splunk> a CISCO company

お客様事例

オリンパス、グローバルSOCの統合により分断されたリージョン運用を集約

課題

EMEA・米国・APACの各リージョンで異なるMSSPとツールを運用していたため、グローバルでの可視性が確保できず、「単一の管理画面（以下、Single Pane of Glass）」が存在しなかった。地域横断的な脅威検知やコンプライアンス徹底が困難な状況にあり、統合的なSIEM基盤の整備が急務となっていた。

導入効果

グローバルで統一されたSplunkプラットフォームの導入により、ログ検索時間が数時間から数秒～1分以内へと劇的に短縮。フィッシング攻撃やビジネスメール詐欺（以下、BEC）への対応時間は数日から数時間以内へと改善し、SOARによる自動対応でアナリストの負荷も大幅に軽減された。

OLYMPUS

業界・業種：製造業

ソリューション：セキュリティ、プラットフォーム

製品：Splunk Cloud Platform, Splunk Enterprise Security, Splunk SOAR

オリンパスのグローバルセキュリティ改革を支えるSplunk

世界40の国や地域に拠点を展開し、内視鏡をはじめとする医療機器・精密機器の世界的リーダーとして知られるオリンパス株式会社。患者の命に関わる医療機器を扱う同社にとって、サイバーセキュリティは事業継続の根幹をなす重要課題です。

同社のセキュリティオペレーションはこれまで、EMEA、米国、APACなどのリージョンごとに独自のMSSPとツールで個別に運用されており、グローバルとしての統一的な可視性が確保されていない状態でした。

そこで同社は、Splunk Cloud Platform・Splunk Enterprise Security・Splunk SOARを核とした全社的なセキュリティ変革を推進。2024年7月の採用決定から1年未満というスピードでグローバル展開を実現し、ログ検索時間の劇的な短縮、インシデント対応の自動化、そして念願だったグローバルのSingle Pane of Glassの確立を果たしました。

成果

- フィッシングやBECへの対応時間が数日から数時間以内に短縮
- ログ検索時間は3～5時間から1分以内に短縮
- 24時間365日対応のグローバルSOC体制を確立
- SOARによるアラート自動対応で、アナリストの負荷を軽減

リージョンの壁が生み出す「見えないリスク」

日本やシンガポール、北京、ハンブルク、米センターバレー、トロント、ロンドンと世界各地に拠点を持つ同社のセキュリティオペレーションのグローバルヘッドを務めるSenior Director Global Security OperationsのMatthew W. Stephan氏は、「以前はEMEA、アメリカ、APACなど、地域ごとに別々のMSSPやITツールを使っており、データは各地域でサイロ化されていました」と話します。異なるMSSPが地域ごとに個別のITソリューションを運用する状況では、グローバルでの統合的な分析は困難でした。

最大の問題は「可視性の欠如」です。「可視性がなければ、システムやアプリケーションで何が起きているか分かりません。ネットワークへの脅威やリスクを認識できなければ、ビジネス資産を守ることはできない。そして、守るべきものが把握できなければ、コンプライアンスを徹底することも困難になります」とStephan氏は言います。

グローバルレベルでSingle Pane of Glassが存在しないことは、単なる運用上の不便にとどまりません。経営上の意思決定に必要なリスクの全体像が見えず、重大インシデントの検知・対応が大幅に遅延するという、ビジネスの根幹を揺るがすリスクを抱えていました。

Stephan氏はNISTのサイバーセキュリティフレームワークを軸に自らの担当領域を「特定」「検知」「対応」と定義し、着任以来、可視性のレベルと対応に必要なアラートのレベルを引き上げることに費やしてきました。その中核に位置づけられたのが、グローバルSIEM統合プロジェクトです。

「技術」と「信頼」の両軸で選ばれたSplunk そして計画的なグローバル展開

グローバルSIEMの統合にあたり、同社はまず自社の要件を整理するところから着手しました。「当社は製造業であり、非常に多様なシステムやアプリケーションを抱えています。IT部門が管理するシステムだけでなく、工場やR&D、その他の事業部門のシステムまで含めると、あらゆる種類のログを統合できるプラットフォームが必要でした」とStephan氏は説明します。「市場にある多くのSIEMは、こうした多様なログをネイティブに統合し、解析・取り込みを行ってアラートを出す機能が不足しており、膨大なバックエンド作業が発生します」。

複数候補から最終的にSplunkが選ばれた決め手は、ログの取り込み能力、アラート、SOARによる自動化、そして検知・対応サービスの構築能力といった「技術面」に加え、Splunkチームとの間に育まれた「信頼関係」でした。「Splunkのチームは、要件ヒアリングの段階から当社の組織構造やリスク姿勢、長期的なロードマップを深く理解しようとし、重要なタイムラインにどうサービスを組み込めるかを一緒に考えてくれました」とStephan氏は話します。

今回導入されたアーキテクチャは、「検知して対応する能力」の向上を軸に設計されています。Splunk Enterprise Securityにより、ビジネス、アプリケーション、製造現場など、あらゆる場所からログを取り込んで可視化し、相関ルールを作成して検知を行います。Splunk Cloud Platformへデータを集約し、そこにSplunk SOARを組み合わせることで対応能力をさらに高めています。

