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: 1/25/2026	**Entry:** 1
Description	Ransomware attack on a small U.S. health care clinic that disrupted business operations
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • An organized group of unethical hackers caused the incident • A phishing email was sent containing a malicious attachment. Once downloaded, ransomware was deployed encrypting the computer files. • The incident occurred on Tuesday at 9:00am • The incident occurred at a small U.S. health care clinic. • The reason behind the incident is likely financial gain.
Additional notes	What specific date did it occur on and what did the company do about it?

Date: 1/25/2026	2
Description	Cybersecurity Incident pertaining to malicious payload sent via email
Tool(s) used	SHA256, VirusTotal
The 5 W's	Capture the 5 W's of an incident. • Unknown who caused it • An email was sent to an employee containing an attachment. A password was provided to gain access and when the employee downloaded the file a malicious payload was executed on their computer. • Occurred at 1:11pm • Financial service company • To gain access to computer network using injection
Additional notes	Need to look further into who caused it, e.g. email origins.

Date: 1/25/2026	**Entry:** 3
Description	Phishing scam
Tool(s) used	Playbook
The 5 W's	Capture the 5 W's of an incident. • Unknown who caused it

	• An employee received a phishing email and downloaded the attachment, it got flagged as malicious. • Email sent July 20, 2022, 09:330:14 am • Finance service company • To gain access to the company network.
Additional notes	

Date: 1/25/2026	**Entry:** 4
Description	Review the final report for a breach in the company before I worked there.
Tool(s) used	Packet sniffer
The 5 W's	Capture the 5 W's of an incident. • Unknown who caused it • An individual was able to gain unauthorized access to PII and steal information of around 50,000 customers. It is determined to be a ransomware attack because they demanded more money each day. • Occurred on December 28,2022 at 7:20pm, PT. • Mid-sized retail company • There was a vulnerability in the e-commerce web application. The attacker used a forced browsing attack and accessed customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.
Additional notes	