYN flood, disrupted a public website.
Tool(s) used	Wireshark (Packet capture and analysis tool) Firewall and intrusion prevention system
The 5 W's	Capture the 5 W's of an incident. ● **Who** Website visitors, malicious actors ● **What** SYN flood attack or excessive number of SYN packet requests. ● **When** Detected June 9, 2025 at 2:17pm ● **Where** Public website of an organization ● **Why** To disrupt and slow down server resources without completing the TCP handshake.
Additional notes	TCP handshake exploitation through SYN packets. Used available connection slots, so legitimate users can't access the site. Mitigate through configuration rate limits, implementing upstream traffic filtering through ISP.