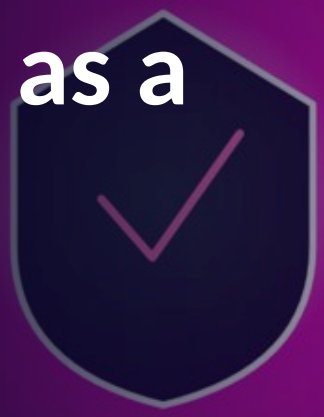
Q-FEEDS

WHITEPAPER · MSP & MSSP

Threat intelligence as a service



Hoe managed service providers geselecteerde threat intelligence omzetten in een schaalbaar, terugkerend securityaanbod voor hun klanten.

qfeeds.com
Versie 2026

MADE IN EUROPE

01

Managementsamenvatting

Kleine en middelgrote organisaties zijn inmiddels een belangrijk doelwit van cybercriminelen, terwijl de meeste geen toegang hebben tot threat intelligence. Managed service providers zijn bij uitstek in de positie om dat gat te dichten: zij beheren al de firewalls, SIEM's en DNS-filters waar intelligence haar werk doet.

Deze whitepaper laat zien hoe MSP's en MSSP's met Q-Feeds geselecteerde threat intelligence toevoegen aan de infrastructuur die zij al beheren, en hoe zij daar diensten van maken die hun klanten begrijpen en waarvoor zij willen betalen: geharde firewalls, verrijkte SIEM-detectie, exposure monitoring en bescherming tegen phishing.

2.500+	20 min	20+	€0
commerciële, OSINT- en overheidsbronnen	update-interval bij Premium	native en gedocumenteerde integraties	om te starten: Community-editie, voor altijd gratis

De belangrijkste punten

- Threat intelligence is een van de weinige beveiligingslagen die u over een volledig klantenbestand kunt uitrollen zonder nieuwe hardware of agents.
- Selectie is belangrijker dan volume. Ongefilterde lijsten veroorzaken false positives, en elke false positive wordt een supportticket.
- Eén leveranciersonafhankelijke feed werkt op Fortinet, Palo Alto, Sophos, Check Point, OPNsense, pfSense, MikroTik en de grote SIEM's. Zo dekt één propositie een gemengde omgeving.
- Licenties op basis van begunstigde gebruikers, actieve apparaten en looptijd houden de prijs voorspelbaar voor dienstverleners en eerlijk voor klanten.

02

De kans voor dienstverleners

Aanvallen op kleine en middelgrote organisaties zijn grotendeels geautomatiseerd. Botnets scannen het hele internet op openstaande VPN's en remote desktops, phishingkits zijn per uur te huur en ransomwaregroepen kiezen hun slachtoffers niet op bedrijfsgrootte. Organisaties met minder dan 500 medewerkers krijgen met dezelfde dreigingen te maken als grote ondernemingen, maar hebben zelden een securityteam dat kan reageren.

Tegelijk nemen regelgeving en klantverwachtingen toe. NIS2 verplicht veel organisaties om passende maatregelen tegen cyberrisico's te nemen, en eisen aan de toeleveringsketen leggen securityvragen ook bij kleinere leveranciers neer. De meeste van deze organisaties kloppen voor het antwoord aan bij hun IT-dienstverlener.

Klanten vragen erom

Vragenlijsten over security, NIS2 en cyberverzekeringen belanden op het bureau van de IT-dienstverlener. Een concrete, uitlegbare maatregel maakt dat gesprek eenvoudiger.

De infrastructuur staat er al

MSP's beheren al firewalls, SIEM's en DNS-filters voor hun klanten. Threat intelligence maakt die bestaande infrastructuur slimmer.

Van nature terugkerend

Threat intelligence is per definitie een abonnement. Het past vanzelf in managed-servicecontracten en maandelijks terugkerende omzet.

