導入事例

EBSCO Industries, Inc.

EBSCOインダストリーズは、一元化された可視性と制御のための社内セキュリティ運用ソリューションを構築します

Stellar CyberのオープンXDRプラットフォームは、ポートフォリオ企業に包括的な可視性と自動化された脅威対応を提供します

アラバマ州バーミンガムを拠点とするEBSCOインダストリーズは、米国で最大の株式非公開企業の1つです。 出版、製造、不動産、情報サービス、保険など、さまざまな業界グループにわたって約40の中小企業（SMB）を所有または管理しています。SMBに対するサイバー攻撃のインシデントが増加し始めると、EBSCOの取締役会はセキュリティ体制を強化したいと考え、CIOのライアン・ロイは効果的なセキュリティ運用ソリューションを構築する手段としてStellar CyberのOpen XDRを選択しました。

STELLAR CYBER®

EBSCO Industries, Inc.

“プラットフォームは本当に私たちのニーズに応えます。 ダッシュボードのレイアウトとすべてのアクティビティのキャプチャ方法は非常に直感的であるため、基本レベルのアナリストをスピードアップしてチーム全体に付加価値を与えるために多くのトレーニングを行う必要はありません。”

導入前

アラート疲労
低効率の運転

散在するリソース
セキュリティ機能を実行するいくつかのリソース

無駄な時間
チームはソリューションのコードを書くのに時間を浪費します

STELLAR CYBER 導入後

機械学習
アラート疲労を劇的に削減

合理化
適切なリソースを使用して、より重大な脅威に焦点を当てる

最小限のトレーニング
アナリストに製品にすぐに慣れさせる

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

“キルチェーン全体を表示することで、Stellar CyberのOpen XDRプラットフォームは、人々をはるかに迅速にスピードアップさせます。 数日対数か月のトレーニングの問題です。 これまでは、CIOとしてのフラストレーションの一部でした。チームがコード、スクリプト、カスタマイズソリューションを作成することは望んでいません。 セキュリティの専門家が意味のある事件や脅威を見て、それらに迅速に対処することを望んでいます。”

STELLAR CYBER

https://jp.stellarcyber.ai

当初、EBSCOには、IDおよびアクセス管理、ファイアウォール、およびその他の基本的なセキュリティ機能を実行する約10のセキュリティツールがありました。 チームに参加したとき、ライアンは、会社にログアグリゲーター、セキュリティ情報およびイベント管理（SIEM）システム、または構造化されたセキュリティオペレーションセンター機能がないことに気づきました。プログラムを成熟させ、ポートフォリオ全体のリスクを軽減するために、チームは一元化された共有サービスを作成し、ポートフォリオ企業にセキュリティを提供しました。 このSOC-as-a-Serviceは、効果的なプログラムの構築に必要な時間を短縮するため、EBSCOは最先端のセキュリティ分析および管理プラットフォームを必要としていました。

“私の目標は、セキュリティ体制を成熟させ、リスクを軽減し、既存の組織に追加の構造を構築することでした”とライアン・ロイは言います。 “チームは、セキュリティ状況の単一のビューに対して、企業のポートフォリオ全体にわたって一元化された可視性を提供するソリューションを構築したいと考えていました。”

Open XDRの選択

チームがソリューションを探し始めたとき、ロイは、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ために、自動化された脅威の調査と対応とともに、EBSCOがセキュリティ体制に関する”全体像”を提示するソリューションを必要としていることに気付きました。 Stellar Cyberは、他の競合他社よりも際立っていました。

“私たちは次世代のSIEMを望んでいませんでした。次世代のSecOpsセンターが必要でした”と彼は言います。 “Open XDRを際立たせたのは、機械学習に基づく分析でした。チームが座って、脅威に基づいて侵害のすべての指標を最初から作成する必要はありませんでした。グローバル企業での以前の仕事で、私はそのような取り組みが5年間にわたって進化するのを見てきました。そして、”Open XDRを際立たせたのは、機械学習に基づく

