KnowBe4
Human error. Conquered.

SOAR プラットフォーム選びに欠かない8つの機能

フィッシング攻撃に対する防御の強化を考える企業や組織は、常にセキュリティ意識の向上を最優先しなければなりません。しかし、サイバー犯罪者の手口が年々巧妙になる中で、強固で包括的なフィッシング攻撃への防御戦略の必要性が非常に高まってきています。セキュリティオペレーションセンター（SOC）やインシデントレスポンス（IR）チームでは、フィッシング攻撃が被害を与える前に攻撃を迅速に調査し、終了させることができるツールの導入が不可欠です。

これを受けて、フィッシング攻撃に対抗する強力なツール「SOAR（Security, Orchestration, Automation and Response）」が登場し、テクノロジーと人間の専門知識を組み合わせた総合的なアプローチを提供しています。フィッシング攻撃や標的型スピアフィッシングキャンペーンなど、拡大する脅威への対策を考えるITセキュリティ担当者にとって、フィッシング対策は今や重要な要素となっています。

しかし、すべてのSOAR製品が同じように作られているわけではありません。まず優れたSOAR製品は、悪意あるメールの分析と優先順位付けを自動で行う機能を備え、リスクの高いフィッシング脅威の推測による特定を排除するものであるべきです。さらに、ここ数年で強力な機能が追加され、SOAR製品は受け身の分析および識別からよりプロアクティブにフィッシング攻撃を軽減できるツールへと進化しています。こうした機能や進化を理解することは、市場を見極める上で重要です。

本ホワイトペーパーでは、フィッシング対策にSOAR製品を選ぶ際に優先すべき8つの機能について解説します。

#1 エンドユーザーのエンパワーメント

フィッシング攻撃やソーシャルエンジニアリングの脅威に対する企業や組織の防御の要は、エンドユーザーです。エンドユーザーを起点とするサイバー脅威の特定・報告は、企業や組織がフィッシング攻撃から身を守り、そのリスクを低減する上での基盤となります。これを実現するため、優れたSOAR製品はエンドユーザーのエンパワーメント（自発的行動）を促す機能を備えていなければなりません。

まず1つは、エンドユーザーが不審なメールを簡単に報告できる機能です。企業や組織のメールクライアントに組み込まれたPhish Alertボタンにより、ユーザーは疑わしいメールを指定のIT受信トレイまたはSOARプラットフォームに直接報告できるようにする必要があります。

2つ目は、テンプレートと自動返信メール機能です。これを活用して、従業員が情報セキュリティーチームに報告したメールについて、そのメールがスパムメールなのか、それとも全体の90%にあたる「脅威ではないメール」なのかどうかをSOAR製品が迅速に確認し、従業員に伝えます。

#2 機械学習とAI

人工知能（AI）と自動化を活用したSOARプラットフォームは、強力なフィッシング対策を可能にします。人員の足りないIRチームやSOCチームが対応できない場合でも、AIと自動化機能でフィッシング攻撃の脅威の特定と優先順位付けをより簡単、迅速、正確に行います。

AIと自動機能がスケーラビリティ、正確性、プロアクティブな軽減策を提供し、次のタスクの達成と劇的なスピードアップを可能にします。

- メールの自動分析と優先順位付けにより、ユーザーから報告されるすべてのメッセージからリスクの高いフィッシングの脅威を推定・特定する作業を削減

- セキュリティワークストリームを自動化し、ユーザーから報告されるメールの「その他の90%」を管理
- T部門と従業員との迅速なコミュニケーションを可能にする自動メール応答
- 機械学習によるパターン認識に基づいて、メッセージをグループ化またはクラスタ化し、インシデント対応チームが広範なフィッシング攻撃を特定
- 自動ブロックリスト、クラウドソーシングによる脅威インテリジェンス、プロアクティブなフィッシング対策
- 実際のフィッシング攻撃をシミュレートしたフィッシングテンプレート

#3 自動脅威分析と優先順位付け

IRチームやSOCチームの多くは、今だに不審なメールのトリアージを手作業で行っています。フィッシングメールを手作業でトリアージするのにかかる時間は平均で27分です。対応時間が適切でないと、フィッシング攻撃によるリスクと被害の増大につながる可能性があります。

企業・組織を効果的に保護し、セキュリティチームを健全に保つために、機械学習を活用したメールの分析と優先順位付けを行うSOAR製品を導入することをおすすめします。これにより、ユーザーから報告される大量のメールから、リスクの高いフィッシング攻撃の脅威を推測によって特定する作業をなくすことができます。

機械学習を活用し、報告されたメールに人の手を介さず自動的に優先順位をつけることができる製品を検討すると良いでしょう。たとえば、メールをClean（正常）、Spam（スパム）、Threat（脅威）のカテゴリーに分類し、件名、送信者、受信者、添付ファイル、本文などのメール属性を分析することによって、疑わしいメールを優先順位に基づいてランク付けできる機能は備えているべきです。