03

Waarom threat intelligence op schaal leveren lastig is

Veel dienstverleners hebben geëxperimenteerd met gratis blocklists of met feeds die bij een leverancier zijn inbegrepen. In de praktijk lopen zij tegen dezelfde problemen aan:

Uitdaging	Wat het betekent voor een MSP
Ruis en ongevalideerde lijsten	Gratis lijsten bevatten vaak verouderde vermeldingen en legitieme infrastructuur, zoals gedeelde cloud- of CDN-adressen. Wie die blokkeert, legt applicaties plat en krijgt tickets.
Verouderde data	Lijsten die één keer per dag worden bijgewerkt, missen kortlevende phishing- en command-and-control-infrastructuur die soms maar een paar uur actief is.
Vendor lock-in	Feeds van een leverancier werken alleen op de apparaten van die leverancier. Een dienstverlener met een gemengde omgeving krijgt dan per klant andere intelligence, een andere kwaliteit en een andere prijs.
Enterpriseprijzen	Commerciële threat intelligence platforms zijn doorgaans geprijsd voor grote ondernemingen en SOC-teams, niet voor een klant met 40 medewerkers achter één firewall.
Operationele overhead	Een eigen pipeline voor verzamelen, ontdubbelen en valideren bouwen en onderhouden kost engineeringtijd die de meeste dienstverleners niet hebben.

DE KERN

Voor een dienstverlener zit de waarde van threat intelligence niet in het aantal indicatoren, maar in **hoe weinig false positives de klant bereiken** en hoe weinig werk het kost om honderden apparaten actueel te houden.

04

Wat Q-Feeds levert

Q-Feeds brengt intelligence uit meer dan 2.500 commerciële, open-source- en overheidsbronnen, waaronder ons eigen honeypotnetwerk, samen in één geselecteerde set. Elke dataset doorloopt hetzelfde proces voordat deze wordt gepubliceerd:

1. **Verzamelen**
   Doorlopende verzameling bij commerciële aanbieders, OSINT-projecten, overheidsbronnen en honeypots.
2. **Opschonen**
   Normaliseren en ontdubbelen, en verwijderen van indicatoren die niet meer actief zijn.
3. **Valideren**
   Validatie op false positives, zodat legitieme diensten en gedeelde infrastructuur buiten de lijst blijven.
4. **Verrijken**
   Priority scoring, categorisering en MITRE ATT&CK-mapping voor context.
5. **Leveren**
   Gepubliceerd als kant-en-klare feeds, via TAXII 2.1 en via de API, bij Premium elke 20 minuten ververst.

Eén platform, meerdere bouwstenen

Onderdeel	Wat het doet
Threat intelligence feeds	Geselecteerde feeds met kwaadaardige IP-adressen, domeinen en URL's voor firewalls, DNS-filters, proxy's en SIEM's.
Threat Lookup & IOC Lookup API	Direct context bij elk IP-adres, domein, URL of filehash: malicious score, bronnen en MITRE ATT&CK-mapping. Beschikbaar in het portal en als API voor SOAR- en ticketingworkflows.
TAXII 2.1-server	Op standaarden gebaseerde STIX 2.1-collecties voor SIEM's, threat intelligence platforms en SOAR-tools.
Dark web monitoring	Geplande zoekopdrachten naar gelekte inloggegevens en gelekte data die aan klantdomeinen zijn gekoppeld.
Attack surface & vulnerability scanning	In kaart brengen van assets die vanaf internet bereikbaar zijn, open poorten en kwetsbaarheden in netwerk en web, op aanvraag of volgens schema.

Onderdeel	Wat het doet
CVE alerts	Een doorzoekbare CVE-catalogus met CVSS- en EPSS-score en CISA KEV-status, plus een dagelijks of wekelijks overzicht per e-mail van nieuwe CVE's in de software die u in het portal opgeeft.
Brand protection	Detectie van lookalike-domeinen, typosquatting en phishingpagina's, met takedown-verzoeken.

