VECTRA
SECURITY THAT THINKS.®

競合分析概要

Darktraceのダークサイド：Vectraが選ばれる理由とは

ネットワークの検知および対応（NDR: Network Detection and Response）ソリューションは、全てが同様のアプローチというわけではありません。Darktrace社が、PoCの検証結果を Vectra® プラットフォームと比較する形で紹介している状況をよく目にしますが、それ自体は歓迎すべきことだと考えています。

それは、お互い切磋琢磨することで、NDRの市場を成長・発展させていくことができるからです。そして、両社を正しく比較検証した場合、Vectra の優位性が明らかになります。特にお客様がレッドチームを使って、現実の攻撃をシミュレーションするような場合は、それが顕著に現れます。なぜなら、Vectra のAIモデルは、教師あり、教師なし、ディープラーニングの機械学習アルゴリズムを持ち、セキュリティリサーチャーとデータサイエンティストが共同で開発した独自のものだからです。個別の異常を使用するDarktraceとは異なり、Vectraは複数のAIの振る舞いモデルを使用し、潜在的な脅威に対して最適なものを選択します。Vectraが充実した優先順位の高い分析を提供することで、お客様は作業量の削減や調査の無駄を省くことができるのです。

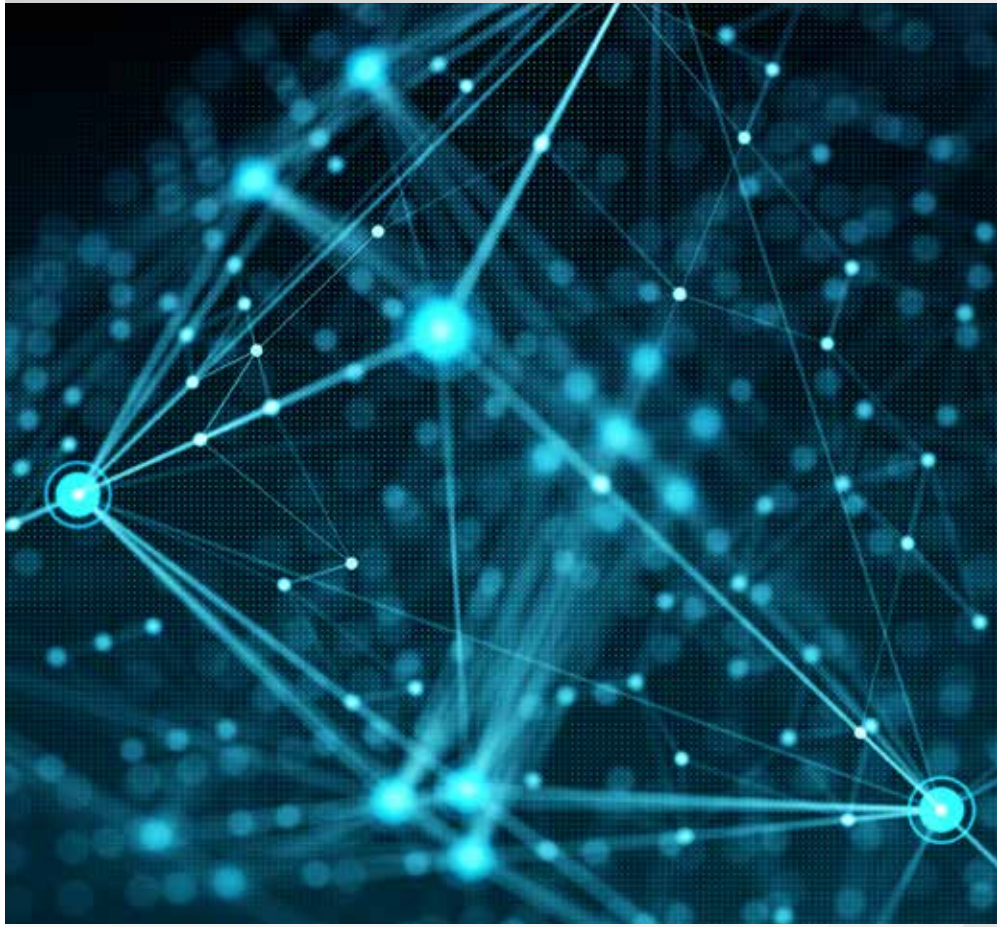
学習に長時間を要するDarktrace

Vectra AIプラットフォームは、導入直後から脅威の検知を開始しますが、Darktraceはベースラインの作成に2週間を要し、それまでお客様は脅威の検知はもちろん、ソリューションを確認することさえできません。

