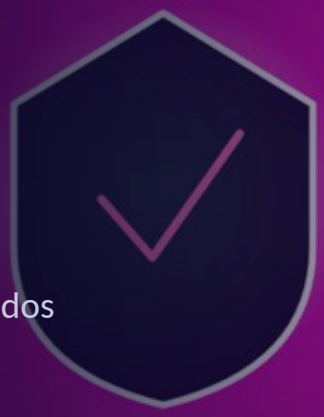
Q-FEEDS

WHITE PAPER · MSP Y MSSP

Threat intelligence como servicio



Cómo convierten los proveedores de servicios gestionados una threat intelligence seleccionada en una oferta de seguridad escalable y recurrente para sus clientes.

qfeeds.com
Versión 2026

MADE IN EUROPE

01

Resumen ejecutivo

Las organizaciones pequeñas y medianas son hoy un objetivo prioritario de la ciberdelincuencia y, sin embargo, la mayoría no tiene acceso a threat intelligence. Los proveedores de servicios gestionados están en la mejor posición para cerrar esa brecha, porque ya administran los firewalls, los SIEM y los filtros DNS donde la inteligencia hace su trabajo.

Este white paper explica cómo los MSP y los MSSP pueden usar Q-Feeds para añadir threat intelligence seleccionada a la infraestructura que ya gestionan y convertirla en servicios que sus clientes entienden y por los que pagan: firewalls reforzados, detección enriquecida en el SIEM, monitorización de la exposición y protección frente al phishing.

2.500+	20 min	20+	€0
fuentes comerciales, OSINT y gubernamentales	intervalo de actualización en Premium	integraciones nativas y documentadas	para empezar: edición Community, gratis de por vida

Ideas clave

- La threat intelligence es una de las pocas capas de seguridad que puede desplegarse en toda una cartera de clientes sin hardware ni agentes nuevos.
- La selección importa más que el volumen. Las listas sin filtrar generan falsos positivos, y cada falso positivo acaba en un ticket de soporte.
- Un único feed, independiente del fabricante, funciona con Fortinet, Palo Alto, Sophos, Check Point, OPNsense, pfSense, MikroTik y los principales SIEM, de modo que una sola propuesta cubre un parque heterogéneo.
- Un modelo de licencias basado en usuarios beneficiarios, dispositivos activos y duración mantiene los precios previsibles para los proveedores y justos para los clientes.

02

La oportunidad para los proveedores de servicios

Los ataques contra organizaciones pequeñas y medianas están en gran medida automatizados. Las botnets rastrean todo internet en busca de VPN y escritorios remotos expuestos, los kits de phishing se alquilan por horas y los grupos de ransomware no eligen a sus víctimas por el tamaño de la empresa. Las organizaciones con menos de 500 empleados se enfrentan a las mismas amenazas que las grandes empresas, pero rara vez cuentan con un equipo de seguridad que responda.

Al mismo tiempo, aumentan la regulación y las expectativas de los clientes. NIS2 obliga a muchas organizaciones a adoptar medidas adecuadas frente a los ciberriesgos, y los requisitos de la cadena de suministro trasladan las preguntas sobre seguridad a los proveedores más pequeños. La mayoría de estas organizaciones acude a su proveedor de TI en busca de respuesta.

Los clientes lo piden

Los cuestionarios sobre seguridad, NIS2 y ciberseguros acaban en la mesa del proveedor de TI. Una medida concreta y fácil de explicar simplifica esa conversación.

La infraestructura ya está ahí

Los MSP ya gestionan firewalls, SIEM y filtros DNS para sus clientes. La threat intelligence hace más inteligente esa infraestructura existente.

Recurrente por naturaleza

La threat intelligence es, por definición, una suscripción. Encaja de forma natural en los contratos de servicios gestionados y en los ingresos recurrentes mensuales.

03

Por qué cuesta ofrecer threat intelligence a escala

Muchos proveedores han probado con listas de bloqueo gratuitas o con los feeds que incluye cada fabricante. En la práctica, se topan con los mismos problemas:

Reto	Qué supone para un MSP
Listas con ruido y sin validar	Las listas gratuitas suelen contener entradas obsoletas e infraestructura legítima, como direcciones compartidas de nube o de CDN. Bloquearlas rompe aplicaciones y genera tickets.
Datos obsoletos	Las listas que se actualizan una vez al día no detectan la infraestructura efímera de phishing y de command-and-control, que a veces solo está activa unas horas.
Dependencia del fabricante	Los feeds propios de un fabricante solo funcionan en sus dispositivos. Un proveedor con un parque heterogéneo acaba con una inteligencia, una calidad y unos precios distintos para cada cliente.
Precios de gran empresa	Las plataformas comerciales de threat intelligence suelen tener precios pensados para grandes empresas y equipos SOC, no para un cliente de 40 personas detrás de un único firewall.
Carga operativa	Construir y mantener un proceso propio de recopilación, deduplicación y validación exige un tiempo de ingeniería que la mayoría de los proveedores no tiene.

