Arista DANZ Forensic Exchange で実現する、インテリジェントな可観測性とセキュリティ運用

ドキュメント・バージョン 1.0

はじめに

この 10 年間、多くの組織がデジタル・インフラの変革を進めてきましたが、コロナ禍によるリモートワークの普及で、この流れはさらに加速しました。結果として、デバイスや接続の種類や特性が多様化しただけでなく、アーキテクチャの観点からもネットワークが拡大し、これまで境界と認識されていたものは、もはや意味のあるセキュリティ境界ではなくなりました。さらに、近年途切れることのないサイバー攻撃が、企業をゼロトラスト・アーキテクチャへと向かわせています。従来のネットワーク監視ツールや脅威検知・対応ツールは規模の拡張が難しく、こうした最新の課題についていくことができません。レガシー・ソリューションはオール・オア・ナッシングの手法に依存しており、お客様独自のリスク・プロファイルに基づく可視化をキュレーションするのは困難です。スケーラビリティにも制限があり、きめ細かな脅威検出を行うための自律的な（AI/MLドリブン型の）インテリジェンスはなく、全社に展開するには桁違いの投資支出と運用コストが必要になる傾向があります。その結果、この「新しいネットワーク」と、それが表す攻撃対象領域の大部分を把握できない状況にある企業が増えています。

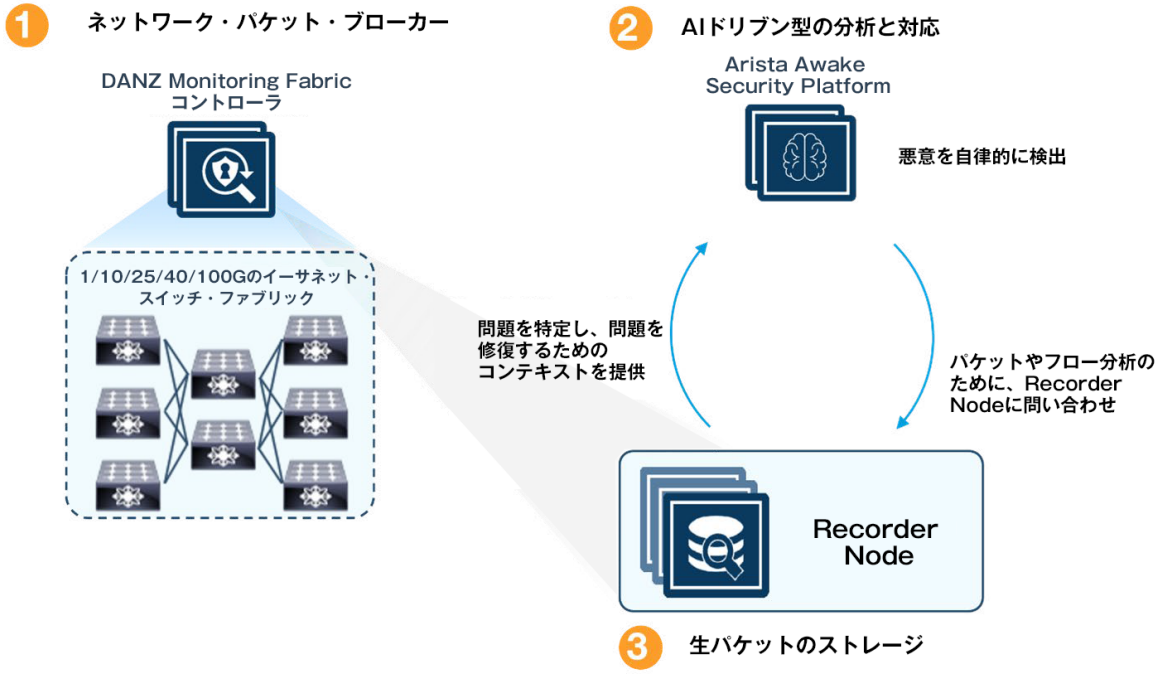
アリスタの DANZ Forensics Exchange（DFX）ソリューションは、現代の新しいネットワークにおいて、組織全体をカバーする可観測性と脅威検出・対応を可能にします。このスケールアウト・ソリューションはさまざまなフォーム・ファクタで提供されるため、組織はオンプレミス、ハイブリッド、およびクラウドベースのインフラを監視できます。たとえば、エンタープライズ・データセンターでは、DFX ソリューションのスケールアウト・アーキテクチャを、垂直型（ユーザー対アプリ）のトラフィックに適用するほか、最大 5 倍のトラフィック増強を必要とする水平型（アプリ対アプリ）のトラフィックにも適用します。データセンター・ネットワークのリンク速度は 10G/40G から 25G/100G に移行していますが、DFX の高性能設計はあらゆる帯域幅をサポートしており、アーキテクチャ上は、今後提供される 100G/400G の速度にも対応しています。また、監視対象のネットワーク・プロトコルとシステムを、組織の要件に適した設定へと簡単にキュレーションできます。

これにより、現在と過去のイベントを包括的にカバーすると同時に、組織のアナリストに意思決定のサポート・データを提供することが可能になります。その結果、ソリューション展開の初期費用と継続的な運用コストの両方を最小限に抑えられます。

