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: 1/31/2026	**Entry: #1**
Description	A small healthcare clinic experienced a security incident on Tuesday morning. Several employees reported they could not access critical files, and business operations were shut down. Additionally, a ransom note was displayed on the employee's computer. The note stated that the company's files were encrypted and demanded a large sum of money for the decryption key. The attackers were an organized group of ethical hackers who gained access using phishing emails. Once inside, they deployed their ransomware.
Tool(s) used	None
The 5 W's	• **Who** caused the incident? An organized group of unethical hackers • **What** happened? Critical files were encrypted, and a ransom was demanded for the decryption key (ransomware) • **When** did the incident occur? Tuesday, around 9:00 AM • **Where** did the incident happen? A small U.S. healthcare clinic • **Why** did the incident happen? Several targeted phishing emails were sent out to employees. The emails contained a malicious attachment

	that installed malware on the target's computer. Once the attackers gained access, they deployed their ransomware, which encrypted critical files
Additional notes	• The healthcare clinic employees are not educated on social engineering attacks, such as phishing • Should they pay the ransom for the decryption key?

Date: 2/3/2026	**Entry: #2**
Description	Investigating a suspicious file hash
Tool(s) used	VirusTotal • a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content • Users can submit and check artifacts • can compare file hashes to known malicious files • Extensive summary including: Description, Details, Relations, Behavior, and Community
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An employee • **What** happened? An employee received an email containing a password-protected spreadsheet file (the password was provided in the email). The employee downloaded the file, entered the password, and opened the file. Once opened, a malicious payload was then executed on their computer.

	• **When** did the incident occur? 1:20 PM • **Where** did the incident happen? Financial services company • **Why** did the incident happen? The employee was a victim of a phishing attack
Additional notes	Did the security team quickly take the employee's device off the network?

Date: 2/3/2026 Record the date of the journal entry.	**Entry: #3**
Description	Responding to a phishing incident using a playbook
Tool(s) used	Playbook
The 5 W's	• **Who** caused the incident? A malicious actor: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> • **What** happened? An employee received a phishing email and downloaded a suspicious file. • **When** did the incident occur? Wednesday, July 20th, 2022 at 9:30 AM • **Where** did the incident happen? At a financial services company • **Why** did the incident happen? An employee downloaded a suspicious file from an email that contained malware.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 2/4/2026	**Entry: #4**
Description	Reviewing a final report about a major security incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A malicious attacker • **What** happened? The attacker gained unauthorized access to customer personally identifiable information (PII) and financial information • **When** did the incident occur? December 28, 2022, at 7:20 p.m., PT, • **Where** did the incident happen? Mid-sized retail company • **Why** did the incident happen? The attacker exploited a vulnerability in the e-commerce web application, which allowed the attacker to access customer purchase confirmation pages
Additional notes	How long was the vulnerability present? Implement routine vulnerability scans

---

Date: 2/16/26	**Entry: 5**
Description	Capture and filter network traffic in a Linux environment using tcpdump
Tool(s) used	**tcpdump:** • Command-line network protocol analyzer

	• used for troubleshooting network issues • can identify malicious activity • filter for specific traffic • Use various options for specific output
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	What patterns in network traffic are an indicator of malicious activity? What other options can I use to filter for specific traffic?
