導入事例

SOLUTIONS GRANTED
PROTECTING THE PROTECTORS

Solutions Grantedは、Stellar Cyber Open XDRでインテリジェントSOCを強化します

Stellar Cyber Open XDRプラットフォームがバージニアMMSSPに新しい脅威ハンティングパワーを付与

Solutions Grantedは、バージニアを拠点とするマスターマネージドセキュリティサービスプロバイダー（マスターMSSP）です。 最小値や契約のない消費ベースの月次サービス契約を通じて、MSPおよびMSSPに情報セキュリティソリューションを提供します。 現在、同社には500を超えるMSPパートナーがあり、それぞれに30～50の顧客がおり、Stellar Cyberプラットフォームを使用して100,000を超えるエンドポイントを管理しています。

同社は、次の3つの主要な強みを中心に急成長しているビジネスを構築してきました。

- 人：パートナーと協力して作業する訓練を受けたセキュリティ専門家
- プロセス：ゲームを変えるプロセス
- テクノロジー：絶えず変化する脅威を保護、検出、対応するマネージドコントロール

STELLAR CYBER®

SOLUTIONS GRANTED
PROTECTING THE PROTECTORS

“Open XDRプラットフォームでは、すべてが非常に合理化されています。セットアップして、希望どおりに機能するように焦点を合わせるために、トレーニングに1営業日もかかりませんでした。 以前のシステムでは、自分が何をしているかを理解できるようになるまでに1週間以上かかりました。”that roll out over time.

導入前

制限付き
他のSIEMは、バックエンドログデータへのアクセスを許可しませんでした

無駄な時間
学習曲線は貴重な時間を無駄にしました

費用がかかる
エンドポイントごとのモデルは費用対効果が高くありませんでした

STELLAR CYBER 導入後

アクセシビリティ
Syslogとバックエンドデータにアクセスする

合理化
使いやすく、迅速なセットアップ

顧客サービス
フィードバックに対するStellar Cyberの応答は比類のないものです

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

“Syslogとすべてのバックエンドデータにアクセスできるため、独自のアラートメカニズムを作成できました。 IOCは常に変化しており、静的なソリューションでは、新しい脅威に対応して進化し、何らかの形で修復を行うことはできません。Stellar Cyberはそうしました。”

SOCプラットフォームのアップグレード

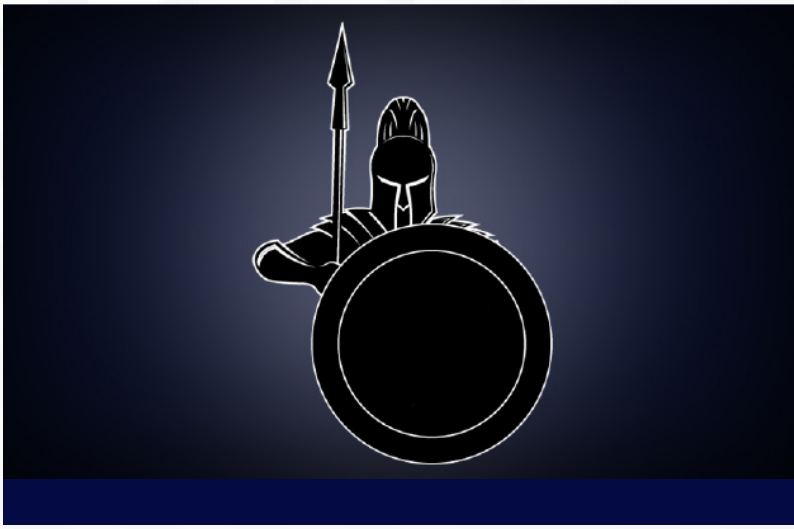
Solutions Grantedは、Windowsイベントログ、ファイアウォールログ、およびsyslogを調べて、侵害のインシデント（IOC）を特定および特定することで多くの作業を行いますが、最初に試したSOCプラットフォームでは、表示する必要のあるデータへのアクセスが許可されていませんでした。

“私たちが使用していたプラットフォームは、SOCを実行するための最低限の必要性を提供しましたが、問題を実際に掘り下げることを可能にするバックエンドログデータへのアクセスが制限されていました”と、Solutions Grantedの脅威インテリジェンスディレクターであるコリー・クラークは述べています。 “Stellar Cyberを試し、ログデータをそこにダンプしたとき、私たちは自分たちが何であり、何になりたいかを見ました。 Syslogとすべてのバックエンドデータにアクセスできるため、独自のアラートメカニズムを作成できました。 IOCは常に変化しており、静的なソリューションでは、新しい脅威に対応して進化し、何らかの形で修復を行うことはできません。Stellar Cyberはそうしました。

従来のプラットフォームとStellar Cyberプラットフォームのもう1つの大きな違いは、Stellar Cyberの使いやすさです。 クラーク氏は次のように述べています。”プラットフォーム内ではすべてが非常に合理化されています。プラットフォームをセットアップし、希望どおりに機能するように焦点を合わせるために、トレーニングに1営業日もかかりませんでした。 以前のシステムでは、自分が何をしているかを理解できるようになるまでに1週間以上かかりました。”

