ホワイトペーパー

Akamai API Security の異常検知

API は、組織が顧客へのサービス、収益の創出、効率的な事業運営を行えるようにするための重要な要素です。しかし、その継続的な増加、機微な情報への近接性、セキュリティ制御の欠如により、API は今日の攻撃者にとって魅力的なターゲットとなっています。API が悪用される可能性や攻撃の兆候をプロアクティブに特定するためには、ユーザーのふるまいに関するリアルタイムの知見を得ることが重要です。

Akamai API Security ソリューションの異常検知機能の目的は、組織の API を悪用しようとする悪性の試みの兆候を示す、ユーザーの異常なふるまいを特定することです。通常のトラフィックのベースラインを確立することにより、Akamai の異常検知機能は受信したリクエストをベースラインと比較し、攻撃者によって実行されている可能性があるかどうかを判断できます。

Akamai の異常検知アルゴリズムは、次のような異常なふるまいを特定します。

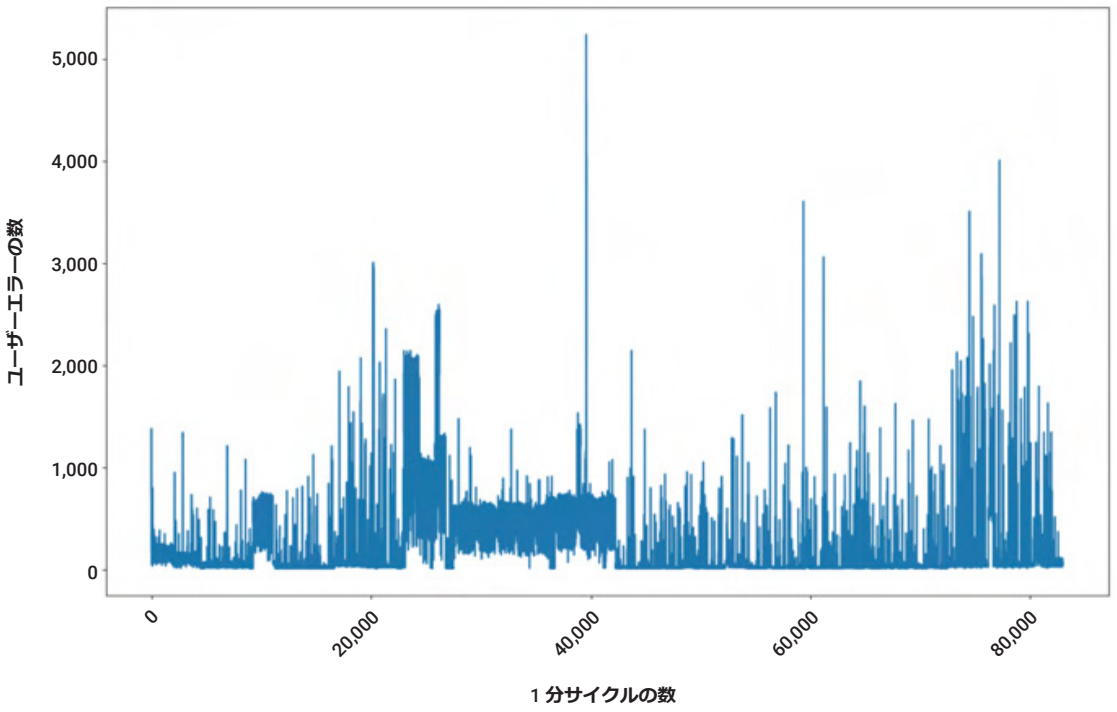
- API リクエストにおいて予期しないフィールドを使用している
- 通常のユーザーよりも多くのデータをサーバーから取得している
- 他のユーザー／管理者リソースを使用しようとしている
- 予期しない順序で API を呼び出している

このアルゴリズムは教師なしのオンライン学習人工知能および機械学習（AI ／ ML）モデルをベースとしており、このモデルはトラフィックの統計的挙動の複数の特性を学習し、一定の学習期間後に異常なインシデントを検知します。Akamai のモデルは時間の経過とともにトラフィックの変化に適応し、ユーザーによってフォールス・ポジティブ（誤検知）とラベル付けされた異常に適応します。

学習フェーズでは、顧客のデータを解析し、さまざまな API、認証方法、ユーザー、データ型などを識別します。API ごとに、API ヒット数、生成されたエラー数、認証されたリクエストの割合、サーバーから取得されたデータの量など、通常のユーザートラフィックの特性のリストが作成されます。Akamai のアルゴリズムは、ユーザーの特性と API の特性を、アルゴリズムが学習した統計モデルで予想される結果と比較して、ユーザーの異常を検知します。

