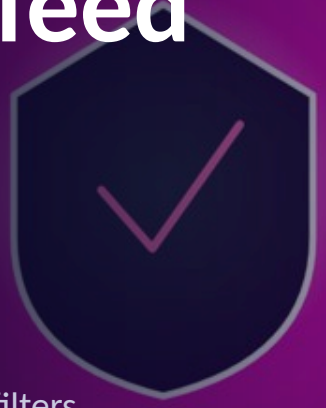
Q-FEEDS

WHITEPAPER · INTEGRATIES

Eén geselecteerde feed voor uw hele securitystack



Hoe de threat intelligence van Q-Feeds integreert met firewalls, SIEM's, threat intelligence platforms en DNS-filters, en hoe u er het meeste uit haalt.

qfeeds.com
Versie 2026

MADE IN EUROPE

01

Inleiding

Threat intelligence levert pas waarde op als die ook wordt afgedwongen. Q-Feeds is ontworpen om aan te sluiten op de securitytools die u al gebruikt, via hun eigen mechanismen. Zo bereikt geselecteerde intelligence binnen enkele minuten de rand van uw netwerk, uw SIEM en uw analisten.

Deze whitepaper beschrijft de leveringsmethoden van Q-Feeds, welke feeds bij welke licentie beschikbaar zijn, hoe elk groot platform de intelligence verwerkt en met welke best practices een integratie betrouwbaar blijft. Uitgebreide stapsgewijze handleidingen voor elk platform vindt u in de kennisbank op qfeeds.com.

20+	3	TAXII 2.1	5 min
gedocumenteerde integraties	feedtypen: IP, domein, URL	levering op basis van standaarden	gemiddelde tijd tot de eerste feed

02

Leveringsmethoden

Q-Feeds biedt vijf manieren om de intelligence af te nemen. De meeste integraties gebruiken de eerste; de andere zijn bedoeld voor SIEM's, threat intelligence platforms en eigen tooling.

Methode	Hoe het werkt	Meest geschikt voor
HTTPS-feed-URL's	Uw apparaat haalt periodiek een lijst op via HTTPS: standaard platte tekst, op verzoek CSV. Met een limit-parameter begrenst u de lijstgrootte voor apparaten met een maximum.	Firewalls, DNS-filters, proxy's
Native plugin	Een Q-Feeds-plugin in de officiële OPNsense-repository maakt firewall-aliassen en DNS-blocklists automatisch aan en houdt ze bij.	OPNsense
TAXII 2.1 / STIX 2.1	Een TAXII 2.1-server met STIX 2.1-collecties, inclusief categorie, MITRE ATT&CK-mapping en filehashes. Clients halen alleen op wat nieuw is sinds de vorige poll.	SIEM's, TIP's, SOAR

Methode	Hoe het werkt	Meest geschikt voor
IOC Lookup API	Vraag één IP-adres, domein, URL of hash op en ontvang dezelfde context als in Threat Lookup: score, bronnen en MITRE ATT&CK-mapping.	Verrijking van alerts, SOAR, ticketing
Open-sourcescripts	Onderhouden installers en scripts voor platforms zonder native feedondersteuning, gepubliceerd op GitHub.	MikroTik, Linux-hosts, Wazuh

03

Feeds en beschikbaarheid per licentie

Feed	Inhoud	Beschikbaar bij
malware_ip	Kwaadaardige IP-adressen (IPv4 en IPv6): botnets, command-and-control-servers, scanners en malwarehosting.	Community, Plus, Premium
malware_domains	Kwaadaardige domeinen die worden gebruikt voor phishing, malwareverspreiding en command-and-control.	Community, Plus, Premium
malicious_urls	Specifieke kwaadaardige URL's, zoals phishingpagina's en malwaredownloads.	Premium
TAXII-collecties	STIX 2.1-indicatoren voor IP-adressen, domeinen, URL's en filehashes, met categorie, MITRE ATT&CK-mapping en context.	Enterprise TAXII-pakket

Licentie	Verversing van de feed	Aanbevolen polling-interval
Community	Elke 24 uur	Eén keer per dag
Plus	Elke 4 uur	Elke 4 uur
Premium	Elke 20 minuten	Elke 20 minuten

URL-FEEDS VRAGEN OM EEN APPARAAT DAT URL'S KAN ZIEN

Een packetfilter dat op IP-adressen matcht, of een DNS-filter dat op domeinnamen matcht, kan geen URL-lijst afdwingen. Voor kwaadaardige URL-feeds is een proxy of webfilter nodig, en voor HTTPS-verkeer heeft dat apparaat **TLS-inspectie** nodig; anders ziet het alleen de hostnaam.

