VECTRA
SECURITY THAT THINKS.®

ホワイトペーパー

人工知能（AI）によるセキュリティ運用センターの強化方法

目次

Vectra® AI社は、サイバー攻撃をいち早く検知および阻止することで、ビジネスの安全性を担保します。

ネットワークの検知と対応（NDR）におけるリーダーであるVectra® AI社は、最新のテクノロジーを駆使して皆様のデータやシステム、インフラストラクチャーを確実に保護します。Vectra AI社の提供ソリューションによって、SOCチームは、攻撃者が実際に行動を開始する前にその兆候を検知し、対応することが可能となります。

対象がオンプレミスかクラウドかに関わらず、Vectra製品は、ネットワーク上の不審な振る舞いや活動を素早く検知します。また、セキュリティ担当者が攻撃に迅速に対応できるよう、その検知・識別を行いアラートを発信します。

Vectra AI社は、「自ら思考するセキュリティソリューション（Security that thinks®）」を実現します。人工知能を駆使することによって、時間の経過と共に検知および対応能力が向上し、誤検知が排除され、実在する脅威に集中できるようになります。

90% **AIを駆使したCognito Detectの自動化機能によって、SOCチームは脅威の調査に必要な時間を最大90%短縮し、データの喪失を防ぐための対応に集中できるようになります。**

ハイライト

- ネットワーク侵害の検知は、正に時間との勝負です。重要なアセットを盗難や被害から守るためには、サイバー攻撃に関するリアルタイムでの検知が不可欠となります。
- AIを活用した最新のセキュリティソリューションでは、24時間365日稼動しながら、Tier-1アナリストの作業の多くを自動化し、脅威の検出と修正に要する時間を大幅に短縮すると共に、SOC担当者の数を減らしコストを削減することができます。
- Cognito Detectの中核を成すのは、自動化されたサイバー攻撃検知機能です。そのアプローチは、隠れた脅威を発見するためのシンプルな原則に基づいています。つまり、「最も信頼できるデータソースであるネットワークトラフィックに対してAIを適用する」ということです。
- Cognito Detectは、行動検知アルゴリズムを使ってパケットから取り込んだメタデータを分析し、トラフィックが暗号化されているかどうかに関わらず、隠れた攻撃あるいは未知の攻撃をリアルタイムに検知します。
- 攻撃をリアルタイムに可視化し、その振る舞いを常時学習し続けるモデルを使って、無停止で脅威を自動ハンティングするCognito Detectによって、SOCはサイバー犯罪者が滞留する時間を短縮し、対応時間を迅速化することができます。

増加し続けるサイバー攻撃に対応するため、セキュリティ運用センター（SOC）を設置する企業が増えています。

この背景には、リスクや脅威、攻撃者の数が増加しているだけでなく、その手口がますます高度化し、ビジネスに与える影響が大きくなっているという実情があります。特に危険なのが標的型攻撃で、この検知には多くの時間を要します。

SOCを設置することによってセキュリティ対応を最適化できるだけでなく、インシデントの検知と対応能力が大きく向上します。人、ポリシー、テクノロジーこそが、SOCを機能させる基盤であることは広く認知されています。しかし多くの企業が、効果的かつ費用対効果に優れたSOCの構築に苦慮しています。

Cognitoは、時間の浪費につながる手作業によるセキュリティイベントのTier-1分析を、AIを活用して自動化することで、数週間あるいは数ヶ月を要する作業を数分にまで短縮します。これにより、脅威の調査に必要な時間は最大90%短縮され、SOCチームはデータの喪失を防止するための対応に集中できるようになります。

本ホワイトペーパーでは、企業による脅威への対応を阻害する要因や、人工知能（AI）に基づくセキュリティソリューションが、現代のSOCにとっていかに重要であるかという点について解説します。AIを活用したソリューションによって、SOCチームは、より効率的な運用が可能になるだけでなく、重要なアセットが盗難にあったり損害を受ける前に、攻撃の兆候を早期にリアルタイムで検知できるようになります。

Vectra AI社が提供するCognito Detect™の基盤となる、AIを駆使したサイバー攻撃の検知および脅威ハンティングのプラットフォームであるCognito®は、人間の技能や高度な調査結果をデータサイエンスや最新の機械学習テクノロジーと組み合わせることで、企業全体に関わる脅威を24時間365日にわたって自動的に検知し、トリアージや関連付けを行います。

Cognitoによってデータの収集、脅威の検知、分析と対応を自動化することで、検知に必要な時間とコストを削減できます。これによりSOCチームは、攻撃を迅速に阻止するための実践的な情報を得ることができます。

