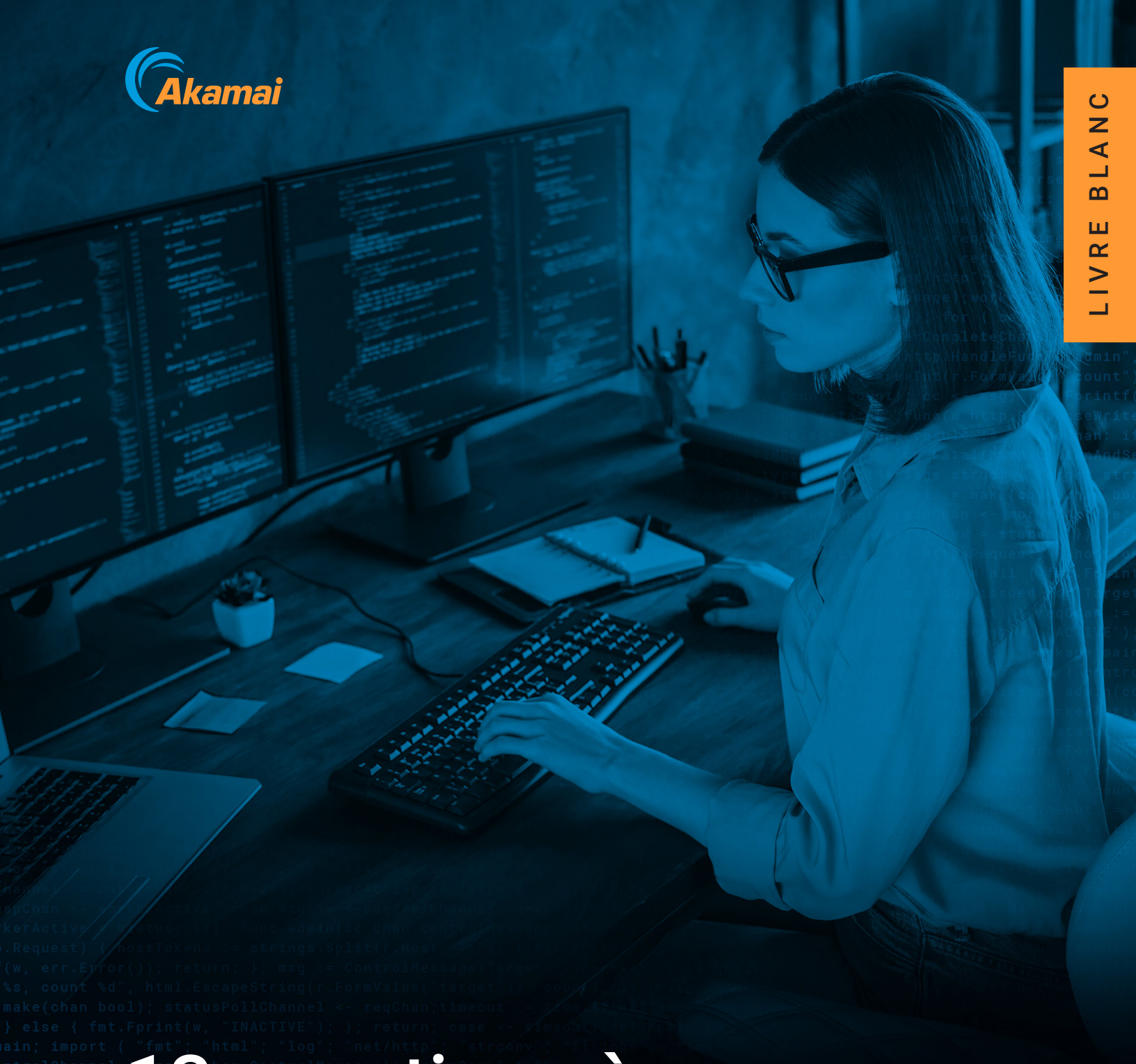
Akamai

LIVRE BLANC



13 questions à poser à votre fournisseur de solutions de sécurité des API

Introduction

Le réseau d'API B2B enregistre une forte croissance. En parallèle, l'univers en pleine expansion de terminaux IoT offre aux développeurs de nouvelles opportunités d'utiliser des API pour intégrer des données réelles dans leurs applications.

