Guide de l’acheteur de solutions de sécurité des API

Relever le défi de la sécurité des API

À mesure que les organisations se centrent sur le cloud et le digital, leurs API gagnent en ampleur, ce qui augmente leur valeur. Désormais, les API :

- opèrent au cœur des applications et des services répondant aux besoins de vos clients et partenaires, y compris des dernières innovations en IA ;
- sont intégrées dans des environnements cloud, des services que vos développeurs utilisent aux charges de travail que vos ingénieurs réhébergent (« lift-and-shift ») ;
- représentent elles-mêmes des sources de revenus, en contribuant à la croissance de votre entreprise et à la création d'un écosystème de développeurs.

Cependant, si vous êtes comme les 78 % des professionnels de l'informatique et de la sécurité qui ont connu des incidents de sécurité des API[1], vous avez également constaté par vous-même que les API représentent un risque croissant. Les API exposées ou mal configurées sont nombreuses, non protégées et faciles à compromettre. De nombreuses organisations ne connaissent souvent même pas toutes leurs API et omettent de les gérer. Ces API dormantes, ou zombies, représentent des vecteurs d'attaque majeurs.

Les enjeux sont très importants. Les attaques contre vos API peuvent compromettre les revenus, la résilience et la conformité réglementaire d'une entreprise. La plupart des organisations ne disposent pas encore des contrôles et des capacités adéquats pour prévenir les attaques d'API. Certes, de nombreuses entreprises ont des outils API dans leur pile existante, y compris des passerelles API et des pare-feux d'applications Web, mais bien que ces outils puissent offrir une certaine protection, ils ne sont pas conçus pour fournir le degré de visibilité, de sécurité en temps réel et de tests continus nécessaire pour se défendre contre les attaques d'API actuelles.

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

Alors, que faut-il faire pour protéger pleinement l'ensemble de vos API ? Bien qu'une multitude de produits de sécurité des API aient vu le jour au cours des dernières années, il peut être difficile de s'y retrouver parmi l'éventail de plus en plus large des fournisseurs et de leurs capacités.

Les menaces actuelles nécessitent une solution de sécurité des API complète, englobant quatre domaines critiques : découverte des API, gestion de la posture, détection et correction des menaces, et tests de sécurité. Ce guide de l'acheteur décrit les principales fonctionnalités requises par une solution de sécurité des API complète, et définit les fonctionnalités et les contrôles de sécurité dont vous avez besoin pour concevoir et maintenir des API sécurisées, tout en localisant et en protégeant chaque API de votre écosystème.

Fonctionnalités clés pour une sécurité complète des API

Pour déterminer les fonctionnalités de sécurité des API dont vous avez besoin, il est important de comprendre la nature des défis auxquels vous êtes confrontés.

Les API sont souvent réparties dans plusieurs environnements, sur site et dans le cloud hybride. La complexité est encore accrue du fait que votre écosystème d'API s'étend probablement bien au-delà de votre propre réseau et de votre présence dans le cloud. Pensez à la myriade de connexions que vos API ont établies avec des applications, des services et des systèmes appartenant à des tiers, qui peuvent ou non donner la priorité à la sécurité des API.

De plus, il est difficile d'obtenir des informations en temps réel sur :

- l'endroit où vos API sont acheminées ;
- la façon dont elles sont configurées ;
- les données sensibles qu'elles déplacent ;
- les risques qu'elles posent.

À mesure que les entreprises développent et déploient rapidement de nouvelles applications et API, la surface d'attaque augmente de façon exponentielle. Pour ce qui est des API plus anciennes, votre entreprise peut en avoir un cluster, créé et produit il y a des années, avant que la sécurité des API ne devienne un besoin critique.

Le manque de visibilité conduit à des constats inquiétants : seuls 4 professionnels de la sécurité sur 10 disposant d'inventaires API complets savent lesquelles de leurs API renvoient des données sensibles lorsqu'elles sont appelées. Bon nombre de ces appels d'API proviennent d'acteurs malveillants qui testent des vulnérabilités. Et, une fois qu'ils détectent une lacune, les attaques sont souvent implacables.

Lors de l'évaluation des fournisseurs de services de sécurité qui affirment pouvoir sécuriser entièrement vos API, il est important de vous assurer qu'ils ont mis en place des contrôles et des fonctionnalités en production dans quatre domaines critiques.

