人的関与による Phishing 対策

世界クラスのセキュリティ・ソリューションを提供することに専念する

侵害の90%以上が phishing キャンペーンの成功に起因しており、組織にとって、従業員に日々解決すべき根本原因を指摘することは簡単に思えます。そうでしょうか。当社はそうは思いません。Cofense は、従業員 – 人間 – こそ、ソリューションの一部として、進行中の攻撃を阻止するために防御を強化し、リアルタイムの攻撃情報を収集するのに役立つ役割を与えられるべきだと考えています。

Phishing は最大の攻撃方法

Phishing は世界中のサイバー攻撃の実に90%を占める主要な方法です。注目を浴びている侵害の多くは、たった 1 件の成功を収めた phish から発生しているのです。侵害を検出するには通常200日以上かかるので、世界中の組織は、この非常に成功している攻撃手法を無力化するために、予防と対応への取り組みに努力を集中する必要があります。

人間主導の Phishing ソリューション

記録的な投資が注ぎ込まれているにも関わらず、phishing の攻撃に起因する侵害の数は増え続けています。もはや技術だけではこの問題を解決できないことは明白です。これこそが、予防と対応をより向上させるために、phish が他のテクノロジーをすり抜けてしまった後の最後の防波堤として、Cofense ソリューションが人を関与させることに焦点を当てる理由です。Cofense は、従業員を強化し、標的とされた phishing 攻撃をインシデント対応チームが迅速に分析し対応できるようにすることに焦点を当てた、総合的な人的関与による phishing 防護対策プラットフォームを配信します。

当社からのソリューション

認識する

phish が御社の技術を通過するときに、従業員はその試みを認識できる必要があります。

報告する

進行中の攻撃を報告するように従業員を引き込めば、進行中の脅威や攻撃の展開に対応するための時間を大幅に短縮することができます。

対応する

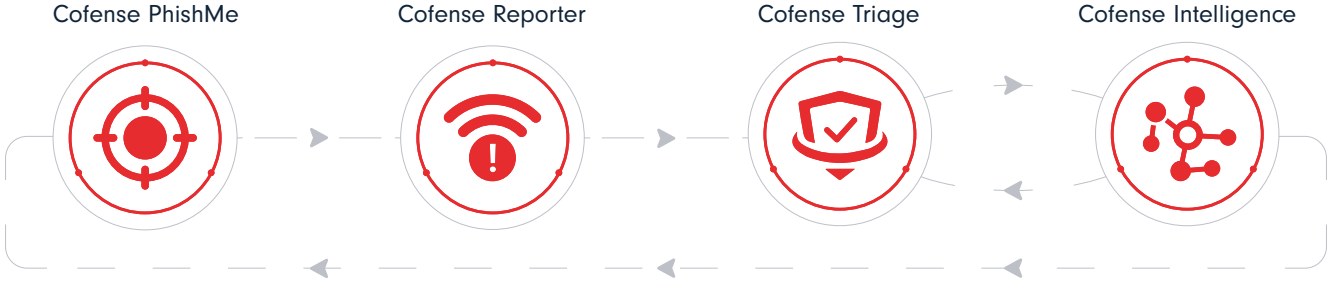
Cofense は、実際の phishing 脅威に対する収集、分析、対応を大幅にスピードアップします。

調査する

Cofense は、phishing 固有の脅威に重点を置き、phishing やランサムウェアのキャンペーン、それに含まれるマルウェアの人が吟味した分析を提供します。

その仕組み

CONDITION EMPLOYEES
To Recognize and Report Threats



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

従業員を情報提供者にする

Cofense PhishMe™ と Cofense Reporter™ の強力な組み合わせは、従業員を phishing 攻撃に抵抗するよう適用させ、潜在的に悪質な phishing 攻撃をリアルタイムで報告できる役割を与え、防衛の一部を担うようにします。

Cofense PhishMe™ - 従業員の Phishing に対する脆弱さを軽減する

Cofense PhishMe は、業界で実証済みの行動コンディショニング法を使用して、従業員が悪意のある phishing 攻撃を認識し抵抗できるようにより周到に準備させ、従業員という最大のマイナス要因を最強の防衛に転換します。

