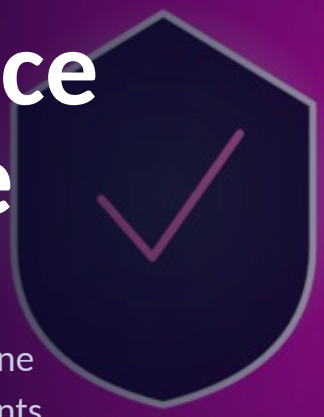
Q-FEEDS

LIVRE BLANC · MSP ET MSSP

La threat intelligence en tant que service



Comment les fournisseurs de services managés transforment une threat intelligence sélectionnée en une offre de sécurité récurrente et évolutive pour leurs clients.

qfeeds.com
Version 2026

MADE IN EUROPE

01

Synthèse

Les petites et moyennes organisations sont devenues une cible de choix pour la cybercriminalité, et pourtant la plupart n'ont pas accès à la threat intelligence. Les fournisseurs de services managés sont les mieux placés pour combler cet écart, car ils gèrent déjà les pare-feu, les SIEM et les filtres DNS, là où la threat intelligence produit ses effets.

Ce livre blanc explique comment les MSP et les MSSP peuvent utiliser Q-Feeds pour ajouter une threat intelligence sélectionnée à l'infrastructure qu'ils gèrent déjà, et en faire des services que leurs clients comprennent et acceptent de payer : pare-feu renforcés, détection SIEM enrichie, surveillance de l'exposition et protection contre le phishing.

2 500+	20 min	20+	€0
sources commerciales, OSINT et gouvernementales	intervalle de mise à jour avec Premium	intégrations natives et documentées	pour démarrer : édition Community, gratuite à vie

À retenir

- La threat intelligence est l'une des rares couches de sécurité que l'on peut déployer sur l'ensemble d'un parc clients sans nouveau matériel ni agent.
- La sélection compte plus que le volume. Les listes non filtrées génèrent des faux positifs, et chaque faux positif devient un ticket de support.
- Un seul flux, indépendant des constructeurs, fonctionne avec Fortinet, Palo Alto, Sophos, Check Point, OPNsense, pfSense, MikroTik et les principaux SIEM : une même offre couvre ainsi un parc hétérogène.
- Une tarification fondée sur les utilisateurs bénéficiaires, les équipements actifs et la durée reste prévisible pour les prestataires et équitable pour les clients.

02

L'opportunité pour les prestataires de services

Les attaques contre les petites et moyennes organisations sont en grande partie automatisées. Des botnets parcourent tout Internet à la recherche de VPN et de bureaux à distance exposés, des kits de phishing se louent à l'heure et les groupes de ransomware ne choisissent pas leurs victimes selon la taille de l'entreprise. Les organisations de moins de 500 salariés font face aux mêmes menaces que les grandes entreprises, mais disposent rarement d'une équipe de sécurité pour y répondre.

Dans le même temps, la réglementation et les attentes des clients se renforcent. NIS2 impose à de nombreuses organisations de prendre des mesures appropriées contre les cyberrisques, et les exigences liées à

la chaîne d'approvisionnement reportent les questions de sécurité sur les plus petits fournisseurs. La plupart de ces organisations se tournent vers leur prestataire informatique pour y répondre.

Les clients le demandent

Les questionnaires sur la sécurité, NIS2 et la cyberassurance arrivent sur le bureau du prestataire informatique. Une mesure concrète et facile à expliquer simplifie cet échange.

L'infrastructure est déjà en place

Les MSP gèrent déjà les pare-feu, les SIEM et les filtres DNS de leurs clients. La threat intelligence rend cette infrastructure existante plus intelligente.

Récurrente par nature

La threat intelligence est par définition un abonnement. Elle trouve naturellement sa place dans les contrats de services managés et dans le revenu mensuel récurrent.

03

Pourquoi la threat intelligence est difficile à fournir à grande échelle

De nombreux prestataires ont essayé les listes de blocage gratuites ou les flux fournis avec les équipements d'un constructeur. Dans la pratique, ils se heurtent aux mêmes problèmes :

Difficulté	Ce que cela implique pour un MSP
Listes bruitées et non validées	Les listes gratuites contiennent souvent des entrées obsolètes et des infrastructures légitimes, comme des adresses cloud ou CDN partagées. Les bloquer casse des applications et génère des tickets.
Données obsolètes	Les listes mises à jour une fois par jour passent à côté des infrastructures de phishing et de command-and-control éphémères, parfois actives quelques heures seulement.
Dépendance à un constructeur	Les flux natifs d'un constructeur ne fonctionnent que sur ses propres équipements. Un prestataire qui gère un parc hétérogène se retrouve avec des renseignements, une qualité et des tarifs différents pour chaque client.
Tarifs grands comptes	Les plateformes commerciales de threat intelligence sont généralement tarifées pour les grandes entreprises et les équipes SOC, pas pour un client de 40 personnes derrière un seul pare-feu.
Charge opérationnelle	Construire et maintenir sa propre chaîne de collecte, de dédoublonnage et de validation demande un temps d'ingénierie dont la plupart des prestataires ne disposent pas.

