Incident handler's journal

Date: 09/08/2024	**Entry: 1**
Description	Ransomware health clinic
Tool(s) used	N/A

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ This incident was caused by an unethical hacker; it is currently unknown whether they are internal or external.
	• **What** happened?
	  ○ The threat actor managed to access the company's email network and carried out a phishing attack. The emails contained an attachment with malware that included ransomware. Once deployed, the ransomware encrypted the key and critical files necessary for the clinic's operations.
	• **When** did the incident occur?
	  ○ This incident occurred on 08/09/2024 at 09:00 AM.
	• **Where** did the incident happen?
	  ○ This incident occurred on the clinic's computers, where the files and software necessary for its operation were stored.
	• **Why** did the incident happen?
	  ○ This incident occurred due to human error, where someone fell for the phishing scam, allowing the attacker to execute their ransomware.

Additional notes	A backup system that adheres to the 3-2-1 rule (3 copies, 2 different formats, 1 minimum off-site location) is recommended. Additionally, a cybersecurity

	training campaign for employees should be conducted to reduce the likelihood of them falling victim to another phishing attack or any other form of social engineering attack.

Date: 28/12/2022	**Entry: 2**
Description	Filtering Customer PII and financial information
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ Unknown individual ● **What** happened? ○ An employee received an e-mail where the attacker asked for a crypto payment ensuring stolen customer data. The first e-mail asked for a $25,000 cryptocurrency payment and the second e-mail increased the payment asking for a $50,000 cryptocurrency payment. The employee received a second e-mail because he checked the first e-mail as spam. ● **When** did the incident occur? ○ December 22, 2022 at 15:13:00 ● **Where** did the incident happen? ○ The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying 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. ● **Why** did the incident happen? ○ The incident occur for vulnerabilities in the web-site of the e-commerce
Additional notes	Implement routine vulnerability scans and access control mechanisms

---

Date: N/A	**Entry: 3**
Description	Infected attachment that creates unauthorized executables
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An unknown individual who sent Infected attachment by e-mail ● **What** happened? ○ An infected attachment created unauthorized executables in the moment at employee opened the file ● **When** did the incident occur? ○ Day no specified at 23:00:00 ● **Where** did the incident happen? ○ On employee pc ● **Why** did the incident happen? ○ Bad detection on infected files received via email

Additional notes	Hash file SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b 59 supplies indicated the file as malicious and -220 points of the community. Besides is file without signature verification, the file had 11/96 without specific status code detections on contacted urls and 1 detection on Contacted IP addresses with the ip 104.115.151.81. In conclusion, this file is potentially malicious, and I recommend taking actions.

Date: 05/12/2024	**Entry:4**
Description	SERVER-MAIL Phishing attempt possible download of malware
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ An unknown individual ● **What** happened? ○ An employee received a malicious email ● **When** did the incident occur? ○ July 20, 2022 09:30:14 AM ● **Where** did the incident happen? ○ On the Server mail and employee pc ● **Why** did the incident happen? ○ Lack of filters on the server mail, and bad detection of malicious attachments

Additional notes	The incident had medium on severity level, contains attachments and in the email body has grammatical errors. Therefore, this incident is considered a possible phishing attempt.

Date: 06/12/2024	**Entry: 5**
Description	Investigating domain
Tool(s) used	Cronicole, VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ ashton-davison-pc ○ bruce-monroe-pc ○ coral-alvarez-pc ○ emil-palmer-pc ○ jude-reyes-pc ○ roger-spencer-pc ● **What** happened? ○ Multipĺe persons acceded to malicious domain ○ Possible phishing ● **When** did the incident occur? ○ July 08 2023 | UTC ● **Where** did the incident happen? ○ signin.office365x24.com

	• **Why** did the incident happen? ○ Malicious domain
Additional notes	The domain signin.office365x24.com resolved two ips, 104.215.148.63 and 40.100.174.34 and has a sibling domain, that is: login.office365x24.com In the domain signin.office365x24.com, it does POST to http://signin.office365x24.com/login.php. In the domain 40.100.174.34 it found 3 POST. Additionally, this ip address resolves two domains: signin.accounts-gooqle.com and signin.office365x24.com. Therefore, all that indicated possible phishing.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
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: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
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: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
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: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
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.

Reflections/Notes: Record additional notes.