

AQUILA - Setup Integration from Auth0

Auth0 Integration Guide

Integrate **Auth0** to ingest identity-related logs such as login attempts, user authentications, MFA usage, and blocked requests to support identity threat detection and correlation.

Credentials & API Access Setup (Auth0)

Before setting up the integration, create a Machine-to-Machine application in Auth0 to collect logs via API.

Steps:

1. **Log in** to the Auth0 Dashboard.
2. Go to **Applications → APIs**.
3. Create or select your **Management API** (typically named `Auth0 Management API`).
4. Under **Machine-to-Machine Applications**, authorize your log collector app.
5. Take note of the following credentials:
 - **Auth0 Domain** (e.g., `your-tenant.us.auth0.com`)
 - **Client ID**
 - **Client Secret**
 - **Audience**: usually `https://your-tenant.us.auth0.com/api/v2/`

Required Detail	Value
Auth0 Domain	<code>your-tenant.auth0.com</code>
Client ID	From your M2M Application

Required Detail	Value
Client Secret	From your M2M Application
Audience	<code>https://your-tenant.auth0.com/api/v2/</code>
Token URL	<code>https://your-tenant.auth0.com/oauth/token</code>

Permissions Reference (Auth0 M2M App)

Ensure the app is granted the following scopes from the **Auth0 Management API**:

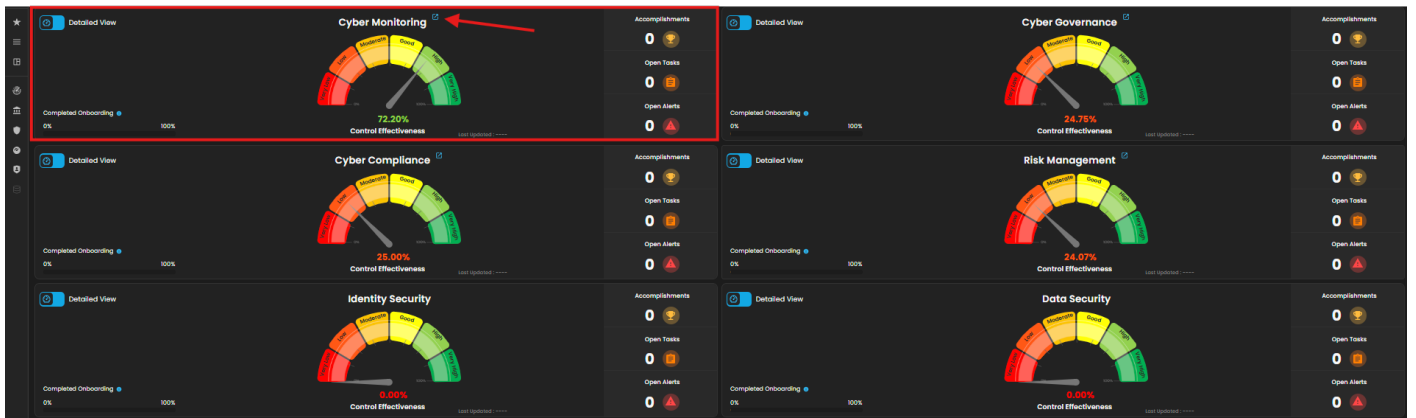
Data Stream	Scope Required
Login Activity	<code>read:logs</code> , <code>read:users</code>
MFA Logs	<code>read:logs</code>
Failed Logins	<code>read:logs</code>
User Access Logs	<code>read:users</code> , <code>read:logs</code>

“ ” You can test token access using Postman or curl before ingesting.

