Unitel社：インシデント対応を2倍迅速化して顧客の常時接続を維持

主な課題

Unitel社では、システムを十分に可視化できていなかったため、インシデントをすばやく解決することが難しく、機密データの保護に不安がありました。

主な成果

複雑な手動プロセスを自動化し、環境を包括的に可視化したことで、インシデントにリアルタイムで対応できるようになり、セキュリティ侵害のリスクを低減できました。

業種：通信

ソリューション：セキュリティ、プラットフォーム

モンゴルの人口の大半が利用する通信を維持するのは至難の業

モンゴルの大手情報通信テクノロジーグループであるUnitel社は、数十万の契約者にモバイル通信サービスを提供しています。そのネットワークのレジリエンスを確保するには、すべてのデジタル資産とネットワークリソースを保護するとともに、情報の機密性、完全性、可用性を維持する必要があります。しかし、以前使用していたSIEM製品はデータ分析、監視、脅威インテリジェンス機能が不十分だったため、インシデントの調査と対応を効果的に行えず、サイバー脅威がビジネス上の深刻なリスクになっていました。

成果

最大**50%**
SIEMの効率を向上

2〜3倍
インシデント対応を迅速化

50%
ログ管理を効率化

Unitel社は、状況を改善するために新しいSIEMソリューションが必要だと判断しました。求められるのは、サイバーセキュリティ態勢をフルスタックでリアルタイムに可視化し、避けられないインシデントが発生してもシステムをすばやく復旧できることです。そこで、10社のソリューションプロバイダーを対象に複数回の技術評価を実施した結果、Splunkを選択しました。「Splunkは、当社のセキュリティ運用に求められる柔軟性、カスタマイズ性、拡張性、使いやすさ、統合機能のすべてが優れていました」と、Unitel社でCISOを務めるMendsaikhan Amarjargal氏は言います。「セキュリティ業界のソートリーダーとしてもSplunkを高く評価しました」

包括的な可視化を実現

Unitel社のセキュリティ要件にはさまざまな要素が含まれます。「当社は、サイバー脅威や脆弱性の悪用を防ぐための適切なセキュリティコントロールを維持しながら、セキュリティインシデントの監視と対応に取り組む必要があります。また、機密データを体系的に管理するためのポリシーと手順を確実に適用し、改善していく必要もあります」とAmarjargal氏は説明します。

これらの要件への対応に加えて、Unitel社では統合されたデータ分析プラットフォームも必要としていました。そこでSplunkプラットフォームにログを集約したところ、ログ管理が大幅にシンプルになり、ネットワークトラフィック、侵入検知ログ、エンドポイント保護や脅威インテリジェンス情報などのすべてのデータソースを対象としたログの検索と取り込みにかかる時間が半減しました。

「Splunkのおかげで、組織のサイバーセキュリティ態勢を包括的に可視化し、全体像を把握できるようになりました。これにより、セキュリティ脅威をリアルタイムで検出して対応できるようになり、セキュリティ侵害のリスクとセキュリティインシデントの影響を低減できました」とAmarjargal氏は評価します。「さらに、Splunkのパートナーであるunity社での支援でソリューションをスムーズに導入できました。エンジニアに初期トレーニングを実施してもらい、最適なサポートを受けられるよう手配してもらえたことも大きな助けになりました」

> 以前は手動で作業していたため、1つの問題を特定して修正するのに1時間ほどかかっていました。スピードが求められる今日の社会で1時間は長すぎます。Splunkプラットフォームではデータが自動的に相関付けられて分析されるため、インシデント対応の速度が2 ～ 3倍上がりました”
>
> Unitel社CISO
> **Mendsaikhan Amarjargal氏**

効率が飛躍的に向上

Splunkの導入以来、Unitel社では、問題解決にかかる時間が大幅に短縮され、システムの稼働率が向上しました。「以前は手動で作業していたため、1つの問題を特定して修正するのに1時間ほどかかっていました。スピードが求められる今日の社会で1時間は長すぎます」とAmarjargal氏は言います。「Splunkプラットフォームではデータが自動的に相関付けられて分析されるため、インシデント対応の速度が2 ～ 3倍上がりました」

インシデント対応の迅速化はビジネス全体に良い影響をもたらしています。問題による顧客への影響が最小限に抑えられ、解決も迅速で、デバイスのバッテリーを無駄に消費することがなくなったため、顧客満足度が向上しました。社内でも、セキュリティイベントの相関付けが自動化されたことで、手作業に費やしていた時間を節約でき、システムの統合とデータの解析にかかる時間が半分になりました。

「Splunkは、ネットワーク、インフラ、アプリケーション、データの保護に役立つ、強力で信頼できるサイバーセキュリティソリューションです。脅威への備えにおいても、発生した問題からの復旧においても、以前より体制が強化されました」とAmarjargal氏は説明します。「Unitelは、モンゴルで最大の情報通信テクノロジー (ICT)企業として、通信事業だけでなく、電話、インターネット、放送、OTT (ネット配信)などのメディアサービスも手掛けています。Splunkの優れたカスタマイズ性と柔軟性のおかげで、複数のソースのデータを簡単に処理して、ビジネスのデジタルレジリエンスを維持できています」

Splunkで新しい可能性を切り開く

優れた製品機能だけでなく、モンゴルに多くのSplunkユーザーがいることも、Unitel社にとって思いがけないメリットでした。「地元企業のさまざまなユースケースから学び、Splunkの価値を最大限に引き出すことができました」とAmarjargal氏は説明します。すぐに使えるセキュリティユースケースに加えて、SplunkbaseのAppを活用したユースケースもUnitel社独自のニーズを満たすために役立っています。

「現在は、Splunkの活用範囲を他の領域に広げる計画を立てています。その1つがカスタマーエクスペリエンス管理で、顧客向けサービスを改善し、顧客離れを防いで、新たな収益の柱を開拓したいと考えています」とAmarjargal氏は付け加えます。「また、SplunkをIoT分析プラットフォームとして使用して、デバイスのパフォーマンスを監視し、異常を検出して、運用効率の向上を目指すことも検討しています。さらに、ネットワークパフォーマンス監視、異常検出、トラブルシューティングにもSplunkを活用したいと考えています」

Splunkパートナー
Unity Data Technology社

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

23-207662-Splunk-APAC Unitel Case Study-CS-SS-JA-202308