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: 10/06/2023	**Entry:** #1
Description	Documenting Ransomware cybersecurity incident
Tool(s) used	N/A
The 5 W's	• **Who:** An organized group of unethical hackers. • **What:** Encrypted the organization's files and demanded ransom to have those files decrypted. • **When**: Tuesday at 9:00am. • **Where**: U.S. healthcare clinic • **Why**: This incident occurred because the group of unethical hackers were able to gain access into the organization's network and systems. They did this by conducting a phishing attack to gain entry into a computer. Once into the network they were able to launch their ransomware to encrypt the organization's files. The attack seems to be due to financial motivating factors due to the ransom note demanding a large sum of money to decrypt the files.
Additional notes	By having proper disaster recovery techniques in place the organization could

	have recovered from this incident and not have to pay a ransom. The organization could have also prevented this incident from spreading to their other computers by implementing the principles of least privilege.

Date: 10/12/2023	**Entry:** # 2
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal
The 5 W's	• **Who:** Financial Services company. • **What**: Phishing email containing malware was opened by an employee. • **When**: Around 1:11 p.m. to 1:20 p.m. • **Where**: Malicious file was opened nn the employees computer. • **Why**: Phishing attempt
Additional notes	**SHA256 file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b When reviewing the SHA256 hash of the suspected file on VirusTotal has revealed that this same file has been reported by 55 other vendors. This malware is known as trojan flagpro.

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.