Arista NDR

はじめに

ネットワークは従来のデスクトップやノート PC に加え、IoT デバイスや OT デバイス、クラウド、SaaS、Work-From-Anywhere、サプライチェーン、契約業者のデバイスなど、さまざまな機器をシームレスに接続するようになり、かつてないほど重要性を増しています。ハイブリッド・ワークの登場は、今日の企業の運営形態に多大な柔軟性と選択肢をもたらしました。ハイブリッド・ワークにはマルチクラウドとマルチデバイスのコラボレーションが欠かせないため、新しいネットワークには真にエッジレスであることが求められます。しかし残念ながら、これまでのネットワーク・セキュリティは、この強力な「新しいネットワーク」に追い付いていません。その結果、多くの組織が、セキュリティ運用の過大なコスト、長期間の攻撃による大きな影響、被害を受けたネットワーク内でのアクセス、攻撃見逃しのリスクの増加といった問題に直面しています。

セキュリティ対策を事後対応型から事前対応型のアプローチへと転換し、データ侵害が生じる前に脅威を確実に検知する、コンテキスト対応の継続的なネットワーク監視を行う必要があります。アリスタのゼロトラスト・ネットワーキング原則は、NIST 800-207 の規定に従い、企業における脅威の状況を 360 度完全に可視化して制御することに重点を置いた、事前対応型のセキュリティ・エコシステムの構築を支援します。

Arista NDR は、この戦略の重要な構成要素であり、ネットワーク脅威の検知と対応、デジタル・フォレンジック、脅威検出といった領域の課題解決に力を入れています。受賞歴のあるこのプラットフォームは、非マルウェア攻撃や内部脅威への対策から、フォレンジック調査の実行まで、お客様の幅広いユースケースに対応します。

背景

近年は、検出が難しい次のような脅威ベクトルを使用した攻撃による侵害が増えています。

- 攻撃対象の環境内にある既存の正規ツール（Microsoft Office、リモート・アクセス・サービスなど）を不正使用
- 内部アクセスを不正使用
- 人気のある Web サイトやネットワークの宛先を秘密通信チャンネルとして使用

また、セキュリティ予算への投資を増やしても、パブリック・クラウドとプライベート・クラウド、センサー、その他の IoT（モノのインターネット）デバイス、BYOD（私物デバイスの業務使用）、サードパーティ・サプライヤや契約業者のデバイスなどを含む「新しいネットワーク」は、把握するだけでも難しく、保護することはさらに難題になっています。

これらの課題を解決するには膨大な手作業と専門家の知識が不可欠ですが、そうしたリソースを見つけるのも維持するのも簡単ではありません。そこで必要となるのが、ネットワーク全体を可視化し、さまざまな脅威ベクトルを相関付けて悪意ある活動を把握し、正当な業務活動に紛れ込んでいる悪意をも自動的に検出して調査する、ゼロトラスト重視のプラットフォームです。これにより、経験豊富なアナリストが抱えている業務の負担を減らすと同時に、経験の浅いアナリストの生産性を大幅に高めることができます。

Arista NDR の位置付け

Arista NDR は、複雑な不正行為を迅速に検出して相関付け、脅威の調査とインシデント対応をサポートします。さらに、長い機械学習トレーニング期間と運用のオーバーヘッドを必要とせずに稼働を開始できるため、短期間で価値を創出できます。

Arista NDR は、数十億のネットワーク通信を分析して、新しいネットワーク（境界、コア、IoT、およびクラウドのネットワーク）に存在するすべてのデバイス、ユーザー、アプリケーションを自律的に検出し、プロファイル化と分類を行います。この攻撃対象領域に関する深い理解に基づいて、これらのエンティティを出入りする脅威を検出し、迅速な対応をするために必要なコンテキストを提供します。

この分析は、「新しいネットワーク」にまたがってディープ・パケット・インスペクションを実行する AVA Sensor から始まります。これらのセンサーは、物理ハードウェア、仮想、クラウドベースなど、さまざまなフォーム・ファクタで提供され、現在はアリスタのキャンパス・スイッチにも搭載されています。

センサーから抽出されたアクティビティ・データは、オンプレミスまたはクラウド上の AVA Nucleus に読み込まれます。この構成要素は、複数の検出モデルを組み合わせて悪意を検出します。多次元機械学習（ML）を使用して、複雑な敵対行為をモデル化し、エンティティ、時間、プロトコル、および攻撃ステージに見られる点と点を結んで脅威を検出します。前世代のネットワーク検出対応ツールとは異なり、このアプローチは、誤検知と検知漏れの少ない脅威検出を実現し、トリアージ、インシデント対応、修復に必要なコンテキストを提供します。

