YOUR **PROBLEM.**

Cutting through the noise to find real phish takes too long. When your analysts have to slog through piles of reported spam, you lose precious time as threats begin to spread—and potentially dwell on your network for days, weeks, or months. Empower your analysts to identify false positives quickly and answer the vital question: “Where should we focus first?”

OUR **SOLUTION.**

With Cofense Triage, prioritize and remediate phishing threats faster. A culture of user-reporting is key to stopping phishing attacks, but your overburdened SOC team needs to prioritize what’s reported. Instead of slowing their efforts with time-consuming manual processes—the numerous steps required to find and understand real indicators of threats—automate analysis with Cofense Triage and focus on making decisions to speed remediation.

Cofense Triage lets you speed analysis of user-reported emails, find real phish faster, and respond more effectively.

**IMPROVE RESPONSE.**

When users report emails, you need to search for relevant indicators of a phishing threat. Cofense Triage’s continuously updated library of thousands of rules gives analysts indicators and insights around threat actor tactics—quickly, to isolate high-risk messages and significantly improve response time.

**FIND THE THREAT.**

Cofense Triage clusters reported emails based on payload to aid campaign identification. An industry leading spam engine classifies emails to identify false positives and known bad. Proprietary to Cofense Intelligence rules identify known threats and provide valuable analyst context.

**STRENGTHEN DEFENSE.**

Using Cofense Reporter™, trusted users become a valuable source of phishing threat intelligence to surface genuine threats. Let reporters know if a message contained malicious content or not, creating a partnership with the SOC team that strengthens your phishing defense.
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.

**WHAT IS COFENSE TRIAGE?**

Cofense Triage is a cloud-based platform that streamlines the phishing response process, enabling rapid resolution of threats. With intuitive task management, automated threat qualification, and customizable alerting, Cofense Triage provides SOC teams with the tools they need to respond effectively to phishing attacks.

**HOW COFENSE TRIAGE WORKS.**

Cofense Triage gives incident responders the ability to act on all alerts quickly by automating threat qualification and investigation. SOC teams can focus on interpreting results and responding to phishing threats effectively.

**GETTING STARTED.**

No matter the size of your organization, we have a deployment option: on premises, available as a virtual appliance completely managed by your internal teams; cloud dedicated instance, hosted in the Cofense secure cloud infrastructure; or hosted and fully managed by the Cofense Phishing Defense Center™.

**EXPORT DATA TO SIEM.**

Cofense Triage can export report data to SIEM solutions, such as LogRhythm, to provide additional layers of analysis and to leverage other assets that your organization already uses. Cofense Triage also enables you to import alerts and events into incident management systems, ticketing systems, or other logging systems via syslog or the API to monitor, manage, and respond to alerts and events.

**INTEGRATION WITH COFENSE VISION™.**

User-reported emails are a rich source of intelligence. But what about all those users who don’t report a phish? Cofense Vision helps you identify them and quickly contain the threat. When Cofense Vision is configured as an integration in Cofense Triage, superusers and operators with the right permissions can search for domains and attachments in reported emails and quarantine messages that users fail to report—from all inboxes, directly from Triage, with a single click.

**SHIPS WITH VIRUS TOTAL.**

Cofense Triage ships with a private subscription to VirusTotal to support threat analysis, or you can use your own VirusTotal API key. Cofense Triage can auto-submit file hashes or URLs to VirusTotal for analysis enabling the detection of malicious content using AV engines and website scanners.

**GETTING STARTED.**

No matter the size of your organization, we have a deployment option: on premises, available as a virtual appliance completely managed by your internal teams; cloud dedicated instance, hosted in the Cofense secure cloud infrastructure; or hosted and fully managed by the Cofense Phishing Defense Center™.

**EXPORT DATA TO SIEM.**

Cofense Triage can export report data to SIEM solutions, such as LogRhythm, to provide additional layers of analysis and to leverage other assets that your organization already uses. Cofense Triage also enables you to import alerts and events into incident management systems, ticketing systems, or other logging systems via syslog or the API to monitor, manage, and respond to alerts and events.

**INTEGRATION WITH COFENSE VISION™.**

User-reported emails are a rich source of intelligence. But what about all those users who don’t report a phish? Cofense Vision helps you identify them and quickly contain the threat. When Cofense Vision is configured as an integration in Cofense Triage, superusers and operators with the right permissions can search for domains and attachments in reported emails and quarantine messages that users fail to report—from all inboxes, directly from Triage, with a single click.

**SHIPS WITH VIRUS TOTAL.**

Cofense Triage ships with a private subscription to VirusTotal to support threat analysis, or you can use your own VirusTotal API key. Cofense Triage can auto-submit file hashes or URLs to VirusTotal for analysis enabling the detection of malicious content using AV engines and website scanners.