AQUILA - Microsoft Office 365 Integration

Overview

This integration with Microsoft Office 365 supports the ingestion of user, administrator, system, and policy-related events. It leverages the Office 365 Management Activity API to retrieve activity logs from both Office 365 and Azure Active Directory (Azure AD).

This guide outlines the required steps to integrate with **Microsoft Office 365 and Azure AD** using the **Office 365 Management Activity API**. It covers application registration, permission setup, audit log configuration, and retrieval of key credentials for secure API access.

Summary of Actions Required:

1. **Register an Application** in Microsoft Entra ID (formerly Azure AD) to establish identity and enable API access.
2. **Configure API Permissions** for Microsoft Graph and Office 365 Management APIs to authorize required data access.
3. **Grant Admin Consent** to ensure permissions are applied tenant-wide.
4. **Collect Key Credentials** such as Application ID, Tenant ID, and Client Secret for use in your integration.
5. **Verify if Unified Audit Logging is Enabled** in Microsoft 365 to ensure activity data is available via the API.

Action Items Before Proceeding:

- Ensure you have **Global Admin** access to your Azure/Microsoft 365 tenant.
- Prepare to create or use an existing **App Registration** in Microsoft Entra ID.
- Confirm that **Unified Audit Logging** is enabled; otherwise, prepare to activate it via the Microsoft 365 portal or PowerShell.
- Take note of your **admin email address** for PowerShell commands if using CLI to manage audit log settings.

Steps to Configure Office 365 Integration for the Client

Step 1: Microsoft Entra ID - App Registration

Register Your Application in Microsoft Entra ID:

- Log in to your Azure Account, click here - **Azure Portal Link**.
- Navigate to Azure Active Directory > **App registrations**.
- Click **New Registration**.
- Provide a Name for the application, we can suggest "**CyTechAQUILA-Monitoring**".
- Click **Register**.

Step 2: API Permissions

Microsoft Graph API Permissions:

If **User.Read** permission under **Microsoft Graph** tile is not added by default, add this permission.

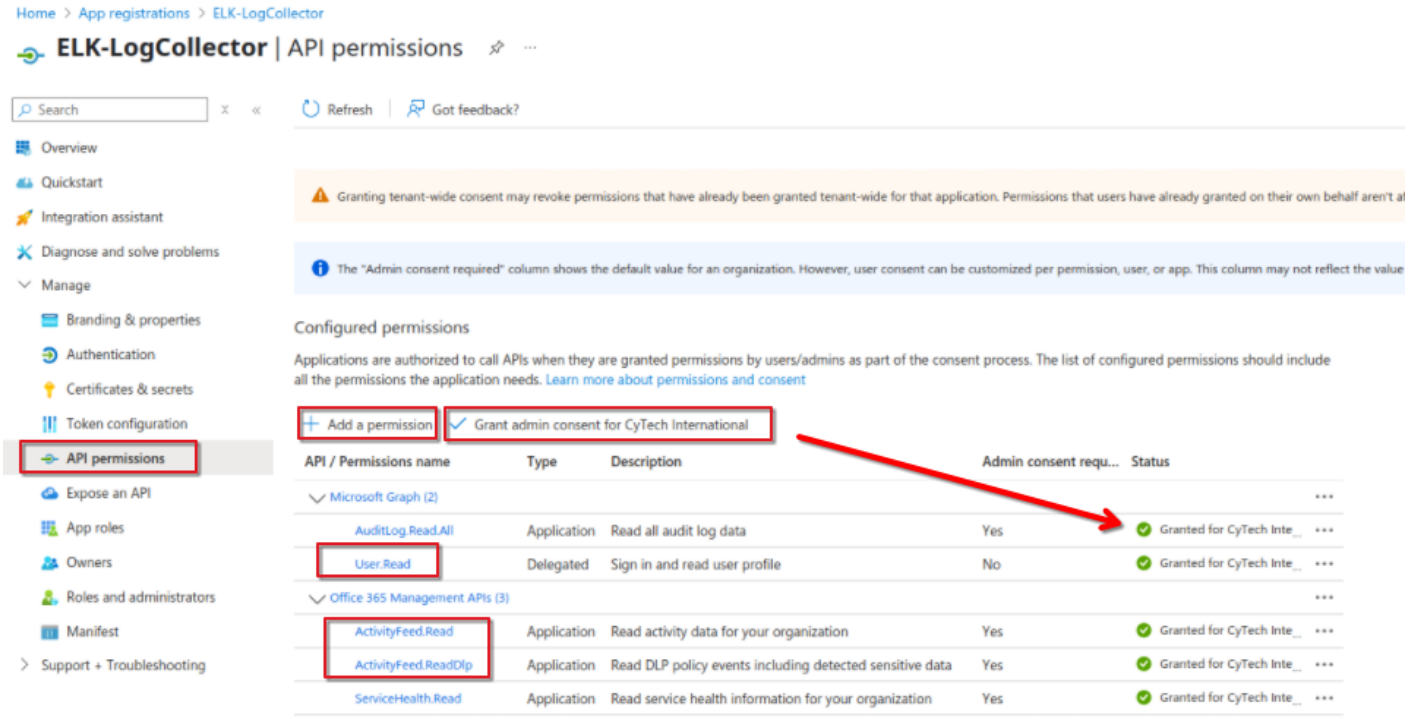
- Navigate to **App registrations** in the Azure Portal.
- Select the App you just created, then go to **API Permissions**.
- Search for **Microsoft Graph.**
- Click **Add a permission**.
- Select **Microsoft Graph > Delegated permissions**.
- Search for and add **User.Read**.

