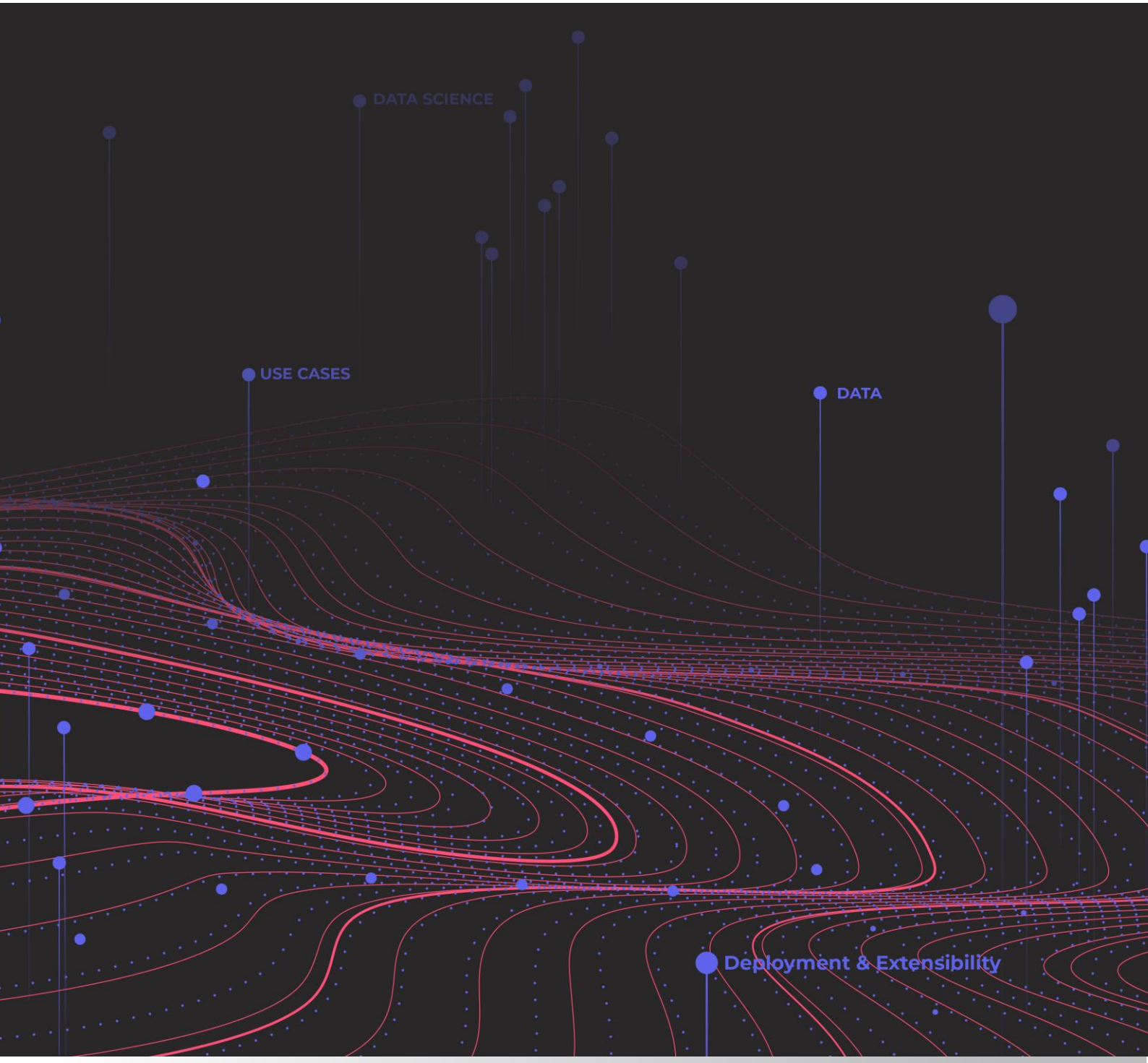
Arista NDR と Darktrace の比較

この比較では、第 1 世代の動作分析アプローチと、より新しく高度なネットワーク・トラフィック分析ソリューションの違いを明らかにします。



組織に最適なNDRプラットフォームを選ぶことは、その企業が疑わしいアクティビティを検出して迅速に対応し、結果としてより強力なセキュリティ態勢を獲得できるかどうかに大きな影響を与えます。