DFX ソリューションは、エンドユーザーの幅広いユースケースに対応し、ネットワーク・パフォーマンス監視と AI 運用から、AI ドリブン型の脅威ハンティング、検知、対応までを、単一ベンダーのソリューションで実現します。アリスタのオープンで文書化された API と、難しい設定なしで使えるインテグレーションは、IT インフラの他の部分でも利用でき、現在は人手に大きく依存しているアクションを自動化するのに役立ちます。また、お客様はアリスタの Awake Labs チームとつながり、このソリューションの 24 時間 365 日の監視や、脅威ハンティングおよびインシデント対応に関する専門的なアドバイスを得ることができます。

ソリューションのアーキテクチャ

デジタル変革は、今の社会で組織が競争に打ち勝つための鍵を握っています。デジタル変革への道を歩み始めると、データセンターの規模、帯域幅、トラフィックが急に増大するとともに、データセンターのパフォーマンス、セキュリティ、整合性を保証するために、広範なネットワーク・オブザーバビリティの実現が急務になります。セキュリティ脅威は増加し続けているので、ビジネス・ニーズを満たすアプリケーションのパフォーマンスを確保することは非常に重要です。



独自のデータセンターを運用する組織や、独自の SaaS アプリケーションをホスティングする組織は、次の点を可視化することに苦戦しています。

- エンタープライズ全体のトラフィックの規模（高性能データセンターの水平型アプリ間トラフィックを含む）
- 高性能ネットワークのリンク速度（40G/100G や、最新の 400G など）
- そのインフラ上で動作しているサービスとアプリケーション
- インフラ内および外部との通信に使用されているプロトコル
- インフラにアクセスするユーザー、デバイス、アプリケーション

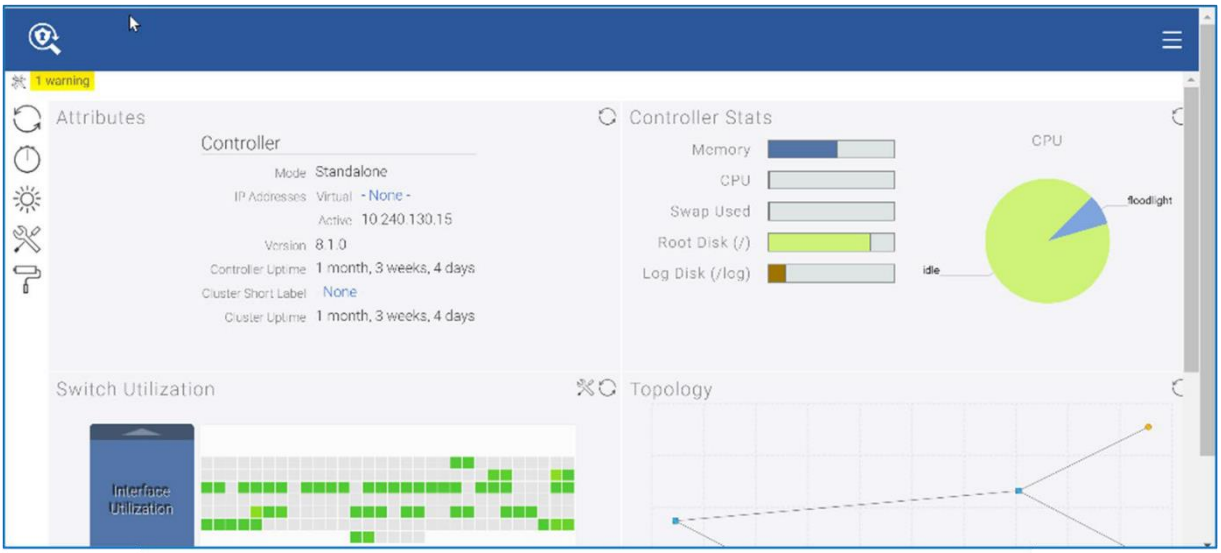
DFX ソリューションは、DANZ Monitoring Fabric（DMF）のネットワーク・パケット・フィルタリング、フォワーディング、ストレージ機能と、AVA を活用した Arista NDR プラットフォームの高度なネットワーク脅威検知・対応（NDR）機能を組み合わせたものです。拡張性と柔軟性に優れた DFX ソリューションは、ネットワーク、デバイス、ワークロード、アプリケーション、ユーザー単位での可視化を提供するとともに、自律的な脅威ハンティング、脅威検知、対応を実現します。このソリューションは高度なプログラミングが可能であるため、データセンター内の水平型トラフィックだけを監視するなど、特定の要件を満たす対象のみを監視できます。

アリスタの他にない強みは、可観測性、コンプライアンス、フォレンジック、脅威検知・対応のユースケースに適したデータセットをキュレーションできる最高水準の個別コンポーネントを、単一のソリューションにまとめて提供していることです。このソリューションは、オンプレミス、クラウド、ハイブリッド・クラウドのネットワークに展開でき、その環境内に現在展開されている複数のツールを統合できます。アリスタの管理対象サービスは、世界有数の侵害行為に対応してきたエキスパートなど、長年の経験を持つ専門家の知識に支えられています。

最新のデータセンターには、一元管理、ゼロタッチでの拡張、自動化を提供する、インテリジェントで俊敏性と拡張性に優れたセキュアな監視アーキテクチャが必要です。DFX ソリューションは、すべてのスイッチと Recorder Node を自動的に発見するゼロタッチ・ネットワーキング（ZTN）によって、これらを実現します。ユーザーがスイッチ上で設定する必要はありません。

