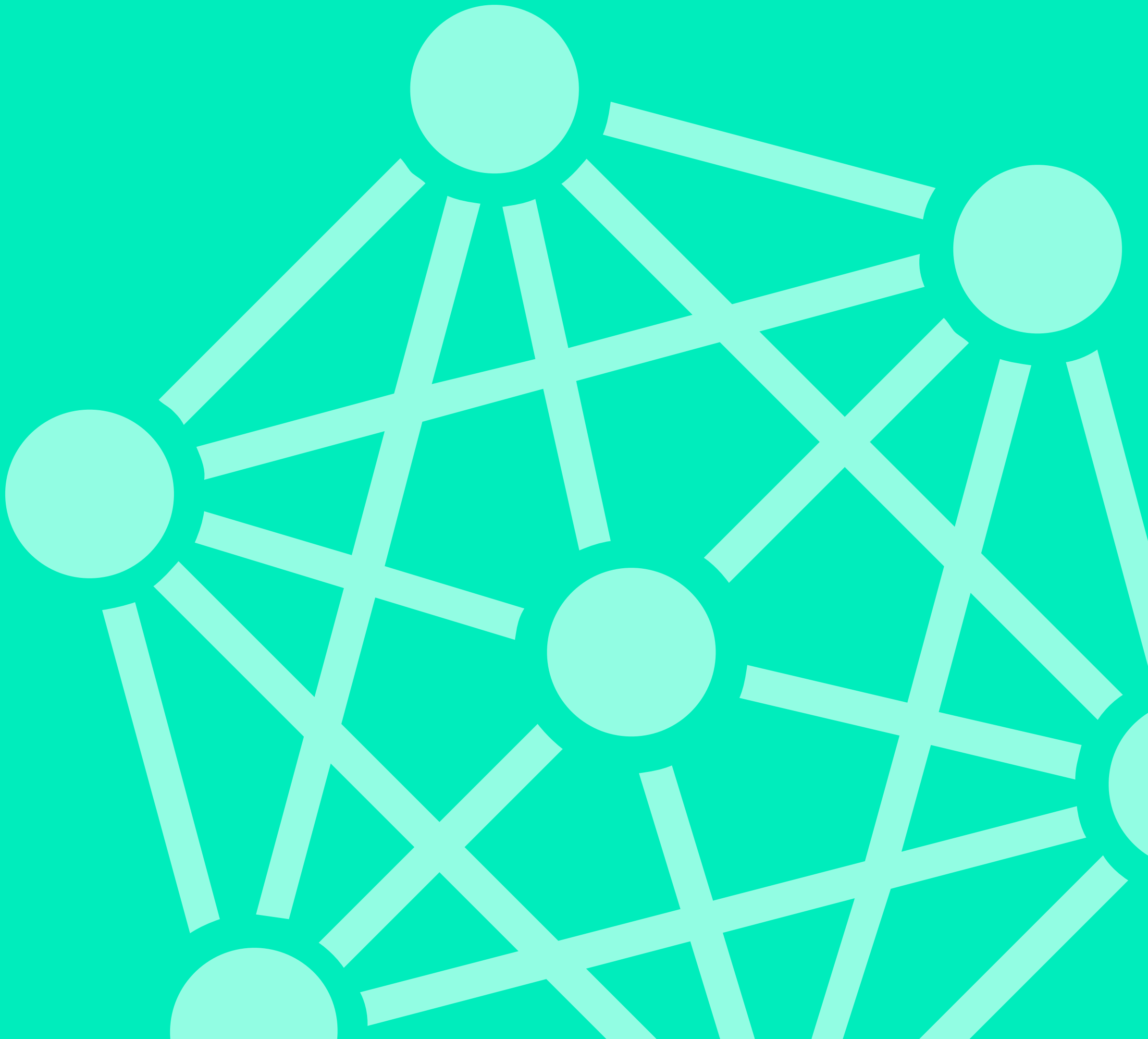
Logsign®

Logsign Security Orchestration, Automation and Response (SOAR) Use Case:

Phishing Attacks

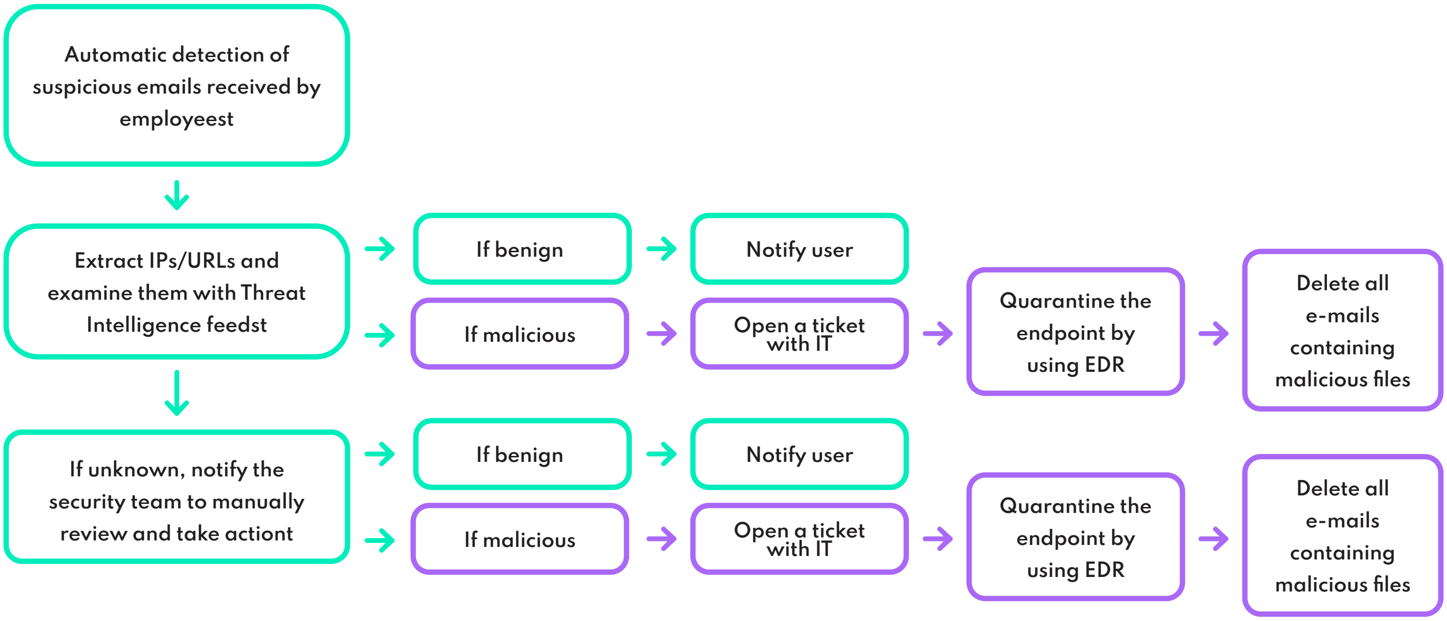


Phishing Attacks

Customer Challenge

The primary objective behind phishing attacks is to trick the victims into sharing sensitive or confidential information such as corporate network credentials, credit card information, email credentials, etc. Attackers employ social engineering techniques to manipulate their targets into clicking on a malicious link or downloading a malicious file. At times, attackers disguise themselves as a trusted individual or organization for manipulating the victims into voluntarily revealing confidential information. If a phishing attempt has been successful and the organization has not been able to detect it, the extent of potential damages widens substantially.

How to prevent phishing attacks with Logsign SOAR


Automatic detection of suspicious emails received by employeest
Extract IPs/URLs and examine them with Threat Intelligence feedst
If benign
Notify user
If malicious
Open a ticket with IT
Quarantine the endpoint by using EDR
Delete all e-mails containing malicious files
If unknown, notify the security team to manually review and take actiont
If benign
Notify user
If malicious
Open a ticket with IT
Quarantine the endpoint by using EDR
Delete all e-mails containing malicious files

Business Process Analysis

It may take a security analyst up to 45 minutes to deal with a phishing attack. Logsign SOAR cuts down this time consumption to 1-2 minutes.

Benefits

With the help of Logsign SOAR, your security team can automate close to 90% of tasks for detecting and responding to phishing emails. It requires minimal efforts from your SOC team and overall mean time to response (MTTR) is significantly decreased. The SOAR platform detects phishing emails in a matter of few seconds and if needed, categorizes a set of emails for manual review by the security team.