IBM Security Trusteer Pinpoint Detect

デジタル不正のライフサイクル管理に関する包括的なソリューション

ハイライト

- 証拠に基づく不正検出機能を使用して、誤検出を大幅に削減しながら不正を検出します
- 組織が不正のライフサイクル全体で不正を正確に特定して防止するための、簡略化された不正管理アプローチを採用します
- IBM のグローバルな脅威情報ネットワークに裏打ちされた、すぐに使用可能な保護機能を利用します

残念なことに、サイバー犯罪者は高度な対策がリリースされたほんの数日後にはその対策をバイパスすることができます。サイバー犯罪者は既存の対策と新しい対策の両方をより効率的にバイパスできるよう、継続的に技術を更新しています。

不正の標準的なソリューションが提供するテクノロジーは、不正のリスクを予測するためにデータを統合し、分析するものです。しかしそういったテクノロジーは通常、単一層の保護しか提供せず、導入に時間がかかりすぎるか、あるいは絶え間なく変化を続ける脅威の状況についていくことができません。

IBM® Security Trusteer® Pinpoint™ Detect が提供するアプローチはそれらとは根本的に異なっており、金融機関による不正検出を支援し、誤検出を大幅に削減することができます。IBM の不正検出アプローチは、可視性、グローバルな脅威情報ネットワーク、および意図的な俊敏性という 3 つの中核となる原則に基づいています。

可視性

Trusteer Pinpoint Detect の中核となるのは、フィッシング攻撃、マルウェア感染、危険にさらされた資格情報、高度な回避手段といったさまざまな重大不正行為の徴候を、拡張デバイス、地理位置情報、およびトランザクション・モデルに関連付けて、不正行為のより正確な検出を支援するエンジンです。

グローバルな脅威情報ネットワーク

IBM のグローバルな脅威情報ネットワークは 2 億 7 千万のエンドポイントならびにエンド・ユーザー・エンドポイントの行動プロファイルから脅威情報を収集し、この情報を使用して動的 ID を作成します。ネットワークは、セキュリティー・インテリジェンスを絶え間なく受信し続けています。このインテリジェンスを備えた Trusteer の脅威分析者は、最先端のアナリティクス・テクノロジーを使用して業界固有ならびに組織固有の脅威を研究および調査します。分析者は、金融機関による労力を重ねることなく、自動的に防御策を適用することができます。Trusteer Pinpoint Detect はこの独自のインテリジェンスを利用して、多数のセッション属性、データ、および不正の徴候に基づく莫大なデータ・セット内で正確に不正を特定します。

意図的な俊敏性

Trusteer Pinpoint Detect は、非常に柔軟で迅速な対応プロセスを可能にするアジャイル・アーキテクチャーを備えています。IBM はクラウド・ベースのテクノロジーを使用して、新しく出現した脅威に対する迅速な検出、分析、対策の構築および導入を支援できます。また、金融機関は自らのニーズと自らが直面している脅威に合わせて特別に調整された、アプリケーション認識の防御策を得ることもできます。

不正のライフサイクルを通じての徹底した可視性

Trusteer Pinpoint Detect は、拡張デバイス ID、地理位置情報、 およびトランザクション・モデルをさまざまな不正徴候と組み合わせて脅威の性質と潜在的なリスクの両方を判別することによって、オンライン・バンキングをアカウントの乗っ取りや不正なトランザクションから保護します。

この集約情報はビッグデータ・テクノロジーを使用して関連付けられ、時間、ユーザー、およびアクティビティーを越えてイベントをリンクすることで、セキュリティー侵害からアカウント・アクセス、そして現金の引き出しに至るまでの不正のライフサイクル全体に、包括的な可視性および洞察をもたらします。

脅威の状況に関する継続的なインテリジェンス

不正への対処の成功は、検出、分析、および対策の導入スピードと大きな関わりがあります。IBM アプローチの中核となるのは、グローバルな脅威情報ネットワークです。このネットワークには、絶え間なく変化を続ける脅威の状況への対処に使用される、多数の情報源から得られた膨大な量の集約情報が含まれます。このインテリジェンスはすべての IBM Security Trusteer ソリューションからもたらされる情報によって絶えず更新され、クラウド・ベースのアーキテクチャーを使用して Trusteer Pinpoint Detect に迅速に導入されます。結果として、Trusteer Pinpoint Detect は新たな脅威が出現したときに組織の対応を支援できるのです。

改善された不正検出のためのシームレスなプロセス

Trusteer Pinpoint Detect は、可視性、インテリジェンス、および俊敏性を組み合わせることによって高度なサイバー・セキュリティー・ソリューションを実現します。Web アプリケーション・センサーに基づいてオンライン・バンキング・セッションから情報を収集し、リアルタイムにカスタマー・データ・センターに通知します。

