

**Lab Manual- Setup and Manage Azure Sentinel with Preloaded data**

**Prepared for**:

**Date:** 18th Nov 2021

**Prepared by:**

Document Name: Lab Manual **Document Number** AZLabn990

**Contributor:**

Contents

[*1.* Introduction 3](#_Toc100855907)

[2. Lab: Setup Azure Sentinel workspace 3](#_Toc100855908)

[2.1 Enable Microsoft Sentinel 3](#_Toc100855909)

[3. Exercise 2: Deploy the Microsoft Sentinel Training Lab Solution 5](#_Toc100855910)

[4. Exercise 3: Configure Microsoft Sentinel Playbook 8](#_Toc100855911)

[5. Connect to Active Directory 9](#_Toc100855912)

[6. Connect to Azure Activity 11](#_Toc100855913)

[7. Enable Microsoft Defender for Cloud data connector 16](#_Toc100855914)

[8. Enable Threat Intelligence TAXII data connector 17](#_Toc100855915)

# Introduction

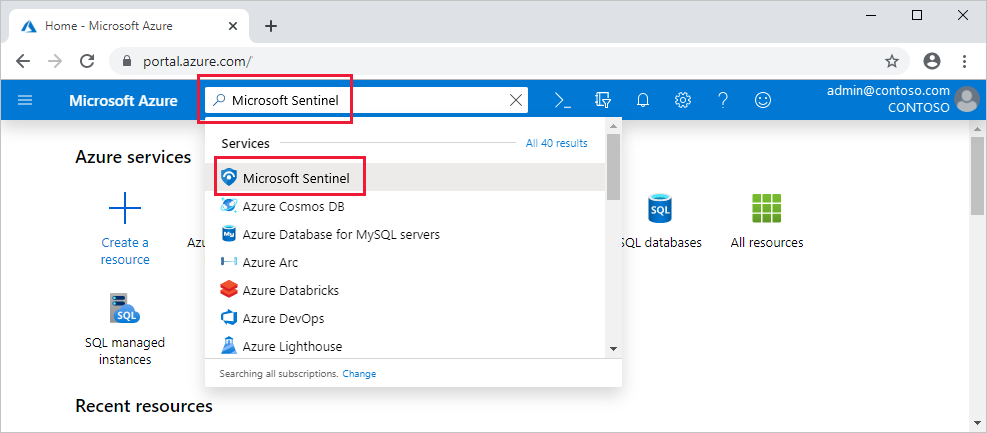
Microsoft Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Defender for Cloud Apps, security alerts from Microsoft Defender for Cloud, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Microsoft Sentinel

In this Lab , we will understand how to create an Azure sentinel workspace and connect with Data source

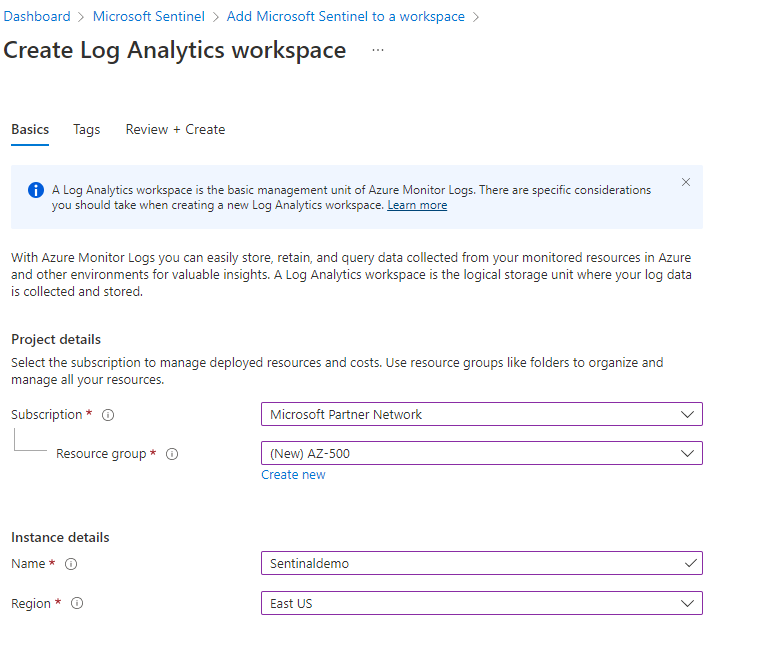
# Lab: Setup Azure Sentinel workspace

## Enable Microsoft Sentinel

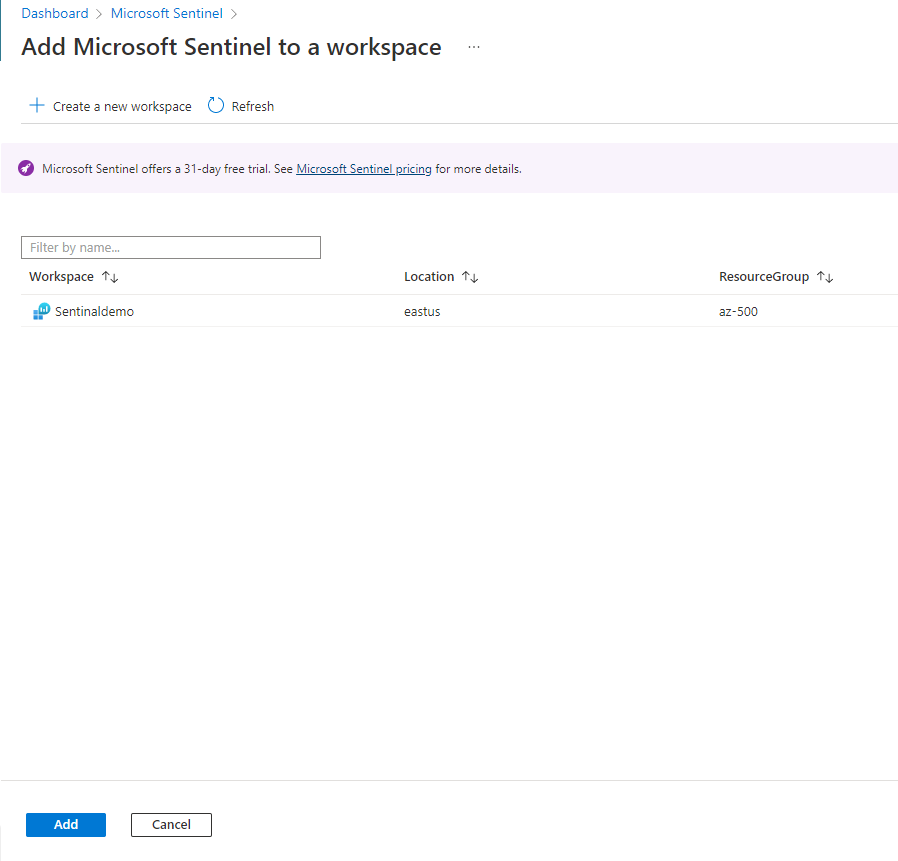
1. Sign in to the Azure portal. Make sure that the subscription in which Microsoft Sentinel is created is selected.
2. Search for and select **Microsoft Sentinel**.



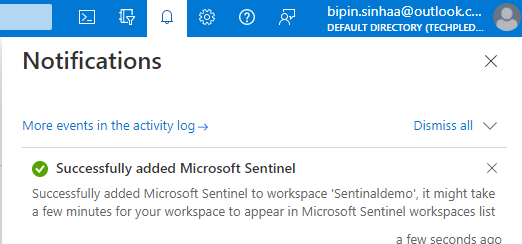
1. Select **Add**.
2. create a new one.



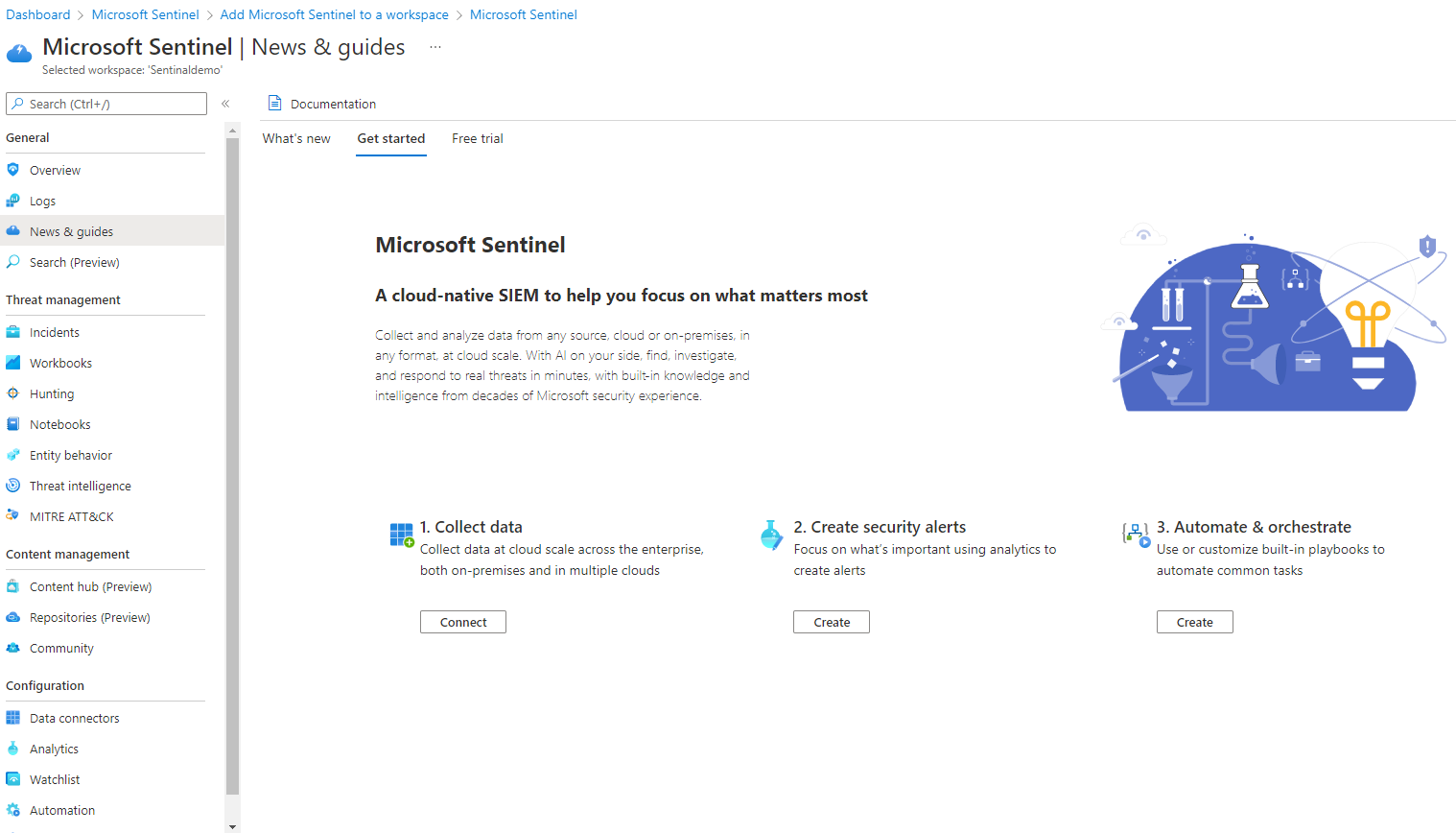
1. Click Review and Create
2. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade,



1. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade



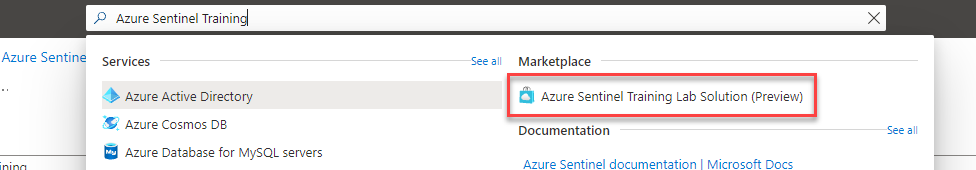
1. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade



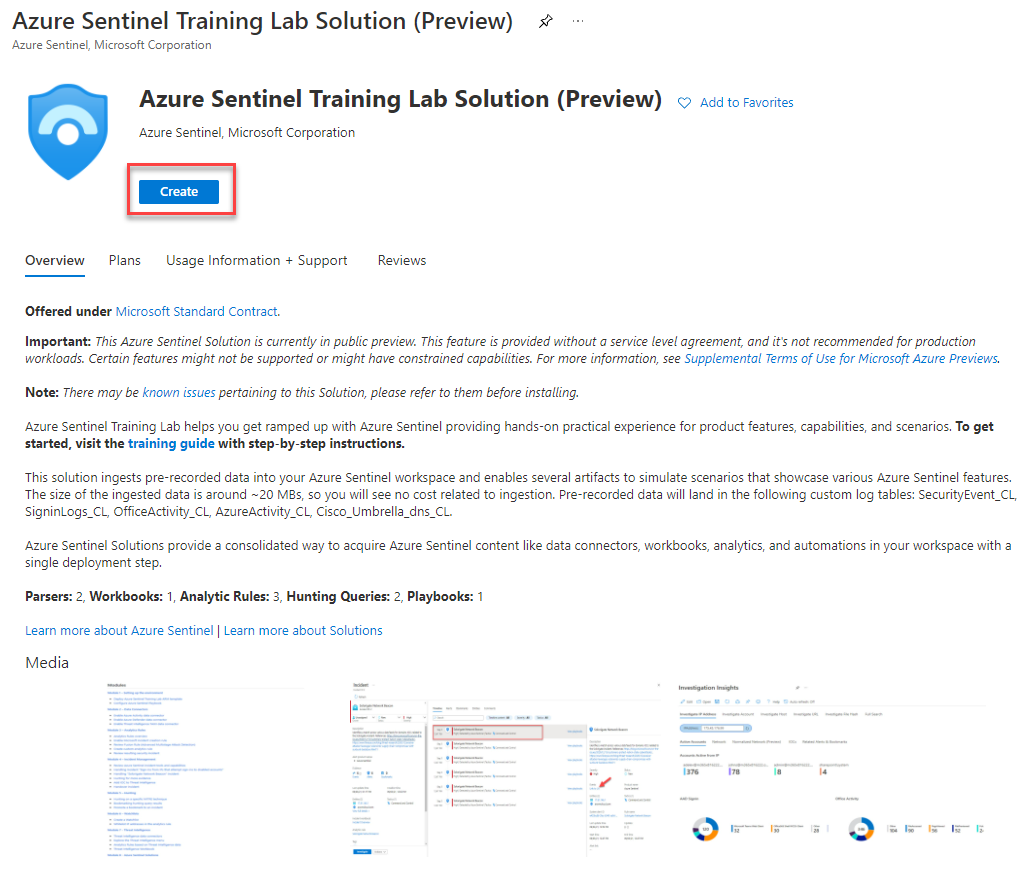
# Exercise 2: Deploy the Microsoft Sentinel Training Lab Solution

In this exercise you will deploy the Training Lab solution into your existing workspace. This will ingest pre-recorded data (~20 MBs) and create several other artifacts that will be used during the exercises.

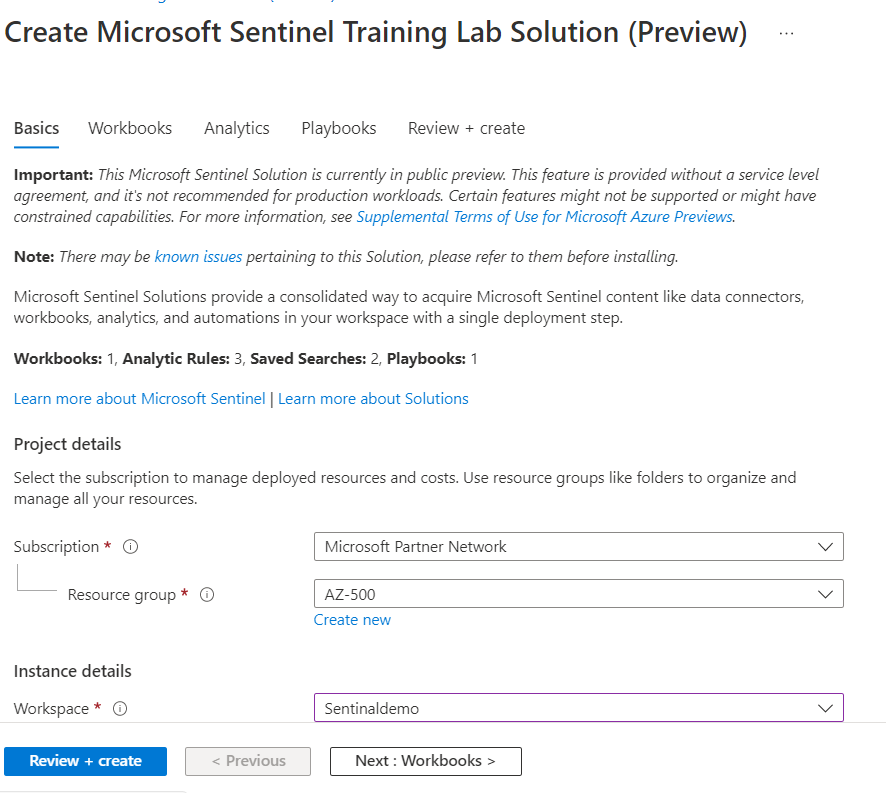
1. In the Azure Portal, go to the top search bar and type *Microsoft Sentinel Training*. Select the **Microsoft Sentinel Training Lab Solution (Preview)** marketplace item on the right.

[](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Training/Azure-Sentinel-Training-Lab/Images/deployment5.png)

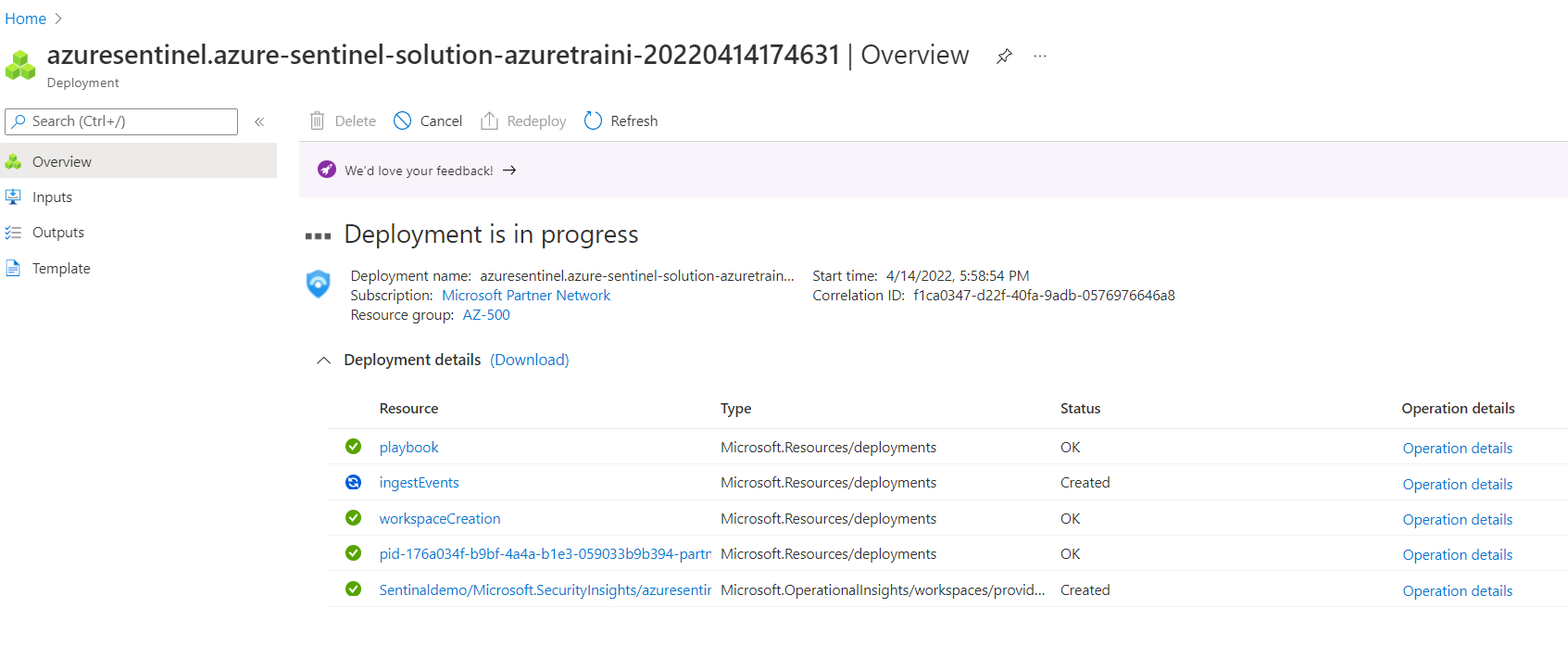
1. Read the solution description and click **Create** at the top.

[](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Training/Azure-Sentinel-Training-Lab/Images/deployment6.png)

1. In the Basics tab, select the Subscription, Resource Group and Workspace that you created in Exercise 1, or the details for your existing workspace. Optionally, review the different tabs (Workbooks, Analytics, Hunting Queries, Watchlists, Playbooks) in the solution. When ready, click on **Review + create**.

