Akamai

LIVRE BLANC

Comment éviter une violation des API

Découvrir 5 types de violations des API et comment vous en protéger

Dans ce rapport

Introduction **3**

Qu'est-ce qu'une violation d'API ? 3

Type de violation : vulnérabilités connues **4**

Comment les éviter 5

Comment Akamai API Security peut vous aider 6

Type de violation : API fantômes, indésirables, zombies et obsolètes **7**

Comment les éviter 8

Comment Akamai API Security peut vous aider 8

Type de violation : expositions externes **9**

Comment les éviter 10

Comment Akamai API Security peut vous aider 10

Type de violation : erreurs de configuration et erreurs de l'opérateur **11**

Comment les éviter 12

Comment Akamai API Security peut vous aider 12

Type de violation : vulnérabilités non découvertes **13**

Comment les éviter 13

Comment Akamai API Security peut vous aider 14

5 types de violation, 5 principes de prévention **15**

Introduction

Les API connectent votre entreprise en échangeant des données avec des partenaires, des fournisseurs et des clients. Et pourtant, dans la plupart des entreprises, la sécurité des API reste loin d'être complète. En fait, ces dernières années, les API vulnérables sont devenues une faiblesse ciblée pour les entreprises. Les pirates en abusent pour accéder à des données sensibles, les vendre à d'autres acteurs malveillants ou les publier aux yeux du monde entier. En 2024, des marques mondiales des secteurs des télécommunications grand public, de l'informatique d'entreprise et de la collaboration virtuelle ont été victimes de violations d'API qui ont permis de publier d'énormes quantités de données clients et autres données sensibles, entraînant de lourds coûts financiers et de réputation.

Qu'est-ce qu'une violation d'API ?

Pour faire simple, toute mauvaise utilisation ou utilisation abusive intentionnelle d'une API, souvent pour accéder à des données sensibles, constitue une violation d'API. Les types de violations des API peuvent être divisés selon divers critères. Pour identifier les risques et éviter les dysfonctionnements dans les opérations de production, il est utile de considérer le schéma suivant, qui répartit les risques en cinq catégories :

1. **Vulnérabilités connues**
   - Les pirates exploitent des vulnérabilités connues qui n'ont pas été corrigées.
2. **API fantômes, indésirables, zombies et obsolètes**
   - Les API non gérées et oubliées peuvent rendre les opérations vulnérables.
3. **Expositions externes**
   - Des informations d'identification, des clés et autres éléments peuvent se retrouver exposés sans que vous ayez de contrôle dessus.
4. **Erreurs de configuration et erreurs de l'opérateur**
   - Les erreurs de configuration de la sécurité dans l'infrastructure et les services peuvent créer des points d'entrée pour l'exploitation par les acteurs malveillants.
5. **Vulnérabilités et bogues non découverts**
   - Les acteurs malveillants cherchent à identifier les bogues et les vulnérabilités qui ont pénétré dans l'environnement de production malgré tous vos efforts.

Ce livre numérique explique où se produisent les défaillances de sécurité dans chacun de ces cinq types de violations d'API et comment les prévenir. Il vise également à vous aider à identifier les faiblesses spécifiques de votre programme de sécurité des API pour maximiser la sécurité des API et minimiser les risques.

Type de violation : vulnérabilités connues

Les violations d'API qui tirent parti de vulnérabilités connues (qui n'ont pas été corrigées) sont peut-être les plus courantes. Si les cybercriminels veulent récupérer vos données, la première étape consiste généralement à vérifier si votre entreprise a laissé des portes dérobées ouvertes.

En janvier 2024, un pirate a compromis un outil de gestion de projet largement utilisé en exploitant un point de terminaison d'API dépourvu de contrôles d'authentification. Après s'être introduit dans l'API, l'acteur malveillant a obtenu un accès non autorisé à des informations sur des millions d'utilisateurs et, quelques mois plus tard, a divulgué plus de 21 Go de données (notamment des adresses e-mail et des données sur les membres de conseils d'administration) sur Internet.

Les problèmes d'authentification et d'autorisation font partie des problèmes d'API les plus courants. Les 10 principaux risques pour la sécurité des API de l'OWASP fournissent une formation sur les 10 vulnérabilités les plus critiques pour les API contre lesquelles les entreprises doivent se protéger, y compris la violation d'authentification.

