CS-091 · Threat Intelligence

Threat Feeds

Streams of machine-readable threat data that keep detection tools current on known bad activity.

Executive Summary

A threat feed is a continuously updated stream of threat data, most often indicators such as malicious IP addresses, domains, URLs, and file hashes, delivered in a machine-readable format. Feeds keep detection tools current without manual effort, so a firewall, SIEM, or endpoint tool can block or flag freshly reported bad activity. The value of a feed depends heavily on how relevant, timely, and accurate its data is for the organization consuming it.

What It Is

A threat feed is a data stream that supplies information about current threats to security tools and analysts. Most feeds deliver indicators, but some also carry richer context such as the malware family, the campaign, or the technique associated with each entry. Feeds come from several origins: government and community sharing programs, commercial intelligence providers, open source projects, and an organization's own internal detections. They are consumed through open standards such as STIX for the data format and TAXII for the transport, or through simpler formats and interfaces. A feed is only raw material; on its own it is data, not finished intelligence. It becomes useful when it is filtered for relevance, checked for quality, and connected to the tools that will act on it.

Why It Matters

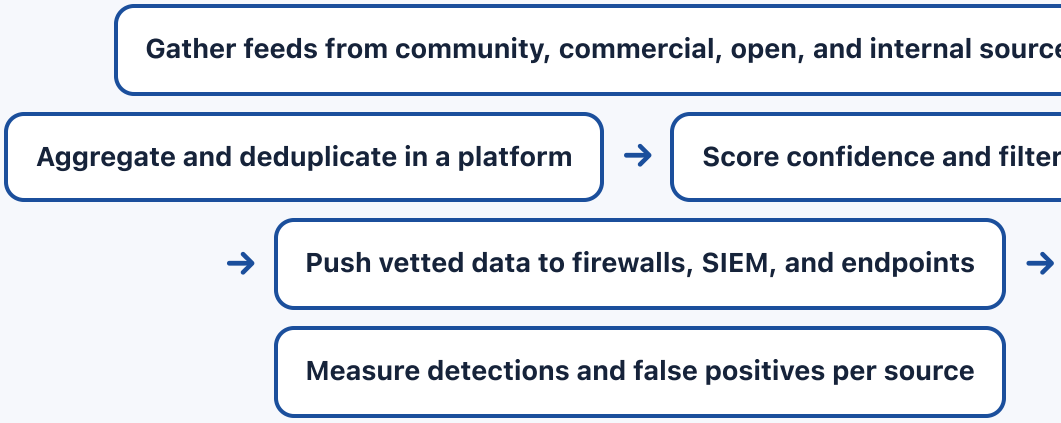
The threat landscape changes constantly, and no single organization can observe all of it alone. Feeds let defenders benefit from the collective visibility of the wider community, so an attack seen elsewhere can be blocked before it reaches them. Automating this flow means detection tools stay current at machine speed instead of waiting for an analyst to add each indicator by

hand. The risk is that a low-quality or poorly matched feed does more harm than good: stale entries, false positives, and irrelevant data create noise, waste analyst time, and can even block legitimate traffic. For professionals, knowing how to select, evaluate, and operationalize feeds, rather than simply subscribing to as many as possible, is what turns raw data into real defensive value.

