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: 01/02/2025	**Entry:** #2
Description	Level1 SOC at a financial services company. Alert about sus file being downloaded on employee computer. Investigation is done⟶ discovered that the employee received an email containing an attachment(Password provided in email) . Attachment = password-protected spreadsheet file. Employee downloaded file and entered password, prompted a file download of malicious payload. In result SOC individuals hash file.
Tool(s) used	VirusTotal
The 5 W's	● **Who**: ● **What**: File that contained malicious payload ● **Where**: Online via employee computer ● **When**: 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. ● **Why**:
Additional notes	**Email Security and Phishing Analysis**:

	● The email containing the malicious attachment appears to be a phishing attempt designed to bypass standard email filters using a password-protected file. ● Review email headers to identify the sender's IP address and domain for additional IoCs. **Malware Behavior**: ● Initial analysis suggests the malicious payload was executed immediately upon opening the file. ● It is likely the payload performed unauthorized actions such as installing backdoors or stealing data. This requires further dynamic analysis in a sandbox environment. **User Awareness**: ● The employee's action highlights the need for ongoing security training. Recommend incorporating this incident into future phishing simulation exercises. **File Attributes**: ● The malicious file's password protection was an intentional evasion tactic. Ensure detection mechanisms are configured to flag such file types in emails. **Incident Tracking**: ● Record this incident in the organization's incident management system for documentation, compliance, and trend analysis purposes. ● Add the identified IoCs (file hash, sender domain, IPs) to blocklists and share them with threat intelligence platforms if appropriate.