導入事例

CYFLARE

CyFlareは、Stellar CyberのOpen XDRを使用してサービスとしての卸売SOCサービスを構築します

小規模なMSPから大企業までのマルチテナントソリューションの拡張

CyFlareは、ニューヨーク州ロチェスター郊外に拠点を置くグローバルマネージドセキュリティサービスプロバイダー（MSSP）のトップ100です。 同社は、マネージドセキュリティサービスを中小規模のVAR、MSP、MSSPに卸売りし、包括的で費用対効果が高く、導入が容易なセキュリティオペレーションセンター（SOC）のサービスとしての機能を提供することで顧客に価値をもたらします。 CyFlareは、サービスとしてのSOCサービスの中核として、Stellar CyberのOpen XDRソリューションに依存しています。

STELLAR CYBER®

CYFLARE

XDRにより、アナリストは実際の脅威を非常に効率的に特定できます。 従来のSIEMソリューションは、アプリケーションID、完全なパケットキャプチャ、精選された機械学習ルール、ファイルサンドボックス、12を超える統合された商用脅威インテリジェンスフィードなど、Open XDRが提供する多くのセキュリティエンジンを提供していません。” While many managed 多くの

導 入 前

散在するセキュリティ

問題を解決するために使用されるいくつかのセキュリティプラットフォーム

高コスト

石畳のソリューションは高価でした

限られた機能

他のSIEMオプションは柔軟性を提供しませんでした

STELLAR CYBER 導 入 後

Open XDR

クラウド、エッジ、またはターンキーアプライアンスを介してソフトウェアとして展開します

スケーラブル

小規模から大規模の顧客アカウントに簡単に拡張できます

合理化

実際の脅威を簡単に見つける

事前統合

箱から出してすぐに使えるコア機能により、プラットフォームが正確になります

すぐ反応する

自動化されたセキュリティカバレッジ

“ Open XDRは、コンプライアンスを可能にし、既存のSIEMソリューションに取って代わるだけでなく、他のソリューションよりも高度な脅威ハンティングを提供するハイパーパラノイドセキュリティプラットフォームと呼んでいます。

STELLAR CYBER®

https://jp.stellarcyber.ai

マネージドセキュリティプロバイダーは、12以上の異なる製品からの完全なソリューションをまとめていますが、CyFlareのCEO兼共同創設者のジョー・モリンは、彼にはもっと良い方法があると考えています。

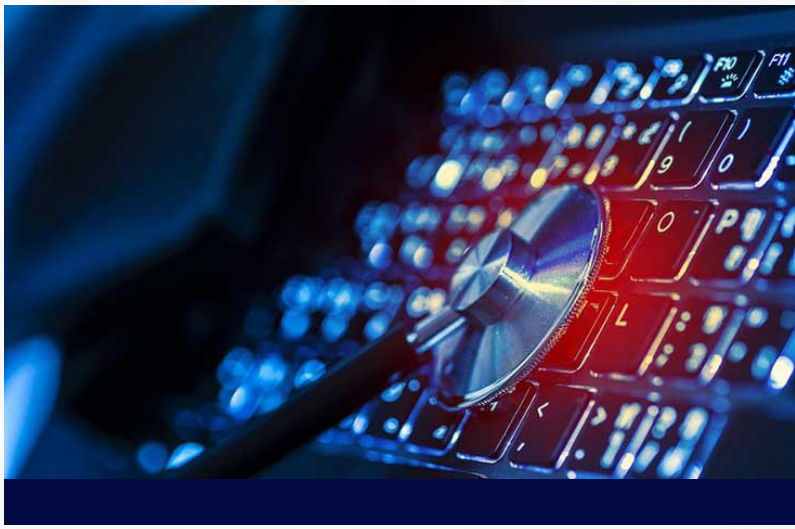
“私は、ボックスの購入からサービスとしてのインフラストラクチャの購入への移行の中心になり、MSPおよびMSSPへのサービスとしてのSOCの最高のプロバイダーになることを望んでいます”とモリン氏は言います。 “独自のSOCをゼロから構築することは、非常に非効率的です。これは、AWSを使用する代わりに独自のデータセンターを構築する人々と同じです。 SOC-as-a-serviceを提供することで、お客様の価値実現までの時間を短縮し、効率を高め、再販業者の利益率を向上させることができます。”

ただし、すべてのSOC製品がSOC-as-a-serviceの優れた基盤となるわけではありません。 一部のセキュリティプロバイダーは、市場プロファイルをファイアウォールまたはSIEMからフルオンSOCに拡張して、Everything Detection and Response（XDR）と呼ばれるものを提供しようとしていますが、これらの取り組みには通常、そのベンダーのセキュリティシステムをすべて購入する必要があります。つまり、 顧客はすでに持ってるシステムを交換する必要があります。 CyFlareは別のパス Open-XDR を選択しました。

