Incident handler's journal

Date: 02/09/2025	**Entry:** Use a playbook to respond to a phishing incident
Description	This activity involves responding to a phishing incident with a verified malicious file hash. As a SOC analyst, you'll follow a playbook to investigate, evaluate the alert, determine escalation or closure, and update the alert ticket with findings. You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert.
Tool(s) used	Alert ticket - template that allows us to organize information Phishing Playbook-To help level-one SOC analysts provide an appropriate and timely response to a phishing incident
The 5 W's	• **Who**: Myself, a level-one SOC at a financial service company • **What**: Verified that the file was malicious, now will follow up and complete the investigation/resolve issue • **Where**: Financial Services company • **When:**Post-Verification of file being malicious • **Why:** To complete the investigation and resolve it to a level-two SOC analyst
Additional notes	Perform routine, vulnerability, scans, and penetration testing. Implement the following access control mechanisms.:Implement allow listing to allow access

	to a specific specified set of URLs, and automatically block all requests outside of this URL range ensure that only authenticated users are authorized access to content. Lastly, incorporating employee meetings, email enhancements MFA and lease privileged protocols are all things that should be taken into accountability that will help employees and companies not go through this again.