Webster Bank：Splunk Enterprise Security Premierで信頼を構築し、運用効率を向上

主な課題

Webster Bankは、厳しいコンプライアンス規制に対応し、内部脅威に対処し、可視性を高めることによって、価値と強力なガバナンスをステークホルダーに対して証明するために、セキュリティ能力を強化する必要がありました。

主な成果

同行のセキュリティチームは統合プラットフォームを導入することで、検出を迅速化し、対応の取り組みについて改善と最適化を進め、効率の向上を実現するとともに、主要なメトリクスやインサイトを共有して価値を証明できるようになりました。

製品：Splunk Enterprise Security Premier

業種：金融サービス

安心、信頼、コミュニティ

これらは、Webster Bankが、顧客、職員、ステークホルダーのために日々の業務で守り続けている価値観です。地方銀行として、創業から100年近くにわたり、地域社会の良き世話役、ビジネスパートナー、そして企業市民の役割を担い、地元の住人、家族、組織に貢献してきました。

信頼はWebster Bankの業務の根幹として、あらゆる活動の原動力になっています。その信頼を支える取り組みの1つが、同行の金融システムと重要データについて、セキュリティと完全なコンプライアンスを確保することです。ニューヨーク州金融サービス局(DFS)、米国通貨監督庁(OCC)、米国金融業規制機構(FINRA)などによる規制に対応するため、同行のCISOであるPatricia Voight氏とそのチームは、監査証跡、ユーザーアクティビティの監視、データストレージの拡張のための高度な機能を強化して導入する必要がありました。

成果

- MTTRを短縮して、脅威の検出と封じ込めを迅速化
- 高いインシデント解決率でSLAを堅持、迅速な修復
- コンピューティング資産全体にわたり、可視性と網羅性を向上

ニューヨークに拠点を置く同行では、テクノロジー環境の拡大を受けて、セキュリティ業務を単一の統合プラットフォームに集約するために、Splunk Enterprise Security Premierを導入しました。SIEM、SOAR、UEBA (ユーザーとエンティティの行動分析)を統合したSplunkプラットフォームによって、セキュリティ環境をエンドツーエンドで包括的に可視化できるようになり、チームの業務はスピード、一貫性、信頼性が向上しました。詳細な調査機能と複雑なデータセットのドリルダウン機能を備えたSplunk ES Premierは、同行がセキュリティへの取り組みを進めていくうえで理想的なソリューションでした。

Voight氏はこう語ります。「Splunkとは長年のパートナーです。日々の業務ではSplunk Enterprise Securityソリューションを活用して、組織全体の監視とコンプライアンス維持に役立てています。あらゆるアプリケーション、あらゆるデータソースから送られるすべてのマシンデータが、Splunkに集約され、そこを経由して流れています。Splunkは、当行の環境の基盤なのです」

Splunk Enterprise Security Premierで透明性と信頼を確保

信頼の構築にまず必要なのは、透明性です。Webster Bankのセキュリティリーダーは、厳しさを増すコンプライアンス規制に対応しながら、経営幹部や取締役会に強力なガバナンスを証明し続けるために、テクノロジー環境を常時継続的に可視化する必要があります。

Splunk Enterprise Security Premierが威力を発揮しているのは、まさにこの点です。強力なUEBA、SIEM、SOAR機能が統合プラットフォーム上でシームレスに連携されることで、組織全体が包括的に可視化されているというわけです。Webster Bankのセキュリティチームは現在、複数のポイントソリューションを管理するのではなく、検出や調査から対応までのアクションが緊密に連携された1つの画面を使って業務を行っています。これにより、複雑さが軽減されるとともに、すばやい相関付けによる豊富なインサイトや、精度の高い分析が得られています。

フィッシングや外部からの攻撃を検出するには、迅速かつ正確な相関付けが非常に重要です。たとえば、Splunkで収集したログを調査することで、IPアドレスが特定のVPNサービスに関連付けられており、さらにはそのサービスが環境への侵入を狙うAPT (Advanced Persistent Threat)などの攻撃者に関連していることを迅速に特定できます。それがわかれば、脅威を緩和してシステムへの影響を軽減するための検出ルールを速やかに作成できます。

Voight氏は、この統合的なアプローチのおかげで、重要なデータにアクセスしやすくなっただけでなく、経営幹部や取締役、主要なステークホルダー、さらには各種の事業部門や技術部門の同僚まで、主要なメトリクスやインサイトを組織全体で共有して、チームの取り組みの価値を証明できるようにもなったと言います。

同氏はこう説明します。「成果と取り組みを簡単に可視化できるようになった今、当行の経営幹部に向けて、それぞれの事業分野でのメリットを1つの画面で示すというコンセプトの実現を目指しています。報告は取締役会に向けても行っているので、同じように1つの画面を見せることにより、安心して利用できる環境を日々の業務でどのように維持しているかを実証したいとも考えています」

透明性の確保は、Webster Bankの経営幹部や取締役会の安心につながっているだけではありません。同僚や顧客からの信頼を確立し、ニーズや環境の変化に適応してその信頼を維持するうえでも大きな役割を果たしています。Voight氏によると、Splunk ES Premierはセキュリティと説明責任を実証するための明確で透明性の高い手段を提供してくれるものです。

