People-Centric セキュリティでリスクを低減する

攻撃者より優位に立つサイバーセキュリティ戦略の立案

主なメリット

以下を明らかにすることにより、可視化とコントロールを実現します：

- 脅威がどのように人を狙うか
- 人がどれほどリスクの高い方法で仕事をしているか
- 人が重要なデータにどのようにアクセスしているか

最新の脅威ランドスケープの基本的な特徴は、ソーシャルエンジニアリングの利用です。攻撃はテクノロジーやインフラではなく、「人」を標的にするようになっています。そしてクラウドへのシフトがこの傾向をさらに強めています。プルーフポイントは可視性の向上やインサイトの収集をサポートし、また最大のセキュリティリスクである「人」それぞれに適切な制御を施すアダプティブ コントロール（適応型制御）を可能にします。重要視しているのは「人」だけではありません。人がアクセスする「データ」、そして彼らが最新のソーシャル エンジニアリング攻撃に騙される可能性、またはすでに騙されていることを示唆する「行動」にも注目しています。

攻撃者は人にフォーカス

攻撃者は組織を狙ったキャンペーンの準備として、GoogleやLinkedInなどを使ってインターネット上で偵察活動を行い、より高度な攻撃戦略を練り、幅広いターゲティングを行います。ほとんどのIT/サイバーセキュリティプロフェッショナルはいまだにネットワークやIPアドレスを中心に据えて考えています。しかし、会社のネットワークを介さずに会社のデータにアクセスしようとするユーザーも存在し、リモートワーク向けにデジタル トランスフォーメーションが進むにつれ状況が複雑化しているため、従来のネットワークセキュリティのアプローチでは、これまでと同じレベルの防護はできなくなっています。攻撃者は世界をネットワーク構成図の視点では見ていません。さらに、Microsoft 365やGoogle Workspaceのようなクラウドアプリやプラットフォームの利用が増えるにつれ、ネットワークをベースにした防御アプローチは限界を迎えつつあります。クラウドアプリには重要な企業情報が含まれていますが、これらはファイアウォールやその他のネットワーク制御を通さずにインターネット上のトラフィックに乗っています。そのため人に影響を及ぼすあらゆる脅威を可視化するのは非常に困難です。また組織に関係するリスクを基にアラートやインシデントを優先順位付けすることも困難です。

Proofpoint Attack Indexでリスクを数値化

People-Centric の視点でリスクを数値化する方法の一つに、Proofpoint Attack Index があります。プルーフポイントは標的になっている「人」を識別し、日々の脅威アクティビティからノイズを取り除いて本当に対処すべき脅威を明確にするため、Proofpoint Attack Indexを考えだしました。Proofpoint Attack Indexは「人」を狙うすべての脅威を加重複合スコアで、4つの要因に基づいて点数付けされています。

- 攻撃の量:脅威の数を示します。
- 攻撃のタイプ:使用されたマルウェアのタイプを示します。このスコアは脅威の危険度と、攻撃者がどれほど手間をかけているかを考慮にいれます。例えば リモートアクセスツール(RAT) やスティーラーは、一般的なコンシューマーを狙うクレデンシャル(認証情報)フィッシングよりもスコアは高くなります。
- 攻撃の標的:標的がどれほど絞られているかを示します。攻撃対象は一人だけなのか、それとも全世界なのか?特定のユーザー、企業、業種、または地域を狙っているのか?または地球の半分に運任せで乱射するようなばらまき型の攻撃キャンペーンか?前者は後者よりもスコアが高くなります。
- **攻撃者の高度さ:**攻撃者がどれほど高度な技術を持っているかを示します。例えば国家を後ろ盾にするAPT 攻撃者は、ありきたりな小規模の攻撃者よりも高いスコアになります。

Proofpoint Attack Indexを用いると、ユーザーが直面する個々のリスクと全体リスクを評価・報告でき、脅威への最も効果的な対応策を優先順位付けできます。

攻撃対象になる人を特定する

Proofpointは、「人」を標的にして利用しようとする脅威にフォーカスしてセキュリティリスク管理を行います。このため、まず、Very Attacked People™ (VAP) を識別することから始めます。VAP™ の識別は基本となりますが、それだけでは人的リスクを理解することはできません。人的リスクには複数の変数が関わります。プルーフポイントの Nexus People Risk Explorer ではリスクの特定、そして以下のような洞察を可能にします。