また、Nucleus は、環境内の他の IT およびセキュリティ・ソリューションと連携することで対応と修復の自動化を提供できます。

Arista NDR の根底には、企業のゼロトラスト・セキュリティ戦略を可能にする 3 つの主要イノベーションがあります。

- EntityIQ™は、新しいネットワーク上のすべてのデバイス、ユーザー、およびアプリケーションを識別、プロファイル化、追跡する、世界で唯一の人工知能ベースのセキュリティ・ナレッジ・グラフです。
- AVA™は、機械学習、脅威インテリジェンス、および体系化された専門家の知識を使用して自律的なトリアージと調査を実行するとともに、データをお客様のインフラストラクチャ内に保全する、世界初のセキュリティ・エキスパート・システムです。
- Adversarial Modeling™は、EntityIQ™のヒューリスティック分析を使用して攻撃者をその意図に基づいて識別する、こちらも業界初の機能です。Arista NDR は、攻撃の特定の兆候のみを探すのではなく、悪意を認識することで、攻撃者、特に悪意を持ちながら正当な活動に紛れ込んでいる攻撃者を発見して阻止する能力を大幅に向上させます。この機能を利用して、社内のセキュリティ・アナリストが組織固有の脅威を検出する独自機能を構築することもできます。

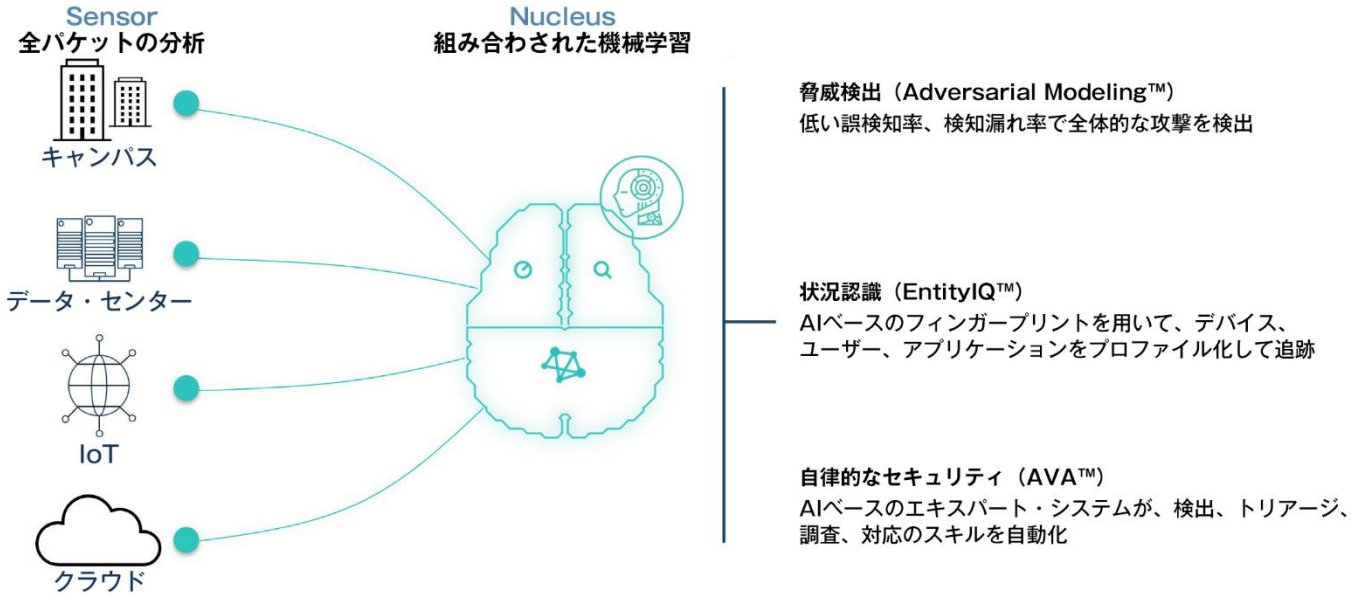


図 1：Arista NDR を支える 3 つの主要イノベーション

お客様のメリット

- 検出時間と対応時間の短縮：Arista NDR のお客様は、攻撃の検出に要する時間と対応に要する時間を最大 88%短縮し、環境の状況認識を平均で 3 倍向上させています。
- 誤報の低減：Tolly Group[1]による独立した比較試験で、Arista NDR は検知漏れ率が最も低く、重大な脅威を見逃さないことが証明されています。SN 比は 95%に達し、これは競合製品の約 15 倍に当たります。つまり、誤ったアラートを大量に生成してアナリストの仕事を増やす競合ソリューションとは異なり、Arista NDR は日々の運用コストを大幅に削減することができます。
- 迅速な調査： Tolly の調査レポートは、NDR プラットフォームが迅速な修復に必要なコンテキストと情報を調査ワークフローに提供する点に注目し、脅威の検証においてもクラス最高と評価しています。
- 暗号化トラフィック分析：Arista NDR は、市場の他のソリューションよりも詳細にデータを解析します。トラフィックが暗号化されている場合でも、全ネットワーク・パケットを分析して、データ・サイエンスに基づく推論を行います。
- 迅速な立ち上げ：重要なのは、プラットフォームを 30 分以内に立ち上げることができ、エンドユーザーのデバイスや
- インフラストラクチャの他の部分に影響を及ぼさないことです。これらの指標に基づき、Kuppinger Cole[2]などの分析会社は、Arista NDR をこの重要なセキュリティ技術分野のリーダーと評価しています。

