VECTRA
SECURITY THAT THINKS.®

CASE STUDY

世界的金融サービス会社、サイバー攻撃を阻止するためにNDRを活用

Vectra®のネットワーク検知および対応ソリューション（NDR）を導入した後、「セキュリティ業務に関する霧が突然晴れたかのようでした」という言葉を、ある世界的な金融サービス会社のサイバーセキュリティ責任者からいただきました。

このNDRソリューションとはクラウドやデータセンターのワークロード、Microsoft Office 365のようなサービス、ユーザーやIoTデバイスに対するサイバー攻撃を瞬時に検出し、対応するVectra AI社のNDRプラットフォームCognito®を指しています。

銀行業務と資産管理において150年という長い歴史を誇り、約12兆円を超える資産を持つこの独立系金融サービス会社にとって、サイバー攻撃者の隠れた振る舞いを可視化することは非常に重要なことでした。

ゼロから100まで

「Vectraを使用することで、攻撃者の振る舞いの可視性がゼロから100へと向上しました。驚いたのは、ネットワークトラフィックの内部まで見ることができることです。すべての攻撃のコンテキストと詳細がわかり、どの攻撃への対応が最も重要なのかを把握できます」と同社のサイバーセキュリティ責任者は言います。

この成功への道のりは簡単ではありませんでした。「私が担当を始めたときには、SIEMを使っていました。しかし、誰も真の意味で管理していなく、すでに時代遅れで、多くのソフトウェアパッチが必要でした。再起動したり、持っていたセキュリティツールを使ってみたりしましたが、かなりの挑戦でした。」

当時、同社のセキュリティ・オペレーション・センター (SOC) は常にレスポンスモードでした。SOCメンバーは不審な兆候を見つけると、徹底的に調査を行っていました。煙をみつけるとすぐに駆けつけ調査するといった状態だったそうです。

「Vectraを使用することで、攻撃者の振る舞いの可視性がゼロから100へと向上しました。」

サイバーセキュリティ責任者
世界的金融サービス会社

組織

金融企業

分野

金融サービス

挑戦

セキュリティチームは常に対応しなければならず、多くのソフトウェアパッチを必要とする社内開発のソリューションを使っていた。

選定基準

ネットワーク内の隠れた脅威を先を見越して検出し、対応できるようにするプラットフォーム。

結果

- 1年運用していたSIEMから得られる高い情報価値をわずか1週間で取得。
- 調査中にDHCPログをふるいにかけたり、IPアドレスの変更を特定したりする必要がなくなった。
- Cognito Detectが調査すべき全ての重要なアラートを通知、さらに対処方法も通知されるようになった。

同社は、まずDarktraceやVectraなどのNDRソリューションの選定評価から始めました。SOC担当者には、適切なNDRソリューションがあれば、ネットワーク内部に潜む脅威を先回りして検知し、対応できるようになるという期待がありました。

「Darktraceには納得できませんでした。素晴らしいインターフェイスを持っていましたが、あまり効率的に動作しませんでした。」

逆に、同社のSOC担当チームは、Vectraを初めて使った時に「非常に快適」で「力強いツール」だと感じたと評しています。Vectra は、暗号化されたトラフィック中の攻撃者の振る舞いを検出し、復号化やパケット検査を必要としません。

「Vectraはすぐに稼働しました」とサイバーセキュリティの責任者は言います。「使いやすく、グラフィカルなダッシュボードは直感的に操作できました。サイバーセキュリティの専門家でなくても、Vectraを使うことができます。」

この金融サービス会社は、NDRソリューションとして、最終的にVectra Cognito Detect™ for Office 365、Cognito Detect、Cognito Recall™を選択しました。これらはすべてCognitoプラットフォーム上で稼働します。

実行するハンティング

認証情報の悪用は、月間2億人以上のユーザーを抱えるOffice 365に対するサイバー攻撃の主な手法です。ずる賢い攻撃者は、人間の振る舞いを悪用してパスワードを乗っ取り、アカウントを乗っ取り、重要なデータを盗み出します。

同社のSIEMは、これに対応するためにOffice 365のログを受信していたため、SOC担当者はルールを設定することに時間がとられていました。しかし、Cognito Detect for Office 365を導入してからは、この面倒な手作業は必要なくなりました。

サイバーセキュリティの責任者によると「1年かけてSIEMを構成するよりも多くの価値を、1週間でVectraから得ることができました」とのことです。

Cognito for Office 365は、Office 365、Azure Active Directory、SharePoint、OneDrive、Exchangeなど複数のサービスからアクティビティログを取得します。Vectraは、ログイン、ファイルの作成と操作、DLP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を分析します。