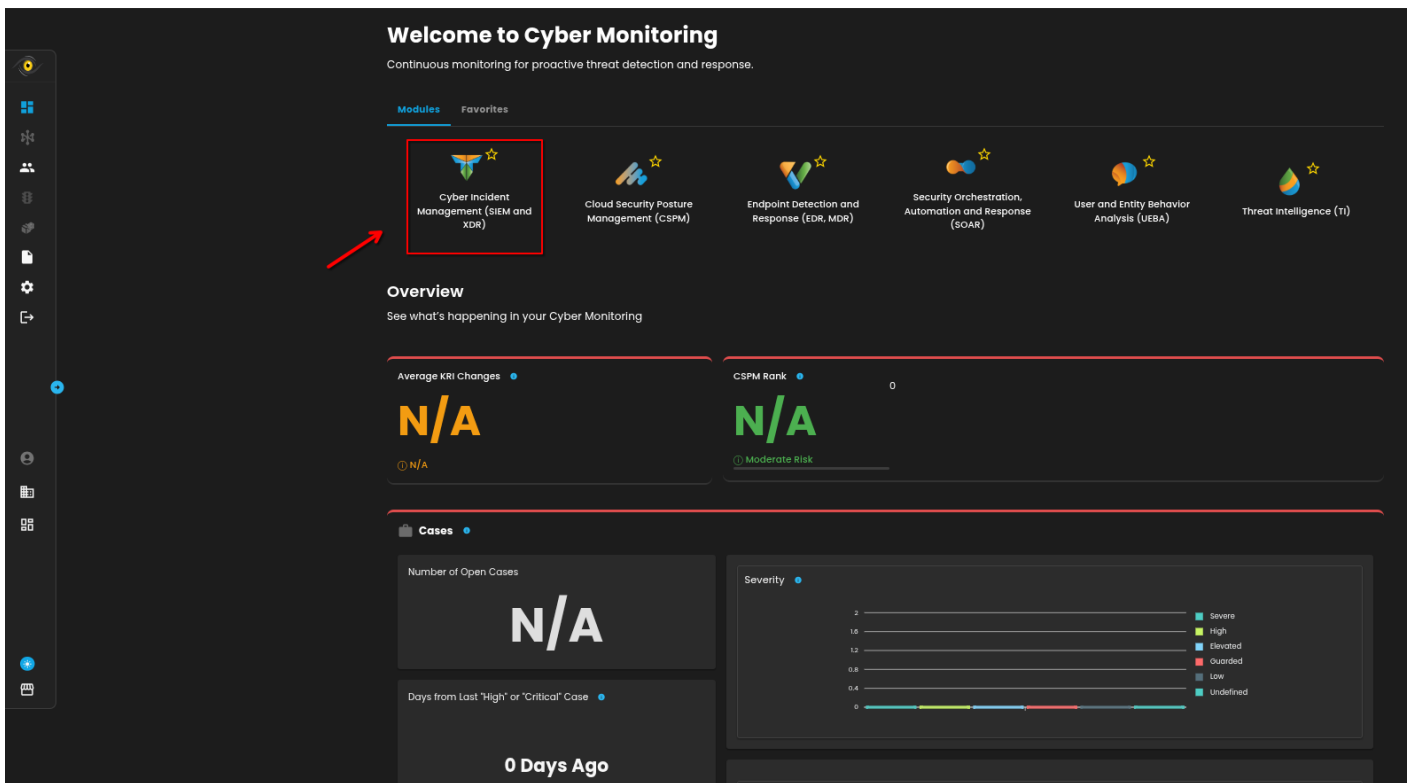
Aquila Integration Configuration

AQUILA - Microsoft 365 Integration

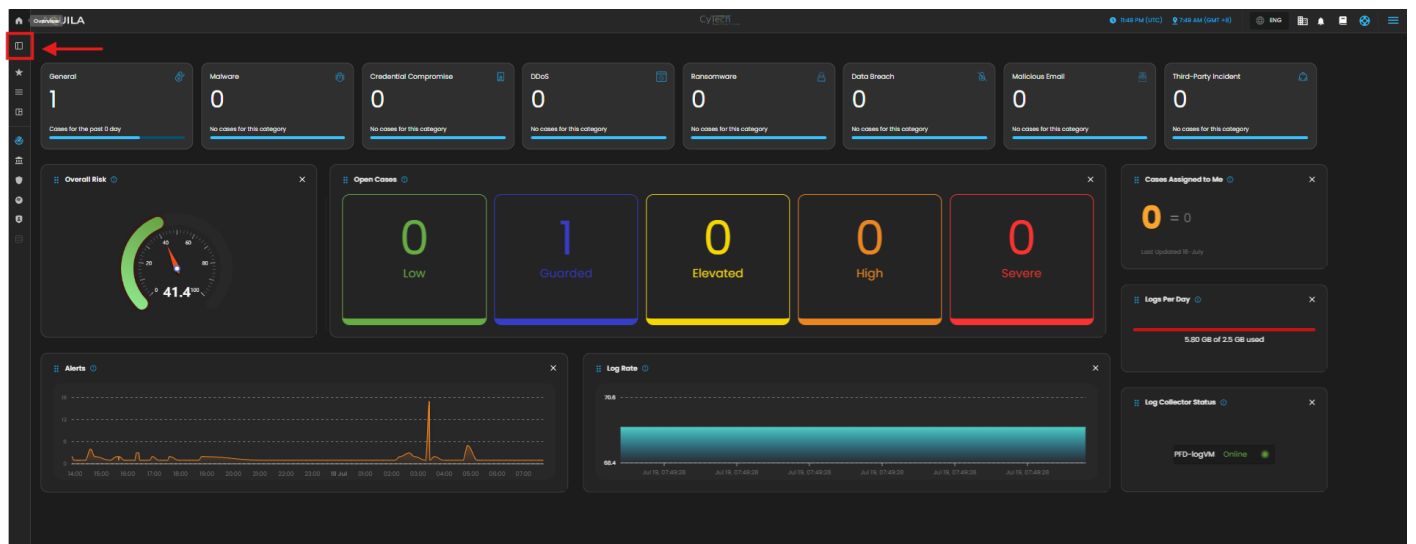
1. Log in to AQUILA click here - [CyTech - AQUILA](#). Choose **Cyber