En plus de sécuriser les API contre les types de risques inclus dans la liste des 10 principaux risques pour la sécurité de l'OWASP, les entreprises doivent protéger le code des API contre la liste complète des vulnérabilités et expositions courantes (CVE) créée par le U.S. National Cybersecurity Federal Funded Research and Development Center (FFRDC), exploité par MITRE. Vous vous souvenez peut-être de toute la médiatisation survenue autour de la vulnérabilité Apache Log4j 2 (CVE-2021-44228), également appelée « Log4Shell ». En raison d'un bogue dans la bibliothèque Log4j, bibliothèque de journalisation open source populaire pour le langage de programmation Java, des pirates pouvaient exécuter du code arbitraire à distance pour accéder au système. Les acteurs malveillants sondent régulièrement les systèmes d'entreprise à la recherche de vulnérabilités connues comme celle-ci.

La liste des 10 principaux risques pour la sécurité des API de l'OWASP a été établie en 2019 et mise à jour en 2023. Malgré son utilité, elle ne peut pas suivre la vitesse de changement au niveau de la surface d'attaque. Rien qu'en 2024, plus de 24 000 nouvelles CVE ont été ajoutées au catalogue de la CISA, dont plus de 500 sont liées aux API (à la mi-août 2024).

Protéger complètement votre entreprise contre les vulnérabilités connues nécessite un double effort :

1. Assurez-vous que vos processus de développement et de test sont suffisamment robustes pour éviter d'introduire des vulnérabilités connues dans la production.

2. Corrigez les nouvelles vulnérabilités aussi rapidement que possible après leur identification.

De nombreuses organisations éprouvent des difficultés à gérer ces deux étapes. En outre, elles utilisent des API et du code provenant de sources tierces qui peuvent introduire un ensemble distinct de vulnérabilités. En 2022, une équipe de chercheurs a découvert des failles critiques dans les API qui ont affecté plusieurs constructeurs automobiles. Ces failles auraient pu exposer des données sensibles des clients et même l'emplacement d'un véhicule, permettant de déverrouiller, de démarrer ou de désactiver une voiture à l'aide d'un système de gestion à distance compromis.

Comment l'éviter

Mettre à jour rapidement les logiciels et les systèmes lorsque des correctifs de sécurité sont publiés constitue un moyen reconnu de protéger votre entreprise contre les violations d'API dues à des vulnérabilités connues. Il est également essentiel de s'assurer que vos processus de développement et de test sont complets et ancrés dans les meilleures pratiques de sécurité des API. Cela consiste à :

- **Sécuriser votre chaîne logistique logicielle :** assurez-vous que les bibliothèques, logiciels open source (OSS) et autres codes tiers que vous utilisez sont sécurisés.
- **Mettre en œuvre des tests de sécurité shift-left :** déplacez les tâches liées à la sécurité des API et aux tests logiciels plus tôt dans le processus de développement. Cette action peut vous aider à découvrir des vulnérabilités telles que les erreurs de codage et les erreurs de configuration effectuées par des équipes de développeurs sous pression pour publier rapidement des logiciels ou des mises à jour.
- **Exploiter la gestion de la posture de sécurité des API :** cette approche combine la découverte des API avec l'identification des données sensibles et la détection des vulnérabilités, ce qui garantit que les efforts de correction se concentrent en premier sur les API les plus critiques.

Comment Akamai API Security peut vous aider

Akamai API Security permet à vos équipes de réduire les vulnérabilités connues pour chaque nouvelle version, sans sacrifier la vitesse. API Security est une solution de test de sécurité des API spécialement conçue pour fournir une couverture complète des vulnérabilités spécifiques aux API. Active Testing peut vous aider à intégrer des tests de sécurité des API à chaque phase de développement.

- **Trouvez et testez chaque API** grâce à votre connaissance de la logique métier de l'application.
- **Déplacez** les intégrations plus tôt au niveau de l'ensemble du cycle de vie du développement logiciel. Les équipes bénéficient d'une visibilité dynamique des API sur plusieurs états et environnements tout au long du processus CI/CD.
- **Offrez aux développeurs** une facilité d'utilisation inégalée, comme une configuration et une automatisation simples, des résultats de test en ligne et des conseils contextuels pour atténuer les défaillances des requêtes.

La gestion de la posture d'API Security fournit également une vue complète du trafic, du code et des configurations pour évaluer votre propre posture de sécurité des API. API Security examine l'ensemble le plus large possible de sources pour détecter les vulnérabilités, notamment les fichiers journaux, les relectures de l'historique du trafic, les fichiers de configuration et bien plus encore. Elle détecte également toutes les vulnérabilités figurant dans la liste des 10 principaux risques pour la sécurité des API de l'OWASP (pour en savoir plus sur la gestion de la posture, voir la section « Erreurs de configuration et erreurs de l'opérateur »).

