ANY.RUN

ANY.RUN's TI Feeds:
Integration with SentinelOne

Configuration guide

Table of Contents

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.

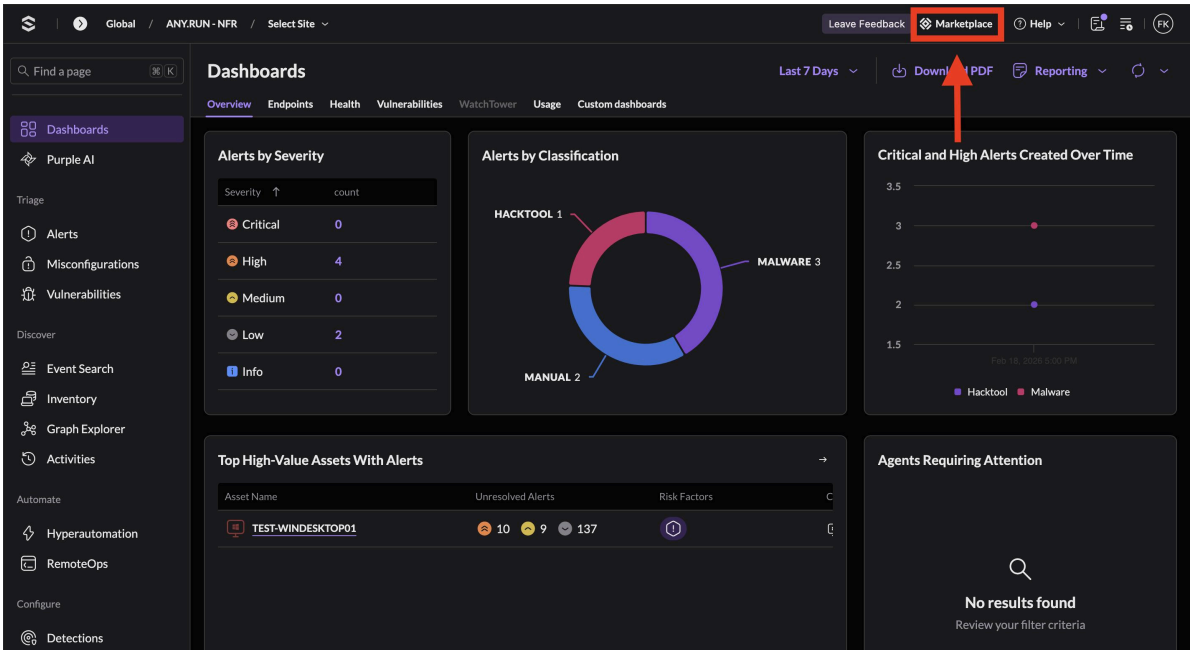
TI Feeds are available for integration using API or SDK and support TAXII protocol.

For more details, feel free to contact us.

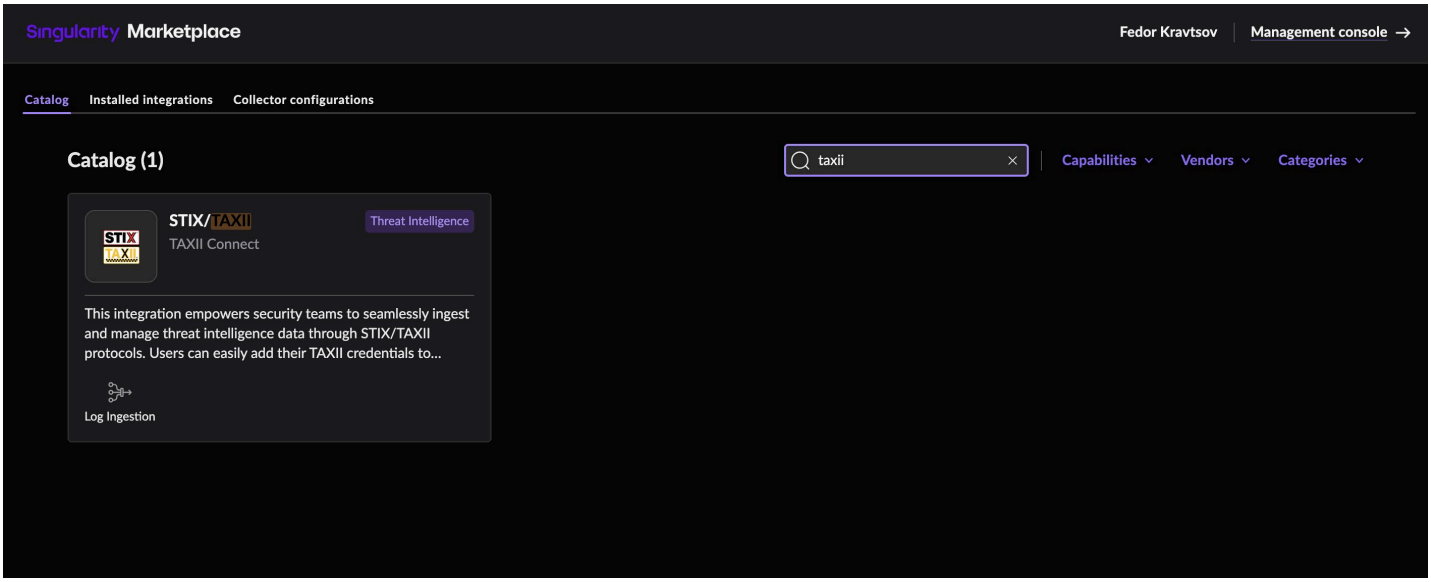
How to Integrate TI Feeds with SentinelOne

Installation and configuration

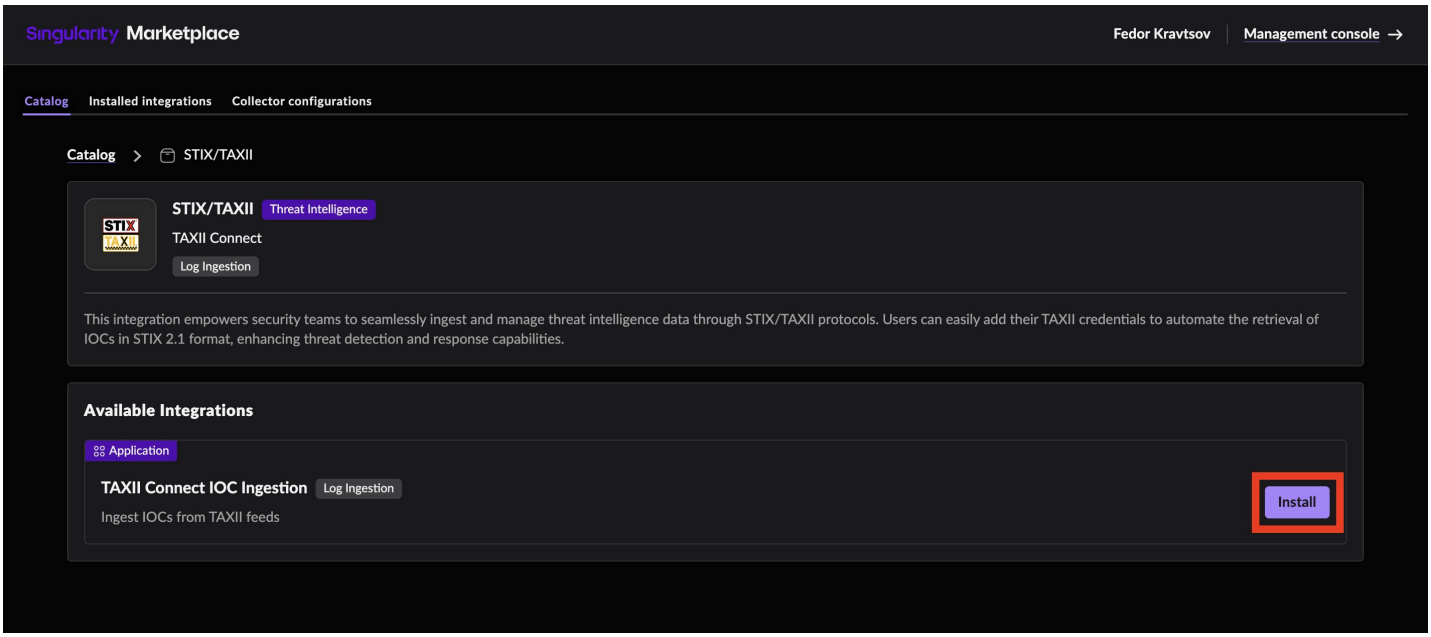
1. Open the SentinelOne **Management Console** and go to **Marketplace**.