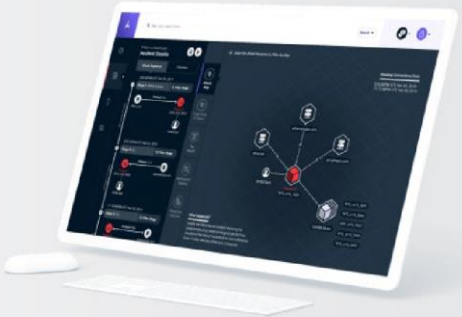
主なユースケース

Arista NDR は、新しいネットワークの状況認識、脅威検知とインシデント対応、脅威検出、フォレンジックなど、さまざまなユースケースをサポートします。

図 2：Arista NDR で解決する主なユースケース

[1] https://awakesecurity.com/white-papers/tolly-test-report-darktrace-enterprise-immune-system-vs-awake-security-platform/

[2] https://www.arista.com/assets/data/pdf/Analysts/



ケース・スタディ：機密が話される場所での IP 電話の盗聴

背景：

米国のある大手消費者金融機関は、Arista NDR を使用して、ネットワーク上に 17,000 台以上ある IP 電話のうち 4 台が、悪意のある内部関係者によって電子的に盗聴されていることを突き止めました。

課題：

この組織の大規模なセキュリティ・チームは、既存のセキュリティ制御では IP 電話を可視化できないことに悩んでいました。この IP 電話は社外とのやり取りにのみ使用されるもので、大量のトラフィックが外部ソースと交換されることは珍しくありません。しかし、少数の IP 電話が特定の疑わしい宛先にデータを頻繁にアップロードしている状況は、普通とは言えません。

解決策：

Arista NDR がこのアクティビティを見つけるために実施した分析は、これらのデバイスの現在と過去の動作の単純比較ではありません。このケースでは、Arista プラットフォームを導入するずっと前にデバイスが侵害されていたので、

基本的な異常分析では、悪意のある活動も、過去に観測した活動と変わりがないため「正常」と判断されてしまった可能性があります。それに対して、Arista NDR は、まず類似する動作フィンガープリントを持つデバイスをすべて特定し、次にこれらのデバイスを相互に比較しました。その結果、標準から外れている 4 台のデバイスが見つかりました。さらに、暗号化されたトラフィックの分析から、通信の送信元と宛先をプロファイル化し、その情報を脅威評価に組み入れることができました。