Cognitoは、時間の浪費につながる手作業によるセキュリティイベントのTier-1分析を、AIを活用して自動化することで、数週間あるいは数ヶ月を要する作業を数分にまで短縮します。これにより、脅威の調査に必要な時間は最大90%短縮され、SOCチームはデータの喪失を防止するための対応に集中できるようになります。

SOC構築の阻害要因

企業がSOCを構築する際には、幾つかの課題に直面します。以下のセクションでは、これらの主要な課題について詳しく説明します。

人材不足

SOCの構築には、高度なスキルを備えた「サイバー兵士（cyberwarrior）」が不可欠となります。しかし残念なことに、熟練したサイバーセキュリティやデータサイエンスの専門家に対する求人が過多の状況下で、適切な人材を雇用して維持していくことは非常に困難です。例えば米国では、年間で約4万名のサイバーセキュリティ担当者が不足していると推定されています。

SOCは、一般的に3層のアナリストで構成されるマルチレベルの人員構成となっており、それぞれの層に特化した専門知識が必要となります。

Tier-1のアナリストは、24時間365日セキュリティアラートの監視とトリアージにあたります。分析対象となるデータは膨大な数におよぶため、最も人数を要するのがTier-1のアナリストです。多くの企業では、最低でも2～3名の人員を配備しており、場合によっては6名以上であることも珍しくありません。

Tier-1アナリストでは脅威の修正ができない場合、Tier-2のアナリストにエスカレーションします。Tier-2のアナリストでも脅威を修正できない場合は、最上位のTier-3のアナリストに対してエスカレーションが行われます。

Tier-1アナリストとは異なり、Tier-2およびTier-3のアナリストの場合には、24時間365日の対応は不要です。脅威のインシデントの重大度や求められる対応期限に応じて、必要な場合に対処を行います。

重大度については、すぐ対応が必要な重要なものから、数時間あるいは数日以内に対応すれば十分なリスクの低いものまで、様々な内容があります。Tier-3のアナリストについては、最も費用がかかるため、最も困難でリスクの高い脅威インシデントにのみ対応できるようにすることが重要となります。

企業のプロセスやリソースに応じて、専任の対応チームによってSOCを構成したり、重大なインシデントに対して様々なリソースを活用する場合もあります。このような対応にあたって、必要な担当を緊急招集したり、外部のインシデント調査担当者や、状況に応じて専門家を雇い入れる場合もあります。

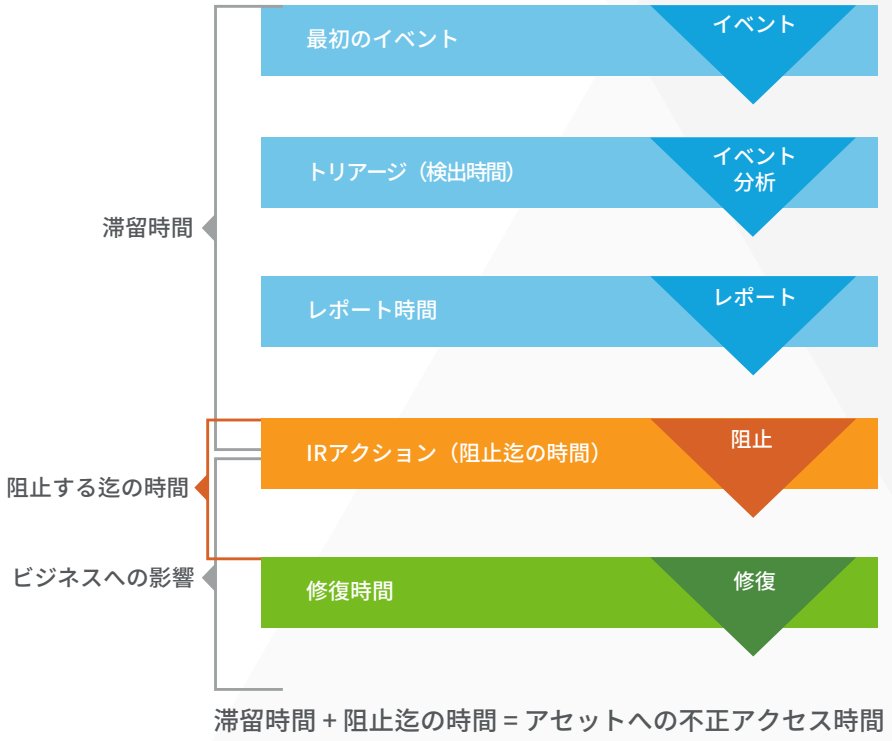
大規模なデータ侵害や複雑な脅威インシデントを解決するために、独立したフォレンジック調査担当者を雇い入れる場合、インシデント1件に対して、100万ドル以上の費用が必要になることも少なくありません。

