VECTRA
SECURITY THAT THINKS.®

ケーススタディ

農業協同組合Fenaco、SOCにVectra AIを採用

スイスの農業協同組合Fenacoは、Deloitte社の格付けで大規模消費財メーカーとされていますが、世界的な知名度は高くありません。その理由として、ほぼスイス国内のみで製品を運営、販売していることが挙げられます。

1993年に6つの農業協同組合が合併して設立された、70億スイスフラン（約8,300億円）の資産を持つこの企業は、1万人の従業員を抱え、約4万3,000人の組合員（そのうち2万2,000人は現役の農家）が間接的なオーナーとなっています。

Fenacoは、果物、野菜、いも類、穀物から肉、飲料に至るまで、スイスの食料品を消費者に提供。農業、エネルギー、小売、食品産業、輸送、化学、獣医学など幅広い分野をカバーするビジネスユニットを有しています。

Frescoの50のビジネスユニットからなる複雑なエコシステムの安全と運用を支えているのは、協同組合のIT・通信・セキュリティ部門であるFenaco Informatikです。

「Fenacoのセキュリティオペレーションは分散化しており、各チームが独自のセキュリティツールを使用していました。ほとんどがファイアウォールとログに頼った境界型セキュリティでした」

Gustavo Ricco氏
Fenaco Informatik、セキュリティオペレーションマネージャー

fenaco

組織

Fenaco

業種

消費財メーカー

課題

セキュリティオペレーションが分散しており、境界線上のセキュリティツールでは可視性に限界があった

選定基準

SOCの非効率性を自動化するための、AIベースのネットワークの検知および応答（NDR）ソリューション

結果

- ネットワーク内やインターネットに出入りするトラフィック内の攻撃の振る舞いを可視化し、脅威をカバー
- マニュアル作業を自動化することで、脅威探索やインシデント調査などの重要な要件に集中する時間を確保
- 重要なアラートへの対処を容易にする、優先順位付けされた検知機能

「Vectra AIは、ネットワーク内での攻撃者の振る舞いについて、優れた可視性を提供してくれます」

課題：SOCの構築

Fenaco Informatikのセキュリティ・オペレーション・マネージャーであるGustavo Ricco氏は「当社のセキュリティオペレーションは分散化されており、各チームが独自のセキュリティツールを使用していました。ほとんどがファイアウォールとログに頼った境界型セキュリティでした」と語ります。

境界型セキュリティは、規模の拡大が難しく、コストもかかり、サイバー攻撃者に簡単に回避されてしまいます。また、境界線の防御を回避してネットワーク内部をスパイ、拡散、窃盗を行う攻撃者に対する可視性もありません。

コストの増加につながる不要な冗長性や重複を防ぐために、組織内を単一のセキュリティ・オペレーション・センター（SOC）に統一し、最新化するという時が来ていたのです。

SOCの責任者であるRicco氏は、ネットワークやデータセンターにおけるサイバー脅威に対処するには、フル稼動できるSOCが唯一の方法であると理解しておりました。さらに、SOCの多くの非効率性を自動化するために、AIベースのネットワークの検知および対応（NDR）が果たす役割をはっきりと分かっていました。

多くのセキュリティオペレーション担当者は、1日あたり数千件の脅威の可能性があるアラートを手動で調査する必要があります。それによって大きな負担を強いられているのです。すべての指標を追いかけることは、膨大な数のアラートによる疲労を引き起こし、実際の攻撃に集中できないために、攻撃が拡散する時間を増やす結果となってしまいます。

解決策：AI駆動型のNDR

Fenaco Informatikは、いくつかのNDRソリューションを検討しました。「Vectra AIは、攻撃者のネットワーク内の振る舞いにおいて、優れた可視性を提供してくれます。そこで、Cognitoプラットフォーム上で動作するCognito DetectとCognito Streamソフトウェアを採用しました」

