splunk>

CASE STUDY

三菱重工業株式会社　Splunkを活用した監視環境の実現
脅威に即応できる情報セキュリティ体制を確立

三菱重工

ログデータの収集・整理に要していた時間と手間を払拭し
リアルタイムなリスクの可視化でグループ全体のセキュリティレベルを向上

エグゼクティブ・サマリー

エネルギー・環境、交通・輸送、防衛・宇宙、機械・設備システムなどの多様な事業ドメインで、常に最先端の技術を活用した製品をつくり続ける三菱重工業株式会社。ものづくり大国・日本の象徴とも言える同社及び同社グループにとって、高い技術力を支える膨大な知的財産に代表される情報資産は、まさに競争力の源泉となるものです。だからこそ万全の情報セキュリティ対策を施すことは、三菱重工グループ挙げての最重要課題でもあるのです。

ICTソリューション本部には、通信・制御、電気計装、システム技術開発、ITサービスの技術領域にまたがる、人材・技術リソースが揃っています。そのミッションは、三菱重工グループの4つの事業ドメインそれぞれの営業、設計、製造、サービス等のものづくりのプロセスを支援し、そこで生み出される様々な製品やサービスを、最先端のICT技術でサポートすること。ひいては、サイバー脅威の監視などを通じて、三菱重工におけるICT活用業務の安全と安心も支えています。そうしたなか、Splunk Enterpriseを導入することにより、下記のような効果があり、全体のセキュリティレベルが向上しました。

- ログの収集・整理・加工の作業の時間と手間が解消
- リアルタイムなセキュリティデータの取得と監視が可能に
- 問題の発見から対策の実施までの時間を大幅に短縮

Splunk 導入理由

サイバー攻撃の兆候などを確認する際には、まず社内のネットワークセキュリティ機器からログ等を収集、データを加工した上で可視化を行い判断しなければなりません。ログはものによって管理属性が異なることから、加工には膨大な時間と手間がかかってしまい、担当者の大きな負担となります。しかも状況の把握までに時間を要するため速やかな対策を阻害するのも課題でした。そうしたなか同社では、課題を解決するソリューションとしてSIEM（Security Information and Event Management）に着目して、その要件をまとめていきました。

SIEM製品の評価・選定は、RFIやRFPの段階でのかなりシビアな性能要求に基いて進められました。SIEM製品の選定に当たり特に重視されたのが、システムのパフォーマンスです。社内随所に設置されたネットワークセキュリティ機器から集約されるログデータは膨大な量となるためです。RFPの要求に対して各社が示した性能情報のなかで、高いパフォーマンスを見せたのが、Splunkでした。Splunkは、アラート発生時の原因究明など、検索処理が速く、同社の求める性能を十二分に満たすと

業種

- 重工業

課題/背景

- ログデータの収集・加工に割かれる時間と手間を解消
- リアルタイムなセキュリティデータの取得
- ログデータの分析精度を向上
- 問題の発見から対策を実施するまでの時間を短縮化

ソリューション

- Splunkソフトウェアを活用したSIEMによる監視環境構築

Splunkによる事例の使用

- セキュリティ
- 監視およびレポート

導入効果

- ログの収集・整理・加工の作業がゼロに
- アラート発生から原因調査、対策実施までの時間を大幅に短縮
- プロアクティブな問題改善を実現
- 組織全体のセキュリティレベル向上に寄与

データソース

- ネットワーク機器のログ

判断しました。その後、三菱重工では、発注からわずか5ヶ月という短期間でSplunkを活用したSIEM環境を整備しました。

運用スタッフも巻き込み構築を5か月で完了

こうして三菱重工ではSplunkを活用したSIEM構築フェイズへと移行しました。プロジェクト推進中は会議室を貸し切り、多田氏らプロジェクトメンバーはもちろん、監視業務に当たるスタッフも加わって、新たな運用環境づくりに向けた密なコミュニケーションを重ねていきました。多田氏は、「完成後にすぐに運用開始できるよう、現場でオペレーションを行うスタッフにも入ってもらい、具体的なイメージをつかんでもらうようにしました。また、細かい仕様の変更などが生じても、開発パートナーからのレスポンスが速かったこともあり、プロジェクトが滞ることはほとんどありませんでした」と話します。このようにシステム構築作業は極めてスムーズに推移し、発注から5ヶ月という短期間での導入を成し遂げたのです。

分析の迅速化で、プロアクティブなセキュリティ対策も実現

正式運用を開始した三菱重工では、ネットワークセキュリティ機器等のログ分析に要する手間と時間の大幅な軽減を実現しました。また、以前はログが一箇所に集約されておらず、分析の前にまず手作業でデータを収集し整理・加工するといった作業が生じていましたが、Splunkの活用後、そうした作業が一切必要なくなったのに加えて、機器から上げられたアラートの原因調査から結果が出るまでを非常に迅速に完了できるようになったのです。多田氏はこう語ります。「Splunkの導入前はデータを集めるだけで数時間もかかってしまうこともありましたが、今は常に最新のデータが集約されているので必要な時にすぐに確認することができます。そのため、脅威の可能性検知から対策を施すまでの時間が一気に短縮されました。さらに、分析が容易に行えるようになったので、“ここがちょっと怪しいかもしれない”とスタッフが感じた段階で、事前に詳しく検証して脅威の芽を摘むといった対策も実現しました。監視チームでは、『集約された膨大なログデータを分析して可視化することで、新しいリスクの兆候を見つけて潰していく、といった地道な取り組みを繰り返すことが大切だ』、という意識も根付いています。かつてデータの収集・整理に費やされていた時間を、危険が生じそうな箇所を事前に見つけ出し、問題を改善してしまうといった時間に充てられるようになったことは、組織全体のセキュリティレベル向上に寄与していると自負しています」

「実運用では、システムからのアラートを受け取った後、脅威を低減するためにどれだけ迅速に行動できるかがとても重要だと考えていました。Splunkは、アラート発生時の原因究明など、分析の肝となる検索処理が圧倒的に速いので、我々の求める性能を十二分に満たすと判断しました。また、国内外ともに導入事例が増えているので、他の企業での具体的なSplunkの活用方法を知ることができた点も大きかったですね。」

三菱重工株式会社
ICTソリューション本部

Splunkを活用して分析を拡大・深化させたい

基盤にSplunkを取り入れたことで、脅威への対応力を高めることができた三菱重工では、今後は分析の対象範囲をより広く深くしていく構えです。高松氏は、「Splunkを利活用できるスタッフをできる限り増やすことで、もっと高度な分析が行えるようにしていきたいと考えています」と話します。続いて多田氏は、「リアルタイム性に対するニーズの高い業務を筆頭に、Splunkはセキュリティとはまったく異なる分野でも有効な製品だと感じています。我々ICTソリューション本部はあらゆる業務プロセスの効率化を支援する立場にあるので、他にSplunkが役立ちそうな業務があれば積極的に情報提供ができるのではと期待しています」と未来への抱負を示します。