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: 04.04.24 Record the date of the journal entry.	**Entry:** Record the journal entry number. 3
Description	Provide a brief description about the journal entry. Documentation of USA banking industry phishing incident
Tool(s) used	List any cybersecurity tools that were used. Online research, AlienVault OTX
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Akira and Royal ransomware groups ● **What** happened? An employee opened an unknown file named “AKIRA.EXE” via email that contained a malicious payload which spread through the employee's computer and subsequently infected several other machines within the organization's network. ● **When** did the incident occur? April 6, 2023 and April 12, 2023 ● **Where** did the incident happen? USA, Washington DC ● **Why** did the incident happen?

	The malicious file was not detected by the employee’s computer and was able to run, the employee did not practice proper practices regarding phishing and it is possible that the systems on the employee’s computer was not updated regularly. Ransomware groups are money motivated.
Additional notes	Include any additional thoughts, questions, or findings. https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/