ホワイトペーパー
公開

Cisco Secure Network Analytics

高度な脅威に対する検出と対応を可能にする、独自の振る舞いモデリングと機械学習の手法について詳しく説明します。

目次

はじめに

エンタープライズ ネットワークが複雑化したことで、セキュリティの抜け穴が数多く生まれました。今日、従業員はさまざまな場所からネットワークに接続しています。また、接続するためのデバイスも 一つではありません。ネットワークにアクセスするスマートデバイスの数と、パブリッククラウドサービスの使用は増える一方です。さらに、データ保護とプライバシーのため、暗号化トラフィックが増加しています。これらすべてにより、企業はビジネス成果の促進とデジタル化への移行を実現できました。これは同時に、攻撃者が検出されることなくデジタルビジネス内に潜んでいる可能性の上昇も意味します。脅威は、規模と手口の面で急速に進化し続けています。

攻撃者の主な目的は、侵入し、その状態を維持することです。攻撃者はランサムウェアを要求したり情報を盗んだりすることで、自分の存在を知らせることもありますが、それまで待っては手遅れです。攻撃者を早期に発見することが重要です。脅威は進化し続けるため、境界ベースのソリューションは 100% 効果的ではありません。攻撃者はネットワークのセキュリティを破るのではなく、盗んだログイン情報で易々とログインする場合もあります。攻撃のライフサイクルの早い段階で、つまり攻撃者がネットワークに侵入して重大な影響を与える前に、高度な脅威を検出できるソリューションが必要です。

Cisco Secure Network Analytics（旧 Stealthwatch）は、拡大したネットワークに対する包括的な脅威を可視化する、業界をリードするセキュリティ分析ソリューションです。高度な脅威を検出して対応でき、**振る舞いモデリング、マルチレイヤ機械学習、グローバルな脅威インテリジェンス**を組み合わせて使用することで、ネットワーク セグメンテーションの簡素化を支援します。攻撃者がネットワークに侵入する方法は 1 通りだけではないため、Secure Network Analytics は複数の分析手法を使用して脅威を早期に検出し、確実に除去します。また、暗号化されたトラフィックのマルウェアを復号せずに検出できる業界初で唯一のソリューションです。

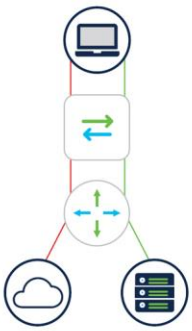
既存のネットワークを使用して適切なデータを収集する

デジタルビジネスとその日常的な動作を把握するには、必要かつ十分なテレメトリが必要です。テレメトリは、ルータ、スイッチ、ファイアウォールなど、すべてのネットワーク製品から得られます。これを受けて、Secure Network Analytics は暗号化されたトラフィックを分析し、復号せずにマルウェアを検出し、デジタルビジネス内のネットワーク暗号化の品質を管理できます。

また、Cisco Identity Services Engine、Cisco AnyConnect® Network Visibility Module、およびその他のサポートシステムからメタデータを収集し、ネットワークの振る舞い分析用にユーザとアプリケーションのコンテキストを取得できるようにします（図 1）。Secure Network Analytics はデジタルビジネスの「総勘定元帳」として機能するため、誰が、何を、どこで、いつ、どのように振る舞っているかを把握できます。

単一のエージェントレス ソリューションにより、デジタルビジネスに合わせて拡張可能なスケーラブルなセキュリティが実現します。ネットワーク全体に何百ものセンサーを実装する代わりに、ネットワーク インフラストラクチャ自体がセンサーとなり、攻撃者の隠れ場所をなくします。また、Secure Network Analytics はベンダーに依存しないソリューションで、多くのサードパーティエクスポータからテレメトリを取り込むことができます。
そのため、どのようなネットワーク インフラストラクチャを使用していても、Secure Network Analytics はそれをデータソースとして活用し、セキュリティを強化できます。

