API 探索の決定版ガイド

目次

API 探索の重要性

API セキュリティの取りくみを始めたばかりでも、戦略をさらに強化する場合でも、組織全体で使われているすべての API を見つけてリスト化することは、基礎として欠かせない手順です。何故なら、企業が構築するアプリケーション、クラウドに移行するワークロード、そして従業員がコラボレーションに使用するツールのすべてにおいて、その裏側ではデータの交換、多くの場合は機微な情報の交換を行う API が存在するからです。課題となるのは、ほとんどの組織（完全なインベントリの価値を理解している組織でさえも）が、実際には API の大部分を見ることができないことです。

見えないもののセキュリティを確保することはできません。

組織がクラウド中心のデジタル化を進めるにつれ、その API 資産の範囲、規模、複雑性は増大します。API は、多くの場合、オンプレミスからハイブリッドクラウドまで、複数の環境に分散しています。事態をさらに複雑にしているのは、API エコシステムが自社のネットワークやクラウドを超えて広がっていることにあります。サードパーティや開発者エコシステムに属するアプリ、サービス、システムと、貴社の API が築いてきた無数の接続を思い出してください。

API の対象範囲、規模、複雑性が増すにつれて、次のような点についてリアルタイムで知見を得ることが困難になります。

- 独自の開発チームを持つことも多い、さまざまな事業部門のどこに API があるか
- API がどのように設定されているか、どこにルーティングされているか、認証と認可が適切に制御されているか
- API が呼び出された際に機微な情報を返す場合、誰がそのデータにアクセスできるか

問題をさらに厄介にしているのが、組織が蓄積した API の大部分が管理されておらず、目に見えない上に、多くの場合保護もされていないことです。このような API には、休眠 API、シャドウ API、ゾンビ API が含まれ、多くの場合、API ゲートウェイや Web アプリケーションファイアウォール（WAF）など、一般的に使用されるツールの防御をすり抜けてしまいます。確かにこれらの防御ツールにはメリットがあり、基本的な保護を提供しますが、今日の API の脅威の状況では、特化型の API セキュリティソリューションが提供する、より高度な可視性、リアルタイムの保護、継続的なテストが必要です。

すべての API を探索できれば、各 API のリスクの評価、組織の API セキュリティ体制の把握、攻撃を防止するリアルタイム保護を適用するために得られた知見の活用など、次の必須ステップへの基盤が得られます。このホワイトペーパーでは、以下について説明しています。

- 特定のタイプの API がセキュリティチームにとって非常に把握しにくい理由についての知見
- 可視性を高めて攻撃の防止に役立つ API 探索機能の詳細

API を見つけるのが非常に難しい理由

運用チームやセキュリティチームが把握していない未管理の API が本番環境にあるケースも珍しくなく、さまざまなサイバー・セキュリティ・リスクや運用上の問題にさらされています。公開された API や誤設定の API が蔓延し、保護されていないため、攻撃者に侵害されやすくなっています。そして、その影響は甚大です。API に対する攻撃は、企業の収益、回復力、規制コンプライアンスを脅かす可能性があります。

野良 API が発生する原因は 4 つあります。

1. API ショートカットとプロセスの失敗

不正な API の一部は、適切なユーザーに通知しなかったことが原因で発生します。たとえば、事業部門（LOB）チームが IT 部門に通知せずに特定のニーズに対応する API を作成したり、開発者が手順を無視して実行したりする場合があります。企業買収の一環として「継承」した API も頻繁に見落とされます。このようなタイプの野良 API は、多くの場合、シャドウ API と呼ばれます。

2. 古いバージョンの API

古いバージョンの API はセキュリティが弱い可能性や既知の脆弱性がある可能性が高いのですが、多くの場合、いつまでも削除されないことがあります。ソフトウェアが更新されるまでの一定期間、古いバージョンと新しいバージョンの共存が必要となる場合があります。しかし、最終的にその API を無効化する担当者が退職したり、配置転換になったり、単に古いバージョンのシャットダウンを忘れてしまったりすることがあります。API を正式に廃止したにもかかわらず、見過ごしが原因で引き続き運用されている場合があります。どちらの場合も、ゾンビ API と呼ばれることがあります。

3. 継承された API

合併や買収の一環として継承された API も見落とされることが多く、シャドウ API になります。（存在する場合）インベントリは、システム統合の困難で複雑な作業の中で失われることがよくあります。小規模な企業の API 資産は、しばしば広範囲にわたって文書化されていないことが多いため、多数の小規模企業を買収している大企業は、特にリスクが高いと言えます。

4. 商用 API

一部の商用ソフトウェアパッケージには、他のアプリケーションや外部データソースと接続するための API が含まれています。このような API は、誰にも気づかれずにアクティベートされることがあります。

