



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.

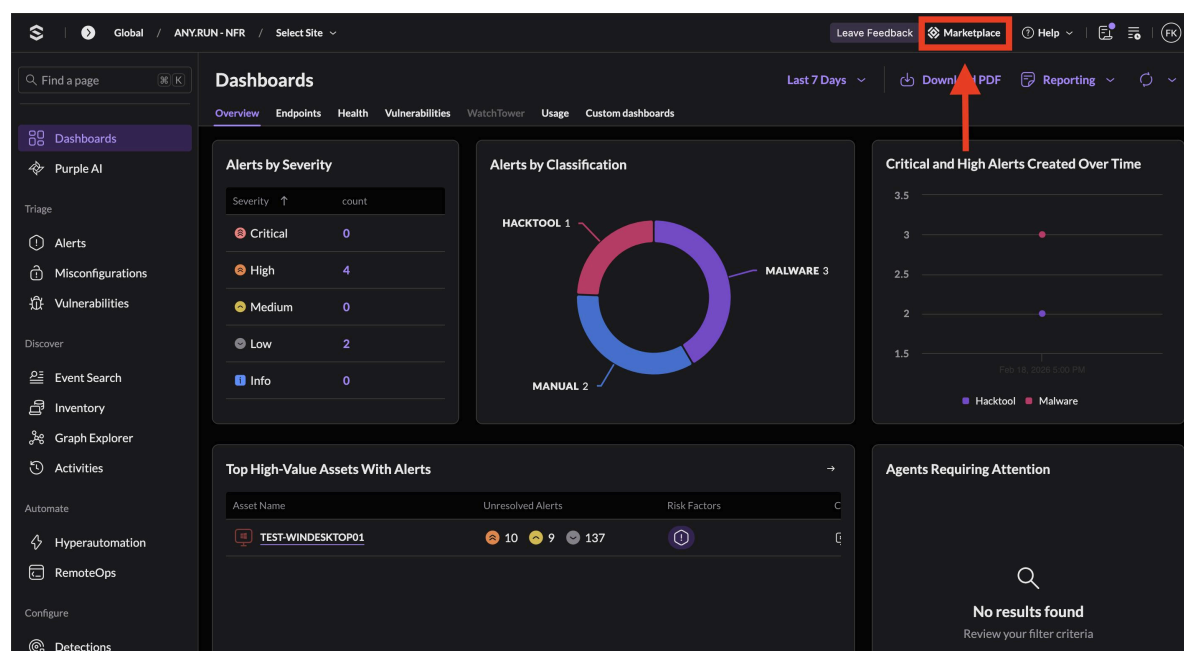
TI Feeds are available for integration using API or SDK and support TAXII protocol.

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

How to Integrate TI Feeds with SentinelOne

Installation and configuration

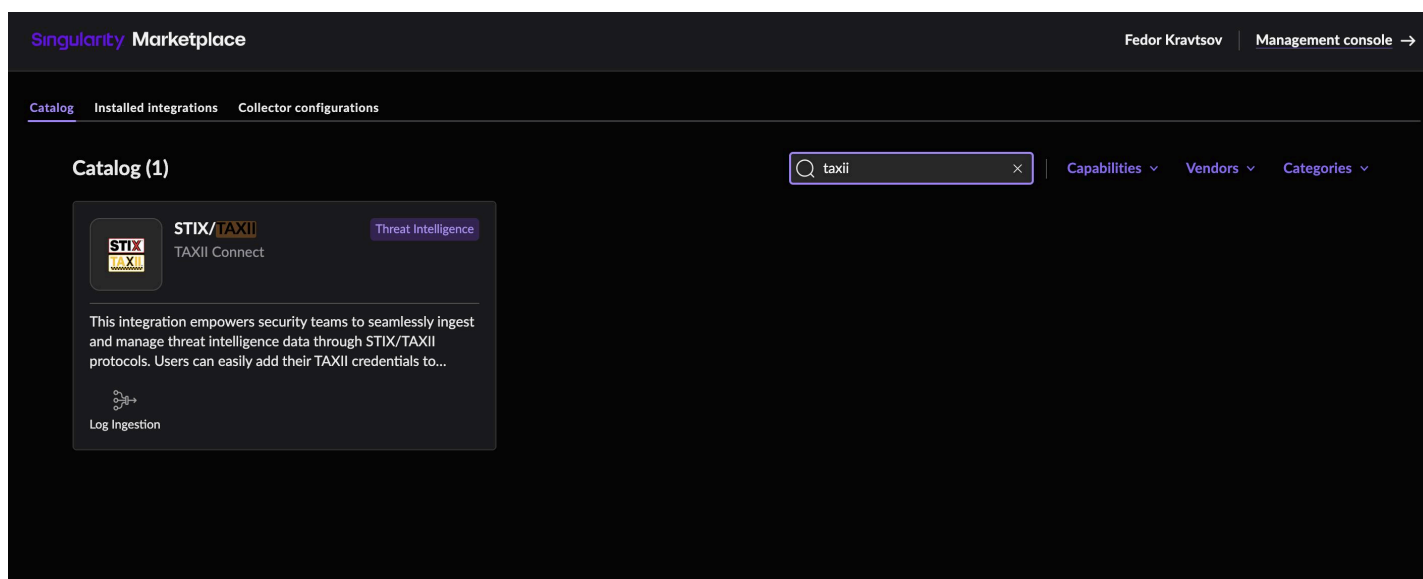
1. Open the SentinelOne **Management Console** and go to **Marketplace**.