監視されるネットワーク・トラフィックのソースは、スイッチの SPAN ポート（アリスタおよび他社製）、ネットワーク・タップ、sFlow IPFIX、仮想環境など、多岐にわたります。DMF コントローラは、ポリシーベースのフォワーディング設定を保持し、インフラ・コンポーネントに配布して、Awake Nucleus（中央セキュリティ分析ノード）と DMF Recorder（スケーラブルなインテリジェント・パケット・ストレージ）の両方で、目的とするトラフィックのきめ細やかな一元管理と監視を可能にします。リアルタイムのトラフィックはスイッチから Nucleus に直接転送され、Nucleus が AI ドリブン型手法を用いて数十億のネットワーク通信を徹底的に分析し、個々のデバイス、ユーザー、アプリケーションを検出、プロファイリング、分類します。Recorder Node は、インフラから提供されるデータを、DMF コントローラから配布されるポリシーの下で保存します。

Nucleus は API を通じて Recorder Node に直接統合され、コンプライアンス・レポートの作成や脅威ハンティングのために、全パケット・データを長期的に保存、分析できるようにします。これにより、Nucleus によって分析されたパケットを DMF 内に保存しておき、アナリストが調査中のエンティティに関するパケットをオンデマンドで取得することが可能になります。さらに Nucleus は、攻撃の封じ込めと軽減のために、Splunk や QRadar などの SIEM や、Sentinel1 や CrowdStrike などの EDR ソリューションといった幅広いネットワークおよびセキュリティ・インフラとのインテグレーションをサポートします。



プログラム可能な可観測性 – DMFコントローラ

DFX ソリューションのコンポーネント

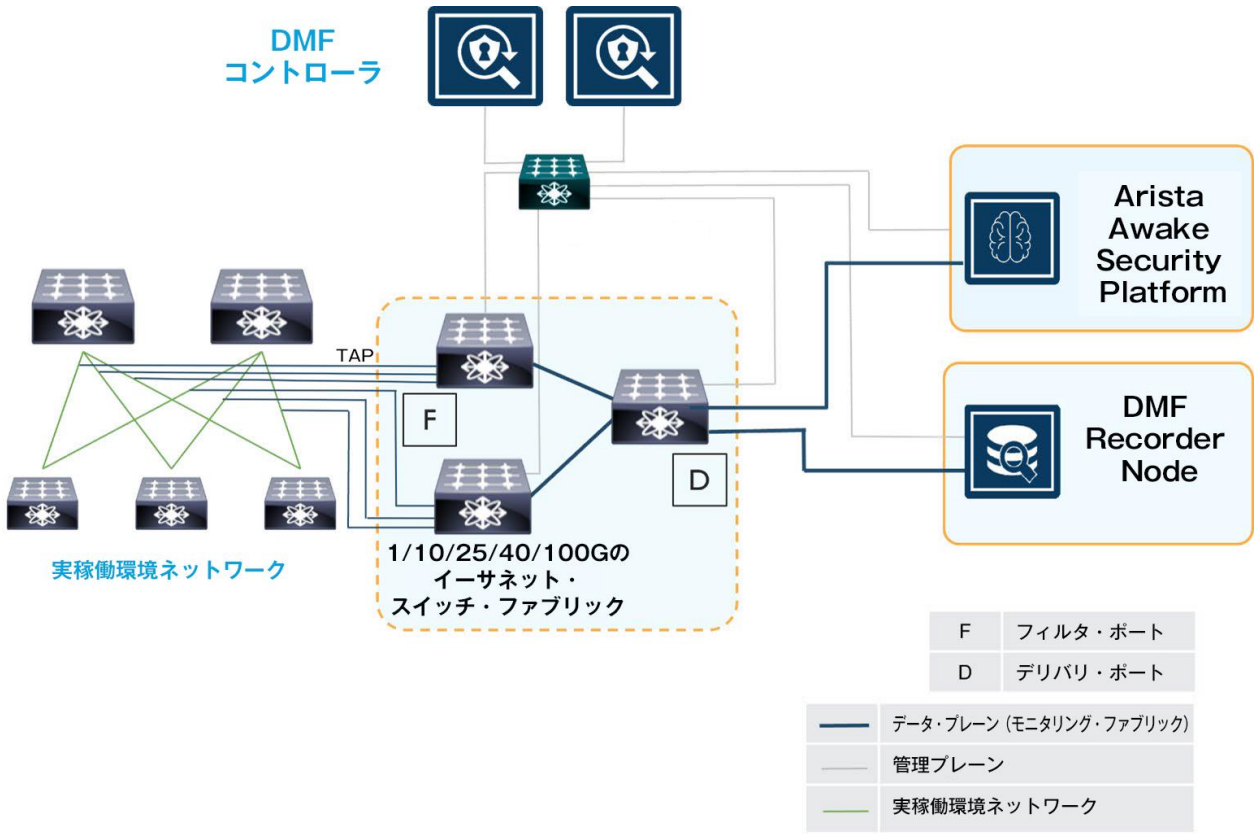
DFX ソリューションは、以下のコンポーネントで構成されます。

- DMF コントローラとスイッチのライセンス
- DMF Recorder Node（とオプションの Service Node および Analytics Node）
- AVA Nucleus

