SFBLI社：Splunk Attack Analyzerで業務を効率化し、セキュリティ態勢を強化

主な課題

Southern Farm Bureau Life Insurance (SFBLI)社では、外部と接続するWebアプリケーションで受け取ったファイルを分析するソリューションがボトルネックとなり、営業活動が遅滞し、大量のアラートが生成され、組織をリスクにさらしかねない状況を招いていました。

主な成果

SFBLI社 はSplunk Attack Analyzerを導入したことで、業務を効率化するとともに、セキュリティ侵害のリスクを低減し、顧客の機密データの保護を強化して、全体的なセキュリティ態勢を強固にすることができました。

SOUTHERN FARM BUREAU LIFE INSURANCE COMPANY

業種：金融サービス

ソリューション：セキュリティ

製品：Splunk SOAR、Splunk Attack Analyzer

人生の大きな苦難に直面する家族のサポートからデータ窃取の防止まで

Southern Farm Bureau Life Insurance (SFBLI)社は、米国の11の州で農家、警察官、教師とその家族をはじめとした一般の人々に安心を届けている保険会社です。不測の事態が起こったときには、被保険者の立場に立ち、説明責任を果たしながら、誠実さと尊重の念を持って保険業務を遂行しています。こうした価値観を経営理念としている同社にとって、顧客の機密データと自社の知的財産を守るのは当然のことです。しかし、もし守れなかった場合、たとえばマルウェア攻撃を受ければ、業務停止に追い込まれ、復旧のめども立たず、顧客の医療記録、銀行情報、社会保障番号がサイバー犯罪者の手に渡ることもありえます。

特に狙われやすいのが、外部と接続するWebアプリケーションです。保険契約部門や電子サービス部門は、代理店や顧客からこのWebアプリケーションにアップロードされた機密性の高い書類や保険証券を使用して業務を遂行しています。SFBLI社では外部の代理店に業務を委託しているため、代理店が侵害されると、攻撃者がこのWebアプリケーションを糸口にSFBLI社に攻撃を仕掛けてくる可能性があります。そのため、このアプリケーションは大きなリスクを抱えていました。

成果

70%
ファイルのスキャン時間を短縮

減少
6カ月で誤検知が26%からほぼゼロに

約5分
分析のみで約20分かかっていたところが、分析からオーケストレーション、対応まですべて合わせても約5分に短縮

壊滅的な影響を及ぼすマルウェア攻撃やデータの窃取から防御するために、ミシシッピ州ジャクソン支店に拠点を持つサイバーセキュリティチームは、サンドボックスソリューションを中心的に活用して、アップロードされたファイルに悪質なコンテンツが含まれていないかを分析していました。しかし、誤検知の数が手に負えないほど多く、わずかな人数しかいないチームは大量のアラートに振り回され、不正アクセスの兆候を見逃しかねない状況でした。さらに、スキャンには毎回20分近くかかり、営業活動が遅滞するだけでなく、通常の業務にも影響が生じていました。そこでSFBLI社は、同社が顧客に提供しているような安心感をもたらし、精度が高く迅速な対応を可能にするソリューションを探し求めました。

スキャンを自動化し、詳細なアラートを提供するSOARを導入して、大幅な効率化を実現

SFBLI社とSplunkの出会いは数年前、サイバーセキュリティアーキテクトのKyle Notvest氏がチームの日々の業務を自動化し、効率を高める方法を探していたことに始まります。調査の末、最終的にSplunk SOARを選んだNotvest氏は、その成果にこの上なく満足しています。Splunk SOARの導入後、最初に行ったことのひとつは、サーバーのスキャン処理を自動化することでした。30〜40分かかっていた処理がわずか数秒に短縮され、少数精鋭のチームは貴重な時間を節約できるようになりました。現在では、各種ツールからアラートを取得して補強するなど、さまざまなユースケースでSplunk SOARを使用しています。「今ではSplunk SOARで、初期調査を行ってその結果をチケットにまとめ、アラートの調査に必要なデータを追加してチケットのコンテキストを補強する、といった処理を自動化しています」とNotvest氏は述べます。組織と顧客の機密データの保護を任務とするセキュリティチームは、業務に集中して取り組めるようになり、組織の全体的なセキュリティ態勢の強化に貢献しています。

