

Threat Intelligence Feeds: a Getting Started Guide

Posted on February 27, 2025

Despite actively improving cybersecurity defenses, the cost of cybercrime only continues to grow. Statista draws a [steadily ascending graph](#), predicting that the global cost of cybercrime will go up more than a trillion \$USD in 2025 – to \$USD 10.29 trillion from 9.22 trillion in 2024. And it will continue the same way in 2026, 2027, and further on.


To avoid contributing to this growing number, organizations are switching toward proactive and even predictive cybersecurity – that is one of the main [2025 cybersecurity trends](#). Cybersecurity automation is another trend that has gained significant momentum. In their 2024 research, Wakefield Research concluded that [80% of organizations](#) planned to increase their investment in cybersecurity automation.

There's an intersection between these trends – an area of cybersecurity that belongs to both and is critically important in 2025: cyber threat intelligence feeds. This guide provides you everything you need to know about them.

What Is a Threat Intelligence Feed?

A threat intelligence feed is a continuously updated stream of data that provides information on potential and active cyber threats. This information may include indicators of compromise (IoCs) such as malicious domains, IP addresses, malware signatures, as well as attack patterns, tactics, techniques, and procedures (TTPs). Some organizations enrich their feeds with attribution details such as associated threat actor information.

These feeds offer real-time insights into emerging threats, enabling security teams to detect, analyze, and respond to new risks more effectively. By integrating threat intelligence feeds into their security infrastructure, organizations can proactively strengthen their defenses, improve incident response, and stay ahead of the adversaries.



A threat intelligence feed is a continuously updated stream of data that provides information on potential and active cyber threats.



www.whoisxmlapi.com

Types of Threat Intelligence Feeds

There are different classifications for threat intelligence feeds that one might care about. Here, we'll discuss two of these classifications: by application and by source.

Types of Threat Intelligence by Application

- **Tactical feeds.** This is the most down-to-earth, actionable threat intelligence type that

provides data for immediate threat detection and blocking. Tactical threat intelligence feeds offer IoCs such as domain names, malware hashes, and malicious IP addresses, that can be added directly to security tools such as security information and event management (SIEM) systems or firewalls.

- **Operational feeds.** This type focuses on tactics, techniques and procedures used by threat actors, as well as some additional details about attacks. Operational threat intelligence feeds are not meant to be consumed by automated tools, but rather by security practitioners such as threat hunters and incident response teams.
- **Strategic feeds.** This type covers high-level cyber risk trends to support decision-making and risk management. Strategic threat intelligence feeds may include cyber threat landscape change outlines, geopolitical risk overviews, and industry-specific security challenges. These are meant for cybersecurity decision-makers, such as CISOs.

Types of Threat Intelligence Feeds by Source

- **Open-source feeds.** These are freely available and sourced from public platforms, research organizations, and cybersecurity communities. Often, they are a product of crowd-sourced knowledge sharing – security specialists openly share their findings which are compiled into a feed. Some are offered by government agencies such as [AIS by CISA](#) or [FBI InfraGard](#). Open-source threat intelligence feeds are offered free of charge, which is one of their main advantages. The crowd-sourced ones might suffer from poor data reliability or irregular updates though.
- **Commercial feeds.** These are premium, paid feeds provided by cybersecurity vendors, offering curated, high-quality, and regularly updated threat data. The main differences between commercial and open-source feeds boils down to data reliability, exclusivity, and support. Commercial threat intelligence feeds often have much more reliable data than the open-source ones, they also come with support and service-level agreements (SLAs), ensuring their timely provision. Also, they often are unique in one way or the other. For example, WhoisXML API's [Threat Intelligence Data Feeds](#) offer high quality data about

known attacks. We also have [Predictive Threat Intelligence Feeds](#) that can assist with highlighting domains that are likely to turn malicious, even though no malicious activity has been detected yet.

- **Local/internal feeds.** These are the feeds generated and distributed by internal security teams or managed security services providers (MSSPs). The data comes from internal network logs, past security incidents, honeypots, and endpoint security data collected within the organization. Local security feeds are, on the one hand, the most relevant, on the other, they have limited scope and require a security team to maintain.

TYPES OF THREAT INTELLIGENCE FEEDS



	Open-Source & Free	Commercial	Local
Data Reliability	Low	High	High
Exclusive Data	No	Yes	Yes
Scope	Broad	Broad	Narrow

www.whoisxmlapi.com

Standards for Threat Intelligence Feeds

Since there are so many organizations and communities providing their own threat intelligence feeds, some standardizing was necessary so that the feeds are consistent, machine readable, and can be effectively shared across security tools and organizations. Below, we discuss the most

important standards for cyber threat intelligence feeds.

