API セキュリティポスチャ管理の決定版ガイド

目次

API セキュリティが不可欠になった理由

組織の開発者は、職業柄、スピードが常に求められるため、API を使用して開発の効率性を向上させることがあります。しかし、API は開発者にとって使いやすく、ソフトウェアとデータ資産の相互運用性の鍵でもありますが、API セキュリティはその進歩の速さに追いついていません。

過去 12 か月間に API セキュリティインシデントに見舞われた組織の割合は 84% で、2023 年の 78% から増加しました [1]。その理由の 1 つは、攻撃者にとって API は効率のよい攻撃対象であることです。API は、構築の段階で設定ミス、コーディングエラー、認証制御の欠如という問題を誘発しがちです。そのため、非常に簡単に API 攻撃を実行して、データを直接盗むことができます。

また、データに関しては、完全な API インベントリを備え、どの API が顧客データや知的財産などの機微な情報を返すかを把握している企業はわずか 27% です（2023 年の 40% から低下）[2]。攻撃が増加している一方で可視性が低下しているため、企業は API セキュリティポスチャを評価、改善する方法を必要としています。

1、2.Akamai「API セキュリティの影響に関する調査」（2024）

包括的な API セキュリティとはどのようなものか

企業による API の使用が拡大するにつれ、アタックサーフェスも拡大し、新しいセキュリティ上の課題が生じています。

API のセキュリティを確保するにあたっては、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など、組織が従来使用してきたツールで、ある程度保護することはできます。しかし、API 資産は複雑化しています。たとえば、管理されていない API が無秩序に広がると、それを把握し、セキュリティを確保することが困難になるため、何らかの対策を講じる必要があります。

API は、企業のセキュリティ対策計画において大きく扱うべき要素です。また、現在の API リスクと攻撃方法に対抗するよう設計された専用の API セキュリティソリューションを使用することで、その計画の実施に必要な可視化と能力を得ることができます。これは、複数のツールが相互に補完して攻撃パスのすべてのステップをカバーする、多層防御の概念とは異なります。

API の探索、ポスチャ管理、ランタイム保護、セキュリティテストを実行するよう構築された包括的な API セキュリティプラットフォームがあれば、隠れた API リスクの把握、API 攻撃パスの特定、発見した脅威のリアルタイム緩和を実現しやすくなります。

Akamai の関連 e ブック『API 探索の決定版ガイド』では、API セキュリティの 1 つ目の重要な要素である、API の特定について説明しています。組織全体で使用されているすべての API を探索してインベントリを作成したら、次のステップは API セキュリティポスチャ全体を強化することです。

ポスチャ管理は、サードパーティプロバイダーのアプリケーションを購入し、それを自社のものとして使用、ブランド化、販売する企業にとって特に重要です。たとえば、過去 5 年間のほぼすべての新車に、ほぼ同じテレマティクス機能が搭載されています。攻撃者は、製造業者の API エンドポイントに脆弱性を発見すると、そこを容易な侵入口として使用し、リモートからアカウント乗っ取り攻撃を仕掛け、データを漏えいさせることが可能になります。

本書の内容

API ポスチャ管理により、組織は API ライフサイクル全体を通じて API のセキュリティを管理、監視、維持するためのツールを使用できるようになります。このガイドブックでは、脆弱性の検知や機微な情報の保護など、API セキュリティポスチャ管理の主要な要件について説明します。ポスチャ管理の方法を取り上げ、Akamai API Security ソリューションのポスチャ管理機能を紹介します。

なぜポスチャ管理が必要なのか

API セキュリティを維持する上で、API ポスチャ管理は非常に高い効果を発揮します。どのような種類のデータが流れているか、脆弱性や設定ミスがあるか、API が適切に認証されているかなどを明らかにすることで、探索された API のリスクを把握できます。API の脆弱性を特定して迅速に修正できるようになるため、攻撃が発生する前に是正措置を講じることができます。

包括的なポスチャ管理により、API に関するすべてのアクティビティが可視化されるため、セキュリティポリシーの適用、規制へのコンプライアンスの確立、API エコシステムの変更の監査が可能になります。攻撃、不正なユーザー、データ漏えいから API が保護され、セキュリティが確保されます。それらはいずれも、評判に対する深刻なダメージ、ビジネス上の損失、規制上の罰則につながる可能性があります。

完全な API インベントリを備え、どの API が機微な情報を返すかを把握している企業はわずか 27% です（2023 年の 40% から低下）[3]。

3. Akamai「API セキュリティの影響に関する調査」（2024）

ポスチャ管理のベストプラクティスを実行すると、API アタックサーフェスが最小限に抑えられ、API リスクの大部分が緩和されます。組織の API や機密データストアをすべて網羅したインベントリを作成することは、ポスチャ管理を適切にする上で不可欠です。これより、API ポスチャ管理のその他の要素（脆弱性の検知、API の監視、問題の修正）について説明します。

