Singapore Pools社：運用の可視性とセキュリティを変革してデジタルトランスフォーメーションを前進

主な課題

運用フレームワークが直面した重大な課題により、サービスの継続性とカスタマーエクスペリエンスの両方が脅かされていました。

主な成果

ログインテリジェンスを集約して運用とセキュリティのニーズに対応し、リアルタイムの相関付けによる可視化を通じてサービスをプロアクティブに最適化し、セキュリティ監視を自動化して脅威に先手を打てるようになりました。

業種：オンラインサービス

製品：Splunk Enterprise、Splunk Enterprise Security

ソリューション：IT運用、セキュリティ

機能：セキュリティインシデント対応、サービスの監視とインサイト取得、インシデント対応と自動化

オペレーショナルエクセレンスのための基盤を構築

シンガポールで唯一の公認ギャンブル事業者であるSingapore Pools社は、地域で特にトランザクション量の多いデジタルプラットフォームを管理しています。その技術インフラは、毎日数百万件ものやり取りを支えながら、システムの信頼性とセキュリティを維持しています。しかし、数百台のアプリケーションサーバーが3つのデータセンターに分散していたため、システムネットワークが複雑化して、効果的な監視が難しくなっていました。

アプリケーションのパフォーマンスと可用性を一元的に把握できず、技術チームは、システムの問題を調査するために複数のサーバーのデータを手動で相関付ける必要がありました。また、アプリケーションサポートスタッフは、サーバーログにアクセスするためにインフラチームにサービスリクエストを提出しなければなりませんでした。Singapore Pools社のインフラ運用担当ディレクターのAlex Chan氏によると、「手動による情報収集と事後対応的なトラブルシューティングの終わりのないサイクル」が繰り返されており、1件のインシデントへの対応に通常、数時間かかっていました。解決の遅れは、時間的な制約のある取引を行う顧客にとっても不満の種となります。

SOC (セキュリティオペレーションセンター)も可視化の課題に直面していました。アナリストは、分断されたログシステムをまたいでセキュリティの脆弱性を手動で探さなければならず、その作業に毎日8時間を費やしていました。自動の相関付け機能がなかったため、高度な攻撃パターンを検出するのも困難でした。こうした技術的な制約は、実際のビジネスリスクにつながります。アプリケーションの軽微な不具合が、検出される前にしばしば問題に発展し、利用のピーク時にトランザクションが失敗することもありました。セキュリティチームが潜在的な侵害をすばやく調査できないことで、コンプライアンス上のリスクも生じていました。最大の課題は、リアルタイムの運用インテリジェンスを獲得できなかったため、アプリケーションのパフォーマンスをプロアクティブに監視できず、アプリケーションの問題への対応が後手に回っていたことです。

こうした運用フレームワークが直面した重大な課題により、サービスの継続性とカスタマーエクスペリエンスの両方が脅かされていました。そこでSingapore Pools社は、オペレーショナルエクセレンスのための基盤を構築することを目指して、Splunkの導入を決めました。

成果

99%
問題の調査時間を短縮

80%
トランザクションの分析にかかる時間を短縮

50%
日常的な脅威ハンティングの時間を短縮

ボトルネックを解消してセキュリティ運用を変革し、プロアクティブな監視を実現

Singapore Pools社はSplunkに対して、譲れない要件を3つ設定しました。それは、ロールベースアクセス制御を備えた統合的なログ管理、脅威インテリジェンスを統合した自動セキュリティ監視、リアルタイムのパフォーマンス分析のためのカスタマイズ可能なダッシュボードです。Splunk Enterpriseは、これらのニーズに応えるだけでなく、ログインテリジェンスの一元化という期待以上の機能も提供して、デジタルインフラの管理方法に変革をもたらし、運用とセキュリティの両方のニーズを満たしました。

以前は、エンジニアが、複数のシステムをまたぐトランザクションの流れを何時間もかけて追跡していましたが、Splunkを導入した今は、すべてのサーバーのログが、きめ細かなアクセス制御を備えた単一のサーチ可能なリポジトリに統合されたため、Splunkの直感的なクエリーインターフェイスを使って2分以内には詳細な監査証跡を取得できます。また、リアルタイムの相関付けによる可視化により、チームが問題を追跡するためにばらばらな情報を手作業でかき集める必要がなくなり、サービスをプロアクティブに最適化できるようになりました。

「インフラチームは、手動でのログ取得に奪われていた数百時間分もの生産的な時間を取り戻すことができました」と、Singapore Pools社のインフラ運用担当ディレクターであるAlex Chan氏は言います。「さらに重要なのは、お客様に影響を及ぼす問題の平均解決時間を最大99%短縮できたことです」

