Incident handler's journal.

Date: 10.15.2024	**Entry:** 3
Description	In our previous investigation, we have found that an employee downloaded a malicious spreadsheet that was password protected. Upon completion that opened spreadsheet would execute a malicious payload. For the following, we are tasked to resolve the alert using a playbook in our companies policy
Tool(s) used	Playbook, Alert System (IDS)
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Employee has opened a Malicious Excel Download ● **What**: Payload Malicious File ● **When**: 1:11-1:20PM Company working hours ● **Where**: Financial Services Company ● **Why**: Incident handle
Additional notes	Ticket was escalated due to the nature of the file. Deemed malicious from sourced VirusTotal.