PSAT Enterprise

(Proofpoint Security Awareness Training Enterprise)

従業員向けセキュリティ意識向上トレーニング エンタープライズ版

製品

- Proofpoint Security Awareness Training(PSAT) Enterprise / オンライン セキュリティ意識向上トレーニング
- 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
- Proofpoint TRAP (Threat Response Auto-Pull) / インシデント レスポンスの自動化

主なメリット

- フィッシング攻撃の被害とマルウェア感染のリスクを最大 90% 低減
- ユーザーの行動を変えることで、フィッシングなどのサイバー攻撃によるリスクを低減
- ユーザーの実情に合ったトレーニングを行うことで、最大の学習効果を実現
- ユーザー教育とインシデント レスポンスの自動化でリスクと IT 部門の負荷を軽減
- CISO ダッシュボードとリアルタイムレポートでユーザーの行動変容を測定

85%以上の侵害にヒューマンエラーが関係しています[1]。この点からも、サイバー攻撃を防ぐ方法を従業員に教育することが、いかに重要であるかが分かります。結局のところ、脅威を検知して、ユーザーに届く前にブロックするというテクノロジーだけでは脅威を阻止することはできません。フィッシング、ランサムウェア、ビジネスメール詐欺（BEC）にユーザーが直面したときに、それを脅威と認識し、適切に対処できるようにすることが重要です。

Proofpoint Security Awareness Training (PSAT) Enterprise で適切なトレーニングを適切な人に、適切なタイミングで実施することで、現在の危険な攻撃に対して適切に対応することが可能になります。これにより、ユーザーが組織を守る強固な砦に変わり、組織をプロアクティブに保護できます。

このソリューションを利用することで、次のことが可能になります。

- 診断
- 行動変容
- 評価

図 1: 行動変容を持続させるための継続的なトレーニングの実施

1 Verizon「2019 Data Breach Investigations Report（2019年データ漏洩調査レポート）」2019年7月

図 2: Very Attacked People™（VAP）レポートのサンプル
最新の攻撃傾向を利用した攻撃シミュレーションを高リスクのユーザーに実施できます。
またシミュレーションで不合格のユーザーをトレーニングに自動登録できます。

診断

攻撃されているユーザーを特定し防御能力を評価

すべての従業員が同じように攻撃されているわけではありません。攻撃の頻度も異なります。サイバー攻撃者にとって魅力的な対象が標的となるため、攻撃される理由も従業員によって様々です。Proofpoint TAP（Targeted Attack Protection）との統合により、管理者は最もリスクの高い領域と人物を特定できます。こうした情報を活用することで、より効果的な対策を準備し、実施することができます。また、実際のリスクに基づいて、より具体的で影響力のあるセキュリティ意識向上プログラムを作成し、実施できます。

この強力な統合により、組織内でのVery Attacked People™（VAP）とクリック数の最も多いユーザーを特定し、これらのユーザーに発生している脅威の情報を確認できます。このデータを使用することで、該当するユーザーをシミュレーションとナレッジアセスメントに登録し、リスクを診断できます。また、トレーニングを割り当てて行動変容を促すこともできます。

プルーフポイントのフィッシング シミュレーションは、フィッシング攻撃に対する組織の弱点を明らかにします。13のカテゴリにわたる数千種類のフィッシング テンプレートがあり、複数の脅威タイプを用いてユーザーを評価できます。脅威タイプとしては、次のようなものがあります。

- 添付ファイル（DOC、HTML、PDF、DOCX、XLSX）を利用する脅威
- リンクを利用する脅威
- データ入力/認証情報を利用する脅威

常に更新を行うことで、最新の攻撃傾向を把握できます。プルーフポイントでは、プルーフポイント脅威インテリジェンスからDynamic Threat Simulationフィッシング テンプレートを作成しています。このテンプレートは、お客様からの要望や流行のトピックに対応できるように設計されています。

