Centripetal

CASE STUDY

金融サービス会社、よりスマートな脅威インテリジェンスによって成功を収める!

会社概要

この金融サービス会社は世界経済 において重要な役割を果たしています。
同社は、自社が絶えず多くの多様な敵対グループの標的にされていることから、自社が確実に保護されることに重点を置いています。
自社データが安全であることを確実にしなければならないため、ネットワークセキュリティはこの組織の優先事項です。

● 脅威ランドスケープ

脅威ランドスケープは常に拡大と適応を続けています。サイバー脅威は2016年から2017年にかけて2倍になり、トラフィックは223%増加しました。2017年には、セキュリティインシデントの検出数は2億2300万件超まで跳ね上がり、平均すると1日当たり611,141件になりました。

数百万の悪意のあるユーザが数十億の合法的なユーザの中に隠れているため、サイバーセキュリティシステムは今日のサイバー攻撃の幅に対応することができなければなりません。このソリューションが実施されなければ、次の侵害がすぐにやって来る可能性があります。

会社のセキュリティスタックに対する侵害を予測する際の最も大きな要因の1つは、その組織がどの業種に根差しているかに基づいています。厳しい規制下にある金融サービスなどの業種では、1人当たりのデータ侵害のコストは全体平均よりも著しく高くなっています。実際、金融サービス組織は常に、フィッシング攻撃、URL/電子メールによるマルウェア攻撃、及びスパムのような脅威の標的にされる上位10業種の1つとなっています。

● 課題

この金融サービス会社は、全米各地の様々な自社データセンタにあるインフラに対する敵対者の変化を管理することができていませんでした。
この組織は、自社のセキュリティチームが無関係の又は不正確な脅威インテリジェンスソースから見つけた高いS/N比（信号対ノイズ比）を補正する一方で、自社に対する特定の脅威の状況認識を得る方法を必要としていました。

金融サービス組織として 、この会社は自社が直面しているサイバー攻撃による高いリスクを認識しており、顧客記録のプライバシー及び自社ネットワークの完全性を確保することを望んでいました。この組織のセキュリティチームは、自社ネットワークのトラフィックの完全相関データ並びに関連する脅威インテリジェンスをリアルタイムで運用可能にする方法を提供するソリューションを必要としていました。

金融サービス組織として、この会社は自社が直面しているサイバー攻撃による高いリスクを認識しており、顧客記録のプライバシー及び自社の重要インフラの完全性を確保することを望んでいました。

この組織のセキュリティチームは、以下を提供する高度なソリューションを必要としていました。

- **絶えず更新されるサイバー脅威インテリジェンスの完全相関データ**
- **数十億のIOCに対するノイズ及び誤検知（フォールスポジティブ）を自動的にフィルタ除去できる機能**
- **強化されたSIEM脅威ダッシュボードを構築するためのアナリティクス及びデータ**

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

● ソリューション

Centripetalは、この組織が自社ネットワークを防御するためにどのソース及びタイプの脅威インテリジェンスが使用されるかを制御する方法を提供しました。
また、このソリューションにより、セキュリティチームは全てのデータセンタ拠点に対する迅速なインシデントレスポンス 及びリアルタイムの脅威ランドスケープ可視性を提供することに重点を置くことが可能になりました。

リアルタイムの脅威インテリジェンスフィード及びアナリティクスの機能と組み合わせたCentripetalの高度なパケットフィルタリングは、この組織のセキュリティチームが自社ネットワークを防御するためにどのソース及びタイプの脅威インテリジェンスが使用されるかを制御する方法を提供しました。

Centripetalは、重要度評価、信頼性、タグ、及び深いコンテキスト関連付けを活用して、警告及びブロックのためのきめ細かいポリシーを定義します。
Centripetalのソリューションにより、この組織は自社ネットワークのリアルタイム保護のために自社調査、オープンコミュニティ及びプライベートコミュニティ、並びに第三者ベンダーからの脅威インテリジェンスを入力することが可能になりました。

このソリューションにより、この組織のセキュリティチームは、これまで以上に迅速なインシデントレスポンスを提供すること及び自社の複数のデータセンタ拠点にわたる脅威ランドスケープに対するリアルタイムの可視性を得ることに調査リソースを集中させることができ ました。
さらに、このソリューションは、脅威インテリジェンスを運用可能にすることで、動的な脅威インジケータの即時のエンフォースメントを可能にしました。

● 持続的な脅威は持続的な保護を必要とする

Centripetalは、高忠実度のインジケータを用いた大規模で動的なポリシーにより、リアルタイムでネットワークをアクティブに保護することを可能にします。

Centripetalのソリューションは、ネットワークパフォーマンス又はユーザエクスペリエンスを低下させることなく、**数百万のルールを用いてサイバーセキュリティポリシーをフルラインレートで実施します**。このソリューションが展開されると、その広範なカバー範囲のおかげで、この会社のアナリストは以前には気付かれなかった脅威を検出することができるようになりました。以前のサイバーセキュリティシステムでは、自社のニーズを満たすように拡張することができませんでした。