図 1. あらゆるテレメトリをエンドツーエンドで可視化



ルータ
ISR ASR
CSR WLC

スイッチ
Catalyst
IE

ファイアウォール
ASA Meraki
FTD

データセンター
Nexus
Tetration

Web
Secure Web

エンドポイント
セキュア VPN

ポリシーとユーザ情報
セキュア
ネットワーク
アクセス

その他
Secure Network Analytics フロー センサー
パブリッククラウド

Secure Network Analytics は、多くのサードパーティエクスポータからテレメトリを取り込むこともできます。

ISR = シスコのサービス統合型ルータ、ASR = Cisco アグリゲーション サービス ルータ、CSR = シスコ クラウド サービス ルータ、WLC = シスコワイヤレス LAN コントローラ、IE = シスコ産業用イーサネット、ASA = Cisco Secure Firewall 適応型セキュリティアプライアンス、FTD = Cisco Secure Firewall Threat Defense

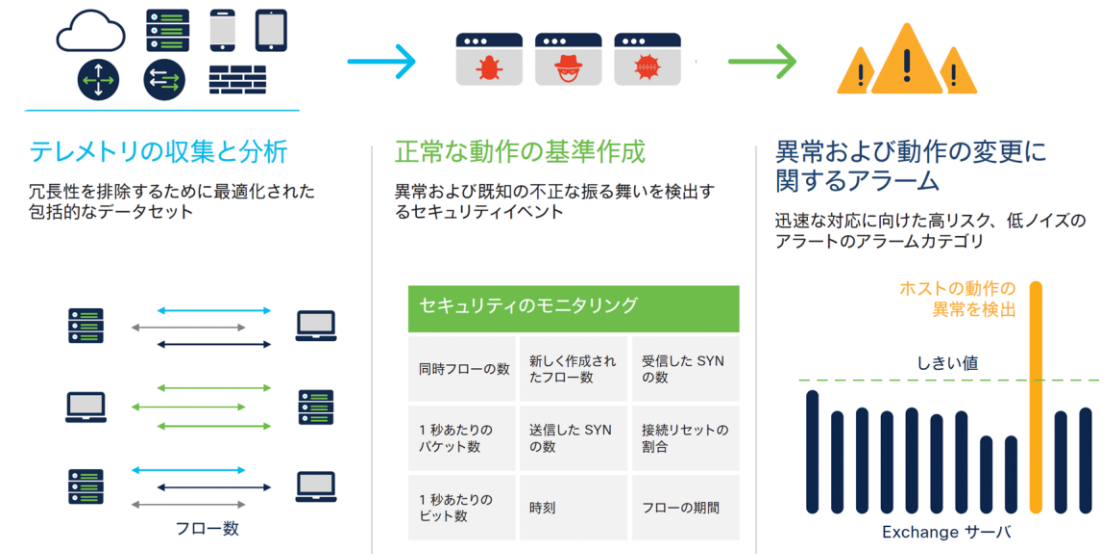
複数の分析手法が連携

Secure Network Analytics には 3 つのコアアプローチがあります。それらが連携することで、攻撃の最も早い段階で脅威を捕捉できるよう隅々まで漏れなく調査します。

1. 振る舞いモデリング

Secure Network Analytics はネットワーク上の各デバイスのアクティビティを詳細に監視し、正常な動作の基準を作成できます。さらに、既知の不正な振る舞いについても深いレベルで把握しています。Secure Network Analytics は、100 種類近くのセキュリティイベント、またはスキャンやビーコン発信ホスト、ブルートフォースログイン、データ蓄積の疑い、データ損失の疑いなどさまざまなタイプのトラフィック動作を調べる発見的手法を適用します。これらのセキュリティイベントは、高レベルの論理アラームカテゴリに分類されます。一部のセキュリティイベントは、自身でアラームをトリガーすることもできます。Secure Network Analytics は個別に発生した複数の異常なインシデントを関連付け、それからどのような攻撃が行われているかを総合的に判断します。各攻撃の侵入経路をデバイスやユーザ単位で追跡することもできます（図 2）。インシデントは、時間や関連付けられたテレメトリによりさらに詳細に調査できます。これは、セキュリティの診断という点で理想的な状況です。患者を診察する医師は、どこが悪いのかを把握する際に症状だけを切り離して調べることはありません。全体像を見て診断を行います。同様に、 Secure Network Analytics はネットワーク内のすべての異常なアクティビティを記録し、それを包括的に見てコンテキストに基づくアラームを生成し、セキュリティチームがリスクに優先順位を付けられるよう支援します。