Mais si les API ouvrent de nombreuses nouvelles opportunités d'innovation et de croissance, elles introduisent également toute une série de défis en matière de sécurité, notamment :

- vol d'informations d'identification d'API ;
- reconnaissance d'API non détectées ;
- authentification et autorisation mal configurées ;
- API zombies et fantômes non protégées ;
- exécution de code à distance, injection, inclusion de fichiers locaux et autres techniques d'attaque ;
- fuite ou exfiltration de données ;
- extraction d'API ;
- abus de logique métier.

Les fournisseurs de solutions de sécurité proposent de nombreuses options permettant de détecter et d'atténuer ces problèmes ou d'autres menaces liées aux API, mais toutes ne sont forcément efficaces ou faciles à utiliser.

Les 13 questions suivantes vous aideront à cadrer vos discussions avec les fournisseurs de sécurité des API et à évaluer dans quelle mesure leurs produits répondront efficacement aux besoins de sécurité des API de votre organisation.

1 Votre produit de sécurité des API est-il capable de détecter les API à l'échelle de l'entreprise ?

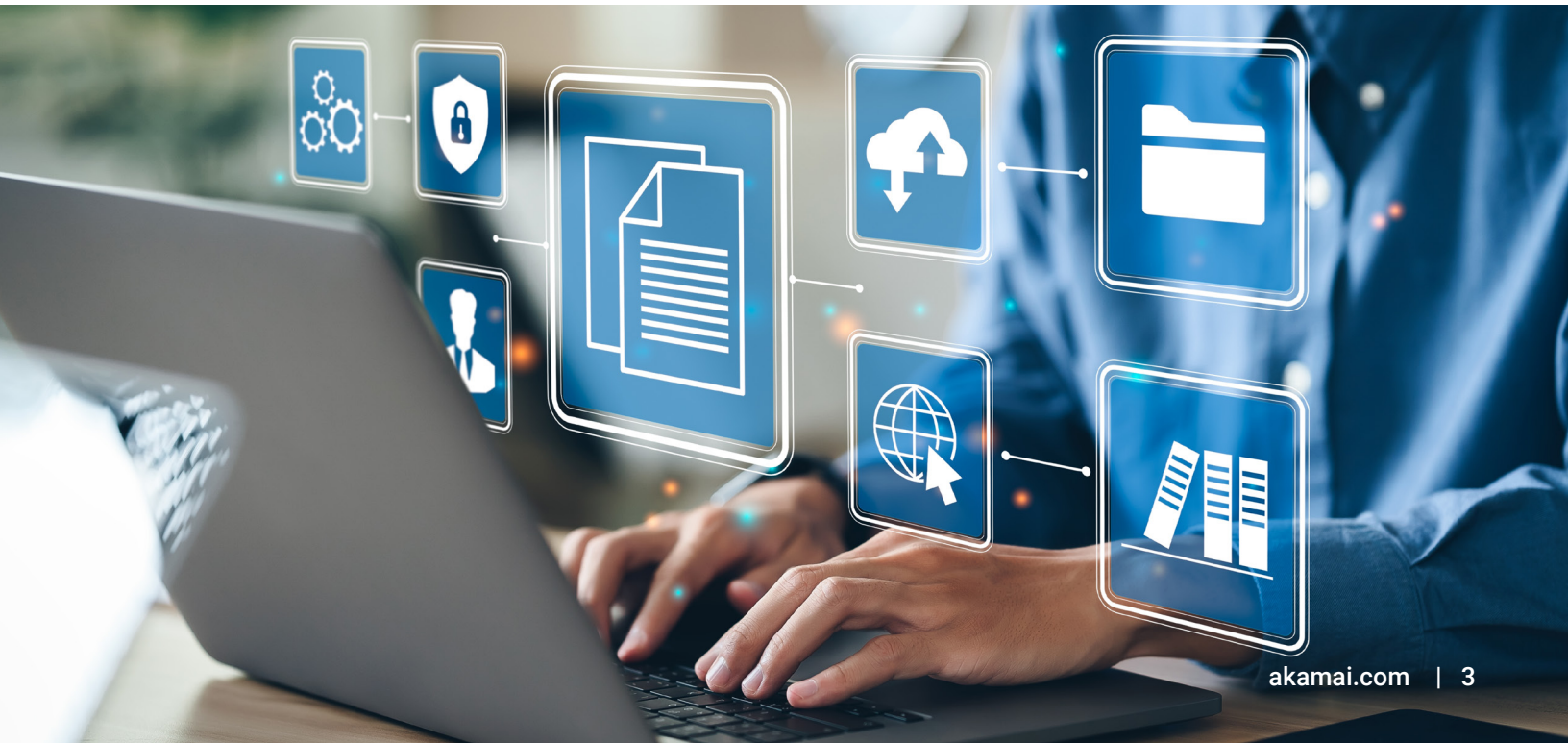
L'un des plus gros problèmes auxquels sont confrontées les équipes de sécurité est qu'elles ne disposent pas d'un inventaire complet et précis de toutes les API exposées par leur entreprise. Bon nombre des API fantômes non documentées qui passent entre les mailles du filet ne font pas partie du cadre formel de gestion et de sécurité des API. Il arrive aussi fréquemment que les API zombies (que l'entreprise pensait avoir supprimées) soient toujours accessibles. Quant aux API approuvées et documentées, elles peuvent dissimuler des paramètres non documentés que des hackers pourraient exploiter. Il est impératif de détecter toutes les API nord-sud, est-ouest et sortantes. La seule façon d'assurer une visibilité complète des API à l'échelle de l'entreprise consiste à examiner les données d'activité des API existantes provenant d'un large éventail de technologies et de plateformes cloud.

