

Cisco AMP for Endpoints API Integration

To integrate **Cisco AMP for Endpoints (now part of Cisco Secure Endpoint)** with **Elastic**, follow these general steps:

Get Cisco AMP API Credentials

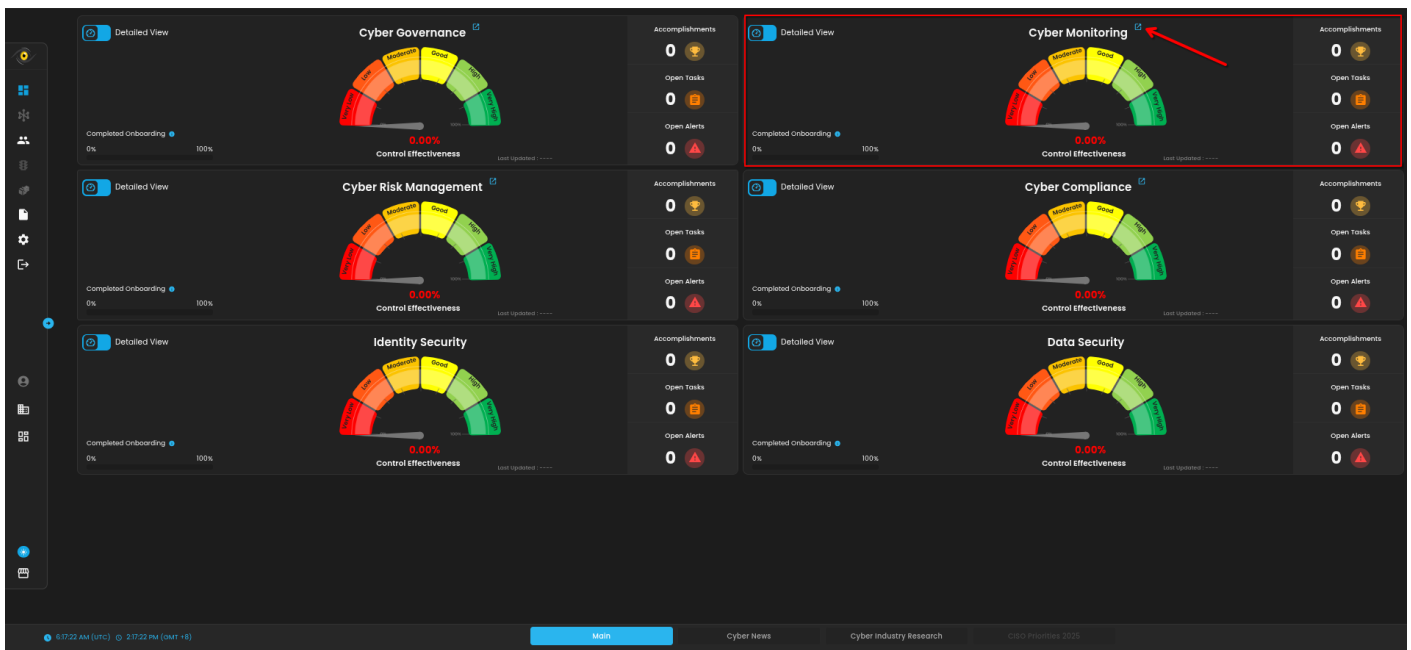
You need to enable API access from the Cisco Secure Endpoint console.

