Anomali Match

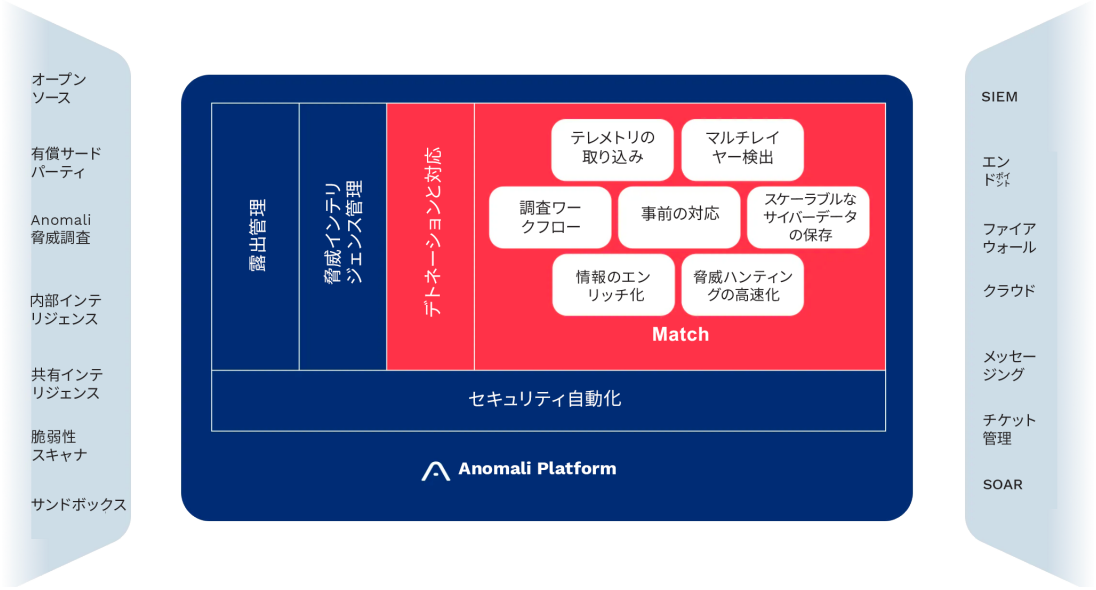
メリット

- **リアルタイム監視：**
  ログデータを継続的に収集、保存、分析、レポートして、脅威のリアルタイム検出とインシデント対応を実現します。
- **保護、検索、可視化：**
  セキュリティログを深く分析し、パターンを表面化し、未加工のセキュリティデータをすぐに使用可能な洞察に変換する分析エンジンです。
- **遡及的なフォレンジック分析：**
  侵害が発生した場合、Anomaliプラットフォームで収集および保存された履歴データによって、セキュリティインシデントのフォレンジック分析と調査を行うことができます。
- **自動インシデント対応：**
  特定のタイプのインシデントに自動対応することで、対応に必要となる手作業を減らすことができます。
- **誤検出の低減：**
  スマートな相関ルールと機械学習アルゴリズムにより、誤検知のセキュリティアラートの数を大幅に削減し、アナリストの時間を解放します。
- **コスト効率：**
  わずかなコストで長期間のセキュリティログを保存し、インフラストラクチャの管理と安全の確保のために稼働する機器の数を削減します。

IT インフラストラクチャの「死角」の特定となると、セキュリティチームが困難に直面することはよくあることです。そして、従業員やパートナーがそのようなシステムを使用または操作すると、重要なアセットの可視性が制限されるということにつながります。可視性の獲得には出費がかさむかもしれません。旧式のセキュリティインシデントソリューションやイベント管理ソリューションに依存しているからです。そのため、費用効果の高い、セキュリティコントロール全般にわたるテレメトリデータの管理ができません。これによって、長期間にわたってデータを保持できず、セキュリティの有効性とコストのバランスが取れず、妥協を犠牲が強いられることになります。さらに、保存された情報には、実行可能な措置をタイムリーに講じるために必要なコンテキストが欠けていることが往々にしてあります。