Trusteer Pinpoint Detect のエンジンは、収集されたセッション情報をそのアカウントの履歴レコードとともに評価します。評価は、単一のオンライン・バンキング・アプリケーションのレベル単位で、複数の不正検出ポリシーによってリアルタイムに実行されます。

不正検出ポリシーは、IBM のグローバルな脅威情報ネットワークからもたらされる詳細な脅威情報に基づき、IBM の不正分析者によって作成されます。すべてのセッションが、実績ある防御策を使用して既知の攻撃パターンに照らし合わされます。その後、ユーザーの行動プロファイルと比較して、検出された動作がそのユーザーの普段の行動と異なっていないかどうかを判別します。この設計により、誤検知の件数は低く抑えられます。更新は透過的に導入され、最新の脅威を正確に検出します。

ポリシーが実行されたら、セッション評価はアプリケーション・プログラミング・インターフェース (API) を通じてリアルタイムに戻されるため、銀行は返ってきた最終的な推奨に基づいて即時アクションを実行することができます。

複数のデジタル・チャネルをまたぐ包括的な対象範囲

Trusteer Pinpoint Detect は、オンライン・バンキング・アプリケーション上で実行されるユーザー・アクティビティーを対象範囲とします。PC のブラウザーを介したアクセスとモバイル・ブラウザーを介したアクセスの両方が対象です。ただし、大部分の銀行にはネイティブ・モバイル・アプリケーションがあり、急速に一般化し、主要なチャネルになりつつあります。

現在のところ多くの金融機関のチャネルでは、特に不正検出において、オンラインとモバイルが個別に管理されています。犯罪者たちはこの不備をよく認識しており、結果としてモバイルとオンラインを含むクロスチャネル型の攻撃が頻発するようになっています。

Trusteer モバイル・ソリューションは、モバイル・チャネルでの検出をさらに改善するため、組み込み型 Software Development Kit (SDK) を介して Trusteer Pinpoint Detect とシームレスに統合することができます。このコンポーネントは、マルウェア感染、root 化/Jailbreak に関する情報、正確な地理位置情報、および Wi-Fi のセキュリティー状況といった、詳細なリスク情報をモバイル・デバイスから収集します。

IBM をお勧めする理由

Trusteer Pinpoint Detect はスタンドアロンの不正検出ソリューションとしても、IBM Security Trusteer Fraud Protection Suite の一部としても入手可能で、不正検出、対策、調査、修復に関する IBM のソリューションに対し、すぐに使用可能な統合を提供します。

Trusteer Fraud Protection Suite を使用すると、組織は Trusteer Pinpoint Detect を購入して特定の不正検出の問題に取り組み、その後必要に応じて組み込みの統合を使用し、対策、調査、修復のレイヤーを追加できます。統合によって、不正管理のライフサイクル全体で情報を容易に共有できるようになり、管理にかかる初期コストと運用コストの両方を削減できます。

詳細情報

Trusteer Pinpoint Detect または Trusteer Fraud Protection Suite の詳細については、 IBM 担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。**ibm.com**/security あるいは **ibm.com**/software/products/en/trusteer-fraud-protection-suite

IBM Security ソリューションについて

IBM Security は、エンタープライズ・セキュリティー製品およびサービスの最先端かつ統合されたポートフォリオの 1 つを提供します。このポートフォリオは、世界的に有名な IBM X-Force® 研究開発機関によってサポートされており、人、インフラストラクチャー、データ、アプリケーションを企業が全体的に保護できるように支援し、ID とアクセス管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーなどに対するセキュリティー・インテリジェンスを提供します。このようなソリューションにより、企業はリスクを効果的に管理でき、モバイル、クラウド、ソーシャル・メディアをはじめとするエンタープライズ・ビジネス・アーキテクチャー向けの統合セキュリティーを実装できます。IBM は、世界最大級の規模を誇るセキュリティー研究・開発・提供機関を運用しており、130 カ国以上の国々で 1 日当たり 150 億件のセキュリティー・イベントをモニターし、3,000 件以上のセキュリティー関連の特許を保持しています。

さらに、IBM グローバル・ファイナンシングはお客様のビジネスの成長に必要なテクノロジーの取得を支援するため、さまざまな支払いオプションをご用意しています。IBM は IT 製品およびサービスの取得から処分まで、全ライフサイクルの管理を提供します。詳細については、次の Web サイトをご覧ください。**ibm.com**/financing/jp

IBM Security

東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2016 年 2 月