Lisez la suite pour découvrir une série de listes de contrôle de l'acheteur que vous pouvez utiliser pour évaluer les fonctionnalités des fournisseurs.

01

Découverte des API

Il n'est pas rare d'avoir des API dont personne ne connaît l'existence. Or, sans inventaire précis, votre entreprise est exposée à toute une série de risques. Pour inventorier efficacement vos API, vous devez être en mesure de :

- ☑ localiser et inventorier vos API, indépendamment de leur configuration ou leur type ;
- ☑ détecter les API inactives, héritées et zombies ;
- ☑ identifier les domaines oubliés, négligés ou autrement inconnus ;
- ☑ éliminer les angles morts et déceler les voies d'attaque potentielles.

02

Gestion de la posture des API

De simples erreurs de configuration d'API peuvent ouvrir la voie aux pirates. Une fois à l'intérieur, ils peuvent rapidement accéder aux données sensibles et les exfiltrer. Pour comprendre comment toutes vos API sont configurées, vous devez pouvoir :

- ☑ analyser automatiquement l'infrastructure et découvrir les erreurs de configuration ainsi que les risques cachés ;
- ☑ créer des workflows personnalisés pour informer les principales parties prenantes des vulnérabilités ;
- ☑ identifier les API et les utilisateurs internes capables d'accéder aux données sensibles ;
- ☑ attribuer des niveaux de gravité aux problèmes détectés afin de hiérarchiser les mesures correctives.

03

Détection et correction des menaces ciblant les API

Les attaques d'API sont inéluctables. Pour détecter et corriger efficacement les menaces, vous devez être en mesure de :

- ☑ surveiller la falsification et la fuite de données, les violations de règles, les comportements suspects et les abus d'API ;
- ☑ analyser le trafic d'API de toutes les sources et l'intégrer aux flux de travail existants (système de tickets, gestion des informations de sécurité et des événements, etc.) pour alerter les équipes chargées des opérations de sécurité ;
- ☑ prévenir les attaques et les abus en temps réel grâce à une correction partielle ou entièrement automatisée.

04

Tests de sécurité complets des API

La rapidité est essentielle pour toutes les applications que vos développeurs mettent au point, mais elle permet à une vulnérabilité ou à un défaut de conception de passer plus facilement inaperçu. Pour tester correctement vos API, vous devez pouvoir :

- ☑ exécuter un large éventail de tests automatisés qui simulent le trafic malveillant et suivent la logique métier des API sous-jacentes ;
- ☑ découvrir les vulnérabilités avant que les API n'entrent en production afin de réduire le risque de réussite des attaques ;
- ☑ inspecter les spécifications de vos API par rapport aux politiques et règles de gouvernance établies ;
- ☑ exécuter des tests de sécurité axés sur les API à la demande ou dans le cadre d'un pipeline CI/CD.

Détection des API : plongée en profondeur dans les fonctionnalités clés

De nombreuses organisations utilisent des API héritées et nouvelles. Il n'est pas rare d'avoir des API non gérées en production que personne au sein des équipes d'exploitation ou de sécurité ne connaît, ce qui expose l'entreprise à un éventail de risques de cybersécurité et de difficultés opérationnelles. Les API indésirables peuvent provenir de facteurs tels que les raccourcis, les échecs de processus et la non-fermeture lors de la mise hors service. À la page suivante, vous trouverez des exemples clés à surveiller.

API commerciales

Certaines applications logicielles commerciales incluent des API permettant de se connecter à d'autres applications et sources de données externes. Ces API peuvent être activées sans que personne ne s'en aperçoive.

Échec de la désactivation

Les API peuvent également être officiellement mises hors service, mais restent en service en raison d'oublis opérationnels. Ces API sont parfois appelées API zombies.

Anciennes versions d'API

Parfois, une ancienne version d'API n'est jamais mise hors service. Deux versions différentes peuvent avoir à coexister un certain temps lors de la mise à jour du logiciel. Mais que se passe-t-il si la personne responsable de la désactivation de l'API quitte l'entreprise, est mutée ou oublie simplement d'arrêter l'ancienne version ?