04

Authenticatie

Alle toegang verloopt via een persoonlijke API-key, die u aanmaakt onder Manage API Keys in het Threat Intelligence Portal.

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

- **Feeds:** de meeste apparaten gebruiken HTTP Basic-authenticatie, met api_token als gebruikersnaam en uw key als wachtwoord. Apparaten die geen Basic-authenticatie ondersteunen, kunnen de key als URL-parameter meegeven.
- **IOC Lookup API en TAXII:** stuur de key mee als Bearer-token in de Authorization-header.
- Behandel de key als een geheim: iedereen die de key heeft, kan uw feeds ophalen.

05

Firewalls

Firewalls dwingen de intelligence van Q-Feeds af aan de rand van het netwerk en blokkeren inkomend en uitgaand verkeer naar bekende kwaadaardige infrastructuur, voordat het gebruikers of servers bereikt. Elke integratie gebruikt het eigen mechanisme van de leverancier, dus er is geen extra appliance of agent nodig.

Platform	Integratiemechanisme	Feeds
Fortinet FortiGate	Native External Connectors (threat feeds), afgedwongen in firewall-, DNS-filter- en webfilterpolicy's.	IP, domein, URL
Palo Alto Networks	Native External Dynamic Lists (EDL's), afgedwongen in Security policy rules. Werkt ook in omgevingen die met Panorama worden beheerd.	IP, domein, URL
Sophos Firewall (XGS)	Third-party threat feeds, afgedwongen in firewallregels en webpolicy's, naast de beveiliging van Sophos zelf.	IP, domein, URL
Check Point	Native Custom Intelligence Feeds, afgedwongen via de Anti-Bot en Anti-Virus Software Blades.	IP, domein
OPNsense	Native Q-Feeds-plugin uit de officiële repository (meegeleverd met OPNsense 26.1): firewall-aliassen, plus domeinblokkering via Unbound DNS of DNSCrypt-Proxy.	IP, domein
pfSense	pfBlockerNG-pakket: IP-feeds als firewall-aliassen, domeinfeeds via DNSBL.	IP, domein

Platform	Integratiemechanisme	Feeds
SonicWall	Dynamic Botnet List Server met Botnet-filtering op access rules (SonicOS 6.5.2+ voor geauthenticeerde downloads).	IP
MikroTik RouterOS	Open-source RouterOS-scripts: volledige import plus differentiële updates naar een firewall address-list, met automatische rollback als een download mislukt.	IP
Linux nftables / iptables	Open-source installer die de blocklist in aparte sets laadt en updates inplant.	IP

EEN AANVULLING OP DE INTELLIGENCE VAN UW LEVERANCIER

Q-Feeds draait naast abonnementen op FortiGuard, WildFire, ThreatCloud of Sophos X-Ops. Het voegt onafhankelijke intelligence uit meerdere bronnen toe en geeft dienstverleners één consistente feed voor verschillende merken.

06

SIEM-platforms

In een SIEM worden de indicatoren van Q-Feeds gecorreleerd met logdata. Activiteit waarbij bekende kwaadaardige IP-adressen, domeinen, URL's of hashes betrokken zijn, komt zo naar boven als een geprioriteerde alert met MITRE ATT&CK-context.

Platform	Integratiemechanisme
Splunk	Indicatoren worden ingelezen als lookups of in het threat intelligence framework van Splunk Enterprise Security, klaar voor correlation searches. TAXII/STIX 2.1 is beschikbaar voor ingestie.
Microsoft Sentinel	Native Threat Intelligence-dataconnector via TAXII/STIX 2.1. Indicatoren komen in de tabel ThreatIntelligenceIndicator terecht, voor analytics rules, hunting queries en workbooks.
Wazuh	Open-source installer voor Wazuh 4.x: CDB-lijsten plus decoders en rules die bij een match een alert genereren. Optioneel automatisch blokkeren met Active Response. Werkt met de standaard-API of met TAXII.

