Team Cymru Scout for Microsoft Sentinel Installation, Usage and Troubleshooting User Guide

www.cymru.com
901 International Parkway, Suite 350, Lake Mary, FL 32746, USA

Contents

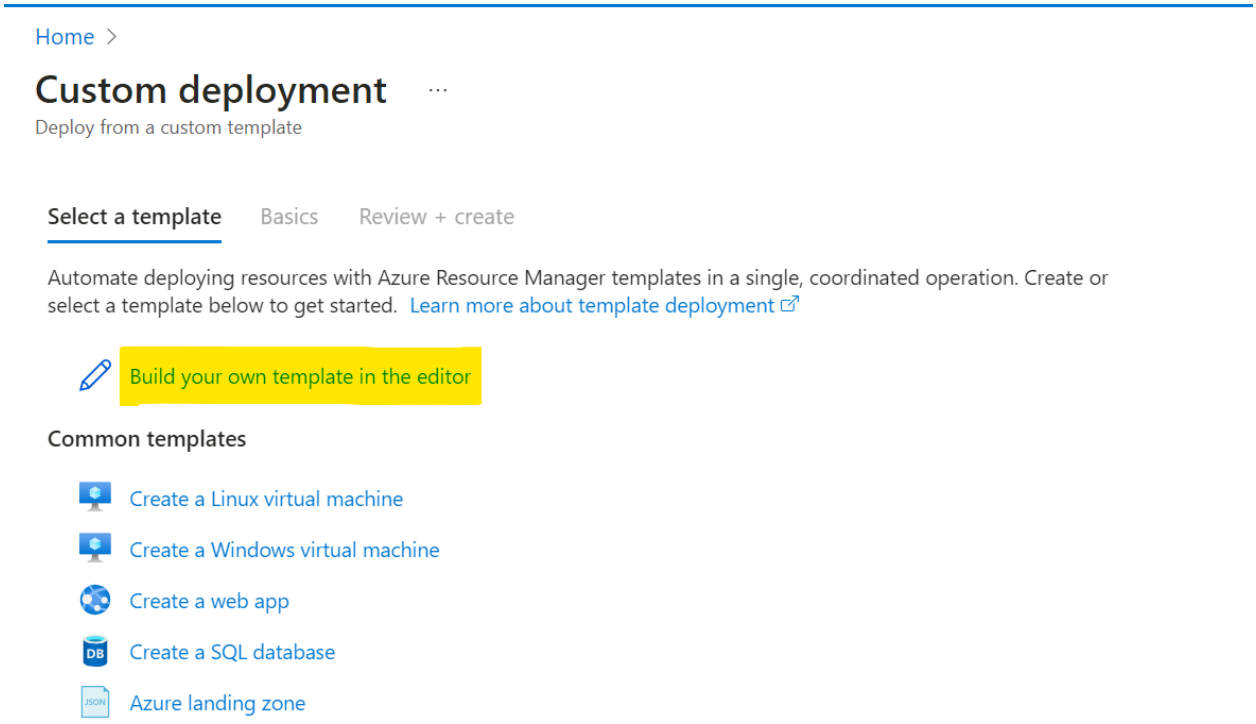
Prerequisites

The following requirements are essential for configuring all components:

- Azure Account with subscription
- Resource Group
    - This requires **Microsoft Sentinel Contributor Role** at **Subscription Level**
- Microsoft EntraID Application
    - The Azure account user must have an **Application Developer or Application Owner** role at subscription level to create Microsoft EntraID Application
- Log Analytics Workspace (Reference Link)
- Microsoft Sentinel Workspace (Reference Link)

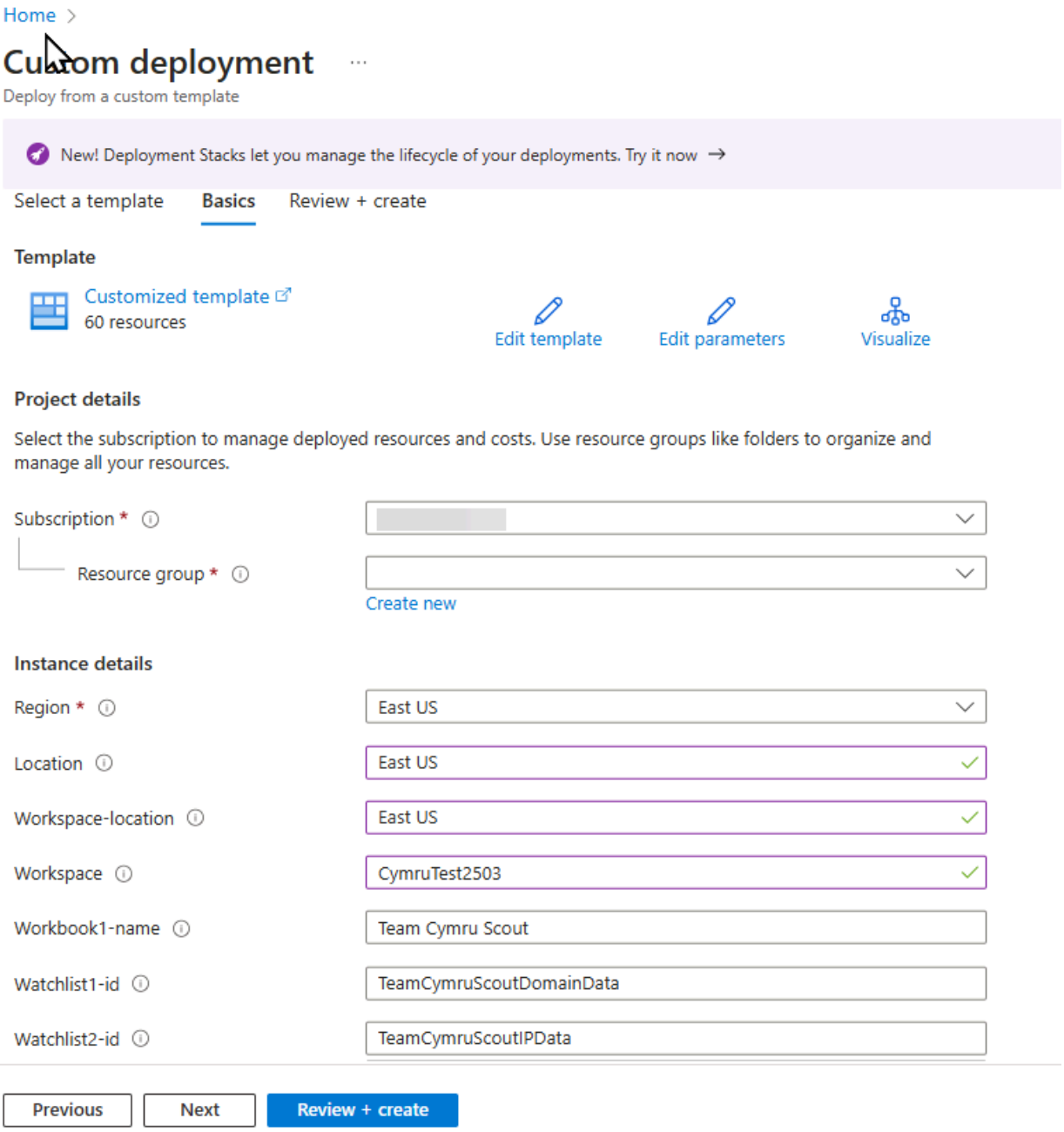
Steps to Install the Team Cymru Scout MS Sentinel Integration

1. Log in to the **Azure Portal** using this link: Azure Sentinel. Search for **"Deploy a custom template"** and select **"Build your own template in the editor"** option.

