SentinelOne Integrations

The SentinelOne integration collects and parses data from SentinelOne REST APIs. This integration also offers the capability to perform response actions on SentinelOne hosts directly through the Elastic Security interface

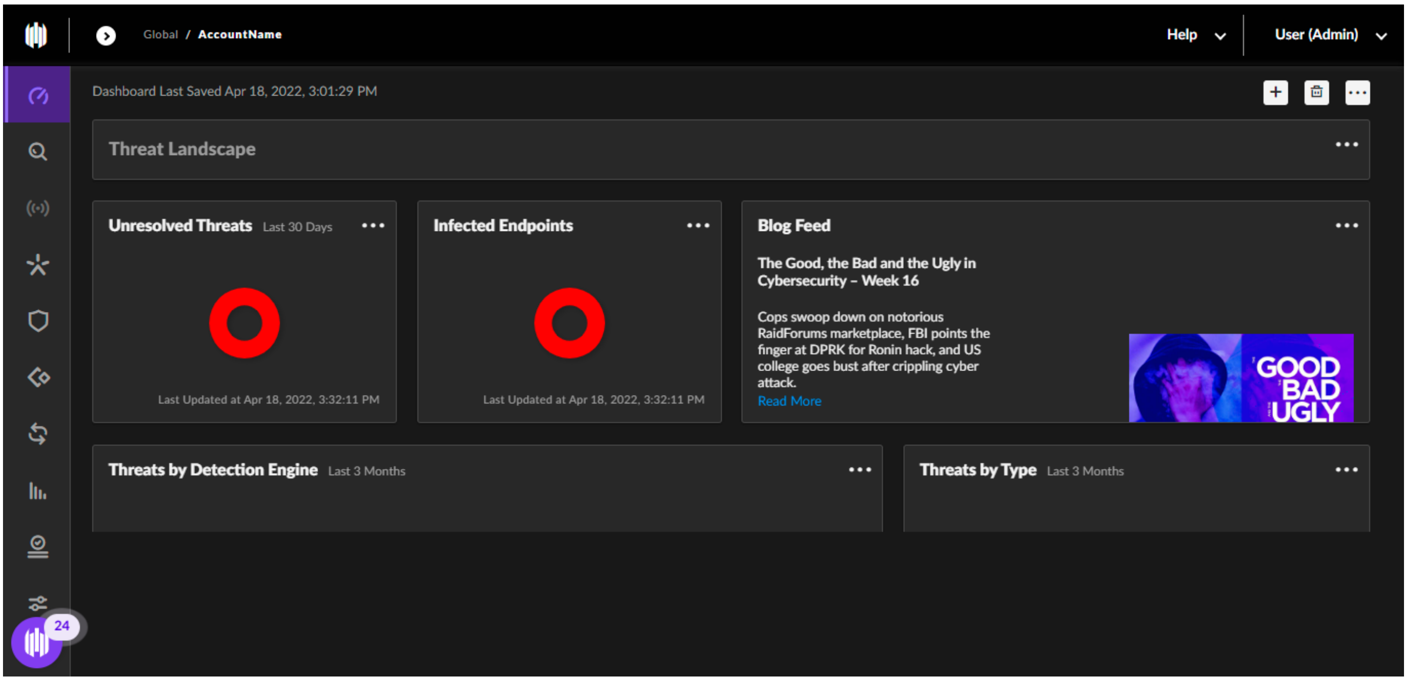
Compatibility

This module has been tested against `SentinelOne Management Console API version 2.1`.

API token

To collect data from SentinelOne APIs, you must have an API token. To create an API token, follow these steps:

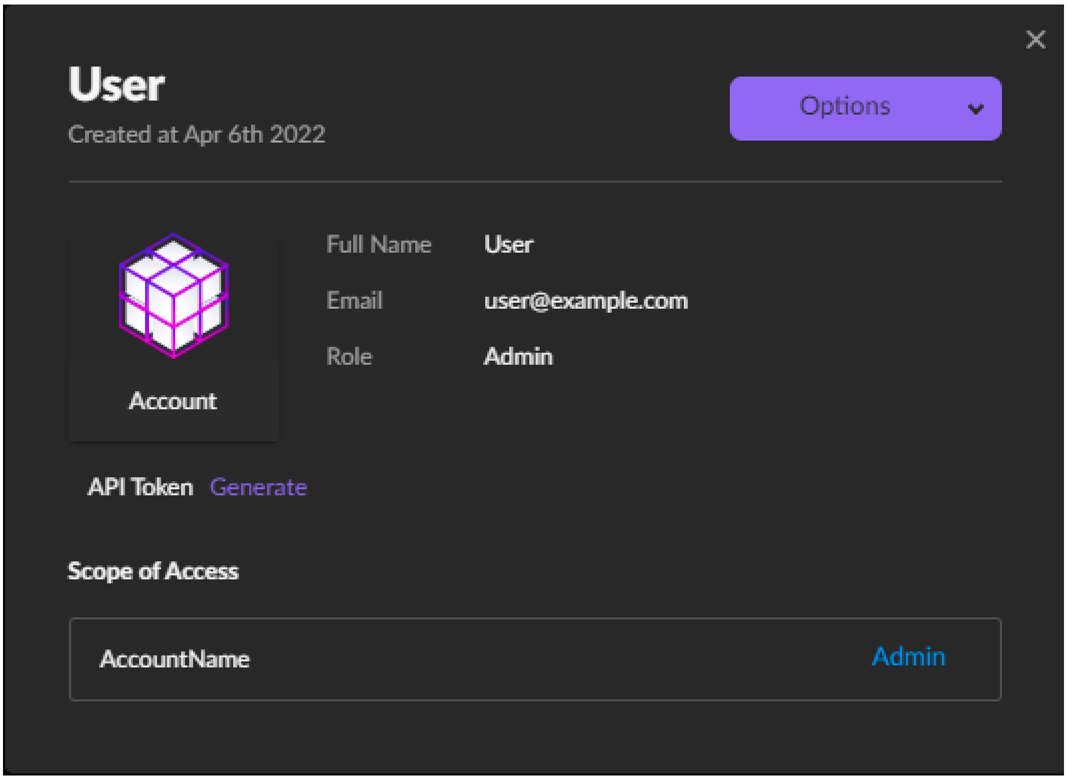
1. Log in to the **SentinelOne Management Console** as an **Admin**.


Global / AccountName
Help
User (Admin)
Dashboard Last Saved Apr 18, 2022, 3:01:29 PM
Threat Landscape
Unresolved Threats Last 30 Days
Last Updated at Apr 18, 2022, 3:32:11 PM
Infected Endpoints
Last Updated at Apr 18, 2022, 3:32:11 PM
Blog Feed
The Good, the Bad and the Ugly in Cybersecurity – Week 16
Cops swoop down on notorious RaidForums marketplace, FBI points the finger at DPRK for Ronin hack, and US college goes bust after crippling cyber attack.
Read More
GOOD BAD UGLY
Threats by Detection Engine Last 3 Months
Threats by Type Last 3 Months
24

