VECTRA
SECURITY THAT THINKS.®

ホワイトペーパー

サイバーセキュリティに関わるROIと運用効率の改善方法

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。

75-90% **Vectra AI社のお客様からは、調査に要する時間が75%から90%削減され、また単価の高い専門家にインシデント対応を引き継ぐことなく、ITのジェネラリストだけで対応できるようになったという声が数多く寄せられています。**

ハイライト

- SANS Instituteは、インシデント対応チームの業務を阻害する2つの要因として、効果的な改善を行うために必要となる人的リソースの不足とスキルの欠如を挙げています。
- Cognito NDRプラットフォームでは、通常、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手作業で何時間もかけて実施するセキュリティ調査を、独自の手法で自動化することができます。
- 最高レベルの信頼性を備えたCognito NDRプラットフォームは、通常であれば見逃されてしまうセキュリティイベントも確実に検知します。これにより対象となる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。
- セキュリティチームは、Cognito NDRプラットフォームを使用し、攻撃を受けている特定のホストの関連付けとスコアリングを行い、わずか数分で分析を実施することができます。これにより、数日や数週間といった長い時間をかけて、調査やログのレビュー、さらにSIEMベースの分析を行う必要がなくなります。
- Cognito NDRプラットフォームを使って脅威ハンティングを自動化することで、全てのトラフィックを対象に調査を実施し、手作業で調査や関連付けを行う時間を削減すると共に、全ての担当者が活動中の脅威を迅速に修正できるようになります。

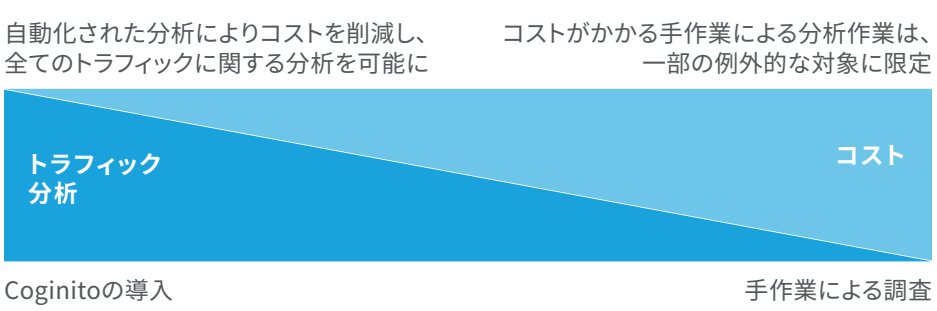
はじめに

ITに関わるセキュリティ対策にあたっては、運用効率の確保に向けた持続的な取り組みが必要になります。リスク、脅威、そして攻撃者は、無限に存在しますが、企業側のリソースには限界があります。このように相反する状況が存在する中、セキュリティ製品を評価する場合には、セキュリティ対応の効率や現状のIT運用に対する影響を十分に考慮する必要があります。セキュリティ製品の導入が、マンパワーやリソースの浪費に繋がっていませんか？また、クラウドやデータセンター、IT、IoTネットワーク全体で生産性を向上させ、迅速な対応を実現するものになっていますか？

現在の高度化するサイバー攻撃への対応にあたっては、効率性が特に重要となることは言うまでもありません。標的型攻撃が企業のビジネスに与える影響は、不特定多数を標的にした攻撃よりも遙かに深刻で、その検知と対応にあたっては、多くの時間とスキルが必要となります。

これまでのシグネチャベースのセキュリティソリューションは、数千の攻撃を自動的に排除する能力を備えていました。しかし、より高度な攻撃はシグネチャや予防的コントロールを簡単に擦り抜けるまでに進化し、その勢力を拡大しつつあります。内部的な脅威に加え、これが新しいセキュリティ手法を必要とする状況を生み出し、高度なセキュリティスキルを備えた担当者の需要と評価が急速に高まる要因となっているのです。

