



ANY.RUN's TI Feeds: Integration with SentinelOne

Configuration guide

Table of Contents

Threat Intelligence Feeds (TI Feeds)	3
How to Integrate TI Feeds with SentinelOne	3-12
↳ Installation and configuration	3-4
ANY.RUN's TI Feeds collections	5-6
Browsing indicators	6-9
Detection of ingested IOCs	10-12

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 15,000+ 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.

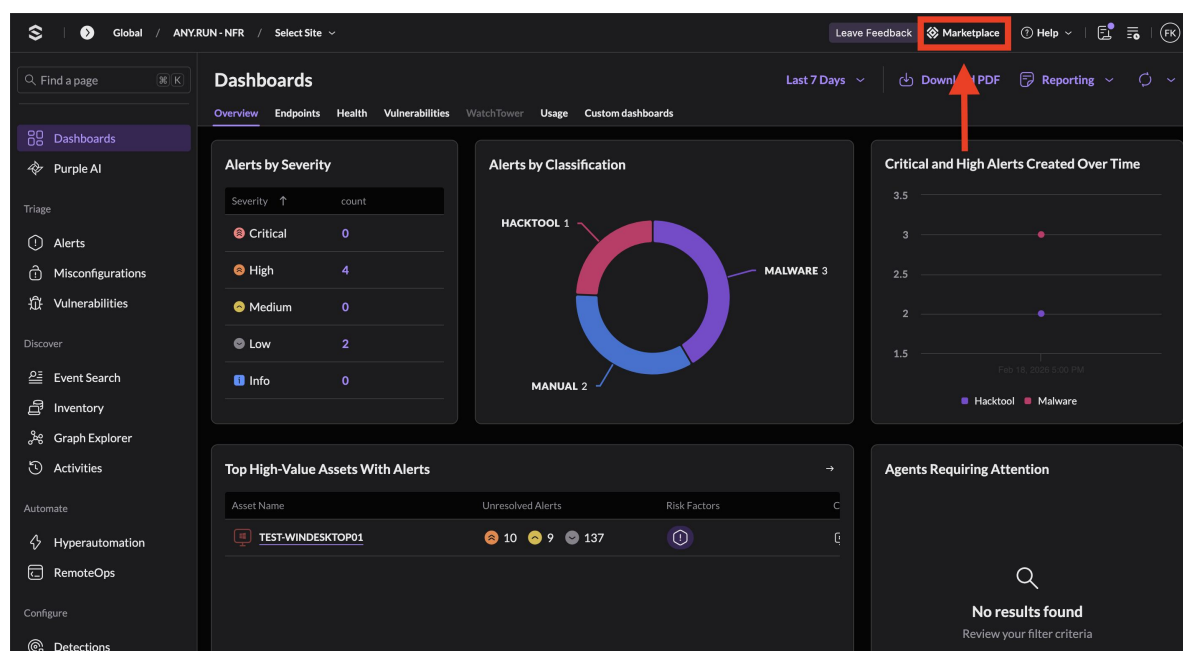
TI Feeds are available for integration using API or SDK and support TAXII protocol.

➡ For more details, feel free to [contact us](#).