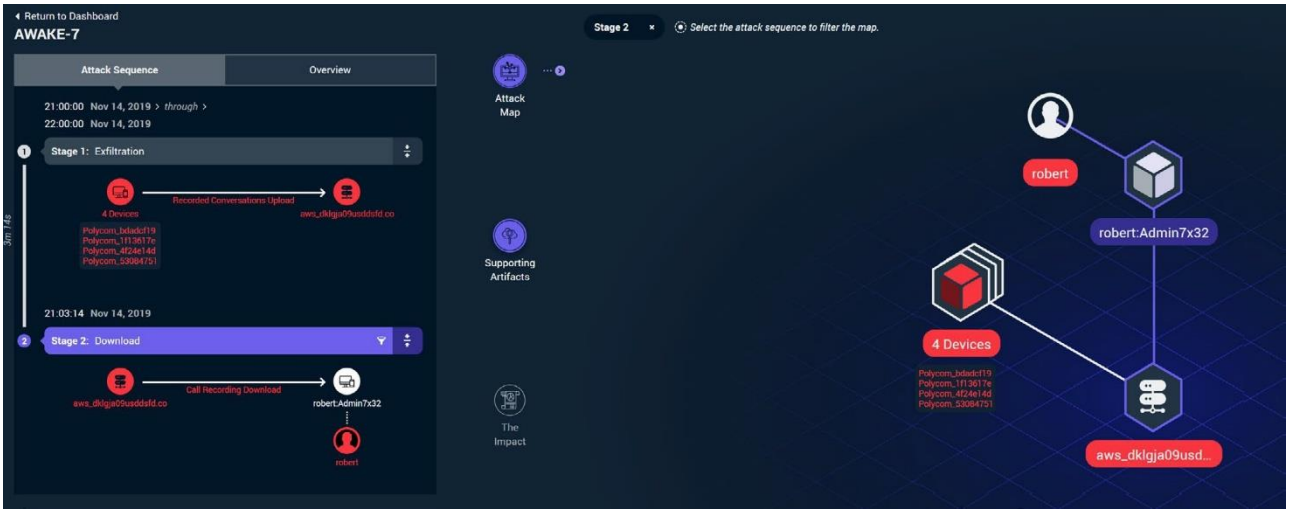


図 3：Arista NDR で内部脅威の多段分析を実行

結果：

セキュリティ・チームは、IT 部門の従業員の 1 人がこの攻撃に関与していたことを突き止めました。この人物は、収集した情報を恐喝や身代金目的に利用しようとしていました。このプラットフォームの分析により、セキュリティ・チームは、会社の機密事項が話されることの多い役員会議室などの場所に設置された電話が侵害されていたことを迅速に発見できました。Arista NDR で獲得した詳細な情報に基づいて、同社はこうしたアクティビティを即座に阻止し、法的措置に必要な証拠を得ることができました。

Arista NDR の利点

このプラットフォームは、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プロファイル化します。そして、経験豊富な脅威ハンターが行うように、プラットフォーム・モデルが攻撃者の戦術、手法、手順を見つけ出して可視化します。Arista NDR では、時間、エンティティ、プロトコルという多次元の点を自律的に結び付けられるため、セキュリティ・アナリストは単なる個別のアラートだけでなく、攻撃の全体像を把握できます。その後、アナリストは関連する調査や修復のオプションをすばやく、高い精度で開始できます。

より質の高いデータ・ソース ➔ より高精度の結果

Arista NDR は、セキュリティ・アナリストが、セキュリティ・アナリストのために開発した製品です。したがって、このプラットフォームは、アナリストの仕事を増やさないことに重点を置いています。他のプラットフォームの場合は、発行されたアラートをセキュリティ・チームが選別し、有害な問題か、無害な問題あるいは誤検知かを見分ける必要がありますが、Arista NDR は、悪意を示す有力な証拠がない限り、問題にフラグを付けません。そのために重要となるのが、パケット・ヘッダーや NetFlow だけでなく、可能な限り詳細なデータを取り込むことです。

他の NDR ソリューションは、プロトコル・ヘッダーや NetFlow 情報など、レイヤ 3 と 4 のメタデータを主に処理します。レイヤ 7 までの全パケット・データははるかに量が多く、リアルタイムで処理するのが難しいからです。しかし、その大量のデータが提供する大量のシグナルは、検出精度の向上とエンティティの追跡に役立ち、さらに、このソリューションを大規模で複雑なネットワークへと拡張するために役立ちます。たとえば、Kerberos パケットが提供するユーザー情報のようなシグナルは、プロトコル・ヘッダーや NetFlow には含まれません。全パケットは、アクティビティの理解や、アクティビティ・レコードの保存にも役立ちます。これはネットワーク上のエンティティ間で発生する実際のトランザクションであり、意味のないプロトコルのビットやバイトではありません。このフォレンジック・データにより、プラットフォームと調査者は過去にさかのぼり、最初の発生時には見過ごされていた悪意ある動作を検出できます。アクティビティ・レコードは、全パケット・データよりもストレージ・フットプリントが大幅に小さいことも重要です。

Arista キャンパス・スイッチ上の AVA Sensor を使用すると、元のデバイスにさらに近いところでこの分析を実行でき、非 NAT トラフィックや送信元 IP アドレスなどを観測できるという利点があります。リーフ・スイッチ上のこのディープ・パケット・インスペクション機能は、実際のアクティビティから複数ホップ離れた境界に配置されたネットワーク・セキュリティ・デバイスよりもはるかに効果的に、ラテラル・ムーブメント、認証情報の悪用、およびその他の East/West の脅威を検出できます。また、キャンパス・スイッチに展開できる Arista の機能により、別のネットワーク・セキュリティ・ハードウェアを追加することなく NDR 機能を提供でき、運用コストと労力を削減できる点も重要です。

インテグレーション

Arista NDR は、業界最高水準の SIEM、ビジネス・インテリジェンス、チケッティングと分析、エンドポイント検出、およびセキュリティ・オーケストレーション・ツールを既存のソリューションに統合し、それらを強化します。また、ワークフローとインテグレーションをカスタマイズするための完全な API もサポートしています。たとえば、SIEM が統合されると、それまで IP アドレスまたは電子メールアドレスが含まれるアラートを頼りにしていたアナリストは、関連するユーザーとロール、オペレーティング・システムとアプリケーションの詳細が含まれるデバイス・プロファイル、フォレンジックな脅威タイムライン、およびキャンペーン分析用のデバイスのリストが使えるようになります。同様に、エンドポイント統合によって、1 回のクリックで侵害デバイスを隔離したり、エンドポイントのフォレンジック・データを取得したりすることが可能になります。

