ゴールドコースト市がコモンウェルスゲームズに向けてリアルタイムの可視化を実現

概要

ゴールドコースト市は、居住人口においてオーストラリアで第2の規模を誇る地方自治体です。3,900人の市職員が、住民と旅行者向けに、雇用機会、図書館、都市経営、水管理、廃棄物処理、観光案内を含む幅広いサービス、アクティビティ、施設を提供しています。市は、コモンウェルスゲームズ2018年大会の開催地に選ばれたことで、組織全体のセキュリティ運用を強化し、可視性を向上させる必要がありました。そのセキュリティ強化策の一環として、Splunk CloudとSplunk Enterprise Security (ES)を導入し、次の成果を達成しました。

- 複数の環境をリアルタイムで可視化
- 統合された監視機能と調査機能により、脅威が高まるサイバー環境でのリスクを大幅に緩和

Splunkが選ばれた理由

Splunkの導入前、ゴールドコースト市は、市の機関によって異なる複数のセキュリティシステムを運用していました。「複数の環境をまとめて可視化できなかったため、産業用制御システムから従来型のITシステムまで、異なるタイプの環境に対応してすべてを統合できるソリューションが必要でした。私たちが重視したのは、包括的な単一のプラットフォームで、環境ごとに異なる脅威プロファイルを異なる優先順位で監視できるか、という点です」と、ゴールドコースト市の情報テクノロジーセキュリティアドバイザーを務めるMatthew Walker氏は述べています。

サイバーセキュリティ対策への長期的なニーズを背景に、市は、サービスプロバイダーのEnosys社が提案するソリューションの一部としてSplunk CloudとSplunk Enterprise Securityの導入を決定しました。この決定をさらに後押ししたのが、コモンウェルスゲームズ2018年大会です。コモンウェルスゲームズは、イギリス連邦に所属する71の国と地域のアスリートがさまざまな競技で競い合う国際的なスポーツイベントであり、今日のサイバー環境での脅威の高まりを考えると、セキュリティ脅威を検出して対応するための体制作りは喫緊の課題でした。

大規模なスポーツイベントの開催地が直面する主な課題の1つは、大勢の人の安全確保です。市は、地元、州、国レベルのパートナーと協力して、サイバーリスクの緩和と大会参加者および地域住民の保護に取り組む必要がありました。大規模なスポーツイベントは知名度が高く、世界的な注目を集めるため、サイバー犯罪の主要ターゲットになります。そのため、サイバー攻撃のリスク対策は必要不可欠です。さらに、電力や水道などの重要インフラに障害が発生すると、イベントの成功が妨げられるだけでなく、主催者と開催地の評価を大きく下げることにもなります。

ゴールドコースト市

業種

- 公共機関

Splunkのユースケース

- セキュリティ

課題

- 異なる複数のテクノロジー環境で発生するセキュリティイベントの可視性の向上
- 脅威が高まる国際スポーツイベント期間中の脅威の検出と対応

ビジネスへの影響

- 効率的な脅威の追跡と対応により、運営に影響を及ぼすことなくセキュリティ面での成果を達成
- 組織内外の複数の環境およびシステムをリアルタイムで可視化し、実用的な運用インサイトを取得

データソース

- アプリケーションログ
- 主要なセキュリティおよびサーバーインフラ
- 運用技術と情報技術に関するネットワークトラフィック
- 外部ソース

Splunk製品

- Splunk Cloud
- Splunk Enterprise Security

市は、Splunkソリューションを導入することによって、大会期間中だけでなく将来のニーズにも対応できるサイバーセキュリティ運用のコア基盤を確立しました。

セキュリティの課題への対応

ゴールドコースト市は、パートナーエコシステムを活用してセキュリティ面で最善の成果を達成し、コモンウェルスゲームズを円滑な運営で成功に導きました。それを支えたのが、複数の利害関係者の意見を反映し、上下水道管理のための産業システムから、従来型の基幹ITシステムまで、4つの異なる環境にサービスを提供する総合的なプラットフォームです。

市は、各種の資産のオーナーと密接に協力し、各環境でのユースケースに個別対応するソリューションをSplunkで実現しました。その幅広い対応力により、ニーズの異なる環境を効果的に監視できます。たとえば、産業用制御システムではデータの可用性と完全性が最優先課題である一方、IT運用ではデータの機密性が最優先されます。市は、資産ごとの優先順位の違いを考慮して、Splunkユースケースと各環境の監視方法を開発しました。

コモンウェルスゲームズの開催期間中は、Splunk CloudとSplunk ESの柔軟性を活かして、運営のセキュリティ状況をリアルタイムで可視化し、市のセキュリティチームの協力の下で、脅威インテリジェンスを州当局、スポンサー、パートナーと共有しました。

“Splunkのおかげで私たちのセキュリティサービスの成熟度は飛躍的に向上しました。サービスが安定し、運用プロセスが確立した今は、組織内の他の領域でも新しいユースケースと新しいデータソースを活用できるよう取り組む予定です”

— Matthew Walker氏 (ゴールドコースト市情報テクノロジーセキュリティアドバイザー)

Splunkで得た将来への自信

脅威が高まる期間にSplunkソリューションで監視を強化し成功につなげたことで、ゴールドコースト市は当局全体で自信を深めることができました。コモンウェルスゲームズの開催後、市のチームはサービスをさらに調整し、盤石なものとしました。市のセキュリティ委員会はかつてないほど強力になり、新しいプラットフォームで得られる機会を活用する体制も整いました。

「Splunkのおかげで私たちのセキュリティサービスの成熟度は飛躍的に向上しました。サービスが安定し、運用プロセスが確立した今は、組織内の他の領域でも新しいユースケースと新しいデータソースを活用できるよう取り組む予定です」とWalker氏は述べています。

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

2019-Splunk-RET-City of Gold Coast-A4-JA-201911