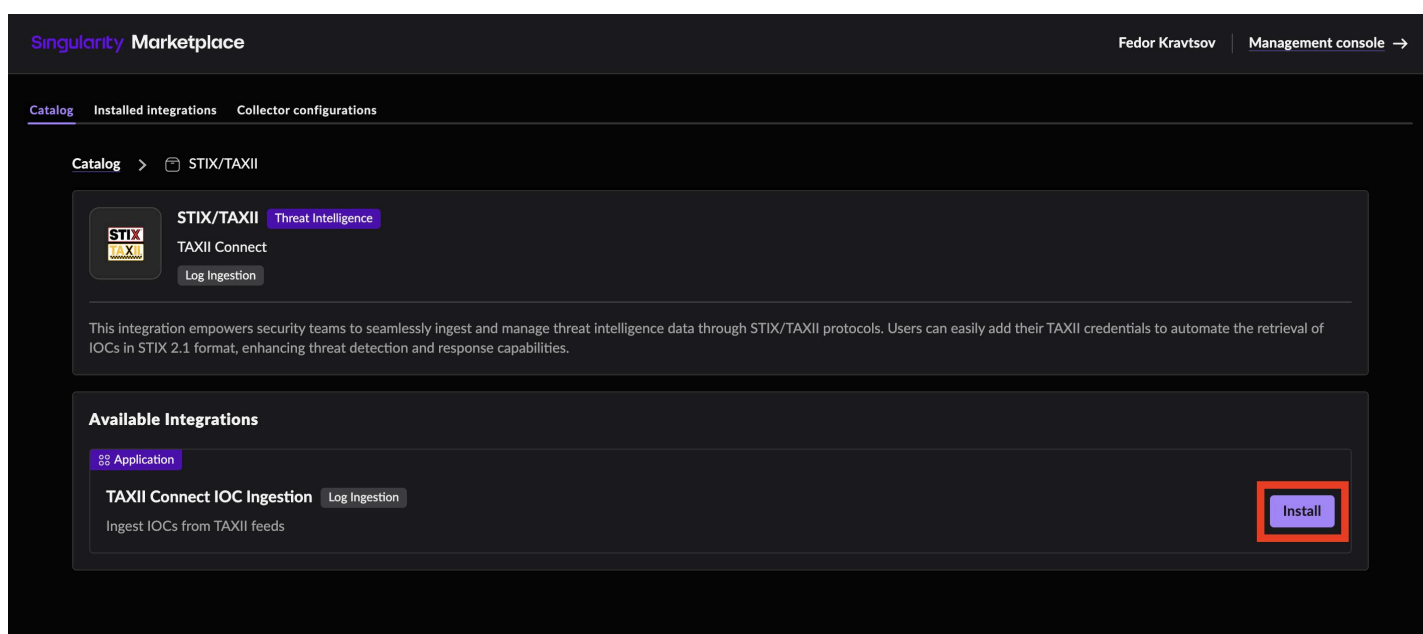
The screenshot displays the SentinelOne Management Console interface. The top navigation bar includes 'Leave Feedback', 'Marketplace' (highlighted with a red box and an arrow), 'Help', and other utility icons. The main dashboard is divided into several sections:

- Alerts by Severity:** A table showing the count of alerts for each severity level.
- Alerts by Classification:** A donut chart showing the distribution of alerts by classification: HACKTOOL 1, MALWARE 3, and MANUAL 2.
- Critical and High Alerts Created Over Time:** A line chart showing the number of critical and high alerts created over time.
- Top High-Value Assets With Alerts:** A table listing assets with high-value alerts, including 'TEST-WINDESKTOP01' with 10 unresolved alerts and 137 risk factors.
- Agents Requiring Attention:** A section indicating 'No results found' for agents requiring attention.

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:

