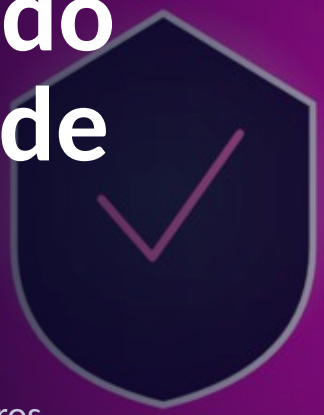
Q-FEEDS

WHITE PAPER · INTEGRACIONES

Un feed seleccionado para todo su stack de seguridad



Cómo se integra la threat intelligence de Q-Feeds con firewalls, SIEM, plataformas de threat intelligence y filtros DNS, y cómo sacarle el máximo partido.

qfeeds.com
Versión 2026

MADE IN EUROPE

01

Introducción

La threat intelligence solo aporta valor cuando se aplica. Q-Feeds se ha diseñado para conectarse a las herramientas de seguridad que usted ya utiliza, a través de sus mecanismos nativos, de modo que la inteligencia seleccionada llegue en cuestión de minutos al perímetro de su red, a su SIEM y a sus analistas.

Este white paper describe los métodos de entrega que ofrece Q-Feeds, qué feeds están disponibles con cada licencia, cómo consume la inteligencia cada una de las principales plataformas y qué buenas prácticas mantienen fiable una integración. En la base de conocimiento de qfeeds.com encontrará guías detalladas, paso a paso, para cada plataforma.

20+	3	TAXII 2.1	5 min
integraciones documentadas	tipos de feed: IP, dominio, URL	entrega basada en estándares	tiempo habitual hasta el primer feed

02

Métodos de entrega

Q-Feeds ofrece cinco formas de consumir su inteligencia. La mayoría de las integraciones usan la primera; las demás están pensadas para SIEM, plataformas de threat intelligence y herramientas propias.

Método	Cómo funciona	Ideal para
URL de feed por HTTPS	Su dispositivo descarga periódicamente una lista por HTTPS: en texto plano por defecto y en CSV si se solicita. Un parámetro limit acota el tamaño de la lista en dispositivos con un máximo.	Firewalls, filtros DNS, proxies
Plugin nativo	Un plugin de Q-Feeds en el repositorio oficial de OPNsense crea y actualiza automáticamente alias de firewall y listas de bloqueo DNS.	OPNsense
TAXII 2.1 / STIX 2.1	Un servidor TAXII 2.1 con colecciones STIX 2.1, que incluyen categoría, mapeo MITRE ATT&CK y hashes de archivo. Los clientes solo descargan lo nuevo desde la última consulta.	SIEM, TIP, SOAR

Método	Cómo funciona	Ideal para
API IOC Lookup	Consulte una única IP, dominio, URL o hash y reciba el mismo contexto que en Threat Lookup: puntuación, fuentes y mapeo MITRE ATT&CK.	Enriquecimiento de alertas, SOAR, ticketing
Scripts de código abierto	Instaladores y scripts mantenidos para plataformas sin soporte nativo de feeds, publicados en GitHub.	MikroTik, hosts Linux, Wazuh

03

Feeds y disponibilidad por licencia

Feed	Contenido	Disponible en
malware_ip	Direcciones IP maliciosas (IPv4 e IPv6): botnets, servidores de command-and-control, escáneres y alojamiento de malware.	Community, Plus, Premium
malware_domains	Dominios maliciosos utilizados para phishing, distribución de malware y command-and-control.	Community, Plus, Premium
malicious_urls	URL maliciosas concretas, como páginas de phishing y descargas de malware.	Premium
Colecciones TAXII	Indicadores STIX 2.1 de IP, dominios, URL y hashes de archivo, con categoría, mapeo MITRE ATT&CK y contexto.	Paquete Enterprise TAXII

Licencia	Actualización del feed	Intervalo de consulta recomendado
Community	Cada 24 horas	Una vez al día
Plus	Cada 4 horas	Cada 4 horas
Premium	Cada 20 minutos	Cada 20 minutos

LOS FEEDS DE URL NECESITAN UN DISPOSITIVO CAPAZ DE VER URL

Un filtro de paquetes que trabaja con direcciones IP, o un filtro DNS que trabaja con nombres de dominio, no puede aplicar una lista de URL. Los feeds de URL maliciosas requieren un proxy o un filtro web y, en el tráfico HTTPS, ese dispositivo necesita **inspección TLS**; de lo contrario, solo ve el nombre de host.

