Akamai

LIVRE BLANC

8 choses à faire et à ne pas faire en matière de sécurité des API

Quelques facteurs critiques pour renforcer votre posture de sécurité en matière d'API

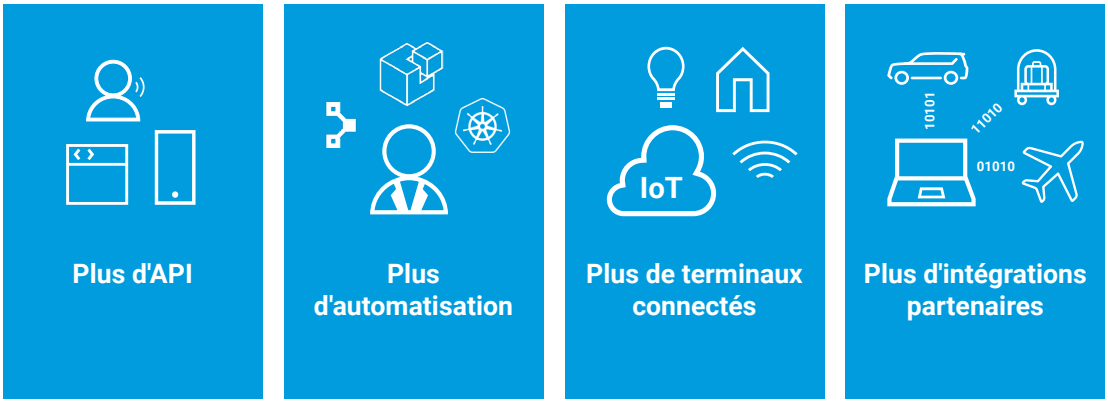
Qu'y a-t-il de si compliqué à protéger les API ?

De nombreux DSI considèrent la sécurité des API comme une priorité absolue. Et cela, à juste titre :

« L'explosion des API crée une surface d'attaque attractive, et la sécurité des API ne cesse de mettre en déroute les responsables de la sécurité. »

— The Eight Components Of API Security, Forrester Research, Inc., 28 septembre 2023

Facteurs de croissance du risque lié aux API



Face à de tels risques, les organisations doivent comprendre un certain nombre de choses avant de se lancer dans la mise en œuvre d'une stratégie efficace en matière de sécurité des API :

Les API sont une cible mouvante	
Connaissance des API internes	**Exposition des API externes**
Les processus DevOps en évolution rapide créent et désactivent des API en continu, ce qui conduit à un inventaire d'API incomplet	Les pratiques immatures en matière d'API entraînent une exposition involontaire d'API sensibles à des parties externes, avec notamment de nombreuses API fantômes

Les API sont vulnérables à deux types de menaces différents	
Vulnérabilités techniques	**Utilisation malveillante et abusive**
Les hackers peuvent exploiter les vulnérabilités logicielles et les erreurs de configuration, y compris les 10 principaux risques pour la sécurité des API selon l'OWASP	Les abus de logique métier et d'autres comportements, comme l'extraction agressive de données, peuvent se produire indépendamment d'une vulnérabilité technique

Pour relever le défi complexe associé à la sécurité des API, il est essentiel d'adopter une approche mûrement réfléchie qui englobe tous les aspects suivants :

Intégrer les dernières avancées technologiques

Abattre les barrières organisationnelles

Couvrir l'ensemble de l'écosystème des menaces liées aux API

Vous trouverez ci-dessous quelques stratégies essentielles à mettre en œuvre (et les pièges à éviter) pour élaborer une stratégie de sécurité des API plus sophistiquée pour votre entreprise.