> 処理が速いほど、常に物事がスムーズに進むとは限りません。しかし、悪意のあるコンテンツを見つけるのにかかる時間と、保険の引き受けや保障の提供に必要なファイルの入手にかかる時間は、短いほど理想的です。当社はSplunk Attack Analyzerを導入したことで、業務のスピードと効率を向上させることができました。
>
> **Chris Powell氏、**Southern Farm Bureau Life Insurance社、サイバーセキュリティ対策およびセキュリティオペレーション担当ディレクター

セキュリティ、信頼性、効率性に優れたソリューションでビジネス上の深刻な課題を解決

Notvest氏は、.confで発表されたSplunk Attack Analyzerを見た瞬間、これこそが、SFBLI社の外部と接続する脆弱なWebアプリケーションを保護するために必要なソリューションであると確信しました。「これまで使っていたサンドボックスとSplunk Attack Analyzerでは雲泥の差があります」とNotvest氏は言います。

SFBLI社は、Splunk Attack Analyzerを導入したことで、スキャン時間を70%短縮できました。Notvest氏によると、サンドボックスソリューションの大きな問題は、時間がかかりすぎてプレイブックがタイムアウトすることでした。タイムアウトが発生すると、セキュリティチームのメンバーがファイルを手動で確認して承認し、再度アップロードしなければなりません。また、スキャンの失敗を知らせるアラートを見逃したときには、重要な書類が事業部門になかなか届かず、業務が大幅に滞っていました。

そのような中、Splunk Attack Analyzerを活用したことで、誤検知率をほぼゼロにすることができました。「以前はアップロードされたファイルの27%が悪質または疑わしいファイルとして検出されたこともありましたが、結果はどれも正常でクリーンなファイルでした。しかしAttack Analyzerを導入してから6カ月間の誤検知はほぼゼロです。これは私たちにとって、とても大きなメリットです。ノイズが多すぎて過剰な負荷がかかっていたときには、脅威ではなかったアラートの調査に時間を取られすぎて、正真正銘の脅威を見逃す可能性があったからです」とNotvest氏は振り返ります。無駄な作業に手を取られることも、大量のアラートに振り回されることもなくなったNotvest氏率いる7人のチームは、生産性と効率性を全体的に高め、顧客の機密データの保護に自信を深めた結果、初めてSOCのように業務を遂行できるようになりました。

セキュリティチームに新しいメンバーを迎えることも、かつてないほど容易になりました。「一貫性のある分析を行えるようになったことで、新しいメンバーのレベルも上がり、業務を安心して見ていられるようになりました」とNotvest氏は語ります。「チームメンバーを信頼できるのも、会社のセキュリティに自信が持てるのも、Splunk Attack Analyzerがあってこそです」

効率的になった業務を洗練させる

日々、何十通もの不審なメール、ファイル、URLを手動で調査していたSFBLI社のサイバーセキュリティチームは、今ではこうした重要な調査をより迅速かつ正確に行う手段としてSplunk Attack Analyzerを使用しています。その結果、Attack Analyzerの導入前は分析だけで最大20分ほどかかっていたのに対し、現在では、分析からオーケストレーション、対応までを5分足らずで完了できるようになりました。「Attack Analyzerを導入する前は、アラートをひとつ残らず調査するのは困難でした。しかし今では、アラートを見逃していないと自信を持って言えるようになり、大量のアラートに振り回されることもなければ、業務上の大きな負担に悩むこともありません」とNotvest氏は胸を張ります。現在、Notvest氏は、フラグが立ったコンテンツをAttack AnalyzerのUIにアップロードするプロセスの自動化に力を入れています。「最終的には、SOARで悪質な可能性のあるアーティファクトにフラグを立て、それらをAttack Analyzerに自動的に取り込んで詳しく調査できるようにすることを目指しています」

splunk>

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

25-557801-Splunk-Farm Bureau Insurance-CS-JA-202408