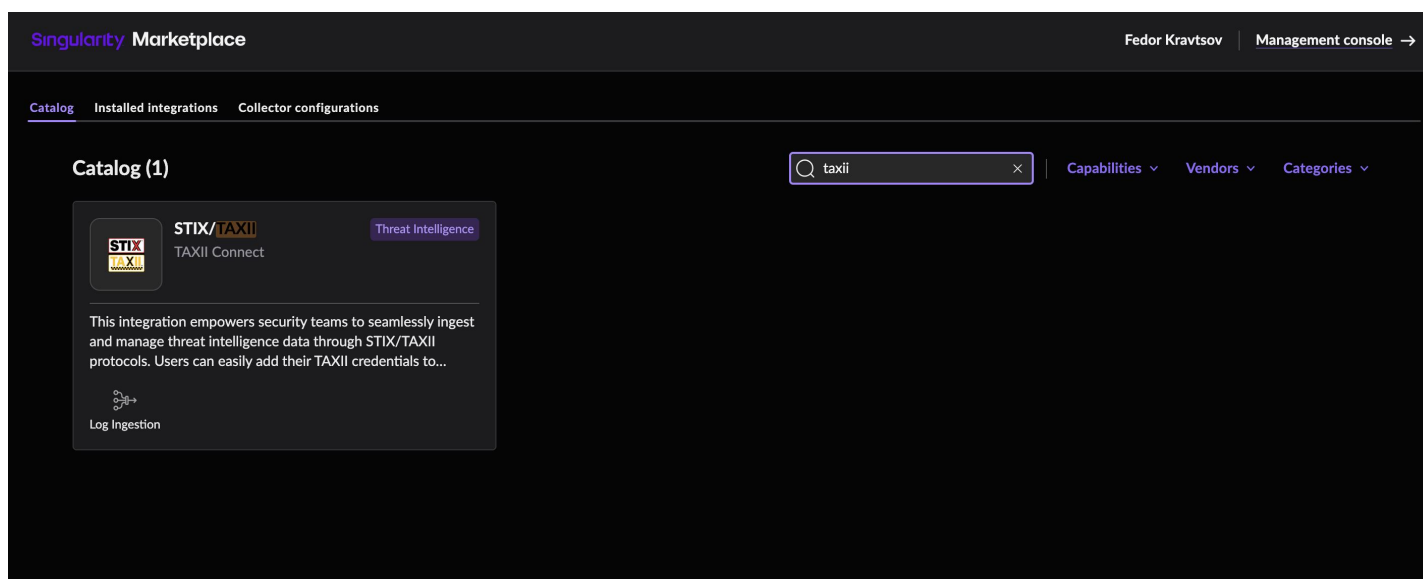
How to Integrate TI Feeds with SentinelOne

Installation and configuration

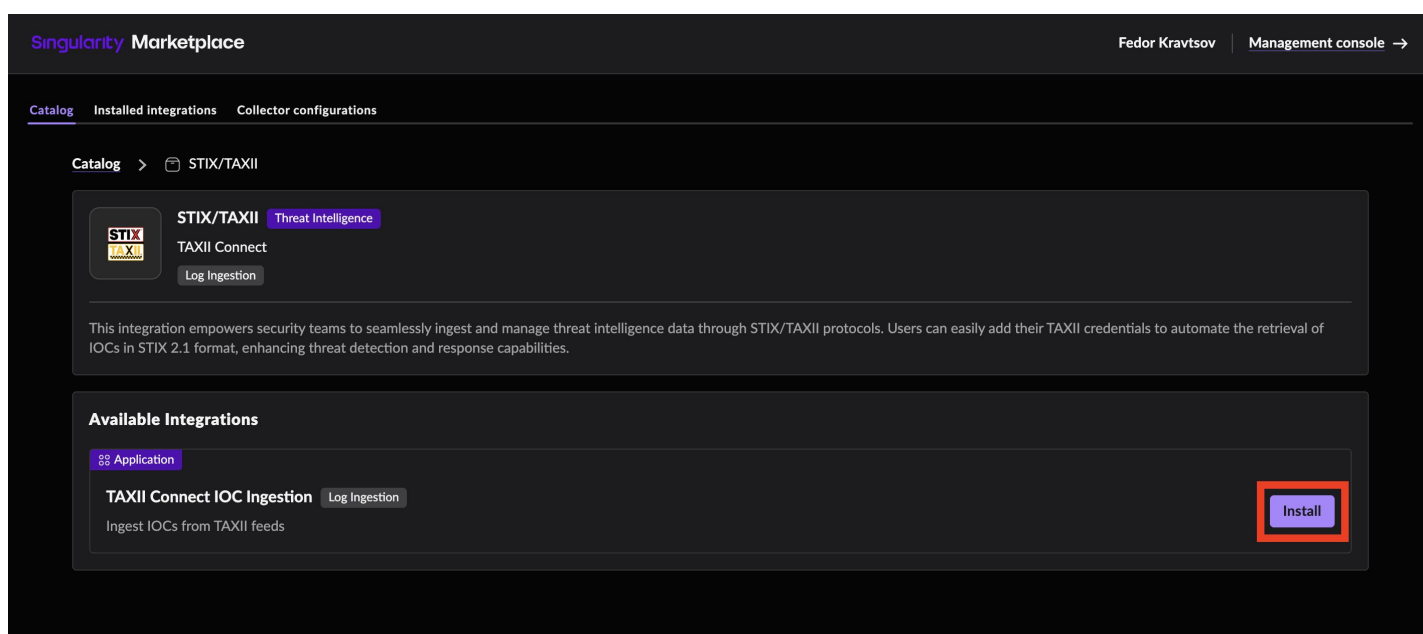
1. Open the SentinelOne **Management Console** and go to **Marketplace**.



