Phishing Incident Response – Alert Ticket

# Ticket Details

Ticket Status: Escalated

# Ticket Comments

The alert pertains to a phishing incident involving a password-protected spreadsheet file that was received via email. The file was opened by an employee and executed a malicious payload.

This alert has been escalated for the following reasons:  
- The SHA256 hash of the file was verified as malicious through VirusTotal analysis, flagged by multiple vendors.  
- The file was downloaded and opened by the user, which triggered the execution of unauthorized executable files.  
- The message body and sender details raised suspicion of phishing activity based on inconsistencies and the presence of a password-protected attachment.

Escalation is recommended to ensure full remediation steps are taken, including malware removal, user notification, and further investigation into any lateral movement or data exfiltration.