Raccourcis et échecs de processus

Certaines API indésirables viennent du fait que l'on omet d'informer les bonnes personnes. Par exemple, une équipe métier (LOB) peut créer des API pour répondre à des besoins spécifiques sans en informer le service informatique, ou les développeurs peuvent être plus préoccupés par l'exécution que par le respect de la procédure. Les API « héritées » dans le cadre d'une acquisition sont également souvent négligées. Ces types d'API indésirables sont souvent appelées API fantômes.

Lorsque vous discutez avec des fournisseurs, demandez-leur d'expliquer comment ils s'assurent que les API indésirables, héritées, zombies et fantômes sont identifiées et traitées avant qu'elles ne puissent être exploitées. Les API héritées et zombies sont souvent le maillon faible de la sécurité des API. Il est donc essentiel de découvrir les API qui ne sont pas gérées par une passerelle d'API et de les localiser, de les inventorier et de déterminer si elles nécessitent une correction ou une mise hors service.

Principales fonctionnalités de détection des API

Une solution de sécurité des API doit intégrer les fonctionnalités de détection suivantes

Détection des ressources API et inventaire granulaire

Un outil de détection des API doit être capable de localiser et d'identifier les API dont vous disposez, indépendamment de leur configuration ou de leur type, y compris RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC et gRPC. Il doit également créer un inventaire mis à jour automatiquement pour éviter qu'il ne devienne obsolète, et fournir la possibilité de rechercher, d'étiqueter, de filtrer, d'attribuer et d'exporter des API en fonction de n'importe quel attribut.

Détection des API inactives, héritées et zombies

Les API héritées et zombies peuvent précéder les initiatives de sécurité des API de votre organisation. Ces API n'ont généralement pas de propriétaire et fonctionnent sans visibilité ni contrôle de sécurité. Il est essentiel que l'outil de détection des API soit en mesure de localiser ces API.

Détection des domaines fantômes

En plus des API fantômes, vous pouvez avoir des domaines fantômes entiers : des noms de domaine API dont vous ne savez rien. Les outils de détection des API doivent être en mesure d'identifier les domaines fantômes oubliés, négligés ou autrement inconnus qui pourraient présenter un risque de sécurité.

Analyses automatiques

L'analyse est essentielle pour éliminer les angles morts et identifier les problèmes critiques, notamment :

- les divulgations de clés d'API et d'informations d'identification ;
- l'exposition de code API et de schémas ;
- les mauvaises configurations d'infrastructure ;
- les vulnérabilités dans la documentation, les référentiels GitHub, les Postman workspaces, etc.

L'identification de ces sources et d'autres sources de renseignements exploitables peut également aider les équipes à comprendre les voies d'attaque potentielles pouvant être exploitées par les cybercriminels.

Développement personnalisé limité

Enfin, doté du bon outil de détection des API, vous ne devriez pas avoir besoin de développement personnalisé pour les sources de trafic. Ces outils doivent être fournis avec des intégrations prédéfinies pour les principaux composants de l'infrastructure. Le développement personnalisé est généralement chronophage, et si l'origine de la source est modifiée, l'intégration doit probablement être retravaillée, ce qui n'est pas évolutif pour les équipes de sécurité informatique surchargées.

Gestion de la posture des API : plongée en profondeur dans les fonctionnalités clés

Les menaces pesant sur l'ensemble de vos API augmentent rapidement en raison de tendances telles que le passage de l'informatique centralisée à des opérations LOB décentralisées, l'utilisation accrue des ressources cloud et la transition vers des architectures basées sur les microservices.

La mise en place d'un outil de détection robuste (comme décrit dans la section précédente) est la première étape de la sécurisation de vos API. Vous devez identifier et inventorier les API de tous types qui sont actuellement utilisées.

Plusieurs fonctionnalités supplémentaires sont essentielles pour gérer votre posture de sécurité des API. Vous devez être en mesure d'identifier les API qui accèdent aux données sensibles et les transmettent, et de les classer en conséquence, car les API qui touchent des données telles que les informations client doivent absolument être authentifiées. Il est également important d'identifier les vulnérabilités de l'infrastructure qui rendent les API plus vulnérables.

