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: 03.04.2025	**Entry:** 1
Description	Documenting security incident of a healthcare company
Tool(s) used	
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: Phishing email that contained a malicious attachment with ransomware • **When**: Tuesday at 9:00 a.m. • **Where**: Small U.S. health care clinic • **Why**: The group demanded ransom for decrypting the patient data
Additional notes	Was the ransom paid? Where employees trained in cybersecurity? Was there anu anti-malware software present?