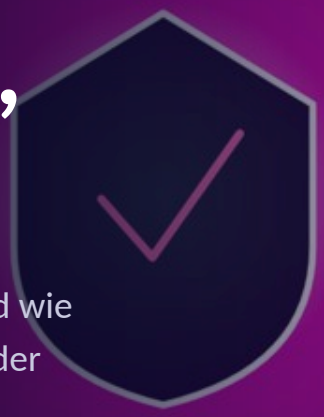
Q-FEEDS

WHITEPAPER · ÜBER Q-FEEDS

Threat Intelligence, für alle zugänglich



Wer wir sind, warum wir Q-Feeds gegründet haben und wie wir Intelligence aufbereiten, mit der Organisationen jeder Größe arbeiten können.

qfeeds.com
Version 2026

MADE IN EUROPE

01

Wer wir sind

Q-Feeds ist ein europäisches Unternehmen für Cyber Threat Intelligence mit Sitz in Hilversum in den Niederlanden. Wir führen Intelligence aus über 2.500 Quellen zu einem verlässlichen Datenbestand zusammen und liefern ihn an Firewalls, SIEMs, DNS-Filter und Security-Teams auf der ganzen Welt.

Q-Feeds wurde 2024 gegründet und arbeitet für Managed Service Provider, Reseller und interne Security-Teams, die verlässliche, direkt nutzbare Intelligence suchen, ohne Enterprise-Preise und ohne langwierige Integrationsprojekte. Unsere Plattform reicht von Blocklisten-Feeds für eine einzelne Firewall bis zu TAXII-Collections für Threat-Intelligence-Plattformen und umfasst außerdem Dark-Web-Monitoring, Attack-Surface-Scans, CVE-Alerts und Brand Protection.

2.500+	20 min	20+	2024
Intelligence-Quellen	Update-Intervall bei Premium	unterstützte Integrationen	gegründet in den Niederlanden

02

Unsere Mission

Threat Intelligence sollte allen offenstehen.

Cybersecurity-Unternehmen sind im Kern Datenverarbeiter: Wer etwas blockieren will, muss zuerst wissen, was. Hochwertige Threat Intelligence war jahrelang großen Konzernen mit eigenen Security-Teams und entsprechenden Budgets vorbehalten.

Gleichzeitig nehmen Angreifer immer häufiger kleinere Organisationen ins Visier, gerade weil sie schlechter geschützt sind. Unternehmen mit weniger als 500 Beschäftigten sind denselben automatisierten Angriffen ausgesetzt wie multinationale Konzerne, werden vom Markt aber kaum bedient. Q-Feeds schließt diese Lücke: Premium-Intelligence zu fairen Preisen, einfach einzuführen.

Geprüfte Qualität

Jeder Datensatz durchläuft Qualitätsprüfungen, ein Priority-Scoring und eine Fehlalarm-Validierung, bevor er veröffentlicht wird.

Zugänglich

Faire Preise, eine kostenlose Community Edition und Integrationen, die in wenigen Minuten eingerichtet sind. So kann jede Organisation ihr Sicherheitsniveau anheben.

Europäisch

In den Niederlanden entwickelt, an europäischen Standards und Datenschutzerwartungen ausgerichtet, für Kunden weltweit.

03

Was wir tun

Q-Feeds hat sich von einem Threat Intelligence Feed zu einer Threat-Exposure-Plattform entwickelt. Alles steht an einem Ort bereit: im Q-Feeds Threat Intelligence Portal.

Funktion	Beschreibung
Threat Intelligence Feeds	Geprüfte Feeds mit schädlichen IPs, Domains und URLs, bereit für Firewalls, SIEMs, DNS-Filter und Proxys.
Threat Lookup	Untersuchen Sie beliebige IPs, Domains, URLs oder Datei-Hashes, mit Malicious Score, den meldenden Quellen und MITRE-ATT&CK-Zuordnung.
IOC Lookup API & TAXII 2.1	Programmatischer Zugriff für SOAR, Ticketing und eigene Tools sowie standardbasierte STIX-2.1-Collections für SIEMs und Threat-Intelligence-Plattformen.
Dark-Web-Monitoring	Laufende Überwachung von Marktplätzen, Foren, Paste-Sites und Breach-Dumps auf geleakte Zugangsdaten und Daten.
Attack Surface & Schwachstellenscanner	Erfassung und Scan öffentlich erreichbarer Assets, Netzwerke und Webanwendungen.
CVE-Alerts	Ein durchsuchbarer CVE-Katalog mit CVSS- und EPSS-Score sowie CISA-KEV-Status, dazu eine tägliche oder wöchentliche Übersicht per E-Mail zu neuen CVEs in der Software, die Sie im Portal hinterlegen.
Brand Protection	Erkennung von Look-alike-Domains, Typosquatting und Phishing-Seiten, mit Takedown-Anfragen.

04

Wie wir Intelligence aufbereiten

Der Wert von Threat Intelligence liegt nicht in den Rohdaten, sondern in dem, was mit ihnen geschieht, bevor sie Ihre Abwehr erreichen. Wir kombinieren vier Arten von Quellen:

Kommerzielle Quellen

Professionelle Cybersecurity-Anbieter, die Bedrohungsdaten mit eigenen Systemen sammeln und anreichern.

Open Source (OSINT)

Community-Projekte, Forschungsgruppen, offene Listen, Foren und Veröffentlichungen.

Staatliche Quellen

Intelligence, die nationale und internationale Cybersicherheitsbehörden bereitstellen.