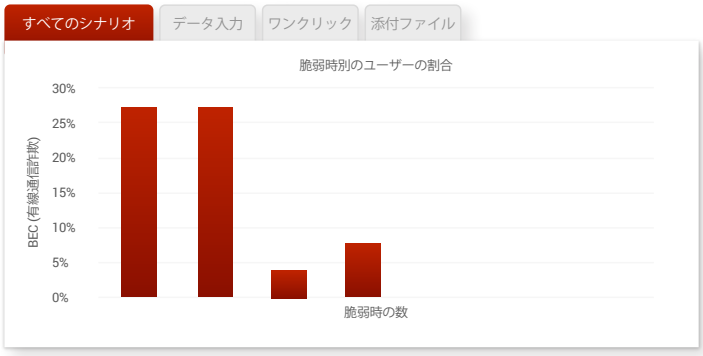
SaaSベースの条件付けプラットフォームとして利用可能な Cofense PhishMe は、カスタマイズされた phishing 攻撃のシナリオを作成し、次のような現実世界の様々な攻撃手法を再現します：

- **Spear phishing（スピアフィッシング）攻撃**
- **ソーシャルエンジニアリング攻撃**
- **マルウェアおよび悪意のある添付ファイル**
- **ドライブバイ（ダウンロード）攻撃**
- **高度な会話式 phishing 攻撃**

Cofense PhishMe は管理が容易で、ディープメトリクス、ベンチマークおよびレポートオプションを提供します。このソリューションは、事前に組み込まれたカスタマイズ可能なphishingシナリオを拡大を続けるコンテンツライブラリー（19言語）で提供すると共に、HTML5のテンプレート、ビデオ、ゲームモジュールを備えています。

トピックは、以下を含むセキュリティ上の様々な懸念を対象としています：

- **Phishing**
- **セキュリティ認識**
- **リスクとコンプライアンス**
- **さまざまな形式のソーシャルメディア**



Cofense PhishMe は管理が容易で、ディープメトリクス、ベンチマークおよびレポートオプションを提供します。

Cofense Reporter™ - 全従業員のための簡単な報告

Cofense Reporter は使いやすい電子メールクライアントアドインで、ユーザーは単にクリックするだけで不審なメールを報告することができます。ユーザーが作成した報告はその後、報告された電子メールの完全なヘッダーと添付ファイルを含めて、さらなるセキュリティ分析やインシデント対応のためにセキュリティチームに転送されます。Cofense Reporter は標準の Cofense PhishMe ライセンスの一部として含まれており、ユーザーが内部攻撃情報を収集するのに役立ちます。この Reporter は、Outlook、Office 365、Gmail、IBM Notes を含む標準的な電子メールソリューションと連携します。

Cofense Reporter は、Outlook、Office 365、Gmail、またはLotus Notes の電子メールツールバーを使用して、PCまたはMAC用のアドインを簡単にインストールして使用できます。

Cofense CBFree™ - 無料 CBT（コンピュータベースのトレーニング）

Cofense では、セキュリティ認識コンピュータ・ベース・トレーニング（CBT）がコンプライアンスニーズを満たすためのチェックボックスに役立つことが認識しています。これが、それを必要とする組織のすべてを対象に無料の SCORM 準拠のマテリアルセットを当社が開発した理由です。セキュリティ認識CBTの当社ライブラリには、学習者による実質的な関与を促進する、最新eラーニング技術や動向を利用して開発された15のモジュールが含まれています。各モジュールを完了するには約5分かかります。オプションでさらに5分のインタラクティブなQ＆Aが付いています。CBFree は LMS 付きまたは LMS なしで機能するので、オンライン学習プログラムに簡単に追加できます。また、Cofense のセキュリティ認識CBTは現在6ヶ国語に対応しており、今後さらに多くの言語でご利用いただけます。Cofense は、3つのコンプライアンスに重点を置いた英語版 CBT モジュールも提供しています。

