KnowBe4
Human error. Conquered.

セキュリティ意識向上トレーニングのベンダー選びで重要な7つのポイント

セキュリティ意識向上トレーニングのベンダー選びで重要な7つのポイント

目次

はじめに

セキュリティ意識向上トレーニング（SAT）ベンダーの市場環境は、革新的であると同時に実に多様です。市場はこの数年間で大きく変化しました。　最高情報セキュリティ責任者（CISO）をはじめとしたセキュリティリーダーは、SATプログラムを使ってサイバーセキュリティの脅威を理解した上でそのリスクを減らし、監視することが、ユーザーの行動変容とビジネスの強化につながると考えています。

そのためSATベンダーは、次のような方法でこれを実現するためのプラットフォームを提供していかなければなりません：

- セキュリティカルチャーや人的リスク管理について、より広い視点で捉えられるようサポートする
- ユーザーの行動変容を促進し、成果を測定するために必要なツールを提供する
- ユーザーこそがサイバー攻撃やデータ漏洩に対する組織のヒューマンファイアウォール（「人」による防御壁）であり、最終防衛ラインとなることを強調する

このホワイトペーパーでは、SATプラットフォームを厳選する前に知っておくべきことの概要と、組織の目標達成を支援するSATベンダーを選ぶ際に必ずチェックしてほしい、最も重要な7つのポイントを紹介します。

セキュリティ意識向上トレーニングプラットフォームの厳選方法

従来のSATプログラムの多くは、いわゆる「知識」－「意図」－「行動」の間に起こり得るギャップが考慮されていません。簡単に言えば、セキュリティ意識に関連する情報やデータを提供したとしても、必ずしもユーザーがそこから何かを学んだり関心を持ったりするとは限らない、ということです。

情報だけでは人の行動を変えることはできません。　結局のところ、抵抗感の少ない方法やこれまでの習慣に流れてしまうのです。まずは組織内のステークホルダーに次の3点を理解してもらい、その上でSATベンダーを選定していきましょう。

- **意識を持つように促しても、自ら進んで意識するようにはならない**
  従業員にやみくもに情報、データ、手順を与えても、セキュリティ意識を高めることはできません。ほとんどの従業員は、セキュリティに関する推奨情報を受けとっても、他の優先事項と比較した結果「あとで検討しよう」と後回しにしてしまうことでしょう。
- **人間の本性に逆らおうとすると失敗する**
  会社のポリシーへの期待値とさきに述べたような行動実態にギャップが生じてしまえば、SATプログラムを導入しても期待値を大きく下回る可能性があります。これはデータプログラミングとは違います。訓練し、期待値を設定する対象は人間だからです。
- **従業員がどれだけ知識があるかより、実際にどう動くかが重要である**
  知識があるだけでは、組織の情報漏洩は防ぐことができません。組織のセキュリティ態勢が強化されるか侵害を招くかは、その行動にかかっています。情報や会社のポリシーを提供するだけでなく、どう行動するかに焦点を当てましょう。

SATベンダーを選択するうえで不可欠な7つのポイント

SATベンダーを選ぶ際には、以下の7つのポイントに注目し、すべてを満たすベンダーを選びましょう。そうすることで、短期間でSATプログラムを成功させると同時に今後の可能性を示し、結果的に将来の成功につなげることができるでしょう。

#1 コンテンツのバリエーションと多様性

外出先でもトレーニングできるように、モバイル学習をサポートするプロバイダーを選びましょう。

教育が成功するか否かは、その内容にかかっています。SATプログラムも例外ではありません。また、「誰でも同じように学べる」プログラムが良いという考えも一旦捨てましょう。ユーザーは、自分の学びのスタイルに合ったコンテンツに魅力を感じるものだからです。まずはこのことを念頭に置いてください。組織内で従業員の行動を変え、強固なセキュリティカルチャーを構築するためには、従業員の心に響くさまざまなタイプのコンテンツがあることが重要です。SATプラットフォームを選ぶ際には、インタラクティブモジュール、ビデオ、ゲーム、ポスター、ニュースレター、アセスメントなど豊富なコンテンツを含むライブラリがあり、多言語対応で、常に最新の状態にアップデートされているものを検討すると良いでしょう。

さらに、業務別や優先度別でのトレーニングも検討しましょう。例えば、コールセンター部門とIT部門に対しては教える内容が違う部分があるかもしれません。SATコンテンツでは、このように従業員それぞれの違いをサポートしていなければなりません。統計学的に考えた場合、ユーザーの学習スタイルは組織内でもさまざまです。3〜5分のキャッチーなビデオ視聴学習のほうが良いと考える人がいたとしても、経営陣はそのアプローチでは説得力がないと感じるかもしれません。SATプラットフォームを選ぶ際は、誰もが必要なコンテンツを得られるように、中核となるトレーニングテーマを柔軟に設定できることが重要なポイントになります。

