Automated Phishing Threat Analysis and Incident Remediation

Phishing emails are one of the most frequent, easily executable, and harmful security attacks that organizations – regardless of size – face today. Many data breaches begin with a malware-based or credential-stealing phishing email capable of inflicting financial and reputation damage.

Security analysts face numerous challenges while responding to phishing attacks. A barrage of attacks, multiple screens to coordinate response, manual and repetitive tasks, non-standardized processes and reporting are all sources of stress.

Cofense Triage and Intelligence combines automated phishing analysis and human-verified indicators of phishing. Cofense Triage ingests, clusters and analyzes reported phishing emails to prioritize risk. Cofense Intelligence enriches Demisto playbooks with rich contextual data for automated incident response actions and analyst investigation.

Cofense Triage and Intelligence and Demisto integration features:

- Demisto playbooks leverage the combination of Cofense indicators of phishing and human-verified intelligence in automated and/or manual playbooks for the incident response team to mitigate and eliminate the attack.
- Run thousands of commands (including for Cofense alerts) interactively via a ChatOps interface while collaborating with other analysts and Demisto’s chatbot.

Benefits

- Prioritize risk quickly with automated email analysis and extraction of phishing indicators.
- Shorten decision-making cycle and response by automating key tasks.
- Gain insights for future threat hunting from cross-correlation of phishing data.

Compatibility

- Products: Demisto Enterprise, Cofense Triage™ and Cofense Intelligence™
**Challenge:** There is often a mismatch between the high-volume nature of phishing attacks and analyst agility in responding to them. For analysts, phishing attack identification, triage, reputation checks, and response usually involves switching between multiple screens and repeated manual tasks.

**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.

**Benefit:** Playbooks can provide standardized response procedures and post-response documentation, helping analysts bypass repeatable manual steps and giving them access to scalable, comprehensive reports based on a rich pool of indicators and investigation actions that are common across incidents.
**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 limited resources and lack of visibility into these larger attack campaigns.

**Solution:** While responding to a particular phishing attack, analysts can query Cofense Triage and Intelligence from within Demisto for details about categorized phishing threats such as crime-ware and advanced threats. These details can be used for additional indicators of compromise validation linking, highlighting the severity and attack payload method. This information can be used for subsequent threat hunting exercises on Demisto to identify 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, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit [www.demisto.com](http://www.demisto.com).