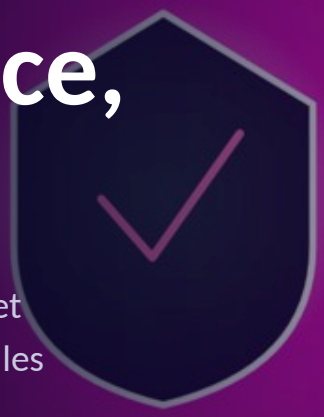
Q-FEEDS

LIVRE BLANC · À PROPOS DE Q-FEEDS

La threat intelligence, à la portée de tous



Qui nous sommes, pourquoi nous avons créé Q-Feeds et comment nous sélectionnons des renseignements que les organisations de toute taille peuvent exploiter.

qfeeds.com
Version 2026

MADE IN EUROPE

01

Qui nous sommes

Q-Feeds est une entreprise européenne de cyber threat intelligence basée à Hilversum, aux Pays-Bas. Nous réunissons les renseignements de plus de 2 500 sources en un ensemble fiable, que nous livrons aux pare-feu, aux SIEM, aux filtres DNS et aux équipes de sécurité du monde entier.

Fondé en 2024, Q-Feeds s'adresse aux fournisseurs de services managés, aux revendeurs et aux équipes de sécurité internes qui veulent des renseignements fiables et directement exploitables, sans tarifs réservés aux grands comptes ni longs projets d'intégration. Notre plateforme va des flux de listes de blocage pour un seul pare-feu aux collections TAXII pour les plateformes de threat intelligence, et comprend aussi la surveillance du dark web, l'analyse de la surface d'attaque, les alertes CVE et la protection de marque.

2 500+	20 min	20+	2024
sources de renseignement	intervalle de mise à jour avec Premium	intégrations prises en charge	création aux Pays-Bas

02

Notre mission

La threat intelligence doit être accessible à tous.

Les entreprises de cybersécurité sont avant tout des entreprises de traitement de données : pour bloquer quelque chose, il faut d'abord savoir quoi bloquer. Pendant des années, la threat intelligence de qualité est restée réservée aux grandes entreprises dotées d'équipes de sécurité dédiées et des budgets qui vont avec.

Dans le même temps, les attaquants visent de plus en plus les petites structures, précisément parce qu'elles sont moins bien protégées. Les entreprises de moins de 500 salariés subissent les mêmes attaques automatisées que les multinationales, mais le marché les sert très mal. Q-Feeds existe pour combler cet écart : une threat intelligence premium, à un prix juste et simple à mettre en place.

Qualité sélectionnée

Chaque jeu de données passe par des contrôles qualité, une notation de priorité et une validation des faux positifs avant sa publication.

Accessible

Des tarifs justes, une édition Community gratuite et des intégrations qui se font en quelques minutes : chaque organisation peut ainsi renforcer sa sécurité.

Européen

Conçu aux Pays-Bas et aligné sur les normes européennes et les attentes en matière de confidentialité, au service de clients du monde entier.

03

Ce que nous faisons

D'abord simple flux de threat intelligence, Q-Feeds est devenu une plateforme de gestion de l'exposition aux menaces. Tout est accessible depuis un seul endroit : le Q-Feeds Threat Intelligence Portal.

Fonctionnalité	Description
Flux de threat intelligence	Flux sélectionnés d'IP, de domaines et d'URL malveillants, prêts pour les pare-feu, les SIEM, les filtres DNS et les proxys.
Threat Lookup	Analysez n'importe quelle IP, n'importe quel domaine, URL ou hash de fichier, avec un score de malveillance, les sources qui l'ont signalé et le mappage MITRE ATT&CK.
API IOC Lookup et TAXII 2.1	Accès programmatique pour le SOAR, le ticketing et vos outils sur mesure, et collections STIX 2.1 conformes aux standards pour les SIEM et les plateformes de threat intelligence.
Surveillance du dark web	Surveillance continue des places de marché, forums, sites de paste et fuites de données, à la recherche d'identifiants et de données divulgués.
Surface d'attaque et scanner de vulnérabilités	Identification et analyse des actifs, réseaux et applications web exposés sur Internet.
Alertes CVE	Un catalogue de CVE consultable, avec scores CVSS et EPSS et statut CISA KEV, ainsi qu'un récapitulatif quotidien ou hebdomadaire par e-mail des nouvelles CVE touchant les logiciels que vous indiquez dans le portail.
Brand Protection	Détection des domaines sosies, du typosquatting et des pages de phishing, avec demandes de suppression.

04

Comment nous sélectionnons nos renseignements

La valeur de la threat intelligence ne tient pas aux données brutes, mais à ce qu'elles deviennent avant d'atteindre vos défenses. Nous combinons quatre types de sources :

Sources commerciales

Des éditeurs de cybersécurité professionnels qui collectent et enrichissent les données sur les menaces avec leurs propres systèmes.

Open source (OSINT)

Projets communautaires, groupes de recherche, listes ouvertes, forums et publications.

Sources gouvernementales

Les renseignements partagés par les organismes publics de cybersécurité, nationaux et internationaux.

Nos propres honeypots

Des capteurs qui attirent et enregistrent du trafic d'attaque réel, pour des observations de première main.