手作業による対応

高度な不正行為者は、境界に配置されたシグニチャベースのセキュリティツールやサンドボックスなどのセキュリティをすり抜ける技術に長けています。一旦攻撃者が境界線のコントロールをすり抜けてしまうと、手作業による長時間を浪費する対応が必要になります。

調査にあたっては、マルウェア分析、パケットとログ分析のフォレンジックといった幅広い専門的なスキルセットが必要となり、さらに様々なソースから大量のデータを収集する必要があります。セキュリティイベントの調査には何時間も必要となり、高度な脅威の完全な分析には、数日、数週間、あるいは数か月必要となる場合さえあります。

ネットワーク侵害の検知は、正に時間との勝負です。重要なアセットを盗難や被害から守るためには、サイバー攻撃に関するリアルタイムでの検知が不可欠となります。



AIは、膨大なトラフィックが発生する現代のネットワークの監視や分析においてキーとなる技術です。AIを適切に活用したセキュリティソリューションによって、24時間365日稼動を継続しながら、Tier-1のアナリストの作業の多くを自動化し、脅威の検出と修正にかかる時間を大幅に短縮すると共に、SOC担当者の数を減らし、コストを削減することができます。

専門家向けセキュリティテクノロジー

従来、セキュリティ製品の利用にあたっては、実践的なサイバーセキュリティインテリジェンスの抽出に熟練した、高度なスキルを備えたプロフェッショナルが膨大な時間を費やす必要がありました。

企業には、ネットワークやユーザー、アプリケーションの不審な振る舞いを継続的に監視し、セキュリティ分析のための重要なデータを自動的に集約できる、新しい手段やツールが必要なのです。

また、ネットワークフロー分析、システムログ、エンドポイント・エンフォースメント・ポイント、アイデンティティおよびアセットコンテキスト、脅威インテリジェンス、セキュリティイベントなど、様々なソースから重要なデータを集約できる必要もあります。

AIは、膨大なトラフィックが発生する現代のネットワークの監視や分析においてキーとなる技術です。AIを適切に活用したセキュリティソリューションによって、24時間365日稼動を継続しながら、Tier-1のアナリストの作業の多くを自動化し、脅威の検出と修正にかかる時間を大幅に短縮すると共に、SOC担当者の数を減らし、コストを削減することができます。

SOCの効率性を測る

SOCのパフォーマンスを測る上では、その成熟度と効果の2つが最も重要な指標となります。

成熟度は、リスクや脅威の認知や再現性、順応性など、企業のサイバーセキュリティリスクの管理手法に対する進展度合を反映したものです。

米国国立標準技術研究所（NIST）は、SOCにおけるセキュリティ実装の成熟度をその階層によって評価しています。最下層に属するのは、あくまで部分的なセキュリティ実装に留まっている場合で、非公式に事後的な対応を必要としている点が特徴となります。逆に最上層に属するのは、俊敏かつリスク情報を活用したサイバー攻撃の状況に最適な実装を行っている場合です。