2 Votre produit détecte-t-il des API en permanence ? Si oui, ce processus est-il manuel ?

Avec l'évolution rapide des processus DevOps, il n'est pas rare de voir des API apparaître et disparaître régulièrement. Il ne suffit donc plus de dresser des inventaires ponctuels. Votre produit de sécurité des API doit prendre en charge une détection continue pour faire en sorte que les nouvelles API documentées soient correctement inventoriées, analysées et protégées. Dans l'idéal, il doit également être capable d'anticiper toute instance d'API fantôme ou zombie. De plus, les produits qui imposent à votre équipe une charge continue pour interpréter les résultats et agir en conséquence ne sont pas viables sur le long terme. Les produits qui, à l'inverse, s'appuient sur l'automatisation et l'apprentissage automatique à la fois pour détecter et pour évaluer les API aideront votre entreprise à fonctionner de manière plus fluide, sans alourdir la charge de travail de votre équipe par l'introduction de nouvelles tâches manuelles.

3 En quoi votre produit peut-il soutenir mes outils et processus de documentation des API ?

Il est avantageux à plus d'un titre d'intégrer votre approche de documentation à votre plateforme de sécurité des API, c'est pourquoi vous devez vous assurer que votre fournisseur dispose de cette capacité. Par exemple, le fait de télécharger automatiquement la documentation Swagger existante sur votre plateforme de sécurité des API dans le cadre de votre processus d'intégration et de déploiement continus (CI/CD) permet de détecter les API fantômes et d'identifier les paramètres fantômes avec davantage de précision (si le fournisseur a la possibilité de comparer les paramètres d'API détectés à des paramètres déjà documentés). Votre plateforme de sécurité devrait également être capable de créer des fichiers Swagger personnalisés en un clic pour toutes les API qui ne sont pas documentées, afin de permettre à vos développeurs de commencer à améliorer leurs processus de documentation.