他の優れた機械学習プラットフォームと同様に、学習も不可欠です。エンドユーザーから報告された不審なメール、SOCチームからのデータ、サードパーティの脅威インテリジェンスフィードによって検証された脅威情報などの新しいデータがシステムに入力されると、精度は継続的に向上し、さらに多くのメールをより正確に自動的に優先順位付けできるようになります。

メールの分析と優先順位付けは、優れたSOAR製品の基本であり、より簡単、より迅速、より正確なメールの優先順位付けへとつながります。

1　フィッシングのビジネスコスト、2022年版レポート

#4 隔離と除去

フィッシング脅威を特定したら、類似するフィッシングメールを隔離し、すべてのユーザーの受信トレイから削除する機能が最も重要です。この機能は、国家による脅威行為や標的型スピアフィッシング攻撃に対して、フィッシング攻撃を大規模に軽減するためには必要不可欠です。

このメール検疫機能は、Microsoft 365やGoogle Workspaceなどのサードパーティのメールサービスに直接統合できるほか、以下のタスクに対応できるものをおすすめします。

- **削除**
  脅威が特定されたら、SOCチームが受信トレイ、送信済み、ゴミ箱など、すべてのメールフォルダから同一または類似のメッセージを削除できるオプションが必要です。
- **予防**
  すべてのエンドユーザーが不審なメールを報告するわけではありません。そのため、報告されていないメールを監視して検出した上で、これを報告・隔離し、最終的な分析ができるようにします。
- **保護**
  次の攻撃を阻止するためには、事後分析が不可欠です。差し迫った脅威が緩和された後、影響を受けたユーザーへのフォローアップの送信、ユーザーのメールボックスからのメッセージを削除・隔離、正当と確認されたメッセージの復元などの機能は、製品を評価する際に重要な機能のチェックリストに入れるべきものです。

#5 ブロックリスト

ブロックリストは、悪意のあるメールがユーザーの受信トレイに届くのを防ぐための、最も基本的でプロアクティブなアプローチです。Microsoft 365やGoogleのようなメールサービスは基本的なブロックリスト機能を提供していますが、AIが作成したフィッシングメールの数々を阻止するには十分とは言えません。

検討するSOAR製品は、エンドユーザーからのフィードバックと機械学習ベースのメール分析に基づく優れたブロックリスト機能を提供し、企業や組織が利用するメールフィルターを強化するものでなければなりません。

また、送信者、URL、添付ファイル、ファイルハッシュなど、さまざまな属性や値に基づいてメールをブロックする機能をIRチームやSOCチームに提供する必要があります。さらに、サードパーティのメールサービスにある機能を上回る、より強固な条件ベースのルール作成機能も必要です。

最後に、そしておそらく最も重要なことですが、脅威の状況を先取りし、フィッシング攻撃が企業・組織を襲う前に未然に防ぐためには、エンタープライズグレードのSOAR製品がAIとクラウドソーシングの脅威インテリジェンスの力を活用することで、ブロックリストをもう一段上のレベルに引き上げる必要があります。
その理由を以下の#6でご説明します。

#6 クラウドソーシングによる脅威インテリジェンスとプロアクティブなフィッシング対策

どんなに規模が大きく、十分なリソースを持つSOCやIRチームであっても、フィッシングやソーシャルエンジニアリングの脅威の状況を先取りすることは不可能だと言えます。脅威は非常に多様で、進化を続けており、ますます巧妙になっています。AIによって、サイバー犯罪者は従来のメールセキュリティフィルターを回避できる新しいフィッシングメールを作成できるようになりました。

だからこそ、フィッシング対策においては積極性が重要なのです。導入するSOARプラットフォームは、リアルタイムの脅威インテリジェンスデータをシームレスに統合し、警戒監視の役割を果たす必要があります。これによって、新たな脅威に関する最新の洞察がすぐに得られるようになり、迅速な適応と対策が可能になります。

組織・企業が脅威インテリジェンスのハブとしてサイバーセキュリティベンダーをますます頼りにするようになっているのは、このためです。SOARベンダーは、クラウドソーシングによる脅威インテリジェンスとAIを活用したブロックリストを提供し、何百万ものエンドユーザーがすでに報告した、検証済みの実際のフィッシング脅威に基づいて、ユーザーの受信トレイからフィッシング脅威を自動的に隔離・削除する必要があります。

クラウドソース脅威インテリジェンスは、他のすべてのフィルターを通過した脅威を検出します。これにより、セキュアなメールゲートウェイをすり抜け、ユーザーの受信トレイに侵入する悪意のあるメールにも追加の保護レイヤーを提供します。

ArmorBloxによると、2022年には、メールベースの攻撃の56%が従来のセキュリティフィルターをすり向けており、フィッシングメールの18.8%がMicrosoft Exchange Online ProtectionおよびDefenderをすり抜けてユーザーの受信トレイに到達したと、Check PointのEメール調査チームが報告しています[1]。

#7 カスタマイズ可能なワークフロー

フィッシングの分析と被害軽減は、1つのモデルですべて解決できるものではありません。ワークフローやプロセスは企業や組織によって異なります。企業・組織独自のニーズに合わせて自動化ワークフローを成形できる柔軟性を備えたSOARプラットフォームを選択することが重要です。不審なメールの分析、インシデントの分類、事前定義されたレスポンスの開始など、カスタマイズが重要な鍵となります。

