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: Date	**Entry:** Entry #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who**: an organized group of unauthorized hackers • **What**: ransomware security incident • **When**: Tuesday at 9:00am • **Where**: Health care company • **Why**: Phishing attack turned into and looking to launch ransomware for monetary gain
Additional notes	Include any additional thoughts, questions, or findings.

Date:	**Entry:**

August 15th, 2023	Entry#2
Description	Documenting a cybersecurity incident
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who** Employee who attempted to access a dangerous file. • **What** A suspicious file being downloaded on an employee's computer. • **Where** At the office. • **Why** The employee entered his password into an unknown site. The payload was then installed onto his computer.
Additional notes	Include any additional thoughts, questions, or findings.

Date: August 15, 2023	**Entry:** Entry #3
Description	After figuring out the file's hash was malicious, we must now document it.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** The employee that opened the file. • **What** We must now use the playbook to fill out information about harm • **Where** In the office. • **Why** Inappropiate handling of external files.
Additional notes	Include any additional thoughts, questions, or findings.