Office 365 Management API Permissions:

- Search for **Office 365 Management APIs** and add the required permissions.
- In **Application Permissions**, look for permissions.
- Under ActivityFeed select: **ActivityFeed.Read**
- Optionally, select **ActivityFeed.ReadDLP** to read DLP policy events.

Grant Admin Consent:

- In API Permissions, click **Grant admin consent** for <tenant name>.
- **Confirm** the action.



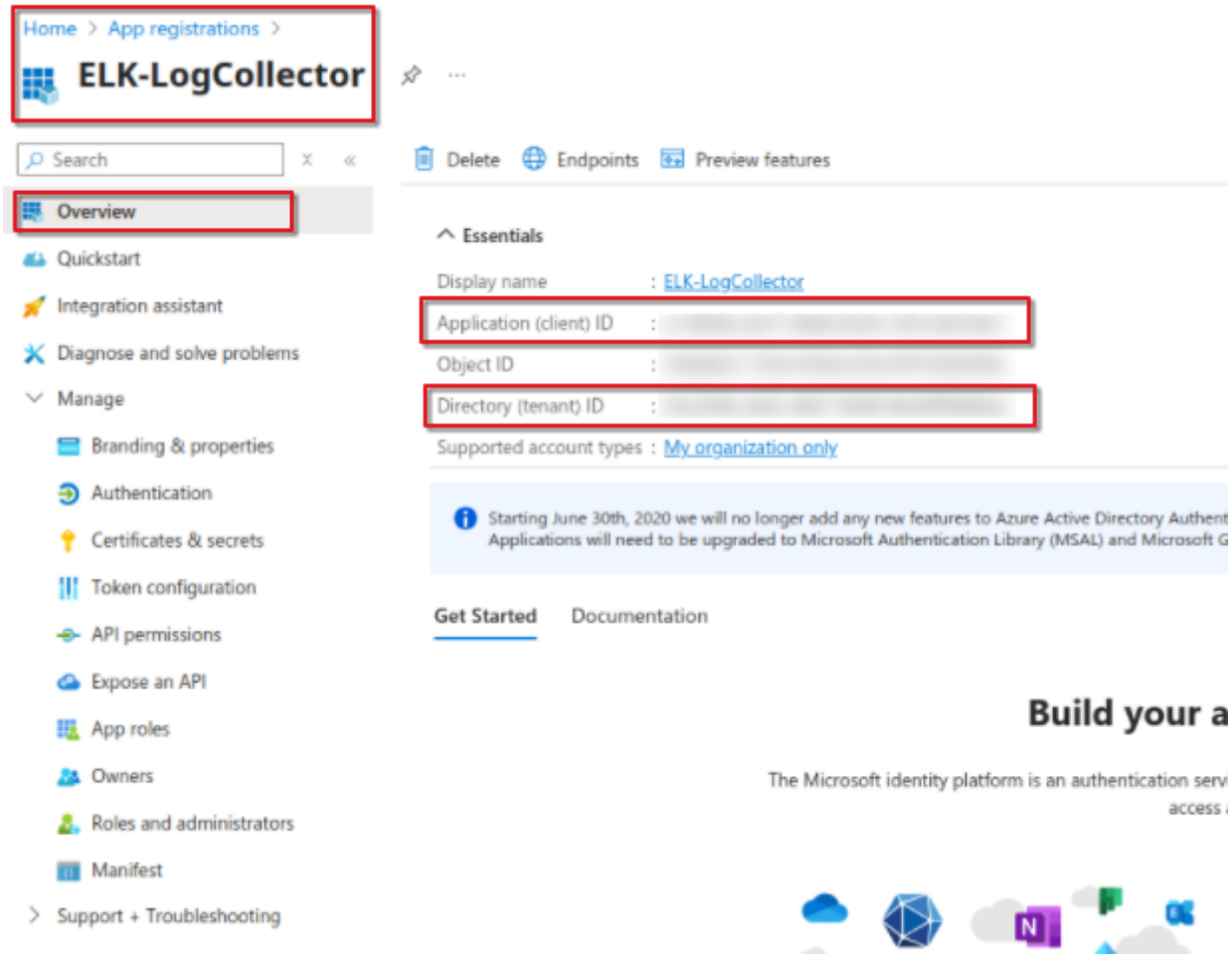
Step 3: Integration Requirements for Office 365

Application (Client) ID:

- Go to **App registrations** > **Select your application**.
- Copy the **Application (client) ID** from the overview page.

Directory (Tenant) ID:

- In the Azure Portal, navigate to **Azure Active Directory** > **Overview**.
- Copy the **Directory (tenant) ID**.



