Automated Phishing Threat Intelligence and Remediation

Benefits

- Automate phishing incident response with seamless ingestion and specific playbooks.
- Cross-correlate phishing campaign data for threat hunting and future learning.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, Cofense Intelligence™

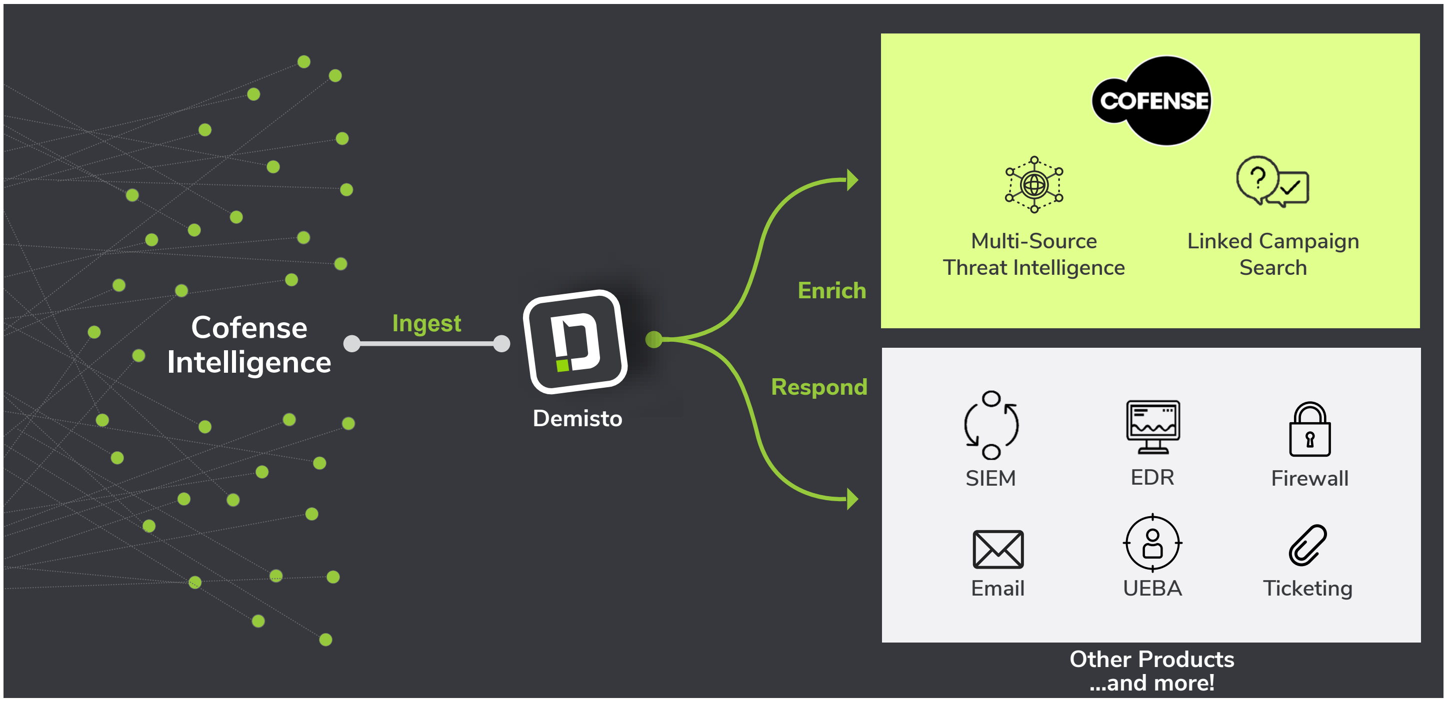
Phishing emails are one of the most frequent, easily executable, and harmful security attacks that organizations – regardless of size –face today. With over 90% of all data breaches starting with a phishing email, the potential for financial damage is real and immediate.

Security analysts face numerous challenges while responding to phishing attacks. Handling attack numbers without burning out,switching between multiple screens to coordinate response, avoiding errors while completing mundane tasks, and standardizing response and reporting procedures are all sources of worry.

Cofense Intelligence helps meet these challenges with a combination of human-verified phishing indicators, trends, and context data. This intelligence can be ingested into Demisto to kick off automated playbooks for response at machine speed. This combination improves the security team's response posture to the phishing malaise.

Integration features

- Timely, accurate, relevant and consumable human-vetted threat intelligence delivered as machine-readable threat intelligence by Cofense Intelligence and ingested into Demisto Enterprise.
- Trigger specific playbooks based off Cofense Intelligence data to coordinate actions across the security product stack.
- Visibility into linked phishing campaigns for specific attacks from Cofense Intelligence into Demisto Enterprise.



