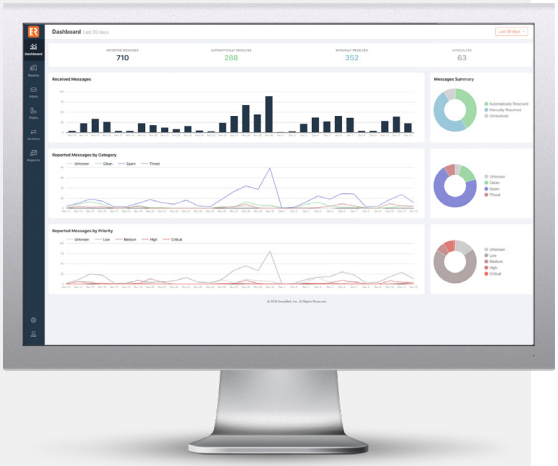
PhishER

KnowBe4
Human error. Conquered.



主なメリット

- KnowBe4のPhish Alert Buttonとの完全なインテグレーションにより、優先度付け（トリアージ）を自動化し、脅威でないメールに自動で優先順位を設定
- セキュリティ担当者の受信ボックスに送られる不要なメールをカットし、より迅速かつ効率的に最も危険な脅威に対応
- メッセージの90%についてスパムか正当なメールかを識別し、管理することでセキュリティ担当者の負担を軽減
- メッセージをパターンに基づいて分析・分類し、自社の組織内で広がるフィッ シング攻撃をいち早く特定、防御
- 自社組織内のミッションクリティカルなSLAを満たし、脅威と正常なメールとを分類し、優先順位付け（トリアージ）
- 自動化されたメール応答テンプレートの設定により、さらなる処置が必要とされる場合にも迅速に報告者へフィードバックが可能
- 優先順位付けやアラートなどのタスクに対応した独自のカスタムワークフローを作成することにより、セキュリティ担当者の負担を軽減。必要な作業に集中することが可能に

PhishER：メールの脅威を迅速に特定し、すばやく対応

フィッシング攻撃は依然として、サイバー攻撃の手段として最も広範に使用されている手口です。そのため、多くのスパムメールや 「疑わしい」メールが企業や組織・ 団体へ向けて日々送信されており、インシデントレスポンスチームに寄せられる報告件数も増加しています。 セキュリティ意識向上トレーニングを組織内で行っているか否かにかかわらず、従業員は日々多くの不審メールを受信しており、それをセキュリティ担当者へ逐一報告していることでしょう。**このような不審メールトラフィックの増加により、セキュリティ担当者は新たな問題を抱えることとなりました。**

ネットワークを攻撃する大量のスパムや悪意のあるメールの約7〜10%がフィルタをすり抜けているのです。従業員が報告する10件のメールのうち、実際に悪意あるメールは1件程度。高リスクのフィッシング攻撃に対処する一方で、インシデントレスポンスチームはいかにして残り90%のメールに正確かつ効率的に対応しているのでしょうか？**そんなときに活躍するのがPhishER™です。**

PhishERとは？

PhishERは、セキュリティに不可欠なワークフローを構成するために必要不可欠なツールです。PhishERは軽量なSOAR（Security Orchestration Automation & Response）プラットフォームで、脅威への対応をオーケストレーションし、ユーザーから報告される膨大な悪意のあるメッセージに迅速に対応できるようにします。メールの優先順位付け（トリアージ）を自動化することによって、PhishERは、IT管理者やセキュリティ担当者に送られる不要なメールをカットし、最も危険な脅威への対応を迅速化・効率化するようサポートします。

加えて、PhishERでは、報告されたメールのうち脅威ではない90%のメールへの対応を自動化することができます。このような「インシデント対応の効率化」はセキュリティ担当者の負担を即座に軽減するため、メリットとして実感していただきやすいポイントです。また、セキュリティ対策の一環としてそれ以上の潜在価値も秘めています。適切な戦略とプランニングがあれば、フィッシング脅威に対抗するべくオーケストレーションされたインテリジェントなSOCを構築することができます。

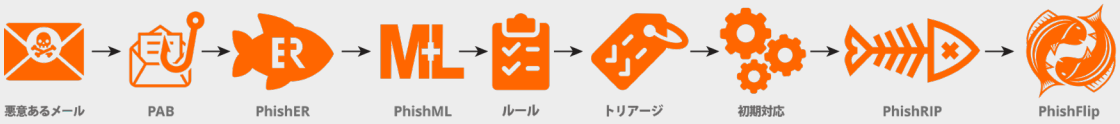
PhishERは、IRチームが協力してフィッシングの脅威を軽減するための重要な基盤づくりに最適です。悪意のある可能性のあるメッセージを自動的に優先順位付けして管理したい、とお考えのあらゆる組織に適しています。PhishERは、スタンドアロン製品、またはKnowBe4のお客様向けのアドオンオプションとして提供が可能です。

PhishERが選ばれる理由

PhishERは使いやすいWebベースのプラットフォームで、フィッシングER（Emergency Room：緊急対策室）としての重要な機能を備えています。PhishERは、届いたメールが正当なメッセージかどうかを優先順位付きで迅速に分析します。