ハードウェアとソフトウェアのオプション

このソリューションで使用するハードウェアとソフトウェアのコンポーネントを以下に示します。

コンポーネント	ハードウェア/ソフトウェア
DMF コントローラ	ハードウェア・アプライアンスまたは VM ソフトウェア
Recorder Node	ハードウェア・アプライアンス
AVA Nucleus	ハードウェア・アプライアンス（分析する Mbps 単位のライセンス）

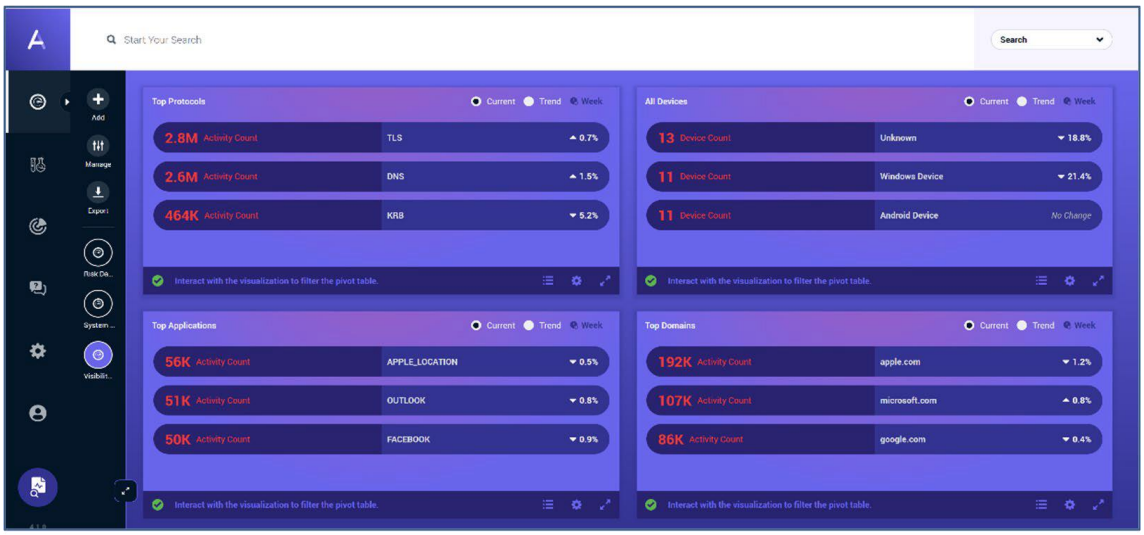


このソリューション・ガイドでは、生のネットワーク・データから可視化、セキュリティ分析までの運用ワークフローに重点を置いています。DMF コントローラは、ネットワーク・ファブリックのトラフィック・フィルタリング・ポリシーとフォワーディング・ポリシーの定義、配布、監視に責任を負います。オペレーターは、これを利用して組織の脅威モデルを考慮し、それに応じて適切なトラフィックがネットワークからモニタリング・ファブリック経由で AVA Awake Nucleus に流れるようにできます。

ワークフロー

ネットワーク・トラフィックは動的なもので、社内外の無数の宛先と通信するデバイス、ユーザー、IP アドレス、アプリケーション、サービス、ワークロードが含まれ、その混在具合も絶えず変化しています。Awake Nucleus はこれらの構成要素すべてを自動的に分析し、相関付け、統合して、わかりやすいフォーマットで結果を表示します。

Arista NDR のダッシュボードは、オペレーターにとって特に重要なデータを表示するようにカスタマイズ可能です。また、個人やグループのニーズに合わせて、用意されている多数のウィジェットから選択し、アレンジできます。ダッシュボードは、一般的なオペレーターの可視化ワークフローの出発点となります。たとえば、IT 運用の担当者は通常は可用性の確保や、業界や組織のポリシーへの準拠を保証するために、ネットワークを監視します。

