米国州政府：セキュリティとコンプライアンスを統合して監査での指摘を1,200件削減

主な課題

ある米国州政府のITチームは、レガシーシステムや連携のないばらばらなセキュリティツール、いくつもの手動ワークフローを頻繁に切り替える必要がありました。そのため、脅威の検出、住民データの保護、厳格なコンプライアンス要件の遵守が困難になっていました。

主な成果

Splunkの導入により、州政府はIRSコンプライアンスに関する問題を1,200件以上解消し、誤検知を減らし、対応時間を短縮させることで、セキュリティ運用をモダナイズして州全体のサイバー防御の基盤を築くことに成功しました。

業種：行政・公共機関

製品：Enterprise Security、SOAR、ITSI

ソリューション：セキュリティ、オブザーバビリティ

機能：SIEM/セキュリティ分析、統合セキュリティ運用、自動化とオーケストレーション、セキュリティインシデント対応

レガシーシステムとセキュリティ課題への取り組み

この州政府では、行政府のあらゆるITリソースとテクノロジー資産をIT機関が一元的に管理しています。IT運用のモダナイズによってサービス品質を向上させ、住民データを保護する任務を担う、州務長官兼CIOは、次のように述べています。「データは州にとって最も重要な資産です。データを適切に整え安全に保護できれば、住民に提供するあらゆるサービスの質と信頼性を向上させられます」

同州政府は、テクノロジーニーズの高まりとともに、深刻な課題に直面しました。それは、セキュリティ管理の標準化、レガシーシステムの運用、機密性の高い住民情報に関するデータのプライバシー保護です。情報セキュリティ担当レベル3アナリスト兼チームスーパーバイザーはこう述べています。「レガシーシステムと従来型のプロセスは、まるで問題の入れ子人形のようです。問題を1つ取り除くと、新たな問題が3つ現れるのです」

以前、州政府のアプリケーションチームは、サイロ化した環境で働いていました。使っていたのは、連携のない複数のシステムと、一貫性のないセキュリティワークフローです。同機関には、強力なソリューションが必要でした。目的は、セキュリティイベントを監視し、運用の複雑さを軽減し、州政府のさまざまな部門にわたるコンプライアンスを維持することです。

州務長官兼CIOの主導の下、州政府はSplunkのセキュリティおよびオブザーバビリティソリューションを採用しました。それ以降、監視とコンプライアンスのプロセスが合理化され、セキュリティインシデントが減少し、すべての州政府機関でインシデント対応時間が大幅に短縮されました。

成果

- **1,200件を超えるIRSコンプライアンスの問題が解消。**Splunkで構築したコンプライアンスダッシュボードにより、わずか1回の監査サイクルでこれが実現しました。
- **検出と対応が大幅に迅速化。**ほとんどの問題の解決時間が数時間から数分に短縮されました。
- **アラートノイズが低減。**アナリストが、誤検知ではなく本当の脅威に集中できるようになりました。

Splunkによるセキュリティ、コンプライアンス、インシデント対応の最適化

州政府は、深刻化するITセキュリティとコンプライアンスの課題に対処するため、Splunkを導入しました。デジタルインフラ全体にわたるリアルタイム監視、インシデント対応、データ分析のための包括的なソリューションとして活用するためです。さらに、Splunk Enterprise Security、SOAR、ITSIソリューションを統合することで、セキュリティイベントを一元的に可視化し、運用効率を向上させました。

同州はこれまで、レガシーシステムの監視、手動のセキュリティワークフロー、分散型のデータ分析手法に課題を抱えてきました。これらが障壁となり、特に個人情報(PII)や連邦税情報(FTI)といった機密性の高い住民情報に関するデータのプライバシー保護が困難になっていました。Splunkでは、さまざまなソースからデータを取り込み、正規化し、大規模に分析できます。これにより、州政府は、IT環境を包括的に可視化し、セキュリティ態勢を強化できました。また、独立した3つのSplunkインスタンスとその他のSIEMツールを単一の統合プラットフォームに集約できたため、連携していない複数のシステムを切り替えながら調査を行う必要がなくなりました。

> データは州にとって最も重要な資産です。データを適切に整え安全に保護できれば、住民に提供するあらゆるサービスの質と信頼性を向上させられます。
>
> **州務長官兼CIO**

このことは、州政府のより広範なビジョンである「ステートセオリー」の基盤を築くことにもなりました。そのビジョンとは、あらゆる機関と自治体を保護するにあたり、それらをセキュリティ態勢がばらばらの個別のチームとしてではなく、一体化した組織として保護するというものです。これに向けてSplunk Enterprise Securityを使うことで、アラートをリアルタイムで一元的に可視化できるようになったため、脅威を迅速に特定して対応できるようになりました。また、SOARによって日常的な対応ワークフローが自動化されたため、セキュリティチームがアラートのトリアージに費やす時間を削減できました。さらに、ITSIがITパフォーマンスに関するより詳細なインサイトをもたらしたことにより、問題の影響が住民に及ぶ前の段階で、トレンドを見極め、リソースを最適化し、ダウンタイムを削減できるようになりました。

これらのツールを組み合わせることで、州政府は包括的なセキュリティとオブザーバビリティの基盤を確立しました。現状では、インシデントに迅速に対応し、データアクセスを効果的に管理し、厳格な州規制や連邦規制へのコンプライアンスを維持するためのより強固な体制が実現しています。このような成果により、業務をモダナイズし、デジタルサービスのレジリエンスを向上させることができました。

「Splunkは、私たちの業務の中枢システムとなっています。何かを見る必要があれば、それは必ずSplunkにあるべきです。そうでなければ、その情報は本当に安全とは言えません」と情報セキュリティアナリストは述べています。