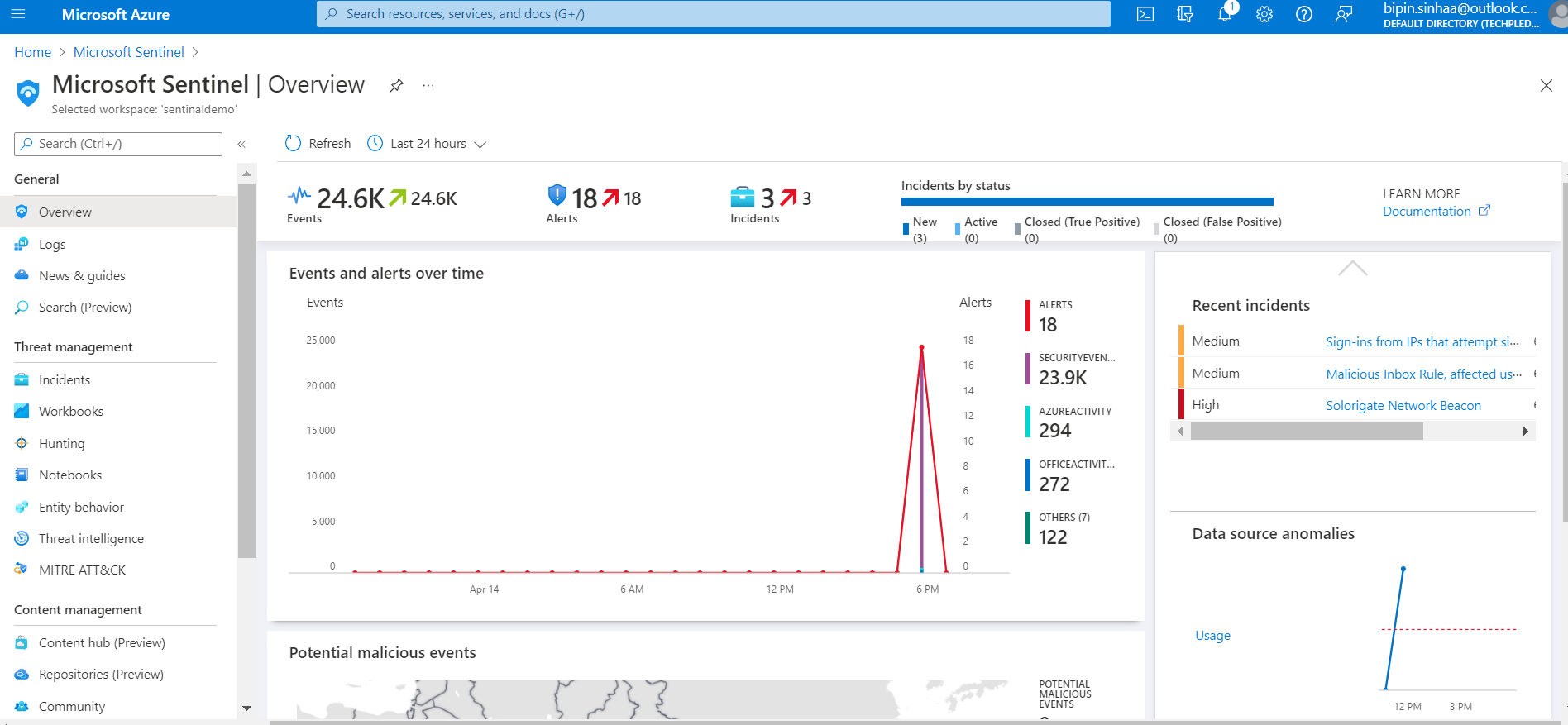


1. Once validation is ok, click on **Create**. The deployment process takes **about 15 minutes**, this is because we want to make sure that all the ingested data is ready for you to use once finished.



1. Once the deployment finishes, you can go back to Microsoft Sentinel and select your workspace. In the home page you should see some ingested data and several recent incidents.

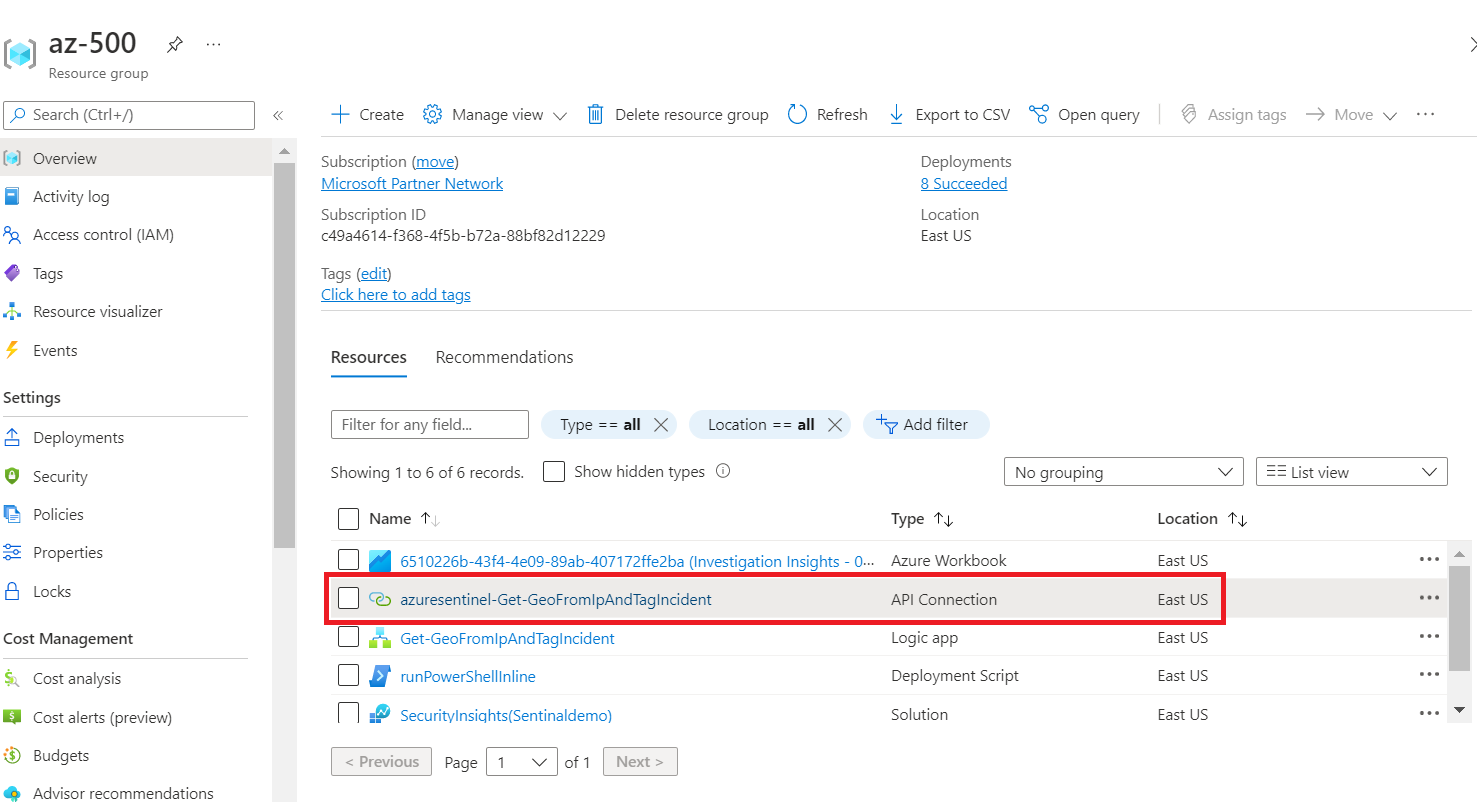
*Don't worry if you don't see 3 incidents like in the screenshot below, they might take a few minutes to be raised.*



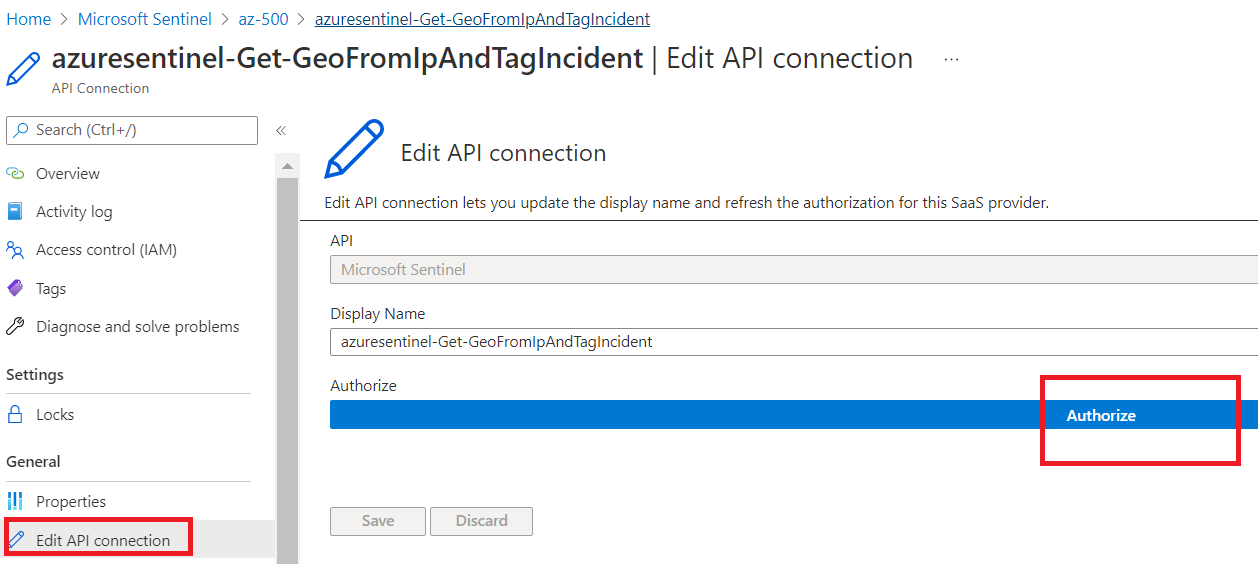
# Exercise 3: Configure Microsoft Sentinel Playbook

In this exercise, we will configure a Playbook that will be later used in the lab. This will allow the playbook to access Sentinel.

