Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 07/28/24	**Entry:** 001
Description	A health clinic was attacked with ransomware via phishing, causing the company to shut down temporarily.
Tool(s) used	Ransomware, phishing, malware, encryption
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers • **What** happened? Attackers gained access to company data by phishing employees into installing malware. The data was encrypted and attackers left a ransom note asking for a large sum of money for decryption keys. • **When** did the incident occur? Tuesday @ 9:00am • **Where** did the incident happen? A small US health clinic • **Why** did the incident happen? Attackers seeking money phished employees via email
Additional notes	The organization lost access to important documents and data causing major damage to operations.

Date: 07/30/24	**Entry:** 002
Description	An employee downloaded a file on their computer via email, which had malicious code deployed once they opened the file.
Tool(s) used	Phishing
The 5 W's	Capture the 5 W's of an incident. • **Who** An employee • **What** happened? A virus was downloaded via email link from an unknown sender • **When** did the incident occur? 1:15pm • **Where** did the incident happen? Employee's computer • **Why** did the incident happen? An attacker used phishing to get the employee to download the malware
Additional notes	The sender had several spelling and grammatical errors in the email. The attached file ends with .exe, which indicates it is executable (This would not be necessary for a resume file). When entering the hash value into VirusTotal, 52 vendors have flagged this file as malware.

Date: 09/04/24	**Entry:** 003

Description	Traffic monitoring and alert configuration for an employer's network.
Tool(s) used	**Suricata, Linux**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? `$HOME_NET` 172.21.224.0/20 subnet • **What** happened? Traffic flow from $HOME_NET -> `$EXTERNAL_NET` • **When** did the incident occur? `11/23/2022-12:38:34` • **Where** did the incident happen? Employer's network server • **Why** did the incident happen? Common traffic flow
Additional notes	Created custom rules and ran them in Suricata, monitored traffic captured in a packet capture file, and examined the `fast.log` and `eve.json` output.

Date: 09/05/24	**Entry:** 004
Description	Examining a potentially malicious domain.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? signin.office365x24.com • **What** happened? Domain is redirecting traffic to itself, most likely from phishing attacks. • **When** did the incident occur?2023-01-31 14:40:40

	• **Where** did the incident happen? signin.office365x24.com (domain) which also shares a domain with login.office365x24.com • **Why** did the incident happen? Attacker uses these to phish.
Additional notes	Virus Total shows this domain has been flagged as malicious by multiple users. It has a sibling domain under login.office365x24.com .

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.