Vectra MDR（管理型検知とレスポンス）サービス

進化し続けるハイブリッドクラウド環境と、サイバー攻撃者の高度な戦術の組み合わせにより、セキュリティチームが対処すべき未知の脅威が数多く生み出されています。セキュリティチームの多くは、すでに圧倒的な数のアラートに追われており、加えてリソースの制約や、人材の定着と採用という継続的な課題も存在します。

現在直面している課題は、分析するためのツールやデータセットを増やしたところで解決できるものではありません。逆にそのような対策をしても、アナリストの負担が増えて、疲労、過度なストレスを招き、最終的には離職につながるだけです。セキュリティ、リスク、コンプライアンスチームを率いるリーダーは、サイバー攻撃者が組織に侵入するのを検知し、阻止するために、シグネチャベース、異常ベースもしくはルールに依存する検知とレスポンスという手法に、もう頼ることはできません。従来のアプローチはすでに破綻しており、最新の脅威を防御するためには、24時間365日体制の脅威検知とレスポンスが必須なのです。

「セキュリティリーダーの83%が、従来のアプローチは、最新の脅威に対して有効でないと考えている。」 Global Research Study、"Fit for Purpose or Behind the Curve"（目的に適合するか、遅れをとるか）

主なポイント：

- 高スキル人材不足とアナリストの負担増による過度なストレス
- 進化し続けるクラウド環境に対するセキュリティ
- Vectra TDRプラットフォームの最適化
- 脅威ハンティング・調査の専門知識
- 24時間365日体制のVectraの脅威検知とレスポンス
- ツールの普及と管理

Vectra MDR、24時間365日体制で専門知識と共に未知の脅威を排除

Vectra MDR（管理型検知とレスポンス）は、24時間365日、脅威を検知、調査、対応するために必要なサイバーセキュリティスキルを提供いたします。Vectraのアナリストとお客様のセキュリティチームが、**共有責任モデル**を生かし、Vectraの脅威検知とレスポンスプラットフォームで連携することで、完全な可視化、コラボレーション、解決時間の短縮を実現できます。Vectraのプラットフォームでは、お客様は自社のセキュリティについてコントロールを失うことはありません。また、当社のアナリストチームと調査や対応について必要なだけやりとりを行えるリアルタイムのコラボレーションも提供します。Vectra MDRのメリットは次のとおりです。

カバレッジ

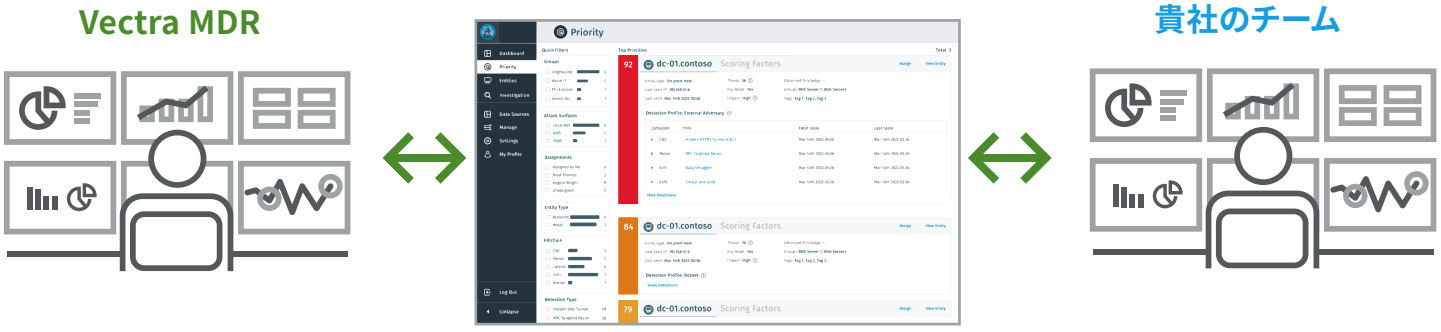
Vectra MDR は、パブリッククラウドサービス、SaaS アプリケーション、IDシステム、およびネットワークインフラストラクチャ全体の攻撃を、先を見越して調査して阻止する、24 時間 365 日の監視サービスです。

明確さ

Vectra MDR は、24 時間 365 日の調査とアラートの優先順位付けに対応できるエキスパートアナリストを備えており、貴社のセキュリティチームの延長として支援いたします。

制御

一般的なMDRサービスを超えたサービスを提供。お客様のセキュリティアナリストとVectraのアナリストは同じプラットフォームで作業し、脅威を完全に可視化、制御し、共同で調査、解決することができます。



