Incident handler's journal

Date: July 14, 2024	**Entry:** #1
Description	Documenting a security incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who:** A group of unethical hackers ● **What:** A ransomware security incident ● **When:** Tuesday at 9:00 am ● **Where:** At a small U.S. health care clinic ● **Why:** Employees were victims of a phishing attack.
Additional notes	None.

Date: July 15, 2024	**Entry:** #2
Description	Documenting a suspicious file hash
Tool(s) used	VirusTotal to analyze the file hash. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I

	had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	Capture the 5 W's of an incident. - **Who:** BlackTech - **What:** A phishing attack aim at an employee email with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b - **When:** 1:11 p.m. - **Where:** At a financial services company - **Why:** An employee downloaded and executed a file attach to a malicious email
Additional notes	The malware in question is known as Flagpro. I choose to escalate the alert ticket to a level-two SOC analyst to take further action. How can this type of incident be prevented in the future? Should we consider improving the employees security awareness with training?

Date: July 16, 2024	**Entry:** #3
Description	Documenting a data breach
Tool(s) used	Not specified
The 5 W's	Capture the 5 W's of an incident. - **Who:** A hacker - **What:** A ransomware security incident

	● **When:** December 28, 2022 ● **Where:** At a mid-sized retail company ● **Why:** A vulnerability in the e-commerce web application. The security team found that by modifying the order number in the URL you could access customers data.
Additional notes	1. Should the company pay the ransom? 2. How could the team prevent an incident like this to happen?

Date: July 16, 2024	**Entry:** #4
Description	Documenting a phishing investigation
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who:** Not identified ● **What:** A Phishing email ● **When:** July 8, 2023 ● **Where:** at a financial services company ● **Why:** An employee received a phishing email in their inbox.
Additional notes	None.
