LexisNexis®
RISK SOLUTIONS

ケーススタディ

グローバル銀行がLexisNexis® Risk Solutionsと連携して、金融取引における不正トラフィックを直ちに低減

LexisNexis® ThreatMetrix®の動的なデジタルアイデンティティ・インテリジェンスが高速認証情報テストをブロックし、正規の顧客にスムーズな体験を提供

概要

会社

グローバル銀行

要件

- 金融取引の不正トラフィックの正確な検出と防止
- 資金管理アプリケーションへのシームレスなデータ転送の確保
- 正規顧客にとっての余分な手続きの低減

ソリューション

グローバル銀行は、LexisNexis ThreatMetrixの動的なデジタルアイデンティティ・インテリジェンスを活用して、金融取引のトラフィックに対するほぼリアルタイムの可視化を実現しています。これにより、不正トラフィックのブロックとユーザーの認証情報の保護を可能にし、金融アプリケーションを利用している顧客にスムーズな体験を提供することができます。

最終結果

- 金融取引から130万件の不正取引をブロック
- 50万人以上の信頼できるユーザーを正確に認証し、スムーズな顧客体験を促進
- 9万件の認証情報をボット攻撃から保護

ケーススタディ

概要

グローバル銀行の商業銀行部門が金融取引を使用して顧客の取引データを資金管理アプリケーションに転送する際に、その取引が新たなサイバー犯罪の温床となることを確実に阻止する必要がありました。

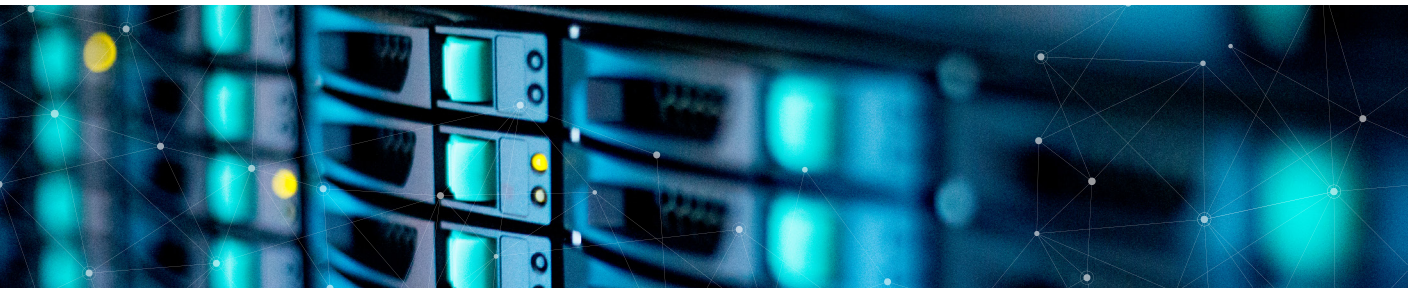
グローバル銀行はLexisNexis® Risk Solutionsと連携することで、以下を実現しています。

- サイバー犯罪者が金融取引で盗難IDをテストすることを確実にブロック
- 金融取引における顧客のトラフィックに対するより明確な可視化を実現
- 信頼できるリピートユーザーの顧客体験を向上

ビジネス上の問題

多くの企業や消費者は、予算編成、請求書の追跡と支払い、取引の分類をすべて一か所で行うことで財務の包括的な全体像を把握するのに役立つ資金管理アプリケーションを使用して損益を管理しています。顧客は、資金管理アプリケーションを介してユーザー情報を送信することで、そのアプリケーションを銀行とクレジットカード口座に関連付けています。そして、取引データは銀行からインターネット上で金融取引を介してアプリケーションに転送されます。多くの銀行はOpen Financial Exchange (OFX)を使用しています。これはオープンな標準APIであり、バンキング、株式ポートフォリオ、予算編成、資金管理などに使用されるデータを金融アプリケーションに提供します。

グローバル銀行は、金融取引で発生する活動に対する洞察を提供し、正規の顧客に余分な手間をかけずに不正トラフィックをブロックできる不正対策ソリューションを必要としていました。



ケーススタディ

グローバル銀行でサーバーのクラッシュが始まったときに、その金融取引は高速の認証情報テストを実行していたサイバー犯罪者からの攻撃を受けやすいことが明らかになりました。盗まれた認証情報が検証されると、サイバー犯罪者は多くの場合、さらなる犯罪を重ねるためにそれらを使用したり、ダークウェブ上で販売したりします。グローバル銀行は、金融取引で発生する活動に対する洞察を提供し、正規の顧客に余分な手間をかけずに不正トラフィックをブロックできる不正対策ソリューションを必要としていました。

グローバルネットワークの力を活用

LexisNexis® Digital Identity Network® はログイン、決済、新規アカウントの申請などの数百万件に及ぶ日常的な消費者とのやり取りからのグローバルな共有インテリジェンスを収集および処理しています。LexisNexis® ThreatMetrix® 製品の機能とDigital Identity Networkからの情報を利用して、同社はデバイス、場所、匿名化された個人情報との間の無数の関連性を分析することで、各ユーザーに対する一意のデジタルアイデンティティを作成することができます。この信頼できるデジタルアイデンティティから逸脱した行動はほぼリアルタイムで正確に特定することができ、銀行には潜在的な不正に関する警告が発せられます。

グローバル銀行は、LexisNexis ThreatMetrixの動的なデジタルアイデンティティ・インテリジェンスを活用して、金融取引のトラフィックに対するほぼリアルタイムの可視化を実現することで、不正トラフィックのブロックとユーザーの認証情報の保護を可能にし、金融アプリケーションを利用している顧客にスムーズな体験を提供することができます。

ケーススタディ

盗まれた認証情報とアイデンティティテスト攻撃を検出

グローバルデータの侵害が引き続き進化するサイバー犯罪の主流となっており、サイバー犯罪者は盗まれた大量のID認証情報に簡単にアクセスすることができます。サイバー犯罪者は多くの場合、自動ボット攻撃を使用してこれらの認証情報の大量テストを実行し、既存のデータを検証および補強してより完全な盗難IDを作成するため、今まで以上に、デジタル企業が取引相手を正確に把握することが難しくなっています。

LexisNexis® Risk Solutionsは、信頼できるユーザーとサイバー犯罪者のデジタルアイデンティティとの間の行動上の変則性を正確に特定することで、これらの認証情報テスト攻撃（たとえサイバー犯罪者がその速度を調整して正規の顧客のトラフィックのように見せかけようとしても）を検出することができます。

- **LexisNexis Risk Solutionsはコンテキストベースの情報を使用して、通常の業務時間中にユーザーの行動分析を実施してボット攻撃を検出し、**攻撃中にこれらのデータと収集したデータを比較します。これにより、同銀行はユーザーのログイン/取引の時点で瞬時に人間とボットを識別することができます。
- **詳細な接続分析テクノロジー**によって、同銀行は隠れプロキシやVPNなどのテクノロジーの使用を検知し、グローバルなアイデンティティデータに基づき、真のIPアドレス情報、地理的位置、各イベントのその他の属性を確認することができます。
- **スマートID**では、クッキーの削除、プライベートブラウジングの使用、他のパラメータを変更してデバイスフィンガープリンティングの迂回を行うリピートユーザーを特定します。これはリピートユーザーの検出を向上させ、誤検出を低減し、同じデバイスを使用して複数の決済を行っている可能性があるサイバー犯罪者を特定するのに役立ちます。

LexisNexis® RISK SOLUTIONS

詳細については、risk.lexisnexis.co.jp/corporations-and-non-profits/fraud-and-identity-management にアクセスしてください