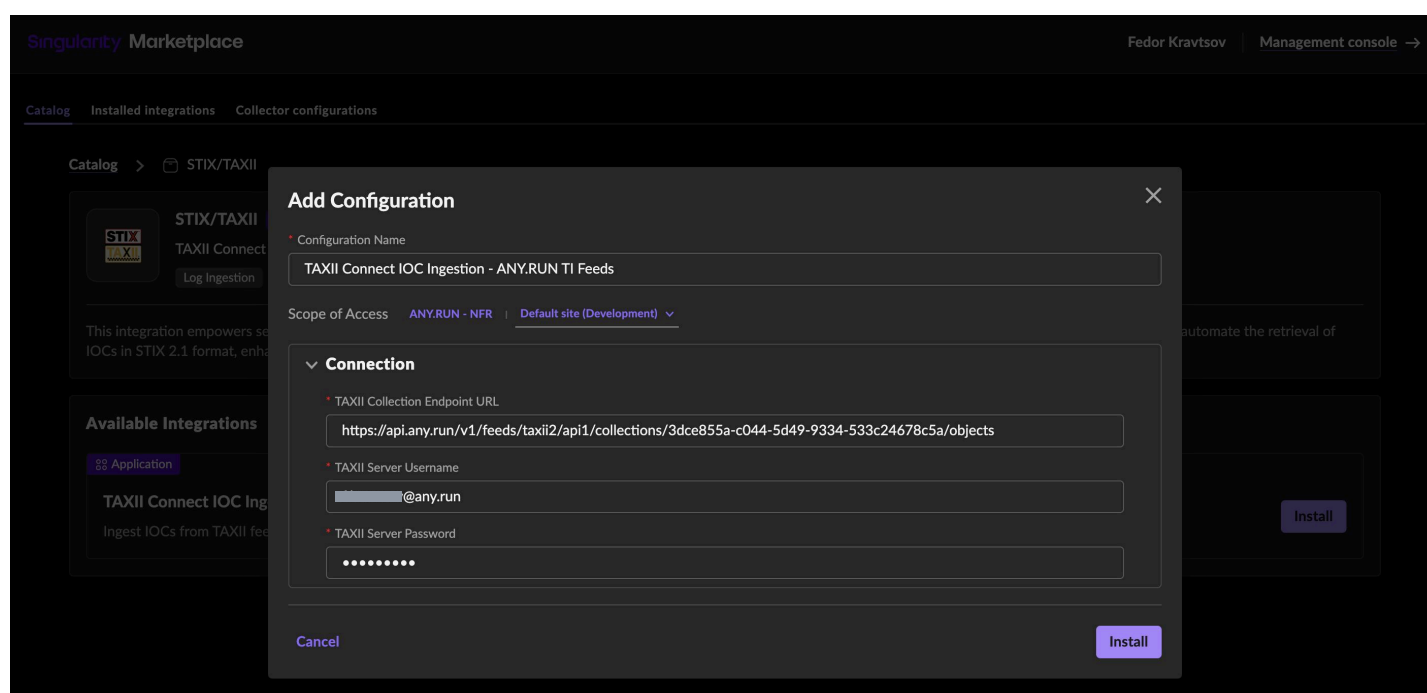
- **Configuration Name:** Name your configuration
- **Scope of Access:** Select the appropriate scope.
- **Endpoint URL:** Enter the URL for ANY.RUN's TI Feeds collection. See collection IDs below.
- **TAXII Server Username:** Enter your email for ANY.RUN account with an active TI Feeds subscription.
- **TAXII Server Password:** Enter the password for your ANY.RUN account.

ANY.RUN's TI Feeds collections

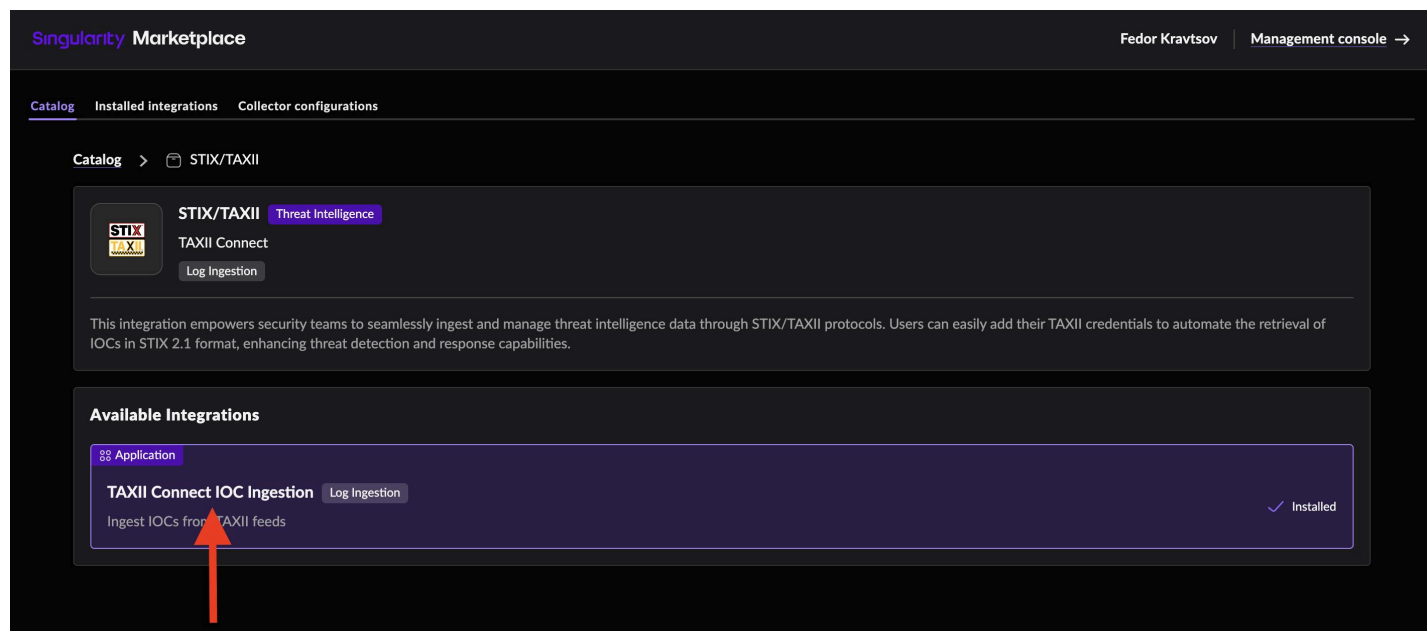
Via this link, you can explore information about all collections hosted under the ANY.RUN API Root, including each collection's ID, which is required to request objects from it:

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

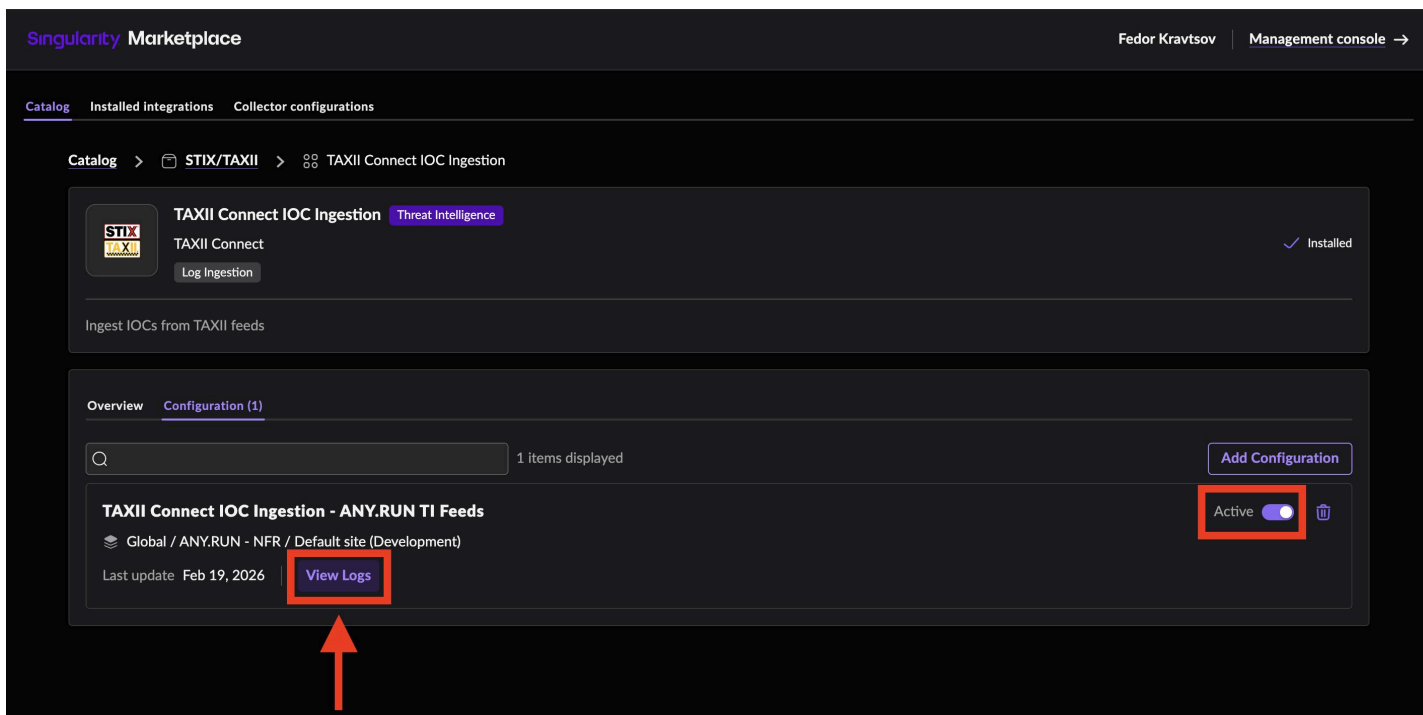
Name	Description	ID
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs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