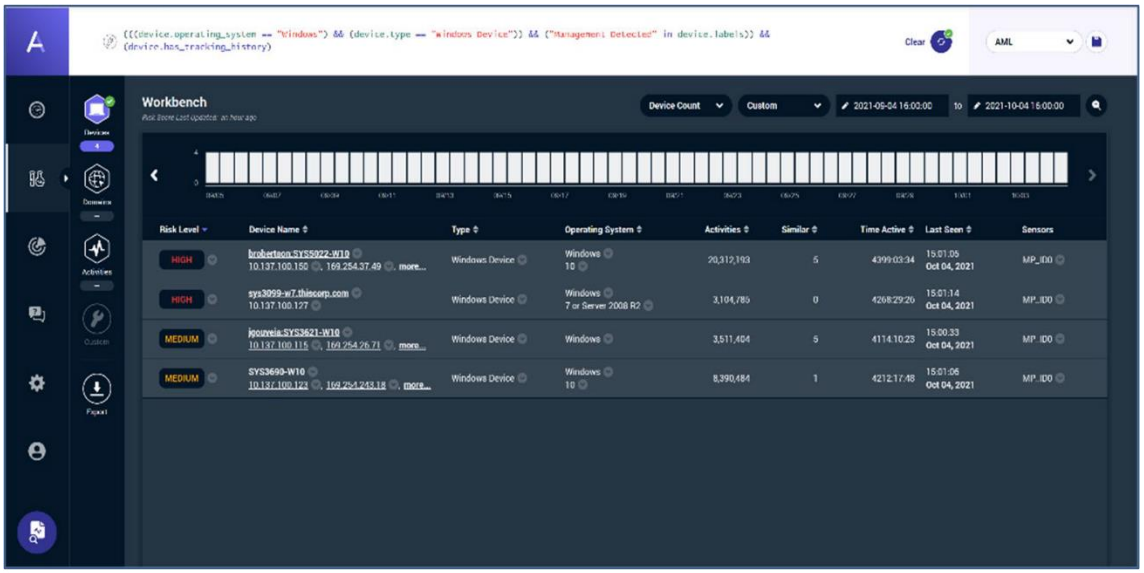


Nucleusのカスタマイズ可能なインタラクティブ可視化ダッシュボード

Nucleus に内蔵されている高度な AI エンジンは、組織の IT 運用チームが可視化を必要とするすべての主要な構成要素を相関付け、追跡します。階層的な表示により、データの発生元であるパケット自体まで完全にドリルダウンできます。プロトコルやアプリケーションなどに関連付けられたアクティビティのレベルの変化も、自動的に計算され、表示されます。そのため、オペレーターはネットワーク内での問題発生やポリシー違反の可能性を示唆するトレンドやアクティビティの急増を観測し、詳細な調査や問題の修復（詳しくは後述）を行うための適切なアクションを実施できます。さらに、こうした変化を自動的に警告するカスタム・モデルを作成することも可能です。

DFX は高度なフィンガープリント手法を使って、エンドポイント検出・対応（EDR）エージェントやエンドポイント保護プラットフォーム（EPP）などのアプリケーションによって能動的に管理されているデバイスを判定します。そして、アプリケーション、オペレーティング・システムのバージョン、使用しているドメインやプロトコル、管理対象デバイスの割合など、さまざまな要素のコンプライアンス状況の追跡に役立つレポートを作成できます。

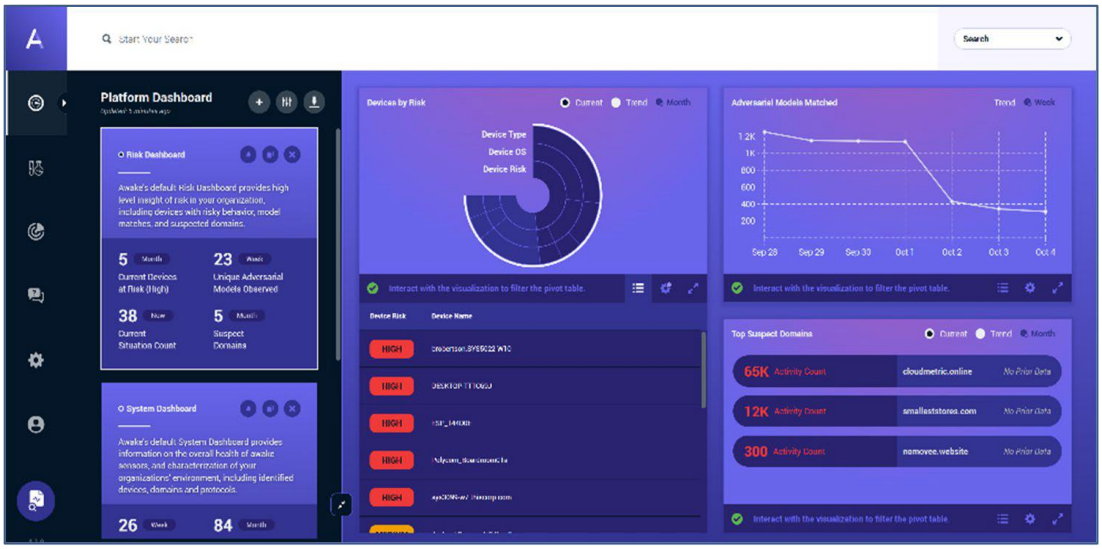
これらの値があらかじめ計算されるようにすれば、重要ながら定型的な作業にかける時間と労力を削減し、IT ポリシーとセキュリティ・リスクを簡単に相関付けることができます。ポリシー違反はセキュリティ・イベントの前触れであることが多いため、重要なネットワーク・データを表示する、IT 運用チームとセキュリティ運用チームの両方が利用できる最適化された共通ビューがあれば、シームレスなワークフローを実現できます。



管理対象デバイスのインタラクティブ表示

システムが自律的に検出した脅威は、追跡され、重み付けされ、リスク・ダッシュボードに表示されます。このダッシュボードでは、システムが検出し、自動的に優先順位付けされた新しい脅威がわかりやすく可視化されるので、セキュリティ・オペレーターは最も急を要する問題にいち早く対応できます。

システムが検出した新しい脅威を評価するには、通常のワークフローでは、このダッシュボードから、危険にさらされているデバイスの表示へと移動します。オペレーターは、システムが自動的に相関付けた現在の情報と履歴情報を表示する EntityIQ エンジンを使用して、新しいアラートの詳細を引き続き直接調べることができます。あるいは、アナリストが新しい「状況」を手作業で作成し、AVA AI に自動調査の開始を指示することも可能です。この方法では、追加のコンテキストを拡張して相関付け、エンティティのアクティビティを追跡することで、組織内に他の犠牲者がいないか、その脅威で使われている一連の攻撃インフラは何かといった点を調査します。