4 Combien le déploiement de votre produit dans mon environnement me coûtera-t-il en termes de temps et d'effort ?

Le point de départ le plus rapide et le plus efficace consiste à utiliser un produit de sécurité des API de type « Security as-a-service » (SECaaS), capable de capter et d'analyser de manière non intrusive les données d'activité des API sur vos systèmes existants. Si elle repose sur une conception solide, une architecture SECaaS adaptée à la sécurité des API peut être intégrée à votre environnement en seulement quelques minutes, ce qui peut accélérer sensiblement votre délai de rentabilisation, tout en éliminant les coûts et les risques continus associés aux mises à jour du système. Pour gagner encore en agilité, privilégiez un fournisseur qui à la fois assure une protection des applications Web et des API (WAAP), et offre des fonctions de détection d'API et de réponse, afin que les données de trafic d'API circulent de manière fluide entre la solution qui protège votre trafic entrant et la solution qui protège l'ensemble du trafic d'API au sein de votre organisation.

5 Comment votre produit permet-il d'identifier et de hiérarchiser les API détectées qui présentent un risque ?

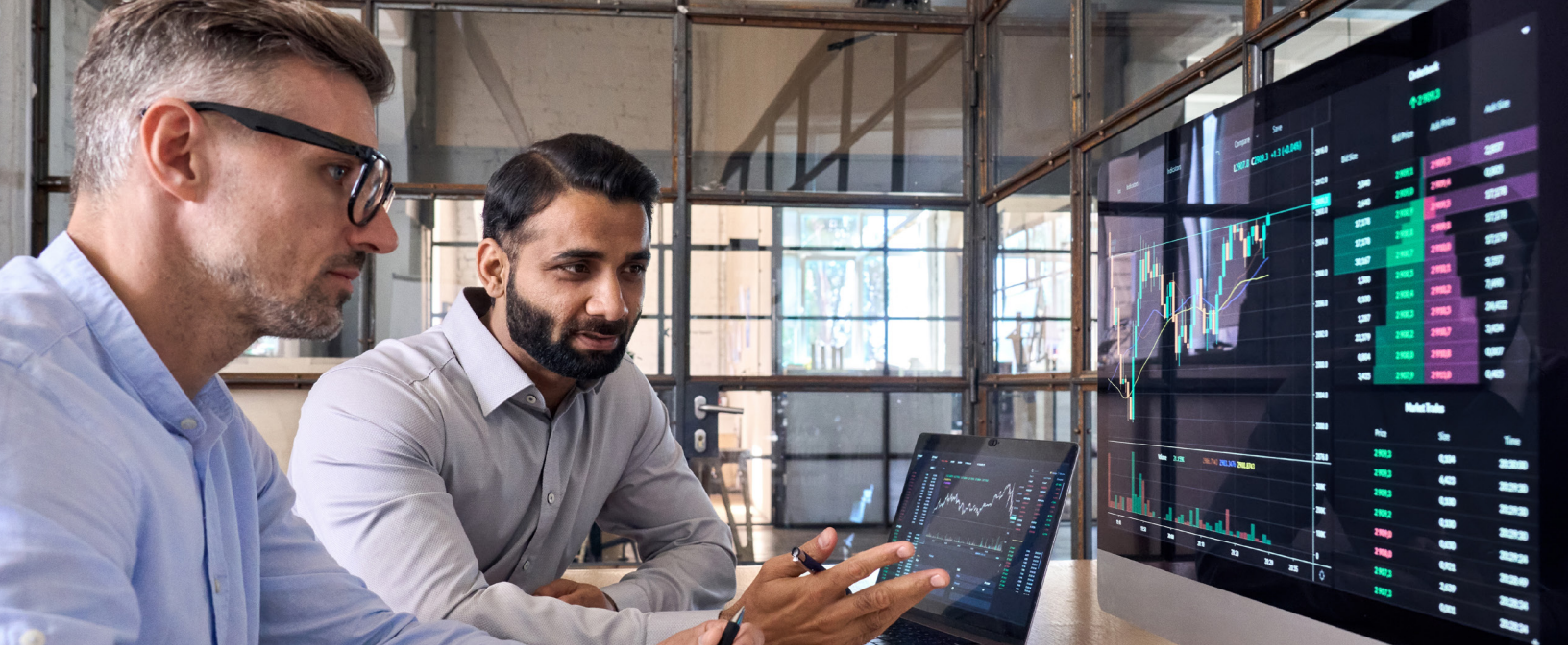
Obtenir pour la première fois un inventaire complet des API peut être une expérience à la fois stimulante et accablante. De nombreuses équipes de sécurité souffrent d'une surcharge d'informations et peinent à identifier les zones sur lesquelles cibler leurs efforts de sécurité des API. Le meilleur moyen d'éviter ce problème consiste à choisir un produit de sécurité des API qui assume à votre place une majeure partie de cette tâche, à savoir :