図 2. 振る舞いモデリングを使用した異常検出



2. マルチレイヤ機械学習

また Secure Network Analytics は「教師あり」と「教師なし」の**機械学習**も適用して、高度な脅威と悪意のある通信を検出します。クラウドベースのマルチステージ機械学習分析パイプラインと統合し、企業内で見られる脅威の動作をグローバルで見られる脅威の動作と関連付けます。

システムはユーザとデバイスの動作を分析し、マルウェア感染、コマンド & コントロールの通信、データ漏洩、組織のインフラストラクチャで動作する不要と思われるアプリケーションを検出します。処理には複数の階層があり、人工知能や機械学習、数学的統計の手法を組み合わせることで、ネットワークが正常なアクティビティを自己学習し、悪意のあるアクティビティを特定できるよう支援します。

暗号化トラフィックを含め、拡張ネットワークのすべての部分からテレメトリを収集するこのネットワークセキュリティ分析パイプラインは、Secure Network Analytics 独自の機能です。「異常なものは何か」という概念を徐々に構築し、実際の個々の「脅威アクティビティ」を分類し、デバイスやユーザが実際に侵害されているかどうかを最終的に判断します。また、非常に注意深い分析と相関関係を通じて、侵害されたエンティティが最終的に有害であると総合的に判断するための証拠を提供します。

多くの企業は日々大量のアラートを受信しており、リソース不足のセキュリティチームがこれらすべてのアラートを調査することはできないため、この機能は重要です。機械学習エンジンは大量のデータをほぼリアルタイムで処理し、重大なインシデントを高い信頼性で検出し、迅速に修復するための一連のアクションも明確に提案できます。

3. グローバル脅威インテリジェンス

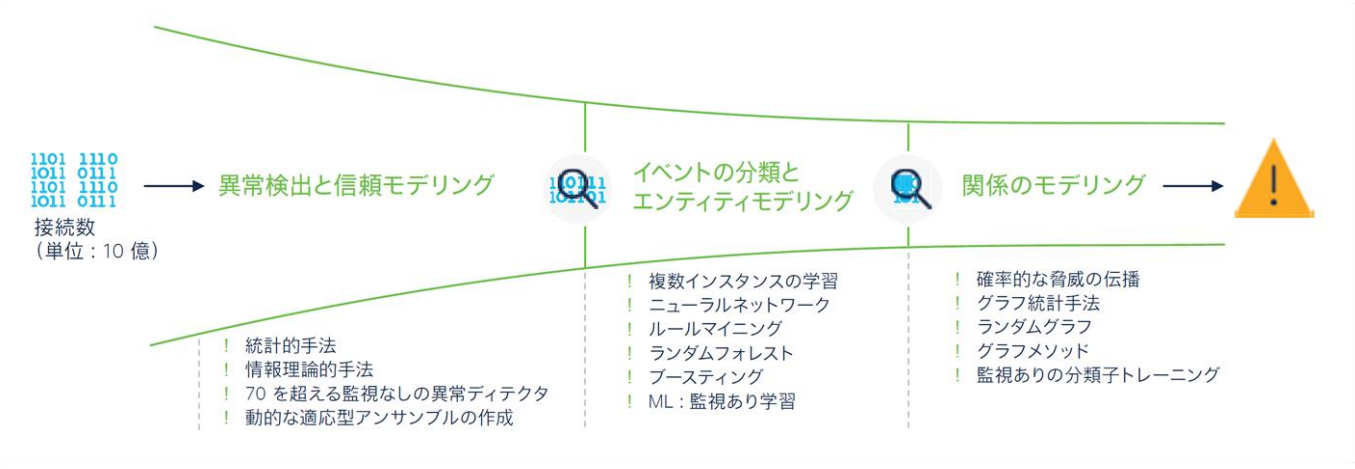
攻撃者の利点の 1 つは、複数のターゲットに同じ攻撃を適用できることです。また、これらの攻撃対象はすべて脅威アクティビティのローカルビューに拘束されるため、すべてのターゲットで攻撃が成功する可能性があります。しかし、悪意のある IP やドメイン、またはキャンペーンで使用された新種のマルウェアに関する情報を