Évaluation de la configuration

De nombreuses cyberattaques aboutissent en raison d'une simple mauvaise configuration des réseaux, des passerelles API ou des pare-feux qui servent d'intermédiaires et protègent le trafic API.

La solution de sécurité des API doit analyser régulièrement les configurations d'infrastructure et de logiciels, y compris les fichiers journaux, les rediffusions du trafic historique, les fichiers de configuration, etc. Cela vous permet de détecter les erreurs de configuration et les vulnérabilités, et d'éliminer le risque de dérive de la configuration.

Gravité personnalisable

Au fur et à mesure que la solution identifie de nouvelles vulnérabilités dans votre environnement, elle doit également attribuer un niveau de gravité aux problèmes découverts afin qu'ils puissent être traités par ordre de priorité.
Les niveaux de gravité doivent être personnalisables pour s'aligner sur la tolérance au risque, les exigences réglementaires et les stratégies internes de votre organisation.

Flux de travail personnalisés

En plus de la gravité personnalisable, l'outil idéal de gestion de la posture doit vous permettre de créer des flux de travail personnalisés vous permettant de prendre des mesures immédiates lorsque vous identifiez des vulnérabilités.
Ces workflows peuvent aller de la création de tickets à la notification des parties prenantes clés en passant par la mise à jour des configurations réseau.

Documentation générée automatiquement

La documentation sur les API indique aux utilisateurs d'une API ce qu'elle fait et comment l'utiliser. Les organisations doivent évaluer la conformité des API sécurisées par rapport aux spécifications et à une documentation précise. Une documentation médiocre ou inexistante rend les tests de sécurité plus difficiles et augmente le risque qu'une API parvienne en production avec une vulnérabilité non détectée. Ce problème est souvent exacerbé par l'externalisation du développement des API. Quelle que soit la source du problème, une documentation obsolète, incomplète ou manquante est inacceptable si vous voulez que votre programme de sécurité des API soit efficace.

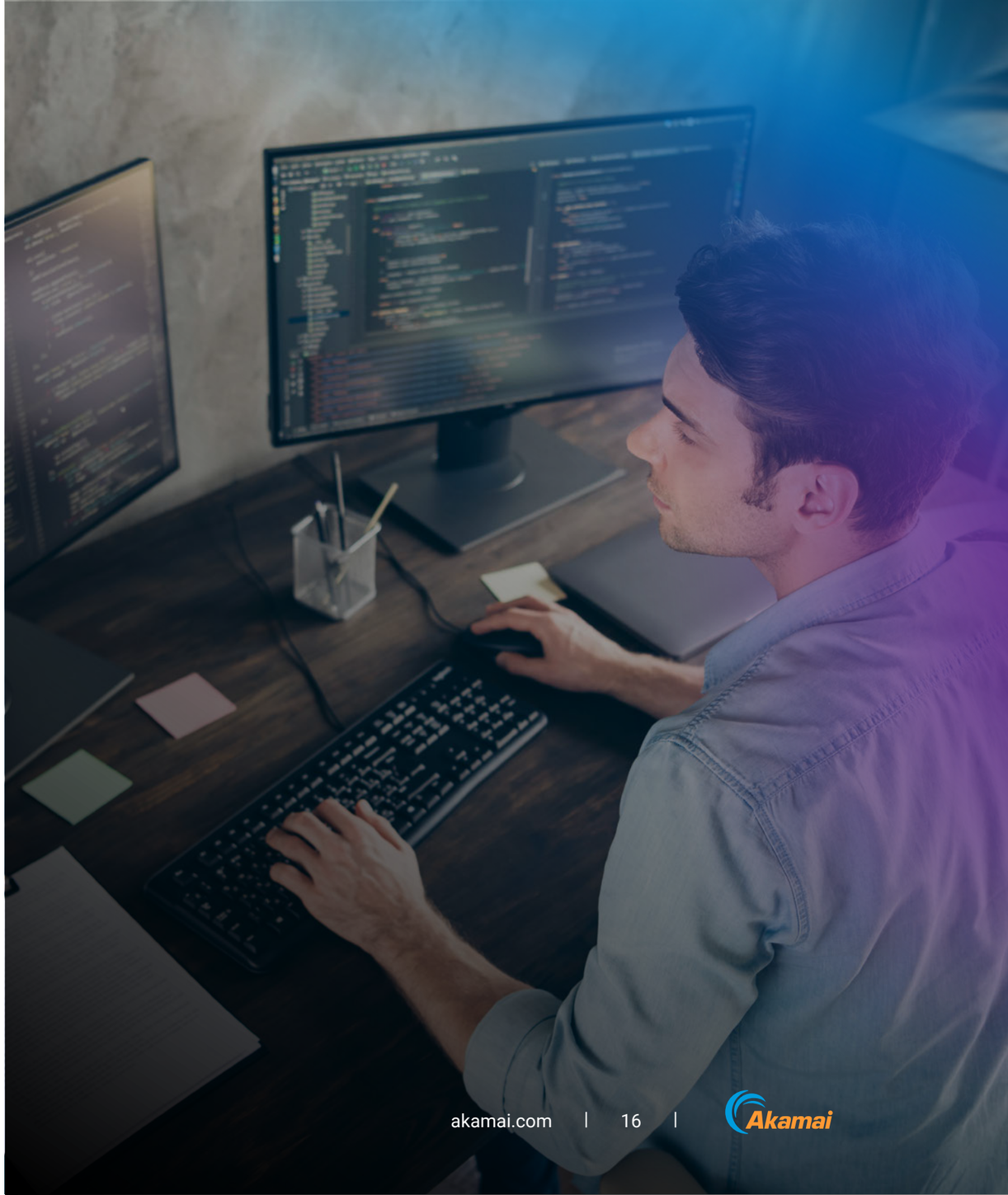
La spécification OpenAPI définit les descriptions d'interface standard. Une solution de sécurité des API doit être en mesure de :