04

Autenticación

Todo el acceso se realiza con una clave de API personal, que se crea en Manage API Keys, dentro del Threat Intelligence Portal.

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

- **Feeds:** la mayoría de los dispositivos usan autenticación HTTP Basic, con api_token como nombre de usuario y su clave como contraseña. Los dispositivos que no admiten autenticación Basic pueden pasar la clave como parámetro de la URL.
- **API IOC Lookup y TAXII:** envíe la clave como token Bearer en la cabecera Authorization.
- Trate la clave como un secreto: cualquiera que la tenga puede descargar sus feeds.

05

Firewalls

Los firewalls aplican la inteligencia de Q-Feeds en el perímetro de la red y bloquean el tráfico entrante y saliente hacia infraestructura maliciosa conocida antes de que llegue a usuarios o servidores. Cada integración utiliza el mecanismo propio del fabricante, por lo que no hace falta ningún equipo ni agente adicional.

Plataforma	Mecanismo de integración	Feeds
Fortinet FortiGate	External Connectors nativos (threat feeds), aplicados en las políticas de firewall, filtro DNS y filtro web.	IP, dominio, URL
Palo Alto Networks	External Dynamic Lists (EDL) nativas, aplicadas en las reglas de Security policy. Compatible con entornos gestionados con Panorama.	IP, dominio, URL
Sophos Firewall (XGS)	Third-party threat feeds, aplicados en las reglas de firewall y las políticas web, junto a las protecciones de Sophos.	IP, dominio, URL
Check Point	Custom Intelligence Feeds nativos, aplicados mediante los Software Blades Anti-Bot y Anti-Virus.	IP, dominio
OPNsense	Plugin nativo de Q-Feeds del repositorio oficial (incluido en OPNsense 26.1): alias de firewall y bloqueo de dominios mediante Unbound DNS o DNSCrypt-Proxy.	IP, dominio
pfSense	Paquete pfBlockerNG: feeds de IP como alias de firewall y feeds de dominios mediante DNSBL.	IP, dominio

Plataforma	Mecanismo de integración	Feeds
SonicWall	Dynamic Botnet List Server con filtrado Botnet en las reglas de acceso (SonicOS 6.5.2+ para descargas autenticadas).	IP
MikroTik RouterOS	Scripts de código abierto para RouterOS: importación completa y actualizaciones diferenciales en una address-list del firewall, con reversión automática si falla una descarga.	IP
Linux nftables / iptables	Instalador de código abierto que carga la lista de bloqueo en sets dedicados y programa las actualizaciones.	IP

UN COMPLEMENTO A LA INTELIGENCIA DEL FABRICANTE

Q-Feeds funciona junto a las suscripciones de FortiGuard, WildFire, ThreatCloud o Sophos X-Ops. Aporta inteligencia independiente y de múltiples fuentes, y ofrece a los proveedores un feed homogéneo para distintas marcas.

06

Plataformas SIEM

En un SIEM, los indicadores de Q-Feeds se correlacionan con los datos de log, de modo que la actividad relacionada con IP, dominios, URL o hashes maliciosos conocidos aparece como una alerta priorizada con contexto MITRE ATT&CK.

Plataforma	Mecanismo de integración
Splunk	Los indicadores se incorporan como lookups o en el framework de threat intelligence de Splunk Enterprise Security, listos para las búsquedas de correlación. TAXII/STIX 2.1 disponible para la ingesta.
Microsoft Sentinel	Conector de datos nativo de Threat Intelligence por TAXII/STIX 2.1. Los indicadores llegan a la tabla ThreatIntelligenceIndicator para reglas de análisis, consultas de hunting y libros de trabajo.
Wazuh	Instalador de código abierto para Wazuh 4.x: listas CDB, decodificadores y reglas que generan alertas cuando hay coincidencias. Bloqueo automático opcional con Active Response. Funciona con la API estándar o con TAXII.