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



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



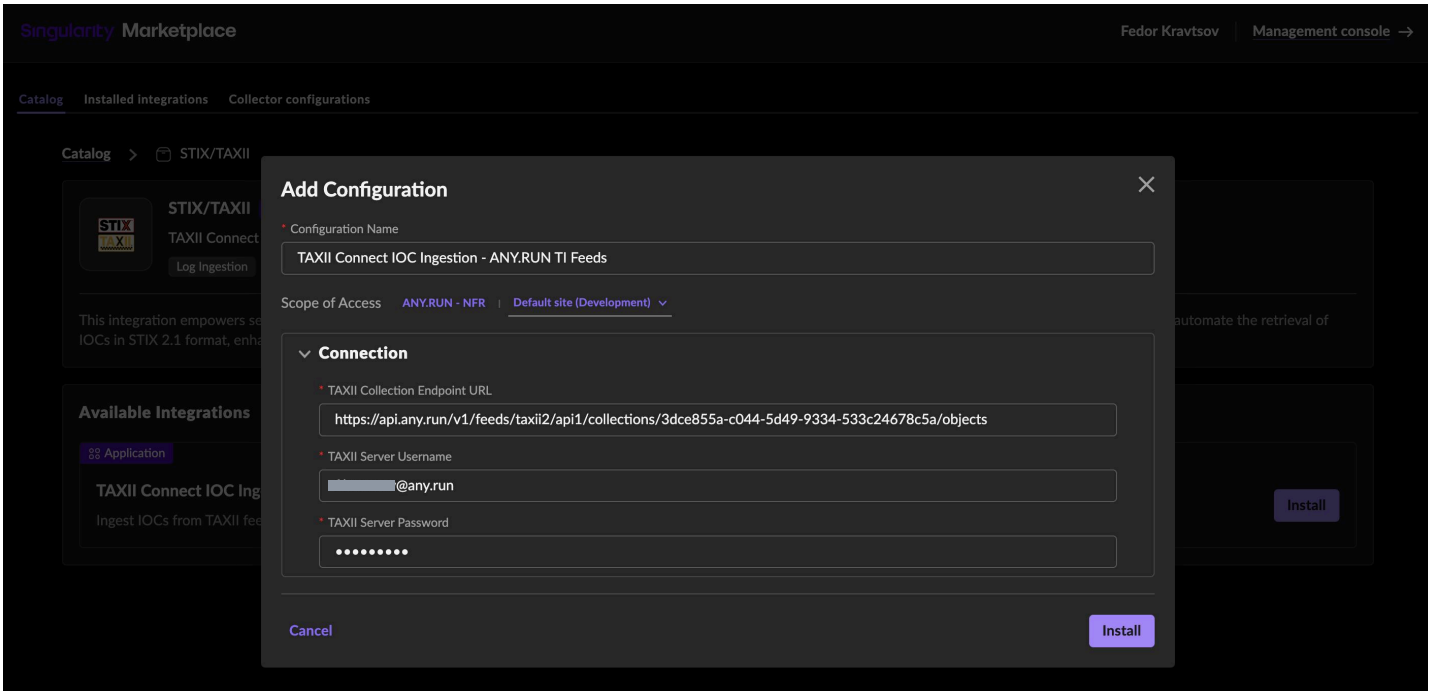
4. In the **Add Configuration** window, fill out the following fields:

- **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.