Eigene Honeypots

Sensoren, die echten Angriffsverkehr anziehen und aufzeichnen und uns so Beobachtungen aus erster Hand liefern.

Unabhängig von der Herkunft durchläuft jeder Indikator denselben Prozess:

1. **Sammeln**
   Kontinuierliche Erfassung aus allen Quellen.
2. **Bereinigen**
   Normalisierung, Deduplizierung und Ablauf von Indikatoren, die nicht mehr aktiv sind.
3. **Validieren**
   Fehlalarm-Validierung, damit legitime Infrastruktur nicht auf den Listen landet.
4. **Anreichern**
   Priority-Scoring, Kategorisierung und MITRE-ATT&CK-Zuordnung.
5. **Ausliefern**
   Veröffentlicht als Feeds, TAXII-Collections und API-Antworten, bei Premium alle 20 Minuten aktualisiert.

OSINT UND KOMMERZIELL, DERSELBE STANDARD

OSINT-Feeds und kommerzielle Feeds unterscheiden sich in ihrer Herkunft, nicht in der Art, wie wir sie behandeln. Beide durchlaufen dieselben Qualitätsprüfungen. Deshalb erfüllen alle Indikatoren auf unserer Plattform denselben Anspruch an Genauigkeit und Zuverlässigkeit.

05

Wie wir arbeiten

Prinzip	In der Praxis
Offene Standards	Auslieferung über HTTPS-Feeds, CSV, TAXII 2.1 und STIX 2.1. So passt unsere Intelligence zu nahezu jedem Tool, ohne Herstellerbindung.
Open Source, wo es hilft	Unsere Integrationsskripte für MikroTik, Linux nftables / iptables und Wazuh sind als Open Source veröffentlicht.
Kostenloser Einstieg	Die Community Edition ist dauerhaft kostenlos. So kann jeder unsere Intelligence im eigenen Netzwerk prüfen, bevor er etwas kauft.

Prinzip	In der Praxis
Faire Lizenzierung	Lizenzen richten sich nach den tatsächlich geschützten Personen und den tatsächlich genutzten Geräten, nicht nach der gesamten Unternehmensgröße oder nach Standby-Hardware.
Verantwortungsvolles Scannen	Unser Schwachstellenscanner prüft nur Assets, deren Eigentümer zugestimmt hat, und jede Scan-Anfrage wird protokolliert.
Responsible Disclosure	Wir veröffentlichen eine Sicherheits- und Disclosure-Richtlinie und freuen uns über Meldungen aus der Security-Research-Community.

06

Ökosystem und Partner

Wir arbeiten mit einem wachsenden Netzwerk aus Technologiepartnern, Distributoren und Resellern, die Q-Feeds vor Ort liefern, einführen und betreuen.

Technologie

Q-Feeds ist als natives Plugin im offiziellen OPNsense-Repository verfügbar und wird mit OPNsense 26.1 ausgeliefert, entwickelt gemeinsam mit Deciso. Dokumentierte Integrationen decken die wichtigsten Firewalls, SIEMs und Threat-Intelligence-Plattformen ab.

Distribution

In den Niederlanden ist Q-Feeds über die Value-Added-Distributoren Infinigate und DSD Europe erhältlich.

Reseller

Zertifizierte Reseller-Partner in den Niederlanden, Deutschland, dem Vereinigten Königreich, Italien und Polen. Über die Partnersuche auf qfeeds.com finden Sie einen Partner in Ihrer Nähe.

Wer Q-Feeds nutzt

Q-Feeds wird von Managed Service Providern, Resellern sowie internen IT- und Security-Teams in Branchen wie Hotellerie und Tourismus, Logistik, Gesundheitswesen und Non-Profit eingesetzt. Organisationen wie Landal stärken ihre Firewalls mit geprüfter Threat Intelligence von Q-Feeds.

In den Medien

Q-Feeds beteiligt sich regelmäßig an der öffentlichen Diskussion über Sicherheit für kleine und mittlere Unternehmen, unter anderem in der Reihe De Staat van Security mit Sophos sowie mit Beiträgen in Dutch IT Channel, Dutch IT Leaders und ITchannelPRO.

07

Pakete

	Community	Plus	Premium
Feed-Updates	Alle 24 Stunden	Alle 4 Stunden	Alle 20 Minuten
Feed schädlicher IPs	OSINT	OSINT + Premium-IP-Daten	OSINT + Premium-IP-Daten
Feed schädlicher Domains	OSINT	OSINT	OSINT + Premium-DNS-Daten
Feed schädlicher URLs	–	–	Enthalten (Proxy / Web-Filter)
Dark-Web-Monitoring	–	Enthalten	Enthalten
Threat Lookup	–	Enthalten	Enthalten
Schwachstellenscanner	–	1 Scan pro Woche pro IP	1 Scan pro Tag pro Asset, inkl. Web-Apps
CVE-Katalog	Enthalten	Enthalten	Enthalten
CVE-Alerts	–	Enthalten	Enthalten
Brand Protection	–	–	Enthalten, mit Takedown-Anfragen
Preis	Dauerhaft kostenlos	Ab 99 € / Jahr	Ab 249 € / Jahr

Die Auslieferung über TAXII 2.1 / STIX 2.1 ist als separates Enterprise-TAXII-Paket erhältlich. Die IOC Lookup API gibt es ab 49,99 € pro Monat. Preise laut qfeeds.com/pricing zum Zeitpunkt der Veröffentlichung.

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

Q-Feeds · Handelsregister (KvK) 94910774 · Oude Amersfoortseweg 43, 1213 AB Hilversum, Niederlande