STIX

[Structured Threat Information Expression \(STIX\)](#) is a language and serialization format originally developed by MITRE that is used to exchange cyber threat intelligence. The format defines objects and properties that threat intelligence feed entries can have. Since 2015, the governance over the format has been transferred to OASIS Open, a global nonprofit consortium that focuses on the standard development.

Currently, STIX is at version 2.1 that has added various new objects as well as concepts such as confidence.

TAXII

[Trusted Automated Exchange of Intelligence Information \(TAXII\)](#) is an application protocol for exchanging cyber threat intelligence over HTTPS in a secure and scalable manner.

While STIX defines the structure of threat data, TAXII dictates how that data is shared. It supports two primary models: push, where threat intelligence is sent automatically to recipients, and pull, where users can request specific threat information when needed. Integrating TAXII with SIEM systems or threat intelligence platforms (TIPs) helps organizations automate threat detection and response.

TAXII is also maintained by OASIS Open and is also currently at version 2.1.

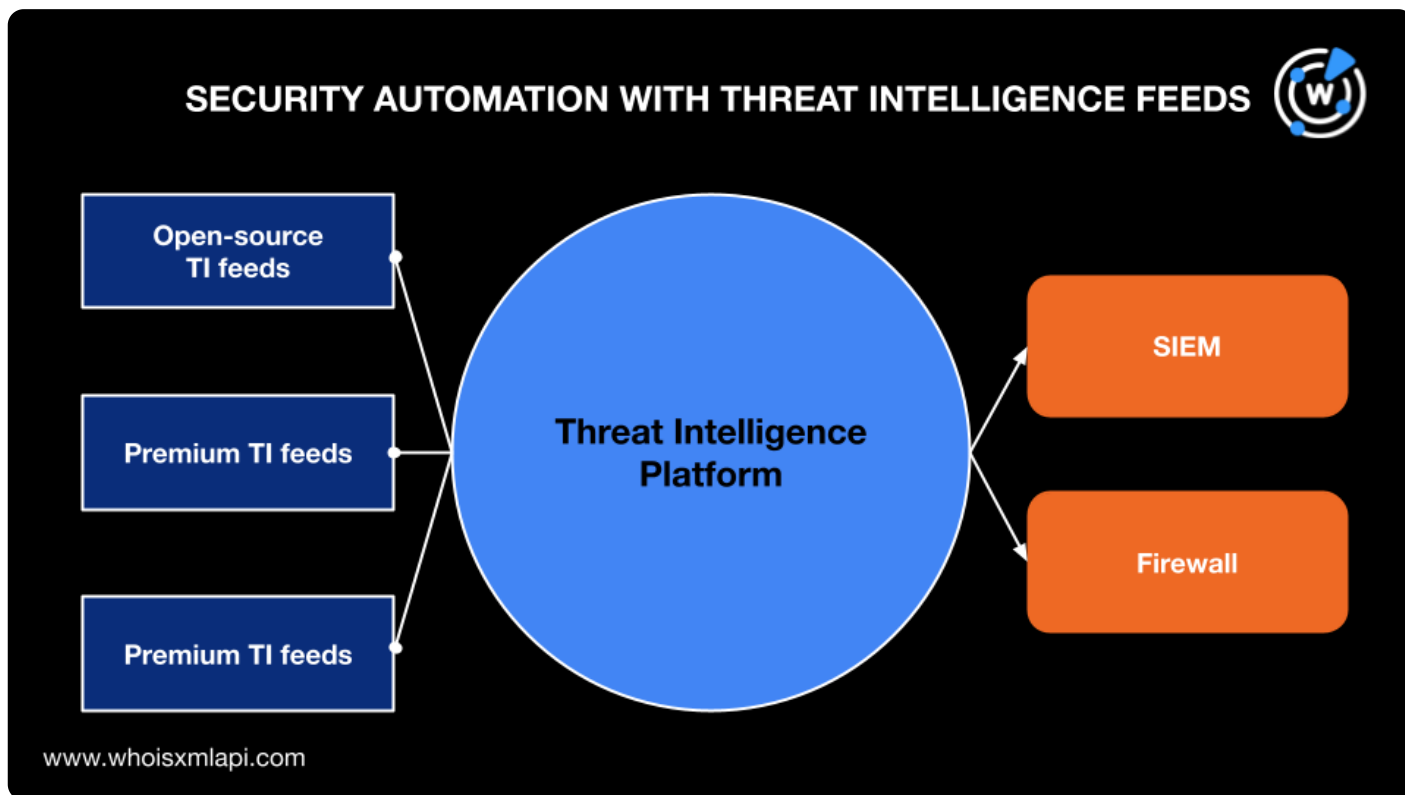
Other cyber threat intelligence standards include, for example, Open Indicators of Compromise (OpenIOC), developed by FireEye, and CybOX, also developed by MITRE and later integrated into STIX.

