Incident handler's journal

Date: November 20, 2024	**Entry:** #1
Description	Recording a cybersecurity incident
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An organized group of unethical hackers who are known to target organizations in the healthcare and transportation industries ● **What** happened? ○ The company encountered a ransomware security incident. Medical files were encrypted and inaccessible to employees. A ransom note was left on all company computer systems, demanding a large sum of money in exchange for the decryption key. ● **When** did the incident occur? ○ Tuesday 9:00 am ● **Where** did the incident happen? ○ At a small U.S. healthcare company ● **Why** did the incident happen? ○ Unethical hackers obtained access to the company's systems using a phishing attack, launching their ransomware and encrypting critical files. ○ The motivation seems to be financial, leaving a random note demanding a large sum of money in exchange for the decryption key
Additional notes	Include any additional thoughts, questions, or findings.

	1. How could the company prevent this from happening again? 2. Is it ethical to pay the ransom?

Date: November 24, 2024	**Entry:** #2
Description	Documenting an alert email that contains malicious attachments.
Tool(s) used	Phishing playbook
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An email sender who has malicious intentions ● **What** happened? ○ A malicious attacker sends an email disguised as a job application, including malicious attachments as what the attacker claims to be a resume and cover letter. ● **When** did the incident occur? ○ Wednesday, July 20, 2022, 09:30:14 AM ● **Where** did the incident happen? ○ This email was sent to the HR department of a company called Inergy ● **Why** did the incident happen? ○ The employee downloaded and opened a malicious file from a phishing email.
Additional notes	Include any additional thoughts, questions, or findings. - Did the email not seem suspicious to the employee who opened it? - How could emails like this be prevented in the future?

Date: November 26, 2024	**Entry:** #3
Description	Documenting a security incident on December 28, 2022, at 7:20 pm PT.
Tool(s) used	- Web application access logs - Web server logs
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An attacker performed a forced browsing attack to access customer transaction data. ● **What** happened? ○ The attacker sent a ransom email claiming they had stolen customer data and demanded a large amount in cryptocurrency. ● **When** did the incident occur? ○ December 28, 2022, at 7:20 pm PT. ● **Where** did the incident happen? ○ In the e-commerce web application ● **Why** did the incident happen? ○ There was a vulnerability in the e-commerce web application ○ The attacker found the vulnerability and performed a forced browsing attack by modifying the order number in the URL string of the confirmation page ○ This leads to acquiring access to customer data
Additional notes	Include any additional thoughts, questions, or findings. 1. How could this vulnerability have been prevented? 2. Was it right for the employee to ignore the first ransom email? 3. Could it have been less damaged if the employee had reported the first ransom email?

Date: November 22, 2024	**Entry:** #4
Description	Analyzing a packet capture file
Tool(s) used	Wireshark: a network protocol analyzer that uses a GUI.
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? N/A
Additional notes	Include any additional thoughts, questions, or findings. This is my first time using Wireshark, the interface was initially overwhelming. It is noticeable that this tool is powerful and provides the user a good understanding of network traffic.

Reflections/Notes: Record additional notes.