取得でき、そのアラートをグローバルな脅威インテリジェンスにマッピングできるとしたらどうでしょうか。検出までの時間を大幅に短縮し、検出の精度を高めることができます。

Cisco Talos™ インテリジェンス プラットフォームを活用したグローバル脅威インテリジェンスフィードは、ボットネットやその他の高度な攻撃に対する保護を強化します。ローカルネットワーク環境における疑わしいアクティビティを、何千もの既知のコマンド & コントロールサーバやキャンペーンのデータと関連付けて、高精度の検出と迅速な脅威対応を実現します。これらの攻撃者の視点を想定して、この立場から優位性を獲得できます。

マルチレイヤ機械学習とは、またはその有効性は?

Secure Network Analytics で使用される複数の機械学習手法について詳しく見てみましょう。インシデントが Cisco Secure Network Analytics の機械学習エンジンに渡されると、教師ありと教師なしの機械学習を組み合わせたセキュリティ分析のファネルを通過します（図 3）。



レイヤ 1：異常検出と信頼モデリング

このレイヤでは、統計的な**異常ディテクタ**を使用してトラフィックの 99% を破棄できます。これらのディテクタは、正常なものと異常なものの複雑なモデルを合わせて管理します。しかし、異常なものに必ずしも悪意があるとは限りません。ネットワークには、脅威とは関係のない、単に**奇妙な**ことが数多くあります。ただし、これらを脅威の動作とは分離することが重要です。そのため、これらのディテクタの出力をさらに分析して、奇妙ではあるものの、説明でき、信頼できる動作を記憶します。その結果、最も関連性の高いフローと要求のごく一部がレイヤ 2 とレイヤ 3 に渡されます。このような機械学習手法を適用しない場合、ノイズからシグナルを分離する運用コストが非常に高くなります。

異常検出：最初のステップでは、統計的に正常なトラフィックと異常なトラフィックを分離するために、統計的機械学習法を適用します。Secure Network Analytics がネットワーク周辺を通過するトラフィックで収集した会話のテレメトリレコードを、70 を超える個別のディテクタが処理し、内部ドメインネームシステム（DNS）トラフィックを、そして利用可能な場合はプロキシデータを選択します。各要求は 70 を超えるディテクタによって処理され、各ディテクタは異なる統計アルゴリズムを適用して、検出した異常のスコアを生成します。これらのスコアは統合され、複数の統計手法を再度適用することで、個々の要求ごとに 1 つのスコアが生成されます。この集約スコアは、通常のトラフィックと異常なトラフィックを分離するために使用されます。

信頼モデリング：次に、同様の要求をグループ化し、それらのグループの異常スコアを長期平均として集約します。時間の経過とともに、より多くの要求が分析され、長期平均異常スコアが生成されるため、誤検出と検出漏れが減少します。信頼モデリングの結果を使用して、動的に決定された特定のしきい値を超える異常スコアを持つトラフィックのサブセットを選択し、次の処理レイヤに移ります。