Create New Client Secret (Value):

- In **App registrations > Select your application**, go to **Certificates & secrets**.
- Click **New client secret**.
- Add a description and expiration period, then click Add.
- Copy the **Value (displayed only once)**.

Step 4: Verify Unified Audit Logging is Enabled

Unified Audit Logging must be enabled before accessing data via the Office 365 Management Activity API.

Method 1: Using Microsoft 365 Security & Compliance Center

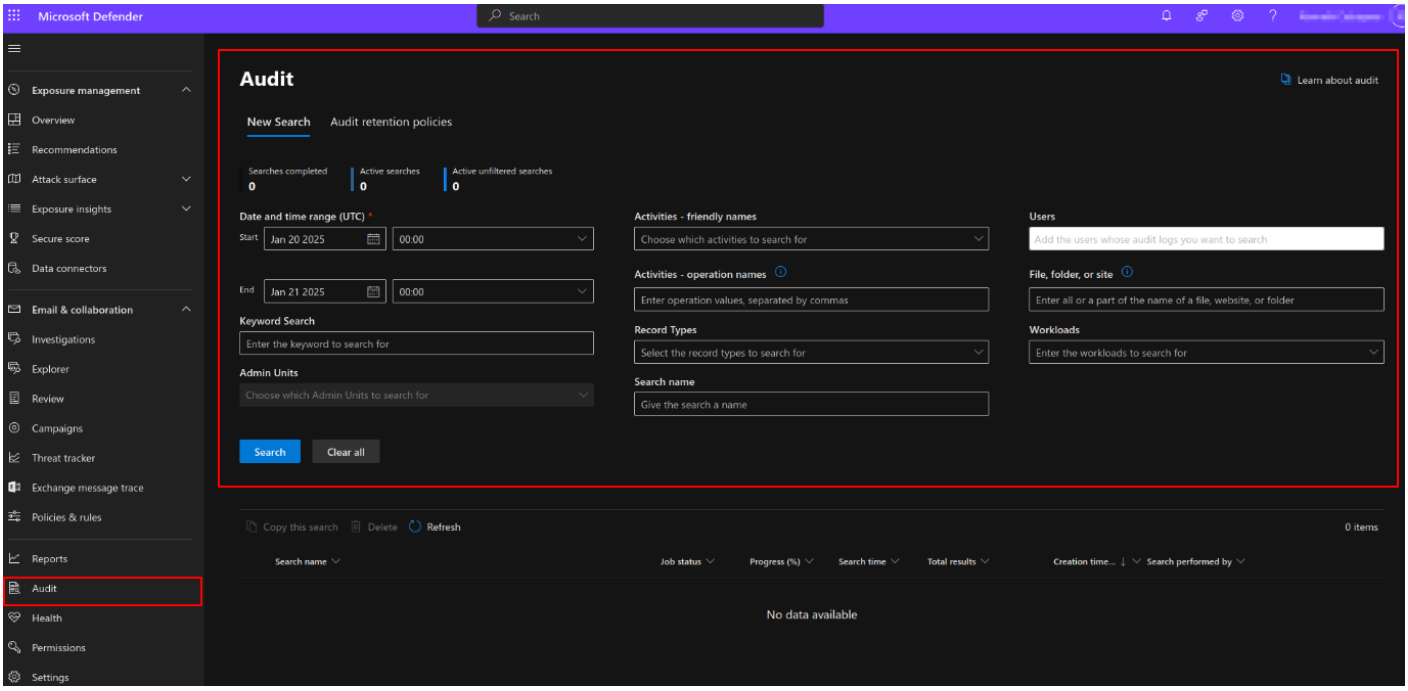
1. Sign in to Microsoft 365:

- Go to https://admin.microsoft.com and sign in with your Global Admin credentials.

2. Access the Security & Compliance Center:
   - In the left-hand menu, under Admin centers, click on Security (or go directly to https://security.microsoft.com).

3. Navigate to Audit Log Search:
   - In the Security & Compliance Center, go to Search in the left-hand menu and click on Audit log search.

4. Check Audit Log Status:
   - If you see an option to search the audit log, then audit logging is already enabled.
   - If you see a banner that says "Start recording user and admin activity" or a prompt to enable auditing, it means that audit logging is not yet enabled.



5. Enable Audit Logging:
   - If audit logging is not enabled, you can click on the prompt to enable it. This will enable auditing for all activities within your Microsoft 365 environment. The process may take a few hours to be fully operational.

Method 2: Using Powershell

1.Install and Update Exchange Online Management Module

- Open PowerShell as Administrator.
- Install the module:

```
Install-Module -Name ExchangeOnlineManagement
```

- Update the module:

```
Update-Module -Name ExchangeOnlineManagement
```

- Import the module

```
Import-Module ExchangeOnlineManagement
```

2.Connect to Exchange Online

- Run the following command:

```
Connect-ExchangeOnline -UserPrincipalName <admin-email-address>
```

- Replace <admin-email-address> with the admin email. Authenticate if required.