- Log in to: <https://console.amp.cisco.com>
- Go to **Accounts > API Credentials**
- Click **Create API Credential**
- Choose "**Read & Write**" or at minimum "**Read-only**"
- Save:
 -
 -

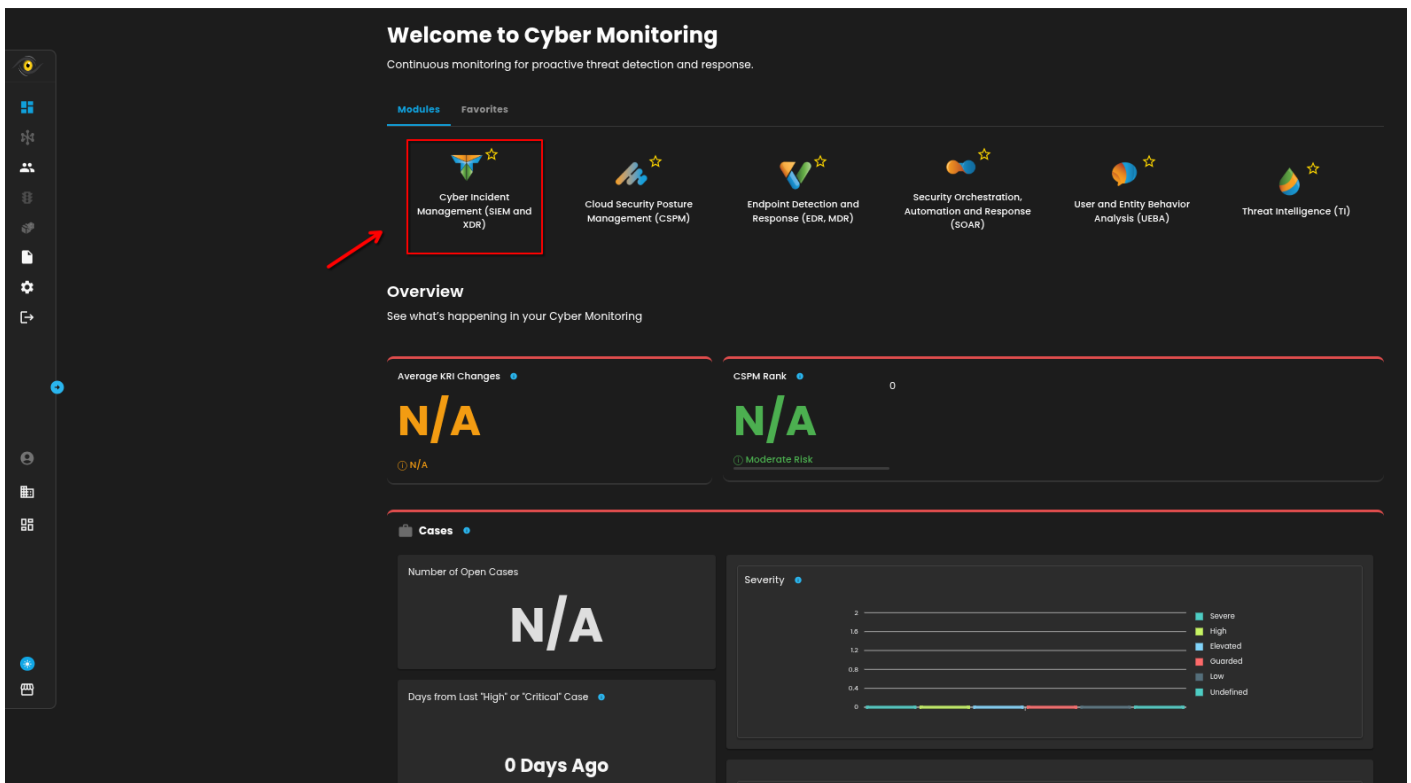
These will be used to pull events from the AMP API.