マルチレイヤの機械学習とグローバルリスクマップを活用したセキュリティ分析には、次のようなメリットがあります。

- 既知の脅威に加えて、「既知 - 未知」の脅威（以前は発見できなかった、既知の脅威、マルウェアのサブファミリ、または関連する新しい脅威のバリエーション）と「未知 - 未知」の脅威（まったく新しいマルウェア）を検出
- 信頼性の高い自動アラートにより、リソースが限られたセキュリティチームがリスクの高いインシデントに注力
- ローカル脅威とグローバルキャンペーンの関連付けにより、迅速に脅威を緩和
- 膨大な量のテレメトリ処理能力を活かしたスケーラブルなセキュリティを実現

レイヤ 2：イベントの分類とエンティティモデリング

このレイヤでは、前のステージの結果を特定の悪意のあるイベントに分類します。イベントの分類は、90% を超える一貫した精度を目指す機械学習分類子によって行われます。以下の対策が考えられます。

- ネイマン・ピアソンベースの線形モデル
- 複数インスタンス学習を使用したサポートベクターマシン
- ニューラルネットワークとランダムフォレスト

次に、これらの分離されたセキュリティイベントは、時間の経過とともに 1 つのエンドポイントに関連付けられます。ここで脅威の様子が組み立てられ、この攻撃者が特定の結果に向けてエスカレートしていった全体像が明らかになります。

イベントの分類：前のレイヤからの統計的に異常なサブセットは、分類子を使用して 100 以上のカテゴリに分類されます。多くの分類子は個別の動作やグループの関係、グローバルやローカル規模の動作に基づきますが、他のものは非常に具体的です。

たとえば、分類子がコマンド & コントロールトラフィック、拡張の疑い、または不正なソフトウェアアップデートを示す場合があります。このフェーズの出力は、セキュリティ関連に分類された異常なイベントのセットです。

エンティティモデリング： 特定のエンティティに関する悪意のある仮説を裏付ける証拠の量が重要度のしきい値を超えると、脅威が作成されます。

脅威の作成に寄与したイベントはその脅威に関連付けられ、エンティティの個別の長期モデルの一部になります。時間の経過とともに証拠が蓄積されて重要度のしきい値に達すると、新しい脅威が作成されます。このしきい値は動的で、脅威のリスクレベルやその他の要因に基づいてインテリジェントに調整されます。脅威は Web インターフェイス ダッシュボードに表示され、次のレイヤに進みます。

レイヤ 3：関係のモデリング

関係のモデリングはグローバルな観点から前のレイヤを統合することを目的としていて、このインシデントのローカルコンテキストだけでなく、グローバルコンテキストも提供します。ここでは、この攻撃を受けた組織の数を特定し、特定の標的にされているのかグローバルキャンペーンによる影響を受けているのかを確認できます。

インシデントは**確認されたもの**または**検出されたもの**になります。これらの手法やツールは以前に比べてより広いグローバルな範囲で監視されているため、確認されたインシデントには **99 ～ 100% の信頼性**があります。検出されたインシデントは固有のものであり、ターゲットを絞ったキャンペーンの一部です。確認の結果は既知の一連の対処法とともに提供されるため、対応に要する時間とリソースを節約できます。検出の結果は、攻撃者とデジタルビジネスの対象となるキャンペーンの範囲を把握するために必要な調査ツールとともに提供されます。想像できるように、確認されたインシデントの数は検出されたインシデントの数よりもはるかに多くなります。これは、インシデントは新しくカスタマイズされたものである必要があり、確認されたインシデントは攻撃者が提供するためのコストが低く、一方検出されたインシデントは攻撃者が提供するためのコストが高いという単純な理由からです。確認されたインシデントを検出できるようにすることで、ゲームの経済性が最終的に防御者側に有利になり、優位性を与えるようになります。

グローバルリスクマップ

グローバルリスクマップは、業界で最大規模のデータセットの 1 つに機械学習アルゴリズムを適用した分析の結果です。これにより、インターネット上のサーバに関する広範な動作統計情報が（サーバが未知の場合でも）提供されます。これらのサーバは、攻撃に関連していたり、悪用されていたり、将来の攻撃の一部として使用されている可能性があります。これはブラックリストではなく、セキュリティの観点から疑わしいサーバの全体像です。これらのサーバのアクティビティに関するコンテキスト主導の情報により、Secure Network Analytics の機械学習ディテクタと分類子は、これらのサーバとの通信に関連付けられたリスクレベルを正確に予測できます。