5. Once the connector is installed, open it.



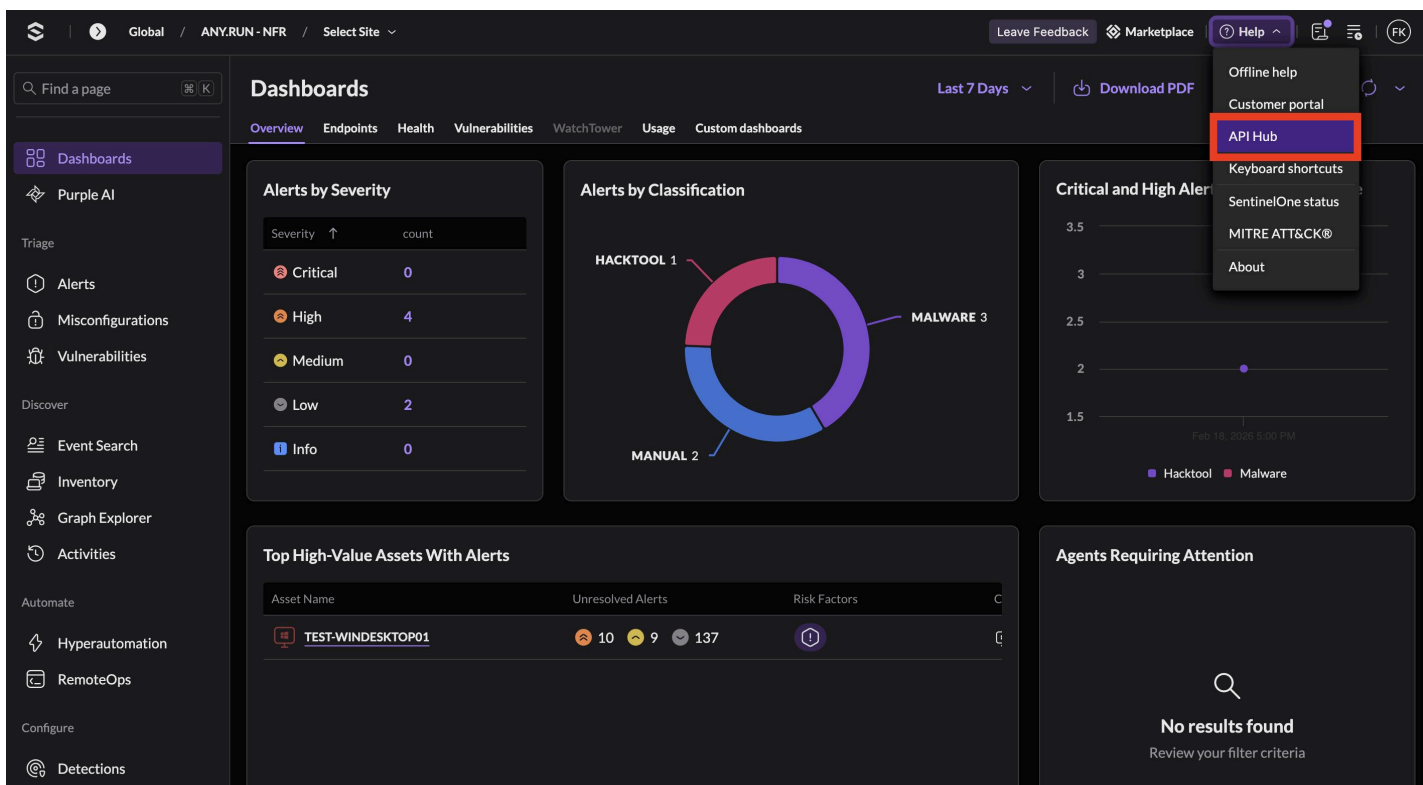
6. Confirm its status is **Active** and click **View Logs** to verify the connector's activity.



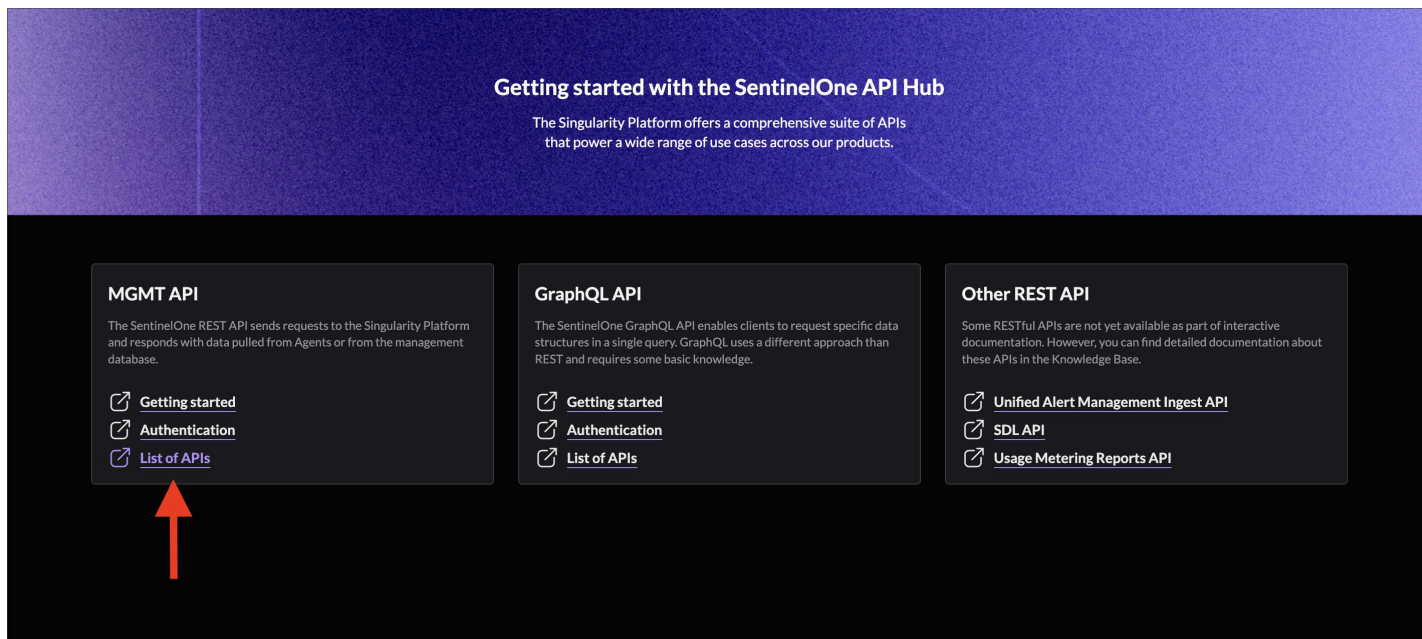
7. Ensure that your connection is stable and the indicators are being successfully ingested. **Note:** Indicators are updated every 5 minutes. You can monitor the updates via **View Logs**.

