ANY.RUN's Threat Intelligence Feeds: FAQ

Table of Contents

1 What are ANY.RUN's TI Feeds for, and who benefits from them?

ANY.RUN's **Threat Intelligence Feeds** provide cybersecurity teams with access to real-time, unique, and verified Indicators of Compromise (malicious IPs, domains, URLs) collected from the world's largest interactive sandbox used by 15K organizations and 500K security analysts.

These feeds can be used by SOC teams, MSSPs, DFIR specialists, and CTI analysts, to monitor incidents, investigate attacks, correlate events, and enrich their own Threat Intelligence systems.

TI Feeds are also useful for security decision-makers who need reliable and up-to-date threat sources to enhance infrastructure protection.

2 What data formats do TI Feeds support?

TI Feeds are available in STIX/TAXII format for integration with TIP/CTI systems (SIEM/EDR/XDR/TIP/NDR). They are also accessible via API/SDK.

3 How often are TI Feeds updated?

Fresh IOCs are added to TI Feeds in real time (based on 16,000 new threats per day). This ensures that your defenses remain current and that you don't miss emerging malware and phishing attacks.

4 What is the false positive (FP) rate?

The false positive rate is near zero. While it's difficult to achieve an exact "zero" level, the goal is to make the feeds as "clean" as possible.

5 Can TI Feeds be filtered by industry, region, or threat type?

Currently, pre-filtering by industry or region is not available, but we plan to add this feature within the next six months.

6 Where do the indicators come from?

Indicators are derived from analyzing samples investigated in ANY.RUN's **Interactive Sandbox**. 500K analysts from 15K organizations examine malware and phishing samples from alerts and incidents in the sandbox every day to identify artifacts, network activity, and malware configurations.

The data is enriched with results from Suricata IDS, malware configurations, and other technical sources, ensuring broad coverage of threats across industries and regions. We do not track specific attacks or their actors behind them. TI Feeds reflect real malicious activities detected during sample analysis.

7 How are TI Feeds better than "raw" public feeds?

ANY.RUN's TI Feeds stand out by delivering filtered and sandbox-verified indicators, which significantly reduce false positives and ensure reliability. Unlike generic public feeds, they include unique indicators, such as those extracted from malware configurations and Suricata IDS signatures, that are often unavailable elsewhere. Each indicator is enriched with context and metadata, making analysis and response faster and more intuitive.

The feeds are designed for seamless integration, supporting API/SDK access and standard formats like STIX/TAXII, so they can be easily incorporated into most security systems. With real-time updates, new threat data is continuously added, ensuring your defenses are always up to date.

8 Can I trace the context and behavior of an indicator?

Yes, each indicator is linked to a sandbox analysis session, where you can review how the sample behaved and identify its TTPs (Tactics, Techniques, and Procedures).

9 How do TI Feeds help save SOC resources and speed up response times?

ANY.RUN's TI Feeds provide actionable indicators derived from the latest malware and phishing attacks, empowering security teams to detect and stop threats before they can impact critical infrastructure. The feeds integrate seamlessly with existing SOC systems, such as SIEM, SOAR, and TIP platforms, enabling immediate threat blocking and streamlined incident response.

Every indicator is directly linked to a detailed sandbox report, offering full threat context. This ensures security teams have the insights they need to respond quickly and with confidence.

See the **list of integrations**.

10 How can I prove the ROI of implementing TI Feeds to management?

By implementing ANY.RUN's TI Feeds, you can measure the impact on your team's efficiency by comparing workloads before and after adoption. Specifically, you can track how much time was previously spent manually verifying alerts. The feeds enable earlier detection of threats, including those that might have gone unnoticed with traditional methods, so you can act before incidents escalate.

With access to verified, high-quality threat data, your team gains greater confidence in your protective measures, ensuring decisions are based on reliable intelligence rather than assumptions.

11 What are the minimum infrastructure requirements for integration?

To integrate ANY.RUN's TI Feeds, your infrastructure should support STIX/TAXII formats or be capable of receiving indicators through API/SDK. You'll need a TIP, SIEM, or SOAR system in place to ingest and process the indicators effectively.

Since the feeds are updated frequently, your environment should be able to handle real-time data processing and synchronization. The best part is that integration is non-disruptive, TI Feeds can simply connect to your existing systems without requiring changes to your current workflows or production logic.

12 How do TI Feeds help quickly check a suspicious IP from a SIEM alert?

When a SIEM or SOAR system flags a suspicious IP, it instantly cross-references the indicator with ANY.RUN's Threat Intelligence Feeds. If the IOC is recognized, the system immediately surfaces the relevant indicator along with its metadata, giving analysts a head start.

From there, the analyst can dive into the linked sandbox session in ANY.RUN's Interactive Sandbox, where they can examine the threat's behavior in detail, including network requests, system processes, configurations, and TTPs. For deeper insight, they can explore related IOCs, connected sessions, and correlations within the TI Feeds.

With verified, actionable data at their fingertips, analysts can quickly assess the nature of the malicious activity and make informed decisions. The result? Incidents that once took hours to investigate are now resolved in minutes, eliminating the need for time-consuming manual research and accelerating response times.

13 How does using TI Feeds together with TI Lookup change SOC operations?

When TI Feeds and **TI Lookup** are used together, your SOC gains a seamless process for detecting, verifying, and responding to incidents.

TI Feeds provide real-time, actionable signals about malicious activity, while TI Lookup enables analysts to instantly verify and analyze those threats, all within the ANY.RUN ecosystem.

This powerful combination eliminates the need for manual cross-checking, reduces response times, and ensures decisions are based on accurate, context-rich intelligence. As a result, your SOC becomes capable to detect, validate, and address threats with confidence, while the resources are focused on real risks, not false alarms.

14 How does using TI Feeds and TI Lookup change SOC operations if a TIP is already in place?

For organizations already using a Threat Intelligence Platform (TIP), ANY.RUN's solutions do not just add more data, they enhance and enrich your existing capabilities.

TI Feeds integrate seamlessly into your TIP through STIX/TAXII or API/SDK, delivering fresh, sandbox-verified IOCs that expand your threat coverage.

TI Lookup adds context to indicators in your TIP, making them actionable by linking them to sandbox reports, showing complete threat behavior. This enables SOC teams to validate incidents quickly and efficiently.

As a result, your TIP evolves from a static repository into a dynamic decision-making tool, empowering SOC analysts to verify threats faster and respond with precision without disrupting their established workflows.

15 Can I test TI Feeds before purchasing?

Yes, you can contact sales for a **14-day trial**. You can also manually **download a demo sample**.

Integrate TI Feeds in your SOC

Request a trial by reaching out to ANY.RUN's experts via the **official form** or use a QR code.