ASL社：プロアクティブな脅威管理でセキュリティインシデントを40%削減

主な課題

運用の俊敏性を損なうことなく、さまざまなシステムから収集したインテリジェンスやインサイトを統合および相関付けるとともに、データ分析を自動化して、リアルタイムの脅威検出を強化する必要がありました。

主な成果

データの統合とインテリジェンスの活用に優れたSplunkの監視プラットフォームを導入して、脅威のプロアクティブな検出と対応、効率の最適化、セキュリティインシデントの削減、重要なシステムの保護を実現しました。

業界：テクノロジー

ソリューション：プラットフォーム、セキュリティ

製品：Splunk Enterprise、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、インシデント対応と自動化

次世代のセキュリティで顧客の信頼を高める

優れたITサービスとイノベーションを提供し続けるAutomated Systems (H.K.) Limited (ASL)社は、最先端のソリューションを通じて数々の企業を支援しています。サイバー脅威が高度化する時代に顧客の信頼を高めるために、同社はSOC (セキュリティオペレーションセンター)の戦略的な強化に乗り出し、相互につながる多様なシステム全体をリアルタイムでプロアクティブに監視して、既存のセキュリティ体制におけるスピードとインテリジェンスを新たなレベルに引き上げることを目指しました。

セキュリティへのコミットメントは顧客とのパートナーシップの基盤であるとASL社は明言しています。拡大するハイブリッドIT環境の複雑さに対処するために、同社では、従来の監視アプローチからの脱却に重点を置いています。そこで、Splunk EnterpriseとSplunk Enterprise Securityを導入して、データドリブンでインテリジェンスを活用した新しい監視プラットフォームを構築しました。

Splunkの統合プラットフォームの導入によりファイアウォール、サーバー、アプリケーション、クラウドリソースなど、さまざまなソース間でデータをシームレスに相関付け、運用の課題を戦略的な機会に転換できるようになったと同社は説明しています。また、セキュリティ、生産性、コンプライアンスのどの領域でも、顧客の要求の進化に合わせてセキュリティ態勢を強化できるようになったと評価しています。

成果

2分の1
トラブルシューティングの時間短縮率

40%
1カ月あたりのセキュリティインシデントの減少率

60%
セキュリティ監視に必要な人員の削減率

ボトルネックを解消してプロセスを効率化

ASL社では、Splunk Enterpriseは中央集約型プラットフォームとして機能し、多様なシステムやアプリケーションで生成されるログデータを一元的に収集、インデックス化、分析するために活用されています。これにより、データの管理と分析が簡素化されただけでなく、データからシステムのパフォーマンスに関する実用的なインサイトを得ることで、タイムリーかつ効果的に異常を検出し、問題を修正できるようになりました。同時に、Splunk Enterprise Securityによって、ファイアウォール、ウイルス対策ソリューション、EDR (エンドポイント検出/対応)ソリューションなどのセキュリティツールから収集したセキュリティ関連データが自動的に相関付けられます。

Splunkプラットフォームは、すべてのプロセスを効率化して、セキュリティとパフォーマンスの向上を支援します。ASL社では、重大なセキュリティインシデントに24時間体制で対応しながら、悪質なアクティビティや潜在的な脅威をプロアクティブに検出しています。また、ITのトラブルシューティングは以前の半分の時間で完了するようになりました。

さらに、同社は高度な可視化を実現するダッシュボードを使って、すべてのサーバー、ネットワークデバイス、ストレージシステム、仮想化環境、クラウドリソースの健全性を包括的に把握しています。カスタマイズされたアラートやロールベースのダッシュボードを個別に調整することで、チームは対応ワークフローを迅速化できます。特にトランザクションの急増時に、顧客の行動の傾向を追跡しながら、パフォーマンスのボトルネック、キャパシティの問題、インフラ関連の異常をプロアクティブに特定できるようになったのは大きなメリットです。これにより、リソースを拡張してSLA (サービスレベル契約)に準拠しながら、最適で価値の高いサービスを顧客に提供できます。

> Splunkのおかげで、SOCは、最新の脅威インテリジェンスを活用したセキュリティの強化、インシデント対応の迅速化、継続的な監視を実現して、ステークホルダーの信頼を高めることができました。
>
> **Automated Systems (H.K.) Limited社**

ハイブリッド環境でのプロアクティブなセキュリティ対策の最適化

Splunk EnterpriseとSplunk Enterprise Securityを組み合わせることで、ASL社は、セキュリティインシデントを1カ月あたり40%削減しました。Splunkは、同社の無停止で稼働するITインフラ全体で異常をリアルタイムで検出する(プロアクティブな脅威ハンティングの基盤)だけでなく、データの統合を自動化します。これにより、同社はウイルス対策システム、EDRシステム、ファイアウォールなど、さまざまなソースから収集したセキュリティイベントを統合・分析できるようになりました。

ASL社はもともと、セキュリティ強化の取り組みの一環として、包括的な可視化を実現するソリューションを探していました。そして、他の製品と比べ、特に際立っていたSplunkがすぐに選ばれました。分析、ハイブリッド環境の監視、製品イノベーションにおけるSplunkのリーダーシップが同社のビジョンと完全に一致している点が評価されたのです。さらに、最も重要な点として、Splunkによって相関付けが自動化され、実用的なインテリジェンスをリアルタイムで獲得できるようになったことで、データの俊敏性が飛躍的に向上したことが高く評価されています。

ASL社では、新たな脅威にすばやく対応し、セキュリティ対策を継続的に強化できるようになりました。同社は、Splunkが目標達成に役立つだけでなく、テクノロジーチームの専門知識を補完し、より効果的な形でイノベーション、生産性、インテリジェンスを再定義できる点を強調しています。

データを戦略的成果に変える

Splunk導入の成功要因には、高度な分析機能と機械学習機能もあります。これにより、運用パターンの追跡、予測分析、情報に基づくリアルタイムの意思決定が可能になり、セキュリティリスクの軽減とITインフラの可用性の維持につながっています。たとえば、トランザクションの急増やキャパシティのボトルネックを検出し、リソースをプロアクティブに増強して、ピーク需要時でもSLAを維持できるようになりました。

さらに、Splunkの導入によって、セキュリティ監視に必要なアナリストの人数を60%削減することもできました。これにより手の空いたアナリストは、重要なタスクや創造力に富む活動をサポートしています。

Splunkのダッシュボードは汎用性が高いため、今後、他部門のステークホルダーにも利用してもらう予定です。主要なユーザーは今でもITアナリストとセキュリティアナリストですが、ネットワーク管理者、アプリケーション開発者、コンプライアンス担当者も、カスタマイズしたダッシュボードを使って、それぞれの業務の運用状況を監視することが増えています。

ASL社の有能なチームがSplunkの活用方法を熟知していることで、システムの効率が向上し、ニーズに応じたインサイトの獲得が可能になりました。その結果、リアルタイムデータに基づく迅速な問題対応とパフォーマンスの最適化により、顧客に最高レベルのサービスを提供できるようになりました。

Splunkを無料で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。

26_CMP_cust_Automated-Systems-Limited-HK_v3-JA-202603