最後に、トレーニングコンテンツをユーザーにどのように提供するかは、コンテンツそのものと同じくらい重要です。外出先でもトレーニングできるように、モバイル学習をサポートするプロバイダーを選びましょう。さらに、リスクの増減を把握し、組織としてもっと介入が必要な部分について知るためには、トレーニングの内容を割り当ててその状況を追跡し、習熟度を測定・報告することができるユーザーフレンドリーな管理インターフェースを備えていることが不可欠です。また、他社のカスタムコンテンツを組み込むことができる柔軟性もあればなお良いでしょう。

#2 ローカライゼーションへの対応

ローカライゼーションとは、コンテンツの翻訳に加え、ユーザーにとって地域特有の事例やイメージ、インタラクティブな要素を提供する重要なプロセスです。これは、グローバルに展開する組織や、さまざまな言語を話す従業員を抱える組織にとっては単なるコンテンツの翻訳に留まらない綿密なプロセスであり、業務に欠かすことができません。

ユーザーの所在地または希望言語や国・地域を選択できるSATベンダーと提携することは、ユーザーがトレーニング教材の内容をしっかりと身につけ、応用できるようにするための重要な要素です。高品質のローカライゼーションを提供し、現地に精通したエキスパートによりコンテンツや事例が適切かどうかを適時判断しているSATベンダーかどうかを確かめましょう。

#3 プログラムの構造とオートメーション機能

SATは「1回やれば終わり」のトレーニングではありません。セキュリティカルチャーを築くには、継続的なトレーニングとテスト、そして知識を深めることが必要です。さらに、SATプログラムを作成する際には、学習を3つのステージに分けて行うことを念頭に置き、それぞれの学習ステージに必要なコンテンツとツールを備えたSATプラットフォームを探すことが重要です。

- **フォーマル学習 (10%)** – 教室ベースのトレーニング、学習管理システム（LMS）を通じたオンライン学習、トレーニングの実施など。
- **インフォーマル学習 (20%)** – 他のチームメンバーとの意見交換、共同作業、テーマに関するビデオ鑑賞、テーマに関する本を読んだりすることなど。
- **体験型学習 (70%)** – 現場での仕事、社会的交流、ビジネスワークフロー、企業や部門の文化などを通じて得られる、日々の実践的な学習機会など。

人の学習の90%は、形式的に構造化された場以外で行われています。

このように、人の学習の90%は、形式的に構造化された場以外で行われています。多くのSATプログラムは、最初の10%の部分にのみ焦点を当てているから失敗するのです。3つのステージすべてに対応していること、そして使用するプラットフォームが3つの学習ステージすべてに対応できるツールを備えているSATプログラムを選びましょう。例えば、組織のパスワード変更ページにパスワードに関するショートビデオを掲載し、必要な時にすぐに視聴ができるようにする、などがよい例です。

最後に、オートメーション機能も重要です。オートメーション要素が組み込まれたSATプログラムだとプロビジョニングが容易になります。また、プログラム管理者が手動で操作しなくても、ユーザーに提供するトレーニングを数週間前にスケジュールできるといった便利な機能があることを確認しておきましょう。これにより、プログラム管理時間の効率化を図ると同時に適切なタイミングで適切なユーザーにコンテンツを提供することができるため、使いやすさとROI（Return On Investment、投資収益率）も向上します。オートメーション機能はまた、必要に応じて行う「オンデマンド型トレーニング」のための事後対応／是正措置ベースのイベント提供や、経営陣やエグゼクティブ向けの定期的なレポーティングにも活用できなければなりません。

#4 シミュレーションテスト

SATプログラムの基礎となるのはトレーニングですが、テストも重要な役割を果たします。フィッシングテストを通じてユーザーの反応をシミュレーションすることで、彼らのセキュリティ行動がトレーニングによって変わり、人的リスクを軽減できているかどうかを確認できるからです。フィッシングメールが届いた場合、ユーザーはメールをクリックするのでしょうか？または報告するのか、それとも何もしないのでしょうか？
さらに、組織がレジリエンスを構築するためには、ユーザーが簡単にフィッシングメールを報告する仕組みが必要です。フィッシング被害の報告メカニズムが確立していれば、ITチームが組織を標的とした潜在的な攻撃

の状況を把握できるだけでなく、それらの情報を社内で共有することが可能になります。

ほとんどのSATプラットフォームは、フィッシング報告をサポートするエンドユーザーツールに加え、さまざまな種類のシミュレーションやフィッシングテンプレートを提供していますが、ベンダー選びの際はこうしたテンプレートを細部まで確認することが重要です。脅威の状況を常に把握し、実際に起こりそうな脅威に近いフィッシングメールのテンプレートを提供しているSATベンダーと提携することをお勧めします。

