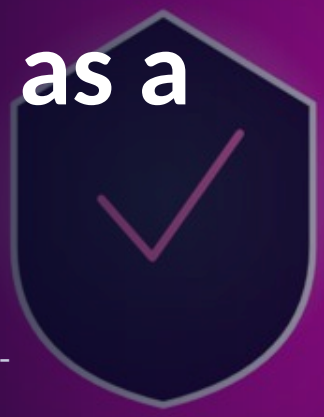
Q-FEEDS

WHITEPAPER · MSP & MSSP

Threat Intelligence as a Service



Wie Managed Service Provider aus geprüfter Threat Intelligence ein skalierbares, wiederkehrendes Security-Angebot für ihre Kunden machen.

qfeeds.com
Version 2026

MADE IN EUROPE

01

Management Summary

Kleine und mittlere Organisationen sind inzwischen ein Hauptziel der Cyberkriminalität, doch die meisten haben keinen Zugang zu Threat Intelligence. Managed Service Provider können diese Lücke am besten schließen, denn sie verwalten bereits die Firewalls, SIEMs und DNS-Filter, in denen Intelligence ihre Wirkung entfaltet.

Dieses Whitepaper zeigt, wie MSPs und MSSPs mit Q-Feeds geprüfte Threat Intelligence in die Infrastruktur einbringen, die sie ohnehin betreuen, und daraus Services machen, die ihre Kunden verstehen und für die sie zahlen: gehärtete Firewalls, angereicherte SIEM-Erkennung, Exposure-Monitoring und Schutz vor Phishing.

2.500+	20 min	20+	€0
kommerzielle, OSINT- und staatliche Quellen	Update-Intervall bei Premium	native und dokumentierte Integrationen	zum Start: Community Edition, dauerhaft kostenlos

Das Wichtigste in Kürze

- Threat Intelligence ist eine der wenigen Sicherheitsebenen, die sich ohne neue Hardware oder Agenten über einen gesamten Kundenstamm ausrollen lassen.
- Sorgfältige Auswahl zählt mehr als Masse. Ungefilterte Listen erzeugen Fehlalarme, und jeder Fehlalarm wird zum Support-Ticket.
- Ein herstellerneutraler Feed funktioniert mit Fortinet, Palo Alto, Sophos, Check Point, OPNsense, pfSense, MikroTik und den großen SIEMs. So deckt ein einziges Angebot auch gemischte Umgebungen ab.
- Eine Lizenzierung nach begünstigten Nutzern, aktiven Geräten und Laufzeit hält die Preise für Dienstleister kalkulierbar und für Kunden fair.

02

Die Chance für Service Provider

Angriffe auf kleine und mittlere Organisationen laufen weitgehend automatisiert ab. Botnets durchsuchen das gesamte Internet nach offenen VPNs und Remote-Desktops, Phishing-Kits werden stundenweise vermietet, und Ransomware-Gruppen wählen ihre Opfer nicht nach Unternehmensgröße aus. Organisationen mit weniger als 500 Beschäftigten sind denselben Bedrohungen ausgesetzt wie Großunternehmen, haben aber selten ein Security-Team, das reagieren kann.

Gleichzeitig steigen die regulatorischen Anforderungen und die Erwartungen der Kunden. NIS2 verpflichtet viele Organisationen zu angemessenen Maßnahmen gegen Cyberrisiken, und Anforderungen an die Lieferkette reichen Sicherheitsfragen an kleinere Zulieferer weiter. Die meisten dieser Organisationen wenden sich damit an ihren IT-Dienstleister.

Kunden fragen danach

Fragebögen zu Sicherheit, NIS2 und Cyberversicherung landen auf dem Tisch des IT-Dienstleisters. Eine konkrete, gut erklärbare Maßnahme erleichtert dieses Gespräch.

Die Infrastruktur ist schon da

MSPs verwalten bereits Firewalls, SIEMs und DNS-Filter für ihre Kunden. Threat Intelligence macht diese vorhandene Infrastruktur intelligenter.