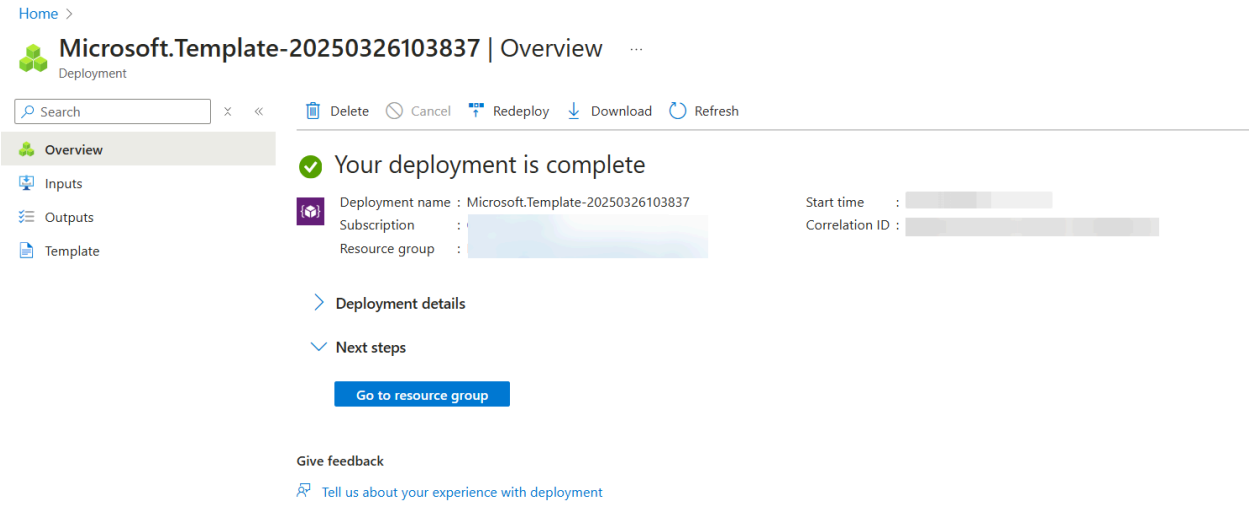


2. Click **"Load File"**, select the **mainTemplate.json** file, and then click the **"Save"** button.

3. Enter the required details, including **Resource Group**, **Workspace Location** (same as the region), and the **Log Analytics Workspace** name where you want to deploy the integration. Click **"Review + Create"**, then select **"Create"**.



4. This will start the deployment process. Once completed, you will receive a confirmation message.



Steps to Install the Team Cymru Scout Data Connector

Usage

The **Team Cymru Scout Data Connector** ingests **three types of data** via **three functions**:

1. **IPDataCollector**
2. **DomainDataCollector**
3. **AccountUsageDataCollector**

IP and Domain Data Input:

- Requires users to provide an **input list of IPs and Domains** in **two ways**:
  - **Data Connector Configuration Parameter** (IP Values and Domain Values)
  - **Watchlists** (for large IP and Domain lists)
- If inputs are provided **in both places**, **both will be considered**.

Functionality:

- Based on the provided **input**, the **Function App** will **fetch data periodically** for the specified **IPs and Domains** from Scout API.
- The **AccountUsageDataCollector** function provides data of account usage stats for your account periodically.
- The collected data will then be **ingested into the MS Sentinel Table**.

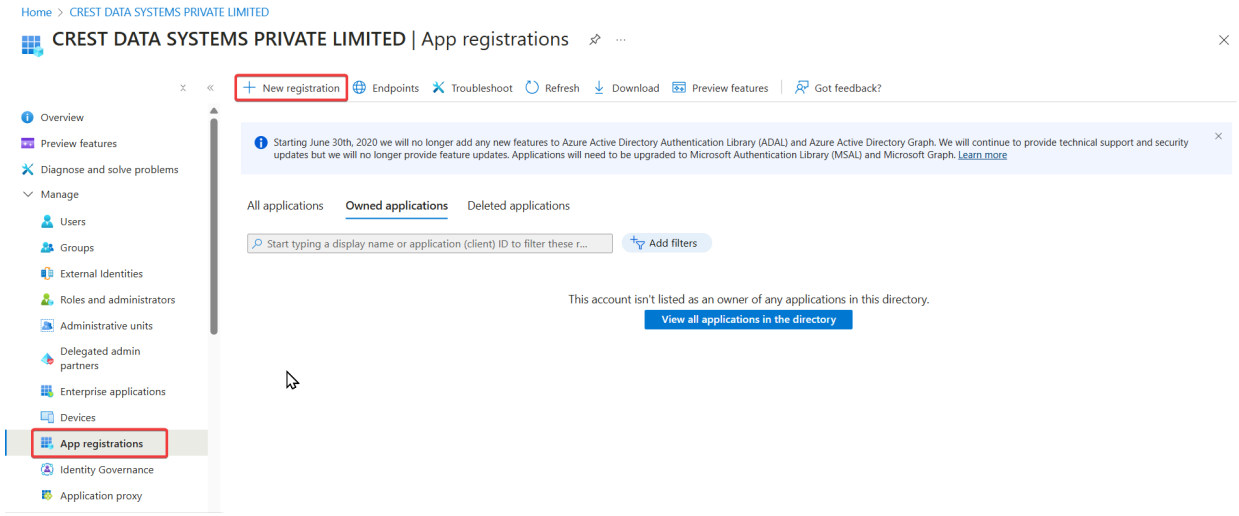
Prerequisites

App Registration steps for the Application in Microsoft Entra ID

This integration requires an **App Registration** in the **Azure Portal**. Follow the steps below to create a new application in **Microsoft Entra ID**:
Note: If you already have an application and have the **Client ID** and **Client Secret** ready, you can skip the steps below. Redirect

- **Sign in** to the **Azure Portal**.
- Search for and select **Microsoft Entra ID**.

- Under Manage, select **App registrations**
- Click on **New Registration**



- Enter a **Display Name** for your application.
- Click **Register** to complete the initial app registration.
- Once the registration is complete, the **Azure Portal** will display the **App Registration Overview** pane. Here, you will find the **Application (Client) ID** and **Tenant ID**, which are required as configuration parameters for the **Team Cymru Scout MS Sentinel Data Connector**.

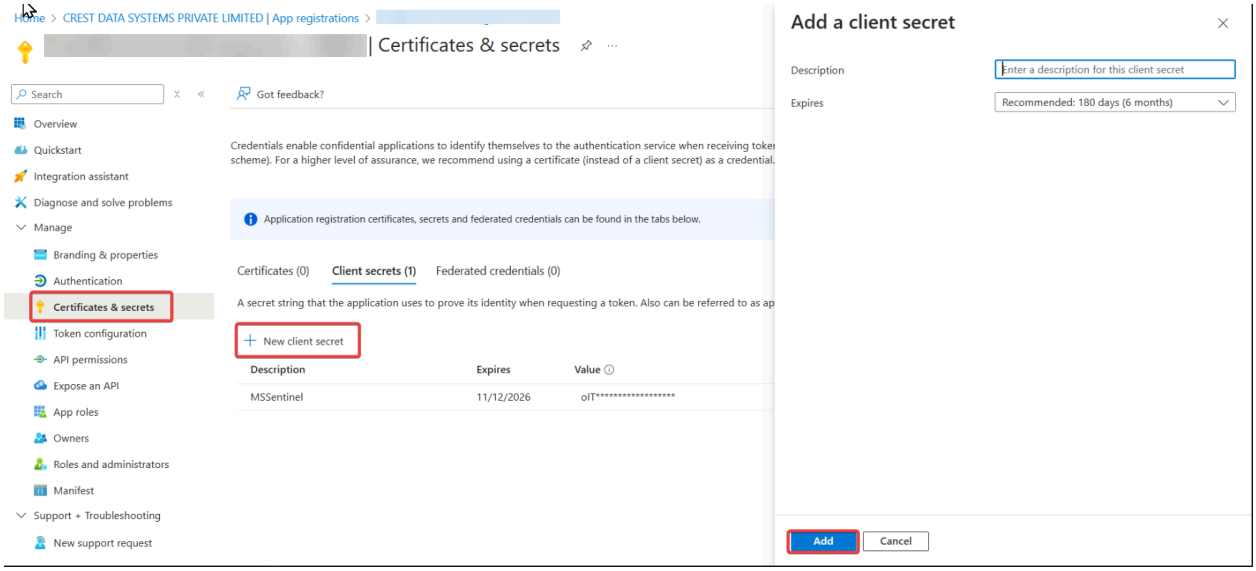
Reference link:
https://learn.microsoft.com/azure/active-directory/develop/quickstart-register-app

Add a client secret for application in Microsoft Entra ID

To create a new **Client Secret** (also known as an **application password**) for the **Team Cymru Scout MS Sentinel Data Connector**, follow these steps:

- **Sign in** to the **Azure Portal**.
- Navigate to **App registrations** and select your application.
- Go to **Certificates & secrets** > **Client secrets** > **New client secret**.
- Enter a **description** for your client secret.
- Choose an **expiration period** or specify a **custom lifetime** (maximum limit is **24 months**).

- Click **Add** to generate the client secret.



- Make sure to **record the client secret's value**, as it will not be displayed again once you leave this page.
- The **client secret value** is a required configuration parameter for the **Team Cymru Scout MS Sentinel Data Connector**.