- comparer les spécifications d'API au trafic observable réel et identifier les différences, ce qui permet aux organisations de voir lesquelles de leurs API déployées ne sont pas conformes aux spécifications et représentent un risque potentiel ;
- générer automatiquement une documentation OpenAPI complète basée sur l'état actuel et futur des API pour vous assurer que toutes les API sont correctement documentées et que la documentation est à jour. L'identification de ces sources et d'autres sources de renseignements exploitables peut également aider les équipes à comprendre les voies d'attaque potentielles pouvant être exploitées par les cybercriminels.

Détection et correction des menaces API : plongée en profondeur dans les fonctionnalités clés

Les attaques qui tentent d'exploiter les vulnérabilités des API sont désormais une réalité. La question n'est plus de savoir si votre organisation sera attaquée, mais quand et comment. Il est devenu impératif de détecter les attaques rapidement et de les bloquer avant qu'elles ne causent des dommages importants, comme l'exfiltration d'informations à caractère personnel. Même si vos API sont aussi sécurisées que possible, il vous faut une protection active de la durée d'exécution pour détecter les fuites de données, la falsification de données, les violations de stratégies de données, les comportements suspects et les attaques de sécurité des API. Cette protection doit inclure la journalisation du trafic d'API, la surveillance de l'accès aux données sensibles, la détection des menaces et le blocage ou la correction des vecteurs d'attaque.

Dans les deux pages suivantes, nous décrivons les principales fonctionnalités qu'une solution de sécurité des API doit inclure.



Surveillance hors bande en temps réel

La surveillance de la sécurité des API ne doit pas affecter ni ralentir le trafic d'API. Recherchez des fournisseurs capables de fournir une approche sans agent, permettant aux entreprises d'effectuer un déploiement plus rapide et de visualiser plus de trafic. Toutefois, dans des circonstances appropriées (par exemple, environnements complexes sur site), la solution doit être suffisamment flexible pour prendre également en charge des agents.

La solution de sécurité des API doit refléter le trafic provenant de sources de données identifiées et effectuer une analyse de ces données de trafic en arrière-plan, avec des alertes en temps réel à chaque fois qu'un problème est détecté.

Détection des anomalies des API et des tentatives d'exploitation

La collecte passive de données ne suffit pas, d'autant plus que le nombre d'API et le volume total de trafic API continuent d'évoluer. L'activité des API doit être analysée en permanence pour détecter les événements anormaux et alerter les équipes de sécurité et d'exploitation.

