VectraのセキュリティAI駆動型Attack Signal Intelligence™

何十年もの間、サイバーセキュリティは既知の脅威に対応してきました。サイバー攻撃に対する脅威の検知とレスポンスの手法は、シグネチャー、アノマリー検知、ルール識別によって、攻撃者が内部に侵入したことを認識し、データが盗まれることを阻止してきました。しかし、このアプローチはすでに破綻しています。

企業がハイブリッドおよびマルチクラウド環境に移行し、デジタルID、デジタルサプライチェーン、エコシステムを採用するにつれ、セキュリティ、リスク、コンプライアンスの担当者が抱える課題は増加しています。

- カバーすべき攻撃領域の増加
- セキュリティ対策を回避する巧妙な攻撃者
- 分析するツール、データセットの増加
- 維持すべきシグネチャ、異常、ルールの増加
- アラートノイズ、トリアージ、誤検知の増加
- アナリストの負担が増え、離職率が増加

ツール、データ、シグネチャ、ポリシー、ルール、アラート、人材を増やしても、根底にある問題は変わりません。

「今起きている侵害を、把握できていない」

未知の脅威に対し、攻撃者は優位に立っている

- 防御の回避
- シグネチャや異常検知ルールの迂回
- 侵入、横方向への侵入拡大
- データの盗用

VectraのセキュリティAI駆動型Attack Signal Intelligenceが未知の脅威を排除する

VectraのセキュリティAI駆動型Attack Signal Intelligenceは、サイバー攻撃に対するリスクベースのアプローチを採用することで、手動タスク、アラートノイズを減らし、アナリストが限界まで追い込まれることを防ぎます。Attack Signal Intelligenceによって、セキュリティアナリストは次のことが可能となります。

攻撃者の目線で考える

AI駆動型の検知は、シグネチャや異常値だけではなく、攻撃者の振る舞いを理解し、攻撃のシナリオを完全に明らかにします。

悪意のある脅威に焦点を当てる

AIによるトリアージは、アクティビティを悪意のあるものと無害なもので区別し、アラートノイズを減らします。無害なものはログに記録され、悪意のある振る舞いのみ検知されます。

何が重要かを把握する

AIによる優先順位付けは、ノイズを減らし、アラートのトリアージを自動化します。ビジネスにとって最も影響のある脅威の優先順位付けに対する効果が85%向上します。

異常な振る舞いではなく、リアルな脅威を検知

攻撃者の振る舞いに関するセキュリティ研究とデータサイエンスに根ざしたAttack Signal Intelligenceは、単なる異常検知にとどまらず、サイバーキルチェーン全体を通して実際の攻撃とその進行を検知することができます。

AI駆動型検知

- 攻撃を進行させるために使用される攻撃者のTTPに焦点を当てる。
- 振る舞いベースのモデルは、攻撃者のTTPを正確に検知することができる。
- 適切な検知のために最適なMLアプローチを利用する。

AI駆動型トリアージ

- すべてのアクティブな検知の共通性のための継続的な分析。
- 悪意のあるものと無害なアクティビティを区別するため、直感的で使いやすい設計。
- 悪意のあるアクティビティを公開し、無害なアクティビティをログに残すための自動化。

AI駆動型の優先順位付け

- ドメイン全体で攻撃者のTTPを相関的に検知。
- 完全な攻撃シナリオの包括的な可視化。
- 脅威の深刻度や影響度による優先順位付けを一元的に表示。

AI駆動型検知

攻撃者の目線で考える
単なる異常検知にとどまらない

攻撃者のTTPに焦点を当てる

振る舞いベースのTTP検知

最適なMLを活用

AI駆動型トリアージ

悪意のある脅威に焦点を当てる
ノイズを低減する

継続的な分析

直感的に操作できる設計

悪意のある攻撃を公開する

AI駆動型の優先順位付け

何が重要かを把握する
調査とレスポンスに備える

TTP検知の相関性

総合的な可視性

優先順位の高いビューを統一

AIを活用した運用で、形勢を逆転させる

セキュリティリーダー、アーキテクト、アナリストを備え、最新のサイバー攻撃に先手を打ち、常に一歩先を行けるようにする。

Integrated Investigations (統合調査) によって、アナリストはすぐに答えを得ることができます。

- 深刻度と影響度によってランク付けされた重要な脅威に焦点を当てる。
- 攻撃対象領域全体に潜む脅威を探す。
- 単一のユーザーインターフェイスで、コンテキストとフォレンジックを使用して調査することができる。

Automated Workflows (自動化ワークフロー) は、手動作業を自動化することで、複雑さとコストを削減します。

- アナリストのワークストリームを1つのインターフェイスに集約。
- SIEMのデータフィード、ダッシュボード、レポーティングをシンプル化。
- 既存のチケット制や報告ワークフローの統合カスタマイズ。

Targeted Response (ターゲットレスポンス) は、アナリスト主導で実施されるため、人によるレスポンスの制御が可能です。

- アカウントのロック、エンドポイントの隔離、SOARやITSMのプレイブックの起動など、自動または手動で起動する柔軟なレスポンスアクションを提供する。
- EDRおよびSOARのトッププロバイダーとの統合。
- Vectra MDRサービスを活用した管理型レスポンス。

単純な異常検知に重きを置き、人によるチューニングやメンテナンスを必要とする他のアプローチとは異なり、Vectraのセキュリティ AI駆動型Attack Signal Intelligenceは、人手を介さずに脅威の検知、トリアージと優先順位の決定を自動化します。この技術を活用することで、セキュリティチームは未知の脅威を阻止し、攻撃者に対抗し、世界をより安心で安全な場所にすることができるのです。

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。世界中の組織は、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