

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

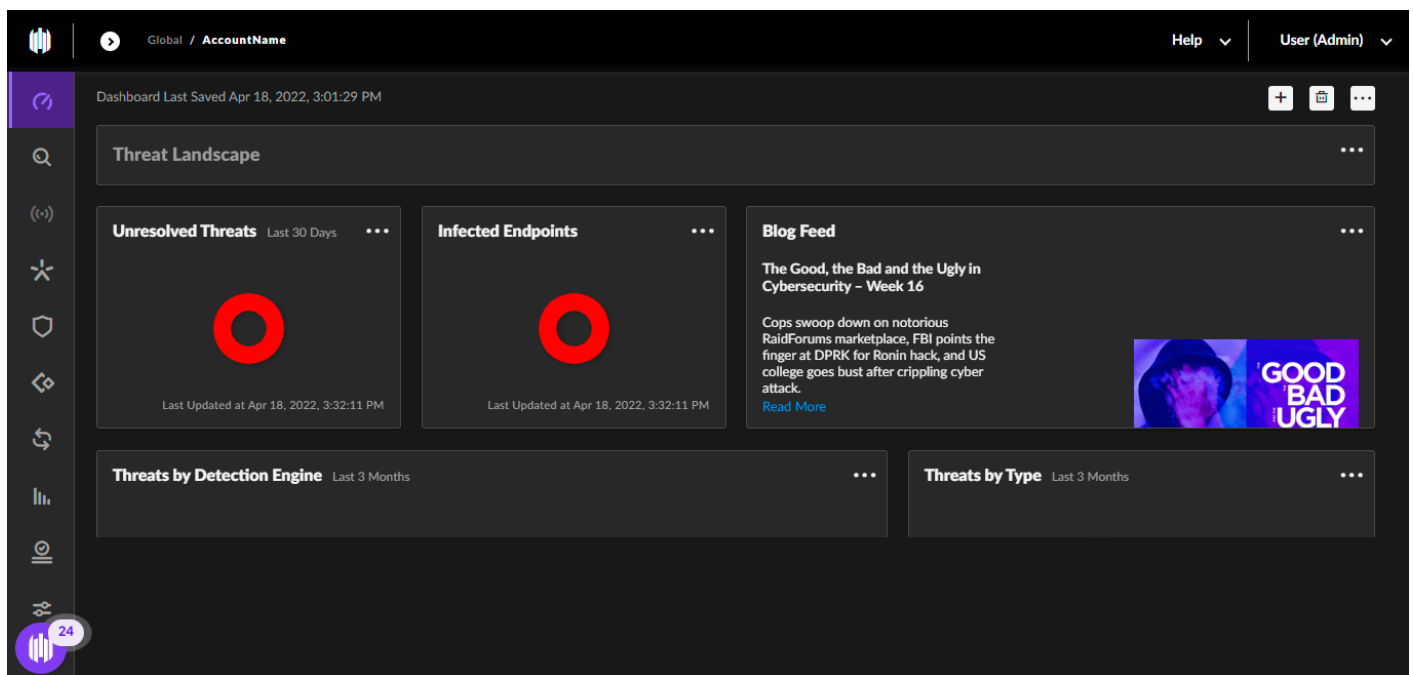
Compatibility

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**.




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

Options



Account

Full Name

User

Email

user@example.com

Role

Admin

API Token [Generate](#)