これらの課題に企業が向き合うためには、高度化する攻撃に対する検知と対応を自動化すると共に、セキュリティチームの効率性や生産性を最大限に高める必要があります。Vectra® AI社が提供するCognito® Network Detection and Response (NDR) は、これらいずれの要求についても対応が可能です。本ドキュメントでは、担当者や時間、リソースに限りのあるセキュリティチームを、Cognito NDRプラットフォームがどのようにサポートするかについて説明します。



重点を置く領域

現在、クラウドやデータセンター、IT、IoTネットワークにおける脅威の検知は、手作業によるコストのかかるプロセスに依存しています。Cognito NDRプラットフォームは、これらのプロセスを自動化し、コストを低減できるよう設計されています。Cognitoの価値は、次の3つの点から説明することができます。

スキル 現在のセキュリティチームが抱える最大の課題の1つとして、優れたセキュリティ担当者およびデータサイエンティストの雇用と維持があります。このような分野に関する優れた才能や経験を持つ人材は稀ですが、クラウドやデータセンター、IT、IoTネットワークへの侵入に成功した攻撃者の、初期段階の兆候を把握するためには、不可欠な存在となります。

時間 サイバー攻撃の検知は、時間との勝負です。重要なアセットが盗難にあったり被害を受ける前に、攻撃をほぼリアルタイムに検知しなければなりません。しかし残念なことに、このような攻撃の検知には、どうしても長い時間を要します。攻撃を見極めるためには、様々なスキルと調査に関する深いノウハウが必要になります。

コスト サイバー攻撃への対応には、時間と担当者のコストを超える直接的なコストが発生します。攻撃を受けた後、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ことは決して珍しくありません。Cognitoによって、インシデント対応やサードパーティーに依頼する調査コストを抑制し、手作業によるログ分析への依存度を低減することができます。

分析対象に関する注意事項

本ドキュメントでご説明する内容は、Cognitoが企業のセキュリティチームに対してもたらす節減効果に限定しています。ネットワークデータの侵害が財務に与える全般的な影響を推計するものではありません。したがって、罰金を受ける可能性や影響を受けた顧客の信用に関わる損失、法的費用、ブランド価値の低下、その他の一切の損失に関する費用を考慮に入れたものではありません。

これらのコストは極めて現実的なものですが、企業ごとに異なる状況、保有するデータのタイプ、データ侵害のハードとソフトのコストの多様性により、侵害によって発生する実際のコストを見積ることは決して容易ではありません。

コスト削減の企業が向き合うためには、高度化する攻撃に対する検知と対応を自動化すると共に、セキュリティチームの効率や生産性を最大限に高める必要があります。

例えば、最新の調査結果によれば、侵害に遭ったデータレコードあたりのコストは、企業独自の要因や見積り方法によって、50円から2万円以上まで大きな開きがあります。このため本ドキュメントでは、Cognito NDRプラットフォームの全ての経済的なメリットを特定するのではなく、セキュリティチームとITチームのコスト削減に焦点を絞っています。

最重要課題であるスキル不足にVectra製品が対応

セキュリティ技術の進化に伴い、企業はより高度かつ特別なスキルを持った人材を求めるようになっています。上位にランクされるのは、セキュリティとデータサイエンスに関するスキルですが、このようなスキルを持った人材は、どこにでもいるわけではなく、そのコストも高額になります。Cognito NDRプラットフォームでは、大規模で単調な作業を自動化することで、専任のスペシャリストの必要性を低減し、既存のセキュリティチームに在籍する全ての担当者の効率や生産性を高め、より高度な作業に集中できるようにします。

現在のスキルギャップ

ここ数年、不足するスキルとして最も多く聞かれるようになったのが、情報セキュリティに関するスキルです。SANS Instituteは、インシデント対応チームの業務を阻害する2つの要因として、効果的な改善を行うために必要な人的リソースの不足とスキルの欠如を挙げています。従来からのセキュリティ対応に向けた役割に加え、データサイエンティストもまた、セキュリティチームのメンバーとして引く手あまたな状態です。SIEMからより多くの価値を引き出したり、内部の脅威を検出するカスタマイズされた振る舞いモデルの構築まで、データサイエンスへの依存度が高まっていることが、このような状況が発生する要因の1つになっています。