Type de violation : API fantômes, indésirables, zombies et obsolètes

Vous ne pouvez pas protéger ce que vous ne pouvez pas identifier et, dans de nombreuses entreprises, un pourcentage important des API ne sont pas gérées, ce qui fait des API fantômes, indésirables, zombies et obsolètes (voir encadré sur la page suivante) des cibles qui sont invisibles ou non prises en compte dans votre parc d'API. En outre, les pirates recherchent souvent des variantes d'API qu'ils peuvent exploiter en examinant les API exposées d'une entreprise, puis en adoptant une technique appelée fuzzing ou en modifiant des valeurs pour trouver d'anciennes versions.

C'est ce qui est arrivé à une grande entreprise australienne de télécommunications qui a accidentellement exposé plus de 11,2 millions de dossiers clients, y compris les noms, adresses, dates de naissance, et certains numéros d'identification émis par le gouvernement. L'attaque a tiré parti d'une API utilisée pour les tests qui était devenue, sans que l'on ne sache vraiment comment, accessible à l'Internet ouvert. Comme cette API indésirable ne disposait pas de contrôles d'authentification, un pirate a pu demander et recevoir des millions d'enregistrements.

La plupart des entreprises utilisent différentes API héritées et nouvelles. Malheureusement, il est bien trop courant de trouver à leurs côtés des API indésirables, zombies et fantômes qui exposent l'entreprise à une série de risques de cybersécurité et de difficultés opérationnelles.

Ces API invisibles sont issues de sources variées :

- **API commerciales :** certaines applications logicielles commerciales incluent des API permettant de se connecter à d'autres applications et sources de données externes. Celles-ci peuvent être activées sans que personne ne s'en aperçoive (problème qui peut être résolu grâce à une découverte approfondie des API).
- **Anciennes versions d'API :** dans de nombreux cas, il se peut qu'une ancienne version d'une API, éventuellement avec une sécurité plus faible ou une vulnérabilité connue, ne puisse jamais être supprimée. Il peut être nécessaire de conserver une ancienne version en même temps que la nouvelle pendant un certain temps lors de la mise à jour du logiciel. Toutefois, lorsque des défaillances de processus empêchent la fermeture de l'ancienne API, celle-ci se transforme en une API zombie.
- **Raccourcis et échecs de processus :** les API fantômes viennent du fait que l'on omet d'informer les bonnes personnes. Par exemple, une équipe métier peut créer des API pour répondre à des besoins spécifiques sans en informer le service informatique ou l'équipe de sécurité, ou un développeur peut ne pas respecter une procédure.
- **API héritées :** les API héritées dans le cadre de fusions ou d'acquisitions sont également souvent négligées et deviennent des API fantômes.
- **Code réactivé :** dans certains cas, les anciennes versions des API peuvent être accidentellement réactivées.

Comment les éviter

Effectuer un audit manuel des API afin de documenter toutes les entrées qui doivent être inventoriées avec précision peut prendre plusieurs heures, surtout si l'on considère le temps nécessaire pour évaluer et agir sur chaque API que vous trouvez. Cette tâche n'est pas réaliste pour des équipes de sécurité qui sont déjà surchargées. Pour protéger votre entreprise contre l'exploitation des API indésirables, zombies et fantômes, il vous faut un système de détection automatisée des API capable d'identifier toutes les API utilisées, de tous types. Il est essentiel de localiser et d'inventorier chaque API dans vos opérations et de découvrir les API et les domaines d'API qui ne sont pas gérés par une passerelle d'API.

Comment Akamai API Security peut vous aider

API Security exploite un large éventail de sources d'intégration pour ingérer des données d'API, telles que le trafic brut, la journalisation et bien plus encore. Les données issues de ces sources permettent à API Security d'identifier les API, les erreurs de configuration, les vulnérabilités et les abus d'API. Nos outils de détection détectent toutes les vulnérabilités figurant dans les 10 principaux risques pour la sécurité des API de l'OWASP.

Des fonctionnalités de détection supplémentaires vous permettent de :

- localiser et inventorier toutes vos API, quels que soient leur configuration ou leur type, y compris RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC et gRPC ;
- détecter les API inactives, héritées et zombies ;
- identifier les domaines oubliés, négligés ou autrement inconnus ;
- tenir à jour les inventaires des API et garantir l'exactitude de la documentation des API.