攻撃者（アタッカー）が最初の攻撃をわずか数分で実行できることを考えれば、導入直後に脅威の検知が可能なVectra の優位性は一目瞭然です。Darktraceは、既知の悪意のある振る舞いを良性のイベントとして学習するという大きなリスクを持ちます。Darktraceでは、誤検出や誤認識が起きてしまうのです。

85%

Vectra NDRプラットフォームは、MITREのATT&CKフレームワークの85%以上をサポートしています。



Vectra AIプラットフォームは、導入直後から脅威の検知を開始しますが、Darktraceはベースラインの作成に2週間を要し、それまでお客様は脅威の検知はもちろん、ソリューションを確認することさえできません。

VPN経由で結果を操作

DarktraceがPoCのトライアルで、VPN接続を使用するのはなぜでしょう？Darktraceは、PoC期間中、常時接続VPN “Call-Home”ファンクションを要求します。もしお客様がこの接続を許容できない場合、Darktraceの検知精度は劇的に低下します。

そして、VPN接続先では、PoCの結果を最適化するためにカスタマイズしているオペレーターがいるのです。残念ながらそのような人は、Darktraceソリューションには含まれていないので、Darktraceを導入した場合には、人材を自社で準備する必要があります。

膨大なアノマリーアラートに備える

Vectraのアルゴリズムは攻撃者の視点で一連の流れを捉えるため、単純なシグネチャーベースであるDarktraceの検知よりも、遙かに優れた検知精度となっています。実際にVectraプラットフォームは、MITREのATT&CKフレームワークの85%以上をサポートしています。このような包括的な検知機能の存在は、お客様が実施するPoCの過程ですぐに明らかになります。

アノマリーベースの検知システムであるDarktraceでは、最もリスクの高い攻撃を特定することができないだけではなく、大量に発生するアラートによって、詳細調査が必要なセキュリティチームを疲弊させる結果となります。

この状況とは全く対照的に、Vectraの場合、セキュリティオペレーションにおける負荷を1/34へと削減することができます。Vectraでは、アラートを自動的にトリアージしてインシデントに落とし込み、高いリスクを持つホストデバイスに対して優先順位付けを行います。さらにネットワークトラフィックからセキュリティ強化メタデータを抽出し、調査やフォレンジックのために提供します。

一方、Darktraceのアラートは、手作業で個別にトリアージを行う必要があるため、セキュリティオペレーションの負荷が増加します。そのため、NDRソリューションをお求めのすでにオーバーワーク気味のセキュリティチームに、さらなる運用負荷をかけることになります。

他と連携ができないDarktrace

Darktraceは他のセキュリティソリューションと完全に連携することができない、サイロ化したテクノロジーであることを、ほとんどのセキュリティリーダーが認識しています。Darktraceでは、syslogをSIEMに送ることが、セキュリティソリューション連携と考え、それによるインシデント対応が可能だと信じています。しかし、Darktraceは主にネットワークリセットの送信や自社製品との統合に依存しており（EDRやNACなどへの投資を置き換えることになります）、ファイアウォールにアクティブリストを適用しているため、結果としてはお客様の管理の手間が増えてしまいます。

Vectra：機能するNDR

一方、Vectraプラットフォームの場合には、API経由で企業のセキュリティスタックと容易に連携し、新たなクラスの脅威を阻止することができます。Vectraのテクノロジーパートナーのエコシステムは、エンドポイントセキュリティ（EDR）、次世代ファイアウォール、SIEM、セキュリティオーケストレーション（SOAR）、ネットワークアクセスコントロール（NAC）など、いずれも各分野のリーディング企業によって形成されています。また、クラウドへ移行するお客様向けにVectraはAWSやAzureとの密接な統合を行なっています。

またVectraは、優れたセキュリティインサイトやコンテキストを含め、セキュリティ強化ネットワークメタデータをデータレイクやSIEMに提供することで、インシデント調査や遡及的な脅威ハンティングの優れたスターティングポイントとなります。

Vectraプラットフォームは、以下のような点でDarktraceよりも優れています。

- 教師あり、および教師なしの機械学習アルゴリズムをベースに、クラウドのワークロードからユーザやIoTのデバイスに至るまで、現実世界の攻撃を検知します。
- ベースラインの学習期間なしに、導入直後から脅威の検知を行うことができます。
- SOCのワークロードを1/34へ削減することができます。Vectraでは、セキュリティアラートをトリアージして、攻撃者の目的をMitreフレームワークに自動的に重ね合わせ、ユーザ、ホスト、サービス、クラウドのアイデンティティを関連付けることで、迅速な原因特定が可能となります。
- お客様所有のセキュリティソリューションと連携しながら、プラットフォームの能力を発揮できます。

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