Incident handler's journal.

Date: 28th July 2025	**Entry: IHJ 001**
Description	**Documenting a cybersecurity incident at the U.S clinic**
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. ● **Who:** An organised group of unethical attacker ● **What:**Ransomware security incident. ● **When:**Tuesday morning at 9:00am ● **Where:**U.S healthcare clinic ● **Why:**.The incident occurred due to a successful phishing attack that allowed malicious hackers to infiltrate the company's systems. After gaining access, the attackers deployed ransomware that encrypted essential files. Their primary motive appears to be financial, as they demanded a substantial ransom in exchange for the decryption key.
Additional notes	The healthcare clinic needs to put security measures in place to ensure there is no re-occurrence of such events. Which includes: - Employee phishing awareness training - Regular system backups - Endpoint security and antivirus deployment - Network monitoring and incident response planning - It is generally not recommended to pay the ransom, as it does not guarantee file recovery and may encourage further attacks. Alternative recovery

	strategies (backups, forensic recovery) should be prioritized.

Date:10th Aug 2025.	**Entry: IHJ 002**
Description	This entry documents a phishing security incident at **Inergy Financial Organization**. The incident involved an employee receiving a malicious email and attempting to download an infected file, which was later detected as malware.
Tool(s) used	Virustotal
The 5 W's	Capture the 5 W's of an incident. ● **Who:A phishing threat actor who sent an malicious email** ● **What**: Phishing incident involving a malicious file download ● **When:** Wednesday, July 20, 2025 09:30:14 AM ● **Where:** At Inergy finance organization ● **Why**:An employee who downloads a malicious hash file into the computer of the organisation. The file was discovered to be malicious from a threat actor.
Additional notes	It was discovered that there is a mismatch between the sender email and the name.Futher Investigation revealed that the file is malicious because its hash has been flagged by 59 of 72 security vendors .It was also revealed that this file hash is known as the malware fragpro/fragtor. Which has been previously

	used by an advanced persistent threat actor agent.Oa!S1 **Recommendations** 1. Educate employees on identifying phishing emails, including checking sender addresses carefully 2. Deploy advanced email filtering and threat detection solutions 3. Implement a policy to verify attachments and links before opening 4. Regularly monitor and analyze suspicious file hashes 5. Include phishing simulations in ongoing security awareness training

---

Date:12TH August 2025	**Entry:IHJ 003**
Description	Documenting a data theft incident of an e-commerce company
Tool(s) used	Burp Suite
The 5 W's	Capture the 5 W's of an incident. ● **Who**:A data theft attacker who gained unauthorised access to the website stole client data and sought for ransom. ● **What**:Data theft incident ● **When** 28th December 2022 ● **Where** E-comerce company ● **Why** : An attacker performed a forced browsing attack and accessed customer transaction data, then modified the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages,

	exposing customer data, which the attacker then collected and exfiltrated. **Impact** - Customer transaction and personal data were exposed - Resulting to l financial and reputational loss for the company
Additional notes	The cause of the attack was a single log source showing an exceptionally high volume of sequentially listed customer orders.

Date: 16TH AUGUST 2025	**Entry:**OHJ 004
Description	Analyzing a Packet Capture File with Wireshark
Tool(s) used	I used Wireshark to analyze a packet capture file. Wireshark is a powerful network protocol analyzer that provides a graphical interface for examining network traffic in detail. Its value in cybersecurity lies in its ability to capture, filter, and analyze packets at various layers of the OSI model. By doing so, it enables security analysts to detect anomalies, investigate potential malicious activity, troubleshoot network issues, and verify security controls. This makes Wireshark an essential tool for incident response, forensic analysis, and overall network security monitoring.
The 5 W's	Capture the 5 W's of an incident. ● **Who**:NA ● **What** :NA

	- **When**:NA - **Where**:NA - **Why** :NA
Additional notes	I had never used Wireshark before, so I was excited to begin this exercise and explore a packet capture file. At first, the interface felt overwhelming due to the large amount of data and the variety of options available. However, this also highlighted why Wireshark is considered such a powerful tool: it provides detailed visibility into network traffic at a granular level. Even in my first experience, I could see how valuable it is for learning about network protocols, analyzing communication patterns, and ultimately strengthening cybersecurity skills.

Date: 20th August 2025	**Entry:IHJ 005** Capturing my first packet
Description	For this activity, I used tcpdump to capture and analyze network traffic.
Tool(s) used	I used tcpdump to capture and analyze network traffic. Tcpdump is a command-line based network protocol analyzer that enables the real-time capture and inspection of packets. While it does not provide a graphical interface like Wireshark, it offers powerful filtering options that allow analysts to focus on specific protocols, hosts, or ports. The value of tcpdump in cybersecurity lies in its ability to quickly capture and filter traffic for troubleshooting, incident response, and forensic analysis. Its lightweight and scriptable nature makes it especially useful for monitoring traffic on remote