Ihre menschliche Phishing-Verteidigungslinie

WIR BIETEN WELTWEIT FÜHRENDE SICHERHEITSLÖSUNGEN

Mehr als 90 % der Sicherheitsverletzungen in Unternehmen werden durch erfolgreiche Phishing-Kampagnen verursacht. Da ist es für Unternehmen einfach, die Schuld bei ihren Mitarbeitern zu suchen und diese als das Problem zu betrachten. Doch wir sehen das anders. Cofense ist der Meinung, dass Mitarbeiter – Menschen – Teil der Lösung sind, die zum Schutz des Unternehmens beitragen und in Echtzeit Informationen zu akuten Bedrohungen sammeln können.

Phishing ist die Angriffsmethode Nr. 1

Bei 90 % aller weltweiten Cyberattacken haben sich die Angreifer vor allem mittels Phishing Zugang verschafft. Die meisten groß angelegten Datenschutzverletzungen sind auf einen einzigen erfolgreichen Phishing-Angriff zurückzuführen. Da es für gewöhnlich mehr als 200 Tage dauert, bis ein Verstoß entdeckt wird, müssen sich international tätige Unternehmen vor allem auf die Vorbeugung und Vermeidung dieser höchst erfolgreichen Angriffe konzentrieren, um ihnen einen Riegel vorzuschieben.

Menschliche Abwehr von Phishing-Angriffen

Auch wenn Unternehmen Rekordsummen in die Vermeidung von Sicherheitsverstößen investieren, so nimmt die Zahl der Datenschutzverletzungen durch Phishing doch weiterhin zu. Es ist offensichtlich, dass Technologien allein das Problem nicht lösen können. Um Phishing-Angriffen besser vorbeugen und sie besser abwenden zu können, richten sich die Lösungen von Cofense deshalb auf die menschliche Komponente als Ihre allerletzte Verteidigungsinstanz, nachdem ein Phishing-Angriff die installierten Technologien umgangen hat. Cofense liefert eine umfassende Plattform für die menschliche Abwehr von Phishing-Angriffen, die darauf beruht, das Bewusstsein der Mitarbeiter zu schärfen und Teams zu befähigen, gezielte Phishing-Attacken schnell zu analysieren und unmittelbar darauf zu reagieren.

UNSERE SICHERHEITSLÖSUNGEN FÜR IHR UNTERNEHMEN

Erkennen

Wenn ein Phishing-Angriff Ihre Verteidigungsmaßnahmen umgeht, müssen Ihre Mitarbeiter in der Lage sein, diesen Angriff zu erkennen.

Melden

Wenn Mitarbeiter Angriffe melden können, können Sie erheblich schneller auf akute Bedrohungen reagieren.

Reagieren

Mit Cofense erfassen und analysieren Sie Daten zu echten Phishing-Bedrohungen erheblich schneller und können diese somit auch schneller abwehren.

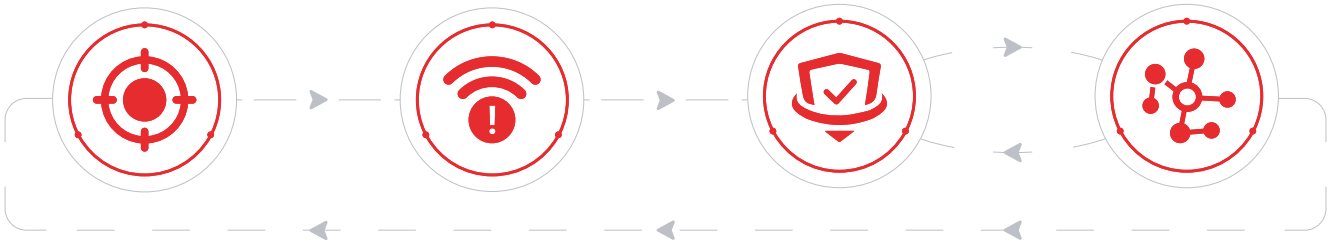
Nachforschen

Cofense konzentriert sich auf durch Phishing verursachte Bedrohungen und bietet von Menschen überprüfte Analysen zu Phishing- und Ransomware-Angriffen und der darin enthaltenen Malware.