3.Check and Enable Unified Audit Logging

Check Status:

- Run:

```
Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled
```

- If the output is True, Unified Audit Logging is already enabled.

Enable Logging (if needed):

- If the output is False, enable it:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

- Verify again:

```
Get-AdminAuditLogConfig | Format-List UnifiedAuditLogIngestionEnabled
```

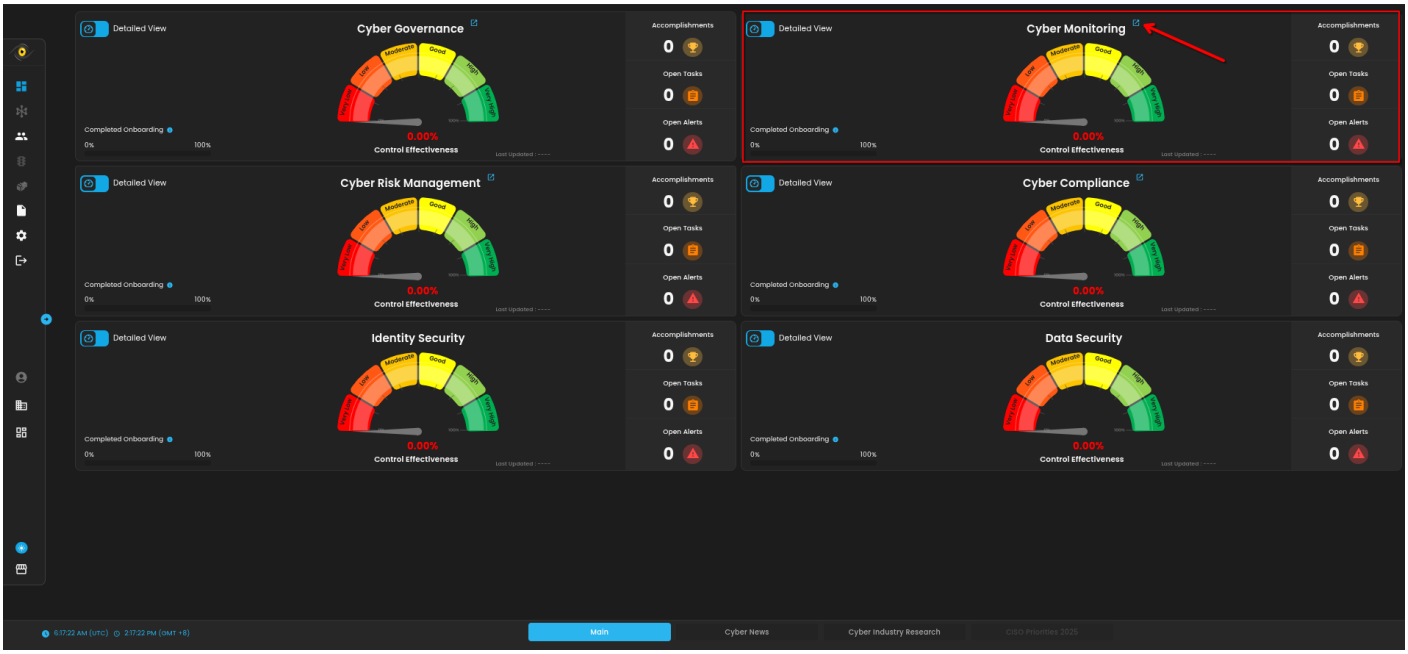
AQUILA – Microsoft 365 Integration Requirements

Please saved and provide this values to AQUILA Support Team.