また効果については、次のようなセキュリティ運用や脅威ハンティングに関する現実的な指標を使って評価を行います：

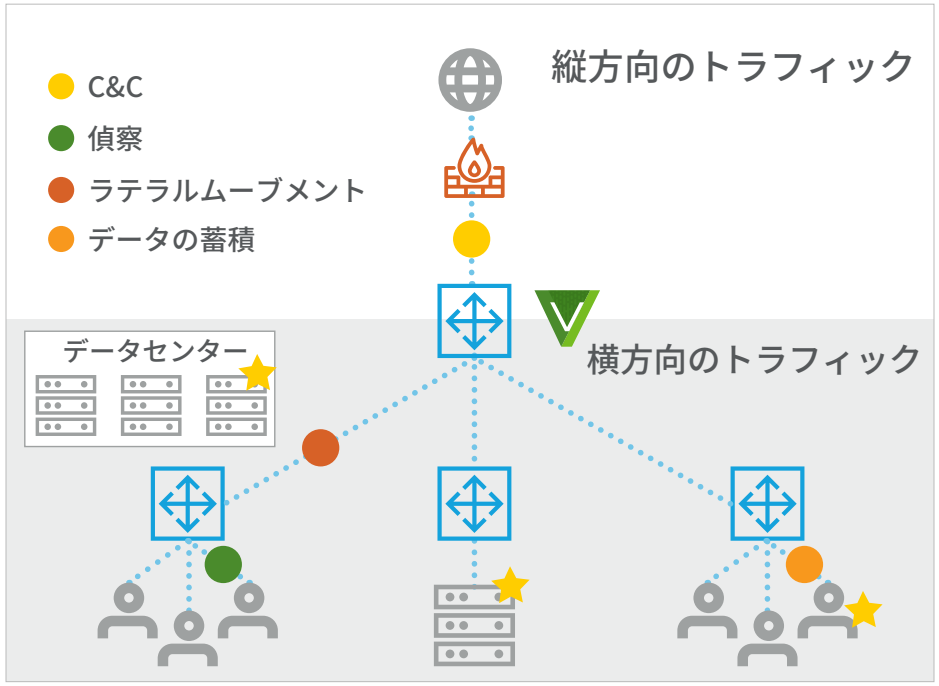
1. **攻撃者の滞留時間** ― 最も重要な指標である滞留時間は、攻撃者が侵害を行った時点から検知、阻止に至るまで、ネットワーク内に存在した時間を示すものです。これは、実際の攻撃対象の広がりや防御が攻撃者の速度低下に与えた効果、脅威の可視性、さらに企業の対応能力に対するインサイトを提供するものです。
2. **ネットワークの可視性** ― 見えないものを検知することはできません。SOCチームは、管理対象ホスト、管理対象外ホスト、パーソナルデバイス、IoTデバイス、仮想サーバー、クラウドリソース、インターネットの境界や内部のトラフィックを可視化できる必要があります。
3. **ラテラルムーブメント** ― ラテラルムーブメントは、攻撃者がいかに容易にかつ自由にネットワーク内を移動し、どれだけの数のシステムが侵害を受けているのかを示すものです。
4. **対応時間** ― SOCがセキュリティイベントに対応するまでに要した時間です。対応時間には、脅威やインシデントの検知、トリアージ、レポート、阻止までに要した全ての時間が含まれます。
5. **再侵害率** ― 企業が以前と同じ敵や脅威に狙われた、あるいは侵害受けた回数を示します。

データサイエンス：Cognitoを支えるブレイン

サイバーセキュリティの専門家の不足、手作業による遅々とした対応、複雑なセキュリティツールなどは、インシデント対応の妨げとなります。Cognito Detectは、脅威の検知、レポート、トリアージを行うための人間の専門知識と、幅広いデータサイエンスや機械学習テクノロジーを組み合わせ、Tier-1アナリストが必要とする主要な機能を提供します。

Cognito Detectの中核を成すのは、自動化されたサイバー攻撃検知機能です。Vectra AI社のアプローチは、隠れた脅威を発見するためのシンプルな原則に基づいています。つまり、「最も信頼できるデータソースであるネットワークトラフィックに対してAIを適用する」ということです。

Cognito Detectは、全てのネットワークトラフィックに対して、詳細で継続的な分析を行うことによって、攻撃者が企業の重要なアセットを盗み出すために、ネットワーク全体でスパイ行為を行い拡散していく、基本的な活動や振る舞いを検知します。



ネットワーク全体を対象に可視化するCognito Detectは、全てのネットワークトラフィックを24時間365日監視し、分析しています。この中には、内部（横方向）のネットワークトラフィックとインターネットバウンド（縦方向）のトラフィック、さらに1つのIPアドレスを使った物理と仮想ホストの間の内部トラフィックも含まれます。

このような広範な可視化は、ラップトップやサーバー、プリンター、BYOD、IoTといった全てのデバイスやオペレーティングシステム、アプリケーション、さらにはデータセンターとクラウドの仮想ワークロード、パブリッククラウド間のトラフィックにまで及びます。

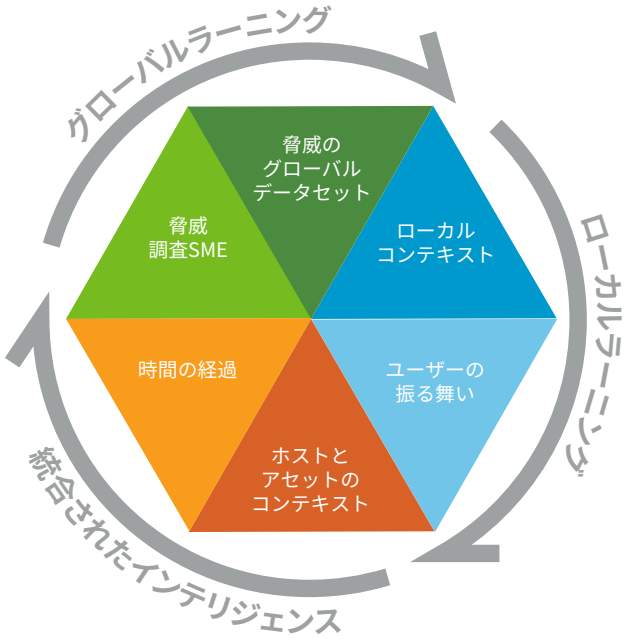
またCognito Detectは、権限を持つ従業員による重要なアセットへの不審なアクセスの監視と検知、さらにクラウドストレージやUSBストレージの使用、その他の手段を使ったネットワーク外へのデータの移動といったポリシー違反の監視と検知も実施します。