Reference link:
https://learn.microsoft.com/azure/active-directory/develop/quickstart-register-app#add-a-client-secret

Assign role of Microsoft Sentinel Contributor to application in Microsoft Entra ID

Follow the steps in this section to assign the role:

- In the Azure portal, Go to Resource Group and select your resource group.
- In the left menu, click on **Access control (IAM)**.
- Click on **Add**, then choose **Add role assignment**.
- Select Microsoft Sentinel Contributor as the role and click on next.

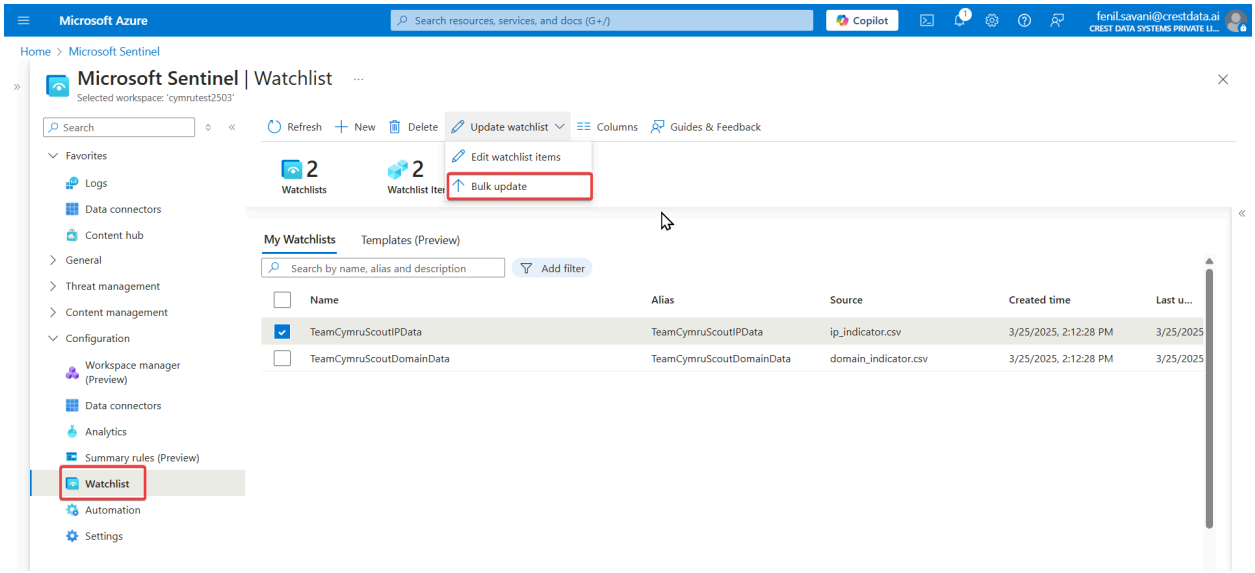
- In Assign access to, select User, group, or service principal.
- Click on **Add members**, type the name of the application you created, and select it. Now click on Review + assign and then again click on Review + assign.

Reference link:
https://learn.microsoft.com/azure/role-based-access-control/role-assignments-portal

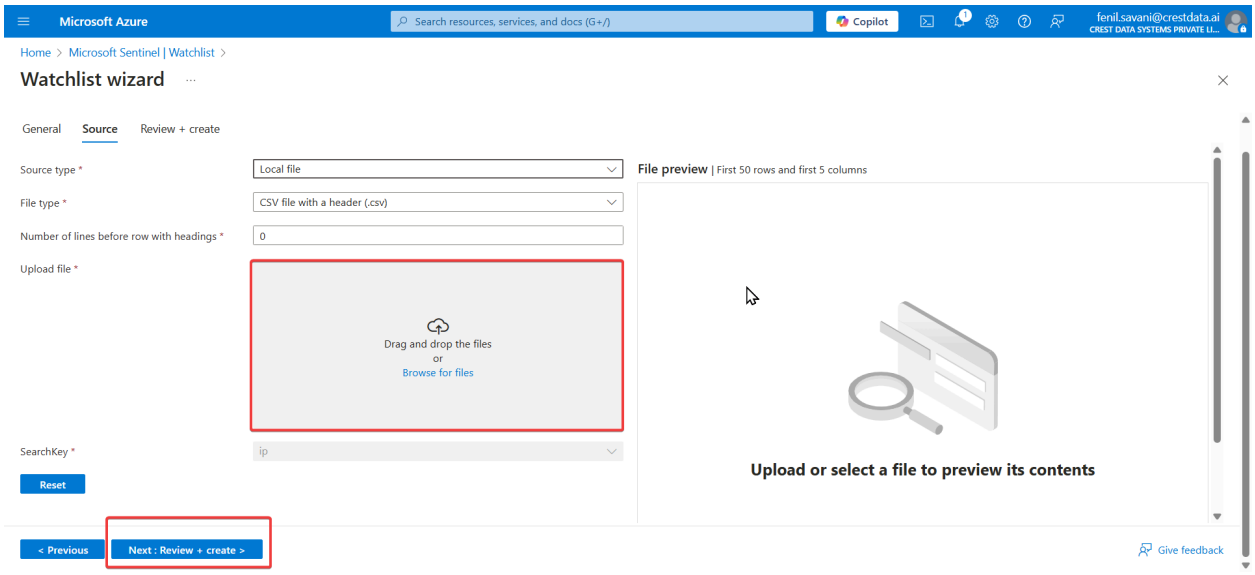
Upload Indicators csv in Watchlists to get data related to ip/domain from Team Cymru Scout

Follow the steps in this section to upload csv containing indicators in watchlist:

- In the Azure portal, Go to **Microsoft Sentinel** and select your workspace.
- Go to **Watchlist** under the Configuration section from the left panel.
- Click on **TeamCymruScoutDomainData**, and then select **Bulk update** from **Update watchlist**



- Upload your csv files with domain indicators in **Upload file** input and click on **Next: Review+Create**



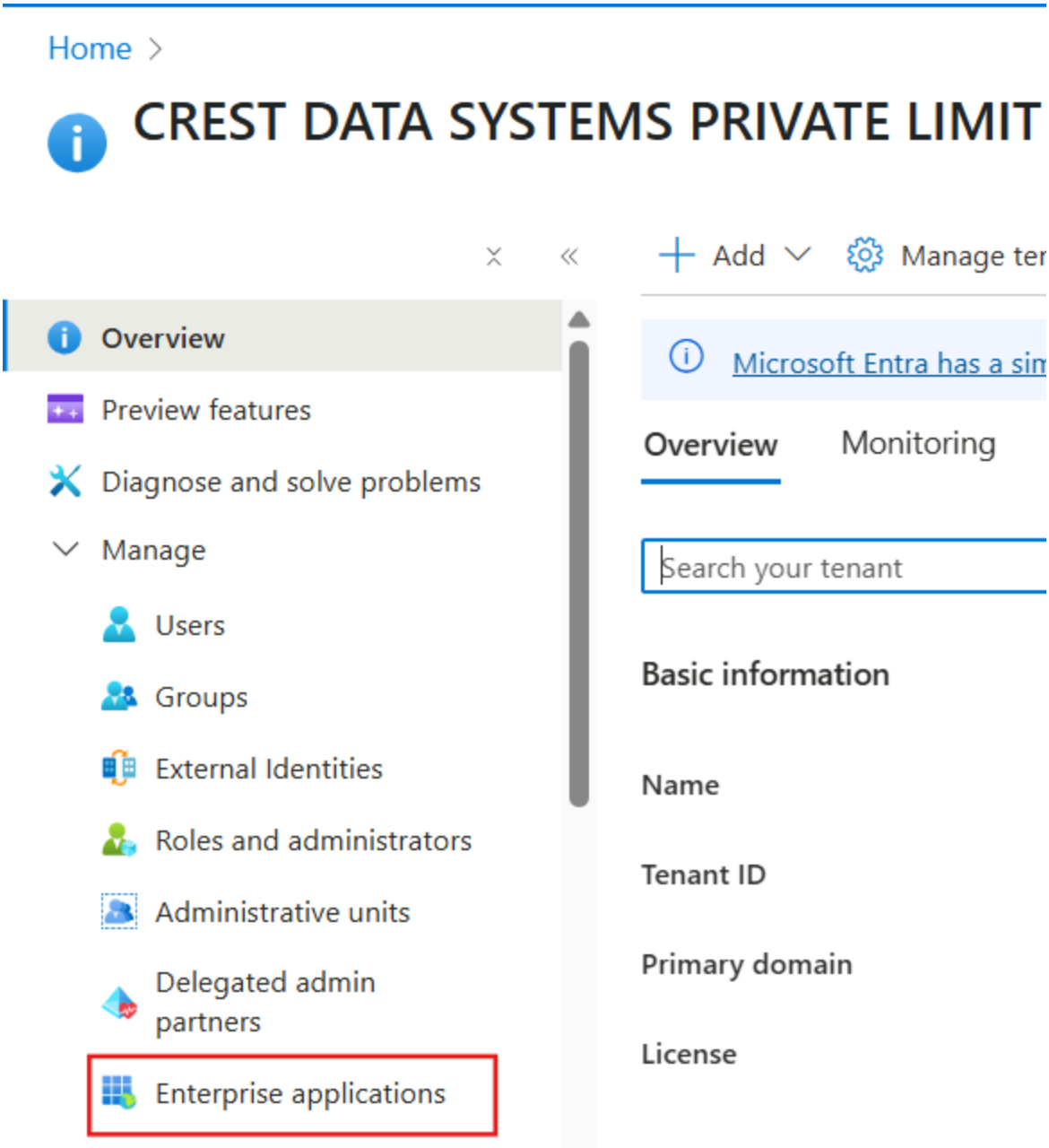
- Once validation is successful, click on **Update**
- Follow the same steps to update **TeamCymruScoutIPData** watchlist for ip indicators.