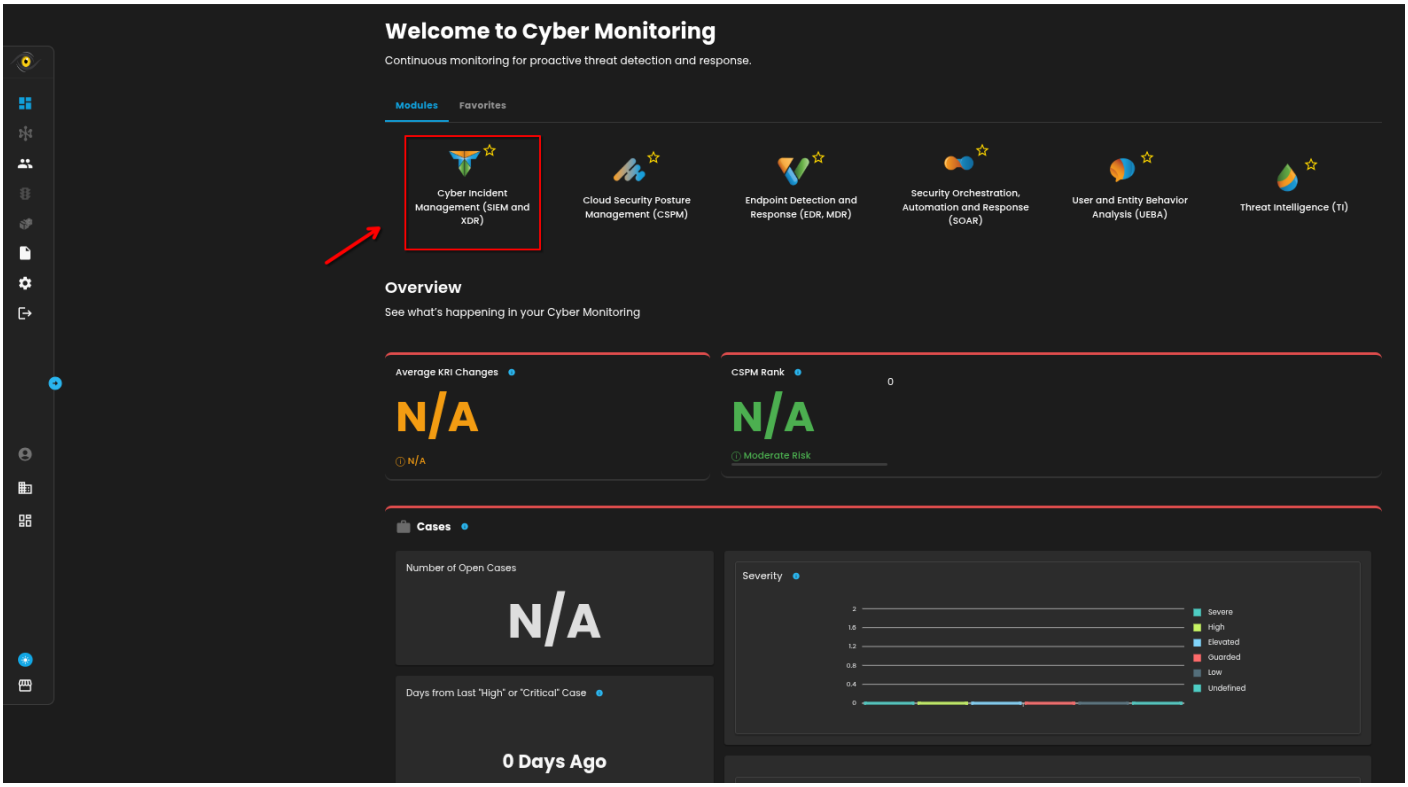
1. **Directory (tenant) ID:**
2. **Application (client) ID:**
3. **Client Secret Value:**

AQUILA – Microsoft 365 Integration

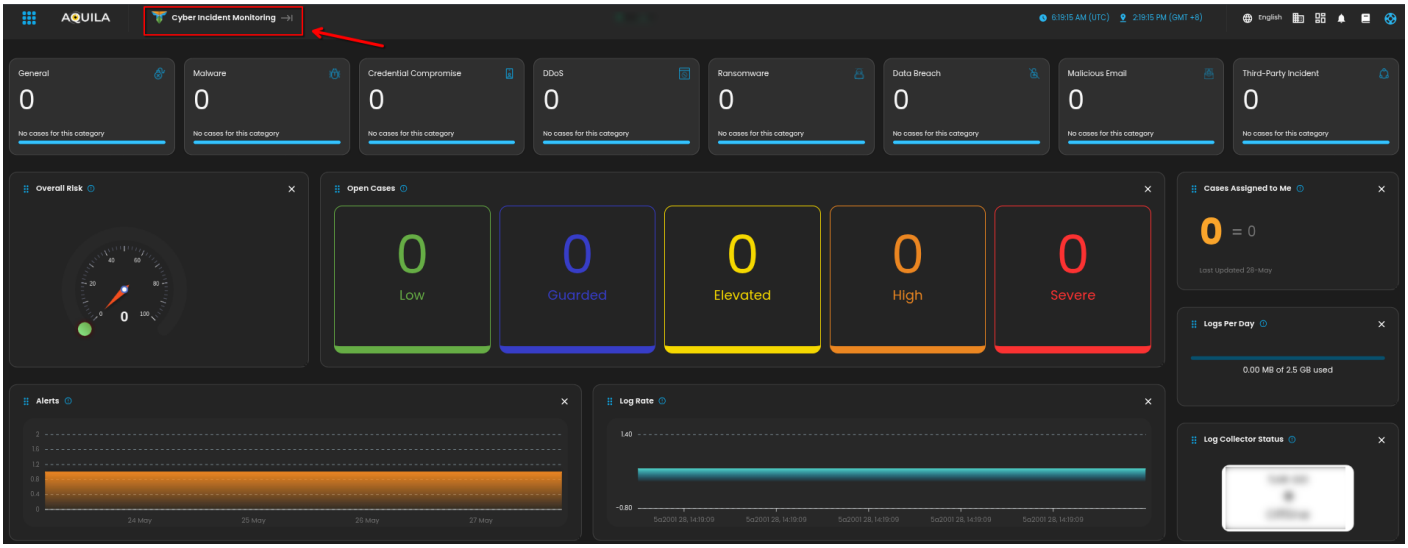
1. Log in to AQUILA click here - **CyTech - AQUILA**. Choose **Cyber Monitoring** and click the **small arrow icon** to redirect you to the Cyber Monitoring Dashboard.