インテリジェンスなテクニックを組み合わせ活用するCognito Detectは、次のような攻撃ライフサイクルの全ての局面で、脅威を自動的に検知します。

- コマンドアンドコントロールや隠れた通信
- 内部偵察
- ラテラルムーブメント
- アカウント認証情報の不正使用
- データ流出
- ランサムウェア攻撃の初期段階での兆候
- ボットネットによる収益化
- 全てのホストのマッピングや関連する攻撃指標などの攻撃キャンペーン

Cognito Detectは、行動検知アルゴリズムを使ってパケットから取り込んだメタデータを分析し、トラフィックが暗号化されているかどうかに関わらず、隠れた攻撃あるいは未知の攻撃をリアルタイムに検知します。ユーザーのプライバシー保護のため、機密のペイロードを詮索することなく、取得したパケットのメタデータだけを抽出して分析します。

それでは、ここからはCognito　Detectを支えるテクノロジーの視点から、どのように担当者不足の問題を解消し、SOCのプロセスを合理化できるかという点について説明します。



グローバルラーニング

グローバルラーニングでは、脅威に共通する基本的な特徴を特定します。グローバルラーニングについては、マルウェア、攻撃ツール、テクニック、手順を継続的に分析し、脅威の検知や新たな傾向の把握などを担当するサイバーセキュリティや脅威の調査に特化したVectra Threat Labs™ のグループが実施します。

この結果は、教師ありの機械学習など、Cognito Detectが使用するデータサイエンスモデルに反映されます。これを使って大規模な攻撃トラフィックを分析し、不正なトラフィックを特徴づける重要な特性を抽出します。

例えば、教師ありの機械学習モデルは、リモートアクセスツール（RAT）独自の振る舞いを検出し、こうしたツールのトラフィックと正常なトラフィックの違いを学習することができます。このようなインテリジェンスによってCognito Detectは、新たにカスタマイズされた未知のRATをリアルタイムかつシグニチャ不要で、高い精度をもって検知することができます。

ローカルラーニング

ローカルラーニングは、ローカルネットワーク内で正常な対象と正常でない対象を区別することで、攻撃パターンを明らかにします。ここで使用される主要なテクノロジーは、教師なしの機械学習とアノマリー（異常値）検知機能です。

Cognito Detectは、教師なしの機械学習モデルを使って特定のお客様の環境を、データサイエンティストの直接的な監督なしに学習します。例えば、Cognito Detectはローカルラーニングを使って、ユーザーの振る舞いが過去と異なることを検知することができます。

Cognito Detectは、異常値の発見やレポートに集中するのではなく、攻撃者がネットワークの内部を偵察したり、攻撃対象とするホストを見定めたり、盗み出した認証情報を使用するなど、攻撃の重要な局面や攻撃テクニックの証跡を調査します。

こうした振る舞いを検知するためには、長期的に使用されるIPアドレスなど、ローカルネットワーク環境に対する長期的な記録が必要となります。同様に、データの段階的なステージングを観察することも可能ですが、コンテキストを構築し、同じ量のデータが様々なタイミングで準備され抽出されていることを認識するためには、メモリとインテリジェンスが必要になります。

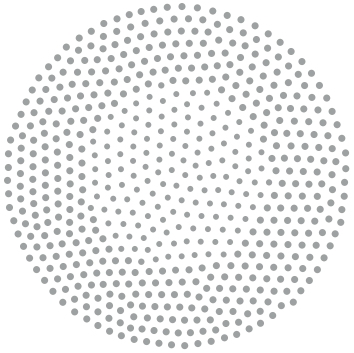
Cognito Detectは、強力なセキュリティメカニズムを提供する教師なしの学習や関連するテクニックによって、侵害を受けたホストからの有効な認証情報の盗み出しといった不審な活動を、リアルタイムかつピンポイントで検出することができます。

統合されたインテリジェンス

今日のサイバー攻撃は複雑であり、侵入者は時間と共に進化する多段階の攻撃を仕掛け、多様なテクニックや戦略を駆使しながら、ネットワークの奥深くまで入り込んで行きます。

このため、部分的なイベントだけでなく、攻撃全体の把握に必要となる全ての情報を取り込み、攻撃に関する長期的な進行状況をトラッキングできることが、脅威の検知モデルにとって非常に重要となります。

