API セキュリティ バイヤーズガイド

API セキュリティの課題に対応するために立ち上がる

クラウド中心のデジタル化が進むにつれ、API の範囲と規模が拡大し、価値が増大しています。現在の API は次のような状況です。

- 顧客やパートナーに提供するアプリケーションやサービス（最新の AI イノベーションを含む）の中心で使用されている
- 開発者が使用するサービスからエンジニアがリフト＆シフトするワークロードまで、クラウド環境全体に組み込まれている
- 収益源として、ビジネスの成長と開発者エコシステムの構築を支援している

しかし、IT やセキュリティ専門家の 78%[1] と同様に、API のセキュリティインシデントを経験したことがある場合は、API のリスクが増大していることを肌で感じているはずです。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、侵害されやすくなっています。多くの組織が、すべての API を把握することなく、未管理のまま放置しています。これらの休眠 API（ゾンビ API）は、主な攻撃ベクトルとなります。

そして、その影響は甚大です。API に対する攻撃は、エンタープライズの収益、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。ほとんどの組織は、API 攻撃を防止するための適切な制御や機能をまだ導入していません。確かに、多くの企業が 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の API ツールを既存のスタックに組み込んでいます。しかし、これらのツールである程度の保護は実現できるものの、最新の API 攻撃を防御できるだけの可視性、リアルタイムのセキュリティ、継続的なテストを提供するようには設計されていません。

1. Akamai Technologies, “API Security Disconnect Report,” 2023

では、API 環境を完全に保護するためには何が必要でしょうか。ここ数年で多くの API セキュリティ製品が登場しましたが、増え続けるベンダーとその機能を把握するのは簡単ではありません。

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。このバイヤーズガイドでは、包括的な API セキュリティソリューションに求められる主要機能について説明します。また、エコシステム内のすべての API を特定して保護しながら、安全な API を開発および維持するための機能とセキュリティ制御について紹介します。

包括的な API セキュリティのための主な機能

必要な API セキュリティ機能を判断するためには、直面する課題の性質を理解することが重要です。

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。貴社の API は、無数のサードパーティのアプリ、サービス、システムと接続しています。そして、サードパーティの中には API セキュリティを重視している組織もあれば、重視していない組織もあります。

さらに、次の点についてリアルタイムの知見を得ることは困難です。

- API がどこにルーティングされているのか
- API がどのように設定されているのか
- API がどのような機微な情報を転送しているのか
- どのようなリスクがあるのか

エンタープライズが次々と新しいアプリケーションや API を開発して展開するのに伴い、アタックサーフェスは急拡大しています。また、組織によっては、API セキュリティの重要性が表面化する何年も前に作成した古い API が大量に存在するかもしれません。

可視性が欠如していると、次のような問題が発生します。API のインベントリを完全に把握しているセキュリティ専門家のうち、機微な情報を返す API コールを把握しているのは、わずか 10 人に 4 人にとどまっています。このような API コールの多くは、攻撃者が脆弱性をテストするために行うものです。攻撃者はセキュリティギャップを見つけると、容赦なく攻撃を実行します。

API のセキュリティを完全に保護できると主張するセキュリティベンダーを精査する場合は、4 つの重要な領域にわたって、本番環境用の実績ある制御と機能を提供していることを確認することが重要です。

ベンダーの機能を精査するためのバイヤーズチェックリストについては、以降のセクションで紹介します。

01

API 探索

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。

- ☑ 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
- ☑ 休眠 API、レガシー API、ゾンビ API を検知する
- ☑ 忘れられているドメイン、見落とされているドメイン、またはその他の不明なシャドウドメインを特定する
- ☑ 盲点を解消し、潜在的な攻撃経路を明らかにする

02

API 対策管理

API の単純な設定ミスにより、攻撃者に攻撃機会を与えてしまう可能性があります。侵入に成功した攻撃者は、機微な情報に簡単にアクセスして窃取できてしまいます。すべての API がどのように設定されているかを理解するためには、次のことができる必要があります。

- ☑ インフラを自動的にスキャンして、設定ミスや隠れたリスクを把握する
- ☑ カスタムワークフローを作成して、主要関係者に脆弱性を通知する
- ☑ 機微な情報にアクセスできる API と内部ユーザーを特定する
- ☑ 検知した問題に重大度ランキングを割り当てて、修復の優先順位を設定する

