TRENNEN SIE DAS RAUSCHEN VOM **PHISHEN.**

COFENSE TRIAGE™

IHR **PROBLEM.**

Das Rauschen manuell von echten Phishing-Angriffen zu trennen ist sehr aufwendig. Wenn Ihre Analysten sich durch ein Haufen gemeldeter Spam-Mails arbeiten müssen, verlieren Sie wertvolle Zeit, da sich die Bedrohungen ausbreiten und möglicherweise Tage, Wochen oder Monate lang in Ihrem Netzwerk verweilen. Wir ermöglichen Ihren Analysten, falsch-positive Ergebnisse schnell zu identifizieren und die entscheidende Frage zu beantworten: „Worauf sollen wir uns zuerst konzentriert?“

UNSERE **LÖSUNG.**

Mit Cofense Triage können Sie Phishing-Bedrohungen schneller priorisieren und beheben. Eine wirksame Kultur der Benutzerberichterstattung ist der Schlüssel, wenn es darum geht, Phishing-Angriffe zu stoppen, aber Ihr überlastetes SOC-Team muss in der Lage sein, die Berichte effektiv zu priorisieren. Anstatt ihre Arbeit mit zeitaufwändigen manuellen Prozessen zu verlangsamen (um echte Indikatoren für Bedrohungen zu finden und zu verstehen, sind zahlreiche Schritte erforderlich) automatisieren Sie die Analyse mit Cofense Triage und konzentrieren Sie sich auf die Entscheidungsfindung, um die Abwehr von Bedrohungen zu beschleunigen.

Mit Cofense Triage können Sie die Analyse der von Benutzern gemeldeten E-Mails beschleunigen, echte Phishing-Mails schneller finden und effektiver auf die wahren Bedrohungen reagieren.

REAKTION VERBESSERN.

Wenn Benutzer E-Mails melden, müssen Sie nach relevanten Indikatoren für eine Phishing-Bedrohung suchen. Die ständig aktualisierte Bibliothek von Cofense Triage mit Tausenden von Regeln gibt Analysten Indikatoren und Einblicke in die Taktiken der Bedrohungsakteure. So können sie schnell gefährliche Nachrichten isolieren und ihre Reaktionszeit deutlich verbessern.

BEDROHUNGEN IDENTIFIZIEREN.

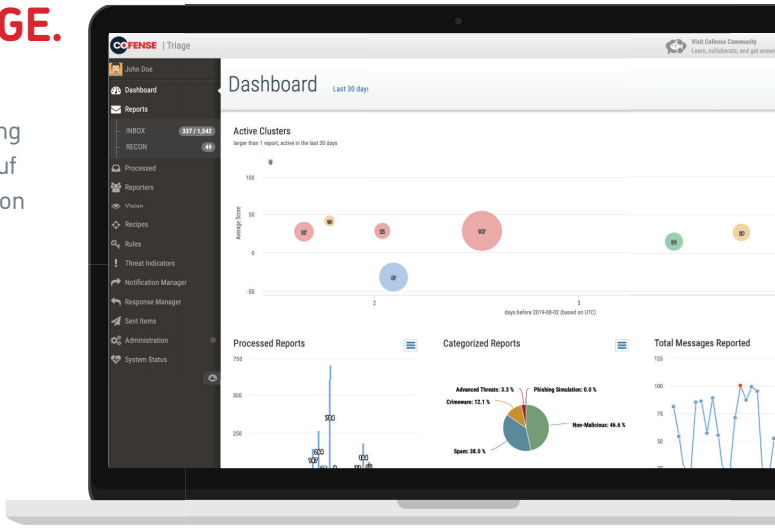
Cofense Triage gruppiert E-Mails auf Basis der Schadlast, um die Identifizierung einer Angriffskampagne zu erleichtern. Eine branchenführende Spam-Engine klassifiziert E-Mails, um falsch-positive und bekanntermaßen schädliche E-Mails zu identifizieren. Die proprietären Regeln von Cofense Intelligence identifizieren bekannte Bedrohungen und liefern wertvollen Analystenkontext.

STÄRKEN SIE IHRE VERTEIDIGUNG.

