M bank：プロアクティブなリアルタイムの可視化で、デジタルバンキングのセキュリティを強化

主な課題

M bankは、分散型マルチプラットフォームのコンピューティング環境全体にわたるリアルタイムの可視化ができなかったため、サイバー脅威に先手を打つための強力なセキュリティ態勢の維持に困難を抱えていました。

主な成果

Splunk SIEMプラットフォームでセキュリティを一元的に可視化することにより、プロアクティブな脅威検出と対応、リスクの低減、デジタルレジリエンスの強化、顧客からの信頼の向上を実現しました。

業種：金融サービス

ソリューション：セキュリティ

製品：Splunk Enterprise Security

機能：SIEM/セキュリティ分析、統合セキュリティ運用、セキュリティインシデント対応、インフラ監視とトラブルシューティング、インシデント対応と自動化、オブザーバビリティのログ

後手の対応から先手の対応へ：プロアクティブな脅威ハンティングでサイバーセキュリティを強化

モンゴルを拠点とするM bankは、完全にデジタルなネオバンクとして、金融サービスのエクスペリエンスをモバイルファーストサービスで刷新することを目指しています。支店がなく店頭での行列もなく、営業終了時間さえないため、顧客はスマートフォンアプリやWebプラットフォームを利用して、どこからでも資金を管理できます。

M bankはサイバーセキュリティを常に最優先事項としていますが、同行のセキュリティオペレーションセンター (SOC)は、異機種が混在した分散型コンピューティングインフラの監視に苦労していました。このインフラを構成していたのは、100以上のサイロ化されたホスト、オンプレミスとクラウドベースの運用システム、アプリケーションログです。これらのプラットフォームの多くは、各部門が独自の戦略に基づいてさまざまなプログラミング言語で自力で開発したもので、ログの相関付けや情報の共有が不可能でした。

異常の調査は手動で行う必要があり、SOCチームはシステムごとにログを1件ずつ確認していました。これは膨大な手作業を必要とする業務でしたが、さらに困ったことに多くの場合、重大なインシデントやその発生場所を把握できませんでした。M bankはこうした状況に対応するため、SIEM (セキュリティ情報/イベント管理)プラットフォームを導入し、セキュリティの可視性を高めることにしました。そこで選んだのが、パートナーのUnity Data Technology社が提供していたSplunkです。Splunk Enterprise Security (ES)は、パフォーマンスと使いやすさが際立っていました。最も重要なのは、これによって、可視化できなかったものをリアルタイムで可視化し、プロアクティブな脅威ハンティングを実現できたことです。

成果

- **短縮**：セキュリティ管理にかかる時間を数時間から数秒に
- **50%**：インシデントの検出と対応を高速化
- **強化**：事業継続性とデジタルレジリエンス

「何も知らない」から「全体像を把握」へ

Splunk Enterprise Securityはガートナー社2025年SIEM部門のマジック・クアドラントで11回連続のリーダーに選出されており、さまざまなソースのデータを一元管理し、運用状況をリアルタイムで可視化する統合的なSIEMプラットフォームをM bankに提供します。また、セキュリティ態勢、インシデントレビュー、脅威アクティビティなどの事前構築済みダッシュボードによって、SOCの運用効率化を支援します。これにより、同行SOCチームはセキュリティ態勢全体を監視し、主要なセキュリティデータや相関関係をリアルタイムで確認できるようになりました。

また、Splunkの導入により、不正行為の検出、異常アクセス、インフラセキュリティ監視といった特殊なユースケースに対応するカスタムダッシュボードの開発も可能になりました。さらに同行SOCチームは、これらのダッシュボードをカスタムのSplunkアプリとしてパッケージ化することで、再利用やロールベースのアクセス制御を可能にし、ライフサイクル管理を改善しました。

Splunk Enterprise Securityをこれらのカスタムダッシュボードと組み合わせれば、リアルタイムのログ分析、セキュリティ監視、トラブルシューティングを単一のインターフェイスで行えるようになります。また、Splunkの予測分析機能を利用することにより、行動データ分析を通じて異常や脅威を早期に検出できます。

