Aflac社：Splunkの分析主導型セキュリティプラットフォームを導入

主な課題

脅威の状況の急速な変化に直面したAflac 社は、顧客、1 万人の従業員、そしてブランドの評判を守るために堅牢なセキュリティプラットフォームを必要としていました。

主な成果

20種類以上のセキュリティテクノロジー間で脅威インテリジェンスを統合し、分析主導型のセキュリティアプローチを構築して、ROIを早期に達成しました。

業種：金融サービス

ソリューション：セキュリティ

米国の大手保険会社であるAflac社は、高まるセキュリティ対策の重要性を理解しています。

セキュリティ上の脅威が増え、またそのスピードも加速しているため、Aflac社は、顧客、1万人近くの従業員、およびブランドの評判を守るため、新しい分析主導型のセキュリティアプローチを必要としていました。同社は、自社の脅威インテリジェンスシステム(TIS)の中核としてSplunkプラットフォームを導入しました。

脅威インテリジェンスプラットフォームの強化

Aflac社は新しい市場に参入して新しいサービスを提供するようになったため、スピアフィッシングからマルウェアの拡散に至るまで、急速に変化する脅威に対応できるように、セキュリティプログラムを継続的に更新する必要がありました。Splunkプラットフォームを導入する以前は、旧来のSIEMソリューションに依存しており、適切に攻撃を検出し対応するための強力な脅威インテリジェンスプラットフォームを必要としていました。

Aflac社のセキュリティオペレーション兼脅威管理担当ディレクターを務めるD.J.Goldsworthy氏は次のように述べています。「前のSIEMでは、データをよく理解してから行動を起こす必要がありましたが、Splunkの場合は瞬時にデータを把握することができます。Splunkのおかげで迅速に行動を起こすことができるようになり、すべての関係者に対してすぐに価値を示すことができるようになりました」

Aflac社はまず、脅威を検出するためにSplunk Enterprise Security (ES)を導入しました。Goldsworthy氏は、「実際のところPoCでは脅威のユースケースにSplunk ESを使用しており、予想よりもはるかに短期間で価値を実感することができました。本当に短い時間で、高度な脅威を検出することができたのです。最終的にはこれがポイントとなり、セキュリティのさまざまなユースケースでSplunk ESとUBA (User Behavior Analytics)に莫大な投資を行うという決定に至りました」と述べています。

データ活用の成果

2週間
企業向け実装までに要した期間

200万件
半年間でブロックされたセキュリティ脅威

40時間
手動プロセスを自動化して節約した1カ月あたりの時間

ROI目標の早期達成

Goldsworthy氏によると、Splunkプラットフォームを企業向けに実装するのに要した時間は、わずか数週間でした。「取り込むデータソースの量と、導入したいユースケースの数を考えると、これは非常に驚くべきことでした」と、Goldsworthy氏は説明します。「Splunkの投資効果をすぐに実感できました」

現在ではAflac社のセキュリティオペレーションセンター (SOC)にSplunk ESを導入し、フルタイム従業員の多くの時間を節約しています。Goldsworthy氏は次のように述べています。「計算したところ、レポート作成に関しては月に40時間以上も節約できています。以前は手作業でレポートを作成していましたが、今では完全に自動化されています。Splunkを使用すると、さまざまなソースからデータを簡単に取り込み、役員会やその他のリーダーシップなどの関係者に対して有意義な方法でデータを提示できます」

約40人の人員で構成される6つのチームがSplunkプラットフォームを使用しており、脅威の検出、脅威インテリジェンス、セキュリティ運用、インシデントレスポンス、アプリケーションセキュリティ、セキュリティ管理、不正行為対策などの幅広いセキュリティユースケースを管理しています。

「最初に脅威インテリジェンス、次にセキュリティ運用のためにSplunkを実装したところ、このソリューションがさまざまな用途に使用できることがわかったため、次のステップとして不正行為対策に使用することを決めました」とGoldsworthy氏は語っています。

> 本当に短い時間で、高度な脅威を検出することができたのです。最終的にはこれがポイントとなり、セキュリティのさまざまなユースケースでSplunk ESおよびUBAに莫大な投資を行うという決定に至りました”
>
> Aflac社セキュリティオペレーション兼脅威管理担当ディレクター、
> **D.J. Goldsworthy氏**

脅威インテリジェンスの自動化

Aflac社のTISの導入は、当初の予定より1カ月早く5カ月で完了しました。このシステムは戦術的/戦略的な機能を提供し、自動化と併せて、日々の脅威データの入力効率を向上させ、時間の節約とミスの削減に役立っています。TISにより、20以上の脅威インテリジェンスソースから送られるIoC (indicators of compromise, 侵害の痕跡)データが自動的に処理され、各IoCの信頼性スコアとリスクプロファイルが提供されます。こうして得られた数千単位のIoCをSplunkのセキュリティ分析プラットフォームで追跡し、ネットワークログやシステムログとリアルタイムで相関付けます。そして、インシデントの兆候が検出されたらSOCアナリストがすばやく対応します。Aflac社では、半年のうちに200万件を超えるセキュリティ上の脅威をブロックし、誤検知をわずか12件未満に抑えることができました。

「契約者の方々の立場で考えれば、自分の個人情報を守るために保険会社が最善を尽くすことを期待するのは当然です。私たちは、自社の情報の管理だけでなく、お客様の個人情報の管理にも細心の注意を払っています。それを可能にしてくれるのがSplunkです」と、Aflac社で情報セキュリティ担当バイスプレジデント務めるBen Murphy氏は評価します。

異常検出による価値向上

ネットワークに特権アクセスできる請負業者や関係者が増えると、ユーザー全員がすべてのセキュリティポリシーとベストプラクティスを守っているかどうかや、ユーザーのアクティビティに隠れたリスクがないかどうかを把握するのが極めて困難になります。「Splunk UBAのおかげで、普段監視している行動の外で起きている状況を把握できるようになり、Aflacのセキュリティ体制に強力な検出層が1つ追加されました」とGoldsworthy氏は評価します。

splunk>

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp
splunkjp@splunk.com

20-14314-Tier 2-Aflac-A4-CS-JA-202201