Q-FEEDS

LIVRE BLANC · INTÉGRATIONS

Un flux sélectionné pour toute votre stack de sécurité



Comment la threat intelligence de Q-Feeds s'intègre aux pare-feu, aux SIEM, aux plateformes de threat intelligence et aux filtres DNS, et comment en tirer le meilleur parti.

qfeeds.com
Version 2026

MADE IN EUROPE

01

Introduction

La threat intelligence ne crée de la valeur qu'une fois appliquée. Q-Feeds est conçu pour se brancher sur les outils de sécurité que vous utilisez déjà, via leurs mécanismes natifs. Des renseignements sélectionnés atteignent ainsi en quelques minutes la périphérie de votre réseau, votre SIEM et vos analystes.

Ce livre blanc décrit les modes de livraison proposés par Q-Feeds, les flux disponibles selon la licence, la façon dont chaque grande plateforme exploite ces renseignements et les bonnes pratiques qui rendent une intégration fiable. Des guides détaillés, pas à pas, sont disponibles pour chaque plateforme dans la base de connaissances sur qfeeds.com.

20+	3	TAXII 2.1	5 min
intégrations documentées	types de flux : IP, domaine, URL	livraison conforme aux standards	délai habituel avant le premier flux

02

Modes de livraison

Q-Feeds propose cinq façons d'exploiter ses renseignements. La plupart des intégrations utilisent la première ; les autres s'adressent aux SIEM, aux plateformes de threat intelligence et aux outils sur mesure.

Méthode	Fonctionnement	Idéal pour
URL de flux HTTPS	Votre équipement récupère régulièrement une liste en HTTPS : en texte brut par défaut, en CSV sur demande. Un paramètre limit plafonne la taille de la liste pour les équipements soumis à un maximum.	Pare-feu, filtres DNS, proxys
Plugin natif	Un plugin Q-Feeds, disponible dans le dépôt officiel d'OPNsense, crée et met à jour automatiquement les alias de pare-feu et les listes de blocage DNS.	OPNsense
TAXII 2.1 / STIX 2.1	Un serveur TAXII 2.1 avec des collections STIX 2.1, comprenant la catégorie, le mappage MITRE ATT&CK et les hashs de fichiers. Les clients ne récupèrent que les nouveautés depuis la dernière interrogation.	SIEM, TIP, SOAR

Méthode	Fonctionnement	Idéal pour
API IOC Lookup	Interrogez une IP, un domaine, une URL ou un hash et recevez le même contexte que dans Threat Lookup : score, sources et mappage MITRE ATT&CK.	Enrichissement des alertes, SOAR, ticketing
Scripts open source	Des installeurs et des scripts maintenus pour les plateformes sans prise en charge native des flux, publiés sur GitHub.	MikroTik, hôtes Linux, Wazuh

03

Flux et disponibilité selon la licence

Flux	Contenu	Disponible avec
malware_ip	Adresses IP malveillantes (IPv4 et IPv6) : botnets, serveurs de command-and-control, scanners et hébergement de malwares.	Community, Plus, Premium
malware_domains	Domaines malveillants utilisés pour le phishing, la diffusion de malwares et le command-and-control.	Community, Plus, Premium
malicious_urls	URL malveillantes précises, comme des pages de phishing et des téléchargements de malwares.	Premium
Collections TAXII	Indicateurs STIX 2.1 pour les IP, domaines, URL et hashs de fichiers, avec catégorie, mappage MITRE ATT&CK et contexte.	Offre Enterprise TAXII

Licence	Actualisation du flux	Intervalle d'interrogation recommandé
Community	Toutes les 24 heures	Une fois par jour
Plus	Toutes les 4 heures	Toutes les 4 heures
Premium	Toutes les 20 minutes	Toutes les 20 minutes

LES FLUX D'URL EXIGENT UN ÉQUIPEMENT CAPABLE DE VOIR LES URL

Un filtre de paquets qui travaille sur les adresses IP, ou un filtre DNS qui travaille sur les noms de domaine, ne peut pas appliquer une liste d'URL. Les flux d'URL malveillantes nécessitent un proxy ou un filtre web et, pour le trafic HTTPS, cet équipement a besoin de l'**inspection TLS** ; sans elle, il ne voit que le nom d'hôte.

