フランス郵政公社：誤検知を10分の1に削減し、130万人分の顧客データを保護

主な課題

データの増加によって、社内のサイバーセキュリティチームが使用していたシステムで遅延やクラッシュが頻発するようになり、調査に遅れが出て、顧客情報のセキュリティが低下していました。

主な成果

Splunk Enterprise Securityを導入したことで、脅威の検出および対応能力が向上し、誤検知が10分の1に減って、アラートをすばやく解決できるようになりました。

業種：行政・公共機関

ソリューション：セキュリティ

製品：Splunk Enterprise Security

フランス最大の郵便サービス会社

オンラインでショッピングを楽しんだときや、新しいクレジットカードを作ったとき、または、おばあちゃんに手紙を送ったときに、商品を時間どおりに配達し、クレジットカードを安全に送り届け、手紙をおばあちゃんに直接手渡してくれる頼もしい存在、それが郵便サービス会社です。63カ国の130万人の顧客が、フランス郵政公社に日々、手紙や小包はもちろん、個人の住所や連絡先情報などのデータを託しています。そのため、同社にとっては、信頼性の高い郵便サービスを提供するだけでなく、顧客のデータを保護することも重要な任務です。

その責任を主に担うのが、80人のメンバーで構成される強力なサイバーセキュリティ部門、SLCC (Service de Lutte Contre la Cybercriminalité)です。その仕事は容易ではありません。多くの組織と同様に、フランス郵政公社もサイバー攻撃の巧妙化や国際情勢の不安定化による脅威の高まりに直面しています。2024年のパリオリンピックのような注目度の高いイベントもあり、組織の防御力を強化することがこれまで以上に重要になっています。

成果

- アラートの80%を13分以内に処理
- 誤検知のアラートを10分の1に削減
- 1日あたり最大20テラバイトのデータを処理

フランス郵政公社のサイバーセキュリティチームは、2015年に、SIEMとしてSplunk Enterprise Securityを導入しました。環境が複雑化していたため、チームは、膨大な量のデータと多様なシステムに対応できるだけでなく、脅威の調査と阻止能力に優れたソリューションを必要としていました。「私たちの使命は、脅威や攻撃から組織を守ることです」と、フランス郵政公社のセキュリティインシデント検出責任者であるOlivier Cassignac氏は言います。「それは、攻撃の形態や規模に関係なく、あらゆる脅威からインフラ、従業員、お客様を守ることを意味します」

調査を迅速化

SLCCの主な目的は、異常をできるだけ早期に検出して、レベル1アナリストが対応し、関連支部に通知できるようにすることです。しかし、データの増加により、システムがクラッシュして調査に遅れが出るようになりました。フランス郵政公社では通常、1日あたり20テラバイト以上のデータを処理しており、SLCCだけでも1日平均5テラバイトのデータを扱っています。Splunkの導入前は、データ量がそれよりはるかに少ないときでも、特定のイベントを検索するのに数時間かかったり、システムがクラッシュしたりしていました。

Splunk Enterprise Securityの導入後は、過去数週間または数カ月分の膨大な量のデータを数秒で分析できるようになりました。これにより、貴重な時間とリソースを節約するとともに、サイバーセキュリティインフラの基盤を強化できました。「調査では膨大な量のデータを扱うため、検索ツールのパフォーマンスは極めて重要です。Splunkの大きなメリットはクエリーが高速で処理されることです。その分、アナリストがデータの理解と調査に多くの時間を費やせるようになりました」とOlivier氏は評価します。

アラート処理を効率化

SLCCには年間で数千件のアラートが届くため、潜在的な脅威をフィルタリング、分類、優先順位付けするソリューションが必要でした。その解決策として、Splunkのリスクベースアラート(RBA)ソリューションを導入したところ、これらのニーズをすべて満たしただけでなく、アラート処理の平均時間を13分にまで短縮することができました(時間は、SLCCがアラートを受け取ってから次の関連支部に転送するまでの時間)。

では、どのようにしてそれを実現したのでしょうか。SLCCは、Splunk Enterprise Securityの機能を社内のニーズに合わせてカスタマイズし、アラートのダッシュボード、機能、ルール、サーチをそれぞれ調整しました。リスクベース機能も活用し、イベントにリスクスコアを割り当てて、スコアが特定のしきい値に達したときにアラートを生成します。これにより、潜在的な脅威や不審なアクティビティを包括的に検出できるようになりました。また、誤検知が10分の1に減ったため、アナリストは緊急性の高い実際の脅威への対応に集中し、より効率的に作業を行えるようになりました。

> “Splunkのカスタマイズレベルは非常に重要です。このツールには限界がないのです。市場にはたくさんのソリューションがありますが、私の知る限り、これほど高度なカスタマイズ機能を提供するソリューションは他にありません。すべてのダッシュボード、機能、ルール、サーチをニーズに合わせて細かく調整できます”
>
> フランス郵政公社
> セキュリティインシデント検出責任者、
> **Olivier Cassignac氏**

社内で連携して新たな脅威に対処

リスクが絶えず変化する中、Splunk Enterprise Securityの脅威インテリジェンス管理機能は、フランス郵政公社にとって貴重な武器になっています。SLCCチームでは、新たな脅威を検出すると、脅威インテリジェンス管理機能によって分析し、技術的なメトリクスに変換しています。このメトリクスを取り入れてアラートを強化することで、以降、その新たな脅威の特定と分類が可能になります。重要なのは、過去に遡って検出する点です。イベントを遡って調査し、新たな脅威が以前に発生していたかどうかを確認します。

脅威を阻止し、組織を守るには、組織全体で協力する必要があります。同公社のサイバーセキュリティ組織は200人規模で、これにはSLCCのほかに、各支部のさまざまなSOCメンバーが含まれています。Splunkなら、すべてのチームのインサイトを統合し、共通のツールを使いながら、高度な分析、KPIの監視、手動でのサーチなど、ユースケースに応じてカスタマイズしたインターフェイスで作業できます。これにより、サイバーセキュリティの各チームは、徹底した調査をすばやく行うだけでなく、他のチームと密接に連携できるようになりました。