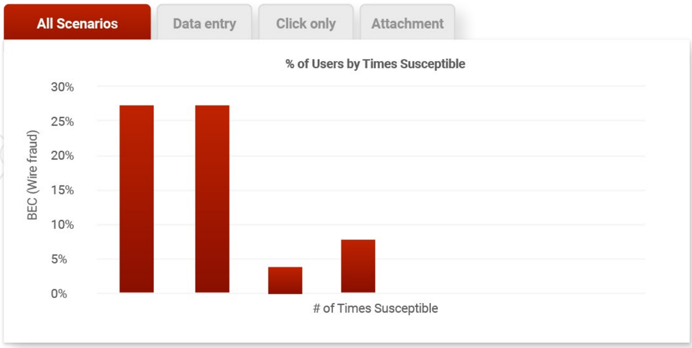
Cofense PhishMe™

EMPLOYEE CONDITIONING FOR RESILIENCY AGAINST PHISHING

Cofense™ research determined that ransomware accounts for more than 97% of all phishing emails. With such alarming numbers, how do you prevent your enterprise from becoming another statistic? Cofense PhishMe empowers employees to become your last line of defense with industry-proven behavioral conditioning methods to better prepare employees to recognize and resist malicious phishing attempts–transforming one of your biggest liabilities into your strongest defense. Cofense PhishMe has been proven to reduce the threat of employees falling victim to advanced cyber attacks by up to 95% – preparing your last line of defense to recognize and resist tricky phishing attempts.



Key Benefits

- ✓ Most effective simulations – The Cofense Intelligence™ product provides the latest phishing tactics and threats which we then turn into the most up-to-date and real-life phishing emails used in Cofense PhishMe to keep your users ahead of the most recent attacks.
- ✓ Automate scenario deployment with Playbooks - automate your phishing program over the course of a year by leveraging built-in playbooks.
- ✓ Recipient Management made easy, just upload your user list and Cofense PhishMe will do the rest.
- ✓ All compliance and awareness modules are included with the award winning Cofense PhishMe product.
- ✓ Cofense PhishMe Certification - The first and only industry-certification for phishing simulation programs.
- ✓ Customers are able to implement the Cofense Reporter™ button which provides end users with easy one-click reporting of suspicious emails from their computers or mobile devices.
- ✓ Board reports providing customers with executive level customized reports.
- ✓ Gartner lists Cofense is a leader in the computer awareness computer based training (CBT) space.
- ✓ Forrester case study showed a 336% ROI for Cofense solutions with a 2.7 month payback.
- ✓ HTTPS for Scenarios allows you to educate your employees on the increasing use of fake SSL certificates in phishing emails and websites.

What is Cofense PHISHME?

Cofense PhishMe is a purpose-built SaaS platform that improves employee response to phishing attacks and empowers employees to provide real-time threat intelligence by immersing them in a real-world spear phishing experience. The solution's customizable scenarios focus on emulating the most relevant threats and providing in the moment feedback and education to recipients who fall victim to these exercises.

Our patented technology provides an unmatched range of cyber attack themes, content and customization, and delivers detailed analysis and reporting for each scenario. Cofense's world class customer support ensures exercises are conducted in a controlled manner that does not compromise security or create negative backlash.

> “
>
> Cofense PhishMe’s enhanced analytics reporting is invaluable. Using that data, we were able to modify our phishing defense programs with more targeted education, specifically for those employees with high click rates in an effort to reduce that number.
>
> **Jim Stewart, CISO, United Community Bank**

Customizable Content and Relevant Training

Cofense PhishMe’s scenarios can be customized to simulate a variety of attack techniques including drive-by, malware, and social engineering attacks, as well as more advanced tactics such as Business Email Compromise (BEC), conversational phishing, and highly personalized spear phishing. Additionally, customers can run scenarios to benchmark their progress against Cofense’s growing number of customers.

Customers can build their own scenarios or use one of dozens of customizable pre-built templates. Our expanding library of content covers a multitude of security topics such as phishing, security awareness, compliance, and social media in various formats, including HTML5 templates, videos, and a game module. With multilingual content and education, Cofense addresses the diverse cultural needs of regional and global businesses.

For organizations that require more comprehensive training, Cofense offers fully SCORM compliant educational content that covers general security topics. Available training covers the following topics:

- Spear phishing awareness
- Malicious links
- Malware
- Password security
- Data protection
- Mobile devices
- Safer web surfing
- Social engineering
- Social networking
- Physical security
- Working outside the office
- Reporting suspicious activity
- Ransomware
- Business Email Compromise (BEC)
- Advanced spear phishing

Secure Delivery Platform

The Cofense PhishMe SaaS platform is certified as a Service Organization Controls (SOC) 2 Type I environment with regard to security, availability, and confidentiality principles defined by the American Institute of Certified Public Accountants (AICPA). Cofense PhishMe environments are regularly audited by internal and external auditors. Cofense never collects sensitive data from customers when they are using data-entry scenarios in Cofense PhishMe product.

Detailed Analytics

Each scenario provides metrics to track a multitude of data points that, when analyzed over time, provide insight into organizational suspceptibility and offer a path for continuous improvement.