API 探索とは

API 探索とは、組織が自社の API を識別、カタログ化、管理し、リスクを評価するプロセスと一連の機能です。API 探索は、適切に実行すれば、次のような点で組織の役に立ちます。

- API スプロール（適切なドキュメントや監督なしに急増した API の積み重ね）を削減し、セキュリティ体制を改善する
- 現在の API の状況に対する理解を深め、今後の開発について十分な情報に基づいた意思決定を行う
- API へのアクセスを監視・制御し、認証されたユーザーのみがアクセスできるようにする

可視性を高めリスクを軽減する主な API 探索機能

多くの企業が自社の API を完全には把握していないのは、珍しいことではありません。ただし、正確なインベントリがなければ、さまざまなリスクにさらされます。API のインベントリを効果的に把握するためには、次のことができる必要があります。

検索

設定やタイプに関係なく、API を検索してインベントリを把握する

検知

休眠 API やゾンビ API などの未管理の API を検知する

特定

忘れられているドメイン、見落とされているドメイン、またはその他の不明なシャドウドメインを特定する

解消

可視性のギャップを解消し、潜在的な攻撃経路を明らかにする

API 探索のための新しいソリューションを評価する際は、以下の機能に留意してください。探索ツールには、これらすべてが組み込まれている必要があります。

あらゆる API タイプの探索

API 探索ツールには、RESTful、GraphQL、SOAP、XML-RPC、JSOF-RPC、gRPC など、あらゆる設定やタイプの API を特定できる機能が必要です。

きめ細かい API インベントリ

API 探索ツールには、インベントリを作成して、自動更新を通じて常に最新の状態を維持し、API を任意の属性に基づいて検索、タグ付け、フィルタリング、割り当て、エクスポートするための機能も必要です。

発見の困難な API の検知

未管理の API は、組織の API セキュリティイニシアチブより前から存在している場合があります。API スプロールの起源は、もはや企業に存在しない開発者チームにある可能性があります。このような API は通常、可視性もセキュリティ制御もなく、責任の所在が不明です。このような API を見つけられる機能が API 探索ツールには必要です。

シャドウ API ドメインの探索

シャドウ API に加えて、全体がシャドウなドメイン（まったく把握されていない API ドメイン名）が存在する場合があります。API 探索ツールは、セキュリティリスクをもたらす可能性のある、忘れられているドメイン、見落とされているドメイン、またはその他の未知のシャドウドメインを特定できる必要があります。

自動 API スキャン

スキャンは、盲点をなくし、次のような重要な問題を特定するために不可欠です。

- API キーや認証情報の漏えい
- API コードやスキーマの公開
- インフラの設定ミス
- ドキュメント、GitHub リポジトリ、Postman ワークスペースなどにおける脆弱性

このような問題や悪用できる情報源を特定することで、サイバー犯罪者に悪用される可能性のある潜在的な攻撃経路を把握できます。

統合が不要

API 探索ツールは、特別な統合やソフトウェアのインストールを必要とせずに、API 資産をくまなく探索し、脆弱な API やシャドウドメインを発見できる必要があります。これは、単純に適切なエージェントをインストールできなかった、またはツールを正しく設定できなかったために発生する可視性のギャップを回避するためには重要です。

限定的なカスタム開発

最後に、API 探索ツールは、トラフィックソースのためのカスタム開発が必要にならないように設計されている必要があります。これらのツールには、主要なインフラコンポーネントの統合があらかじめ組み込まれているべきです。通常、カスタム開発には時間がかかり、ソースオリジンに変更があると、統合をやり直す必要があるため、ただでさえ多忙な IT セキュリティチームでは対応が困難となります。

Akamai セキュリティは全 API の探索にどのように役立つか

包括的で継続的な API 探索機能により、次のようなメリットをビジネスに実現することができます。

- API アタックサーフェス全体の把握
- API のインベントリとドキュメントの更新にかかるコストの削減
- 規制要件や社内ポリシーへのコンプライアンスの強化

今日の脅威に対応するためには、次の 4 つの重要な領域を含む、完全な API セキュリティソリューションが必要です。その領域とは、API 探索、対策管理、脅威の検知と修復、セキュリティテストです。Akamai API Security は、これらの必須モジュールの 4 つすべてを備え、開発から運用まで、ライフサイクル全体を通じて API を保護します。API Security ソリューションは、API をパートナー、サプライヤー、ユーザーに公開する組織向けに構築されており、API を探索して、リスク状況を把握し、そのふるまいを分析し、内部に潜む脅威を阻止します。

API の攻撃手法、API の一般的な脆弱性、組織のセキュリティを確保する方法について詳しくは、こちらをご覧ください。

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。

Akamai

Akamai のセキュリティについて

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツ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：2024 年 10 月。