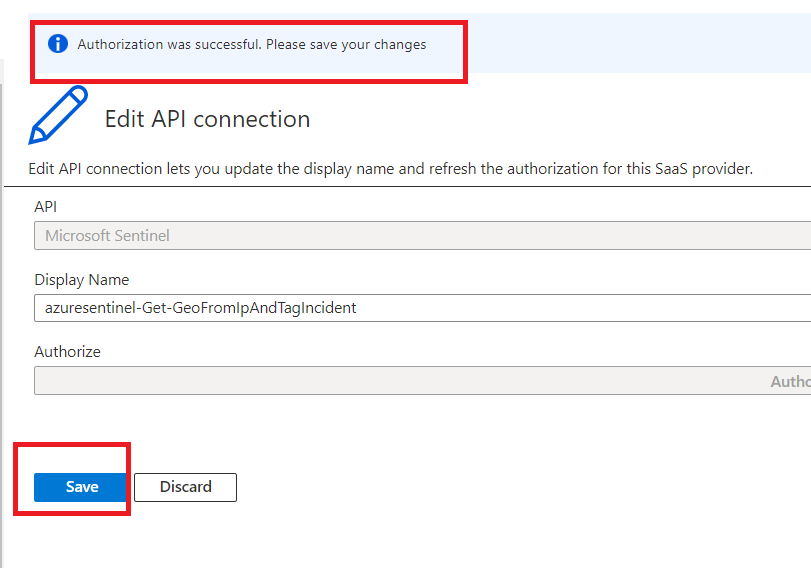
1. Navigate to the resource group where the lab has been deployed.
2. In the resource group you should see an API Connection resource called **azuresentinel-Get-GeoFromIpAndTagIncident**, click on it.



1. Click on Edi **API connection** under **General**.

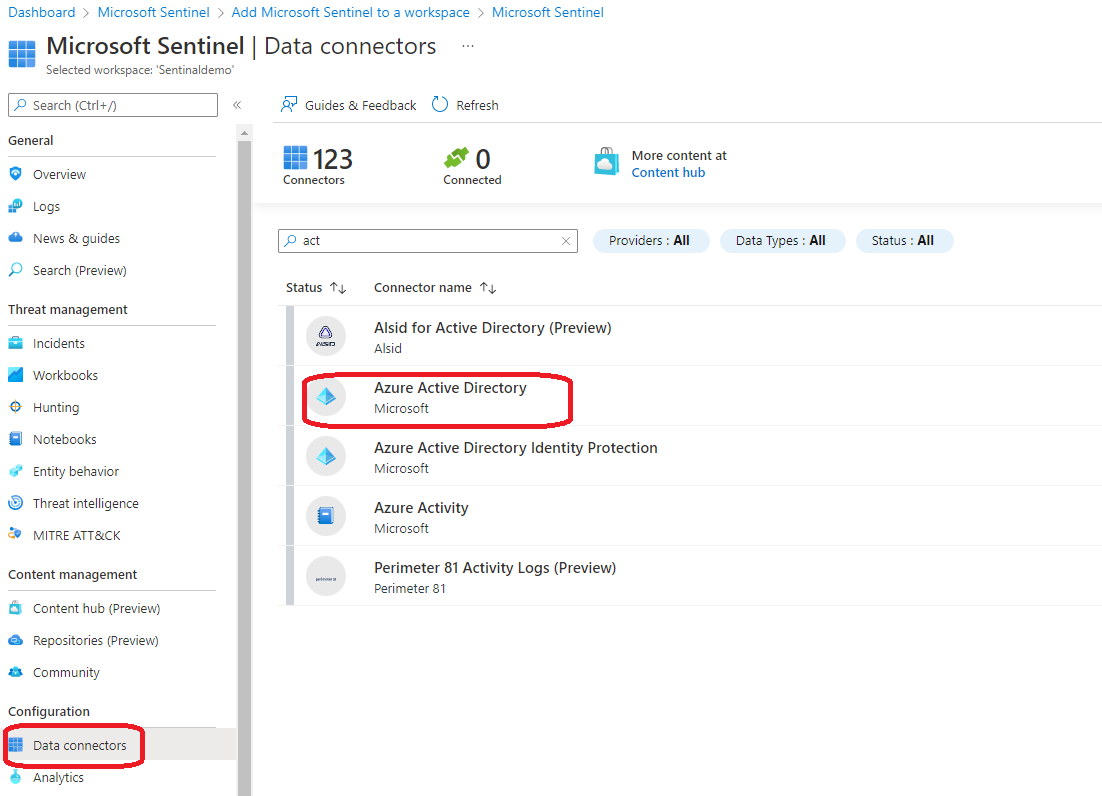


1. Click on **Authorize** and a new window will open to chose an account. Pick the user that you want to authenticate with. This should normally be the same user that you're logged in with.
2. Click **Save**.

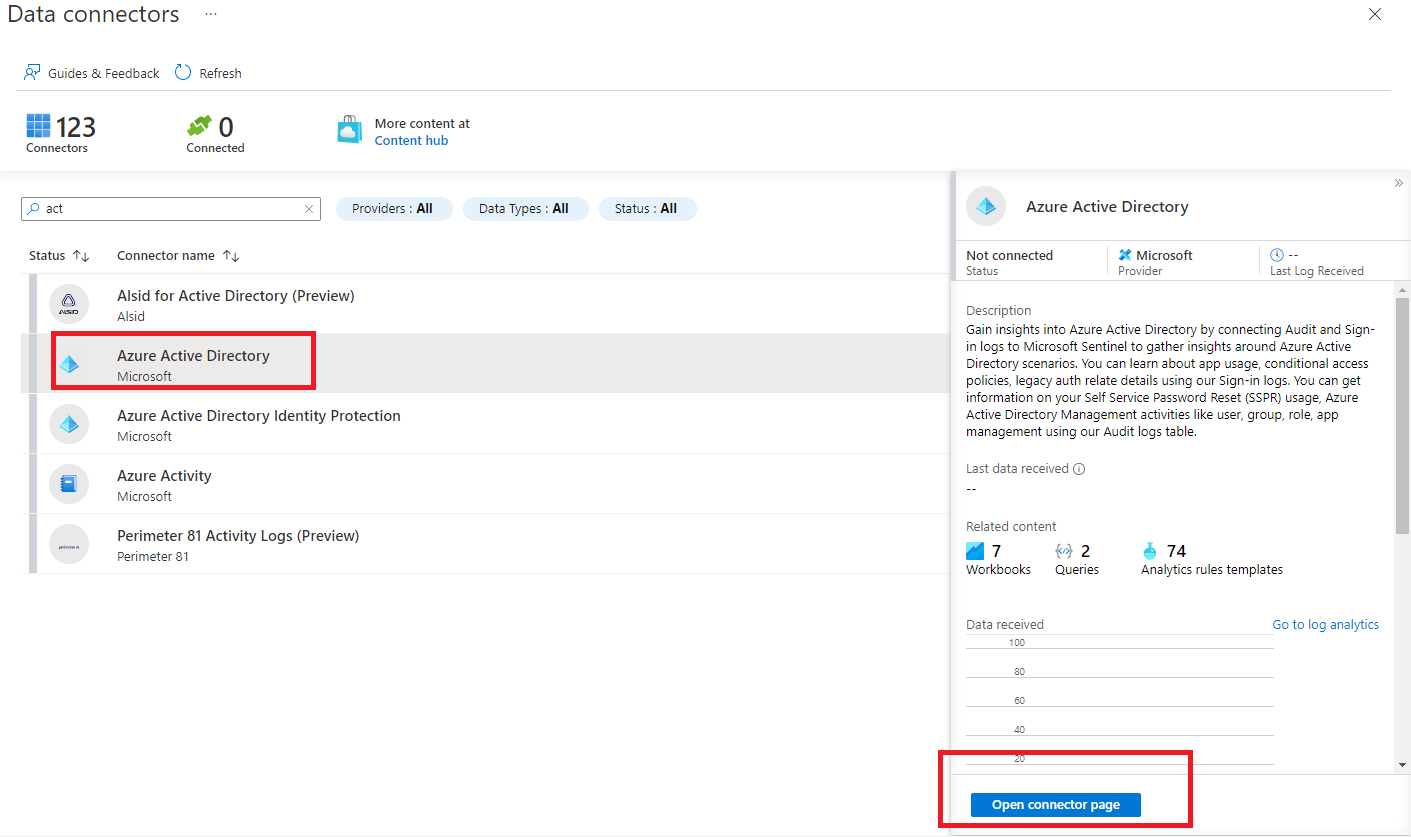


# Connect to Active Directory

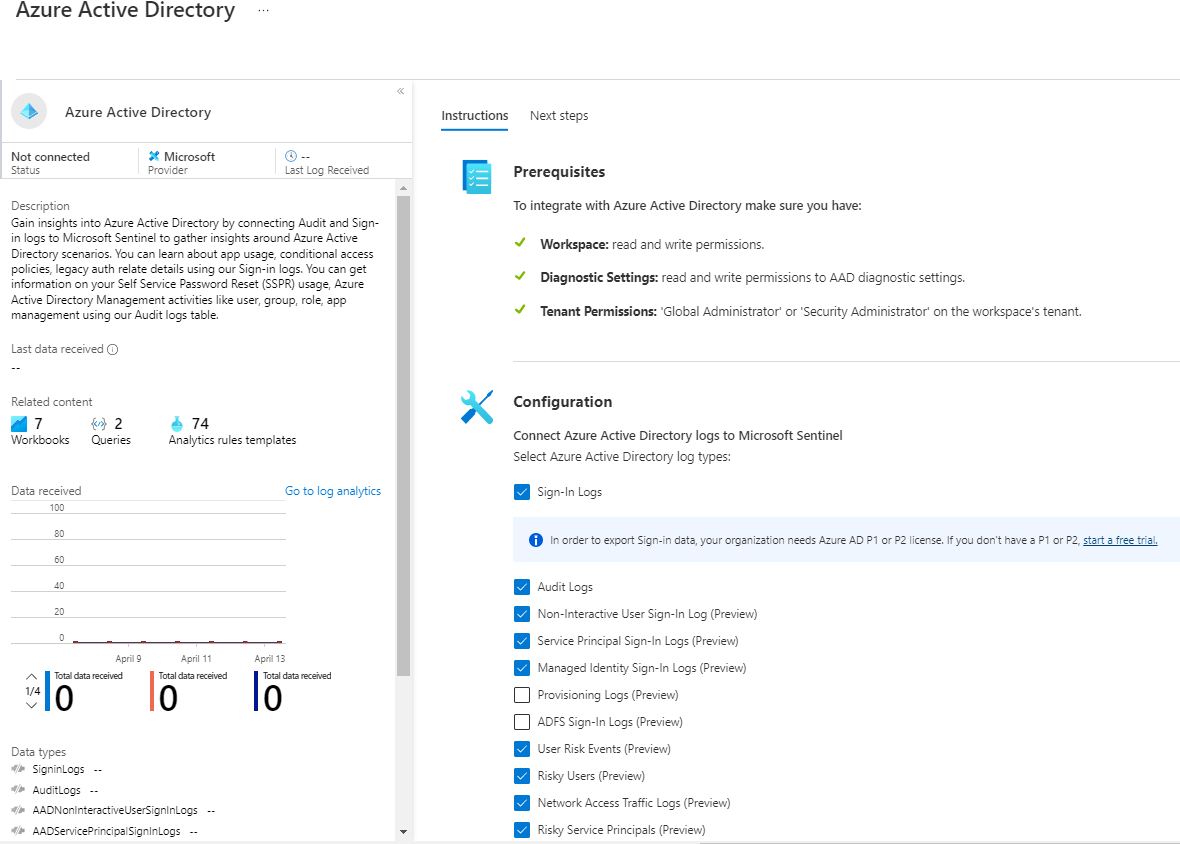
1. In Microsoft Sentinel, select **Data connectors** from the navigation menu.
2. From the data connectors gallery, select **Azure Active Directory**



