HKIX社：ネットワーク管理システムをプロアクティブに監視してコンプライアンスを達成

主な課題

多様化するデバイスのトラブルシューティングが後手に回り、解決時間の長さと効率の悪さが問題になっていました。

主な成果

Splunk Cloudの活用により、負担となっていた問題管理システムを刷新して、リアルタイムの状況確認、プロアクティブな情報セキュリティ、システムの包括的な可視化を実現することで、運用を改善し、ISO 27001への準拠を達成しました。

業種：通信

ソリューション：セキュリティ

今日の世界で成功を収めるにはプロアクティブなセキュリティ対策が不可欠

香港インターネットエクスチェンジ(以下HKIX、Hong Kong Internet eXchange)社がセキュリティインシデント調査の改善を最優先事項にあげた理由はそこにあります。同社は、アジアパシフィック地域最大級のインターネットエクスチェンジポイントを運営し、地域レベルのネットワークと国際的なネットワークを高速回線で簡単に相互接続するサービスを提供しています。

「ISO 27001認定取得の準備をしていたときに、コンサルタントや監査担当者から、セキュリティ管理のためにSIEM (セキュリティ情報/イベント管理)ツールを導入することを勧められました」と、HKIX社でCOO (最高執行責任者)を務めるKenneth Chan氏は振り返ります。そこで、社内の管理ツールを運用しているネットワーク管理システムのセキュリティを確保するために、予測的かつ予防的な分析を行える最適なソリューションを調査し、最終的に、データをアクションにつなげられると評判のSplunkを選択しました。

データ活用の成果

- MTTIとMTTRを数時間から数分に短縮
- チームメンバーがリアルタイムのインサイトにすばやく手軽にアクセス可能に
- 情報セキュリティ管理をリアクティブからプロアクティブなアプローチに転換

プロアクティブなインシデント対応によってチームの負担を軽減

Splunkの導入により、HKIX社のチームはインシデントをプロアクティブに調査できるようになりました。Splunk Cloudによってシステムの挙動分析とログ監視がリアルタイムで行われ、異常な傾向が追跡されるため、チームはシステムの運用状況をすばやく確認して、問題がシステム障害や重大な被害に発展する前に対応できます。

Chan氏とそのチームは、以前は問題の発生時にネットワーク管理システムの脆弱性や潜在的なリスクを特定するだけでも、スクリプトを記述して数ギガバイトにのぼるログを調査したり、キーワードを1つずつ検索して記録を照合したりしなければなりませんでした。しかし今は、その手間から解放されました。「今日では問題を先回りして回避しています」とChan氏は胸を張ります。また、Splunk Security Cloudで、異常な挙動を検出するルールベースのアプローチを活用することで、セキュリティイベント調査を効率化して、コンプライアンスニーズに対応できるようにもなりました。

Splunk Cloudは問題対応の時間短縮に役立っているだけでなく、SaaS運用モデルのメリットを活かして、オンプレミス製品では避けられない導入の課題を解消し、シームレスな展開を可能にしました。「購入後1週間以内にポータルを利用できるようになりました。システムにログインした後、簡単なデータオンボーディングワークフローに従うだけで、スムーズに本番稼動へと移行できました」とChan氏は説明します。システム監視とトラブルシューティングからメンテナンスとアップデートまで、すべての作業の負担を軽減したことで、チームはより付加価値の高い業務に集中できるようになりました。

何時間もかかるプログラミングからリアルタイム分析へ

HKIX社では、Splunk Cloudの導入以来、ネットワーク管理システムを統合ビューで可視化しています。「以前は、システムの状況を示すチャートやグラフが入ったレポートを作成するために、何時間もかけてプログラムスクリプトを記述していました」とChan氏は振り返ります。しかし今日では、ボタンを1つクリックするだけで、豊富なグラフを含むインタラクティブなSplunkダッシュボードに、組織のセキュリティ環境に関するさまざまなメトリクスが瞬時に表示されます。さらに、表示方法を柔軟にカスタマイズすることもできます。

HKIX社のネットワーク管理環境では、多数のサーバー、エンドポイント、ファイアウォール、WindowsやLinuxオペレーティングシステムのログが生成されますが、そのすべてをSplunkプラットフォームに集約して1つの画面で管理できます。セッションログの収集、検索、分析が容易になったことは、組織のセキュリティ環境の強化にもつながっています。

Splunkを導入したことで、HKIX社ではセキュリティ管理が大幅に改善し、MTTI (平均特定時間)とMTTR (平均対応時間)が数時間から数分に短縮されました。さらに、Splunk Cloudの導入効果として、ユーザーがデータを手軽に活用してアクションにつなげられるようになるとともに、HKIXチームが大規模なリポジトリにアクセスしてさまざまなベストプラクティスやインサイトに富んだユースケースを参照できるようにもなりました。

> 私たちは成功するために利便性、正確さ、効率を向上させる必要があります。Splunkソリューションはまさにその期待に応えてくれています”
>
> **Kenneth Chan氏**、HKIX社COO
> (最高執行責任者)

「Splunkナレッジベースから簡単にダウンロードできる大量のセキュリティ分析コンテンツが特に気に入っています。これらのコンテンツは、情報セキュリティに対する視野を広げてくれます」とChan氏は評価します。「さらに、SaaSモデルのSplunk Cloudは、地理的な冗長性やオフサイトのディザスタリカバリという形でデータ保護を新しいレベルに引き上げ、ハードウェアプラットフォームの管理負担を最小限に抑えてくれます。これにより、複数のデータセンターをコスト効果の高い方法で運用できるようになりました」

成長に応じて拡張し、クラウドトランスフォーメーションをさらに推進

Splunk Cloudを使用するようになってから、HKIX社は、ISO 27001が規定する要件に準拠できるようになりました。当時、この情報セキュリティ管理標準の認定を受けたインターネットエクスチェンジ組織はまだ珍しい存在でした。HKIX社は今後、Splunk Cloudを拡張して、より多くのデータを取り込み、情報セキュリティライフサイクルをさらに最適化する計画です。「結局のところ、ISO認定を受けるということは、継続的な改善を続けていくということなのです」とChan氏は言います。「Splunkは、私たちが目指す改善を常に後押ししてくれます」

HKIX社は現在、ローカルや地域レベルのインターネットサービスプロバイダー、コンテンツプロバイダー、データセンター、DDoS対策プロバイダーを含め、さまざまな業種の約340社の提携企業をサポートしています。「当社の事業は日々拡大し、ネットワークトラフィックは年間で約30%ずつ増えています」とChan氏は説明します。HKIX社は、Splunkによって安定した基盤を手に入れ、増え続けるログ、システム、セキュリティツールをシームレスに管理し、クラウドジャーニーを通じて着実に成長しています。

Splunkの無料トライアルを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。

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

22-22986-Splunk-HK Internet eXchange-A4-CS-JA-202212