2. Find the **STIX/TAXII** integration in the catalog and open it.



3. Install **TAXII Connect IOC Ingestion**.



4. In the **Add Configuration** window, fill out the following fields:

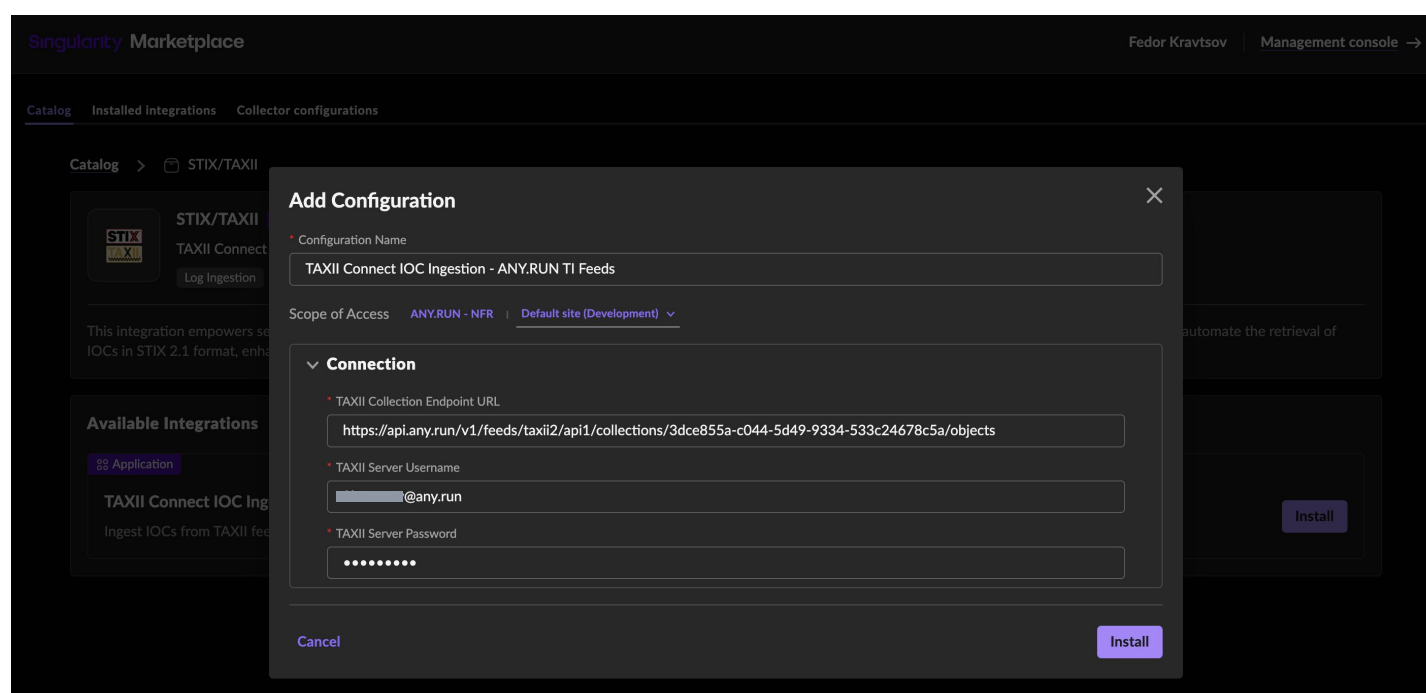
- **Configuration Name:** Name your configuration
- **Scope of Access:** Select the appropriate scope.
- **Endpoint URL:** Enter the URL for ANY.RUN's TI Feeds collection. See collection IDs below.
- **TAXII Server Username & Password:** Use the username and password provided in the access credentials email sent after your TI Feeds access was activated.