1. Then select **Open connector page**.



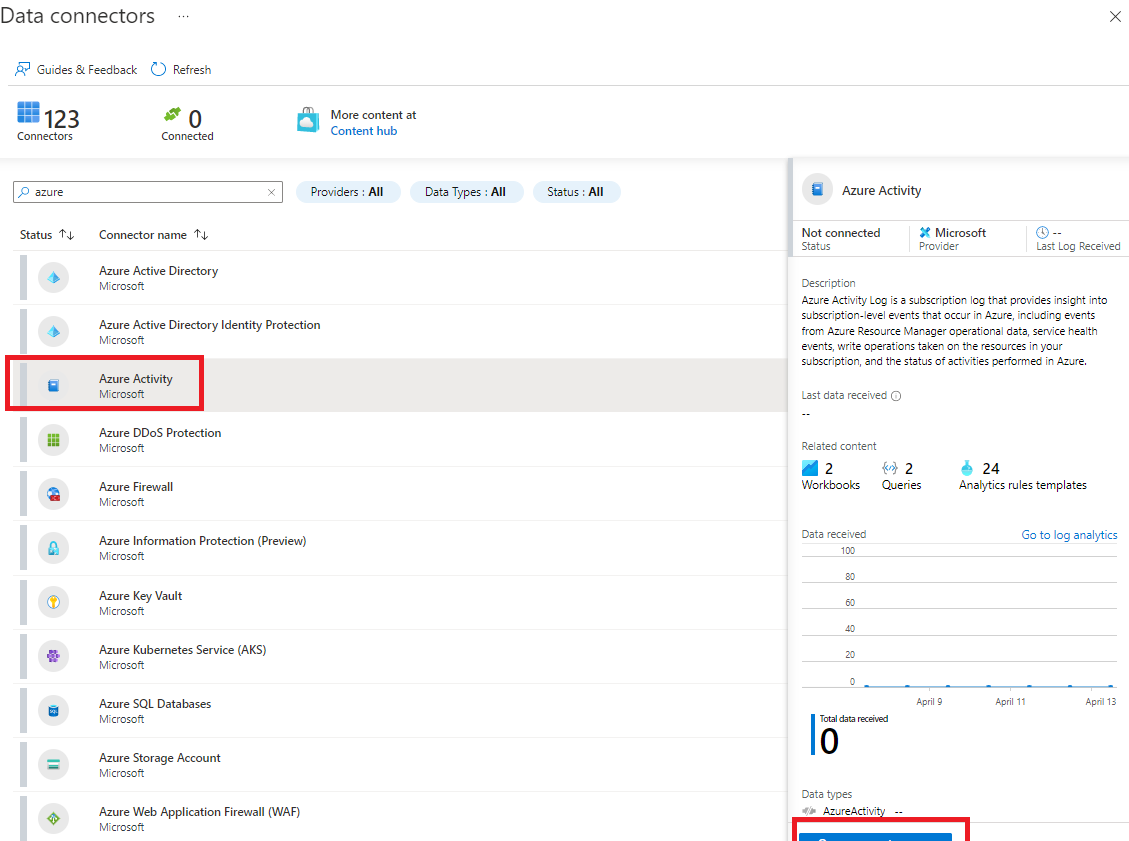
1. Mark the check boxes next to the log types you want to stream into Microsoft Sentinel (see below), and select **Connect**.



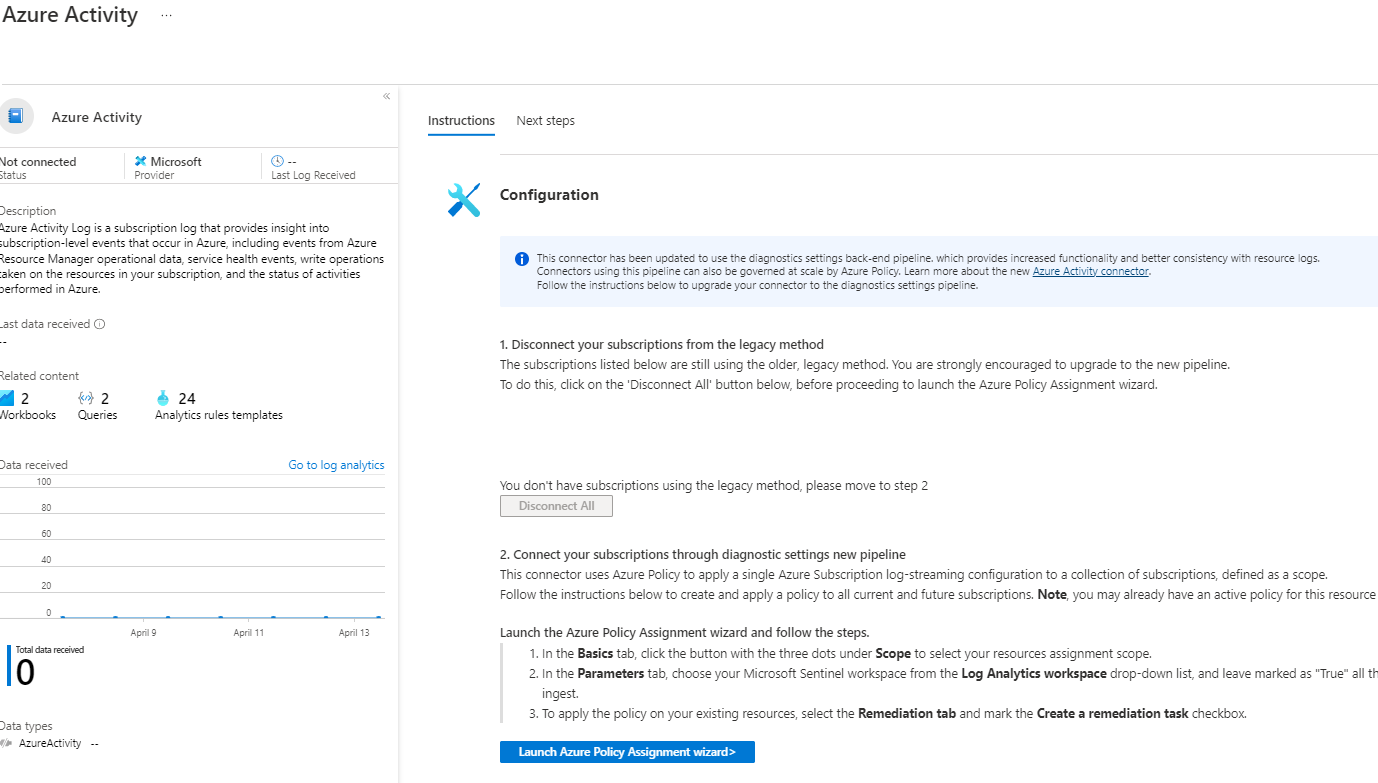
1. Mark the check boxes next to the log types you want to stream into Microsoft Sentinel (see below), and select **Apply Changes**

# Connect to Azure Activity

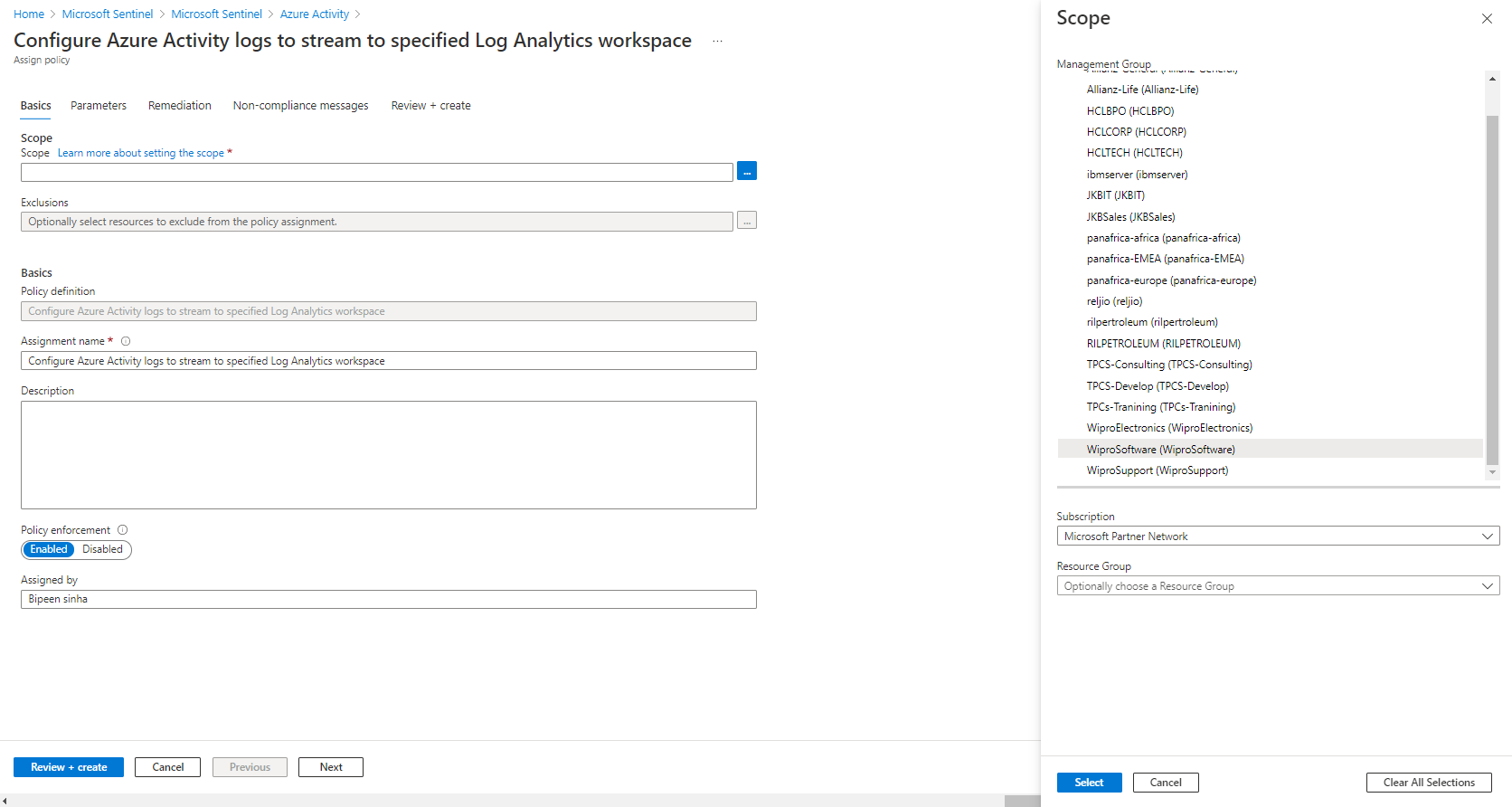
1. On the **Microsoft Sentinel | Data connectors** blade, review the list of available connectors, type **Azure** into the search bar and select the entry representing the **Azure Activity** connector

.