Von Natur aus wiederkehrend

Threat Intelligence ist per Definition ein Abonnement. Sie passt ganz selbstverständlich in Managed-Service-Verträge und zu monatlich wiederkehrenden Umsätzen.

03

Warum Threat Intelligence im großen Maßstab schwer bereitzustellen ist

Viele Dienstleister haben es mit kostenlosen Blocklisten oder mit Feeds versucht, die der Hersteller mitliefert. In der Praxis stoßen sie auf dieselben Probleme:

Herausforderung	Was das für einen MSP bedeutet
Unsaubere, ungeprüfte Listen	Kostenlose Listen enthalten oft veraltete Einträge und legitime Infrastruktur wie gemeinsam genutzte Cloud- oder CDN-Adressen. Wer sie blockiert, legt Anwendungen lahm und erzeugt Tickets.
Veraltete Daten	Listen, die nur einmal täglich aktualisiert werden, verpassen kurzlebige Phishing- und Command-and-Control-Infrastruktur, die mitunter nur wenige Stunden aktiv ist.
Herstellerbindung	Herstellereigene Feeds funktionieren nur auf den Geräten dieses Herstellers. Ein Dienstleister mit gemischter Umgebung hat am Ende je Kunde andere Intelligence, andere Qualität und andere Preise.
Enterprise-Preise	Kommerzielle Threat-Intelligence-Plattformen sind in der Regel auf Großunternehmen und SOC-Teams zugeschnitten, nicht auf einen Kunden mit 40 Beschäftigten hinter einer einzelnen Firewall.
Betrieblicher Aufwand	Eine eigene Pipeline für Erfassung, Deduplizierung und Validierung aufzubauen und zu pflegen, kostet Entwicklungszeit, die den meisten Dienstleistern fehlt.

DIE ZENTRALE ERKENNTNIS

Für einen Service Provider bemisst sich der Wert von Threat Intelligence nicht an der Zahl der Indikatoren, sondern daran, **wie wenige Fehlalarme beim Kunden ankommen** und wie wenig Aufwand es macht, Hunderte Geräte aktuell zu halten.

04

Was Q-Feeds liefert

Q-Feeds führt Intelligence aus über 2.500 kommerziellen, Open-Source- und staatlichen Quellen, darunter unser eigenes Honeypot-Netzwerk, zu einem geprüften Datenbestand zusammen. Jeder Datensatz durchläuft vor der Veröffentlichung denselben Prozess:

1. **Sammeln**
   Kontinuierliche Erfassung bei kommerziellen Anbietern, OSINT-Projekten, staatlichen Quellen und Honeypots.
2. **Bereinigen**
   Normalisierung und Deduplizierung sowie Entfernen von Indikatoren, die nicht mehr aktiv sind.
3. **Validieren**
   Fehlalarm-Validierung, damit legitime Dienste und gemeinsam genutzte Infrastruktur nicht auf der Liste landen.
4. **Anreichern**
   Priority-Scoring, Kategorisierung und MITRE-ATT&CK-Zuordnung für den Kontext.
5. **Ausliefern**
   Veröffentlicht als sofort nutzbare Feeds, über TAXII 2.1 und per API, bei Premium alle 20 Minuten aktualisiert.

Eine Plattform, mehrere Bausteine

Baustein	Was er leistet
Threat Intelligence Feeds	Geprüfte Feeds mit schädlichen IPs, Domains und URLs für Firewalls, DNS-Filter, Proxys und SIEMs.
Threat Lookup & IOC Lookup API	Sofortiger Kontext zu jeder IP, Domain, URL oder jedem Datei-Hash: Malicious Score, Quellen und MITRE-ATT&CK-Zuordnung. Verfügbar im Portal und als API für SOAR- und Ticketing-Workflows.
TAXII-2.1-Server	Standardbasierte STIX-2.1-Collections für SIEMs, Threat-Intelligence-Plattformen und SOAR-Tools.
Dark-Web-Monitoring	Geplante Suchen nach geleakten Zugangsdaten und kompromittierten Daten, die mit Kundendomains verknüpft sind.
Attack-Surface- & Schwachstellenscans	Erfassung öffentlich erreichbarer Assets, offener Ports sowie von Schwachstellen in Netzwerk und Web, auf Abruf oder nach Zeitplan.

