Novuna社：稼働率を高めて数百万の顧客からの信頼を深める

主な課題

顧客データを適切に保護し、サービスの信頼性を向上させるために、セキュリティ態勢を強化する必要がありました。

主な成果

ダウンタイムを削減し、脅威をプロアクティブに緩和することで、顧客が安心して利用できる金融ソリューションを提供しています。

Novuna

業種：金融サービス

ソリューション：セキュリティ

製品：Splunk SOAR、Splunk ES

情報セキュリティへの投資がもたらす価値

英国の大手金融サービスプロバイダーであるNovuna社は、個人および企業の顧客の目標達成をサポートしています。社名は「New Together (新たな道をともに)」を意味し、社会の急速な変化の中で顧客を継続的に支援するためにデジタルトランスフォーメーションを推進して進化を続ける同社の姿勢をよく表しています。

金融サービス企業の成功には、顧客からの信頼が不可欠です。しかし、信頼を得ること、そして、得た信頼を維持することは容易ではありません。数百万の顧客の信用に値する英国屈指の金融サービスプロバイダーであり続けるために、商品やサービスの完全性とセキュリティを最高レベルに保つことは、Novuna社にとって必須課題です。

卓越したカスタマーエクスペリエンスを提供するために、同社の情報セキュリティチームはたゆまぬ努力で、複数の事業部門と多数のシステムを抱える組織全体を脆弱性やサイバー攻撃から守っています。「情報セキュリティ (IS)自体が利益をもたらすことはないかもしれませんが、一歩間違えれば、顧客を失う可能性があります」と、Novuna社の情報セキュリティグループ責任者であるIan Stacey氏は言います。

成果

- 導入後8カ月で50万ドルのコストを節約
- Splunk SOARで8万件のセキュリティイベントを管理、統制、封じ込め
- 3年間に及ぶ手動のイベントログ処理に終止符
- プラットフォームをシームレスに統合

Novuna社は以前から、アプリケーションパフォーマンス監視のためにSplunkプラットフォームを利用していましたが、最近になってSIEMとしても利用するようになり、情報セキュリティ管理システムをSplunkプラットフォームに一本化しました。現在では、Splunk Enterprise Securityを使って、セキュリティ分析と脅威インテリジェンスの管理を1つのプラットフォームに統合しています。これにより、ITチームとISチームの連携が深まり、攻撃の兆候や潜在的なサイバー脅威をより高い精度で検出できるようになりました。

包括的なアラートは信頼できる資産

Novuna社は、さまざまな個人と企業を対象に、革新的なソリューションと卓越したカスタマーエクスペリエンスを提供しています。顧客の優先事項はそれぞれ異なりますが、自身の財務データの保護に最高レベルのセキュリティを求める点は共通しています。

顧客のニーズに応え、サイバー脅威に先手を打つために、Novuna社は、既存のSplunkインスタンスをSplunk Enterprise Securityと統合することを選択しました。その絶大な効果がすぐに表れたのがセキュリティ監視です。セキュリティチームのもとに包括的なアラートが届くようになり、実際に危険な脅威にすばやく対処して被害を未然に防げるようになったことで、サービスの稼働率が向上しました。

また、Splunk Enterprise Securityによってすべてのセキュリティ運用を単一のプラットフォームに集約したことで、ISチームとITチームの連携が容易になり、組織のセキュリティ態勢が飛躍的に強化されました。Novuna社のサイバーセキュリティ製品オーナーであるCallum Taylor氏は次のように述べています。「最大の課題は、変化のスピードに合わせて新しい商品を提供し、全員が同じ目標を目指せるようにすることでした。今回の統合におけるSplunkのソリューションの価値は計り知れません。ISチームとITチームに明確な方向性を示し、信頼の獲得こそが私たちのモチベーションであることを再認識させてくれたのです」

最大の課題は、変化のスピードに合わせて新しい商品を提供し、全員が同じ目標を目指せるようにすることでした。今回の統合におけるSplunkのプラットフォームの価値は計り知れません。ISチームとITチームに明確な方向性を示してくれたのです。

Callum Taylor氏、Novuna社
サイバーセキュリティ製品オーナー

自動化による利益

Novuna社は、Splunk SOARを使って初期段階のアラート分析を自動化し、誤検知にはフラグを付け、そうでないアラートはサイバーチームにエスカレーションする仕組みを構築して、コストの最適化とワークフローの効率化につなげました。1年足らずで、Splunk SOARを使って8万件のイベントを処理し、適切に封じ込めたほか、ライセンスの削減、ユーザーの効率向上、チームのオンコール時間の削減により、50万ドル以上のコストを節約しました。

Splunkにより、プラットフォーム間の統合やアップグレードのパッチ適用が大幅に容易になり、シームレスなプロセスが実現しました。以前は、ITチームとISチームが3つの切り離された環境と2つの異なるクラウドを個別に運用していて、複雑なインフラを管理するための一貫したアプローチがありませんでした。現在では、インフラ全体で監視と運用を一元化することで、リアルタイムの一貫した管理が可能になり、リスクが低減され、パッチをすばやく効率的に適用できるようになりました。設定に問題があった場合はすばやくアラートを受け取り、問題を解消して、パッチを適用できるようになったことで、サービスの品質が全体的に向上しました。

こうしたデジタルトランスフォーメーションの成果として、サービスの信頼性が向上し、サイバーセキュリティの成熟度が高まり、顧客からの信頼が強化されました。しかし、Novuna社のジャーニーはここで終わりではありません。チームは、Splunk Enterprise Securityでの機械学習ユースケースの導入や、Splunk Attack Analyzerによる脅威分析の自動化など、Splunkがもたらす新たな可能性を積極的に模索しています。そして、これらの取り組みを通じて、チームの負担を軽減し、付加価値の高い業務に集中できるようにして、すべての従業員の潜在力を最大限に引き出すことを目指しています。

splunk>

お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

24-569598-Novuna-SC-JA-202407