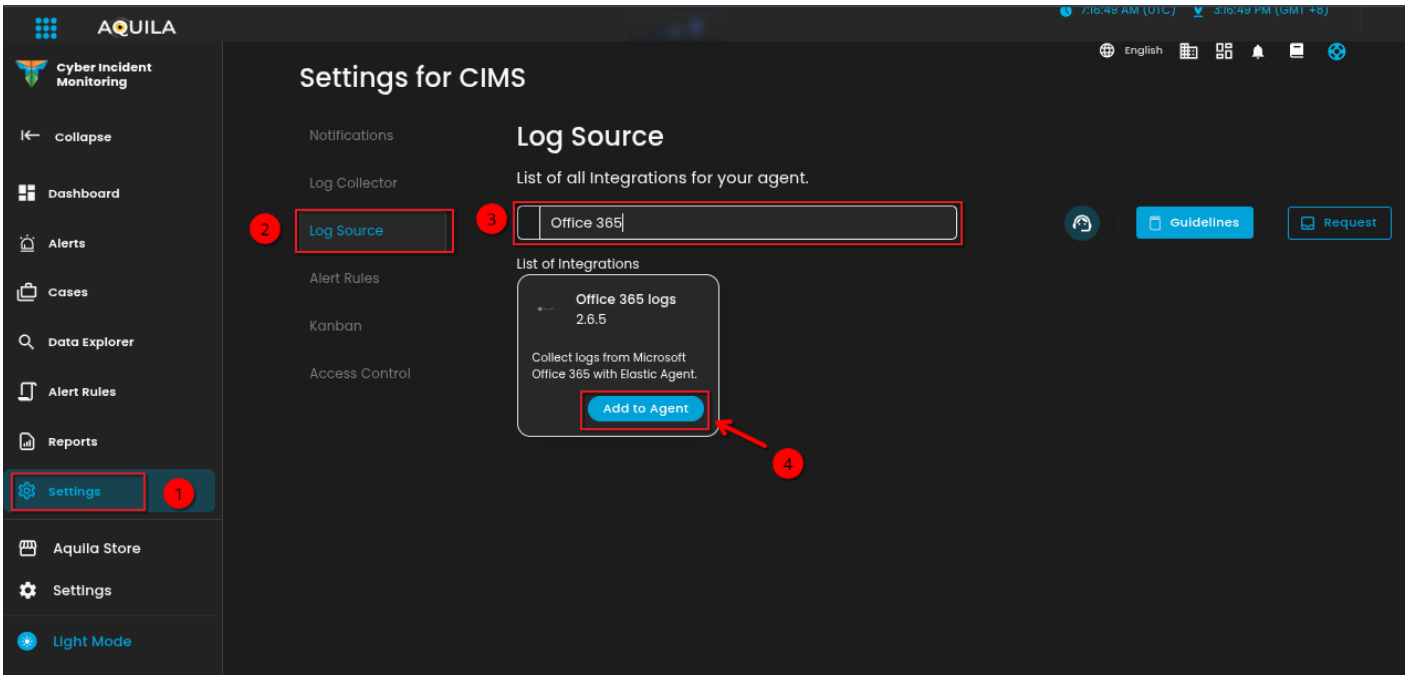
2. In the dashboard, choose **Cyber Incident Management (SIEM and XDR)**.