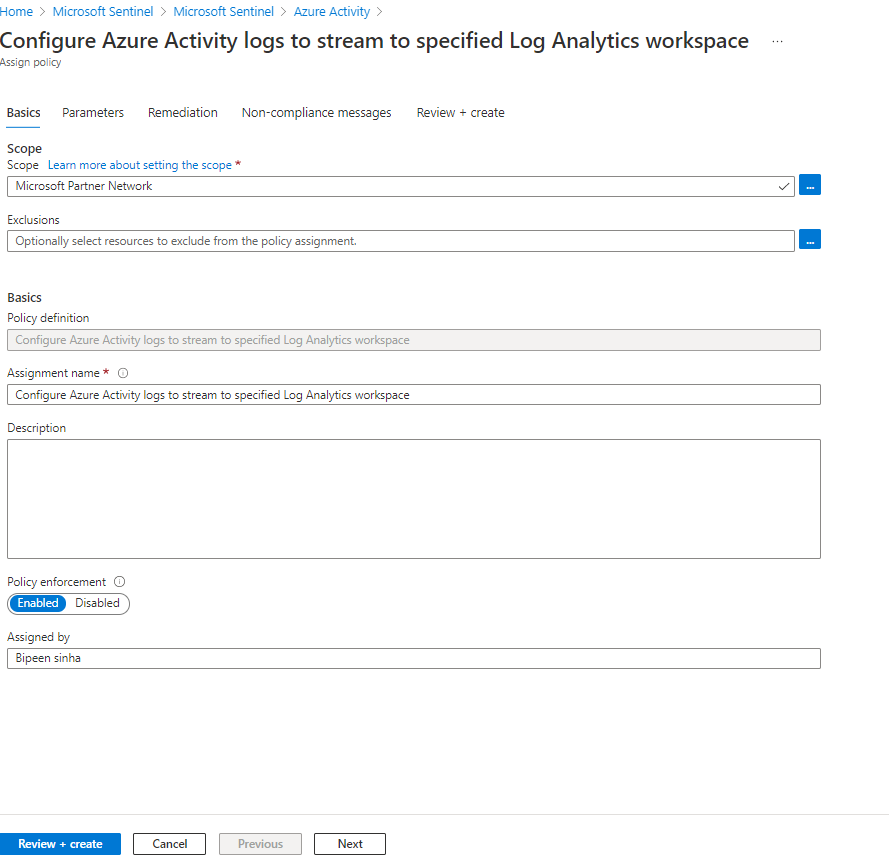
1. Then select **Open connector page**.
2. On the **Azure Activity** blade the **Instructions** tab should be selected, note the **Prerequisites** and scroll down to the **Configuration**. Take note of the information describing the connector update. Your Azure Pass subscription never used the legacy connection method so you can skip step 1 (the **Disconnect All** button will be grayed out) and proceed to step 2.
3. In step 2 **Connect your subscriptions through diagnostic settings new pipeline**, review the "Launch the Azure Policy Assignment wizard and follow the steps" instructions then click **Launch the Azure Policy Assignment wizard>**.



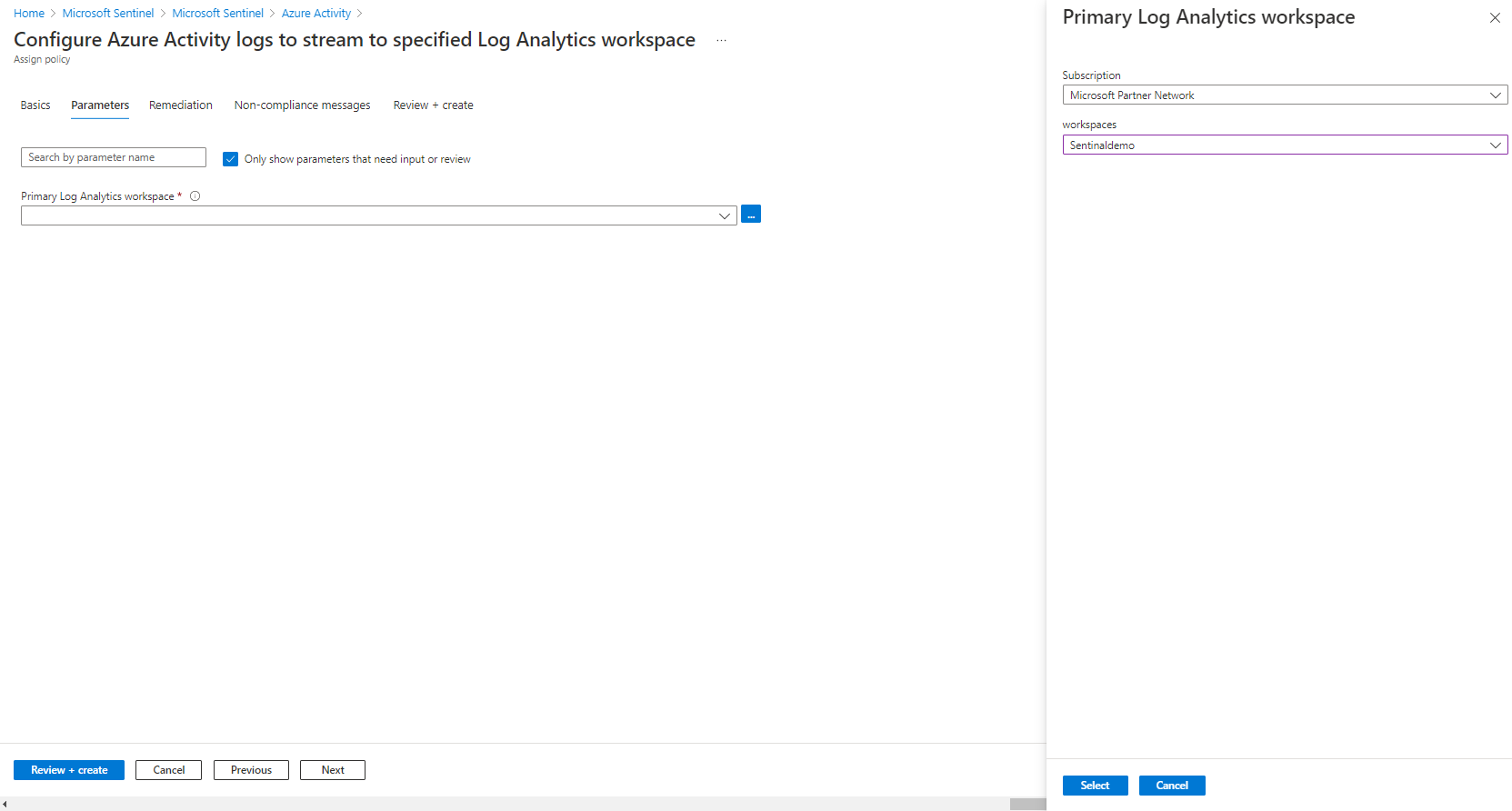
1. On the **Configure Azure Activity logs to stream to specified Log Analytics workspace** (Assign Policy page) **Basics** tab, click the **Scope elipsis (...)** button. In the **Scope** page choose your Azure Pass subscription from the drop-down subscription list and click the **Select** button at the bottom of the page.



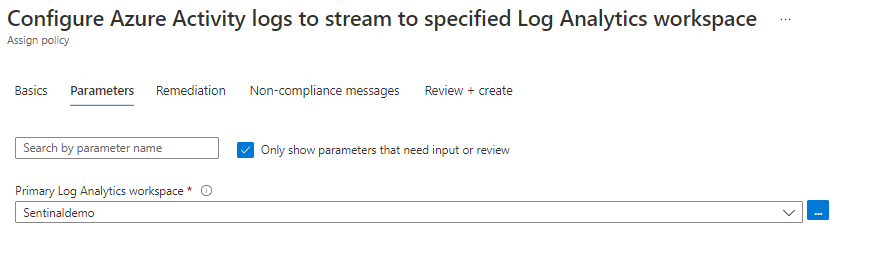
1. Click Next



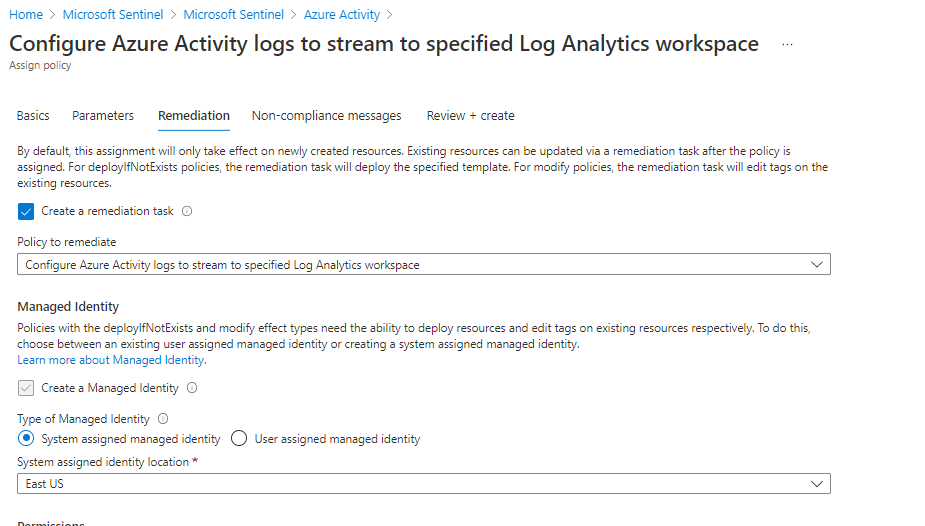
1. Click Next
2. Click the **Next** button at the bottom of the **Basics** tab to proceed to the **Parameters** tab. On the **Parameters** tab click the **Primary Log Analytics workspace elipsis (...)** button. In the **Primary Log Analytics workspace** page, make sure your Azure pass subscription is selected and use the **workspaces** drop-down to select the Log Analytics workspace you are using for Sentinel.