ANY.RUN's TI Feeds collections

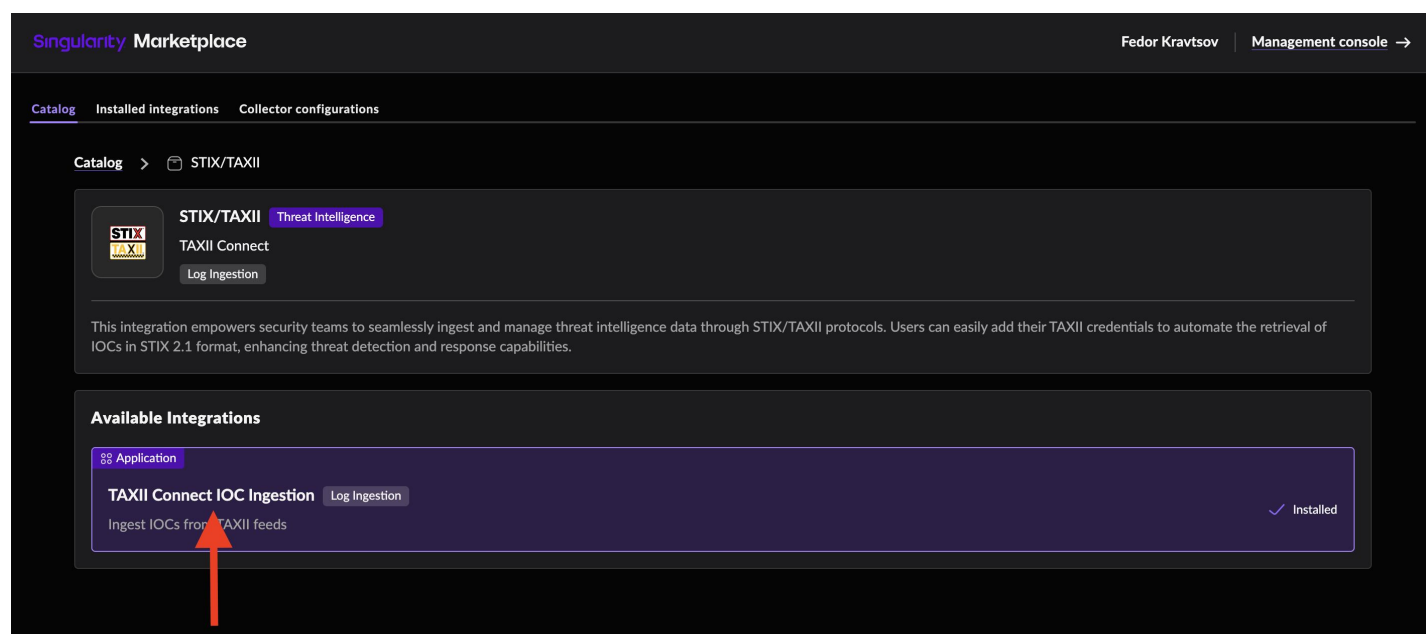
Via this link, you can explore information about all collections hosted under the ANY.RUN API Root, including each collection's ID, which is required to request objects from it:

https://api.any.run/v1/feeds/taxii2/api1/collections/{collection_id}/objects

Name	Description	ID
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs	05bfa343-e79f-57ec-8677-3122ca33d352



5. Once the connector is installed, open it.



6. Confirm its status is **Active** and click **View Logs** to verify the connector's activity.

The screenshot shows the Singularity Marketplace interface. The user is logged in as Fedor Kravtsov and is in the Management console. The breadcrumb trail is: Catalog > STIX/TAXII > TAXII Connect IOC Ingestion. The connector is listed as 'TAXII Connect IOC Ingestion' with a 'Threat Intelligence' tag and a 'Log Ingestion' button. Below this, there is a section for 'Configuration (1)' showing one configuration item: 'TAXII Connect IOC Ingestion - ANY.RUN TI Feeds'. This configuration is for the 'Global / ANY.RUN - NFR / Default site (Development)' and was last updated on Feb 19, 2026. The status is 'Active' (indicated by a toggle switch) and there is a 'View Logs' button. An orange arrow points to the 'View Logs' button.

