VECTRA
SECURITY THAT THINKS.®

ケーススタディ

ドラッグストアチェーンROSSMANNのデータ漏洩をVectra AIが阻止

ドイツ国内に2,196店舗、東欧に1,892店舗を展開するROSSMANNは、総店舗数4,088、従業員数56,200人のヨーロッパ最大級のドラッグストアチェーンです。

ドイツを代表する小売業者であるROSSMANNのITセキュリティチームは、ネットワーク内部の脅威を特定するソリューションを必要としていました。チームリーダーのDaniel Luttermann氏が率いるROSSMANNのITセキュリティチームは、ネットワークの境界でサイバー攻撃者を捕捉し、ネットワーク内部の脅威を特定するために、セキュリティ体制の強化に着手していました。

PoC（概念実証）テストでベンダーを評価する前に、ROSSMANNは潜在的なセキュリティ上の弱点や脆弱性を特定するためのレッドチーム演習を実施しました。このペネトレーションテストの結果は、PoCテストの段階でベンダーを評価するために使用されるものでした。このような検討工程を経て最終的には、Vectra® AIのCognito®ネットワークの検知および応答（NDR）プラットフォームを含む、多様なソリューションを選択しました。

「Vectra AIのThreat Certainty Index™は、自動的に検知の優先順位をつけるので、最も重要な脅威の振る舞いを簡単に確認することが可能です。我々は何百ものイベントと履歴を統合して、最大の脅威をもたらすホストデバイスをピンポイントで特定できます」

Daniel Luttermann氏
ROSSMANN、IT
セキュリティチームリーダー

ROSSMANN

組織

ROSSMANN

業種

小売業

課題

ディープ・パケット・インスペクションを行わずに、脅威の振る舞いや復号化を特定する方法が必要であった

選定基準

トラフィックのペイロードやコンテンツを詮索することなく、セキュリティ中心のメタデータを取得して脅威を特定する、ネットワークを中心とした検知および対応ソリューション

結果

- 何百ものイベントを統合し、最大の脅威となるホストデバイスをピンポイントで特定できるようになった
- すべての脅威の背後にあるコンテキストの理解が深まった
- Vectra Threat Certainty Indexによる自動スコアリングと優先順位付けが可能になった

「Cognitoプラットフォームは、かなり短時間でレッドチームの振る舞いを明らかにしました。この演習によって、実際の脅威に対しても迅速に対応でき、脅威を軽減できることが分かりました」

評価基準

GDPR（EU一般データ保護規則）のコンプライアンスと監査を担当するセキュリティアナリストのMonika Engel氏は、「脅威の振る舞いを特定するために、ディープ・パケット・インスペクションによる復号化という選択はできません」と語ります。「当社は厳格なデータ保護法を遵守しており、データトラフィックの内容を調査できるのは、特定の状況と範囲に限られています」

ROSSMANNのITセキュリティチームは、Vectra AIが行う、すべてのネットワーク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抽出し、不審もしくは脅威となる振る舞いを検知する方法に感心しました。

「Vectra AIは、データを詮索せずに保護を実現してくれます。トラフィックのペイロードやコンテンツを見るのではなく、セキュリティ中心のメタデータのみを取得して脅威を特定します。Vectra AIのソリューションはGDPRに準拠しており、社内でのPoCはもちろん、当社の労働者による評議会でも承認されました」とLuttermann氏は言います。

同氏によると、Vectra AIのソリューションはPoCテストにおいて直ちに稼動し、迅速なTime-to-Value（価値実現までの時間）を示しました。

「Vectra AIのThreat Certainty Indexは、自動的に検知の優先順位をつけるので、簡単に最も重要な脅威の振る舞いを確認することを可能にします。我々は何百ものイベントと履歴を統合して、最大の脅威をもたらすホストデバイスをピンポイントで特定できます」

Vectra AIは、サイバー攻撃者の捜索を自動化し、どこに隠れているのか、何をしているのかを明らかにします。最もリスクの高い脅威は即座に優先順位付けされ、侵害されたホストデバイスと相関し、優先されるため、ITセキュリティチームは進行中の攻撃を阻止し、データ損失を回避するために迅速に対応することができるのです。

「我々は、Vectra AIの使いやすさと自動化できる点、ノイズの少なさ、そして強力な脅威に対する信号の組み合わせが時間を節約し、すべての脅威の背景をより深く理解することができると考えました」とLuttermann氏は言います。これがVectra AIのCognito NDRプラットフォームを選択する際の大きな理由となりました。

立ち上げと稼動

Cognito NDR プラットフォームの導入後、ROSSMANNの IT セキュリティチームは、再度レッドチームによるペネトレーションテストを実施しました。

「Cognitoプラットフォームは、かなり短時間でレッドチームの振る舞いを明らかにしました。この演習によって、実際の脅威に対しても迅速に対応でき、脅威を軽減できることが分かりました」とLuttermann氏は語ります。

クラウド、データセンター、IoT、エンタープライズ環境でサイバー攻撃者を発見し、阻止することができるCognitoプラットフォームは、AIを活用してリアルタイムの脅威の可視化を実現し、脅威の詳細をすぐに把握することが可能です。

ディープラーニングやニューラルネットワークなどの高度な機械学習技術と、常に

学習される振る舞いモデルを組み合わせることで、Cognitoプラットフォームは、隠れた未知の脅威が被害をもたらしたり、データを盗まれたりする前に、迅速かつ効率的にそれを明らかにします。

活用方法

Cognitoプラットフォームは、クラウド、エンタープライズ、認証システム、Office 365などのSaaSアプリケーション、ワークロード、ユーザーやIoTデバイスなど、すべてのネットワークトラフィックからセキュリティに対してエンリッチ化したメタデータを分析することで、隠れた脅威の振る舞いをエンタープライズ全体で可視化します。

攻撃者に隠れる場所を与えないように、セキュリティに対してエンリッチ化したネットワークメタデータの分析は、すべての内部トラフィック（東西）、インターネットトラフィック（南北）、仮想インフラ、クラウド環境に適用されます。

「Cognitoのダッシュボードを見れば、直感的にアラートを確認すべきであることが分かります」とLuttermann氏は言います。「山のようなログをかき集めて、ひとつひとつ追いかけていく必要はないのです。Vectra Threat Certainty Indexによって自動化されたスコアリングと優先順位付けは、私たちの時間を大幅に節約してくれます」

手動で時間のかかるセキュリティイベントの分析を自動化することで、Cognitoプラットフォームは数ヵ月の作業を数分に凝縮し、セキュリティアナリストの作業量を大幅に削減します。これにより攻撃に包囲された状態であったITセキュリティチームは、攻撃者の先を行き、隠れた脅威に迅速に対応することができます。

「Cognitoプラットフォームが、サイバー攻撃に対して効果を発揮するのには、それほど労力を必要としません」と同氏は結論づけます。「強力で確実な脅威のシグナルが発信されるのでノイズがなく、アラートによる疲労も発生しません。重要な検知がCognito UIのダッシュボードに表示されれば、それは注目に値するものだということです」と述べています。

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

Vectra AIのソリューションが稼働したことで、ROSSMANNのITセキュリティチームは、高度な脅威を軽減するために、さらに迅速な対応を可能とするインシデント対応機能を構築しています。

「強力で確実な脅威のシグナルが発信されるのでノイズがなく、アラートによる疲労も発生しません。重要な検知がCognito UIのダッシュボードに表示されれば、それは注目に値するものなのです」