Monitoring** and click the **small arrow icon** to redirect you to the Cyber Monitoring Dashboard.



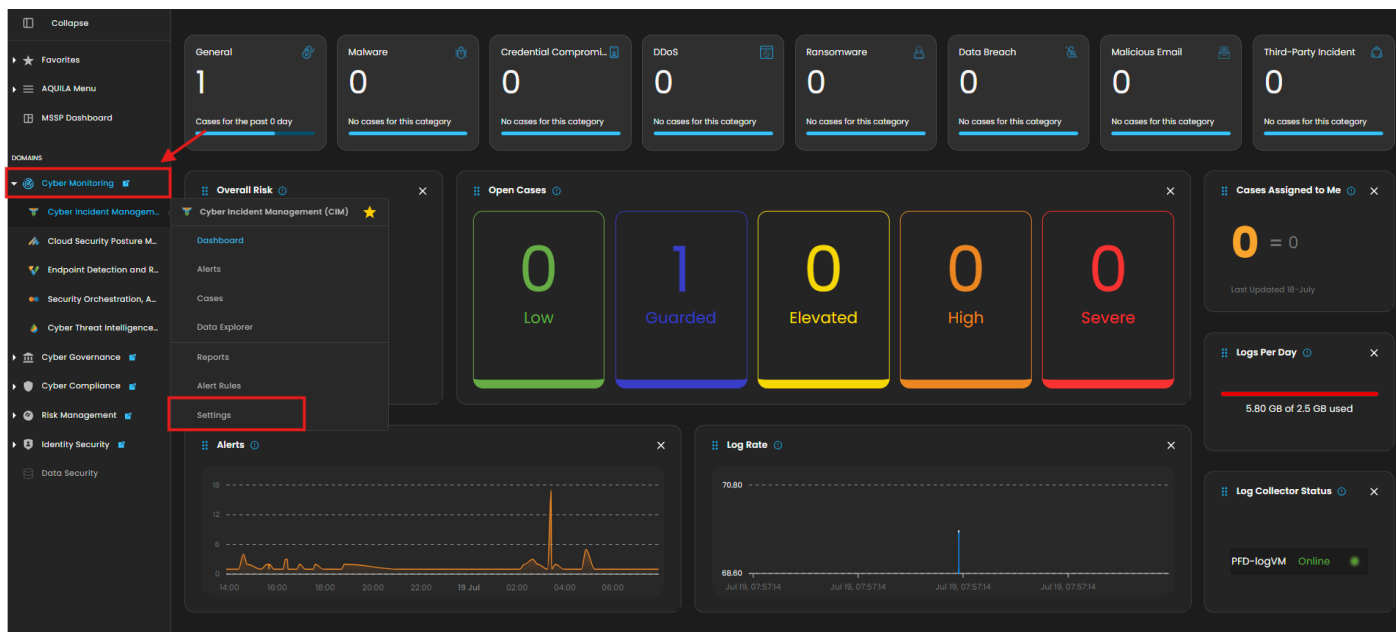
2. In the dashboard, choose **Cyber Incident Management (SIEM and XDR)**.



