攻撃者のターゲットを防衛者に変える.

COFENSE PHISHME™

お客様が抱えている問題.

どんなに素晴らしいメールゲートウェイ(SEG)を導入しても、フィッシングメールは依然としてユーザーに届き、侵害を引き起こす恐れがある. Cofense Phishing Defense Center™ は、ユーザーから報告されたメールの 90%が、セキュアメールゲートウェイ(SEG)を使用する環境にあることを見出しています。従業員に届くフィッシングメールはすべて、組織に対する攻撃です。テクノロジーが失敗するならば、従業員は、SOCが脅威を修復できるようにするために、人間のセンサーになってフィッシングを報告する必要があります。しかし、ユーザーが今日の日々進化する攻撃を認識しなければ、どうやって報告できるでしょうか?

Cofense のソリューション.

(本物の) フィッシングメールを識別できるようにユーザーを訓練します. Cofense PhishMe は、企業が直面している実際のフィッシング戦術についてユーザーを教育します。弊社は広範な調査、脅威インテリジェンス、および他のプロバイダーにはない最前線のフィッシング防御リソースを活用しています。実際のフィッシングメールはまさに現実の問題です。経験的な学習(最新のフィッシング脅威のシミュレーション)を通じて、よりスマートなメールでの行動を訓練し、脆弱で攻撃を受けやすいターゲットを不可欠な防御層へと変換します。

Cofense PhishMe は、ユーザーが悪意のあるメールを認識して報告するように訓練し、フィッシングとの戦いで人間の防御者たちを団結させます.

関連している.

効果を最大にするため、フィッシング訓練プログラムは、組織に対する本物の脅威に焦点を合わせる必要があります。セキュリティアウェアネスチームは、訓練メールを送信する機会が限られています。したがって、すべての機会を考慮に入れる必要があります。

効率的である.

自動化により時間を節約します。Cofense PhishMe は、ベストプラクティスであり、組織のセキュリティニーズと優先順位に合わせたフィッシング認識プログラムを定義、スケジュール、および配信するオーバーヘッドを自動的に軽減するのに役立ちます。

自信を持つ.

Cofense はこの市場の開拓者であり、豊富な経験によって、フィッシングプログラムを成功させて最大の結果を達成できる機能を提供することができます。Cofense は、セキュリティアウェアネスのコンピューターベーストレーニングにおける Gartner Magic Quadrant のリーダーに一貫して指名されています。信頼できるイノベーターと共に進みましょう。

COFENSE PHISHMEの仕組み.

Cofense PhishMe は、ユーザーを現実世界のフィッシング体験に浸らせる SaaS プラットフォームです。ソリューションのカスタマイズ可能なシナリオは、最も現実の問題に直結する脅威で訓練し、これらの攻撃の影響を最も受けやすい従業員に即座に関連性のある教育を提供します。

弊社の特許取得済み技術は、比類ないほど広範囲のサイバー攻撃のテーマ、コンテンツ、カスタマイズを提供します。それは各シナリオの詳細な分析と報告を実現します。弊社のカスタマーサポートチームが、セキュリティを侵害したりバックラッシュを発生させたりしない、制御された方法で御社での演習が行われるように保証します。

インテリジェントオートメーション.

フィッシングアウェアネスプログラムを維持するための労力を節約します。Cofense PhishMeプレイブックは、あらかじめ用意された一連のフィッシングシナリオ、ランディングページ、添付ファイル、および教育コンテンツを提供して、年間を通じて実行します。弊社のSmart Suggest機能は、機械学習を使用して、プログラムの履歴と業界の関連性に基づいてシナリオを推奨します。Responsive Deliveryを使用すれば、ユーザーが受信トレイでアクティブなときにだけシミュレーションを配信することにより、メール訓練の効果を最大化できます。これにより、技術的およびタイムゾーンに関連するスケジューリングの問題も解消されます。

アクティブな脅威のシナリオ.

Cofense Intelligence™、Cofense Labs™、およびCofense Phishing Defense Center™ はすべて、アクティブな脅威に関する情報をシナリオに提供します。フィッシング攻撃者のトリックとテクニックに関しては、これ以上に優れている組み合わせソースはありません。「アクティブな脅威」のテンプレートを使用すると、企業や業界に対する攻撃に一致するフィッシングシナリオを見つけることができ、従業員が実際の攻撃をより効果的に見つけて報告するのに役立ちます。組織で導入されているようなセキュアメールゲートウェイ(SEG)をバイパスするのが 判明されたフィッシングメールに基づいたシナリオを検索することもできます。単に SEGMisses フィルターを使用するだけです。会社に対する最も深刻な脅威について従業員に教えていない場合、従業員はセキュリティチームがそれらを阻止するのを支援できません。弊社の「アクティブな脅威」シナリオは、常に変化する環境に合わせてフィッシングアウェアネスプログラムを維持します。

安全な配信プラットフォーム.

Cofense PhishMe SaaS プラットフォームは、米国公認会計士協会（AICPA）によって定義されたセキュリティ、可用性、および機密性の原則に関して、Service Organization Controls（SOC）2 Type II 環境として認定されています。Cofense PhishMe 環境は、内部監査員および外部監査員によって定期的に監査されています。堅固な匿名化は、プライバシーに敏感な環境をサポートします。

価値ある報告指標.

従業員に潜在的なフィッシングメールを報告するように奨励することで、従業員を積極的な防御者に変えることができます。時間とともに、焦点はクリック率から最も重要な指標である報告率と切り替わります。プログラムの有効性とフィッシングのレジリエンス(報告率 ÷ クリック率)向上の実態を把握するには、報告データを組み合わせて、実際の攻撃中に従業員がどのように反応するかを理解し、予測します。さらに、役員レポートを使用すると、経営陣が会社のパフォーマンスを監視し、フィッシング攻撃に対する組織のレジリエンシーの変化を追跡できます。

COFENSE

ウェブサイト: cofense.com/contact **電話:** 703.652.0717
住所: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175