05

Diensten die u kunt bouwen

Hetzelfde platform ondersteunt meerdere dienstproposities. De meeste dienstverleners beginnen met firewall hardening en voegen de andere diensten toe naarmate hun klanten daaraan toe zijn.

Managed firewall hardening

Voeg geselecteerde IP-, domein- en URL-feeds toe aan de firewalls die u al beheert. Bekend kwaadaardig verkeer wordt automatisch geblokkeerd, zowel inkomend als uitgaand. **Resultaat voor de klant:** minder geslaagde phishingklikken, geblokkeerd command-and-control-verkeer en minder ruis van scanners.

Verrijking van SIEM en SOC

Voed Splunk, Microsoft Sentinel, Wazuh of een andere SIEM met TAXII-ondersteuning met geselecteerde IOC's en MITRE ATT&CK-context. **Resultaat:** minder valse alerts, snellere triage en beter gedocumenteerde incidenten.

Exposure- en dark web-rapportage

Gebruik de vulnerability scanner, de attack surface-tools, CVE alerts en dark web monitoring om periodiek een exposure-rapport te leveren. **Resultaat:** een tastbaar, terugkerend product dat de waarde van uw dienst laat zien.

Phishing en brand protection

Monitor lookalike-domeinen en phishing die uw klant imiteren, en vraag takedowns aan. **Resultaat:** bescherming van de klanten en de reputatie van uw klant.

DETECTIE ALS BIJVANGST

Wanneer een firewall uitgaand verkeer naar een bekende command-and-control-server blokkeert, laat de logregel zien welk intern apparaat verbinding probeerde te maken. Voor een MSP is elke blokkade van dit type een vroege waarschuwing dat een apparaat van de klant mogelijk geïnfecteerd is, vaak nog voordat een andere tool alarm slaat.

06

Eén feed voor een gemengde omgeving

Dienstverleners beheren zelden maar één merk. Q-Feeds is leveranciersonafhankelijk en wordt via open mechanismen geleverd. Daardoor werken dezelfde geselecteerde intelligence en dezelfde propositie voor het hele klantenbestand.

Categorie	Ondersteunde platforms
Firewalls	Fortinet FortiGate, Palo Alto Networks, Sophos XGS, Check Point, SonicWall, OPNsense (native plugin), pfSense, MikroTik RouterOS, Linux nftables / iptables
SIEM	Splunk, Microsoft Sentinel, Wazuh, Exabeam en andere SIEM's via TAXII 2.1, feeds of API (bijv. IBM QRadar, Elastic Security, LogRhythm, Google SecOps)
Threat intelligence platforms	OpenCTI, MISP, EclecticIQ, Anomali ThreatStream, ThreatConnect
DNS-filtering	Pi-hole, AdGuard Home, Technitium DNS
Ontwikkelaars	IOC Lookup API, TAXII 2.1-server, open-source integratiescripts

Stapsgewijze installatiegidsen voor elk platform vindt u in de Q-Feeds-kennisbank en als pdf-handleiding. Zie de bijbehorende whitepaper **Q-Feeds integreren** voor de technische details.

07

Werken op schaal

Beheer van meerdere klanten

Partners beheren hun klanten vanuit een reselleraccount in het Threat Intelligence Portal. Licenties die de partner aanschaft, worden aan dat account gekoppeld en kunnen aan afzonderlijke eindklanten worden toegewezen, elk met eigen gebruikers. De partner houdt de klantrelatie; Q-Feeds zorgt voor de intelligence.

Instellen en klaar

- Apparaten pollen hun feed-URL's automatisch; er zijn geen lijsten die u handmatig moet bijhouden.
- Stem het polling-interval af op de licentie: elke 24 uur bij Community, elke 4 uur bij Plus, elke 20 minuten bij Premium.
- Gebruik de limit-parameter om de lijstgrootte af te stemmen op de capaciteit van kleinere apparaten.
- Plaats de blokkeerregels boven de allow-regels en schakel logging in, zodat blokkades zichtbaar worden en u erover kunt rapporteren.

