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: 7/14/25	**Entry:** #1
Description	Documenting a cybersecurity incident. (Containment)
Tool(s) used	None.
The 5 W's	● **Who:** An organized group of unethical hackers. ● **What:** A ransomware security incident. ● **Where:** A small U.S. health care clinic specializing in delivering primary-care services. ● **When:** Tuesday at 9:00 a.m. ● **Why:** The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company.
Additional notes	We need to investigate the targeted employees and incorporate a standard phishing awareness program in the health care clinic going forward.

Date: 7/16/25	**Entry:** #2
Description	Documenting a cybersecurity incident. (Detection and Analysis)
Tool(s) used	Sha256, Virustotal
The 5 W's	● **Who:** Unknown threat actor. ● **What:** A malware security incident. ● **When:** 1:15 pm. ● **Where:** Financial services company. ● **Why:** Employee downloaded malware and then opened it.
Additional notes	I am currently investigating the sha256 hashing of this malware on virustotal to gain deeper insight into what we're dealing with.

Date: 7/17/25	**Entry:** #3
Description	Reviewing a final report. (Post-Incident Activity)
Tool(s) used	None.
The 5 W's	● **Who:** Lone threat actor. ● **What:** Data exfiltration. ● **When:** December 28, 2022, at 7:20 p.m. PT. ● **Where:** Mid-sized retail company. ● **Why:** Vulnerability exploited in the e-commerce web application.
Additional notes	It's pretty crazy this happened as I'm being trained to handle security incidents

	just like this. I will be sure to commit this to memory and use it as a significant reference in my future at the company.

Date: 7/18/25	**Entry:** #4
Description	Utilizing Splunk. (Detection and Analysis)
Tool(s) used	Splunk (SIEM)
The 5 W's	● **Who:** Undetermined. ● **What:** Mail server investigation. ● **When:** Before 7/28/25 at 6:19:58. ● **Where:** Buttercup Games (e-commerce store). ● **Why:** Tasked with specific investigation.
Additional notes	For preliminary findings, there are 346 events that have occurred as failed SSH logins for the root account.

---

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

   Analyzing the sha256 trojan on Virustotal was a bit challenging for me. Mostly due to the fact that I wasn't sure of how to navigate the site or the findings until I really broke it down within the exemplar and took the extra time to really understand it.

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

   Absolutely. I had next to no knowledge on incident detection and response prior to this course. And now? It's like a whole other world just opened itself.

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

   I think the two tools I enjoyed the most were investigating with Virustotal and investigating with Splunk. Virustotal for the extra effort needed to really comprehend my findings and to see how involved the cyber security community is. Splunk for adding practicality to what I'll be doing in the near future and for really getting a sense of the 'professional' aspect to cyber security professionals.