LA IDEA CENTRAL

Para un proveedor de servicios, el valor de la threat intelligence no está en el número de indicadores. Está en **los pocos falsos positivos que llegan al cliente** y en el poco trabajo que cuesta mantener al día cientos de dispositivos.

04

Qué ofrece Q-Feeds

Q-Feeds reúne inteligencia de más de 2.500 fuentes comerciales, de código abierto y gubernamentales, incluida nuestra propia red de honeypots, en un único conjunto seleccionado. Cada conjunto de datos pasa por el mismo proceso antes de publicarse:

1. **Recopilar**
   Recopilación continua de proveedores comerciales, proyectos OSINT, fuentes gubernamentales y honeypots.
2. **Depurar**
   Normalización y deduplicación, y eliminación de los indicadores que ya no están activos.
3. **Validar**
   Validación de falsos positivos, para que los servicios legítimos y la infraestructura compartida queden fuera de la lista.
4. **Enriquecer**
   Puntuación de prioridad, categorización y mapeo MITRE ATT&CK para aportar contexto.
5. **Entregar**
   Publicación en forma de feeds listos para usar, por TAXII 2.1 y mediante API, actualizados cada 20 minutos en Premium.

Una plataforma, varios componentes

Componente	Qué hace
Feeds de threat intelligence	Feeds seleccionados de IP, dominios y URL maliciosos para firewalls, filtros DNS, proxies y SIEM.
Threat Lookup y API IOC Lookup	Contexto inmediato sobre cualquier IP, dominio, URL o hash de archivo: puntuación de riesgo, fuentes y mapeo MITRE ATT&CK. Disponible en el portal y como API para flujos de SOAR y ticketing.
Servidor TAXII 2.1	Colecciones STIX 2.1 basadas en estándares para SIEM, plataformas de threat intelligence y herramientas SOAR.

Componente	Qué hace
Dark Web Monitoring	Búsquedas programadas de credenciales filtradas y datos comprometidos vinculados a los dominios de los clientes.
Superficie de ataque y análisis de vulnerabilidades	Descubrimiento de activos expuestos a internet, puertos abiertos y vulnerabilidades de red y web, bajo demanda o de forma programada.
Alertas CVE	Un catálogo de CVE con buscador, puntuaciones CVSS y EPSS y estado CISA KEV, además de un resumen diario o semanal por correo con las nuevas CVE del software que indica en el portal.
Brand Protection	Detección de dominios similares, typosquatting y páginas de phishing, con solicitudes de retirada.

05

Servicios que puede construir

La misma plataforma da soporte a varias propuestas de servicio. La mayoría de los proveedores empieza por el refuerzo de firewalls y añade los demás servicios a medida que sus clientes maduran.

Refuerzo gestionado de firewalls

Añada feeds seleccionados de IP, dominios y URL a los firewalls que ya gestiona. El tráfico malicioso conocido se bloquea automáticamente, tanto de entrada como de salida. **Resultado para el cliente:** menos clics de phishing con éxito, tráfico de command-and-control bloqueado y menos ruido de escáneres.

Enriquecimiento de SIEM y SOC

Alimente Splunk, Microsoft Sentinel, Wazuh o cualquier SIEM compatible con TAXII con IOC seleccionados y contexto MITRE ATT&CK. **Resultado:** menos falsas alertas, un triaje más rápido e incidentes mejor documentados.

Informes de exposición y dark web

Use el escáner de vulnerabilidades, las herramientas de superficie de ataque, las alertas CVE y la monitorización de la dark web para entregar un informe periódico de exposición. **Resultado:** un entregable tangible y recurrente que demuestra el valor de su servicio.

Protección de marca y frente al phishing

Vigile los dominios similares y el phishing que suplantan a su cliente y solicite su retirada. **Resultado:** protección para los clientes y la reputación de su cliente.

LA DETECCIÓN, UN BENEFICIO AÑADIDO

Cuando un firewall bloquea tráfico saliente hacia un servidor de command-and-control conocido, la entrada del log muestra qué dispositivo interno intentó conectarse. Para un MSP, cada bloqueo de este tipo es un aviso temprano de que un dispositivo del cliente puede estar infectado, a menudo antes de que cualquier otra herramienta dé la alarma.

06

Un único feed para un parque heterogéneo

Los proveedores de servicios rara vez gestionan una sola marca. Q-Feeds es independiente del fabricante y se entrega mediante mecanismos abiertos, de modo que la misma inteligencia seleccionada y la misma propuesta sirven para toda la cartera de clientes.

