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: 08.23.2024	**Entry:** 1
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Organized group of unethical hackers known to target healthcare companies ● **What**: Ransomware Security Incident ● **When**: Tuesday @ 9:00 AM ● **Where**: Healthcare company ● **Why**: The incident unfolded due to unethical hackers gaining access to sensitive data by deploying a phishing attack to several employees. This attack launched malicious code upon opening email link which would encrypt sensitive files and deploy ransomware message. The group of hackers seem to be motivated financially and would exchange a large sum for the decryption key.
Additional notes	1) In most ransom cases, even if they pay the total amount, this does not prevent them from asking for more or even turning over the decryption key... Should they pay the ransom? 2) We should install a training regiment that would inform employees of typical phishing emails and help prevent future attacks.