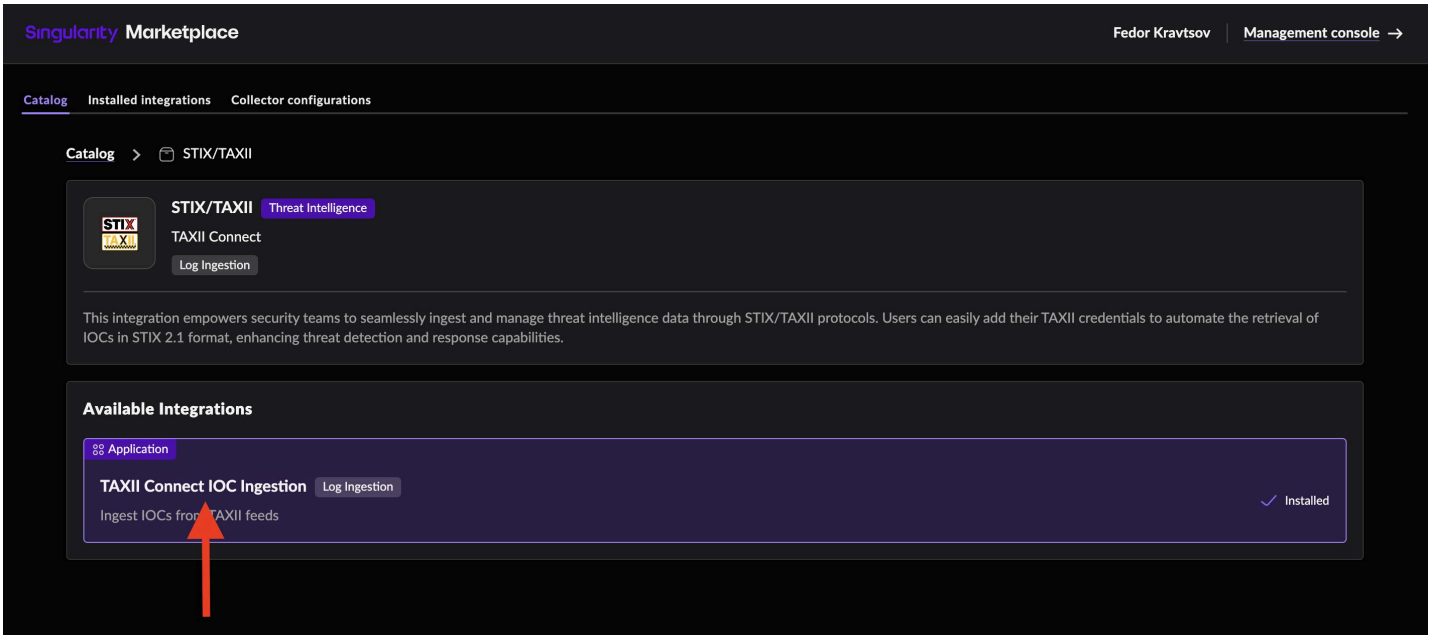
ANY.RUN's TI Feeds collections

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`

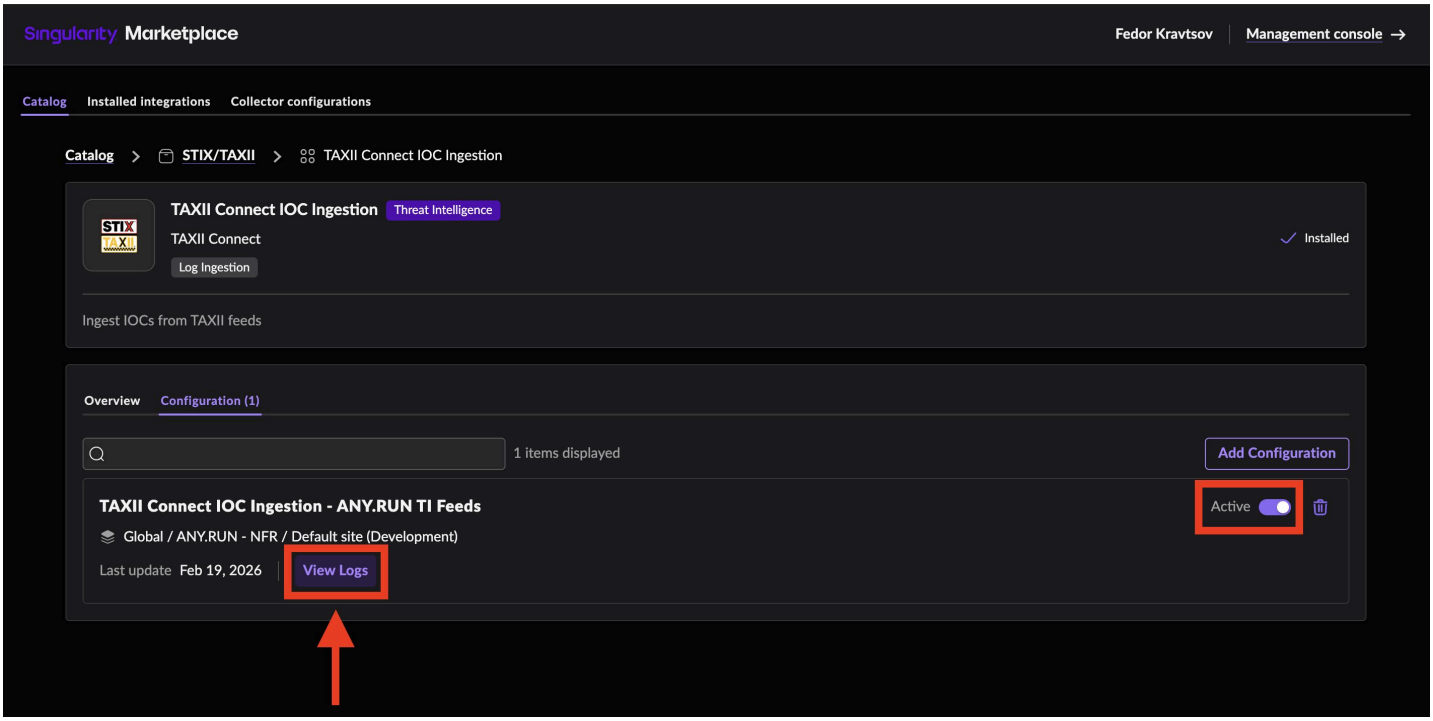
Name	Description	ID
All indicators	Contains IOCs of all formats (IPs, Domains, URLs)	3dce855a-c044-5d49-9334-533c24678c5a
IPs collection	Contains only IPs	55cda200-e261-5908-b910-f0e18909ef3d
Domains collection	Contains only Domains	2e0aa90a-5526-5a43-84ad-3db6f4549a09
URLs collection	Contains only URLs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

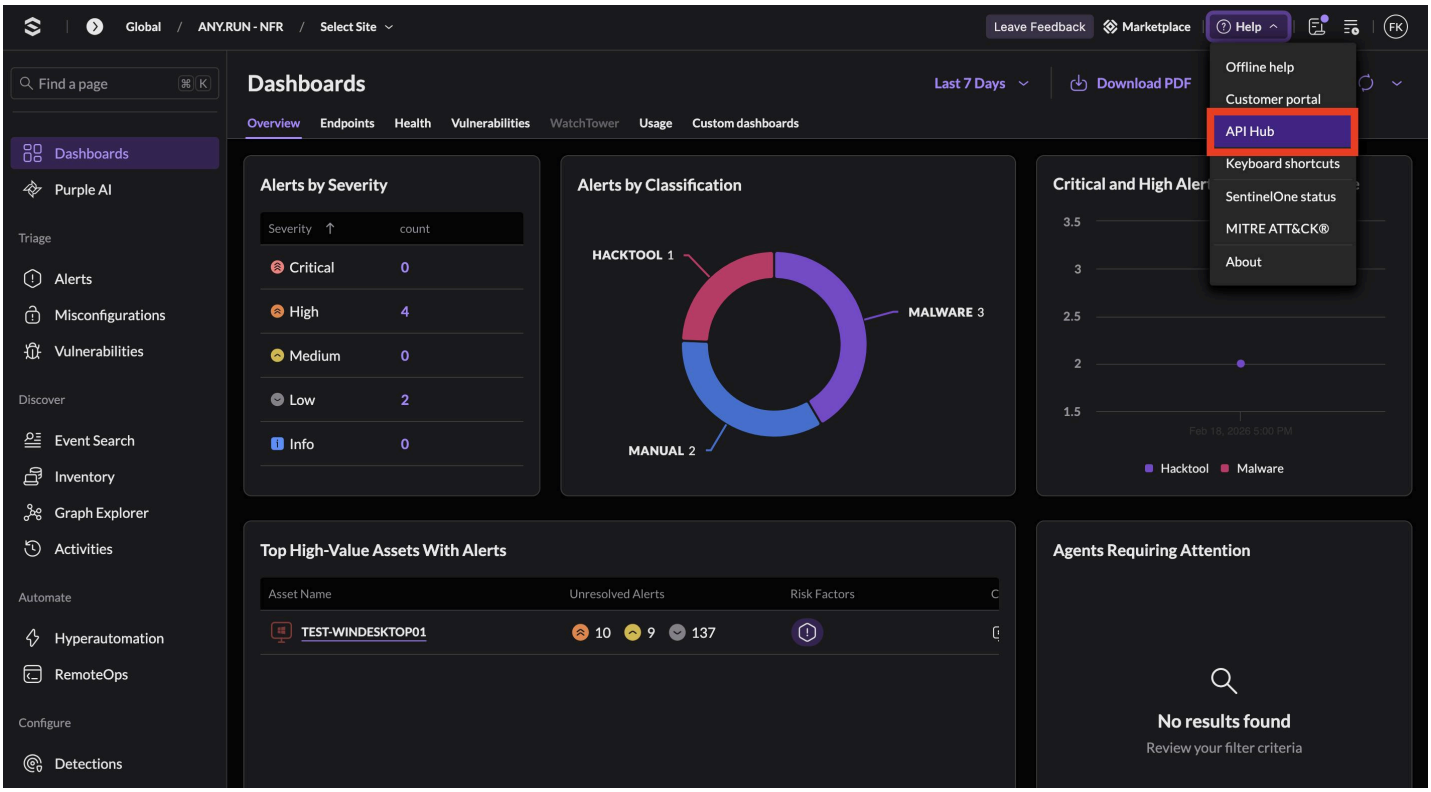


7. Ensure that your connection is stable and the indicators are being successfully ingested.

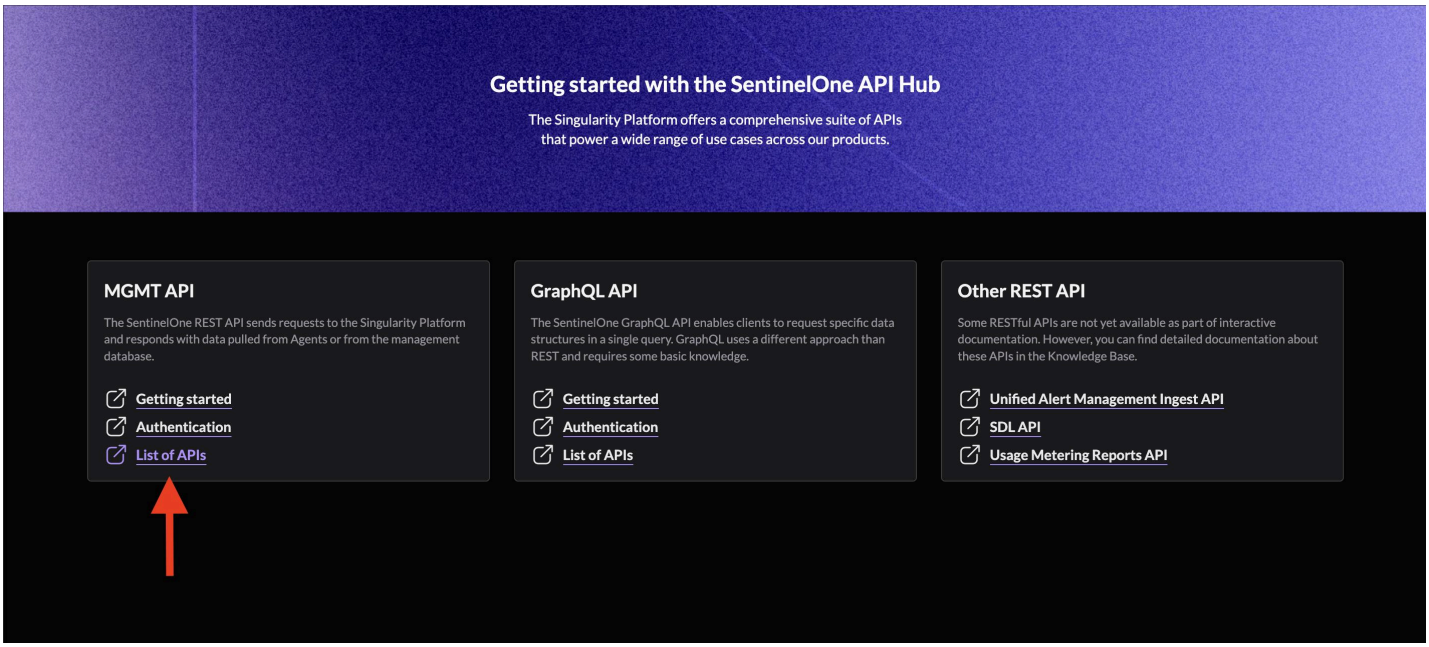
Note: Indicators are updated every 5 minutes. You can monitor the updates via **View Logs**.

