SecurityCoach

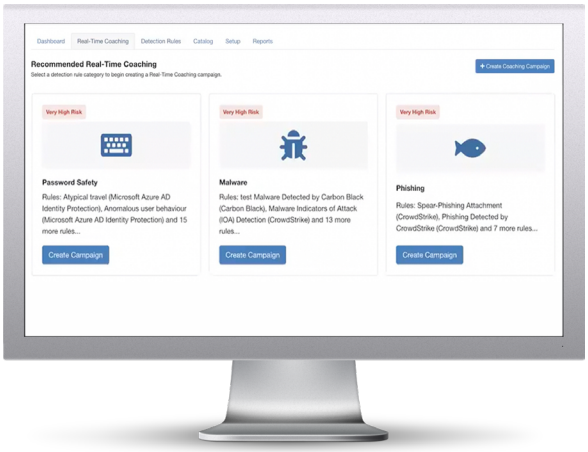
KnowBe4
Human error. Conquered.

リスクの高いユーザー行動に対応したリアルタイムコーチングを提供

全体的なセキュリティカルチャーを向上し、リスクを低減

様々なソーシャルエンジニアリング手口が横行する中、サイバー犯罪者はユーザーを利用して、サイバーセキュリティの防御層を突破しようとしています。Verizonのデータ侵害調査報告（Verizon 2022 Data Breach Investigations Report）によると、データ侵害の82%に人的要因が含まれていることが指摘されています。また、従業員が危険な行動を取るたびにアラートが出され、セキュリティチームの業務量は激増します。業務が多すぎるためにチームが疲弊に追い込まれないよう、繰り返し発生する従業員の危険な行動を減らす必要性も考慮しなければなりません。

既存のセキュリティスタックで検出されたユーザーイベントデータを利用して、セキュリティ上のミスに対応したリアルタイムコーチングをユーザーに提供できるとすればどうでしょう。また同時に、セキュリティオペレーションセンター（SOC）チームが受ける、繰り返し発生する危険な行動によるアラートノイズの回数を減らすことができるとしたら？ **これらすべてがSecurityCoach™で実現します。**



主なメリット

- セキュリティトレーニングや確立されたセキュリティポリシーの理解・定着を、実際の行動に対するリアルタイムコーチングで強化
- 既存のセキュリティスタックを活用し、リスクの高いユーザーにリアルタイムコーチングを提供することで、既存の投資にさらなる価値を付加
- サイバー犯罪者に狙われやすい、あるいは危険な行動を繰り返すハイリスクユーザーやロールに対するカスタムキャンペーンを構築
- 組織全体における実際のセキュリティ行動の改善を測定・報告し、継続的な投資の有用性を証明
- 繰り返し発生するリスクの高いセキュリティ行動によるアラートノイズを減らすことで、SOCの負担を軽減し、有効性を向上

SecurityCoachとは？

SecurityCoachは、ITチームやセキュリティオペレーションチームが、組織内で最大の攻撃対象である**「従業員」**を保護するために作られた初のリアルタイムセキュリティコーチング製品です。

SecurityCoachは、ユーザーの危険なセキュリティ行動に対し、リアルタイムなコーチングを行うことでセキュリティカルチャーの強化をサポートします。既存のセキュリティスタックを活用してリアルタイムコーチングキャンペーンを設定するため、セキュリティ意識向上トレーニングやポリシーを強化する文脈的なSecurityTipを即座にユーザーに提供することができます。これにより、知識の定着率が向上し、ユーザーが自分の行動に関連するリスクを理解することができるようになります。

SecurityCoachなら、KnowBe4のNew Schoolセキュリティ意識向上トレーニングプラットフォームと既存のセキュリティスタックを統合し、エンドユーザの危険なセキュリティ行動に対応したリアルタイムのコーチングを提供することができます。

SecurityCoachを選ぶ理由

組織のユーザーをターゲットにしたソーシャルエンジニアリング攻撃は増加の一途を辿っています。最善の防御策は、組織全体で強力なセキュリティカルチャーを醸成してユーザーを巻き込んでいくとともに、組織のセキュリティポリシーに従うことの重要性、およびヒューマンファイアウォールを強化することです。

