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: 26/11/2025	**Entry:** Journal Entry #2
Description	Investigated a suspicious file hash using VirusTotal and extracted related indicators of compromise (IoCs) categorized using the Pyramid of Pain model.
Tool(s) used	VirusTotal, MITRE ATT&CK database, OSINT threat intelligence sources
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Likely external threat actors using malware delivered through phishing and malicious attachments. ● **What**: A password-protected spreadsheet executed a malicious payload, creating unauthorized executable files. VirusTotal confirmed the hash as malicious with multiple IoCs. ● **When**: Activity timeline: ➔ 1:11 p.m. – Email received ➔ 1:13 p.m. – File opened ➔ 1:15 p.m. – Malicious files created ➔ 1:20 p.m. – IDS alert triggered ● **Where**: On an employee workstation connected to the organization's internal network, triggering alerts at the SOC. ● **Why**: The Phishing email bypassed security controls, and a malicious attachment was executed due to a lack of user awareness and insufficient email filtering.
Additional notes	The file was flagged as malicious by multiple vendors and had a negative community score. Malware behavior included creating new processes, contacting a remote server, and using PowerShell to download additional payloads. IoCs should be blocked across endpoints, firewalls, and SIEM threat feeds.

Date: 26/11/2025	**Entry:** Journal Entry #3
Description	Followed the organization's Phishing Incident Response Playbook to evaluate a suspicious email alert, verify a malicious attachment, and determine whether to escalate or close the incident ticket.
Tool(s) used	VirusTotal · Email Header Analysis · SIEM Logs · Phishing Response Playbook (v1.0)
The 5 W's	Capture the 5 W's of an incident. • **Who**: External attacker impersonating a business contact; an internal employee downloaded a malicious attachment. • **What**: A phishing email with a malicious spreadsheet attachment containing malware, verified via SHA256 hash. • **When**: Email received at 1:11 p.m., opened at 1:13 p.m., malicious files created at 1:15 p.m., IDS alert at 1:20 p.m. • **Where**: Employee on the workstation, corporate network; malware attempted execution internally. • **Why**: The Phishing email bypassed filters; the user opened the attachment without verification, and a malicious payload was executed.
Additional notes	This incident reinforces the importance of: ✔ Email filtering and attachment sandboxing. ✔ Employee phishing awareness training. ✔ Mandatory verification of external attachments.

Date: 27/11/2025	**Entry:** Journal Entry #4
Description	Reviewed a final incident report of a major data breach at a retail company's e-commerce platform. Extracted key event details, response actions, root cause, and recommendations.
Tool(s) used	Incident Final Report • Log Analysis • Vulnerability Assessment Report
The 5 W's	Capture the 5 W's of an incident. • **Who**: External attacker exploiting a web application vulnerability. • **What**: A forced browsing attack on an e-commerce site exposed 50,000 customer records, including PII and financial data. • **When**: First contact: Dec 22, 2022 · Breach confirmed: Dec 28, 2022 at 7:20 p.m. PT. • **Where**: E-commerce web application and database holding customer records. • **Why**: Vulnerable URL access control; attacker modified order numbers to access unauthorized purchase pages.
Additional notes	This case emphasizes the importance of validating access control enforcement on URL parameters. Input manipulation allowed direct access to sensitive customer data. Highlights the need for secure coding practices, web app firewalls, and session-based access validation.

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.

Reflections/Notes: Record additional notes.