Browsing indicators

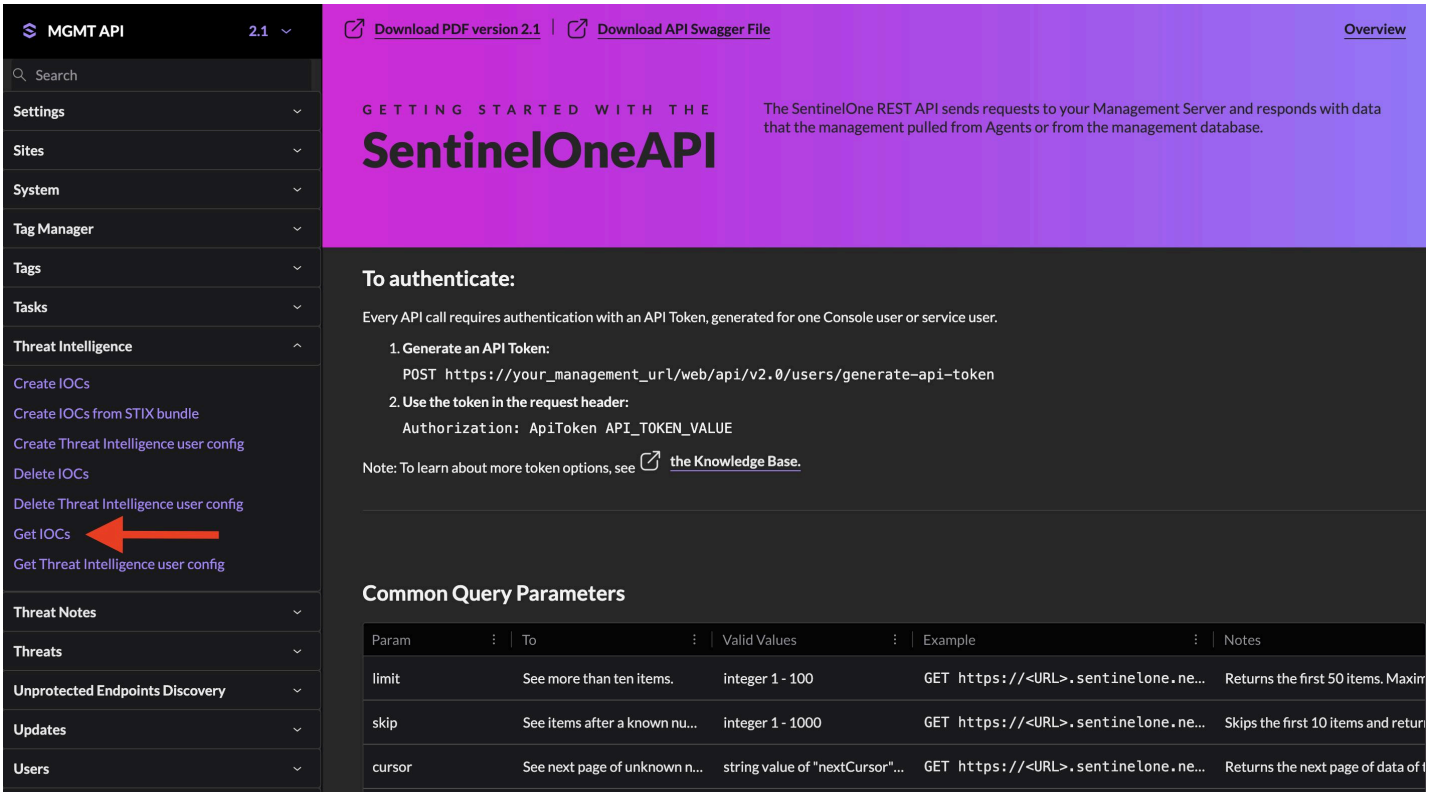
1. Open the SentinelOne **Management Console**. From the **Help** dropdown menu, select **API Hub**.



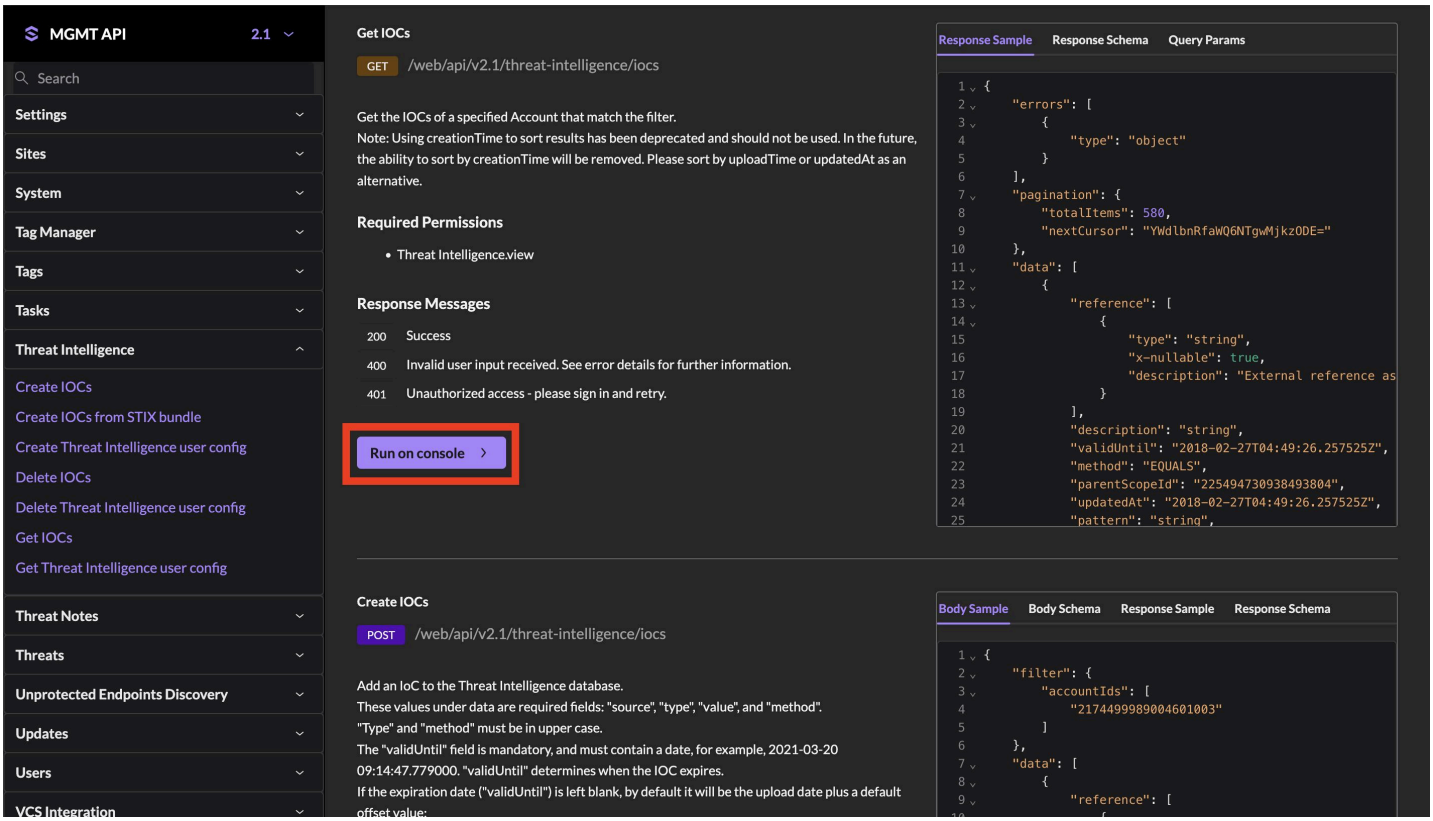
2. In the **MGMT API** section, click **List of APIs**.