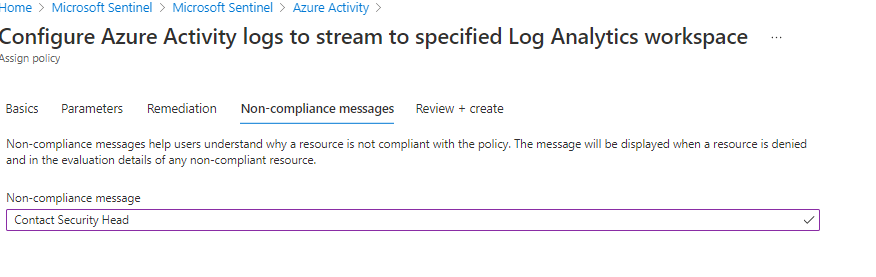
1. When done click the **Select** button at the bottom of the page and click **Next**



1. Click the **Next** button at the bottom of the **Parameters** tab to proceed to the **Remediation** tab. On the **Remediation** tab select the **Create a remediation task** checkbox. This will enable the "Configure Azure Activity logs to stream to specified Log Analytics workspace" in the **Policy to remediate** drop-down. In the **System assigned identity location** drop-down, select the region (East US for example) you selected earlier for your Log Analytics workspace.

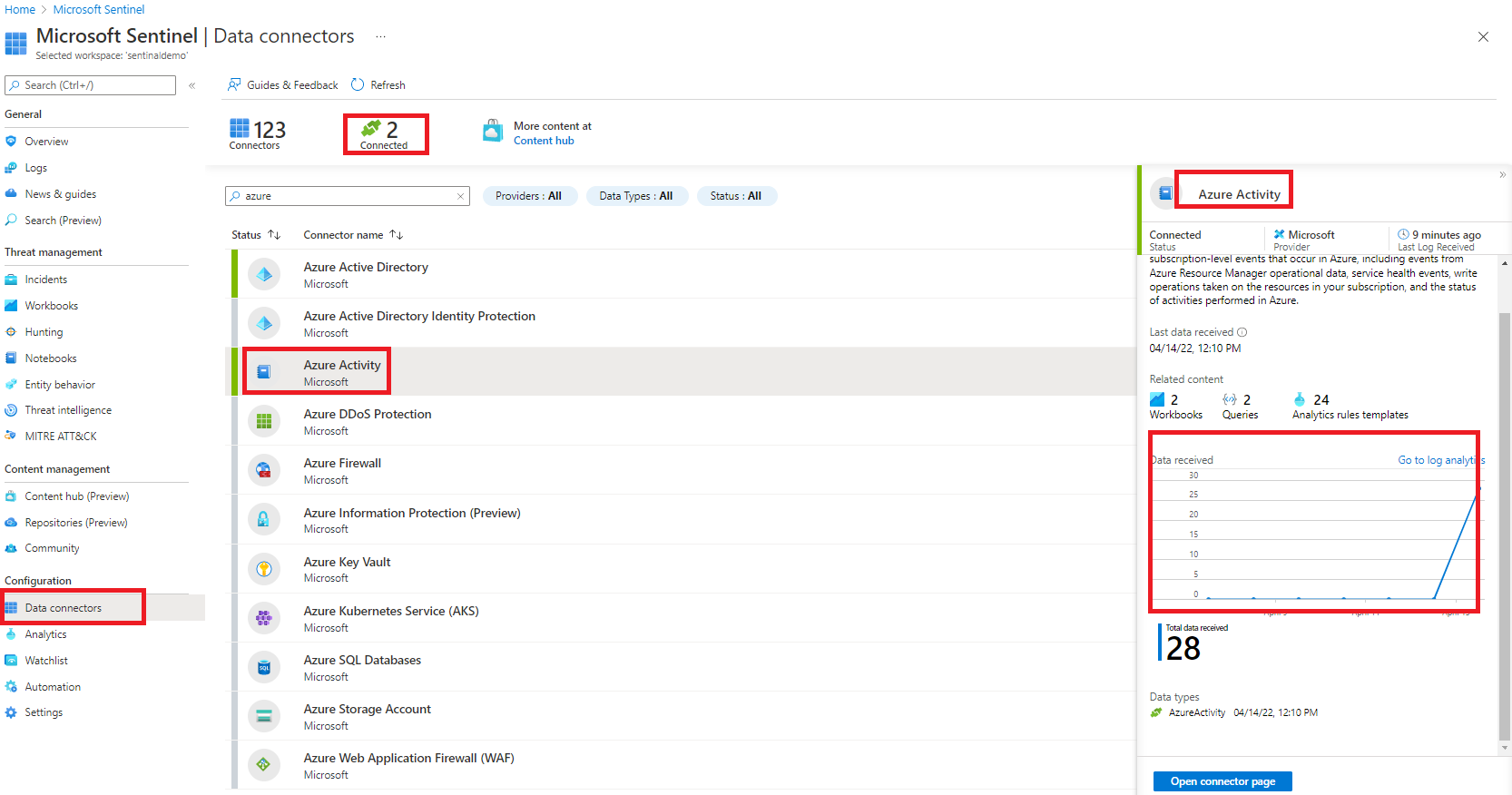
c

1. Click the **Next** button at the bottom of the **Remediation** tab to proceed to the **Non-compliance message** tab. Enter a Non-compliance message if you wish (this is optional) and click the **Review + Create** button at the bottom of the **Non-compliance message** tab.



1. Click the **Create** button. You should observe three succeeded status messages: **Creating policy assignment succeeded, Role Assignments creation succeeded, and Remediation task creation succeeded**.
2. Verify that the **Azure Activity** pane displays the **Data received** graph (you might have to refresh the browser page).

**Note**: It may take over 15 minutes before the Status shows "Connected" and the graph displays Data received.

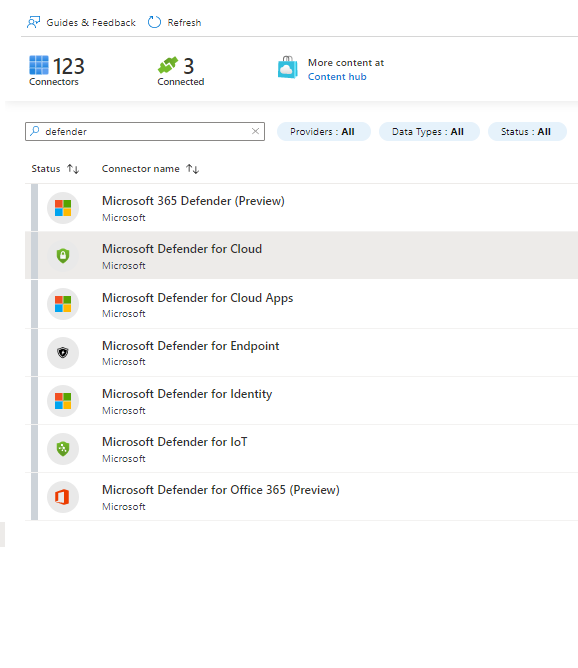


# Enable Microsoft Defender for Cloud data connector

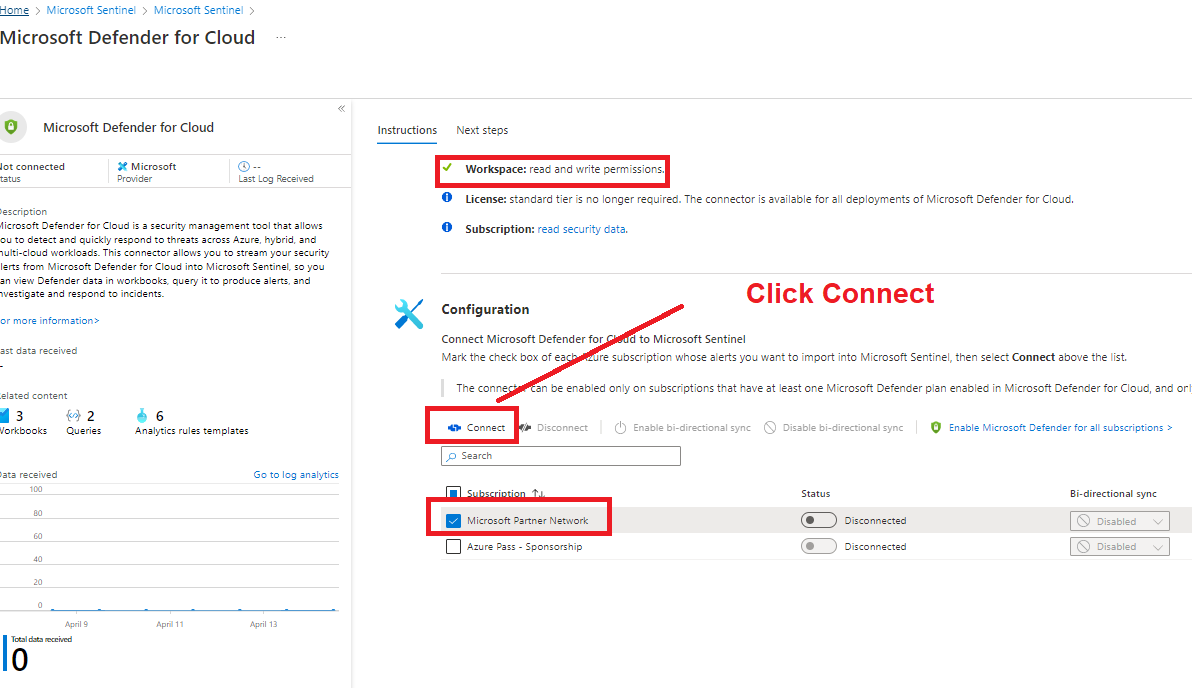
This exercise shows you how to enable the Microsoft Defender for Cloud data connector. This connector allows you to stream your security alerts from Microsoft Defender for Cloud into Microsoft Sentinel, so you can view Defender data in workbooks, query it to produce alerts, and investigate and respond to incidents.

**NOTE**: To do this exercise, your user must have the Security Reader role in the subscription of the logs you stream. If not done already, you will need to enable any of the Defender plans in Microsoft Defender for Cloud.

1. Go to you Microsoft Sentinel workspace and select **Data Connectors** under Configuration section.
2. In the data connectors screen, type defender in the search bar, select the **Microsoft Defender for Cloud** connector and click on Open connector page.