API non gérées à haut risque recherchées par les pirates

Les API fantômes (alias « API non documentées ») existent et fonctionnent en dehors des canaux officiels surveillés d'une entreprise. Elles peuvent être créées par des développeurs bien intentionnés pour accélérer leur travail, ou elles peuvent être un vestige de versions logicielles précédentes.

Les API indésirables sont des API non autorisées ou malveillantes qui présentent un risque de sécurité pour un système ou un réseau.

Les API zombies englobent toute API qui continue de s'exécuter, même après avoir été remplacée en intégralité par de nouvelles versions ou d'autres API.

Les API obsolètes sont des API dont l'utilisation n'est plus recommandée en raison de modifications apportées aux API. Bien que les classes, méthodes et champs obsolètes soient toujours implémentés, ils peuvent être supprimés dans les futures implémentations, vous ne devez donc pas les utiliser dans le nouveau code.

Type de violation : expositions externes

Les vulnérabilités externes aux API sont généralement le résultat de mauvaises pratiques ou d'erreurs de procédure, telles que la fuite de clé API et d'informations d'identification, l'exposition de code API et de schémas, une perte de documentation et des vulnérabilités de référentiel. Il est devenu impératif de pouvoir détecter des vecteurs d'attaque potentiels en dehors des limites de vos opérations. Au cours de l'année écoulée, un certain nombre de violations très médiatisées ont été le fruit de l'exposition accidentelle de clés API ou d'autres informations d'identification provenant de sources externes. Par exemple, les pirates ont utilisé une campagne d'hameçonnage pour obtenir un accès non autorisé à 130 référentiels du code source de Dropbox. Ils ont ainsi pu accéder à des clés API stockées de manière incorrecte sur GitHub. Ce type d'exposition est devenu si courant que GitHub a pris des mesures pour empêcher les fuites de clés API et d'autres secrets, mais d'autres référentiels publics peuvent encore être vulnérables.

Dans un autre exemple très médiatisé d'exposition externe, des chercheurs ont découvert plus de 3 000 applications pour mobile qui ont exposé les clés API de X (anciennement Twitter) au public. Ce type d'erreur est étonnamment courant, car les développeurs intègrent souvent des clés API dans le code de l'application pendant le développement par commodité. S'ils ne parviennent pas à supprimer ces clés intégrées avant une diffusion publique, ces intégrations peuvent devenir une source d'exposition des clés.

Comment les éviter

Pour réduire ou éliminer ces types d'expositions externes, il convient de s'appuyer sur une double approche :

- Renforcer les procédures d'identification et d'élimination des sources d'exposition comme les fuites de clés et d'informations d'identification, l'utilisation inappropriée des référentiels, etc. ;
- Analyser régulièrement la surface d'attaque externe pour détecter et corriger les vulnérabilités.

Pour vous protéger contre le plus large éventail de menaces API, il vous faut un instrument de détection des risques internes (comme décrit dans la section « Violations à partir d'API indésirables ») comme externes, capable d'identifier les expositions et de réduire votre surface d'attaque externe.

Comment Akamai API Security peut vous aider

API Security vous aide à garder une longueur d'avance sur les pirates en simulant les techniques de reconnaissance qu'ils utilisent et en vous permettant d'identifier et de résoudre rapidement les problèmes. Grâce à la détection externe, API Security analyse automatiquement votre surface d'attaque externe à intervalles réguliers pour détecter les vulnérabilités avant que les pirates ne s'en chargent, ce qui vous permet ce qui suit :

- **Identifier les vulnérabilités publiques :** repérez et corrigez rapidement les problèmes critiques tels que les fuites de clés API et d'informations d'identification, l'exposition du code, les erreurs de configuration, les vulnérabilités de référentiel et bien plus encore.
- **Détecter les domaines et sous-domaines liés à votre entreprise :** exploitez les données recueillies à partir de diverses sources, y compris les bureaux d'enregistrement Internet, les bureaux d'enregistrement de certificats et les open sources.
- **Intégrer de véritables méthodes d'attaque :** simulez un pirate effectuant une reconnaissance externe pour collecter des informations en exécutant des requêtes limitées sur des domaines ou sous-domaines de l'entreprise.