Reference link: Bulk update a

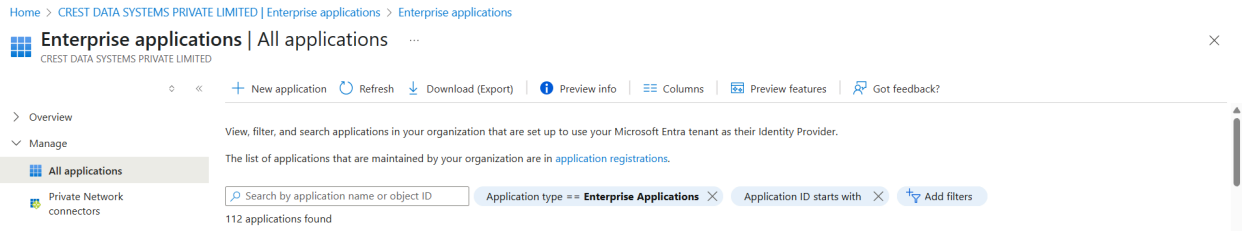
Get Object ID of your application in Microsoft Entra ID

Follow the steps to get your entra application id:

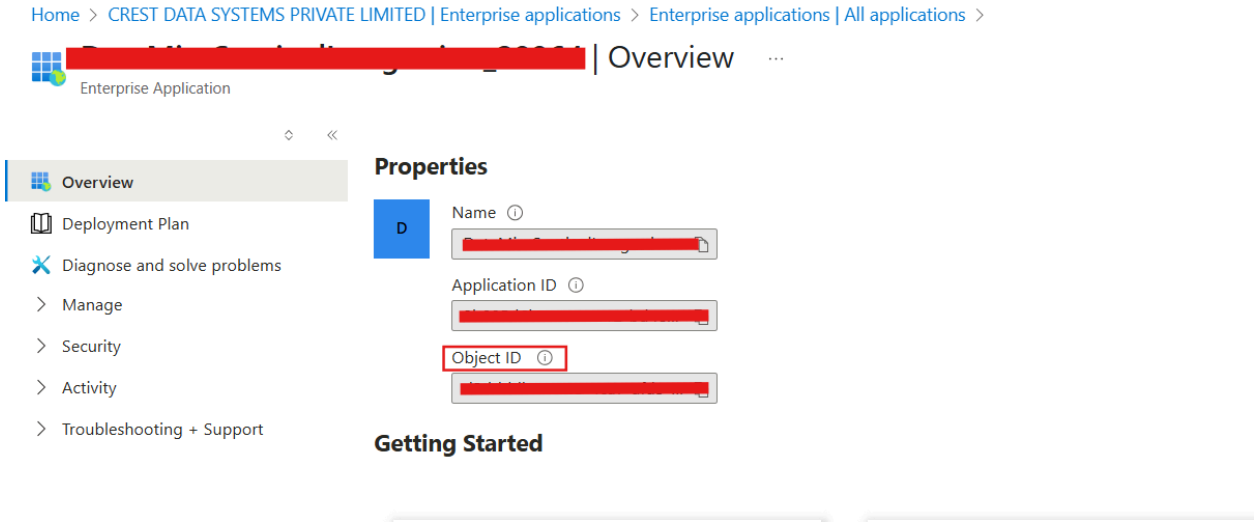
- Go to "**Microsoft Entra ID**"
- Select "**Enterprise applications**" from the left menu.



- Find your newly created application in the list (you can search by the name you provided).



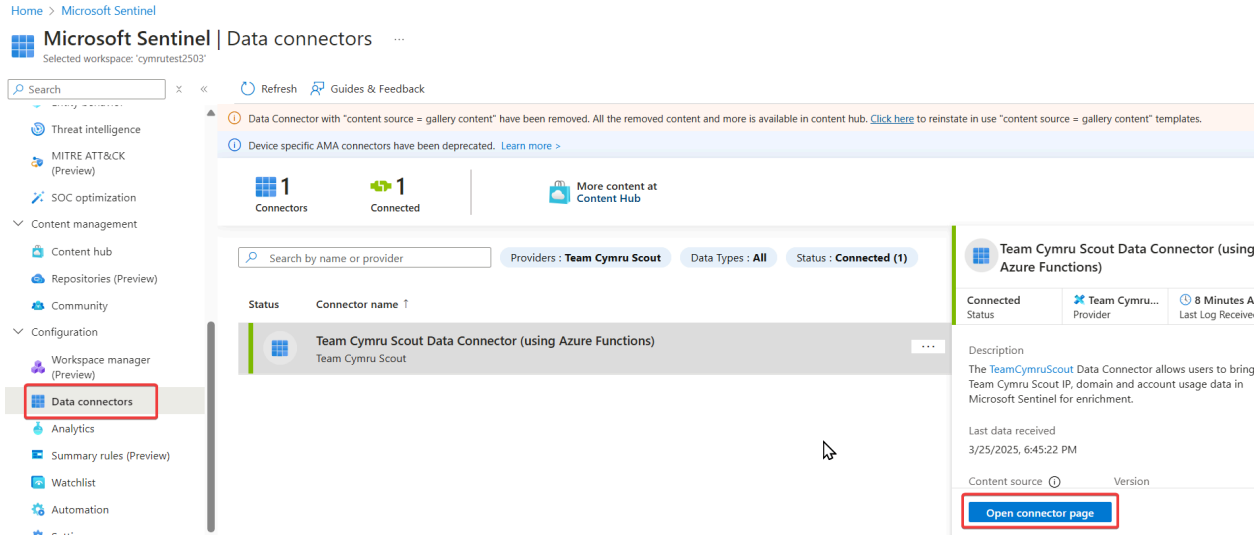
- Click on the application.
- On the overview page, copy the **Object ID**.



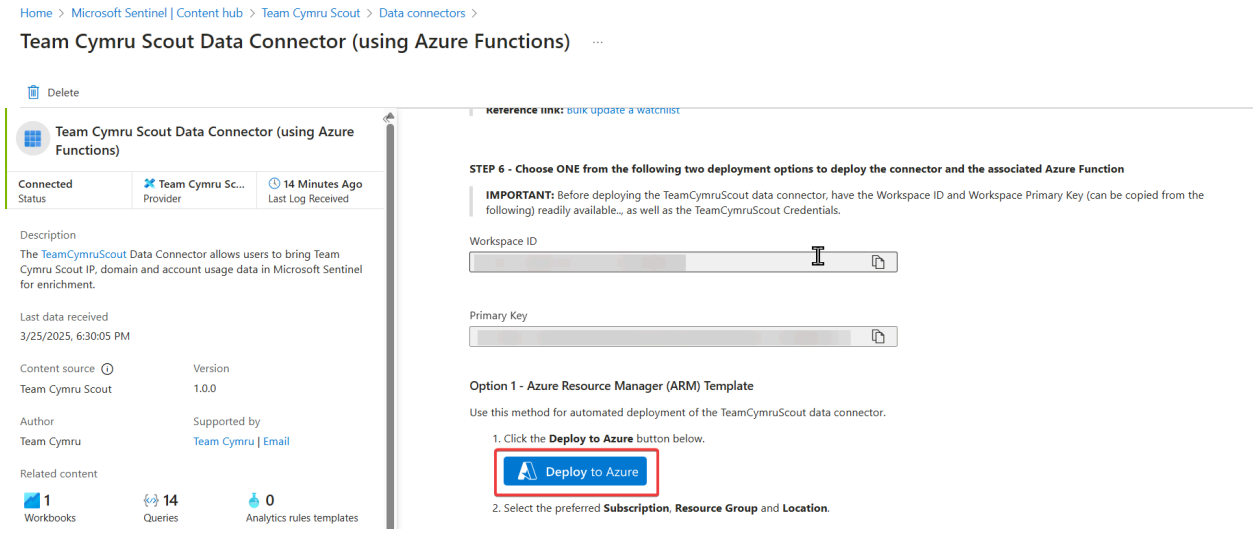
- This is the "**AzureEntraObjectId**" needed for your ARM template role assignment.

