ACE社：セキュリティ基準への対応と10%のコスト削減を実現しながらパフォーマンスを向上

主な課題

Splunkの導入前、ACE社では複数のデバイスから収集したセキュリティデータを統合して相関付けることができなかったため、マルチクラウド環境を十分に可視化できず、イベント対応が遅れる一方で人件費が増大していました。

主な成果

Splunkの導入により、セキュリティ監視が強化され、迅速な脅威ハンティングとリアルタイムのイベント対応が可能になるとともに、10%のコスト削減、システムメンテナンスの効率化、業務効率の向上、ユーザー資産のセキュリティ強化を実現しました。

ACE Exchange

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

適切なセキュリティプラットフォームがないことで問題が多発

ACE Exchange社は、2018年に設立された台湾初の暗号資産取引所です。ビットコイン(BTC)、イーサリアム(ETH)、テザー (USDT)とニュー台湾ドルを交換できます。DeFi (分散型金融)からCeFi (中央集権型金融)への資金移動の促進を目的とした多数の金融ツールと、さまざまなクロスチェーンサービスを提供しています。広範なブロックチェーントランザクションとインキュベーションエコシステムをサポートするために、ACE社は、効果的なセキュリティ監視プラットフォームを必要としていました。そのプラットフォームには、ユーザーの資産を守り、コンプライアンスと事業継続性を確保しながら、同社の着実な成長を後押しすることが求められます。

しかし、当時使用していたオープンソースの分析プラットフォームは、ACE社が求めるレベルに達していませんでした。データを統合することも、異常なトランザクションを検出するためにログを相関付けることも、拡大し続けるマルチクラウド環境でのリソースの使用状況や割り当て状況を監視することもできませんでした。その結果、同社のセキュリティチームは、1つの問題を調査するだけでも多数のコンソールにログインしなければならず、MTTDが長引き、高度な脅威を予測するのも困難になっていました。また、プラットフォームの保守にも手間がかかり、データのオンボーディングやダッシュボードのカスタマイズに人手が必要で、チームの負担が増大し、ハードウェアの機能を十分に活用できていませんでした。

複雑な環境を詳細に可視化するために、ACE社はSplunkを導入し、結果として、セキュリティ態勢の強化、脅威ハンティングの精度向上、運用効率の向上を実現できました。

成果

70%
セキュリティ監視に必要な人間の介在を削減

10%
使用していないクラウドリソースを開放してコストを削減

24時間365日
運用状況をリアルタイムで可視化して常時稼働を実現

セキュリティ監視を一元化して生産性を向上

「Splunkのおかげでついに理想のセキュリティ分析プラットフォームを手に入れることができました」と、ACE Exchange社の最高情報セキュリティ責任者であるFngi Hsu氏は胸を張ります。Splunkは、同社のマルチクラウド環境の複雑さを克服するために完璧なソリューションでした。Google Cloud、アマゾン ウェブ サービス(AWS)、Microsoft Azureなど、同社が使用するすべてのパブリッククラウドプラットフォームから自動的にログデータを収集し、組織全体のセキュリティ態勢を可視化して、脅威対応の

迅速化、リアルタイムのイベント対応、監視の信頼性向上を実現したのです。また、セキュリティチームは、Splunkの直感的なダッシュボードを使ってさまざまなタイプの脅威を予測、検出し、対応できるようになりました。

Splunkの導入により、セキュリティチームの負担は大幅に軽減されました。「シンプルで覚えやすいSplunkサーチ処理言語により、古いプラットフォームでのサーチの遅さの問題が解決しただけでなく、ダッシュボードやアラート設定を柔軟に調整して組織のセキュリティニーズに対応できるようになりました。特に、ISO27001:2022プラクティスの新しい『A.8.16 アクティビティの監視』コントロール項目に対応できたことは大きいです」とHsu氏は説明します。「Splunk Mobile Appも大いに役立っています。外出先でもダッシュボード、レポート、アラートに単一のインターフェイスからアクセスできます。以前は夜間にスタッフがオフィスに待機していましたが、今ではいつどこにいてもSplunkプラットフォームを利用できます」

> Splunkのおかげで最適なハイブリッドマルチクラウドジャーニーを実現し、ROIを最大化できました”
>
> ACE Exchange社最高情報セキュリティ責任者、**Fngi Hsu氏**

ACE社では、サイバー脅威を予測してセキュリティインシデントをアラートする機械学習モデルの開発にもSplunkを活用しています。これによって定型的な手動作業を減らすことで、以前は7日間かかっていた業務を2日で終えられるようになりました。生産性が向上したことで、チームメンバーがより重要な業務に集中できるようになり、組織全体としても他の戦略的なセキュリティイニシアチブにリソースを回す余裕ができました。

リアルタイムのリソース管理でROIを最大化

ACE社では、マルチクラウド環境の運用状況の可視性が向上したことで、リソース管理も改善されました。Splunkでクラウドサービス全体の支出に関する有用なインサイトを獲得することで、不要なサービスをリアルタイムで特定してリソースの割り当てを変更できるようになり、全体のROIが向上しました。Hsu氏によると、使用していないクラウドリソースを特定して開放することで、10%以上のコスト削減を達成しています。

Splunkの使いやすさは組織全体で評価されています。「クラウドとオンプレミスのどちらの環境でも幅広いブランドの製品に対応した、すぐに使えるAppが多数提供されているため、データのオンボーディングと統合を効率的に行えます」とHsu氏は説明します。「継続的な保守はAppをアップグレードするだけです。一方で、複数の監視ソフトウェアを導入しなくても、単一の情報源を、情報セキュリティ、IT運用、ビジネス分析など、幅広いユースケースに活用できます」

ジャーニーは続く

SplunkによってACE社のサイバーセキュリティは大きく向上しました。しかし、これはほんの始まりにすぎません。Hsu氏は今後の展望について、「Splunkを活用してさらに進化し、さらに多くを成し遂げます。次のステップは、セキュリティ自動化のレベルを上げることです」と話しています。その実現のために、Splunk SOARを導入してセキュリティ運用の効率をさらに向上させ、インシデントの調査とシステムの復旧を加速することを目指しています。また、Splunkを活用して不正行為を検出し、異常な社内トランザクションを削減して、レジリエンスを維持すると同時に、未来の暗号通貨取引に向けた新しい道を切り拓くことも計画中です。

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

23-301744-Splunk-ACE Exchange APAC PDF_CS-JA-202311