Cyber Threat Intelligence Formats

While standards dictate the objects that the entries can have and the way they are shared, threat intelligence feeds are delivered in traditional file formats that are easy to read for both humans and computers:

- CSV
- JSON
- RAW (TXT)

Despite the standardization efforts, many organizations and communities still deliver threat intelligence without proper formatting. So, the cybersecurity community has developed tools that connect, streamline, unify, and enrich the feeds so that the information can be fed to the cybersecurity automation tools or easily consumed by security analysts. These tools are called threat intelligence platforms. [Collective Intelligence Framework](#) is an open-source example of such a tool.



Threat Intelligence Feeds Use Cases

Proactive Threat Detection

The threat intelligence feeds main use case for organizations is using them to proactively identify potential threats before they impact their systems. By continuously looking for IoCs, such as known malware signatures or suspicious IP addresses, security teams can detect and neutralize threats in their early stages, improving the organization's overall security posture.

Incident Enrichment and Response

Security Operations Centers (SOCs) and Incident Response (IR) teams often face generic alerts

lacking context. By integrating threat intelligence feeds, these alerts can be enriched with detailed information about malicious IP addresses, domains, and attacker tactics. With this context, a generic alert about an unknown anomaly on the network becomes much more actionable, helping accelerate the investigation process and enabling security teams to prioritize and respond to threats more effectively. This part can be automated to a high extent, which, given the permanent shortage of security personnel, is really valuable.

Strategic Decision-Making

Beyond immediate threat detection, threat intelligence feeds provide insights into emerging cyber attack trends, threat actor motivations, and geopolitical risks. This strategic intelligence informs decision-makers about long-term cyber risks, guiding investments in security infrastructure and the development of policies to mitigate future threats.

Threat Hunting

Threat intelligence feeds support proactive threat hunting, where security teams actively search for hidden threats within an organization's network. By using feeds that contain IOCs, tactics, techniques, and procedures, security analysts can uncover security threats that may have evaded automated detection systems. This approach helps identify advanced persistent threats (APTs) and reduces dwell time for undetected attacks.

Third-Party Risk Management

Organizations rely on numerous third-party vendors, which, unfortunately, can introduce third-party security risks. Threat intelligence feeds help assess the cybersecurity posture of third parties by tracking malicious domains, breached credentials, or malicious activity linked to suppliers and service providers. This enables businesses to make informed decisions about vendor relationships and mitigate potential supply chain risks.

Where Does the Data in Threat Intelligence Feeds Come From?

So, threat intelligence feeds are a stream of very useful threat data. Where does this data come from though? The answer depends on the feed in question, actually, but generally, there are several main sources of data that vendors and individual cybersecurity analysts transform into actionable intelligence:

- **Honeypots.** Cybersecurity vendors deploy honeypots — decoy systems designed to lure attackers and analyze their behavior. These traps help researchers collect real-world attack data, identify new malware strains, and understand evolving tactics, techniques, and procedures.
- **Malware analysis and sandboxing.** Security researchers analyze malware samples in controlled environments (sandboxes) to extract indicators of compromise. This data is fed into threat intelligence platforms to help detect and block similar threats.
- **Passive DNS and WHOIS data.** Tracking domain registrations and DNS activity helps identify suspicious patterns. For example, we track [newly registered domains](#) in a separate feed because such data notably helps with early threat detection and brand protection. Another example of a feed based on WHOIS and passive DNS data is our [DGA early detection feed](#) of algorithmically generated domain names — threat actors often use these inherently suspicious domains for attack infrastructure. Finally, WHOIS and DNS data provides insights into domain ownership, aiding in threat attribution, so it's good to combine it with other threat intelligence sources.
- **Automated threat data collection.** Many organizations deploy sensors, intrusion detection systems (IDS), and security logs that automatically collect and report on suspicious network activity. This machine-generated intelligence feeds directly into SIEM systems and threat intelligence platforms — this is what internal feeds are often made of.

- **Dark web and cybercrime forums.** Threat intelligence vendors monitor underground forums, marketplaces, and dark web sites where cybercriminals sell exploits, stolen credentials, and malware. This helps predict emerging threats and is one of the main sources of information for strategic threat intelligence.
- **Open-source intelligence (OSINT).** Security researchers collect data from public sources such as security blogs, academic research, vulnerability disclosures, social media, and government advisories (e.g., CISA, Europol). These sources provide early warnings on emerging threats, attack trends, and vulnerabilities.

