Partenariat pour un Internet plus sûr le rôle des API

Pour protéger les utilisateurs et les diverses organisations des acteurs malveillants, nous développons et partageons des interfaces de programmation d'applications (API) qui détectent et bloquent les menaces en ligne et contribuent à rendre Internet plus sûr pour tous.

CRÉER

Nous créons des API de sécurité pour protéger les utilisateurs dans trois domaines clés. En voici quelques exemples :

Sécurité des enfants

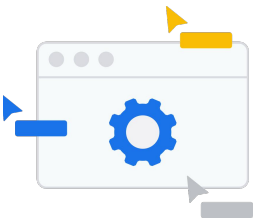
- API Content Safety
- API CSAI Match
- API Hash Matching

Sécurité

- API Safe Browsing
- API Project Shield
- API VirusTotal

Qualité des informations

- API Perspective
- API Vision
- API FactCheck
- API Civics Information
- Text Moderation



DÉPLOYER À GRANDE ÉCHELLE

Pour étendre notre impact, nous partageons nos API de sécurité avec nos partenaires :

46 millions

En 2022, l'API Cloud Armor a bloqué l'une des plus grosses attaques DDOS de couche 7 de l'histoire, qui atteignait 46 millions de requêtes par seconde.

2 milliards

Chaque jour, l'API Perspective est appelée presque 2 milliards de fois, par plus de 1 000 partenaires.

4 milliards

Le kit pour la sécurité des enfants (API Content Safety + API CSAI Match) a traité plus de 4 milliards d'images et de vidéos au cours des 30 derniers jours.

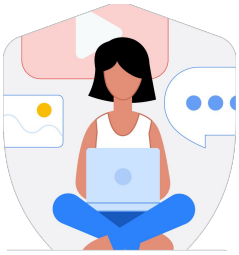
LIMITER

Pour nous assurer que seuls nos partenaires de confiance ont accès à nos API et que celles-ci sont utilisées de façon conforme et sûre, nous avons mis en place une procédure en trois étapes cruciales :

Sélectionner — Limiter — Appliquer

Nous limitons l'accès à nos API de sécurité à certains partenaires soigneusement sélectionnés, nous restreignons l'utilisation non autorisée de ces outils et nous appliquons nos conditions d'utilisation de manière stricte. En mettant à la disposition de nos partenaires de confiance nos API de sécurité nous pouvons œuvrer ensemble à la création d'un Internet plus sûr pour tous.

API de sécurité de Google



API pour la sécurité des enfants

Kit pour la sécurité des enfants

Content Safety

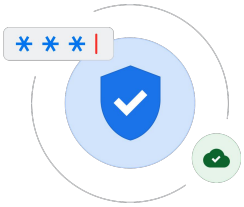
Notre modèle propriétaire aide nos partenaires à classer et à hiérarchiser des milliards de contenus d'abus sexuels sur mineurs. Il utilise des classificateurs de machine learning pour identifier ces contenus afin que ceux-ci soient examinés, supprimés et signalés rapidement.

CSAI Match

La technologie propriétaire de YouTube, la première à utiliser les correspondances de hachage, identifie les vidéos d'abus sexuels sur mineurs et les signale systématiquement à nos partenaires afin qu'ils les examinent, confirment qu'elles enfreignent nos règles, les signalent et prennent les mesures adéquates.

Hash Matching

Nous fournissons notre API Hash Matching au NCMEC pour l'aider à hiérarchiser et à examiner plus efficacement les rapports CyberTipline, afin que ses équipes puissent traiter au plus tôt ceux qui concernent des enfants ayant besoin d'une aide urgente.



API de sécurité

Solution WAAP de Google

Cloud Armor

Protège les sites Web, les services et les API contre les attaques de déni de service distribué (DDoS) sophistiquées, automatisées et ciblées, qui visent à censurer les informations.

reCAPTCHA

Protège les sites Web contre les activités frauduleuses, le spam et autres utilisations abusives. reCAPTCHA Enterprise utilise un moteur d'analyse des risques adaptatif pour empêcher les logiciels automatisés d'agir de manière abusive.

Apigee

La plate-forme Google Cloud de gestion du cycle de vie complet des API permet aux entreprises de concevoir, de sécuriser, d'implémenter, de surveiller et de déployer à grande échelle des API.

Safe Browsing

Notre API Safe Browsing permet aux applications clientes de comparer des URL aux listes de ressources Web non sécurisées que nous mettons constamment à jour. Cet outil protège chaque jour cinq milliards d'appareils en mettant les utilisateurs en garde contre des sites hébergeant des logiciels malveillants ou indésirables.

VirusTotal

Permet aux développeurs d'envoyer des fichiers ou des URL pour analyse et de recevoir un rapport d'infection par des logiciels malveillants.

API liées à la qualité des informations

Perspective

API Open Source qui utilise le machine learning pour identifier les commentaires "toxiques". Elle sert non seulement à faciliter les interactions entre utilisateurs, mais aussi à promouvoir des interactions humaines de qualité à l'aide de grands modèles de langage et de l'IA générative.

Vision

Permet aux développeurs d'intégrer facilement des fonctionnalités de détection dans leurs applications, comme l'étiquetage d'images, la détection de visages et de points de repère, la reconnaissance optique des caractères (OCR), et l'ajout de tags au contenu explicite.

FactCheck

Vise à aider les fact-checkers, les journalistes et les chercheurs à découvrir les informations qui ont été réfutées ou non à travers le monde. Grâce à cet outil, les utilisateurs peuvent rechercher des affirmations dans une base de données de plus de 300 000 informations vérifiées par des éditeurs réputés.

Civic Information

L'API Civic Information aide les développeurs à créer des applications qui permettent aux citoyens et électeurs américains d'en savoir plus sur leur représentation politique, d'accéder à des informations électorales et de connaître l'emplacement des bureaux de vote. Lors des élections prises en charge par l'API, les électeurs peuvent rechercher leur bureau de vote, les sites de vote anticipé et de dépôt des bulletins, ainsi que des informations sur les différents candidats.

Text Moderation

L'outil Text Moderation de Google, disponible par le biais de l'API Cloud Natural Language, aide les organisations à détecter les contenus sensibles et nuisibles. Il est capable d'identifier une grande variété de contenus nuisibles, y compris l'incitation à la haine, l'intimidation et le harcèlement sexuel.

Vous protéger toujours mieux au quotidien avec Google

Nous investissons dans la création et le partage d'API qui détectent et bloquent les menaces en ligne, afin de garantir que **Google vous offre chaque jour une plus grande sécurité**. Visitez notre Centre de sécurité pour en savoir plus sur la manière dont nous offrons une sécurité en ligne à plus de personnes que n'importe quel autre acteur du marché.