Plataforma	Mecanismo de integración
Exabeam	Tabla de contexto personalizada que se rellena con indicadores de Q-Feeds a través de la Exabeam Context Management API (CSV) y se actualiza automáticamente.
Otros SIEM	IBM QRadar, Elastic Security, LogRhythm, Google SecOps y otras plataformas mediante TAXII 2.1, feeds o la API.

La entrega por TAXII requiere el paquete Enterprise TAXII.

07

Plataformas de threat intelligence

Para los equipos de analistas, Q-Feeds es una capa base fiable y seleccionada. Los indicadores conservan la atribución a Q-Feeds como fuente, de modo que puede filtrarlos, elaborar informes sobre ellos y eliminarlos sin tocar el resto de su conocimiento.

Plataforma	Mecanismo de integración	Licencia
OpenCTI	Ingesta TAXII integrada, sin nada que desarrollar ni mantener. Con otras licencias, las listas de IP y de dominios pueden incorporarse como feed.	Enterprise TAXII (feeds en todos los paquetes)
MISP	Feeds nativos de MISP: apunte MISP a las listas completas y defina la frecuencia de descarga.	Todos los paquetes (URL en Premium)
EclecticIQ	Feed TAXII entrante estándar; los indicadores se convierten en entidades en el espacio de trabajo que elija.	Enterprise TAXII
Anomali ThreatStream	Configuración estándar de un feed TAXII; los indicadores conservan su propia etiqueta de fuente.	Enterprise TAXII
ThreatConnect	La aplicación TAXII de ThreatConnect, disponible en su catálogo; cada colección se convierte en una fuente independiente.	Enterprise TAXII

08

Filtrado DNS

Los filtros DNS bloquean los dominios maliciosos en el momento de la resolución, antes de que llegue a establecerse una conexión. Pi-hole, AdGuard Home y Technitium DNS se suscriben directamente a la lista de dominios de malware de Q-Feeds, lo que la convierte en una opción eficaz para oficinas pequeñas, sedes remotas y redes domésticas.

09

Buenas prácticas

Práctica	Por qué importa
Ajuste la consulta a su licencia	Consultar con más frecuencia de la que se actualiza el feed añade carga sin añadir protección. Consultar con menos frecuencia supone desaprovechar protección.
Respete los límites del dispositivo	Muchos firewalls tienen un tamaño máximo de lista. Use el parámetro limit para no superarlo, sobre todo en modelos pequeños o antiguos.
Bloquee en ambos sentidos	Los bloqueos entrantes detienen escáneres e intentos de fuerza bruta; los salientes detienen los clics en enlaces de phishing y el malware que intenta contactar con el servidor del atacante.
Coloque primero las reglas de bloqueo	Sitúe las reglas de Q-Feeds por encima de las reglas de permiso; de lo contrario, el tráfico podría permitirse antes de que se evalúe la lista.
Active el registro	Los bloqueos registrados muestran el valor de la inteligencia y señalan dispositivos internos que podrían estar infectados.
Tenga en cuenta la alta disponibilidad	Un clúster activo-pasivo necesita una licencia de dispositivo; un clúster activo-activo necesita una por dispositivo.
Pruebe su configuración	Use la herramienta gratuita Q-Feeds Testing Tool para confirmar que la integración funciona y medir su protección.

10

Primeros pasos

1. **Cree una cuenta**

   Regístrese en el Threat Intelligence Portal y active la edición Community gratuita, que incluye 7 días de prueba Premium.

2. **Cree una clave de API**

   Vaya a Manage API Keys en el portal y cree su clave.

3. **Componga la URL de su feed**

   Elija el tipo de feed y, si lo necesita, un límite y un formato de salida.

4. **Siga la guía de configuración**

   Utilice la guía paso a paso de su plataforma en la base de conocimiento o los manuales en PDF de la página de descargas.

5. **Verifique**

   Compruebe que la lista tiene contenido, que las reglas de bloqueo están activas y que los bloqueos aparecen en los logs.

Evalúe Q-Feeds hoy mismo

Cree una cuenta gratuita en el Threat Intelligence Portal, en tip.qfeeds.com. La edición Community es gratis de por vida e incluye 7 días de prueba Premium, sin tarjeta de crédito. Para programas de partners, licencias por volumen o una demo guiada, contacte con nuestro equipo.



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