03

API 脅威の検知と修復

API 攻撃は避けられない段階にまで来ています。脅威を効果的に検知して修復するためには、次のことができる必要があります。

- ☑ データの改ざんや漏えい、ポリシー違反、不審なふるまい、API 悪用を監視する
- ☑ あらゆるソースからの API トラフィックを分析し、既存のワークフロー（チケット発行、セキュリティ情報およびイベント管理など）と統合して、セキュリティ運用チームに警告する
- ☑ 攻撃や悪用をリアルタイムで阻止し、修復の一部または全部を自動化する

04

API セキュリティテスト

開発者がアプリケーションを構築する際にはスピードが不可欠です。しかし、スピードが速いと、脆弱性や設計上の欠陥が発見されにくくなります。API を適切にテストするためには、次のことができる必要があります。

- ☑ さまざまな自動テストを実行して悪性トラフィックをシミュレーションし、基盤となる API ビジネスロジックに従う
- ☑ API を本番環境に展開する前に脆弱性を発見し、攻撃が成功するリスクを緩和する
- ☑ 定められたガバナンスポリシーやルールに照らして、API の仕様を確認する
- ☑ API に特化したセキュリティテストをオンデマンドで、または CI／CD パイプラインの一環として実行する

API 探索：主な機能の詳細

多くの組織は、レガシー API と新しい API の両方を運用しています。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。ショートカット、プロセスの失敗、または廃止時に適切にシャットダウンしなかったことなどが原因でローグ（野良）API が生まれることもあります。次のページでは、注目すべき主な例を紹介します。

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。

無効化の失敗

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。このような API は、ゾンビ API と呼ばれることがあります。

古いバージョンの API

古いバージョンの API が廃止されていない場合があります。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、API を無効化する担当者が退職した場合、配置転換になった場合、または単に古いバージョンのシャットダウンを忘れた場合は、古いバージョンが廃止されないまま残ることになります。

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。

ベンダーと話をする際には、野良 API、レガシー API、ゾンビ API、シャドウ API をどのように特定および対処して、悪用を阻止するのかについて説明してもらうことが重要です。レガシー API とゾンビ API は、多くの場合、API セキュリティの最大の弱点になります。そのため、API ゲートウェイで管理されていない API を探索して、それらを特定してインベントリを作成し、修復や廃止の必要性を判断することが重要です。

主な API 探索機能

API セキュリティソリューションには、次のような探索機能が必要です

API 資産の探索と詳細なインベントリ

API 探索ツールには、RESTful、GraphQL、SOAP、XML-RPC、JSOF-RPC、gRPC など、設定やタイプに関係なく、所有している API を見つけて、特定するための機能が必要です。また、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。

休眠 API、レガシー API、ゾンビ API の検知

レガシー API やゾンビ API は、API セキュリティイニシアチブの開始前から存在している場合があります。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。そのため、このような API を見つけられる API 探索ツールが必要です。

シャドウドメインの探索

シャドウ API に加えて、シャドウドメイン（まったく把握していない 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、またはその他の不明なシャドウドメインを特定できる必要があります。

自動スキャン

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。

限定的なカスタム開発

最後に、適切な API 探索ツールがあれば、トラフィックソースのためのカスタム開発は必要ありません。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はずです。
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。

API 対策管理：主な機能の詳細

集中型 IT から分散型 LOB 運用への移行、クラウドリソースの利用拡大、マイクロサービスベースアーキテクチャへの移行などのトレンドにより、API 環境に対する脅威は急速に高まっています。

前のセクションで説明したように、API 環境を保護するための最初のステップは、堅牢な探索です。現在使用中のあらゆるタイプの API を探索し、インベントリを作成する必要があります。

API 全体のセキュリティ体制を管理するために必要な機能が他にもいくつかあります。機微な情報にアクセスして送信する API を特定し、それらの API を適切に分類できる必要があります。顧客情報などのデータを取り扱う API は認証が必要となるためです。また、API をより脆弱にするインフラの脆弱性を特定することも重要です。

設定評価

サイバー攻撃の多くは、API トラフィックを仲介し、保護するネットワーク、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。

API セキュリティソリューションは、ログファイル、履歴トラフィックの再生、設定ファイルなどを含め、インフラとソフトウェアの設定を定期的にスキャンする必要があります。これにより、設定ミスや脆弱性を明らかにし、設定ドリフトによるリスクを排除できます。