IDGの「State of the CIO」によれば、不足する人材の上位を占めるのは、データサイエンティストとセキュリティ担当者になっています。

当然のことながら、このような貴重なスキルを持つサイバーセキュリティのアナリストやデータサイエンティストの報酬は、IT分野での最も高額なコストの1つになっています。Glassdoorの最近の報告によれば、データサイエンティストの平均年俸は、熟練プログラマーが約650万円であるのに対し、約900万円となっています。

最上位のデータサイエンティストの場合であれば、さらに高額な報酬が必要になります。人材紹介会社であるBurtch Worksの分析によれば、一般社員としてのトップクラスのデータサイエンティストの平均年俸は約1,500万円です。

もちろん、従業員にかかるコストは報酬だけではないため、実際にはもっと多くのコストが必要になります。いずれにせよ、この給与の比較はセキュリティとデータサイエンスの能力に対するプレミアム度を示すものとなっています。

Vectra製品がもたらす価値：自動化によってスキルギャップを埋める

人工知能 (AI) とデータサイエンスを使った脅威検知の自動化によって、Cognito NDRプラットフォームは、手作業の調査では発見することができなかった脅威の検知を実現し、セキュリティチームの作業時間やリソースに関する負荷軽減を図ることができます。

Cognito NDRプラットフォームが利用するインテリジェンスは、高度なサイバーセキュリティテクニックや検知戦略に特化した我々のセキュリティ調査とデータサイエンスの専任チームが提供します。

Vectra AI社のリサーチャーは、何百万ものマルウェアサンプルや攻撃ツール、回避テクニックの分析に加え、世界中のお客様から提供されるメタデータを監視して、最新の傾向や攻撃テクニックを特定しています。オプトインされたデータによるグローバルなスコープによって、単にデータを分析するだけでは把握できない傾向を明らかにすることができます。

このグローバルなデータセットが、Cognito NDRプラットフォームの自動分析能力を継続的に向上させているのです。Cognito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、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可能となります。

この結果、企業はITセキュリティにおける最も切迫した課題であるサイバーセキュリティ分析やインシデント対応、データサイエンスにおけるスキル不足を解消することができます。また、わずかな数の不審なトラフィックに着目する手作業によるアプローチとは異なり、Cognito NDRプラットフォームは、クラウド、データセンター、IT、IoTネットワークの全てのトラフィックを横断的に分析します。

この自動化のレベルがいかに価値あるものであるかは、簡単な分析を行うだけですぐに明らかになります。500ホストのネットワークを監視する、Cognito NDRプラットフォームソフトウェアの年間ライセンス費用は約400万円です。実際のスループットは様々ですが、例えば500ホストのネットワークで毎秒500メガビットのトラフィックが発生すると仮定しましょう。

既にご紹介した通り、最上位のセキュリティアナリストやデータサイエンティストの人件費は、年間で約3,000万円（2名）に上りますが、それでも分析できるのは、これらのトラフィック全体のほんの一部に過ぎません。以下の図は、前にご紹介した図を、分析対象となるギガビットあたりのコストで表現した、より詳細な指標を示すものです。

分析の自動化機能によって、企業は専門家を追加で雇用する必要なく、より迅速なセキュリティインシデントの管理が可能となります。追加の雇用が発生しないことは、財務面で考えても大きな意味があります。

担当者コストの年間節減金額	
新規雇用を延期した人数	1名
フルタイムの専門家の1時間あたりのコスト（NSSの説明による）	5,200円
年間コスト	**1,100万円**

時間：侵害検知において、最も高いコストが費やされる指標

隠れたサイバー攻撃を検知する上で、最も重要となる要因は時間です。被害を軽減するためには、重要なアセットが盗難にあう前に、攻撃をほぼリアルタイムで検知しなければなりません。セキュリティチームにとって問題なのは、このような攻撃の検知に最も多くの時間がかかっている点です。

