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: October 17, 2025	**Entry:** 1		
Description	Ransomware attack on a U.S. healthcare clinic that disrupted business operations. The incident involved phishing emails with malicious attachments that deployed ransomware, encrypting critical patient data and system files.		
Tool(s) used	None specified at this stage. Potential tools for investigation could include: antivirus software, email security gateways, network monitoring tools, forensic analysis tools, and incident response platforms.		
The 5 W's	**Who caused the incident?** An organized group of unethical hackers known to target healthcare and transportation industries. **What happened?** Ransomware attack encrypted all company files and critical patient data. Employees were unable to access medical records and software. A ransom note was displayed demanding payment for the decryption key. **When did the incident occur?** Tuesday morning at approximately 9:00 a.m. **Where did the incident happen?** At a small U.S. healthcare clinic specializing in primary-care services. **Why did the incident happen?** The attackers gained access through targeted phishing emails sent to several employees. The emails contained malicious attachments that installed malware when downloaded, which then deployed the ransomware.		
Additional notes	This incident highlights the importance of employee security awareness training, particularly regarding phishing emails. Questions to consider: What specific ransomware variant was used? Were backups available? What was the recovery process?		

Date: October 17, 2025	**Entry:** 1		
	Were authorities notified? This case demonstrates the vulnerability of healthcare organizations to targeted cyberattacks and the critical need for robust email security and incident response plans.		

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.		