Akamai

ホワイトペーパー

API セキュリティベンダーにするべき 13 の質問

はじめに

BtoB の API ネットワークは爆発的に拡大しています。Internet of Things（IoT）デバイスの世界は拡大し続け、実際のデータをアプリケーションに取り入れる新たな機会を開発者にもたらしています。

しかし API は多くの新たなイノベーションや成長の機会を生み出している一方で、次のような新たなセキュリティ上の課題ももたらしています。

- API 認証情報の盗難
- API 偵察の見落とし
- 認証と認可の誤設定
- 保護されていないシャドー API やゾンビ API
- リモートコード実行、インジェクション、ローカル・ファイル・インクルージョンなどの攻撃手法
- データの漏えいや窃盗
- API スクレイピング
- ビジネスロジックの悪用

セキュリティベンダーは、こうした API 脅威やその他の API 脅威を検知し、緩和する多くの選択肢を提供していますが、そうした選択肢はどれも同様に効果的で使いやすいわけではありません。

以下の 13 の質問を、API セキュリティベンダーとの話し合いの枠組みにし、各ベンダーの製品がいかに効果的に貴社の API セキュリティニーズに対応しているかを評価することができます。

1 貴社の API セキュリティ製品は全社的な API 探索を実行できますか？

セキュリティチームが直面する最大の問題の 1 つに、自社が接するすべての API の完全で正確なインベントリを持っていないという問題があります。セキュリティチームが見落としている未登録のシャドー API の多くは、正式な API 管理やセキュリティフレームワークに含まれていません。組織がもう廃止したと考えているゾンビ API に、依然としてアクセス可能であることもよくあります。許可されている登録済みの API の中にも未登録の API パラメーターがあり、利用可能になっている場合があります。東西、南北、アウトバウンドのすべての API を探索することが必要不可欠です。全社的な API の完全な可視性を確保するためには、さまざまなテクノロジーやクラウドプラットフォームの既存の API のアクティビティデータをテストするしかありません。

2 貴社の製品は API を継続的に探索できますか？できる場合、そのプロセスはどの程度手動ですか？

DevOps のプロセスは迅速に進められるため、API は常に現れては消えています。そのため、API のある時点でのインベントリでは不十分です。API セキュリティ製品は、継続的に探索を実行して、新たな登録済み API のインベントリを確実に作成し、分析し、保護できる必要があります。また、新たなシャドー API やゾンビ API も検知できる必要があります。さらに、調査結果の解釈と対処が必要になってチームに継続的な負担を掛ける製品は、長期的には持続可能ではありません。一方で、API の探索と評価に自動化と機械学習を適用する製品は、チームの毎日の「やることリスト」に手作業を追加せず、運営を円滑にします。

3 貴社の製品は API 登録ツールと登録プロセスをどうサポートしていますか？

登録アプローチを API セキュリティプラットフォームに統合すると多くのメリットがあるため、ベンダーがこうした機能を提供していることを確認する必要があります。たとえば、継続的インテグレーションと継続的デリバリー（CI ／ CD）プロセスの一環として、既存の Swagger ドキュメントを API セキュリティプラットフォームに自動的にアップロードすることで、シャドー API の検知やシャドーパラメーターの特定の精度が向上します（ただし、探索した API パラメーターと登録済みのパラメーターを比較する機能を備えている必要があります）。セキュリティプラットフォームは、ボタンをクリックするだけで、未登録の API のカスタム Swagger ファイルを作成できる必要もあります。こうした機能を利用して、開発者は登録プロセスに着手し、改善することができます。

4 貴社の製品を当社の環境に導入するのに、どのくらいの時間と労力がかかるでしょうか？

既存のシステムから API アクティビティデータを負担なくインジェストして分析できる、サービスとしてのセキュリティ（SaaS）ベースの API セキュリティ製品を使用すると、最も迅速かつ効率的に導入できます。API セキュリティ向けに入念に設計された SaaS アーキテクチャを数分で自社環境に統合することで、価値創出までの時間を桁違いに短縮し、システムアップデートに伴う継続的なコストとリスクを排除できます。さらにアジリティを高めるためには、Web アプリケーションと API の保護（WAAP）機能と API 検知応答機能の両方を提供するベンダーを探して、「着信するトラフィックを保護するソリューション」と「組織内のすべての API トラフィックを保護するソリューション」間を API トラフィックデータがシームレスに流れるようにする必要があります。

5 貴社の製品は、探索されたリスクの高い API の特定と優先順位付けをどうサポートしていますか？

包括的な API インベントリを初めて見たら、心強く思うと同時に圧倒されるかもしれません。多くのセキュリティチームは、情報過多に悩まされ、API セキュリティで取り組むべき対象エリアを特定するのに苦労しています。こうした状況を回避する最善策は、セキュリティチームに代わって、こうした以下のような作業の多くを実行できる API セキュリティ製品を選択することです。