はじめに

世界中の組織が攻撃者によるネットワーク侵入を防ぐことを目的としたソリューションやテクノロジーに投資してきた金額は数十億ドルに及びます。それにもかかわらず、執拗な攻撃者は今なお境界の防御をくぐり抜けて、攻撃対象のネットワークにアクセスできています。そのような足がかりがひとたび確立されると、何か月も攻撃者に気付かない可能性があり、データ・アセットの盗難や破損のリスクが高まります。

既知のマルウェアのシグネチャや静的な侵害インジケーター（IoC）に焦点を合わせた従来のポイントインタイム予防ソリューションも引き続き必要ですが、広範囲にネットワーク・セキュリティをカバーするには不十分です。現在では、従来型のセキュリティ・ソリューションを補完するため、シグネチャや IoC 不要で疑わしいアクティビティを検出し、対応するソリューションが不可欠になっています。この市場の最前線に立っているのが、ネットワーク脅威検知・対応（NDR）と呼ばれる新しいテクノロジーです。

アナリスト会社 Gartner は、2020 年 6 月の『Market Guide for Network Detection and Response』で、このテクノロジーについて「エンタープライズ・ネットワーク上の疑わしいアクティビティを検出するため、機械学習、高度な分析、ルールベースの脅威検知を組み合わせて利用するものです。NDR ツールは、生のトラフィックやフロー・レコード（NetFlow など）を継続的に分析し、正常なネットワーク動作を反映したモデルを作成します。疑わしいアクティビティや悪意あるアクティビティを検出すると、NDR ツールはアラートを発行、または対応します。NDR ソリューションは、エンタープライズ境界をまたがる垂直型トラフィックの監視に加え、戦略的に配置されているネットワーク・センサーからのネットワーク・トラフィックやフロー・レコードを分析して、水平型の通信も監視することができます」と説明しています。

適切なソフトウェア・プラットフォームを選択する

Gartner の NDR 市場ガイド [1] では、Arista NDR の Arista NDR プラットフォームと Darktrace の Enterprise Immune System の 2 つのネットワーク脅威検知・対応ソリューションを取り上げています。市場をリードするポジションと強力な製品群から、NDR プラットフォームを選定している多くの企業の選択肢はこの 2 社に絞られています。

組織に最適な NDR プラットフォームを選ぶことは、その企業が疑わしいアクティビティを検出して迅速に対応し、結果としてより強力なセキュリティ態勢を獲得できるかどうかに大きな影響を与えます。Darktrace と Arista NDR の比較では、第 1 世代の動作分析アプローチと、新たに出現した高度なネットワーク脅威検知・対応ソリューションの違いを明らかにします。このドキュメントでは、処理対象のデータ、そのデータに適用される機械学習やその他のデータ・サイエンス技術、それによって実現されるユースケース、展開と拡張性に関する運用上の考慮事項など、企業のお客様にとって最も重要な基準に沿って、両社のプラットフォームを比較します。

データ

アクティビティ・データはあらゆる NDR プラットフォームにとって血液のようなもので、送信元、送信先、送信者、送信元デバイスなど、ネットワーク上のトラフィックに関する情報を伝えます。現在および過去の（保存されている）データを含め、利用・分析できるデータが詳細であればあるほど、セキュリティが向上します。IP アドレスだけでなく、デバイス、ユーザー、アプリケーション、組織が含まれている方が、コンテキストを踏まえて包括的に理解できるからです。

データ・ソースの豊富さ

ARISTA NDR		DARKTRACE
L2～L7 のネットワーク・データ		BRO アラート（L2～L4）

この基準では、プラットフォームが分析するデータの深度を調べます。Darktrace は L2～L4 のデータに基づく BRO（Zeek）アラートを利用しますが、Arista NDR は L2～L7 のネットワーク・データを利用します。このため、Arista NDR には、プロトコル・ ヘッダーのメタデータ以外も調べて、マルウェアや非マルウェアの脅威を発見できるという強みがあります。