- mettre en évidence la présence d'API qui rendent les données sensibles accessibles ;
- étiqueter automatiquement les données sensibles par type (par exemple, informations personnelles identifiables, adresses e-mail, données de carte de crédit, etc.).

Votre plateforme de sécurité des API doit également vous permettre de créer des catégories d'étiquetage personnalisées afin que vos équipes responsables des API et de la sécurité parlent le même langage, qui soit cohérent avec vos objectifs métier et vos préoccupations en matière de sécurité.

6 Votre produit utilise-t-il l'analytique comportementale pour établir un comportement attendu de référence et détecter des anomalies ?

De nombreux types d'attaques peuvent être détectés en utilisant des signatures d'attaque qui permettent de les bloquer au niveau de la WAAP. Mais cette approche ne permet pas de détecter certaines attaques référencées dans la liste 2023 des 10 principaux risques pour la sécurité des API selon l'OWASP (Open Web Application Security Project), notamment les autorisations brisées au niveau de l'objet. Ces types d'attaques, plus passifs et davantage axés sur les abus, se révèlent plus difficiles à détecter. Le seul moyen de se défendre efficacement contre tous les vecteurs de menaces liées aux API est d'utiliser l'analytique comportementale et l'apprentissage automatique. Une véritable analytique comportementale implique des ensembles de données volumineux et des algorithmes d'apprentissage automatique qui apprennent les spécificités de votre environnement. Elle doit également offrir la flexibilité et l'agilité nécessaires pour se mettre à jour et s'adapter automatiquement sur la base d'informations globales. Un modèle SECaaS est le seul moyen pratique de réaliser ces activités à grande échelle.



7 Êtes-vous en mesure de collecter et analyser des ensembles de données suffisamment significatifs pour déterminer un comportement normal de référence et détecter les anomalies ?

De nombreux produits de sécurité des API se concentrent sur la surveillance des appels d'API individuels ou, au mieux, sur l'activité de session à court terme. Cette approche est insuffisante car de nombreux processus métier légitimes et bon nombre d'attaques interviennent sur une période bien plus longue. L'utilisation des API doit être analysée sur une fenêtre temporelle glissante (30 jours minimum). Cela fournit une base de référence plus complète et plus précise du comportement attendu, qui tient également compte des processus métier qui n'interviennent qu'une fois par mois (par exemple, la facturation). Cela permet également de détecter les attaques qui sont exécutées lentement sur plusieurs jours ou plusieurs semaines et sur de nombreuses sessions d'API.

