導入事例

# 5ironは、サービスを拡張するための自動化されたマルチテナントセキュリティシステムを実装しています

セキュリティ応答を自動化して、アナリストの生産性を向上

5ironは、金融機関へのサービス提供に重点を置いた高度なマネージドセキュリティサービスプロバイダーです。 テネシー州ナッシュビルを拠点とする同社は、安全な電子メール保護、侵入検知（IDS）、セキュリティ情報およびイベント管理（SIEM）、ファイアウォール、ファイアウォールなど、さまざまなサービスを米国中の銀行や信用組合に提供しています。 高度なエンドポイント。すべて5ironセキュリティオペレーションセンター（SOC）から24時間体制で管理されます。

“私たちはマネージドセキュリティオペレーション（SOC）を提供します”と5ironのCEO、ジェレミー・ホップウッドは言います。“多くの場合、セキュリティの層を追加する別のボックスを購入することに焦点が当てられますが、CISOは、それが管理するためのより多くのことを意味することを知っています。 5ironマネージドソリューションは、24時間体制の管理、検出、検証、および応答を提供することにより、クライアントの内部負担を軽減し、セキュリティ体制を強化します。”

## 導入前

### サポートの欠如
製品の質問への回答を待つ必要がありました

### 非自動化
脅威の応答時間に遅れが生じた

### マルチインターフェース
高価で複雑なアドオンにつながる

### 高価
会社がサービスに従事することを制限される

### 脅威の過負荷
繰り返しの脅威通知は圧倒的でした

## STELLAR CYBER 導入後

### 24時間年中無休
自動化されたセキュリティカバレッジ

### 自動化
自動化されたインシデント対応

### 単一のプラットフォーム
情報を合理化します

### 固定費
追加のプラットフォームアドオンはありません

### 合理化された通知
時間を節約するためにノイズをフィルタリングします

**“Open XDRを使用すると、独自のサービスを拡張できます。 マネージドセキュリティオペレーションの一環として、セキュリティ分析を提供できるようになりました。”**

## SIEMの災い

5ironのマネージドSIEMサービスは、クラス最高のプラットフォーム上に構築されており、クライアントが可能な限り最も実用的なインテリジェンスを確実に利用できるようにします。 同社は主に最大規模のSIEMプロバイダーのプラットフォームを使用していましたが、必要なサービスやサポートを利用できませんでした。 主要なSIEMプロバイダーの規模が大きいめ、5ironは、問題がどれほど大きくても、製品の質問や問題への回答を待つ必要がありました。 自社のクライアントへの迅速な応答サービスに誇りを持っている企業として、5ironはプロバイダーからの応答時間が遅いことに不満を募らせていました。

さらに、既存のSIEMは検出とレポートに優れていましたが、5ironは、セキュリティアナリストをより効果的にし、脅威への対応を迅速化するために、収集、検出、調査、および対応のプロセスを自動化するプラットフォームを望んでいました。

マルチテナンシーは別の重要な問題でした。 5ironは、単一のインターフェイスからすべてのクライアントを効率的に管理できる必要がありましたが、既存のSIEMでは、マルチテナンシーをサポートするために高価で複雑なアドオンが必要でした。 同社は、マルチテナンシーをネイティブに提供し、運用とクライアント管理を簡素化するプラットフォームを望んでいました。

最後の問題はコストでした。 既存のSIEMの価格設定は、多くの組織にとって参入障壁であることが証明されました。 特に中小規模の顧客はサービスのコストを抑えており、大企業でさえコストを懸念していた。 その結果、5ironは、これらの組織のセキュリティ運用を効果的に管理するために必要な品質のツールを提供できませんでした。 Open XDRの価格設定モデルにより、5ironは、より堅牢なプラットフォームと競争力のある価格設定モデルの両方をクライアントに提供できるようになりました。

> “Open XDRは、アナリストチームをより効率的にし、サービスを日々改善し続けます。 これは、既存のSIEMでは不可能だったことです。”

