Incident handler's journal

Date: 11/21/2025	**Entry:** #1
Description	Record documenting a security event affecting a healthcare organization.
Tool(s) used	No tools were necessary for producing this report.
The 5 W's	● **Who:** A coordinated team of malicious, unethical hackers. ● **What:** A ransomware-related security breach. ● **Where:** Within a company operating in the healthcare sector. ● **When:** Tuesday morning at around 9:00 a.m. ● **Why:** The attackers infiltrated the company's environment through a phishing message. Once inside, they executed ransomware that encrypted vital operational data. Their motive appears to be financial, as they left a ransom note demanding a substantial payment for the decryption key.
Additional notes	1. What preventive measures could the healthcare company implement to avoid similar attacks in the future? 2. Is paying the ransom a viable or advisable option for recovering the encrypted data?

Date: 11/22/2025	**Entry:** #2
Description	Analyzed network traffic in *sample.pcap* to inspect IPs, protocols, and DNS/TCP/ICMP packets.

Tool(s) used	Wireshark Windows VM (Qwiklabs)
The 5 W's	● **Who:** A legitimate user generating normal web traffic. ● **What:** Normal network communication occurred, including DNS queries, HTTP traffic, TCP sessions, and ICMP packets. ● **Where:** Within the Windows VM environment. ● **When:** During the timeframe captured in *sample.pcap*. ● **Why:** To analyze web traffic and practice Wireshark filtering.
Additional notes	Applied filters (DNS, TCP, ICMP, MAC). Confirmed DNS resolution for opensource.google.com. No malicious activity observed.

Date: 11/23/2025	**Entry:** #3
Description	Investigated a malicious spreadsheet file received via email. Generated SHA256 hash and analyzed it using VirusTotal to identify IoCs.
Tool(s) used	VirusTotal
The 5 W's	● **Who:** A threat actor distributing a malicious spreadsheet via email. ● **What:** An employee downloaded and opened a password-protected spreadsheet containing a payload that executed malware on their computer. SOC received an alert from the IDS. ● **Where:** On the employee’s workstation within the corporate network. ● **When:** Between 13:11 and 13:20, based on the email receipt, file execution, and IDS alert timeline.

	● **Why:** The employee opened a malicious file attached to a phishing email, executing malware.
Additional notes	1. VirusTotal confirmed the file as malicious. 2. Identified IoCs: additional hashes, malicious IP, and domain contacts. 3. Behavior observed in sandbox: unauthorized executable creation, registry/file modifications, and network connections.

Date: 11/24/2025	**Entry:** #4
Description	Reviewed the organization's final incident report to understand the lifecycle of a major data breach affecting over one million users.
Tool(s) used	Final Incident Report (provided by the company) Internal SOC documentation
The 5 W's	● **Who:** An external threat actor exploiting vulnerabilities in the company's e-commerce web application. ● **What:** A major data breach occurred: attackers accessed and exfiltrated customer data by exploiting a web application flaw. ● **Where:** Within the company's e-commerce platform and supporting infrastructure. ● **When:** During the period outlined in the report's timeline section (exact times documented in the final report). ● **Why:** Due to an unpatched vulnerability and insufficient security controls within the web application, allowing attackers to gain unauthorized access.
Additional notes	Focused on understanding: 1. Root cause explained in the *Investigation* section

	2. Attack method used to exploit the web vulnerability 3. Incident response actions listed in the *Timeline* 4. Future improvement recommendations such as access controls and routine vulnerability scans

Date: 11/25/2025	**Entry:** #5
Description	Monitored network traffic using Suricata with custom rules; triggered alerts on simulated HTTP traffic and analyzed Suricata log outputs.
Tool(s) used	Suricata IDS/IPS sample.pcap file custom.rules file jq (for JSON log analysis)
The 5 W's	● **Who:** N/A — simulated network traffic for lab exercise. ● **What:** Custom Suricata rules triggered alerts on HTTP GET requests; alerts were recorded in fast.log and detailed in eve.json for analysis. ● **Where:** On the lab virtual machine processing the sample.pcap file. ● **When:** During lab activity session (simulated timeframe). ● **Why:** The custom Suricata rule was configured to detect HTTP GET traffic from the home network to external IPs.
Additional notes	1. Alerts captured included `GET on wire` messages. 2. fast.log provided a quick summary of triggered alerts; eve.json contained full JSON-formatted event data. 3. jq tool enabled structured analysis of timestamps, flow IDs,

	protocols, alert messages, and destination IPs. 4. Destination IPs observed in alerts included 142.250.1.139 and 142.250.1.102.

Date: 11/26/2025	**Entry:** #6
Description	Phishing incident involving potential malware download.
Tool(s) used	No tools were necessary for producing this report.
The 5 W's	- **Who:** Unethical hacker (sender: Def Communications <76tguyhh6tgftrt7tg.su>) - **What:** Phishing email attempting to trick the recipient into downloading malware (`bfsvc.exe`) - **Where:** Financial services company (Inergy) - **When:** Tuesday morning around 09:30 AM - **Why:** Employee opened a malicious email attachment protected by a password (`paradise10789`). The email contained multiple spelling errors and inconsistencies, indicating a phishing attempt.
Additional notes	The attached file hash `54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b` is known to be malicious. The phishing email exploited social engineering by pretending to be a job applicant. **Preventive measures / Recommendations:** 1. Conduct regular security awareness training for employees to recognize phishing emails.

	2. Implement email filtering solutions to block suspicious attachments and domains.