Incident handler's journal

Date: 25/11/2025	**Entry:** Journal Entry #1
Description	This entry documents a ransomware incident at a healthcare clinic where phishing emails led to system-wide file encryption and business disruption.
Tool(s) used	SIEM logs, Email security gateway, Antivirus/malware scanner, Incident reporting system.
The 5 W's	Capture the 5 W's of an incident. • **Who**: An organized cybercriminal group known for targeting healthcare organizations launched the attack using phishing. • **What**: Employees received phishing emails with malicious attachments that deployed ransomware, encrypting critical files and displaying ransom notes. • **When**: The incident occurred on Tuesday morning at approximately 9:00 a.m. • **Where**: The incident occurred at a small U.S. healthcare clinic across multiple employee workstations and network systems. • **Why**: Employees unknowingly downloaded malicious attachments, which allowed attackers to deploy ransomware due to a lack of security awareness and insufficient email filtering.
Additional notes	This is a targeted attack on a vulnerable sector with weak email security and limited incident preparedness. Incident response procedures, backup strategies, and employee phishing awareness training should be regularly reviewed and updated as needed. It is unclear whether data backups were available or if law enforcement was contacted.

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