Splunk ARIを使い、セキュリティ運用の日次チェック時間を40%短縮

主な課題

あるヘルスケア企業では、1億2,000万件以上の受診データを安全に保護し、厳格なセキュリティ基準を遵守するため、ネットワーク全体にわたりIDアクションと資産との相関付けを簡単に行う必要がありました。

主な成果

Splunk Asset and Risk Intelligence (ARI)を導入したことで、同社のSOCは、資産とIDを包括的に可視化できるようになりました。これによって、よりプロアクティブな運用体制を確立して、セキュリティ関連リスクとコンプライアンス関連リスクの両方を軽減しています。

業種：医療・ヘルスケア

製品：Splunk Asset and Risk Intelligence (ARI)、Splunk Enterprise Security (ES)

ソリューション：セキュリティ

機能：調査とフォレンジック、SIEM/セキュリティ分析、インフラ監視とトラブルシューティング、サービスの監視とインサイト取得、インシデント対応と自動化

21,000人を超えるヘルスケア従事者とその患者にサービスを提供する企業に、デジタルレジリエンスは不可欠

この企業では、定期的な診察から高度な治療まで、受診件数にして年間1億2,000万件を超える支払い情報を取り扱っています。このサービスによって、病院や診療所では医療報酬を確実に効率よく受け取り、地域社会で医療を継続できているのです。機密性がきわめて高い患者の個人情報を扱っているため、ハッカーにとっては絶好の標的です。そのため、同社ではセキュリティと厳格なコンプライアンス基準の遵守を最優先に据えています。

しかし、医療費決済サービスプロバイダーである同社において、既存のツールでは資産とIDを包括的に可視化できないことが判明しました。このままでは、セキュリティとコンプライアンス態勢がリスクにさらされてしまいます。そこで同社のセキュリティオペレーションセンター (SOC)では、さまざまなソースから手動でデータを取得することになりました。社内の厳格なセキュリティ構成基準に基づき、ネットワーク内のデバイスはウイルス対策ソフトウェアに登録され、毎日検証されます。同社の情報セキュリティ担当ディレクターはこう述べています。「データがさまざまなツールに分散していたため、このプロセス全体に最大5時間かかることもありました」。SOCではこれらの標準チェックに毎日何時間も費やしていたため、よりプロアクティブなセキュリティ対策の策定など、他の重要なタスクに注力する余裕がほとんどありませんでした。担当ディレクターはこう認めています。「以前はデバイスの最新状況についての情報を定期的に更新していなかったので、このプロセスはもっと大変でした。デバイスの存在すら知らなかったら、セキュリティやコンプライアンスの問題があるかどうかなど、どうやって判断できるでしょうか」

もっと良い方法があるはずです。そして、実際にあったのです。

成果

40%
セキュリティの日次チェックで短縮された時間の割合

800台超
重要なセキュリティパッチの適用対象として特定されたデバイスの数

1.2億件
1年間に処理する受診件数

節約したすべての時間を有効に活用

Splunk Asset and Risk Intelligence (ARI)を導入したことで、このSOCでは、ネットワーク内の資産とIDアクションとの相関付けを、すべて1カ所から簡単に行えるようになりました。調査においてはARIが単一の情報源となり、「誰が」「何を」「いつ」「どこで」「なぜ」「どのように」行ったかを確認できるため、コンプライアンスリスクを軽減できます。

担当ディレクターは話を続けます。「ARIは、優れたフォレンジックツールです。デバイスがVPNに接続するたびにすべてのIPアドレスを確認できるので、必要な情報を探してSIEMを駆使したり、カスタムサーチを大量に作成したりせずに済みます」

また、セキュリティの定期チェックにかかる時間が40%短縮されました。ときには、わずか5分で終わることもあります。SOCは節約できた時間を使い、厳しい廃棄プロセスにおける不備を解消し、ネットワークデバイスの構成ミスへの対応を迅速化するとともに、ARIをいっそう最適化して、組織全体にさらなる価値を提供しています。

> ARIによって、当社のデジタルレジリエンスがレベルアップするのです。
>
> ヘルスケアソフトウェア企業、
> **情報セキュリティ担当ディレクター**

ARIは、ネットワーク内の異常を検出するのに役立っています。SOCでは、ARIを脆弱性管理ツールとして活用することで、パッチが適用されていない少数のデバイスを発見できました。手遅れになる前に、セキュリティ上の死角を把握できるのです。担当ディレクターはこう説明します。「リスクを軽減するためのプロアクティブな防御を初めて実行できるようになりました」