Type de violation : erreurs de configuration et erreurs de l'opérateur

De nombreux cyberpirates accèdent au système en exploitant une mauvaise configuration des serveurs, des réseaux, des passerelles d'API et des pare-feux qui servent d'intermédiaires et protègent le trafic API. D'après une étude d'IBM Security X-Force, les deux tiers des violations dans le cloud sont liés à des API mal configurées. Les erreurs de configuration de la sécurité peuvent être causées par des configurations par défaut non sécurisées, un stockage dans le cloud sans contrôle d'accès (étonnamment fréquent) et des configurations incomplètes ou ad hoc. À mesure que votre empreinte digitale se développe, vos opérations peuvent s'étendre à d'autres emplacements, y compris plusieurs zones de disponibilité du cloud public ou des clouds publics tels qu'AWS, Microsoft Azure et Google Cloud. Ces environnements fonctionnent souvent sous des contrôles de sécurité différents, en conséquence il devient complexe et difficile de vérifier que la sécurité est correctement configurée partout.

Comment les éviter

Pour se protéger au mieux contre les erreurs de configuration de la sécurité côté infrastructure, il convient d'éviter autant que possible de configurer manuellement les serveurs, les terminaux réseau, les passerelles et les pare-feux. Si les équipes d'administration de votre entreprise configurent régulièrement les contrôles de sécurité de l'infrastructure et des applications manuellement, ou les « modifient » régulièrement, les risques d'introduire des vulnérabilités de configuration augmentent.

En matière de sécurité, l'automatisation est votre meilleure alliée. Pour éviter les erreurs manuelles, certaines entreprises adoptent une infrastructure immuable.

Même si vous avez fait tout votre possible pour vous assurer que votre infrastructure, vos services et vos API sont à toute épreuve, vous avez toujours besoin de gérer la posture des API. Cette gestion de la posture vous fournit les outils pour gérer, surveiller et maintenir la sécurité de vos API tout au long de leur cycle de vie.

Comment API Security peut vous aider

Le module de gestion de la posture d'API Security analyse les appels d'API et l'infrastructure pour identifier les erreurs de configuration. Il s'agit généralement de problèmes de compartiment Amazon S3, de données sensibles sur des API non authentifiées et de différentes erreurs de configuration basées sur l'accès Kubernetes.

Le module de gestion de la posture fournit une vue complète du trafic, du code et des configurations, et donc une vue de l'ensemble de la surface d'attaque sur les API et les applications Web, y compris toutes les formes de données sensibles circulant via vos API, telles que les informations personnelles identifiables. Il vous permet également de confirmer que votre outil de gestion des API utilise des protocoles et des chiffrements forts pour éviter un chiffrement faible qui pourrait exposer ces données sensibles. En outre, les API ne doivent pas accepter les jetons Web JSON expirés, sous peine de permettre un accès non autorisé et d'augmenter les risques de sécurité. Le module permet également d'éviter les erreurs de configuration, telles que les équilibrages de charge d'application qui écoutent sur des ports non sécurisés sans redirection. Ensemble, toutes ces mesures renforcent la posture de sécurité des API, assurant une défense plus résiliente contre les menaces potentielles.

Type de violation : Vulnérabilités non découvertes

Comme pour la plupart des types de violations, les cybercriminels qui analysent votre infrastructure recherchent régulièrement des CVE, les 10 principaux risques pour la sécurité des API selon l'OWASP, et d'autres erreurs de configuration courantes, ainsi que des API indésirables, zombies et fantômes. Ils sondent également vos API exposées pour détecter de nouvelles vulnérabilités qu'ils peuvent exploiter dans les bibliothèques, le code open source et d'autres types de code public, ainsi que dans les erreurs de codage, les bogues et les mauvaises configurations de votre parc d'API. Ces vulnérabilités permettent aux cybercriminels de manipuler les appels d'API et d'insérer des chaînes de fuzzing dans les requêtes. Les techniques utilisées par les cybercriminels sont donc en constante évolution.

Comment l'éviter

S'assurer que votre code comporte aussi peu de bogues et de vulnérabilités que possible constitue une partie importante de la prévention (voir la section « Vulnérabilités connues »). Cependant, vous devez toujours partir du principe que les acteurs malveillants trouveront des bogues ou auront accès à des clés ou des informations d'identification qui leur permettront d'exploiter les API.

La protection de la durée d'exécution des API est conçue pour identifier les pirates informatiques qui exploitent toute vulnérabilité, connue ou inconnue. C'est le seul moyen de protéger votre parc d'API contre les bogues et les erreurs de configuration non identifiés qui se glissent dans la production, et c'est aussi la meilleure protection contre les informations d'identification et les clés qui ont été compromises.