> **Splunkは、強固なセキュリティ態勢を維持し、サイバー脅威から組織を守るプロアクティブで効率的な手段を構築するのに役立っています。**
>
> M bank、情報セキュリティ部門責任者、Nyamdorj Miya氏

M bankで情報セキュリティ部門の責任者を務めるNyamdorj Miya氏はこう述べています。「Splunkを利用すれば、すべての要素をつなげ、あらゆるセキュリティリスクを完全に把握し、原因を迅速に突き止めることができます。IT環境で何が起きたのか把握できない状態だったところから、サイバーセキュリティ態勢を明確に把握できる状態にまでなりました。初めて、リアクティブなセキュリティ管理からプロアクティブな脅威ハンティングへと移行したのです」

Miya氏は続けてこう強調しています。「実現するだけではなく、効率も重要です。以前は、インシデントの根本原因を突き止めるのに、SOCチームがあらゆるシステムやアプリケーションのログをすべて手動で確認していました。そのため少なくとも1時間、ときには1日かかるのが普通でした。今では、異常のチェックやインシデントのレビューは、Splunkダッシュボードの自動操作によって数秒で完了します」。実際に脅威の検出と対応がどれくらい効率化されるかは、状況によって異なると同氏は考えています。それでも、同行では「MTTD (平均検出時間)」と「MTTR (平均対応時間)」が平均で50%減少しました。

運用の効率化とデジタルレジリエンスの強化

M bankはSplunkによって、リアルタイムでプロアクティブな脅威ハンティングを実現しただけでなく、業務の効率化を達成できました。「Splunkは、これまでにないシンプルさと利便性を提供してくれます」とMiya氏は言います。Splunkは運用が比較的簡単で、サーチ言語の複雑な構文を学ぶ必要もありません。

同氏が他に重宝しているのは、Splunkなら単一ベンダーによる単一ツールで複数のセキュリティニーズを管理できることです。Splunkのリスクベースアラート機能により、同行SOCは資産やユーザーに対してその重要度に応じたリスクスコアを割り当て、セキュリティ調査の優先順位をより的確に決定できるようになりました。

また、同行の経営陣も、従来にはなかったレベルの可視性を獲得しています。「Splunkは複雑なセキュリティデータを実用的なインサイトに変換して、新たな可視性を提供してくれます。これにより、取締役会のメンバーはより充実した情報に基づいて意思決定ができるようになりました。このことは、セキュリティインシデントからの迅速な回復やインシデントのプロアクティブな阻止を目指したセキュリティ戦略の最適化に役立っています。その結果、デジタルレジリエンスを強化し、運用リスクをさらに低減し、事業継続性を確保できているのです」と、Miya氏は付け加えます。

デジタル時代における安心の確保

安心感が顧客満足度とロイヤルティを高める重要な要素となる中、M bankはSplunkによって、テクノロジーの進歩を真の顧客価値に転換する力を得られました。

たとえば、Splunkを利用してセキュリティ管理を飛躍的に向上させた結果、同行は情報セキュリティ管理システムの国際標準であるISO/IEC 27001やデータセキュリティ規格のPCI DSSといった国際的規制に準拠できるようになりました。「これにより、進化を続けるサイバー脅威から顧客の金融情報や機密データを保護する当行の能力について、顧客からの信頼は高まっています」と、Miya氏は説明します。

Splunkを導入したことにより、M bankはデータドリブンなセキュリティ分析でデジタルバンキングを強化する先駆者となりました。同行はさらに、データの中に潜む「見えなかったものを見る」ようにして、将来的により迅速かつ賢明な意思決定を実現するために、Splunk AI Toolkitの利用可能性を検討しています。こうした取り組みは、次世代のデジタル銀行として、顧客の経済的幸福を実現し、健全な金融習慣を育み、金融サービスのカスタマーエクスペリエンスを刷新するというM bankの使命と一致するものです。

26_CMP_cust_M-Bank_v2-JA-202609