Proofpoint Threat Response Auto-Pull

配送済の悪意あるメールを自動で隔離

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[1]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

1 Abuseメールボックス:
ユーザーから迷惑メールなどを報告(転送)してもらうための組織で管理するメール受信箱

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は悪意のあるメールを自動または手動で隔離します。これは、ユーザーの受信箱に届いてしまった脅威を排除する効果的な手法です。TRAPを使えば、メールおよ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。

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、配信後に害を及ぼすような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。

Proofpoint Nexus Threat Graph でさまざまなベクトルのインテリジェンスを共有

Proofpoint Nexus Threat Graph は、メール、クラウド、ネットワーク、ソーシャルメディア上の脅威データを集約し、相関分析をおこない、プルーフポイント製品でのリアルタイム脅威対策を強化します。これはプルーフポイントのプラットフォームの一部であるため、個別のインストール、デプロイ、管理は不要です。以下のようなメリットを享受でき、進化し続ける脅威の先を行くことができるようになります。

- 115,000 以上の顧客から得られた脅威インテリジェンスをリアルタイムに共有
- メール、クラウド、ネットワーク、ソーシャルメディアをすべて可視化
- 100 以上の攻撃者をトラッキングして動機と戦術を理解し、対策を強化

TRAP は Proofpoint Nexus Threat Graph のインテリジェンスを活用して受信者とユーザー アイデンティティを関連付けし、関係するキャンペーンを特定し、攻撃に用いられた IP アドレスやドメインを明らかにします。これに基づいて、TRAP は特別な権限を持つ特定の部門やグループに属するターゲットユーザーには自動的にアクションを実行します。

また、顧客環境内で悪意のあるリンクや添付ファイル、または不審な IP を含むメールを検知した場合は、すべての顧客でその情報を活用して、今後それらが届く前に対処できるようにします。また、受信箱に届いてしまったメールは取り除いて隔離します。

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。Proofpoint 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するため、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および優先順位付け）、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[1]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が確認されます。
そしてメールは受信箱から自動的に隔離されます。

アウトバンドのメール管理

TRAPはCSVファイルとProofpoint Email Protectionの検索機能の一つである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、そしてポリシーに違反した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隔離します。これにより時間の短縮と労力も軽減することができます。

高度な優先順位付け

SOC アナリストは TRAP を用いて、URL に関連するインシデントを優先順位付けできます。そして Proofpoint Browser Isolation 技術でこれらの URL を安全に調査し、URL のコンテンツを確認し、組織へのリスクを低減することができます。

1 ユーザーから迷惑メールなどを報告（転送）してもらうための組織で管理するメール受信箱

詳細

詳細は **proofpoint.com/jp**でご確認ください。