opentext™ | Cybersecurity

お客様事例

金融サービス企業

ArcSight Intelligence によって、ビジネスクリティカルな取引アルゴリズムが保護されます。

小規模のセキュリティチームの生産性が向上

金融サービスのような規制の厳しい業界では、機密データの保護が重要視されます。この組織は、知的財産 (IP) の差別化の要因となっている特定の取引アルゴリズムを特に保護したいと考えていました。同社のセキュリティアーキテクトは別の課題を認識しており、次のように発言しています。「私たちのセキュリティチームは少人数でありながら、さまざまな優先事項を抱えています。適切な異常検出の必要性は理解しており、ベンダーから提供される「ブラックボックス」のようなメッセージではなく、真の分析結果を得られるソリューションが必要でした。しかも、オープンソースソリューションを試してみたところ、リソースを大量に消費していることがわかりました。簡単にメンテナンスできるものが必要でした」

「ArcSight Intelligence は、認証に失敗しているにもかかわらず特定のリソースへのアクセスに成功しているローカルサービスアカウントを特定しました。これは偵察活動であり、データ盗難につながる可能性があったと考えています。ArcSight Intelligence のおかげで、現在調査中です」

セキュリティアーキテクト
金融サービス企業

ArcSight Intelligence by OpenText™ は分析主導のアプローチを採用しており、ベースライン作成とリスク評価のプロセスを使用して、セキュリティチームが脅威を検出、トリアージ、調査、対応するうえでの効率とスピードを向上できるようにします。直感的な Web ベースのダッシュボードにより、潜在的なリスクが最も高いアラートがどれなのかを迅速かつ簡単に特定できます。

ArcSight Intelligence により未知の脅威ベクトルを特定して無力化

ArcSight Intelligence の導入形態は SaaS モデルであるため、保守とサポートの心配は不要です。初期の分析結果では、使われなくなったターゲットアプリケーションに接続されている複数のアクティブなサービスアカウントが存在するという、未知の脅威ベクトルが特定されました。これらの脅威は無力化された後に調査され、同社は IP の安全性を確保できるようになりました。

同社は ArcSight Intelligence のデータソースを拡張し、すべてのネットワークデバイスをプロファイリングして、カバーする範囲を広げることを計画しています。

概要

業種
金融

所在地
米国

課題
高度な異常検出機能を導入して、ビジネスの成功の中核を成す機密性の高い取引アルゴリズムを保護

製品とサービス
ArcSight Intelligence

主な成功要因

- 保守とサポートが容易な SaaS の導入
- 分析主導のセキュリティアプローチにより、小規模のチームの生産性が向上
- 未知の脅威ベクトルを特定して無力化

opentext™ | Cybersecurity

768-JA0031-002 | O | 12/23 | © 2023 Open Text