04

Authentification

Tous les accès passent par une clé API personnelle, créée dans Manage API Keys sur le Threat Intelligence Portal.

```
https://api.qfeeds.com/api?feed_type=malware_ip&limit=130000
Authorization: Basic  (username: api_token, password: YOUR_API_KEY)
```

- **Flux :** la plupart des équipements utilisent l'authentification HTTP Basic, avec api_token comme nom d'utilisateur et votre clé comme mot de passe. Les équipements qui ne prennent pas en charge l'authentification Basic peuvent transmettre la clé en paramètre d'URL.
- **API IOC Lookup et TAXII :** envoyez la clé sous forme de jeton Bearer dans l'en-tête Authorization.
- Traitez la clé comme un secret : toute personne qui la détient peut récupérer vos flux.

05

Pare-feu

Les pare-feu appliquent la threat intelligence de Q-Feeds en périphérie du réseau : ils bloquent le trafic entrant et sortant vers les infrastructures malveillantes connues avant qu'il n'atteigne les utilisateurs ou les serveurs. Chaque intégration utilise le mécanisme propre au constructeur ; aucun boîtier ni agent supplémentaire n'est donc nécessaire.

Plateforme	Mécanisme d'intégration	Flux
Fortinet FortiGate	External Connectors natifs (threat feeds), appliqués dans les politiques de pare-feu, de filtrage DNS et de filtrage web.	IP, domaine, URL
Palo Alto Networks	External Dynamic Lists (EDL) natives, appliquées dans les règles de Security policy. Compatible avec les parcs gérés par Panorama.	IP, domaine, URL
Sophos Firewall (XGS)	Flux de menaces tiers, appliqués dans les règles de pare-feu et les politiques web, en complément des protections Sophos.	IP, domaine, URL
Check Point	Custom Intelligence Feeds natifs, appliqués par les Software Blades Anti-Bot et Anti-Virus.	IP, domaine
OPNsense	Plugin Q-Feeds natif issu du dépôt officiel (livré avec OPNsense 26.1) : alias de pare-feu, et blocage de domaines via Unbound DNS ou DNSCrypt-Proxy.	IP, domaine

Plateforme	Mécanisme d'intégration	Flux
pfSense	Paquet pfBlockerNG : flux d'IP sous forme d'alias de pare-feu, flux de domaines via DNSBL.	IP, domaine
SonicWall	Dynamic Botnet List Server avec filtrage Botnet sur les règles d'accès (SonicOS 6.5.2+ pour les téléchargements authentifiés).	IP
MikroTik RouterOS	Scripts RouterOS open source : import complet et mises à jour différentielles dans une address-list du pare-feu, avec retour arrière automatique si un téléchargement échoue.	IP
Linux nftables / iptables	Installeur open source qui charge la liste de blocage dans des sets dédiés et planifie les mises à jour.	IP

EN COMPLÉMENT DE LA THREAT INTELLIGENCE DE VOTRE CONSTRUCTEUR

Q-Feeds fonctionne en parallèle des abonnements FortiGuard, WildFire, ThreatCloud ou Sophos X-Ops. Il apporte une threat intelligence indépendante et multisource, et offre aux prestataires un flux homogène quelle que soit la marque.

06

Plateformes SIEM

Dans un SIEM, les indicateurs Q-Feeds sont corrélés aux journaux : toute activité impliquant des IP, domaines, URL ou hashs connus pour être malveillants remonte sous forme d'alerte priorisée, avec le contexte MITRE ATT&CK.

Plateforme	Mécanisme d'intégration
Splunk	Indicateurs ingérés sous forme de lookups ou dans le framework de threat intelligence de Splunk Enterprise Security, prêts pour les recherches de corrélation. TAXII/STIX 2.1 disponible pour l'ingestion.
Microsoft Sentinel	Connecteur de données Threat Intelligence natif en TAXII/STIX 2.1. Les indicateurs arrivent dans la table ThreatIntelligenceIndicator, pour les règles d'analyse, les requêtes de hunting et les classeurs.
Wazuh	Installeur open source pour Wazuh 4.x : listes CDB, décodeurs et règles qui déclenchent des alertes en cas de correspondance. Blocage automatique possible avec Active Response. Fonctionne avec l'API standard ou TAXII.

