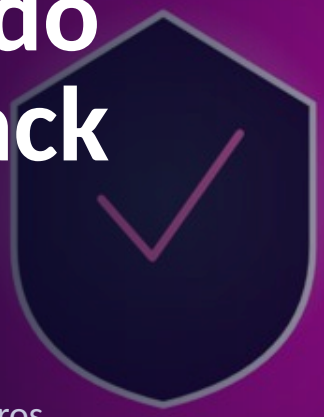
Q-FEEDS

WHITE PAPER · INTEGRAÇÕES

Um feed selecionado para todo o seu stack de segurança



Como a threat intelligence da Q-Feeds se integra com firewalls, SIEM, plataformas de threat intelligence e filtros DNS, e como tirar o máximo partido dela.

qfeeds.com
Versão 2026

MADE IN EUROPE

01

Introdução

A threat intelligence só cria valor quando é aplicada. A Q-Feeds foi concebida para se ligar às ferramentas de segurança que já utiliza, através dos mecanismos nativos de cada uma, para que a inteligência selecionada chegue em poucos minutos ao perímetro da sua rede, ao seu SIEM e aos seus analistas.

Este white paper descreve os métodos de entrega que a Q-Feeds disponibiliza, que feeds estão disponíveis em cada licença, como cada uma das principais plataformas consome a inteligência e que boas práticas mantêm uma integração fiável. Na base de conhecimento em qfeeds.com encontra guias detalhados, passo a passo, para cada plataforma.

20+	3	TAXII 2.1	5 min
integrações documentadas	tipos de feed: IP, domínio, URL	entrega baseada em normas	tempo habitual até ao primeiro feed

02

Métodos de entrega

A Q-Feeds disponibiliza cinco formas de consumir a sua inteligência. A maioria das integrações usa a primeira; as restantes destinam-se a SIEM, plataformas de threat intelligence e ferramentas próprias.

Método	Como funciona	Ideal para
URL de feed por HTTPS	O seu dispositivo vai buscar periodicamente uma lista por HTTPS: em texto simples por omissão, em CSV a pedido. Um parâmetro limit restringe o tamanho da lista em dispositivos com um máximo.	Firewalls, filtros DNS, proxies
Plugin nativo	Um plugin da Q-Feeds no repositório oficial do OPNsense cria e atualiza automaticamente aliases de firewall e listas de bloqueio DNS.	OPNsense
TAXII 2.1 / STIX 2.1	Um servidor TAXII 2.1 com coleções STIX 2.1, incluindo categoria, mapeamento MITRE ATT&CK e hashes de ficheiros. Os clientes só vão buscar o que é novo desde a última consulta.	SIEM, TIP, SOAR

Método	Como funciona	Ideal para
API IOC Lookup	Consulte um único IP, domínio, URL ou hash e receba o mesmo contexto do Threat Lookup: pontuação, fontes e mapeamento MITRE ATT&CK.	Enriquecimento de alertas, SOAR, ticketing
Scripts de código aberto	Instaladores e scripts mantidos para plataformas sem suporte nativo de feeds, publicados no GitHub.	MikroTik, hosts Linux, Wazuh

03

Feeds e disponibilidade por licença

Feed	Conteúdo	Disponível em
malware_ip	Endereços IP maliciosos (IPv4 e IPv6): botnets, servidores de command-and-control, scanners e alojamento de malware.	Community, Plus, Premium
malware_domains	Domínios maliciosos usados para phishing, distribuição de malware e command-and-control.	Community, Plus, Premium
malicious_urls	URL maliciosos específicos, como páginas de phishing e transferências de malware.	Premium
Coleções TAXII	Indicadores STIX 2.1 para IP, domínios, URL e hashes de ficheiros, com categoria, mapeamento MITRE ATT&CK e contexto.	Pacote Enterprise TAXII

Licença	Atualização do feed	Intervalo de consulta recomendado
Community	A cada 24 horas	Uma vez por dia
Plus	A cada 4 horas	A cada 4 horas
Premium	A cada 20 minutos	A cada 20 minutos

OS FEEDS DE URL PRECISAM DE UM DISPOSITIVO QUE CONSIGA VER URL

Um filtro de pacotes que trabalha com endereços IP, ou um filtro DNS que trabalha com nomes de domínio, não consegue aplicar uma lista de URL. Os feeds de URL maliciosos exigem um proxy ou um filtro web e, no tráfego HTTPS, esse dispositivo precisa de **inspeção TLS**; caso contrário, só vê o nome do host.