ネットワークの可視化

デバイス、ユーザー、アプリケーション、外部ネットワーク、組織、ドメイン		IP アドレスに限定される

可視性を規定するのはデータ・ソースです。プラットフォームがメタデータのみを調べる場合、得られるのはポートや IP アドレスなどネットワーク・プロトコル情報だけです。Arista NDR プラットフォームはネットワーク全体を調べて、デバイス、ユーザー、アプリケーション、ドメインなどの関係を解決することができます。これにより、エンティティのコンテキストを提供して、垂直型通信と水平型通信で脅威を発見できます。Darktrace は、IP アドレスに基づく異常の検出に焦点を合わせています。Arista NDR は、すべての異常が悪意があるわけではなく、すべての悪意ある活動が異常であるわけでもないことを認識しています。そのため、脅威を統合してエンドツーエンドのキャンペーンを特定することで、さらに踏み込んだ対策を講じることができます。

Darktrace は、ユーザーによる Twitter への接続など、これまで行われたことはないが、セキュリティの観点から懸念をもたらす可能性は低い動作を異常と識別する場合があります。しかし、より詳細なネットワーク可視化機能を備えた Arista NDR は、Microsoft Word から Twitter への接続を正当なユーザーが行うことはあまりないが、攻撃者がよく利用する戦術であるということも把握しています。Darktrace にはこのコンテキストがまったくないので、異常な Twitter 接続が発生するたびにセキュリティ・アナリストに多大な負荷をかけたり、このように高度な攻撃者の戦術を完全に見逃してしまいます。

組織のデータ・プライバシー

顧客の環境内にデータを保持 – 必要に応じて分析機能をプライベート・クラウドに展開可能		顧客の環境内にデータを保持

データ・サイエンス

もちろん、データの収集は第一歩にすぎません。ネットワーク全体から収集したデータからインサイトや情報を獲得できるようにするのがデータ・サイエンスです。Arista NDR プラットフォームは、さまざまな科学的手法、プロセス、アルゴリズム、システムを利用して、構造化データおよび非構造化データからインサイトを抽出します。Arista NDR では、高度な AI と機械学習による分析が完全に統合されています。Darktrace は、従来の機械学習ツールをきわめて限定的に提供しています。これは主として教師なし学習で、誤検知が生じたり、説明性に欠ける傾向があります。

エンティティ相関付けの自動化

✓あり		限定的
プラグアンドプレイ方式、AI ベースの動作に基づくフィンガープリントで、デバイス、ユーザー、アプリケーションなどのエンティティをトラッキング		IP アドレスベースで、Active Directory などのテクノロジーとの統合や、DNS および DHCP トラフィックの観測が必要

この機能は、IP アドレス・レベルではなく、エンティティ・レベルで動作を調べて、さらに詳細にネットワークを可視化するものです。Arista NDR は、アプリケーションを使用しているエンティティやデバイスを自動的に判断し、そのエンティティの移動をトラッキングします。たとえば、あるデバイスが今日はニューヨークのオフィスにあり、明日はダラスのオフィスにある場合、Arista NDR はそのデバイスをトラッキングして、すべてのアクティビティをそのエンティティに関連付けます。Darktrace のケースと同様に可視化がネットワーク情報に限定されている場合、このデバイスは明日はまったく異なる IP アドレスになる可能性があるので、別のエンティティと見なされます。その情報を手動で相関付けようとすると、セキュリティ・アナリストの仕事が増えます。

抽出する検出特徴

～1200		～300

Darktrace が機械学習に利用する特徴は限定的で、ネットワーク・メッセージ、ポート、プロトコルなどセキュリティに特化していません。そのため、正当な業務のトラフィックに紛れ込んでいることが多い最新の脅威を、特に低いアラート誤検知率で検出することは困難です。Arista NDR は、ポートやプロトコルの情報だけでなく、ネットワーク通信全体への影響に基づいて、多数の特徴を抽出します。たとえば、あるパケットを Kerberos と識別することも、ログイン試行の成功と失敗を区別することもできます。これにより、誤検知と検知漏れを減少させ、悪意ある動作の高精度の脅威検知が可能になります。