高度なデータ・サイエンス

従来のデータ・サイエンス・アプローチは、最新のネットワークの規模と多様性に対応するうえで重大な課題を抱えています。人工知能（AI）モデルの有効性は、モデルのトレーニングに使用するラベル付きサンプルの有効性に左右されます。しかし、今日の最も単純なネットワークでも、データの量と条件の種類が多いため、有効なラベル付けが十分に行われていません。さらに、脅威の急速な進化など、さまざまな要因でラベル自体がすぐに古くなり、頻繁な再トレーニングとその運用コストが必要になるという問題があります。これらの課題を克服したとしても、結果として得られるモデルはほとんどが巨大でモノリシックで不透明なものであり、動作が遅く、説明可能でないため、あまり役に立ちません。これはつまり、人間のアナリストが結果を見たときに、ネットワークまたはセキュリティの問題としてフラグが付けられても、その理由を理解できない、ということです。その結果、与えられた情報に対して、次に何をすべきかわからない状況が発生します。

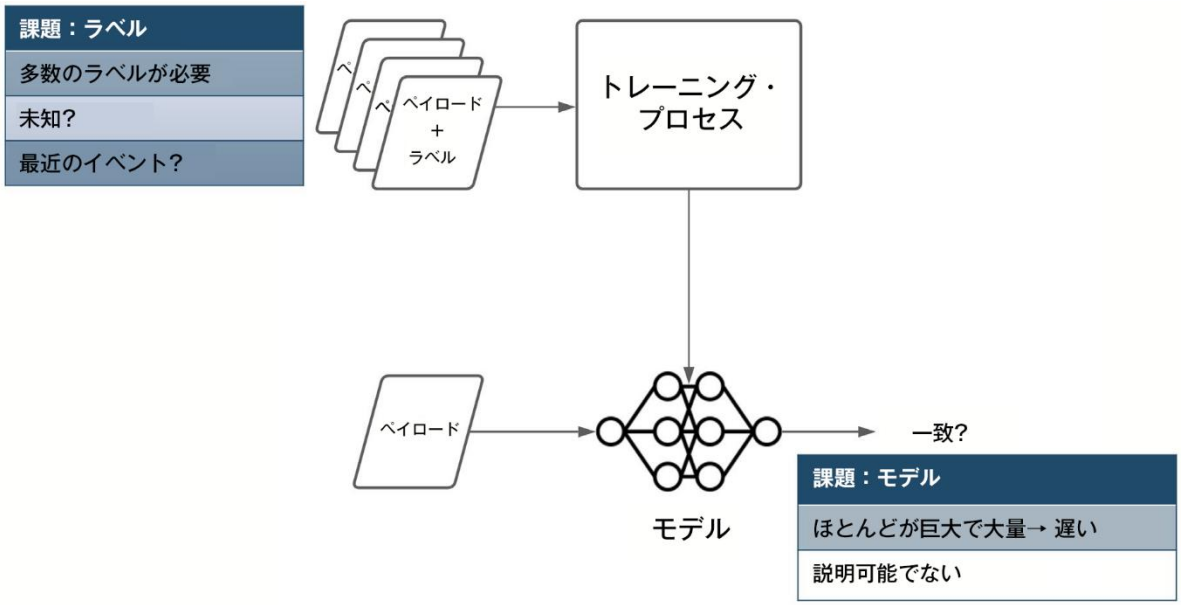


図 4：ネットワーク・セキュリティに対する従来の AI アプローチの課題

競合ソリューションの多くは、主に教師なしの学習を使用して、「正常」の基準から外れた異常を検出します。しかし、悪意のない異常を検知する誤検知や、逆に、以前から存在する侵害を「正常」と想定して見逃す検知漏れがよく発生します。リスクと隣り合わせのまま気付かない状況が続くという意味では、検知漏れの方がより危険です。

それに対して Arista NDR は、まず正常の状態、つまり各ネットワークの普段の状態を学習します。多くの場合、これには電子メール、パッチ適用、さらには部門やワークグループ固有のアプリケーションの使用などのトラフィックが含まれます。AVA モデルをトレーニングするために、この種のネットワーク動作を示すラベルが豊富に用意されています。前述した従来のアプローチが「悪いトラフィック」の特徴を学習しようとするのに対し、Arista NDR はまずネットワーク・データという干し草の山から大半の干し草を取り除く作業を行います。その後、かなり小さくなった干し草の山から、目指す針を探します。