プルーフポイントの脅威インテリジェンスは、Fortune 100、Fortune 1000、Global 2000の企業で最も多く採用されているソリューションから収集され、リアルタイムで共有されています。このテンプレートには、ユーザー側で実際に発生している攻撃の情報が反映されています。

シミュレーション攻撃に気づくことができなかったユーザーは、攻撃にひっかかったまさにそのタイミングで「ジャストインタイム」のレッスンを受講します。これらのレッスンでは、次のことを学習します。

- 演習の目的
- 実際に発生している攻撃の危険性
- 今後、攻撃を回避する方法

フィッシング シミュレーションで騙されたユーザーには別のトレーニングを自動的に割り当てます。

また、ウイルスに感染した外付けのメモリデバイスについてユーザーがどれほど理解しているかも確認します。USBシミュレーションでは、ウイルスに感染したUSBデバイスの危険性を教育します。シミュレーション攻撃で騙されたユーザーには、そのタイミングで受講できる「ジャストインタイム」の教育を実施できます。USBシミュレーションには、キャンペーンの制限はなく、いつでもアクセス可能です。

ただし、これらのシミュレーションでカバーされるのは、特定の脅威ベクトルのリスクにすぎません。プルーフポイントのナレッジ アセスメントを使用すると、様々なドメインのリスクに対するユーザーの理解度を診断できます。たとえば、クラウドアプリケーション、内部脅威、モバイルデバイス、パスワードなどのトピックについて診断できます。

また、次のことが可能です。

- すべての制御ドメインを網羅する総合的な診断
- 40以上の言語に対応している数百の質問ライブラリから事前定義されたアセスメントを選択
- 基準を下回るユーザーを関連するトレーニングに自動登録

図 3: ユーザーが継続して取り組めるように様々なコンテンツを提供

また、カスタマイズした質問も作成できます。この機能を使用すると、組織のポリシーや手順についての理解度を測定できます。ユーザーのベースラインを設定した後、推奨事項に従って弱点を解消し、リスクを低減できます。

行動変容

実際の脅威、ユーザーの行動、知識レベルに応じたトレーニングを実施

究極の目標は行動変容です。プルーフポイントの教育プログラムは、ユーザーが効果的に学習できるように調整できます。Proofpoint TAPが識別したVAP™やクリック数の多いユーザーにプログラムを配信することで、リスクの高い領域に重点的に取り組むことができます。さらに、シミュレーションに合格しなかったユーザーや、ナレッジ アセスメントで基準を満たしていないユーザーを重点的に教育することができます。

プルーフポイントは、これまでに数百万のユーザーのリスク状態を改善してきました。このようなユーザーは現在、組織の強固な防衛線となっています。

プルーフポイントのコンテンツには次のような特長があります。

利用率を向上させるための方法論
- ユーザーの行動変容に対して実績のあるベストプラクティス
- コンテンツ ライブラリからコンテンツの利用と検索が可能
- 数百種類のトレーニング モジュールとプログラム教材
- ユーザーのタイプ（権限、ロールベースなど）に応じて必要なスキルを習得できるようにCISOが基本カリキュラムを監修

多言語に対応
- 基本カリキュラムを40以上の言語に翻訳し、地域に合わせてローカライズ（ドメイン、名称など）
- 包括的で多様なテキストと画像

新しい脅威にも対応
- 業界最高の脅威インテリジェンスで新しい脅威に対応
- メール、クラウド、ソーシャルメディアから毎日数十億の脅威サンプルを収集
- Threat Alerts、Attack Spotlightモジュール、シミュレーション テンプレートなど、脅威を中心としたコンテンツ

プルーフポイントのベストプラクティス、キャンペーン、カリキュラムにより、マルチチャネルの教育体験を実現できます。コンテンツの多様性は重要です。プルーフポイントのライブラリには300以上のトレーニング モジュールがあり、その数は急速に拡大しています。この中には、数百のPDF、インフォグラフィック、ビデオ、メモなどが含まれています。組織の文化やユーザーの好みに合うように、様々なスタイルとタイプのマテリアルが用意されています。さらに、TeachPrivacyとのパートナーシップにより、コンプライアンス対応コンテンツを強化しています。

