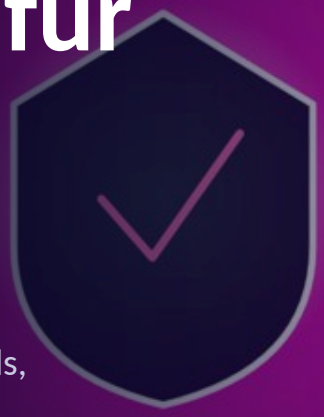
Q-FEEDS

WHITEPAPER · INTEGRATIONEN

Ein geprüfter Feed für Ihren gesamten Security-Stack



Wie sich die Threat Intelligence von Q-Feeds in Firewalls, SIEMs, Threat-Intelligence-Plattformen und DNS-Filter einbinden lässt und wie Sie das Beste daraus machen.

qfeeds.com
Version 2026

MADE IN EUROPE

01

Einleitung

Threat Intelligence schafft erst dann Mehrwert, wenn sie auch durchgesetzt wird. Q-Feeds ist dafür gemacht, sich über die nativen Mechanismen in die Security-Tools einzufügen, die Sie bereits betreiben. So erreicht geprüfte Intelligence innerhalb von Minuten den Rand Ihres Netzwerks, Ihr SIEM und Ihre Analysten.

Dieses Whitepaper beschreibt die Auslieferungswege von Q-Feeds, welche Feeds mit welcher Lizenz verfügbar sind, wie die wichtigsten Plattformen die Intelligence verarbeiten und mit welchen Best Practices eine Integration zuverlässig bleibt. Ausführliche Schritt-für-Schritt-Anleitungen für jede Plattform finden Sie in der Wissensdatenbank auf qfeeds.com.

20+	3	TAXII 2.1	5 min
dokumentierte Integrationen	Feed-Typen: IP, Domain, URL	standardbasierte Auslieferung	typische Zeit bis zum ersten Feed

02

Auslieferungswege

Q-Feeds bietet fünf Wege, die Intelligence zu beziehen. Die meisten Integrationen nutzen den ersten; die übrigen sind für SIEMs, Threat-Intelligence-Plattformen und eigene Tools gedacht.

Methode	So funktioniert es	Geeignet für
HTTPS-Feed-URLs	Ihr Gerät ruft regelmäßig eine Liste per HTTPS ab: standardmäßig als Klartext, auf Wunsch als CSV. Ein limit-Parameter begrenzt die Listengröße für Geräte mit einer Obergrenze.	Firewalls, DNS-Filter, Proxys
Natives Plugin	Ein Q-Feeds-Plugin im offiziellen OPNsense-Repository legt Firewall-Aliase und DNS-Blocklisten automatisch an und hält sie aktuell.	OPNsense
TAXII 2.1 / STIX 2.1	Ein TAXII-2.1-Server mit STIX-2.1-Collections, inklusive Kategorie, MITRE-ATT&CK-Zuordnung und Datei-Hashes. Clients rufen nur ab, was seit dem letzten Poll neu ist.	SIEMs, TIPs, SOAR

Methode	So funktioniert es	Geeignet für
IOC Lookup API	Fragen Sie eine einzelne IP, Domain, URL oder einen Hash ab und erhalten Sie denselben Kontext wie in Threat Lookup: Score, Quellen und MITRE-ATT&CK-Zuordnung.	Alert-Anreicherung, SOAR, Ticketing
Open-Source-Skripte	Gepflegte Installer und Skripte für Plattformen ohne native Feed-Unterstützung, veröffentlicht auf GitHub.	MikroTik, Linux-Hosts, Wazuh

03

Feeds und Verfügbarkeit je Lizenz

Feed	Inhalt	Verfügbar in
malware_ip	Schädliche IP-Adressen (IPv4 und IPv6): Botnets, Command-and-Control-Server, Scanner und Malware-Hosting.	Community, Plus, Premium
malware_domains	Schädliche Domains, die für Phishing, die Verbreitung von Malware und Command-and-Control genutzt werden.	Community, Plus, Premium
malicious_urls	Konkrete schädliche URLs wie Phishing-Seiten und Malware-Downloads.	Premium
TAXII-Collections	STIX-2.1-Indikatoren für IPs, Domains, URLs und Datei-Hashes, mit Kategorie, MITRE-ATT&CK-Zuordnung und Kontext.	Enterprise-TAXII-Paket

Lizenz	Feed-Aktualisierung	Empfohlenes Polling-Intervall
Community	Alle 24 Stunden	Einmal täglich
Plus	Alle 4 Stunden	Alle 4 Stunden
Premium	Alle 20 Minuten	Alle 20 Minuten

URL-FEEDS BRAUCHEN EIN GERÄT, DAS URLS SEHEN KANN

Ein Paketfilter, der IP-Adressen abgleicht, oder ein DNS-Filter, der Domainnamen abgleicht, kann keine URL-Liste durchsetzen. Für Feeds mit schädlichen URLs ist ein Proxy oder Web-Filter erforderlich, und bei HTTPS-Verkehr benötigt dieses Gerät **TLS-Inspektion**; andernfalls sieht es nur den Hostnamen.