Categoría	Plataformas compatibles
Firewalls	Fortinet FortiGate, Palo Alto Networks, Sophos XGS, Check Point, SonicWall, OPNsense (plugin nativo), pfSense, MikroTik RouterOS, Linux nftables / iptables
SIEM	Splunk, Microsoft Sentinel, Wazuh, Exabeam y otros SIEM mediante TAXII 2.1, feeds o API (p. ej., IBM QRadar, Elastic Security, LogRhythm, Google SecOps)
Plataformas de threat intelligence	OpenCTI, MISP, EclecticIQ, Anomali ThreatStream, ThreatConnect
Filtrado DNS	Pi-hole, AdGuard Home, Technitium DNS
Desarrolladores	API IOC Lookup, servidor TAXII 2.1, scripts de integración de código abierto

En la base de conocimiento de Q-Feeds y en los manuales en PDF encontrará guías de configuración paso a paso para cada plataforma. Para los detalles técnicos, consulte el white paper complementario **Integrar Q-Feeds**.

07

Operar a escala

Gestión de múltiples clientes

Los partners gestionan a sus clientes desde una cuenta de reseller en el Threat Intelligence Portal. Las licencias que compra el partner quedan vinculadas a esa cuenta y pueden asignarse a cada empresa cliente final, con sus propios usuarios. El partner conserva la relación con el cliente; Q-Feeds se ocupa de la inteligencia.

Configurar y olvidarse

- Los dispositivos consultan automáticamente sus URL de feed; no hay listas que mantener a mano.
- Ajuste el intervalo de consulta a la licencia: cada 24 horas en Community, cada 4 horas en Plus y cada 20 minutos en Premium.
- Use el parámetro limit para adaptar el tamaño de las listas a la capacidad de los dispositivos más pequeños.
- Sitúe las reglas de bloqueo por encima de las de permiso y active el registro, para que los bloqueos sean visibles y pueda informar sobre ellos.

Gestión de falsos positivos

La validación hace que los falsos positivos sean poco frecuentes. Si se bloquea una dirección legítima, el proveedor puede añadir una excepción temporal en el dispositivo y notificar el indicador a Q-Feeds. Q-Feeds evalúa el aviso, determina si se trata de un falso positivo y actualiza el feed cuando procede, de modo que la corrección beneficia a todos los clientes.

08

Licencias que encajan con el negocio del proveedor

Las licencias de Q-Feeds se basan en tres elementos: el número de **usuarios beneficiarios** (las personas realmente protegidas, no la plantilla total de la empresa), el número de **dispositivos activos** y la **duración** (1, 2 o 3 años). Así, los clientes pequeños resultan asequibles y el dimensionamiento es previsible.

Configuración	Licencias de dispositivo
Un solo firewall	1
Dos firewalls independientes	2
Clúster activo-pasivo	1 (el dispositivo en espera no cuenta)
Clúster activo-activo	2

Tramos de usuarios beneficiarios: Small (< 50), Medium (de 50 a 250), Large (de 250 a 1.000) y Enterprise (1.000+). La misma estructura se aplica a Plus y Premium; la diferencia está en el alcance de las funciones.

	Community	Plus	Premium
Actualizaciones de feeds	Cada 24 horas	Cada 4 horas	Cada 20 minutos
Feed de IP maliciosas	OSINT	OSINT + datos IP premium	OSINT + datos IP premium
Feed de dominios maliciosos	OSINT	OSINT	OSINT + datos DNS premium
Feed de URL maliciosas	–	–	Incluido (proxy / filtro web)
Dark Web Monitoring	–	Incluido	Incluido
Threat Lookup	–	Incluido	Incluido
Escáner de vulnerabilidades	–	1 análisis por semana por IP	1 análisis al día por activo, incl. aplicaciones web
Catálogo de CVE	Incluido	Incluido	Incluido
Alertas CVE	–	Incluido	Incluido
Brand Protection	–	–	Incluido, con solicitudes de retirada
Precio	Gratis de por vida	Desde 99 € / año	Desde 249 € / año

La entrega por TAXII 2.1 / STIX 2.1 está disponible como paquete Enterprise TAXII independiente. La API IOC Lookup está disponible desde 49,99 € al mes. Precios publicados en qfeeds.com/pricing en la fecha de redacción.

PROGRAMA DE PARTNERS

Los resellers y los proveedores de servicios reciben precios de partner, onboarding, formación y materiales de venta, además de acceso directo al equipo de Q-Feeds para pruebas de concepto. La entrega en marca blanca está disponible para los proveedores que quieran ofrecer threat intelligence con su propia marca. Contacte con nosotros para conocer los detalles.

09

Primeros pasos

1. **Regístrese**

   Cree una cuenta gratuita en el Threat Intelligence Portal. La edición Community incluye 7 días de prueba Premium.

2. **Compruébelo en su propia red**

   Conecte un firewall o un SIEM con ayuda de las guías de configuración y mida lo que se bloquea. La herramienta gratuita Testing Tool le ayuda a evaluar su protección actual.

3. **Hágase partner**

   Solicite su incorporación al programa de reseller para obtener una cuenta de reseller, precios de partner y onboarding.

4. **Despliegue**

   Empiece por el refuerzo de firewalls para sus clientes y añada con el tiempo el enriquecimiento del SIEM, los informes de exposición y la protección de marca.

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