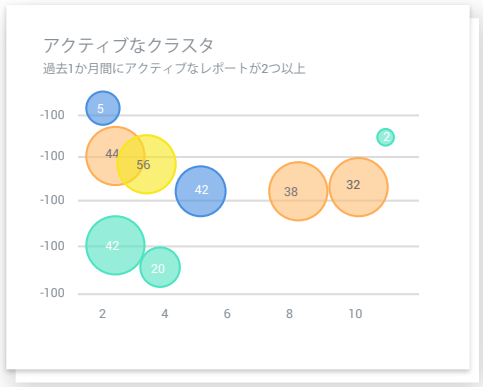
スピード・インシデント・レスポンス

Cofense Triage™ と Cofense Intelligence™ は、進行中の phishing 攻撃を組織が迅速に特定し対応できる能力を強化します。今や全従業員ベースで悪質な電子メールを報告している状況では、SOCとIRチームは、報告された脅威の量に対応するため、効率よく収集し、優先順位を決め、分析し、対応しなければなりません。

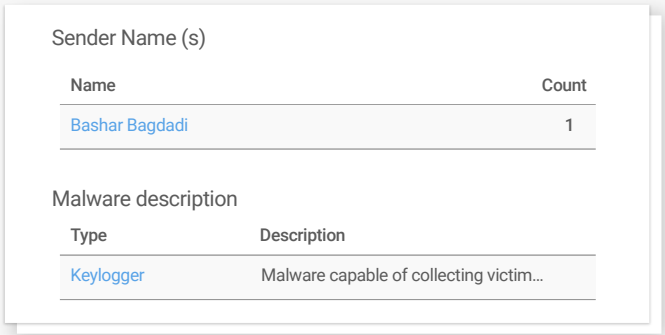
Cofense Triage™ - Phishing インシデント対応

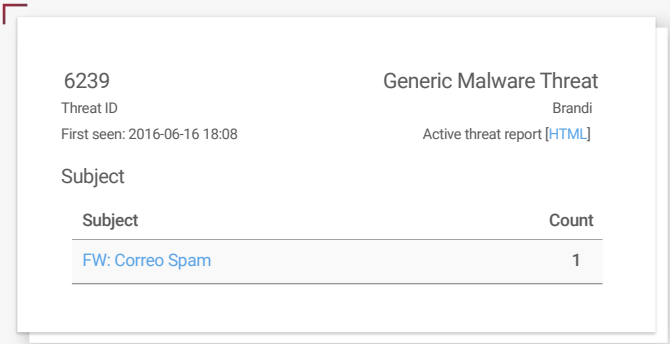
Cofense Triage は業界初の phishing に特化されたインシデント対応プラットフォームであり、セキュリティ操作とインシデント応答者が phishing メールを介して配信される脅威を自動的に識別、優先順位付け、および対応できるようにします。

Cofense Triage は、組織を標的に発生する電子メールベースの攻撃に対して必要な可視性と分析を、インシデント応答者にほぼリアルタイムで提供します。Cofense Triage は、他のソースからか Cofense Reporter から直接かを問わず、従業員が報告する脅威の収集と優先順位付けを可能にします。オンプレミスまたはクラウドベースの仮想アプライアンスとして入手可能な Cofense Triage は、既存の SIEM、マルウェアとドメイン分析、さらに脅威インテリジェンスソリューションを、様々なインフラストラクチャ環境全体にわたってシームレスに統合します。



Cofense Triage は、進行中の攻撃の可視性と迅速な検証をリアルタイムで提供します。





Cofense Intelligence は、STIX、JSON、および CEF 形式の機械可読型脅威インテリジェンス（MRTI）にアクセスするための RESTful API を介して利用できます。

Cofense Intelligence™ - Phishing 脅威インテリジェンス

スタンドアロン製品として、あるいは Cofense ソリューションスイートに統合された形で入手可能な Cofense Intelligence は、高品質で人間検証済みのインテリジェンスサービスで、セキュリティチームが進行中の進化している脅威を識別し、ブロックし、調査できるようにします。脅威データは、攻撃に対して効果的に準備し対応するために、複数のフォームで配信されます。