Akamai API Security の異常検知の仕組み

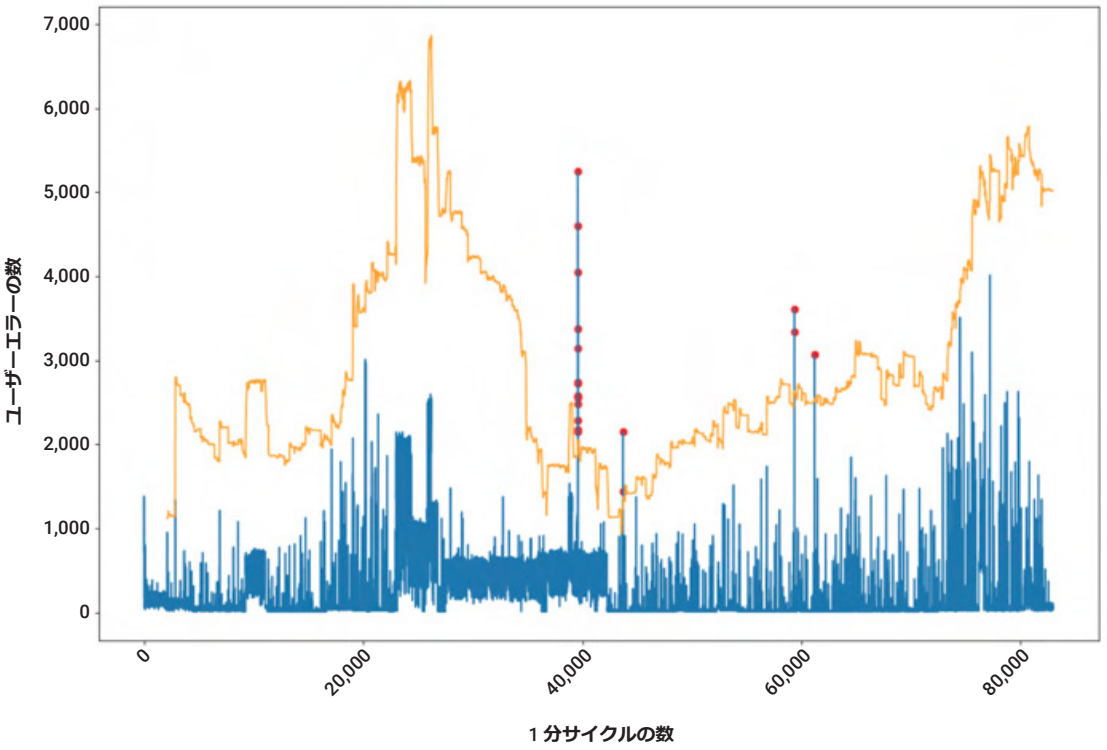
Akamai API Security の異常検知機能は、他のユーザーよりも過度に多くのエラーを発生させるユーザーを特定します。これにより、総当たり攻撃、パススキャン、スクレイピングなどの攻撃を特定できます。次のグラフは、環境内で 1 分サイクルごとにユーザーが生成するユーザーエラーの最大量を示しています。



このシナリオでは、異常を特定する上で次のようなさまざまな課題があります。

1. しきい値を計算する際、モデルはデータドリフトを把握している必要がある。
2. モデルの学習期間中に異常を学習しないようにしたい。
3. 学習は続々と行われるため、モデルはデータ全体を見ておらず、時間ステップごとに調整する必要がある。
4. アラートはリアルタイムである必要があるため、アルゴリズムは将来のデータを頼りに異常を予測することはできない。
5. ユーザーに対するスパミングを回避するために、そのデータに関する統計的に確かなしきい値を学習する必要がある。

次のグラフでは、モデルが受信データに応じてしきい値を調整することにより、こうした要件をどのように満たしているかを確認できます。



オレンジ色の線はモデルによって計算されたしきい値関数を表し、赤い点はその関数に基づいて検知された異常を表します。

よくある質問

Akamai の異常検知アルゴリズムに必要な学習期間はどれくらいですか？

Akamai のほとんどのアルゴリズムは、2 ～ 7 日間の学習期間が必要です。また、アルゴリズムの学習期間は、学習期間中に観測されたさまざまなユーザーのふるまいの数によって変動します。