一旦攻撃者が境界防御を擦り抜けてしまうと、その後は多くの時間を要する手作業での対応となります。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フォレンジック分析のスキルに加え、様々なソースから大量のデータが必要になります。これらの作業には、幅広い専門的なスキルと膨大な時間が必要となります。

境界に配置されたシグニチャやサンドボックスなどのセキュリティ技術を擦り抜けることは、高度な攻撃者にとって、さほど困難なことではありません。その一方で、このようなイベントに関する簡単な調査でさえ数時間を要し、持続的標的型攻撃（APT）を完全に分析しようとすれば、数日から数週間もの時間が必要になります。

Cognito NDRプラットフォームは、分析フェーズを自動化し、瞬時に脅威を検知します。分析プロセスでは、マルウェアの振る舞いの理解や回避テクニック、ユーザーの振る舞いの分析といった多くの領域を連携させ、また脅威の紐付けを行うことによって、クラウドやデータセンター、IT、IoTネットワーク内の標的型攻撃の存在と場所を特定します。

この手法によって、他では検知することができない脅威も、人の関与なしに検知できるようになります。Cognito NDRプラットフォームは、イベントを自動的に優先順位付けし、攻撃のそれぞれのフェーズを解釈し、またパケットから取得したソースメタデータに素早くアクセスして、検知した脅威を検証できるようにします。

簡潔な言葉を使って検出結果を説明すると共に、次のステップに向けて有効となる助言をMITRE ATT&CKフレームワークにマッピングし、セキュリティチームがすぐに修正のアクションを図れるようにします。これにより担当チームは、数時間から数日はかかる手作業での対応を、数分、数秒にまで短縮し、損害が発生する前にアクションを取ることが可能となります。

セキュリティ調査とインシデント対応のためのコスト

本セクションでは、セキュリティイベントの調査とインシデント対応のコストを推定するための基本的なフレームワークについて説明します。セキュリティ調査やインシデント対応では、2つとして同じケースが存在しないため、コストの推定には様々な業界標準やベンチマークが用いられてきました。ここでは皆様の組織の実態により近づけるために、特定の指標をカスタマイズすることも可能です。

セキュリティ調査に必要な労力と費用は、3つのフェーズに分けて考えることができます。

1. **日々のセキュリティ分析と調査** この中には、セキュリティソリューションからのイベントやアラートの調査、ログの分析、ホストベースのアラート、新しく特定された、または既存の脅威の分析などが含まれます。最終的な目的は、顕著なセキュリティイベントが発生していなかどうかを見極めることです。特にAPTの存在を検出することが目的の場合、このフェーズは時間を要するものとなります。
2. **内部でのインシデント対応** 前のフェーズで深刻なセキュリティイベントが検知された場合、このフェーズが発生します。これは多くの場合、セキュリティインシデント対応チーム（SIRT）に依存します。SIRTは、専任の担当者、あるいは専任がいない場合は既存のチームの中からアドホックな形で選んで構成することができます。この工程は、イベントを封じ込めて修正するまで、数分から数ヶ月間続くことがあります。
3. **外部のインシデント対応** 外部のインシデント対応サービスの多くは、侵害が発生した後で契約を行い、支援を受けるという形態を取ります。これは通常、内部の担当者では攻撃を検知できなかった場合、あるいは攻撃ライフサイクルの後半で攻撃が検知された場合に実施されます。

それぞれの領域で同様の指標、つまりイベント発生の頻度、担当者がイベント対応に要する時間、および担当者の時間単価について調べる必要があります。

推定コスト＝
イベント発生回数 × 解決までの所要時間 × 担当者の時間単価

これらの要素は各フェーズで同じですが、実際の値は分析フェーズによって異なります。例えば、日々の分析の場合には、簡単な調査を多数行う場合もあり、インシデント対応に要する時間は、数日、数週間、あるいは数ヶ月となる場合があります。計算結果については、これらの違いを説明できるよう、各フェーズ毎に表示されます。