Funktionsweise

CONDITION EMPLOYEES
To RECOGNIZE AND REPORT Threats

Cofense PhishMe → Cofense Reporter → Cofense Triage → Cofense Intelligence



SPEED INCIDENT RESPONSE
Collect, Analyze, and RESPOND to Verified Active Threats

Aus Mitarbeitern werden Informanten

Dank der leistungsstarken Kombination aus Cofense PhishMe™ und Cofense Reporter™ werden Mitarbeiter bestärkt, Phishing-Versuchen zu widerstehen und potenziell bösartige Phishing-Angriffe in Echtzeit zu melden. So werden sie zu einem wichtigen Bestandteil Ihrer Verteidigungslinie.

Cofense PhishMe™ – Für eine geringere Anfälligkeit Ihrer Mitarbeiter gegenüber Phishing

Cofense PhishMe nutzt bewährte Methoden der Verhaltenssteuerung, damit Mitarbeiter auf bösartige Phishing-Versuche besser vorbereitet sind und diese eher erkennen. Damit werden Ihre Mitarbeiter, die bisher die größte Schwachstelle in Ihrem Unternehmen waren, zum wertvollsten Schutzmechanismus.

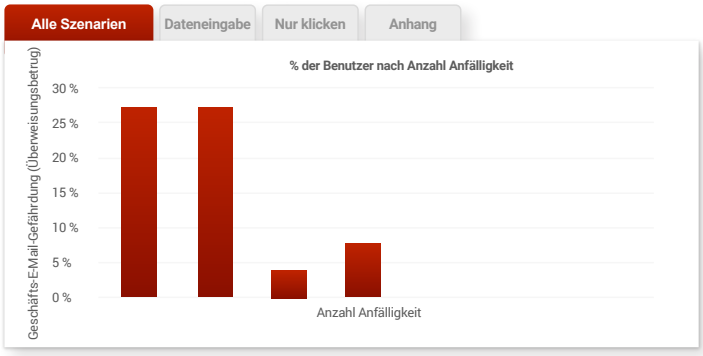
Cofense PhishMe wird als SaaS-basierte Plattform zur Verhaltenssteuerung bereitgestellt und erzeugt individuelle Phishing-Szenarien, bei denen verschiedene Angriffstechniken aus der realen Welt nachgestellt werden:

- **Spear-Phishing-Angriffe**
- **Social-Engineering-Angriffe**
- **Malware und bösartige Anhänge**
- **Drive-by-Angriffe**
- **Fortschrittliche Conversational-Phishing-Angriffe**

Cofense PhishMe lässt sich einfach administrieren und liefert umfangreiche Messwerte, Benchmarking-Daten sowie Berichtsoptionen. Die Lösung stellt vordefinierte und anpassbare Phishing-Szenarien im Rahmen eines ständig erweiterbaren Archivs zur Verfügung. Die Inhalte in Form von HTML5-Vorlagen, Videos und Spielmodulen sind dabei in 19 Sprachen erhältlich.

Zu den behandelten Themen gehören verschiedene Sicherheitsprobleme wie:

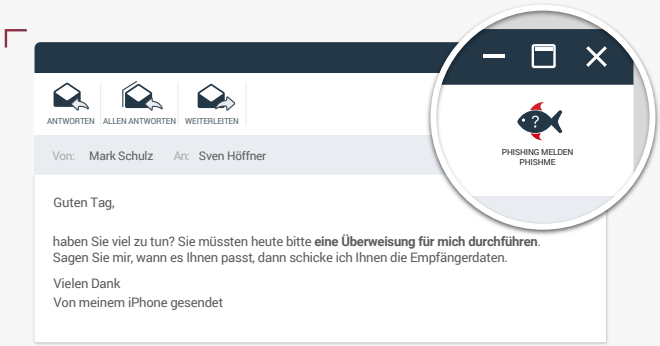
- **Phishing**
- **Sicherheitsbewusstsein**
- **Risiken und Compliance**
- **Social Media in verschiedenen Formaten**



Cofense PhishMe lässt sich einfach administrieren und liefert umfangreiche Messwerte, Benchmarking-Daten sowie Berichtsoptionen.

