世界有数の研究大学：平均検出時間(MTTD)を60%短縮

主な課題

大学のキャンパスITセキュリティチームは、ダッシュボードの分散がもたらす課題に直面していました。一方、医療システムのセキュリティアナリストは、システム間でログを相関付けできない状態でした。どちらのチームも、学生、教職員、患者、知的財産の安全を守るために、脅威をすばやく検出して対応する必要がありました。

主な成果

Splunkの導入により、キャンパスセキュリティチームと医療セキュリティチームは環境を可視化し、1つの画面で状況を把握できるようになりました。その結果、MTTDが60%以上短縮され、重要な研究から医療データまで、すべての資産を保護できるようになりました。

業種：大学・研究機関および医療・ヘルスケア

製品：Splunk Enterprise Security (ES)、Splunk Enterprise

ソリューション：セキュリティ、コンプライアンス、プラットフォーム

機能：SIEM/セキュリティ分析、調査とフォレンジック、リスクベースアラート、コンプライアンスの監視とレポート作成、インフラ監視とトラブルシューティング、インシデント応答と自動化

数万人の関係者が大学の重要システムへの安全なアクセスに依存している状況では、盲点は許されません。

4万人以上の学生、教員、職員が在籍する世界的に著名なこの学術機関には、数十の学部と研究センター、そして著名な医学部があり、卓越した医療システムを運用しています。一方で、その名声の高さから、サイバー攻撃者の格好の標的になっていました。大学と医療システムは、脆弱な認証情報を悪用した重要な知的財産へのアクセス、医療データの漏えい、業務や患者ケアの妨害など、国家を後ろ盾とした攻撃や場当たり的な攻撃に度々さらされていました。

大規模なAI中心の戦略を構築するには、膨大な量のデータを効率的に管理し、システムのレジリエンスを維持するための強固な基盤が必要です。Splunkはその基盤を支え、サイバーセキュリティとコンプライアンスだけでなく、ITインフラ、ネットワーク運用、研究環境の監視もサポートします。

成果

60%以上
MTTDを短縮

40%
チケットの調査時間を短縮

数百
管理対象外でも保護しているエンドポイントの数

この大学のセキュリティ運用チームは、学術および研究環境を保護するチームと、医学部および医療システムのセキュリティを管理するチームの2つに分かれています。キャンパスを担当するチームでは、ユースケースごとに構築されたダッシュボードが多数あり、セキュリティに関するインサイトが分散していることが課題になっていました。一方、医療システムを担当するチームでは、アナリストが生のログデータを精査していましたが、イベントを相互参照したり相関付けたりできないことが問題でした。環境を包括的に可視化できないために盲点が生じ、問題への対応に時間がかかって、キャンパスと病院が脆弱な状態に陥っていました。

Splunkの導入後は、こうした複雑さが解消され、どちらのセキュリティチームも環境全体を可視化できるようになりました。大学では現在、学生、患者、研究、基幹業務を保護する強固なデータ基盤を確立しています。

セキュリティの可視性を合格ラインまで高める

今回取材したシニアITセキュリティアナリストがこの大学のIT部門に配属された当時、セキュリティダッシュボードはあったものの、それぞれが孤立し、用途が限定されていたため、キャンパスのセキュリティ態勢を包括的に可視化できませんでした。

そこで、Splunk Enterpriseを使って、キャンパスレベルから部門やホスト単位まで情報をドリルダウンしてセキュリティ態勢を分析できる階層型のダッシュボードを作成しました。これにより状況が大きく改善されました。

> ノイズを追いかけるのではなく、実際のリスクに基づいて優先順位を付けることができます。
>
> **SIEMエンジニア**

環境が包括的に可視化されたことで、アナリストは脆弱性をすばやく検出し、豊富なコンテキストに基づいて調査を行えるようになりました。Splunk Enterpriseを利用するようになってから、キャンパスセキュリティチームでは、リスクの高いセキュリティイベントの検出時間が60%以上、チケットの調査時間が40%短縮されました。その結果、セキュリティ態勢ダッシュボードの拡張や自動アラートの改良など、高レベルのプロジェクトに集中できるようになりました。また、ITリーダー向けのスコアボード形式のビューでは、未解決の脆弱性とその平均経過期間が強調表示されるため、修復の遅れを明確に把握できるようになりました。

盲点をなくし、厳重な保護を実現

キャンパスセキュリティチームでは、可視性が向上したことで、より深刻な問題も明らかになりました。「Splunkは、管理対象であることに誰も気づいてすらいなかった数百のシステムを検出しました」とシニアITセキュリティアナリストは言います。このような「忘れられた資産」を洗い出すことで、攻撃者に悪用される可能性があったセキュリティ上のギャップを解消し、シャドー ITを削減して、コンプライアンスレポートの基準を明確化しました。こうして、かつてはバラバラに感じられた作業が、説明責任が組み込まれた一貫性のあるプログラムに生まれ変わりました。