日々のセキュリティ分析に必要となるコストの計算

セキュリティ調査や分析に関わる日常的な作業は、それぞれの企業によって異なります。専任の専門家チームが行う場合でも、またセキュリティのジェネラリストによってアドホックに構成されたチームが行う場合でも、事実上全てのセキュリティ製品は、サイバーセキュリティに関する実践的なインテリジェンスを引き出すために、相応の時間を必要とします。アナリストは、さらなる調査や対応が必要なセキュリティイベントが存在するかどうかを見極める必要があります。

日々のセキュリティ活動に費やされる時間を分析する際には、イベントの調査と分析に向け、1日に費やされる時間の合計を見積る必要があります。このような作業は、様々な経験や専門性を持った担当者によって行われます。

スタッフの時給 これらの計算では、チームメンバーのコストを推定するために、デフォルトで1時間あたり5,200円という単価を使用します。この単価は、セキュリティソリューションの総所有コスト（TCO）を決定するために、経験豊富なセキュリティエンジニアがフルタイムで活動した場合を想定して使用されます。

以下の表は、標準的な想定値を基に、中小規模の企業における調査コストの単純な見積りをまとめたものです。

日々の分析に必要な担当者のコスト	
調査に費やされる1日あたりに作業時間の割合	20%
調査に関与する担当者数	2名
調査に費やされる年間平均時間	832時間
担当者の時間単価	5,200円
年間コスト	**433万円**

Vectra製品がもたらす価値

Cognito NDRプラットフォームは、クラウド、データセンター、IT、IoTネットワークの内部で活動する脅威を一元的かつ自動的に特定します。検知機能によって、数十から数百ものイベントやメタデータのサンプルを集約し、最終的な診断を行います。

さらに各イベントについては、脅威の程度、信頼度、攻撃ライフサイクルのフェーズに応じて、スコアリングと優先順位付けが行われます。これにより担当者は、アドウェア・ボットネットや他の優先順位の低い脅威と、企業のアセットを盗み出す目的で活動中の標的型攻撃を、容易に区別できるようになります。

このような自動化は2つの効果をもたらします。それはセキュリティ担当チームがより短時間で調査を行えること、また専門外の担当者であっても多くの調査が可能になることです。

Vectra AI社のお客様による報告では、調査に要する時間が75%～90%削減され、また単価の高い専門家にインシデント対応を引き継ぐことなく、ITのジェネラリストだけで対応できるようになったという声が寄せられています。以下の分析結果では、控えめに見ても分析に要する時間が50%削減され、平均時間単価も5,200円から3,900円に低減されたことが示されています。これを前に示した基準に照らし合わせると、3万9,520ドル、つまり63.3%の節約が達成されたことになります。

内部担当者によるインシデント対応コストの計算

インシデント対応のための作業量やプロセスは、企業によって大きく異なります。ここでは、SANS Instituteにおける企業のインデント対応の調査結果を、合理的な基準値として使用しました。

この調査では、250社以上の企業からイベント発生の頻度や阻止に要した時間など、インシデント対応に関するデータを収集しています。また、従業員100名以下の小規模事業者を含む、ほとんどの企業がセキュリティインシデントを経験していることが分かっています。

インシデントの件数 多くの企業が1～25件のインシデントを報告していますが、最も顕著な環境では500件を超えている場合もあります。SANSのデータによれば、控えめに推定しても1企業あたり年間平均17のインデントが発生していることが分かります。

阻止するまでの時間 阻止するまでの時間には、大きな開きがあります。最も多い対応時間は6～8時間ですが、最大では6ヶ月以上もの時間が費やされているケースがあります。偏りを回避するために、報告があった共通性の高いカテゴリのみを使用した場合には、阻止するまでに要する平均時間は29時間でした。

VECTRA製品を使用した内部担当者によるインシデント対応コスト	
調査に費やされる1日あたりの作業時間の割合	10%
調査に関与する担当者数	2名
調査に費やされる年間平均時間	416時間
担当者の時間単価	3,900円
年間コスト	162万円
年間削減コスト	**271万円**

内部担当者によるインシデント対応の人件費	
年間の発生イベント数	17回
阻止までの平均時間	29時間
SIRTチームの担当者数	3名
平均時間単価	5,200円
SIRTの年間人件費	**769万円**

