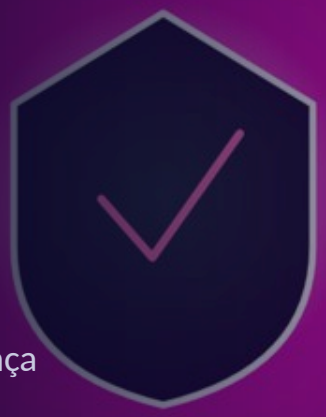
Q-FEEDS

WHITE PAPER · MSP E MSSP

Threat intelligence como serviço



Como os prestadores de serviços geridos transformam threat intelligence selecionada numa oferta de segurança escalável e recorrente para os seus clientes.

qfeeds.com
Versão 2026

MADE IN EUROPE

01

Sumário executivo

As pequenas e médias organizações são hoje um alvo preferencial do cibercrime e, no entanto, a maioria não tem acesso a threat intelligence. Os prestadores de serviços geridos estão na melhor posição para fechar essa lacuna, porque já gerem as firewalls, os SIEM e os filtros DNS onde a inteligência faz o seu trabalho.

Este white paper explica como os MSP e os MSSP podem usar a Q-Feeds para acrescentar threat intelligence selecionada à infraestrutura que já gerem e transformá-la em serviços que os seus clientes compreendem e pelos quais pagam: firewalls reforçadas, deteção enriquecida no SIEM, monitorização da exposição e proteção contra phishing.

2.500+	20 min	20+	€0
fontes comerciais, OSINT e governamentais	intervalo de atualização no Premium	integrações nativas e documentadas	para começar: edição Community, gratuita para sempre

Pontos-chave

- A threat intelligence é uma das poucas camadas de segurança que pode ser implementada em toda uma carteira de clientes sem novo hardware nem agentes.
- A seleção conta mais do que o volume. As listas não filtradas geram falsos positivos, e cada falso positivo transforma-se num pedido de suporte.
- Um único feed, independente do fabricante, funciona com Fortinet, Palo Alto, Sophos, Check Point, OPNsense, pfSense, MikroTik e os principais SIEM, pelo que uma só proposta cobre um parque heterogéneo.
- Um licenciamento baseado em utilizadores beneficiários, dispositivos ativos e duração mantém os preços previsíveis para os prestadores de serviços e justos para os clientes.

02

A oportunidade para os prestadores de serviços

Os ataques a pequenas e médias organizações são, em grande parte, automatizados. As botnets percorrem toda a internet à procura de VPN e de ambientes de trabalho remotos expostos, os kits de phishing alugam-se à hora e os grupos de ransomware não escolhem as vítimas pela dimensão da empresa. As organizações com menos de 500 colaboradores enfrentam as mesmas ameaças que as grandes empresas, mas raramente têm uma equipa de segurança para lhes responder.

Ao mesmo tempo, a regulamentação e as expectativas dos clientes estão a aumentar. A NIS2 obriga muitas organizações a adotar medidas adequadas contra os ciber-riscos, e os requisitos da cadeia de abastecimento

fazem as questões de segurança chegar aos fornecedores mais pequenos. A maioria destas organizações recorre ao seu prestador de serviços de TI para lhes dar resposta.

Os clientes estão a pedir

Os questionários sobre segurança, NIS2 e ciberseguros vão parar à secretária do prestador de serviços de TI. Uma medida concreta e fácil de explicar simplifica essa conversa.

A infraestrutura já existe

Os MSP já gerem firewalls, SIEM e filtros DNS para os seus clientes. A threat intelligence torna essa infraestrutura existente mais inteligente.

Recorrente por natureza

A threat intelligence é, por definição, uma subscrição. Encaixa naturalmente nos contratos de serviços geridos e na receita mensal recorrente.

03

Porque é difícil disponibilizar threat intelligence em escala

Muitos prestadores de serviços experimentaram listas de bloqueio gratuitas ou os feeds incluídos por cada fabricante. Na prática, deparam-se com os mesmos problemas:

Desafio	O que significa para um MSP
Listas com ruído e não validadas	As listas gratuitas contêm frequentemente entradas desatualizadas e infraestrutura legítima, como endereços partilhados de cloud ou de CDN. Bloqueá-las deixa aplicações sem funcionar e gera pedidos de suporte.
Dados desatualizados	As listas atualizadas uma vez por dia deixam escapar a infraestrutura efémera de phishing e de command-and-control, que por vezes só está ativa durante algumas horas.
Dependência do fabricante	Os feeds nativos de um fabricante só funcionam nos dispositivos desse fabricante. Um prestador de serviços com um parque heterogéneo acaba com inteligência, qualidade e preços diferentes para cada cliente.
Preços de grande empresa	As plataformas comerciais de threat intelligence têm normalmente preços pensados para grandes empresas e equipas SOC, não para um cliente de 40 pessoas atrás de uma única firewall.
Carga operacional	Construir e manter um processo próprio de recolha, deduplicação e validação exige um tempo de engenharia que a maioria dos prestadores de serviços não tem.

