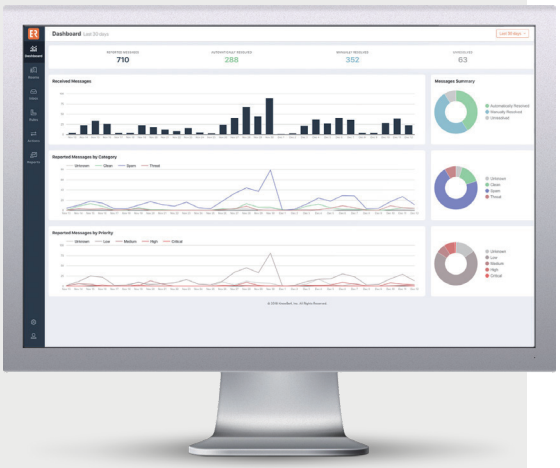
PhishER

フィッシングER（Emergency Room：緊急対策室）

KnowBe4
Human error. Conquered.



主な利点と特徴

- KnowBe4 の Phish Alert ボタン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、脅威でないメールを自動的に分類する。
- セキュリティ担当者の受信ボックス内のノイズをカットし、最も危険な脅威への対応を迅速化・効率化する。
- セキュリティ担当者の負担を軽減し、脅威ではないと分類されたメールの 90%の対応を自動化する。
- メールメッセージをパターンに基づいて分析・分類し、自社の組織内で拡散するフィッシング攻撃をいち早く特定し、防御する。
- 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）する。
- 自動化されたメール応答テンプレートによって、さらなる処置が必要とされるメールについて迅速に報告者へフィードバックする。
- 優先順位付け（トリアージ）や警告などの作業のための独自のワークフローを作成することができ、セキュリティ担当者の作業負荷を軽減する。
- PhishFlip™は PhishER 機能の 1 つで、今発生している実際のフィッシングメールをフィッシングメール演習用にテンプレート化して、即時に全社レベルの演習を可能にする。

PhishER：メール脅威を迅速に特定し、素早く対応する

フィッシング攻撃がサイバー攻撃手段として最も広範に使用されている中、多くのスパムメールや "疑わしい" メールが企業や組織・団体へ向けて発信されています。セキュリティトレーニングを組織内に展開しているか否かにかかわらず、日々多くの不審メールを従業員が受信して、何らかの形態でセキュリティ担当者へ既に報告していることは不変の事実です。**この不審メールトラフィックの増加は、セキュリティ担当者にとっての新たな問題を発生させています。**

現在、企業ネットワークを標的とするスパムメールや悪意あるメールの約 7-10% は、メールフィルターをすり抜けてします。従業員が報告する 10 件のメールのうちで、実際には、悪意あるメールは 1 件ほどしかありません。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？

PhishER とは何か？

PhishERは軽量な SOAR（Security Orchestration Automation & Response）プラットフォームです。脅威への対応を自動化し、セキュリティ担当へ報告される大量の不審メールの迅速な対応を可能にします。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の受信ボックス内のノイズをカットし、最も危険な脅威への対応を迅速化・効率化することを可能にします。

PhishER を使用することで、報告されたメールの 90% にあたる “脅威ではないメール” への対応を自動化することができ、インシデント対応の効率化というメリットを即座にセキュリティ担当者へもたらします。さらに、インシデントレスポンス（IR）オーケストレーションの潜在的な価値は、それよりはるかに大きいものです。例えば、適切な戦略とプランニングによって、フィッシング脅威に対抗するためのオーケストレーションを実現するインテリジェントな SOC を構築することを可能にします。

PhishER は、フィッシングの脅威を軽減するためにインシデントレスポンスチームが連携する上での重要な構成要素です。いかなる組織においても、悪意のあるメールを自動的に優先順位付けして迅速に対応するために最適です。PhishER は、スタンドアロン製品として、または、KnowBe4 の年間サブスクリプション契約のアドオンオプションとしてご利用いただけます。

なぜ PhishER を選択するか？

PhishER は使い易い 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。疑わしいメールとして報告されたメールメッセージへの初動対応をサポートします。PhishER は、どのメッセージが正当で、どのメッセージが正当でないのかを優先順位付けして分析します。このトリアージプロセスによって、インシデントレスポンス（IR）チームは大量のメールメッセージの優先順位付け・分析・管理を迅速に行えるようになります。PhishER が目指すところは、セキュリティ担当者の初動対応を支援し、より多くのメールメッセージに出来る限り自動的に対応し、適切な初動対応を取ることを可能にすることです。

いかにPhishERが機能するか

PhishERは、ルール、タグおよびアクションに基づいてグループ化・カテゴリー化することで、従業員からPhish Alertボタン（PAB）によって報告されたフィッシングメールや不審なメールを優先順位付けして、対応します。メッセージの優先順位付け（トリアージ）プロセスの最初のステップで、PhishERの機械学習モジュールであるPhishMLが、報告された疑わしいメッセージの重大度をタグ付けして、分類します。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付け出し、検疫・隔離することができます。さらに、PhishFlipは、今、社内で発生している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、即時に全社レベルのフィッシングメール演習を可能にします。

自動メッセージ優先順位付け（トリアージ）

PhishER は、従業員から報告されたメッセージを次の 3 つのカテゴリー（Clean（正常）、Spam（スパム）、Threat（脅威））の 1 つに分類して、優先順位を付けます。設定ルールに従って、最適なトリアージプロセスを開発することを支援します。これによって、人の介入なしに、出来る限り多くのメールメッセージを自動的に優先順位付け（トリアージ）することを可能にします。