特定の日に、攻撃者がこれらの検出手法の一つを回避できる可能性はありますが、すべてがパイプラインに統合して適用され、関連するデータを相互にフィードする中で、隠れることは不可能です。

機械学習や人工知能の適用に関連したさまざまなセキュリティ製品の日々の要求を検証することは非常に困難です。そのため、テレメトリに適用される高度な分析手法（機械学習を含む）を説明するために**調査を公開**しました。製品チームは、進化する脅威の一歩先を行くため、ディテクタと分類子の改善に継続的に取り組んでいます。また、生成したすべてのアラートについてユーザからのフィードバックを収集し、有効だったかどうかを判断します。有効なアラートの数は **90% を大きく上回っており**、引き続きこのパフォーマンスインジケータに取り組んでいきます。結局のところ、私たちは最高のデータサイエンティストとして存在するのではなく、お客様の役に立つために存在します。

では、この分析パイプラインはどのようなものを見つけることができるでしょうか。

さらに重要なこととして、前述のさまざまな分析手法を適用することで、Secure Network Analytics が検出できる脅威について説明します。

暗号化されたトラフィックでのマルウェア検出（暗号解読なし）

通信とオンラインでのビジネス取引にインターネットを利用する企業では、暗号化技術がプライバシーとセキュリティの実現に貢献してきました。しかし、暗号化の恩恵を受けるのは企業だけではありません。攻撃者は、検出の回避と悪意のあるアクティビティの保護にこの恩恵を利用しました。脅威の検査時に暗号解読、分析、再暗号化を一括して行う従来の方法は、パフォーマンスやリソースの観点から、常に実践または実現できるとは限りません。

Secure Network Analytics では、暗号化されたトラフィック内のマルウェアを暗号解読せずに検出でき、これは業界初の機能です。次世代のシスコネットワークのテレメトリと Secure Network Analytics フローセンサーは、パケットの長さと時間のシーケンス、および初期データパケットの 2 つの新しいデータ要素を生成します。初期データパケットはメタデータの宝庫です。すべての暗号化されたセッションは、最初は暗号化されない状態で開始されるためです。シスコ独自の特定用途集積回路（ASIC）アーキテクチャは、データネットワークの速度を低下させずにこれらのデータ要素を抽出できます。

この拡張されたテレメトリは Secure Network Analytics に渡され、そこでは前のセクションで説明した複数の分析手法を適用して、暗号化されたトラフィック内のマルウェアを高精度で検出します。

Advanced Persistent Threat（APT）

APT は、検出されることなく貴重な情報を盗み出すことを主な目的とする、組織に対する標的型攻撃です。検出されないため、長期間にわたって存続できます。高度な振る舞いモデリングを使用する Secure Network Analytics は、グローバルリスクマップを使用して、既知の不正な動作に関する知識と組み合わせて組織内の正

常な動作を詳細に把握できます。これにより、偵察やスキャン、コマンド & コントロールの通信、疑わしい水平方向のネットワーク動作など、APT に関連付けられたアクティビティも検出できます。

内部関係者による脅威

組織にとって最も価値ある資産の 1 つは、知的財産、機密情報、企業ネットワークに保存されている情報です。データ漏洩によって組織が被るコストは、何百万ドルにも及びます。紛失した、または盗まれたレコードあたりの平均コストは 158 ドルで、データ漏洩に関するコストは年間約 400 万 ドルに相当します。侵害されたユーザのログイン情報や不満を抱く従業員などの内部関係者による脅威は、金銭的な利益を得るため、または単に損害を与えるために、データを蓄積して外部に流出させます。