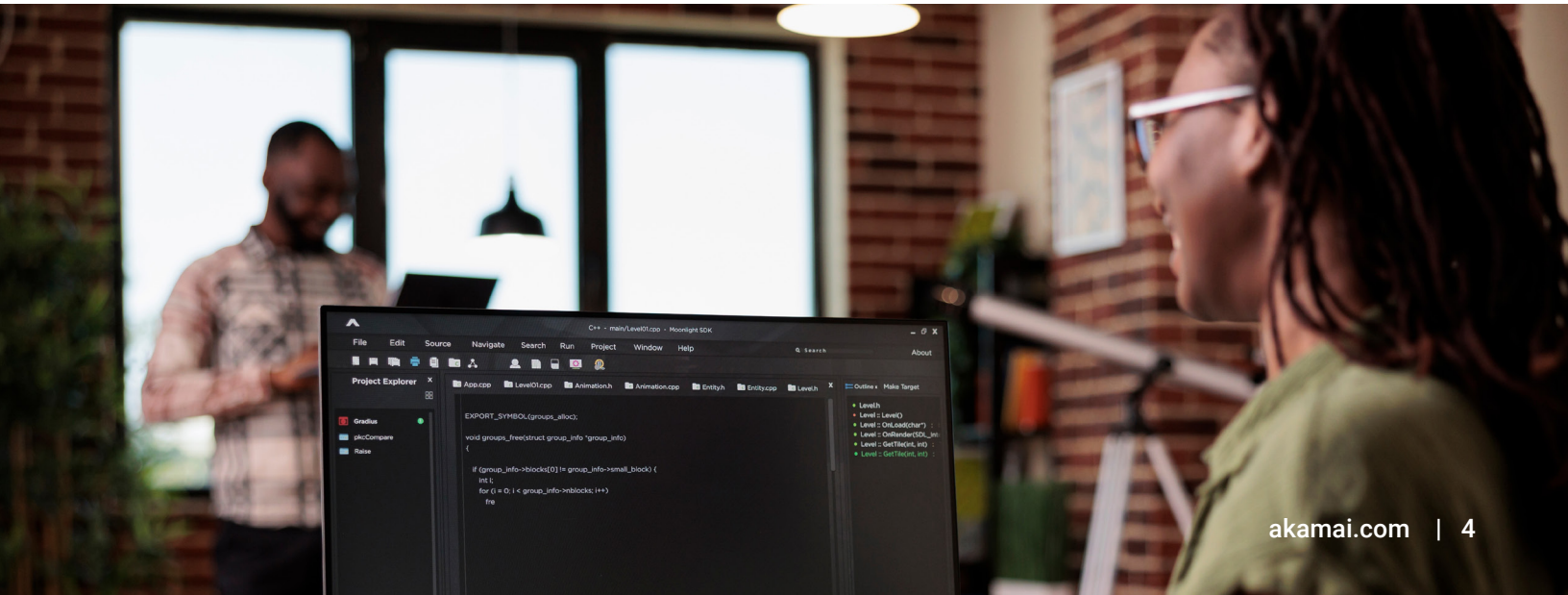
8 choses à faire et à ne pas faire pour une sécurité des API efficace

1 À faire : obtenir une visibilité complète sur les API

On ne le répétera jamais assez : il est impossible de protéger ce que l'on ignore. Plus vous mettrez de temps à identifier une API, et donc à la surveiller, plus elle risque de devenir la cible d'un hacker. Pour bénéficier d'une visibilité complète, l'idéal est de vérifier que votre plateforme de sécurité des API est capable d'ingérer des informations provenant de sources de données les plus variées (passerelles d'API, terminaux réseau, solutions d'orchestration de microservices, fournisseurs de cloud, etc.). Plus précisément, votre solution de sécurité des API doit pouvoir prendre en charge les fonctionnalités suivantes :

Temps	Localisation
• Détecter les API en continu • Surveiller les appels d'API individuels • Enregistrer l'activité de session à court terme • Analyser le comportement des API au fil du temps	• Détecter les API dans toute l'entreprise • Détecter les anciennes API • Détecter les API fantômes

En bénéficiant d'une visibilité complète sur vos API, vous serez en mesure de prévenir les violations de données d'API ; cela est d'autant plus vrai que la toute dernière technique de violation de données consiste pour les hackers à utiliser des attaques de type « low-and-slow » pour extraire des données des API. Savoir où se trouvent toutes vos API est la première étape pour prévenir ce type d'attaque émergent.



