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: July 21, 2025	**Entry:** 1
Description	Ransomware attack on a small U.S. healthcare clinic caused by a phishing campaign. Critical patient files were encrypted, forcing the clinic to shut down operations. This entry documents the key details and analysis of the incident.
Tool(s) used	- Email Security Gateway (e.g., Proofpoint, Mimecast) - Endpoint Detection and Response (EDR) - SIEM platform (e.g., Splunk, Microsoft Sentinel) - Threat Intelligence Feeds - Incident Response Plan Document
The 5 W's	Who caused the incident? An organized group of unethical hackers known for targeting healthcare and transportation sectors. They gained access via phishing emails. What happened? The attackers sent phishing emails with malicious attachments. When an employee opened the attachment, ransomware was installed and encrypted sensitive files. A ransom note demanding payment appeared on the infected

	systems. When did the incident occur? Tuesday morning at approximately 9:00 a.m. Where did the incident happen? At a small healthcare clinic in the United States. The attack affected the clinic's internal network and employee workstations. Why did the incident happen? Due to successful phishing attacks and lack of endpoint detection or advanced email security. Employees downloaded a malicious attachment, triggering the ransomware.
Additional notes	- The incident highlights the importance of cybersecurity awareness training, especially regarding phishing threats. - It also underscores the need for endpoint protection, regular backups, and strong incident response protocols. - The clinic likely had no zero-trust or segmentation in place, allowing lateral movement. - Recommend implementation of MFA, secure email gateways, and regular phishing simulations.