USE CASE #1 AUTOMATED PHISHING INCIDENT RESPONSE

Challenge: There is often a mismatch between the high-volume nature of phishing attacks and analyst agility in responding to them. Phishing attack identification, triage, reputation checks, and response involves switching between multiple screens, mundane and repeatable tasks, and tunnel vision that precludes knowledge of larger phishing campaigns that encompass a particular attack.

Solution: Using rule-sets, analysts can map phishing attack categories from Cofense Intelligence to specific Demisto playbooks that automate repeatable tasks such as indicator collection, reputation checks, and mail communication with affected parties. The phishing response playbook will trigger and execute automatically on receipt of a phishing attack.

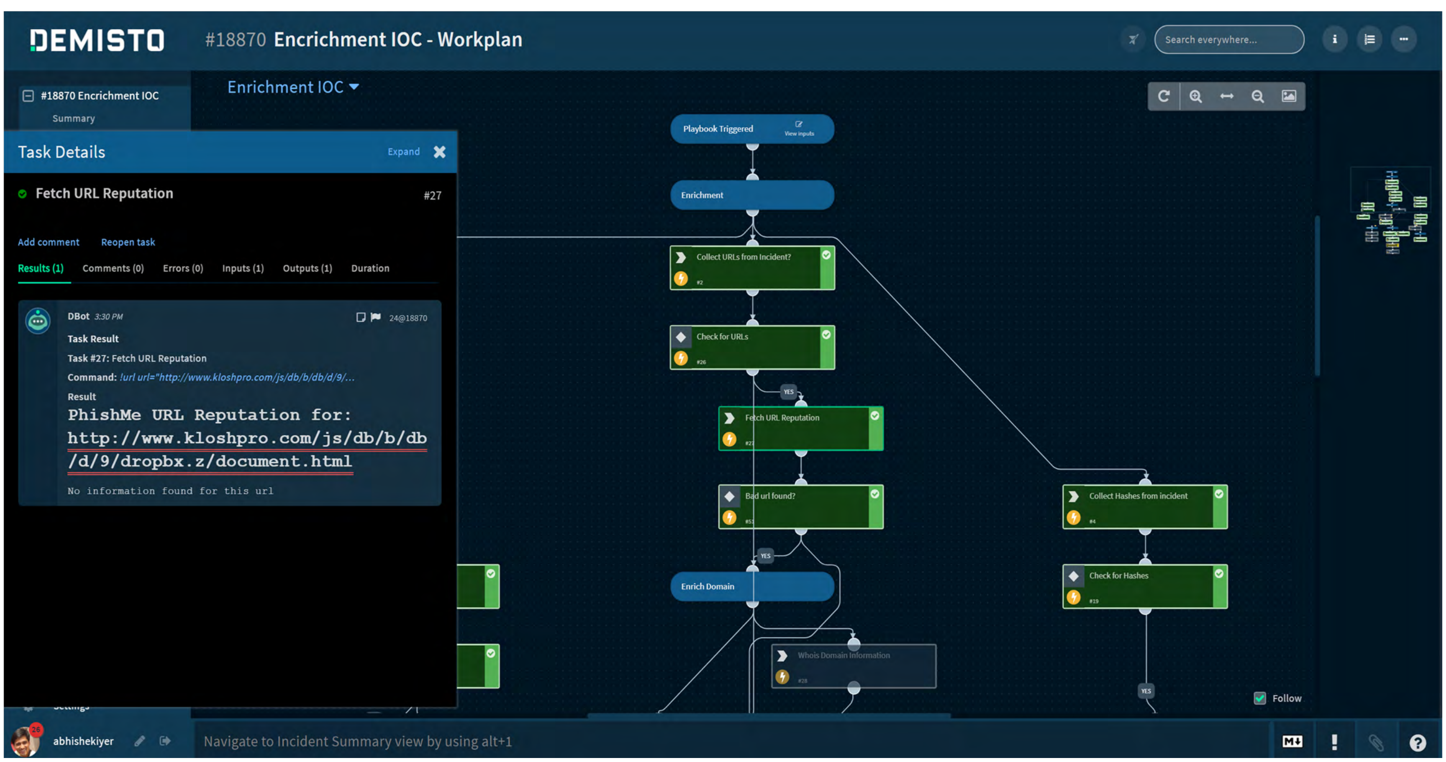


Fig 1: Live automated playbook run with Cofense URL reputation checks

Benefit: Playbooks can provide standardized response procedures and post-response documentation, helping analysts respond to phishing attacks quicker and generate scalable, comprehensive reports based on a rich pool of indicators and investigation actions that are common across incidents.

