Akamai

ホワイトペーパー

API セキュリティに関する 8 つの推奨事項・非推奨事項

堅牢な API セキュリティ体制に不可欠な要素

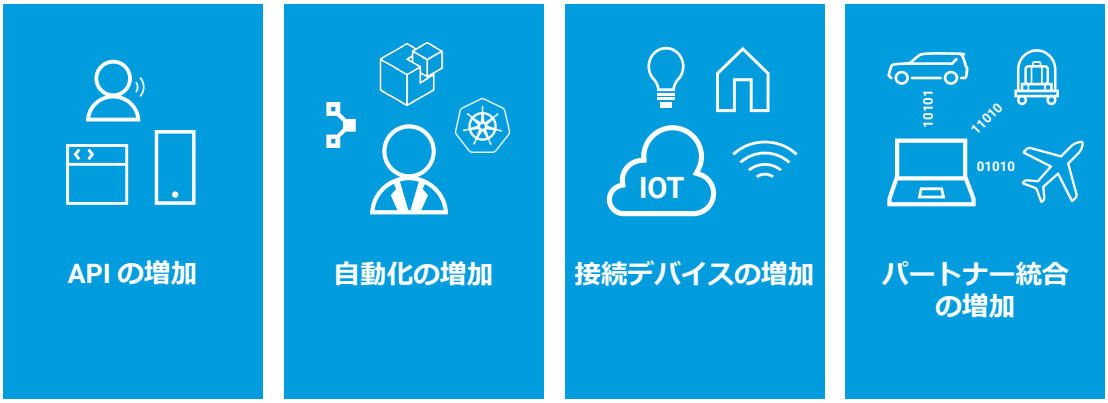
API の保護が複雑である理由

API セキュリティは多くの IT 幹部にとっての優先事項になっています。そして、それには正当な理由があります。次の事項について考えてみましょう。

「API の急増に伴い、API は攻撃者にとって魅力的なアタックサーフェスとなっており、セキュリティ担当責任者はその保護に苦心しています」

—『The Eight Components Of API Security』、Forrester Research, Inc、2023 年 9 月 28 日

API のリスク拡大要因



これらのリスクに対応するためには、以下の事実を踏まえて、効果的な API セキュリティを実装することが重要です。

API は動く標的である	
内部での API 認識	**外部への API 公開**
DevOps プロセスは高速に進展し、API の作成と廃止が目まぐるしく繰り返されるため、API のインベントリを正確な状態に維持することが困難である	API の取り扱いが未成熟だと、機密性の高い API を誤って外部に公開したり、多数のシャドー API が生まれる危険性がある

API は以下の 2 種類の脅威に対して脆弱である	
技術的脆弱性	**誤用と悪用**
攻撃者は、ソフトウェアの脆弱性や誤設定（OWASP API Security Top 10 など）を悪用する場合がある	技術的脆弱性がなくても、ビジネスロジックの悪用やデータスクレイピングなどが活発に行われる場合がある