振る舞いモデリングを使用して異常な動作を検出すると、「データ蓄積」または「データ漏洩」アラームが生成されます。アラームをトリガーしたホストは、ワンクリックで調査できます。Secure Network Analytics は、ネットワークを使用して、ホストに関する追加のコンテキスト情報（ユーザ名、MAC アドレス、場所など）を提供します。また必要に応じて、疑わしいホストをネットワークから**隔離**できます。これは、Cisco Identity Services Engine との統合によって実現されます。

マルウェアの伝播

Cisco Secure Network Analytics は、ホストがマルウェアに感染しているかどうかを検出するだけでなく、マルウェアがネットワーク内でどのように伝播したか、他にどのホストが感染したかも追跡できます。この知識は、脅威の修復に重要です。最後に、感染したホストが特定されたら、インシデント対応担当者は感染者と関係のあった他のホストまたはマシンを Secure Network Analytics に尋ね、攻撃者が侵害したウィンドウ内で動作しているときにバックドアが作成されないようにすることができます。

セグメンテーションポリシーの設定とモニタリング

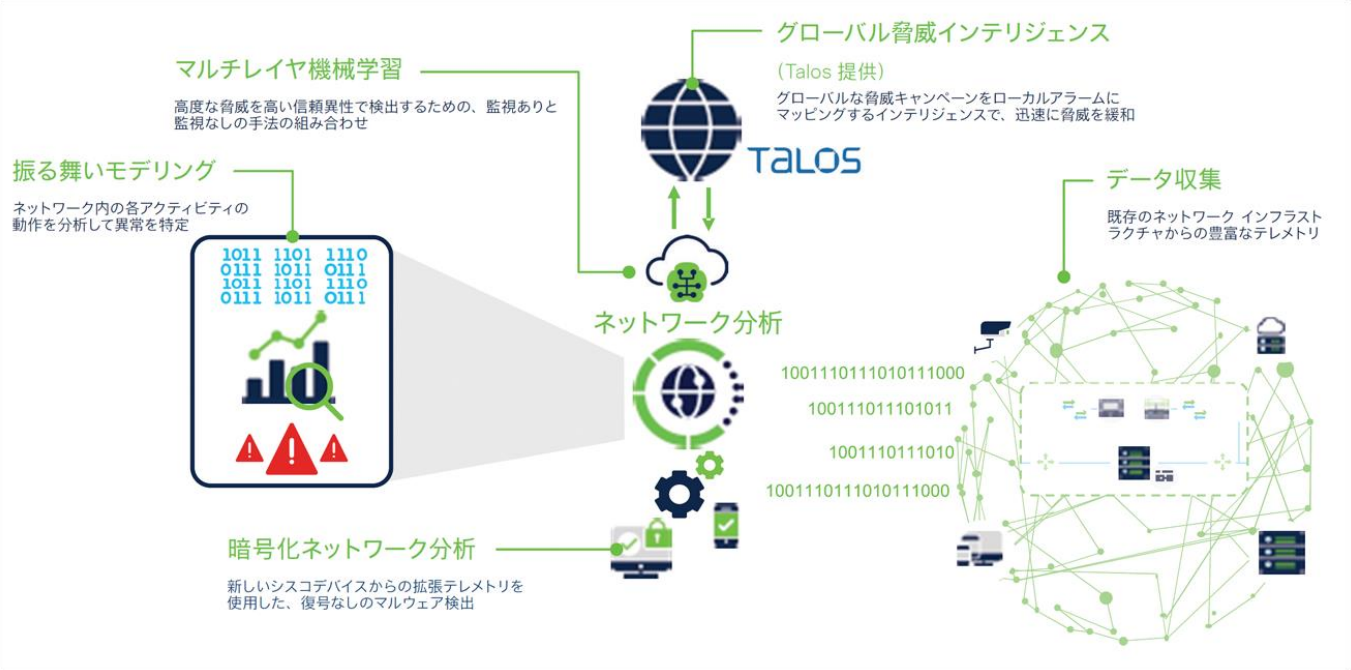
デジタルビジネスの運用方法を可視化することで、重要なリソースへのアクセスを制御するスマート セグメンテーション ポリシーを作成できます。この機能は、脅威の拡散や重大な影響を防止するために非常に重要です。ただし、設定したポリシーによって重要なビジネスワークフローが中断しないようにすることも重要です。そのため、Secure Network Analytics では、ファイアウォールやソフトウェア定義型ネットワーキング オーバーレイなどを使用して、提案したポリシーを設定する前にモデル化できます。設定したポリシーに違反すると、コンテキストアラームがトリガーされます。これらのアラームを調査し、ビジネスへの影響を評価した後、ファイアウォールまたはソフトウェア定義型ネットワーキング オーバーレイを使用してこのポリシーを設定できます。また、同じアラームを通じて、設定したポリシーが効果的に適用されていることを確認できます。