Stellar Cyberの組み込みのマルチテナンシーは、決定のもう1つの重要な要素でした。 クラークはこれを”確固たる要件”と呼んでおり、500を超えるパートナーが管理する理由を簡単に理解できます。 さらに、クラークと彼のチームがプラットフォームの切り替えに関して持っていた予約は、Stellar Cyberチームの応答性を確認したときに、完全に排除されました。 “私は製品を評価するときに一緒に仕事をするのが最も簡単な人ではありません。私はそれを分解します”とクラークは言います。 “1日目から、Stellarチームは私の苦情や推奨事項を吸収し、それらを処理してきました。 私の質問や推奨事項は、製品の次のバージョンで出てきます。 Open XDRプラットフォームは素晴らしいですが、Stellarチームから得た反応は比類のないものです。”

> “Open XDRプラットフォームは素晴らしいですが、Stellarチームから得た反応は比類のないものです。”



Open XDR：攻撃に焦点を合わせる

多くの攻撃がMicrosoft365（MS 365）アプリケーションを標的にしているため、Solutions Grantedのパートナーは特にそれらからの保護を求めていました。 Stellar Cyberを使用すると、チームは組み込みのMS 365分析を使用して自動アラートを取得できましたが、プラットフォームの自動化ツールを使用してクエリを作成することもできました。 “たとえば、MS365では、誰かが管理者として追加されたときにアラートを設定するのに約15分かかりました。 さらに良いのは、Stellar Cyberに新しいアラートを作成したことを報告すると、その状況に対して自動アラートを作成することで製品が改善されることです。”

過去2.5～3年間で、スピアフィッシング攻撃は急速に増加しています。 ハッカーはユーザーの個人的な電子メールアカウントを標的とし、それらを使用して企業のデータにアクセスします。たとえば、フィッシング攻撃には、Googleドライブファイルへのリンクが含まれます。このファイルは、ダウンロードされると、ユーザーのアカウントを乗っ取り、企業サーバーからのデータのエクスポートを開始します。 “私たちは、これらのアカウントの乗っ取りを攻撃し、迅速に修正できるようにしたいと考えています”とクラーク氏は述べています。

ハッカーは、IOCを特定するのが難しいため、IOCをステージングする必要があることを知っています。 Emotetマルウェアの亜種はその一例です。 Solutions Grantedチームは、偽のPOまたは請求書ファイルを使用してシステムに感染するEmotetの新種を発見しました。 “Emotetは昨年の私たちの最大の問題点でした。今年は復活するという記事を目にしました。 Stellar Cyberプラットフォームを使用してそれを見ることができました。 特定のファイルを開いている人を特定し、時間の経過とともに展開するEmotetキャンペーンを特定し始めることができます。

以前は侵害されたEXEファイルでしたが、今では実行中のスクリプトの種類、データのダウンロードと抽出を確認できます。Stellarを使用した簡単なクエリですべてを実行できます。”

Docusignは別の例です。“私たちのSOCアナリストの1人は、顧客がマシンで使用している個人の電子メールを攻撃するZipファイルを介してIOCが入ってくるのを見ました。 Googleドライブへのリンクを介して取得され、Zipファイルをダウンロードしてから、スクリプトの実行を開始します。 この3つの事例を、24時間以内に特定して停止することができ、この攻撃のニュースがメディアに届く24～36時間前に発見されました。”

もちろん、IOCは絶えず進化しており、自動化できない特定のIOCがあります。 このような状況では、SolutionsGrantedはログ分析を使用して攻撃を特定します。 たとえば、ファイルが特定のディレクトリのルートに保存されている場合、データが通常保存される場所ではないため、これは珍しいことです。“私たちはすべてのシフトで積極的に脅威を探し、24時間以内に数週間または数か月間見過ごされていたであろうものを見つけています”とクラークは言いました。

将来の機能強化

これまでのStellar Cyberプラットフォームでの成功に基づいて、クラークと彼のチームは、できるだけ多くのデータをプラットフォームに取り込むことを計画しています。“ファイアウォールをStellarに取り込む予定です。サーバーログ、デスクトップログをもっと取得したいのです”とクラーク氏は言います。“Stellarキルチェーンを使い始めたいです。 できるだけ多くのIOCを特定できるように、そこにできるだけ多くの情報が必要です。 見ることができるデータが多ければ多いほど、私たちは成功します。”

Solutions Grantedは、何百ものパートナーとその顧客を喜ばせることに加えて、Stellar Cyberプラットフォームを使用してビジネスケースを改善しました。 クラーク氏は、”Stellarを使用した取り込みモデルは、以前のプロバイダーを使用したエンドポイントごとのモデルよりも収益性が高いことが証明されています”と述べています。

Open XDRプラットフォームのおかげで、Solutions Grantedは、より優れた脅威検出とIOCへのより迅速な対応により、大規模な顧客ベースにサービスを提供しています。 プラットフォームの購入モデルも会社の収益性を高めていますが、それは単なるアイシングです。

> **“Stellarで使用した取り込みモデルは、以前のプロバイダーで使用したエンドポイントごとのモデルよりも収益性が高いことが証明されています。”**