A IDEIA CENTRAL

Para um prestador de serviços, o valor da threat intelligence não está no número de indicadores. Está em **quão poucos falsos positivos chegam ao cliente** e em quão pouco trabalho é preciso para manter centenas de dispositivos atualizados.

04

O que a Q-Feeds oferece

A Q-Feeds reúne inteligência de mais de 2.500 fontes comerciais, de código aberto e governamentais, incluindo a nossa própria rede de honeypots, num único conjunto selecionado. Cada conjunto de dados passa pelo mesmo processo antes de ser publicado:

1. **Recolher**
   Recolha contínua junto de fornecedores comerciais, projetos OSINT, fontes governamentais e honeypots.
2. **Limpar**
   Normalização e deduplicação, e remoção dos indicadores que já não estão ativos.
3. **Validar**
   Validação de falsos positivos, para que os serviços legítimos e a infraestrutura partilhada fiquem fora da lista.
4. **Enriquecer**
   Pontuação de prioridade, categorização e mapeamento MITRE ATT&CK para dar contexto.
5. **Entregar**
   Publicação sob a forma de feeds prontos a usar, por TAXII 2.1 e através de API, atualizados a cada 20 minutos no Premium.

Uma plataforma, vários componentes

Componente	O que faz
Feeds de threat intelligence	Feeds selecionados de IP, domínios e URL maliciosos para firewalls, filtros DNS, proxies e SIEM.
Threat Lookup e API IOC Lookup	Contexto imediato sobre qualquer IP, domínio, URL ou hash de ficheiro: pontuação de risco, fontes e mapeamento MITRE ATT&CK. Disponível no portal e como API para fluxos de SOAR e de ticketing.
Servidor TAXII 2.1	Coleções STIX 2.1 baseadas em normas para SIEM, plataformas de threat intelligence e ferramentas SOAR.

Componente	O que faz
Dark Web Monitoring	Pesquisas agendadas de credenciais divulgadas e de dados comprometidos associados aos domínios dos clientes.
Superfície de ataque e análise de vulnerabilidades	Descoberta de ativos expostos à internet, portas abertas e vulnerabilidades de rede e web, a pedido ou de forma agendada.
Alertas CVE	Um catálogo pesquisável de CVE, com pontuações CVSS e EPSS e estado CISA KEV, além de um resumo diário ou semanal por e-mail com as novas CVE do software que indica no portal.
Brand Protection	Deteção de domínios semelhantes, typosquatting e páginas de phishing, com pedidos de remoção.

05

Serviços que pode construir

A mesma plataforma suporta várias propostas de serviço. A maioria dos prestadores de serviços começa pelo reforço das firewalls e vai acrescentando os outros serviços à medida que os clientes ganham maturidade.

Reforço gerido de firewalls

Acrescente feeds selecionados de IP, domínios e URL às firewalls que já gere. O tráfego malicioso conhecido é bloqueado automaticamente, à entrada e à saída. **Resultado para o cliente:** menos cliques de phishing bem-sucedidos, tráfego de command-and-control bloqueado e menos ruído de scanners.

Enriquecimento de SIEM e SOC

Alimente o Splunk, o Microsoft Sentinel, o Wazuh ou qualquer SIEM compatível com TAXII com IOC selecionados e contexto MITRE ATT&CK. **Resultado:** menos falsos alertas, uma triagem mais rápida e incidentes mais bem documentados.

Relatórios de exposição e de dark web

Use o scanner de vulnerabilidades, as ferramentas de superfície de ataque, os alertas CVE e a monitorização da dark web para entregar um relatório periódico de exposição. **Resultado:** um entregável tangível e recorrente, que mostra o valor do seu serviço.

Proteção de marca e contra phishing

Monitorize os domínios semelhantes e o phishing que se fazem passar pelo seu cliente e peça a sua remoção. **Resultado:** proteção para os clientes e para a reputação do seu cliente.

A DETEÇÃO COMO BENEFÍCIO ADICIONAL

Quando uma firewall bloqueia tráfego de saída para um servidor de command-and-control conhecido, a entrada de log mostra que dispositivo interno tentou estabelecer a ligação. Para um MSP, cada bloqueio deste tipo é um aviso precoce de que um dispositivo do cliente pode estar infetado, muitas vezes antes de qualquer outra ferramenta dar o alarme.

06

Um único feed para um parque heterogéneo

Os prestadores de serviços raramente gerem uma só marca. A Q-Feeds é independente do fabricante e é entregue através de mecanismos abertos, pelo que a mesma inteligência selecionada e a mesma proposta funcionam em toda a carteira de clientes.

Categoria	Plataformas suportadas
Firewalls	Fortinet FortiGate, Palo Alto Networks, Sophos XGS, Check Point, SonicWall, OPNsense (plugin nativo), pfSense, MikroTik RouterOS, Linux nftables / iptables
SIEM	Splunk, Microsoft Sentinel, Wazuh, Exabeam e outros SIEM através de TAXII 2.1, feeds ou API (p. ex., IBM QRadar, Elastic Security, LogRhythm, Google SecOps)
Plataformas de threat intelligence	OpenCTI, MISP, EclecticIQ, Anomali ThreatStream, ThreatConnect
Filtragem DNS	Pi-hole, AdGuard Home, Technitium DNS
Programadores	API IOC Lookup, servidor TAXII 2.1, scripts de integração de código aberto

Na base de conhecimento da Q-Feeds e nos manuais em PDF encontra guias de configuração passo a passo para cada plataforma. Para os detalhes técnicos, consulte o white paper complementar **Integrar a Q-Feeds**.