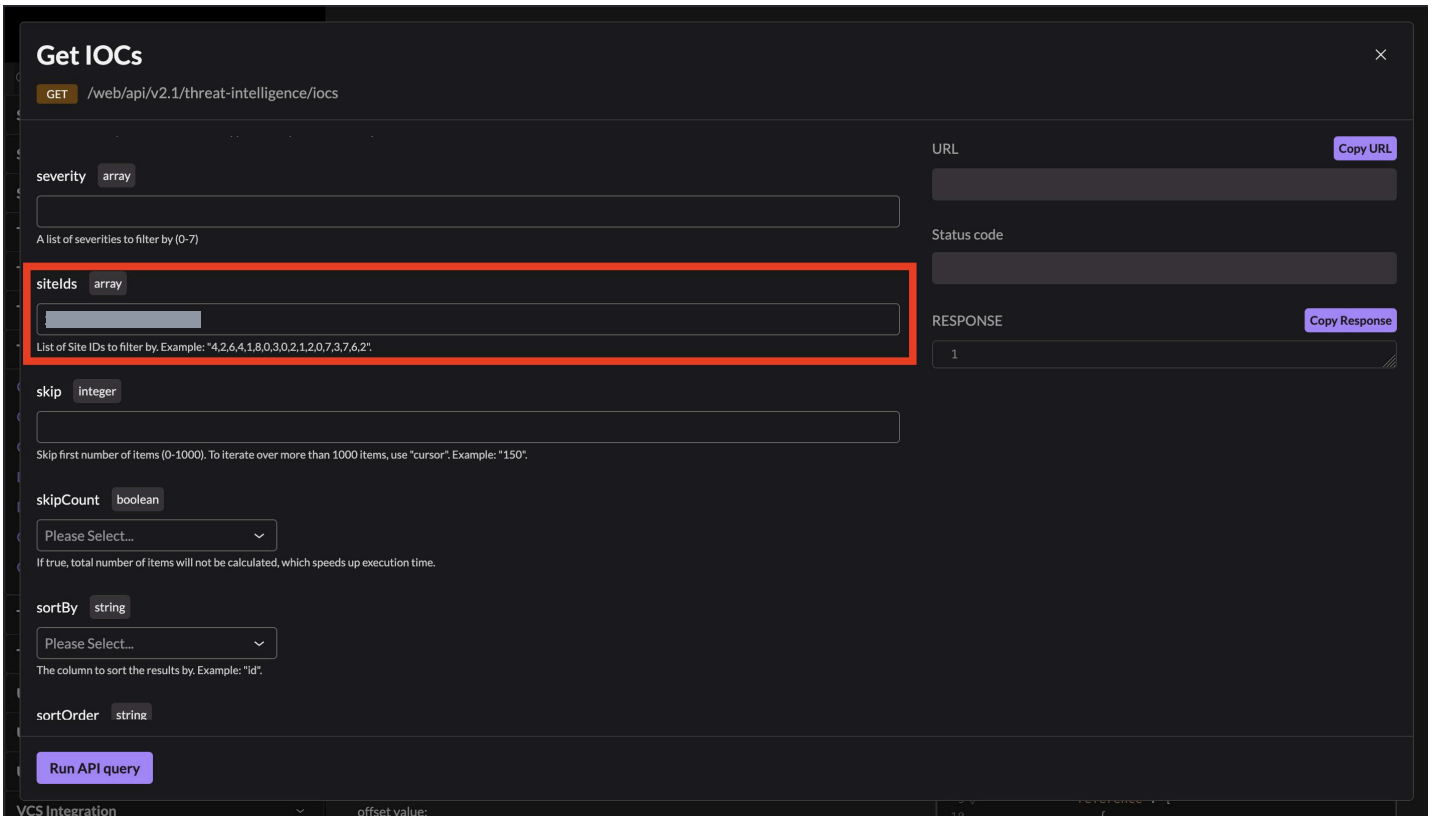
3. Go to **Threat Intelligence** tab and click **Get IOCs**.



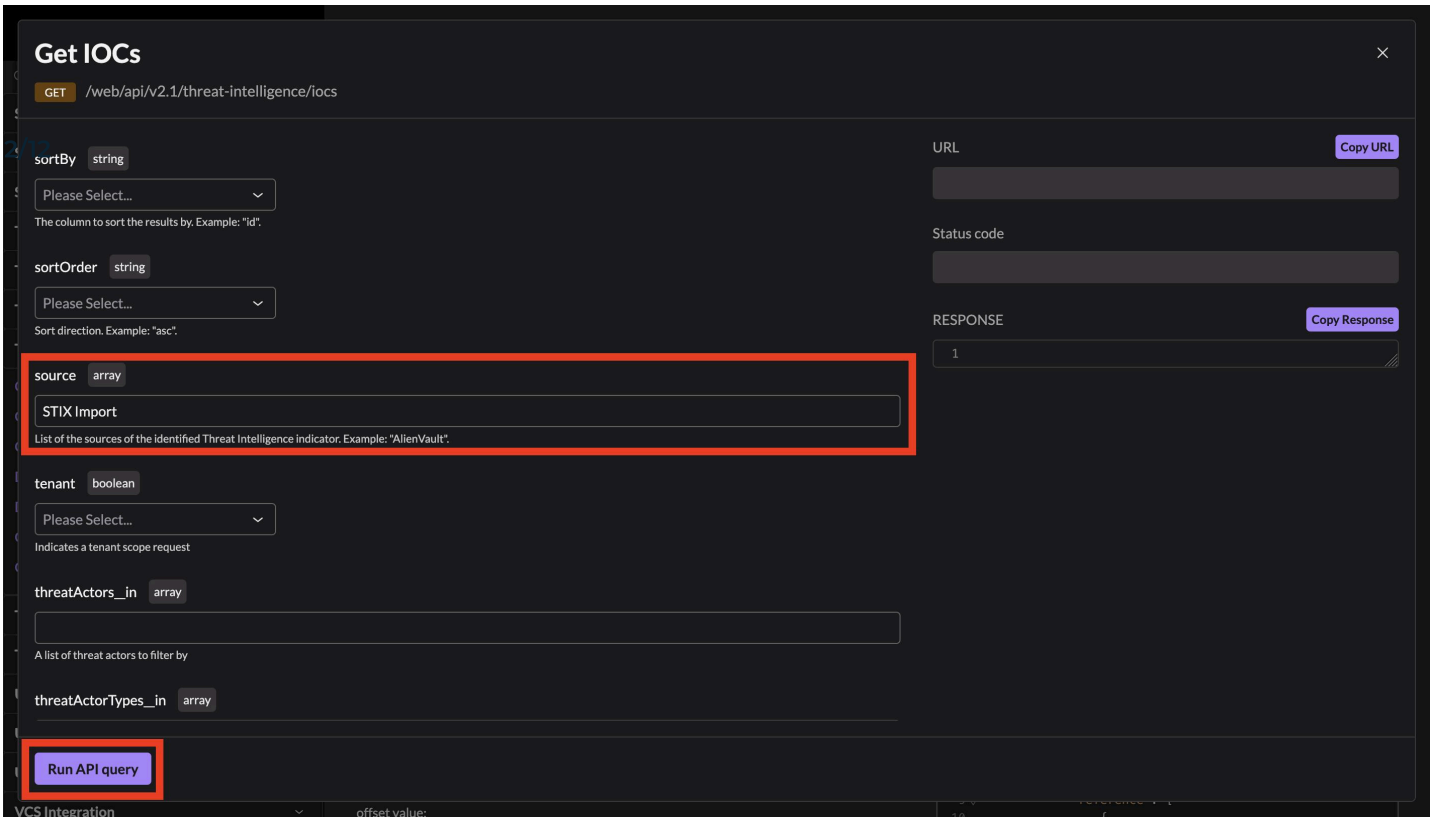
4. Click **Run on console**.



