



ANY.RUN's TI Feeds:

Integration with Rapid7

Configuration guide



Threat Intelligence Feeds (TI Feeds)

TI Feeds help MSSPs and SOCs fortify their security with filtered, high-fidelity indicators of compromise (IPs, domains, URLs) enriched with threat context from ANY.RUN's Interactive Sandbox.

Sourced from real-time sandbox investigations of active attacks across 16,000+ organizations, TI Feeds integrate seamlessly with SIEMs/XDRs/firewalls and other security solutions to monitor and identify malware and phishing threats.

ANY.RUN's feeds are updated every two hours, allowing you to track threats as they emerge, develop, and spread to take critical security actions early.

- **Unique data:** Fresh indicators from live detonations of attacks with links to sandbox sessions with full threat context, including TTPs.
- **No false alerts:** TI Feeds provide reliable IOCs with a near-zero false positive rate thanks to pre-processing.
- **Prioritization of incidents:** SOC teams use TI Feeds as part of alert triage, incident response, and proactive hunting to effectively handle urgent threats.

TI Feeds are available for integration using API or SDK and support TAXII protocol. For more details, feel free to [contact us](#).

How to Connect TI Feeds to Rapid7

1. Open your Rapid7 environment and go to the **Intelligence Hub** tab. In the **Sources** section, click **Add Feed**.

The screenshot shows the Rapid7 Intelligence Hub interface. The left sidebar contains navigation options: Insight Platform Home, THREAT COMMAND, INTELLIGENCE HUB (highlighted with a red box and '1'), IOC Summary, IOCs, Investigation, Threat Library, Sources (highlighted with a red box and '2'), Integrations, AUTOMATION, and SETTINGS. The main content area displays a table of threat intelligence feeds under the 'Allowlist' tab. The table includes columns for Confidence, Feed name, Last update, and Status. Feeds listed include E-ISAC, FS-ISAC, GovCERT.ch, Guardicore, H-ISAC, LS-ISAO, RH-ISAC, SWIFT-ISAC, and ThreatConnect. Below this, there are sections for STIX/TAXII feeds (1), MISP servers (0), and Public feeds (22). The 'Add Feed' button is highlighted with a red box and '3'.

Confidence	Feed name	Last update	Status
● ● ●	E-ISAC	● Feed disabled	●
● ● ●	FS-ISAC	● Feed disabled	●
● ● ●	GovCERT.ch	● Feed disabled	●
● ● ●	Guardicore	● Feed disabled	●
● ● ●	H-ISAC	● Feed disabled	●
● ● ●	LS-ISAO	● Feed disabled	●
● ● ●	RH-ISAC	● Feed disabled	●
● ● ●	SWIFT-ISAC	● Feed disabled	●
● ● ●	ThreatConnect	● Feed disabled	●

STIX/TAXII feeds (1)

Confidence	Feed name	Last update	Status
● ● ●	ANY.RUN	11 hours ago	●

MISP servers (0)

No feeds have been added. To add a feed, click Add Feed.

Public feeds (22)

These are public feeds provided by external sources and are not curated by Rapid7. While they can offer broad coverage, they may include noisy or low-quality data, potentially leading to false positives. Enable with caution based on your specific needs.

Confidence	Feed name	Last update	Status
● ● ●	AlienVault OTX	● Feed disabled	●

2. Configure the integration by filling in the required fields.

- Enter a **Name** for the feed and the following **URL**:
`https://api.any.run/v1/feeds/taxii2`
- Set the **Confidence level** to the maximum and enable **I have credentials to this feed**.
- Enter the **Username** and **Password** for your ANY.RUN account with access to TI Feeds.
- Click **Test Credentials**, then click **Next**.

3. Select the feed collections you want to include: All indicators, IPs, Domains, or URLs. We recommend choosing **All indicators**.

Collection ID	Collection Name
☒ 3dce855a-c044-5d49-9334-533...	All indicators
☐ 55cda200-e261-5908-b910-f0e...	IPs collection
☐ 2e0aa90a-5526-5a43-84ad-3d...	Domains collection
☐ 05bfa343-e79f-57ec-8677-312...	URLs collection

4. The setup is complete. Once the feed loads, indicators from ANY.RUN TI Feeds will appear in the **IOCS** section. You can now use them in your daily SOC workflows and detection rules.

IOCS Customer Portal Any.Run Analyst

Search Type Severity Reporting Feeds Last Reported Allowlist More (6) Clear Filters Export CSV

56 IOCs (sorted by last reported)

☐ IOC

☐ 18.231.131.170

☐ xn-xzuremsst-5

☐ https://xelexe...

☐ 208.91.199.91

☐ rioricoacademy

☐ bsbjaeimfa.actu

☐ https://whoops...

☐ financeline.voic

☐ login.voicemsg-

☐ khalilelabed.com

☐ nbikbyrvaj.mypromed.com

208.91.199.91

High

State: Active

Last reported: Sep 12, 2026 | 4:16 AM

MITRE tags: N/A

Kill Chain tags: N/A

Related cyberterms: N/A

Investigation map

Recent IOC events

Sep 12, 2026 | 12:46

IOC severity was updated to High

Sep 12, 2026 | 04:16

Reported by the feed, ANY.RUN

Dec 08, 2022 | 05:45

IP address resolved to ct3233.ramapuis1000.com

[Investigate IOC](#)

reported	Last reported	State	Policy rules	System/User tags
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
29, 2025	Sep 12, 2026	✓	N/A	N/A
15, 2020	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A
12, 2026	Sep 12, 2026	✓	N/A	N/A

If you have any questions,
contact us via [this form](#) or write to techsupport@any.run