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: November 12, 2024	**Entry:** 003
Description	Received a phishing alert regarding a malicious file downloaded on an employee's computer. Verified the file hash against the threat intelligence database, confirming it as a malicious attachment. Followed organizational procedures to contain and remediate the threat..
Tool(s) used	● SIEM (Security Information and Event Management) for alert monitoring and log analysis ● Threat Intelligence Database for file hash verification ● Endpoint Detection and Response (EDR) for investigating and isolating the affected endpoint
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An employee unknowingly downloaded a malicious attachment from a phishing email.

	● **What** happened? A phishing email was sent to the employee, which led to the download of a verified malicious file. This triggered a phishing alert, flagging potential data compromise. ● **When** did the incident occur? The download occurred on July 20, 2022. Alert received on July 20, 2022 at 9:30 AM ● **Where** did the incident happen? The incident occurred on the employee's workstation within the organization’s network. ● **Why** did the incident happen? The employee was tricked by a phishing attempt, failing to recognize the malicious intent of the email and its attachment.
Additional notes	● Confirmed malicious file hash through VirusTotal. ● Updated the alert ticket with a summary of findings, including evidence of the attachment’s malicious nature. Escalated the ticket to a Level-2 SOC Analyst for further investigation and remediation. ● Followed the playbook’s incident response steps: isolated the affected system, escalated the incident, and communicated with IT for further action. ● Followed up with IT for potential user training to mitigate future phishing risks. ● Updated the alert ticket with all findings and closed the incident after confirming containment and remediation actions.