API セキュリティという複雑な課題に対処するためには、入念なアプローチを通じて、以下のことを実現する必要があります。

最新テクノロジーを採用する

組織内の障壁を克服する

API 脅威環境全体に対応する

組織の API セキュリティを強化するために導入すべき重要な戦略（および避けるべき落とし穴）を以下にご紹介します。

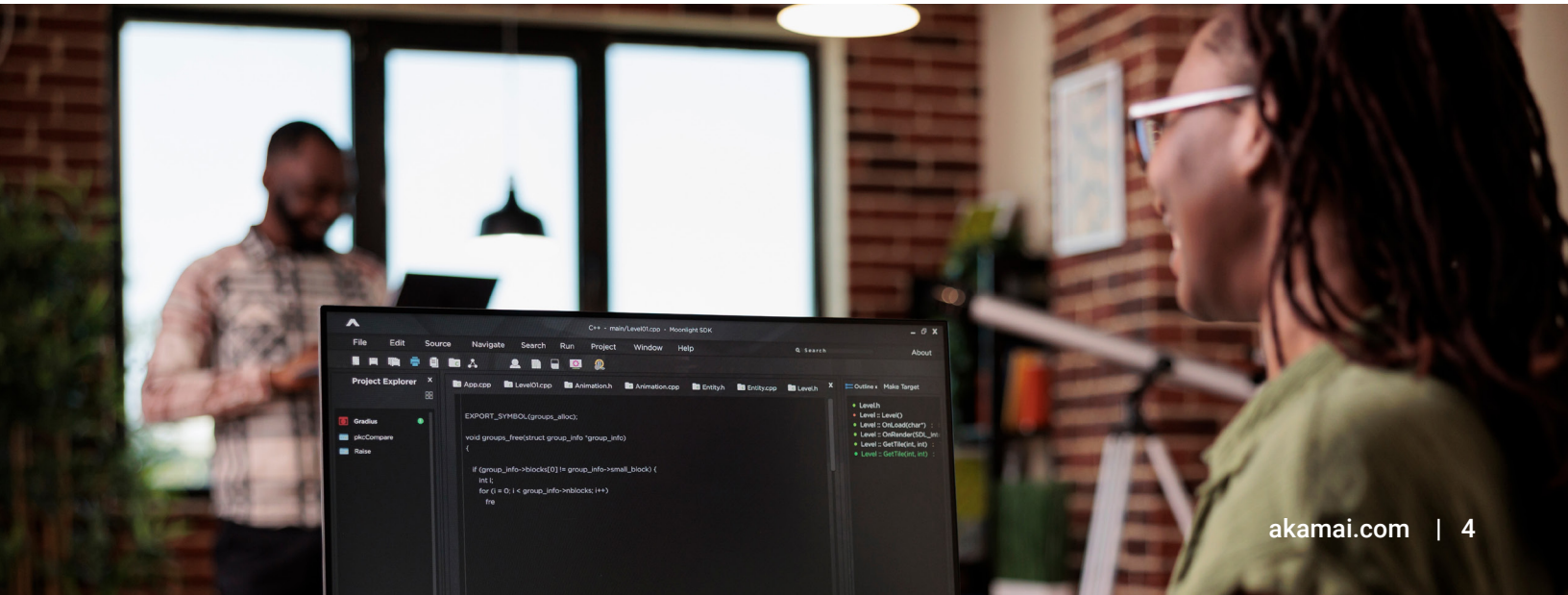
効果的な API セキュリティのための 8 つの推奨事項・非推奨事項

1 推奨 すべての API を可視化する

繰り返しになりますが、API の存在を認識していなければ、その API を保護することはできません。API の確認と監視が遅れると、その API は標的になる可能性が高くなります。すべての API を可視化するためには、API セキュリティプラットフォームを使用して、幅広いデータソース（API ゲートウェイ、ネットワークデバイス、マイクロサービス・オーケストレーション・ソリューション、クラウドプロバイダーなど）から情報をインジェストすることが重要です。具体的には、以下のことを実行できる API セキュリティソリューションが必要です。

時間	場所
• API を継続的に探索 • 個別の API コールを監視 • 短期セッションアクティビティを記録 • API のふるまいを経時的に分析	• エンタープライズ内のすべての API を探索 • レガシー API を探索 • シャドー API を特定

すべての API を可視化することで、API データ漏えいを防止できます。現在の攻撃者は、Low & Slow（少しずつ時間をかけた）攻撃を通じて API からデータをスクレイプするという、最新のデータ漏えい手法を用いています。この種の新たな攻撃から防御するための第一歩は、組織内のすべての API の場所を把握することです。



2 非推奨 クラウドを恐れる

Web アプリケーションファイアウォール（WAF）は、シグネチャベースの手法を用いて、不正 API が組織に入り込むことを防止するソリューションです。API 攻撃は進化しているため、幅広いリスクから API を完全に防御するためには、ふるまい分析を活用して、防御を強化しなければなりません。外部に公開する API だけでなく、組織内の API についても、ふるまいを監視することが重要です。

ふるまい分析を効果的に行うためには、API トラフィックをクラウドで分析する必要があります。セキュリティチームは、自社の活動に関する機微な情報をクラウドに送信したがらない場合があります。しかし、拡張性と柔軟性に優れたクラウドを活用しなければ、エンタープライズで生成される膨大な量の API データを幅広い検知と応答技術を用いて、ふるまい分析を行うことは極めて困難です。