04

Autenticação

Todo o acesso é feito com uma chave de API pessoal, criada em Manage API Keys, no Threat Intelligence Portal.

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

- **Feeds:** a maioria dos dispositivos usa autenticação HTTP Basic, com api_token como nome de utilizador e a sua chave como palavra-passe. Os dispositivos que não suportam autenticação Basic podem passar a chave como parâmetro do URL.
- **API IOC Lookup e TAXII:** envie a chave como token Bearer no cabeçalho Authorization.
- Trate a chave como um segredo: qualquer pessoa que a tenha pode obter os seus feeds.

05

Firewalls

As firewalls aplicam a inteligência da Q-Feeds no perímetro da rede, bloqueando o tráfego de entrada e de saída para infraestrutura maliciosa conhecida antes de este chegar aos utilizadores ou aos servidores. Cada integração usa o mecanismo próprio do fabricante, pelo que não é necessário nenhum equipamento nem agente adicional.

Plataforma	Mecanismo de integração	Feeds
Fortinet FortiGate	External Connectors nativos (threat feeds), aplicados nas políticas de firewall, de filtro DNS e de filtro web.	IP, domínio, URL
Palo Alto Networks	External Dynamic Lists (EDL) nativas, aplicadas nas regras de Security policy. Funciona em ambientes geridos com o Panorama.	IP, domínio, URL
Sophos Firewall (XGS)	Third-party threat feeds, aplicados nas regras de firewall e nas políticas web, a par das proteções da Sophos.	IP, domínio, URL
Check Point	Custom Intelligence Feeds nativos, aplicados através das Software Blades Anti-Bot e Anti-Virus.	IP, domínio
OPNsense	Plugin nativo da Q-Feeds a partir do repositório oficial (incluído no OPNsense 26.1): aliases de firewall e bloqueio de domínios através do Unbound DNS ou do DNSCrypt-Proxy.	IP, domínio

Plataforma	Mecanismo de integração	Feeds
pfSense	Pacote pfBlockerNG: feeds de IP como aliases de firewall, feeds de domínios através de DNSBL.	IP, domínio
SonicWall	Dynamic Botnet List Server com filtragem Botnet nas regras de acesso (SonicOS 6.5.2+ para transferências autenticadas).	IP
MikroTik RouterOS	Scripts de código aberto para RouterOS: importação completa e atualizações diferenciais para uma address-list da firewall, com reversão automática se uma transferência falhar.	IP
Linux nftables / iptables	Instalador de código aberto que carrega a lista de bloqueio em sets dedicados e agenda as atualizações.	IP

UM COMPLEMENTO À INTELIGÊNCIA DO FABRICANTE

A Q-Feeds funciona a par das subscrições FortiGuard, WildFire, ThreatCloud ou Sophos X-Ops. Acrescenta inteligência independente, de múltiplas fontes, e dá aos prestadores de serviços um feed consistente entre marcas diferentes.

06

Plataformas SIEM

Num SIEM, os indicadores da Q-Feeds são correlacionados com os dados de log, pelo que a atividade que envolve IP, domínios, URL ou hashes maliciosos conhecidos surge como um alerta priorizado, com contexto MITRE ATT&CK.

Plataforma	Mecanismo de integração
Splunk	Os indicadores são ingeridos como lookups ou no framework de threat intelligence do Splunk Enterprise Security, prontos para as pesquisas de correlação. TAXII/STIX 2.1 disponível para ingestão.
Microsoft Sentinel	Conector de dados nativo de Threat Intelligence por TAXII/STIX 2.1. Os indicadores chegam à tabela ThreatIntelligenceIndicator, para regras de análise, consultas de hunting e livros.
Wazuh	Instalador de código aberto para o Wazuh 4.x: listas CDB, descodificadores e regras que geram alertas quando há correspondências. Bloqueio automático opcional com Active Response. Funciona com a API padrão ou com TAXII.