Arista NDR は、エンティティの動作が時間の経過とともに変化する場合に、異常な動作の識別と特定を支援します。そのために、1 回限りの「トレーニング用」の静的スナップショットに頼るのではなく、普段の「正常」な状態を継続的に学習します。データ・サイエンスに対するこの独自のアプローチは、前世代のアプローチの課題を克服します。その筆頭がナレッジ・グラフを提供する EntityIQ™です。このプラットフォームで使用するデータはまず、パケットをユーザーに、または IP をデバイスやアプリケーションなどに変換する技術で処理されます。両者の関係は、EntityIQ でマッピングされます。これがナレッジ・グラフの中核となります。このグラフは、ヒューリスティックの形でドメインの専門家から得た知識と、人間のオペレーターからの継続的なフィードバックによって、繰り返し強化することができます。ナレッジ・グラフのサイズは未加工のフィーチャーよりも大幅に小さいため、追加の AI アプローチを繰り返し適用できます。

これにより、優れた AI 分析が可能になるだけではありません。従来の ML モデルとは異なり、Arista NDR では、アルゴリズムの出力を現実世界のエンティティとその特性として取得できます。この人間が読んで理解できる出力により、次の手順をアナリストに明確に示す説明可能な AI がもたらされます。

アリスタは、人工知能を目的達成のための手段と考えています。この場合の目的は、お客様のセキュリティの成果を向上させることです。そこで、このプラットフォームでは、最終目的を達成するためのさまざまなデータ・サイエンス手法を使用しています。たとえば、次のようなものです。

- 悪意のあるドメインと疑わしいドメインの識別など、分類のためのディープ・ニューラル・ネットワークを含む、教師なし、教師あり、および連合機械学習アルゴリズムの組み合わせ
- 暗号化トラフィック分析などを用いた、分類のための意思決定ツリー
- エンティティ追跡のための多次元クラスタリング

- 異常を特定するための異常値検出
- リスク・スコアリングのための確率伝播法
- トピック・モデリングと自然言語処理。これにより、人間の専門調査者が行うのとほぼ同じ方法で、オープンソース・インテリジェンスと脅威調査を自動的に実行します。

暗号化トラフィック分析のための機械学習

近年のネットワーク・トラフィックは大部分が暗号化されており、ポリシーやプライバシー上の理由から、復号化を避けようとする組織が増えています。たとえば、TLS 1.3 を利用すれば、従来の方法でネットワーク・トラフィックを傍受して復号化することは困難になります。攻撃者の側でも、ネットワーク検出を回避する手段として暗号化トラフィックを使用することが増えています。事実、Gartner によると、現在の悪意あるトラフィックの 70%以上が暗号化されています。

Arista NDR は、データ・サイエンスに基づく暗号化トラフィック分析を行い、プライバシーとポリシーの制約の範囲内で、セキュリティ・チームに有益な情報を提供します。よくあるユースケースは、通信しているアプリケーションの種類や、回線を通過するトラフィックの性質を特定することです。たとえば、暗号化されたファイルが Web 会議セッションで転送されるのは問題ないかもしれませんが、そのファイルが PowerShell スクリプトから外部の無許可の場所に転送される場合は要注意です。

Arista NDR は、暗号化トラフィック分析を可能にするために、さまざまなデータ・サイエンス技術を使用します。たとえば、攻撃者の TTP に関連するアクティビティのパターンを特定するために、教師ありの ML を使用します。これにより、コマンド・アンド・コントロールに使われるリモート・アクセス・ツール、リバース・シェル、不正なアプリケーションを特定します。さらに、データ流出などに使われているドメインを、レピュテーションの有無やレベルに関係なく特定することが可能です。また、ディープ・ニューラル・ネットワークと意思決定ツリーを使用して、暗号化されたセッションをトラフィックの性質（インタラクティブ・シェル・セッション、Web ブラウジング、ビデオ会議、ファイル転送など）に基づいて分類します。