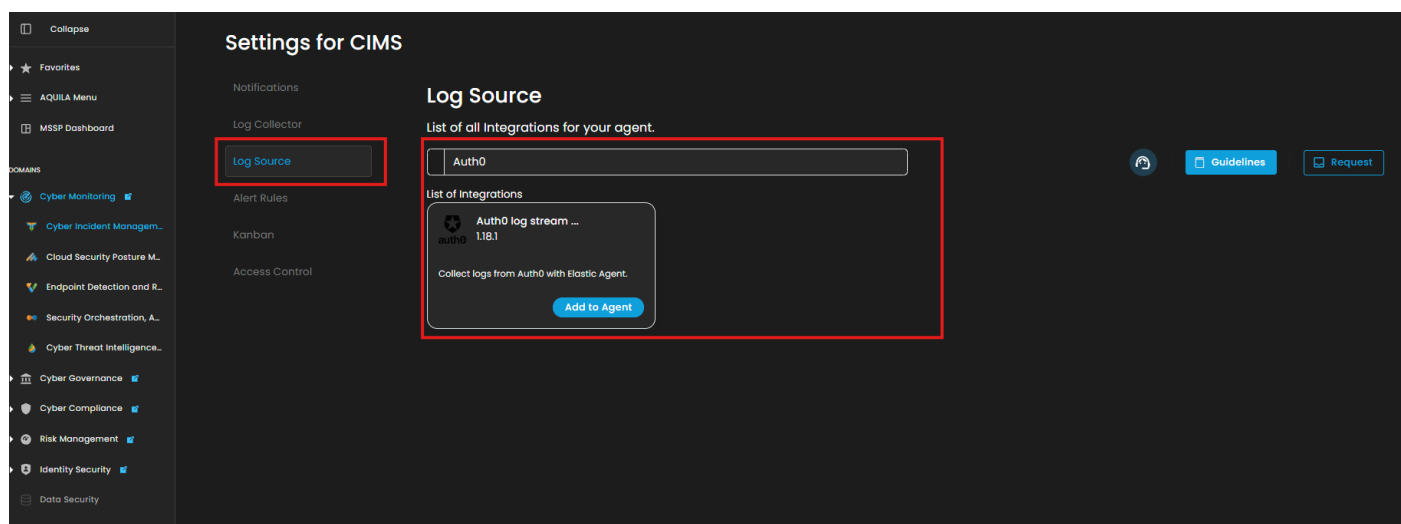
3. Navigate through the leftmost top and click **Cyber Incident Monitoring**.



