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: 10/08/2025	**Entry:** 1st
Description	Documenting a cybersecurity incident.
Tool(s) used	Ransomeware A ransomware is a malicious program that encrypt important user data and asks for ransome to decrypt them.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers who specifically target the health care industry. • **What** happened? Critical files in employee computers were encrypted • **When** did the incident occur? The incident occurred on Tuesday at 9:00 a.m • **Where** did the incident happen? The incident happened at a small U.S. health care clinic specializing in delivering primary-care services. • **Why** did the incident happen?

	The attack was done for financial gains as the group demanded a hefty ransome to decrypt the files.
Additional notes	The attack was a classic example of social engineering using phishing email that installed malicious ransomware on the employee computers locking down the files.

Date: 14/07/2025	**Entry:** 2nd
Description	Documenting a file hash analysis with virustotal
Tool(s) used	Virus total Virus total is an online platform that can be used to upload files, URL, file hash to get them scanned to check if they are safe or not.
The 5 W's	• **Who** caused the incident? A malicious actor who wanted to find company secrets. • **What** happened? Attacker sent a malicious file attached to a mail that looked like a legitimate file so after my investigation the alert is further escalated. • **When** did the incident occur? The incident occurred on Thursday 01:11 pm • **Where** did the incident happen? At a financial service company • **Why** did the incident happen? The attacker was trying to get sensitive information from the employee computers.

Additional notes	It is fascinating how social engineering can still be one of the most effective attack types even when someone is well aware of them.

Date: 15/08/2025	**Entry:** 3rd
Description	Using phishing playbook to respond to a phishing incident
Tool(s) used	Playbook
The 5 W's	• **Who** caused the incident? The incident was caused by a malicious actor using a phishing email. • **What** happened? Employee who received the email opened the attachment containing malware • **When** did the incident occur? The incident occurred around 01:11pm • **Where** did the incident happen? The incident was • **Why** did the incident happen?
Additional notes	Playbooks are an essential part of the response lifecycle as they help employees by providing them a clear step based standardized process with less room for confusion.

Date: 15/08/2025	**Entry:** 4th
Description	Reviewing a Final report
Tool(s) used	none
Details Found	• A hacker who gained access to customer PII by exploiting a vulnerability in the web application • The attacker sent an email with PII of customers and a demand of $50,000 to delete the data he has. • Occurred around 07:20pm • The incident happened at the e-commerce web app of the organisation. • The attacker wanted to get financial gain by stealing sensitive financial information about the customers.
Additional notes	Reading a final report gave me a lot of insight on how these are documented and why it is important to make a final report in the post-incident activity phase of the incident response lifecycle.

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: 1. Were there any specific activities that were challenging for you? Why or why not?

I found the chat dialogue with the coach a bit tricky. Sometimes you can't pinpoint what exactly he wants you to answer. As sometimes his questions can be a bit difficult to understand but that is on my part no that coach was not helpful.

2. Has your understanding of incident detection and response changed since taking this course?

I definitely now have a better and thorough understanding of what the process of actual detection and response include, how to respond what steps to take and how team work and clear communication is very important for an effective incident response.

3.Was there a specific tool or concept that you enjoyed the most? Why?

I enjoyed learning about splunk and chronicle as it gave me a real insight in how these SIEM tools work and how they actually look 😂.

I found them most enjoyable as it was something I was looking forward to them.