導入事例

inSOC

inSOCは、Stellar Cyber Open XDR NIST800サイバーセキュリティフレームワークベースのツールセットを使用してエンタープライズレベルのソリューションをMSP市場にもたらします

AI主導のテクノロジーがXDRキルチェーンを公開：単一画面の下にあるすべての主要なセキュリティテクノロジーと24時間年中無休のSOCラップアラウンドを組み合わせて、MSPの生産性を大幅に向上させます

inSOCは、管理セキュリティプロバイダー（MSP）および管理セキュリティサービスプロバイダー（MSSP）へのサービスとしてセキュリティオペレーションセンター（SOC）を提供します。inSOCはロサンゼルスに拠点を置き、英国のロンドンとオーストラリアのシドニーに国際オフィスを構えています。同社は、Stellar CyberのOpen XDRテクノロジーを利用してサービスを提供しています。 inSOCは当初AT＆T Cybersecurityを使用して、サービスのセキュリティ情報およびイベント管理（SIEM）機能を提供していましたが、製品が複雑なため、会社は収益性を維持することが困難でした。

STELLAR CYBER®

inSOC

inSOCのCEOであるエリック・ロックウェルは、次のように述べています。”ノイズだけでなく実際の情報を確認するまで、新しいクライアントを立ち上げて展開を調整するのに数か月かかりました。“私たちの目標は、1時間以内に新しいクライアントを立ち上げることができる適切なセキュリティパートナーを見つけることでした。”

導入前

アラート疲労
誤検知が多すぎます

無駄なコスト
大量の偽の脅威を整理するために人的資源が費やされました

限られたオプション
他のSIEMは、ハードウェアへの展開を提供していませんでした

STELLAR CYBER 導入後

合理化
本当の脅威を見つける

マルチテナント
新しいクライアントのオンボーディングが簡単になります

導入が簡単
ハードウェアオプションにより、ユーザーはプラグインしてすぐに使用を開始できます

Open XDR
包括的な可視性を提供し、複雑な攻撃をつなぎ合わせます

統合ツール
アナリストの仕事を簡単にします

“Stellar Cyberがダッシュボードに情報を表示する方法が気に入りました。非常に明確で、チームのスピードを上げるのが簡単でした。”

ただし、inSOCチームが代替案を調査したところ、ほとんど同じことがわかりました。 主な問題は、他のソリューションでは誤検知が多すぎ、必要なセキュリティ機能がすべて提供されておらず、違反を特定するために適切に機能するために面倒な調整が必要だったことです。“そのとき、チームは現在のソリューションでは得られない種類のことを発見しました。”

Stellar Cyberのすべての検出と応答（XDR）に対する考え方も際立っていました。他の製品とは異なり、収集されたデータをキュレートし、ランダムなイベントのように見えるものを相互に関連付けて、誤検知ノイズと実際のアラートの違いを発見するためです。 Stellar Cyberにより、inSOCチームは、サイバーセキュリティフレームワーク、そのポリシー、およびCERTの上位20のセキュリティ制御に基づいて、最も重要な情報にすぐに集中できるようになりました。 チームはテンプレートを作成したので、新しいクライアントをオンボーディングするために必要なのは、環境について簡単な質問をし、簡単なハードウェアセンサーをプロビジョニングして出荷し、その時点から1時間以内に稼働することだけでした。 ボックスはクライアントのネットワークに接続されました。

当然のことながら、Stellar CyberのRBACマルチテナント機能はinSOCに必須でした。“マルチテナンシーがなければ、Stellar Cyberを検討することすらできなかったでしょう”とinSOCのCIOであるジェフ・グリック氏は述べています。“私たちは数十のクライアントをオンボーディングできる必要があり、他のソリューションがそれを行うのを困難または高価でした。”

さらに、グリック氏は、”Stellar Cyberがダッシュボードに情報を表示する方法が気に入りました。非常に明確で、チームのスピードを上げるのが簡単でした”と付け加えています。

Stellar Cyberは、ハードウェアに展開するオプションも提供しました。“他の多くのツールは仮想化に基づいており、仮想化環境から抜け出したいと思っていたため、ハードウェアを使用して展開するオプションが気に入りました”とグリック氏は言います。私たちは、さまざまな仮想化プラットフォームを備えた環境に足を踏み入れていました。人々はそれらを正しく構成することができませんでした。クライアントがハードウェアを接続するだけで、すぐに作業を開始できるため、ハードウェアの導入に関してははるかに優れた経験が得られました。”

> “ブルートフォース攻撃に飛び込むことができます... Stellar CyberのOpen XDRが包括的な可視性を提供し、複雑な攻撃をつなぎ合わせる方法により、これらすべてが可能になります...”

Open XDRはセキュリティ分析を簡素化します

Stellar Cyberを試すために、inSOCチームは新しいクライアントをオンボーディングし、彼らの活動のレビューを開始しました。 Stellar CyberのOpen XDR相関機能は、クライアントが不正なリモートアクセス、不正なリモートコントロールツール、デフォルトの管理者名を突破しようとしている人々、ファイアウォールの開いているポートを持っていることをすぐに示しました。 Stellar Cyberはこれらの重要な脅威について警告しましたが、同様に重要なこととして、誤検知については警告しませんでした。

“ブルートフォース攻撃（Windowsログオンの失敗、特権のエスカレーション）に飛び込むことができます。これはすべて、Stellar CyberのOpen XDRが包括的な可視性を提供し、クラウド、エンドポイント、ユーザー、ネットワーク全体で複雑な攻撃を統合し、ログの解析を支援するために可能です。 そして、情報に関する簡潔なレポートを作成するためにネットワーク上で聞いたこと”とグリック氏は言います。“AT＆Tサイバーセキュリティではそれができませんでした。”

製品のネイティブアプリケーションにより、inSOCのアナリストの仕事を容易にするために、ツールの数を簡単に統合できました。 “サイバーセキュリティの予算を適切なものに費やしたかったのです”とロックウェル氏は言います。 “多くの企業が人的資源に大金を費やしており、エリートセキュリティの専門家が多くのありふれたタスクを実行し、誤検知を証明しています。

“さまざまなツールに多額の費用を支払う必要がある場合、競争できるのはエンタープライズ スペースだけです”とロックウェル氏は言います。 “私たちの使命はそれをはるかに超えています。私たちはこれをすべての人に伝えようとしています。お金のために誰もがノーと言ってほしくないのです。 Stellar Cyberはそれを可能にします。”

“さまざまなツールに多額のお金を払う必要がある場合、私たちはエンタープライズ スペースでしか競争できません。私たちの使命はそれをはるかに超えています。私たちはこれをすべての人に伝えようとしています。お金のために誰もがノーと言ってほしくないのです。 Stellar Cyberはそれを可能にします。”