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

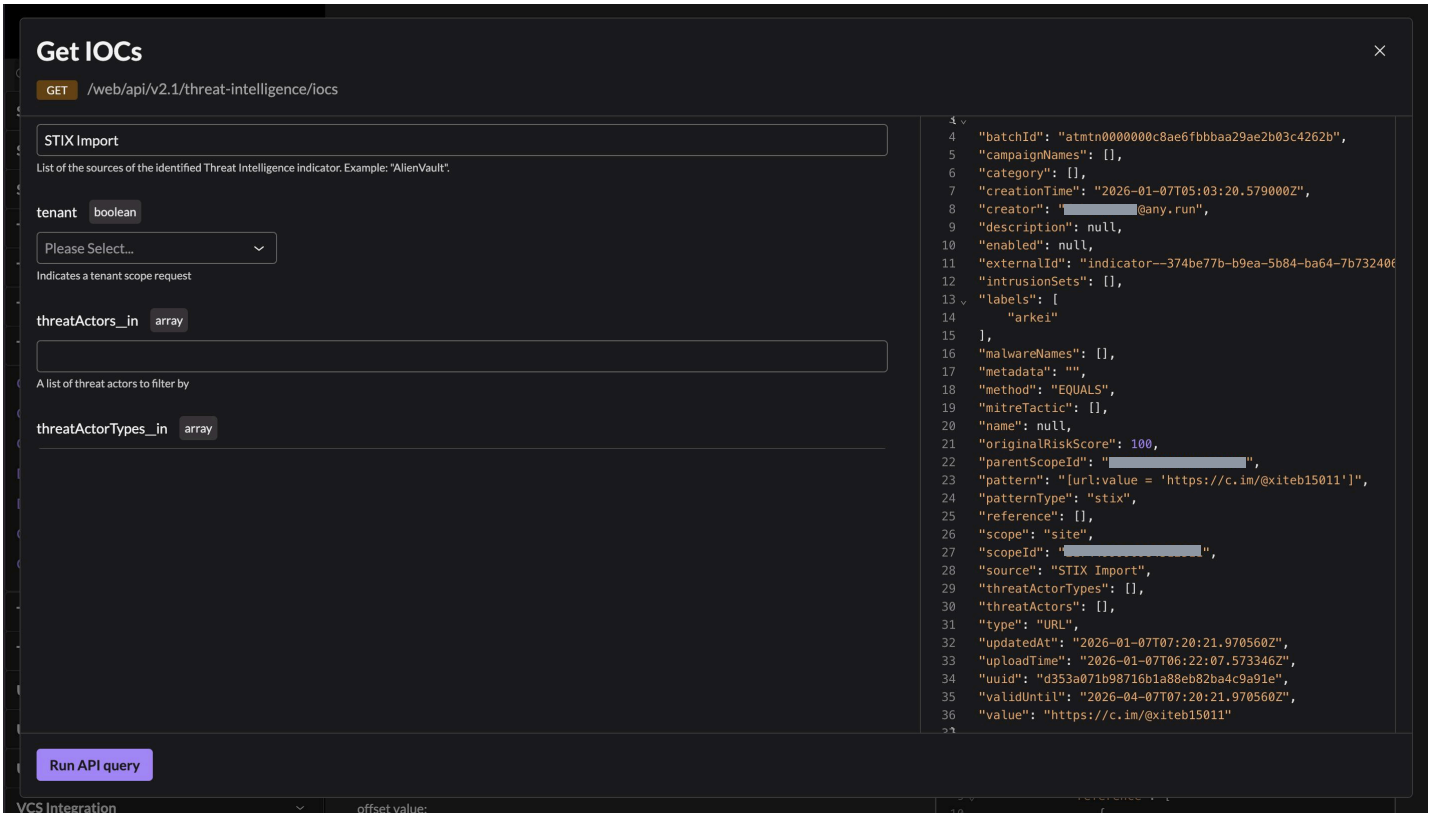


6. Enter *STIX Import* into the **source** field and click **Run API query**.



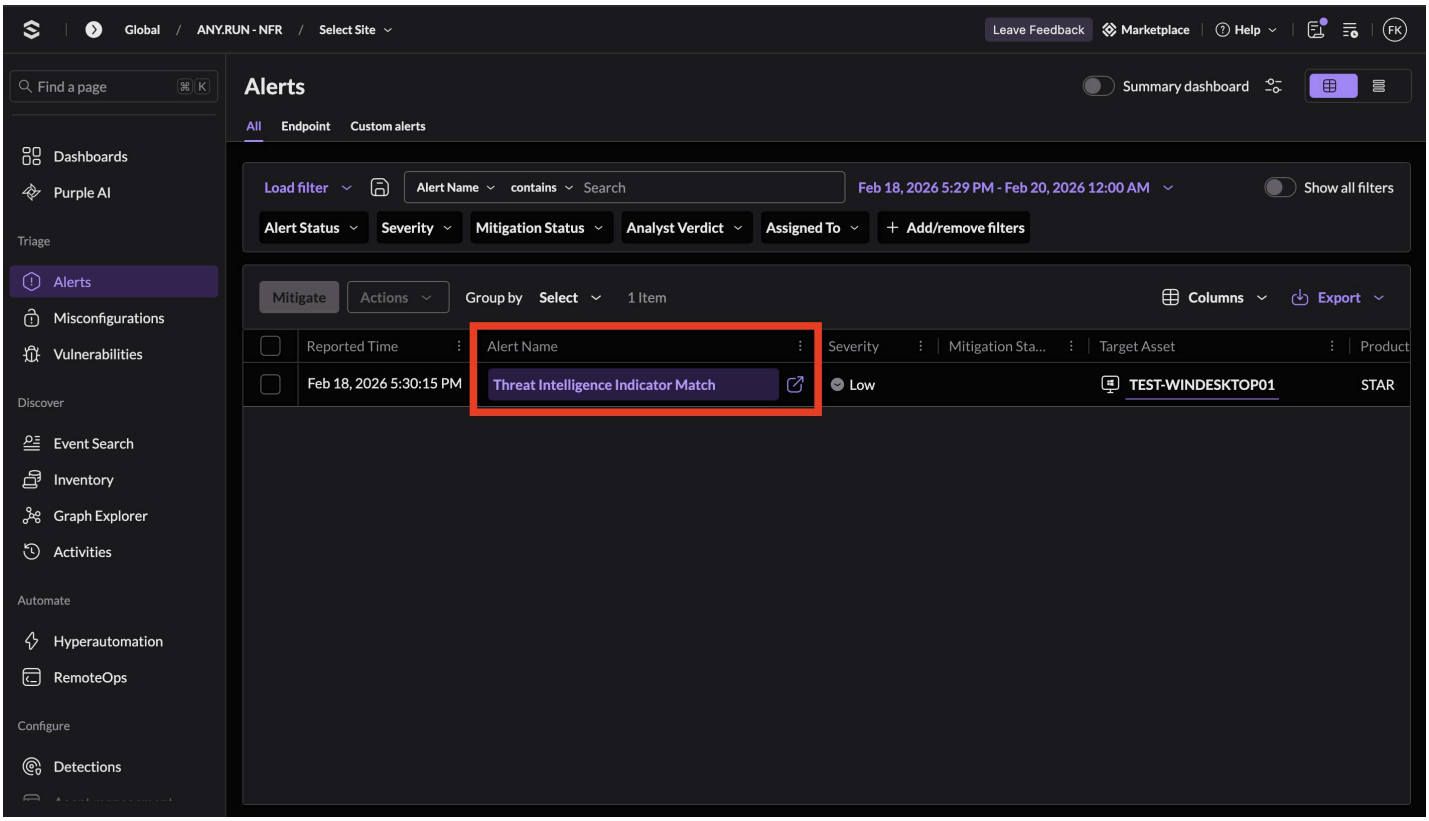
7. You'll see a **Get IOCs** window with **JSON-formatted** data on indicators from ANY.RUN's TI Feeds.