How It Works

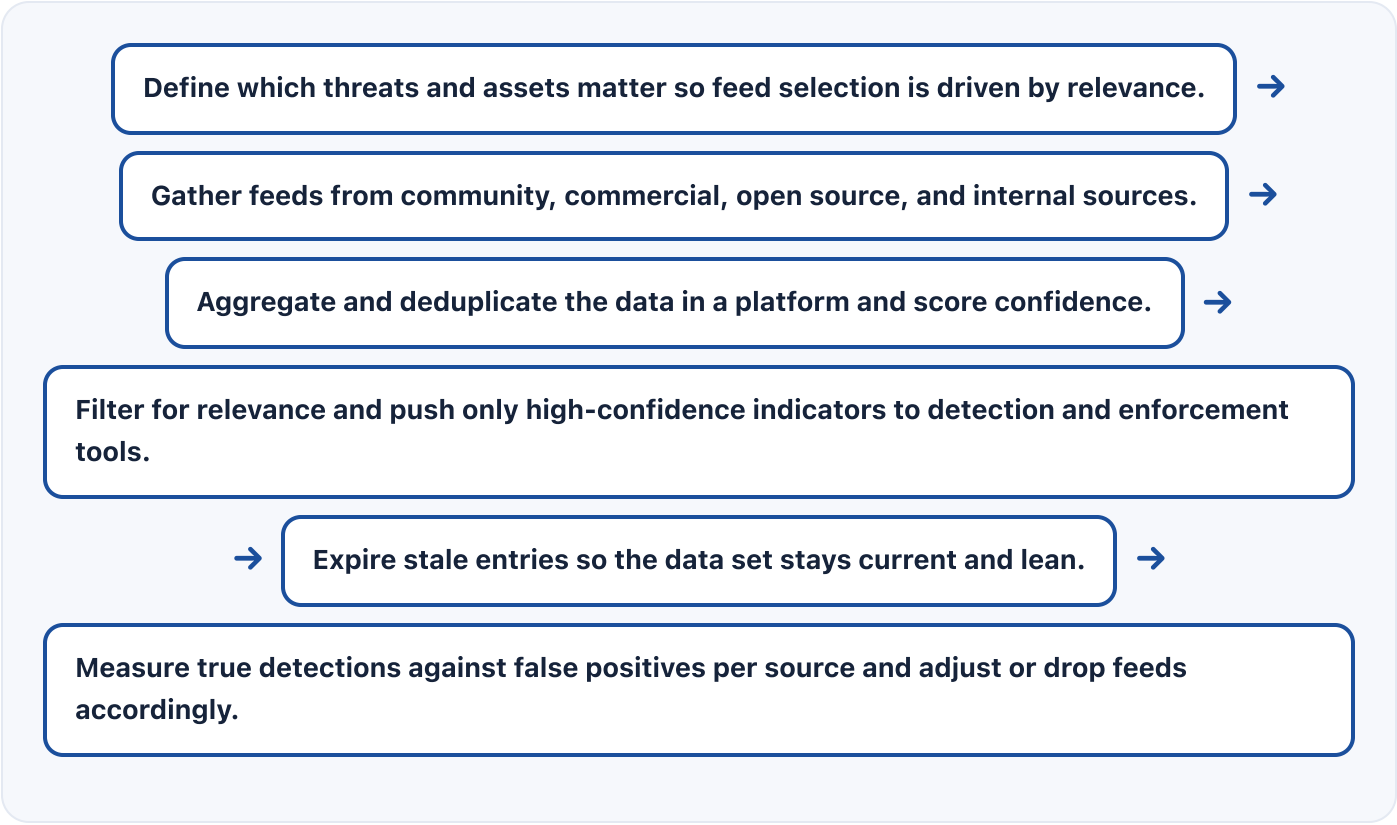
Feeds are typically pulled into a threat intelligence platform that aggregates multiple sources, removes duplicates, scores confidence, and applies context. From there the platform pushes selected, high-confidence data to the tools that enforce or detect: firewalls, DNS filters, a SIEM, or endpoint agents. Well-run programs filter aggressively so only relevant, timely, and trustworthy indicators reach production, and they expire old entries so the data set does not grow stale. Many feeds use STIX and TAXII so different tools can consume the same data consistently, and organizations often contribute their own vetted indicators back to sharing communities. The most important practice is measurement: tracking how often each feed produces a true detection versus a false positive so that sources can be tuned, kept, or dropped based on evidence rather than reputation.

Architecture Diagram



Multiple sources flow into a platform that aggregates and vets the data, then pushes only high-confidence indicators to enforcement and detection tools.

