ファクトシート

NICE · ACTIMIZE

IFM-X ダークウェブインテリジェンス（Dark Web Intelligence）情報で先手を取り詐欺犯罪を劇的に削減

他の追随を許さない人材の知識と占有技術の組み合わせにより、詐欺の損失と金融犯罪を劇的に削減して安定した投資収益率（ROI）をもたらします。

すぐに稼働可能、カスタマイズ済、常に更新される、侵入後・詐欺発生前のシナリオにまたがるインテリジェンスとモニタリング。

ダークウェブ、ディープウェブ、マルウェアネットワーク、ボットネット、プライベートメッセージのプラットフォーム、そして地下の詐欺インフラとコミュニティに対し包括的で多言語に対応。

詐欺防止業務を後手から先手へと変革

- 3つのキュレート済の、独自の、高度に分化されたデータフィードを通し、顧客の口座乗っ取り、侵入された支払いカード、そしてミュール口座にわたる**包括的な対象範囲**。
- 詐欺防止と調査関連部門の**運営費を大幅に削減**。
- **利用だけでなく**、ダウンストリームプロセスや分析の必要なしに既存の詐欺防止過程及び管理、そしてセキュリティシステムと**のスムーズな統合が簡単にできるよう設計**。
- 様々な交流や取引において、顧客に不具合をもたらさずに**断定的に疑わしい行動を検出し対処**。
- 現在と将来の攻撃ベクトルに基づき、**詐欺防止モデルを構築し最適化**。
- **共有された情報を活用し**、金融犯罪、アンチマネーロンダリング（AML）、詐欺防止、そして情報セキュリティチームをさらに強力に。

リアルタイム情報。迅速な詐欺防止。

顧客の口座乗っ取りの試みを阻止
金融機関はダークウェブインテリジェンス（Dark Web Intelligence）を活用し、検出が難しい口座乗っ取り及び広い範囲の金融犯罪を全ての支払いチャネルにおいて対処できます。口座乗っ取りの試みをリアルタイムで検出し、侵入された口座を修正して乗っ取りとその結果である顧客の不具合を阻止します。金融機関は侵入された口座を利用する最新の犯罪者の手口を知り、確固とした対抗策を実施できます。

顧客への不具合なしに支払いカード詐欺に対処
金融機関は侵入された支払いカードを利用停止・再発行できます。そして顧客に不具合が生じる前に詐欺を予想して発生を事前に防止します。サイバー犯罪者に盗難された、あるいはダークウェブのマーケットプレイスで販売されているなど危険な支払いカードに関する継続的に更新されるデータフィードにより、オフライン・オンライン両方における詐欺の損失をリアルタイムで防止します。侵入された支払いカード（Compromised Payment Card）のフィードがあれば、金融機関は共通の購買時点分析を行うことができ、支払いカードのデータをさらす侵入行為を正確に検出、そしてカードのポートフォリオをお守りします。

ダークウェブのモニタリングでミュール活動を防止
ミュール口座を広くデータ駆動型で可視化することで、金融機関はミュール口座が関わる不正な金融取引を検出し必要な予防措置を取る能力が得られます。ダークウェブインテリジェンス（Dark Web Intelligence）は、氏名、メールアドレス、銀行口座番号、電話番号を含むミュール口座のすぐに活用できる詳細データフィードを金融機関にまたがって提供します。

この脅威の情報によって、ミュール口座が顧客口座と一致するか、あるいはミュール口座がサードパーティーの金融機関と関係があるか確認し、新規口座開設申請をミュールデータに対してスクリーニングができます。

準備はよろしいですか？ お問い合わせはinfo@niceactimize.comにどうぞ。〉