加えて、ARIの導入前、SOCとネットワークオペレーションセンター (NOC)の間では、情報の伝達がスムーズに行われていませんでした。担当ディレクターは、次のように認めます。「相手とやり取りする最良の方法については、いつも悩んでいました。たとえば、ファイル整合性監視ソフトウェアを使う新しいデバイスがあった場合、そのデバイスの登録を最後に確認した日時や、最後のログを受信した日時といった詳しい情報を伝える方法です」。しかし、ARIの導入により作業量とサーチ時間が大幅に削減されたことで、この問題が解決されました。

担当ディレクターはこう続けます。「今ではもっと優れたプロセスを運用しています。これによって、SOCとNOC間のコミュニケーションを改善するだけでなく、対応の質とスピードの向上も実現しており、社内で設定した高い基準を常に確実に守れています」

> すでに多くのユースケースにARIを適用してはいるものの、ARIで可能だとわかっている能力を実際に活用することに関しては、まだまだ始まったばかりです
>
> ヘルスケアソフトウェア企業、
> **情報セキュリティ担当ディレクター**

ネットワークのゼロデイ脆弱性への対応

2件のゼロデイ脆弱性が突然明らかになったとき、担当ディレクターは従来の脆弱性管理ツールを使って問題の調査に乗り出しました。そこで思い知ったのは、これらのツールでは自社が危険にさらされているかどうかを判断できないということでした。

幸いなことに、ARIがこの窮地を救ってくれました。担当ディレクターはわずか数分で、4つの異なるソースにわたる構成データの相関付けを行い、重要なセキュリティパッチの適用が必要なデバイス800台以上を特定しました。「ARIのおかげで、ネットワーク内のすべての資産とIDを、オンラインでもオフラインでも包括的に可視化できます」というわけです。

この迅速な判断によって、危機は直ちに回避されました。そのことをこう説明します。「標準的な脆弱性診断ツールでは、問題の一部しかわかりません。ARIを使えば、全体像を把握できるのです。さらに重要なのは、脆弱なデバイスを補強できたことで、ビジネスに直接プラスとなる効果を達成できたことです。その気分は格別ですね」

可視性の向上とプロアクティブなセキュリティ対策を継続

同社は今後も続けて、既存ツールの一部をARIに統合していく予定です。また、ARIを活用して脆弱性の誤検知を削減する計画もあります。情報セキュリティ担当ディレクターは、次のように打ち明けます。「妙な話ですが、すでに多くのユースケースにARIを適用してはいるものの、ARIで可能だとわかっている能力について、その十分な活用に関してはまだ始まったばかりなのです」

同社はSplunk Enterprise Security (ES)を10年近く利用していたので、ESとのシームレスな統合が可能なARIを導入するという選択はスムーズに決まりました。今はARIなどのツールを使用することで、セキュリティ構成に関する高い基準をさらに強化し、顧客とその患者をデータ侵害から保護する新たな方法を模索しています。これによって、命を救う仕事に顧客が専念できるようにするためです。

担当ディレクターはこう述べます。「計画を進めることで、情報セキュリティにできることがさらに増えるでしょう。可視性と状況認識が高まり、いっそうプロアクティブな対応ができるようになるでしょう」。さらに、考えられる最良の展開は、ARIがIT運用の観点から活用され、IT運用チームでもいっそうプロアクティブな対応が実現するというものです。そのことは次のように語られています。「ITインフラチームはデータセンターでARIを活用でき、デスクトップチームは新規構築に際して、さらには主なメンテナンス作業にもARIを利用できます。ARIによって、当社のデジタルレジリエンスがレベルアップするのです」

> ARIのおかげで、ネットワーク内のすべての資産とIDを、オンラインでもオフラインでも包括的に可視化できます
>
> ヘルスケアソフトウェア企業、
> **情報セキュリティ担当ディレクター**

Splunkを無料でダウンロードするか、Splunk Cloudの無料トライアルをお試しください。Splunkは、クラウドかオンプレミスか、また組織の規模の大小などにかかわりなく、お客様のニーズに最適な展開モデルでご利用いただけます。

26_CMP_cust_Healthcare-software-company_v4-JA-202603