Baustein	Was er leistet
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.

05

Services, die Sie darauf aufbauen können

Dieselbe Plattform trägt mehrere Service-Angebote. Die meisten Dienstleister beginnen mit Firewall-Härtung und ergänzen die weiteren Services, sobald ihre Kunden so weit sind.

Firewall-Härtung als Managed Service

Ergänzen Sie die Firewalls, die Sie bereits verwalten, um geprüfte IP-, Domain- und URL-Feeds. Bekannt schädlicher Verkehr wird automatisch blockiert, ein- wie ausgehend. **Ergebnis für den Kunden:** weniger erfolgreiche Phishing-Klicks, blockierter Command-and-Control-Verkehr und weniger Rauschen durch Scanner.

SIEM- und SOC-Anreicherung

Speisen Sie geprüfte IOCs mit MITRE-ATT&CK-Kontext in Splunk, Microsoft Sentinel, Wazuh oder jedes TAXII-fähige SIEM ein. **Ergebnis:** weniger Fehlalarme, schnellere Triage und besser dokumentierte Vorfälle.

Exposure- und Dark-Web-Reporting

Nutzen Sie den Schwachstellenscanner, die Attack-Surface-Tools, CVE-Alerts und das Dark-Web-Monitoring für einen regelmäßigen Exposure-Bericht. **Ergebnis:** ein greifbares, wiederkehrendes Arbeitsergebnis, das den Wert Ihres Service zeigt.

Phishing-Schutz und Brand Protection

Überwachen Sie Look-alike-Domains und Phishing, die sich als Ihr Kunde ausgeben, und fordern Sie Takedowns an. **Ergebnis:** Schutz für die Kunden und den Ruf Ihres Kunden.

ERKENNUNG ALS NEBENEFFEKT

Blockiert eine Firewall ausgehenden Verkehr zu einem bekannten Command-and-Control-Server, zeigt der Logeintrag, welches interne Gerät die Verbindung aufbauen wollte. Für einen MSP ist jede solche Blockierung ein Frühwarnsignal, dass ein Gerät des Kunden infiziert sein könnte, oft noch bevor ein anderes Tool Alarm schlägt.

06

Ein Feed für gemischte Umgebungen

Service Provider betreuen selten nur eine Marke. Q-Feeds ist herstellerneutral und wird über offene Mechanismen ausgeliefert. Dieselbe geprüfte Intelligence und dasselbe Angebot funktionieren deshalb im gesamten Kundenstamm.

Kategorie	Unterstützte Plattformen
Firewalls	Fortinet FortiGate, Palo Alto Networks, Sophos XGS, Check Point, SonicWall, OPNsense (natives Plugin), pfSense, MikroTik RouterOS, Linux nftables / iptables
SIEM	Splunk, Microsoft Sentinel, Wazuh, Exabeam sowie weitere SIEMs über TAXII 2.1, Feeds oder API (z. B. IBM QRadar, Elastic Security, LogRhythm, Google SecOps)
Threat-Intelligence-Plattformen	OpenCTI, MISP, EclecticIQ, Anomali ThreatStream, ThreatConnect
DNS-Filterung	Pi-hole, AdGuard Home, Technitium DNS
Entwickler	IOC Lookup API, TAXII-2.1-Server, Open-Source-Integrationsskripte

Schritt-für-Schritt-Einrichtungsanleitungen für jede Plattform finden Sie in der Q-Feeds-Wissensdatenbank und als PDF-Anleitungen. Technische Details enthält das ergänzende Whitepaper **Q-Feeds integrieren**.