Scope of Access

AccountName

Admin

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

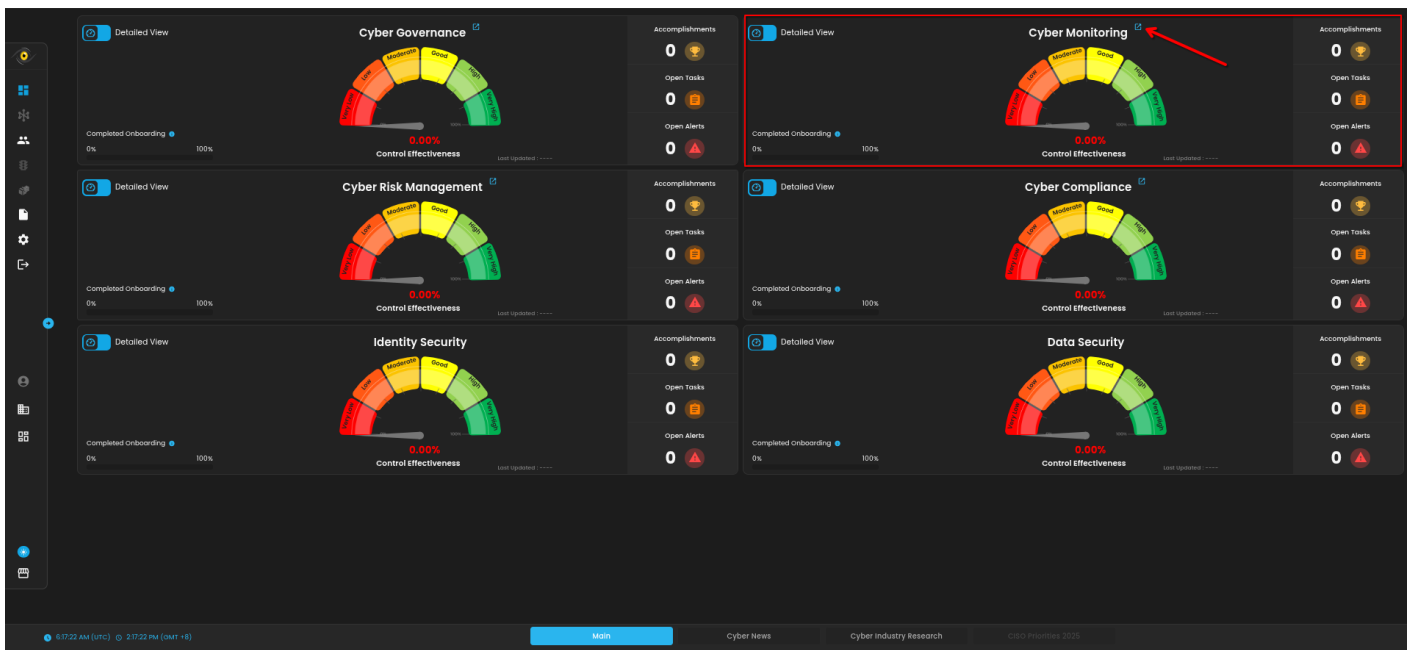
Please provide the credenetials to AQUILA Support.

1. **SentinelOne console URL** (<https://<your-sentinelone-domain>.sentinelone.net>, where "Domain" is the domain name of your SentinelOne account.)

