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: 22/06/25 Record the date of the journal entry.	**Entry: 001** Record the journal entry number.
Description	Documenting a cybersecurity incident.
Tool(s) used	None.
The 5 W's	• **Who:** An organized group of unethical hackers. • **What:** A ransomware security incident. • **When:** On Tuesday at 9a.m. • **Where:** In a small U.S. healthcare clinic. • **Why:** The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	Proper training for the employees for Social engineering attacks is a must and either IDS or IPS should be installed to take a proactive approach.

Date: 24/06/25 Record the date of the journal entry.	**Entry: 002** Record the journal entry number.
Description	Documenting a cybersecurity incident.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who**: A malicious actor. • **What**: A malicious file was downloaded. • **When**; At 1:11pm. • **Where**; At a financial services company. • **Why**: The incident happened because an employee while downloading a file which was password protected, failed to understand that it was malicious and hence various executable files were downloaded in the system, resulting in an attack.
Additional notes	1. Employees must be given proper training to not download files from unauthorized places. 2. How was the malware discarded from the computer?

Date: 25/06/25 Record the date of the journal entry.	**Entry: 003** Record the journal entry number.
Description	Documenting a phishing alert mitigation using playbook.

Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who**: Def communications phishing email. • **What**: Contained a malicious exe file that was downloaded in the user's system. • **When**: At 1:11 PM. • **Where**: At Inergy company. • **Why**: Escalated to Level-II SOC Analyst, because the email contained a malicious executable file, which after downloading created various executable programs, leading to a phishing attack.
Additional notes	The file had an extension of .exe and there were grammatical errors along with spelling mistakes.

Date: 25/06/25 Record the date of the journal entry.	**Entry: 004** Record the journal entry number.
Description	Reviewing a final report.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who:** An attacker. • **What**: The attacker has stolen the customer data and asked for $50,000 for not releasing the data to the public. • **When**: On December 28, 2022 at 7:20pm.

	• **Where**: A mid-sized retail company. • **Why**: There was a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.
Additional notes	Regular vulnerability scans and penetration testing should be performed. The final report has been reviewed.