Cofense Reporter™ – Einfache Vorfallmeldung für alle Mitarbeiter

Bei Cofense Reporter handelt es sich um ein nutzerfreundliches Add-in für E-Mail-Clients, mit dem Nutzer verdächtige E-Mails mit nur einem Klick melden können. Die nutzergenerierten Berichte, einschließlich der kompletten Kopfzeile sowie aller Anhänge der gemeldeten E-Mail, werden dann an die zuständigen Sicherheitsteams weitergeleitet, die den Vorfall weiter auswerten und entsprechend darauf reagieren. Cofense Reporter ist im Lieferumfang jeder Standardlizenz von Cofense PhishMe enthalten und hilft Kunden bei der Erfassung von Daten über Angriffe auf die Datensicherheit. Es ist mit den meisten bekannten E-Mail-Programmen wie Outlook, Office 365, Gmail sowie IBM Notes kompatibel.



Cofense Reporter ist ein einfach zu installierendes und zu verwendendes Add-in für PC oder Mac mit Outlook, Office 365, Gmail oder Lotus Notes E-Mail-Symbolleisten.

Cofense CBFree™ – Computergestützte Schulungen GRATIS

Cofense hat erkannt, dass computergestützte Schulungen, die das Sicherheitsbewusstsein schärfen, dabei helfen, den Compliance-Anforderungen gerecht zu werden. Deshalb haben wir eine Reihe von SCORM-konformen Materialien erstellt, die wir allen Unternehmen bei Bedarf kostenlos zur Verfügung stellen. Unser Archiv an computergestützten Schulungen zur Schärfung des Sicherheitsbewusstseins umfasst 15 Module, die anhand der neuesten Methoden und Trends des E-Learning entwickelt wurden und den Lernenden aktiv mit einbeziehen. Jedes Modul dauert etwa 5 Minuten und umfasst ein optionales interaktives Quiz mit einer Dauer von erneut 5 Minuten. CBFree funktioniert mit oder ohne LMS, sodass es problemlos in jedes Online-Schulungsprogramm eingebunden werden kann. Außerdem sind nun auch computergestützte Schulungen zur Schärfung des Bewusstseins für Phishing-Angriffe in 6 Sprachen verfügbar. Weitere Sprachen werden vorbereitet. Darüber hinaus bietet Cofense drei computergestützte Schulungen zum Thema Compliance in englischer Sprache an.

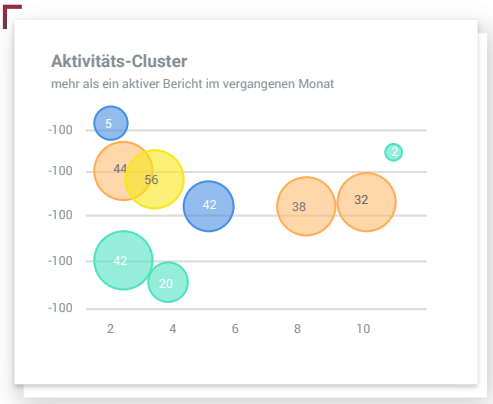
Schnelle Reaktion auf Vorfälle

Cofense Triage™ und Cofense Intelligence™ stärken die Fähigkeit Ihres Unternehmens, akute Phishing-Angriffe schnell zu erkennen und darauf zu reagieren. Da nun alle Mitarbeiter bösartige E-Mails melden, müssen die SOC- und IR-Teams diese sammeln, priorisieren, analysieren und effizient reagieren, um mit der Menge der gemeldeten Bedrohungen Schritt halten zu können.

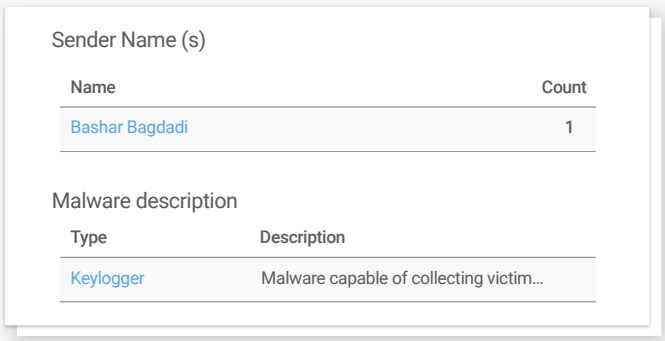
Cofense Triage™ – Phishing-Incident-Response-Management