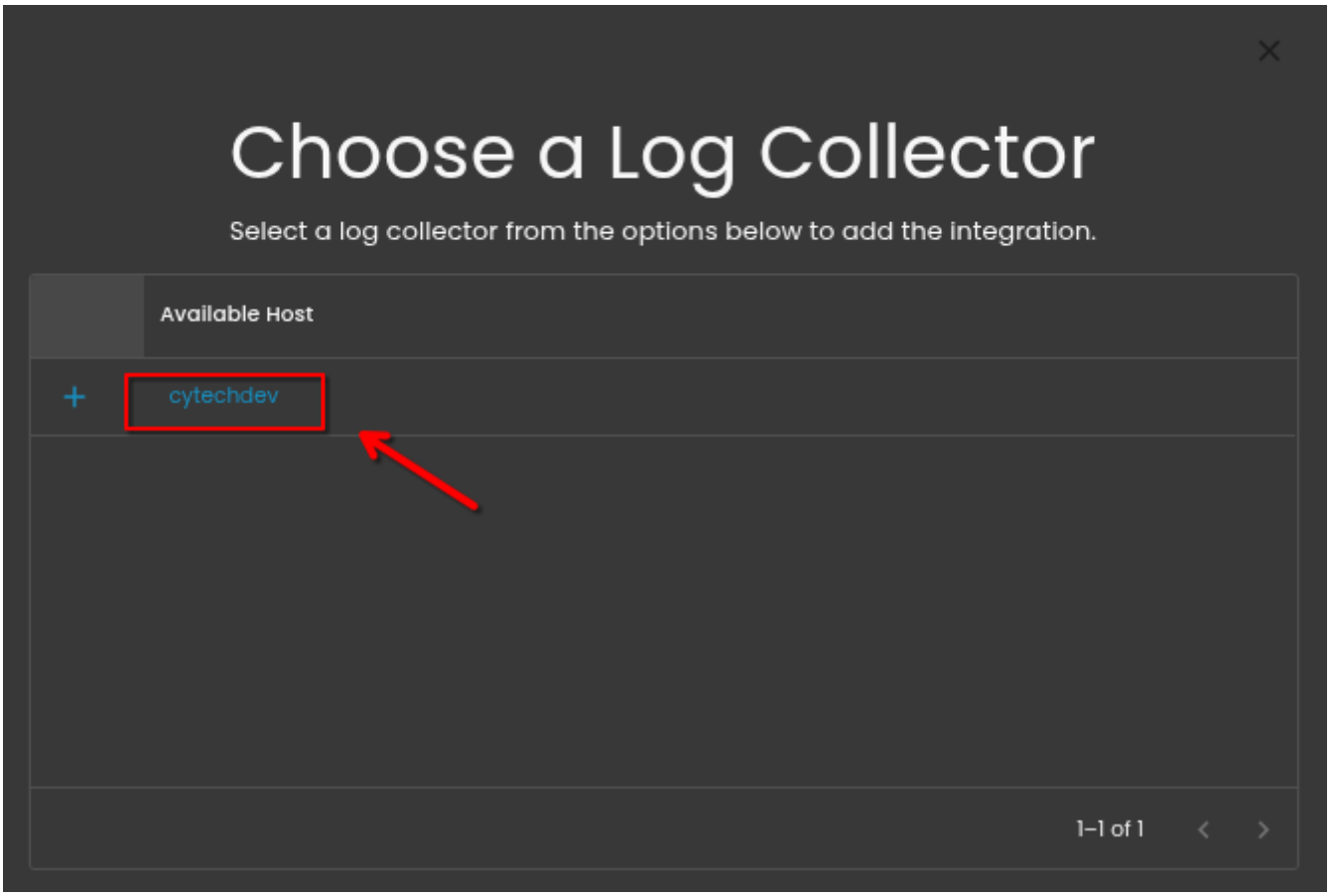
3. Navigate through the leftmost top and click **Cyber Incident Monitoring**.