カスタマイズ可能な重大度

ソリューションが環境内の新しい脆弱性を特定する際には、発見された問題に重大度レベルを割り当て、修復の優先順位を付ける必要があります。重大度レベルは、組織のリスク許容度、規制要件、社内ポリシーに合わせてカスタマイズできることが重要です。

カスタムワークフロー

最適な対策管理ツールは、重大度をカスタマイズできるだけでなく、脆弱性を特定した際に即座に対策を講じるためのカスタムワークフローを作成できる必要があります。これらのワークフローは、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。組織は、安全な API が仕様や正確な文書に準拠しているかどうかを評価する必要があります。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。

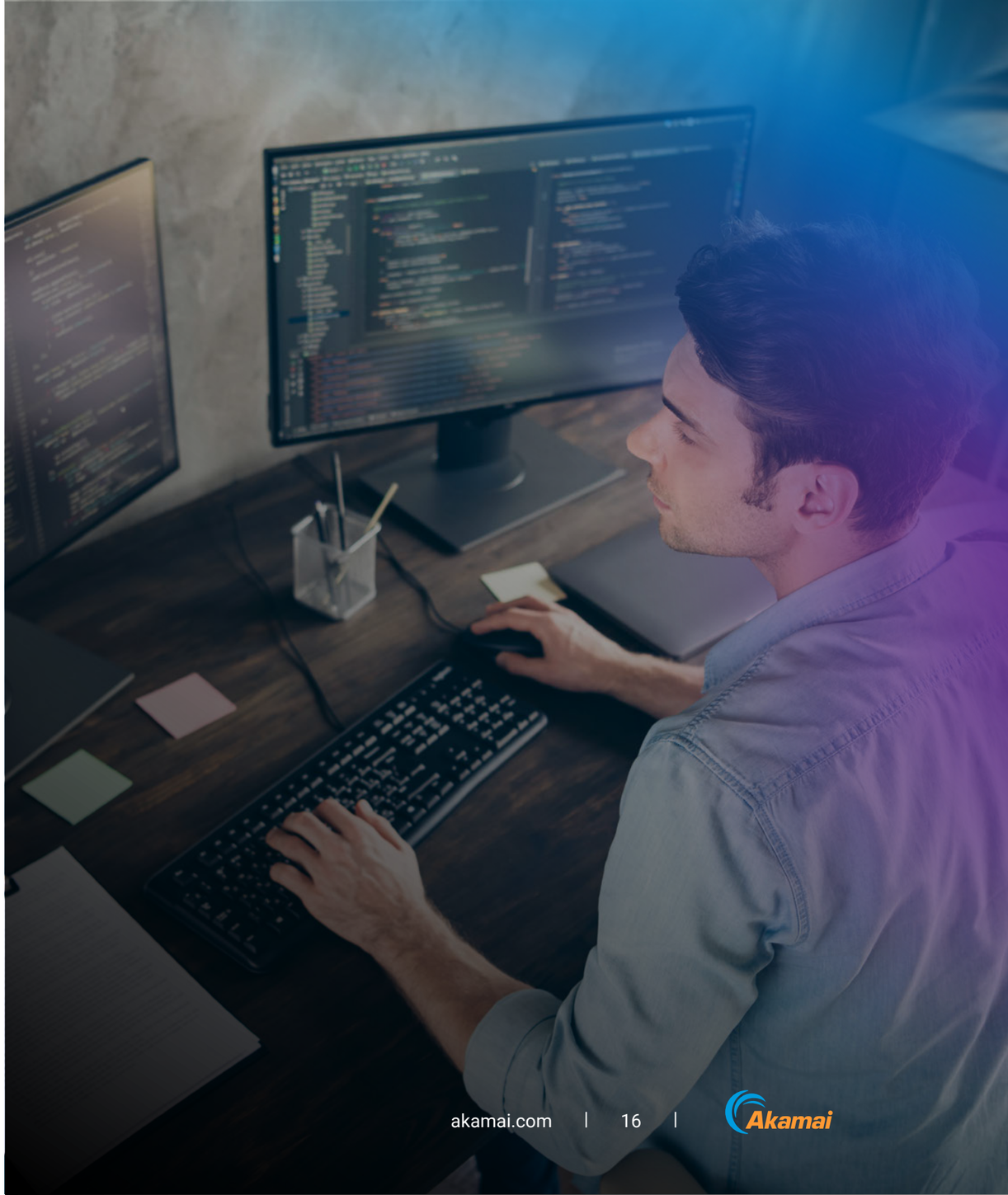
OpenAPI 仕様では、標準インターフェースの説明が定義されています。API セキュリティソリューションは、次のことができる必要があります。

