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: Record the date of the journal entry.	**Entry: January 28, 2025**
Description	Journal Entry #1; Ransomware on U.S health care clinic
Tool(s) used	A social engineering technique was used called phishing via email.
The 5 W's	Capture the 5 W's of an incident. • **The incident was caused by a malicious actor; the victim clicked on the bait.** • **A malicious actor sent a phishing email to an employee that contained ransomware.** • **The incident happened on a Tuesday at 9.00am.** • **The incident happened at a U.S health care clinic.** • **Ransomware involves malware and a ransome of money.**
Additional notes	The phishing emails were sent to all employees.

Date: Record the date of the journal entry.	**Entry: January 28, 2025**
Description	Journal Entry #2
Tool(s) used	**VirusTotal.com**
The 5 W's	Capture the 5 W's of an incident. • **The incident was caused by an outside threat actor.** • **An email was sent to an employee that tricked them into revealing password information and it contained trojan malware.** • **The incident occurred between 1:10 - 1:20 p.m.** • **The incident occurred during working hours at the company.** • **An employee was tricked**
Additional notes	The trojan can damage or do more potential harm to systems.

Date: Record the date of the journal entry.	**Entry:** January 29, 2025
Description	Journal Entry #3
Tool(s) used	SIEM tool
The 5 W's	Capture the 5 W's of an incident. • **Malicious threat actor** • **Customer data theft**

	• **At approximately 3:13 p.m., PT, on December 22, 2022** • **Company website** • **Company website vulnerability**
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** January 31, 2025
Description	Journal Entry #4
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. • **IP from Buttercup Games** • **Failed authentication** • **9/8/22 6:13pm** • **Buttercup Games mail server** • **Authentication error**
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** January 31, 2025
Description	Journal Entry #5
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. • **An outside malicious threat actor** • **The threat actor sent phishing emails to employees** • **The incident occurred at 4:45am** • **Incident happened in the company network** • **An employee was a victim of social engineering attack**
Additional notes	Include any additional thoughts, questions, or findings.

	•