2024年7月の採用決定から、Splunkのグローバル展開は綿密な計画のもとで進められました。「旧MSSPが収集していたすべてのログをSplunkにも同時に取り込み、既存の2つの主要SIEMを並行稼働させることで、カバレッジのギャップ（抜け漏れ）を特定しました。そのギャップを埋めてSplunkのカバレッジが完全になった段階で、旧SIEMからの切り替えを行ったのです」とStephan氏は移行の手順を説明します。さらに資産管理ツールを活用してネットワーク上の資産状況を可視化し、Splunkの情報と照らし合わせることで、取り込み漏れのないログ収集体制を構築しました。

このプロジェクト全体を通じてStephan氏が最も印象に残ったのが、Splunkチームの一体感でした。「Splunkの営業、SE、そしてプロフェッショナルサービスの各チームが『一つのチーム』として密に連携し、複雑な要件を短期間で的確に実装しました。地域を問わず一貫したコミュニケーションと技術支援を受けられたことで、プロジェクトの進行スピードが劇的に向上しました」。

> **このパートナーシップは当社の成功に不可欠なものです。Splunkは単に製品を売って終わりではなく、将来のニーズを予測し、会社として成功するためのソリューションを共に考えてくれます。**
>
> オリンパス株式会社
> Senior Director Global Security Operations
> Matthew W. Stephan 氏

「数時間」が「数秒」に。対応時間の劇的短縮とグローバルな「可視性」の確立

現在の運用体制は、2024年秋に新たに導入したインドを拠点とするMSSPが24時間365日体制でSOCを運用し、Stephan氏率いるグローバルチームが「Follow-the-sun（日照時間に合わせたリレー方式）」で連携する形をとっています。

Splunk導入による最も顕著な改善はインシデント対応時間の短縮です。「フィッシング攻撃やBECへの対応時間が劇的に短縮されました。以前は検知・対応に数日かかっていたものが、現在では数時間以内に処理できています」とStephan氏は話します。

ログ検索のパフォーマンスも劇的に向上しました。「以前のSIEMではログを検索するだけで3~5時間かかっていました。Splunkでは同じ検索が長くても数秒~1分以内で完了するようになりました」。この差が、インシデント発生時のアナリストの初動対応の質と速度を向上させています。

SOARの実装による自動化も現場に大きな変化をもたらしています。Stephan氏が実際にインドのMSSPチームを訪問した際には、その効果を肌で感じたと言います。「彼らはSplunkを通じて非常にシームレスに仕事をしていました。SOARにより疲労が軽減され、本当に重要なアラートの対応のみに集中できるようになっています。Splunk内で情報を瞬時に共有し、別の席にいるメンバーとケースを引き継ぐなど、統合された一つのSOCチームとして機能しています」。

定性面での最大の変化は、長年の懸案だった「グローバルレベルでのSingle Pane of Glass」の実現です。「サイバー攻撃は国境を越えてやってきます。ネットワーク全体の脅威の動きをグローバルな視点で見える化できるようになったことは、セキュリティ戦略の根幹を変えました」とStephan氏は言います。

また、外部のMSSPに対して詳細なメトリクスやSLA/KPIを設定・管理できるようになり、「何に投資し、どのような価値が提供されているか」をビジネス部門に対して定量的に示せるようになったことも大きな成果です。セキュリティがコストセンターとして見られがちな中、データに基づいた説明責任を果たせるようになったことは、経営との信頼関係構築においても重要な意味を持ちます。

SOC・NOC統合、OT・R&D領域へ拡張し続けるSplunkの可能性

グローバル展開を果たしたSplunkの活用は、今後さらに広がりを見せようとしています。まず近い将来の取り組みとして、Stephan氏は「現在、インフラチームと同じSplunkインスタンスを共有し、ネットワークモニタリングやアプリケーションモニタリングを行う可能性について協議を進めています。SOCとNOCを同じプラットフォームに統合することで、より結束したグループとして情報共有が図れると考えています」と話します。

さらに、OT領域とR&D領域への拡張も視野に入れています。「Splunkにはすでに豊富なパーサーのライブラリやOT/R&D領域での強力なコミュニティがあります。独自のパーサー作成も容易であり、これらの領域への拡張に非常に適したプラットフォームです」とStephan氏は期待を寄せます。

Splunkとのパートナーシップについて、Stephan氏は社内での高い評価を話します。「将来のニーズを予測し、会社として成功するためのソリューションを共に考えてくれます。初期の導入段階から裏方として強力にサポートしてくれ、問題が発生した際も非常に迅速に対応してくれました。私はCIOに対し『すべてのベンダーとこういう関係を築くべきだ』と報告しています」。

最後に、グローバルなセキュリティ統合を目指す企業に向けてStephan氏は次のようにメッセージを送りました。「変革は難しく、数年を要する長い道のりです。成功の鍵は、CIOや取締役会などトップレベルからの賛同とサポートを得て、会社として無理のないペースで進めることです。これはテクノロジーだけの問題ではなく、人の問題でもあります。ビジネス部門やリーダー、チームとコミュニケーションを取り、彼らを巻き込んでワンチームで進める必要があります。そして、その旅を助けてくれる優秀なパートナーを見つけることが不可欠です。私たちにとって、Splunkがその素晴らしいパートナーの一社になってくれたことを大変幸運に思っています」。