Configuration of Data Connector

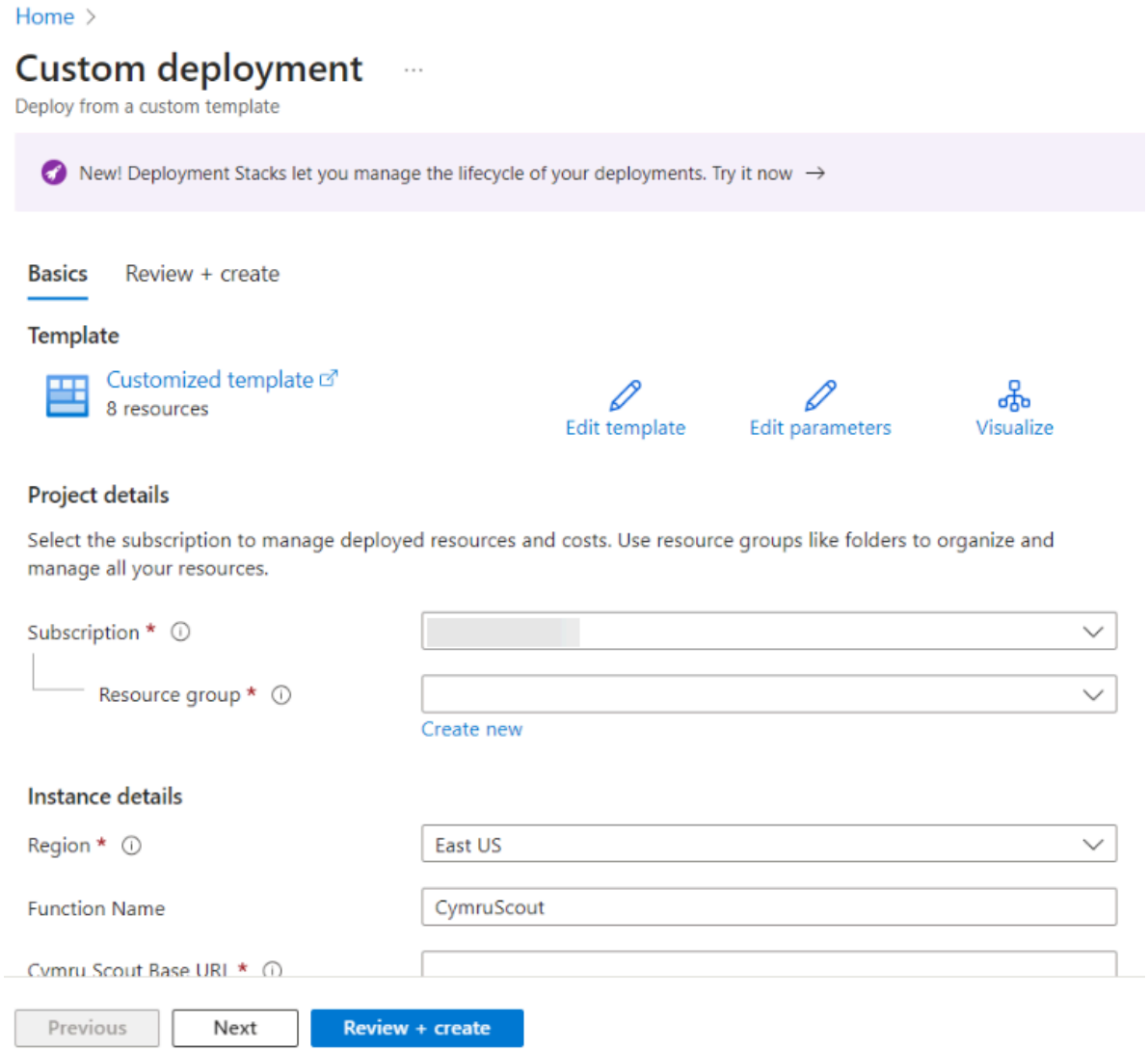
1. Go to **Microsoft Sentinel**, select the **Workspace** where the solution was installed, navigate to **Data Connectors**, search for **Team Cymru Scout Data Connector**, and click **Open Connector Page**.



2. On the **connector page**, scroll down the right-side section, locate the **Deploy to Azure** button, and click on it.



3. After clicking **Deploy to Azure**, you will be redirected to the **configuration screen** for the **Team Cymru Scout Data Connector**.



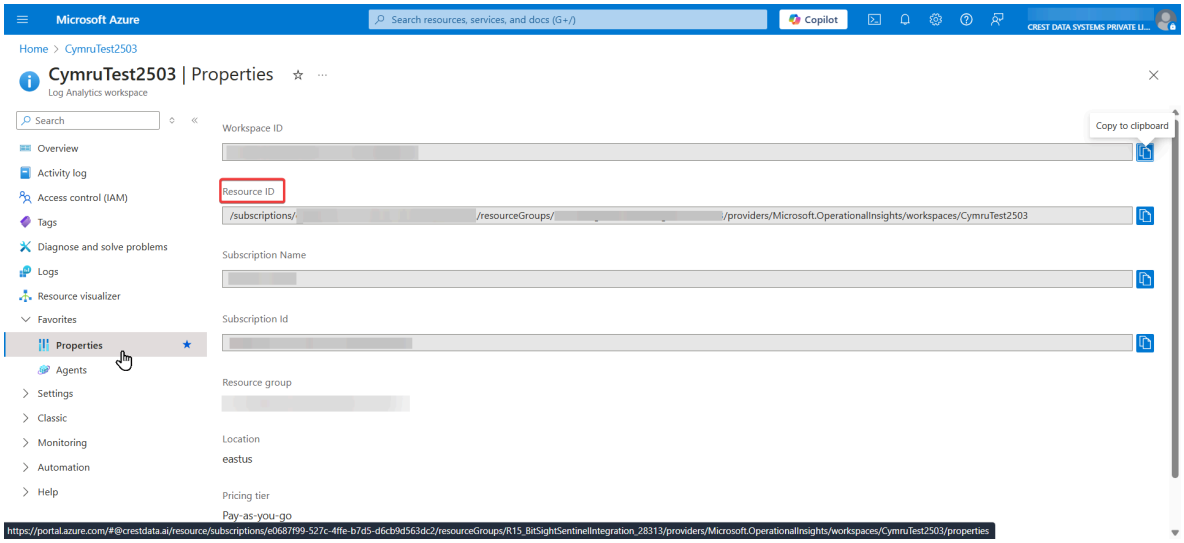
4. Enter the required **parameters** and click **Review + Create**.

