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: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	A small U.S. healthcare clinic experienced a ransomware attack that encrypted critical patient files and disrupted daily operations. Employees were locked out of their systems and presented with a ransom note demanding payment for decryption.
Tool(s) used	Email security gateway, antivirus logs, and incident documentation tools
The 5 W's	Capture the 5 W's of an incident. • **Who:** A known organized group of unethical hackers targeting healthcare and transportation industries. • **What:** A ransomware attack delivered via phishing emails containing malicious attachments; files were encrypted, and a ransom note was displayed. • **When:** Tuesday morning at approximately 9:00 a.m. • **Where:** Internal network of a small U.S. healthcare clinic.

	• **Why:** The attackers sought financial gain by demanding ransom payment for the decryption key.
Additional notes	The attack originated from phishing emails opened by employees, highlighting the need for stronger user awareness training and improved email filtering. Future preventive measures should include staff phishing simulations, regular backups, and endpoint protection to minimize the impact of future attacks.