検出：数百～数千におよぶイベントと
ネットワーク特性を1つのCognito Detect に集約



レポート：アナリストは、次のステップの決定と推奨を
行うための十分な情報を必要とする

トリアージ：攻撃の中心にある物理ホストを
特定するために自動的に検出機能が紐付けられる

SOC

- SIEM
- インシデントレスポンス

Cognito Detectは実行およびインシデント
対応プラットフォームと連携

- ファイアウォール
- エンドポイント
- NAC

Cognito Detectは、数千のイベントやネットワークの痕跡を1つの検知結果として集約します。Cognito Detectは、イベントの関連付けやホストのスコアリングといったテクニックを駆使して、以下を実施します。

- 全ての検知イベントは、脅威の振る舞いの兆候を示す特定のホストに紐付けられます。
- Cognito Threat Certainty Index™ を使って把握した脅威の重大度や信頼度をベースに、全ての検知結果やホストを自動的にスコアリングします。
- イベントとサイバー攻撃のキルチェーン全てのフェーズを長期でトラッキングします。

Cognito Detectは、特にネットワーク内の重要なアセットを危険にさらす可能性のあるイベントや、攻撃者にとって戦略上価値のあるイベントに重点を置いています。サイバー攻撃のキルチェーンの複数のフェーズにまたがる振る舞いを示すデバイスも、優先順位が高くなります。

結果的に、お客様は高い信頼度を持つ重大なリスクを含んだ攻撃の振る舞いや、ネットワーク内のホストに対するインサイトを取得することが可能となります。

Cognito Detectのアプローチによるメリット

人間が持つ専門知識と幅広いAIテクニックを組み合わせたCognito Detectは、時間を浪費する手作業によるTier-1のセキュリティイベント分析を自動化することで、お客様に多くのメリットを提供します。

Tier-1での分析自動化によるSOCチームの強化

Cognito Detectでは、高度なトレーニングを受けたアナリストやデータサイエンティストが、通常、手作業で何時間もかけて実施するセキュリティ調査を自動化することができます。Tier-1アナリストが通常実施する検知、レポーティング、トリアージ機能を完全に自動化し、SOCチーム全てのメンバーの効率や生産性を向上させることができます。

例えば、Cognito Detectは、高いリスクを示す侵害に受けたホストの優先順位付けの結果や、ホストの脅威や信頼度に関わるスコアの変化、攻撃を受けた証跡のある重要なアセットなど、検知に関する情報をシンプルなダッシュボードを使って表示します。Cognitoの脅威と信頼度スコアに応じて、SOCのメンバーに通知を送ることができます。

この1ページの概要通知には、検知に至ったイベントやコンテキストの履歴、考えられるトリガー、根本原因、業務への影響、確認手順など、検知した攻撃内容の説明が記載されています。

SOCチームは、時間の経過による脅威の進行を確認の上、攻撃の重大度や優先順位の決定に貴重な時間を浪費することなく、直ちに修正対応に着手することができます。

またCognito Detectは、当事者間でやり取りされるデータが、通常の方法に違反する、あるいは一致しない方法で転送されると、SOC担当者に警告を発し、データを送信しているホスト、場所、量、データの送信に使用しているテクニックに関するインサイトを提供します。

さらにSOCチームは、同じマルウェアの攻撃を受けているホストや、悪意あるサイトに繰り返し接続しているホストを表示するダッシュボードビューを作成することで、再侵害率を容易にトラッキングできるようになります。

多くの情報を持つCognito Detectは、ネットワーク上の何が正常で、攻撃がどのように拡散して進行するのかをSOCのチームメンバーに教育する上での、必要不可欠なトレーニングツールとなります。

トリガー

- 内部のホストが、HTTPSを使って外部のIPと通信を行っているが、HTTPSセッション上では別のプロトコルが稼動している場合
- 通常の暗号化Webトラフィックを模倣し、長期間にわたり複数のセッションを取り込んでいる非表示のトンネルの存在
- トンネル経由で送られるデータ量によって、脅威スコアが上昇している場合
- セッション数とその永続性によって、信頼度スコアが上昇している場合

多くのお客様にとって、Cognito Detectの自動化機能とその使いやすさは、学生インターンなどのセキュリティジェネラリストを採用したり、経験豊富なセキュリティアナリストを昇進させ、より高度なセキュリティポジションに着かせるための後押しをするものとなります。

例えば、ある医療機関のCISOは、「私達のインターンは、Cognito Detectを使って素晴らしい仕事をしてくれました」と述べています。これにより、残りのSOCチームのワークロードを75%も削減することができたからです。

Texas A&M University Systemは、Cognito Detectを導入したことで、インターンが価値の高い研究や調査に関するデータの保護を実施できるようになりました。サイバーセキュリティに対するキャリアの構築に興味を持つ学生インターンは、SOC内でのTier 1アナリストとしてCognito Detectを使用するよう訓練されています。