脅威でないメールの自動優先順位付けによって、インシデントレスポンス（IR）チームは、最も危険な脅威により迅速に対応することが可能になります。また、PhishER は、KnowBe4 のメールアドインボタンの Phish Alert と統合することができ、Phish Alert ボタンで報告されたメールを専用のメールボックスへ転送します。

ER（Emergency Room：緊急対策室）

PhishER には、ER（Emergency Room：緊急対策室）という機能があり、報告された同様なメッセージを特定し分類することができます。この機能には事前フィルタリングされたビューが含まれており、各自の PhishER 受信ボックス内で未対応であるメッセージを仕分けます。これらのメッセージは共通性によって動的にグループ化され、Top Subject Line（上位主題）、Top Sender（上位発信者）、Top Attachment（上位添付）および Top URL（上位 URL）別に事前フィルタリングされたメッセージのシステムビューに含められます。

各 ER はインタラクティブに機能し、メッセージのフィルタリングされた受信ボックスビューをドリルダウンすることが可能です。また、すべての関連メッセージを横断して同時にアクションを取ることができます。

SIEM インテグレーション

PhishER は、Splunk や QRadar などの SIEM プラットフォームとのプッシュ型でデータ連携することで、自社の組織への統合を実現しています。複数の syslog デスティネーションがサポートされており、さまざまなユーザー要件に対応し、その他のシステムとのデータ連携も可能にしています。

PhishML™ (Machine Learning モジュール)

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（トリアージ）プロセスにおいて、報告された疑わしいメッセージを特定して評価します。PhishER プラットフォームへ入ってくるすべてのメッセージを分析し、トリアージプロセスがより容易に、より高速に、より正確になるようにサポートします。

PhishML は、トレーニングの受講者によって、または 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いて常に学習します。これによって、PhishML は新しいデータを常時フィードし、正確性を高めています。さらに、より多くのメッセージが PhishER のカテゴリー化に基づいて自動的に優先順位付けされることで、不審メールを見極めるためのユーザーの負担が軽減されます。

簡単かつ高度なルール生成

独自ルールを生成することができます。これに加えて、ビルトインの YARA ベースのルールを使用することも、既存の YARA ルールを編集して使うこともできます。また、ルール要件を簡素化するためにシステムルールを使うこともできますが、自社のインシデントレスポンスチームのスキルに応じて、ルールをカスタマイズするためにシステムルールをコピーして変更することもできます。

データエンリッチ化インテリジェンス

PhishER は、添付や悪意あるドメインを解析するために VirusTotal のような外部サービスと統合することもできます。URL Unwinding を使って、PhishER は短縮 URL を自動的に拡張します。これによって、最終デスティネーションの潜在的な脅威レベルを確認することが可能になります。

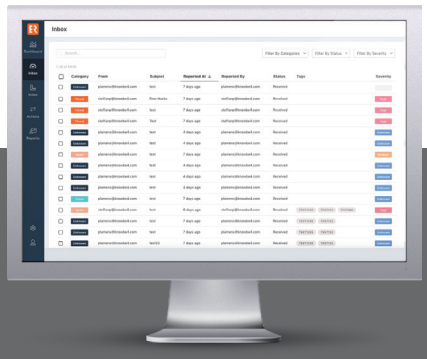
PhishRIP™

PhishRIP は、メール検疫・隔離機能です。Microsoft 365 および G Suite にインテグレーションされ、メールの脅威を監視・検出し、報告、隔離、分析することで、アクティブなフィッシング攻撃を迅速にシャットダウンします。PhishRIP は、PhishER 内のユーザー報告のメールメッセージを監視し、脅威となるメールメッセージを検出します。PhishRIP は全企業または全組織内のすべてのエンドユーザーの受信トレイをサーチし、検出された脅威メールと類似または同一の脅威メールが受信されていないかを見付け出します。結果、PhishRIP が検出した要注意のメールは、インシデントレスポンスチームによって迅速に分析できるようになり、適時にエンドユーザーの受信トレイから隔離または完全に削除されるようになります。

PhishFlip™

PhishFlip は、今、発生している実際のフィッシングメールをフィッシングメール演習用にテンプレート化して、即時に全社レベルの演習を可能にします。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て、即座に全社レベルで情報共有することを可能にし、タイムリーなメール演習を実現することができます。PhishFlip は、Phish Alert ボタン (PAB) によって現場の従業員から IT 管理者へ報告されたフィッシング攻撃の脅威を適用し、フィッシングメール演習へ展開します。

PhishFlip は、PhishRIP によって検疫・隔離された、実際に発生している個人宛のフィッシング攻撃を無害化し、演習テンプレートへ変換し、現実そのもののフィッシング攻撃を再現します。次に、PhishRIP が他の従業員に同一の危険なフィッシングメールが届いていないかを特定し、同一のフィッシングメールが存在する場合は、PhishFlip がこれを安全なテンプレート化された演習メールに置き換えて、メール演習を実施することを可能にします。PhishFlip によって、実際に発生している危険なフィッシング脅威を全社レベルで即時に対処する実践的な演習を手に入れることができます。



詳細はここから：

www.KnowBe4.com / www.KnowBe4.jp

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社 〒100-6510 東京都千代田区丸の内1-5-1 新丸の内ビルディング10F EGG 内
www.KnowBe4.com / www.KnowBe4.jp | お問い合わせ：Info@knowbe4.jp

2022年10月発行