VECTRA
SECURITY THAT THINKS.®

ケーススタディ

エネルギー業界における、サイバーセキュリティの重要性

Tri-State Generation and Transmission Associationは、コロラド州、ネブラスカ州、ニューメキシコ州、ワイオミング州にまたがる200,000平方マイル（約500,000平方キロメートル）のサービスエリア内の44の電気協同組合に電力を卸供給しています。アメリカ国内の電力網に対するサイバー攻撃の脅威レベルは過去最高であり、インフラを守ることは、消費者や企業のデータを守ることと同様に最重要事項となっています。

公益事業におけるサイバー攻撃をリアルタイムで検知

アメリカにおいて、国家安全保障局や国土安全保障省が、国家の電力網の脆弱を確認すると、人々の不安は高まります。そして実際は、サイバー攻撃によって国家の電力網が停止するという脅威は、現実に起こりうることです。そこで、電力会社は家庭や企業の明かりや暖房を維持するために、セキュリティ対策を強化することが必要とされます。

Tri-State Generation and Transmission Associationは、Vectra® AIのCognito®ネットワーク検知および対応（NDR）プラットフォームを用いてセキュリティ脅威をリアルタイムに追跡することで、電力供給に対する攻撃によるリスクを回避しています。Tri-State社のシニアITセキュリティアドミニストレーターであるDave Buffo氏は「サイバー攻撃に対してセキュリティの観点から、常に懸念しています」と述べています。

「Vectra AIはネットワークを可視化してくれるので、内部のホストを監視し、リアルタイムにセキュリティ問題に対処することができます」

TRI-STATE
Generation and Transmission Association, Inc.
A Touchstone Energy® Cooperative

組織

Tri-State Generation and Transmission Association

業種

エネルギー

課題

Tri-State社の企業データおよび加入者データを守り、電力網へのサイバー攻撃を回避する

選定基準

内部ネットワークと重要なホストの活動を可視化する、使いやすいセキュリティソリューション

結果

- 内部ホストへの可視化によりアクティブなネットワークへの侵入を阻止
- 本物の脅威と偽の脅威に対する洞察をリアルタイムに入手
- 偽のアラートを追跡する時間を削減

「Vectra AIはホストを監視し、本当の脅威を示してくれます。偽のアラートを出すような通常のトラフィックに惑わされることはありません」

Dave Buffo氏
Tri-State社
シニアITセキュリティアドミニストレーター

本物の脅威を明らかにする

Tri-State社は、4つの州にまたがる200,000平方マイル（約500,000平方キロメートル）のサービスエリアで発電と送電を行っています。そして、自らの企業情報および150万人のお客様のデータを保管する内部ネットワークを保護する必要があります。複数のホスト（マスターコンピュータ）は広域ネットワーク全体に配置され、1,500人以上の従業員をサポートしています。

これらのホストは、公益事業のビジネスにとって重要であり、セキュリティのリスクを冒すことはできません。しかし、ホストのトラフィックパターンを把握することに関しては、問題がありました。Tri-State社は、ホストの活動を可視化することができず、潜在的な脅威が発生しても、脅威の種類や程度を示すコンテキストがなく、優先順位もつけられていませんでした。

「我々は、内部のホストで何が起こっているのかを知る必要がありました。ホストが何をしているのか、何と通信しているのか、なぜある特定の通信が行われているのかを把握したかったのです」とBuffo氏は言います。「Vectra AIはホストを監視し、本当の脅威を示してくれます。偽のアラートを出すような通常のトラフィックに惑わされることはありません」

Cognitoプラットフォームは、アクティブなネットワーク侵害をリアルタイムに検知し、分析します。Cognitoは、Tri-State社の内部およびインターネット・ネットワーク・トラフィックを深く継続的に分析し、攻撃者が高い価値のあるデータをスパイ、拡散、窃取しようとする侵害のすべてのフェーズを自動的に検知します。

インテリジェント・セキュリティを求めて

Tri-State社は、Cognitoを導入する前、多くの偽陽性の脅威と戦っていました。ファイアウォール、侵入防止システム、ウイルス対策ソフトウェアを頼りにしてきましたが、これらのツールはBuffo氏の希望通りの結果をもたらしてくれませんでした。「我々はかなり長い間、Vectra AIのソリューションのようなものを探していましたが、やっと出会えました」

以前のTri-State社の侵入防止システムは、危険ではない振る舞いをブロックし、不必要にビジネスを中断させていました。「システムが正常に動作していても、IPSがトラフィックをブロックしてしまうため、ビジネスにとって適切ではありませんでした」

窮地に陥らないために

Cognitoは、Buffo氏やチームの貴重な時間を無駄にはしません。データサイエンス、機械学習、振る舞い分析を組み合わせることで、既知および未知の脅威の一歩先を見据えて検知し、自動的にスコアリングと相関付けを行います。Vectra AIのThreat Certainty Index™は、コンテキストに沿ったスコアリングに基づいて、より重要な脅威をリアルタイムで自動的に表示するため、最も重要な検知に対処することができます。

「以前は何度も窮地に陥っていました」とBuffo氏。「Vectra AIはスマートで、何が脅威で、何が脅威でないかを確実に把握します」以前使っていた監視ツールは、ネットワークをスキャンして潜在的な問題を引き起こす何かがあると、アラートを送信してきました。「Vectra AIを使って、あるアラートのホストを特定しましたが、実際は問題ないものでした。プリンターのマネージドプリントサービスがインクのレベルを調べて、自動発注しているだけだったのです」

Cognitoは、自動化された検知をコンテキストと共に提供してくれるので、セキュリティアナリストは、周辺情報を探すために無駄な時間を費やすことなく、迅速な意思決定を行うすべての情報を一度に得ることができます。

必要なものがすべてあります

Cognitoについては同僚からのメールで知り、読んですぐにBuffo氏は、詳細を調べる価値があると考えたそうです。「すぐに飛びつきました。そして、概念実証を行い、我々の環境にVectra AIのソリューションが適していることが分かりました」

セキュリティチームの2名は、Vectra AIの導入やその使い方を学ぶ中で、特に問題には直面しませんでした。「Vectra AIは非常にクリーンで使いやすく、必要なものはすべて揃っており、問題なく使い方を理解し、導入することができました」

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

遠隔地の工場を即座に可視化

Tri-State社は、現状の企業環境でCognitoを使用して非常に良い結果を得たので、Cognitoのネットワーク検知と対応を、発電所と現場のフィールドに拡大することを計画しています。導入に対する検証は、1つの遠隔地の発電所に配備されたVectra S-seriesセンサーですでに進行中です。

Sシリーズのセンサーは、ネットワーク・トラフィックをパッシブに監視し、重要なメタデータを抽出して、脅威分析のためにXシリーズのアプライアンスに転送します。「このセンサーの設定と導入はとても簡単で、すぐに、何が起こっているのかを可視化することができました」とBuffo氏は言います。Sシリーズのセンサーにより、Tri-State社は、自動化されたリアルタイムの侵入検知を重要なインフラの隅々まで拡張することができます。

1年以内に、発電所や現場の至る所にセンサーを設置することを予定しています。「結果がとても楽しみです。残念ながら、セキュリティにおける脅威がなくなることはありません。そこで、セキュリティを維持するために、最もスマートで最高のソリューションを活用したいのです」

「かなり長い間、Vectra AIのソリューションのようなものを探していましたが、やっと出会えました」