Proofpoint NPRE
(Nexus People-Risk Explorer)
人に起因するサイバーセキュリティリスクの特定、評価、低減

主なメリット

- 脅威の経路およびリスク要因全体を People-Centric アプローチに基づき「人」を中心にセキュリティリスクを理解
- リスク低減策を最適化し、新たにセキュリティコントロールを配備するコストを削減
- 自社の状況を監視し、他社との対比において自社の従業員ごとのセキュリティリスクを把握

Proofpoint NPRE (Nexus People-Risk Explorer) を用いれば、人が組織にもたらすリスクを可視化できます。このツールは人が原因となるサイバーセキュリティ上のリスクを特定、評価、緩和します。

働き方は変化しています。今日のサイバー脅威やコンプライアンスの要件も変化しています。しかし、セキュリティやコンプライアンスのリスクからユーザーと組織を保護することには変わりはありません。ユーザーはどこから接続した場合でも、安全にオンプレミスシステムやクラウド アプリケーションを利用しなければなりません。最新のサイバーセキュリティ戦略において人を中心に考えなければならない理由は、ここにあります。さらに、人に焦点を合わせたセキュリティ プログラムを配備するには、適切な可視化、コントロール、統合が必要になります。

Proofpoint NPRE (Nexus People-Risk Explorer) はこれらを容易に実現できます。プルーフポイント製品やサードパーティ製品を含む組織全体の People-Centric なセキュリティリスクについて、統一されたビューが得られます。

また、セキュリティリーダーが以下のような重要な問題を把握できるようにサポートします。

1. 自社の従業員を標的にするさまざまな脅威の優先順位をどのように決めるべきか?
2. ビジネスを中断させずにリスク低減のプロセスを短縮するにはどうすればよいか?
3. セキュリティコストを説明し、今後セキュリティに投資してもらうよう理解を得るにはどうすればよいか?

セキュリティ上のメリットの他にも、「人」のレンズを通して防護体制を構築することで、関係者や取締役に対して技術的な言葉を使わずにビジネスへの影響を日々説明することができます。

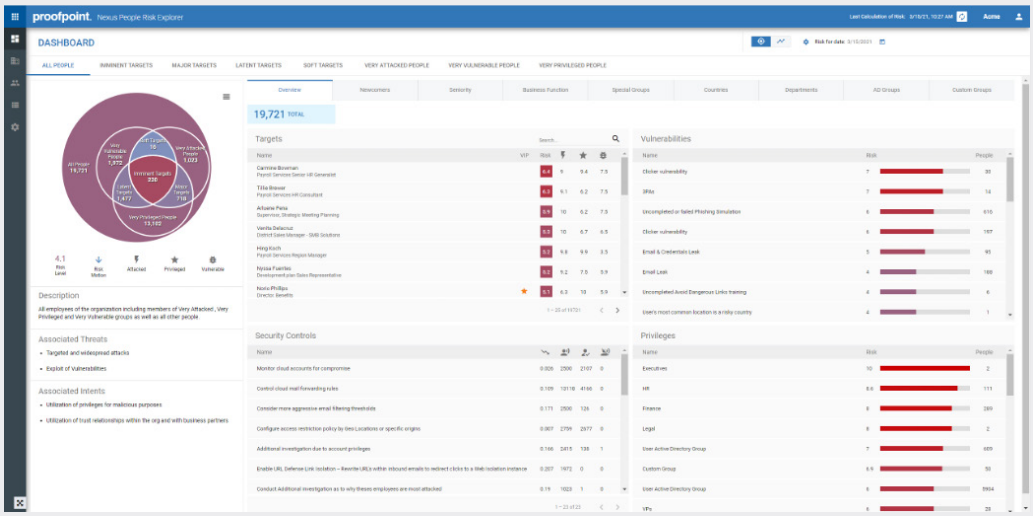

図 1：Proofpoint NPRE (Nexus People Risk Explorer) のメイン ランディング ページ
左側に Vulnerability(脆弱性)、Attack(標的)、Privilege(権限) の VAP マップが表示される

プロセス

ユーザーに関連するリスクを低減するプロセスは、複数のステップから成り立ちます。まず、環境内のセキュリティ製品のデータを分析し、ユーザーがどのように組織にリスクをもたらしているのかを特定します。その後、リスクプロフィールに基づいて従業員をセグメント化し、グループ別に適切なセキュリティ コントロールを提案します。このプロセスを通じて、組織は的を絞り、リスクに基づいてリソースを優先付けできるようになります。

統合製品：

- Proofpoint TAP (Targeted Attack Protection)
  未知の標的型攻撃に対抗するクラウド型サンドボックス
- PSAT (Proofpoint Security Awareness Training)
  オンラインによるセキュリティ意識向上トレーニング、フィッシング訓練メール
- Proofpoint CAD (Cloud Account Defense)
  SaaS アカウント侵害対策
- Proofpoint CASB (Cloud App Security Broker)
  クラウドアプリケーションの保護 (CASB)