Plataforma	Mecanismo de integração
Exabeam	Tabela de contexto personalizada, preenchida com indicadores da Q-Feeds através da Exabeam Context Management API (CSV) e atualizada automaticamente.
Outros SIEM	IBM QRadar, Elastic Security, LogRhythm, Google SecOps e outras plataformas através de TAXII 2.1, dos feeds ou da API.

A entrega por TAXII requer o pacote Enterprise TAXII.

07

Plataformas de threat intelligence

Para as equipas de analistas, a Q-Feeds é uma camada de base fiável e selecionada. Os indicadores mantêm a atribuição à Q-Feeds como fonte, pelo que os pode filtrar, incluir em relatórios e remover sem tocar no resto do seu conhecimento.

Plataforma	Mecanismo de integração	Licença
OpenCTI	Ingestão TAXII integrada, sem nada para desenvolver ou manter. Nas outras licenças, as listas de IP e de domínios podem ser ingeridas como feed.	Enterprise TAXII (feeds em todos os pacotes)
MISP	Feeds MISP nativos: aponte o MISP para as listas completas e defina a frequência de recolha.	Todos os pacotes (URL no Premium)
EclecticIQ	Feed TAXII de entrada padrão; os indicadores passam a ser entidades no espaço de trabalho que escolher.	Enterprise TAXII
Anomali ThreatStream	Configuração padrão de um feed TAXII; os indicadores mantêm a sua própria etiqueta de fonte.	Enterprise TAXII
ThreatConnect	A aplicação TAXII da própria ThreatConnect, disponível no seu catálogo; cada coleção passa a ser uma fonte independente.	Enterprise TAXII

08

Filtragem DNS

Os filtros DNS bloqueiam os domínios maliciosos no momento da resolução, antes de qualquer ligação ser estabelecida. O Pi-hole, o AdGuard Home e o Technitium DNS subscrevem diretamente a lista de domínios de malware da Q-Feeds, o que faz desta uma opção eficaz para pequenos escritórios, filiais e redes domésticas.

09

Boas práticas

Prática	Porque é importante
Ajuste a consulta à sua licença	Consultar com mais frequência do que o feed é atualizado acrescenta carga sem acrescentar proteção. Consultar com menos frequência é desperdiçar proteção.
Respeite os limites do dispositivo	Muitas firewalls têm um tamanho máximo de lista. Use o parâmetro limit para não o ultrapassar, sobretudo em modelos mais pequenos ou mais antigos.
Bloqueie nos dois sentidos	Os bloqueios de entrada travam scanners e tentativas de força bruta; os de saída travam cliques em links de phishing e malware que tenta contactar o servidor do atacante.
Coloque as regras de bloqueio primeiro	Coloque as regras da Q-Feeds acima das regras de permissão; caso contrário, o tráfego pode ser autorizado antes de a lista ser avaliada.
Ative o registo de logs	Os bloqueios registados mostram o valor da inteligência e apontam para dispositivos internos potencialmente infetados.
Tenha em conta a alta disponibilidade	Um cluster ativo-passivo precisa de uma licença de dispositivo; um cluster ativo-ativo precisa de uma por dispositivo.
Teste a sua configuração	Use a ferramenta gratuita Q-Feeds Testing Tool para confirmar que a integração funciona e avaliar a sua proteção.

10

Primeiros passos

1. **Crie uma conta**

   Registe-se no Threat Intelligence Portal e ative a edição Community gratuita, que inclui 7 dias de teste Premium.

2. **Crie uma chave de API**

   No portal, aceda a Manage API Keys e crie a sua chave.

3. **Construa o URL do seu feed**

   Escolha o tipo de feed e, se necessário, um limite e um formato de saída.

4. **Siga o guia de configuração**

   Use o guia passo a passo da sua plataforma na base de conhecimento ou os manuais em PDF da página de transferências.

5. **Verifique**

   Confirme que a lista tem conteúdo, que as regras de bloqueio estão ativas e que os bloqueios aparecem nos logs.

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