Cofense PhishMe’s reporting tracks, for example:

- Geolocation
- Timestamps
- Individual responses
- Trends
- Time spent on training
- Time to first report (Reporter required)
- Browser enumeration
- Organizational Resiliency (Reporter required)

Ensure Customer Success

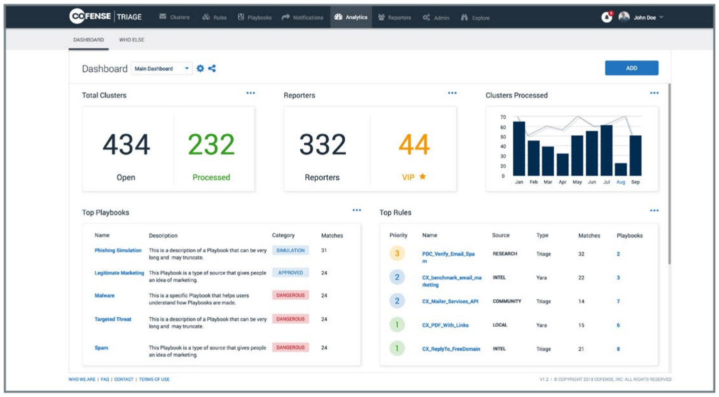
Each Cofense PhishMe license includes access to Cofense’s world class customer support. In addition to ensuring proper delivery of email-based scenarios, our support team provides expert advice for implementing Cofense PhishMe, reviewing email scenarios against industry best practices, tailoring the program to an organization’s culture, leadership, and user base, and providing assistance for new features and scenarios.

If resources are limited, organizations can also leverage Cofense PhishMe as a partially or fully-managed solution with a dedicated professional assigned to their account who creates, executes, and analyzes the results of campaigns. Programs are customized for an organization’s requirements and culture.

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? 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.



Total Clusters

434 Open

232 Processed

Reporters

332 Reporters

44 VIP ★

Clusters Processed

Top Playbooks

Name	Description	Category	Matches
Phishing Simulation	This is a description of a Playbook that can be very long and may truncate.	SIMULATION	31
Legitimate Marketing	This Playbook is a type of source that gives people an idea of marketing.	APPROVED	24
Malware	This is a specific Playbook that helps users understand how Playbooks are made.	DANGEROUS	24
Targeted Threat	This is a description of a Playbook that can be very long and may truncate.	DANGEROUS	24
Spam	This Playbook is a type of source that gives people an idea of marketing.	DANGEROUS	24

Top Rules

Priority	Name	Source	Type	Matches	Playbooks
3	PDC_Verify_Email_Spam	RESEARCH	Triage	32	2
2	CX_benchmark_email_marketing	INTEL	Yara	22	3
2	CX_Mailer_Services_API	COMMUNITY	Triage	14	7
1	CX_PDF_With_Links	LOCAL	Yara	15	6
1	CX_ReplyTo_FreeDomain	INTEL	Triage	21	8

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

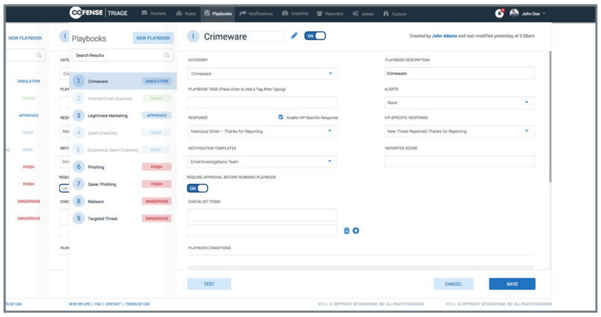
Cofense Triage integrates with your existing SIEM, malware and domain analysis, and threat intelligence solutions. Cofense continually develops new partnerships and integrations to improve functionality and accommodate market needs. A current list of available integrations is available on https://cofense.com/technology-partners/.

> 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.



Search Results

1 Crimeware SIMULATION
2 Internal Email (Inactive) TRIAGE
3 Legitimate Marketing APPROVED
4 Spam (Inactive) SPAM
5 Suspicious Spam (Inactive) SPAM
6 Phishing PHISH
7 Spear Phishing PHISH
8 Malware DANGEROUS
9 Targeted Threat DANGEROUS

1 Crimeware ON

Created by John Adams and last modified yesterday at 9:58am

CATEGORY: Crimeware
PLAYBOOK DESCRIPTION: Crimeware
PLAYBOOK TAGS (Press Enter to Add a Tag After Typing)
ALERTS: None
RESPONSE: Malicious Email – Thanks for Reporting
☑ Enable VIP-Specific Response
VIP-SPECIFIC RESPONSE: New Threat Reported! Thanks for Reporting
NOTIFICATION TEMPLATES: Email Investigations Team
REPORTER SCORE
REQUIRE APPROVAL BEFORE RUNNING PLAYBOOK: ON
CHECKLIST ITEMS
PLAYBOOK CONDITIONS

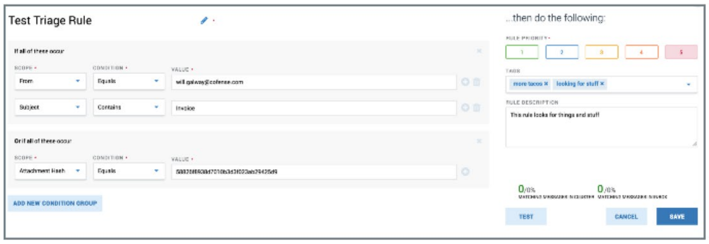
V1.2 | © COPYRIGHT 2018 COFENSE, INC. ALL RIGHTS RESERVED

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.



Test Triage Rule

If all of these occur

SCOPE	CONDITION	VALUE
From	Equals	will.galway@cofense.com
Subject	Contains	Invoice

Or if all of these occur

SCOPE	CONDITION	VALUE
Attachment Hash	Equals	5882fdf6080d7010b3d3f023ab29425d9

...then do the following:

RULE PRIORITY: 1 2 3 4 5
TAGS: more tacos × looking for stuff ×
RULE DESCRIPTION: This rule looks for things and stuff

0/0% MATCHING UNKNOWN IN CLUSTER
0/0% MATCHING UNKNOWN IN INBOX

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.

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.