> Splunkは当社の運用の在り方を根本から変えました。検証可能なパフォーマンスデータとセキュリティ監視により、システム全体で可視性が向上しました。運用においてこのレベルの確実性を得ることは、ビジネスに必要な信頼性を維持するために不可欠です。
>
> Singapore Pools社インフラ運用担当ディレクター、**Alex Chan氏**

運用チームは、Splunkのダッシュボードをカスタマイズして、システムの健全性に関するメトリクスをかつてないほど詳細に可視化しました。リアルタイムに情報を把握できることで、データセンター別のトランザクション量、アプリケーションの遅延傾向、ユーザーアクティビティのパターンを追跡し、異常をプロアクティブに検出して、サービス品質に影響が及ぶのを防げるようになりました。その効果は運用効率の向上に表れています。以前は4時間以上かかっていた問題の調査時間が2分で済むようになり、99%短縮されたほか、トランザクションを手動で調整していたときと比べて、トランザクション分析にかかる時間が80%短縮されました。

セキュリティ運用とカスタマーエクスペリエンスを強化

今日の脅威の状況に対応するには、セキュリティ監視を自動化することが非常に重要です。Singapore Pools社の脅威管理に変革をもたらしたのが、Splunk Enterprise Securityです。システム間のセキュリティイベントの相関付けを自動化したことにより、誤検知が60%削減されたほか、MITRE ATT&CKフレームワークとの統合により、アナリストが潜在的な脅威のコンテキストを理解できるようになりました。

SOCチームが日常的に行う脅威ハンティングは、以前は8時間かかっていましたが、4時間で完了するようになり、50%短縮されました。現在では、節約した時間を高度な検出ルールの開発に割り当てています。最も重要な成果は、シンガポールの厳格なギャンブル規制への準拠を証明するために必要な情報基盤をSplunkの監査証跡によって構築できたことです。「Splunkは、脅威ハンティングの効率を向上させるとともに、当社が必要とする厳然たる証拠を提供してくれます」と、Singapore Pools社のITセキュリティ運用担当シニアマネージャーであるEugene Teo氏は評価します。「まさに当社のセキュリティと規制戦略の基盤です」

Singapore Pools社では、プロアクティブな監視を通じて、アプリケーションサーバーのメモリーリークのパターンを検出し、障害を未然に防ぐことで、カスタマーエクスペリエンスの向上にもつなげています。システムとアプリケーションの状況を可視化したことで、トラフィックが増えるイベント時のシステムの応答性を改善したほか、強力なデータ保護の仕組みを導入していることを示すことにより、顧客からの信頼を高めることができました。

Splunkとの今後の展望

Singapore Pools社でのSplunk導入は、包括的なデータ分析がシステムの信頼性とセキュリティの具体的な向上につながることを示しています。高度な監視ソリューションを適切に取り入れれば、分散するシステムを可視化して実用的なインサイトを引き出し、事後対応的なトラブルシューティングからプロアクティブなメンテナンスへと転換できることが証明されました。監視とセキュリティの主要課題を解決したSingapore Pools社は、現在、Splunkを活用して過去のパフォーマンスデータに機械学習を適用することにより、予測的なキャパシティプランニングなどの戦略的イニシアチブを推進しています。インフラチームがシステム需要を予測できるようになったことで、大規模なスポーツイベントの開催時や宝くじの抽選時に最適なリソースを割り当てられるようになりました。

今後は、Splunk SOAR (Splunk Security Orchestration, Automation and Response)を導入して、一般的な脅威シナリオへの対応をプレイブックで自動化し、SOCの作業負荷をさらに軽減するとともに、セキュリティの自動オーケストレーションによってインシデント対応の一貫性を向上させる計画です。また、クラウド環境の拡大に対応するために、Splunkの統合サーチ機能を取り入れて、すべてのプラットフォームをシームレスに可視化することも検討しています。シンガポールのデータ主権規制が強化される中、ハイブリッドクラウドを包括的に可視化することは重要課題になっています。

Splunkは、Singapore Pools社のデジタルオペレーショナルエクセレンスの設計図を描き、規制の厳しい業界でインテリジェントなデータ管理を実現することが、いかに運用レジリエンスに変革をもたらすかを証明し続けています。Splunkの導入により、Singapore Pools社は、技術面での喫緊の課題を解消するとともに、データに基づく意思決定を実現して事後対応的な態勢から脱却し、まったく新しい運用モデルを構築しています。このことが、最高水準の規制コンプライアンスを維持しながら、安全で信頼性の高いサービスを提供するという同社のコアミッションを直接支えています。

26_CMP_cust_singapore-pools_v3-JA-202603