● 脅威インジケータ照合

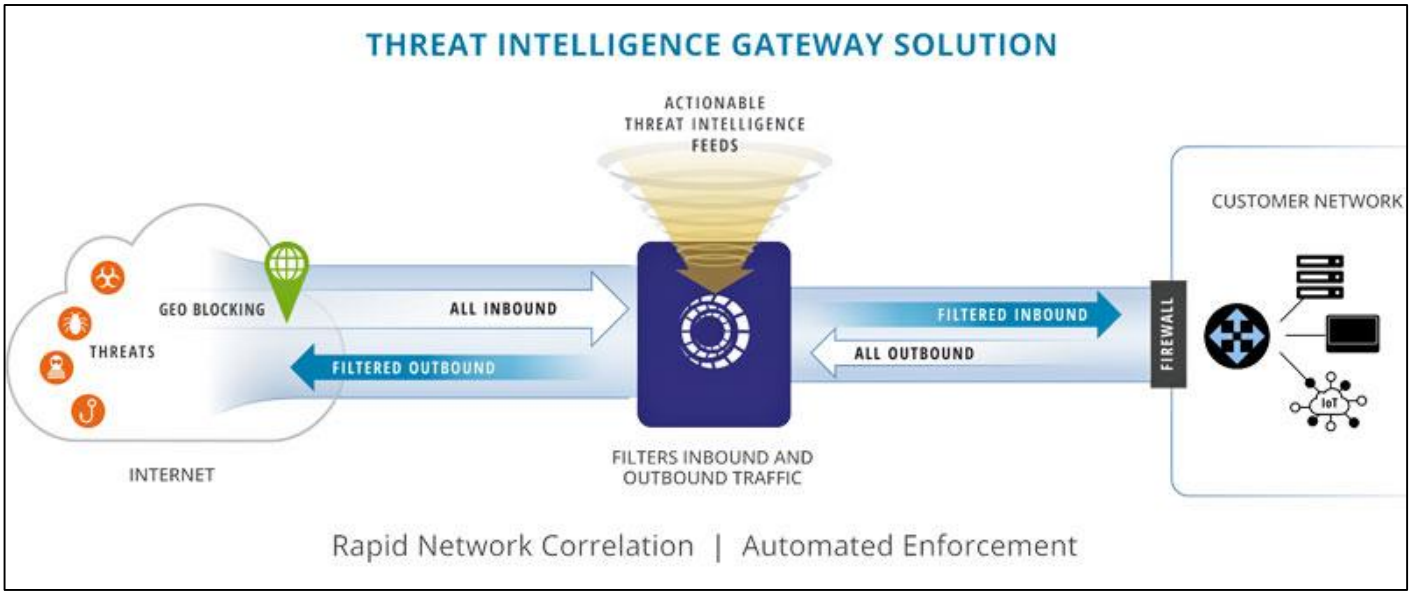
Centripetalは、ネットワークに関する研究を行っているセキュリティ運用センタ(SOC)チームにリアルタイムのフィードバックを提供しました。
複数の拠点におけるネットワーク上の既知の内部ホストに対するアクティビティに起因していたIOC(Indicator of Compromise: 侵害指標)が特定されました 。
このことは、インシデントの深刻度に関するより迅速な協力及びインシデントレスポンスチームによる対象を絞った取り組みにつながりました。

● 結果

この金融サービス会社は、自社ネットワークの保護において継続的で明らかな成功を収めています。
このソリューションの 展開により、インバウンドとアウトバウンドでのデータの完全相関が可能になっています。この統合 ソリューションは、この組織が以前には検出されなかったアウトバウンドネットワーク脅威を見つけることを可能にし、以前のセキュリティソリューションにはなかった可視性と制御のレベルを実現しました。

この組織は、自社ネットワーク上の悪意のあるホストを特定し、ネットワークを 切断することなしに既知のバッドアクターへのアウトバウンド通信をブロックすることができました。
このインテグレーションにより、セキュリティチームはより迅速に脅威に対応し、脅威データに従って行動することができました。

このアクティブ脅威ブロックソリューションにより、この顧客は自社ネットワークの体系的な制御を取り戻し、
自社データをセキュアに維持することが可能になりました。



コーネットソリューションズ株式会社
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

※本資料はCENTRIPETAL NETWORKS社が公開している英文資料に基づいて、弊社が翻訳、作成した和文資料です。英文と和文資料に差異がある場合には、英文資料が優先されます。