Integrate on AQUILA

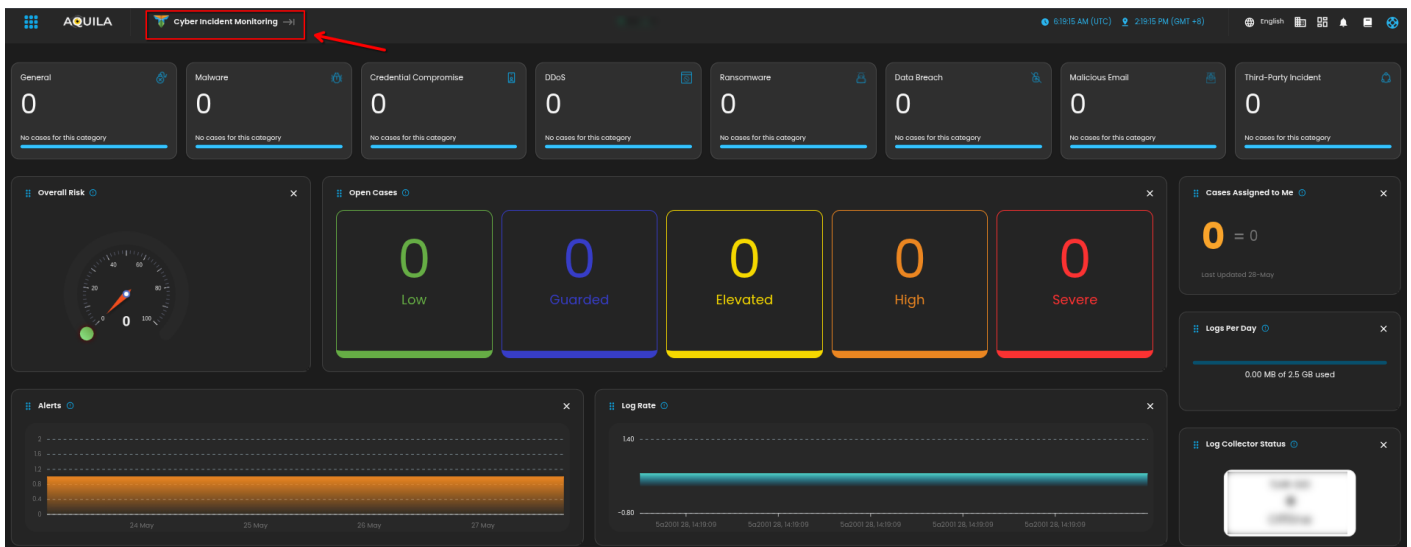
1. Log in to **CyTech - AQUILA**. Choose **Cyber Monitoring** and click the **small arrow icon** to redirect you to the Cyber Monitoring Dashboard.



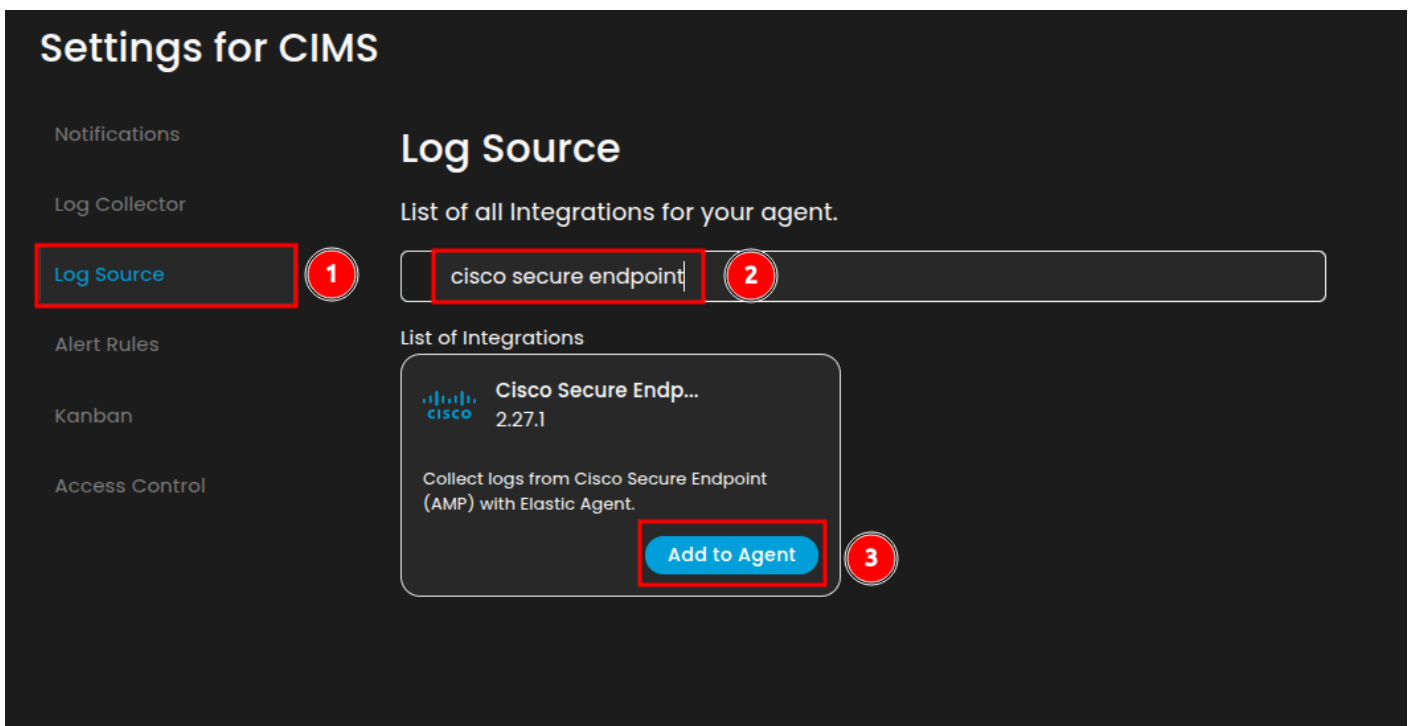
2. In the dashboard, choose **Cyber Incident Management (SIEM and XDR)**.