Quelle que soit son origine, chaque indicateur suit le même processus :

1. **Collecter**
   Collecte continue auprès de toutes les sources.
2. **Nettoyer**
   Normalisation, dédoublonnage et expiration des indicateurs qui ne sont plus actifs.
3. **Valider**
   Validation des faux positifs, pour que les infrastructures légitimes restent hors des listes.
4. **Enrichir**
   Notation de priorité, catégorisation et mappage MITRE ATT&CK.
5. **Livrer**
   Publication sous forme de flux, de collections TAXII et de réponses d'API, actualisés toutes les 20 minutes avec Premium.

OSINT ET COMMERCIAL, MÊME EXIGENCE

Les flux OSINT et les flux commerciaux diffèrent par leur origine, pas par la façon dont nous les traitons. Tous passent par les mêmes contrôles qualité : chaque indicateur de notre plateforme répond donc au même niveau d'exactitude et de fiabilité.

05

Notre façon de travailler

Principe	En pratique
Standards ouverts	Livraison par flux HTTPS, CSV, TAXII 2.1 et STIX 2.1 : nos renseignements s'intègrent à presque tous les outils, sans dépendance à un éditeur.
L'open source quand il est utile	Nos scripts d'intégration pour MikroTik, Linux nftables / iptables et Wazuh sont publiés en open source.
Gratuit pour commencer	L'édition Community est gratuite à vie : chacun peut évaluer nos renseignements sur son propre réseau avant d'acheter.

Principe	En pratique
Des licences justes	Les licences reposent sur les personnes réellement protégées et les équipements réellement utilisés, pas sur la taille totale de l'entreprise ni sur le matériel de secours.
Des scans responsables	Notre scanner de vulnérabilités n'analyse que les actifs dont le propriétaire a donné son autorisation, et chaque demande de scan est enregistrée.
Divulgation responsable	Nous publions une politique de sécurité et de divulgation, et les signalements de la communauté des chercheurs en sécurité sont les bienvenus.

06

Écosystème et partenaires

Nous nous appuyons sur un réseau croissant de partenaires technologiques, de distributeurs et de revendeurs qui fournissent, déploient et assurent le support de Q-Feeds localement.

Technologie

Q-Feeds est disponible sous forme de plugin natif dans le dépôt officiel d'OPNsense et est livré avec OPNsense 26.1, développé en collaboration avec Deciso. Des intégrations documentées couvrent les principaux pare-feu, SIEM et plateformes de threat intelligence.

Distribution

Aux Pays-Bas, Q-Feeds est disponible auprès des distributeurs à valeur ajoutée Infinigate et DSD Europe.

Revendeurs

Des revendeurs partenaires certifiés aux Pays-Bas, en Allemagne, au Royaume-Uni, en Italie et en Pologne. Trouvez-en un près de chez vous grâce à la recherche de partenaires sur qfeeds.com.

Qui utilise Q-Feeds

Q-Feeds est utilisé par des fournisseurs de services managés, des revendeurs et des équipes IT et sécurité internes dans des secteurs comme l'hôtellerie et les loisirs, la logistique, la santé et le secteur associatif. Des organisations comme Landal renforcent leurs pare-feu avec la threat intelligence sélectionnée de Q-Feeds.

Dans les médias

Q-Feeds prend régulièrement part au débat public sur la sécurité des petites et moyennes entreprises, notamment dans la série De Staat van Security avec Sophos, et à travers des articles dans Dutch IT Channel, Dutch IT Leaders et ITchannelPRO.

07

Offres

	Community	Plus	Premium
Mises à jour des flux	Toutes les 24 heures	Toutes les 4 heures	Toutes les 20 minutes
Flux d'IP malveillantes	OSINT	OSINT + données IP premium	OSINT + données IP premium
Flux de domaines malveillants	OSINT	OSINT	OSINT + données DNS premium
Flux d'URL malveillantes	–	–	Inclus (proxy / filtre web)
Surveillance du dark web	–	Inclus	Inclus
Threat Lookup	–	Inclus	Inclus
Scanner de vulnérabilités	–	1 scan par semaine et par IP	1 scan par jour et par actif, applications web incluses
Catalogue CVE	Inclus	Inclus	Inclus
Alertes CVE	–	Inclus	Inclus
Brand Protection	–	–	Inclus, avec demandes de suppression
Prix	Gratuit à vie	Dès 99 € / an	Dès 249 € / an

La livraison TAXII 2.1 / STIX 2.1 est proposée dans une offre Enterprise TAXII distincte. L'API IOC Lookup est disponible dès 49,99 € par mois. Tarifs indiqués sur qfeeds.com/pricing à la date de rédaction.

Évaluez Q-Feeds dès aujourd'hui

Créez un compte gratuit sur le Threat Intelligence Portal, à l'adresse tip.qfeeds.com. L'édition Community est gratuite à vie et comprend un essai Premium de 7 jours, sans carte bancaire. Pour les programmes partenaires, les licences en volume ou une démo accompagnée, contactez notre équipe.



qfeeds.com · +31 (0)85 00 22 932 · Oude Amersfoortseweg 43, 1213 AB Hilversum, Pays-Bas

Q-Feeds · Chambre de commerce (KvK) 94910774 · Oude Amersfoortseweg 43, 1213 AB Hilversum, Pays-Bas