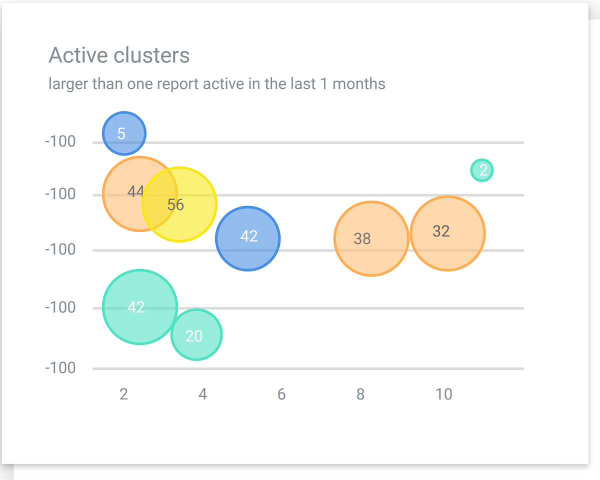
Cofense Triage™

INCIDENT RESPONSE PLATFORM

With over 90% of breaches attributed to employee targeted phishing, relying on technology alone isn't enough – we must utilise people to build our best defence. Cofense Triage is the first phishing-specific incident platform that allows security operation (SOC) and incident responders to automate the prioritisation, analysis and response to phishing threats that bypass your email security technologies, providing the visibility and analytics needed to speed response and mitigate risk.



Key Benefits

- ✓ Unique and comprehensive phishing-specific incident response solution
- ✓ Full integration with Cofense Reporter™ allows threat prioritisation based on user reputation, attributes, and threat intelligence
- ✓ Provides active report clustering to identify threats faster
- ✓ Integrates with security technologies such as sandboxes, URL analysis solutions, and SIEM solutions for enhanced detection capabilities
- ✓ Allows Incident responders to share results with upstream security teams to prevent future attacks

What is Cofense Triage™?

Cofense Triage is the first phishing-specific incident response platform that allows security operations and incident responders to automate the identification, remediation, and sharing of phishing threats.

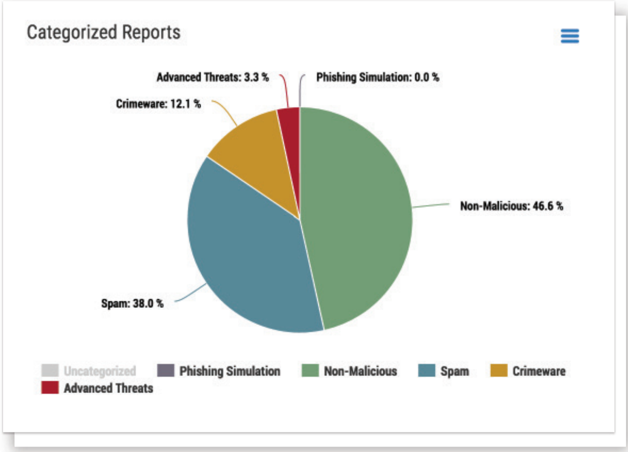
Cofense Triage gives incident responders the analytics and visibility into email-based attacks occurring against their organisations in near real-time.Triage is the only offering that operationalises the collection and prioritisation of employee-reported threats and seamlessly integrates with Cofense Reporter™.

Triage is currently available on-premises or as a cloud-based virtual appliance.

3rd Party Integrations

Triage integrates with your existing SIEM, malware and domain analysis, and threat intelligence solutions. Cofense is continuously developing new partnerships and integrations to improve functionality and accommodate market needs. The most current list of available integrations are available online.

> Cofense Triage provides our response teams with the rapid, detailed information they need to address email threats quickly and efficiently without wasting time chasing false positives.
>
> **Kevin Emert, CISO, Scripps Networks Interactive**



Key Features

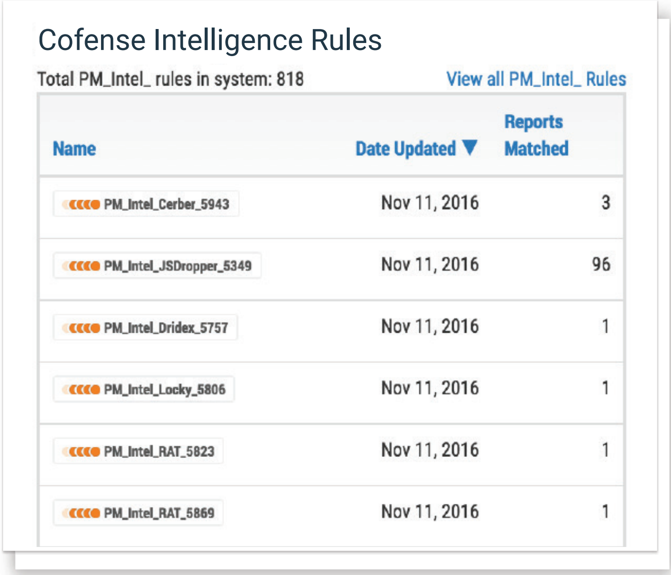
Dashboard and reporting – Gain insight into the volume and types of emails being reported by your users and understand attack trends impacting your organisation.

Smart Clustering – Triage can identify key commonalities among multiple reports. As these commonalities are discovered, Triage will create a cluster of reports. A cluster of reports can identify a campaign against your organisation. Triage or operators can process all reports in a cluster as a single unit rather than having to process each report individually. By enabling clustering, Triage dramatically reduces the volume of individual reports that you must process and helps you identify and track campaigns.

Reporter Reputation – Reporter reputation is the equivalent of a trusted source. Reporters with higher reputation scores do a better job of distinguishing and reporting real threats. Reporters with lower, or negative, reputation scores may have previously submitted reports that Triage determined to be non-malicious or spam.

User Feedback – Triage allows administrators to customise and automate feedback responses to Reporters—based on the type of email they have reported via Response Manager.

YARA – Triage provides a powerful rules editor that enables you to write and edit strong YARA rules. The rules editor enables you to test a rule immediately to validate that it works against one or more reports. In addition, Cofense shares a substantial library of tested YARA rules that you can use as-is or modify to your specific needs. Cofense uses YARA to develop rules to identify and respond to user reports, while using YARA logic to develop Indicators of Phishing (IoP).



Cofense Intelligence Rules

Total PM_Intel_ rules in system: 818 View all PM_Intel_ Rules

Name	Date Updated ▼	Reports Matched
PM_Intel_Cerber_5943	Nov 11, 2016	3
PM_Intel_JSDropper_5349	Nov 11, 2016	96
PM_Intel_Dridex_5757	Nov 11, 2016	1
PM_Intel_Locky_5806	Nov 11, 2016	1
PM_Intel_RAT_5823	Nov 11, 2016	1
PM_Intel_RAT_5869	Nov 11, 2016	1

Escalations – Share valuable and actionable threat intelligence with upstream security teams to better protect against future threats via Notification manager. These one-time messages allow for teams to perform additional actions on the message or elements of the message.

Cofense™, formerly known as PhishMe®, is the leading provider of human-driven phishing defence solutions for organisations concerned with their susceptibility to sophisticated cyber attacks. Cofense delivers a collaborative, cooperative approach to cybersecurity by enabling organisation-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.

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