Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	High	An employee unknowingly interacted with a phishing email, resulting in the download of a malicious file.	Escalated

Ticket comments

Summary of Investigation:
Upon receiving the phishing alert, the following steps were taken to investigate and confirm the malicious nature of the incident:

1. **Evaluated Alert Details**: Verified alert severity as **High** due to the presence of a suspicious file attachment. Collected receiver details (email and IP address) and sender information (email and IP address) for further analysis.
2. **Analyzed Email Components**: Inspected the subject line, message body, and attachment. Noted the file's suspicious nature and proceeded to validate its hash against a threat intelligence database.
3. **Hash Verification**: Confirmed through VirusTotal that the attachment was malicious.

Reason for Escalation:

1. **High Severity of Alert**: The alert was marked as high priority, which requires immediate escalation under our security protocol to prevent potential compromise of sensitive systems.
2. **Confirmed Malicious File**: The attachment was verified as malicious via threat intelligence tools, warranting further action by a Level-2 SOC Analyst to fully assess and remediate any potential impact on the network.
3. **Potential for Data Breach**: Due to the nature of the phishing attempt, there is a risk of lateral movement or data exfiltration if additional protective measures are not implemented promptly.

Conclusion:
Escalated to Level-2 SOC Analyst for advanced response and containment measures. Ticket status updated to **Escalated**.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Clyde West
Attachment: filename="bfsvc.exe"