- **人間が読める脅威インテリジェンスレポートは、最大の脅威に対するディープダイブ分析を提供します。**
- **機械可読型脅威インテリジェンス（MRTI）は、セキュリティデバイスや脅威リポジトリに直接流れ込みます。**
- **SaaS 調査アプリケーションが phishing およびマルウェア攻撃を調査します。**
- **業界をリードするベストプラクティスを実装するための当社グローバルセキュリティチームによる専門家の指導が、phishing 防衛成果を改善し、脅威を軽減します。**

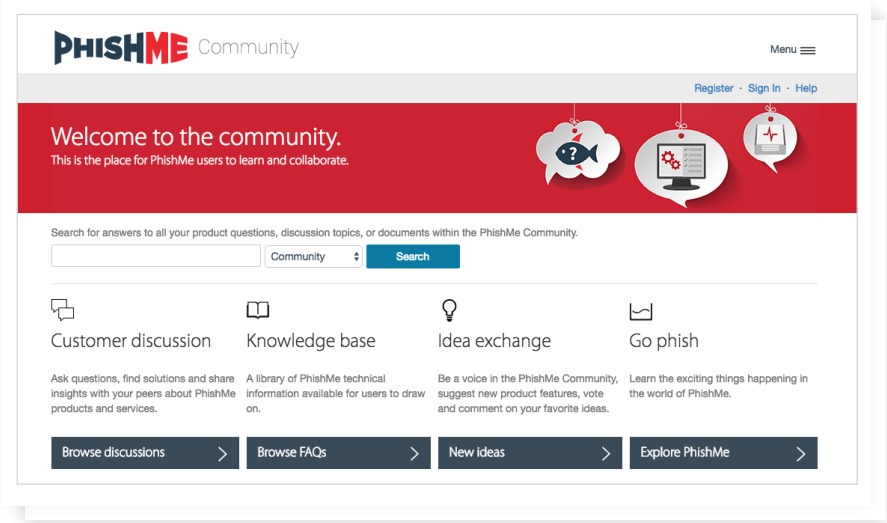
Cofense Intelligence は世界の「フォーチュン100」の多くの企業で使用され、phishing 固有の脅威情報に関する信頼できる高品質なソースとして称賛されています。

お客様の成功を Cofense Services が保証

リソースが限られている場合は、プロフェッショナルサービスとして、部分的あるは、包括的なManaged Serviceを提供し、組織の防御プログラムの作成、実行、分析を各アカウント 毎に排他的にCofense 専任のセキュリティ専門家をが支援します。プログラムは、組織の要件や多様な文化的環境に合わせてカスタマイズされます。

Cofense サポートとコミュニティ

各Cofenseライセンスには、当社の世界クラスの顧客サポートの他、お客様コミュニティプラットフォームへのアクセスが含まれます。



Cofense サポート

当社のサポートは、次のような Cofense ソリューションの実施に対する専門家のアドバイスを提供します。

- **業界のベストプラクティスに照らしたシナリオの検討**
- **Cofense ソリューションの効果的活用**
- **新機能やシナリオに対する支援の提供**
- **総合的な phishing 防衛プログラムの各組織に適した調整**

Cofense コミュニティ

Cofense コミュニティは簡単にアクセスできるオンラインのナレッジベースを提供します。ここでユーザーたちは、共有、協力し発見や開発を進め、さらには専門家のリソースやピアアドバイザーへとつながり、各自の Cofense プログラムを改善、成長させることができます。Cofense コミュニティは、Cofense ソリューションおよび製品のユーザーが、そのphishing 対策プログラムを向上、拡大させるために必要なすべての情報やツールにアクセスできる場所です。

Cofense(旧PhishMe)は、人間主導型のフィッシング防御ソリューションを全世界的に提供する大手プロバイダーです。私たちは、能動的な電子メールの脅威に対する組織を挙げた取り組みを可能にすることで、サイバーセキュリティに対する協調して対応するアプローチを提供します。

当社の集合的防御スイートは、最上級のインシデント対応技術を、従業員からもたらされたタイムリーな攻撃情報と組み合わせます。Cofenseのソリューションは、スピアフィッシング、ランサムウェア、マルウェア、および業務電子メール漏洩の影響を素早く軽減します。今やこれは、国際的組織、企業にとってすべて現実となっています。　より詳しくは、www.cofense.comをご覧ください。

COFENSE

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