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: April 27th 2025	**Entry:** 1
Description	A small health care clinic had a security incident on Tuesday 9 am. Their systems were encrypted by ransomware, which was downloaded to one of the systems due to a phishing email attachment. The threat actors are an organized group of unethical hackers that are asking for a considerable sum of money in exchange for the decryption key.
Tool(s) used	List any cybersecurity tools that were used. N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers • **What** happened? An employee downloaded an attachment from a phishing email, which encrypted the company's files. • **When** did the incident occur? 9 am on Tuesday • **Where** did the incident happen? A small US healthcare clinic • **Why** did the incident happen? An employee downloaded an attachment from a phishing email.
Additional notes	Periodic training on the dangers of phishing emails may be necessary for the employees in this clinic.

Date: April 29th 2025	**Entry:** 2
Description	Malware phishing attack. An employee received an email with a file that they downloaded and executed.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who:** A threat actor that sent the file to the employee, and the employee who downloaded and executed the file. • **What:** A file was downloaded and executed by an employee. The file created multiple unauthorized files on the employee's computer. • **When:** The email was received at 1:11pm, and executed4 minutes later. • **Where:** On an employee's computer. • **Why:** A phishing email got through our spam filter. The file attached to the email was then executed by an employee.
Additional notes	The employee's computer may need to be restored to a backup. The email spam filter needs to be improved. Training about phishing is necessary. The IDS should have responded sooner and may need to be improved.

Date: April 29th 2025	**Entry:** 3
Description	A phishing attack led to PII getting compromised, leading to $100,000 in damages
Tool(s) used	**INCIDENT FINAL REPORT**
The 5 W's	Capture the 5 W's of an incident. • **Who**: A threat actor • **What**: Someone tried to blackmail the company after they stole PII • **When:** December 22 2022 • **Where**: A mid-sized retail company • **Why**: Someone found a vulnerability in the e-commerce web application. They used the vulnerability to perform a forced browsing attack and obtained the PII of 50,000 users. They used this to try and blackmail the company.
Additional notes	The company should perform routine vulnerability scans and penetration testing. A penetration test might have found this vulnerability before a threat actor could find it.

Date: May 1st 2025	**Entry:** 4
Description	Examining logs in Suricata using Linux
Tool(s) used	Suricata and Linux CLI
The 5 W's	Capture the 5 W's of an incident. • **Who:** I did. To practice Suricata • **What:** I examined a custom rule/signature and applied it to a provided captured packets file sample.pcap • **When:** Today • **Where:** In my home • **Why:** Because practicing Suricata on Linux is a good way to practice
Additional notes	I didn't know you could apply Signatures to previously captured data packets. I thought it only examined live network traffic.

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: The five Ws is a useful way to write comprehensive notes. I have used similar rules for incident note taking before, for Tech support. ABS: Action, Blocker, Solution