07

Betrieb im großen Maßstab

Verwaltung mehrerer Kunden

Partner verwalten ihre Kunden über ein Reseller-Konto im Threat Intelligence Portal. Lizenzen, die der Partner erwirbt, sind diesem Konto zugeordnet und lassen sich einzelnen Endkunden mit eigenen Nutzern zuweisen. Die Kundenbeziehung bleibt beim Partner; Q-Feeds kümmert sich um die Intelligence.

Einmal einrichten, fertig

- Die Geräte rufen ihre Feed-URLs automatisch ab; es gibt keine Listen, die von Hand gepflegt werden müssen.
- Passen Sie das Polling-Intervall an die Lizenz an: alle 24 Stunden bei Community, alle 4 Stunden bei Plus, alle 20 Minuten bei Premium.
- Mit dem limit-Parameter passen Sie die Listengröße an die Kapazität kleinerer Geräte an.
- Platzieren Sie die Blockierregeln oberhalb der Allow-Regeln und aktivieren Sie das Logging, damit Blockierungen sichtbar und auswertbar werden.

Umgang mit Fehlalarmen

Dank der Validierung sind Fehlalarme selten. Wird doch einmal eine legitime Adresse blockiert, kann der Dienstleister auf dem Gerät eine vorübergehende Ausnahme einrichten und den Indikator an Q-Feeds melden. Q-Feeds prüft die Meldung, stellt fest, ob es sich um einen Fehlalarm handelt, und passt den Feed bei Bedarf an. So profitieren alle Kunden von der Korrektur.

08

Lizenzierung, die zum Geschäftsmodell von Dienstleistern passt

Die Lizenzierung von Q-Feeds beruht auf drei Größen: der Zahl der **begünstigten Nutzer** (der tatsächlich geschützten Personen, nicht der gesamten Belegschaft), der Zahl der **aktiven Geräte** und der **Laufzeit** (1, 2 oder 3 Jahre). So bleiben kleine Kunden bezahlbar, und die Dimensionierung wird planbar.

Konfiguration	Gerätelizenzen
Einzelne Firewall	1
Zwei getrennte Firewalls	2
Active-Passive-Cluster	1 (das Standby-Gerät zählt nicht mit)
Active-Active-Cluster	2

Stufen für begünstigte Nutzer: Small (< 50), Medium (50 bis 250), Large (250 bis 1.000) und Enterprise (1.000+). Für Plus und Premium gilt dieselbe Struktur; der Unterschied liegt im Funktionsumfang.

	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.

PARTNERPROGRAMM

Reseller und Service Provider erhalten Partnerpreise, Onboarding, Schulungen und Vertriebsmaterial sowie direkten Zugang zum Q-Feeds-Team für Proofs of Concept. Für Dienstleister, die Threat Intelligence unter eigener Marke anbieten möchten, ist eine White-Label-Bereitstellung möglich. Sprechen Sie uns an.

09

Erste Schritte

1. **Registrieren**

   Erstellen Sie ein kostenloses Konto im Threat Intelligence Portal. Die Community Edition enthält eine 7-tägige Premium-Testphase.

2. **Im eigenen Netzwerk erproben**

   Binden Sie mithilfe der Einrichtungsanleitungen eine Firewall oder ein SIEM an und messen Sie, was blockiert wird. Mit dem kostenlosen Testing Tool vergleichen Sie Ihren aktuellen Schutz.

3. **Partner werden**

   Bewerben Sie sich für das Reseller-Programm und erhalten Sie ein Reseller-Konto, Partnerpreise und Onboarding.

4. **Ausrollen**

   Beginnen Sie mit der Firewall-Härtung für Ihre Kunden und ergänzen Sie nach und nach SIEM-Anreicherung, Exposure-Reporting und Brand Protection.

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