## Open XDRへの切り替え

2018年のRSAショーでStellar CyberのOpen XDRのデモンストレーションを見て、5ironはチャンスを見ました。 Open XDRは、自動化されたインシデント対応、マルチテナンシー、およびアジャイルサポートチームをすべて固定費で提供し、既存のSIEMよりも低コストでより多くの価値を提供しました。

“戦略に重点を置いたサービスプロバイダーとして、既存のSIEMベンダーから必要なレベルのパートナーシップがありませんでした”とホップウッド氏は言います。 “Stellar Cyberは、クライアントを効果的にサポートするために必要なプラットフォームとサポートの両方を提供してくれます。 同社は、要求された機能をはるかに迅速に処理し、サポート要求に迅速に対応します。これは非常に大きな価値です。 自社の顧客に対して可能な限り機敏に対応しようとする場合、真のパートナーとして機能するベンダーが必要です。”

5ironがOpen XDRを採用する動機となったのは、プラットフォームの堅牢性でした。 “クリンチャーは、Open XDRが当初考えていたよりもはるかに多くのことを実行することでした”とホップウッド氏は言います。 “Open XDRを使用すると、独自のサービスを拡張できます。 マネージドセキュリティオペレーション製品の一部としてセキュリティ分析を提供できます。 Open XDRの組み込みIDS、脅威インテリジェンス、脅威ハンティング、およびその他の機能により、従来のSIEMよりもはるかに多くの機能が提供されます。”

適切な情報を収集し、異常を検出し、原因を調査し、脅威に対応するOpen XDRの業界をリードする機能により、他のセキュリティ分析やSIEMプラットフォームとは一線を画しています。

“Stellar Cyberは単なる警告エンジンではなく、行動を起こすことができます”とホップウッド氏は言います。 “同じアラートを1000回見る必要はありません。 一度見ると、システムと連携してブロックできます。 従来のSIEMは大量のアラートノイズを生成し、このノイズをフィルタリングすると、アナリストの効果が低下する可能性があります。 代わりに、彼らは実用的なインテリジェンスとセキュリティ体制の強化に焦点を当てるべきです。 たとえば、従来のSIEMでは、毎日数千または数百万ものアラートが発生する可能性があり、この多くのアラートに応答するアナリストは効率的ではなく、応答に数分または数秒ではなく数時間かかる原因になります。 Open XDRは、アナリストに提示される前に、これらのアラートをより効果的に関連付けて対処します。 その結果、アナリストはより少ないがより具体的なアラートに応答するため、アナリストの有効性が向上します。 Open XDRにより、クライアントのセキュリティ体制を継続的に強化することができました。これは価格に見合う価値があります。”

さらに、Stellar Cyberの価格設定は、5ironのビジネス戦略と一致していました。 Stellar Cyberの価格設定モデルにより、5ironは、競合他社を購入できなかった人々の手にサービスを提供できるようになりました。 実際には、Open XDRは製品の支払いに十分なSIEMソリューションへの5ironの支出を削減したため、当初は現在のSIEMを改良する製品と見なされていたものが、拡張サービスのための新しく非常に費用効果の高いプラットフォームになりました。

“この製品は、以前よりもはるかに多くの人に届けることができます”とホップウッド氏は言います。 “これは、すべてのお客様にとってコアプラットフォームになりました。”

5ironは、Open XDRベースのサービスを金融業界の顧客に展開するにつれて、サービスを提供するための新しい方法を開発しています。 “プラットフォームとサービスの可能性が拡大していることがわかります”とホップウッド氏は言います。 “Open XDRは、アナリストチームをより効率的にし、実際に日々のサービスを改善します。 これは、既存のSIEMでは不可能だったことです。”

> **“この製品は、以前よりもはるかに多くの人に提供できます...すべてのお客様のコアプラットフォームになりました。”**