Cofense Solution Brief

INCREASING SOC EFFICIENCY AND REDUCING RISK WITH EFFECTIVE THREAT PRIORITIZATION

BUSINESS CHALLENGE

Organizations with a strong reporting culture can generate significant volumes of email reports for a SOC team to manage, much of it noise. When a large phishing campaign strikes, responders struggle with the number of reports requiring analysis, delaying remediation and increasing the risk of compromise.

SOLUTION BENEFITS

- Quickly identify and automatically process clusters of non-malicious email
- Combat morphing attacks effectively by classifying and clustering malicious emails based on payload
- Analyze entire campaigns as easily as a single email
- Prioritize clusters based on email attributes, Indicators of Phishing, reporter reputation, and reporter status

WHY SECURITY OPERATIONS NEEDS INTELLIGENT EMAIL CLUSTERING

Phishing threat actors constantly innovate to bypass technical controls such as Secure Email Gateways and firewalls. When a threat bypasses these controls, the user is the last line of defense. Not all who report emails are equal, however, and analysts receive large volumes of non-malicious emails. Reviewing them causes delays that increase the risk of compromise and data breach, as credentials are stolen or malware spreads the organization.

MORPHING ATTACKS MAKE THREAT HUNTING HARDER

The phishing defense industry continues to witness changes in attackers' Tactics, Techniques, and Procedures (TTPs) to bypass Secure Email Gateways. Advanced attacks make use of morphing strategies to vary email subjects and senders, making common phish detection strategies obsolete. Security analysts must analyze and respond to large volumes of campaign emails due to these morphing tactics, slowing them down.

DELAYED INCIDENT RESPONSE INCREASES RISK

The Mean Time To Identify (MTTI) a data breach has a direct impact on the total cost of a breach[1]. User email reporting is just the first step in faster response. Reporting does not lead to visibility unless security teams can identify, prioritize, analyze, and understand what has been reported. A SOC team needs the ability to clear the noise and focus on the threats that could lead to a compromise.

[1] $3.92M - 2019 Ponemon Cost of Data Breach Report

COFENSE TRIAGE™

Cofense Triage accelerates phishing qualification and investigation by automatically analyzing reported emails, making analysts more efficient and driving out actionable intelligence. The rules library is powerful and constantly updated to leverage our comprehensive view of the phishing threat landscape—your analysts gain indicators and insights on evolving threat actor tactics and campaigns. Intelligent, automated clustering handles large-scale phishing campaigns as easily as a single email, reducing SOC workload and decreasing threat dwell time.

BENEFITS OF COFENSE TRIAGE

REDUCE NOISE

Cofense Triage uses a powerful Noise Reduction engine to evaluate and score emails. An extensive library of rules derived from millions of human sensors filter marketing, commercial, and other non-malicious emails, automatically reducing the noise of over-reporting and surfacing high priority reports for action.

IDENTIFY MORPHING ATTACKS

Most phishing defense tools are limited to phish classification by subject and sender. Attackers, however, have increased the complexity of their campaigns by morphing those indicators. Cofense Triage identifies campaigns by attack payload rather than subject and sender alone. Domains, URLs, attachments, and hashes provide the digital fingerprints used to generate campaign-level clusters for analysis and response.

PROCESS ENTIRE CAMPAIGNS AS EASILY AS A SINGLE EMAIL

Using intelligent clustering, Cofense Triage analyzes multiple, related emails as one. Analysts can perform data enrichment on an entire cluster to evaluate all Indicators of Phishing, building a complete picture to drive incident response. Once the threat is remediated, analysts can easily respond to phish reporters, providing positive feedback to support a reporting culture.

PRIORITIZE CLUSTERS TO FOCUS SOC EFFORTS

Cofense Triage clusters are easily prioritized to focus efforts on the highest risk attacks. Using rules and reporter reputation, as well as recipient attributes such as VIP status, each cluster is quickly classified so the appropriate team of responders can act.

REMEDIATE THREATS QUICKLY WITH COFENSE VISION

Cofense Triage integrates with Cofense Vision for fast threat remediation. Analysts can use the intelligence gained from reported emails to find all instances of a phishing campaign delivered throughout the organization. Once found, emails may be quarantined rapidly and automatically, with a single click, reducing threat exposure.

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.

COFENSE

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175