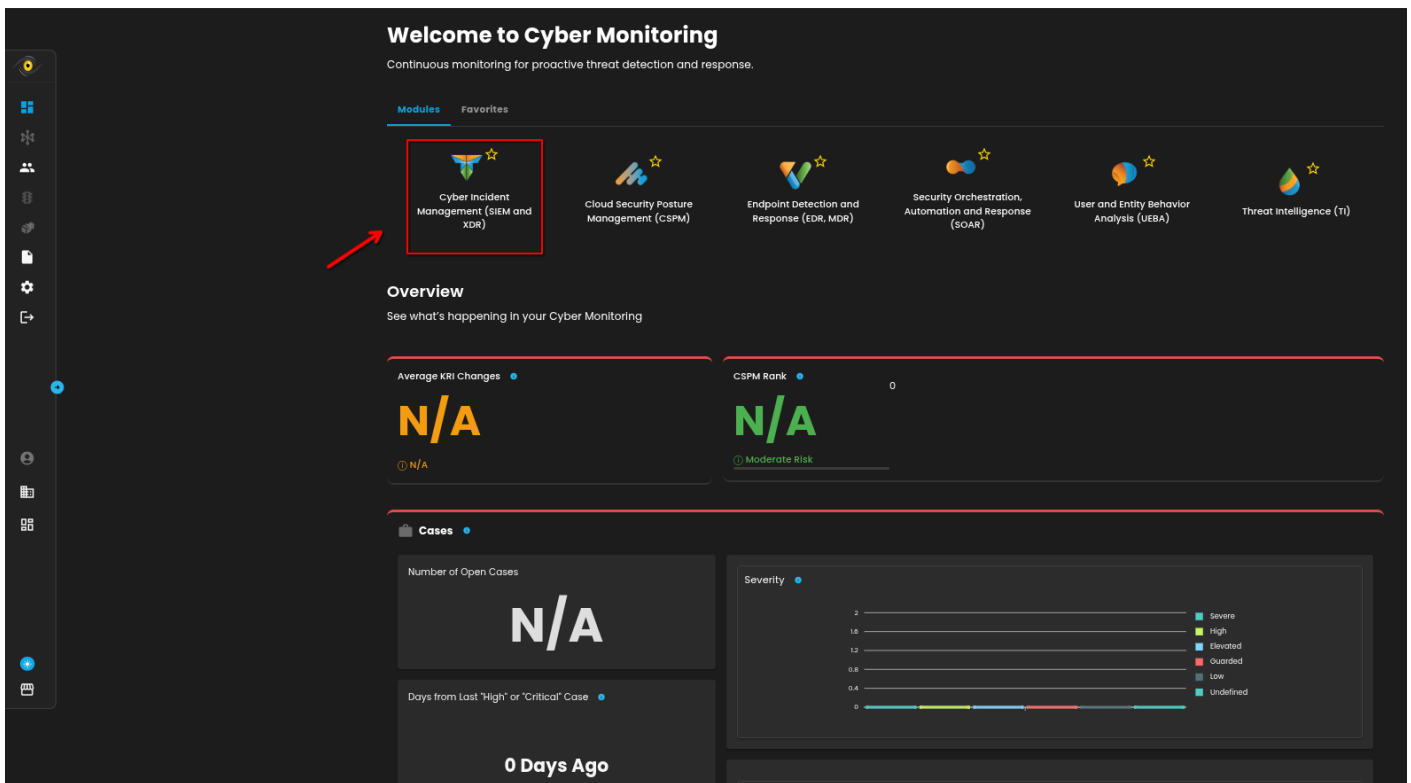
2. **API token**

Integrate on AQUILA

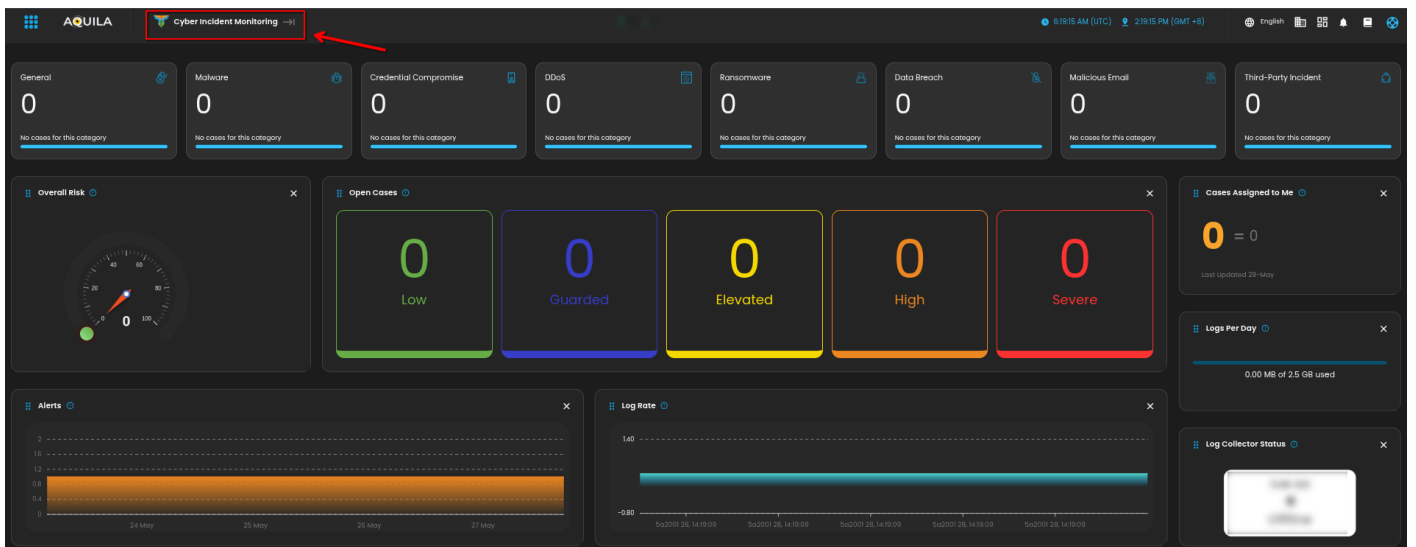
1. Log in to **CyTech - AQUILA**. Choose **Cyber Monitoring** and click the **small arrow icon** to redirect you to the Cyber Monitoring Dashboard.