Visual Workflow



Common Attacks

- Fast-flux and rapidly rotating infrastructure that outpaces slow feeds
- Attacker use of legitimate cloud and hosting services that feeds may over-block
- Poisoning or noise designed to erode trust in a shared feed
- Reused malicious domains and IPs across campaigns that feeds can catch early
- Newly registered domains staged for phishing that timely feeds flag quickly

Common Mistakes

- Subscribing to many feeds without measuring which ones actually produce good detections
- Pushing raw feed data straight to enforcement without vetting, causing false blocks
- Ignoring relevance, so a generic feed floods analysts with irrelevant indicators
- Never expiring old entries, letting stale data accumulate and slow the pipeline
- Confusing raw feeds with finished intelligence and skipping analysis and context

Best Practices

- Select feeds by relevance to your industry, geography, and technology, not by volume
- Aggregate through a platform that deduplicates, scores confidence, and adds context
- Vet and filter data before it reaches enforcement tools to avoid false blocks
- Use STIX and TAXII so feeds are consumed and shared consistently across tools
- Expire indicators on a schedule so the data set stays current
- Measure detections versus false positives per source and keep only what earns its place

Quick Checklist

- [x] Feed selection is documented and tied to the organization's actual risk profile
- [x] A platform aggregates, deduplicates, and confidence-scores incoming data
- [x] Data is vetted before it reaches any enforcement tool
- [x] Indicators have expiration so stale data is retired automatically
- [x] True-detection and false-positive rates are tracked per feed
- [x] Internal detections are contributed back to sharing communities where appropriate

Recommended Tools

Threat intelligence platform (TIP)
Aggregates, deduplicates, scores, and distributes feed data to tools

SIEM
Consumes feeds to enrich and match live activity against known bad data

DNS and firewall filtering
Enforces blocking of malicious domains and addresses from vetted feeds

STIX and TAXII clients
Consume and share structured feed data using open standards

Industry Standards

STIX (Structured Threat Information Expression)

TAXII (Trusted Automated Exchange of Intelligence Information)

Open format for representing feed data consistently

Open protocol for transporting feed data between tools

CISA Automated Indicator Sharing
Government program for exchanging machine-readable threat data

Career Relevance

Threat feeds are the daily input for threat intelligence analysts who evaluate and operationalize sources, SOC analysts who act on feed-driven alerts, and security engineers who build and maintain the ingestion pipelines. Knowing how to judge feed quality, avoid false-block risk, and measure value is a marketable skill across security operations, and it helps GRC and AI governance professionals assess whether an intelligence program spends its effort wisely.

Interview Questions

- What is a threat feed, and how is it different from finished threat intelligence?
- How would you decide whether a given feed is worth keeping?
- What risks come from pushing raw feed data directly to enforcement tools?
- Why do STIX and TAXII matter when consuming and sharing feeds?
- How would you measure the value of a feed over time?

Related Certifications

GIAC Cyber Threat Intelligence (GCTI) | CompTIA CySA+ | GIAC Certified Incident Handler (GCIH)

Further Reading

- CISA: Automated Indicator Sharing
- OASIS: STIX and TAXII standards
- NIST: Guide to Cyber Threat Information Sharing (SP 800-150)

Key Takeaways

- A threat feed is a machine-readable stream of threat data, usually indicators, that keeps tools current.
- Feeds provide collective visibility but are raw data, not finished intelligence.
- Relevance, timeliness, and accuracy matter far more than the number of feeds.
- Vet and expire data before enforcement to avoid false positives and false blocks.
- Judging and measuring feed value is a core threat intelligence and security operations skill.

FAQ

Are more threat feeds always better?

Is a threat feed the same as threat intelligence?

How do feeds avoid blocking legitimate traffic?

Related Careers

RELATED ROLES

Threat Intelligence Analyst

Soc Analyst

Threat Hunter

Security Engineer

RELATED CERTIFICATIONS

GIAC Cyber Threat Intelligence (GCTI)

CompTIA CySA+

GIAC Certified Incident Handler (GCIH)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides

Role roadmaps

Salary data

Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Threat Feeds**
3. Go deeper: Indicators of Compromise (IOCs)
4. Go deeper: Indicators of Attack (IOAs)
5. Validate it: work toward **GIAC Cyber Threat Intelligence (GCTI)**
6. Find the role: browse current openings

RELATED SHEETS

CS-089 Indicators of Compromise (IOCs) | CS-090 Indicators of Attack (IOAs) | CS-092 OSINT | CS-088 Threat Hunting | CS-008 MITRE ATT&CK