脅威検出 – リスク・ダッシュボード

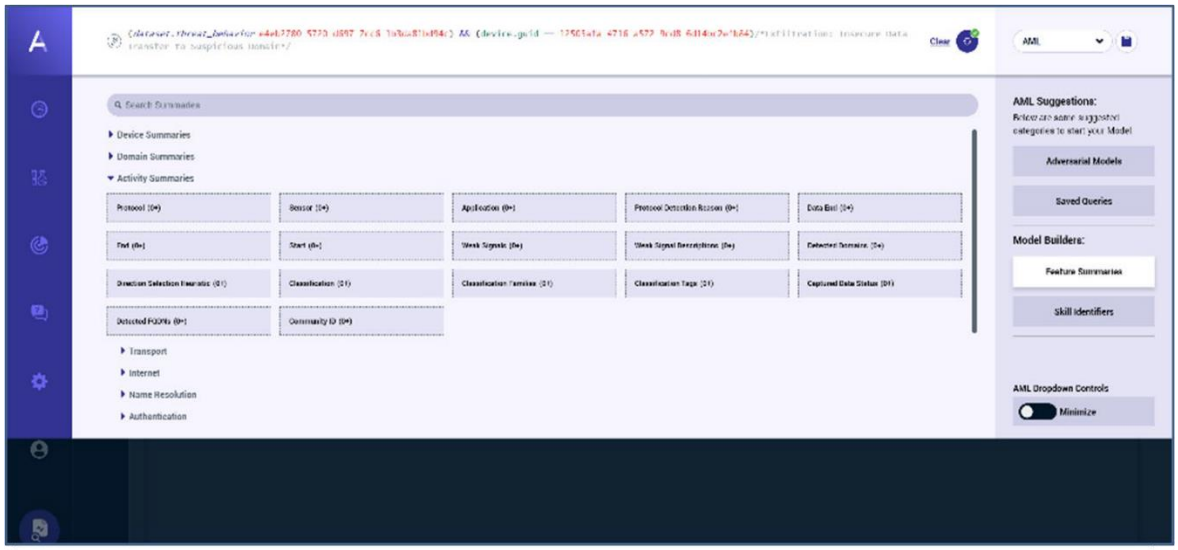
検出され、修復または調査の対象になっているインシデントは、AVA AI による「状況」表示で追跡できます。この「状況」は、検出された攻撃のあらゆる要素を拡張、相関付け、追跡して、オペレーターが最も効果的、効率的な活動を行うためのガイダンスを提示します。それと並行して、AVA はバックグラウンドで自律的に状況の更新を続け、時間の経過と共に利用可能になるコンテキストとデータを追加していきます。

AVAによる「状況」表示 – 自律的な攻撃ワークフロー

追加の調査オプションに関するガイダンスと、詳細な修復手順は、システムから提供されます。攻撃への対応、たとえば EDR エージェントを使用して侵害システムを分離する、影響を受けるデバイスを隔離サブネットに再セグメント化するといった処理は、オペレーターが手動で実行することも、チケッティング・ツールやオーケストレーション・ツールとの連携を通じてプログラムで実行することもできます。

プログラム可能な脅威検出

一般的な組織は、新しい情報が利用可能になったときに、未知の攻撃やデータ侵害の兆候を先回りして検出しようとします。これには、新たに発見された CVE の脆弱性、脅威アクター手法、侵害インジケーターが含まれます。その一方で、自社環境に固有の脅威や、企業ポリシーへの違反にあたるネットワーク動作を探そうとする場合もあります。たとえば、DFXを活用するある小売企業は、このソリューションのプログラマビリティを活かして、ホワイトリスト外のデバイスやユーザーから PCI エンクレーブへのアクセスをすべて監査し、記録しています。オペレーターは Adversarial Modeling 言語（AML）を使用して、高度で詳細な脅威検出を開始できます。機械学習とデータ・サイエンスの高度なトレーニングや、広範な知識は必要ありません。