- 機微な情報へのアクセスを可能にする API の存在を強調表示する
- 自動的に機微な情報にタイプ毎（個人を特定できる情報、メールアドレス、クレジットカードデータなど）のラベル付けをする

API セキュリティプラットフォームは、カスタムのラベル付けカテゴリーを作成可能である必要もあります。そうしたことができれば、API チームとセキュリティチームは共通の言語で話し合い、ビジネス目標やセキュリティ関連の懸念について足並みを揃えることができます。

6 貴社の製品は、ふるまい分析によって望ましいふるまいのベースラインを特定し、異常を見つけることができますか？

多くのタイプの攻撃は、攻撃の特徴によって WAAP レベルでブロックして検知できます。しかし、オブジェクトレベルの認可の不備（BOLA）など、2023 年度の Open Web Application Security Project（OWASP）API Security Top 10 に挙げられている多くの攻撃タイプは、この方法で探索できません。こうしたタイプの攻撃はより受け身で、ビジネスの悪用に特化しているため、検知しにくくなっています。すべての API 脅威ベクトルを効果的に防御するためには、ふるまい分析と機械学習を活用するしかありません。真のふるまい分析を実現するためには、大規模なデータセット、環境の仕様を学習する機械学習アルゴリズム、グローバル情報に基づいて自動的にアップデートし、適応する柔軟性とアジリティが必要です。SaaS モデルは、こうした活動を大規模に実行できる唯一の現実的な手段です。

7 貴社は、有効なデータセットを取得し、分析して、正常なふるまいのベースラインを効果的に特定し、異常を検知することができますか？

多くの API セキュリティ製品は、個々の API 呼び出しか、よくても短期的なセッションアクティビティの監視に特化しています。しかし多くの正当なビジネスプロセスや攻撃は、はるかに長期間にわたって行われるため、これでは不十分です。API の使用を、スライディング・タイム・ウィンドウ（最低でも 30 日間）にわたって分析する必要があります。こうすることで、1 か月に 1 回しか実行されないビジネスプロセス（請求処理など）も含め、望ましいふるまいのより完全で正確なベースラインを割り出すことができます。また、数日間または数週間（および複数の API セッション）にわたり、ゆっくりと実行される攻撃も検知できるようになります。

8 貴社の製品は、API 生データ内のすべてのエンティティ、関係、アクティビティを特定して、ビジネスコンテキストを示すことができますか？

API アクティビティデータを対策に活かす最善策は、API の使用がビジネスにどのように影響しているのか、コンテキストを把握して、データをさらに充実させることです。API セキュリティプラットフォームによってさまざまなエンティティ間の関係を評価し、プロファイリングするためには、以下の特定機能やラベル付け機能が必要不可欠です。

- API ユーザーを示すもの（IP アドレス、API キー、アクセストークン、ユーザー ID、パートナー ID、マーチャント ID、サプライヤー ID などのユーザーエンティティ）
- ビジネスプロセスを示すもの（予約、支払い、請求、口座残高などのビジネス・プロセス・エンティティ）

API によって生成される膨大なデータを望ましいふるまいの有意義かつ理解可能なベースラインに変換するためには、こうしたレベルの詳細な分析を行うしかありません。

9 貴社の製品は、API 内のすべてのエンティティ毎にすべてのアクティビティをプロットして、一定期間のふるまいの変化を示すことができますか？

API アクティビティと脅威をマクロレベルで理解し、監視することが必要不可欠ですが、分析の対象を特定のエンティティに絞り込めることも同様に重要です。たとえば、特定のビジネスパートナーの例外的なふるまいが特定された場合、そのエンティティの一定期間のすべてのアクティビティを確認できることが極めて重要になります。ビジネス・プロセス・エンティティについても同じことが言えます。自社の API 上のすべてのエンティティに、一定期間内のいつ、何が起きたのか、すべての状況を把握できれば、通常の使用とビジネス悪用の状況が明らかになり、強力な可視化が実現します。アクティビティを巻き戻して 1 件のアラートの前後に何が起きたのかを把握できる機能があれば、ビジネスロジックの悪用を理解する強力なツールとなります。

10 貴社の製品は、既存のツール、プロセス、ワークフローにどのように統合できますか？

既存のセキュリティ情報およびイベント管理（SIEM）製品にアラートを送信できれば便利ですが、それは出発点に過ぎません。セキュリティチームはより高度な SOAR（security orchestration, automation, and response）ツールをますます活用して、セキュリティ脅威やインシデントの検知時に事前に定義済みのワークフローを開始するようになっています。また、多くの API セキュリティの問題を解決するためにはセキュリティチーム以外の開発者によるアクションが必要なため、API セキュリティプラットフォームは開発チームの問題追跡ツールやワークフロー管理ツールとも統合できる必要があります。既存のセキュリティツールで API トラフィックを分析している場合、API を使用して、CDN、Web アプリケーションファイアウォール、または API ゲートウェイでのレスポンスをオーケストレーションし、独自のプレイブックを作成できる必要も当然あるでしょう。