「Cognito Detectは直観的で容易に使用できるため、インターンは検知した脅威に自分で対応すべきか、あるいはTire-2のアナリストにさらなる調査を依頼すべきなのかを、数分のうちに判断することができます。このため、高度なスキルを持つTier-1のアナリストを、Tier-2のアナリストに昇格させることができました。これこそがCognitoの真に優れた点なのです」と、Texas A&MのSOC担当エグゼクティブディレクターのDaniel Basile氏は話します。

脅威の検知に留まらない迅速な封じ込めの実現

攻撃をリアルタイムに可視化し、振る舞いを常時学習し続けるモデルを使って、増え続ける脅威を自動的にハンティングするCognito Detectによって、SOCはサイバー犯罪者が滞留する時間を短縮し、対応時間を早めることができます。これによりSOCチームは、NISTの最高レベルの実装成熟度を達成することができます。

Cognito Detectによって脅威の調査に要する時間を劇的に短縮できることで、セキュリティチームはデータの喪失を防止するための対応に集中できるようになります。調査に必要な時間を90%も削減できたお客様もいます。例えば、Texas A&MのSOCチームは、脅威の調査に必要な時間を、数日から数分にまで短縮しました。

さらにCognito Detectは、他の方法では検知できないセキュリティイベントも検知することができます。これによって、正味のイベント数を増やし、より正確でタイムリーなインシデント対応が可能となります。

Texas A&Mは、Cognito Detectを1年間使用した結果、ネットワークの内部で活動する7つの脅威を発見しました。Cognito Detectは、SOCチームが脅威を阻止し、重要なアセットを保護するために必要となる全ての情報を提供します。

確証性の高いインシデント調査

セキュリティアナリストは、Cognitoプラットフォームの重要なコンポートネントの1つであるCognito Recall™ を使って、極めて効率的に、AIが支援する脅威ハンティングや、より詳細な拡張性に優れたインシデント調査を実施することができます。

セキュリティアナリストは、Cognito Recallを使って、Cognito Detectやサードパーティーのセキュリティ製品が検知した一連の関連するイベントや、過去のネットワークメタデータにある検索可能な高品質の脅威インテリジェンスを、容易に過去に遡って活用することができます。

Cognito Detectから脅威の通知を受け取ったCognito Recallは、セキュリティアナリストが全てのワークロードやデバイスのアクティビティを全方位ビューで確認できるようにします。セキュリティアナリストは、Cognito DetectとCognito Recallをワンクリックで切り替えながら、悪意あるネットワーク通信に関する詳細で有益なコンテキストを取得することができます。

Cognito Detectが、特定の攻撃行動や攻撃によって侵害を受けたホストに関する詳細な情報を提供すると共に、セキュリティアナリストはCognito Recallによって、攻撃があった期間と同時に発生したネットワーク通信に関する過去の豊富なメタデータを検索することができます。

コスト削減

攻撃を受けた後、しばしば高額なインシデント対応やフォレンジック分析サービスが必要になる場合があります。Cognito Detectによって、全てをサードパーティーの調査に任せることによるコストの発生を抑えると同時に、手作業によるログ分析への依存度を下げることができます。

Texas A&Mは、Cognito Detectによってコストを大幅に削減することができました。Basile氏は、次のように述べています。「(Cognito Detectによって) セキュリティ運用チームは、攻撃者を迅速かつ容易に発見できるようになり、通常攻撃が終わってから1ヶ月以内に開始される高額なフォレンジック分析を行う必要もなくなりました」

「以前は、侵害後のフォレンジック分析を実施する度に、約100万ドルもかけてコンサルタントを招へいしなければなりませんでした。Vectraによってこの対応が不要となったことで、Texas A&Mは年間700万ドル節約することができたのです」

さらなる効率性の向上

Cognito Detectは、様々な通信や自動化対応のメカニズムを提供することで、状況認識能力や情報共有の促進、インシデント対応活動のサポートを向上し、SOCプロセスの効率をさらに高めることができます。例えば：