加えて、セキュリティ担当者の人数には限りがあり、各担当者は既存の業務で手いっぱいです。オンプレミス製品の導入は複雑で時間がかかるため、業務の停滞の原因となります。API の使用が増加したことで、そのリスクも拡大しています。セキュリティチームは、さらなる後れを取るわけにはいきません。そのため、API セキュリティ戦略の一環として、クラウドを活用することが不可欠です。

3 推奨 戦略を策定する際にはビジネス状況を考慮に入れる

API の探索とセキュリティリスクの特定は、API アタックサーフェスを縮小するための第一歩にすぎません。次の 3 つの点について考えてみましょう。

1. 特定のパートナーの API 認証情報が漏えいしたかどうかを検知する方法は？
2. 企業スパイ活動の一環として、API に対するデータスクレイピングが行われているかどうかを検知する方法は？
3. ユーザーが請求書 API を悪用し、請求書番号を通じてアカウントデータを盗んでいるかどうかを検知する方法は？

1 番目のシナリオの場合、正当なユーザーが API 認証情報の漏えいの原因になっていると考えられます。したがって、この漏えいを検知する唯一の方法は、当該 API に想定外のふるまいが起きていることに気付く必要があります。2 番目と 3 番目のシナリオも、API に正当にアクセスしたユーザーが無許可のふるまいを行っている例です。上記 3 つのシナリオ以外にも、技術的状況だけでなく、ビジネス状況を理解することが重要となるケースは数多くあります。

4 非推奨 データを一方通行にする

効果的な API セキュリティアプローチには、アラートやイベントを任意のセキュリティ管理ツールと IT ワークフローツールに送信する機能が不可欠です。多くのセキュリティベンダー（およびアラートを実装するチーム）が、セキュリティアラートや自動応答を一方通行の通信フローとして考えていますが、これは間違いです。

正当なビジネスプロセスの多くと同様、攻撃も長期にわたって行われる場合があります。API の使用を効果的に分析するためには、少なくとも 30 日以上はふるまい分析を行う必要があります。これにより、ベースラインとなる想定内のふるまいを完全かつ正確に把握できます。また、数日間または数週間（および多数の API セッション）にわたって、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。たとえば、規定のレート制限を下回る Low & Slow のデータスクレイピング攻撃が発生したとします。このような攻撃を検知するためには、過去のふるまいとの差異を調べる以外に方法はありません。

詳細情報のないアラートは、ほぼ間違いなく益となるよりも害となります。一方、原因と影響に関する詳細情報が豊富に含まれたアラートは、実用的なアラートとなります。さらに、その実用的なアラートの受信者がクエリーを行い、より広範なデータセットを取得し、インシデントを分析できるのが理想です。実用的なアラートとクエリー機能があれば、WAF 保護を活用して、脅威となるトラフィックを即座にブロックできます。

5 推奨 部門間コラボレーションを重視する

API セキュリティを強化するための最も効果的な方法の 1 つが、設計、開発、展開の各段階で脆弱性を未然に防ぐことです。そのためにはチーム間コラボレーションが不可欠です。

チーム間コラボレーションを推進するためには、API の実際の使用（悪用）状況について、各 API チームに情報を提供する必要があります。このような情報を提供することで、API の開発と展開の際に、初期段階からセキュリティを考慮に入れる社内文化を醸成できます。さらに、次の点も重要です。

- 各 API チームがより効果的に業務を遂行できるよう、チーム間コラボレーションを通じてセキュリティ以外のメリットも実現する
- セキュリティ担当者以外のユーザー（開発者など）が、API のインベントリとアクティビティ情報を簡単に表示／クエリーできるようにする
- API セキュリティを開発ツール（Jira など）に組み込んで、開発者がセキュリティ修正を必要としている場合にプロアクティブにチケットをオープンできるようにする

セキュリティ担当者だけでなく、すべての従業員が API セキュリティに関与することで、責任の押し付け合いを回避し、開発、運用、セキュリティの各チームが互いの利益のために協力できます。

6 非推奨 サードパーティーの API を見過ごす

API セキュリティ戦略の一般的な落とし穴として、自社の API にしか注意を払わないことが挙げられます。WAF や API ゲートウェイを購入して導入するだけで API セキュリティ戦略全体を標準化できれば理想的ですが、現実は必ずしもそうはいきません。