L'ESSENTIEL

Pour un prestataire de services, la valeur de la threat intelligence ne tient pas au nombre d'indicateurs. Elle tient au **faible nombre de faux positifs qui atteignent le client** et au peu de travail nécessaire pour maintenir à jour des centaines d'équipements.

04

Ce que fournit Q-Feeds

Q-Feeds réunit les renseignements de plus de 2 500 sources commerciales, open source et gouvernementales, dont notre propre réseau de honeypots, en un ensemble sélectionné. Chaque jeu de données suit le même processus avant sa publication :

1. **Collecter**
   Collecte continue auprès de fournisseurs commerciaux, de projets OSINT, de sources gouvernementales et de honeypots.
2. **Nettoyer**
   Normalisation et dédoublonnage, puis retrait des indicateurs qui ne sont plus actifs.
3. **Valider**
   Validation des faux positifs, pour que les services légitimes et les infrastructures partagées restent hors de la liste.
4. **Enrichir**
   Notation de priorité, catégorisation et mappage MITRE ATT&CK pour le contexte.
5. **Livrer**
   Publication sous forme de flux prêts à l'emploi, via TAXII 2.1 et par API, actualisés toutes les 20 minutes avec Premium.

Une plateforme, plusieurs briques

Composant	À quoi il sert
Flux de threat intelligence	Flux sélectionnés d'IP, de domaines et d'URL malveillants pour les pare-feu, les filtres DNS, les proxys et les SIEM.
Threat Lookup et API IOC Lookup	Un contexte immédiat sur n'importe quelle IP, n'importe quel domaine, URL ou hash de fichier : score de malveillance, sources et mappage MITRE ATT&CK. Disponible dans le portail et sous forme d'API pour les workflows SOAR et de ticketing.
Serveur TAXII 2.1	Collections STIX 2.1 conformes aux standards pour les SIEM, les plateformes de threat intelligence et les outils SOAR.

Composant	À quoi il sert
Surveillance du dark web	Recherches planifiées d'identifiants divulgués et de données compromises liés aux domaines des clients.
Surface d'attaque et analyse des vulnérabilités	Identification des actifs exposés sur Internet, des ports ouverts et des vulnérabilités réseau et web, à la demande ou de façon planifiée.
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.

05

Les services que vous pouvez construire

La même plateforme permet de proposer plusieurs offres de services. La plupart des prestataires commencent par le durcissement des pare-feu, puis ajoutent les autres services à mesure que leurs clients gagnent en maturité.

Durcissement managé des pare-feu

Ajoutez des flux sélectionnés d'IP, de domaines et d'URL aux pare-feu que vous gérez déjà. Le trafic connu pour être malveillant est bloqué automatiquement, en entrée comme en sortie. **Résultat pour le client :** moins de clics de phishing aboutis, un trafic de command-and-control bloqué et moins de bruit lié aux scanners.

Enrichissement du SIEM et du SOC

Alimentez Splunk, Microsoft Sentinel, Wazuh ou tout SIEM compatible TAXII avec des IOC sélectionnés, accompagnés du contexte MITRE ATT&CK. **Résultat :** moins de fausses alertes, un tri plus rapide et des incidents mieux documentés.

Rapports d'exposition et de dark web

Utilisez le scanner de vulnérabilités, les outils de surface d'attaque, les alertes CVE et la surveillance du dark web pour remettre un rapport d'exposition périodique. **Résultat :** un livrable concret et récurrent, qui démontre la valeur de votre service.

Protection contre le phishing et protection de marque

Surveillez les domaines sosies et les campagnes de phishing qui usurpent l'identité de votre client, et demandez leur suppression. **Résultat :** une protection pour les clients et la réputation de votre client.

LA DÉTECTION, UN BÉNÉFICE SUPPLÉMENTAIRE

Lorsqu'un pare-feu bloque du trafic sortant vers un serveur de command-and-control connu, l'entrée de journal indique quel équipement interne a tenté de se connecter. Pour un MSP, chaque blocage de ce type est un signal d'alerte précoce : un équipement du client est peut-être infecté, souvent avant qu'un autre outil ne donne l'alerte.