- Eメールやsyslog、他のツールをREST APIで連携させることで、リアルタイムにアラートを発信することができます。
- セキュリティ情報イベント管理 (SIEM) システムやフォレンジックツールを使って、既に関連付けが終わった状態で調査を開始することができます。
- SOCチームは、高度にカスタマイズ可能なCognito Detectレポーティングエンジンを使って、オンデマンドあるいはスケジュールベースで、容易に情報を共有することができます。
- 動的な応答ルールを設定し、他のセキュリティ・エンフォースメント・ソリューションからの応答に自動的に対応することができます。
  - Cognito Detectは、Cisco Identity Services Engine (ISE) および Forescoutと連携し、ホストを直ちに分離または隔離することができます。
  - Cognito Detectは、Carbon Blackと連携し、脅威を検知した場合にホストデバイスを迅速に分離または隔離して、不審なプロセスを停止させることができます。
  - Cognito Detectは、Palo Alto Networks、CiscoおよびJuniper Networkの次世代ファイアウォールと連携し、侵害を受けたホストデバイスをブロックすることができます。
  - Cognito Detectは、DemistoおよびPhantomのセキュリティオーケストレーションプラットフォームと連携し、容易なエンフォースメントを実現します。
  - Cognito Detectは、Splunk、Microsoft Focus、ArcSightおよびIBM QRadarと連携し、セキュリティ運用ワークフローを自動化することができます。

「Cognitoを導入以来、専門家がいなくても、サイバー攻撃に備えてTexas A&Mのネットワークインフラストラクチャー全体を監視し、驚くべき効率でセキュリティ運用センターを稼動できるようになりました」とBasile氏は述べています。

SOCにAIを適用

今後もサイバー攻撃との戦いが続く、あらゆる規模の企業において、SOCの強化を実現するためには、AIベースのソリューションが不可欠となります。Cognitoの背景となるデータサイエンスは、かつてない革新的な検知手法を取っています。

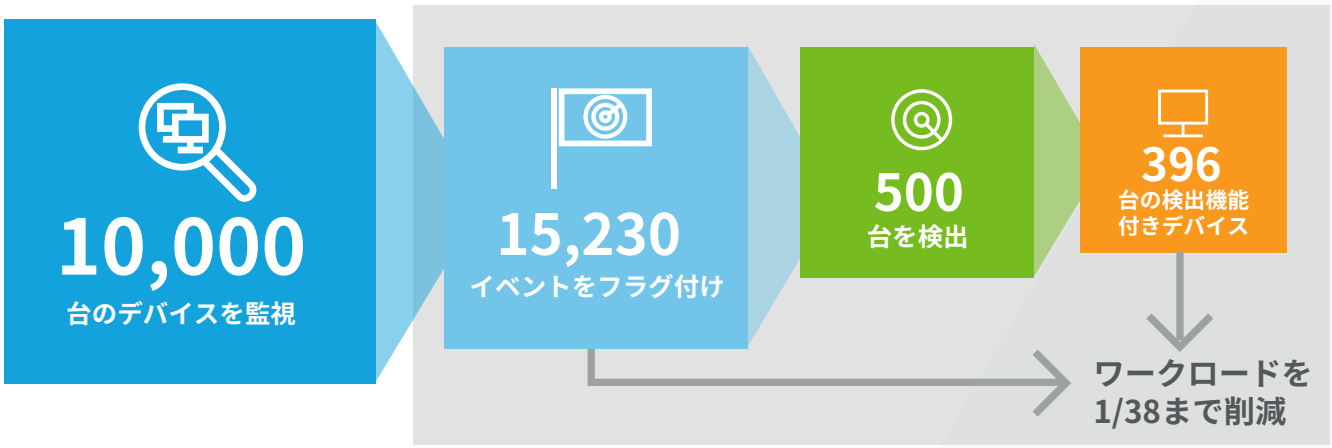
脅威の検知、トリアージ、インシデントレポーティングに、継続的な無停止のネットワークトラフィック監視機能とAIを活用したCognito Detectでは、リモートサイトやキャンパス、データセンターからクラウドに至るまで、あらゆる場所の脅威を自動的に検知し、阻止することができます。

さらにお客様は、サイバーセキュリティの専門家を追加雇用する必要なく、より迅速にセキュリティインシデントを管理することができます。これによって既存のTier-1のセキュリティアナリストは、データの喪失を防止するための対応に集中できるようになります。

Vectra AI社は、絶えずCognitoプラットフォームの改善に努めています。Vectra Threat Labsとメタデータを共有頂いているボランティア企業様のおかげで、継続的なフィードバックループが完成し、攻撃者検知のアルゴリズムの迅速な向上が可能となっているだけでなく、お客様のローカル環境にある既存のアルゴリズムを自在にチューニングすることもできます。

AIによってサポートされるCognito Detectは、手作業による脅威ハンティングに比べて、SOCの負荷を1/38にまで軽減することができます。

隠れた攻撃者の検知を自動化し、セキュリティアナリストの迅速な対応と攻撃の阻止をサポートするCognito　Detectによって、企業は効果的なセキュリティ運用センター（SOC）を手軽に構築することが可能となります。



お問合せ：

製品、ソリューションなどに関するお問い合わせは、Eメール：info-japan@vectra.ai までお願いします。