1. In the Microsoft Defender for Cloud connector page, check that your permissions are enough at the top. If you don't have the required permissions, you can continue to the next exercise.
2. From the list of subscriptions at the bottom of the page, select the desired **subscription** and click on **Connect.** Wait for the operation to complete.



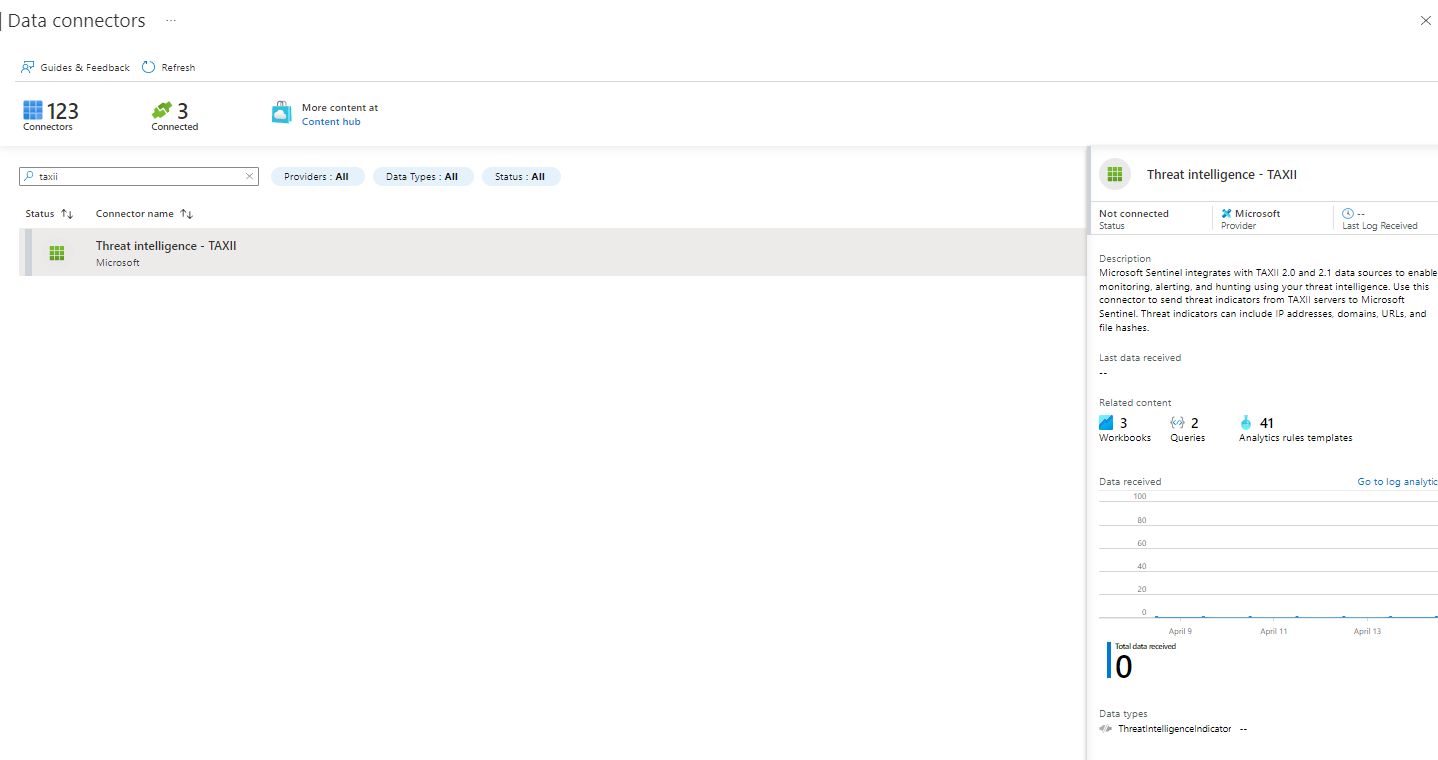
1. Click on Next Steps at the top of the page and explore what content is available for this connector.

# Enable Threat Intelligence TAXII data connector

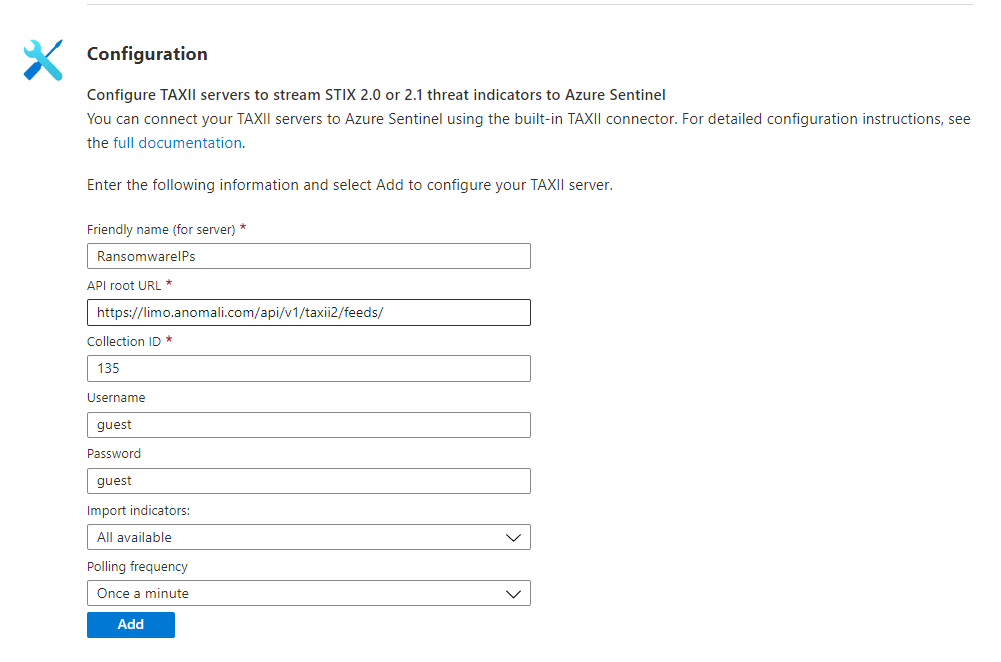
This exercise shows you how to enable the Threat Intelligence - TAXII data connector. This connector allows you to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

**NOTE**: To do this exercise, your user must have the Security Reader role in the subscription of the logs you stream. If not done already, you will need to enable Azure Defender within Azure Security Center.

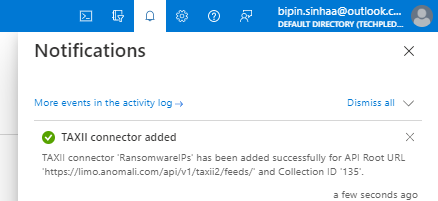
1. Go to you Microsoft Sentinel workspace and select Data Connectors under Configuration section.
2. In the data connectors screen, type taxii in the search bar, select the **Threat intelligence - TAXII** connector and click on **Open connector page.**



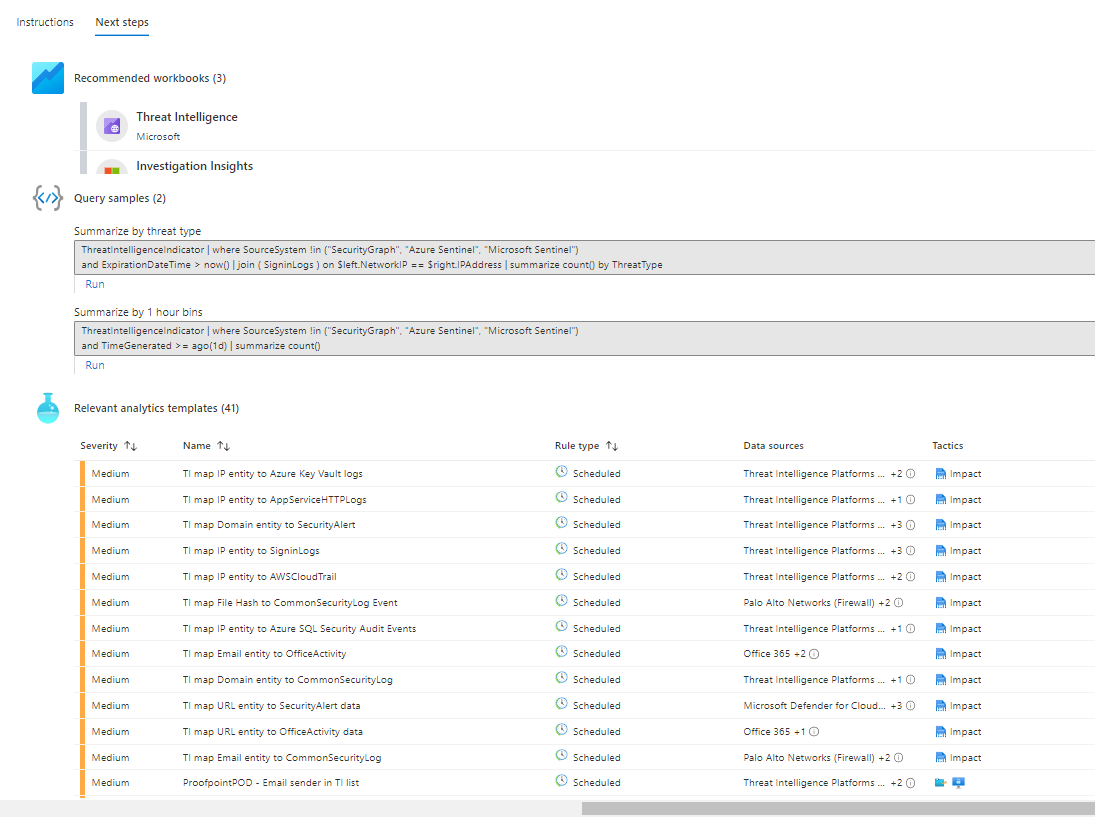
1. In the Threat Intelligence - TAXII connector page, add the following information under Configuration menu:
   * **Friendly name (for server)**: RansomwareIPs
   * **API root URL**: <https://limo.anomali.com/api/v1/taxii2/feeds/>
   * **Collection ID**: 135
   * **Username**: guest
   * **Password**: guest
   * **Import Indicators**: All available (review all available options)
   * **Polling frequency**: Once an minute (review all available options)

[](https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Training/Azure-Sentinel-Training-Lab/Images/taxii11.png)

1. Click **Add** and wait until the operation completes.



1. Click on Next Steps at the top of the page and explore what content is available for this connector. In a few seconds, the ThreatIntelligenceIndicator will be populated with IOCs from Anomali's feed

.