[利用な可能なコンテンツについては、Proofpoint Security Awareness Trainingコンテンツ一覧をご覧ください。]

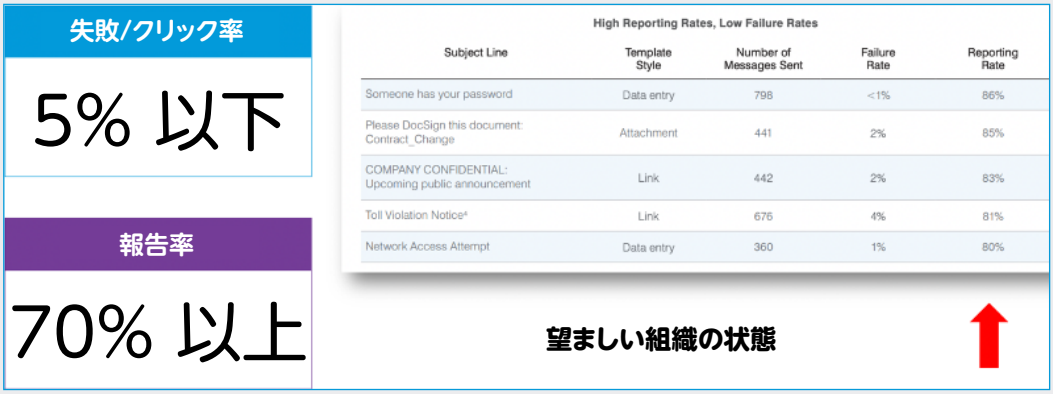

図 4: 最も優れた結果を達成した組織の実際のデータ（プルーフポイントの 2020 年 State of the Phish レポート）

コンテンツの配信
ユーザーごとに関連性の高いコンテンツを配信できます。セルフサービスの Customization Center で、次のことを行うことができます。

- ユーザーに合わせて表現、イメージ、質問をカスタマイズして、トレーニングを調整できます。
- モジュール、レッスン、ページを複製し、リアルタイムで変更可能です。
- トレーニング モジュール（質問付き）から意識向上モジュールにワンスイッチで切り替えができます。
- Learning Science Evaluator で学習効果を維持できます。（画面上のコンテンツの長さや量、質問の数が適切でない場合、フィードバックが提供されます。）

SCORM ベースのファイルを利用する独自の学習管理システム（LMS）を導入している場合は、学習モジュールをカスタマイズして、自社の LMS 用にエクスポートできます。複数の学習モジュールをまとめたり、モジュールの優先順位を設定できます。

知識の身に付いたユーザーがフィッシング脅威を報告することで攻撃対象領域を縮小

PhishAlarm® メールクライアント アドインを使用すると、ユーザー自身が不審なメッセージをワンクリックで報告できます。さらに不審なメールを報告すると、報告に対して感謝を伝えるポップアップメッセージがすぐに表示されます。これにより、ユーザーが今後も協力し、組織の最後の防護壁となり続けるよう動機付けをすることができます。このアドインを使用すると、ユーザーからヘッダーや添付ファイルを入手する必要がなくなるため、ユーザーに不審なメールを転送してもらう必要もなくなります。標準的な組織の場合、シミュレーション攻撃を報告するユーザーの割合は 10% ～ 20% です。ユーザー教育に成功したクライアントでは、この割合は 70% を超えています。

