Incident handler's journal

Date: 14/04/2025	**Entry:** **001**
Description	A small U.S healthcare clinic suffered a ransomware attack on a Tuesday morning around 9:00 am, disrupting operations after employees were logged out of critical systems. The attacker began through phishing emails with malicious attachment, allowing hackers to deploy ransomware that encrypted patient data. The ransom note demanded payment in exchange for the decryption key. The clinic had to shut down the systems and seek external help.
Tool(s) used	None
The 5 W's	● The U.S clinic employees and an organized group of unethical hackers ● The employers clicked on a phishing email sent by hackers and also they went ahead to download a malicious attachment, which caused a ransomware attack disrupting the business operation by encrypting critical files and demanding ransom for decryption. ● The incident occurred on Tuesday morning at 9:00 am ● The incident happened at a small U.S healthcare clinic ● It happened because the employers were deceived to click on phishing emails sent by attackers and they still went ahead to download the malicious attachment, which allowed the hackers to gain access to the network and deploy a ransomware.
Additional notes	To prevent future incidents, I recommend that the clinic should implement regular employee training on phishing awareness and a strong email filtering system. Additionally, the organization should establish an incident plan, implement a multi-factor authentication and also use the principle of least privilege to reduce the risk of unauthorized access.

Date: 16/04/2025	**Entry:** **002**
Description	As a Level 1 SOC analyst at a financial services company, I responded to an alert triggered by an Intrusion Detection System (IDS) concerning a suspicious file downloaded by an employee. The file, a password-protected spreadsheet sent via email, contained a malicious payload that executed upon opening. My investigation involved retrieving the file, generating a SHA256 hash, and using VirusTotal to uncover related Indicators of Compromise (IoCs).
Tool(s) used	VirusTotal, IDS
The 5 W's	● The employee and the threat actor that sent a phishing email ● An employee received and opened a malicious password-protected spreadsheet file from a phishing email. The file executed a payload that created unauthorized executable files, which triggered an alert from the IDS. I retrieved the file, generated its SHA256 hash, and used VirusTotal to investigate further. ● **WHEN** the incident occured (i) **1:11 p.m.** – Employee received the email (ii) **1:13 p.m.** – Employee downloaded and opened the attachment (iii) **1:15 p.m.** – Malicious executables were created (iv) **1:20 p.m.** – IDS detected the activity and generated an alert ● The incident occurred on the employee workstation of the financial service company ● The employee fell victim to a phishing email and unknowingly executed a malicious file. The attack exploited user trust and poor email hygiene. The SOC responded to mitigate potential threats and assess the malware using VirusTotal and file hashing.
Additional notes	I realized that 59 security vendors have flagged this file malicious, this is an indicator of a malware. So I recommend the importance of user awareness

	training, email filtering, and continuous SOC monitoring.

Date: 18/04/2025	**Entry:** 003
Description	Documenting the analysis of a network traffic (packet data Using Wireshark, network traffic was captured and analyzed to inspect data packets exchanged between systems. Filters were applied to examine DNS and TCP traffic, allowing identification of the types of information sent and received. This analysis supports early detection of unusual or malicious activity on the network.
Tool(s) used	Wireshark
The 5 W's	● A cybersecurity analyst (me) inspecting network traffic using wireshark ● Network packet data was captured and analyzed to examine communication between systems. Filters were applied to investigate DNS and TCP traffic for specific information and potential threats ● During a training session on wireshark on Friday 3:30 PM ● It happened on wireshark that is connected to the network under investigation ● It happened because am trying to understand the type of data being transmitted over a network, identify potential security risk and enhance my knowledge about how to navigate the device
Additional notes	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic.

Date: 19/04/2025	**Entry:** **004**
Description	As a network analyst, Am using `tcpdump` on a Linux virtual machine to capture and analyze live network traffic. The task involved identifying network interfaces, filtering and capturing live traffic, and applying filters to the captured data. This process was essential for monitoring real-time network activity and reviewing a sample capture file to answer traffic-related questions.
Tool(s) used	Tcpdump in linux virtual machine
The 5 W's	● A network analyst (me) ● Network traffic was captured and analyzed using tcpdump and also reviewing a sample packet captured file. ● This happened during a lab training session on saturday 4:21 PM ● It happened on a linux virtual machines provided by my learning platform ● It happened because I want to gain practical experience in using `tcpdump` for real-time traffic analysis, identify network patterns, and understand how to filter and interpret captured data.
Additional notes	Using tools like `tcpdump` equips analysts with the ability to monitor network traffic in real time, detect anomalies, and investigate potential threats effectively. Mastering command-line network tools is a crucial skill for incident response and forensic analysis.

Date: 20/04/2025.	**Entry:** 005
Description	As a Level 1 Security Operations Center (SOC) analyst at a financial services

	company, I continued an investigation of a phishing alert involving a malicious email attachment downloaded by an employee. After confirming the file’s hash as malicious, I followed my organization's phishing alert response playbook, conducted further steps as guided by the process, and updated the alert ticket with my final findings and resolution actions.
Tool(s) used	Incident Response Playbook
The 5 W's	● Employee and unknown threat actor who sent a phishing email ● An employee downloaded a malicious file from a phishing email. The file's hash was confirmed as known malware. Following the organization’s incident response playbook, I completed the necessary investigation. ● This occurred on Wednesday, 9:30 AM ● On the employee’s computer system ● The phishing attack was part of a social engineering attempt. The employee executed a malicious file believing it to be legitimate. The incident required verification, containment, and documentation as per standard operating procedures to prevent further impact
Additional notes	This incident reinforced the importance of having a clear, actionable incident response playbook. By following a documented process, the SOC team ensured consistent, thorough handling of phishing threats. Timely alert resolution and documentation helped improve overall organizational resilience against similar future attacks.

Throughout this exercise, I applied the 5 W’s framework Who, What, When, Where, and Why which I used to analyze and document various cybersecurity incidents. I was able to create comprehensive and organized documentation that would be useful for future reference and response actions.

This experience strengthened my understanding of how to approach real-world security alerts and emphasized the importance of accurate documentation. Using the 5 W’s not only helped ensure that no critical details were missed but also sharpened my analytical thinking and attention to detail. I now feel more confident in handling incident response tasks and contributing meaningfully to a security operations team.