Splunk Enterpriseは、アマゾン ウェブ サービス(AWS)の古いアカウントを特定して削除するためにも役立ちました。キャンパスセキュリティチームは、SplunkでAWSのユーザーデータを相関付け、非アクティブなアカウントにフラグを付けて所有者に通知する作業を自動化し、学生が退学した後に乗っ取られる可能性があった数百のアカウントを削除しました。Splunkを導入したことで、最終的に、セキュリティチームの貴重な時間とリソースが節約されました。今日では、アカウントの所有者を追跡する必要がなくなり、調査をすばやく実行できるようになって、リスク状況が改善されました。

構内の医療システムでリスクをリアルタイムに把握

医療システムで以前使用していたログツールでは、組織のデータを一部しか取り込めず、ログの操作やソースの相互参照もできませんでした。そのため、アナリストは複数の異なるツールを使って作業を補う必要があり、手作業が増えて調査に時間がかかり、病院や診療所が脅威に対して脆弱な状態に陥っていました。「以前は、マシンがネットワークに接続できない原因を突き止めるために、少なくとも4つのシステムをチェックしなければなりませんでした」とSIEMエンジニアは振り返ります。

Splunk Enterprise Security (ES)の導入後は、アナリストが必要なデータを見つけるために複数のツールを行き来する必要がなくなりました。現在では、ワークフローに合わせて設計されたダッシュボードですべての作業を行っています。「Splunk Enterprise Securityで作成したダッシュボードで、ホスト名、IPアドレス、またはMACアドレスを入力するだけで、どのチェックでエラーになったかがわかります」とSIEMエンジニアは言います。以前のプロセスとは一変し、アナリストはデバイスの問題をすばやく解決して、医療システムのネットワークを安全に維持できるようになりました。

医療セキュリティチームにとって最も強力な武器となったのがリスクベースアラート(RBA)です。RBAを使えば、すべてのアラートを個別のインシデントとして扱うのではなく、ユーザー、デバイス、システムにリスクスコアを割り当て、複数のデータソースをまたいでスコアを追跡できます。この相関付けにより、これまで見えなかったパターンが明らかになり、不審な挙動に関するインサイトを獲得できるようになって、全体的なセキュリティ態勢が強化されました。「巧妙な攻撃者は、ネットワーク内で活動するときに、決定的な証拠をほとんど残しません」とSIEMエンジニアは説明します。「Splunk ESの最も優れた点は、アラートにリスクプロファイルを重ねることで、全体的なリスクを1つの画面で計算できることです」

また、セキュリティチームは、アラートをリスクスコアに統合することで誤検知を減らし、重要なイベントの調査に集中できるようになりました。「今では、ノイズを追いかけるのではなく、実際のリスクに基づいて優先順位を付けることができます」とSIEMエンジニアは評価します。

学長が信頼できるコンプライアンスレポートの作成

学長から、キャンパス全体のEDR (エンドポイント検出/対応)カバレッジを100%にするように求められたとき、医療システムのSIEMエンジニアは、Splunk ESを活用することを思いつきました。Splunk ESの資産データベースを単一の情報源として使用することで、EDRの対象に含まれているデバイスと含まれていないデバイスを正確に示すことができます。

この正確さは、大学の役員の期待に応えるだけでなく、医療システムのコンプライアンス態勢を高め、将来的に高額な罰金を科されるリスクを軽減することにもつながりました。

> SplunkはSIEMの最高峰です。
>
> **SIEMエンジニア**

Splunkの存在は、医療セキュリティチームに、より高度なイニシアチブに取り組む自信も与えました。前述のSIEMエンジニアは、Splunkの指定エキスパートのサポートにより、データモデルの改良から、検出ルールリポジトリのカスタムSplunk Appへの変換まで、日常の監視を超えた大規模プロジェクトを推進できたと高く評価しています。「専任のエキスパートがいることで、以前ならば躊躇していたプロジェクトにも挑戦できるようになりました」と語ります。「エキスパートは相談相手として頼りになるだけでなく、最適化できる領域を的確に示してくれます」

教育と患者ケアの将来を見据えてレジリエンスを強化

旅はまだ終わっていません。医療セキュリティチームは今後、Splunk Asset and Risk Intelligence (ARI)を使って、資産状況の詳細な把握、セキュリティ調査のさらなる迅速化、すぐに使えるコンプライアンスメトリクスを活用したコンプライアンスとリスクコントロールの状況の明確化に取り組む予定です。

一方、キャンパスセキュリティチームは、セキュリティが確保されていないデバイスがネットワークに接続するのを阻止するために、インベントリの管理やコンプライアンスのプロセスを強化することを目指しています。また、セキュリティ態勢ダッシュボードの拡張や自動アラートの改良にも取り組む計画です。

この大学は、シスコのワイヤレスソリューションの大口顧客でもあり、シスコのスケーラビリティテストでも重要なパートナーとして協力しています。シスコのスタックは、大学のデータセンターから、キャンパス、ワイヤレスネットワークまで広がり、複数のCatalyst Centerを導入して拡張性の課題に対処しています。さらに、シスコの顧客の中でも最大規模のIdentity Services Engine (ISE)を展開しています。

「SplunkはSIEMの最高峰です」とSIEMエンジニアは評価します。この言葉は、Splunkがキャンパスと医療の両方のセキュリティに果たす役割の大きさを物語っています。この名声ある大学は、今後もSplunkを通じて、教育、イノベーション、患者ケアを自信を持って提供し続けることができます。

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_anonymous-university_v3-JA-202603