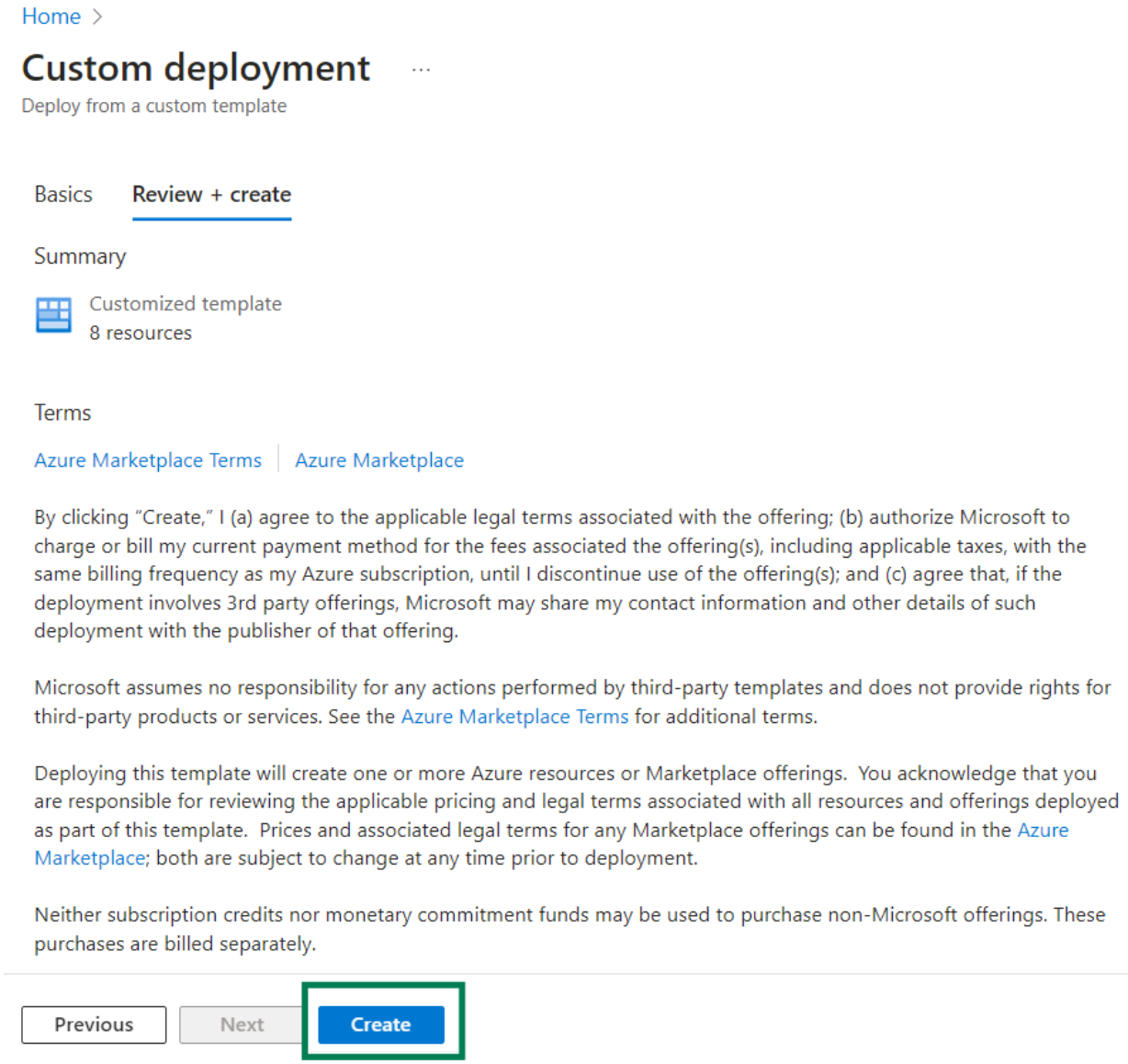
Parameter Name	Description
Resource Group	Resource group of your azure account in which you want to configure this data connector.

Workspace Name	Name of the Log analytics workspac. Can be found under Log analytics "Settings".
Function Name	Name of the Function App Name (**Note:** Keep the default name)
Team Cymru Scout Base URL	Provide base URL of Team Cymru Scout portal.
Authentication Type	Select Authentication Type for Team Cymru Scout APIs. By default it is set to Basic Auth.
Username	Enter the username for the team cymru scout account. Required if Authentication Type is Basic Auth
Password	Enter the password for the team cymru scout account. Required if Authentication Type is Basic Auth
API Key	Enter the API Key for the team cymru scout account. Required if Authentication Type is API Key.
IP Values	Enter comma separated ip values for which data should be collected. **e.g.** 1.2.3.4,10.20.30.40,2.4.3.6
Domain Values	Enter comma separated domain values for which data should be collected. **e.g.** abc.com,xyz.com,def.ai
API Type	Select the type of API to collect data for IP. By default it is set to Foundation.
Azure Client Id	Provide Azure Client Id that you have created during App Registration in the Microsoft Entra ID.
Azure Client Secret	Provide Azure Client Secret that you have created during creating the client secret in the App Registered in the Microsoft Entra ID.
Tenant Id	Provide Tenant Id of your Microsoft Entra ID.
Azure Entra Object Id	Provide Object id of your Microsoft Entra App.
IP Table Name	Table name in which IP data will ingest (Recommended keep the default table name as mentioned in the configuration)
Domain Table Name	Table name in which Domain data will ingest (Recommended keep the default table name as mentioned in the configuration)

Account Usage Table Name	Table name in which Account Usage data will ingest (Recommended keep the default table name as mentioned in the configuration)
Schedule	Enter a valid Quartz cron-expression. The default value is every day at midnight(00:00) for ip and domain data collection.
Account Usage Schedule	Enter a valid Quartz cron-expression. The default value is every 10 minutes for Account usage.
Log Level	Select log level or log severity value. By default it is set to INFO
AppInsightsWorkspaceResourceID	Migrate Classic Application Insights to Log Analytic Workspace which is retiring by 29 February 2024. Use 'Log Analytic Workspace-->Properties' blade having 'Resource ID' property value. This is a fully qualified resourceId which is in format '/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}

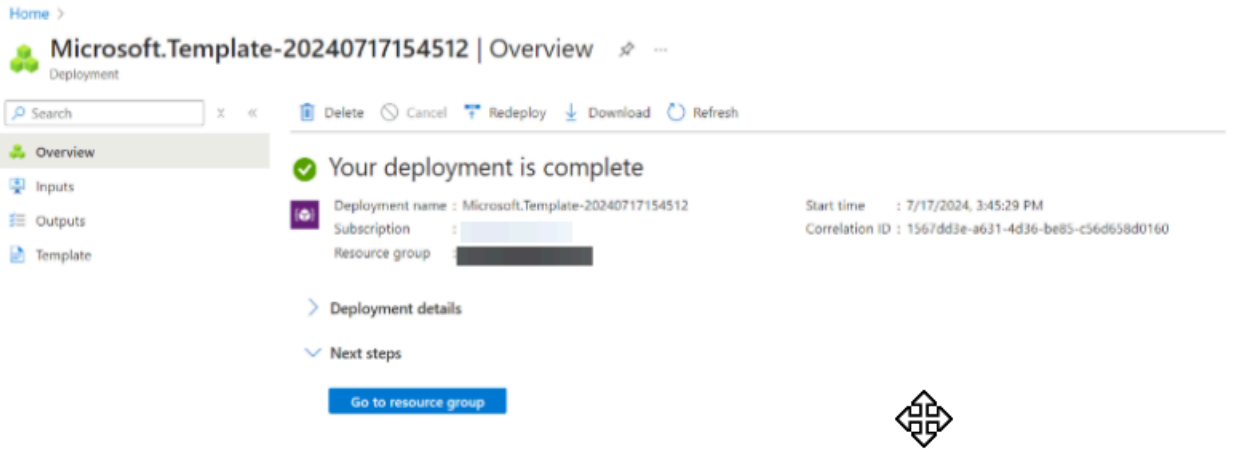
You can find **AppInsightsWorkspaceResourceID** in your **Log Analytics Workspace** under **Properties.**