11 事前に脅威をハンティングし、リスクを緩和するために、貴社製品の API およびアクティビティデータにクエリーを実行することはできますか？

セキュリティツールと開発ツールの統合は、ツールに一方的にアラートを送信するだけのブラックボックスであってはなりません。セキュリティチームや API チームは、アラートや問題の背後にあるソースデータを活用できる必要があります。ユーザーが API セキュリティプラットフォームを他のツールやインターフェースと統合して、組み込みの Web インターフェースから直接、または API 経由で API の詳細についてクエリーを実行できる API セキュリティプラットフォームを探す必要があります。こうしたプラットフォームがあれば、セキュリティチームは自ら、事前の脅威ハンティングを効率的かつ効果的に実行できるようになります。また、開発者をはじめとしたセキュリティを直接担当していない関係者も、API が正当に使用されている一方で、どのように攻撃者に狙われているのか理解することができます。

12 収集したビジネス関連の機微な情報が保護されていることをどのような手順で確認できますか？

今日の脅威環境で API のセキュリティを確保する高度なふるまい分析は、クラウドの規模でなければ実現できません。API データセットの規模と機密性を考慮すると、セキュリティベンダーにデータを確実に保護できることを確認することが重要です。ベンダーがクラウドインフラのセキュリティを確保するために使用している手法を検証することが重要ですが、それは出発点に過ぎません。API セキュリティベンダーに、トークン化（機微な情報をクラウドに送信する前に匿名化されたトークンに置き換える仕組み）などの技法を使用するように求める必要があります。そうすることで、ベンダーや上流のクラウドプロバイダーがセキュリティインシデントに遭遇してもデータプライバシーを確保することができます。

13 このソリューションは API アクティビティデータへのきめ細かなアクセスを提供していますか？

データは、コンプライアンスから攻撃防御のコンテキストに至るまで、あらゆる戦略上、極めて重要な要素です。多くのベンダーは、長期の API データに対応する独自のストレージを提供していますが、実際にどのようなものを提供しているのか深く掘り下げて確実に理解する必要があります。API アクティビティの侵害は、ゆっくり時間をかけて進行する場合があり、1 回のアラートでは済まないため、アラートを発するだけのソリューションですべての状況を把握することはできません。一方、包括的なベンダーは、すべての API アクティビティを記録して盲点を排除し、そうしたアクティビティを詳細に確認できるツールを備えているため、曖昧な機械学習モデルで状況を見失うことがありません。こうしたきめ細かなデータアクセスを確保し、攻撃のアラートを受けてから事後対応する前に、脅威をプロアクティブに監視できるようにすることが重要です。

API セキュリティベンダーにするべき 13 の質問

1. 貴社の API セキュリティ製品は全社的な API 探索を実行できますか？
2. 貴社の製品は API を継続的に探索できますか？できる場合、そのプロセスはどの程度手動ですか？
3. 貴社の製品は API 登録ツールと登録プロセスをどうサポートしていますか？
4. 貴社の製品を当社の環境に導入するのに、どのくらいの時間と労力がかかるでしょうか？
5. 貴社の製品は、探索されたリスクの高い API の特定と優先順位付けをどうサポートしていますか？
6. 貴社の製品は、ふるまい分析によって望ましいふるまいのベースラインを特定し、異常を見つけることができますか？
7. 貴社は、有効なデータセットを取得し、分析して、正常なふるまいのベースラインを効果的に特定し、異常を検知することができますか？
8. 貴社の製品は、API 生データ内のすべてのエンティティ、関係、アクティビティを特定して、ビジネスコンテキストを示すことができますか？
9. 貴社の製品は、API 内のすべてのエンティティ毎にすべてのアクティビティをプロットして、一定期間のふるまいの変化を示すことができますか？
10. 貴社の製品は、既存のツール、プロセス、ワークフローにどのように統合できますか？
11. 事前に脅威をハンティングし、リスクを緩和するために、貴社製品の API およびアクティビティデータにクエリーを実行することはできますか？
12. 収集したビジネス関連の機微な情報が保護されていることをどのような手順で確認できますか？
13. このソリューションは API アクティビティデータへのきめ細かなアクセスを提供していますか？

すでにお気付きかもしれませんが、Akamai API Security は、このリストに挙げた保護を効果的に提供することができます。Akamai のソリューションの詳細をご確認ください。

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 12 月。