Vectraは、AI由来の機械学習アルゴリズムを適用し、これらのサービスにおける攻撃者の振る舞いを積極的に検知し、対応することで、被害や盗難を未然に防ぎます。検知はアカウントと相関し、リスクに基づいて優先順位付けされ、セキュリティ専門家に攻撃の手法を提供することで、脅威を迅速に阻止し、軽減することができます。

「Vectraは必要なすべての脅威情報をSOCアナリストに提供してくれます。Cognito for Office 365には高い価値があります」

Cognito DetectとRecallの導入効果

同社は、ファイアウォールやIDPSなどの境界セキュリティを簡単に回避してしまう進行中のサイバー攻撃者を特定して阻止するためにCognito Detectを使っています。

「Cognito Detectは必要不可欠です。短時間で価値を生み出します。ダッシュボードに表示される重要なアラートはすべて調査する価値があり、Cognitoはその対処方法を正確に教えてくれます。」

ネットワーク内の必要な場所にセンサーを配置できるという柔軟性も評価されました。「トラフィック内の死角を排除するために、必要なだけのセンサーを配置することができます。プラットフォーム全体が使いやすく、高速で、よく統合されています。」

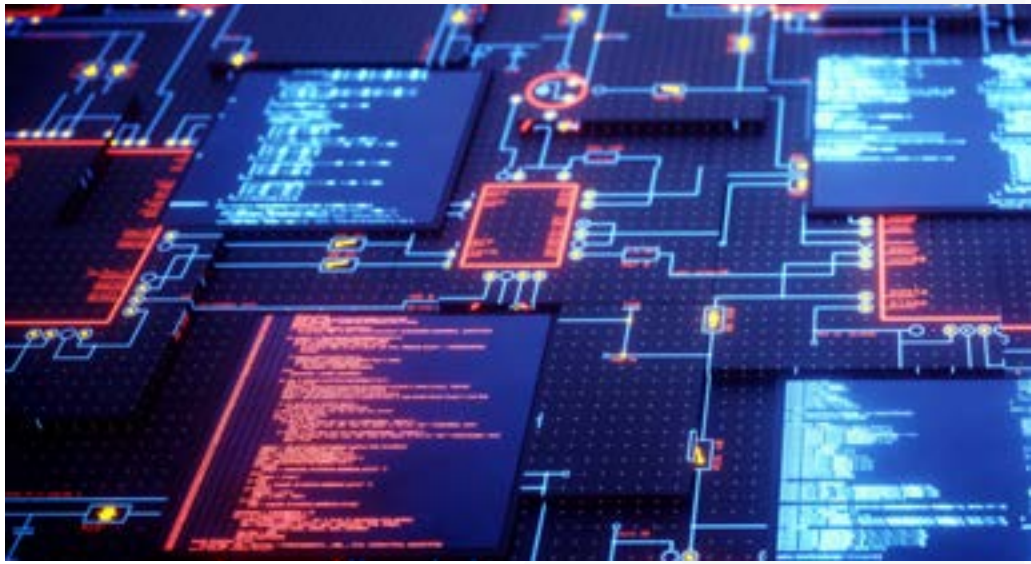
同社はまた、セキュリティ強化されたメタデータを使用して脅威の探索とインシデント調査を劇的に改善するために、クラウド型の調査ワークベンチであるAI駆動型のCognito Recallを導入しました。

Vectraは、クラウド、SaaSやデータセンターのワークロード、ユーザーやIoTデバイスを含むすべてのネットワークトラフィックから、関連するログ、クラウドイベント、メタデータを抽出、分析、保存します。メタデータには個人情報が含まれていないため、データのプライバシーが保護され、厳しい金融サービスポリシーの遵守が保証されます。

このメタデータは、あらゆる攻撃について深いセキュリティのインサイトとコンテキストで強化されます。これにより、同社は、これまでにない可視性を得て、より効率的かつ正確にサイバー脅威の検出、対応、ハント、調査を行うことができます。

「トラフィック内の死角を排除するために、必要なだけのセンサーを配置することができます。プラットフォーム全体が使いやすく、高速で、よく統合されています。」

サイバーセキュリティ責任者
世界的金融サービス会社



強化されたメタデータには個人情報が含まれていないため、データのプライバシーが保護され、金融サービスのガバナンス・ポリシーや規制上必須となるコンプライアンスが保証されます。

メタデータには、IPアドレスだけでなくホスト名も含まれています。よって、「DHCPログをふるいにかけてデバイスのIPアドレスを見つけたり、調査中にIPアドレスの変更を特定したりする必要はありません。お客様の時間がない時ほど、すばやいホスト名検索が有効な手段となるのです。」とサイバーセキュリティの責任者は言います。

この金融サービス会社にとって、Cognitoプラットフォームは SOCの重要な部分であり、組織を破滅させる可能性のあるサイバー攻撃者を特定して阻止することを先回りしたアプローチを取ることを可能にしています。

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