Browsing indicators

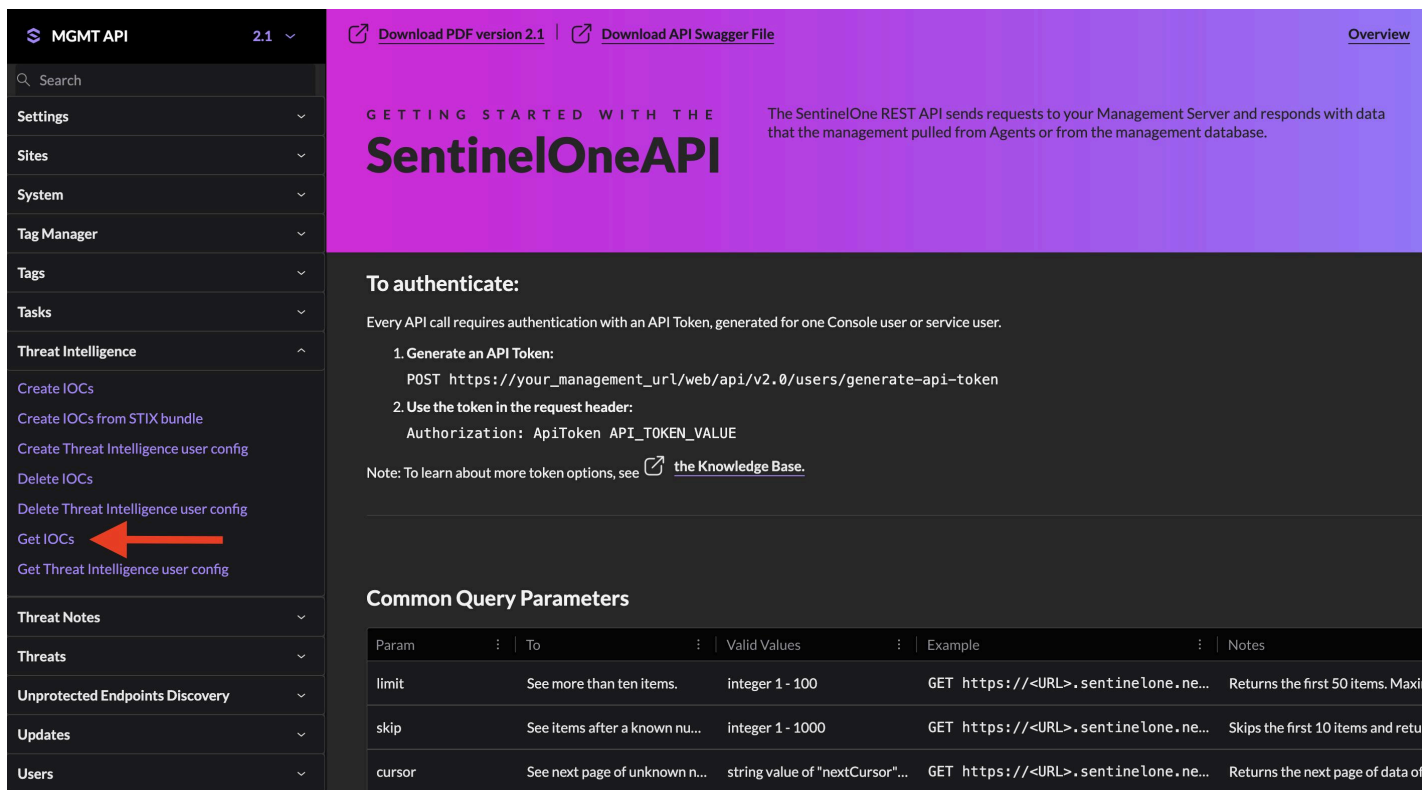
1. Open the SentinelOne **Management Console**. From the **Help** dropdown menu, select **API Hub**.



