Incident Handler's Journal

Date: 15-06-23	**Entry:** 1
Description	A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 am which severely disrupted their business operations.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? **An organised group of unethical hackers.** • **What** happened? **A ransomware was deployed encrypting the organisation's computer files.** • **When** did the incident occur? **Tuesday at 9:00 a.m.** • **Where** did the incident happen? **At the organisation's building (small U.S. health care clinic).** • **Why** did the incident happen? **Several employees were targeted by phishing emails which contained a malicious attachment that installed malware once it was downloaded.**
Additional notes	The incident was organised with time and the attacker's requested money in exchange for the decryption key. The company was forced to shut down their computer systema and contact several organisations to report and receive technical assistance.

Date: 16-06-23	**Entry:** 2
Description	A financial company employee received an email containing a malicious file attachment, which was downloaded and executed triggering an alert on the IDS.

Tool(s) used	VirusTotal and IDS
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? **An employee from a financial services company.** ● **What** happened? **An employee received an email containing a file attachment which was downloaded and executed creating several unauthorized executables files on the employee's computer. This triggered an alert in the IDS.** ● **When** did the incident occur? **Today's between 1:11 p.m. and 1:20 p.m.** ● **Where** did the incident happen? **On the financial services company offices.** ● **Why** did the incident happen? **An employee was victim from a social engineering attack leading to the subsequence installed of the malware.**
Additional notes	Why the employee downloaded and executed the file? It came from a trusted source? What actions can be taken to prevent further events like those? The malicious file was retrieved to create a SHA256 hash of the file with number 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Date: 16-06-23	**Entry:** 3
Description	An investigation has begun to evaluate a phishing alert containing a file attachment which has been already identified as malicious.
Tool(s) used	VirusTotal, IDS and Phishing Incident Response playbook
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? **A malicious actor identified as "Clyde West"**

	● **What** happened? **A malicious file was downloaded and executed through a phishing email attack using password protection.** ● **When** did the incident occur? **Wednesday, July 20, 2022 09:30:14 AM** ● **Where** did the incident happen? **HR employee's workstation** ● **Why** did the incident happen? **An employee was victim of a social engineering attack.**
Additional notes	The file was already identified as malicious using the VirusTotal website tool, known malicious file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b Grammar errors detected at the Subject line as on the body text. The sender's email address doesn't match with the name on the signature. The IP address it is suspicious due to the sequence.

Date: 16-06-23	**Entry:** 4
Description	Review of the final report related to the security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ● **What** happened? ● **When** did the incident occur? ● **Where** did the incident happen? ● **Why** did the incident happen?

Additional notes	Include any additional thoughts, questions, or findings.

Date: 17-06-23	**Entry:** 5
Description	Search perform using SPLUNK cloud tool to identify log data related with login failed attempts. This action is related to the NIST Incident Response Lifecycle phase, *Detection and Analysis*. Here, the tool was used to read the logs file related with the incident to determine if a website was malicious or not.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ● **What** happened? ● **When** did the incident occur? ● **Where** did the incident happen? ● **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.
