導入事例

公的機関は、新しいOpen XDRセキュリティオペレーションセンターでセキュリティを一元化します

Stellar Cyberは、キルチェーン全体にわたって可視性と制御を提供します

北東部に拠点を置く州政府機関は、最近の都市へのサイバー身代金攻撃を考慮して、最も厳格なセキュリティ体制を確保したいと考えていましたが、複数のアプリケーションを統合し、脅威に自動的に対応するセキュリティ運用ソリューションが必要でした。 Stellar CyberのOpen XDRプラットフォームは、アナリストの生産性を高めながら包括的なセキュリティを提供する新しいソリューションの基盤を形成しました。

STELLAR CYBER®

“役に立たない情報が殺到していたため、迅速に対応できませんでした”と同機関のCISOは述べています。“SIEMやIDS / IPSからログ集約やID管理まで、個別のセキュリティアプリケーションに大金を費やしていましたが、脅威に迅速に対応するために必要な情報をまだ取得できていませんでした。”
management, yet we still weren’t getti

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

高コスト

石畳のソリューションは高価でした

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

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

時間とお金を節約し主要な指標を改善します

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

合理化

キルチェーンは、アナリストに実際の脅威に対応する方法を示しています

“Stellar CyberのXDR キルチェーンダッシュボードには、適切な情報が適切なタイミングで表示されます。 このプラットフォームにより、1つのインターフェースで数10の緊密に統合されたセキュリティ機能に1つの価格でアクセスできるため、相関するインシデントを簡単かつ迅速にドリルダウンできます。”

間違った情報の収集

何年にもわたって、エージェンシー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、個別のツールのコレクションが増えているため、分析スタッフの負担が増え続けています。 監視するセキュリティコンソールは複数あり、誤検知に関するアラートが多すぎたため、チームはほとんどの時間を偽の脅威の追跡に費やしました。実際の脅威に対応するには数日から数週間かかりました。

“役に立たない情報が殺到していたため、迅速に対応できませんでした”と同機関のCISOは述べています。 “SIEMやIDS / IPSからログ集約やID管理まで、個別のセキュリティアプリケーションに大金を費やしていましたが、脅威に迅速に対応するために必要な情報をまだ取得できていませんでした。”

Stellar CyberのOpen XDRソリューション

彼が考えられる解決策を検討したとき、CISOは、アナリストチームが最大の効率で実行できるように、複数の脅威ベクトル（クラウド、物理および仮想資産、ネットワーク、エンドポイント）からの情報を単一の画面に統合するセキュリティ運用システムが必要であることに気付きました。

“Stellar Cyberのダッシュボードには、適切な情報が適切なタイミングで表示されます”とCISOは述べています。 “このプラットフォームでは、1つのインターフェースで数10の緊密に統合されたセキュリティ機能に1つの価格でアクセスできるため、相関するインシデントを簡単かつ迅速にドリルダウンできます。”

新しいシステムは、政府機関が使用していた既存のすべてのセキュリティツールへのアクセスを提供する必要もありました。 Stellar CyberのOpen XDRソリューションは、競合他社よりも際立っていました。

“ダッシュボードには、適切な情報が適切なタイミングで表示されます”とCISOは言います。 “セキュリティプラットフォームにより、NDR、UEBA、NG SIEM、ML、IDS、Sandbox、SOARなどのコアセキュリティ機能に1つのインターフェイスで1つの

> “製品の機械学習の側面により、脅威への対応がますます向上するようになります。”

価格でアクセスできるため、時間と費用を大幅に節約し、主要な指標を改善できます。”Stellar Cyberプラットフォームも包括的です。ネットワーク、エンドポイント、クラウド、コンテナ、仮想化された攻撃ベクトルに対応する人気のあるサードパーティツールから有用なデータを収集するため、アナリストはキルチェーン全体の全体像を確認できます。 また、アナリストが実際の脅威に集中できるように、誤検知を却下するのに十分なほど賢いです。

さらに、Stellar Cyberは、AIと機械学習テクノロジーを活用して、時間の経過とともに検出機能と応答機能を実際に改善します。 “製品の機械学習の側面により、脅威への対応がますます向上するようになります”とCISOは述べています。インシデントの相関関係も重要な属性でした。 Stellar CyberのInterFlow™テクノロジーは、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、深夜に管理者がログインしてもアラートは発生しない場合がありますが、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。

“通常、私たちのチームは、古いシステムで見られたさまざまな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しましたが、Stellar Cyberはその負担を排除します。 この製品は、私たちにとって何が重要かを学習し、キルチェーン内でその情報を提示して、アナリストに正確に対応する方法を示します。”マルチテナンシーは別の利点でした。 “私たちには20を超える部門があり、全体的なセキュリティ体制を把握して1つの部門を別の部門と比較できるように、それらを個別のユニットに分割できる

ことが非常に重要です”とCISOは付け加えました。 “Stellar Cyberには、箱から出してすぐにマルチテナンシーが組み込まれています。”

実際の結果

もちろん、その証拠はそれが実際にどれだけうまく機能したかということでした。 概念実証の試行中に、政府機関のセキュリティチームは、Stellar Cyber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。 プラットフォームに脅威がないことを懸念して、チームは警告されていない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の機械学習テクノロジーと、一見ランダムに見える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アラートを取り除くことができました。 Stellar Cyber Open XDRプラットフォームは、本番環境で使用されると、代理店のアナリストの平均検出時間（MTTD）を20分の1に短縮し、平均応答時間（MTTR）を8分の1に短縮しました。この公的機関のために、Stellar Cyberは、明確で使いやすいインターフェースで実際の脅威を特定するセキュリティインフラストラクチャの基盤を形成しました。 アナリストの生産性が向上し、エージェンシーがチームのトレーニングに費やす時間が大幅に短縮され、アナリストは実際の脅威にはるかに迅速に（数日または数週間ではなく数秒で）対応できるため、エージェンシーはサイバー身代金攻撃から保護されます。

> **“通常、私たちのチームは、古いシステムで見られたさまざまな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しましたが、Stellar CyberのOpen XDRはその負担を排除します。 この製品は、私たちにとって何が重要かを学習し、キルチェーン内でその情報を提示して、アナリストに正確に対応する方法を示します。”**