Incident handler's journal

Incident Summary

The following information contains details about the alert that will help you complete this activity. The details include a file hash and a timeline of the event. Keep these details for reference as you proceed to the next steps.

SHA256 file hash:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Here is a timeline of the events leading up to this alert:

1:11 p.m.: An employee receives an email containing a file attachment.

1:13 p.m.: The employee successfully downloads and opens the file.

1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.

1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.

Date:	**Entry:**
Record the date of the journal entry.	25 June 2025
Description	An employee received a phishing email containing a malicious attachment. Upon downloading and opening the file, multiple unauthorized executable files were created on the employee's workstation. The IDS detected this activity and generated an alert to the SOC.
Tool(s) used	IDS, VirusTotal (for hash analysis), SOC alert system (for detection & triage)

The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ● **What** happened? ○ Phishing email was received containing malicious file ● **When** did the incident occur? **At 1:11 p.m** ● **Where** did the incident happen? ○ On employees workstation computer ● **Why** did the incident happen? ○ Phishing attack
Additional notes	The file was malicious and the IDS alert was a True Positive.

Reflections/Notes:
This case highlights the importance of **user awareness and email security training**. Quick detection via IDS prevented possible lateral movement or data exfiltration.