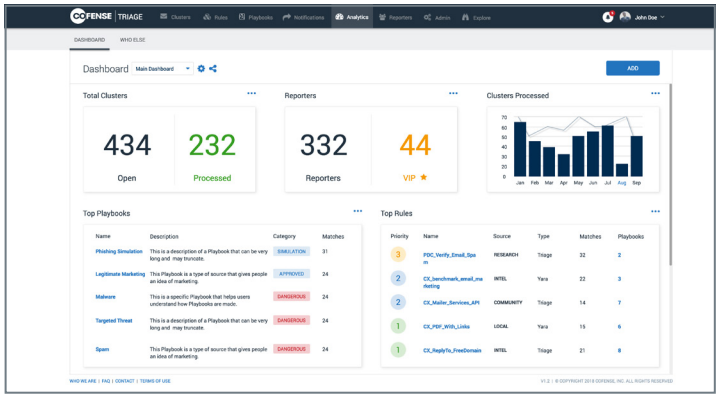
Cofense Triage™

INCIDENT RESPONSE PLATFORM

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? Cofense Triage 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

- Integrates with Cofense Reporter™ to allow threat prioritization based on user reputation, attributes, and threat intelligence
- 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

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

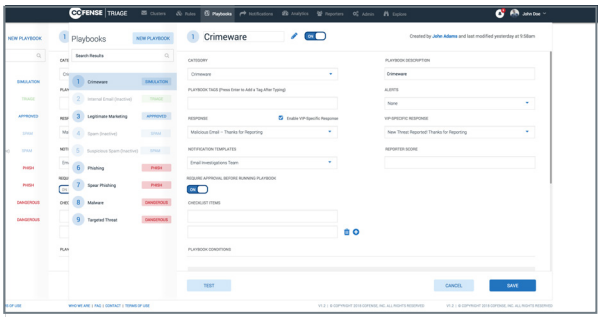
Cofense Triage integrates with your existing SIEM, malware and domain analysis, and threat intelligence solutions. Cofense continually develops new partnerships and integrations to improve functionality and accommodate market needs. A current list of available integrations is available on https://cofense.com/technology-partners/.

> 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 your users are reporting and understand attack trends impacting your organization.

Automated Workflow – Respond faster and improve cross-team efficiency. Operators can create a repeatable workflow to automate the response to a particular threat by defining a set of actions to execute. 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 upstream or downstream team to address the threat.

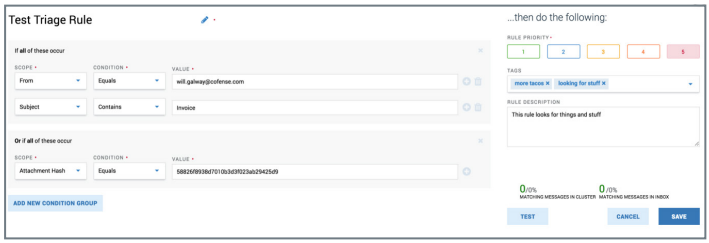


Smart Clustering – Cofense Triage analyzes emails as they are reported. During this analysis, Cofense Triage looks for key commonalities among the emails and groups emails with these commonalities into clusters. Emails in a cluster can be processed as a single unit or individually. Clusters reduce the volume of emails to process and 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 can be removed from the operator's queue, greatly reducing the operator's queue.

Rules Editor – Rules identify specific characteristics that Cofense Triage should look for in a reported email, such as a particular sender or subject. Operators can create their own rules in Cofense Triage's rule editor. Cofense Triage supports YARA rules for operators who want to dig more deeply into advanced analysis.



Reporter Reputation – Some reporters do a better job of recognizing and reporting real threats. These reporters build a reputation as trusted reporters in Cofense Triage. Operators can leverage their awareness of a reporter's reputation as they evaluate and prioritize risk.

Feedback Loop – Acknowledge employees who took the time to report an email by sending them a customized, automated response. Your responses can thank them for reporting, confirm whether or not they found a threat, or point them to your organization's training or policies for more information.

Escalations – Send a notification, from within Cofense Triage, to upstream teams. Notifications can share valuable and actionable threat intelligence or request teams to perform additional actions to mitigate a threat.

COFENSE

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