また、従業員がフィッシングのシミュレーションテストに失敗した場合、SATプラットフォームからオンデマンド型トレーニングを提供して、まだ記憶が新しいうちに再学習の機会を設けることも必要です。

コンテンツ配信やプログラム開発と同様に、こういったフィッシングシミュレーションプログラムにもオートメーション機能と機械学習を活用できるとより良いでしょう。フィッシングシミュレーションのプラットフォームを選ぶ際は、機械学習により収集したユーザーのトレーニングやフィッシングの履歴情報に基づいたパーソナライズが可能なものを検討しましょう。ユーザーのニーズに合ったテンプレートを推奨・提供し、リアリティのあるフィッシングメールをシミュレーションテストに反映できるものでなくてはなりません。

#5 メトリクスとレポーティング

測定とレポーティングも、SATプログラムがいかに効果的にユーザーの行動を変え、人的リスクを低減しているかを判断するには効果的です。また、セキュリティ意識プログラムの成果を経営陣に数値化して示すことも非常に重要なことです。

特定のゴールやターゲットに対してプログラムがどの程度機能しているかを把握し、改善点を明確に示すことができれば、経営陣の賛同を得やすくなるでしょう。組織が最も重要なことを測定できるように、安定したレポーティングおよび分析プラットフォームが提供できるベンダーを選んでください。SATのプログラムマネージャーは、経営陣向けにレポートを準備する必要があります。こうした場合に、レポートの特別なカスタマイズも簡単にできるようなプラットフォームだとなお良いでしょう。

さらに、人的リスクとセキュリティカルチャーの指標を測ることができるかどうかも重要です。従来のSATプログラムは、修了率、修了テストの成績、エンゲージメントを指標の目安とするものが中心でした。個人またはグループ／チームごとのリスクプロファイルを測定し、トレーニングの調整に関してデータに基づいた意思決定を行えるのが理想です。そのためには、組織のリスクが時間とともにどのように変化するかを評価し、トレーニングプログラムのパフォーマンスを真に測定できるプラットフォームが必要です。また、組織のヒューマンファイアウォールを強化するために改善すべき点が分かりやすく示されている必要があります。

#6 調査と評価方法

「サイバーセキュリティはIT部門の仕事である」と認識している従業員は意外に多いものです。形式化されたセキュリティ意識向上トレーニングを継続的に行うよう指示されても、自分とは関係がないことに思えるかもしれません。そのため、SATの実施によって組織内のセキュリティ意識がどう変化しているのかを理解しておく必要があります。そうすることで、うまくいっている部分が明らかになると同時に、改善の必要がある部分も浮き彫りになります。同時にセキュリティカルチャーがどのぐらい浸透しているかを図ることもできますが、これは従業員の傾向、意見、心構えを分析することなので先に述べた指標とは異なります。

アンケートや評価では、感情や態度だけでなく、知識や熟練度も測定する必要があります。SATプラットフォームを選ぶ際には、スキルベースの評価とセキュリティカルチャー調査を行う機能があるか、またユーザーのセキュリティ知識と習熟度を測定し、組織全体でのセキュリティカルチャーに対する姿勢を見極めることができるかどうかを確認しておきましょう。特定の状況への対応方法や、正しい対応方法とは何か、といったことをより熟知しているユーザーを特定することがゴールになります。さらに、業界内の同業他社をベンチマークする機能を提供し、組織の進展状況を正確に測定し、科学的に妥当性のある評価を基準としているプラットフォームでなければなりません。

従業員の人的リスクスコアを測定する機能も必須です。つまり、導入しようとしているSATプラットフォームが人的リスクマネジメントに取り組んでいるかどうかが見極めのゴール地点となるでしょう。個人または各部署のリスクプロファイルを理解すれば、トレーニングを調整し、セキュリティプログラムの改善点に関する貴重な洞察を得ることができ、組織のセキュリティ態勢の強化にもつながります。

#7 SATの枠を超えたサポート

近年、SATベンダーの状況は根本的に変化しています。業界をリードするベンダーは、ユーザーのトレーニングだけにフォーカスした製品から、組織のセキュリティカルチャーの構築や人的リスク管理といったより包括的な問題に取り組むプラットフォーム製品の開発へと移行しています。

そのため、目先の目標を達成するだけでなく、将来的な可能性を示してくれるパートナーとなり得るSATベンダーを選ぶことが重要です。SATベンダーを評価する際には、以下のポイントに留意してください：

