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: 3/6	**Entry:** One
Description	Ransomware Attack at health company
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? • The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. • **What** happened? • A small U.S. health care clinic experienced a RANSOMWARE attack which severely disrupted their business operations. • **When** did the incident occur? • 9:00 AM tuesday • **Where** did the incident happen? • The health clinic headquarter • **Why** did the incident happen?

	• Lack of employee training and weak security controls
Additional notes	The organization should establish a more robust security framework and implement mandatory employee cybersecurity training programs, This incident may have exposed sensitive patient data, leading to potential HIPAA violations and reputational damage.

Date: 19/6/2025	**Entry:** Two
Description	Phishing attack on financial services company
Tool(s) used	VIRUS TOTAL ,Phishing PlayBook
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • The cause of the incident was a phishing attack contain malicious file encrypted by a password one the employee download the file and decrypted it with the password send with it a multiple unauthorized executable files where detected by ids • **What** happened? • A financial services company experienced a phishing attack that led to multiple unauthorized executable files to be downloaded. • **When** did the incident occur? • **1:15 p.m.** • **Where** did the incident happen? • An employee device

	• **Why** did the incident happen? • Lack of employee awareness on phishing attacks and lack of ips on end point device
Additional notes	Include any additional thoughts, questions, or findings

---

Date: Record the date of the journal entry.	**Entry:** 3
Description	review data breach final report.
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? -Vulnerability in the e-commerce app that allows the attacker to perform a forced browsing attack. • **What** happened? -Retail company experience major data breach affecting over one million users. • **When** did the incident occur? - ON 3:13 pm , pt , December 22,2022 an employee receives an email from an external address claiming that he has stolen customers data and demands a payment of 15,000 dollars the employee thought it was a scam and delete it . - ON December 28,2022 the same sender sent another email with proof of the stolen data and raised the price to 50.000 dollars .

	• **Where** did the incident happen? -vulnerability In the e-commerce app ,purchase confirmation page • **Why** did the incident happen? -The incident could be avoided if there is routine penetration testing on the app and implementing access control can significantly reduce the chance of breech happening.
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.

- Reflection :

- Were there any specific activities that were challenging for you? Why or why not?
- Has your understanding of incident detection and response changed since taking this course?
- Was there a specific tool or concept that you enjoyed the most? Why?