COFENSE ソリューション概要

Cofense の Phishing Detection and Response(PDR)プラットフォームを用いてフィッシング攻撃を阻止

ビジネスにおける課題

メールやゲートウェイのセキュリティに多額の投資を費やしているのにもかかわらず、何千通ものフィッシングメールが古くなったセキュリティソリューションを巧みにすり抜ける状況が続いています。フィッシング攻撃の 96% はメールを通じて仕掛けられており、ビジネスメール詐欺(BEC)、知的財産の盗取、生産性の低下につながっています。さらには多額のランサムウェアの身代金、クリーンアップ費用、法令順守やその他の規制にかかわる罰金をもたらします。どう考えても、現行のアプローチは機能していません。

ソリューション

組織がフィッシング問題に効果的に対処するためには、グローバルネットワークを持つクラウドソース型フィッシングインテリジェンスと高度な自動化技術とが組み合わされ、脅威を高速検証して排除することのできるソリューションが必要です。さらにそのソリューションは、ポリシーに基づいて自動的に、またはセキュリティオペレーションセンター(SOC)アナリストのアクションと組み合わせて、フィッシングメールの自動隔離が実行可能である必要があります。Cofense の Phishing Detection and Response(PDR)プラットフォームは、フィッシング攻撃を阻止する効果的で効率的なソリューションをご提供すべく開発されました。

Cofense は平均して

3,500

件以上のフィッシング脅威を各顧客につき毎年発見しています。既存の セキュア Eメールゲートウェイ(SEG)技術はそれらをすべて見逃していました。

PHISHING DETECTION AND RESPONSE(PDR) の利点

- 従業員が受信トレイで見かけるブランドやその他の要素を含む架空のフィッシングメールと対比させて、実際に遭遇するであろうフィッシングメールを特定できるように従業員をトレーニングする現実的なフィッシングシミュレーション。
- シンプルなワンクリックボタンでフィッシングメールを報告し、報告の状況に関する最新情報を報告者に自動フィードバック。
- フィッシングと疑われるメールや報告を受けたフィッシングメールを迅速にクラスタ化して高速検証を行い、セキュリティ侵害インジケーター(IOC)をパッケージ化し他のシステムにインポートして修復を図る機能。
- 高度な自動化により、従業員がフィッシングメールに引っかかり攻撃が成功してしまう前にフィッシングメールを速やかに隔離。
- 事前設定されたポリシーおよびその他のフィッシングインテリジェンスに基づき、フィッシングメールを自動隔離する機能。
- Cofense の精鋭フィッシング研究チームはもとより、フィッシングと疑われるメールを積極的に特定し報告している 全世界2,500 万人以上の人々から集められたインテリジェンスを活用。
- 総合的なインシデントレスポンス情報の入手を目的として、フィッシングインテリジェンスを既存のセキュリティエコシステム(SOAR、SIEM、TIPS など)と統合。

PHISHING DETECTION AND RESPONSE(PDR) 統合製品

Cofense の Phishing Detection and Response(PDR)プラットフォームには 5 つの完全統合型製品が含まれており、市場でもっとも総合的なソリューションをお届けします。

Intelligence:

Cofense の PDC やリサーチアナリスト、そして 2,500 万人もの強力なフィッシングメールのグローバルネットワークから得られるフィッシングインテリジェンスは、Triage またはご利用中の SIEM、SOAR、TIPS ソリューションなどの自動隔離ルールと統合され、コンテキストを追加します。

Vision:

SOC アナリストは Vision を用いて、フィッシングメール認められたメールを組織全体にわたり検索し隔離します。

またVisionは事前に設定されたポリシーに基づいて、フィッシングメールを自動的に隔離することも可能です。

PhishMe:

従業員は潜在するフィッシングメールを特定できるよう、実際の攻撃に基づいたフィッシングメールシミュレーションとトレーニングで定期的に訓練されます。

Reporter:

フィッシングメールの疑いを報告するシンプルなワンクリックボタン。世界各地の 2,500 万人がフィッシングメールを報告する Cofense ネットワークの一翼を担っています。

Triage:

フィッシングと疑われるメールは Triageにより速やかにクラスター化され、SOC アナリストがそれを分析し、Triage、Vision またはその他のテクノロジーによる修復に向けて脅威情報をキューに加えます。

フィッシングのインシデントレスポンスタイムライン

COFENSE の PDR ソリューションを使用すると、
フィッシング攻撃をわずか 8 分間で阻止できます。

* Cofense Phishing Defence Center (PDC) を通じて提供

Cofense は、ユーザーの行動を変えることがセキュリティ向上、インシデントレスポンスの支援、フィッシング攻撃の成功リスク軽減にどれほど貢献するかを理解しています。Cofense の目指すところは、すべての企業をフィッシングの脅威から自己防衛できる組織にすることです。そして、Cofense のグローバルネットワークの強みを活かすことにより、私たちは共に フィッシングの脅威に打ち勝つことができるのです。

COFENSE のPHISING DETECTION AND RESPONSE(PDR)についての詳細は、次のサイトをご覧ください: cofense.com/product-overview/

Cofense について

Cofense® はフィッシング検知対応ソリューションを提供する先進企業です。Cofense の Phishing Detection and Response（PDR）プラットフォームは企業組織向けに設計されており、フィッシングの疑いのあるメールを積極的に報告する 2,500 万人超の人々が作り出すグローバルネットワークの活用と高度な自動化技術とを組み合わせて、フィッシング攻撃をより迅速に阻止し、セキュリティ侵害に対して常に先回りします。Cofense のソリューションを一式そろえて導入していただくことで、組織は従業員に対してフィッシングメールを特定して報告する方法を教育し、自社の環境内でフィッシングメールを検知し脅威修復に向けて迅速に対応することが可能となります。Cofense のソリューションは主要な TIP、SIEM、SOAR の大半とシームレスに統合でき、既存のセキュリティエコシステムと容易に連携を取ることができます。防衛、エネルギー、金融サービス、医療、製造業など幅広い業界にわたる Global 1,000 企業を顧客に持ち、Cofense はセキュリティ向上、インシデントレスポンスの支援、セキュリティ侵害のリスク軽減を実現する方法を会得しています。詳細につきましては、www.cofense.com をご覧いただくか、Twitter および LinkedIn をフォローしてください。

cofense.com/contact
703.652.0717
1602 Village Market Blvd, SE #400
Leesburg, VA 20175