- **意識、行動、セキュリティカルチャーに焦点を当てているか**
  最終的なゴールは、人的リスクを減らすことです。人的リスクの数値化とユーザー行動に基づくリスク計算を提供できるベンダーと提携したいと考える企業が多数みられます（Forrester Research*調べ）。SATは企業でセキュリティカルチャーを形成するための基礎となります。

- **SATの枠組みを超える可能性がある多様なサービスを提供するベンダーかどうか**
  前述のように、SATは組織内にセキュリティカルチャーを構築するための土台ですが、必ずしもそれだけではありません。セキュリティイベントを人的防御の観点から相関付けして、特定・対応するHuman Detection and Response（HDR）、SOAR（Security Orchestration, Automation and Response）プラットフォーム、インシデントレスポンス、脅威インテリジェンスなど、将来的にセキュリティカルチャーのロードマップに加えられる重要な要素もあります。

* The Forrester Wave™調べ：「Security Awareness and Training Solutions（2022年第1四半期）」でリーダーの評価を獲得

SATベンダー選定のチェックリスト

- ☐ 豊富で多様な学習コンテンツを多数備えている
- ☐ ローカライゼーションに対応している
- ☐ 高度に自動化されたトレーニングおよびフィッシング対策プラットフォームである
- ☐ 自社専用のトレーニングコンテンツのアップロードや、ベンダーのプラットフォームからのダウンロードが可能
- ☐ オートメーション機能搭載のトレーニングプラットフォームである
- ☐ 他社のコンテンツをトレーニングプラットフォーム/LMSにアップロードする機能がある
- ☐ カスタマイズやローカライズに対応可能なテンプレートを多数備えた、柔軟性の高いプラットフォームで、シミュレーションも可能である
- ☐ トレーニングプラットフォームとフィッシングプラットフォームにオートメーション、人工知能、機械学習機能を搭載している
- ☐ ユーザーの知識とトレーニングの効果をチェックするための、安定性の高いユーザーテストと評価機能がある
- ☐ ひと目でわかるメトリクスとレポート機能でROIの確認ができる
- ☐ エグゼクティブ向けのレポート機能がある

まとめ

最終的に、これらの機能は、組織で導入したSATプログラムがユーザーの行動を変えること、および企業がサイバーリスクの本質を理解し、その数を削減し、監視することを可能にするための基礎を築くものです。SATは、セキュリティカルチャーと人的リスク管理に関する幅広い理解を深めるためのプラットフォームとして機能し、ユーザーが組織のヒューマンファイアウォールとなるための手助けをしてくれる存在です。ぜひ、このガイドを参考にして自社のニーズに合ったプログラムの導入を検討してみてはいかがでしょうか。

その他のリソース

無料のフィッシングセキュリティテスト
フィッシング攻撃の被害に遭いやすい従業員の割合を、無料のフィッシングセキュリティテストで確認できます。

無料のセキュリティ意識向上プログラムオートメーション機能
自社組織に合わせてセキュリティ意識向上トレーニングプログラムをカスタマイズできます。

無料のPhish Alertボタン
従業員がフィッシング攻撃を発見した場合、このボタンをクリックするだけで安全に報告することができます。

無料のメールエクスポージャチェック
攻撃者に発見される前に、流出したメールを特定できます。

無料のドメインなりすましテスト
組織のドメインを使うメールアドレスがスプーフィング攻撃を受けていないかを確認できます。

KnowBe4について

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション訓練・分析を組み合わせた世界最大の統合プラットフォームのプロバイダーです。サイバーセキュリティにおいて人的要素は見落とされがちです。KnowBe4は、このことを察知し、包括的な新しい形態の意識向上トレーニングプログラム(当社では「New School」と呼んでいます) を通して、企業や組織が継続的なソーシャルエンジニアリングの問題を管理できるようにするために設立されました。

これは、本番さながらの偽装攻撃によるベースラインテスト、学習意欲を高めるインタラクティブなトレーニング、およびエンタープライズクラスの最強のレポーティングを通した継続的なアセスメントを組み合わせた統合型のアプローチです。

金融、医療・介護、エネルギー、官公庁、保険業など規制の厳しい分野を含むあらゆる業界で、多くの企業や団体がKnowBe4のプラットフォームを採用し、防御の最終ラインとしてヒューマンファイアウォールを構築して、日々求められるセキュリティ上の的確な意思決定を可能にしています。

詳細については、www.KnowBe4.jpを参照してください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan合同会社 | 〒100-6510 東京都千代田区丸の内 1-5-1 新丸の内ビルディング 10F EGG
電話：03-4586-4540 | www.KnowBe4.jp | Email: Info@knowbe4.jp

05D03K01