



Incident Handler Journal

Instructions

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.

Date: July 23, 2024	Entry: #1
Description	Cybersecurity incident
Tool(s) used	N/A
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who: Organized group of unethical hackers• What: Ransomware attack• When: Tuesday, 0900 hours• Where: U.S. healthcare clinic• Why: Successful phishing attack by unethical hackers. After access was gained, ransomware was put on the company's system, encrypting files. Hackers appear to be financially motivated - requested a large sum of money in exchange for the decryption key.
Additional notes	<ol style="list-style-type: none">1. How can an incident similar to this one be prevented in the future?2. Are the files critical to the company? Should the ransom be paid for the decryption key?