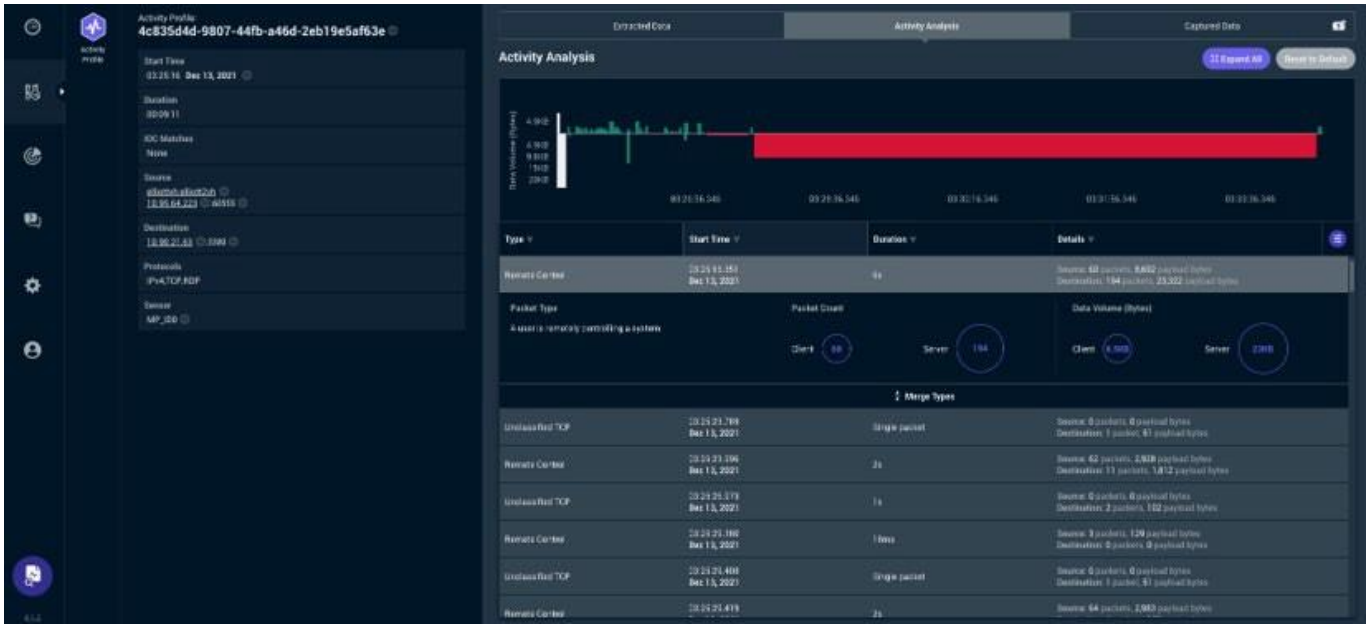


図 5：暗号化トラフィック分析で、Remote Desktop Protocol（RDP）を使った不正なリモート制御を特定

オンデマンドの専門家の知識

アリスタの Awake Labs は、それぞれの組織のセキュリティ耐障害性とインシデント対応のニーズに合わせて調整された、包括的なセキュリティ戦略、運用、アドバイザリーのソリューションを提供します。この専門家チームは、セキュリティ対応について長年の経験を有し、世界でも特に重大な侵害行為への対応や、大規模なセキュリティ・カンファレンスでの講演およびトレーニングを行っています。したがって、Awake Labs を利用するお客様は、実践的なインシデント対応スキル、経営管理の経験、戦略的なビジネス感覚を併せ持つ専門家から、直接アドバイスを受けることができます。