2. Navigate to **Logged User Account** from top right panel in the navigation bar.

3. Click **My User**.

4. In the API token section, click **Generate**.



User

Created at Apr 6th 2022

Full Name User

Email user@example.com

Role Admin

API Token Generate

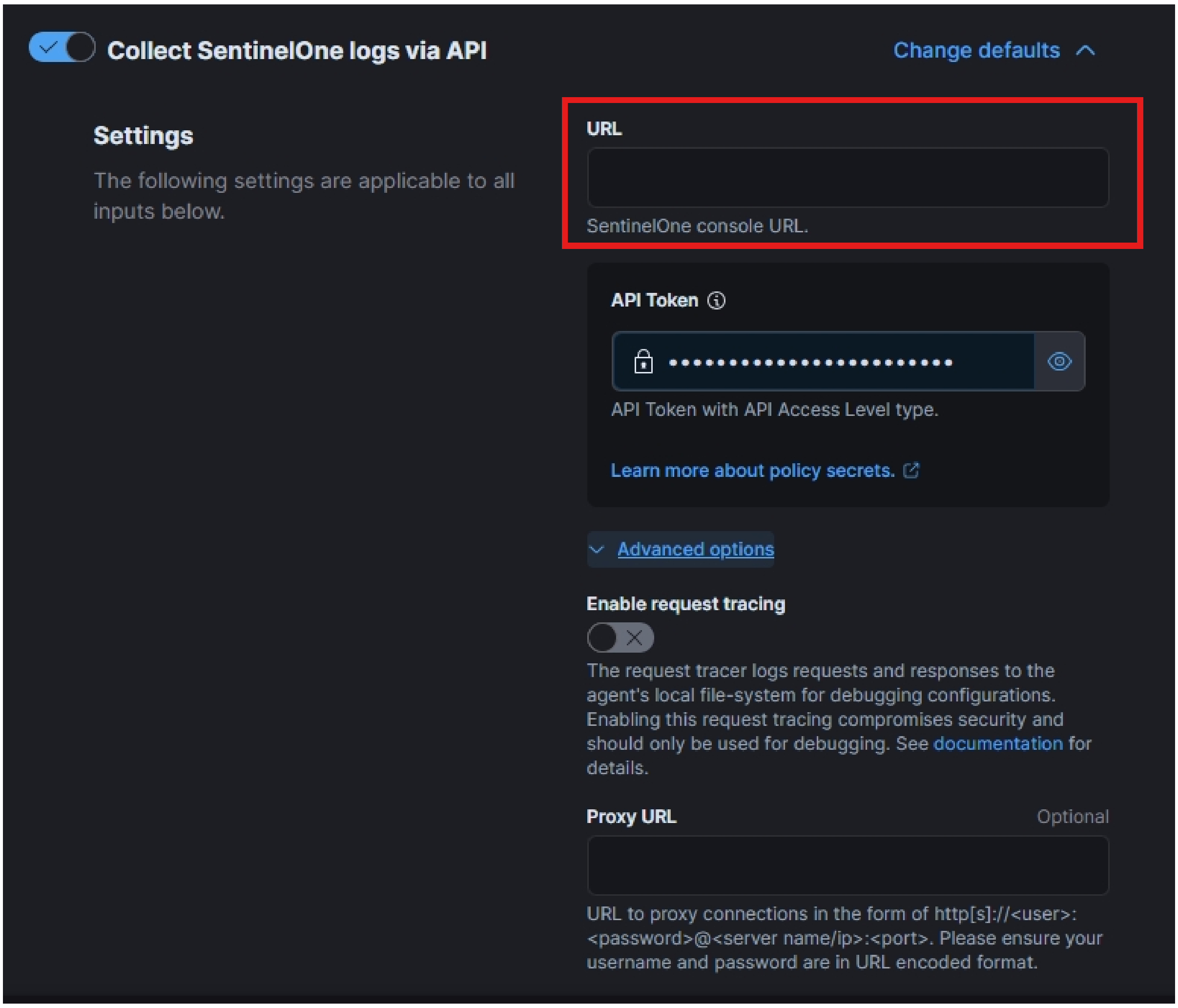
Scope of Access

AccountName	Admin

Note

The API token generated by the user is time-limited. To rotate a new token, log in with the dedicated admin account.

Integrate on Elastic



Collect SentinelOne logs via API

Change defaults

Settings

The following settings are applicable to all inputs below.

URL

SentinelOne console URL.

API Token

••••••••••••••••••••••••

API Token with API Access Level type.

Learn more about policy secrets.

Advanced options

Enable request tracing

The request tracer logs requests and responses to the agent's local file-system for debugging configurations. Enabling this request tracing compromises security and should only be used for debugging. See documentation for details.

Proxy URL Optional

URL to proxy connections in the form of http[s]://<user>:<password>@<server name/ip>:<port>. Please ensure your username and password are in URL encoded format.

1. Add SentinelOne console URL (`https://<DomainName>.sentinelone.net/`, where `<DomainName>` is the domain name of your SentinelOne account.)

2. Add API token

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #3
Created 21 October 2024 01:46:38 by David Napoleon Romanillos
Updated 21 October 2024 02:42:06 by David Napoleon Romanillos