7. Ensure that your connection is stable and the indicators are being successfully ingested.

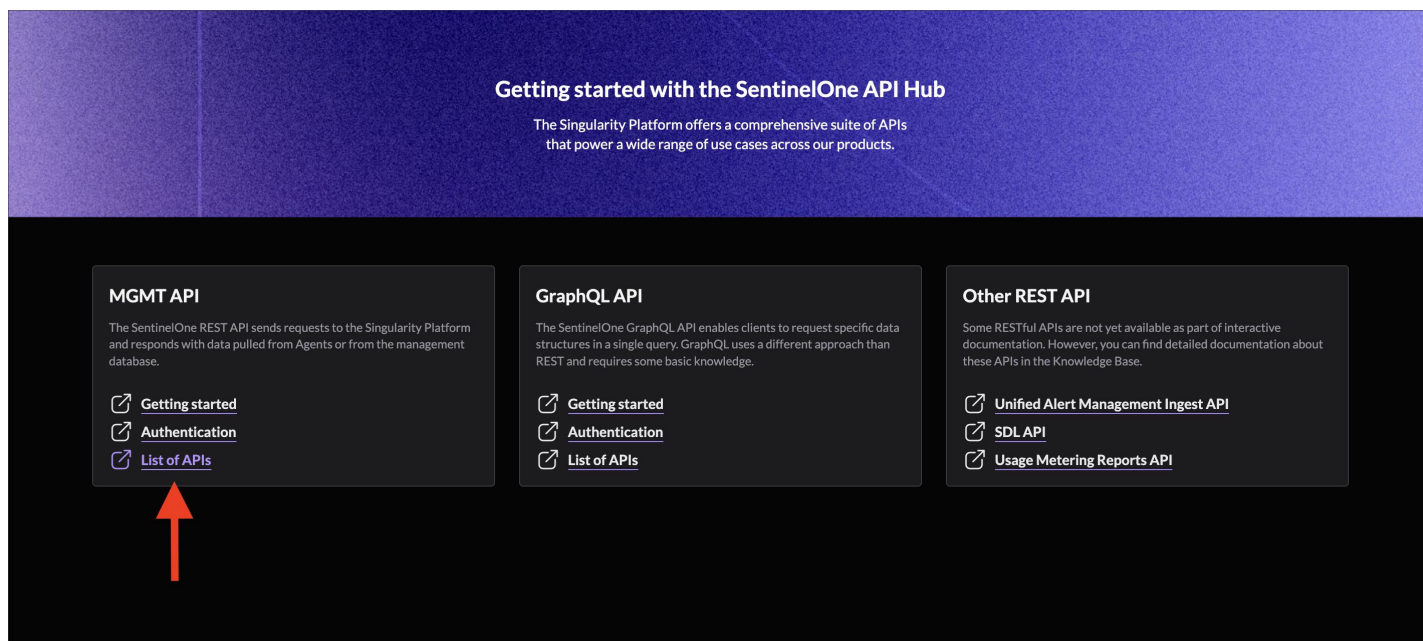
Note: Indicators are updated every 5 minutes. You can monitor the updates via **View Logs**.

Browsing indicators

1. Open the SentinelOne **Management Console**. From the **Help** dropdown menu, select **API Hub**.

The screenshot shows the SentinelOne Management Console interface. The user is logged in as 'Global / ANY.RUN - NFR / Select Site'. The 'Help' dropdown menu is open, showing options: Offline help, Customer portal, API Hub (highlighted with an orange box), Keyboard shortcuts, SentinelOne status, MITRE ATT&CK®, and About. The main dashboard displays various security metrics and charts, including 'Alerts by Severity', 'Alerts by Classification', 'Top High-Value Assets With Alerts', and 'Agents Requiring Attention'.

