Incident handler's journal

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

Date: 10.14.24	**Entry:** 2
Description	Employee downloaded a malicious password protected spreadsheet file. Upon opening the file - a payload was initiated.
Tool(s) used	VirusTotal, SHA256 File Hash
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Employee caused incident provided by malicious actor • **What** happened? Download of a password protected spreadsheet file which caused a payload to unfold • **When** did the incident occur? During work hours • **Where** did the incident happen? On employee's company computer • **Why** did the incident happen? File looked normal to the naked eye however has signs of malicious content after file was opened

Additional notes	Period of time: 1:11pm - 1:20pm ● 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 SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b VirusTotal Report: Community Score - (-216) VirusTotal Score - (60/73) Contains: Malware, Backdoor, Trojan