04

Authentifizierung

Jeder Zugriff erfolgt über einen persönlichen API-Key, den Sie im Threat Intelligence Portal unter Manage API Keys erstellen.

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

- **Feeds:** Die meisten Geräte nutzen HTTP-Basic-Authentifizierung, mit api_token als Benutzername und Ihrem Key als Passwort. Geräte ohne Basic-Authentifizierung können den Key als URL-Parameter übergeben.
- **IOC Lookup API und TAXII:** Senden Sie den Key als Bearer-Token im Authorization-Header.
- Behandeln Sie den Key wie ein Geheimnis: Wer ihn hat, kann Ihre Feeds abrufen.

05

Firewalls

Firewalls setzen die Intelligence von Q-Feeds am Netzwerkrand durch. Sie blockieren ein- und ausgehenden Verkehr zu bekannter schädlicher Infrastruktur, bevor er Nutzer oder Server erreicht. Jede Integration nutzt den herstellereigenen Mechanismus, sodass weder eine zusätzliche Appliance noch ein Agent nötig ist.

Plattform	Integrationsmechanismus	Feeds
Fortinet FortiGate	Native External Connectors (Threat Feeds), durchgesetzt in Firewall-, DNS-Filter- und Web-Filter-Richtlinien.	IP, Domain, URL
Palo Alto Networks	Native External Dynamic Lists (EDLs), durchgesetzt in Security-Policy-Regeln. Funktioniert auch in Umgebungen, die über Panorama verwaltet werden.	IP, Domain, URL
Sophos Firewall (XGS)	Third-Party Threat Feeds, durchgesetzt in Firewall-Regeln und Web-Richtlinien, ergänzend zu den Schutzfunktionen von Sophos.	IP, Domain, URL
Check Point	Native Custom Intelligence Feeds, durchgesetzt über die Software Blades Anti-Bot und Anti-Virus.	IP, Domain
OPNsense	Natives Q-Feeds-Plugin aus dem offiziellen Repository (in OPNsense 26.1 enthalten): Firewall-Aliase sowie Domain-Blocking über Unbound DNS oder DNSCrypt-Proxy.	IP, Domain
pfSense	pfBlockerNG-Paket: IP-Feeds als Firewall-Aliase, Domain-Feeds über DNSBL.	IP, Domain

Plattform	Integrationsmechanismus	Feeds
SonicWall	Dynamic Botnet List Server mit Botnet-Filterung in den Access Rules (SonicOS 6.5.2+ für authentifizierte Downloads).	IP
MikroTik RouterOS	Open-Source-Skripte für RouterOS: Vollimport plus differenzielle Updates in eine Firewall-Address-List, mit automatischem Rollback, falls ein Download fehlschlägt.	IP
Linux nftables / iptables	Open-Source-Installer, der die Blockliste in eigene Sets lädt und Updates einplant.	IP

ERGÄNZUNG ZUR INTELLIGENCE IHRES HERSTELLERS

Q-Feeds läuft parallel zu Abonnements von FortiGuard, WildFire, ThreatCloud oder Sophos X-Ops. Es ergänzt sie um unabhängige Intelligence aus vielen Quellen und gibt Dienstleistern einen einheitlichen Feed über verschiedene Marken hinweg.

06

SIEM-Plattformen

Im SIEM werden die Indikatoren von Q-Feeds mit Logdaten korreliert. Aktivitäten mit bekannten schädlichen IPs, Domains, URLs oder Hashes erscheinen so als priorisierter Alert mit MITRE-ATT&CK-Kontext.

Plattform	Integrationsmechanismus
Splunk	Indikatoren werden als Lookups oder in das Threat Intelligence Framework von Splunk Enterprise Security übernommen und stehen für Correlation Searches bereit. TAXII/STIX 2.1 ist für den Import verfügbar.
Microsoft Sentinel	Nativer Threat-Intelligence-Datenconnector über TAXII/STIX 2.1. Die Indikatoren landen in der Tabelle ThreatIntelligenceIndicator und stehen für Analytics Rules, Hunting Queries und Workbooks bereit.
Wazuh	Open-Source-Installer für Wazuh 4.x: CDB-Listen sowie Decoder und Regeln, die bei Treffern Alerts auslösen. Optional automatisches Blockieren mit Active Response. Funktioniert mit der Standard-API oder mit TAXII.