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



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



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",

```

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": [

```

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

Get IOCs

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

severity **array**

URL [Copy URL](#)

Status code

siteIds **array**

RESPONSE [Copy Response](#)

1

skip **integer**

skipCount **boolean**

sortBy **string**

sortOrder **string**

Run API query

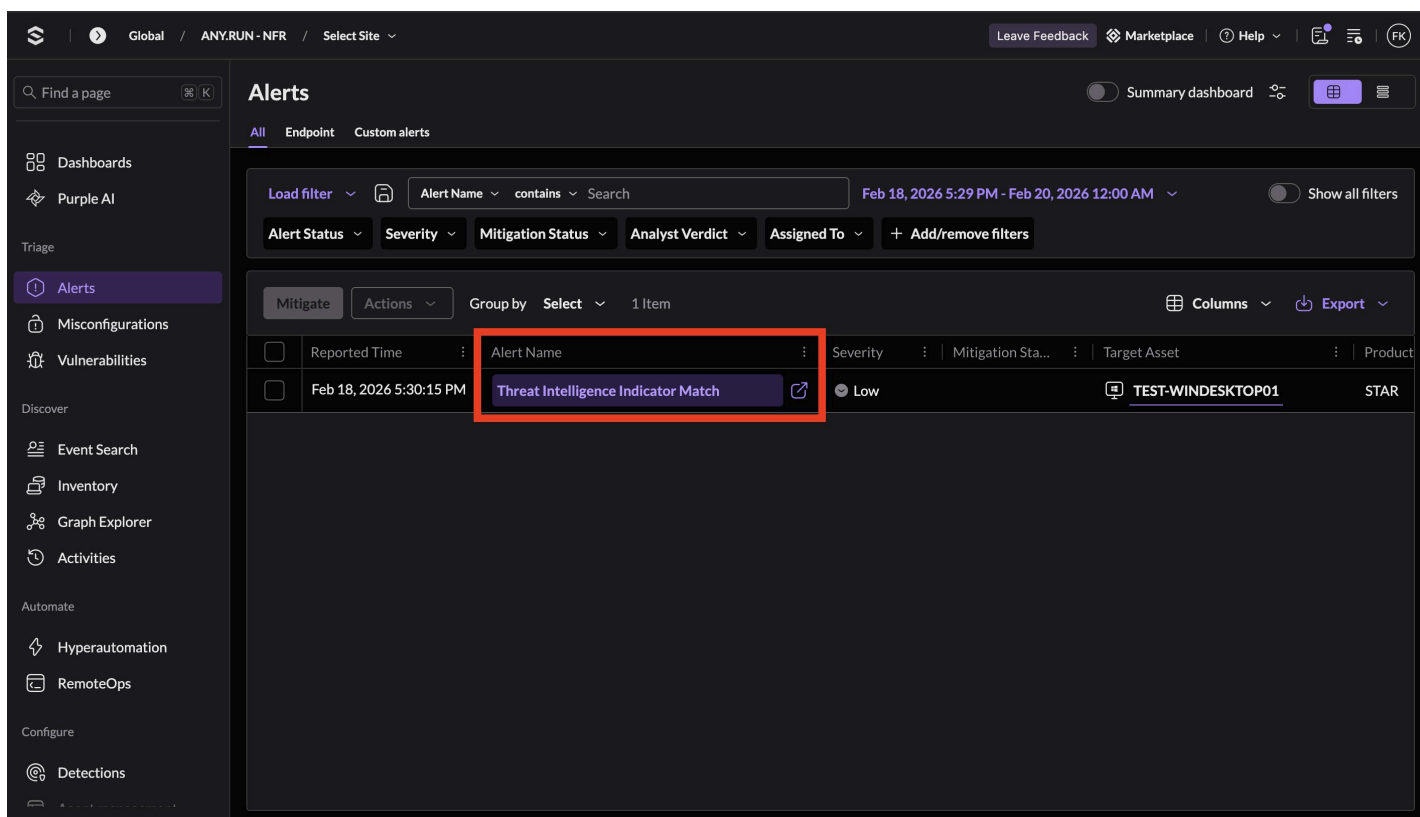
6. Enter *STIX Import* into the **source** field and click **Run API query**.

