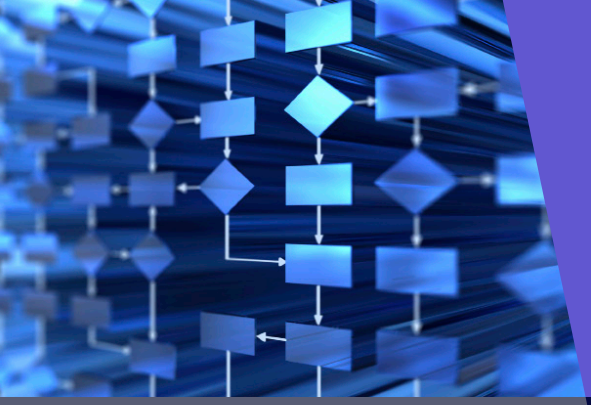
導入事例

医療機関がOpen XDRを導入–リスクを軽減し、パフォーマンスを向上させ、コストを大幅に削減

Stellar Cyberは点をつなぎ、すべての実際の脅威を表示し、アラートの疲労を劇的に削減します

南東部に拠点を置く複数施設の医療機関は、最近広く公表されている患者の請求情報の違反に照らして、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。HIPAAの要件と患者の財務情報を保護する必要性の間で、組織は、Stellar CyberのOpen XDRプラットフォームが見つかるまで、セキュリティがますます複雑で費用のかかる提案であることに気づきました。

STELLAR CYBER®



“私のアナリストチームは過労でした”と同社のCISOは言い、私たちはSIEMおよびIDS / IPSからログ集約およびID管理まで1ダース以上の個別のツールに大金を費やしていました。脅威を追跡し、管理レポートを作成するには、複数のコンソールから情報を取得する必要がありました。もっとシンプルで統合されたものが欲しかったのです。”

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

複数ツール

分析スタッフの負担が増える

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

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

生産性の向上

ソフトウェアは誤った脅威を取り除きます

効率的

アナリストのトレーニング時間を節約

“…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。”

アラート疲労

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、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、チームは誤検知の追跡に多くの時間を費やしました。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。

“私のアナリストチームは過労でした”と同社のCISOは言います。”そして、SIEMやIDS / IPSからログ集約やID管理まで、12以上の個別のツールに大金を費やしていました。 脅威を追跡して管理レポートを作成するには、複数のコンソールから情報を取得する必要があり、よりシンプルで統合されたものが必要でした。”

Open XDRの選択

彼女が考えられる解決策を検討したとき、CISOは、組織が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して、アナリストチームが最大の効率で実行できるようにするセキュリティ運用環境が必要であることに気付きました。Stellar Cyberのインテリジェントな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。

“Stellar Cyberを見ると、キルチェーン全体の脅威を特定する非常に明確で効率的なダッシュボードが見つかりました”とCISOは言います。 “また、プラットフォーム全体と、1つの傘の下で1つの価格で数10の緊密に統合されたコアセキュリティ機能を提供する機能も気に入りました。”

コンセプトの証明

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、組織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。

“機械学習は新しいフロンティアですが、セキュリティソリューションが実際の脅威を発見する上でますます良くなることを可能にします”とCISOは言います。 “ソフトウェアを信頼し、それ

> “Stellar Cyberを見ると、攻撃対象領域全体で脅威を特定する非常に明確で効率的なダッシュボードが見つかりました。”

があなたに代わって意思決定を行えるようになると、生産性が劇的に向上します。”

アナリストの生産性の向上

イベ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、複数のイベ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、深夜に病院の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、そのイベントは、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と相関しており、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”とCISOは言います。

“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。”

Stellar Cyberは完全なソリューションです。“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”とCISOは述べています。

マルチテナンシーは別の利点でした。“私たちには20を超える診療所と病院があり、全体的なセキュリティ体制を把握して1つのサイトを別のサイト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。

このヘルスケア組織では、Stellar CyberがEDRシステムと統合しながら、古いセキュリティツール（ログアグリゲーターなど）を置き換え、脅威情報を明確で使いやすいインターフェイスで提示しています。 アナリストの生産性が向上し、組織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対応できます。 実際、平均検出時間（MTTD）は20倍以上短縮され、平均応答時間（MTTR）は8分の1に短縮されました。

全体として、Stellar Cyberは、このヘルスケア組織の次世代SecOpsプラットフォームの基盤を形成し、セキュリティの認識と保護の最前線に置き、会社のアナリストチームが数日または数週間ではなく数秒で脅威を見つけて対応できるようにしました。

“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 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。”