SecurityCoachは、繰り返し発生する危険な行動による不要なアラートを減らし、SOCが優先度の高い脅威に集中できるようにすることで、負担の大きいSOCチームの業務効率改善に貢献します。

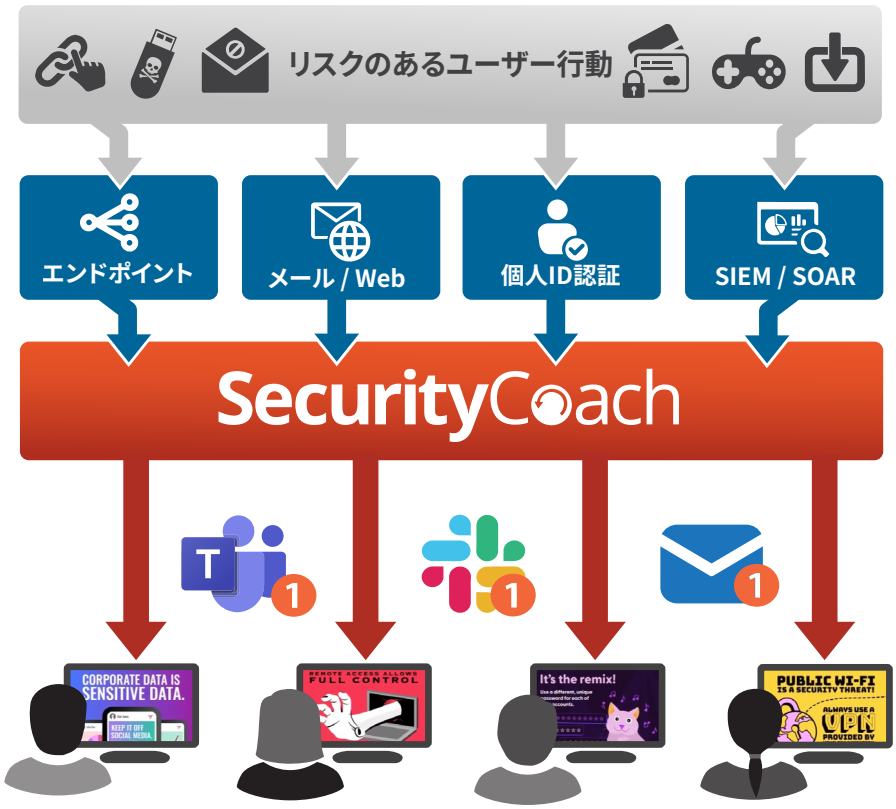
SecurityCoachの仕組み

SecurityCoachは標準的なAPIを使用しているため、Microsoft、CrowdStrike、Cisco、その他多数のベンダーの既存のセキュリティ製品を迅速かつ簡単に統合することができます。セキュリティスタックが生成するアラートをSecurityCoachが分析し、ユーザーのセキュリティ上の危険な行動に関連するイベントを特定します。

例えば、あるユーザーがネットワーク上でランサムウェアを拡散させる可能性のある感染したメールの添付ファイルを開いた、または制限されたコンテンツを含むウェブサイトをコンピューターで閲覧しようとした場合、セキュリティ製品がこれを検知してイベントアラートを生成します。SecurityCoachはそのイベントを特定し、Microsoft Teams、Slackまたはメールを通じて、「これはセキュリティリスクで、その理由は〇〇」ということを知らせるため、SecurityTipをこのユーザーにリアルタイムで送信します。

また、ネットワーク、ID、Webセキュリティ、およびセキュリティスタック内の他のベンダーからのイベントに基づき、リスクの高いユーザーを対象にしたコーチングキャンペーンを設定することができます。これらのキャンペーンは、危険な行動が発生した瞬間にユーザーを指導してリアルタイムのフィードバックを提供するため、現在実施中のセキュリティ意識向上トレーニングキャンペーンの強化につながります。独自のセキュリティポリシーをベースとして使用し、SecurityCoachの自動設定でサポートすることにより、リアルタイムのコーチングキャンペーンを簡単に設定することができます。

SecurityCoachなら、ユーザーの行動を改善し、全体的なセキュリティカルチャーを高めるとともに、組織のセキュリティポリシーに対するコンプライアンス意識の強化にも効果的です。