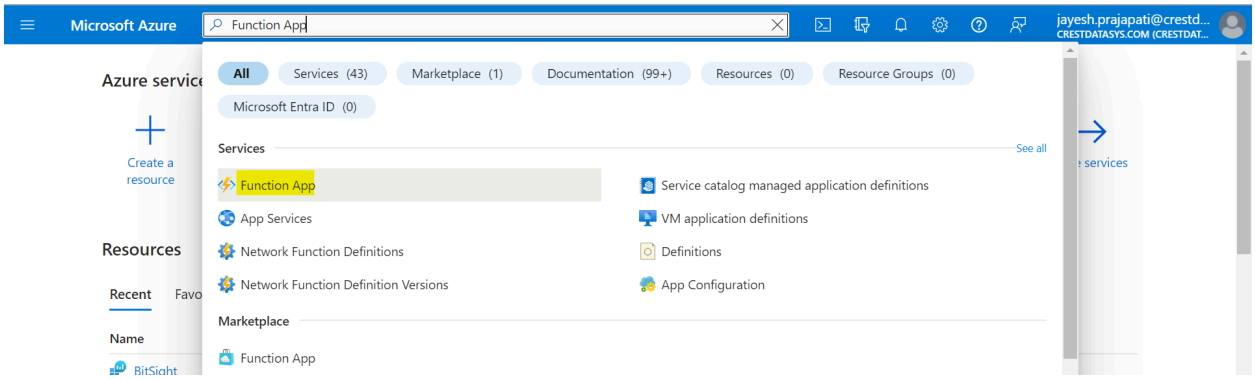


5. Click **Create** to install the **Data Connector**.

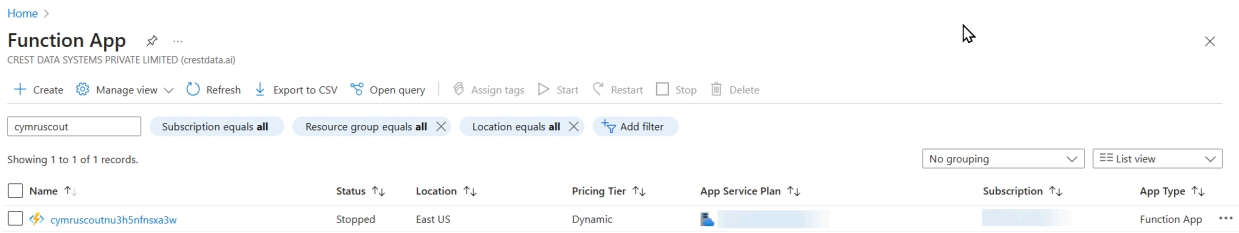
6. After that, you will be able to see the deployment status, as shown in the image below.



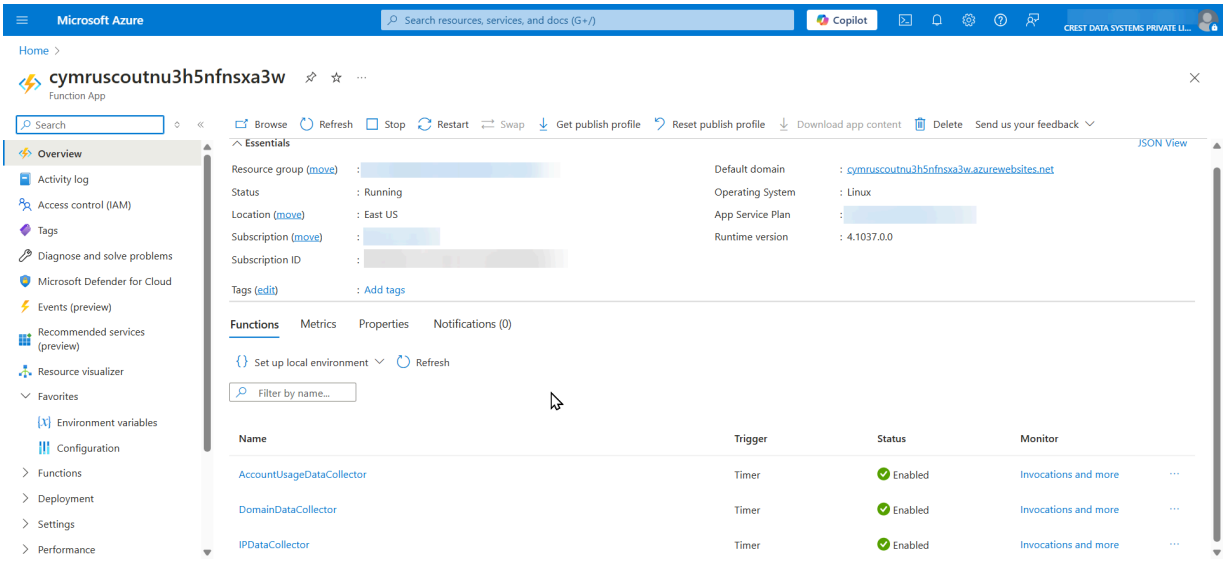
7. After successful installation, the **Data Connector** will be available under **Function App**.
8. Navigate to **Function App** by searching for it in the **Azure Portal**.



9. Locate the **installed Function App** using the name provided during configuration.



10. Click on the **cymruscout Function App**, where you will see the associated **Azure Functions** responsible for ingesting data into **Microsoft Sentinel**.



11. Once the integration is set up, **data will start flowing into Microsoft Sentinel** through the configured **Function App**. You can view this data in the **Log Analytics Workspace tables** specified during setup or use the **parsers deployed** during installation.

Steps to Configure Playbook (Logic Apps)

Note: First, configure the **TeamCymruScoutCreateIncidentAndNotify** Playbook, followed by the **TeamCymruScoutLiveInvestigation** Playbook.

Team Cymru Scout Create Incident And Notify Playbook

Usage

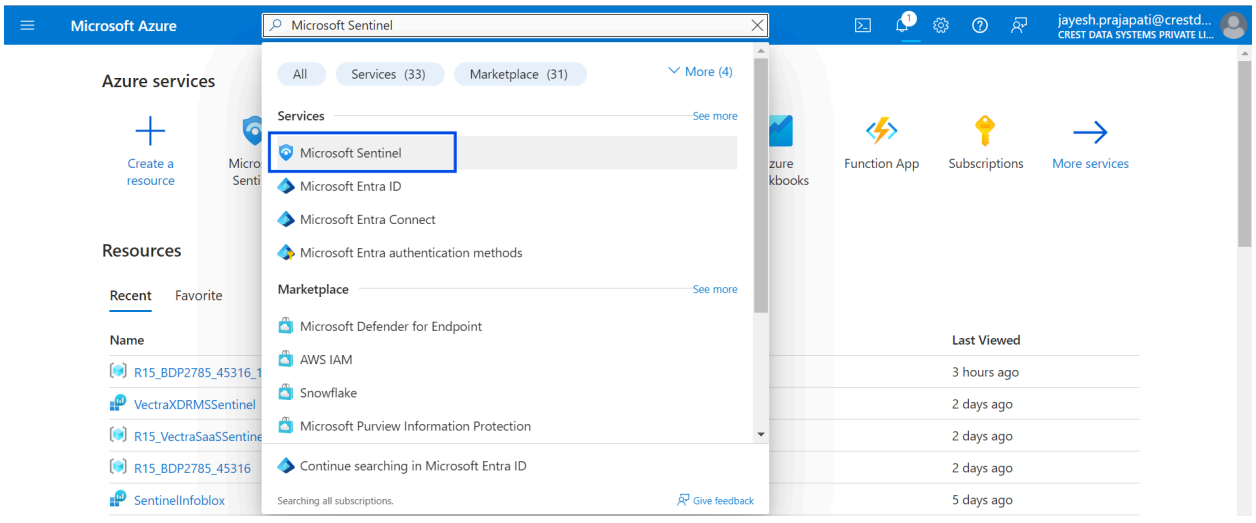
This **playbook** is triggered from two dashboards.

1. **Indicators Overview dashboard** via the **Insights Information by Indicator panel** manually.
2. **Live Investigation dashboard** automatically.

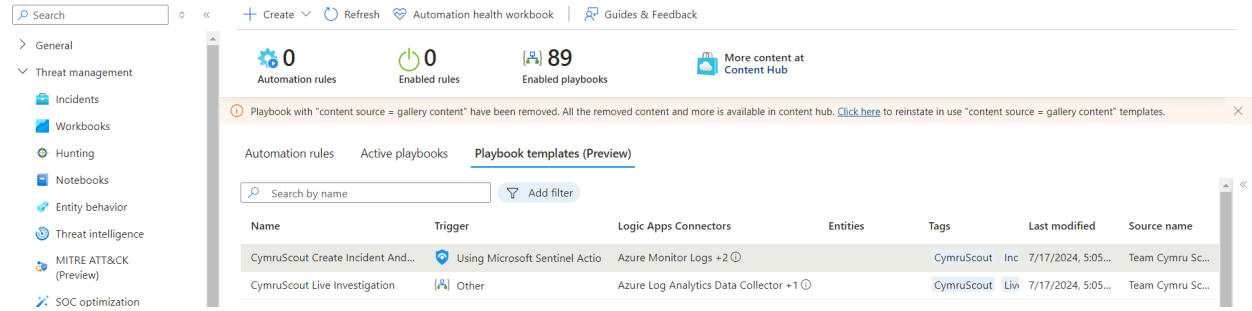
In both the cases, if the **IP's overall rating** is determined to be **suspicious or malicious**, it will **create an incident** in **Microsoft Sentinel**. Additionally, it will **send a notification** to a **predefined or user-customizable email ID**.