- API の仕様を実際の観察可能なトラフィックと比較し、違いを特定することで、展開した API のうち、どの API が仕様から外れており、潜在的なリスクであるかを確認する。
- 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ことを確認する。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。

API 脅威の検知と修復：主な機能の詳細

API の脆弱性を悪用した攻撃は、今や現実のものとなっています。もはや、攻撃されるかどうかではなく、いつ、どのように攻撃されるか、の問題なのです。攻撃を迅速に検知し、顧客の個人データの流出など、重大な被害へと発展する前にブロックすることが不可欠です。API のセキュリティが可能な限り確保されている場合でも、データ漏えい、データ改ざん、データポリシー違反、不審なふるまい、API セキュリティ攻撃を検知するための積極的なランタイム保護が必要です。そして、このランタイム保護には、API トラフィックのロギング、機微な情報へのアクセスの監視、脅威の検知、攻撃ベクトルのブロックや修復などの機能が必要です。

次の 2 ページでは、API セキュリティソリューションに求められる重要な機能について説明します。



リアルタイムのアウトオブバンド監視

API セキュリティ監視は、API トラフィックに影響を与えたり、速度を低下させたりすることがあってはなりません。迅速に展開して、より多くのトラフィックを監視できるエージェントレスアプローチを採用しているベンダーを選択しましょう。ただし、（複雑なオンプレミス環境など）状況に応じて、エージェントもサポートできるだけの柔軟性を備えている必要があります。

API セキュリティソリューションは、特定したデータソースからのトラフィックをミラーリングし、そのトラフィックデータの分析をバックグラウンドで実行し、発見した問題をリアルタイムで警告できる必要があります。

API の異常と悪用の検知

特に API の数と API トラフィックの総量が増加し続けると、受動的なデータ収集だけでは不十分です。API アクティビティを継続的に分析して、異常なイベントを検知し、セキュリティチームと運用チームに警告する必要があります。

高度なツールには、AI 機能と機械学習機能が組み込まれており、リアルタイムでトラフィックを分析し、状況に沿った知見を活用して、データ漏えい、データ改ざん、データポリシー違反、その他の API セキュリティ攻撃を示す異常なアクティビティを特定できます。

API 攻撃の防止

異常などの問題を特定し、アラートを生成した後は、一刻を争います。API を介した機微な情報の不正な移動など、API の悪用が疑われる場合は、検知してブロックする必要があります。API セキュリティソリューションは、既存のファイアウォールや API ゲートウェイとの統合によって悪用をブロックするだけでなく、修復を部分的または完全に自動化する必要があります。ある種のアラートに対しては、半自動的な修復を利用できる必要があります。過去に特定され、繰り返し発生する問題については、完全に自動化された対応を提供するオプションが必要です。

攻撃の信頼度スコア

ソリューションの中には、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など、内外のシグナルを評価するように訓練された機械学習アルゴリズムを使用しているものがあります。このような状況的要素を用いて、検知したランタイムインシデントが悪性アクティビティによるものかどうかの信頼度レベルを判断できます。

インシデント対応の統合

API セキュリティソリューションには、インシデントが発生した場合に修復タスクを適切なチームに割り当てるための統合機能が必要です。設定ミス、データポリシー違反、疑わしいふるまいが検知された場合、API ゲートウェイや SIEM システムなどの情報セキュリティエンジンに報告して、適切な認識レベルを確保する必要があります。

一般的なルールとして、API セキュリティソリューションは、組織が使用している他のセキュリティ、監視、管理ツールと簡単に統合できなければなりません。

API セキュリティテスト：主な機能の詳細

多くの開発チームが犯す間違いは、API テストを開始するまでに時間がかかりすぎて、テストがボトルネックになってしまうことです。シフトレフトのアプローチを採用し、開発プロセスの早い段階で包括的なテストを実施することが重要です。効果的な API セキュリティテストには、次のような大きなメリットがあります。