SecurityCoachのワークフロー

1. KnowBe4コンソールに統合したセキュリティスタックのベンダー側で、ユーザーのデバイス上の危険な行動を監視します。
2. その後、アラートデータがSecurityCoachと共有されます。SecurityCoachはアラートを分析し、どの脅威がユーザーへの指導に最適であるかをリアルタイムに判断します。
3. リスクのあるユーザーの行動が検出されると、SecurityCoachは自動的にMicrosoft Teams、Slackまたはメールを介してそのユーザーにリアルタイムでSecurityTip通知を送信します。

主な機能

リアルタイムコーチング
リアルタイムコーチングキャンペーンを活用すれば、危険な行動についてユーザーにリアルタイムで指導を行うことができます。リスクのある行動が検出されると、その行動に関するSecurityTipと、今後それを回避する方法を記載したコーチング通知がユーザーに送信されます。

SecurityTip通知
危険なユーザーの行動が検出されると、SecurityCoachは自動的にMicrosoft Teams、Slack、またはメールを介してそのユーザーにリアルタイムでSecurityTip通知を送信します。すぐに通知が届くため、セキュリティ意識向上プログラムの内容をさらに習慣づけるという意味でも効果的です。

APIベースの統合
APIを通じて、Microsoft、Cisco、Netskope、Zscalerなど、既存のセキュリティスタックベンダーと迅速かつ容易に統合することができます。当社の技術パートナーシップのエコシステムは、お客様をサポートし、ヒューマンファイアウォールを強化するために急速に拡大しています。

ビルトインの検出ルール
統合セキュリティベンダーから提供されるデータを使用し、どのようなリスクのある行動を追跡するかを検出ルールで指定します。SecurityCoachは、一般的なセキュリティトピックに基づいて「非常に高い」「高リスク」のルールを最初に提示し、優先順位の高い順に検出ルールを提案します。

キャンペーンの提案
SecurityCoachが、検出ルールに最適なリアルタイムコーチングキャンペーンを提案します。異なるカテゴリーの危険な行動を元に、SecurityTipsを選択できます。

ユーザーマッピングが簡単
IDプロバイダーやディレクトリからのユーザーデータとセキュリティイベントログを組み合わせて、ユーザーマッピングのルールを作成します。さまざまなビルトインユーザーマッピングルールとカスタムルールの作成機能を利用して、ルールを簡単に設定し、ユーザーを自動的にマッピングすることができます。

ダッシュボードと詳細レポート
ビルトインダッシュボードでは、コーチングキャンペーン、検出ルール、検出されたセキュリティイベントの全体的なサマリーを確認することができます。詳細レポートは、組織のセキュリティリスクに対する考察を提供し、ユーザーの危険な行動の傾向を時系列で追跡するのに役立ちます。

ルールベースの自動化
既存のセキュリティソフトウェアスタックのルールと、高リスクのユーザーまたはロールの定義に基づいてリアルタイムのコーチングキャンペーンを設定し、リスクの高いユーザーに送信されるSecurityTipの頻度や種類を決定できます。

堅牢なSecurityTipカタログ
60種類のトピックに及ぶ200種類のSecurityTipを利用可能。内容は継続的に改善されています。その多くが34の言語で提供されており、広範なカタログを使用してキャンペーンを作成できます。

強力なセキュリティ統合

SecurityCoachは標準APIを介して、CrowdStrike、Microsoft、Cisco、Netskope、Zscalerなどのベンダーによる既存のセキュリティ製品と迅速かつ容易に統合することができます。当社の技術パートナーシップのエコシステムは、お客様をサポートし、ヒューマンファイアウォールを強化するために急速に拡大しています。

SecurityCoachがセキュリティプラットフォームにアクセスできるよう、KnowBe4コンソールで統合設定を行います。両システムを統合することにより、特定のアクションが検出されたときにSecurityCoachがそのデータを追跡することができるようになります。統合は迅速かつ簡単に設定できます。当社のナレッジベースでは、各ベンダーの統合ガイドも提供していますので、ぜひご覧ください。統合が完了すると、セキュリティプラットフォームからのイベントやその他データがSecurityCoachのダッシュボードに表示されるようになります。

ベンダーとSecurityCoachの統合について詳細は、https://www.knowbe4.com/integrations（英文）を参照してください。