Anomali Match Security Analytics は、エンドポイント、ファイアウォール、クラウドプラットフォーム、プロキシ、および DNS などの、様々なセキュリティコントロールからセキュリティテレメトリを収集します。このデータはスケーラブルなクラウドネイティブデータレイクに保存されるため、効率的なストレージと、大幅なコスト削減が確保されます。Match Security Analytics Engine エンジンは、複数の検出レイヤーを使用して脅威をリアルタイムで検出し、ペタバイト単位のデータに対して数秒以内にレトロスペクティブハンティングを実行します。これらの検出レイヤーには、何十億もの侵害指標（IoC）、行動ルールまたは攻撃指標（IoA）、およびドメイン生成アルゴリズム（DGA）が含まれます。アナリストに有益な洞察を提供するために、検出結果には、攻撃者とその戦略、テクニック、手順（TTPs）に関して、厳選された情報によってコンテキストが与えられます。アナリストに警告するだけでなく、攻撃者や攻撃フローに関する情報も提供するので、後続のステップを予測し、事前に防御することができます。この Match Security Analytic 機能は、人工知能（AI）と自動化によってさらに強化され、自然言語検索、自動スコアリングとエンリッチ化、ワークフロー統合などの機能により、アナリストのワークフローを簡素化して高速化します。

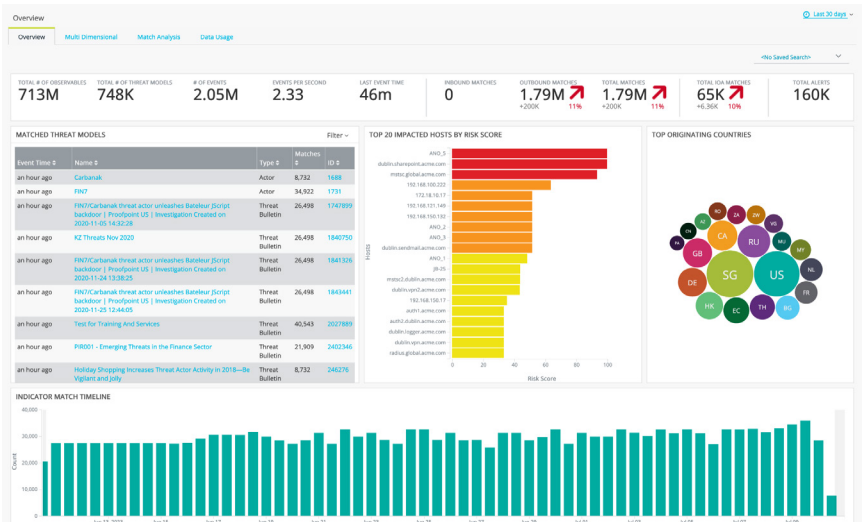
Anomali Match Security Analytics は、大規模に完全な可視化を実現し、コンテキストの洞察に基づくパフォーマンスを提供することで、リアルタイムの意思決定を推進します。Anomali Match を使用すると、少ないリソースでより多くのことを実現できます。