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

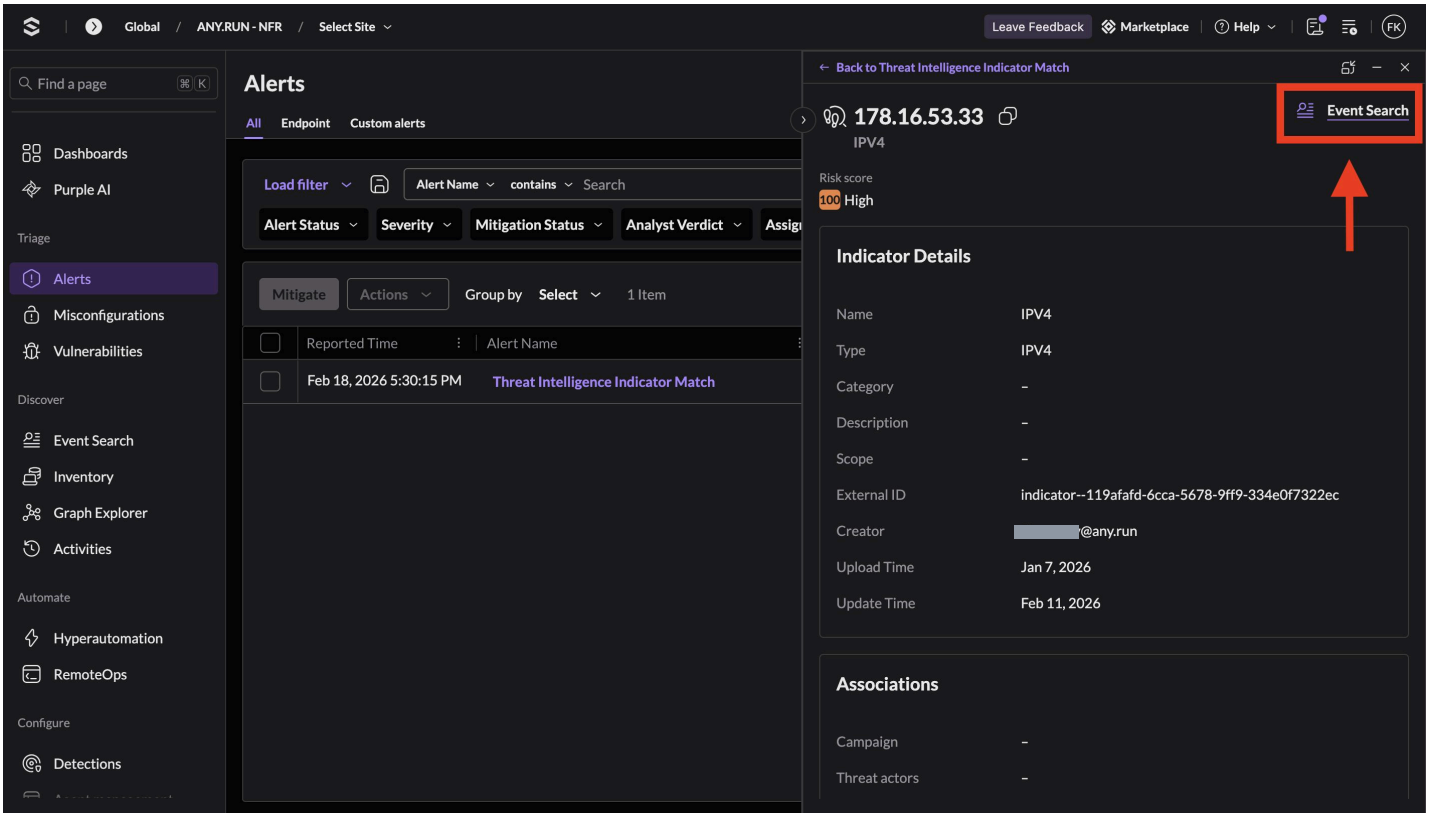


Detection of ingested IOCs

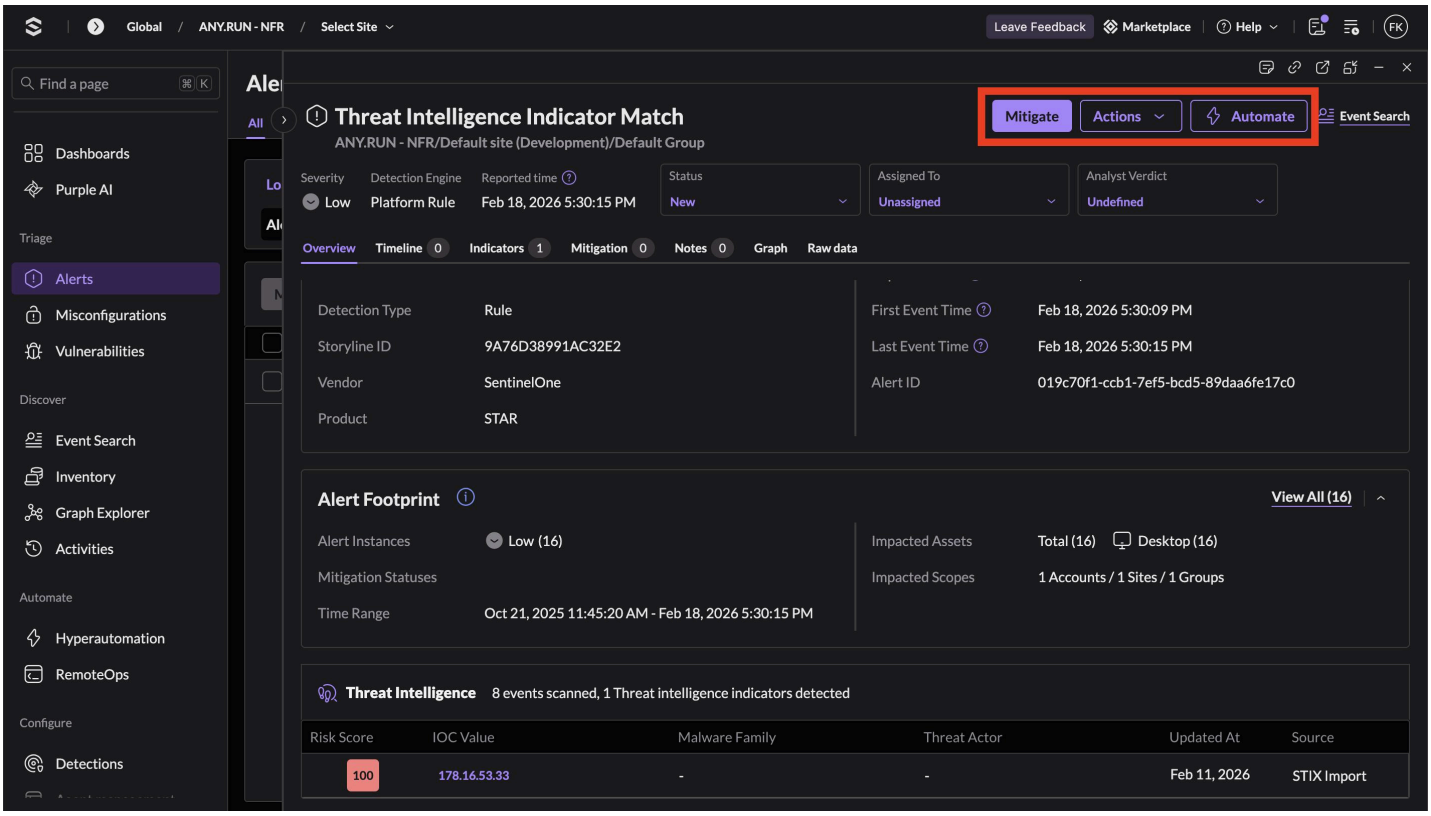
- If an indicator is detected in logs from your endpoints, an **Alert** will be created in your Management Console.