異常なふるまいが検知された場合、アラートが生成されるまでにどれくらいの時間がかかりますか？

Akamai のアルゴリズムは、ほとんどの場合、異常なトラフィックを受信した瞬間から 30 ～ 60 秒以内にクライアントへの関連アラートを生成します。

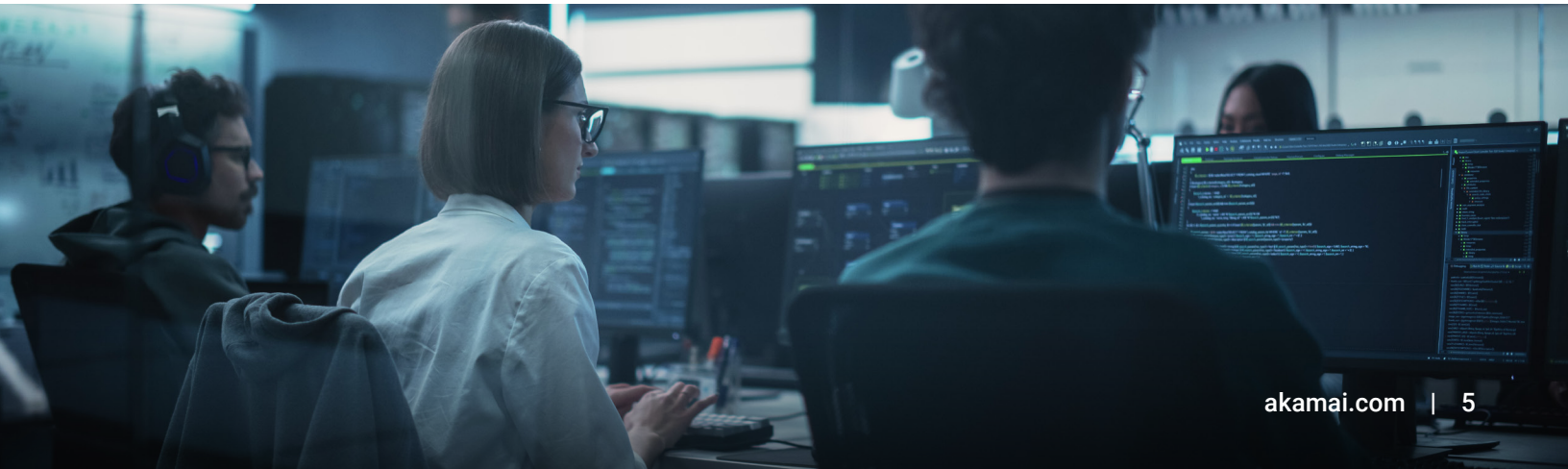
このアルゴリズムでは、教師ありのモデルと教師なしのモデルのどちらが使用されていますか？

Akamai のアルゴリズムは、教師なしのモデルをベースとしています。そのため、顧客の環境の特性に関する情報がなくても、各顧客の環境に適応できます。また、Akamai のアルゴリズムは、オンライン学習により、時間の経過とともに環境の変化に適応します。

Akamai API Security が検知する異常はどのような種類のものですか？

Akamai API Security は、次の 2 種類の異常を検知します。

- パターンベース ― トラフィックの悪性パターンの識別に基づく異常（Web エクスプロイト手法など）や、既知の悪性ユーザーエージェントの識別に基づく異常（コマンドインジェクション、パストラバーサル、不審なユーザーエージェントなど）。
- ふるまいベース ― ユーザーの学習行動に基づく異常や、異常なユーザーの識別に基づく異常（API の過剰使用、範囲違反、オブジェクトレベルの認可の不備など）。



異常をトリガーする際に Akamai API Security はどのパラメーターを考慮しますか？

Akamai のアルゴリズムは、トラフィックの統計分析を実行することによって導き出される次のような複数の特性に基づきます。

- API を使用する異なるユーザーの数
- API の認証ステータス
- サーバーのレスポンスコード
- ユーザーが取得するデータの量
- ユーザーの IP ジオロケーション
- ユーザーのユーザーエージェントなど

ユーザーはアルゴリズムの感度を制御できますか？

はい。ユーザーは関連するポリシー感度を変更することにより、各異常の感度を制御できます。ポリシーの感度は 1（低）から 5（高）までの数値で表されます。最も高い値を指定すると、システムは Akamai API Security の各異常ポリシーに対して設定できる最も高い感度となります。Akamai のアルゴリズムは、このパラメーターをモデルの一部として考慮します。

ユーザーは、Akamai が警告した問題を誤検知としてマークできますか？また、それによってアルゴリズムにどのような影響が生じますか？

はい。異常検知を改善するために、ユーザーは関連する問題を「誤検知」としてマークできます。問題が誤検知としてマークされると、アルゴリズムはこれを考慮し、ユーザーからのインプットに従ってモデルを調整します。

Akamai は、同じ攻撃シナリオを送信し続けるユーザーのいるクライアントに対する「スパミング」をどのように回避しますか？

Akamai のアルゴリズムは、同じユーザーや API についてトリガーされ続けている同様の問題を特定します。この場合、アルゴリズムは同様の問題を一定期間無視します。

Akamai はデータのドリフトや季節変動にどのように対処しますか？

Akamai API Security は、複数の異なるアルゴリズムを使用してデータの異常を検知します。基盤となるデータの前処理とアルゴリズムの複雑さに応じて、しきい値の調整を緩めたり、異常検知のために統計的に確かなしきい値が必要とされるサイクルごとに調整を行ったりできます。スパム制御と組み合わせることで、特定のアルゴリズムがしきい値を調整するために追加のサイクルを必要とする場合でも、簡単なインターフェースを実現できます。

Akamai はデータポイズニングにどのように対処しますか？

Akamai API Security はオンライン学習アルゴリズムであるため、次のようなさまざまな課題に対処する必要があります。

- 新しい API
- 既存の API の新しいフィールド
- フィールドの値タイプ／範囲の変更
- サーバーの可用性の問題
- エラー（404、500 など）を引き起こす可能性のある API のバグや、学習するものとしないものを決定する上でのその他の課題（Akamai は、最低限のユーザー数、期間、持続性の組み合わせを、学習を開始するための要件とすることにより、そのような異常を学習しないよう予防策を講じています）

カスタマイズされた Akamai API Security のデモをスケジュールいただき、Akamai がどうお役に立てるか、ぜひご確認ください。