Vectra製品がもたらす価値

Cognito NDRプラットフォームは、脅威の隠れた兆候を検知するだけでなく、攻撃を受けている特定のホストやワークロード、アイデンティティ/アカウントと、対象となる攻撃を複数の段階で紐付けします。脅威を迅速に阻止するためには、膨大な量のデータを幾つかの特定のホストやワークロード、アイデンティティ、アカウントにまで絞り込むことが重要です。

2020 Mandiant M-Trendsレポートによれば、ネットワークに対する侵入の多くは、平均して56日間検知されずに放置されており、この日数は覚えておくべき数字です。またSANS Instituteの調査によれば、一旦脅威を検知した場合でも、その阻止には数日から数ヶ月の時間が必要になるとしています。

CognitoNDRプラットフォームは、これらいずれについても、その時間を大幅に短縮します。Vectra　AI社が行った分析は、適切な条件で比較ができるよう、インシデント対応に向けた取り組みに限定する形で直接比較を行っています。

最高レベルの信頼度を誇るCognito NDRプラットフォームでは、他の製品では検出することができないセキュリティイベントを検知することができます。これにより対象となる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。Cognito NDRプラットフォームによって、これらのイベントの多くを自動的に管理できるようになると共に、検知対象となるイベント数を倍増さえることも可能になります。

また、修正対象となるホストやワークロード、アイデンティティ、アカウントの診断に必要となる調査件数を削減することができます。攻撃を受けている特定のホスト、ワークロード、アイデンティティ、アカウントを紐付けし、スコアリングを行うことで、Cognito NDRプラットフォームを使用するセキュリティチームは、数日から数週間を要していた調査やログのレビュー、SIEMベースの分析をわずか数分で行えるようになります。

この結果についても、脅威の阻止に必要な時間を30分以下に短縮したVectra AI社のお客様から得られた実際のデータを基にしたものです。以下は、脅威の阻止に必要な全体時間を3時間に短縮したという、標準的な推定を基にした計算結果になります。***この推計によれば、インデント対応に必要なコストが610万円、つまり79.3%削減できたことになります。***

VECTRA製品を使用した1日あたりの分析における担当者のコスト	
年間のイベント数	34回
阻止までの平均時間	3時間
SIRTチームの担当者数	3名
平均時間単価	5,200円
SIRTの年間人件費	159万円
年間削減コスト	**610万円**

外部担当者によるインシデント対応コストの計算

公表されているインシデント対応サービスの契約やレポートを参考にして、外部担当者によるインシデント対応コストの基準を作成しました。この場合、サービスの時間単価は3万円前後であり、全体的なコストは、通常、1,400万円から3,500万円の間となります。

カリフォルニア州南部における時間単価の中央値は386ドルで、コストの合計は50万ドルとなります。

外部担当者による対応コスト	
外部のインシデント対応担当者の時間単価	3万円
合計請求時間	500時間
サードパーティーによるインシデント対応コスト	**1,400万円**

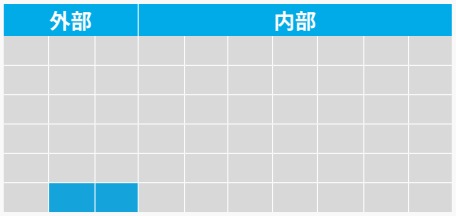
Vectra製品がもたらす価値

全ての企業がこれらのコストを毎年のように負担しているわけではありませんが、これらは重大な未検知の侵害に対するインシデント対応を外部担当者が行った場合の、現実的なコストを反映したものと言えるでしょう。

Cognito NDRプラットフォームがもたらす最も重要な価値は、高度な脅威をプロアクティブに検知して、データの喪失や損害が発生する前にネットワーク侵害を阻止できることです。Vectra AI社では、このような価値を推計するために、インシデント対応サービスコストの下限値を選択し、また4年間の範囲でリスクを正規化しました。この結果では、年間の節減金額は350万円となっています。