- ## 脆弱性の検知

  分析：ソースコードによくある脆弱性がないか検査し、API が外部システムとどのようなやり取りをしているのかを把握し、その認可機能と認証機能を評価します。

  監視：設定ミスを特定し、脆弱性を検知し、ベースラインの API のふるまいを把握するために、API との間のトラフィックを検査します。

API セキュリティプログラム全体から見れば、ポスチャ管理はその一部にすぎません。運用前に包括的なテストを実施し、本番環境に脆弱性が存在しないようにすることも非常に重要です。

- ## API の監視

  本番環境での API コールの識別と監視、API リクエストの追跡、ベースラインの使用状況からの逸脱の検知、予め定められたしきい値を API の使用が超えた場合のアラート作成を行います。

- ## 修正

  脆弱性を特定し、コードの変更、セキュリティ設定の微調整、API の欠陥へのパッチ適用によって API のセキュリティとコンプライアンスを強化します。適切なポスチャ管理を行えば、脆弱性が悪用されないよう事前に修正することができます。

組織の存続に不可欠なポスチャ管理機能

お読みいただいてる方の中には、自分の会社が可能な限り強力な API セキュリティポスチャを講じていないと考えている方や、強く疑っている方もいると思います。ここでは、ポスチャ管理ツールに何が備わっていなければならないのかについて説明します。

- **機微な情報の分類**
  公開されている情報源から気象データを提供する API よりも、クレジットカード情報を送信する API の方がはるかに大きな懸念事項となります。API ポスチャ管理ツールは、クレジットカードのデータ、電話番号、社会保障番号（SSN）などの機微な情報にアクセスできる API の数や、API を介して機微な情報にアクセスしたユーザーの数をすばやく特定する機能を備えている必要があります。

- **設定の評価**
  サイバー攻撃の多くは、API トラフィックの仲介や保護を行うネットワーク、API ゲートウェイ、ファイアウォールの単純な設定ミスが原因で発生します。強力なポスチャ管理には、ログファイルや設定ファイルなど、インフラやソフトウェアの設定を定期的にスキャンする機能が必要です。定期的にスキャンすることで、設定ミスや脆弱性を発見し、設定ドリフトによって生じるリスクを特定できます。

- **攻撃確実度スコア**
  API のふるまい、ネットワーク・トラフィック・パターン、ジオロケーションデータ、脅威インテリジェンスフィード、その他のコンテキスト要素など、外部および内部のシグナルを評価するためにトレーニングされた高度な機械学習アルゴリズムを使用し、攻撃の確実度をスコアリングできるエンジ

ンを探す必要があります。このようなエンジンがあれば、検知されたランタイムインシデントが悪性アクティビティの結果かどうかの確実度を判断する上で役に立ちます。この独自の機能により、顧客は重大な脅威に迅速に狙いを定め、攻撃である可能性の高いアクティビティに対する自動修正および通知フローを作成できます。

- **カスタムワークフロー**
  重大度をカスタマイズできることに加え、脆弱性が特定された場合に直ちにアクションを実行するワークフローを作成できる必要があります。カスタムワークフローは、トラブルチケットの作成から主要関係者への通知、ネットワーク設定の更新まで多岐にわたります。

- **ドキュメントの自動生成**
  API ドキュメントとは、API の機能と使用方法を利用者に伝える文書です。API は、仕様に適合していることが評価され、正確に文書化されていなければ、安全であるとはいえません。ドキュメントが不十分または存在しない場合、セキュリティテストが困難になり、脆弱性が検知されないまま API が本番環境に展開されるリスクが高まります。

この問題は、API 開発をアウトソーシングしている場合、さらに深刻になる可能性があります。API セキュリティプログラムを成功させるためには、問題の原因に関係なく、古いドキュメントや不完全なドキュメント、欠落したドキュメントは許されません。

OpenAPI 仕様（旧称 Swagger）は、標準インターフェースを定めたものです。ポスチャ管理ツールには、API の現在および将来の状態に基づいて完全な OpenAPI ドキュメントを自動的に生成し、すべての API が適切に文書化され、ドキュメントが最新であるようにする機能が備わっていなければなりません。

保険業界のリーダーが Akamai を活用して API セキュリティポスチャを強化

消費者の好みが従来のサービスからデジタルサービスに移っているため、金融サービス企業はイノベーションを加速させる必要があります。米国の大手医療保険会社である Aflac は、他の多くの金融サービス企業と同様、API セキュリティの課題に直面しました。

Aflac は自社のニーズを満たすために、Noname API Security Platform（現在は Akamai API Security の一部）を導入しました。ポスチャ管理モジュールは、同社の API を通過するデータのタイプを識別し、どの API が機微な情報にアクセスするかを可視化し、データアクセスの異常を特定するために役立っています。

詳しくは、Aflac のケーススタディの全文をご覧ください。

「弊社の API フットプリントが大きいことは承知していました。そこで、すべての API が把握されていること、API の運用が完全に可視化されていること、セキュリティリスクがないか継続的にテストしていることを確実にしたいと考えました。

