VECTRA

お客様事例 | 持株会社

ALJがサイバー攻撃を問題なく阻止し、ノイズを90%削減した方法

Abdul Latif Jameel

組織
アブドゥル・ラティフ・ジャミール (ALJ)

業界
持株会社

課題
ALJは、SIEMから大量のアラートを受け取るが、実用的なインサイトが得られないという課題に直面していました。

ソリューション
Vectra AIの導入により、ALJは包括的な可視性と効率化された脅威検知を実現。これにより高優先度の脅威に集中し、対応効率を向上させることができました。

概要

80年近い歴史を持ち、35カ国に拠点を置くアブドゥル・ラティフ・ジャミール (ALJ) は、モビリティやエネルギーから金融サービス、ヘルスケアなど、幅広い産業に事業を展開しています。同社の卓越した業務運営への取り組みにより、成長を続ける中でも、データと顧客の保護に対する確固たる姿勢を維持しています。

セキュリティの変革
プラットフォーム価値の概要

Vectra AIの導入により、ALJは全運用環境を横断する可視性を獲得。防御体制の強化、遅延とエクスポージャーの削減、Microsoft 365の悪用への直接的な対処を実現しました。

Vectra AIのマネージド検知とレスポンス (MDR) サービスを追加導入したことで、ALJチームは高優先度脅威に集中できる一方、継続的な監視と分析をバックグラウンドでシームレスに実行できるようになりました。

導入から1年で、ALJはノイズとアラートが引き起こすストレスを劇的に削減しました。

Vectra AI の Attack Signal Intelligence 導入以前	Vectra AIの Attack Signal Intelligence 導入後	Vectra AI MDR 分析結果	成果
検知件数：8,281件	Vectra MDRによる調査対象エンティティ：856件	Vectra MDRによるエスカレーション対象エンティティ：43件	ノイズ削減率：90% エスカレーションが必要なエンティティの削減率：95%

こうした成果を得るには、まずいくつかの根本的な障壁を克服する必要がありました。

課題

アラート過多と可視性のギャップとの戦い

ALJでは、多くの組織と同様にある困難な課題に直面していました。それは、膨大なアラートと潜在的な脅威に対する明確なインサイトの欠如です。既存のインフラはセキュリティ情報イベント管理ツール (SIEM) に大きく依存していましたが、実用的なインテリジェンスが提供されていませんでした。

ALJのコーポレートCISO兼コーポレートテクノロジー担当マネージングディレクターであるTom Gamali氏は次のように説明しています。「ノイズを排除し、スタッフに負担をかけないソリューションが必要でした。対応すべきことを明確に警告してくれるプラグアンドプレイ型のデバイスを求めていました。」

この簡潔性・正確性・明瞭性への要望は、異なるチーム間の根本的な連携不足を浮き彫りにした。新しいソリューションの検証を担当する概念実証 (PoC) チームは評価中に脅威をより可視化できた一方、日常の運用を担うSOCチームは情報から取り残されてしまったのです。

「PoCチームとSOCチームは隣同士に配置されていましたが、PoCチームのみが重要な脅威指標を把握していました。両チームが完全に切り離されていたのです」と同氏は述べます。

「Vectra AIのレポートが稼働しているのを見ることで、夜も安心して眠れます。もはやSIEMレポートはほとんど確認しません。参照・共有するレポートはVectraだけです」

TOM GAMALI 氏
ALJ、コーポレートCISO兼
コーポレートテクノロジー担当
マネージングディレクター

ソリューション

脅威検知を強化する戦力増強ツール

ALJは既存ツールに深刻な攻撃を特定するコンテキスト情報が不足していると認識し、このギャップを埋めるソリューションを探し始めました。

同社が選んだVectra AIプラットフォームは、データセンター・ネットワーク・クラウド環境を横断した包括的な可視化を実現。

プラットフォームのAI主導型の優先順位付けにより、SOCチームは集中的なインサイトを得ることができ、日々の脅威検知をより迅速かつ効率的に行えるようになり、これまで制限されていた障壁が解消されました。

また、不要なノイズをフィルタリングすることで、最優先の脅威への対処に注力することが可能になりました。

クラウドとオンプレミスを横断した可視性の統合

クラウドとオンプレミスの両方の可視性を提供するプラットフォームの能力は、ALJがVectra AIを採用する決定的な要因でした。

「Vectraがクラウド機能とオンプレミス機能の両方を備えているという事実は、当社にとって極めて重要でした。今ではスケーリングが非常に容易です。SIEMは導入せず、センサーのみを設置する予定です」とGamali氏は語ります。

脅威の検知とレスポンスにおけるVectra AIとSIEMの違いは比較する中でより明確になりました。同氏は次のように述べます。

「Vectra AIは安全性とコンプライアンスの両方を保証してくれます。一方SIEMは規制要件に特化しています。」

AI主導型の検知と迅速なレスポンスでMicrosoft 365の悪用を阻止

Vectra AIによって膨大なデータを分析し悪意ある活動を特定できたことで、ALJチームは断固たる対応が可能となりました。フィッシング攻撃やその他のユーザー主導型脅威が重大なリスクをもたらすMicrosoft 365環境において、こうした機能は極めて重要です。

「Vectra AIの自動化かつカスタマイズ可能なレスポンス機能は当社にとって有用です。Microsoft 365のセキュリティ研修によってフィッシングの被害にならないようにしていますが、万が一悪意のあるリンクを誰かがクリックした場合でも、30分間利用を停止することで、さらなる侵害リスクを冒さずに調査時間を確保できます」とGamali氏は述べます。

このレベルの追跡はレスポンスの効果を向上させただけでなく、経営陣からの好意的な評価も得ました。同氏は「取締役会に565件のアカウントを調査し、Vectraがすべて通知したという事実を報告したところ、内部活動を正確に追跡できている証拠として非常に喜ばれました」と指摘します。

「PoCチームとSOCチームは隣同士に配置されていましたが、PoCチームのみが重要な脅威指標を把握していました。両チームが完全に切り離されていたのです」

TOM GAMALI 氏
ALJ、コーポレートCISO兼
コーポレートテクノロジー担当
マネージングディレクター

MDRによる脅威対応の最適化

ALJのセキュリティチームは、Vectraのマネージド検知とレスポンス (MDR) サービスに価値を見出しました。

「マネージドサービスは、導入において重要な要因でした。当時、MDRを提供していた企業はごくわずかで、Vectraはそのひとつでした」とGamali氏は説明します。

新たな人材を雇わなくとも専門家による24時間体制の分析により、社内のセキュリティチームは時間のかかるタスクを依頼し、より重大な脅威に集中できます。

30日間の概要

Vectra AI の Attack Signal Intelligence 導入以前	Vectra AIのAttack Signal Intelligence 導入後 + MDR	Vectra AI MDR 分析結果	成果
検知件数：575件	Vectra MDRによる調査対象エンティティ：49件	Vectra MDRによるエスカレーション対象エンティティ：20件	ノイズ削減率：91% エスカレーションが必要なエンティティの削減率：59%

確かな意思決定を支える信頼性の高いレポート

プラットフォームが信頼できるデータの主要な情報源となるにつれ、ALJのセキュリティチームは無関係な情報をふるいにかける必要がなくなりました。代わりに、意味のあるインサイトに頼って脅威に自信を持って対処し、円滑なセキュリティ運用を維持できるようになったのです。

Gamali氏はこのように語ります。「Vectra AIのレポートが稼働しているのを見ることで、夜も安心して眠れます。もはやSIEMレポートはほとんど確認しません。参照・共有するレポートはVectraだけです」

「お客様事例」をもっと読む