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

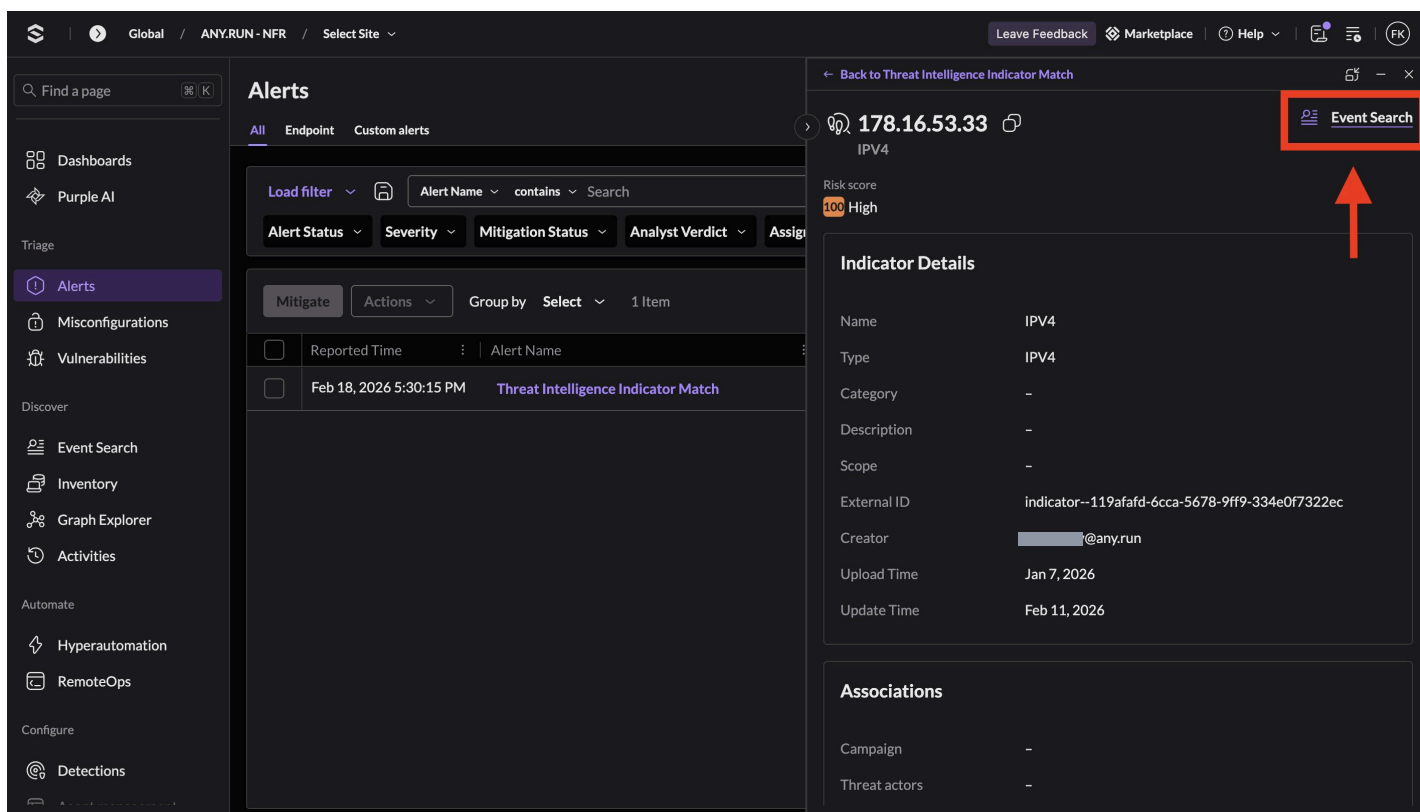
All IOCs imported from ANY.RUN's TI Feeds will now be evaluated and detected by SentinelOne.

Detection of ingested IOCs

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



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



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

The screenshot shows the SentinelOne interface for a 'Threat Intelligence Indicator Match' alert. The alert details include:

- Severity: Low
- Detection Engine: Platform Rule
- Reported time: Feb 18, 2026 5:30:15 PM
- Status: New
- Assigned To: Unassigned
- Analyst Verdict: Undefined

The 'Mitigate', 'Actions', and 'Automate' buttons are highlighted with a red box. Below the alert details, there is an 'Alert Footprint' section showing 16 instances and impacted assets. At the bottom, a 'Threat Intelligence' section shows 8 events scanned and 1 threat intelligence indicator detected.

Risk Score	IOC Value	Malware Family	Threat Actor	Updated At	Source
100	178.16.53.33	-	-	Feb 11, 2026	STIX Import

- 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 first one, but the 'Threat Intelligence' table is highlighted with a red box, and the IOC value '178.16.53.33' is highlighted with a white box. The table data is as follows:

Risk Score	IOC Value	Malware Family	Threat Actor	Updated At	Source
100	178.16.53.33	-	-	Feb 11, 2026	STIX Import

Global / ANY.RUN - NFR / Select Site

Leave Feedback Marketplace Help

Find a page

Event Search

Search Library Preferences Save Copy Link Documentation PowerQuery

2 EDR #ip = "178.16.53.33" Last 72 hours Search

All Events 9 Network Actions 9

9 matching records Feb 16, 2026 6:50 PM - Feb 19, 2026 6:50 PM [UTC+4] - 1 hour / bar Show timeline Show Graph

No Actions Items Jump to << Oldest Most Recent >> Oldest First Wrapping rows Settings

selected

	Log Event
<input type="checkbox"/>	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'
<input type="checkbox"/>	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'
<input type="checkbox"/> ⚠	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'
<input type="checkbox"/> ⚠	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'
<input type="checkbox"/> ⚠	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'
<input type="checkbox"/> ⚠	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'
<input type="checkbox"/> ⚠	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'
<input type="checkbox"/>	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'
<input type="checkbox"/>	endpoint.name='TEST-WINDESKTOP01' event.type='IP Connect' dst.ip.address='178.16.53.33'

SOURCES

SentinelOne 1

FIELDS

Filter Fields

- dst.ip.address 1
- dst.port.number 6
- endpoint.name 1
- endpoint.os 1
- event.category 1
- event.network.connectionStatus 2
- event.network.direction 1
- event.network.protocolName 6
- event.type 1
- src.ip.address 1
- src.port.number 9
- src.process.cmdline 2
- src.process.name 3
- src.process.parent.uid 3
- src.process.user 2
- account.id 1
- account.name 1
- agent.uuid 1
- agent.version 1
- dataSource.category 1

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