VECTRA
SECURITY THAT THINKS.®

ケーススタディ

電力供給を支えるHydro Ottawaのセキュリティ

Hydro Ottawa社、脅威の検知および対応を自動化し、調査にかかる時間を大幅に短縮。

Hydro Ottawa は、32万3,000人以上の企業や家庭に電力を供給しています。現在、電力網や公益事業者への攻撃が急増しており、カナダ、オンタリオ州東部最大の配電会社である同社にとって、電力を供給すると同時に企業のITや重要なインフラシステムをサイバー攻撃から守ることも必須要素となっています。

サイバー攻撃は現実のものである

Hydro OttawaのITセキュリティ・マネージャーであるJojo Maalouf氏は、「サイバー攻撃は必ず起こるものです。できるだけ早く脅威を検知し、修復しなければなりません。私たちは今までログアグリゲーターを使用していましたが、数多くの脅威をマニュアルで探す必要がありました」と述べています。

「それがVectra AIに注目した理由です。Vectra AIはソフトウェア版のセキュリティアナリストといえます。面倒で手間のかかる脅威探索を処理し、最もリスクの高い脅威を自動的に検知し、スコアリングし、優先順位を付けます。これにより、脅威の調査にかける時間を劇的に短縮することができます」

Vectra® AIのCognito®ネットワークの検知および対応プラットフォームは、人工知能と、データサイエンス、機械学習、振る舞い分析の組み合わせを用いて、Hydro Ottawa社のセキュリティアナリストの作業を補強しています。サイバー攻撃者はネットワーク内で存在を隠すことに長けていますが、Cognitoは暗号化されたトラフィックであっても確実に検知し、攻撃の振る舞いを明らかにします。

サイバー攻撃者は、ファイアウォール、侵入防止システム、エンドポイントセキュリティシステムを回避し、盗み出したり破壊したりする重要な資産を探し回ってネットワーク内部に広がります。しかし、そんな攻撃もCognitoを使用することで迅速に検知できます。

HydroOttawa

組織

Hydro Ottawa

業種

公益事業

課題

感染してから検知するまでの時間のギャップをなくす

選択基準

脅威管理を自動化でき、さらに使いやすく、他のセキュリティツールとの統合が容易であること

結果

- 脅威の検知と対応が迅速化できた
- マニュアルでの脅威探索をなくし、脅威調査を迅速化できた
- 最もリスクの高い脅威が自動的にスコアリングされ、優先順位付けされるため、セキュリティチームは被害が拡大する前に攻撃者を迅速に阻止できる
- NISTフレームワークに基づく高度なサイバーセキュリティ保護

「Vectra AIは、面倒で手間のかかる脅威の調査を自動化し、最もリスクの高い脅威を検知し、スコアリングし、優先順位付けします」

Jojo Maalouf氏
Hydro Ottawa、ITセキュリティマネージャー

脅威管理の自動化

Maalouf氏は次のように述べています。「Vectra AIは必要としていることを正確に実行してくれます。よって、我々のチームは、攻撃者がデータを盗んだり、重要なインフラに損害を与えたりする前に、即座に行動して攻撃を阻止することができます。Vectra AIから得られる実用的な情報は非常に有益です」

エンタープライズネットワーク上の脅威をリアルタイムに検知することで、Hydro Ottawaは、標的型攻撃が業務用ネットワークに広がるのを防ぎ、地域全体の配電に支障をきたすのも防ぐことができます。

また同社は、サイバー攻撃のすべてのフェーズを可視化できます。Cognitoは、コマンド&コントロール通信、内部偵察、ラテラルムーブメント、データ流出などの基本的な攻撃の振る舞いだけでなく、ランサムウェア、リモートアクセスツール、隠されたトンネル・暗号化トンネル、バックドアに対する脆弱性、管理者資格の乱用などの攻撃の初期兆候も明らかにします。

さらに、Cognitoは物理ホストと仮想ホストを監視し、侵害や内部からの脅威の兆候を検知します。また、教師あり学習、教師なし学習の機械学習を使用することで、変化するネットワーク環境に容易に適応し、未知および既知の脅威を検知できるのです。

より効果的なセキュリティオペレーション

Maalouf氏は、「Vectra AIの導入により、当社のセキュリティオペレーション全体がはるかに効率的になり、脅威の調査をより効率的に行うことができるようになりました」と語ります。

Vectra Threat Certainty Index™は、効率性の向上に大きな役割を果たしています。これは、何千もの脅威イベントと履歴を自動的に統合し、最大のリスクをもたらす感染したホストを、高い確実性でピンポイントに特定します。

「Vectra AIの4画面のユーザーインターフェイスのデザインが気に入っています。組織にとって最大のリスクとなる脅威は、画面の右上に表示され、直感的に分かります」脅威と確実性のスコアは、Hydro Ottawaのセキュリティチームへの通知や、エンドポイントセキュリティ、ファイアウォール、SIEM、その他のポイントでの応答のトリガーとなります。例えば、同社では、データ流出に関するアラートを設定しています。

Cognitoはまた、セキュリティチームがより早く脅威を阻止できるよう、コンテキストを提供します。キーとなるホストやその他の資産は明示的に追跡され、セキュリティアナリストは感染したホストが通信するデバイスやその通信方法を即座に確認できます。また、パケットキャプチャからメタデータにオンデマンドでアクセスすることで、インシデント対応を迅速化することができます。

同氏は、Cognitoがログデータを後から振り返るのではなく、権威あるソースとしてネットワークトラフィックを分析していることを高く評価しています。「ネットワークトラフィックは唯一の正しい情報源です」

この新たに得た効率化により、同社はCognitoをCarbon Blackエンドポイントセキュリティ、IBM QRadar SIEM、Palo Alto Networksファイアウォールと統合する計画を立て、脅威の修復を改善しています。

監査の簡素化

Maalouf氏は、Cognitoから得られる実用的な脅威情報は、Hydro Ottawaが内部監査を実施し、NISTサイバーセキュリティフレームワークを導入する際にも貢献したと述べています。このNISTサイバーセキュリティフレームワークとは、サイバーセキュリティのリスクを特定し、脅威イベントの検知、対応、回復を行うためのガイドラインと推奨事項を含むものです。

「Vectra AIを導入したことで、感染してから検知するまでの時間のギャップを埋めることができました」と同氏は語ります。さらに「コンプライアンスはあくまでもベースラインですので、電力インフラを守るためには、その規制を満たすだけでなく、強力なセキュリティ対策が必要なのです」と続けます。

すぐに価値を生み出す

Hydro Ottawaにおいて、Cognitoを使って価値を生み出すまでに時間はかかりませんでした。セキュリティの概念実証テストは時間がかかることで知られていますが、Maalouf氏はCognitoへの評価を「非常に簡単である」と表現しました。

Cognitoは、導入初日から価値を提供し続け、Hydro Ottawaのセキュリティオペレーションにとって不可欠な存在となっています。

「Vectra AIの早期検知機能により、重要なインフラがダメージを受けたり、貴重なデータが盗まれたりする前に、サイバー攻撃者を阻止する自信がつきました」と同氏は言います。「特定のネットワークデバイスの設定を変更することで、脆弱性を排除するのにも役立ちました」

Cognitoは、導入初日から価値を提供し続け、Hydro Ottawaのセキュリティオペレーションにとって不可欠な存在となっています。

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