Soriana社：メキシコ最大級のスーパーマーケットチェーンがSplunkを使用してインシデント対応時間を99%短縮

主な課題

Soriana社では、報告の過程で生じる遅れや多種多様なプラットフォームが原因で、インシデント対応や修復に時間がかかっていたうえ、インフラが包括的に可視化されていなかったために、不正行為やセキュリティの問題が発生するリスクが高いといった問題を抱えていました。

主な成果

Soriana社は、ハイブリッドインフラおよび15,000台のPOSすべてをリアルタイムで可視化することで、MTTRの短縮、セキュリティチームへのより深いインサイトの提供、不正行為とセキュリティリスクの低減を実現しました。

Soriana

業種：リテール(小売り)

ソリューション：IT、セキュリティ、DevOps

必要なときに必要なものをすぐに手にできる場所

夜遅くに赤ちゃんのおむつが切れてしまった、常備しているガーリックパウダーがなくなりそう、クレジットカードの決済が迫っている、10代の息子が携帯電話を壊してしまったなど、そういったときに足が向くのがSorianaです。大手小売業者のSoriana社は何十年もの間、メキシコ国内の32の州にわたる280以上の地域で暮らす家庭に、生活に必要なあらゆるものを提供しています。

Soriana社では、おむつから銀行サービス、食料品、携帯電話まで、お客様が必要なものをすぐに手に入れられるよう、実店舗とアプリベースのサービスの両方で事業を展開しています。その舞台裏では、CISOのSergio Gonzalez氏が率いるセキュリティチームが、同社のデジタルシステムを運用しながら、サーバーやノートPCを含む40,000台のデバイスと15,000台のPOSすべてを監視、保護しています。Soriana社は2020年にクラウドへの移行を開始しましたが、多数のサーバーが稼動し、大量のデータが処理されるハイブリッドインフラの監視には、困難が伴いました。また、運用していたプラットフォームとシステムの統合は困難であったため、セキュリティチームはイベントの対応時に監視ツールを切り替えなければならず、貴重な時間を無駄にしていました。

旧式の報告ツールも、インシデント対応の遅れの原因となっていました。リアルタイムのデータやわかりやすいダッシュボードがなく、Gonzalez氏のチームはExcelスプレッドシートで情報を確認していたため、修復に時間がかかっていたのです。この他にもう1つ、可視性の欠如がもたらす問題を抱えていました。それは、不正行為のリスクが高まり、場合によっては平均修復時間(MTTR)が長くなってしまうことです。

ITシステムを包括的に把握し、保護するためのより優れた方法を求めて、Soriana社はSplunk Cloud PlatformとSplunk Enterprise Securityの導入を決断しました。これにより、SOCを統合して効率化し、デジタルリスクにも適切に対応できるようになると考えたからです。

成果

40,000台以上
15,000台のPOSを含む、監視および保護対象のデバイス数

96%
POS監視プロセスの平均修復時間が短縮された割合
(2日から30分に短縮)

99%
インシデントの検出、調査、対応の合計時間が短縮された割合
(48時間から2時間に短縮)

実現したメリット：MTTRの96%短縮とより的確なビジネス上の意思決定

Soriana社のお客様は、食料品の購入やクレジットカードでの決済を、店舗、オンライン、スマートフォンのいずれでもシームレスに行える必要があります。そこで、数多くのPOSデバイスを監視して保護するためにGonzalez氏のチームにとって鍵となったのが、Splunkのセキュリティとオブザーバビリティの統合プラットフォームでした。Splunkを導入した今、より効果的に監視を行い、問題発生時にも迅速に対応できるようになりました。

以前は、店舗で取引に関するITの問題が発生すると、Gonzalez氏のチームメンバーはExcelスプレッドシートで受け取る情報に目を通す必要がありましたが、インシデントが発生してからその情報が手元に届くまでに2日～ 1週間もかかっていました。しかし今では、Splunkのリアルタイムダッシュボードのアラートを活用し、サポートチケットをサービスデスクに自動的に割り当てることで、かつては数日かかっていた修復プロセスを30分に短縮しています。また、お客様の取引に関する問題を迅速に解決し、ショッピング体験を向上させることもできました。これは、買い物客が店舗で購入する場合でも、オンラインで購入する場合でも、重要なポイントといえるでしょう。

