VECTRA
SECURITY THAT THINKS.®

ケーススタディ

Ardagh Group、AIで脅威を封じ込める

金属とガラスの包装容器メーカーArdagh Group、隠れた攻撃者を発見し阻止する

キンキンに冷えた飲み物、ツナ缶などの缶詰、瓶に入った調味料などは誰もが手にしたことがあるでしょう。実はその時、Ardagh Groupの製品を皆さんは手にしているのです。

Ardagh Groupは、世界の有名ブランド向けに金属およびガラス製の包装容器を製造。持続可能なビジネスを運営しているこの会社は、ここ数年で急成長を遂げています。現在、食品、飲料（アルコールを含む）、医薬品などの容器を年間350億個生産しています。

グローバルビジネスを守るために

Ardagh Groupは、22カ国で100カ所以上の以上の金属およびガラス製造施設を運営しています。ビジネス拠点が分散された中でも、Ardagh Groupは迅速かつ効率的なビジネスを実現しています。しかし、分散されているからこそ管理すべきリスクも存在するのです。

Ardagh GroupのグループITディレクターであるDavid Whelan氏は、「我々の課題は地理的なものです」と語ります。Ardagh Groupのネットワークは、ファイアウォール、侵入者からの保護、高度なセグメント化など十分に安全性が確保されています。またエンドポイントも保護されており、さらに脅威の情報は事前にアラートされます。

しかし、モバイルやクラウドが境界線の防御をもはや意味のないものとし、機密情報が世界中に拡散してしまう時代において、従来のセキュリティでは不十分です。ITセキュリティチームは、万全の防御体制をすり抜けて侵入してくる攻撃を、確実に可視化しなければなりません。

ArdaghGroup

組織

Ardagh Group

業種

製造業

課題

地理的に世界中に分散したグローバル・オペレーション・ネットワークの中から、隠れた未知の攻撃者を見つけ出す

選定基準

進化する脅威に対応する、AIを活用した脅威検知プラットフォームであること

結果

- 隠れた脅威、特に役員レベルの社員や決済に関する情報を狙った攻撃を徹底的に検知する
- 世界中のネットワーク・トラフィックの正常なパターンを可視化する
- マニュアル作業で時間のかかる攻撃者の検知を自動化することで、脅威調査の作業負荷を軽減

「Cognitoを使えば、被害が出る前に脅威を止めることができます」

Ardagh Group、グループITディレクター
David Whelan氏

Whelan氏は「ロンドンのワークステーションにアクセスできる人は、アイルランドのダブリン本社にいるのと同じようなものです。ネットワークは高度にセグメント化されていますが、社員は共有のアプリケーションやサービスにも必要に応じてアクセスできます」と言います。

クラウドアプリケーションは、サイバーセキュリティをさらに複雑にします。「Office 365に移行すると、新たな課題が発生します。自社のネットワークと同じような可視性は得られないため、リスクを直接確認することができないのです」と同氏は語ります。

AIを活用した脅威ハンティング

AIを活用した脅威ハンティングの自動化とAIは、サイバーセキュリティにとって非常に重要であり「攻撃者が自動化された技術を用いるのであれば、防御も自動化しなければなりません」とWhelan氏は主張します。

同氏とそのチームは、Vectra® AI社のCognito®脅威の検知とハンティングのプラットフォームの概念実証を行いました。偶然にも2018年のサッカーW杯開催中にこのテストは行われ、結果としてCognitoの価値がすぐに証明されました。

「Cognitoは、10個のIPアドレスが同時に同じWebサイトを訪問するような異常なトラフィックを特定しました。結果として無害なものでしたが、Cognitoの価値を確実に示してくれました」

AIを搭載したCognitoは、クラウドやデータセンターのワークロード、ユーザーやIoTにデバイスに潜む攻撃者のリアルタイムな検知を自動化します。

Cognitoは、Ardagh Groupのグローバルネットワーク上で検出された脅威を瞬時に優先順位付けし、侵害されたホストデバイスと相関させ、最大のリスクをもたらす攻撃を優先します。この忠実な可視性により、セキュリティチームは脅威に対して迅速かつ断固とした対応が可能になります。

「Cognitoが脅威を検知すると、その脅威の場所を特定し、どのように対応するのが最善かを迅速に判断できます」と同氏は述べました。

お金の動きを追う

製造業は、サイバー犯罪者にとって格好の標的です。知的財産、企業秘密、人事情報は魅力的なデータであり、さらにサプライヤーや顧客との安定した取引が行われていればその情報を悪用し大きな利益を期待できます。

「今まで見てきた攻撃は、すべて盗みを目的としたものでした」とWhelan氏は指摘します。

「顧客への請求書が1枚転送されるだけでも数万ユーロの損失になります。今まで見てきた攻撃が、すべて盗み目的なのは当然のことかもしれません」

「請求書は必ず承認されるようにし、さらに銀行口座の詳細が変更されないように管理していますが、それに加えて、第三者が別の経路でデータにアクセスし変更されないようにする必要もあります。ここでCognitoの出番です」と言います。

86億ユーロの売上を誇る企業にとって、請求書1枚の漏洩は些細なことかもしれません。しかし、ハッカーの侵入は、風評被害やサプライチェーン攻撃のリスクも高め、より複雑で長期的な影響を引き起こす可能性があります。

「Cognitoは、攻撃者が第一ステージを通過したことを識別するための方法を提供してくれます。攻撃者が本気で侵入したければ侵入することは出来てしまうかもしれません。ただし、Cognitoを使えば、被害が出る前に脅威を止めることができます」と同氏は述べています。

正常な状態を理解する

「Cognitoによって、自社のネットワーク内の振る舞いパターンの理解度が高まります。これにより、潜在的な攻撃者の振る舞いをリアルタイムで特定できるという自信がつきました」

例えば、オランダオフィスのシニアマネージャーが定期的にダブリンオフィスに来て、サーバーに接続し、それをCognitoが異常と判断したとします。そんな場合「Cognitoは通常のネットワークトラフィックを無視し、代わりに潜在的な攻撃者の振る舞いを暴くことに焦点を当てています」とWhelan氏は述べました。

Cognitoは、ディープ・パケット・インスペクションを行うのではなく、パケットからメタデータを抽出することで、リアルタイムな可視性を提供します。

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

プライバシーを侵害せず保護する

Cognitoは、ディープ・パケット・インスペクションを行うのではなく、パケットからメタデータを抽出することで、リアルタイムな可視性を提供します。これにより、ディープ・パケット・インスペクションに伴うパフォーマンス・ペナルティなしに、プライバシーを侵害せず保護することができます。

それは、Ardagh Groupではとても重要なことです。「我々は長年、データ・プライバシーの遵守を非常に厳しく守ってきました」とWhelan氏は言います。企業はEU一般データ保護規則、欧州労使協議会などその他多くの国内外のデータプライバシー法を遵守する必要があります。

「Cognitoは非侵入型です。ユーザーを追跡するのではなく、攻撃者の振る舞いを知るためにネットワークのメタデータを収集して調査します」