つまり、PhishERを活用すれば、大量のメールに優先順位をつけ、分析し、すばやく管理することができるのです。PhishERが目指すのは、システムが推奨する着眼点を確認し、希望するアクションを取る機会を設けながら、お客様とチームができるだけ多くのメッセージに自動的に優先順位を付けられるようにすることです。

PhishERの仕組み



PhishERは、ユーザー（従業員）から報告されたフィッシングメールやその他の不審なメールを、ルール、タグ、アクションに基づいてグループ化、カテゴリー化して処理します。カスタム機械学習モジュールであるPhishMLがメッセージを分析し、信頼できる値を生成してメッセージへのタグ付けに使用します。次に、PhishRIPによって、全社・全組織内のメールボックスに削除されずに存在している不審なメールを迅速に見つけ出し隔離します。さらに、 PhishFlipは危険なフィッシング攻撃を無害化し、演習用のテンプレートへ変換して、即時に全社レベルでフィッシングメール演習ができるようにします。

自動メッセージ優先順位付け

PhishERは、従業員から報告されたメッセージをClean（正常）、Spam（スパム）、Threat（脅威）の3つのカテゴリーに分類します。YARAルールで重要な内容を割り当てておけば、PhishERを使用して大量のメッセージに自動的に優先順位を付けることができるため、手動の作業を効率的に削減できます。

また、報告されたメッセージの属性を確認し、優先順位に基づいて最も重要なメッセージをランク付けすることにより、チームが最も危険な脅威に迅速に対応できるようにサポートします。

ER（Emergency Room：緊急対策室）

「ER：緊急対策室」は、ユーザーから報告された内容と類似したメッセージを識別するための機能です。PhishERは、これらのメッセージを共通項によってグループ化し、Top Subject Lines（上位件名）、Top Senders（上位送信者）、Top Attachments（上位添付ファイル）、Top URLs（上位URL）といった具合にメッセージを事前フィルタリングして表示します。

各緊急対策室はインタラクティブ仕様で、フィルタリングされたメッセージの受信ボックスビューにドリルダウンし、関連するすべてのメッセージに対するアクションを起こすことができます。

インテグレーション

PhishERはAPIインテグレーションや複数のsyslog送信先もサポートしています。これらの機能を通じてPhishERを既存のセキュリティスタック製品と連携させ、一般的なメールセキュリティ、脅威インテリジェンス、チケット管理、SIEMプラットフォームにデータを送信することができます。さらに、PhishERからイベントを送信し、KnowBe4プラットフォーム内のユーザーのタイムラインに追加することも可能です。これらのイベントを利用して独自のフィッシングやトレーニングキャンペーンを作成し、ユーザーがPhish Alert Buttonから疑わしいメールをよりよく識別して報告できるようにすることができます。

また、PhishERをVirusTotalなどの外部サービスと統合すれば、添付ファイルや悪意のあるドメインの解析に役立ちます。

Microsoft 365ブロックリスト

PhishER Blocklist（PhishERブロックリスト）機能を使用すれば、PhishERコンソールを離れることなく、組織独自のブロックリストエントリーのリストを簡単に作成し、Microsoft 365のメールフィルターの効果を劇的に改善することができます。

報告されたメッセージを利用して、同じ送信者、URL、添付ファイルを含む悪意のあるメールが今後他のユーザーに届くのを防ぐことができます。

PhishML™

PhishMLはPhishERの機械学習モジュールです。メッセージの優先順位付けプロセスの最初に、ユーザーから報告される疑わしいメッセージを特定し、評価します。また、PhishERプラットフォームに入ってくるすべてのメッセージを分析し、優先順位付けのプロセスをより簡単、迅速、かつ正確にするための情報を提供します。

PhishMLは、担当者や、PhishERユーザーコミュニティの他のメンバーによってタグ付けされたメッセージに基づき、常に学習しています。精度の向上をはかるために、学習モデルには常に新しいデータが供給されています。より多くのメッセージをPhishERの分類に基づいて自動的に優先順位付けすることができるため、結果としてユーザーの負担軽減につながります。

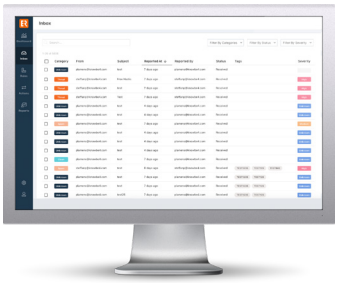
PhishRIP™

PhishRIPはMicrosoft 365やGoogle Workspaceと連携したメール検疫機能です。これによりインシデント対応チームは迅速かつ容易に問題に対処することができます。

PhishRIPがあれば、特定された脅威をすべてのユーザーのメールボックスから削除し、報告されていない脅威を予防することができます。また、データの削除、隔離、また正当なメールの復元など、将来的な脅威からユーザーを保護するための機能が豊富に揃っています。

PhishFlip™

ユーザーから報告されたフィッシング攻撃を、KnowBe4プラットフォーム上で自動的に安全なフィッシングキャンペーンのシミュレーションに変換します。PhishFlipを使うことで、今発生している個人宛の危険な攻撃を無害化し、逆に社内でのメール演習としてタイムリーに使用することができます。



詳しくは以下をご覧ください:
www.KnowBe4.jp