

Proofpoint Threat Response Auto-Pull

悪意のあるメールを 配信後でも自動的に隔離

主なメリット

- 境界型セキュリティソリューションを回避した悪意のあるメールを自動的に隔離
- セキュリティ及びメール管理チームがメールセキュリティの運用と対応にかける作業時間を大幅に短縮
- Proofpoint Threat Intelligence をメールの分類に活用
- abuse メールボックスを自動監視
- 個人や配信リストに転送されたメールを隔離
- 報告が不完全でもフィッシングキャンペーンを追跡し、誤って報告されたメールによる時間の無駄を削減

90%以上の侵害は、最大の攻撃経路であるメールから始まります。メールを介した脅威は進化を続けており、より悪質なメールが増えています。悪意のあるメールには、配信後に有害となるフィッシングリンクを含むもの、または検出を回避するテクニックを使ったものなどがあります。メールセキュリティチームは、リスクと被害を緩和するために適宜メールの分析やクリーンアップをしなければなりません。メール1通だけであれば、隔離はそれほど大変な作業ではなく、10-15分くらいしかかかりませんが、10通以上になれば手間も時間もかかります。

悪意のあるメールを自動的に隔離

Proofpoint Threat Response Auto-Pull (TRAP) を用いれば、メール及びセキュリティ管理チームはメールインシデントへの対応プロセスを効率化することができます。悪意のあるメールが検出されると、TRAPはメールを分析して悪意のあるメールを自動的に除去します。また、ユーザーの受信箱に届いてしまった後でも、不要なメールを隔離できます。TRAPを使えば、メール及びセキュリティ管理チームのメールクリーンアップ作業時間を大幅に短縮できます。

法人向けの脅威インテリジェンスを活用

Proofpoint Threat Intelligence は、メール、ソーシャル、モバイル、クラウド、及びネットワークなど多くの攻撃経路を網羅しており、攻撃者が現在使用している最新の脅威と手法を可視化します。TRAPでは、Proofpoint Threat Intelligenceだけでなく、STIX/TAXII フィード、WHOIS、VirusTotal、Soltra、及びMaxMindなどのサードパーティの脅威インテリジェンスも活用します。これらによって「誰が、何を、どこで」攻撃したかを理解でき、イベントを迅速に選別して優先順位付けでき、また単純な繰り返し作業を減らせます。

メールを検出した後は、上記のインテリジェンスを使って対処します。受信者とユーザーIDを関連付けし、関係するキャンペーンを判別し、攻撃に使用されたIPアドレス及びドメインを明らかにします。これにより、非常に精度の高い分類が可能になります。そして検出されたメールをひとつずつ手作業で調査する必要がなくなり、セキュリティチームは他のタスクに集中できるようになります。

CLEAR によるフィッシングリスクの識別と削減

正しい知識を持ったユーザーは、サイバー攻撃に対する最後の砦になります。Closed-Loop Email Analysis and Response (CLEAR) では、攻撃メールの可能性のあるメールのレポート、分析、修正のサイクルが、数日ではなく数分でできるようになります。Proofpoint Threat Intelligence で強化された CLEAR は、ワンクリックで攻撃を阻止し、また、悪意あるメールを自動的に隔離しますから、セキュリティチームは手間と時間を削減できます。

CLEAR は包括的なソリューションです。CLEAR には、PhishAlarm (メール報告ボタン)、PhishAlarm Analyzer (Proofpoint Threat Intelligence を活用した脅威の分類及び優先順位付け)、TRAP (悪意のあるメールの分析及び自動修復) の機能が含まれています。

報告されたメールは CLEAR を活用するため abuse メールボックスに送られ、TRAP と同じ方法でメールの監視と処理が行われます。さらに Proofpoint Threat Intelligence とサードパーティのインテリジェンスを用いてより詳細に分析され、そのコンテンツが悪意あるコンテンツのマーカーに一致するかどうか確認されます。そしてメールは受信箱から自動的に排除されます。

アウトオブバンドのメール管理

TRAP は CSV ファイルと Proofpoint SmartSearch も活用します。ユーザーは SmartSearch の結果や CSV ファイルをアップロードするか、重要な情報を用いてマニュアルでインシデントを作成するかして、1 通または数千ものメールを隔離するアクションを起こすことができます。ほんのわずかな時間でセキュリティ脅威、そしてポリシー違反メールを受信箱から排除することができます。メールを読んでしまったのは誰か、またそれらのメールの回収が成功したかどうかというアクティビティリストも出すことができます。

転送メールの自動隔離

悪意のある、または望ましくないメールが他のユーザー、部門、配信リストに転送されることがあります。これらのメールを、エンドユーザーに届いてしまった後に取り消すのは、管理者にとって非常に面倒な作業です。そのため TRAP は内蔵のビジネスロジックとインテリジェンスを用いて、いつメールが転送されたか、また配信リストに送られたかを判断します。そして自動的に範囲を拡大して受信者を突き止め、これらのメールを発見して取り消します。これにより時間もストレスも軽減できます。

詳細は [proofpoint.com](https://www.proofpoint.com) でご確認ください。

proofpoint について

Proofpoint, Inc. (NASDAQ:PFPT) は、サイバーセキュリティの主導的企業であり、組織の最大の資産であり同時に最大のリスクでもある「人」を守ります。Proofpoint は、クラウドベースの統合ソリューションによって、世界中の企業が標的型脅威を阻止し、データを守り、ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。また、Fortune 1000 の過半数を超える企業を含むあらゆる規模のトップ企業が、メールやクラウド、ソーシャルメディア、Web 関連の最も重要なセキュリティリスクおよびコンプライアンスリスクを低減させるために、Proofpoint を利用しています。詳細は www.proofpoint.com でご確認ください。

©Proofpoint, Inc. Proofpoint は、米国およびその他の国における Proofpoint, Inc. の商標です。記載されているその他すべての商標は、それぞれの所有者に帰属します。