Shunkhlai Group社：Splunk Enterprise Securityでセキュリティインシデントへの対応時間を半分に短縮

主な課題

異種混在のコンピューティング環境のセキュリティ監視で、対応の遅れや可視性の分断が生じて、インシデント対応に時間がかかり、ダウンタイムが長引いていました。

主な成果

Splunk EnterpriseとSplunk Enterprise Securityを活用して、分散するSOC業務をプロアクティブかつ包括的に可視化することにより、セキュリティインシデントの対応スピードを3倍向上させ、ダウンタイムを最大50%削減しました。

業種：エネルギーおよび公共事業

ソリューション：セキュリティ

製品：Splunk Enterprise、Splunk Enterprise Security

プロアクティブな対応で最高のセキュリティ態勢を目指す

モンゴルに拠点を置くShunkhlai Group社は、製造、貿易、テクノロジーを含む幅広い分野にわたる30以上の事業を統括する持株会社です。円滑な事業運営と顧客への信頼できるサービス提供を維持するために、サイバーセキュリティの強化と、サイバー攻撃に対するレジリエンスの確保に努めています。同社のサイバーセキュリティ部門は、すべての子会社にセキュリティポリシー、フレームワーク、コントロールを導入する司令塔としての役割も果たしています。子会社はそれぞれ、本社の指導の下でサイバーセキュリティプロセスを運用しています。

しかし、Shunkhlai Group社では、各部門でさまざまなベンダーのアプリケーションを使用しており、ネットワーク内には異種のデータソースが数多く分散しています。さらに、ハイブリッドクラウドとオンプレミスインフラを併用しているため、コンピューティング環境も複雑です。こうした複雑さが原因で、以前のセキュリティ監視システムでは、データの分析、脅威の検出、インシデントへの対応を効率的に行うことが難しくなっていました。

成果

2 ～ 3倍
セキュリティインシデントの対応スピード

2分の1
MTTDとMTTRの短縮率

50%
ダウンタイムの短縮率

当時、セキュリティチームには4人しかおらず、手動でセキュリティアラートを監視しながら、インシデント対応に長い時間を費やしていました。何よりも問題だったのが、対応が後手に回っていたことです。セキュリティリスクを未然に検出して対処できないことが多く、サービスの中断がいつ発生してもおかしくない状況でした。そこで、2023年に、中央SOC (セキュリティオペレーションセンター)を設立し、業務を促進するためのデータ分析ソリューションとしてSplunk EnterpriseとSplunk Enterprise Securityを導入しました。

一元的なリアルタイムのデータ分析で、インシデント対応を迅速化し、ダウンタイムを最小化

Splunkの導入後、Shunkhlai Group社はセキュリティ管理モデルを分散型から集中型へと移行して、セキュリティ運用の統合、一貫性、統制を強化しました。「Splunk EnterpriseとSplunk Enterprise Securityを選択したのは、堅牢な分析機能、拡張性の高さ、包括的なセキュリティ機能に魅力を感じたためです」と、Shunkhlai Holding社の情報セキュリティマネージャーであるGombodorj Munkhbat氏は言います。「既存のシステムとの統合とセキュリティ態勢のリアルタイムの可視化を可能にする点でSplunkの能力は群を抜いていました。また、高度な脅威の検出、調査、コンプライアンス機能も優れています」

Splunkを導入したことで、チームは分散するソースをくまなく検索してデータを集めたり、手動でデータを相関付けてサイバー攻撃を調査したりする必要がなくなりました。代わりに、Splunk Enterpriseプラットフォームでログの収集と分析を統合的に行い、ネットワークの運用状況をフルスタックで可視化できるようになりました。SOCでは現在、直感的なダッシュボードでデータの流れを視覚的に監視し、脅威の検出、問題の解決、コンプライアンスの確保、システムパフォーマンスの最適化を行っています。

さらに、Splunk Enterprise Securityで、ユーザー行動分析に基づく高度な脅威検出を活用してセキュリティ監視を強化するとともに、データを集約してサイバーセキュリティの状況を1つの画面で分析することで脅威の調査と対応を迅速化しています。これにより、MTTD (平均検出時間)とMTTR (平均応答時間)がともに50%短縮し、インシデントの対応スピードが2 ～ 3倍向上しました。効率が向上したことで、セキュリティ基盤が強化され、安定した事業運営と顧客への信頼できるサービス提供を維持できるようになりました。

> Splunkのおかげで、セキュリティインシデントの検出と対応のスピードと精度が向上しました。また、以前は得られなかったインサイトを獲得できるようになり、潜在的な問題が表面化する前に対処できるようになりました。
>
> **Shunkhlai Holding社**
> **情報セキュリティマネージャー、**
> **Gombodorj Munkhbat氏**

プロアクティブで予測的なセキュリティにより、ダウンタイムを半減し、99.99%の可用性目標を達成

Splunkでデータから実用的なインサイトをリアルタイムで引き出せるようになったことで、Shunkhlai Group社では、脅威の検出件数が50 ～ 60%増え、セキュリティリスクをプロアクティブに軽減できるようになり、未知の脅威への備えが強化されました。Splunkソリューションと他の脅威インテリジェンスツールやセンサーを組み合わせることで、フィッシング攻撃やマルウェアなどのサイバーセキュリティ脅威をすばやく検出し、業務に影響が及ぶ前に対処できるようになりました。

Splunkの予測分析ダッシュボードを使えば、日々の運用の中でデータの外れ値を検出し、異常な挙動を特定し、パフォーマンス上の問題やボトルネックを追跡できます。これにより、Shunkhlai Group社では、ネットワークのダウンタイムを最大50%短縮し、セキュリティ運用の効率を向上させることができました。

「Splunkのおかげで、最高水準のセキュリティと完全性を維持するための取り組みを強化して、99.99%という並外れた稼働率を達成できています」とMunkhbat氏は評価します。

持続可能でレジリエントな未来に向けて

持株会社として幅広い分野で多角的に事業を展開するShunkhlai Group社には、多様な事業ポートフォリオの持続可能な開発に対応できる柔軟性を備えたデータ分析ソリューションが必要です。

Munkhbat氏は、Splunkが、複数のソースのデータを容易に解析および処理できるカスタマイズ可能なプラットフォームを提供して、ビジネスのデジタルレジリエンスを支えている点を高く評価しています。さらにSplunkは、同社のセキュリティ運用を効率化し、全体的なセキュリティ態勢を強化して、サイバーレジリエンスのレベルを引き上げています。

Munkhbat氏は、Splunkのアカウントチームのサービス品質と対応力にも感銘を受けています。「必要なときはいつでも支援を提供し、貴重なインサイトを共有して、すばやく解決策を提示してくれます。さらに、SplunkのパートナーであるUnity社の支援でソリューションをスムーズに導入できました。また、エンジニアにトレーニングを実施してもらい、最適なサポートを受けることもできました。Splunkは今後も、当社のITロードマップに不可欠な存在として貢献してくれるでしょう。私たちはさらに多くのデータソースをSplunkに統合し、高度な分析機能を活用して、セキュリティと運用効率をさらに高めていく予定です」