Plattform	Integrationsmechanismus
Exabeam	Custom Context Table, die über die Exabeam Context Management API (CSV) mit Q-Feeds-Indikatoren befüllt und automatisch aktualisiert wird.
Weitere SIEMs	IBM QRadar, Elastic Security, LogRhythm, Google SecOps und weitere Plattformen über TAXII 2.1, Feeds oder die API.

Für die Auslieferung über TAXII ist das Enterprise-TAXII-Paket erforderlich.

07

Threat-Intelligence-Plattformen

Für Analystenteams ist Q-Feeds eine verlässliche, geprüfte Basisschicht. Die Indikatoren behalten ihre Quellenangabe Q-Feeds. So können Sie sie filtern, auswerten und entfernen, ohne Ihr übriges Wissen anzutasten.

Plattform	Integrationsmechanismus	Lizenz
OpenCTI	Integrierter TAXII-Import, nichts zu entwickeln oder zu pflegen. Mit anderen Lizenzen lassen sich IP- und Domain-Listen als Feed importieren.	Enterprise TAXII (Feeds in allen Paketen)
MISP	Native MISP-Feeds: MISP auf die vollständigen Listen verweisen und den Abrufplan festlegen.	Alle Pakete (URLs bei Premium)
EclecticIQ	Standardmäßiger Incoming Feed über TAXII; Indikatoren werden zu Entitäten im Workspace Ihrer Wahl.	Enterprise TAXII
Anomali ThreatStream	Standard-Einrichtung eines TAXII-Feeds; Indikatoren behalten ihr eigenes Quellen-Label.	Enterprise TAXII
ThreatConnect	Die TAXII-App von ThreatConnect aus dem eigenen Katalog; jede Collection wird zu einer eigenen Quelle.	Enterprise TAXII

08

DNS-Filterung

DNS-Filter blockieren schädliche Domains bereits bei der Namensauflösung, noch bevor eine Verbindung zustande kommt. Pi-hole, AdGuard Home und Technitium DNS abonnieren die Malware-Domain-Liste von Q-Feeds direkt. Das macht diesen Weg zu einer wirksamen Option für kleine Büros, Zweigstellen und Heimnetzwerke.

09

Best Practices

Empfehlung	Warum das wichtig ist
Polling an die Lizenz anpassen	Wer häufiger pollt, als der Feed aktualisiert wird, erzeugt Last, aber keinen zusätzlichen Schutz. Wer seltener pollt, verschenkt Schutz.
Gerätelimits beachten	Viele Firewalls haben eine maximale Listengröße. Mit dem limit-Parameter bleiben Sie darunter, besonders bei kleineren oder älteren Modellen.
In beide Richtungen blockieren	Eingehende Blockierungen stoppen Scanner und Brute-Force-Versuche; ausgehende stoppen Klicks auf Phishing-Links und Malware, die nach Hause telefoniert.
Blockierregeln zuerst	Platzieren Sie die Q-Feeds-Regeln oberhalb der Allow-Regeln. Sonst wird Verkehr möglicherweise zugelassen, bevor die Liste ausgewertet wird.
Logging aktivieren	Protokollierte Blockierungen machen den Wert der Intelligence sichtbar und weisen auf möglicherweise infizierte interne Geräte hin.
Hochverfügbarkeit einplanen	Ein Active-Passive-Cluster benötigt eine Gerätelizenz, ein Active-Active-Cluster eine pro Gerät.
Einrichtung testen	Prüfen Sie mit dem kostenlosen Q-Feeds Testing Tool, ob die Integration funktioniert, und messen Sie Ihren Schutz.

10

Erste Schritte

1. **Konto erstellen**

   Registrieren Sie sich im Threat Intelligence Portal und aktivieren Sie die kostenlose Community Edition, inklusive 7-tägiger Premium-Testphase.

2. **API-Key erstellen**

   Öffnen Sie im Portal den Bereich Manage API Keys und erstellen Sie Ihren Key.

3. **Feed-URL zusammenstellen**

   Wählen Sie den Feed-Typ und bei Bedarf ein Limit und ein Ausgabeformat.

4. **Der Einrichtungsanleitung folgen**

   Nutzen Sie die Schritt-für-Schritt-Anleitung für Ihre Plattform in der Wissensdatenbank oder die PDF-Anleitungen auf der Download-Seite.

5. **Prüfen**

   Kontrollieren Sie, ob die Liste befüllt ist, die Blockierregeln aktiv sind und Blockierungen in den Logs erscheinen.

Q-Feeds jetzt testen

Erstellen Sie ein kostenloses Konto im Threat Intelligence Portal unter tip.qfeeds.com. Die Community Edition ist dauerhaft kostenlos und enthält eine 7-tägige Premium-Testphase, ganz ohne Kreditkarte. Für Partnerprogramme, Volumenlizenzen oder eine geführte Demo wenden Sie sich an unser Team.

MADE IN EUROPE

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