USE CASE #2 THREAT HUNTING WITH PHISHING CAMPAIGN DATA

Challenge: While phishing attacks are often a part of larger, more coordinated phishing campaigns that exploit multiple entry vectors in an organization, analyst response treats them as isolated incidents due to paucity of time, knowledge, and personnel resources.

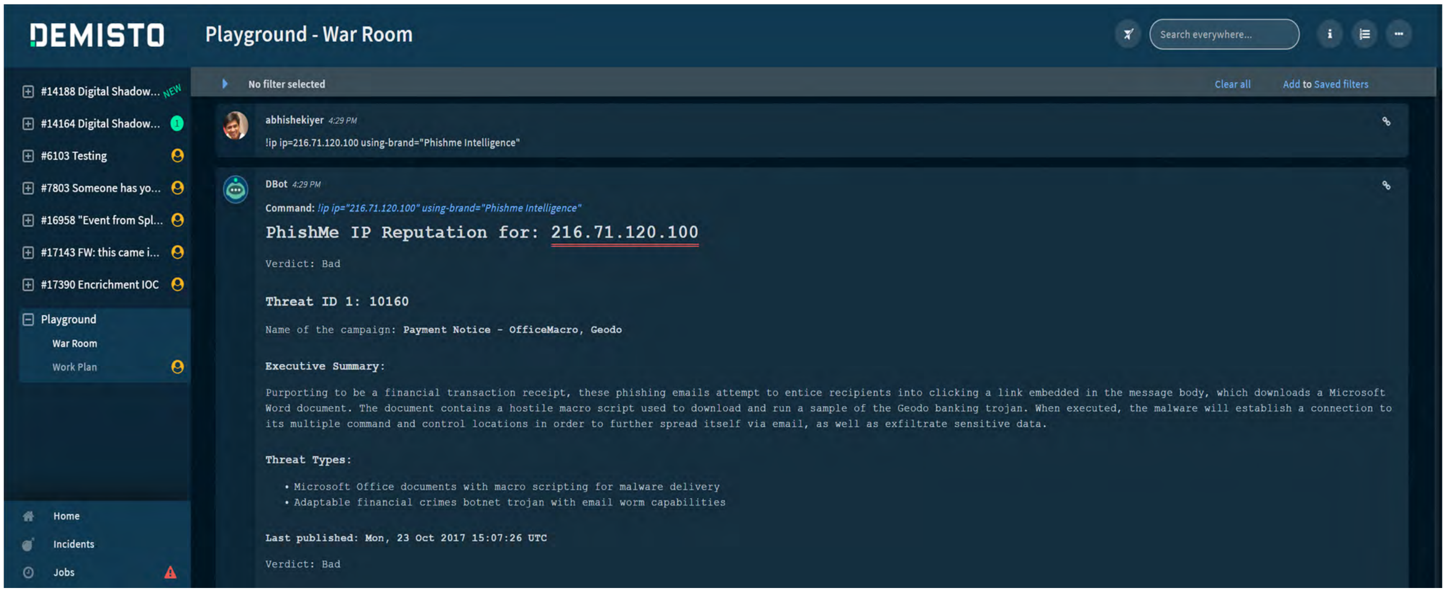


Fig 2: Running Cofense IP check commands interactively through CLI in the Demisto War Room

Solution: While responding to a particular phishing attack, analysts can query Cofense Intelligence from Demisto and get details about the malware family, indicators of compromise, severity and payload method for this attack. This information can be used for subsequent threat hunting exercises on Demisto for similar phishing attacks that have occurred on other organizational entry points.

Benefit: By leveraging common indicators and context across phishing attacks in a campaign, analysts can link incoming incidents accordingly for a more efficient, speedy, and scalable response. These linkages exist in posterity, building a knowledge repository for analysts to learn from and respond better to future attacks.

About Cofense

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defense solutions for organizations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organization wide response to the most used attack vector—phishing. Cofense serves customers of all sizes across multiple industries including financial services, energy, government, healthcare, technology and manufacturing, as well as other Global 1000 entities that understand how engaging user behavior will improve security, aid incident response and reduce the risk of compromise.

About Demisto

Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to resolution (MTTR), create consistent incident management process, and increase analyst productivity. For more information, visit www.demisto.com or email info@demisto.com.