導入事例

金融会社は、攻撃対象領域全体のインシデントを相関させるためのOpen XDR搭載SOCを構築します

Stellar CyberのOepn XDRは、自動化された異常検出と応答を提供し、攻撃応答時間を短縮しながらアナリストの生産性を向上させます

米国中部に拠点を置く金融サービス会社は、ネットワークセキュリティの脅威を検出して対応する能力についてますます懸念を抱いています。 長年にわたり、同社はファイアウォール、ID管理、ログ集約、IDS、IPS、SIEM、およびその他のセキュリティツールを階層化してきましたが、ツールのコレクションが増えるにつれて、分析スタッフの負担も増えました。 監視するセキュリティコンソールは複数あり、アラートの量は、スタッフが実際の脅威と誤った脅威を区別するのが困難であり、実際の脅威に迅速に対応することは言うまでもありませんでした。

STELLAR CYBER®

私のアナリストチームはアラートに溺れていました”と同社のCISOは述べています。”管理するには情報が多すぎ、誤検知が多すぎて迅速に対応できませんでした。 Experian、Targetなど、侵害を検出するのに数か月かかる場所でのエクスプロイトについて聞いたことがあり、その立場になりたくありませんでした。”

導入前

アラート倦怠感
偽の脅威を追いかけて無駄な時間

無駄な時間
チームは対応手順の作成に時間を費やしました

マルチインターフェース
使用中のツールごとに個別のコンソールを参照するようにユーザーに強制しました

STELLAR CYBER 導入後

包括的なダッシュボード
単一画面からのインシデント相関

効率的
アナリストのトレーニング時間を節約

機械学習
時間の経過とともにその検出および応答機能を改善する

統合
NDR、UEBA、NG
SIEM、ML、IDS、Sandbox 、SOAR – 単一のインターフェース

“…システムが適切な情報を適切なタイミングで収集し、管理可能な形式に抽出し、より大きな違反が進行中であることを通知する実際のインシデントからアラートを分離し、自動的に対応する方法について考える新しい方法が必要でした。 それら。 Stellar Cyber Open XDRプラットフォームは、これらの機能を提供できるように見えました。”

and I didn't want to be in that position."

Stellar CyberのOpen XDRを選択

彼が考えられる解決策を検討したとき、チームは、アナリストチームが最大の効率で実行できるように、情報を1つの画面に統合し、データ収集、脅威のハンティング、および応答を自動化するソリューションが必要であることに気付きました。 Stellar Cyberの次世代セキュリティ運用プラットフォームは、競合他社よりも際立っていました。

"他のソリューションで見たのは、同じ大量のデータであり、アナリストがすべてのアラートを追跡するのと同じ要件でした"とCISOは述べています。"私たちは複雑さの別の層を必要としませんでした。 システムが適切な情報を適切なタイミングで収集し、それを管理可能な形式に抽出し、より大きな違反が進行中であることを示す実際のインシデントからアラートを分離し、それらに自動的に対応する方法について考える新しい方法が必要でした。 Stellar Cyber Open XDRプラットフォームは、これらの機能を提供できるように見えました。"

概念実証の試行中に、チームはダッシュボードからのアラートがはるかに少ないことに気づきました。 Stellar Cyberに脅威がないことを懸念して、チームはXDRプラットフォームが警告しなかったいくつかの認識された脅威を追跡し、それらが実際の脅威ではないことを発見しました。 Stellar CyberのAIと機械学習テクノロジー、および複数のセキュリティインシデントを相互に関連付ける機能により、実際の脅威から誤った脅威を取り除くことができました。"これは信頼の飛躍です"とCISOは述べています。"私たちはすぐにソフトウェアを信頼し、それが私たちのために決定を下せるようにすることを学びました。"

InterFlow™の活用

Stellar CyberのInterFlow™テクノロジーは、実際には複数のインシデントを相互に関連付けて、他のソリューションが見逃しているセキュリティ攻撃をキャッチします。 たとえば、信頼できるユーザーから深夜にログインしてもアラートは発生しない可能性がありますが、そのインシデントは、ロシアのドメインにデータを盗み出すというユーザーのリクエストに関連してアラートを発生させます。

> "...チームは、古いシステムで見られた脅威に対抗するための対応手順を作成するために多くの時間を費やす必要がありましが、StellarCyberはその負担を排除します。"

Open XDRプラットフォームのグローバルダッシュボードは、脅威のキルチェーン全体を明らかにし、その自動化されたデータ収集、検出、調査、および対応テクノロジーにより、アナリストチームは誤検知を追跡するために多くの時間を費やす必要がなかったため、トレーニングがはるかに簡単になりました。

"通常、チームは古いシステムで見られた脅威に対抗するための対応手順の作成に多くの時間を費やす必要がありましたが、Stellar Cyberはその負担を排除します"とCISOは述べています。"ソフトウェアはそれ自体で応答し、機械学習を使用して脅威を発見する能力を向上させます。 その結果、当社のセキュリティ機能は時間の経過とともにますます強力になっています。"

Stellar Cyberプラットフォームのもう1つの利点は、NDR、UEBA、NG SIEM、ML IDS、Sandbox、SOARなどのコアセキュリティ機能を単一のインターフェイスに統合します。 他の製品では、使用中のツールごとに個別のコンソールを参照する必要がありますが、Stellar Cyberは、単一の画面の下で利用できるフル機能のセキュリティワークベンチを提供します。

成功の上に構築する

Stellar Cyberは、一般的なサードパーティのセキュリティツール（EDR、ファイアウォールなど）からのデータも統合および解釈するため、完全なソリューションです。”物理資産と仮想資産、コンテナ、エンドユーザー、クラウドプラットフォームなど、潜在的な脅威の場所すべてからデータを収集するため、全体像を把握できます”とCISOは述べています。” 利用可能なすべてのソースから情報を抽出し、それをキュレートし、重要なデータについて決定を下すプラットフォームの機能は、他のソリューションとは一線を画しています。”

この金融サービス会社にとって、Stellar Cyberは、セキュリティチームの生産性を高めるために誤検知と誤検知を削減しながら、同社の次世代セキュリティインフラストラクチャの強固な基盤を形成しました。 チームの平均検出時間（MTTR）は20分の1に短縮され、攻撃に対応する平均時間は8分の1に短縮されました。

Stellar Cyberを使用すると、企業のアナリストチームは、脅威を数日または数週間ではなく数秒で見つけて対応できるため、セキュリティの認識と保護の最前線に立つことができます。

> **“利用可能なすべてのソースから情報を抽出し、それを収集・整理し、重要なデータについて決定を下すプラットフォームの機能は、他のソリューションとは一線を画しています。”**