Les outils avancés intègrent des fonctionnalités d'IA et d'apprentissage automatique pour analyser le trafic en temps réel et tirer parti des informations contextuelles pour identifier les activités anormales pouvant indiquer une fuite de données, une falsification des données, des violations des politiques de données et d'autres attaques de sécurité des API.

Prévention des attaques d'API

Une fois qu'une anomalie ou un autre problème a été identifié et qu'une alerte a été générée, il est essentiel d'agir rapidement. Les mouvements non autorisés de données sensibles via des API ou toute autre utilisation abusive présumée des API doivent être détectés et bloqués. La solution de sécurité des API ne doit pas seulement bloquer les utilisations abusives grâce à son intégration à vos pare-feux et passerelles API existants, elle doit également automatiser partiellement ou totalement la correction. Une correction semi-automatisée doit être disponible pour traiter certains types d'alertes. Pour les problèmes récurrents précédemment identifiés, vous devez avoir la possibilité de fournir une réponse entièrement automatisée.

Score de probabilité d'attaque

Certaines solutions sur le marché utilisent des algorithmes d'apprentissage automatique formés pour évaluer les signaux externes et internes, y compris le comportement des API, les modèles de trafic réseau, les données de géolocalisation et les flux de renseignements sur les menaces. À l'aide de facteurs contextuels comme ceux-ci, la solution peut déterminer le niveau de probabilité qu'un incident de durée d'exécution détecté est le résultat d'une activité malveillante.

Intégrations pour la réponse aux incidents

Lorsqu'un incident se produit, la solution de sécurité des API doit inclure les intégrations nécessaires pour s'assurer que les tâches de correction sont attribuées aux équipes appropriées. Si des erreurs de configuration, des violations des politiques de données ou des comportements suspects sont détectés, ils doivent être signalés à la passerelle d'API, au système SIEM et à d'autres moteurs de sécurité de l'information afin de garantir le niveau approprié de prise de conscience.

En règle générale, la solution de sécurité des API doit s'intégrer facilement aux autres outils de sécurité, de surveillance et de gestion utilisés par votre organisation.

Tests de sécurité des API : plongée en profondeur dans les fonctionnalités clés

L'une des erreurs que commettent de nombreuses équipes de développement consiste à attendre trop longtemps pour commencer les tests d'API, ce qui fait que les tests deviennent des goulots d'étranglement. Les équipes doivent adopter une approche « shift-left » pour s'assurer que les tests commencent suffisamment tôt dans le processus de développement afin qu'ils soient exhaustifs. Les avantages de mener des tests de sécurité des API efficaces sont considérables :

- **Prévention des attaques**
  - En détectant les vulnérabilités avant que les API n'entrent en production, vous réduisez le risque de réussite des attaques.
- **Amélioration de la conformité**
  - Des tests complets vous aideront à garantir la conformité et à éviter les amendes et les atteintes à la réputation.
- **Renforcement de la confiance**
  - Des tests rigoureux et efficaces permettent d'accroître la confiance de votre organisation dans les API et contribuent à ce que les versions de vos développeurs soient disponibles en temps voulu.

Certains fournisseurs sur le marché peuvent proposer aux entreprises des recommandations sur la façon de résoudre les problèmes dans leurs environnements, ainsi que sur la façon d'activer des configurations de test d'API complètes. Les recommandations peuvent inclure des étapes d'action pour configurer les authentifications appropriées ou corriger les dépendances des API. L'avantage : si vous pouvez résoudre les problèmes de logique applicative au sein de votre environnement, vous pouvez augmenter le nombre d'API optimisées pour les tests, ce qui se traduit par une couverture de tests plus étendue.

Cependant, le concept de test de sécurité des API reste quelque peu nébuleux. Les équipes de développement peuvent ne pas comprendre pleinement ce que cela implique. Le test d'API « shift-left » est un processus en trois étapes :

1. **Comprendre l'API :** la compréhension du cas d'utilisation de l'API permet d'éclairer les tests, en particulier pour les questions délicates de logique d'entreprise.
2. **S'assurer de pouvoir interagir correctement avec l'API :** assurez-vous que vous pouvez utiliser l'API comme prévu. Cela est essentiel pour vous assurer que votre compréhension de l'API correspond à son fonctionnement.
3. **Envoyer le trafic d'attaque à l'API :** cela peut inclure la manipulation manuelle des requêtes vers l'API, l'insertion de chaînes de fuzzing dans les requêtes, ou l'utilisation d'un outil automatisé pour effectuer des tests de sécurité des API. Comme pour tout dans l'informatique actuelle, l'automatisation est souvent le meilleur moyen de réaliser une tâche à grande échelle sans renoncer à la vitesse.