セキュリティ・ナレッジ・グラフ

✓あり		✗なし

ナレッジ・グラフはエンティティの相関付けを発展させたもので、エンティティの位置やエンティティ間の関係、共有している属性、他のエンティティと類似しているエンティティを識別します。たとえば、グラフ内のすべてのデジタル電話をグループ化したり、フランスにあるすべてのデバイスをグループ化したりできます。本質的に、ナレッジ・グラフは Arista NDR が作成し特許を取得した基盤となるデータ・ストアで、ピア・グループと異なる可能性があるエンティティの動作を把握するのに役立ちます。対照的に、Darktrace は各 IP アドレスを単独で扱うので、セキュリティ・ナレッジ・グラフのようにエンティティを相関付ける仕組みはありません。

機械学習

✓あり		限定的
教師あり、教師なし、および連合機械学習の組み合わせ		トラフィック分析（ネットワーク・ポート、プロトコル、帯域幅に基づく）

動作についてコンピューター・システムに教える方法は多岐にわたります。Darktrace はデータ・サンプルに対して主に教師なし学習を使用して、デバイスの「日常パターン」、つまり正常な動作パターンを確立します。従来型のパターン・マッチングによる検出が向上する一方、「日常パターン」は新しいソフトウェアの展開や組織の再編などの正当なビジネス上の理由でしばしば変わるため、このアプローチには常に多くのノイズがあります。ただし、日常パターンを学習する前にデバイスが既に侵害を受けていると、このアプローチはうまく機能せず、悪意ある動作が正常として扱われます。Arista NDR の組み合わされた機械学習アプローチでは、過去の動作や組織全体の類似エンティティと比較を行うので、Darktrace のようなソリューションではよく見られる誤検知と検知漏れがなくなります。

立ち上げまでの時間

数時間		1～2 週間のトレーニング期間

Darktracet と Arista NDR が必要とする機械学習のトレーニング期間は大きく異なります。Arista NDR は教師なし学習のみに依存しないので数時間で運用できるようになりますが、Darktrace は 1 週間以上必要です。その上、新しいソフトウェアが展開されたり、その他の組織改変が発生した場合など、正当な動作が変わった際、Darktrace プラットフォームは再トレーニングの必要があります。顧客にとって、余分なトレーニング時間が生じるということは、価値を失うということです。

動作分析

あり トラフィック分析に加えて送信元と送信先のエンティティを分析		限定的 トラフィック分析（ネットワーク・ポート、プロトコル、帯域幅に基づく）

ユースケース

組織はネットワーク脅威検知・対応プラットフォームをどのように活用できるでしょうか。ソリューションがサポートできるユースケースが増えれば増えるほど、価値が高まり、ROI をより短期間で実現できるようになります。

既知の攻撃者 TTP（戦術、技術、手順）の検出

あり 正当な業務活動に紛れ込んでいる非マルウェアやその他の脅威を検知		限定的な機能

これまで、大部分の脅威検知は、以前の攻撃のデータを反映した侵害インジケーター（IoC）を利用して行われてきました。最近では攻撃者が賢くなり、このインジケーターだけでなく戦術や技術を絶えず変更するので、攻撃者の TTP を探すことが脅威を検知する効果的な方法となっています。Darktrace は、非マルウェア脅威を検知することが困難です。また、セキュリティ・チームが既知の攻撃者 TTP に対してカスタム検出モデルを作成する仕組みを提供していません。Arista NDR の充実したクエリ言語は、このような TTP を体系化できるボキャブラリーを提供し、システムが自動的かつ継続的に攻撃者 TTP を探せるようにします。この検出モデルは Arista NDR が提供しますが、顧客が作成したり、カスタマイズしたりすることも可能です。