2. In the **MGMT API** section, click **List of APIs**.



3. Go to **Threat Intelligence** tab and click **Get IOCs**.

MGMT API

2.1

Search

Settings

Sites

System

Tag Manager

Tags

Tasks

Threat Intelligence

Create IOCs

Create IOCs from STIX bundle

Create Threat Intelligence user config

Delete IOCs

Delete Threat Intelligence user config

Get IOCs

Get Threat Intelligence user config

Threat Notes

Threats

Unprotected Endpoints Discovery

Updates

Users

Download PDF version 2.1

Download API Swagger File

Overview

GETTING STARTED WITH THE

SentinelOneAPI

The SentinelOne REST API sends requests to your Management Server and responds with data that the management pulled from Agents or from the management database.

To authenticate:

Every API call requires authentication with an API Token, generated for one Console user or service user.

1. Generate an API Token:
POST `https://your_management_url/web/api/v2.0/users/generate-api-token`
2. Use the token in the request header:
Authorization: `ApiToken API_TOKEN_VALUE`

Note: To learn about more token options, see [the Knowledge Base](#).

Common Query Parameters

Param	To	Valid Values	Example	Notes
limit	See more than ten items.	integer 1 - 100	GET <code>https://<URL>.sentinelone.ne...</code>	Returns the first 50 items. Maxim
skip	See items after a known nu...	integer 1 - 1000	GET <code>https://<URL>.sentinelone.ne...</code>	Skips the first 10 items and retur
cursor	See next page of unknown n...	string value of "nextCursor"...	GET <code>https://<URL>.sentinelone.ne...</code>	Returns the next page of data of

4. Click **Run on console**.

MGMT API 2.1

Search

Settings Sites System Tag Manager Tags Tasks Threat Intelligence

Create IOCs
Create IOCs from STIX bundle
Create Threat Intelligence user config
Delete IOCs
Delete Threat Intelligence user config
Get IOCs
Get Threat Intelligence user config

Threat Notes Threats Unprotected Endpoints Discovery Updates Users VCS Integration

Get IOCs
GET /web/api/v2.1/threat-intelligence/iocs

Get the IOCs of a specified Account that match the filter.
Note: Using creationTime to sort results has been deprecated and should not be used. In the future, the ability to sort by creationTime will be removed. Please sort by uploadTime or updatedAt as an alternative.

Required Permissions
• Threat Intelligence.view

Response Messages
200 Success
400 Invalid user input received. See error details for further information.
401 Unauthorized access - please sign in and retry.

Run on console

Response Sample

```
1 {
2   "errors": [
3     {
4       "type": "object"
5     }
6   ],
7   "pagination": {
8     "totalItems": 580,
9     "nextCursor": "YWdlbnRfaWQ6NTgwMjkzODE="
10  },
11  "data": [
12    {
13      "reference": [
14        {
15          "type": "string",
16          "x-nullable": true,
17          "description": "External reference as"
18        }
19      ],
20      "description": "string",
21      "validUntil": "2018-02-27T04:49:26.257525Z",
22      "method": "EQUALS",
23      "parentScopeId": "225494730938493804",
24      "updatedAt": "2018-02-27T04:49:26.257525Z",
25      "pattern": "string",
26    }
27  ]
28 }
```

Create IOCs
POST /web/api/v2.1/threat-intelligence/iocs

Add an IoC to the Threat Intelligence database.
These values under data are required fields: "source", "type", "value", and "method".
"Type" and "method" must be in upper case.
The "validUntil" field is mandatory, and must contain a date, for example, 2021-03-20 09:14:47.779000. "validUntil" determines when the IOC expires.
If the expiration date ("validUntil") is left blank, by default it will be the upload date plus a default offset value:

Body Sample

```
1 {
2   "filter": {
3     "accountIds": [
4       "2174499989004601003"
5     ]
6   },
7   "data": [
8     {
9       "reference": [
10        {
11          "type": "string",
12          "x-nullable": true,
13          "description": "External reference as"
14        }
15      ],
16      "description": "string",
17      "validUntil": "2018-02-27T04:49:26.257525Z",
18      "method": "EQUALS",
19      "parentScopeId": "225494730938493804",
20      "updatedAt": "2018-02-27T04:49:26.257525Z",
21      "pattern": "string",
22    }
23  ]
24 }
```

5. Enter your site ID in **siteIds** field.

Get IOCs

GET /web/api/v2.1/threat-intelligence/iocs

severity array

A list of severities to filter by (0-7)

siteIds array

List of Site IDs to filter by. Example: "4,2,6,4,1,8,0,3,0,2,1,2,0,7,3,7,6,2".

skip integer

Skip first number of items (0-1000). To iterate over more than 1000 items, use "cursor". Example: "150".

skipCount boolean

Please Select...