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

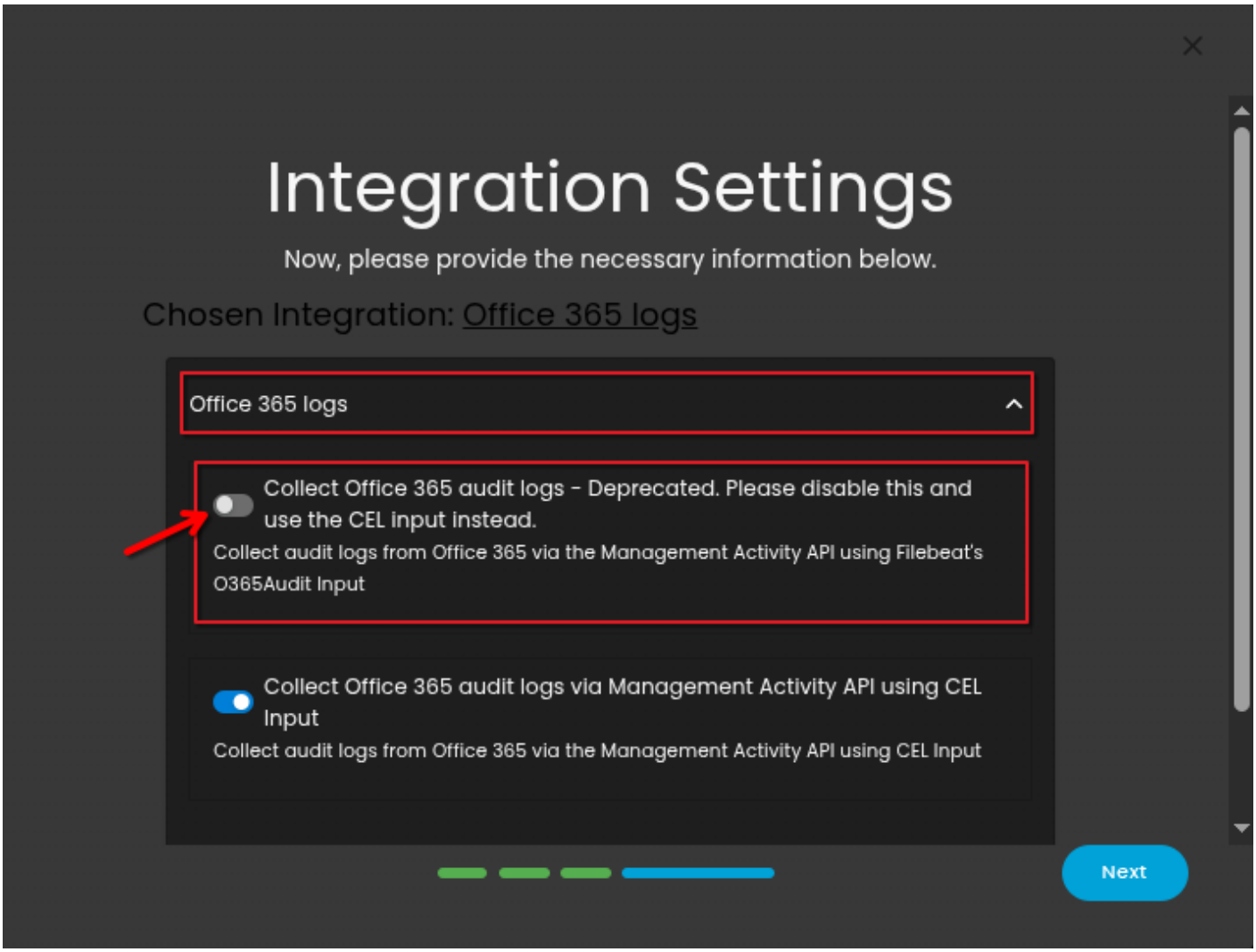


5. Choose your **Log Collector**. *(If you not yet installed your **Log Collector** please refer to this link - **Log Collector Installation.**)*



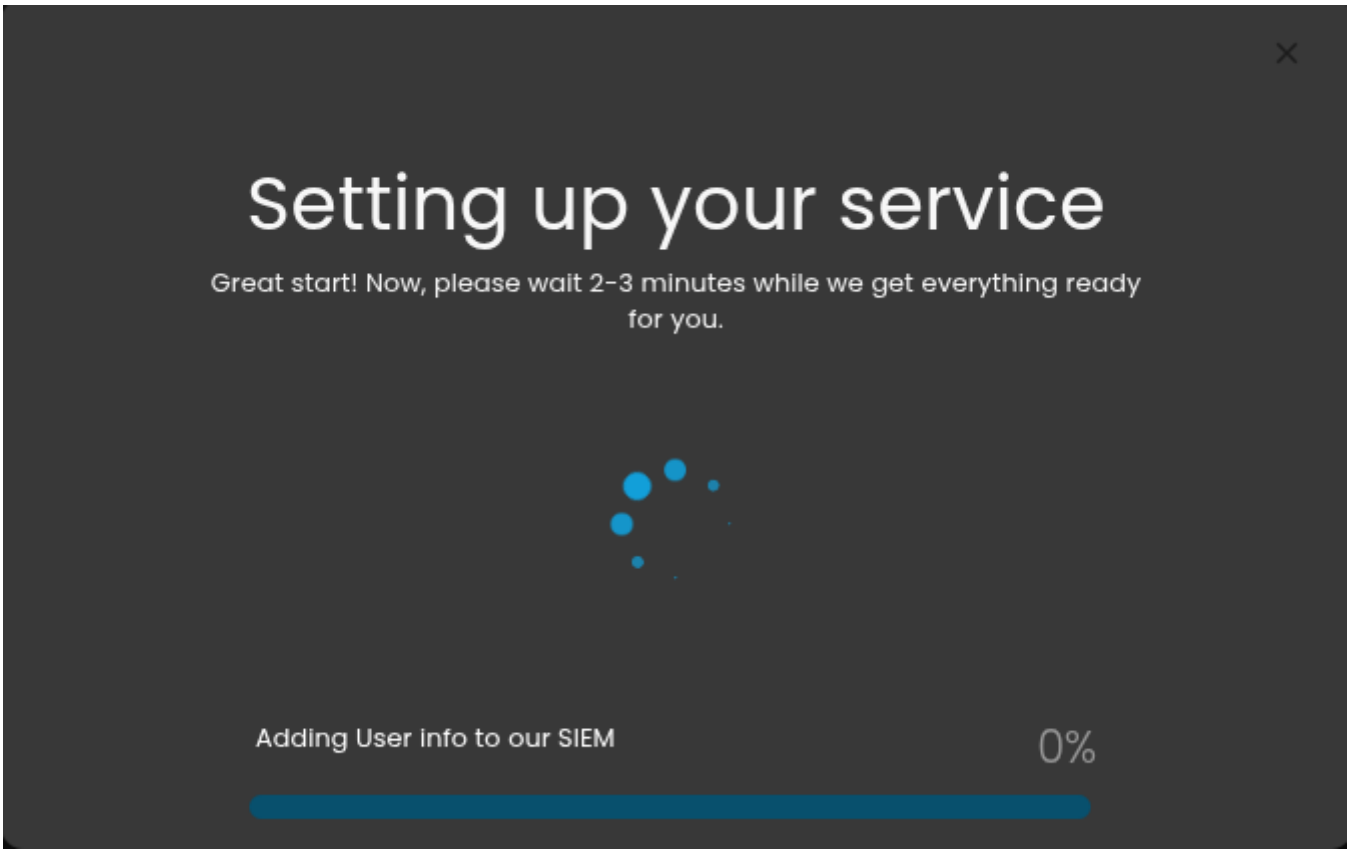
6. In the integration settings follow the instructions given below.

- 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**



- 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.

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



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

Revision #10
Created 21 January 2025 06:15:40 by Richmond Abella
Updated 29 May 2025 08:10:54 by Richmond Abella