Platform	Integratiemechanisme
Exabeam	Custom context table die via de Exabeam Context Management API (CSV) met Q-Feeds-indicatoren wordt gevuld en automatisch wordt ververst.
Andere SIEM's	IBM QRadar, Elastic Security, LogRhythm, Google SecOps en andere platforms via TAXII 2.1, feeds of de API.

Voor levering via TAXII is het Enterprise TAXII-pakket nodig.

07

Threat intelligence platforms

Voor analistenteams is Q-Feeds een betrouwbare, zorgvuldig geselecteerde basislaag. Indicatoren behouden hun Q-Feeds-bronvermelding, zodat u ze kunt filteren, erover kunt rapporteren en ze kunt verwijderen zonder de rest van uw kennis te raken.

Platform	Integratiemechanisme	Licentie
OpenCTI	Ingebouwde TAXII-ingestie: niets om te bouwen of te onderhouden. Bij andere licenties kunnen IP- en domeinlijsten als feed worden ingelezen.	Enterprise TAXII (feeds bij alle pakketten)
MISP	Native MISP-feeds: verwijs MISP naar de volledige lijsten en stel het ophaalschema in.	Alle pakketten (URL's bij Premium)
EclecticIQ	Standaard incoming TAXII-feed; indicatoren worden entiteiten in de workspace van uw keuze.	Enterprise TAXII
Anomali ThreatStream	Standaardconfiguratie voor een TAXII-feed; indicatoren houden hun eigen bronlabel.	Enterprise TAXII
ThreatConnect	De eigen TAXII-app van ThreatConnect uit de catalogus; elke collectie wordt een eigen bron.	Enterprise TAXII

08

DNS-filtering

DNS-filters blokkeren kwaadaardige domeinen al bij de naamresolutie, nog voordat er een verbinding tot stand komt. Pi-hole, AdGuard Home en Technitium DNS abonneren zich rechtstreeks op de malware-domeinenlijst van Q-Feeds. Dat maakt dit een effectieve optie voor kleine kantoren, nevenvestigingen en thuisnetwerken.

09

Best practices

Aanbeveling	Waarom het ertoe doet
Stem polling af op uw licentie	Vaker pollen dan de feed wordt ververst, geeft extra belasting maar geen extra bescherming. Minder vaak pollen betekent dat u bescherming laat liggen.
Houd rekening met apparaatlimieten	Veel firewalls hebben een maximale lijstgrootte. Gebruik de limit-parameter om daarbinnen te blijven, zeker bij kleinere of oudere modellen.
Blokkeer in beide richtingen	Inkomende blokkades stoppen scanners en brute-force-pogingen; uitgaande blokkades stoppen phishingklikken en malware die contact zoekt met de aanvaller.
Zet blokkeerregels bovenaan	Plaats de Q-Feeds-regels boven de allow-regels. Anders kan verkeer al zijn toegestaan voordat de lijst wordt geëvalueerd.
Schakel logging in	Gelogde blokkades maken de waarde van de intelligence zichtbaar en wijzen op mogelijk geïnfecteerde interne apparaten.
Houd rekening met high availability	Een active-passive-cluster heeft één apparaatlicentie nodig; een active-active-cluster één per apparaat.
Test uw configuratie	Gebruik de gratis Q-Feeds Testing Tool om te controleren of de integratie werkt en om uw bescherming te benchmarken.

10

Aan de slag

1. **Maak een account aan**

   Registreer u in het Threat Intelligence Portal en activeer de gratis Community-editie, inclusief 7 dagen gratis Premium.

2. **Maak een API-key aan**

   Ga in het portal naar Manage API Keys en maak uw key aan.

3. **Stel uw feed-URL samen**

   Kies het feedtype en, indien nodig, een limiet en een uitvoerformaat.

4. **Volg de installatiegids**

   Gebruik de stapsgewijze gids voor uw platform in de kennisbank of de pdf-handleidingen op de downloadpagina.

5. **Controleer**

   Controleer of de lijst gevuld is, de blokkeerregels actief zijn en blokkades in de logs verschijnen.

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