VECTRA
SECURITY THAT THINKS.®

ケーススタディ

医療サービスGMMH、Cognito for Office 365で攻撃を阻止

アカウントの乗っ取りとも呼ばれる認証情報の不正利用は、SaaS（Software-as-a-Service）プラットフォームに対してよく行われるサイバー攻撃手法です。月間2億人以上のユーザーを抱えるMicrosoft Office 365においても、この攻撃は発生しています。

サービスを利用する人数が多ければ多いほど、管理は行き届かなくなります。そして攻撃者が人々の振る舞いを悪用して、重要なビジネスデータを取得する権限を入手しようとするのです。

英国の国民医療サービスの一部で、イングランド北西部にあるGreater Manchester Mental Health（GMMH）もこの点を懸念していました。GMMHは、約5,400人の従業員と140以上の拠点を持ち、年間5,300人の患者にメンタルヘルスに関する医療サービスを提供しています。

「Vectra AIを導入する前は、ネットワークトラフィックやOffice 365内での悪意のある振る舞いに対して、可視性が限られていました。今では、可視性が高まり感銘を受けています」

Kevin Orritt氏
GMMH、ICTセキュリティ・マネージャー

Vectra® AIのCognito®プラットフォーム上で動作するCognito for Office 365は、Office 365、Azure Active Directory、SharePoint、OneDrive、Exchangeなどの複数のサービスからアクティビティログを取り込むことができます。

NHS
Greater Manchester Mental Health
NHS Foundation Trust

組織

Greater Manchester Mental Health NHS Foundation Trust

業種

医療サービス

課題

ネットワークトラフィックやOffice 365内の悪意のある振る舞いに対する可視性に限界があった

選定基準

隠れた攻撃を明らかにできる自動脅威検知と、ネットワークの完全な可視化

結果

- ネットワーク全体の脅威の振る舞いを可視化できた
- Office 365の認証情報の不正使用を検知し、阻止する自信がついた
- 発生したことに対処するだけではなく、一歩先を踏まえた行動することで、エンドユーザーコミュニティとの連携に時間を割くことができるようになった

Office 365アプリケーションの動作を深く理解しているVectra AIは、AIベースの機械学習アルゴリズムを適用し、被害や盗難が発生する前に、隠れたサイバー攻撃者を積極的に検知して対応します。

Vectra AIは、ログイン、ファイルの作成と操作、データ漏洩対策の設定、メールボックスのルーティング設定と自動化の変更などのイベントを分析し、攻撃者の振る舞いパターンを明らかにします。

検知された情報は、アカウントに関連付けられ、リスクに基づいて優先順位付けされるため、セキュリティ担当者は完全な攻撃シナリオを把握することができ、脅威に迅速に対応して被害を軽減することができます。

「Vectra AIは、我々のデプロイメント全体における脅威の振る舞いについて、とても優れた可視性を提供してくれます。今では、Office 365内で発生した認証情報の不正使用を検知して阻止できるという自信を持てました」とOrritt 氏は言います。

「導入と設定に多くの時間と労力を必要とする他のシステムと比べて、トレーニングも簡単でした」

分かりやすさと使いやすさ

GMMHは、ネットワーク面でも課題を抱えていました。ウイルス対策ソフトウェア、LogPoint SIEM、次世代ファイアウォールを導入していましたが、加えてネットワークの検知および応答（NDR）にかなり前から注目していました。さまざまなNDRソリューションを検討しましたが、費用がかかり、操作が難しいために導入を踏みとどまっていました。そんな中「Vectra AIははるかに直感的で、使いやすく、理解しやすかったのです」とOrritt 氏は述べています。

すでに導入済みの他の国民医療サービスの組織とも相談し、Vectra AIが同組織の環境でもうまく機能していることを知った上で、GMMHは、Vectra AIを導入するための資金を確保しました。「導入は迅速かつ簡単でした。導入と設定に多くの時間と労力を必要とする他のシステムと比べて、トレーニングも簡単でした」

5,400人の従業員を抱えるGMMHにとって、ネットワークに関する最大の課題のひとつは、すべてのデバイス、ロケーションにおいてセキュリティ監視を行い、各デバイスがどのように通信しているかを把握することでした。

「同じようなことを可能にするツールはいくつかありますが、使うまでには時間を要します。我々は、デバイスからどのような種類のトラフィックが流れているのか、デバイスがどのように動作しているのかを確認する方法がありませんでした。Vectra AIを試すには良い機会だったのです」

「Vectra AIを使うことで、発生したことに対処するだけではなく、一歩先を踏まえた行動ができるようになりました。これは大きな意味があります。無関係なログからアラートを追いかける代わりに、エンドユーザーコミュニティーと協力して、重要なセキュリティ対策について集中し、時間を費やすことができるようになったのです」

可視化で見えてきたこと

Vectra AIのCognitoプラットフォームが稼働して間もなく、企業ネットワーク上で不明なデバイスが検知されました。「我々のネットワークでは許可していないWindows 7のデバイスからで、組織では使用していないAWSクラウドと通信していました」とOrritt 氏は述べます。

確認したところ、該当のデバイスは、GMMHの事務所の清掃を請け負っていた会社のものでした。「外注先の社員が当社のネットワークに接続してしまったのです」と同氏は言います。「起こってはならないことでしたが、このケースは、特に悪意はなかったと考えています。その他にも、許可されたデバイスを持つ正規のユーザーではあるものの、制限されているサービスと通信にアクセスしようとしたことも検知されました」

詳細については、info-japan@vectra.aiまでお問い合わせください。

安全な一日を

現在Vectra AIは、Orritt氏のサイバーセキュリティ業務の重要な一部となっています。「一日の業務にうまくフィットしています。朝一番にすることは、高レベルまたは重要レベルの新しくトリアージされたアラートがあるかどうかをチェックすることです。また、Microsoft Teamsとも統合しているので、外出先でもアラートを確認することができます。何か変わったことや疑わしいことがあれば、その日のうちに対応することができ、以前よりもずっと早い対応が実現しています」

Vectra AIがネットワークの検知および応答を担う間に、同氏はエンドユーザーのセキュリティ意識の向上と管理に注力する時間が増えました。

「Vectra AIを使うことで、発生したことに対処するだけではなく、一歩先を踏まえた行動ができるようになりました。これは大きな意味があります。無関係なログからアラートを追いかける代わりに、エンドユーザーコミュニティーと協力して、重要なセキュリティ対策について集中し、時間を費やすことができるようになったのです」とOrritt氏は語っています。