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 11, 2024	**Entry:** 002
Description	A suspicious file was downloaded on an employee's computer via a password-protected spreadsheet attachment in an email. After the employee entered the provided password, a malicious payload was executed. A SHA256 hash of the malicious file was generated for further investigation.
Tool(s) used	● SHA256 hash generator ● Intrusion detection system (IDS) ● Antivirus/malware detection software ● Security information and event management (SIEM) system ● File analysis tool
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The origin of the malicious file is unknown but appears to have been delivered through a phishing email. The attacker(s) are likely behind the email, tricking the employee into downloading the file.

	● **What** happened? The employee downloaded a password-protected spreadsheet attachment from an email and entered the password provided in the email. Once the file was opened, it triggered the execution of a malicious payload on the system. ● **When** did the incident occur? The timeline is as follows: ● **1:11 p.m.**: The employee received the phishing email with the file attachment. ● **1:13 p.m.**: The employee downloaded and opened the file. ● **1:15 p.m.**: Multiple unauthorized executable files were created on the employee's computer. ● **1:20 p.m.**: The IDS triggered an alert about the unauthorized activity. ● **Where** did the incident happen? The incident took place on the employee's workstation within the corporate network. ● **Why** did the incident happen? The incident occurred due to a successful phishing attempt. The attacker exploited social engineering to trick the employee into downloading the malicious file and entering the password, leading to the execution of the payload.
Additional notes	The SHA256 hash of the file has been generated, and we will proceed to investigate whether this file is part of a known malware signature. The employee has been notified about the incident, and their machine has been isolated to prevent further damage. We need to review email security protocols

	and employee training to prevent future incidents of this nature. Further investigation is required to determine if any data exfiltration or additional system compromise has occurred.