

# 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.

<b>Date: Apr 9, 2024</b> Record the date of the journal entry.	<b>Entry:</b> Record the journal entry number.
Description	A U.S. healthcare clinic faced a security breach on a Tuesday morning around 9:00 a.m. Employees found themselves unable to access files like medical records, which is halting business operations. A ransom note appeared on their screens, informing them that all files had been encrypted by hackers demanding a hefty ransom for decryption. The attackers infiltrated the network via targeted phishing emails, distributing malware through malicious attachments. Their ransomware attack crippled access to critical patient data, forcing the clinic to shut down systems and seek external assistance.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none"><li><b>Who</b> caused the incident? <b>Group of unethical hacker</b></li><li><b>What</b> happened? <b>Ransomware security incident</b></li><li><b>When</b> did the incident occur? <b>Tuesday at 9:00 am</b></li><li><b>Where</b> did the incident happen? <b>U.S Healthcare Clinic</b></li><li><b>Why</b> did the incident happen? <b>The breach occurred due to unethical hackers exploiting a phishing attack to infiltrate the company's systems. Once inside, they deployed ransomware, encrypting vital files. Their motive seems financial, as evidenced by the ransom note demanding a substantial sum in exchange for the decryption key.</b></li></ul>
Additional notes	They should implement security hardening.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.