AI を活用した Security Analytics により、可視性を強化して対処でき、エンリッチ化と対応を自動化できます

主な機能

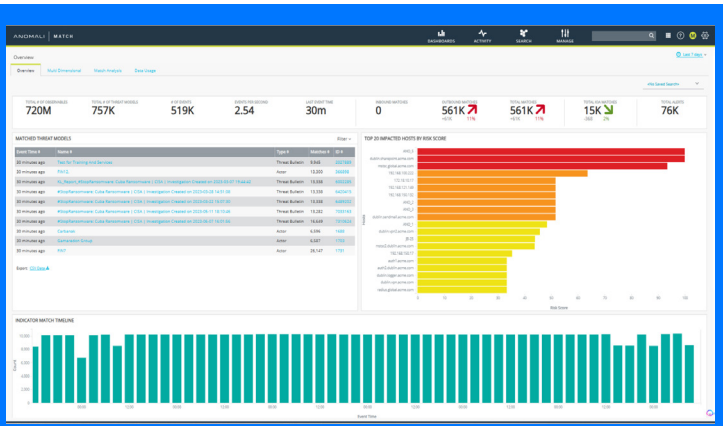
- **自動脅威検出：**侵入指標（IoC）、行動検知または攻撃指標（IoA）、およびドメイン生成アルゴリズム（DGA）を使用したマルチレイヤー検出により、脅威を検出します。
- **ログの集約：**すべてのセキュリティコントロールからテレメトリを取得します。コンプライアンスまたはセキュリティのユースケースのために永年のデータを保存します。
- **Anomali 分析エンジン：** ペタバイト規模のデータを検索し、ダッシュボード、視覚化、すぐに実行可能な洞察を作成します。
- **スケーラブルなデータレイク：**わずかのコストで永年のデータを保存し、重大なイベントに関するタイムリーでレトロスペクティブな洞察を得ることができます。
- **高度な分析：**セキュリティイベントを調査し、コンプライアンスを分析し、セキュリティテレメトリをビジネスリスクへと変換します。Anomali Platform を使用すると、顧客は数秒で検索と分析を実行できます。45 秒以内に 1,400 億件を超えるレコードを実行したり、現在の 10 倍の市場規模でのリアルタイム分析を同時に実行したりできます。すべてを平易な言語で行います。
- **行動分析：**厳選された攻撃指標によって行動の異常を特定し、攻撃者の一歩先に行きます
- **ドメイン生成アルゴリズム：**DGA を使用して悪意のあるコマンドおよびコントロールドメインを予測します
- **調査ワークフロー：**インタラクティブな調査ワークベンチにより、調査ワークフローとアクションアラートをエンリッチ化し、迅速化します
- **アラートのエンリッチ化：**行為者、行動、TTPs などに関する洞察によって、アラートの優先順位付けと対応行動を通知します
- **脅威ハンティング：**攻撃者の洞察によって、仮説に基づく脅威ハンティングを強化します。長期間にわたるデータを検索します。AI の力を活用して、脅威の報告からすぐに対処できます。
- **GPT を活用：**生成 AI の力を活用してアナリストのエクスペリエンスを向上させます。GPT を利用して、脅威とインシデントの概要とエグゼクティブレポートを生成します。
- **対応の自動化：**Anomali Integrator では、統合された対応ワークフローで攻撃者の次のステップを予測し、事前に防御します。または、希望の SOAR と対応を統合します。



ダッシュボードのカスタマイズ、発生中の脅威の把握、リスクの高いアセットの特定など

使用例

- **精密な攻撃検知**厳選された最大の情報リポジトリを使用し、攻撃指標と攻撃者の行動に関する洞察によって、侵害を高い精度で特定します。
- **コンプライアンス:**長期間のログをスケーラブルかつコスト効率に優れた方法で集約し、コンプライアンス目標を達成するために検索できるようにします。
- **高度なセキュリティ分析:**セキュリティイベントを調査し、自然言語を使用してペタバイト単位のデータを検索し、インテリジェンスに関する洞察でセキュリティイベントをエンリッチ化してすぐに使用可能なものにし、セキュリティテレメトリをビジネスリスクに変換します。
- **調査のエンリッチ化:**攻撃者の洞察と侵害のコンテキストにより、アラートの優先順位を設定し、重大なインシデントを迅速に追跡します。
- **情報に基づいたインシデント対応の自動化:**攻撃者を把握し、次のステップを予測して、侵害の影響を阻止します。セキュリティコントロール全体にわたってワークフローを統合することで、対応を迅速化して自動化できます。または、SOAR と統合することができます。
- **脅威ハンティングの高速化:**データのパワーをすぐに活用できます。わずかなコストで、長期間のセキュリティテレメトリの保存と検索が可能。AI の力を活用して、報告から驚異ハンティングまで数秒で完了できます。
- **協働的なセキュリティワークフロー:**部門間の壁を取り払い、同僚グループと連携し、検出と対応の時間を短縮します。脅威とリスクに関する洞察を同僚や幹部と共有し、まったく異なるソースからデータを取り込み、ビジネスニーズに合わせてセキュリティを調整します。



自然言語で数ペタバイト分の長期間のデータを検索します

ANOMALI