Plateforme	Mécanisme d'intégration
Exabeam	Table de contexte personnalisée, alimentée en indicateurs Q-Feeds via l'API Exabeam Context Management (CSV) et actualisée automatiquement.
Autres SIEM	IBM QRadar, Elastic Security, LogRhythm, Google SecOps et d'autres plateformes via TAXII 2.1, les flux ou l'API.

La livraison TAXII nécessite l'offre Enterprise TAXII.

07

Plateformes de threat intelligence

Pour les équipes d'analystes, Q-Feeds constitue un socle fiable et sélectionné. Les indicateurs conservent leur attribution à la source Q-Feeds : vous pouvez les filtrer, en tirer des rapports et les supprimer sans toucher au reste de vos connaissances.

Plateforme	Mécanisme d'intégration	Licence
OpenCTI	Ingestion TAXII intégrée, rien à développer ni à maintenir. Avec les autres licences, les listes d'IP et de domaines peuvent être ingérées sous forme de flux.	Enterprise TAXII (flux avec toutes les offres)
MISP	Flux MISP natifs : pointez MISP vers les listes complètes et définissez la fréquence de récupération.	Toutes les offres (URL avec Premium)
EclecticIQ	Flux TAXII entrant standard ; les indicateurs deviennent des entités dans l'espace de travail de votre choix.	Enterprise TAXII
Anomali ThreatStream	Configuration standard d'un flux TAXII ; les indicateurs conservent leur propre étiquette de source.	Enterprise TAXII
ThreatConnect	L'application TAXII de ThreatConnect, disponible dans son catalogue ; chaque collection devient une source à part entière.	Enterprise TAXII

08

Filtrage DNS

Les filtres DNS bloquent les domaines malveillants dès la résolution, avant même qu'une connexion ne soit établie. Pi-hole, AdGuard Home et Technitium DNS s'abonnent directement à la liste de domaines malveillants de Q-Feeds, ce qui en fait une solution efficace pour les petits bureaux, les agences et les réseaux domestiques.

09

Bonnes pratiques

Pratique	Pourquoi c'est important
Adaptez l'interrogation à votre licence	Interroger plus souvent que le flux n'est actualisé ajoute de la charge sans ajouter de protection. Interroger moins souvent, c'est se priver d'une partie de la protection.
Respectez les limites des équipements	De nombreux pare-feu imposent une taille de liste maximale. Utilisez le paramètre limit pour rester en dessous, surtout sur les modèles plus petits ou plus anciens.
Bloquez dans les deux sens	Les blocages entrants arrêtent les scanners et les tentatives de force brute ; les blocages sortants, les clics de phishing et les malwares qui tentent de joindre le serveur de l'attaquant.
Placez les règles de blocage en premier	Placez les règles Q-Feeds au-dessus des règles d'autorisation, sinon le trafic risque d'être autorisé avant que la liste ne soit évaluée.
Activez la journalisation	Les blocages journalisés montrent la valeur de la threat intelligence et signalent les équipements internes potentiellement infectés.
Tenez compte de la haute disponibilité	Un cluster actif-passif nécessite une seule licence d'équipement ; un cluster actif-actif en nécessite une par équipement.
Testez votre configuration	Utilisez le Q-Feeds Testing Tool, gratuit, pour vérifier que l'intégration fonctionne et évaluer votre protection.

10

Démarrage

1. **Créez un compte**

   Inscrivez-vous sur le Threat Intelligence Portal et activez l'édition Community gratuite, essai Premium de 7 jours inclus.

2. **Créez une clé API**

   Dans le portail, ouvrez Manage API Keys et créez votre clé.

3. **Composez l'URL de votre flux**

   Choisissez le type de flux et, si nécessaire, une limite et un format de sortie.

4. **Suivez le guide de configuration**

   Appuyez-vous sur le guide pas à pas de votre plateforme dans la base de connaissances, ou sur les manuels PDF de la page de téléchargements.

5. **Vérifiez**

   Vérifiez que la liste est bien remplie, que les règles de blocage sont actives et que les blocages apparaissent dans les journaux.

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