Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 4th Nov, 2024	**Entry:** 1
Description	Security incident at a healthcare clinic caused by ransomware attack through phishing emails. The clinic's files were encrypted, disrupting operations and demanding a huge ransom in exchange for restoring access to the encrypted files.
Tool(s) used	IDS/IPS tools, SIEM tools, firewall, antivirus softwares
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Organized group of unethical hackers known for targeting healthcare and transportation sectors. ● **What** happened? Phishing emails were sent to employees with malicious attachments. Upon opening, the attachment deployed ransomware, encrypting critical files and displaying a ransom note demanding payment. ● **When** did the incident occur? Tuesday at approximately 9:00 a.m. ● **Where** did the incident happen?

	A small healthcare clinic in the U.S. ● **Why** did the incident happen? The attackers used phishing emails to exploit the clinic's network vulnerabilities, targeting employees with malicious links and attachments to deploy ransomware.
Additional notes	Consider the clinic's preparedness for similar attacks. Enhanced security awareness training for employees and stricter email filtering could prevent future incidents. Regular backups and a defined incident response plan would aid in faster recovery.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
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?
Additional notes	Include any additional thoughts, questions, or findings.