Omgaan met false positives

Dankzij validatie komen false positives zelden voor. Wordt er toch een legitiem adres geblokkeerd, dan kan de dienstverlener een tijdelijke uitzondering op het apparaat instellen en de indicator bij Q-Feeds melden. Q-Feeds beoordeelt de melding, stelt vast of het om een false positive gaat en past de feed waar nodig aan. Zo profiteert elke klant van de correctie.

08

Licenties die passen bij het verdienmodel van dienstverleners

De licenties van Q-Feeds zijn gebaseerd op drie elementen: het aantal **begunstigde gebruikers** (de mensen die daadwerkelijk worden beschermd, niet het totale personeelsbestand), het aantal **actieve apparaten** en de **looptijd** (1, 2 of 3 jaar). Dat houdt het betaalbaar voor kleine klanten en maakt de omvang voorspelbaar.

Opstelling	Apparaatlicenties
Eén firewall	1
Twee losse firewalls	2
Active-passive-cluster	1 (het stand-by apparaat telt niet mee)
Active-active-cluster	2

Categorieën voor begunstigde gebruikers: Small (< 50), Medium (50 tot 250), Large (250 tot 1.000) en Enterprise (1.000+). Voor Plus en Premium geldt dezelfde structuur; het verschil zit in de functionaliteit.

	Community	Plus	Premium
Feed-updates	Elke 24 uur	Elke 4 uur	Elke 20 minuten
Kwaadaardige IP-feed	OSINT	OSINT + premium IP-data	OSINT + premium IP-data
Kwaadaardige domeinfeed	OSINT	OSINT	OSINT + premium DNS-data
Kwaadaardige URL-feed	–	–	Inbegrepen (proxy / webfilter)
Dark web monitoring	–	Inbegrepen	Inbegrepen
Threat Lookup	–	Inbegrepen	Inbegrepen
Vulnerability scanner	–	1 scan per week per IP	1 scan per dag per asset, incl. webapps
CVE-catalogus	Inbegrepen	Inbegrepen	Inbegrepen
CVE alerts	–	Inbegrepen	Inbegrepen
Brand protection	–	–	Inbegrepen, met takedown-verzoeken
Prijs	Gratis voor altijd	Vanaf €99 / jaar	Vanaf €249 / jaar

Levering via TAXII 2.1 / STIX 2.1 is beschikbaar als apart Enterprise TAXII-pakket. De IOC Lookup API is beschikbaar vanaf €49,99 per maand. Prijzen zoals vermeld op qfeeds.com/pricing op het moment van schrijven.

PARTNERPROGRAMMA

Resellers en dienstverleners krijgen partnerprijzen, onboarding, training en salesmateriaal, plus rechtstreeks contact met het Q-Feeds-team voor proofs of concept. White-labellevering is mogelijk voor dienstverleners die threat intelligence onder hun eigen merk willen aanbieden. Neem contact met ons op voor de details.

09

Aan de slag

1. **Registreer**

   Maak een gratis account aan in het Threat Intelligence Portal. De Community-editie bevat 7 dagen gratis Premium.

2. **Bewijs het in uw eigen netwerk**

   Koppel één firewall of SIEM met behulp van de installatiegidsen en meet wat er wordt geblokkeerd. Met de gratis Testing Tool benchmarkt u uw huidige bescherming.

3. **Word partner**

   Meld u aan voor het resellerprogramma en ontvang een reselleraccount, partnerprijzen en onboarding.

4. **Uitrollen**

   Begin met firewall hardening voor uw klanten en breid in de loop van de tijd uit met SIEM-verrijking, exposure-rapportage en brand protection.

Probeer Q-Feeds vandaag nog

Maak een gratis account aan in het Threat Intelligence Portal op tip.qfeeds.com. De Community-editie is voor altijd gratis en bevat 7 dagen gratis Premium, zonder creditcard. Neem contact op met ons team voor partnerprogramma's, volumelicenties of een demo onder begeleiding.

MADE IN EUROPE

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