Incident handler's journal

Date: 1 Apr 2025 09:00 | Tuesday	**Entry:** 14202509002
Description	*Ransomware infecting the internal network through a social engineering attack originating from a targeted phishing email.*
Tool(s) used	No list of any cybersecurity tools used in this event.
The 5 W's	Capture the 5 W's of an incident. • **Who** organized group of unethical hackers • **What** Phising email incident contain ransomware • **When** Tuesday 1 Apr 2025 09:00 • **Where** Small health care clinic, US • **Why** *Business operations were shut down because unethical hackers able to* exploits human error using phishing attack. Gained access to internal network and launched ransomware on the company's systems, encrypting critical files. The financial extortion with ransom note ask quite a large pool of money in exchange for the decryption key.
Additional notes	*1.This is not something technical security controls can entirely prevent, but their effectiveness can only be maximized through employee training and awareness. The company might need to deploy and update specific playbook to counter social engineering tactics and minimize the damage they cause.* *2. Should the company pay the ransom for decryption key?*

Date: 9 April 2025	**Entry:** 94202515353
Description	Analyze the packet capture file
Tool(s) used	Wireshark
The 5 W's	Capture the 5 W's of an incident. • **Who** The handler • **What** Analyze network traffic • **When** 9 April 2025 | 3:35 PM • **Where** systems on the networks • **Why** To lnvestigate what type of traffic is being sent to and from the systems on the networks by utilize Wireshark. Identify source and destination IP addresses involved in the we browsing session, examine the protocols that are used by filters like TCP, UDP and DNS packet payload.
Additional notes	1. Its confusing to navigate around the Wireshark software. 2. Definitely need more practice for the eyes and command to begin with.

Date: 9 April 2025	**Entry:** 94202515433
Description	Capture and analyze live network traffic from a Linux virtual machine
Tool(s) used	tcpdump
The 5 W's	Capture the 5 W's of an incident. • **Who** The handler • **What** Capture network traffic with tcpdump • **When** 9 April 2025 | 3:43 pm • **Where** Lab in a Linux environment. • **Why** did the incident happen?
Additional notes	1. tcpdump using CLI to list the interface specific to tcpdump is tcpdump -D. 2. tcpdump -nn can disguise the sniffing from alerts the intruder radar. Example: sudo tcpdump -nn -r capture.pcap -v

Date: 10 April 2025	**Entry:** 104202514414
Description	Incident detection and verification
Tool(s) used	Powerpoint and VirusTotal Web Detection
The 5 W's	Capture the 5 W's of an incident. ● **Who** An unknown Malicious actors ● **What** An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **When** At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● **Where** An employee's computer at a financial services company ● **Why** Identify the hash from the VirusTotal report tab as Flagpro, a well-known malware used by advanced threat actros and provides three IoC example found in the Details, Relation and Behavior tabs. **1. Domain names**: org.misecure.com **2. IP address**: 207.148.109.242 is listed as one of many IP addresses
Additional notes	1. Is this the only alternative to uncover any malware artifacts? 2. Can this be prevented in the future?

Date: 10 April 2025	**Entry:** 104202513004
Description	Illustrate documentation best practices during the incident response lifecycle.
Tool(s) used	**Word Processor**
The 5 W's	Capture the 5 W's of an incident. ● **Who** Malicious actors ● **What** Handling incident ● **When** 20 JULY2022 | 9:30AM ● **Where** coursera theoretical place ● **Why** Theoretical alert detected that an employee have been a targeted campaign of social engineer, and opened a malicious file from the phishing email.
Additional notes	1. I did not understand this part the instruction makes me confuse. 2. This is just escalate a ticket why so hard to understand the instruction.

Date: 11 April 2025	**Entry:** 114202512335
Description	Understanding of the incident's life cycle from Final Report.
Tool(s) used	**Word Processor**
The 5 W's	Capture the 5 W's of an incident. ● **Who** Malicious actors ● **What** Data theft ● **When** 22 December 2022 | 7:20 pm ● **Where** Hypothetical organization by coursera ● **Why** Data theft by malicious actors whom manage to gain unauthorized access by exploit vulnerability from e-commerce web application, and therefore have access to customer personal identifiable information (PII) and financial information (SPII). About 50k approximately were affected and estimated around 100k in direct cost and potential loss of revenue.
Additional notes	1. What kind of identity protection that provides to the affected customer 2. I need mentor for this.

Date: 11 April 2025	**Entry:** 114202512335
Description	Understanding of the incident's life cycle from Final Report.
Tool(s) used	**Word Processor**
The 5 W's	Capture the 5 W's of an incident. ● **Who** Malicious actors ● **What** Data theft ● **When** 22 December 2022 ● **Where** Hypothetical organization by coursera ● **Why** Data theft by malicious actors whom manage to gain unauthorized access by exploit vulnerability from e-commerce web application, and therefore have access to customer personal identifiable information (PII) and financial information (SPII). About 50k approximately were affected and estimated around 100k in direct cost and potential loss of revenue.
Additional notes	1. What kind of identity protection that provides to the affected customer 2. I need mentor for this.

Date: 11 April 2025	**Entry:** 114202511505
Description	Monitor network traffic using Suricata
Tool(s) used	**Suricata**
The 5 W's	Capture the 5 W's of an incident. ● **Who** The operator ● **What** Configure Suricata and use it to trigger alerts. ● **When** 11 April 2025 | 11:50 am ● **Where** Google cloud ● **Why** Suricata tool monitors network interfaces annd applies rules to the packets that pass through the interface. Suricata determines whether each packet should generate an alert and be dropped, rejected, or allowed to pass through the interface.
Additional notes	1. I still don’t see the usage or how Suricata works in real-time . 2. I need mentor for this.

Date: 14 April 2025	**Entry:** 114202503031
Description	Overview of SIEM tools
Tool(s) used	**SPLUNK CLOUD**
The 5 W's	Capture the 5 W's of an incident. ● **Who** The operator ● **What** Configure Suricata and use it to trigger alerts. ● **When** 14 April 2025 | 03:03 pm ● **Where** Splunk cloud ● **Why** I learn the introductory activity like upload data to Splunk Cloud, perform ba sic searches on the data and answer series of questions.
Additional notes	1. I got expose to the splunk cloud platform. 2. Need to understand this and fuse it with AI.