> **Splunkとは長年のパートナーです。日々の業務ではSplunk Enterprise Securityソリューションを活用して、組織全体の監視とコンプライアンス維持に役立てています。あらゆるアプリケーション、あらゆるデータソースから送られるすべてのマシンデータが、Splunkに集約され、そこを経由して流れています。Splunkは当行のIT環境基盤なのです。**
>
> Webster Bankおよび
> Webster Financial、CISO、
> Patricia Voight氏

「組織全体にわたり、すべてのセキュリティ要素が統合されます。当行が使っているのは、SIEM、SOAR、UEBAが統合されて強力な機能が集約された、単一のシームレスな統合プラットフォームなのです。これを通じて、組織全体ですべてのチームにわたり、セキュリティの状況を包括的に把握できます」

自動化でイノベーションを加速

透明性が信頼を確立するとしたら、自動化はそれを促進する原動力となります。SIEMとSOARの機能をSplunk ES Premierに統合することにより、アナリストの貴重な時間を奪っていた日常的なセキュリティタスクを自動化することができました。今日では自動化によって、プレイブックを合理化し、プロセスを標準化、ドキュメントを最新の状態に維持しています。これらは、規制の厳しい環境では不可欠の要件です。自動化は、アナリストの負担を軽減することに加えて、インシデント対応のスピードと一貫性の向上にも役立っています。具体的には、自動化によってアラートを優先付けして重大度の低いアラートを除外するので、アナリストは最も深刻なセキュリティ脅威にのみ対処できます。これにより、チームのシニアメンバーは、監視、リスク管理、継続的な改善に集中できるようになっています。Voight氏によると、さらに、Splunk ES PremierのデータをServiceNowに統合することで、レベル1からレベル3のリスク管理およびコンプライアンス対応アクティビティを支援できるようになったということです。

「自動化は、当行の成功にとっても、統合への取り組みにおいても不可欠なものです。SIEMとSOAR機能を統合し、自動化に組み込んだ形にして導入しやすくしました。目標は、レベル1とレベル2のチームで対象分野のエキスパートの負担を解放して、戦略的な業務にもっと注力できるようにすることです」

Webster BankはAIの全面的な導入も開始したところで、将来的にはSplunk ES Premierを中心にイノベーションを推進していく予定です。AIドリブン機能の成熟とともに、特にSOC (セキュリティオペレーションセンター)において、検出、トリアージ、対応をさらに迅速化することで、データ窃取や悪質な脅威に対処し根絶することを目指します。Voight氏は、今後1年間でセキュリティ領域におけるAIの進化は「大きく加速する」という予想のもとに、担当チームではタスクの自動化を引き続き優先していくと述べています。

「当行のAI活用の取り組みは、ほんの初期段階にあります。Splunkは、エンドツーエンドでのすべてのデータ収集と統合における中心的なデータポイントであり、すべてのマシンデータがここに集約されます。当行にとっては、これまでも、これからも、戦略的計画の一端を担う、非常に重要な存在であり続けます」

UEBAによる内部監視

顧客にも職員にも、マルウェアやデータ侵害など、組織内外の脅威から守られているとただ感じるだけでなく、実際に知ってもらう必要があります。そのため、Webster Bankでは、Splunk ES Premierを使って、金融機関が直面する2大脅威である内部脅威とデータ漏えいの検出能力を強化しています。UEBAをプラットフォームに直接組み込むことで、セキュリティチームは、複雑なクエリーの作成に貴重な時間を費やすことなく、行動に関する新たなインサイトを得て、異常なアクティビティを早期に検出しています。Splunkの早期導入企業であり設計パートナーでもあるWebster Bankは、顧客の実際のニーズと規制要件に対応できるよう、Splunkと密接に連携してこれらの機能の構築に取り組んできました。同行のセキュリティチームは包括的な可視化、自動化、行動分析を組み合わせることで、ツールや負担を増やすことなく、脅威の早期検出、対応プロセスの調整と最適化、迅速なインシデント対応、他の技術チームへのユースケースの拡大、運用効率の向上といった数々の成果を達成しました。

> **Splunk ES Premierを導入したことで、素晴らしい成果を得ることができました。組織全体にわたり、すべてのセキュリティ要素が統合されます。当行が使っているのは、SIEM、SOAR、UEBAが統合されて強力な機能が集約された、単一のシームレスな統合プラットフォームなのです。これを通じて、組織全体ですべてのチームにわたり、セキュリティの状況を包括的に把握できます。**
>
> Webster Bankおよび
> Webster Financial、CISO、
> Patricia Voight氏

Voight氏はこう述べています。「プラットフォーム導入の成功を確実にしたいので、Splunkと当行にシスコも加えてパートナーシップを拡大しています。Splunk ES Premierの成功を基盤に、SOAR、Mission Control、その他の機能を環境に統合し、自動化にいっそう注力して手作業を削減したいと考えています。そうすることで、変化の激しい脅威の状況に対応しながら、リーダーシップの発揮と成長の実現に注力できるようにしたいのです」

Webster Bankにとって、究極の成功指標は、顧客がセキュリティを意識しなくても済むようにすることです。それは、同行が業務を適切に運営していると顧客が確信しているということです。つまり、顧客データが保護され、トランザクションは安全で、サービスが中断することはないという状態なのです。

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。

26_CMP_cust_Webster-Bank_v2-JA-202607