分析でした。チームが座って、脅威に基づいて侵害のすべての指標を最初から作成する必要はありませんでした。”脅威を特定するためのSIEMシステムのコーディングに重点を置いたチーム。チームは、EBSCOで別のことをしたいと考えていました。それは、オーバーヘッドを削減しながらセキュリティ運用を合理化することで得られる効率を実際に活用できるようにするためです。Open XDRで見たのは、多くの誤検知と誤検知のノイズをカットできる機械学習をテーブルにもたらしたことです。これは真のパラダイムシフトです。”

“さらに、Stellar CyberのOpen XDRプラットフォームのオープン性は、セキュリティツールへの既存の投資を維持できることを意味しました。プラットフォームはすべてのセキュリティ資産からデータをシームレスに取り込みます。 結果として、信頼できる唯一の情報源としてStellar Cyberを信頼しています。”

ロイのチームがStellar CyberのOpen XDRプラットフォームで概念実証の試行を行ったとき、彼らは多くのアラートを受け取っていないことに気づきました。 システムが正しく機能していないことを懸念して、チームは詳細なログ情報を調べ、複数のログイン失敗を発見しました。 通常の分析ツールはこれらの障害について警告を発していたため、チームは詳細なログをさかのぼって数時間作業し、Open XDRが警告を発しなかった理由を理解しました。 結局、失敗したログインは誤検知であることが判明したため、Stellar CyberのOpen XDRは、悪意のあるものとして報告しないという点で正しかった。

“基本的に、人々は彼らの行動を変えなければなりません”とロイは言います。 “サイバーセキュリティにはまだ”特効薬”はありませんが、Starlightの機械学習が低レベルの脅威に対して正確であると信頼することを学んだので、適切なリソースを使用してより洗練された多くの脅威に集中することができました。

> “Open XDRを際立たせたのは、機械学習に基づく分析でした。 チームが座って、脅威に基づいて侵害のすべての指標を最初から作成する必要はありませんでした。”

Open XDRの包括的なダッシュボードインターフェイスと自動化された脅威ハンティングにより、ログを相互に関連付けるためのコードの記述に多くの時間を費やす必要がなく、誤検知や低レベルのアラートの追跡にかかる時間が短縮されたため、アナリストチームのトレーニングがはるかに簡単になりました。

“既存のSIEMがなかったため、多くのデータを見ることに慣れている人を連れて行き、再トレーニングする必要はありませんでした”とロイは言います。 “GUIは本当に私たちのニーズに応えます。 レイアウトとすべてのアクティビティのキャプチャ方法は非常に直感的であるため、基本レベルのアナリストをスピードアップしてチーム全体に付加価値を与えるために多くのトレーニングは必要ありません。これまで、私たちのスタッフは執筆に集中していました。 特定の種類の脅威を調査する方法、つまり実行するプロセスを説明するプレイブック。 キルチェーン全体を表示することにより、Open XDRは人々をはるかに迅速にスピードアップさせます。数日対数か月のトレーニングの問題です。 これまでは、CIOとしてのフラストレーションの一部でした。チームがコード、スクリプト、カスタマイズソリューションを作成することは望んでいません。セキュリティの専門家が意味のある事件や脅威を見て、それらに迅速に対処することを望んでいます。

” Open XDRのデータ相関機能と包括的なダッシュボードも、アラートと応答のプロセスを簡素化しました。 “これで、単一画面からインシデント相関を行うことができます”とロイは言います。 “以前のシステムでは、追跡する必要があるアラートが提供されていましたが、現在では、実際の異常をすばやく表示し、非常に迅速に対応できるシステムがあります。ダッシュボードを壁に設置し、チームでAnalyst1、Analyst2、およびAnalyst3レベルの役割をプレイしています。 3つの層すべてでツールの機能を積極的に使用できます。”

EBSCOにとって、Stellar CyberのOpen XDR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減らしながら、会社のSecOpsインフラストラクチャの強固な基盤を形成しました。 EBSCOは現在、企業資産を保護するために必要な一元化されたセキュリティの可視性と制御を備えています。

> **“以前のシステムは、追跡する必要があるアラートを提供していましたが、現在は、実際の異常をすばやく表示し、それらに非常に迅速に対応できるシステムがあります...”**