Akamai

LIVRE BLANC

10 capacités stratégiques de détection des API et d'intervention

Faites évoluer votre stratégie de sécurité des API

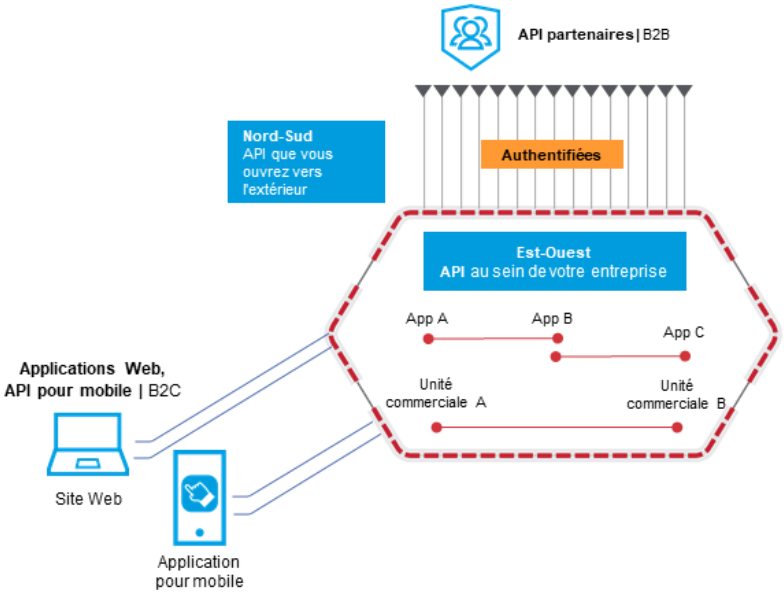
Introduction

Les API sont les éléments clés qui stimulent l'innovation, et les applications B2B et B2C sont au centre de cette transformation. Cela signifie qu'il est essentiel de protéger les communications critiques et souvent sensibles, en interne entre les microservices, et en externe entre les clients et les partenaires. La plupart des entreprises reconnaissent aujourd'hui qu'une stratégie de sécurité des applications solide est nécessaire pour réussir à long terme. Elles utilisent des technologies de sécurité telles que des plateformes de protection des applications Web et des API (WAAP), des fonctionnalités et des produits de sécurité dans le cloud et des outils de test de sécurité pour réduire les risques liés à la sécurité des applications. Il est important de connaitre la façon dont les attaques ont évolué pour contourner les WAAP et cibler les API au sein des organisations. Il est temps d'évoquer la façon d'ajuster votre stratégie de sécurité des API en prévision de ces menaces.

Où la détection et la réponse API s'intègrent-elles dans une stratégie de sécurité des API ?

Au cours des dernières années, les organisations ont créé beaucoup plus de canaux API que d'interfaces d'applications Web, et ces API incluent des volumes croissants de données métier et de logique métier. Les API ont changé les modes de fonctionnement des entreprises, car elles prennent en charge davantage de cas d'utilisation, accélèrent le changement, transportent des données plus sensibles et sont ouvertes à un plus grand nombre d'utilisateurs.

À quoi ressemble votre écosystème API ?



Bien que la plupart des catégories de produits de sécurité prennent en charge les API d'une manière ou d'une autre du fait de leur prévalence croissante, les API constituent une classe d'actifs différente et sont même présentées comme un actif différent dans certains cadres de conformité. Il ne suffit pas d'ajouter des capacités de protection contre les menaces API à un produit de sécurité hérité, tel qu'une plateforme WAAP, pour relever les nouveaux défis introduits par les actifs API. Les organisations de sécurité doivent traiter les API comme une classe d'actifs distincte et reconnaître les fonctionnalités critiques qui protègent entièrement les API à grande échelle.

Commençons par examiner fondamentalement la façon dont les protections API ont évolué pour faire face aux menaces émergentes. Autrefois, une organisation qui disposait d'un inventaire complet de ses API et d'une WAAP robuste pouvait généralement éviter les menaces liées aux API. Désormais, les attaques ciblent les API au sein des organisations et de leurs organisations partenaires de manière à contourner la WAAP.

Par exemple, certaines formes d'abus d'API proviennent de clients et de partenaires qui ont obtenu des informations d'identification d'API mais choisissent de les utiliser de manière non autorisée. Il existe également des moyens de pirater des informations d'identification d'API ou des jetons de sécurité apparemment légitimes. Les vulnérabilités cachées dans les implémentations de clients API constituent un autre vecteur d'attaque que les acteurs malveillants peuvent exploiter pour abuser des API de manière non détectable par les outils de sécurité traditionnels.

La bonne nouvelle est que les capacités essentielles nécessaires pour protéger les API des tendances émergentes, en particulier la détection et la réponse, sont déjà disponibles à grande échelle pour les organisations. Les pages suivantes examinent attentivement les capacités critiques qui rendent ces plateformes efficaces contre un écosystème des menaces sur les API en constante évolution.

Capacité critique n° 1
Protection indépendante de la plateforme

Les services API sont généralement mis en œuvre par différents groupes au sein d'une organisation, utilisant souvent un ensemble diversifié de plateformes et de technologies. Par exemple, certaines API peuvent être mises en place sur site tandis que d'autres peuvent être exécutées dans le cloud public. Des technologies intermédiaires peuvent également être utilisées, telles que les proxys inversés, les passerelles API, les pare-feux d'applications Web (WAF) et les réseaux de diffusion de contenu (CDN), qui créent de la complexité pour la visibilité des API.

Il est impératif de pouvoir accéder aux données d'activité API de chacune de ces différentes technologies. Une approche de protection contre les menaces des API indépendante de la plateforme garantit que votre organisation dispose toujours d'une image complète de toutes les activités des API, quels que soient les détails de mise en œuvre ou l'infrastructure utilisée. Cela fournira une couverture de protection pour :

- Tous les services, sociétés acquises et environnements
- Les API sanctionnées et « fantômes », qu'elles utilisent ou non la passerelle API
- Une visibilité étendue au-delà des API nord-sud, y compris les API est-ouest publiques, partenaires et internes

Veiller à ce que la visibilité de votre plateforme de protection contre les menaces liées aux API soit aussi vaste que possible protégera votre organisation contre les menaces internes et les abus d'API par les organisations partenaires, en plus des risques liés aux acteurs malveillants externes.

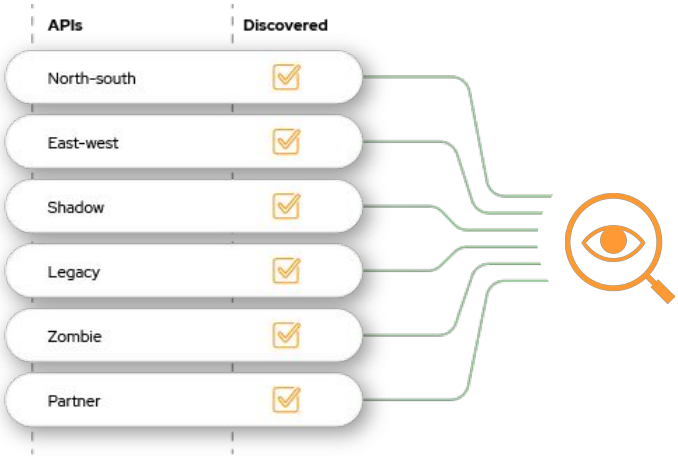
Capacité critique n° 2
Détection continue des API et gestion de la posture

Toute stratégie de sécurité des API repose sur un inventaire complet et continuellement mis à jour pour toutes les API utilisées dans l'organisation. Tout simplement parce qu'une organisation ne peut pas protéger quelque chose dont elle ignore la présence dans son environnement. De nombreux produits de sécurité des API prétendent assurer un certain niveau de découverte des API, mais sont limités à un fonctionnement à la demande ou journalier. Il est important de s'assurer que les capacités de détection des API de votre plateforme incluent :

- La détection automatisée et continue des API 24 heures sur 24, y compris la détection des API qui ne sont utilisées qu'une seule fois (la détection à la demande ou journalière est insuffisante)
- La détection de toutes les API à travers différentes technologies et infrastructures
- La détection des API nouvellement déployées et la comparaison avec des API bien documentées pour identifier les API « fantômes »
- L'évaluation des risques de chaque service API et point de terminaison
- La détection des vulnérabilités API connues, telles que celles décrites dans les 10 principaux risques pour la sécurité des API selon l'OWASP

Visibilité améliorée

Ne perdez plus jamais de vue votre inventaire API

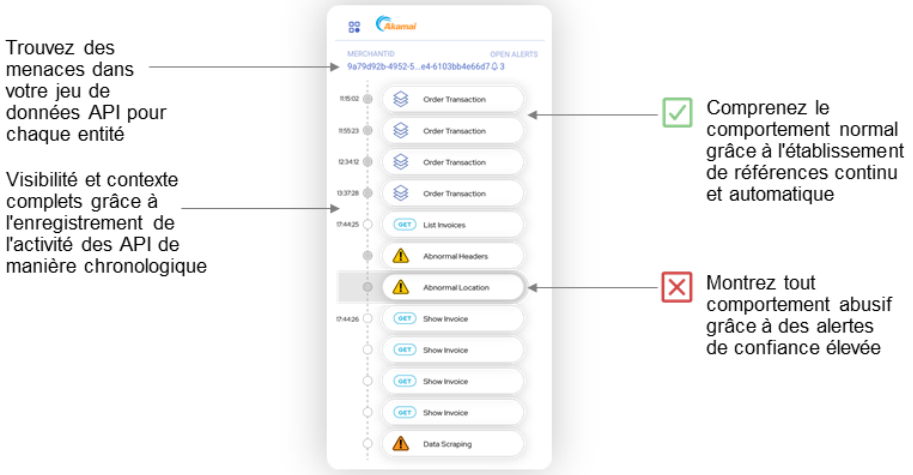


Capacité critique n° 3
Visualisation du comportement des API

La capacité à montrer et à visualiser le comportement réel des API (appels d'API) est une capacité fondamentale d'une plateforme de sécurité des API. Cette capacité est nécessaire pour permettre aux principales parties prenantes des services de sécurité, de développement et des opérations de visualiser et comprendre de quelle manière les API sont utilisées ou exploitées, afin qu'elles puissent communiquer entre elles et enquêter. Les fonctionnalités de visualisation spécifiques à rechercher sont les suivantes :

- **Enquête :** toute alerte doit inclure la possibilité d'inspecter l'activité de l'API d'origine, appel par appel, pour identifier le déclencheur spécifique de l'alerte.
- **Recherche des menaces :** les données historiques doivent couvrir une période continue d'au moins 30 jours et permettre de voir toutes les activités de l'API et de demander des intervalles de temps et des appels au-delà d'alertes spécifiques. Cette fonctionnalité contribue également à la conformité.
- **Fidélité et enrichissement des données :** pour chaque appel d'API, il devrait être possible de dire qui est l'utilisateur, quelle opération il a utilisée, à quels enregistrements il a accédé ou lesquels il a manipulés, quels en-têtes et paramètres ont été utilisés, etc.
- **Confidentialité des données :** bien que la fidélité des données soit importante, les données sensibles ne peuvent pas être stockées au repos. La segmentation en unités est nécessaire pour préserver la richesse des données sans stocker de données sensibles.
- **Visualisation de la chronologie :** les utilisateurs doivent disposer d'une vue qui leur permet d'avancer ou reculer facilement dans les séquences d'activité.

Détectez les menaces à l'aide de l'analyse comportementale



Capacité critique n° 4
Suivi de plusieurs entités utilisateur

Comprendre l'entité et être capable de voir l'activité des API associée offre un contexte pour toute utilisation ou exploitation ; il est donc essentiel que votre plateforme de protection des API soit suffisamment sophistiquée pour suivre chacune de ces entités individuellement. Cela fournit un contexte essentiel, puisqu'une activité normale pour une catégorie d'utilisateurs peut être un signe d'abus pour un autre utilisateur. La possibilité de visualiser l'activité de chaque entité sur une frise chronologique fournit une visibilité indispensable et une compréhension du contexte. Par exemple :

Activité des API	Participants	Entités	Entités de processus métier
Exemples	Utilisateurs internes, partenaires B2B, utilisateurs externes	Adresse IP, jeton API, ID de commerçant, ID de session, ID de locataire	ID de paiement, ID de facture

Capacité critique n° 5
B2B et couverture API est-ouest

Le domaine de croissance le plus important dans l'utilisation des API se trouve dans les cas d'utilisation B2B, à la fois internes et externes. La sécurité des API doit couvrir les API B2B et machine à machine, y compris les instances nord-sud (orientées vers l'extérieur) et est-ouest (orientées vers l'intérieur).

Bien que les applications Web B2C bénéficient d'une protection de la part des plateformes WAAP et WAF, certains des types d'activité API les plus sensibles, tels que les API internes est-ouest ou les fonctionnalités d'applications propriétaires exposées aux partenaires via des API B2B, peuvent encore être compromis même lorsqu'ils traversent la WAAP.

Souvent, une fois qu'un utilisateur est authentifié sur une API d'un partenaire B2B, il est considéré comme sûr et aucune surveillance supplémentaire n'est effectuée. Cela crée une lacune critique dans la posture de sécurité des API de nombreuses organisations. Pour fournir une image complète de l'activité des API et de l'écosystème des menaces plus vaste, les organisations doivent utiliser une approche qui offre une visibilité, une observabilité et une surveillance efficaces pour tous les cas d'utilisation.

Capacité critique n° 6
Analyse comportementale et détection

La détection de menaces API sophistiquées n'est pas possible en analysant les appels API individuels, ni même les sessions individuelles. La détection et la réponse des API nécessitent une compréhension approfondie et un apprentissage à partir de contextes comportementaux. Pour savoir si le comportement d'une API est anormal, ce qui indique qu'elle pourrait être compromise, il est nécessaire d'analyser son utilisation sur des périodes plus longues. La technique de l'analyse comportementale détermine un comportement normal de base de l'utilisateur et surveille en permanence ce comportement afin de détecter les anomalies.

Les ressources de stockage et de calcul requises pour ce niveau d'analyse pour l'activité des API d'une entreprise typique complexifient l'utilisation d'outils de sécurité des API sur site à contrainte d'échelle. Les solutions EDR et XDR ont ouvert la voie en montrant qu'une architecture reposant sur le logiciel en tant que service (SaaS) était nécessaire pour effectuer des analyses comportementales pertinentes. La puissance et l'échelle du cloud permettent le stockage des données au fil du temps, tout en permettant une analyse qui détermine le comportement normal de l'utilisateur au fil du temps, afin de détecter l'aiguille dans la botte de foin qui révèle les abus. Une approche SaaS présente d'autres avantages, tels qu'une mise en œuvre plus rapide et plus simple, ainsi qu'une évolutivité et une élasticité améliorées à mesure que votre utilisation des API augmente.

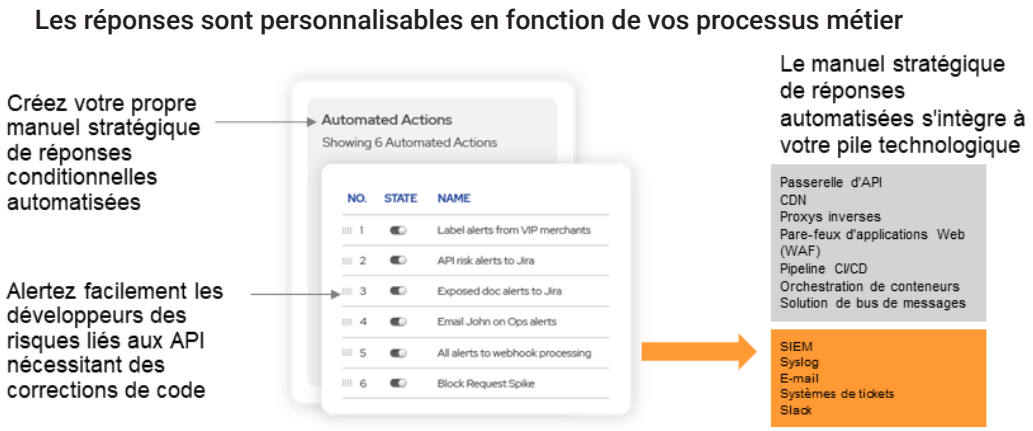
Capacité critique n° 7
Alertes pertinentes en contexte

Une fois qu'une organisation dispose d'une visibilité sur toutes les activités des API et les analyses comportementales à grande échelle, les alertes sur l'activité des API prennent tout leur sens. Les entreprises ont alors éliminé la nécessité d'anticiper toutes les méthodes d'attaque possibles en rendant l'approche de surveillance de la sécurité plus abstraite. Établir une base de référence des comportements normaux et détecter les anomalies permet également de détecter les abus d'API, qui ne peuvent souvent être détectés par le biais d'aucun schéma ou signature. De plus, être capable de rembobiner l'attaque et de voir ce qui s'est passé avant une alerte fournit des informations précieuses sur l'utilisation et l'exploitation d'un domaine d'API.

Capacité critique n° 8
Réponses personnalisées et automatisées

Les approches API traditionnelles en ligne peuvent prendre des mesures automatisées pour bloquer les potentielles attaques d'API, à cela près que les organisations doivent être en mesure d'identifier les attaques. L'analyse comportementale et la détection d'anomalies sur les API sont effectuées au fil du temps, avec un contexte métier beaucoup plus important ; la profondeur de la détection permet donc aux anomalies de faire surface. Cela permet un vaste éventail de réponses automatisées et personnalisées pouvant être fournies avec une grande précision. Quelques exemples :

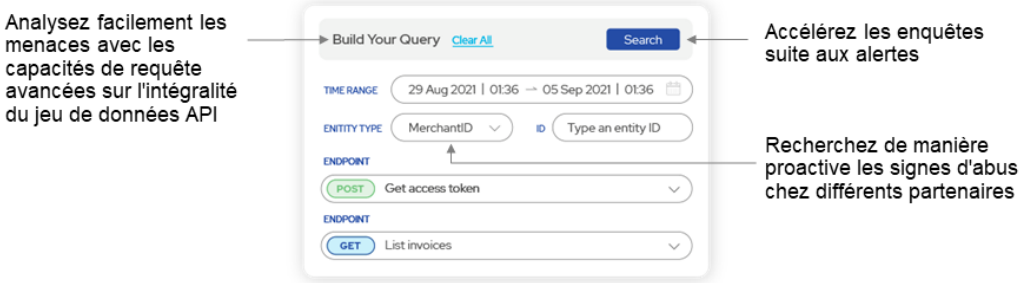
- Blocage ou limitation du trafic au niveau des passerelles d'API et des filtres CDN en bordure de l'Internet pris en charge
- Notifications par e-mail pour les décisionnaires en matière de sécurité et les parties prenantes de l'entreprise
- Création de tickets pour les développeurs
- Déclenchement de webhooks



Capacité critique n° 9
Enquêtes proactives et recherche des menaces

De nombreuses organisations ne peuvent pas se permettre d'attendre qu'un incident de sécurité actif se produise avant d'agir. Une approche plus efficace consiste à identifier les situations indésirables et à les rechercher activement. Par exemple, une alerte qui a détecté un abus sur une API peut être identifiée en exécutant le même comportement sur une autre API via une recherche proactive des menaces. Par conséquent, une plateforme de protection contre les menaces sur les API doit inclure la capacité de rechercher des types de comportement spécifiques au-delà des alertes générées en réponse à des incidents actifs. Les capacités de recherche de menaces nécessitent l'accès aux données historiques pour trouver l'abus caché dans les données d'activité des API. Les solutions à requête unique qui n'enrichissent pas les données en fournissant du contexte ne sont pas en mesure de raconter une histoire cohérente. La recherche de menaces et les enquêtes reposent sur les bases de données historiques.

Le pouvoir d'enquêter et de rechercher les menaces à portée de main



Capacité critique n° 10
Lac de données observable

Parmi toutes les fonctionnalités pour une stratégie de sécurité des API robuste, le contexte est essentiel pour protéger toute API sur une longue période. La meilleure façon de maintenir un contexte suffisant pour observer les menaces, identifier les vulnérabilités potentielles et dépanner en cas d'attaque consiste à consigner tous les comportements des API et à conserver un backlog de cette activité. Ceci peut être accompli en associant un lac de données à la solution de sécurité des API. Recherchez un lac de données qui fournit la plus grande quantité de détails historiques pour éclairer votre stratégie. Bien que l'apport de données de requête de base aux modèles d'apprentissage automatique puisse être utile, disposer de détails tels que les paramètres de requête permet aux organisations d'agir réellement sur leurs données historiques de manière à les protéger contre les menaces et attaques futures.

N° 1 Protection indépendante de la plateforme	Veiller à ce que la visibilité de votre plateforme de protection contre les menaces sur les API soit aussi vaste que possible protégera votre organisation contre les menaces et les abus.
N° 2 Découverte continue des API et gestion de la posture	Un inventaire complet et continuellement mis à jour de toutes les API utilisées dans l'organisation est fondamental car les organisations ne peuvent pas protéger quelque chose dont elles ignorent la présence dans leur environnement.
N° 3 Visualisation du comportement des API	La visibilité est nécessaire pour que les principales parties prenantes des équipes de sécurité, de développement et des opérations puissent voir et comprendre comment les API sont utilisées ou exploitées, et puissent communiquer entre elles et enquêter.
N° 4 Suivi de plusieurs entités utilisateur	Comprendre l'entité et pouvoir voir l'activité API associée offrent un contexte pour toute utilisation ou exploitation ; il est donc essentiel que votre plateforme de protection des API soit suffisamment sophistiquée pour suivre chaque entité individuellement.
N° 5 B2B et couverture API est-ouest	Pour fournir une image complète de l'activité des API et de l'écosystème des menaces plus vaste, les organisations doivent utiliser une approche qui offre une visibilité, une observabilité et une surveillance efficaces pour tous les cas d'utilisation.
N° 6 Analyse comportementale et détection	Pour savoir si le comportement d'une API est anormal, ce qui indique qu'elle pourrait être compromise, il est nécessaire d'analyser son utilisation sur des périodes plus longues. La technique de l'analyse comportementale détermine un comportement normal de base de l'utilisateur et surveille en permanence ce comportement afin de détecter les anomalies.
N° 7 Alertes pertinentes en contexte	Une fois qu'une organisation dispose d'une visibilité sur toutes les activités des API et les analyses comportementales à grande échelle, les alertes sur l'activité des API prennent tout leur sens. Les entreprises ont alors éliminé la nécessité d'anticiper toutes les méthodes d'attaque possibles en rendant l'approche de surveillance de la sécurité plus abstraite.

N° 8 Réponses personnalisées et automatisées	L'analyse comportementale et la détection d'anomalies sur les API sont effectuées au fil du temps, avec un contexte métier beaucoup plus important ; la profondeur de la détection permet donc aux anomalies de faire surface. Cela permet un vaste éventail de réponses automatisées et personnalisées pouvant être fournies avec une grande précision.
N° 9 Enquêtes contextuelles et détection des menaces	De nombreuses organisations ne peuvent pas se permettre d'attendre qu'un incident de sécurité actif se produise avant d'agir. Une approche plus efficace consiste à identifier les situations indésirables et à les rechercher activement.
N° 10 Lac de données observables	La meilleure façon de maintenir un contexte suffisant pour observer les menaces, identifier les vulnérabilités potentielles et dépanner en cas d'attaque consiste à consigner tous les comportements des API et à conserver un backlog de cette activité. Cela peut être accompli en associant un lac de données à votre plateforme de sécurité des API.

Si vous avez trouvé ces informations utiles, l'étape suivante consiste à explorer la solution API Security d'Akamai pour vous assurer de disposer de la stratégie de sécurité des API la plus robuste possible.

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 Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 12/23.