ポイント＆クリック型のAMLモデル・ビルダー

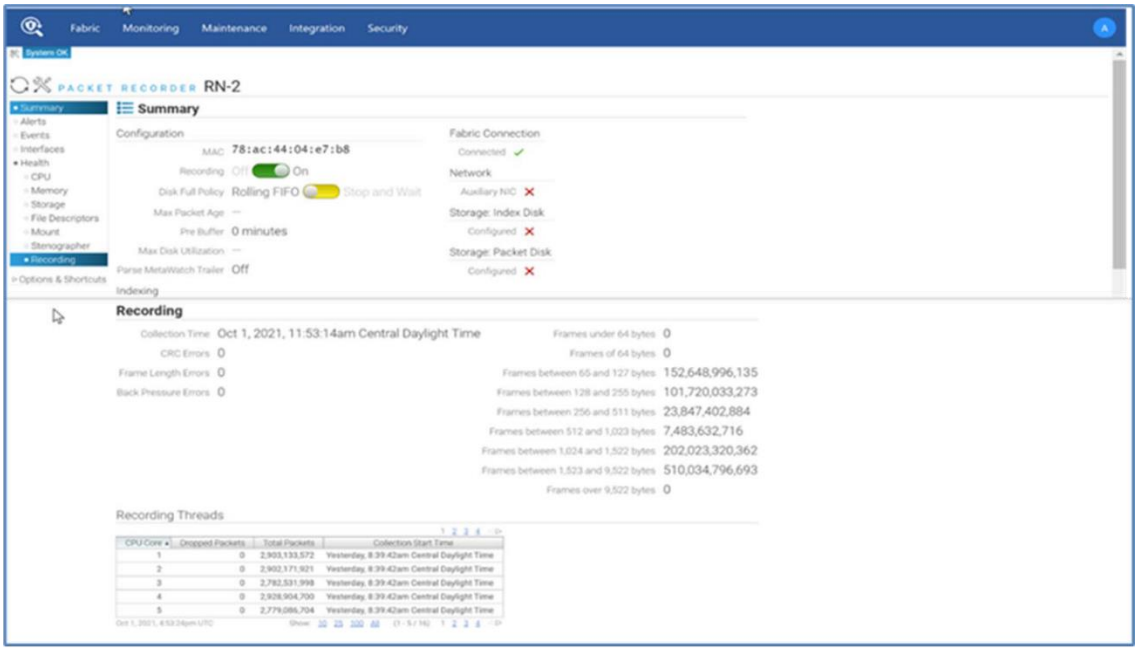
AML は、Nucleus に内蔵されている自律的な AI エンジンを拡張および強化して、ネットワークの内外に位置するエンティティ間の関係やアクティビティを検索します。AI エンジンは、データを自動的に事前計算して保存します。このデータにシンプルなポイント＆クリック・インターフェイスからアクセスし、製品に内蔵されているモジュール型の再利用可能な「レシピ」を使って、強力な脅威ハンティング・モデルを構築できます。

たとえば、ラテラル・ムーブメントや認証情報の悪用テクニックを詳しく知らないアナリストでも、高度な脅威アクター動作を検出するためのクエリを簡単に作成できます。作成した新しい脅威ハンティングのクエリは、保存して、Nucleus の現在実行中の検出機能に追加できるため、カスタマイズしたワークフローを組織全体で利用できます。これらのカスタム脅威のいずれかが見つかったときは、前述のダッシュボードから「状況」表示までのすべての構成要素が、すぐに検出に利用できるように更新されます。

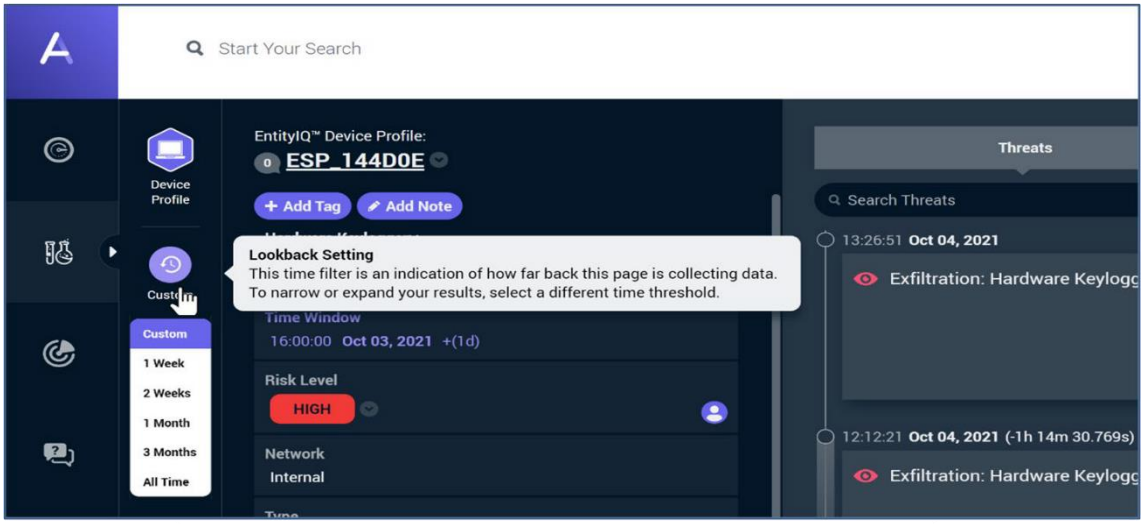
コンプライアンスとフォレンジック調査

規制の厳しい環境では、組織に対し、監査証跡の役割を果たすネットワーク履歴レコードを保持することや、調査ユースケースに対応することが求められます。たとえば、米国連邦金融機関検査協議会（FFIEC）とニューヨーク州金融サービス局（NY DFS）の規制では、ランサムウェアからインサイダー攻撃まで、幅広い脅威についてのサイバー・インシデント対応のフォレンジックを義務付けています。従来のネットワーク・フォレンジック・システムは、展開が複雑で使いにくいうえに、初期費用と日々の運用コストが高くつきます。また、長期契約や独自ストレージで導入企業を囲い込もうとする主要ベンダーも少なくありません。コンプライアンス・チェックが必要な場合や、フォレンジック・データが必要になる数少ない例を除き、このようなシステムに継続的な実用性を見出す導入企業はほとんどありません。

DFX ソリューションは、拡張可能なストレージ、タイム・マシン機能や再現機能と共に、充実したネットワーク・フォレンジック機能を提供します。さらに、自律的なネットワーク監視や、脅威検知・対応のサポートによって、履歴のフォレンジックにとどまらない持続的な価値を実現します。このソリューションは、比較的経験の浅いアナリストでも利用できるようにデザインされていますが、アリスタのエキスパート・チームに 24 時間 365 日の脅威監視、脅威ハンティング、インシデント対応を代行してもらうことも可能です。