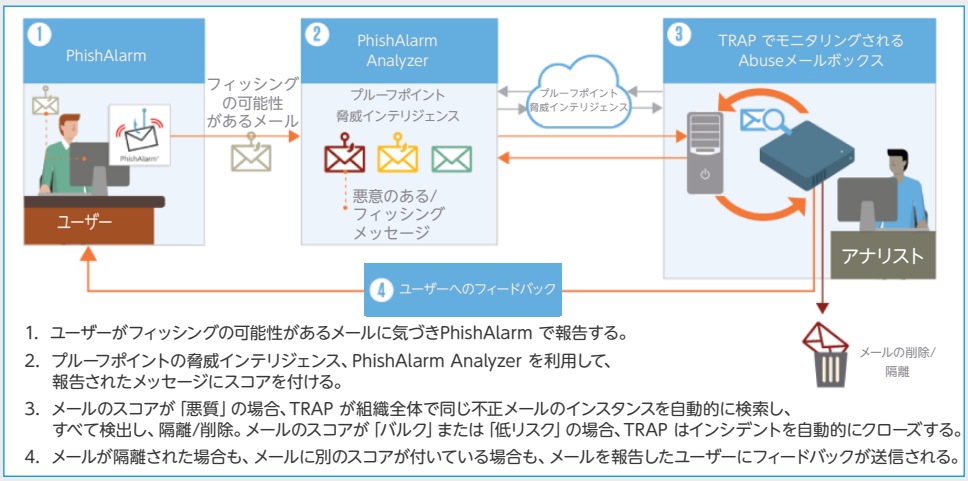

図 5: Proofpoint CLEAR ワークフロー

プルーフポイントの脅威インテリジェンスは、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、相関分析を行う業界最先端の機能を備えています。プルーフポイントは、世界規模の脅威インテリジェンス、サンドボックス、検出エンジンを使用して、不正なメッセージを識別します。ユーザーが報告したメッセージに関する情報は、脅威レポートとして自動的にセキュリティチームに配信されます。脅威レポートには、不正なメッセージと分類された理由も含まれています。これにより、インシデント レスポンス チームは効率的に作業を行うことができます。また、メールベースのリスク軽減に対するセキュリティ意識向上プログラムの効果も確認できます。

Proofpoint CLEAR (Closed-Loop Email Analysis and Response) ソリューションは、報告されたメールをProofpoint TRAP (Threat Response Auto-Pull) に自動的に送ります。Proofpoint TRAPによってこれらのメッセージは自動的に隔離または削除することができます。また、詳細な分析を行うためにインシデント レスポンス チームに送信することもできます。管理者は、メッセージのタイプに基づいて、カスタマイズされたレスポンス メッセージをユーザーに表示するように設定できます。このようなメッセージを返すことで、ユーザーの行動変容を促し、セキュリティ意識の高い文化を構築できます。

評価

ユーザーの行動変容を測定する

プルーフポイントのCISOダッシュボードは、経営幹部に分析結果を提示する強力なツールです。セキュリティ意識向上の結果をCISO/CIOや他の主要な関係者に報告する場合、特別なことを行う必要はありません。

CISOダッシュボードには、次の情報が表示されます。

- プログラム全体のスコア
- プログラムの各コンポーネントのパフォーマンス
- 業種の平均と比較した自社のベンチマーク
- プログラムで注意が必要な領域
- パフォーマンスの傾向データ
- ユーザーの脆弱性データ
  (Proofpoint TAPを使用している場合は、下位の参加者、下位の成績と最も注意すべきユーザーであるVery Attacked People™(VAP) も含まれます)