La protection de la durée d'exécution identifie les schémas inhabituels et les anomalies dans l'utilisation des API et l'accès aux données afin que les attaques en cours qui pourraient passer inaperçues puissent être identifiées et corrigées avant toute extraction de milliers ou de millions d'enregistrements de données.

La protection de la durée d'exécution des API vous permet d'identifier et de bloquer les requêtes API malveillantes, notamment :

- Attaques extrayant de grands volumes de données sensibles à partir d'une API
- Attaques de type autorisation brisée au niveau de l'objet (BOLA)

Une solution de protection de la durée d'exécution des API peut détecter :

- des fuites de données ;
- des violations des politiques de données ;
- des attaques de sécurité des API ;
- une falsification de données ;
- un comportement suspect.

En outre, cette protection consigne le trafic d'API, surveille l'accès aux données sensibles, détecte les menaces et bloque ou corrige les vecteurs d'attaque.

Comment API Security peut vous aider

Considérez la protection de la durée d'exécution comme votre dernière ligne de défense lorsque les autres mesures de prévention ne sont pas suffisantes. Cette protection a pour fonction principale de détecter et de bloquer les attaques d'API en temps réel. La surveillance autonome basée sur l'apprentissage automatique permet d'effectuer une analyse du trafic en temps réel et de fournir des informations contextuelles sur les fuites de données, la falsification de données, les violations de politiques de données, les comportements suspects et les attaques de sécurité des API. API Security détecte les anomalies et les menaces potentielles dans votre trafic API et facilite la correction en fonction de stratégies de réponse aux incidents présélectionnées.

Grâce à l'apprentissage automatique, API Security crée un modèle de comportement pour chaque API. Cette base de référence du comportement normal est ensuite utilisée pour détecter les attaques de logique métier des API. Chaque problème généré par la protection de la durée d'exécution inclut la gravité, l'état, une correspondance avec les 10 principaux risques pour la sécurité des API selon l'OWASP et les informations relatives au pirate, le cas échéant. Les problèmes englobent également des preuves telles que les détails de la session du pirate et une copie de la requête API et de sa réponse pour aider à trier et corriger le problème.

La protection de la durée d'exécution d'API Security offre une détection et une prévention en temps réel des attaques d'API ainsi qu'une détection continue des erreurs de configuration d'API, en plus de nombreuses intégrations de flux de travail populaires qui simplifient les opérations et la correction.

API Security s'intègre aux WAF, aux passerelles d'API, aux ITSM, aux SIEM et à d'autres outils de workflow pour offrir une défense intégrale contre les attaques, ce qui constitue probablement la meilleure réponse pour votre équipe. Vous pouvez choisir d'automatiser entièrement la correction des menaces ou d'exiger différents niveaux d'intervention manuelle pour une visibilité et un contrôle accrus.

5 types de violation, 5 principes de prévention

Maintenant que vous comprenez mieux comment les API sont utilisées par les cybercriminels, vous pouvez vous concentrer sur leur prévention. Voici les cinq outils de prévention et les perspectives stratégiques que vous devez utiliser en combinaison :

1. Sécurité des API shift-left

- La sécurité des API shift-left consiste à tester de manière intensive les API en cours de développement afin de ne pas exposer les vulnérabilités dans votre environnement de production où les cybercriminels peuvent les trouver

2. Détection interne

- Identifiez toutes les API dans l'ensemble de vos opérations

3. Détection externe

- Identifiez et éliminez les sources d'exposition, telles que les fuites de clés et d'informations d'identification et l'utilisation inappropriée de référentiels, et analysez régulièrement la surface d'attaque externe pour détecter et corriger les vulnérabilités

4. Gestion de la posture complète

- Mettez toujours toutes les chances de votre côté en matière de sécurité des API en évitant les erreurs de configuration et les vulnérabilités

5. Protection de la durée d'exécution

- Détectez toute activité anormale de l'API et protégez-vous contre toutes les menaces éventuelles, y compris les vulnérabilités et les bogues non identifiés précédemment

Demander une démonstration

Découvrez la facilité avec laquelle il est possible d'identifier et de corriger les erreurs de configuration dans vos API et de vous protéger contre les attaques API malveillantes en observant Akamai API Security en action. Découvrez par vous-même pourquoi les grandes entreprises choisissent notre solution de sécurité des API.

Obtenir une démonstration