遡及的検出

ありArista NDR		限定的Darktrace

新たな攻撃者 TTP が出現するたび、組織は過去に自社環境が（その TTP に対して）脆弱だったかどうかを知りたいと考えます。Darktrace は遡及的に検出を提供しない代わりに、基盤となる約 30 日間の BRO ログを利用して顧客が検索を実行できるようにしています。Arista NDR は必要に応じて時間をさかのぼり、関連する動作を自動的に突き止めることができます。

暗号化トラフィックの可視化

ありArista NDR 特許取得済みのアプローチ		限定的Darktrace アプリケーションのフィンガープリントに オープンソースの JA3 を利用

暗号化されるネットワーク・トラフィックはますます多くなり、ポリシーやプライバシー上の理由から、復号化したがらない顧客が増えています。さらに、攻撃者の側でも、ネットワーク脅威検知を回避するために暗号化トラフィックを使用することが増えています。Arista NDR ソリューションは、実際のペイロード自体を調べることなく、暗号化されたデータから推論して、この傾向に対抗することができます。これを実現するのが、トラフィックの性質や通信を行っているアプリケーションを識別する暗号化トラフィック分析です。残念ながら、Darktrace はオープンソースの JA3 ライブラリを利用しているため、この機能は限定的で、結果的にかなりの疑わしいアクティビティを見逃す可能性があります。

キャンペーン分析の自動化

ありArista NDR 自動インシデント・トリアージでエンティティ、 キルチェーン・アクティビティ、時間を相関付け		なしDarktrace

現在、ほとんどの攻撃には複数のデバイスと多数のアクションが関わっています。最終目的を達成するため、攻撃者は通常、エンドポイントからサーバーなど、ネットワーク内を移動します。多くのセキュリティ・ソリューションでは、セキュリティ・アナリスト自身が手動でこのような点と点を結ぶ必要があります。Arista NDR ではエンティティ中心の時系列状態を参照できるので、「Situations」機能で時間やプロトコルから点と点を統合し、相関付け、結ぶことができます。この機能により、アラート疲れが減り、セキュリティ・チームが情報をアクションに活かせるようになります。対照的に、Darktrace の IP アドレスに基づく相関付けはきわめて限定的で、検出したアクティビティを個別のアラートとして扱うので、攻撃キャンペーンに関するストーリー全体を把握できません。

クエリ言語と脅威検出

ありArista NDR インシデント、セキュリティ・ナレッジ・グラフ、アクティビティ、 生のパケット・データについて問い合わせることができる 拡張可能なプログラミング言語		限定的Darktrace BRO ログを利用したエラスティック・サーチ

Arista NDR は、インシデント、セキュリティ・ナレッジ・グラフ、アクティビティ、生のパケット・データについて問い合わせることができる拡張可能なプログラミング言語という強みを持っています。

単一のクエリで時間やプロトコルから動作の複雑な組み合わせを識別し、それによってエンドツーエンドの攻撃者 TTP を識別できます。すべてのクエリと脅威検出は、保存して今後の自動検出に利用することができます。Darktrace は、BRO ログを利用したきわめて限定的なエラスティック・サーチ機能を提供しています。

完全なデジタル・フォレンジック

✓あり		✓あり
継続的パケット・キャプチャ		全パケットのフォレンジックは限定的

明らかな脅威がない場合でも、Arista NDR はフォレンジック・エビデンスと履歴レコードを提供します。これにより脅威検出が可能になり、脅威発生後に必要なエビデンスが得られます。Darktrace は全パケットをキャプチャしていないので、このような履歴に基づく観点を提示できません。

展開と拡張性

ネットワーク脅威検知・対応プラットフォームは、ネットワークのあらゆる部分に到達して不可欠な情報を収集する必要があります。また、今日の多くのセキュリティ製品と同様に、単独で動作すべきではありません。

