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: 3/31/2025	**Entry:** 1
Description	A small US health care clinic was hit with a ransomware attack where a significant number of employees lost the ability to access patient data and as such the hospital closed.
Tool(s) used	none
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers instigated the ransomware attack for the sake of personal profit. • **What** happened? The ransomware encrypted the computers data and requested money from the organization in order to allow employees to start accessing patient data again. • **When** did the incident occur? Tuesday at 9AM. • **Where** did the incident happen? The healthcare company.

	• **Why** did the incident happen? The attack happened because unethical hackers motivated by money were able to exploit a flaw in whatever email firewall exists allowing for a successful fishing attack. Through this a ransomware was installed which would be how the hackers would gain a profit.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 4/2/25	**Entry:** 2
Description	Analysis of a phishing email incident at a financial services company
Tool(s) used	VirusTotal.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The individual who sent the malicious email. • **What** happened? An Hr employee received a phishing email from someone posing as Clyde West from Def Communications reaching out for a job. • **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM • **Where** did the incident happen? In the employees inbox. • **Why** did the incident happen? The malicious actor wanted to compromise the employees account.

Additional notes	Include any additional thoughts, questions, or findings.

Date: 4/2/25	**Entry:** 3
Description	The analysis of a final report of a e-commerce companies incident where user data was exposed through a web vulnerability.
Tool(s) used	Looked through a final report
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A malicious actor seeking ransom payment • **What** happened? A malicious actor requested $50,000 in order to not leek customer data onto forums • **When** did the incident occur? December 28, 2022, at 7:20 p.m., PT • **Where** did the incident happen? In the ecommerce web application through forced browsing • **Why** did the incident happen? To earn money
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
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** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
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** caused the incident? • **What** happened?

	• **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
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** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

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.