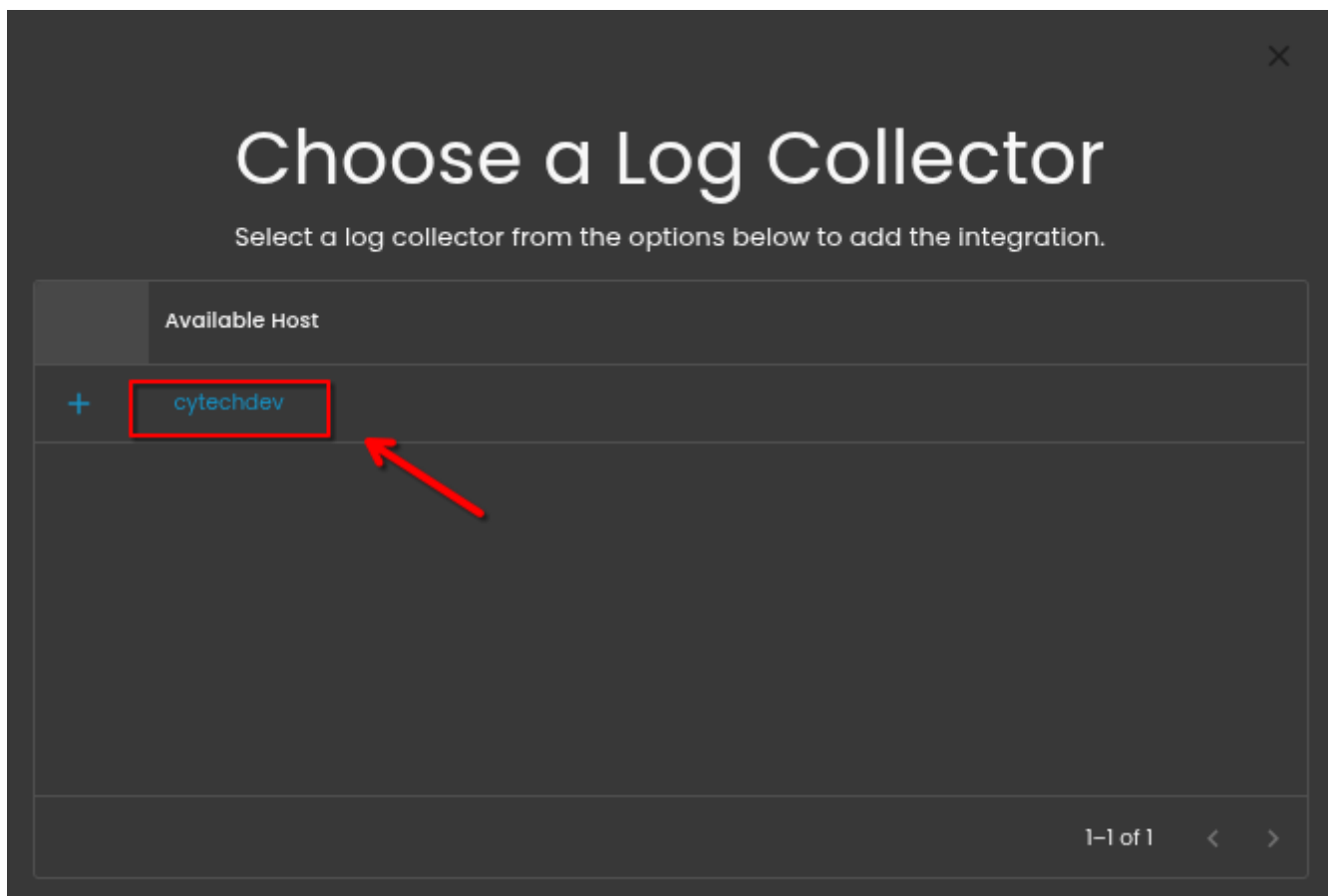
3. Navigate through the leftmost top and click **Cyber Incident Monitoring**.