Mit Cofense Reporter™ werden vertrauenswürdige Anwender zur wertvollen Informationsquelle über Phishing-Bedrohungen und helfen dabei, echte Bedrohungen aufzudecken. So können Sie Ihren Benutzern schnell Feedback geben, ob eine Nachricht bösartige Inhalte enthält oder nicht, und eine Partnerschaft mit dem SOC-Team schaffen, die Ihre Verteidigung gegen Phishing stärkt.

SO FUNKTIONIERT **COFENSE TRIAGE.**

Cofense Triage ermöglicht es Ihren Sicherheitsspezialisten, schnell auf Alarme zu reagieren, indem die Qualifizierung und Untersuchung von Bedrohungen automatisiert wird. SOC-Teams können sich so auf die Interpretation der Ergebnisse und die effektive Beantwortung von Phishing-Bedrohungen konzentrieren.



ERSTE SCHRITTE.

Egal wie groß Ihr Unternehmen ist, wir haben die richtige Bereitstellungsoption: vor Ort, verfügbar als virtuelle Anwendung, die vollständig von Ihren internen Teams verwaltet wird; als dedizierte Cloud-Instanz, die auf der sicheren Cloud-Infrastruktur von Cofense gehostet wird; oder gehostet und vollständig verwaltet vom Cofense Phishing Defense Center™.

DATEN NACH SIEM EXPORTIEREN.

Cofense Triage kann Berichtsdaten in SIEM-Lösungen wie LogRhythm exportieren, um zusätzliche Analysefähigkeiten bereitzustellen und andere bereits in Ihrem Unternehmen verwendete Assets zu nutzen. Cofense Triage ermöglicht es Ihnen außerdem, Warnmeldungen und Ereignisse über Syslog oder die API in Incident Management Systeme, Ticketing Systeme oder andere Logging Systeme zu importieren, um Warnmeldungen und Ereignisse zu überwachen, zu verwalten und darauf zu reagieren.

BEINHALTET VIRUS TOTAL.

Cofense Triage wird mit einem privaten Abonnement von VirusTotal zur Unterstützung der Bedrohungsanalyse ausgeliefert – alternativ können Sie aber auch Ihren eigenen VirusTotal API-Schlüssel verwenden. Cofense Triage kann automatisch Datei-Hashes oder URLs zur Analyse an VirusTotal senden und so die Erkennung von schädlichen Inhalten mit Hilfe von AV-Engines und Webseiten-Scannern ermöglichen.

INTEGRATION MIT COFENSE VISION™.

Von Benutzern gemeldete E-Mails sind eine wichtige Informationsquelle. Aber was ist mit all den Benutzern, die Phishing-Angriffe nicht melden? Cofense Vision hilft Ihnen, solche Benutzer zu identifizieren und die Bedrohung schnell einzudämmen. Wenn Cofense Vision als Integration in Cofense Triage konfiguriert ist, können Superuser und Benutzer mit den richtigen Berechtigungen nach Domänen und Anhängen aus gemeldeten E-Mails und Quarantänemitteilungen suchen, die nicht gemeldet wurden - aus allen Posteingängen, direkt aus Triage, mit einem einzigen Klick.

Cofense™, ehemals PhishMe®, ist der führende Anbieter von Lösungen zur menschlichen Abwehr von Phishing-Angriffen und richtet sich speziell an Unternehmen und Organisationen, die Bedenken hinsichtlich ihrer Anfälligkeit gegenüber raffinierten Cyberangriffen haben. Cofense bietet einen auf Zusammenarbeit und Kooperation basierenden Ansatz beim Thema Cybersicherheit, der es ermöglicht, unternehmensweit gegen den am häufigsten verwendeten Angriffsvektor – Phishing – vorzugehen. Cofense betreut Kunden aller Größen in verschiedenen Branchen (darunter aus den Bereichen Finanzdienstleistungen, Energie, öffentliche Verwaltung, Gesundheitswesen, Technologie und Fertigung) sowie andere Global 1000-Unternehmen, die verstehen, wie ein ansprechendes Nutzerverhalten die Sicherheit verbessert, die Reaktion auf Vorfälle unterstützt und das Risiko von Kompromittierungen verringert.

COFENSE

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