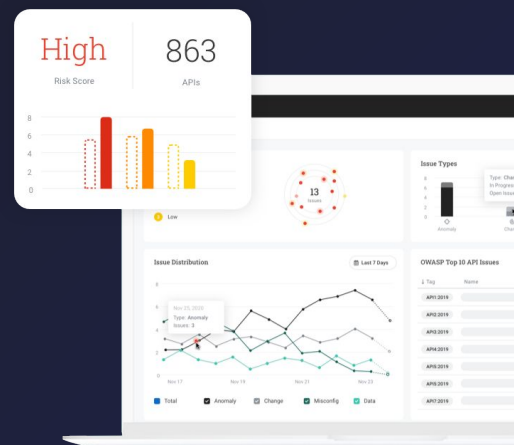


La plateforme de sécurité API des entreprises



Gestion de la posture de sécurité des API, détection des APIs et réponse, sécurisation du cycle complet de développement des APIs... Noname Security agit sur tous les fronts pour s'imposer comme l'un des principaux leaders du marché.

Qui dit transformation digitale dit transformation des APIs

Les APIs constituent l'un des piliers de l'univers du numérique. Agiles, rapides et portables, elles permettent aux développeurs d'assurer une parfaite interopérabilité entre leurs applications et différentes sources de données, créant ainsi un maximum de valeur. C'est pourquoi on les retrouve au cœur des grands chantiers de transformation digitale en cours dans de nombreux domaines :

- Services de cloud public
- Conception d'applications à base de microservices
- Open Banking
- Applications médicales mobiles
- Nouveaux écosystèmes d'entreprises et de développeurs
- Digitalisation du back-office
- Options complémentaires au REST – GraphQL, gRPC et webhooks



Posture de sécurité des APIs

Inventoriez chaque API, y compris les APIs anciennes et non répertoriées, avec **classification des données**.

Identifiez les **erreurs de configuration** et les **vulnérabilités** dans le code source, la configuration réseau et les politiques.



Détection et réponse

Détectez les menaces pesant sur l'environnement d'exécution (runtime) des API à l'aide de modèles d'analyse comportementale.

Bloquez et neutralisez les menaces de façon automatique et semi-automatique.

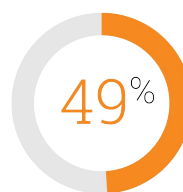


Sécurisation du code des APIs

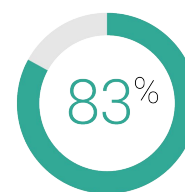
Testez continuellement vos APIs pour identifier les risques en amont.

Optez pour une approche automatisée et dynamique du développement de tests et de leur incorporation dans les pipelines CI/CD.

La croissance exponentielle des APIs va se poursuivre en 2022



Le volume d'appels API a augmenté de 49% en 2020



du trafic web provenait d'APIs en 2019

Revers de la médaille, cet engouement pour les APIs s'est récemment accompagné d'une explosion des incidents de sécurité relatifs aux APIs. Selon Gartner, en 2022, les APIs représenteront le premier vecteur d'attaque contre les applications web. IBM, pour sa part, estime que deux tiers des compromissions du cloud proviennent déjà d'erreurs de configuration des APIs.

C'est pourquoi Noname Security protège les APIs en temps réel et détecte les vulnérabilités et les erreurs de configuration avant que des hackers ne les exploitent. La Noname API Security Platform est une solution hors bande qui s'intègre à vos passerelles API, équilibreurs de charge et pare-feux applicatifs web (WAF) pour plus de visibilité et de sécurité.

La sécurité des APIs selon Noname



Découverte de l'intégralité des APIs, données et métadonnées

Trouvez et inventoriez chaque type d'API (HTTP, RESTful, GraphQL, SOAP, XML-RPC, gRPC, etc.). Identifiez les APIs anciennes ou non autorisées qui ne sont pas gérées par une passerelle API, puis cataloguez leurs attributs et métadonnées.



Analyse comportementale des API et détection des menaces

Faites appel à l'IA pour détecter automatiquement un très large éventail de vulnérabilités API, allant des fuites et altérations de données jusqu'aux attaques, en passant par les erreurs de configuration, les violations de politiques de données et les comportements suspects.



Prévention des attaques et remédiation des vulnérabilités API

Prévenez les attaques en temps réel, corrigez les erreurs de configuration, actualisez automatiquement les règles de pare-feu, paramétrez des webhooks sur vos WAF pour créer de nouvelles politiques contre les comportements suspects, puis intégrez le tout aux workflows existants (gestion des tickets de support, SIEM, etc.).



Tests systématiques des APIs avant leur mise en production

Si la plupart des applications sont rigoureusement testées avant d'être déployées en production, la majorité des APIs ne le sont pas. D'où l'importance d'inclure les tests d'API au cycle de développement logiciel pour identifier les problèmes avant l'envoi en production.



À propos de Noname Security

Noname Security a conçu l'une des plateformes de sécurité des APIs les plus puissantes, complètes et ergonomiques du marché. Sa mission ? Aider les entreprises à détecter, analyser, remédier et tester toutes les APIs, d'ancienne ou de nouvelle génération. De grands groupes internationaux font confiance à la Noname API Security Platform pour protéger leurs environnements API contre les attaques, les vulnérabilités et les erreurs de configuration. Noname est une entreprise à capitaux privés basée à Palo Alto en Californie, avec une filiale à Tel-Aviv (Israël) et Amsterdam.

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371