Proofpoint STP (Supplier Threat Protection)

不正アクセスを受けたサードパーティ アカウントを識別し、これがもたらすリスクに関する知見を得る

主なメリット

- 不正アクセスを受けた既知のサードパーティ アカウントやサプライヤーアカウントをプロアクティブに監視して検知
- 悪意のあるメッセージを組織に送信している、不正アクセスを受けたベンダーアカウントの自動通知を提供
- 不正アクセスを受け、調査や修復が必要なサプライヤーアカウントの優先順位付け
- 不正アクセスを受けたサプライヤーアカウントと最近やり取りした従業員を識別

Proofpoint STP (Supplier Threat Protection) は、Proofpoint TAP (Targeted Attack Protection) の有償アドオンで、サプライヤーやその他のサードパーティによる不正アクセスを受けたアカウントを検知します。これによりProofpoint TAPのパワーを拡大し、フィッシング、マルウェア、ビジネスメール詐欺 (BEC：Business Email Compromise) からサプライチェーンを防御することができます。

脅威インテリジェンスと振る舞い検知の人工知能 (AI) および機械学習 (ML) の独自の組み合わせにより、Proofpoint STP は、アカウントが不正アクセスを受けていると考えられる、組織への既知の送信者からのメールパターンを検知します。また、既知の送信者とその他のプルーフポイントの顧客との間のパターンを検知し、アカウントが脅威を組織に直接送信していなくても組織を保護します。

メールアクティビティの詳細な履歴や豊富なコンテキストデータを提供し、そしてダッシュボードではどのサードパーティ アカウントが最も大きなリスクをもたらしているか確認することができます。この実用的な知見により、脅威がユーザーに到達するのを防止し、リスクの優先順位付け、調査の効率化、迅速な対応が可能となります。

図 1: Proofpoint Supplier Threat Protection は、不正アクセスを受けたと思われるアカウントを検知し、関連するコンテキスト情報を提供します。

可視性

Proofpoint STP (Supplier Threat Protection) は、組織とやり取りをしているサードパーティアカウントを識別し、従業員とサプライヤーのコミュニケーション アクティビティの基準を定めます。続いて脅威インテリジェンスと AI/ML（機械学習）を使用して不審な行動を検知し、不正アクセスを受けたと思われるアカウントを表示します。やり取りの頻度やその他の基準に基づいて高リスクのパートナーの優先順位付けも行います。これにより、組織が最もさらされているパートナーにフォーカスできます。

プロアクティブな防御

Proofpoint STPにより、組織はセキュリティに対し事後対処的ではなく、プロアクティブなスタンスを取ることができます。プルーフポイントのエコシステム全体でデータを監視し、やり取りしているベンダーで不正アクセスを受けたアカウントアクティビティがあれば検知します。不正アクセスを受けたアカウントを持つベンダーが直接あなたの組織に対して、脅威を送信していない場合でも検知が可能です。あなたの組織が今後、そのベンダーのアカウントを通して攻撃される可能性もあるため、この機能は重要です。

Proofpoint STPが、パートナーによる不正アクセスを受けたアカウント アクティビティを特定した場合、速やかに通知されます。続いて脅威を阻止する、あるいは送信者ベースでWeb分離を実施することができます。また、これらのアカウントのいずれかからトラフィックを受信した場合、メールアラートを受け取るか、API によりSIEM (Security Information and Event Management)に通知を送信することができます。

シンプルな調査

Proofpoint STP により、セキュリティアナリストは、何が起こっているか、次に何をすべきかを迅速に知ることができます。これは不正アクセスを受けたサプライヤーのアカウントに関する知見を提供し、アクティビティに関するプルーフポイントによる分析と、タイムラインビューを提供します。また、標的にされている受信者と、その標的に送信された脅威を特定します。

Smart Searchとの統合により、アナリストは不正アクセスを受けたサプライヤーアカウントとやり取りした他のメッセージを迅速に見つけることができます。これにより、チームはこのアカウントが、金銭的資産や機密データにがこのアカウントにさらされたか確認できます。また、このアカウントとやり取りした可能性のある従業員を特定できます。

詳細はこちら

詳細は **proofpoint.com/jp** でご確認ください。