展開に関する考慮事項

✓あり		🕒限定的
生み出されたアーティファクトを利用して、 必要なセンサーの数を最小限に抑える		広範囲にカバーするために 多数のネットワーク・センサーが必要

Darktrace は、広範囲にカバーするために多数のネットワーク・センサーを必要とします。Arista NDR は、「生み出されたアーティファクト」を利用して、必要なセンサーの数を最小限に抑えています。この重要なイノベーションは、多くの通信によって副次的に生み出されるネットワーク・アーティファクトを利用します。その結果、Arista NDR は必要なネットワーク・センサーの数を最小限に抑えることができます。たとえば、データ・センターから発行された Kerberos チケットを観測し、詳細に解析すると、その通信を直接監視することなく、リモート・ネットワークのデバイス間のラテラル・ムーブメントのエビデンスを提供できます。

さらに、Arista 固有の機能として、既存の Arista ネットワーク・スイッチを使用してデータの監視やプリプロセシングを行い、Arista NDR Nucleus に転送して分析することができます。これらの重要なイノベーションにより、Darktrace と比べて、必要な専用ネットワーク・センサーやネットワーク・タップなどの数が大幅に減少します。

他のセキュリティ・ツールとの統合

✓あり		🕒限定的
SIEM や SOAR から EDR やネットワーク・パケット・ ブローカーまで、主要なセキュリティ・ソリューション・タイプを すべてカバー		

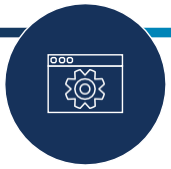
Arista NDR が提供する既存のセキュリティ・ツールとの広範囲にわたる統合機能は、難しい設定なしで使用できます。このセキュリティ・ツールは、ファイアウォール、ネットワーク・スイッチ、SIEM からオーケストレーション・ソリューション、エンドポイント検出・対応システムまで多岐にわたります。Darktrace の他のツールとの統合アプローチは、きわめて限定的です。

脅威インテリジェンスとの統合

✓あり		⊗なし
		

大部分の企業は、脅威インテリジェンスのフィードを外部ソースから入手しています。Arista NDR はこのようなフィードを利用して、継続的および遡及的に既知の侵害インジケーターを検出できます。Darktrace はこの機能をサポートしていません。

API

✓あり		限定的
豊富な API を文書化、サポート		

Arista NDR を利用する組織は、API を通じてこのプラットフォームの機能を拡張したり、カスタマイズしたりできます。顧客は Arista NDR プラットフォームを既存のセキュリティ・プロセスやビジネス・プロセスに組み込み、関連するコンテキストをプラットフォームに注入したり、プラットフォームから引き出したりすることが可能です。Darktrace のこの機能は限定的です。

まとめ

今日、市場には非常に多くの NDR プラットフォームがありますが、Arista NDR は Enterprise Management Associates（EMA）の最新のネットワーク・セキュリティ分析レポートで「バリュー・リーダー」に選出されています。Darktrace や他のソリューション・ベンダーと比較して、Arista NDR は機能とコストのバランスが最も優れていると評価されました。何よりも重要な点は、EMA のベンダー分析には、Arista NDR のセキュリティ・プラットフォームに高い価値を見出す実際の顧客からのインタビューや洞察が含まれています。

Arista NDR プラットフォームを利用して、組織は従来のセキュリティ・ソリューションでは見逃していた脅威を検知・検出することができます。このプラットフォームは、ネットワーク上のすべてのパケットを分析し、疑わしいアクティビティにフラグを立ててランク付けしつつ、デバイス、ユーザー、アプリケーション、およびそれらとやり取りしている相手を自動的に発見し、トラッキングし、プロファイルを作成します。そのため、セキュリティ・チームはそのアクティビティをすばやく調査し、必要な対応を行うことができます。

Arista NDR は、本当に信頼できる唯一の情報源であるネットワーク・データに人工知能を適用することにより、最新の脅威を見つけて対応するために非常に経験豊富な脅威ハンターのみが実行できる、時間のかかる手作業を自動化します。

出典

1. Gartner, Inc.、『Market Guide for Network Detection and Response』（2020 年 6 月）

アリスタネットワークスジャパン合同会社

〒100-0004 東京都千代田区大手町 1-7-2 東京サンケイビル 27F
Tel:03-3242-6401

西日本営業本部
〒530-0001 大阪市北区梅田 2-2 ヒルトンプラザウエストオフィスタワー 19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp

2023 年 9 月 8 日