たとえば、中核となる 1 つの API ゲートウェイ戦略を導入したとしても、その中核的な API ガバナンスアプローチを迂回するシャドー API が存在するかもしれません。サードパーティーの API を使用している場合、自社のエコシステムに接続する前にそのサードパーティー API にセキュリティ侵害が発生していたとしても、ゲートウェイはその API を承認された API として認識します。

使用している主な API テクノロジー（API ゲートウェイなど）に沿って API 保護戦略を策定するだけでなく、さまざまなソース（ネットワークデバイス、クラウドプラットフォーム、マイクロサービス・オーケストレーション・ツールなど）から可能な限り多くの情報を収集することが重要です。これが、API アタックサーフェスを完全に把握し、将来的にテクノロジーやインフラを変更しても陳腐化しないセキュリティ戦略を策定するための唯一の方法です。

7 非推奨 事後的に対応して次に進む

アラートを受信したら迅速かつ効果的に対応するのはもちろん良いことですが、事後的な緩和だけでなく、アラートを事前に回避することも重要です。そこで必要となるのが、プロアクティブな脅威ハンティングです。API セキュリティパートナーがデータクエリー機能を提供している場合は、仮説をテストしたり、関係を把握したり、セキュリティインシデントに発展する前に潜在的脅威を特定したりできます。たとえば、特定のパートナーが API を不適切に使用していることが判明した場合、同様の不適切使用を他のパートナーやサプライヤーがしていないか、数回のクリックで調査できます。

API セキュリティパートナーは、履歴データをデータレイクに保管し、調査や脅威ハンティングを行えるよう、その履歴データに対するアクセスを提供しなければなりません。

このようなリッチなクエリー機能は、次の 2 つの特長を備えているのが理想です。

1. シンプルかつ直感的なユーザー Web インターフェース
2. API セキュリティプロバイダーに対する API インターフェースのセット（より高度なワークフローを開発するため）

8 推奨 継続的なライフサイクルとして API セキュリティに対応する

API セキュリティをビジネスに組み込むための最良の方法は、API をテストすることです。API ライフサイクルに API テストツールを追加することで、誤設定または脆弱な API を開発するリスクを抑制できます。開発の初期段階で API のテストと修正を行うことで、労力、時間、コストを削減できます。

次に、セキュリティチームは、組織内で使用する API のインベントリを作成し、API 保護の取り組みを開始する必要があります。次々と新しい API が追加され、古い API が廃止されるため、API インターフェースの最新のインベントリを作成し、機密性の高いアプリケーション／データリポジトリに保管しておくことが重要です。API を継続的かつ効果的に探索することで、シャドー API、不正 API、忘れられた API、ゾンビ API、放棄された API、非推奨の API などの問題を解消できます。

セキュリティチームには、新しい API セキュリティ脅威を検知して緩和するための可視性が必要です。しかし、ランタイム時に脅威を検知することも重要です。ビジネスロジックの悪用は、実稼働中の API でしか検知できません。ランタイムのふるまいを、ベースラインとなる通常の使用パターンと比較することで、悪用の有無を特定できます。

最後に、API を悪用する脅威を、ランタイム時のあらゆる時点で阻止することが重要です。アラートだけではビジネスをマクロレベルで保護するためには十分ではないため、WAF による自動ブロックが不可欠です。また、API ゲートウェイのレート制限を引き下げたり、Jira のチケットをオープンして開発者に調査を依頼したり、セキュリティチームにメールを送信したりなど、さまざまな自動応答をカスタマイズできます。検知したすべての脅威に適切に対応するためには、状況の理解とカスタマイズ可能な応答メカニズムが不可欠です。

まとめ

推奨	非推奨
✔ すべての API を可視化する	✘ クラウドを恐れる
✔ 戦略を策定する際にはビジネス状況を考慮に入れる	✘ データを一方通行にする
✔ 部門間コラボレーションを重視する	✘ サードパーティーの API を見過ごす
✔ 継続的なライフサイクルとして API セキュリティに対応する	✘ 事後的に対応して次に進む

今すぐ始める

最新の API セキュリティのための体系的なアプローチに興味をお持ちの場合は、

Akamai API Security の詳細をご覧ください

Akamai　のクラウドベースのアプローチにより、数分で使用を開始できます。ビジネスロジックと API の関係に関する詳細情報など、組織内での API の使用について、数時間で完全に把握できます。

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：2023 年 11 月。