DFX Recorder Node – シンプルでスケーラブルなパケット・ストレージ



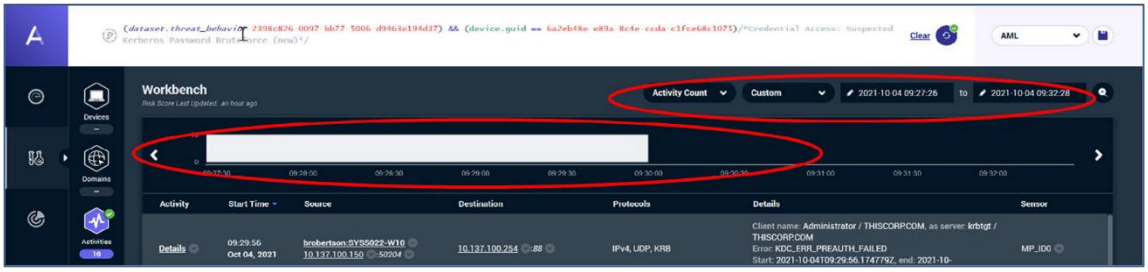
EntityIQの高度な遡及設定

これにより、社内で専門スキルを育成、展開するコストを節約できます。プラットフォームの拡張性を活かして、法規制に抵触する問題を自動的に検出し、監査要件を満たすアラートを発行する、独自のコンプライアンス・モデルを構築することも可能です。このソリューションは、人的資源の調査など、サイバー・セキュリティ以外の目的にも利用できます。

DFX は、今日の組織が直面している履歴コンプライアンスやフォレンジック分析の要件に対して、シンプルでありながら強力なワークフローを提供します。Nucleus に内蔵された強力な EntityIQ エンジンが、ネットワーク上のすべてのエンティティを長期的に分析し、追跡します。EntityIQ は、履歴コンプライアンス・アクティビティと、過去のアクションや動作のフォレンジック分析のどちらにも、信頼できるソースとして機能します。

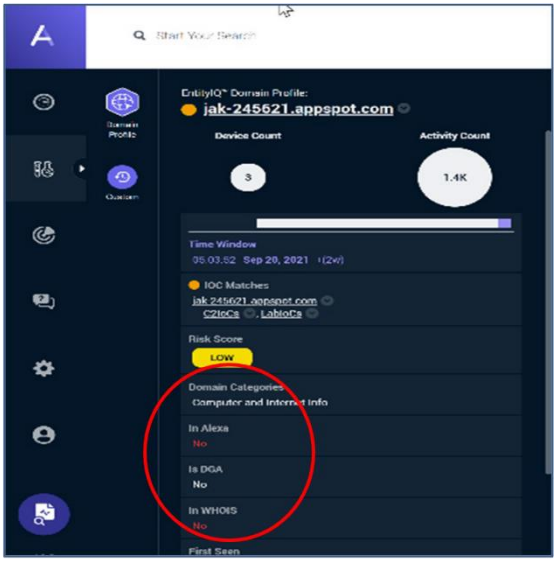
EntityIQ は API を通じて DMF Recorder と透過的に統合され、ファブリックが保守しているパケット・ストア全体に対し、コンテキストに応じたすばやいアクセスを保証します。EntityIQ エンジンにはフォレンジックに関するツール一式が統合されており、セキュリティ・アナリストのための一元的なビューと、セキュリティ・チームが使用するツールの標準化を実現します。

EntityIQ には数種類の遡及間隔があらかじめ定義されており、オペレーターは最適なものを選択できます。問題解決までの時間を短縮したり、過去のイベントを分析する際に不要なバックグラウンド・ノイズを除去したりする目的で、アナリストが非常に細かい間隔を定義する場合もあります。アクティビティ・タイムラインを使用すると、アナリストが最も注目すべき期間を視覚的に判断したり、分析に関連するパケットのみを取得したりできます。



詳細な遡及設定とアクティビティ・タイムライン

Nucleus には、ドメイン・ルックアップ・ツール「Whois」や、ドメイン・ランキング・システム「Alexa」、DGA（ドメイン生成アルゴリズム）リストとドメインのカテゴリ・タイプなど、多数のフォレンジック・ツールが直接組み込まれています。さらに、お客様が作成、構築したツールでパケット分析を行うために、ユーザー・インターフェイスや API を通じてパケットをエクスポートすることができます。これらのツールによって、フォレンジック調査のワークフローに要する全体的な時間が短縮されます。



組み込まれているフォレンジック・ツール

まとめ

アリスタの DFX ソリューションは、高度でプログラム可能な監視および検出機能を提供して、IT 運用チームとセキュリティ運用チームにまたがる可視化および脅威監視ワークフローを能率化します。ゼロタッチ展開と、1 秒あたり数百ギガビットまで拡張できる独自機能により、現在市販されているソリューションの中で最も早く価値を実現できます。DFX は、ネットワーキングとセキュリティの業界リーダーの包括的なプラットフォームに、プログラム可能なポリシーベースのパケット・フィルタリング、スケーラブルなパケット・ストレージと高度なコンプライアンス機能、脅威検出、ポイント＆クリック操作による独自の脅威ハンティング機能を搭載して、完全な統合型のエンドツーエンド・ソリューションを提供します。

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

ARISTA
2021 年 12 月 3 日