2 À ne pas faire : avoir peur du cloud

Les pare-feux d'applications Web (Web Application Firewall, ou WAF) utilisent des techniques basées sur des signatures pour empêcher les API non autorisées de se frayer un chemin dans votre organisation. Comme les attaques d'API ont évolué, vous avez besoin d'une couche supplémentaire pour défendre pleinement vos API face à l'ensemble des risques possibles. Vous devez pour cela recourir à l'analyse comportementale. Car il est devenu essentiel de surveiller le comportement de vos API à l'intérieur de vos murs, sans vous limiter à celles qui sont exposées en externe.

Pour utiliser efficacement l'analyse comportementale, le trafic d'API doit être analysé dans le cloud. Les équipes de sécurité hésitent parfois à envoyer sur le cloud des informations sensibles concernant l'activité de leur entreprise. Mais sans le degré d'échelle et d'élasticité offert par le cloud, il est difficile d'entreprendre de véritables analyses comportementales fondées sur l'utilisation de techniques de détection et de réponse à grande échelle sur le volume de données d'API générées par la plupart des entreprises.

Qui plus est, les équipes de sécurité disposent de ressources limitées et fortement sollicitées ; lorsqu'ils sont longs et complexes, les déploiements de produits constituent donc pour elles un obstacle majeur au progrès. Mais compte tenu de l'intensification des risques associés à une utilisation plus massive des API, les équipes de sécurité ne peuvent se permettre de prendre davantage de retard. C'est pourquoi il est essentiel de sauter le pas et d'amorcer votre transition vers le cloud dans le cadre de votre stratégie de sécurité des API.

3 À faire : placer le contexte de l'entreprise au centre de votre stratégie

La découverte des API et l'identification des risques pour la sécurité ne marquent que les premières étapes d'un parcours qui vous aidera à réduire la surface d'attaque de vos API. Tâchez de répondre aux trois questions suivantes :

1. Comment savoir si les informations d'identification d'API d'un partenaire spécifique ont été visées par une attaque ?
2. Comment savoir si vous n'êtes pas victime d'espionnage, dissimulé sous la forme d'une extraction de données sur une API ?
3. Comment savoir si votre API de facturation est exploitée par un utilisateur peu scrupuleux qui énumère des numéros de facture pour dérober des données de compte ?

Dans le premier scénario, l'activité pourrait sembler provenir d'un utilisateur légitime. Par conséquent, la seule façon de détecter une intention malveillante est de remarquer un changement par rapport au comportement attendu sur l'API en question. Les deuxième et troisième scénarios sont également des exemples de comportements interdits qui exploitent des modèles d'accès API légitimes. Là encore, il est important de comprendre le contexte de l'entreprise, en plus de ce qu'il se passe sur le plan technique.

4 À ne pas faire : utiliser les données comme une voie à sens unique

Pour être efficace, une approche de la sécurité des API doit notamment être capable d'envoyer des alertes et des événements aux outils de surveillance de la sécurité et de workflow IT choisis par l'entreprise. Les fournisseurs de solutions de sécurité (et les équipes qui implémentent les alertes) font souvent l'erreur de considérer les alertes de sécurité et les réponses automatisées comme un flux de communication unidirectionnel.

Tout comme de nombreux processus métier légitimes, les attaques peuvent se produire sur une longue période. Les analyses comportementales portant sur l'utilisation des API doivent être effectuées sur une période d'au moins 30 jours pour être véritablement efficaces. Cette durée permet d'obtenir une représentation plus complète et précise du comportement de base attendu. Elle permet également de détecter les attaques qui sont exécutées lentement sur plusieurs jours ou plusieurs semaines, ainsi que les nombreuses sessions d'API. Soyez attentif à une attaque par extraction de données de type « low-and-slow » qui atteint un niveau inférieur à une limite de débit définie : on ne pourrait identifier ce type de comportement qu'en examinant le comportement historique et en le comparant à d'éventuels changements.

