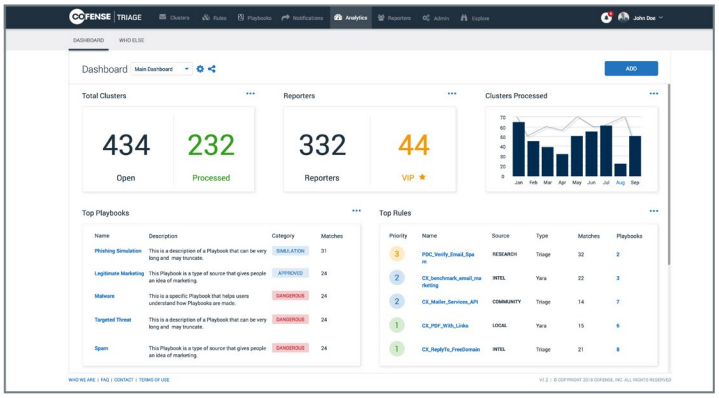
Cofense Triage™

INCIDENT RESPONSE PLATFORM

ONE SOURCE COMMUNICATIONS

COFENSE

Most successful cyber-attacks are the result of a phishing scam. Conditioning employees to detect and report is the best line of defense. But what happens to those reported emails—and the ones users fail to report? With Cofense Triage, you can orchestrate and automate your response to attacks. Our platform analyzes and categorizes user-reported emails while enabling incident responders to investigate and respond. Automated playbooks and workflows coordinate your response. It's the faster, more efficient way to stop phishing attacks in progress.



Key Benefits

- Automates email analysis for known and unknown risks
- Gives SOC teams visibility into active phishing threats
- Groups emails into clusters to identify phishing campaigns
- Integrates with sandboxes, URL analysis solutions and SIEM solutions to enhance response
- Integrates with Cofense Reporter™ to allow threat prioritization based on user reputation, attributes, and threat intelligence
- Cofense Triage, along with Cofense Vision™ delivers a phishing Orchestration, Automation and Response platform to discover emails and rapidly quarantine messages

What is Cofense Triage?

Anti-Phishing Response Platform

Cofense Triage is the first platform that enables security teams to respond to email-based attacks quickly and efficiently. Deployment options include on-premises, cloud-based, or managed service. Only Cofense Triage operationalizes the collection and prioritization of user-reported threats. It seamlessly integrates with Cofense Reporter to ensure coordination between awareness and response.

Integrations

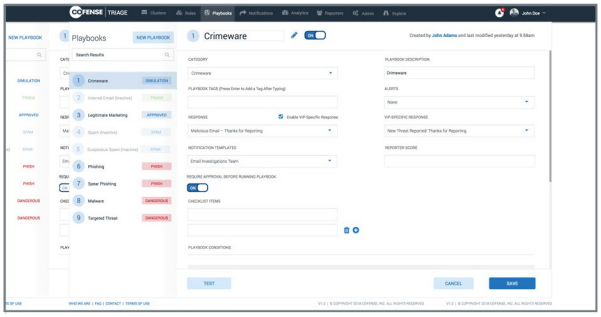
Cofense Triage integrates with your existing SIEM, malware and domain analysis, and threat intelligence solutions. Cofense continually develops new partnerships and integrations to improve functionality and accommodate market needs. A current list of available integrations is available on https://cofense.com/technology-partners/.

> Cofense Triage provides our response teams with the rapid, detailed information they need to address e-mail 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 organization.

Automated Playbooks – Respond faster and improve cross-team efficiency. Operators can create a repeatable workflow to automate a response to a threat. The operator defines a set of criteria to execute an automated response. This may include creating a ticket in a help desk system, notifying the proxy team to block a URL or a domain, or sending information to another up-stream or downstream team to address the threat. Work efficiently and smarter through automation.



Smart Clustering – Since it is impossible to deal with each email reported individually, Cofense Triage clusters emails based on commonalities. As emails are reported, they are analyzed to find commonalities and then grouped into a cluster. Cofense Triage operators can process a cluster as a single unit, rather than dealing with each report individually. With clustering, Cofense Triage dramatically reduces the volume of individual reports to help you identify and track campaigns.

Who Else – Rapidly shut down unreported malicious emails across the organization. A well-conditioned workforce reporting suspicious emails is the first line of defense but what about the emails that are not reported? The Who Else capability in Cofense Triage enables operators to query Microsoft Exchange or Office 365 to find a malicious email, notify the email team to quarantine the message across the organization, and prevent further damage.

Cofense Triage Noise Reduction – Sometimes emails reported to Cofense Triage are not a threat, but are just commercial email or spam that looks suspicious. Cofense Triage Noise Reduction uses an industry leading spam engine to review, score, and categorize reported emails. Emails that are not a threat are then categorized as spam and removed from the operator's queue, greatly reducing the workload of the Cofense Triage operator.

Rules Editor – Cofense Triage includes a set of rules to define operator search criteria. The rules editor provides an easy to use point and click tool with predefined variables like "Subject" and "Hash" and "Reply-To" to help operators quickly create rules. For more advanced analysis, Cofense Triage supports YARA rules to dig deeper.

Reporter Reputation – Leverage your trusted sources and save time. The Reporter Reputation is factored into how the Cofense Triage operator responds to reported emails since 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 Cofense Triage determined to be non-malicious or spam. This enables the team to prioritize their response.

Feedback Loop – Acknowledge your users. The Feedback Loop enables administrators to customize and automate feedback responses to Reporters to confirm whether or not they found a threat.

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