図 6: CISO ダッシュボードのスコアのサマリ
プログラムの現在の状況と、他のプルーフポイントユーザーと比較したベンチマークスコアが表示されます。

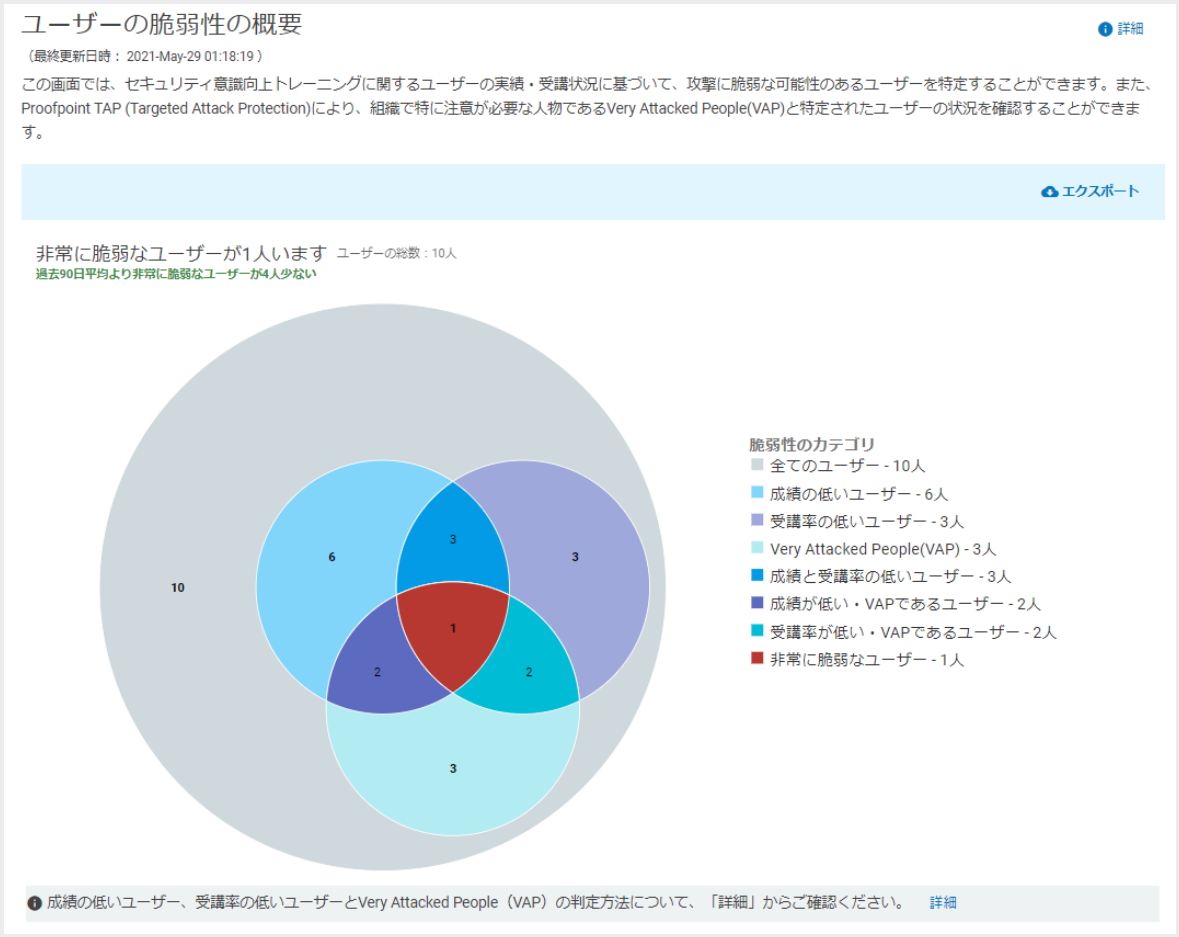

図 7: CISO ダッシュボードのユーザー脆弱性セクション
脆弱なユーザーにアクティビティを設定して、より影響力のあるプログラムを実施できます。

リアルタイムのレポートを使用すると、割り当てのステータスと現状のフィードバックを確認し、プログラムをより最適になるよう調整できます。リアルタイムレポートには、フィッシング トレーニングからトレーニングの割り当てまで様々な情報が表示されます。

これにより、次のことが可能になります。

- 特定の評価やトレーニング割り当ての進捗状況を確認する
- コンプライアンスや監査目的でデータを用いる
- レポートを簡単にエクスポートして、最新のミーティングや関係者からのリクエストを確認する
- 割り当て期限を過ぎているユーザーに対応する

さらに、Results APIを使用すると、トレーニング、フィッシング、ナレッジ アセスメント、ユーザー、メールに関するレポートや分析結果などをビジネス インテリジェンス ツールや学習管理システムに統合することもできます。

詳細

詳細は**proofpoint.com/jp**でご確認ください。