Une alerte sans détails à l'appui est très certainement plus préjudiciable que bénéfique. À l'inverse, il est beaucoup plus facile d'exploiter une alerte qui retrace la cause et l'impact en contexte. Mais l'idéal reste de déclencher des alertes à la fois exploitables et riches en contexte, et de donner à leur destinataire la possibilité d'interroger un vaste ensemble de données afin d'analyser l'incident. Vous pouvez dès lors tirer parti de vos protections WAF pour bloquer immédiatement le trafic qui présente une menace potentielle pour votre entreprise.

5 À faire : donner la priorité à la collaboration transversale

Il peut être judicieux de prévenir les vulnérabilités en amont, au stade de la conception, du développement et du déploiement, car c'est de cette manière que la sécurité des API peut révéler tous ses avantages. Pour y parvenir efficacement, vous devez encourager la collaboration entre vos équipes.

Démarrez ce processus collaboratif en donnant à vos équipes d'API une visibilité sur la manière dont les API sont utilisées (à bon escient ou non) en situation réelle. Au fil du temps, cette exposition favorisera une culture de réflexion sur la sécurité dès les premières phases du processus de développement et de déploiement d'API. Assurez-vous également :

- que les équipes d'API voient, au-delà des fonctions de sécurité de base de votre approche, d'autres avantages qui les motivent à renforcer leur collaboration ;
- que les utilisateurs qui n'ont aucune expertise de la sécurité (les développeurs, par exemple) ont la possibilité d'afficher et d'interroger facilement les informations d'inventaire et d'activité des API ;
- d'utiliser des réponses contextuelles, telles que des intégrations dans des outils de développement, comme Jira, qui ouvrent des tickets de manière proactive pour couvrir les correctifs de sécurité que les développeurs doivent créer.

Dites-vous bien que la sécurité des API est l'affaire de tous et que le fait de favoriser l'implication des parties prenantes extérieures permet d'éviter les accusations infondées, tout en aidant les équipes de développement, d'exploitation et de sécurité à travailler main dans la main d'une manière profitable à tous.

6 À ne pas faire : négliger les API tierces

Dans les stratégies de sécurité des API, il est courant de supposer (à tort) que vous n'avez qu'à vous soucier de vos propres API. Aussi plaisant serait-il de croire que le WAF ou la passerelle d'API dans lesquels vous avez investi standardisent l'ensemble de votre stratégie de sécurité des API, force est de constater que ce n'est pas toujours le cas.

Par exemple, ne partez pas du principe que, parce que vous avez mis en œuvre une stratégie fondée sur une passerelle d'API, les API fantômes ne pourront pas contourner l'approche de gouvernance des API de base. Si votre entreprise s'appuie sur des API tierces, votre passerelle identifierait ces API comme étant authentifiées, et cela même si elles étaient compromises avant de se connecter à votre écosystème.

Votre stratégie de protection des API doit être liée à vos principales technologies d'API, notamment les passerelles d'API, tout en veillant à recueillir autant d'informations que possible à partir d'autres sources, telles que les terminaux réseau, les plateformes cloud et les outils d'orchestration des microservices. C'est la seule façon de créer une image complète de la surface d'attaque de vos API et de pérenniser votre stratégie de sécurité dans un contexte où les transitions de technologies et d'infrastructure sont inévitables.

7 À ne pas faire : répondre et passer à autre chose

Réagir rapidement et efficacement aux alertes est une excellente chose. Cela dit, si vous vous concentrez uniquement sur l'idée d'atténuer les alertes une fois qu'elles ont été déclenchées, vous aurez raté une occasion de les éviter purement et simplement. Envisagez plutôt de vous lancer dans une recherche proactive des menaces. Si le partenaire que vous avez choisi pour la sécurité des API vous permet d'effectuer des requêtes sur les données, vous serez en mesure de tester vos propres hypothèses, de comprendre les relations et d'identifier les menaces potentielles avant qu'elles ne dégénèrent en incident de sécurité. Par exemple, si vous identifiez un mauvais comportement d'utilisation des API chez un partenaire spécifique, vous pouvez rechercher un comportement similaire chez d'autres partenaires ou fournisseurs en seulement quelques clics.

