東亜銀行：Splunkでグローバルなセキュリティ管理を実現してデジタルレジリエンスを強化

主な課題

東亜銀行では、分散環境の可視性の低さが、FinTechイニシアチブの要であるデジタルレジリエンスの構築の妨げになっていました。また、世界各地の支店のチームが独自にSIEMを運用していたため、トラブルシューティングで手動作業が必要になり、時間がかかることも問題でした。

主な成果

香港の銀行業界で初めてクラウドベースのSIEMを導入し、Splunk Cloud Platformによって組織内のSIEMを統一することで、ネットワークを包括的に可視化するとともに、従業員の業務効率を改善しました。

BEA東亞銀行

業種：金融サービス

ソリューション：セキュリティ、プラットフォーム

テクノロジーを最大限に活用して組織をまとめる

上場企業として100年以上の歴史を持つ香港の金融サービスグループ、東亜銀行(BEA)は、世界各国に150以上の支店を展開し、幅広いバンキングサービスを提供しています。テクノロジーイノベーションを精力的に推進する同行は、**BEA**STイニシアチブを立ち上げ、各地で地元のスタートアップと積極的にコラボレーションして、活気あるFinTechエコシステムを築いています。

テクノロジー面で常に最先端を行く東亜銀行では、10年以上前からSplunk Enterprise Securityを使用してオンプレミスのインフラを監視してきました。そのため、世界の全支店でSIEM (セキュリティ情報/イベント管理)を統一する決断をしたときも、パートナーとしてSplunkを選択しました。今日では、Splunk Cloud Platformを導入し、香港でクラウドベースのSIEMを導入した銀行の先駆けとして、組織のビジネス基盤となる環境の包括的な可視化を実現しています。

システムの統一によって効率と生産性を向上

「各支店でSIEMシステムの稼働準備を1カ月以内に終えられるようになりました」と、東亜銀行でインフォメーションテクノロジー部門/FinTech開発部門の責任者を務めるStephen Leung氏は言います。「以前はインフラの整備だけで数カ月かかっていました」

グローバルな可視化を実現したことで、香港本店のITチームはすべての支店のセキュリティデータをリアルタイムで簡単に入手できるようになりました。以前は各支店のチームが独自にSIEMシステムを構築してセキュリティ監視と分析を行い、セキュリティ関連の問題が検出されたときは本店に問い合わせていました。しかし今日では、本店とすべての支店でSplunkダッシュボードをいつでも共有できます。これにより、各支店のチームがそれぞれのセキュリティ態勢を包括的に可視化し、急速に変化する脅威の状況に対応して、大きな被害につながる前に問題をプロアクティブに解決できるようになりました。

成果

1カ月
各支店でSIEMの導入にかかる期間を数カ月から1カ月に短縮

包括的
組織の分散環境を包括的に可視化

ゼロ
問題の調査と対応での手動作業をゼロに削減

「Splunk Cloud Platformへの移行により、ソースがクラウドかオンプレミスかを問わず世界中の各支店で生成されるすべてのセキュリティ関連イベントを集約して、セキュリティ管理を統一できるようになりました」とLeung氏は評価します。「香港を皮切りに、現在、Splunk Cloud Platformの導入範囲をマカオ、台湾、シンガポール、英国、米国などの各支店に段階的に拡大しています」

東亜銀行の統一戦略とSplunk Cloud PlatformによるSaaSアプローチの導入は、IT運用チームの効率と生産性の向上に役立っています。「Splunk Cloud Platformは導入が簡単で、定期的なメンテナンスの手間もありません。また、拡張性に優れているため、進化するデータニーズにも十分に対応できます」とLeungは言います。さらに、導入期間の短縮や設定の簡素化だけでなく、オンプレミスソリューションの導入やアップグレードに必要だった手動作業を削減できるというメリットも生まれました。

> Splunkがあれば、デジタルトランスフォーメーション推進の流れについていくだけでなく、その最先端を走り続けることができます”
>
> 東亜銀行インフォメーションテクノロジー部門/FinTech開発部門責任者、Stephen Leung氏

自動化によって負担を軽減し俊敏性を向上

「予防は治療に勝る」とよく言いますが、これはセキュリティにも当てはまります。東亜銀行では、インシデントの調査と対応のオーケストレーション/自動化ソリューションであるSplunk SOARを活用して、セキュリティアナリストのアラート対応の負担を軽減し、リアルタイムの状況把握とタイムリーな脅威インテリジェンスの利用を通じて問題を未然に防げるよう体制を整えています。また、繰り返しの多い手動のワークフローを排除することで、より戦略的な取り組みやミッションクリティカルな目標の達成に集中できるようにしています。

「Splunkで生成される実用的なインサイトは、セキュリティ関連の判断の向上だけでなく、本店とすべての支店で24時間安定した運用を維持するためにも役立っています」とLeung氏は説明します。Splunkは組織レベルでも、リアルタイムのトラブルシューティング、変化する脅威の状況に合わせた対応、クラウド活用による俊敏性の維持という3つの点で東亜銀行のレジリエンス強化を支え、それが、バンキングサービスを利用する顧客のエクスペリエンス向上につながっています。

デジタルレジリエンスで新境地を切り拓く

東亜銀行は何年もの間、FinTechのイノベーションを精力的に推進してきました。Splunkを通じてクラウドベースのSIEMを導入した同行は、その先駆者として香港金融業界の良い手本になっています。

「デジタルレジリエンスはFinTech戦略の実現に不可欠です」とLeung氏は言います。「当行は変化の激しいデジタル世界で成功するために、サイバーセキュリティの強化とともにイノベーション文化の育成に力を入れています。その一環として、Splunkを活用することにより、自動化を推進して効果的な監視とパッチ適用を実現しながら、セキュリティのオーケストレーションを継続的に最適化して脅威の検出と対応を効率化しています」

将来に目を向けると、Splunk Cloud Platformは今後の成長に対応する柔軟性も備えています。SplunkのSIEMソリューションはクラウドネイティブテクノロジーを念頭に置いて設計されているため、常に最新機能を利用し、使用パターンに合わせて柔軟に拡張できます。東亜銀行のジャーニーは始まったばかりです。そしてSplunkは、今後もその取り組みに伴走して支援し続けていきます。

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

23-75748-Splunk-APAC BEA-CS-SS-JA-202305