8 Open-Source and Commercial Threat Intelligence Feeds for You to Follow

1. WhoisXML API Threat Intelligence Feeds

Distribution: premium

Application type: tactical feeds

[WhoisXML API Threat Intelligence Data Feeds](#) offer a comprehensive collection of IoCs related to cyber attacks, botnets, phishing, malware, spam, and more. They come in structured formats to ensure smooth integration and offer daily updates. They offer increased visibility into malicious activities, help implement zero-trust policies and strengthen network security.

Above, we already mentioned some multi-purpose feeds that WhoisXML API offers in addition to that, such as newly registered domains feed or DGA early detection feed.

2. Open Threat Intelligence by AlienVault (OTX)

Distribution: free

Application type: tactical IoC database

[AlienVault LevelBlue Labs Open Threat Exchange \(OTX\)](#) is one of the largest open-source threat intelligence platforms, where security professionals worldwide share IoCs and cyber threat insights. Its key advantage is its community-driven model, which results in covering a broad spectrum of emerging threats. Users can contribute to and subscribe to specific “pulses” (collections of related IoCs), making it highly customizable for different security needs.

3. WhoisXML API First Watch Malicious Domain Feed (Premium)

Distribution: premium

Application type: tactical predictive feed

[First Watch](#) is WhoisXML API’s high-confidence potentially malicious domain feed based on passive DNS, WHOIS, and other internet activity data analyzed by machine learning algorithms. Unlike general domain reputation feeds, First Watch focuses on newly registered and recently active malicious domains, helping security teams know about potential threats before they even become active. This feed is an organization’s first line of defense, blocking phishing sites, malware distribution networks, and command-and-control (C2) domains. It’s a totally unique feed, with no open-source analogs.

4. AbuseCH URLhaus

Distribution: free

Application type: tactical IoC database

[URLhaus](#) is an open-source crowd-sourced project that tracks URLs used in malware distribution. What sets it apart is its focus on specific URLs rather than just domains or IPs, allowing for granular blocking of malicious content at the URL level. Security researchers and automated systems continuously contribute to this free database.

5. ThreatFox IoC Database

Distribution: free

Application type: tactical IoC database

ThreatFox is a community-powered IoC database, designed to help security teams detect and defend against malware. What makes it stand out is its broad scope, covering malware-related IP addresses, domains, and file hashes. Unlike premium feeds that require subscriptions, ThreatFox database is freely accessible, making it a valuable resource for smaller security teams and independent researchers.

6. SANS Internet Storm Center (ISC) Threat Feeds

Distribution: free (requires registration)

Application type: operational feeds

SANS ISC is a trusted source of cybersecurity intelligence collected from global honeypots and community reports. What makes ISC unique is its emphasis on exploit trends and large-scale cyber attack patterns, rather than just raw IoCs – this is more of an operational feed. It's particularly useful for tracking emerging cyber threats and understanding broader attack trends, helping organizations prepare for new risks.

7. PhishTank

Distribution: free

Application type: tactical phishing database

PhishTank is a collaborative phishing threat intelligence platform, where users submit and verify phishing URLs. It is crowdsourced, with all entries manually verified by the community, which

theoretically reduces false positives. PhishTank is widely used for web filtering and anti-phishing solutions, as its free database integrates easily into security tools.

8. OpenPhish

Distribution: free (RAW, basic data) or premium (enriched)

Application type: tactical phishing feeds and database

[OpenPhish](#) is an automated phishing feed that continuously detects and classifies phishing sites using machine learning algorithms. Unlike PhishTank, which relies on human verification, OpenPhish's AI-driven approach allows for faster and more scalable phishing detection. The free version provides basic phishing site data, while the premium version includes enriched intelligence with more details and advanced detection capabilities.

Conclusion

Threat intelligence feeds provide organizations with data for identifying and mitigating cyber threats in real time, helping them counter attacks and avoid becoming yet another victim of the growing cybercrime scene.

Open-source feeds are very useful thanks to their crowd-sourced nature and wide coverage, but are often not enough for most cybersecurity applications. Commercial feeds provide more reliable, up-to-date, and enriched data, often with exclusive insights. On top of that, to our knowledge, there are no open-source predictive feeds (yet), and these proved to be very helpful for reducing the number of incidents, so for their first line of defense organizations likely have no choice but to rely on commercial ones.

Organizations that integrate multiple feeds into their security infrastructure gain a broader view of threats, better accuracy, and stronger protection against evolving cyber risks. Combining intelligence from multiple sources—both open-source and commercial—is the only way to build a strong defense against modern threats.

Ready to step up your cyber defense game? Sign up for WhoisXML API's [threat intelligence data feeds](#) and [predictive threat intelligence feeds](#).