knowbe4

PhishER Plus

主なメリット

- 脅威を自動的に分類
- 報告に対して即時にフィードバックを提供
- すべてのメールボックスでワンクリックによる対処を可能に
- 専門家による検証、1,300万人以上のグローバルユーザーから得られる脅威のインテリジェンス、そして主要セキュリティプラットフォームとの連携に基づいてメールを分析・分類

自動インシデントレスポンスでAI起因のフィッシングを軽減し、SOC効率を底上げ

PhishER Plusは、慢性的なバックログやリソースの非効率性に悩むセキュリティチーム向けに設計された自動インシデント対応SOARプラットフォームです。

世界最高水準の包括的な脅威インテリジェンスデータベースを利用し、脅威を即座に優先順位付けして封じ込めます。これは、15年にわたる人間の行動データとKnowBe4のThreat Research Labで訓練された当社のAIインサイトと、統合されたサードパーティの脅威フィードを組み合わせたものです。アナリストに包括的なビューを提供し、リスクを評価。すべての受信トレイにわたって迅速な対応が可能です。

従業員のミスによる情報漏洩のリスクを低減

PhishER Plusは、3つの検証プロセスを経た脅威インテリジェンスから生成される「グローバルPhishRIP」および「グローバルブロックリスト」を活用した自動封じ込め機能を、技術スタックにおける重要なセキュリティ層として提供し、ゼロデイ脅威を防止します。これにより、全従業員の受信トレイから脅威を同時に除去できるため、封じ込めまでの時間を数時間から数分に短縮し、攻撃の潜在的な影響を大幅に抑制します。

報告されたメールの分析にSOCチームが週に費やす時間を短縮

PhishER Plusは、エンドユーザーの受信トレイからの危険メールの自動削除、KnowBe4 Threat Research Labの脅威メールインテリジェンス、業界をリードするサードパーティの連携により、メール分析と対処を加速します。導入企業様では平均して導入初年度に360%以上のROIを達成し、手動でのメール確認時間を最大99%削減しています。

従業員のセキュリティ意識向上活動における成果と改善点を可視化

PhishER PlusはKnowBe4セキュリティ意識向上トレーニング（SAT）およびフィッシングシミュレーションと連携し、管理者はどの従業者がメールを報告したか、またPhishFlip経由でシミュレーション化されたフィッシング攻撃の被害者となったかを把握できます。さらに、PhishER Plusのアクションとタグを設定すれば、正常なメールとスパムメールを素早く識別でき、SOCの対応を必要とせずに報告者に追跡可能な学習機会を提供できます。メッセージにタグが割り当てられると、そのタグはPhishER Plus内でのメッセージの処理方法を示します。メッセージにタグが付けられると、アクションによってPhishER Plusがメッセージに対して行う処理が決定されます。

主な機能

3つの検証プロセスを経た脅威インテリジェンス

- **集合知型防御ネットワーク：** 世界で1,300万人以上のユーザーが毎日新たな脅威を報告。他に類を見ない脅威インテリジェンスネットワークを活用
- **独自開発のAIインサイト：** 15年間の人間の行動データで訓練されたAIを活用し、高度なゼロデイ攻撃対策を提供
- **専門家による検証：** KnowBe4 Threat Research Labの業界専門知識とリアルタイム分析を統合
- **サードパーティインテグレーション：** CrowdStrike Falcon Sandbox、VirusTotal、Threat Intel Powered by Webrootを含む、統合されたサードパーティ脅威フィードと内部データを統合

自動化されたインシデント対応と封じ込め

- **グローバルPhishRIP：** ユーザーコミュニティから収集された脅威情報に基づき、配信後の悪意あるメールを全従業員の受信トレイから同時に自動削除
- **Microsoft 365 グローバルブロックリスト：** 既知の脅威がMicrosoft 365環境に入る前にブロックし、自動封じ込めを即座に実行
- **PhishML AI分類：** 報告されたメールの最大90%を「安全」「スパム」「脅威」に自動分類し、問題のないメッセージの手動確認を不要に
- **ワンクリックで対処：** アナリストが単一の統合ビューから迅速にアクションを実行し、すべての受信トレイにおいて脅威の封じ込めを可能に

SOCの効率と可視性

- **高精度の自動化：** アナリストが、組織の許容レベルに基づいてPhishML自動化の閾値をカスタマイズして設定可能
- **PhishMLインサイト：** AIがメッセージの判定を決定する詳細な説明を提供し、AIの意思決定プロセスを可視化
- **リアルタイムのフィードバック：** Phish Alert Button（PAB）を使って不審なメールを報告したエンドユーザーに対し、自動的かつ即時的なフィードバックと詳細情報を提供
- **詳細なレポート・分析：** セキュリティ上の意思決定とROIを包括的に可視化し、どの脅威が阻止されたかを明確に示します

従業員のエンゲージメントとトレーニング

- **PhishFlip：** 受信トレイで特定された実際のフィッシング攻撃を無害なトレーニングシミュレーションに変換し、被害に遭った可能性のあるユーザーを特定
- **セキュリティ行動の強化：** エンドユーザーに警戒を継続させる人間とAIが連携したモデルを採用し、報告プロセスを通じて積極的なセキュリティ行動を促進

さらに詳しく

knowbe4.com/ja/products/phisher-plus

KnowBe4 Japan合同会社 | 〒107-0052 東京都港区赤坂 9−7−1 ミッドタウン・タワー 18F | 03-4586-4540
www.knowbe4.com/ja | info@KnowBe4.jp

CR0541-0226