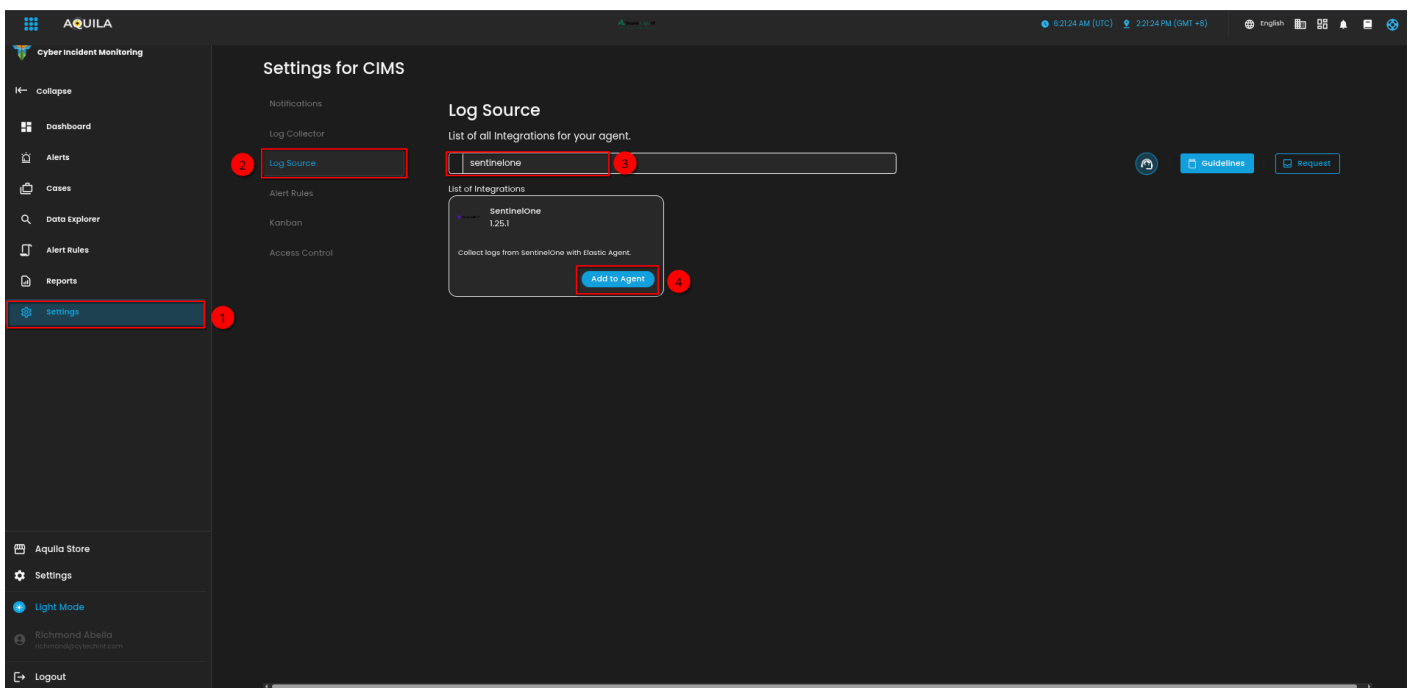
2. In the dashboard, choose **Cyber Incident Management (SIEM and XDR)**.