06

Un seul flux pour un parc hétérogène

Les prestataires de services gèrent rarement une seule marque. Q-Feeds est indépendant des constructeurs et livré par des mécanismes ouverts : les mêmes renseignements sélectionnés et la même offre fonctionnent donc pour l'ensemble du parc clients.

Catégorie	Plateformes prises en charge
Pare-feu	Fortinet FortiGate, Palo Alto Networks, Sophos XGS, Check Point, SonicWall, OPNsense (plugin natif), pfSense, MikroTik RouterOS, Linux nftables / iptables
SIEM	Splunk, Microsoft Sentinel, Wazuh, Exabeam et d'autres SIEM via TAXII 2.1, les flux ou l'API (par ex. IBM QRadar, Elastic Security, LogRhythm, Google SecOps)
Plateformes de threat intelligence	OpenCTI, MISP, EclecticIQ, Anomali ThreatStream, ThreatConnect
Filtrage DNS	Pi-hole, AdGuard Home, Technitium DNS
Développeurs	API IOC Lookup, serveur TAXII 2.1, scripts d'intégration open source

Des guides de configuration pas à pas sont disponibles pour chaque plateforme dans la base de connaissances Q-Feeds et sous forme de manuels PDF. Pour les détails techniques, consultez le livre blanc associé, **Intégrer Q-Feeds**.

07

Opérer à grande échelle

Gestion multi-clients

Les partenaires gèrent leurs clients depuis un compte revendeur sur le Threat Intelligence Portal. Les licences achetées par le partenaire sont rattachées à ce compte et peuvent être attribuées à chaque entreprise cliente, avec ses propres utilisateurs. Le partenaire conserve la relation client ; Q-Feeds s'occupe de la threat intelligence.

Une fois configuré, plus rien à gérer

- Les équipements interrogent automatiquement leurs URL de flux ; il n'y a aucune liste à tenir à jour à la main.
- Adaptez l'intervalle d'interrogation à la licence : toutes les 24 heures avec Community, toutes les 4 heures avec Plus, toutes les 20 minutes avec Premium.
- Utilisez le paramètre limit pour ajuster la taille des listes à la capacité des équipements les plus petits.
- Placez les règles de blocage au-dessus des règles d'autorisation et activez la journalisation, afin que les blocages soient visibles et puissent figurer dans vos rapports.

Gérer les faux positifs

Grâce à la validation, les faux positifs restent rares. Si une adresse légitime est bloquée, le prestataire peut ajouter une exception temporaire sur l'équipement et signaler l'indicateur à Q-Feeds. Q-Feeds examine le signalement, détermine s'il s'agit d'un faux positif et met le flux à jour si nécessaire : la correction profite ainsi à tous les clients.

08

Des licences adaptées au modèle économique des prestataires

Les licences Q-Feeds reposent sur trois éléments : le nombre d'**utilisateurs bénéficiaires** (les personnes réellement protégées, et non l'effectif total de l'entreprise), le nombre d'**équipements actifs** et la **durée** (1, 2 ou 3 ans). Les petits clients restent ainsi abordables et le dimensionnement devient prévisible.

Configuration	Licences d'équipement
Un seul pare-feu	1
Deux pare-feu distincts	2
Cluster actif-passif	1 (l'équipement de secours n'est pas compté)
Cluster actif-actif	2

Paliers d'utilisateurs bénéficiaires : Small (< 50), Medium (50 à 250), Large (250 à 1 000) et Enterprise (1 000+). La même structure s'applique à Plus et à Premium ; la différence tient à l'étendue des fonctionnalités.

	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.

PROGRAMME PARTENAIRES

Les revendeurs et les prestataires de services bénéficient de tarifs partenaires, d'un accompagnement au démarrage, de formations et de supports de vente, ainsi que d'un accès direct à l'équipe Q-Feeds pour les preuves de concept. Une livraison en marque blanche est possible pour les prestataires qui souhaitent proposer la threat intelligence sous leur propre marque. Contactez-nous pour en savoir plus.

09

Démarrage

1. **Inscrivez-vous**

   Créez un compte gratuit sur le Threat Intelligence Portal. L'édition Community comprend un essai Premium de 7 jours.

2. **Faites la preuve sur votre propre réseau**

   Connectez un pare-feu ou un SIEM à l'aide des guides de configuration et mesurez ce qui est bloqué. Le Testing Tool, gratuit, vous aide à évaluer votre protection actuelle.

3. **Devenez partenaire**

   Rejoignez le programme revendeur pour obtenir un compte revendeur, des tarifs partenaires et un accompagnement au démarrage.

4. **Déployez**

   Commencez par le durcissement des pare-feu de vos clients, puis ajoutez progressivement l'enrichissement SIEM, les rapports d'exposition et la protection de marque.

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.

MADE IN EUROPE

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