リスクスコアは、セキュリティ脅威の多様性と深刻度、行動の脆弱性およびアクセス権限を反映しており、各個人が組織に与えるリスクの包括的な全体像を提供します。これにより、ユーザーを比較して、それにしたがって対応方法、戦略、予算に優先順位をつけることができます。

リソースおよび技術への投資を最適化する

新しいセキュリティコントロールを組織全体に配備することは、必ずしもすべてのユーザーにとって最適ではなく、コスト効率もよくありません。プルーフポイント製品では、的を絞り込んだ対策を実施して、リスクの高いユーザーのみに新しいコントロールを適用できます。所属部門、階級、リスク要因の種類で従業員をセグメント化し、各セグメントに対して、独自のセキュリティ ニーズとポリシーに合わせたリスク低減策を適用します。

プルーフポイントの詳細なセグメント化プロセスでは、同じような対策が必要となる、類似したリスクレベルの人をグループにします。こうしてできたグループは通常、全従業員の 1% ～ 5% となり、組織のプロジェクトの範囲を絞り込むことができます。グループ化したユーザーに注力することで、少ないコストで効率的にリスクを低減できます。

要因	属性	意味
Attack： どのように **攻撃** を受けたのか? (確度)	標的を絞った、高度なまたは大量の攻撃を受けている。	攻撃者がこのユーザーに強い関心を持っていることを示す。
Vulnerability: どの程度 **脆弱** なのか? (可能性)	悪意あるコンテンツをクリックしたり、意識向上トレーニングに合格できなかったり、危険なデバイスやクラウドサービスを使用する傾向がある。	このユーザーが攻撃を受けやすいことを示す。
Privilege: どのような **権限** を持っているのか? (影響度)	重要なシステムや機密データにアクセスできることから、ラテラルムーブメント（横移動）の経路になり得ることを意味している。	このユーザーが侵害された場合には、組織に損害が及ぶ可能性が高いことを示す。

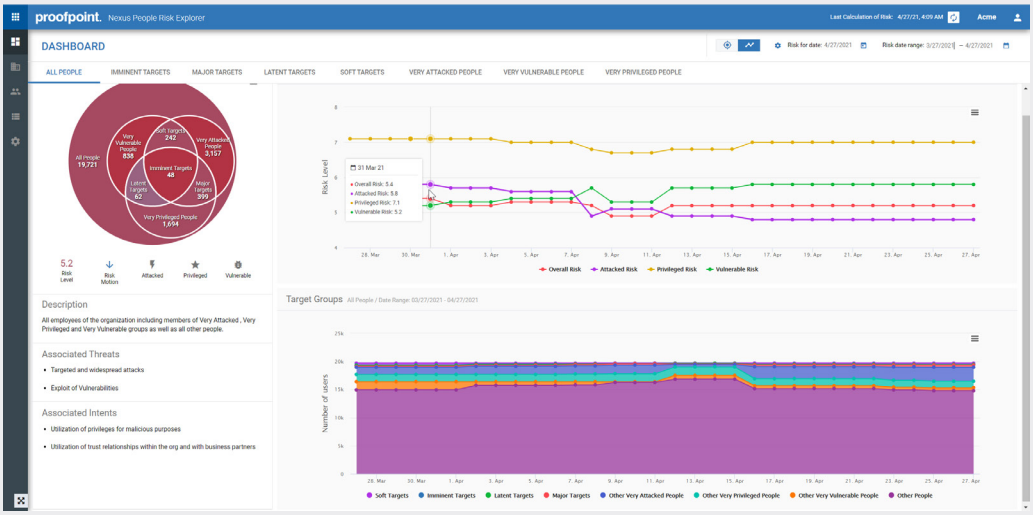

図 2：Proofpoint NPRE (Nexus People Risk Explorer) では全データを視覚的な折れ線グラフで表示

ベンチマークに照らして改善状況を監視

Proofpoint NPRE (Nexus People Risk Explorer) を使えば、個人、グループ、全社に分けて People-Centric なセキュリティリスクスコアを毎日確認することができます。そして同じ地域の同業他社、部門、同規模の企業などの結果を見て、社外のベンチマークに照らして自社の状況を把握することもできます。

また、セキュリティチームは、時間の経過とともに、全体的な People-Centric なセキュリティリスクを監視して、リスク低減策の効果や進捗状況を確認し、どういった調整が必要なのかを把握することができます。

詳細

新時代のサイバーセキュリティは人が中心です。Proofpoint NPRE (Nexus People Risk Explorer) は、必要な可視化、コントロール、統合をし、最新の脅威やコンプライアンス リスクをt低減します。誰がもっとも攻撃されているかを知るだけでは不十分です。人に起因するリスクを統合的に把握し、高リスクユーザーへのセキュリティ コントロールを適切に調整し、他社の進捗状況との比較もできなければなりません。

詳細

詳細は **proofpoint.com/jp** をご覧ください。

Proofpoint | プルーフポイントについて

Proofpoint, Inc.（NASDAQ:PFPT）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。