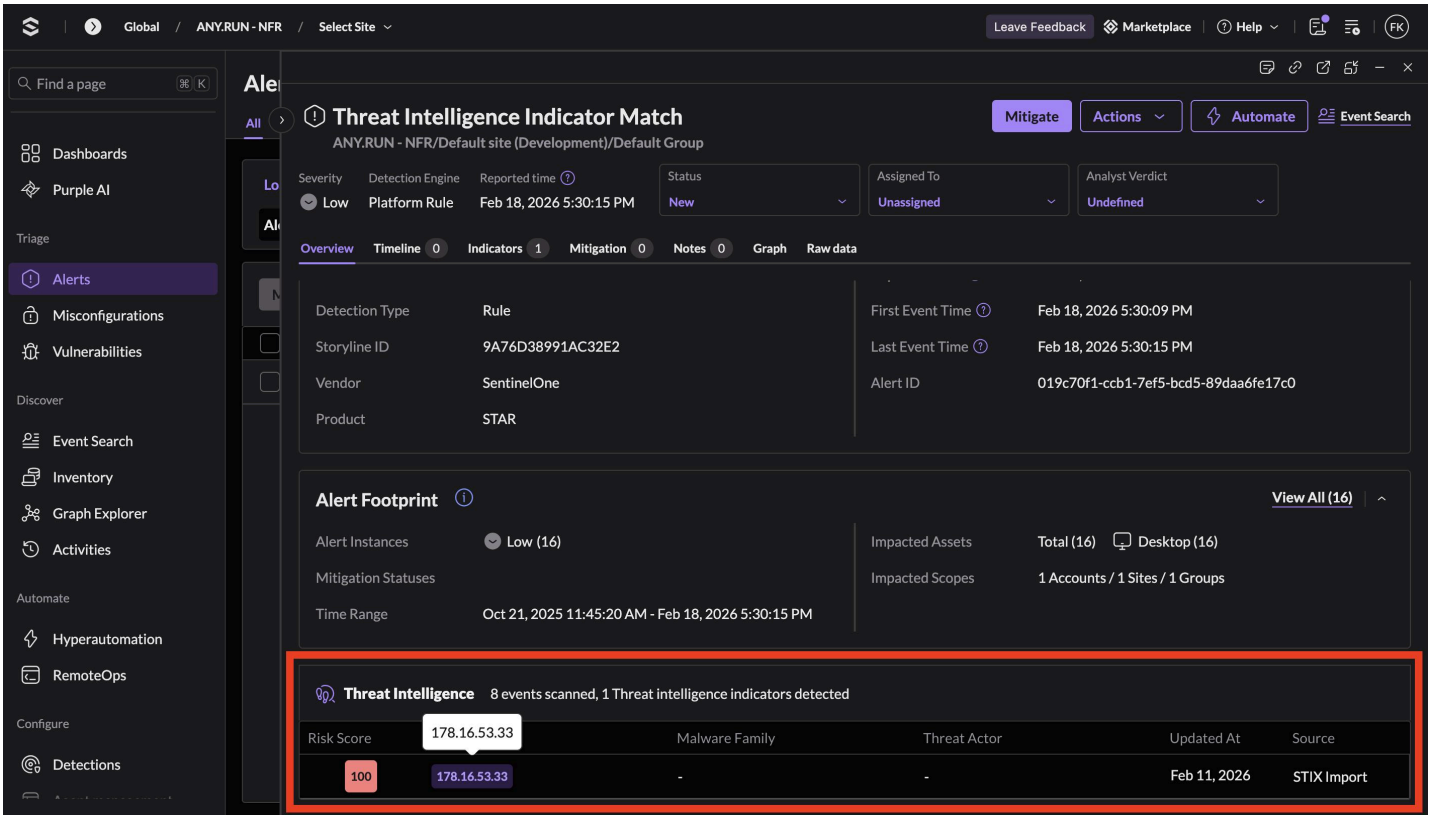
- Here you can see an Alert that was generated because an indicator was detected in logs:

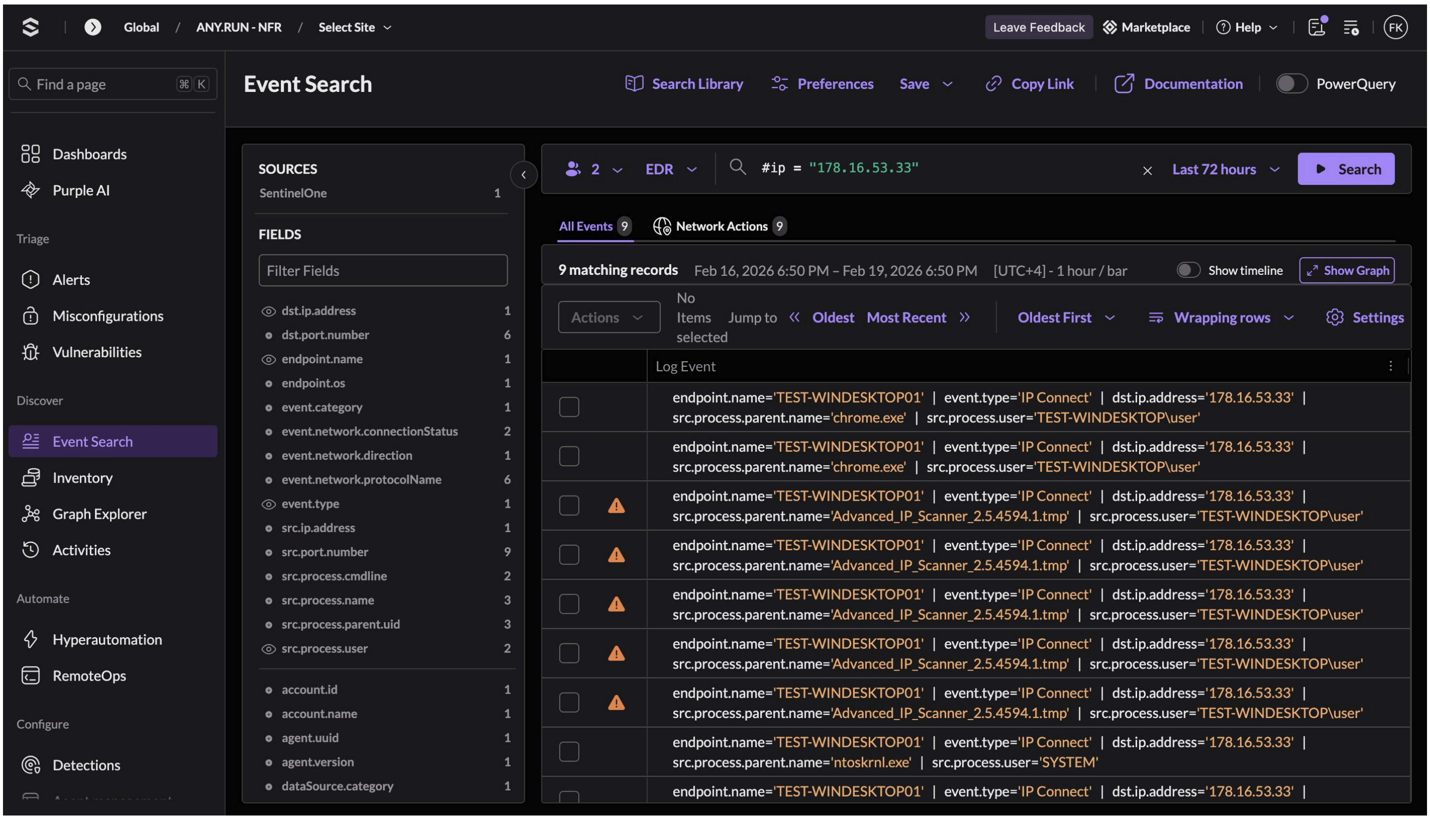


- You can perform initial incident response in SentinelOne via **Mitigate**, **Actions**, or **Automate**.



- 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.





If you have any questions,
contact us via this form or write to techsupport@any.run