8 Votre produit est-il capable d'identifier chaque entité, chaque relation et chaque activité parmi les données d'API brutes de manière à les placer dans le contexte de l'entreprise ?

Pour pouvoir agir sur les données relatives à l'activité des API, le mieux est de les enrichir d'un contexte qui retrace les implications de l'utilisation des API pour l'entreprise. Et pour que votre plateforme de sécurité des API puisse évaluer les relations entre les différentes entités et en établir le profil, elle doit réunir certaines capacités d'identification et d'étiquetage essentielles :

- représentation des utilisateurs d'API (entités utilisateur) : adresses IP, clés d'API, jetons d'accès, ID utilisateur, ID partenaire, ID marchand, ID fournisseur, etc. ;
- représentation des processus métier (entités de processus métier) : réservations, paiements, facturation, solde du compte, etc.

Une analyse granulaire à ce niveau est le seul moyen de transformer la grande quantité de données générées par les API en une base de référence significative et compréhensible du comportement attendu.

9 Votre produit peut-il tracer sur une chronologie chaque activité en fonction de chaque entité contenue dans vos API, de manière à représenter les changements de comportement au fil du temps ?

Bien qu'il soit essentiel de comprendre et surveiller l'activité et les menaces liées aux API à un niveau global, il n'en est pas moins important d'être capable de recentrer votre analyse sur des entités spécifiques. Par exemple, si un comportement anormal est identifié pour un partenaire commercial spécifique, la possibilité de visualiser toutes les activités de cette entité sur une chronologie est un atout inestimable. Il en va de même pour les entités de processus métier. Suivre l'historique complet de ce qu'il s'est passé et à quel moment sur une chronologie établie pour chaque entité de vos API constitue un puissant moyen de visualisation qui permet de mettre clairement en évidence les utilisations normales ou abusives. Pour vous aider à comprendre les abus de logique métier, il est intéressant d'avoir la possibilité de repasser en boucle l'activité pour évaluer les événements avant et après une alerte.

10 Comment puis-je intégrer votre produit à mes outils, processus et flux de travail existants ?

L'envoi d'alertes à votre produit de gestion des informations et des événements de sécurité (SIEM) est certes utile, mais ce n'est qu'un point de départ. Les équipes de sécurité ont aujourd'hui recours à des outils d'orchestration, d'automatisation et de réponse (SOAR) toujours plus sophistiqués pour déclencher des flux de travail prédéfinis chaque fois que des menaces et des incidents de sécurité sont détectés. Et comme de nombreux problèmes liés à la sécurité des API impliquent l'intervention de développeurs extérieurs à l'équipe de sécurité, votre plateforme de sécurité des API doit également s'intégrer aux outils de suivi des problèmes et de gestion des flux de travail de votre équipe de développement. Si votre outil de sécurité analyse le trafic des API, il est logique qu'il utilise également des API pour aider à orchestrer les réponses dans votre CDN, votre pare-feu d'application Web ou votre passerelle d'API et vous permettre de créer vos propres playbooks.

11 Est-il possible d'interroger les données d'API et d'activité de votre produit pour rechercher les menaces et atténuer les risques de manière proactive ?

Les intégrations d'outils de sécurité et de développement ne peuvent pas se résumer à de simples boîtes noires qui envoient des alertes unidirectionnelles à vos outils. Vos équipes responsables de la sécurité et des API doivent pouvoir exploiter les données sources derrière une alerte ou un problème. Privilégiez les plateformes de sécurité des API qui offrent aux utilisateurs la possibilité d'interroger les détails d'API directement via une interface Web intégrée ou au moyen d'API qui permettent d'intégrer la plateforme de sécurité à d'autres outils et interfaces qu'ils aiment utiliser. De cette manière, votre équipe de sécurité sera en mesure d'entreprendre efficacement une recherche proactive des menaces. Cela aidera également vos développeurs et aux autres parties prenantes qui n'interviennent pas dans la sécurité à comprendre comment les API sont ciblées bien qu'elles soient utilisées de manière légitime.

12 Quelles mesures prenez-vous pour garantir la sécurité des données sensibles que vous recueillez sur mon entreprise ?

Les analyses comportementales avancées qui sont indispensables pour sécuriser les API dans l'écosystème des menaces actuel ne peuvent être entreprises qu'avec l'échelle du cloud. Compte tenu de la taille et de la sensibilité de votre ensemble de données d'API, il est important de mettre votre fournisseur de sécurité au défi de s'assurer que vos données seront protégées. Il est important de vérifier les pratiques que votre fournisseur adopte pour sécuriser sa propre infrastructure cloud, mais cela ne suffit pas. Exigez de votre fournisseur qu'il utilise des techniques telles que la tokenisation, c'est-à-dire remplacer les données sensibles par des jetons (« tokens ») anonymisés avant de les transmettre au cloud. Cela garantit la confidentialité des données, même si le fournisseur (ou son fournisseur de cloud en amont) est victime d'un incident de sécurité.

13 Votre solution fournit-elle un accès granulaire aux données d'activité des API ?

Les données sont au centre de la stratégie de prévention des attaques, de la conformité jusqu'à la contextualisation. De nombreux fournisseurs disposent d'un mécanisme qui leur est propre pour stocker les données d'API au fil du temps, mais veillez à creuser davantage cet aspect pour comprendre ce qu'ils proposent réellement. Les solutions fondées uniquement sur les alertes ne font qu'effleurer les événements en surface, car les activités d'API compromises peuvent se dérouler lentement au fil du temps, et pas seulement après le déclenchement de l'alerte. À l'inverse, un fournisseur complet veille à supprimer les angles morts en enregistrant toutes les activités des API et fournit des outils pour examiner cette activité en détail, sans se perdre dans un vague modèle d'apprentissage automatique. Il est important de disposer d'un accès granulaire à vos données, car c'est cette visibilité qui vous permettra de surveiller les menaces de manière proactive, plutôt que de réagir après-coup.

13 questions à poser à votre fournisseur de solutions de sécurité des API

1. Votre produit de sécurité des API est-il capable de détecter les API à l'échelle de l'entreprise ?
2. Votre produit détecte-t-il des API en permanence ? Si oui, ce processus est-il manuel ?
3. En quoi votre produit peut-il soutenir mes outils et processus de documentation des API ?
4. Combien le déploiement de votre produit dans mon environnement me coûtera-t-il en termes de temps et d'effort ?
5. Comment votre produit permet-il d'identifier et de hiérarchiser les API détectées qui présentent un risque ?
6. Votre produit utilise-t-il l'analytique comportementale pour établir un comportement attendu de référence et détecter des anomalies ?
7. Êtes-vous en mesure de collecter et analyser des ensembles de données suffisamment significatifs pour déterminer un comportement normal de référence et détecter les anomalies ?
8. Votre produit est-il capable d'identifier chaque entité, chaque relation et chaque activité parmi les données d'API brutes de manière à les placer dans le contexte de l'entreprise ?
9. Votre produit peut-il tracer sur une chronologie chaque activité en fonction de chaque entité contenue dans vos API, de manière à représenter les changements de comportement au fil du temps ?
10. Comment puis-je intégrer votre produit à mes outils, processus et flux de travail existants ?
11. Est-il possible d'interroger les données d'API et d'activité de votre produit pour rechercher les menaces et atténuer les risques de manière proactive ?
12. Quelles mesures prenez-vous pour garantir la sécurité des données sensibles que vous recueillez sur mon entreprise ?
13. Votre solution fournit-elle un accès granulaire aux données d'activité des API ?

Comme vous l'avez sans doute déjà deviné, la solution API Security d'Akamai peut offrir efficacement toutes les protections recommandées dans cette liste. Découvrez notre solution.

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de sécurité, de calcul 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 12/23.