— Aflac 社、セキュリティ運用および脅威管理担当 VP、DJ Goldsworthy 氏

ポスチャ管理に対する Akamai のアプローチ

Akamai API Security ソリューションのポスチャ管理モジュールによって、トラフィック、コード、設定を包括的に把握して、自社の API セキュリティポスチャを評価できます。Akamai は、API と Web アプリケーション全体を通して真のアタックサーフェスがどのようなものなのかを判断し、API を介して移動するあらゆる形式の機微な情報を明確にすることで、機微な情報のセキュリティを確保できるようにしています。

API に設定ミスがあるだけで、サイバー攻撃に対して無防備になりかねません。ハッカーは内部に侵入すれば、機微な情報にすばやくアクセスし、それを流出させることができます。Akamai API Security ソリューションのポスチャ管理モジュールの主な特徴は次の通りです。

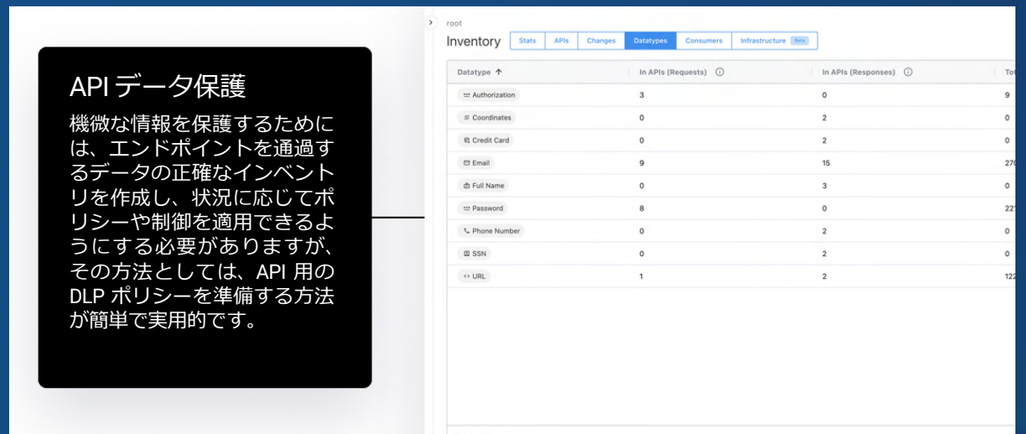
- オンプレミス、ハイブリッドクラウド、パブリッククラウドでの継続的な API 探索のためのアウトオブバンド統合
- スキーマ、ネットワーク配置、データタイプの詳細を含む、シンプルで検索可能な API インベントリ
- API ドキュメントの自動生成（OAS ／ Swagger）
- API の設定ミスや脆弱性のコンテキスト認識分析と優先順位付け
- OWASP API Security Top 10 のすべての脆弱性の検知
- 機微な情報および API の変更の検知と分類の自動化

API のリスクへの対処

API のコード内のリスクを明らかにするだけでなく、ネットワークのコンテキスト内でふるまいが典型的なものなのか、そうでないのかに注意しながら API トラフィックを監視することも重要です。

Akamai API Security ソリューションのポスチャ管理は、ログファイル、トラフィック履歴の再現、設定ファイルなど、可能な限り広範なソースを参照して、脆弱性を検知します。このソリューションは、OWASP API Security Top 10 のすべての脆弱性を検知し、データ漏えい、認可の問題、悪用、不正使用、データ破損から API を保護します。

Akamai は潜在的な脆弱性をインテリジェントに特定し、優先順位を付けます。脆弱性は手動でも、半自動でも修正できます。



また、WAF、API ゲートウェイ、SIEM ツールや ITSM ツール、ワークフローツール、その他のサービスを連携させることで、全自動で修正することもできます。

API データ保護

機微な情報を保護するためには、エンドポイントを通過するデータの正確なインベントリを作成し、状況に応じてポリシーや制御を適用できるようにする必要がありますが、その方法としては、API 用の DLP ポリシーを準備する方法が簡単で実用的です。

API の使用の増加に伴い、コンプライアンスは大きく変貌しつつあります。アタックサーフェスの拡大に応じて、規制がますます厳しくなっています。規制されている業界は今こそ、コンプライアンス計画に API を組み込む必要があります。

Akamai API Security ソリューションのポスチャ管理モジュールは、API を介して移動するあらゆる形式の機微な情報（クレジットカード、SSN、アドレス、保険情報などの個人を特定できる情報（PII）を含む）を特定します。そのような種類のデータへのアクセスの削減とデータ管理フレームワークの導入により、機微な情報が必要な場所にあり、脅威から守られている状態にすることができます。

API ポスチャ管理のメリット

顧客やパートナー、ベンダーとの間で組織がデジタル的にやり取りするたびに、その処理の背後でデータ（多くの場合、機微な情報）を迅速かつスムーズにやり取りできるよう API が機能しています。組織全体のすべての API を可視化し、そのリスクの属性（たとえば機微な情報を返すなど）を評価することで、急速に増加している攻撃ベクトルから組織を保護することができます。また、API セキュリティポスチャ管理は、データ漏えいの防止を目的としたグローバルな規制へのコンプライアンス遵守にも役立ちます。

すべての API を把握してセキュリティを確保することを義務付けているデータ保護規制の詳細をご確認いただけます。

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。

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 12 月。

Akamai