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: 5/21/24	**Entry:** #1
Description	Small US healthcare clinic experienced a ransomware attack caused by a phishing email
Tool(s) used	N/A
The 5 W's	● **Who:** Organized hacker group ● **What:** Phishing email caused a malicious attachment to be downloaded, which deployed ransomware on the organization's network. ● **When:** Tuesday at 9:00am ● **Where:** A small US healthcare clinic's network ● **Why:** A phishing email caused an employee to download a malicious attachment
Additional notes	Potential remediations: Spam filters, antivirus software, employee training

Date: 5/21/24	**Entry:** #2
Description	A financial services company had a suspicious file downloaded on an employee’s computer.
Tool(s) used	Hash analysis
The 5 W's	● **Who**: Malicious actor over email ● **What**: An email with a C2 trojan (Flagpro) was sent to an employee ● **When:** 9:30am ● **Where**: HR employee’s computer/email ● **Why:** The employee was phished which caused them to click on the attachment, which downloaded it to the PC.
Additional notes	According to VirusTotal, the attachment is a malicious C2 Trojan (Flagpro). Ticket has been escalated.

Date: 5/22/24	**Entry:** #3
Description	Packet analysis with Wireshark
Tool(s) used	Wireshark
The 5 W's	● **Who**: User connecting to an internet site ● **What:** Network telemetry was recorded about this connection ● **When**: 12:34pm ● **Where**: Within the organization’s intranet ● **Why**: A user connected to an internet site and transferred data
Additional notes	

Date: 5/22/24	**Entry:** #4
Description	Final report review of major security incident
Tool(s) used	None
The 5 W's	● **Who**: A black-hat hacker ● **What:** A data breach leaked customer transaction information via a vulnerability in a web application ● **When**: December 28, 2022 at 7:20PM ● **Where**: The e-commerce website and internal network of the organization ● **Why**: A vulnerability in an e-commerce web app allowed an attacker to perform a forced browsing attack that revealed customer transaction data via a purchase confirmation page.
Additional notes	Include any additional thoughts, questions, or findings.

Reflections/Notes: Record additional notes.