Tout partenaire de sécurité des API doit stocker des données historiques dans un lac de données et fournir un accès à ces données pour faciliter le travail d'enquête et de recherche des menaces.

Idéalement, ce type de fonctionnalités de requête enrichies doit être mis à votre disposition de deux manières :

1. sous la forme d'une interface Web simple et intuitive ;

2. sous la forme d'un ensemble d'interfaces d'API que les fournisseurs de sécurité des API eux-mêmes utilisent pour développer des flux de travail plus sophistiqués.

8 À faire : aborder la sécurité des API comme un cycle de vie continu

La meilleure façon d'intégrer la sécurité des API directement dans votre entreprise consiste à tester les API. En ajoutant cet outil au cycle de vie des API, vous pouvez limiter les risques qu'une API mal configurée ou vulnérable soit déployée dans votre environnement de production. Cet effort visant à tester et corriger à un stade plus précoce du cycle de développement contribue à réduire la complexité, à faire gagner du temps et à alléger les dépenses.

Les équipes responsables de la sécurité doivent ensuite commencer leurs efforts de protection des API en créant un inventaire des API utilisées par leur organisation. Les API étant ajoutées et supprimées en permanence, il est essentiel pour ces équipes de conserver un inventaire dynamique des interfaces d'API dans leurs applications sensibles et dans leurs référentiels de données. Réalisée efficacement, une découverte continue permet de reléguer au passé le problème des API fantômes, malveillantes, oubliées, zombies, orphelines et obsolètes.

Les équipes de sécurité doivent disposer de la visibilité dont elles ont besoin pour détecter et atténuer un large éventail de menaces émergentes en matière de sécurité des API. Mais la détection des menaces doit également intervenir au moment de l'exécution. Les abus de logique métier ne sont détectés que sur les API en production. Le fait de comparer le comportement d'exécution aux schémas d'utilisation normale de référence permet de révéler les comportements abusifs.

Enfin, il est important d'arrêter les menaces qui pourraient tirer parti de vos API à tout moment pendant l'exécution. Le blocage automatique par le WAF est essentiel à ce stade, car le simple fait de générer des alertes pour tout ne suffira pas à protéger votre entreprise au niveau plus global. D'autres réponses automatisées peuvent être variées et personnalisables : il peut s'agir, par exemple, d'abaisser la limite de débit sur la passerelle d'API, d'ouvrir un ticket JIRA pour qu'un développeur puisse examiner le problème, ou encore d'envoyer un e-mail à l'équipe de sécurité. Il n'est possible de réagir de façon appropriée pour chaque menace détectée qu'à condition de comprendre le contexte et de s'appuyer sur un mécanisme de réponse personnalisable.

Synthèse

À faire	À ne pas faire
✓ Obtenir une visibilité complète sur les API	✗ Ne pas avoir peur du cloud
✓ Placer le contexte de l'entreprise au centre de votre stratégie	✗ Ne pas utiliser les données comme une voie à sens unique
✓ Donner la priorité à la collaboration transversale	✗ Ne pas négliger les API tierces
✓ Aborder la sécurité des API comme un cycle de vie continu	✗ Ne pas répondre et passer à autre chose

Lancez-vous

Prêt à adopter une approche moderne et systématique de la sécurité des API ?

En savoir plus sur Akamai API Security.

L'approche basée sur le cloud d'Akamai vous aide à vous lancer en quelques minutes. En seulement quelques heures, vous disposerez d'une image complète de la manière dont les API sont utilisées dans votre organisation et comprendrez en détail les relations entre votre logique métier et vos API.