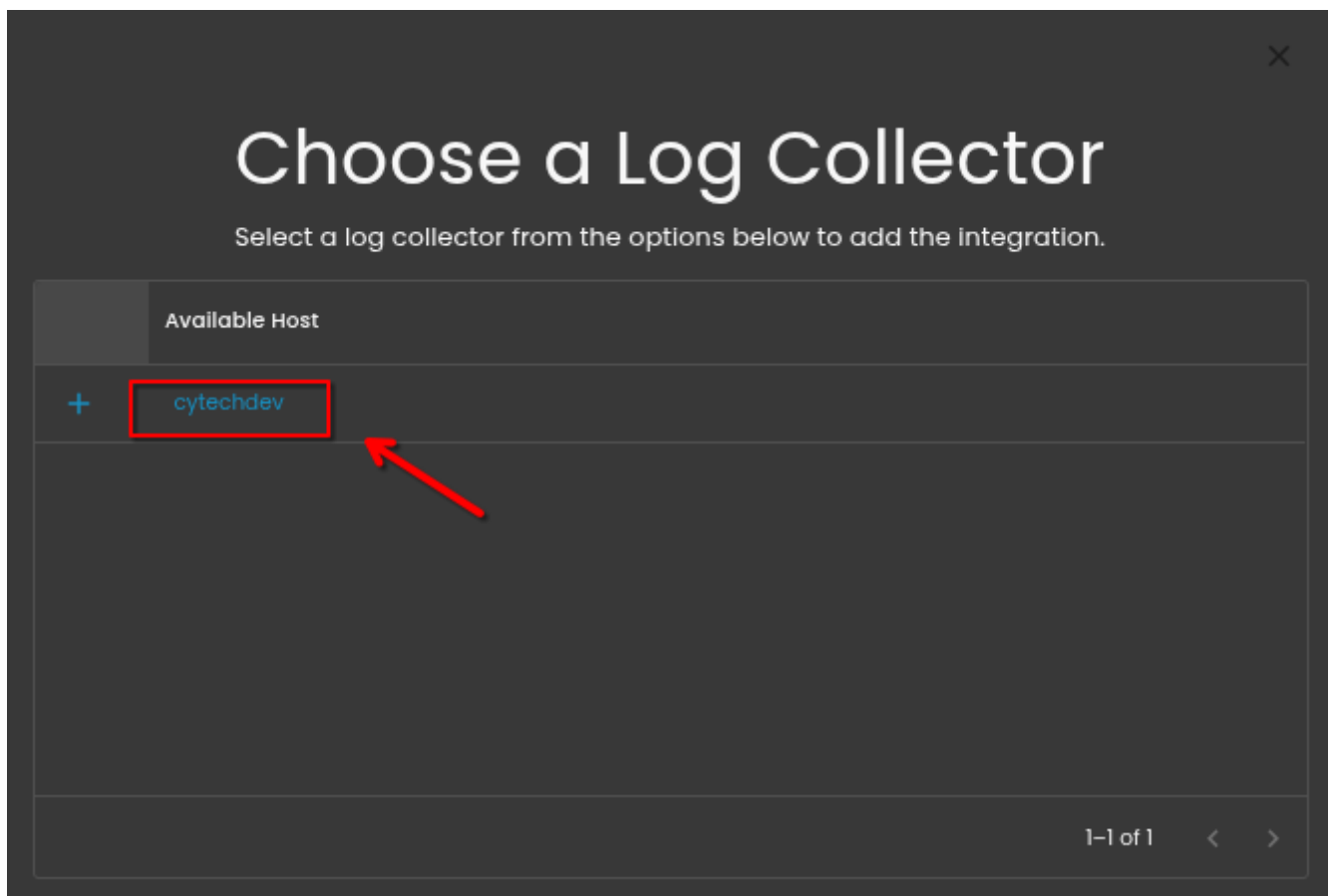
3. Navigate through the leftmost top and click **Cyber Incident Monitoring**.



4. Navigate through **Settings>Log Source>Search Bar>Add to Agent**.



5. Choose your **Log Collector**.



6. In the integration settings follow the instructions given below.

1. Click the **drop arrow** to display the contents needed for the integration setup.
2. Provide **SentinelOne Console URL**.
3. Provide the **API Token**.
4. Finally, click **Next** to install the log source integration.

×

Integration Settings

Now, please provide the necessary information below.

Chosen Integration: SentinelOne

SentinelOne

1

^

2

☒ Collect SentinelOne logs via API

Collecting SentinelOne logs via API.

3

URL *

SentinelOne console URL.

API Token *

API Token with API Access Level type.

4

Next

7. Wait for the **Successfull** window to display, this will confirm the successfull integration.

×

Setting up your service

Great start! Now, please wait 2-3 minutes while we get everything ready for you.

Adding User info to our SIEM

0%

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

Revision #4

Created 21 October 2024 01:46:38 by David Napoleon Romanillos

Updated 28 May 2025 07:18:44 by Richmond Abella