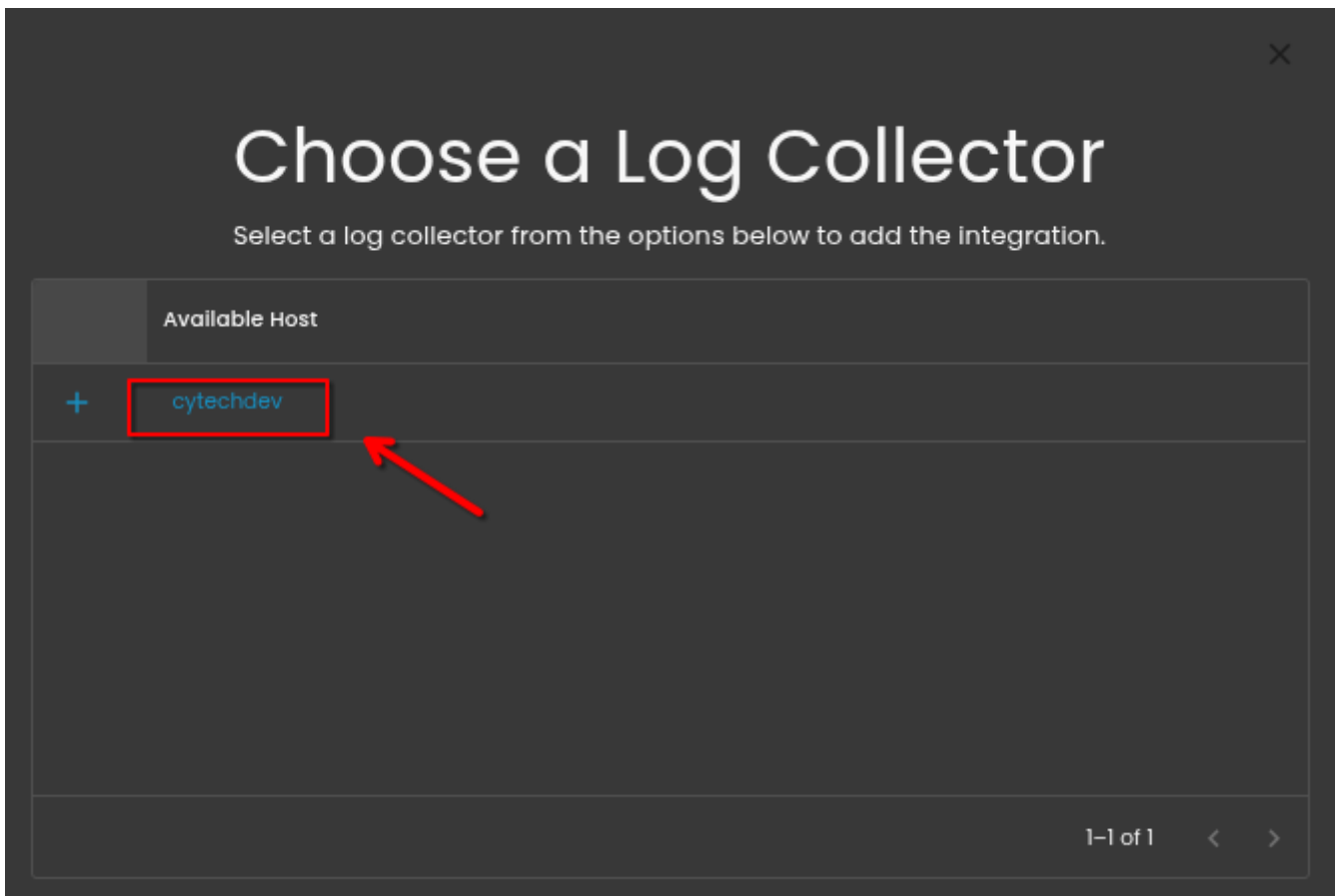
4. Navigate the "Cyber Monitoring" then hover the "Cyber Incident Management" till you see the settings.



5. Click the "Settings, and Navigate through **Settings>Log Source>Search Bar>Add to Agent**.



6. Choose your **Log Collector**. (If you not yet installed your **Log Collector** please refer to this link - **Log Collector Installation**.)



Step 7 and below is just a reference, this is still incomplete. Thorough investigation and research in progress to understand the flow and credentials required.

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

- Click the **drop arrow** to display the contents needed for the integration setup.
- In the **Office 365 logs section > Disable > Collect Office 365 audit logs**

Integration Settings

Now, please provide the necessary information below.

Chosen Integration: Auth0 log stream events

Auth0 log stream events

☒ Collect Auth0 log streams events via Webhooks
Collecting Auth0 log stream events via Webhooks.

☒ Collect Auth0 log events via API requests
Collect Auth0 log events via API requests.

Auth0 logs

Next

- Scroll down and go to **Microsoft Office 365 audit logs section**.
- Input the credentials for **Directory(tenant) ID, Application(client) ID and the Client Secret Value**.
- Finally, click **Next** to install the log source integration.

Auth0 logs

Auth0 log events via Webhooks

Receives log events from Auth0 via Webhooks

Listener Address

localhost

Bind address for the listener. Use 0.0.0.0 to listen on all interfaces.

Listener Port

8383

Webhook path

/auth0/logs

URL path where the webhook will accept requests.

undefined (Optional)

Authorization token

Next

8. 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 #7

Created 17 July 2025 23:47:34 by Kent Lauron

Updated 19 July 2025 00:09:37 by Kent Lauron