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: 27/09/2025	**Entry:** 1
Description	A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.
Tool(s) used	N/A
The 5 W's	● **Who** caused the incident? **Employees who accessed the malicious email link.** ● **What** happened? **Social Engineering attack by hackers made employees access a malicious attachment which resulted in a ransomware attack.** ● **When** did the incident occur? **9:00am, Tuesday** ● **Where** did the incident happen? A small healthcare clinic in the US. ● **Why** did the incident happen?

	Several employees were sent a malicious email attachment. Once accessed, malware was loaded onto the computer, infiltrating the company's network.
Additional notes	Were there no anti-virus or IAM modules installed on the computers to prevent such an incident?