07

Operar em escala

Gestão de vários clientes

Os parceiros gerem os seus clientes a partir de uma conta de revendedor no Threat Intelligence Portal. As licenças compradas pelo parceiro ficam associadas a essa conta e podem ser atribuídas a cada empresa cliente final, com os seus próprios utilizadores. O parceiro mantém a relação com o cliente; a Q-Feeds trata da inteligência.

Configurar e esquecer

- Os dispositivos consultam automaticamente os seus URL de feed; não há listas para manter à mão.
- Ajuste o intervalo de consulta à licença: a cada 24 horas no Community, a cada 4 horas no Plus e a cada 20 minutos no Premium.
- Use o parâmetro limit para adequar o tamanho das listas à capacidade dos dispositivos mais pequenos.
- Coloque as regras de bloqueio acima das regras de permissão e ative o registo de logs, para que os bloqueios fiquem visíveis e possam constar dos seus relatórios.

Lidar com falsos positivos

A validação faz com que os falsos positivos sejam raros. Se um endereço legítimo for bloqueado, o prestador de serviços pode criar uma exceção temporária no dispositivo e comunicar o indicador à Q-Feeds. A Q-Feeds avalia o relato, determina se se trata de um falso positivo e atualiza o feed quando necessário, pelo que a correção beneficia todos os clientes.

08

Um licenciamento à medida do negócio dos prestadores de serviços

O licenciamento da Q-Feeds assenta em três elementos: o número de **utilizadores beneficiários** (as pessoas efetivamente protegidas, e não o número total de colaboradores da empresa), o número de **dispositivos ativos** e a **duração** (1, 2 ou 3 anos). Assim, os clientes pequenos continuam acessíveis e o dimensionamento torna-se previsível.

Configuração	Licenças de dispositivo
Uma única firewall	1
Duas firewalls separadas	2
Cluster ativo-passivo	1 (o dispositivo em standby não conta)
Cluster ativo-ativo	2

Escalões de utilizadores beneficiários: Small (< 50), Medium (50 a 250), Large (250 a 1.000) e Enterprise (1.000+). A mesma estrutura aplica-se ao Plus e ao Premium; a diferença está na abrangência das funcionalidades.

	Community	Plus	Premium
Atualizações dos feeds	A cada 24 horas	A cada 4 horas	A cada 20 minutos
Feed de IP maliciosos	OSINT	OSINT + dados IP premium	OSINT + dados IP premium
Feed de domínios maliciosos	OSINT	OSINT	OSINT + dados DNS premium
Feed de URL maliciosos	–	–	Incluído (proxy / filtro web)
Dark Web Monitoring	–	Incluído	Incluído
Threat Lookup	–	Incluído	Incluído
Scanner de vulnerabilidades	–	1 análise por semana por IP	1 análise por dia por ativo, incl. aplicações web
Catálogo de CVE	Incluído	Incluído	Incluído
Alertas CVE	–	Incluído	Incluído
Brand Protection	–	–	Incluído, com pedidos de remoção
Preço	Gratuito para sempre	A partir de 99 € / ano	A partir de 249 € / ano

A entrega por TAXII 2.1 / STIX 2.1 está disponível num pacote Enterprise TAXII separado. A API IOC Lookup está disponível a partir de 49,99 € por mês. Preços indicados em qfeeds.com/pricing à data de redação.

PROGRAMA DE PARCEIROS

Os revendedores e os prestadores de serviços recebem preços de parceiro, onboarding, formação e materiais de vendas, além de acesso direto à equipa da Q-Feeds para provas de conceito. A entrega em marca branca está disponível para os prestadores de serviços que queiram oferecer threat intelligence com a sua própria marca. Contacte-nos para saber mais.

09

Primeiros passos

1. **Registe-se**

   Crie uma conta gratuita no Threat Intelligence Portal. A edição Community inclui 7 dias de teste Premium.

2. **Comprove na sua própria rede**

   Ligue uma firewall ou um SIEM com a ajuda dos guias de configuração e meça o que é bloqueado. A ferramenta gratuita Testing Tool ajuda a avaliar a sua proteção atual.

3. **Torne-se parceiro**

   Candidate-se ao programa de revendedor para obter uma conta de revendedor, preços de parceiro e onboarding.

4. **Implemente**

   Comece pelo reforço das firewalls dos seus clientes e, com o tempo, acrescente o enriquecimento do SIEM, os relatórios de exposição e a proteção de marca.

Avalie a Q-Feeds hoje mesmo

Crie uma conta gratuita no Threat Intelligence Portal, em tip.qfeeds.com. A edição Community é gratuita para sempre e inclui 7 dias de teste Premium, sem cartão de crédito. Para programas de parceiros, licenciamento por volume ou uma demo guiada, fale com a nossa equipa.



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