> Splunkは、私たちの業務の中枢システムとなっています。何かを見る必要があれば、それは必ずSplunkの中にあるべきです。そうでなければ、その情報は本当に安全とは言えません。
>
> **情報セキュリティアナリスト**

AIと自動化の役割

州政府は、AIと自動化が長期的なセキュリティ戦略にとって不可欠であることは認めているものの、システムの導入は注意深く進めています。それは、これらのシステムが機密性の高い住民データを処理および保管する方法について、引き続き慎重であるからです。

それでもなお、州政府ではすでにSplunk Enterprise Securityの機械学習機能を使用して、異常の特定や脅威の可視化をさらにスピードアップさせています。これらの機能によってノイズが低減されるため、チームは優先度の高い問題に集中できます。「脅威の進展の速さを考えると、すべてを手作業で調査する余裕はありません。信頼できる自動化機能が必要です」と、情報セキュリティアナリストは述べています。

今後はSplunk SOARをAIドリブンのワークフローと組み合わせることに大きな可能性を見出しています。自動化プレイブックを使用すれば、セキュリティ関連の複雑な質問に対して迅速に回答を得られます。たとえば、新たに公表された脅威に対してどのアセットが脆弱かを、手動で延々と調査する必要がなくなるのです。

州全域でのリスク軽減と効率向上

Splunkを導入したメリットは、直ちに測定可能な成果となって現れました。州政府は、直近の監査サイクルでIRSコンプライアンスに関する指摘事項を1,200件以上削減しました。Splunkで構築したIRSコンプライアンスダッシュボードにより、経営陣とコンプライアンスチームは必要なセキュリティコントロールを完全に把握できます。そのため、監査担当者が到着する前にコンプライアンスギャップを突き止めて解消することがはるかに容易になりました。

セキュリティチームはアラートのノイズの大幅な削減にも成功しています。Splunkを導入する前、アナリストは複数のシステムにわたり誤検知を追跡するのに何時間も費やしていました。「Splunkのダッシュボードがあれば、問題箇所をあっという間に突き止めることができます。クエリの実行には2分とかからず、本物の脅威かどうかがすぐに確認できます。そのため、インシデントのチケットをまったく起票せずに済むことも少なくありません。このスピードによって仕事のやり方も変わりました」と、情報セキュリティアナリストは言います。

> 脅威の進展の速さを考えると、すべてを手作業で調査する余裕はありません。信頼できる自動化機能が必要です。
>
> **情報セキュリティアナリスト**

情報セキュリティ担当レベル3アナリスト兼チームスーパーバイザーは、こう付け加えます。「チームのストレスレベルも変化しました。一日中誤検知を追いかける必要は、すでになくなりました。本物の脅威やプロアクティブな取り組みに集中できます」

Splunkの相関サーチとチューニング済みの「要対応イベント」機能によって、本当に重要なアラートのみが浮き彫りになります。この機能はSplunkがマネージドサービスプロバイダーであるNew Harbor社と共同開発したものです。アナリストは本物の脅威に集中できるため、対応時間が大幅に短縮され、チームにかかるプレッシャーも軽減されました。

Splunkのダッシュボードとサーチ機能も日常業務に変革をもたらしています。以前は、ユーザーロックアウトの問題をヘルプデスクのスタッフが複数のチームにエスカレーションする必要があり、そのプロセスには数時間を要することもありました。

情報セキュリティアナリストは述べます。「今では、エスカレーションを一切行わずに、数分で問題を解決できます。これはユーザーにとって良いことですし、ITチームにとっては時間の大幅な節約になります」

アナリストは、クエリを実行してほぼ瞬時に結果を確認できるため、潜在的な問題の真偽を迅速に判断し、不要なインシデント対応を回避でき、これによって節約した時間をよりプロアクティブな取り組みに振り向けることができます。

州政府はまた、信頼性の高い安全な接続環境を提供するために、シスコのスイッチングソリューションとワイヤレスソリューションも活用しています。シスコの高度なスイッチングテクノロジーにより、高性能なネットワークトラフィック管理とシームレスなデータフローを実現しています。その一方で、シスコのワイヤレスインフラを活用して安全かつスケーラブルなWi-Fi接続を提供することで、より効率的な運用環境をサポートすると同時に、州全体に政府のデジタルサービスを届けることを可能にしています。

強固な基盤を礎に発展

州政府は、Splunkでの成功を基盤として、さらなる成果を積み上げていく計画をすでに策定しつつあります。目標は、Splunk SOARの適用範囲を拡大し、さらに多くのセキュリティワークフローを自動化して、スタッフがより価値の高い取り組みに集中できるようにすることです。また、統一的なセキュリティモデルを州全体に行き渡らせる計画もあります。目指すのは、「ステートセオリー」アプローチの下で自治体や各機関の足並みを揃え、より強力で一貫性のあるサイバー防御を実現することです。

このような取り組みによって、州政府は住民データを保護し、厳しいコンプライアンス要件を満たし、レジリエンスの高いデジタルサービスを住民に提供するための能力をさらに強化していくでしょう。

州務長官兼CIOはこう語ります。「私たちは急速な成長を遂げることができましたが、これはまだ始まりにすぎません。今後の目標は、州内すべての機関と自治体におけるレベルの底上げです」

州政府は、Splunkを中核に据えることで、すべての自治体が一貫した保護、より迅速な対応、可視性の向上によるメリットを得る未来像に向かい、確かな足取りで進んでいます。レジリエンスが強化され、一元化されたデジタル政府の実現は、もはや単なるビジョンではなく、次のステージです。

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。

25_CMP_cust_Anonymized-State_v1-JA-202607