概要

効果的なネットワークセキュリティ分析は、1 つだけの手法を適用した機能ではありません。進化する脅威の一歩先を行くには、ネットワーク可視性と分析ソリューションを複数のメソッドと組み合わせて使用できる必要があります。まず、包括的な可視性を得るために適切なデータを収集し、振る舞いモデリングや機械学習などの分

析手法を使用します。これらはすべて、悪意のあるキャンペーンを認識し、疑わしい動作を特定した脅威にマッピングするグローバルな脅威インテリジェンスによって補完され、検出の信頼性が向上します。Secure Network Analytics はこれらの各メソッドを適用して、組織が境界を越えた可能性のある攻撃や組織内の脅威、暗号化されたトラフィックに潜む脅威を特定して阻止できるよう支援します。

図 4. Cisco Secure Network Analytics 内の複数の分析アプローチが連携してセキュリティを改善



詳細はこちら

製品とソリューションのページ：

Cisco Secure Network Analytics

Cisco Secure Cloud Analytics

暗号化トラフィック分析

無料の可視性アセスメント

関連資料

基本

ブログ：暗号化されたマルウェアトラフィックの検出（暗号解読なし）

ブログ：Cognitive Research：悪意のあるネットワークトラフィックのディテクタについて

ブログ：Cognitive Threat Analytics：高度な脅威調査の透明性

ブログ：Cognitive Threat Analytics：プロキシをセキュリティデバイスに変える

ブログ：グローバル規模での暗号化トラフィックの保護

ブログ：学習ループを閉じる：意思決定フォレストを使用した高度な脅威の検出

Advanced

- Anderson B.、McGrew D.（2016 年）。コンテキストフローデータによる、暗号化されたマルウェアトラフィックの特定。AISec 2016 年
- Grill M.、Pevny T.、Rehak M（2017 年）。ローカル適応多変数スムージングによるネットワーク異常検出の誤検出の低減。Journal of Computer and System Sciences。83(1):43–57
- Komarek T.、Somol P.（2017 年）。HTTPS データでのマルウェア検出のためのエンドノード フィンガープリント In Proceedings of the 12th International Conference on Availability, Reliability, and Security（77 ページ）。ACM
- Jusko J.、Rehak M.、Stiborek J.、Kohout J.、Pevny T.（2016 年）。ボットネットのコマンド & コントロール検出に振る舞いの類似性を使用する。IEEE Intelligent Systems。31(5):16–22
- Bartos K.、Rehak M.（2015 年）。IFS：ネットワークセキュリティのためのインテリジェントなフローサンプリング：適応型アプローチ。International Journal of Network Management。25(5):263–282
- Letal V.、Pevny T.、Smidl V.、Somol P.（2015 年）。大規模なコンピュータ ネットワーク データで変分ベイズを使用して新しい悪意のあるドメインを検出。NIPS 2015 Workshop：Advances in Approximate Bayesian Inference（1 ～ 10 ページ）
- Rehak M.、Pechoucek M.、Grill M.、Stiborek J.、Bartos K.、Celeda P.（2009 年）。ネットワークトラフィック モニタリング用の適応型マルチエージェントシステム。IEEE Intelligent Systems。24(3)

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp