LIVRE BLANC

Détection des anomalies avec Akamai API Security

Les API constituent un élément clé de la capacité de votre entreprise à servir ses clients, générer des revenus et fonctionner efficacement. Cependant, leur croissance continue, leur proximité avec les données sensibles et l'absence de contrôles de sécurité en font une cible attrayante pour les pirates d'aujourd'hui. Il est essentiel d'obtenir une visibilité en temps réel sur le comportement des utilisateurs pour identifier de manière proactive les signes d'abus potentiels d'API ou d'une attaque.

L'objectif des fonctionnalités de détection des anomalies de la solution Akamai API Security est d'identifier les comportements anormaux des utilisateurs qui indiquent des tentatives potentiellement malveillantes d'exploitation des API de l'entreprise. En établissant un trafic normal de référence, les fonctionnalités de détection des anomalies d'Akamai peuvent comparer les requêtes entrantes à cette référence et déterminer si elles sont susceptibles d'être menées par un attaquant.

Notre algorithme de détection des anomalies identifie les comportements anormaux, tels que les suivants :

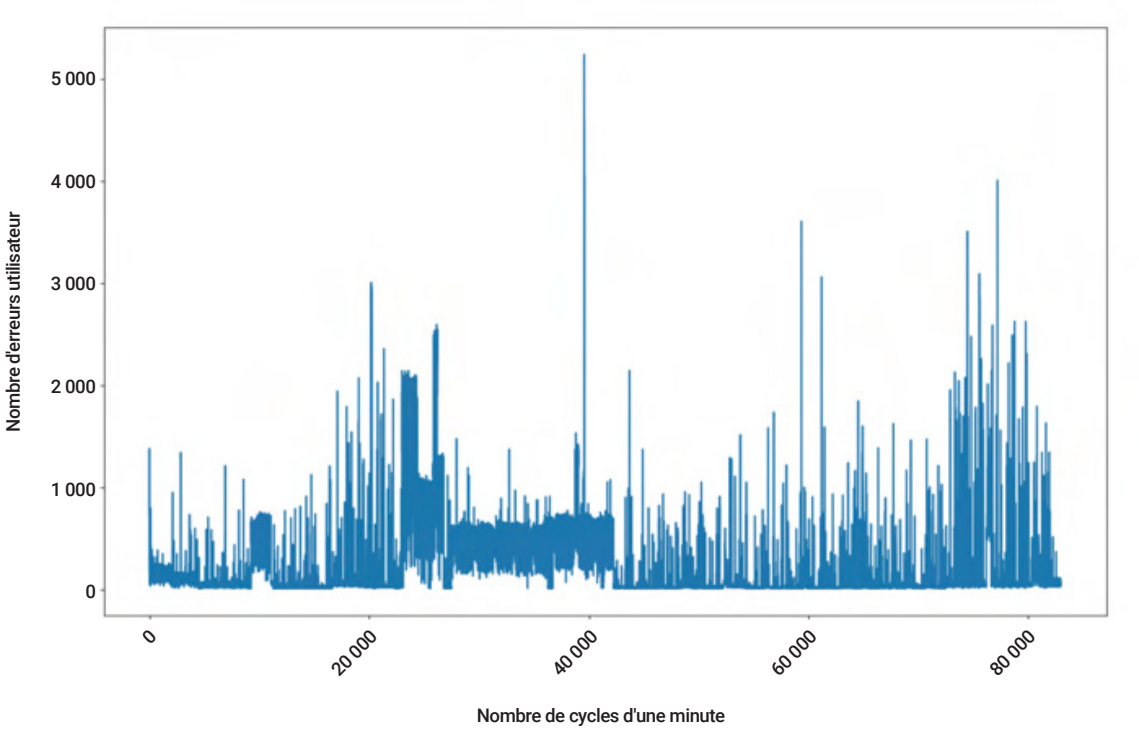
- Utilisation d'un champ inattendu dans la requête d'API
- Extraction de plus de données du serveur qu'un utilisateur normal
- Tentative d'utilisation d'autres ressources utilisateur/administrateur
- Appel des API dans un ordre inattendu

L'algorithme est basé sur un modèle d'intelligence artificielle (en apprentissage en ligne non supervisé) et d'apprentissage automatique (IA/ML) qui apprend les nombreuses caractéristiques du comportement statistique du trafic et détecte les incidents anormaux après une période d'apprentissage fixe. Notre modèle s'adapte aux changements du trafic au fil du temps et aux anomalies identifiées comme faux positifs par les utilisateurs.

Pendant la phase d'apprentissage, notre système analyse les données du client et identifie les différentes API, les méthodes d'authentification, les utilisateurs, les types de données, etc. Comme pour chaque API, le modèle développe une liste des fonctionnalités du trafic utilisateur normal, y compris le nombre d'accès aux API, le nombre d'erreurs générées, le pourcentage de demandes authentifiées, la quantité de données extraites du serveur, etc. Notre algorithme détecte les anomalies d'utilisateur en comparant les caractéristiques de l'utilisateur et de l'API avec les résultats attendus par le modèle statistique que notre algorithme a appris.

Fonctionnement de la détection des anomalies d'Akamai API Security

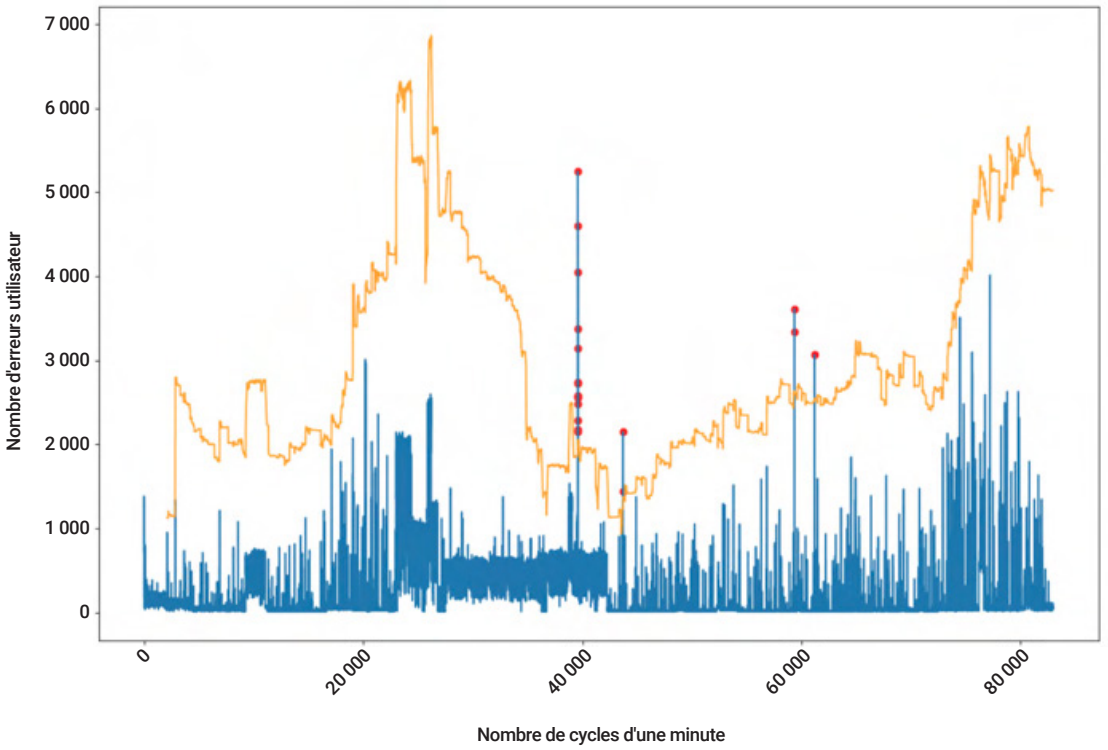
Les fonctionnalités de détection des anomalies d'Akamai API Security identifient les utilisateurs qui génèrent un nombre d'erreurs excessif par rapport aux autres utilisateurs. Cela nous permet d'identifier les attaques comme celles en force, l'analyse de chemin et l'extraction. Le graphique suivant indique le nombre maximal d'erreurs générées par un utilisateur lors de chaque cycle d'une minute dans un environnement.



Dans ce scénario, l'identification des anomalies présente plusieurs défis :

1. Le modèle doit tenir compte de la dérive des données lors du calcul du seuil.
2. L'objectif consiste à éviter les anomalies d'apprentissage pendant la période d'apprentissage du modèle.
3. L'apprentissage est effectué en flux continu, ce qui signifie que le modèle ne voit jamais l'ensemble des données et qu'il s'adapte à chaque étape.
4. Les alertes doivent être émises en temps réel. Par conséquent, notre algorithme ne peut pas se fier aux données futures pour prédire une anomalie.
5. Pour éviter de spammer l'utilisateur, notre modèle doit apprendre un seuil statistiquement garanti sur les données.

Dans le graphique ci-dessous, nous pouvons voir comment notre modèle répond à ces exigences en ajustant les seuils en fonction des données entrantes.



La ligne orange représente la fonction de seuil calculée par le modèle, et les points rouges indiquent les anomalies détectées sur la base de cette fonction.

Foire aux questions

Quelle est la période d'apprentissage nécessaire pour l'algorithme de détection des anomalies d'Akamai ?

La plupart de nos algorithmes nécessitent une période d'apprentissage de deux à sept jours. En outre, le nombre de comportements utilisateur observés a des conséquences sur la période d'apprentissage de l'algorithme.

Lorsqu'un comportement anormal est détecté, combien de temps faut-il pour que l'alerte soit générée ?

Dans la plupart des cas, notre algorithme créera une alerte pertinente pour le client dans un délai de 30 à 60 secondes à partir du moment où il reçoit le trafic anormal.

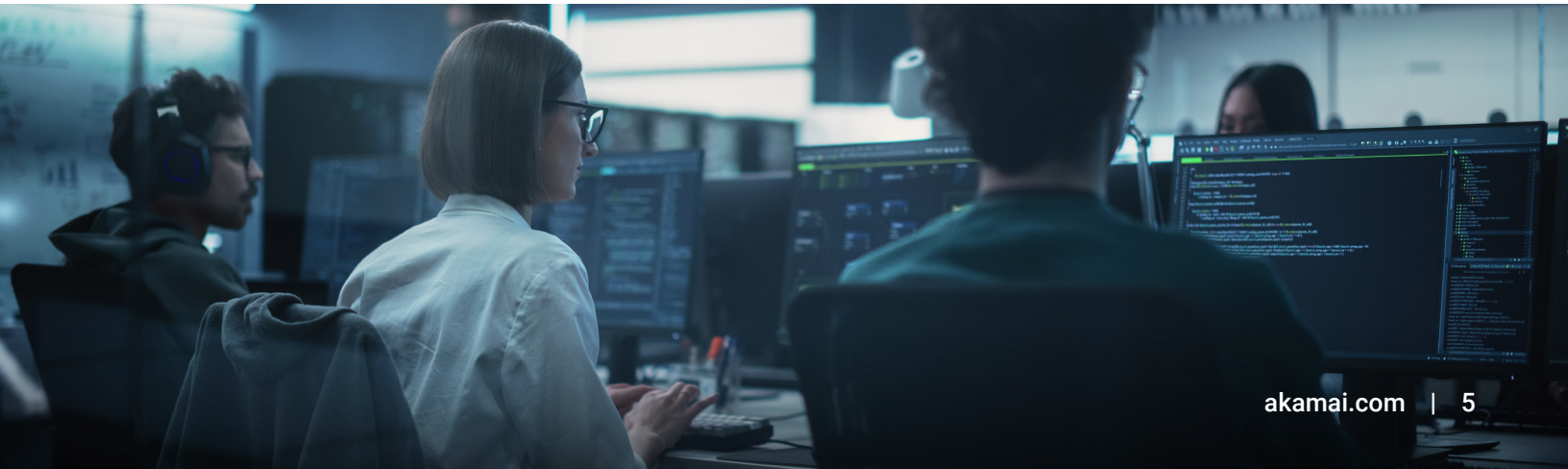
L'algorithme utilise-t-il un modèle supervisé ou non supervisé ?

Notre algorithme repose sur un modèle non supervisé, qui lui permet de s'adapter à l'environnement de chaque client sans avoir de connaissances préalables sur ses caractéristiques. En outre, notre algorithme utilise l'apprentissage en ligne pour s'adapter aux changements de l'environnement au fil du temps.

Quels sont les différents types d'anomalies détectées par Akamai API Security ?

Akamai API Security détecte deux types d'anomalies :

- Basées sur des modèles : anomalies reposant sur l'identification de modèles malveillants dans le trafic, tels que les techniques d'exploitation Web et les agents utilisateurs malveillants connus, comme l'injection de commandes et la traversée de chemins, ainsi que les agents utilisateurs suspects.
- Basées sur le comportement : anomalies reposant sur le comportement d'apprentissage des utilisateurs et sur l'identification des utilisateurs anormaux, tels qu'une utilisation excessive de l'API, une violation de plage et une autorisation brisée au niveau de l'objet.



Quels sont les paramètres pris en compte par Akamai API Security lors du déclenchement d'une anomalie ?

Nos algorithmes reposent sur plusieurs fonctionnalités conçues en effectuant une analyse statistique du trafic, comme les éléments suivants :

- Nombre d'utilisateurs différents qui utilisent une API
- État d'authentification de l'API
- Code de réponse du serveur
- Quantité de données extraites par l'utilisateur
- Géolocalisation IP de l'utilisateur
- Agent utilisateur de l'utilisateur, etc.

L'utilisateur peut-il contrôler la sensibilité de l'algorithme ?

Oui, l'utilisateur peut contrôler la sensibilité de chaque anomalie en modifiant la sensibilité de la règle appropriée. La sensibilité de la règle est un nombre compris entre 1 (faible) et 5 (élevée) ; plus la valeur est élevée, plus le système est configuré de manière sensible pour chaque règle d'anomalie dans Akamai API Security. Notre algorithme prend ce paramètre en compte dans le modèle.

L'utilisateur peut-il marquer un problème signalé par Akamai comme un faux positif, et quelles répercussions cela a-t-il sur l'algorithme ?

Oui, pour améliorer notre détection des anomalies, nos utilisateurs peuvent marquer les problèmes comme étant des « faux positifs ». Lorsqu'un problème est marqué comme étant un faux positif, notre algorithme le prend en compte et ajuste le modèle en fonction des informations fournies par l'utilisateur.

Comment est-ce qu'Akamai évite de « spammer » le client avec un utilisateur qui continue d'envoyer le même scénario d'attaque ?

Notre algorithme identifiera les problèmes similaires qui continuent d'être déclenchés par le même utilisateur et sur la même API. Dans ce cas, notre algorithme ignorera les problèmes similaires pendant une période indéfinie.

Comment est-ce qu'Akamai gère la dérive/saisonnalité des données ?

Akamai API Security utilise plusieurs algorithmes différents pour détecter les anomalies dans les données. En fonction du prétraitement des données sous-jacentes et de la complexité de l'algorithme, nous pouvons assouplir l'ajustement du seuil ou appliquer des ajustements à chaque cycle où nous avons besoin de seuils statistiques garantis pour la détection des anomalies. En conjonction avec le contrôle des spams, nous offrons une interface simple, même lorsqu'un algorithme spécifique nécessite des cycles supplémentaires pour ajuster les seuils.

Comment est-ce qu'Akamai gère l'empoisonnement des données ?

En tant qu'algorithme d'apprentissage en ligne, la solution Akamai API Security doit relever de nombreux défis, tels que les suivants :

- Nouvelles API
- Nouveau(x) champ(s) dans les API existantes
- Modification du type/de la plage de valeurs dans un champ
- Problèmes de disponibilité du serveur
- Les bogues dans les API susceptibles de générer des erreurs (404, 500, etc.) et d'autres difficultés pour déterminer les éléments à apprendre ou non (Akamai fait attention à ne pas apprendre ces anomalies en exigeant un minimum de nombre d'utilisateurs, de durée et de persistance nécessaires pour déclencher l'apprentissage)

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 : 12/24.