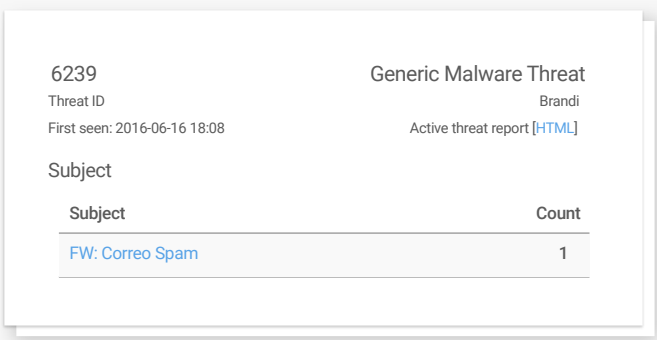
Cofense Triage ist die erste, speziell auf Phishing ausgelegte Response-Plattform, mit der die Identifizierung, Priorisierung und Reaktion auf Bedrohungen durch Phishing-E-Mails mithilfe von Sicherheitsabläufen und Incident-Respondern automatisiert werden können.

Cofense Triage ermöglicht Incident-Respondern, E-Mail-basierte Angriffe auf ihr Unternehmen praktisch in Echtzeit zu erkennen und zu analysieren. Cofense Triage operationalisiert die Sammlung und Priorisierung der von den Mitarbeitern gemeldeten Bedrohungen, ganz gleich ob aus anderen Quellen oder direkt über Cofense Reporter. Das sowohl als vor Ort als auch virtuelle Cloud-basierte App erhältliche Cofense Triage fügt sich in verschiedensten infrastrukturellen Umgebungen nahtlos in Ihre bestehenden Lösungen für SIEM, Malware- und Domainanalyse sowie Bedrohungserkenntnisse ein.



Cofense Triage bietet Echtzeiteinblicke und schnelle Überprüfung von aktuellen Angriffen.





Cofense Intelligence ist über eine RESTful API verfügbar zum Zugriff auf maschinenlesbare Bedrohungserkenntnisse (MRTI) in den Formaten STIX, JSON und CEF.

Cofense Intelligence™ – Phishing-Bedrohungserkenntnisse

Ob als eigenständiges Produkt oder als Bestandteil der Cofense Solution Suite bietet Cofense Intelligence einen hoch zuverlässigen, vom Menschen verifizierten Erkenntnisdienst, der es Sicherheitsteams ermöglicht, akute und sich abzeichnende Bedrohungen zu erkennen, zu blockieren und zu untersuchen. Die Daten zu den Bedrohungen werden in verschiedenen Formen bereitgestellt, um eine effektive Vorbereitung und Reaktion auf Angriffe zu ermöglichen:

- **Menschenlesbare Berichte über Bedrohungserkenntnisse liefern eingehende Analysen der wichtigsten Bedrohungen.**
- **Maschinenlesbare Bedrohungserkenntnisse (MRTI) fließen direkt in Sicherheitsanlagen und Bedrohungsrepositorien ein.**
- **SaaS-Erforschungsanwendungen untersuchen Phishing- und Malware-Angriffe.**
- **Kompetente Unterstützung durch unser globales Sicherheitsteam bei der Implementierung branchenführender, bewährter Verfahren, bei der Optimierung der Phishing-Abwehr und bei der Verringerung von Bedrohungen.**