手作業によるアプローチ

分析対象トラフィック



例外的にトラフィックを分析
- 基本的に境界線上のトラフィックにフォーカス
- 多くの場合、不審あるいは不明のシグニチャ、またはサンドボックスの結果によって、分析を開始
- 場当たり的な対応

活動検知のフェーズ

数時間、数日、数週間の調査

×

人件費の高い特別なスペシャリスト（時間単価5,250円～7,000円）

優秀な担当者が手作業で対応
- 高度な教育を受けた担当者が必要
- 特殊なスキルの組み合わせ（マルウェア、トラフィック、データデバイス）
- すぐに飽和状態に（拡張不可）

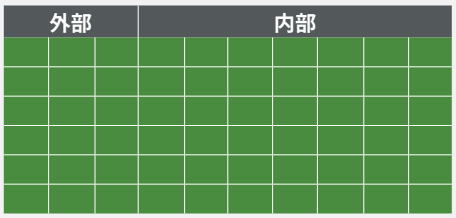
IRフェーズの後

- **非常に高額**
- **2万8,000円/時間**
- **1,400万円～3,500万円**
- **損害を受けた後**

ペナルティフェーズ
- 非常に高額
- 終わりのない調査
- 軽減の機会なし

Vectra製品によるアプローチ

分析対象トラフィック



全てのトラフィックを調査
- 不審なアクションに対する全てのトラフィックを調査
- 縦方法、横方向のトラフィック
- 攻撃の全てのフェーズを検知
- クラウドログ

活動の検知と対応フェーズ

リアルタイムに検知（秒単位）

↓

一般のIT担当者に次の手順を指示

自動化された、実践的な検知
- 調査時間を秒単位に短縮
- 自動修正またはITのジェネラリストによる修正

IRフェーズの後

- 非常に高額
- 2万8,000円/時間
- 1,400万円～3,500万円
- 損害を受けた後

ペナルティフェーズを回避
- 脅威を予防的に管理

結論

本書では、セキュリティ調査に必要な運用コストの推計に対する基本的な手法に加え、クラウドやデータセンター、IT、IoTネットワークにCognito NDRプラットフォームを導入した場合のコスト節減について説明しました。

Cognito NDRプラットフォームによって、以下のような主要な領域で、毎年大きな節約を実現することができます。

領域別の節減	
セキュリティおよびデータサイエンス人件費の削減額	1,100万円
日々のセキュリティ運用に関する時間短縮	271万円
インシデント対応の時間を短縮	610万円
サードパーティーを使ったインシデント対応の回避	350万円
合計	**2,331万円**

これらの削減額は、大規模なセキュリティチームを擁する企業ほど大きくなります。Cognito NDRプラットフォームを使って脅威ハンティングを自動化することで、全てのトラフィックを対象に調査を実施し、手作業で調査や関連付けを行う時間を減らし、全ての担当者が活動中の脅威を迅速に修正できるようになります。

まとめ

新しいタイプの脅威への対応にあたって、新しいセキュリティが必要になるのは当然のことです。しかし、ほとんどのセキュリティ製品がその価値を発揮するためには、人的な作業時間や能力開発に向けた膨大な投資が必要となります。完全な形で導入できなかったという理由や担当者がサポートできなかったという理由により、企業内でセキュリティ製品が使用されないままになっているケースも少なくありません。

Vectra AI社のCognito NDRプラットフォームは、他では検出できない脅威の検知を可能にし、セキュリティ部門の作業時間や担当者の人数、予算を節約することができる、コスト効果に優れた数少ないソリューションの1つです。

Cognito NDRプラットフォームは、時間の浪費に繋がりやすいサイバー攻撃の調査を自動化することで、セキュリティチームのニーズに応えられるよう意図的に設計されており、負担を増やすことはありません。これにより導入企業では、クラウドやデータセンター、IT、IoTネットワークを横断した効率的なセキュリティアーキテクチャー構築し、ボトルネックを排除して、全てのITやセキュリティ担当者が隠れたサイバー攻撃を迅速に検知および対応できるようになります。

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、info-japan@vectra.ai までお願いします。