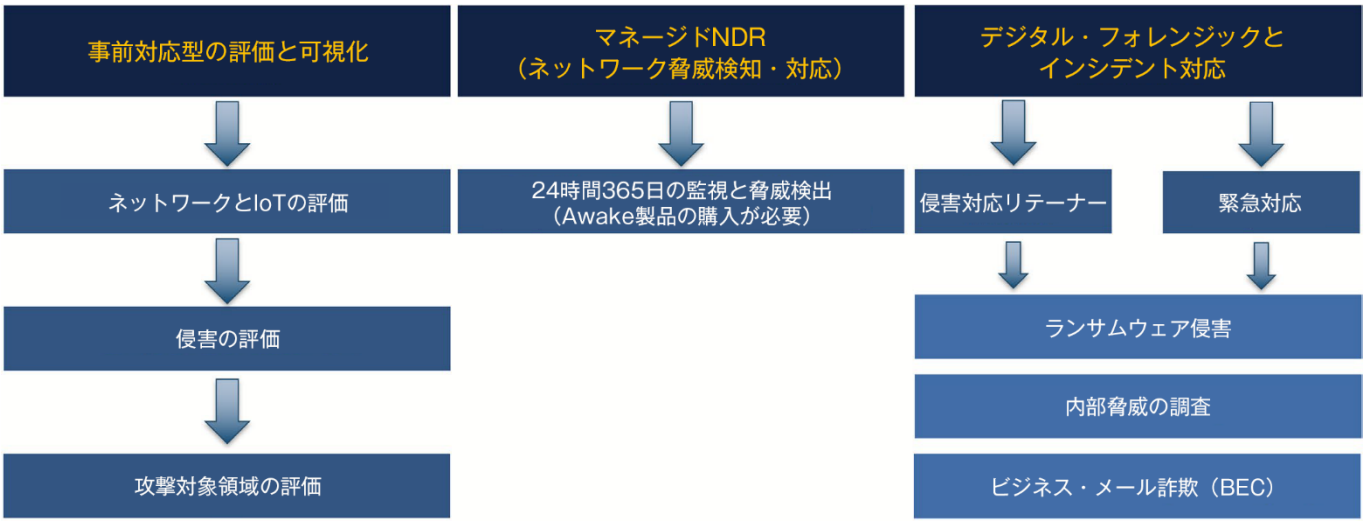


図 6：専門家の知識で、インシデント対応やマネージド脅威検出などお客様のニーズをサポート

この専門家チームは、ネットワークについての事前対応型のセキュリティ評価を行い、お客様の組織の攻撃対象領域の把握、今後起こり得る侵害への準備状況の評価、既に侵害を受けていないかの判定を支援します。長年にわたる最前線のインシデント対応経験を持つこれらの専門家は、ランサムウェア、内部脅威、ビジネス・メール詐欺など、さまざまな侵害行為による被害の軽減と阻止をサポートします。最後に、Awake Labs は、24 時間 365 日の監視と脅威検出を行うマネージド NDR サービスも提供します。

Awake Labs のサービスを利用して、コア、境界、クラウド、IoT、IT、OT のネットワークに対する事前対応型の脅威検出および監視を行うことにより、お客様のリスク対策を強化できます。これにより、ニッチなセキュリティ専門知識を持つ熟練したリソースを独自に雇用および維持するためのコストを削減できます。また、組織の重要な資産を標的とする脅威の優先順位付けは Awake Labs が行うため、既存のチームは組織の主要業務に専念できます。お客様は、ネットワークの調査と修復のための業界最高水準のプレイブックとオンデマンドの専門知識を利用することにより、継続的なセキュリティ運用コストを削減でき、影響を軽減できます。

複合的なイノベーションでお客様のセキュリティ成果を強化

アリスタは、さまざまな角度から NDR プラットフォームを支えるイノベーションに取り組んでいます。その 1 つは、プラットフォーム内に組み込まれた人工知能をより幅広いデータ・ソースに適用し、オペレーショナル・テクノロジー・デバイスや、クラウド、SaaS アプリケーションからのデータに対応できるようにすることです。これにより、デジタル資産がどこにあるかに関係なく、すべてのデジタル資産における検出と対応が実現されます。

もちろん、データを有効に活用するには優れたデータ・サイエンスを適用する必要があります。前述のように、アリスタは、データ・サイエンスのセキュリティへの適用において、既に多くの新分野を開拓しました。その後も引き続き、暗号化トラフィック分析、準教師ありモデル、自然言語処理、トピック・モデリングなどの分野に投資しています。その結果、このプラットフォームは平凡な作業と高度なスキルを必要とする作業の両方を減らし、お客様のアナリストの活動をさらに強化するものになっています。このプラットフォームを利用すれば、アナリストはデータの収集と分析ではなく、意思決定に集中できます。

アリスタの AI ドリブン型のアプローチは、攻撃者の戦術、手法、手順の進化にも重きを置いています。たとえば敵対行為のモデル化などのイノベーションによって、攻撃の中核的要素を検出し、大事に至る前に攻撃を特定します。これにより、お客様はインシデントを迅速に特定、解明、阻止、修復し、侵害の影響を抑えることができます。アリスタは、この目標を達成するために、攻撃者の戦術の進化を継続的に追う脅威研究チームにも多額の投資を行っています。

最後に、ユーザー・エクスペリエンスのイノベーションも大きな重点分野です。アリスタは、経験の浅いレベル 1 のアナリストと、レベル 3 のアナリストや脅威ハンターとでは、セキュリティ・テクノロジーの活用方法が大きく異なることを認識しています。その考え方に基づき、アリスタはロールに応じたユーザー・エクスペリエンスとワークフローのイノベーションを継続的に進めています。単に人間が理解するためのデータを出力するのではなく、ユーザーの視点やニーズを念頭に置いて、わかりやすいストーリーボードとダッシュボードを提供します。

まとめ

Arista NDR は、AI ドリブン型のテクノロジーと、必要に応じて利用可能なセキュリティ専門家によるサポートを独自に組み合わせて提供します。このプラットフォームは、ランサムウェア、サプライチェーン、IoT 攻撃、インサイダー攻撃の初期兆候など、さまざまな脅威の特定を支援します。また、対応に必要なコンテキストを提供することで、迅速かつ効果的な修復を可能にします。 さらに、これらの機能は既存の Arista スイッチング・ファブリックを介して提供できるため、IT およびセキュリティ・チームの運用上の負担を軽減できます。

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

Copyright © 2023 Arista Networks, Inc.
Arista のロゴ、および EOS は、Arista Networks の商標です。その他の製品名またはサービス名は、他社の商標またはサービス商標である可能性があります。

2022 年 7 月 11 日 02-0098-02