If true, total number of items will not be calculated, which speeds up execution time.

sortBy string

Please Select...

The column to sort the results by. Example: "id".

sortOrder string

Run API query

URL

Status code

RESPONSE

1

6. Enter *STIX Import* into the **source** field and click **Run API query**.

Get IOCs

GET /web/api/v2.1/threat-intelligence/iocs

sortBy string
Please Select...
The column to sort the results by. Example: "id".

sortOrder string
Please Select...
Sort direction. Example: "asc".

source array
STIX Import
List of the sources of the identified Threat Intelligence indicator. Example: "AlienVault".

tenant boolean
Please Select...
Indicates a tenant scope request

threatActors_in array
A list of threat actors to filter by

threatActorTypes_in array

Run API query

URL **Copy URL**

Status code

RESPONSE **Copy Response**

1

7. You'll see a **Get IOCs** window with **JSON-formatted** data on indicators from ANY.RUN's TI Feeds.

All IOCs imported from ANY.RUN's TI Feeds will now be evaluated and detected by SentinelOne.

Get IOCs

GET /web/api/v2.1/threat-intelligence/iocs

STIX Import
List of the sources of the identified Threat Intelligence indicator. Example: "AlienVault".

tenant boolean
Please Select...
Indicates a tenant scope request

threatActors_in array
A list of threat actors to filter by

threatActorTypes_in array

Run API query

```

3  {
4    "batchId": "atmtn0000000c8ae6fbbbaa29ae2b03c4262b",
5    "campaignNames": [],
6    "category": [],
7    "creationTime": "2026-01-07T05:03:20.579000Z",
8    "creator": "any.run",
9    "description": null,
10   "enabled": null,
11   "externalId": "indicator--374be77b-b9ea-5b84-ba64-7b732406",
12   "intrusionSets": [],
13   "labels": [
14     "arkei"
15   ],
16   "malwareNames": [],
17   "metadata": "",
18   "method": "EQUALS",
19   "mitreTactic": [],
20   "name": null,
21   "originalRiskScore": 100,
22   "parentScopeId": "any.run",
23   "pattern": "[url:value = 'https://c.im/@xiteb15011']",
24   "patternType": "stix",
25   "reference": [],
26   "scope": "site",
27   "scopeId": "any.run",
28   "source": "STIX Import",
29   "threatActorTypes": [],
30   "threatActors": [],
31   "type": "URL",
32   "updatedAt": "2026-01-07T07:20:21.970560Z",
33   "uploadTime": "2026-01-07T06:22:07.573346Z",
34   "uuid": "d353a071b98716b1a88eb82ba4c9a91e",
35   "validUntil": "2026-04-07T07:20:21.970560Z",
36   "value": "https://c.im/@xiteb15011"
37 }

```

Detection of ingested IOCs

- If an indicator is detected in logs from your endpoints, an **Alert** will be created in your Management Console.

The screenshot shows the ANY.RUN Alerts management console. The left sidebar contains navigation links for Dashboards, Purple AI, Triage (Alerts, Misconfigurations, Vulnerabilities), Discover (Event Search, Inventory, Graph Explorer, Activities), Automate (Hyperautomation, RemoteOps), and Configure (Detections). The main panel displays the Alerts section with a search bar and filters. A table lists alerts, with the first row highlighted: 'Threat Intelligence Indicator Match' with a severity of 'Low' and target asset 'TEST-WINDESKTOP01'.