> Splunkを導入して以来、重大なセキュリティインシデントは発生していません。これまでになくレジリエンスが向上しています
>
> Soriana社CISO、**Sergio Gonzalez氏**

リアルタイムダッシュボードがもたらすメリットは、MTTRの大幅な改善や、優れた購入体験にとどまりません。「財務チームにも、お客様の行動に関する詳細なインサイトをはじめとした、より多くの情報を提供できるようになりました」と、Gonzalez氏は述べます。また、社内の意思決定者に対して、セキュリティチームがビジネスに与える価値や影響を容易に示せるようになったことで、Gonzalez氏は同社のセキュリティ態勢を強化するなど他の重要なプロジェクトの予算も確保できるようになりました。

Splunk導入後：重大なセキュリティインシデントは2年間ゼロ

Soriana社とそのお客様に影響を与える重大なインシデントを効果的に防止するための体制づくりも、CISOであるGonzalez氏の役割の1つです。同氏のチームは、日頃から使用しているダッシュボードの指標に基づいて、問題が小さいうちから監視して、大きな影響を及ぼす前にプロアクティブに対処しています。

Splunkに移行する前の数年間、Soriana社が使用していたセキュリティイベントの検出と処理のプロセスは複雑なものであったとGonzalez氏は振り返ります。しかし、Splunk Enterprise Securityを導入したことでSOCのプロセスが効率化され、チームは異常な動作や疑わしいトラフィックを簡単に発見できるようになりました。Gonzalez氏は次のように語ります。「現在では、システムの脆弱性を特定できるようになりました。前に使っていた他のプラットフォームではできなかったことです。Splunkのおかげで、セキュリティ戦略を改善し、当社の資産と情報を効果的に保護できるようになりました」

監視ツールの切り替えも、過去の話となりました。「たとえば、Splunkを当社のフィッシング対策システムと簡単に統合できたので、フィッシング攻撃をリアルタイムで検出できます」と、Gonzalez氏は述べます。以前は、プラットフォームごとに確認するのに貴重な時間を費やしていたのです。調査だけで2日以上かかっていたのが、今では脅威の検出と調査のプロセス全体に要する時間はわずか2時間です。時間の短縮率でいえば99%に上ります。

クラウドに簡単に移行して包括的な可視化とコンプライアンスの向上を実現

クラウドに移行してハイブリッドインフラを構築することは、面倒で複雑なことのように思われるかもしれません。しかし、SplunkとSplunkパートナーのADV Consultoresの支援により、Soriana社はSplunkインスタンスをデプロイし、SOCを設置して、Azureとオンプレミス全体にわたる1,000以上のコンポーネントをシームレスに統合しました。わずか1カ月ですべてのレコードをSplunkに取り込むことができたのです。

Soriana社が実現したスタック全体の可視化は、不正行為を防止するうえで極めて重要です。「以前は、不正行為を可視化することができませんでした」と、Gonzalez氏は述べます。現在では、購入時におけるお客様の保護対策を幅広く講じることができるようになりました。可視化することで、国のコンプライアンス基準をより簡単に満たすことができ、法的および財務的に表面化しにくい負担を軽減できます。

Gonzalez氏は、Soriana社のビジネスプロセスの改善において、Splunkが将来的にさらに大きな役割を果たすようになると感じています。同社でSplunkを使用したSAP環境の可視化と監視プロジェクトが進む中、Gonzalez氏はSplunk SOARを使用して自動化する領域をさらに増やしたいと考えています。「Splunkには非常に満足しています。Splunkが強力かつ信頼性の高いツールであることはもちろん、製品、チーム、パートナーなど支援体制も万全です」

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

23-117456-Splunk-Soriana-CS-SS-JA-202308