- **人がどれだけリスクの高い方法で仕事をしているか:** 意図的かどうかにかかわらず、悪意のあるリンクや添付ファイルをクリックしたり、脆弱なアプリを使用したりしたことがあるか。
- **脅威がどのように人を狙うか:** 標的を絞った、高度なまたは大量の攻撃を受けているか。
- **人が重要なデータにどのようにアクセスしているか:** 重要なシステムやデータにアクセスしたり、それを管理したりしているか。その場合、ビジネスシステムまたはサードパーティアプリを通したデータの誤用、損失、漏洩のリスクが高い可能性があります。

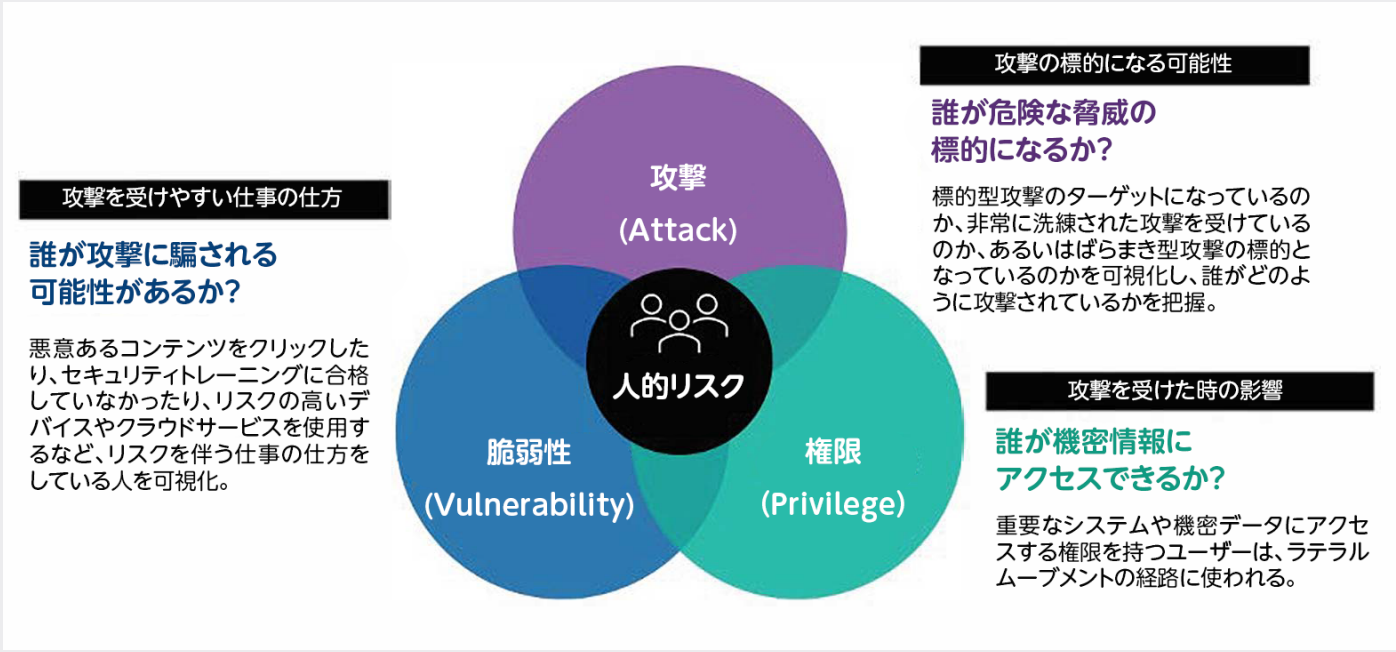

図1: リスクを通知する際にプルーフポイントが考慮する変数のベン図

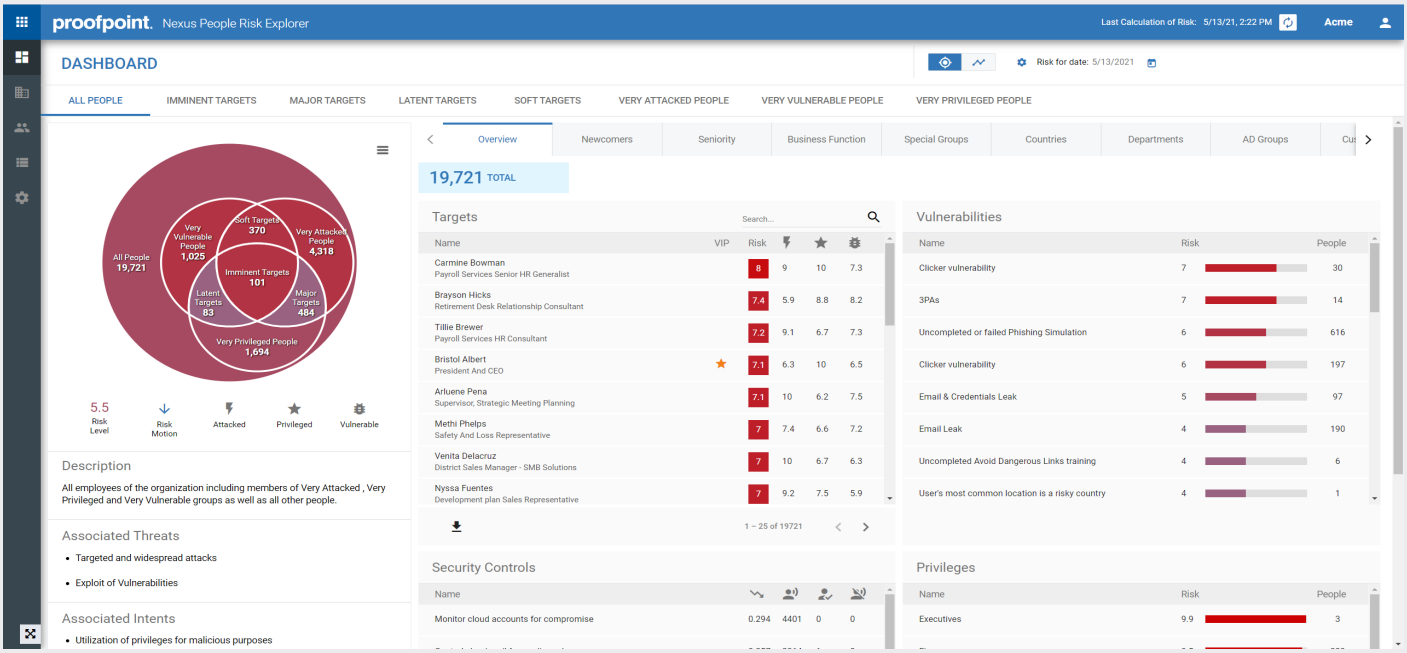

図2: 人的リスクを可視化するNexus People Risk Explorer のダッシュボード

People-Centric セキュリティアプローチ

プルーフポイントは「人」それぞれに適切なセキュリティを構築する People-Centric セキュリティの強化を支援するソリューションを提供しています。

最も多い攻撃経路を防護し、VAP™ を可視化

検知から対応まで、攻撃フェーズ全体でメールの脅威を解決することから始めます。誰が攻撃されているか、どのように攻撃されているか、フィッシングリンクをクリックしたか、または不審に思って報告したか、そして実際に侵害されたかを可視化します。

人を中心とした保護を強化し、クラウドアカウントをセキュアに

人を狙う攻撃経路（社外メール、クラウドアカウント、個人Webメール、社内メールを含む）における脅威対策と情報漏えい対策を実現します。ユーザーが最後の砦となれるよう、教育を徹底します。フィッシング攻撃を認識して報告できるよう教育します。そして自分のアイデンティティ、クレデンシャル、データを自分で守れるよう、ユーザーとベストプラクティスを共有します。

包括的な People-Centric セキュリティプログラムを構築

攻撃対象である人を漏れなくカバーできるように、ビジネスエコシステムまで防護範囲を広げます。仕事相手が自分の組織にリスクをもたらさないようにします。またセキュリティエコシステムを統合することで、既存の投資を最大活用できます。より統合され、アイソレーション可能なアダプティブ コントロールでVAP™を保護します。

詳細

詳細は proofpoint.com/jpでご確認ください。

Proofpoint | プルーフポイントについて

Proofpoint, Inc.は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。プルーフポイントは、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攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を持てるよう支援しています。また、Fortune 1000 の過半数を超える企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web 関連のセキュリティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。