Principales fonctionnalités des tests de sécurité des API

Les tests de sécurité des API doivent inclure des tests statiques, dynamiques et d'intrusion. La solution de sécurité des API doit inclure des outils permettant de faciliter la réalisation de tests approfondis, en automatisant les processus de tests dans la mesure du possible. Vérifiez que la solution de sécurité des API dispose des fonctionnalités de test des API suivantes :

Tests de sécurité des API automatisés et proactifs

Les tests de sécurité automatisés réduisent considérablement les risques et les coûts en identifiant les erreurs de configuration, les vulnérabilités et les non-conformités, avant qu'une API n'entre en production.

Gouvernance d'API

Il est essentiel de réfléchir aux questions de gouvernance liées notamment aux rôles, aux responsabilités et aux politiques. Cela inclut les responsabilités au niveau de l'exécution pour les développeurs, les ingénieurs de sécurité et les ingénieurs de plateforme, ainsi que la surveillance des politiques et les décisions concernant les risques. La solution de sécurité des API doit vous permettre d'examiner les spécifications de vos API par rapport aux politiques et règles de gouvernance établies.

Pipeline CI/CD et intégration du référentiel de code

L'approche DevSecOps est une variante de l'approche DevOps qui ajoute la sécurité au workflow du développement logiciel. La sécurité des API doit faire partie des initiatives DevSecOps. La solution de sécurité des API doit fournir une suite de tests de sécurité axés sur les API qui s'exécutent à la demande ou dans le cadre d'un pipeline CI/CD. L'intégration CI/CD est essentielle, car elle permet d'effectuer des tests de sécurité des API rapides et continus, nécessaires pour suivre le développement des applications.

Tout réunir : identifiez et corrigez les failles de sécurité de vos API

Les API sont une composante essentielle de la capacité des organisations à servir leurs clients, générer des revenus et fonctionner efficacement dans une économie de plus en plus digitale et centrée sur le cloud. Cependant, leur croissance continue, leur proximité avec les données sensibles et l'absence de contrôles de sécurité font des API une cible attrayante pour les pirates d'aujourd'hui.

Les outils existants utilisés par de nombreuses organisations pour gérer les API et obtenir une protection de base permettent dans une certaine mesure de réduire les risques. Mais ils ne sont pas suffisants pour faire face aux menaces API d'aujourd'hui. Ils ne peuvent pas être considérés comme les seules sources de protection.

Les entreprises doivent plutôt rechercher une solution de sécurité des API complète qui peut fournir les quatre composants abordés dans ce guide de l'acheteur : découverte, gestion de la posture, détection et correction des menaces, et tests de sécurité. Il n'est pas nécessaire de délaisser les outils existants qui se sont avérés efficaces dans certains domaines : il vous suffit de rechercher une solution qui s'intègre de façon harmonieuse à vos outils existants.

Faire vos premiers pas dans la sécurité des API ne signifie pas que vous devez y allouer des ressources importantes. Vous pouvez commencer par vous engager dans un projet pilote mesurable à petite échelle, visant à combler des lacunes spécifiques de votre système de sécurité. Vous pouvez aussi démarrer votre parcours de sécurité des API par une mise à jour complète. Chaque organisation est différente.

Avec l'augmentation des attaques dirigées contre les API, l'étape la plus importante consiste à décider d'agir. Nous espérons que ce guide de l'acheteur vous a été utile.

En savoir plus sur les méthodes d'attaque des API, les vulnérabilités courantes des API et la façon de sécuriser votre organisation.

Découvrez comment nous pouvons vous aider en planifiant une **démonstration personnalisée d'Akamai API Security**.

La solution de sécurité d'Akamai protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur **akamai.com** et **akamai.com/blog**, ou abonnez-vous à Akamai Technologies sur **X** (anciennement Twitter) et **LinkedIn**. Publication : 09/24.

Akamai