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: 4/30/2025.	**Entry:** 01
Description	Cybersecurity incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers had caused this incident. • **What** happened? A ransomware security incident • **When** did the incident occur? The incident occurred on Tuesday at 9:00 am. • **Where** did the incident happen? The incident happened in a small US healthcare clinic affecting their business operation due to the encryption of all the files. • **Why** did the incident happen? The incident happened because of a phishing email that contained a malicious attachment, and once it was downloaded it had encrypted all

	organization's files and they were asked for money in exchange for the decryption key.
Additional notes	Should the company pay the ransom to get access to their files?

Date: 5/3/2025	**Entry:** 02
Description	Phishing Incident
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Def Communication had sent an email containing malicious attachment. • **What** happened? A phishing mail was sent as a resume for a job role. • **When** did the incident occur? July 20, 2022 on Wednesday • **Where** did the incident happen? The incident happened within the organization. • **Why** did the incident happen? The user has opened a malicious email. The email's body contained a password-protected attachment, "bfsvc.exe," which was downloaded and opened.
Additional notes	The ticket was created as an alert containing its severity and details.

Date: 5/5/2025	**Entry:** 03
Description	Investigate about suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes les and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An unknown malicious actor • **What** happened? An email was sent to employee containing a malicious file attachment with SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **When** did the incident occur? An employee computer at a financial service company • **Where** did the incident happen? • At 1:20pm, an alert was sent to organization's SOC after the intrusion detection system detected the file • **Why** did the incident happen? The employee downloaded the file which resulted in the execution of malicious file attachment.

Additional notes	How can this incident be prevented in the future? What necessary security controls should be implemented in order to prevent it?

Date: 5/5/2025	**Entry:** 04
Description	Search query in SPLUNK
Tool(s) used	SPLUNK is used for collecting, analyzing and visualizing data to detect threats and monitor network activity. Splunk has its own querying language called Search Processing Language (SPL). SPL is used to search and retrieve events from indexes using Splunk's Search & Reporting app. I used SPLUNK to perform query search using SPL, finding relevant data for security analysis and evaluation.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? N/A • **What** happened? N/A • **When** did the incident occur? N/A • **Where** did the incident happen? N/A • **Why** did the incident happen? N/A
Additional notes	Include any additional thoughts, questions, or findings.

Date: 5/5/2025	**Entry:** 05
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
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	I've never used Wireshark before, so I was excited to begin this exercise and analyze a packet capture file. At first glance, the interface was very overwhelming. I can see why it's such a powerful tool for understanding network traffic.

Reflection/Notes

1. Were there any specific activities that were challenging for you? Why or why not?

   Yes, there were some activities challenging for me. For example, using command line interface and understanding what should be written to produce the result that I want. Specially, when capturing the packet file and analyzing it, I could not understand a thing.

2. Has your understanding of incident detection and response changed after taking this course?

   After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had no knowledge of detection tools and how they should be used. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.

3. Was there a specific tool or concept that you enjoyed the most? Why?

   Yes, the tools that I used for malicious file hash, known as Virus Total. I really enjoyed playing with its interface. Although, I had hard time finding the data that I required, it was fascinating that I can use this tool for any kind of file, website or data and it will provide me with the information about whether it is malicious or not.

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.