Reported Time	Alert Name	Severity	Mitigation Sta...	Target Asset	Product
Feb 18, 2026 5:30:15 PM	Threat Intelligence Indicator Match	Low		TEST-WINDESKTOP01	STAR

- Here you can see an Alert that was generated because an indicator was detected in logs:

The screenshot shows the details of the 'Threat Intelligence Indicator Match' alert. The left sidebar is the same as the previous screenshot. The main panel displays the alert details for the IP address 178.16.53.33. The 'Event Search' link is highlighted with a red box and an arrow. The 'Indicator Details' section shows the following information:

Indicator Details	
Name	IPV4
Type	IPV4
Category	-
Description	-
Scope	-
External ID	indicator--119afafd-6cca-5678-9ff9-334e0f7322ec
Creator	@any.run
Upload Time	Jan 7, 2026
Update Time	Feb 11, 2026

The 'Associations' section shows the following information:

Associations	
Campaign	-
Threat actors	-

- You can perform initial incident response in SentinelOne via **Mitigate**, **Actions**, or **Automate**.

The screenshot shows the ANY.RUN SentinelOne alert interface. The left sidebar contains navigation options: Dashboards, Purple AI, Triage (Alerts, Misconfigurations, Vulnerabilities), Discover (Event Search, Inventory, Graph Explorer, Activities), Automate (Hyperautomation, RemoteOps), and Configure (Detections). The main panel displays a 'Threat Intelligence Indicator Match' alert for 'ANY.RUN - NFR/Default site (Development)/Default Group'. The alert has a severity of 'Low', detected by 'Platform Rule' on 'Feb 18, 2026 5:30:15 PM'. The status is 'New', assigned to 'Unassigned', and the analyst verdict is 'Undefined'. The 'Overview' tab is active, showing details like Detection Type (Rule), Storyline ID (9A76D38991AC32E2), Vendor (SentinelOne), and Product (STAR). It also shows the Alert Footprint with 16 instances and impacted assets. A table at the bottom shows threat intelligence data with a risk score of 100 and IOC value 178.16.53.33.

- Additionally, you can click an indicator and explore related events from your endpoint for rapid investigation of a potentially dangerous activity and to get the final verdict.

This screenshot is similar to the previous one, showing the same SentinelOne alert interface. However, the 'Threat Intelligence' table at the bottom is highlighted with a red box. Within this table, the IOC value '178.16.53.33' is highlighted with a white box, indicating the specific indicator being investigated.

Global / ANY.RUN - NFR / Select Site

Leave FeedbackMarketplaceHelpPreferencesSaveCopy LinkDocumentationPowerQuery

Find a page

Event Search

SOURCES

SentinelOne

FIELDS

Filter Fields

dst.ip.address1

dst.port.number6

endpoint.name1

endpoint.os1

event.category1

event.network.connectionStatus2

event.network.direction1

event.network.protocolName6

event.type1

src.ip.address1

src.port.number9

src.process.cmdline2

src.process.name3

src.process.parent.uid3

src.process.user2

account.id1

account.name1

agent.uid1

agent.version1

dataSource.category1

2EDR#ip = "178.16.53.33"Last 72 hoursSearch

All Events9Network Actions9

9 matching recordsFeb 16, 2026 6:50 PM - Feb 19, 2026 6:50 PM[UTC+4] - 1 hour / barShow timelineShow Graph

Actions

No Items Jump to <<OldestMost Recent>>Oldest FirstWrapping rowsSettings

Log Event

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='chrome.exe' | src.process.user='TEST-WINDESKTOP\user'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='chrome.exe' | src.process.user='TEST-WINDESKTOP\user'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='Advanced_IP_Scanner_2.5.4594.1.tmp' | src.process.user='TEST-WINDESKTOP\user'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='Advanced_IP_Scanner_2.5.4594.1.tmp' | src.process.user='TEST-WINDESKTOP\user'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='Advanced_IP_Scanner_2.5.4594.1.tmp' | src.process.user='TEST-WINDESKTOP\user'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='Advanced_IP_Scanner_2.5.4594.1.tmp' | src.process.user='TEST-WINDESKTOP\user'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' | src.process.parent.name='ntoskrnl.exe' | src.process.user='SYSTEM'

endpoint.name='TEST-WINDESKTOP01' | event.type='IP Connect' | dst.ip.address='178.16.53.33' |

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

12/12