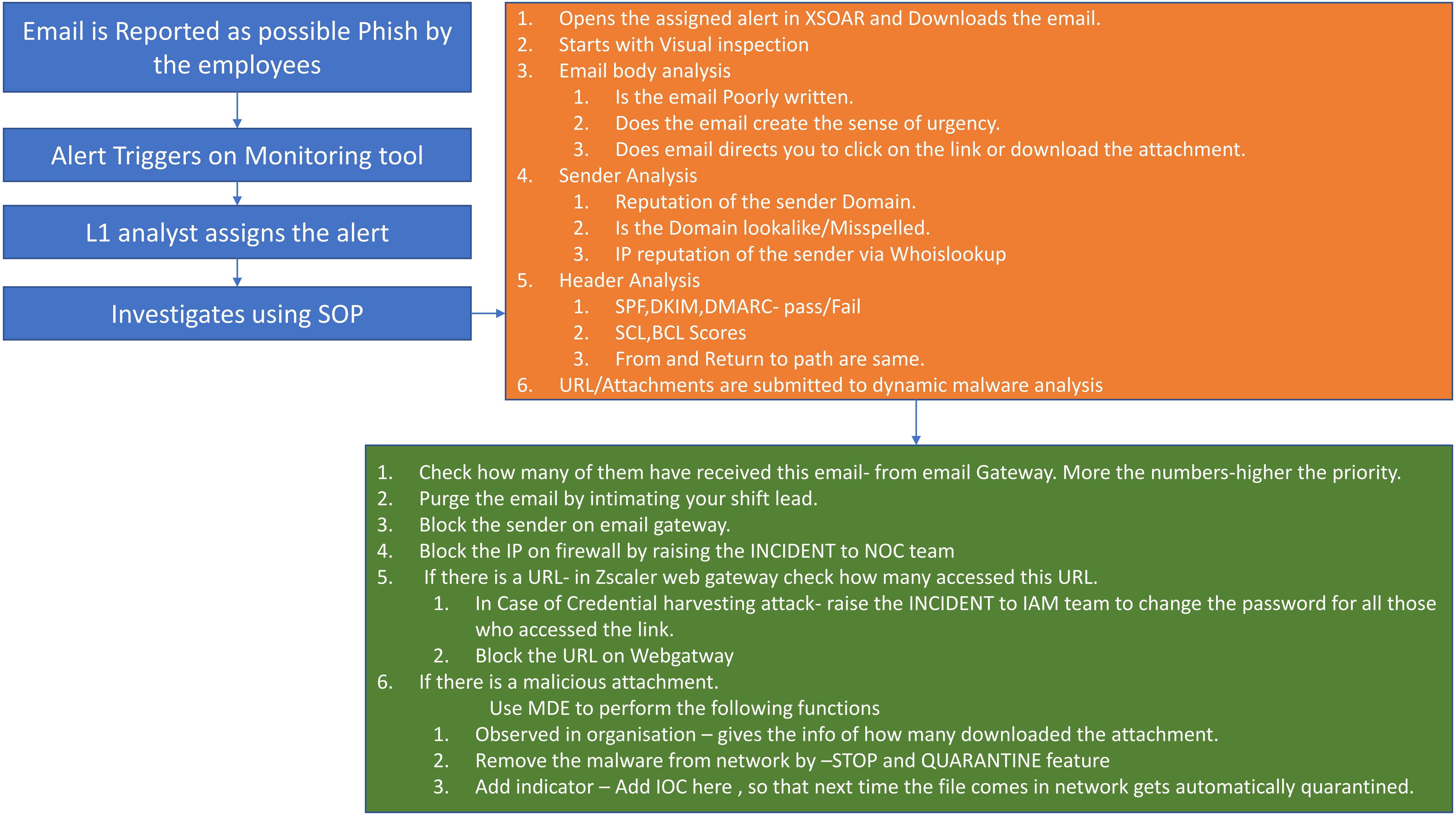
Phishing attacks are a type of social engineering, where a fraudulent message is sent to a target on the premise of arriving from a trusted source. Its basic purpose is to trick the victim into revealing sensitive information like passwords and payment information.

Social engineering is **the term used for a broad range of malicious activities accomplished through human interactions**. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps.



Email is Reported as possible Phish by the employees

Alert Triggers on Monitoring tool

L1 analyst assigns the alert

Investigates using SOP

1. Opens the assigned alert in XSOAR and Downloads the email.
2. Starts with Visual inspection
3. Email body analysis
    1. Is the email Poorly written.
    2. Does the email create the sense of urgency.
    3. Does email directs you to click on the link or download the attachment.
4. Sender Analysis
    1. Reputation of the sender Domain.
    2. Is the Domain lookalike/Misspelled.
    3. IP reputation of the sender via Whoislookup
5. Header Analysis
    1. SPF,DKIM,DMARC- pass/Fail
    2. SCL,BCL Scores
    3. From and Return to path are same.
6. URL/Attachments are submitted to dynamic malware analysis

1. Check how many of them have received this email- from email Gateway. More the numbers-higher the priority.
2. Purge the email by intimating your shift lead.
3. Block the sender on email gateway.
4. Block the IP on firewall by raising the INCIDENT to NOC team
5. If there is a URL- in Zscaler web gateway check how many accessed this URL.
    1. In Case of Credential harvesting attack- raise the INCIDENT to IAM team to change the password for all those who accessed the link.
    2. Block the URL on Webgatway
6. If there is a malicious attachment.

    Use MDE to perform the following functions

    1. Observed in organisation – gives the info of how many downloaded the attachment.
    2. Remove the malware from network by –STOP and QUARANTINE feature
    3. Add indicator – Add IOC here , so that next time the file comes in network gets automatically quarantined.

Tools Used in investigation.

1. XSOAR – Monitoring tool, Download the attachment
2. SNOW- ticketing tool.
3. Open-Source Threat Intel Tools
    1. Sender domain Reputation check
    2. IP Reputation check
    3. Header Analysis -MX toolbox
4. Dynamic Malware Analysis- Any. Run
5. Email Gateway- Barracuda
    1. To Check how many users have received the email.
    2. Block the sender.
6. Web gateway/proxy- Zscaler
    1. To See how many have accessed the URL.
    2. Block the URL
7. EDR/XDR- MDE
    1. To see how many have downloaded the attachment.
    2. To stop and quarantine the file and process run by the file.
    3. Add Indicator.

Incidents Raised

1. NOC team to block the IP.
2. IAM team to change the credentials.