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. Make sure the Collect logs from the Cisco Secure Endpoint API is **Enabled**.
2. Click the other **drop arrow** to display the other contents needed for the integration setup. Input the Client ID and the API Key.
3. **Scroll down**, leave the other text fields to its default value and go to **Tags**. Click the **Tags** text field and add **cisco-secure_endpoint** and **forwarded**.
4. Finally, click **Next** to install the log source integration.



Integration Settings

Now, please provide the necessary information below.

Chosen Integration: Cisco Secure Endpoint logs

Cisco Secure Endpoint logs

2

☒ Collect logs from the Cisco Secure Endpoint API
Collecting logs from the Cisco Secure Endpoint API

1

^

Cisco Secure Endpoint logs

3

v



Next



Cisco Secure Endpoint logs



Cisco Secure Endpoint logs

Collect Cisco Secure Endpoint logs via the API

Client ID *

4

Cisco Secure Endpoint Client ID

API Key *

5

Cisco Secure Endpoint API Key

HTTP Client Timeout (Optional)

60s

Duration before declaring that the HTTP client connection has timed out. Valid time units are ns, us, ms, s, m, h.

Interval *

1h

Interval at which the logs will be pulled. The value must be between 2m and



Next



API URL *

`https://api.amp.cisco.com/v1/events?offset=0&limit=300`

The API URL

Maximum logs per request *

100

Max number of logs pulled on each request

Initial Interval *

24h

Initial Interval for first log pull. Supported units for this parameter are h/m/s.

Tags *

Enter Tags

cisco-secure_endpoint

6

forwarded

7



Next

API URL *

https://api.amp.cisco.com/v1/events?offset=0&limit=300

The API URL

Maximum logs per request *

100

Max number of logs pulled on each request

Initial Interval *

24h

Initial Interval for first log pull. Supported units for this parameter are h/m/s.

Tags *

cisco-secure_endpoint x

forwarded x

Enter Tags

x

☐ Preserve original event *

Preserves a raw copy of the original event, added to the field `event.original`

8

Next

7. Wait for the **Successful** window to display, this will confirm the successful 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 #2

Created 19 June 2025 07:55:08 by Jeff Saguing

Updated 19 June 2025 09:13:47 by Jeff Saguing