“Open XDRプラットフォームにより、製品にとらわれません”とモリン氏は言います。 “お客様は、既存のセキュリティシステムを取り除いて別のベンダーの製品に置き換えることを望んでいません。また、Open XDRを使用すると、既存の機器を維持できます。 このように、Open XDRを使用すると、MSSPがアカウントを簡単に作成できるようになります。”

SOCソリューション要件

CyFlareは、SOC-as-a-serviceの基盤となるプラットフォームを探す際に、典型的な市場をリードするSIEMソリューションを含むいくつかの代替案を検討しましたが、コストが高く、機能が不足しているか、ソリューションの拡張性がないため、実現可能なものはありませんでした。 そのとき、モリンは Stellar Cyberのチーフプロダクトオフィサーであるジョン・ピーターソンと連絡を取りました。



まず、Stellar CyberのOpen XDRソリューションが最初です。市場に出回っているOpen XDRの真のイノベーター。 クラウド、エッジ、またはターンキーアプライアンスを介してソフトウェアとして展開され、顧客が既存のセキュリティハードウェアを交換する必要はありません。 第2に、Open XDRは、非常に小規模な顧客アカウントから非常に大規模な顧客アカウントまで簡単に拡張でき、費用対効果が高くなります。

“Stellar Cyberの魅力は、シンプルなハードウェアデバイスを使用して小規模なクライアントに組み込むことができ、それでも大規模なエンタープライズ展開まで拡張できることでした。 この戦略的提携により、地球上のすべての組織が購入できるハードウェアとソフトウェアを含む、完全なサービスとしてのSOCソリューションを提供できます。”

試験と結果

Open XDRをテストするために、モリンのチームは、Open XDRを会社の内部ネットワークに配置し、友好的なクライアントと一緒に展開しました。 “すぐに、非常に簡単に視覚化できる脅威がたくさんありました”とモリン氏は言います。 “Open XDRは、アナリストが実際の脅威をより効率的に発見できるようにすることで、アナリストにとってより良いものになりました。 これは、ほとんどの従来のSIEMベンダーソリューションよりもはるかに偏執的で高度です。 クラウドの分析エンジンを介

> “Stellar Cyberの魅力は、それが可能だったことです。シンプルなハードウェアデバイスを使用して小規模なクライアントに導入できますが、大規模なエンタープライズ展開まで拡張できます。”

してすべてのデータを取得することは、他の製品と比較してはるかに高速です。”

もう1つの利点は、Open XDRの多層セキュリティアプローチです。“事前に統合されたコア機能は非常に印象的です”とモリン氏は言います。“ツールの数と階層化されたエンジンにより、プラットフォームは非常に正確であり、それは私たちにとって非常にうまく機能するアプローチです。”

さらに、Stellar Cyberのセキュリティダッシュボードは関連するすべてのセキュリティ情報が1つの画面に表示されるため、アナリストの効率が向上します。“ダッシュボードにより、非常に魅力的な顧客デモが可能になります”とモリン氏は言います。“私たちのクライアントの多くはサイバーセキュリティの教育を受けておらず、ダッシュボードはすぐに価値を付加しながら本当にクールに見えます。”

Stellar Cyberは、モリンが協力していた他のベンダーよりもはるかに応答性が高かった。“Stellar Cyberが製品を進化させている間、私たちはサービスを進化させていました。新しい機能を聞いて応答する能力は際立っていました”とモリン氏は言います。“彼らは非常に反応が良く、速かったので、それが私がパートナーに必要なものです。”

現在、CyFlareはOpen XDRソリューションで何百ものアクティブな顧客にサービスを提供しており、今後3か月以内に100を超えるまで加速すると予想しています。 さらに、CyFlareは、Open XDRからのデータをセキュリティオーケストレーション、自動化、および応答（SOAR）プラットフォームに統合して、取締役会などの非技術マネージャーにOpen XDRの有効性を証明するメトリックを生成できるようにする予定です。

このSOC-as-a-service卸売業者にとって、Open XDRはMSPおよびMSSPの顧客にサービスを提供するための理想的なプラットフォームであることが証明されました。

> **“Open XDRプラットフォームにより、製品にとらわれません”とモリン氏は言います。“お客様は、既存のセキュリティシステムを取り除いて別のベンダーの製品に置き換えることを望んでいません。また、Open XDRを使用すると、既存の機器を維持できます。 このように、Open XDRを使用すると、MSSPがアカウントを簡単に作成できるようになります。”**