サイバー防御を強化し、備える

眠ることのない人間の知能

VectraのAttack Signal Intelligenceは、最新の回避的かつ高度な攻撃をAIで検知し、トリアージと優先順位付けを行うことができます。Vectra MDRのアナリストは、24 時間 365 日体制で、調査、対応、プラットフォームの最適化に関する専門知識を提供します。Vectraプラットフォームの能力とアナリストチームによるヒューマンインテリジェンス (人間の知能) を組み合わせることで、より迅速に対応し、お客様に優れた成果を提供いたします。

セキュリティチームの拡張

Vectra MDRでは、お客様のセキュリティチームの延長として、経験豊富なVectraのセキュリティアナリストがプラットフォームの活用を支援します。サービスには、専門家との定期的なミーティングが含まれ、お客様固有のものや世界的な傾向、セキュリティポスチャ、お客様のネットワークで発生したイベントについて話し合います。提供内容は次のとおりです。

- 専門知識と脅威分析
- 24 時間 365 日体制の監視と先を見越した調査
- Vectra導入のカスタマイズ
- アプリ内におけるMDRチームとのリアルタイムなコミュニケーション

Vectraプラットフォームの最適化

Vectraのセキュリティアナリストは、お客様のVectraプラットフォームと連携し、知識と経験を生かして効率的にインシデントを調査し、解決します。Vectraを最大限に活用していただくために次のようなサービスを提供します。

- 調査の専門知識
- コンフィギュレーションの最適化
- グローバルな脅威と攻撃へのインサイト
- プラットフォームの調査、コンテキスト、可視性

人間の知能とAI駆動型の運用で、攻撃者に対して優位に立つ

セキュリティリーダー、アーキテクト、アナリストは、先手を打ち、最新のサイバー攻撃の一歩先を行くことができます。

脅威の早期発見とコンテキスト

Vectra MDRサービスでは、Vectraのセキュリティアナリストの専門的な視点から脅威を調査し、対応します。脅威は自動的に検知され、優先順位が付けられます。

AI駆動型のトリアージとプラットフォームのチューニング

Vectra MDRを担当するセキュリティアナリストは、何百件ものVectraの導入において、無数の脅威の振る舞いを観察し、多くの知識を蓄積しています。許可された振る舞いを承認するためのカスタムフィルターの作成をサポートし、効果的なトリアージプロセスのための個別の提案を提供いたします。

Vectraのセキュリティに特化したAI駆動型のAttack Signal Intelligence™ によって実現できること

- **攻撃者の目線で考える:** AI駆動型の検知によって、攻撃全体の流れを検知することができます
- **悪意のある脅威に焦点を当てる:** AI駆動型のトリアージによって、悪質な真陽性が明らかになります
- **何が重要かを把握する:** AIによる優先順位付けは、重大な脅威の優先順位付けの効果を85%向上します

組織内で使用されているセキュリティツールの数を考えると、それぞれのプラットフォームやソリューションの専門家になることは困難です。同時に、攻撃者の一歩先を行くために、セキュリティ管理を24時間365日体制で、確実に最適化することが、ますます重要になっています。他のアプローチとは異なり、Vectra MDRサービスでは、Vectraプラットフォームで現在のチームを補強するためにサービスを利用する場合でも、セキュリティ運用を完全にアウトソースする場合でも、責任共有モデルによって、組織が制御を維持することが可能です。Vectra MDRのアナリストを組織のSOCチームの一員に加えることで、未知の脅威を排除し、攻撃者より優位に立つことを可能にします。

Vectraの管理型検知とレスポンスのサービスについてもっと知る

Vectraについて

Vectra® は、ハイブリッドクラウドにおけるサイバー脅威の検知とレスポンスにおけるリーダーです。Vectraの特許取得済みAttack Signal Intelligence™は、パブリッククラウド、SaaS、ID、ネットワークにわたる脅威を単一のプラットフォームで検出し、優先順位付けを行います。VectraのAttack Signal Intelligenceは、単なる異常検知にとどまらず、攻撃者の振る舞いを分析することで理解します。その結果として得られる高精度の脅威シグナルと明確なコンテキストにより、セキュリティチームはこれまでよりも速く脅威に対処し、進行する攻撃をより迅速に阻止できます。世界中の組織が、VectraプラットフォームとMDRサービスを活用し、最新のサイバー攻撃に対して一歩先を行く対策を行っています。

vectra.ai/jp
お問い合わせ:info-japan@vectra.ai

© 2022 Vectra AI, Inc. All rights reserved. Vectra、Vectra AI社のロゴ、CognitoおよびSecurity that thinksは、Vectra AI社 の登録商標です。Cognito Detect、Cognito Recall、Cognito Stream、Vectra Threat LabsおよびThreat Certainty Indexは Vectra AI社の商標です。その他の会社名、製品名およびサービス名は、各社の登録商標またはサービスマークです。Version: **111622**