---

2 Check Point Microsoft Defender レポート

#8 フィッシング攻撃をトレーニングに変換

多くの組織では、実際の脅威とよく似たフィッシングメールの識別と報告について、ユーザーをテストしたいと考えています。SOAR製品であれば、悪意のあるフィッシングメールを「変換」させる機能を提供することで、ユーザーにとって実際のトレーニングの機会とすることができます。この機能は、既存のセキュリティ意識向上トレーニングプログラムの強化にも役立ちます。

報告・削除されたメールの脅威を「無害化」し、ユーザーに対して模擬フィッシング攻撃を自動的に開始します。ユーザーの受信トレイに届いた未開封の本物のフィッシングメールを無害なものに変えることで、結果的にユーザーが現実の脅威に対し一層警戒を強めることにつながります。

まとめ

企業や組織を継続して運営していくためには、フィッシング攻撃に対する包括的な戦略が必要です。オーケストレーション、自動化、返信機能を備えたSOARツールは、強力な防御策を提供します。

フィッシング対策SOAR製品の市場は、軽減を目的とされるソーシャルエンジニアリングの脅威と同様、多様化しています。最終的には、導入するSOAR製品は対応にかかる時間を適切に短縮し、ユーザーがフィッシング脅威を受信する前にフィッシングの脅威を軽減し、企業や組織のメールセキュリティ防御を強化することができるものでなければなりません。またITチームの負担を、AIによる自動化とクラウドソーシングによる脅威インテリジェンスにシフトすることで、セキュリティチームがオーケストレーションと分析に集中できるようにすると同時に、フィッシングが企業や組織にもたらすリスクを軽減することができます。

KNOWBE4 PHISHER PLUS

PhishER Plusは、フィッシング脅威への対応を指揮し、企業や組織のメールセキュリティ防御を強化するために設計された軽量なSOAR製品です。強力な機械学習によるEメール分析、優先順位付け、ブロックリスト機能を、業界で最も強力なグローバル脅威フィードと組み合わせることで、プロアクティブなフィッシング対策を実現します。

またPhishER Plusは、3段階の検証ステップを持つグローバル脅威フィードを搭載しており、ユーザーの受信トレイに届く前に自動的にブロックします。このグローバル脅威フィードには次の3つの重要なコンポーネントがあります。

1. 高度なトレーニングを受けた1,000万人を超える以上のKnowBe4エンドユーザーとPhishER管理者で構成されるKnowBe4のグローバルユーザーグループネットワーク
2. 他者のフィルターをすり抜けたフィッシングメールを学習する独自のAIモデル「PhishML」
3. KnowBe4のThreat Research Labが提供する、人の手によって収集・蓄積された脅威インテリジェンス

KnowBe4のPhishER Plusでフィッシングの脅威を特定し、迅速に対応しましょう。

さらに詳しく

KnowBe4のPhishER Plusのデモをリクエストしていただけます。

デモをリクエスト

その他のリソース

無料のフィッシングセキュリティテスト
フィッシング攻撃の被害に遭いやすい従業員の割合を、無料のフィッシングセキュリティテストで確認できます。

無料の自動セキュリティ意識向上プログラム
自社組織に合わせてセキュリティ意識向上トレーニングプログラムをカスタマイズできます。

無料のPhish Alertボタン
ワンクリックでフィッシング攻撃を報告できる安全な方法を従業員に提供します。

無料のメールエクスポージャチェック
攻撃者より先に、流出したメールを特定できます。

無料のドメインなりすましテスト
組織のドメインを使うメールアドレスがスプーフィング攻撃を受けていないかを確認できます。

KnowBe4について

KnowBe4は、セキュリティ意識向上トレーニングおよびフィッシングシミュレーションの世界最大の統合プラットフォームのプロバイダーです。

KnowBe4は、セキュリティの人的要素が著しく軽視されていることを認識し、包括的な新しい形態のセキュリティ意識向上トレーニングプログラム（当社では「New School」と呼んでいます）を通じて、企業や組織がソーシャルエンジニアリングの問題を管理できるようにするために設立されました。

これは、本番さながらの偽装攻撃によるベースラインテスト、学習意欲を高めるインタラクティブなトレーニング、模擬フィッシング攻撃を通した継続的なアセスメント、およびエンタープライズクラスの最強のレポーティングを組み合わせた統合型のアプローチです。

金融、医療・介護、エネルギー、官公庁、保険業など規制の厳しい分野を含むあらゆる業界で、多くの企業や団体がKnowBe4のプラットフォームを採用し、エンドユーザーを最後の防衛ラインとして動員することでよりスマートなセキュリティ上の意思決定を可能にしています。

詳細については、www.KnowBe4.jpを参照してください。

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
電話：03-4586-4540 | www.KnowBe4.jp/www.KnowBe4.com | Email:Info@knowbe4.jp

05D09K01