Vectra® AIの支援により、Fenacoは Cognito® プラットフォームへの投資の価値を、早いタイミングで実際に体験できるようになりました。同社の最新のSOCは、導入からわずか2〜3ヶ月で完全に稼動したのです。

Vectra AIの Cognito プラットフォームは、セキュリティ業界の NDR の定義以上であると言えます。重要なビジネスデータの保護が任務であるSOCチームが直面している手ごわい課題を解決するために、大きく躍進しています。

Cognitoプラットフォーム上で動作するCognito Detect™は、AI派生型の機械学習アルゴリズムを適用し、クラウド/SaaS、データセンター、IoT、エンタープライズネットワークにおける進行中のサイバー攻撃の振る舞いを自動的に検知し、対応します。

実行性が高く、最大のリスクをもたらす攻撃の振る舞いには自動的に優先順位が付けられ、FenacoのSOCアナリストはどこから修復、ハンティング、調査を開始すべきかを即座に判断することができます。

さらに時間とリソースを削減するために、Cognito Detectは複数のアラートを1つのインシデントや攻撃キャンペーンにロールアップして調査します。AIベースの機械学習により、関連する脅威の検出を自動的にイベントの連鎖に結びつけます。

「SOCにおける多くのマニュアル作業がVectra AIによって自動化されました。これにより、脅威ハンティングやインシデント調査といった重要な要件に集中する時間が大幅に増えました」とRicco氏は述べます。

データの絶対的な基準

Cognitoプラットフォームの有効性の秘密は、データにあります。クラウド/SaaSやデータセンターのワークロードからユーザーやIoTデバイスまで、あらゆるネットワークトラフィックから、関連するログやクラウドイベント、メタデータを大規模に抽出、分析、保存します。

このメタデータに、セキュリティに関する深い洞察とコンテキストを付与することで、これまでにない可視性を実現し、サイバー脅威の検知、対応、ハンティング、調査を驚異的な効率と精度で行うことができます。

「ネットワーク内の攻撃の振る舞いやインターネットに出入りするトラフィックを可視化することで、脅威をカバーしています。検知されたものには常に優先順位がついているので、どれが最初に対処すべきで重要なのかがわかります」とRicco氏は説明します。

脅威の探索と調査の迅速化

Fenaco SOC チームは、Cognito プラットフォーム上の Cognito Stream™ を使用して、重要な攻撃の検知に対応し、脅威調査の開始を高速化しています。Cognito Streamは、ネイティブクラウド、ハイブリッドクラウド、エンタープライズトラフィックから、セキュリティを強化したメタデータをスケールアップして提供し、Fenaco SOCのアナリストがより決定的なインシデント調査を行えるようにします。

Cognito Streamにより、Fenaco SOCチームは、Vectra AIから得られる深いセキュリティ洞察と独自のコンテキストを活用して、攻撃の検知、調査、ハントのためのカスタムツールやフィードモデルを構築することができます。

オープンソースのZeekフォーマットで提供されるCognito Streamは、Zeekに付随する経費やスケールの制限なしに、攻撃に関するセキュリティの洞察やコンテキストを、データレイクとシームレスに統合します。Fenacoの場合はSplunk SIEMとの統合となります。

迅速な対応のために、Cognitoプラットフォームは、EDR、SIEM、SOARツールなどのサードパーティのセキュリティソリューションと同じコンテキストや洞察を統合・共有し、エンドツーエンドの脅威管理と可視化を実現します。

「VectraとSplunkの統合は非常にシンプルで簡単だったので、SOCでの運用を非常に早く開始することができました。今では、最も重要なアラートはVectra AIを見て、syslogとメタデータをSplunkで調査しています。Splunkとともに、Vectra AIは脅威の調査を、数日かかっていたものから数時間に短縮するのに役立っています」とRicco氏は述べています。

「Vectra AIとSplunkの統合は非常にシンプルで簡単だったので、非常に早くSOCを立ち上げることができました。今では、最も重要なアラートはVectra AIを見て、syslogとメタデータをSsplunkで調査しています」

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