- **攻撃の阻止**
  - API を本番環境に展開する前に脆弱性を発見することで、攻撃が成功するリスクを緩和できる
- **コンプライアンスの向上**
  - 包括的なテストにより、コンプライアンスを確保し、罰金や風評被害を回避できる
- **信頼性の向上**
  - 厳格で効果的なテストにより、API に対する組織の信頼性が向上し、開発者が予定どおりにリリースできるようになる

ベンダーによっては、問題の修復方法や包括的な API テストの設定方法について、推奨事項を提案している場合もあります。たとえば、適切な認証を設定する方法や、API の依存関係を修正する方法などに関する推奨事項です。メリットとして、環境内のビジネスロジックの問題に対処できれば、より多くの API をテスト用に最適化して、テストの対象範囲を広げることができます。

しかし、API セキュリティテストという概念自体が漠然としています。開発チームは、その内容を十分に理解していないかもしれません。シフトレフトの API テストは、次の 3 段階のプロセスで行われます。

1. **API を理解する：**特に複雑なビジネスロジックの問題に関するテストを実施する場合は、API のユースケースを理解することが重要です。
2. **API が適切に利用できることを確認する：**API が意図したとおりに利用できることを確認します。これは、API に対する理解と、API の実際の機能が一致していることを確認するためには不可欠です。
3. **API に攻撃トラフィックを送信する：**API へのリクエストを手動で操作したり、リクエストにファジング文字列を挿入したり、自動ツールを使用して API セキュリティテストを実行したりします。今日の IT に共通して言えることは、多くの場合、速度を犠牲にすることなく、大規模な作業を行うためには、自動化が最善の方法となります。

主要な API セキュリティテスト機能

API セキュリティテストには、静的テスト、動的テスト、侵入テストが必要です。また、API セキュリティソリューションには、徹底的なテストを容易に行い、可能な限りテストプロセスを自動化できるツールが必要です。次のような API テスト機能を備えた API セキュリティソリューションを選択することをおすすめします。

プロアクティブな自動 API セキュリティテスト

自動セキュリティテストにより、API を本番環境に展開する前に設定ミス、脆弱性、コンプライアンス違反を特定することで、リスクとコストを大幅に削減できます。

API ガバナンス

役割、責任、ポリシーなどのガバナンスの問題について徹底的に考えることが重要です。たとえば、開発者、セキュリティエンジニア、プラットフォームエンジニアの実行レベルの責任、ポリシーの監視、リスクに関する意思決定などについて検討します。定められたガバナンスポリシーやルールに照らして、API の仕様を確認できる API セキュリティソリューションが必要です。

CI／CD パイプラインとコードリポジトリの統合

DevSecOps は、DevOps の一種であり、ソフトウェア開発ワークフローにセキュリティを追加したものです。API セキュリティを DevSecOps イニシアチブに含めることが重要です。API に特化したセキュリティテストをオンデマンドで、または CI／CD パイプラインの一環として実行できる API セキュリティソリューションが必要です。CI／CD 統合は不可欠です。これにより、アプリケーション開発のスピードに後れを取ることなく、迅速かつ継続的に API セキュリティテストを実施できるようになります。

まとめ：
API セキュリティのギャップを特定して対処する

クラウド中心のデジタル経済がますます進む中、顧客へのサービス提供、収益の創出、および効率的な業務運営のためには、API が欠かせません。しかし、その継続的な増加、機微な情報の処理、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 を管理し、基本的な保護を獲得するために多くの組織が使用している既存のツールは、ある程度のリスク緩和を実現します。しかし、API に対する今日の脅威に対処するには不十分です。既存のツールだけで API を保護することはできません。

したがって、このバイヤーズガイドで紹介した 4 つのコンポーネント（API 探索、対策管理、脅威の検知と修復、セキュリティテスト）すべてを備えた包括的な API セキュリティソリューションを探す必要があります。特定の領域で効果が実証されている既存のツールを廃棄する必要はありません。重要なのは、既存のツールとシームレスに統合できるソリューションを探すことです。

API セキュリティに着手したからといって、多大なリソースを割く必要はありません。まずは、セキュリティスタックの特定のギャップに対処する、小規模で測定可能なパイロット版に取り組むことから始めます。または、包括的な更新を通じて API セキュリティの取り組みを始めることもできます。組織はそれぞれ異なります。

API を狙った攻撃は増加の一途をたどっています。最も重要なのは、行動を起こすことです。このバイヤーズガイドが参考になれば幸いです。

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。