DKB社：Splunkで脅威への対応時間を90%短縮し、顧客からの信頼を向上

主な課題

クラウド移行を進める過程で、複雑なシステムの監視と環境内の脅威の検出が課題でした。

主な成果

Splunkを導入してインフラを包括的に可視化したことで、アラートの誤検知が減り、脅威の検出と調査にかかる時間が90%短縮されました。

業種：
金融サービス

ソリューション：
Splunkセキュリティ

金融サービス業界では顧客から信頼を得ることが重要

Deutsche Kreditbank (DKB)社は、ドイツ第2の規模を誇る銀行として、450万人の顧客に融資、クレジットカード、貯蓄などのサービスを提供しています。同社では現在、取引、支払い、その他の処理をシームレスに連携させるため、クラウドへの移行を進めるとともに、サイバーセキュリティの強化に取り組んでいます。当初は、マネージドサービスプロバイダーを介してSplunkを利用していましたが、その後オンプレミスで利用するように切り替えました。

クラウドへの移行によって、DKBのシステムは想定以上に複雑化しました。そのため、各種のセキュリティツールからクラウド環境やオンプレミス環境に至るまで、ハイブリッドインフラに含まれるあらゆるシステムを可視化するソリューションが必要になりました。また、問題を迅速に検出できるようにするためにも環境全体を可視化する必要がありました。特にランサムウェアなどのサイバー脅威は、システムの安定性だけでなく顧客の信頼を損なう可能性もあるため対策が必須です。

成果

- 脅威の検出と調査にかかる時間を90%短縮
- ツールと環境全体の可視性を向上
- 誤検知を削減

盲点を最小限に抑える

DKB社は、まずセキュリティ監視とインシデント管理のためにSplunkを導入し、その後用途を脅威インテリジェンスに拡大しました。すでに多数のセキュリティツールを使用していましたが、Splunkを導入したことで、異なるツールのさまざまなデータを集約し、横断的に検索できるようになりました。

このことは業務の大幅な効率化につながりました。DKB社でSOCの責任者を務めるAndreas Hennich氏は次のように述べています。「Splunkがもたらした最大のメリットは可視化です。可視性が改善したことで、状況を包括的に把握できるようになりました。今では、クラウドかオンプレミスかを問わず、すべての環境内の多様なセキュリティツールで生成されたアラートを1カ所で確認できます。情報が集約されるため、調査やデータ活用の効率が大幅に向上しました」

脅威を見逃さない

DKB社のチームは、アラート対応を迅速化することで、ネットワークのセキュリティを強化しました。それまでは、アラートの数が多すぎて処理しきれないうえに、分散したアラートを個別に対応していたため、解決が遅れ、問題を見逃すこともありました。「以前はいくつものログファイルを調べてネットワークの問題を探し出していましたが、その作業には多くの時間がかかり、アラートの見落としも発生していました。今ではSplunkをSIEMとして活用し、インフラ内のあらゆるコンポーネントのデータを相関付けて、1つのデータベースで状況をすばやく包括的に可視化できるようになりました。そのおかげでネットワークのセキュリティ業務が大幅に改善されました」とHennich氏は評価します。「脅威が発生しても、アラートをすばやく確認して迅速に対応できます」

実際にDKB社では脅威の調査と対応にかかる時間が90%短縮されたとHennich氏は言います。「Splunkを導入する前は、各種のログファイルを調べたり、補足データを検索したり、サーチクエリーを記述したりするなど、大変な手間がかかっていました。しかし今では、Splunkのおかげですべてを効率的に行えます」

> 今では、SplunkをSIEMとして活用し、インフラ内のあらゆるコンポーネントのデータを相関付けて、1つのデータベースで状況をすばやく包括的に可視化できるようになりました。そのおかげでネットワークのセキュリティ業務が大幅に改善されました。脅威が発生しても、アラートをすばやく確認して迅速に対応できます”
>
> **Andreas Hennich氏、**
> **DKB社SOC責任者**

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。

営業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

24-splunk- 133169 - EMEA DKB Customer Story-JA-202403