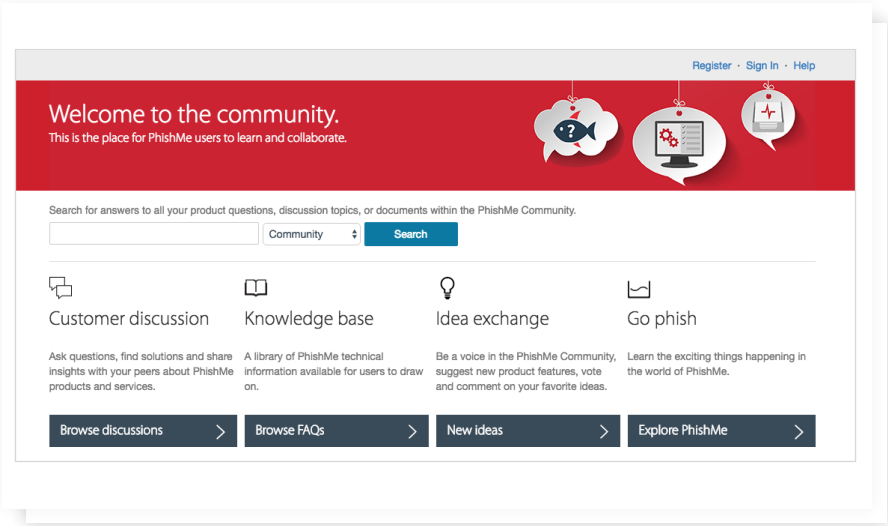
Cofense Intelligence wird von zahlreichen Global-Fortune-100-Unternehmen genutzt und gilt als vertrauenswürdige, hoch zuverlässige Informationsquelle über Phishing-spezifische Bedrohungen.

Kundenerfolg dank Cofense-Diensten

Bei beschränkten Ressourcen bieten wir spezielle professionelle Dienste für teilweise oder vollständig verwaltete Anwendungen von Cofense-Lösungen, darunter einen spezifischen Cofense-Sicherheitsexperte, der jedem Kunden exklusiv zugewiesen wird, um die Entwicklung, Ausführung und Analyse Ihrer Phishing-Abwehrprogramme zu unterstützen. Darüber hinaus werden die Programme an die Anforderungen und kulturellen Gegebenheiten in Ihrem Unternehmen angepasst.

Cofense Support und Community

Jede Cofense-Lizenz beinhaltet Zugang zu unserem erstklassigen Kundensupport und zu unserer Kunden-Community.



Cofense Support

Unser Support bietet kompetente Beratung bei der Implementierung der Cofense-Lösungen, einschließlich:

- **Abgleich von Szenarien mit bewährten Verfahren aus der Branche**
- **Effektive Nutzung der Cofense-Lösungen**
- **Unterstützung bei neuen Funktionen und Szenarien**
- **Individuelle Anpassung umfangreicher Phishing-Abwehrprogramme an jedes Unternehmen**

Cofense Community

Bei der Cofense Community handelt es sich um eine leicht zugängliche Online-Wissensdatenbank, in der sich die Nutzer austauschen und gemeinsam Lösungen entdecken und entwickeln sowie sich von erfahrenen Kollegen bei der Optimierung und Erweiterung ihrer Cofense-Programme unterstützen lassen können. Über die Cofense Community können die Nutzer von Cofense-Lösungen und -Produkten auf alle Informationen und Tools zugreifen, die sie zur Optimierung und Erweiterung ihrer Anti-Phishing-Programme benötigen.

Cofense™, ehemals PhishMe®, ist der weltweit führende Anbieter von Anti-Phishing-Lösungen. Wir bieten einen auf Zusammenarbeit basierenden Cybersicherheitsansatz, mit dem wir es ermöglichen, unternehmensweit gegen aktive E-Mail Bedrohungen vorzugehen. Unsere Verteidigungslösungen kombinieren marktführende Technologien und aktuelle Angriffsintelligenz von Mitarbeitern um laufende Angriffe schneller zu stoppen und weitere Sicherheitsverstöße früh zu erkennen.
Von der Sensibilisierung der Mitarbeiter bis zur Sicherheitsautomatisierung und Integration sind unsere Lösungen darauf ausgelegt, die Angriffskette zu unterbrechen um die Auswirkungen von Spear Phishing, Ransomware, Malware und Business Email Compromise E-Mails schnell einzudämmen.
Tausende globale Unternehmen im Bereich Verteidigung, Energie, Finanzen, Gesundheitswesen und Fertigung profitieren bereits durch angepasstes Mitarbeiterverhalten von der Möglichkeit, schneller auf Vorfälle reagieren zu können und das Risiko von Sicherheitsverstössen zu vermindern.

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

Weitere Informationen finden Sie unter **www.cofense.com.**