Configuration

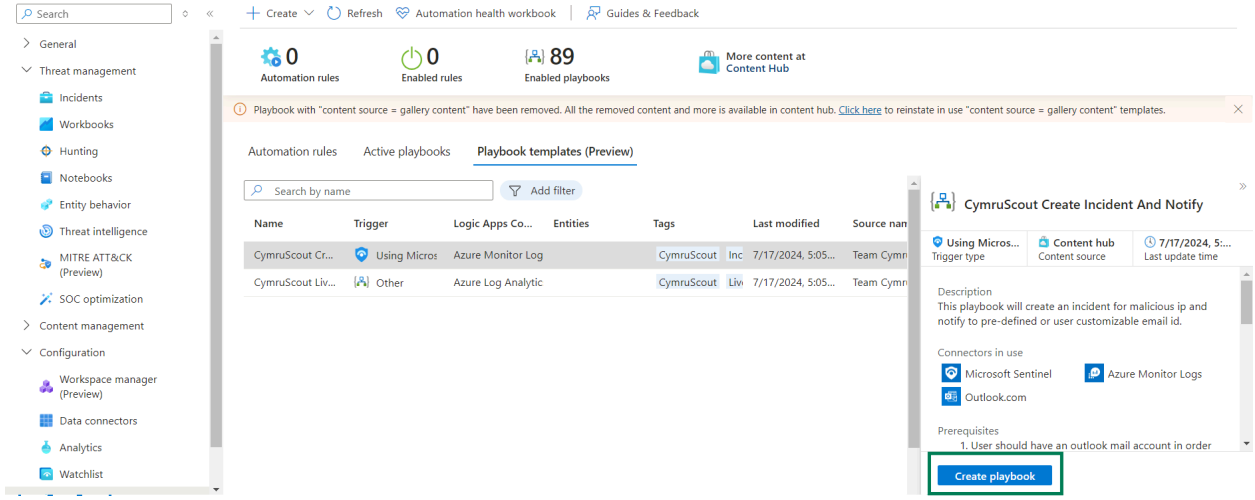
1. Open **Microsoft Sentinel**.



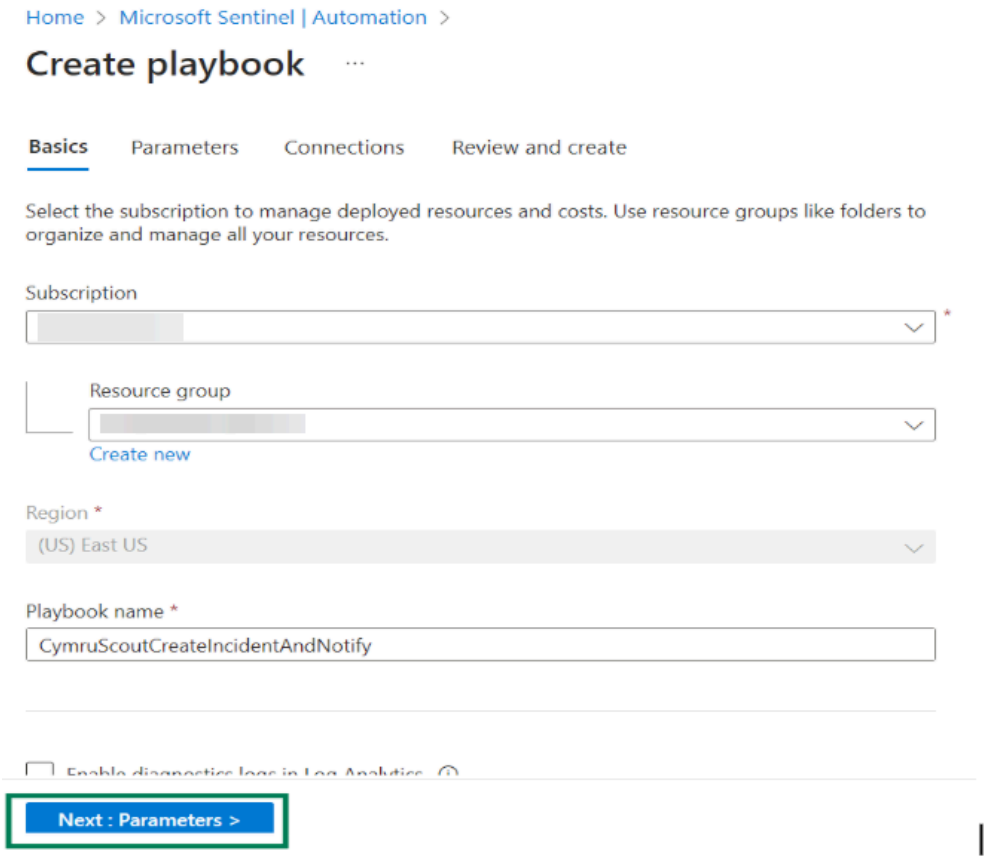
2. Navigate to the **Workspace** where the solution is installed, then go to **Automation** > **Playbook templates (Preview)** and select the **"Team Cymru Scout Create Incident And Notify"** playbook.



3. Click on **Create Playbook**.

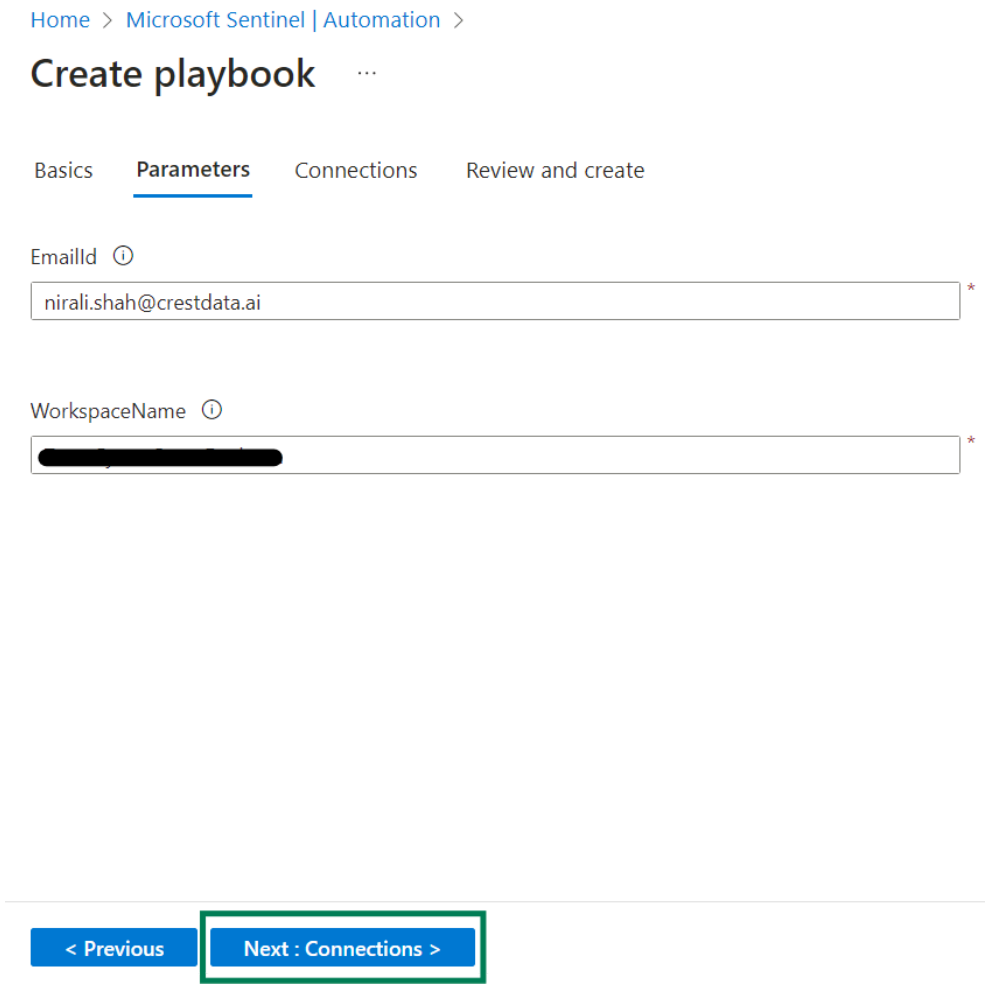


4. In the **Basic** tab, select the appropriate **Subscription** and **Resource Group**, then click **Next: Parameters**.



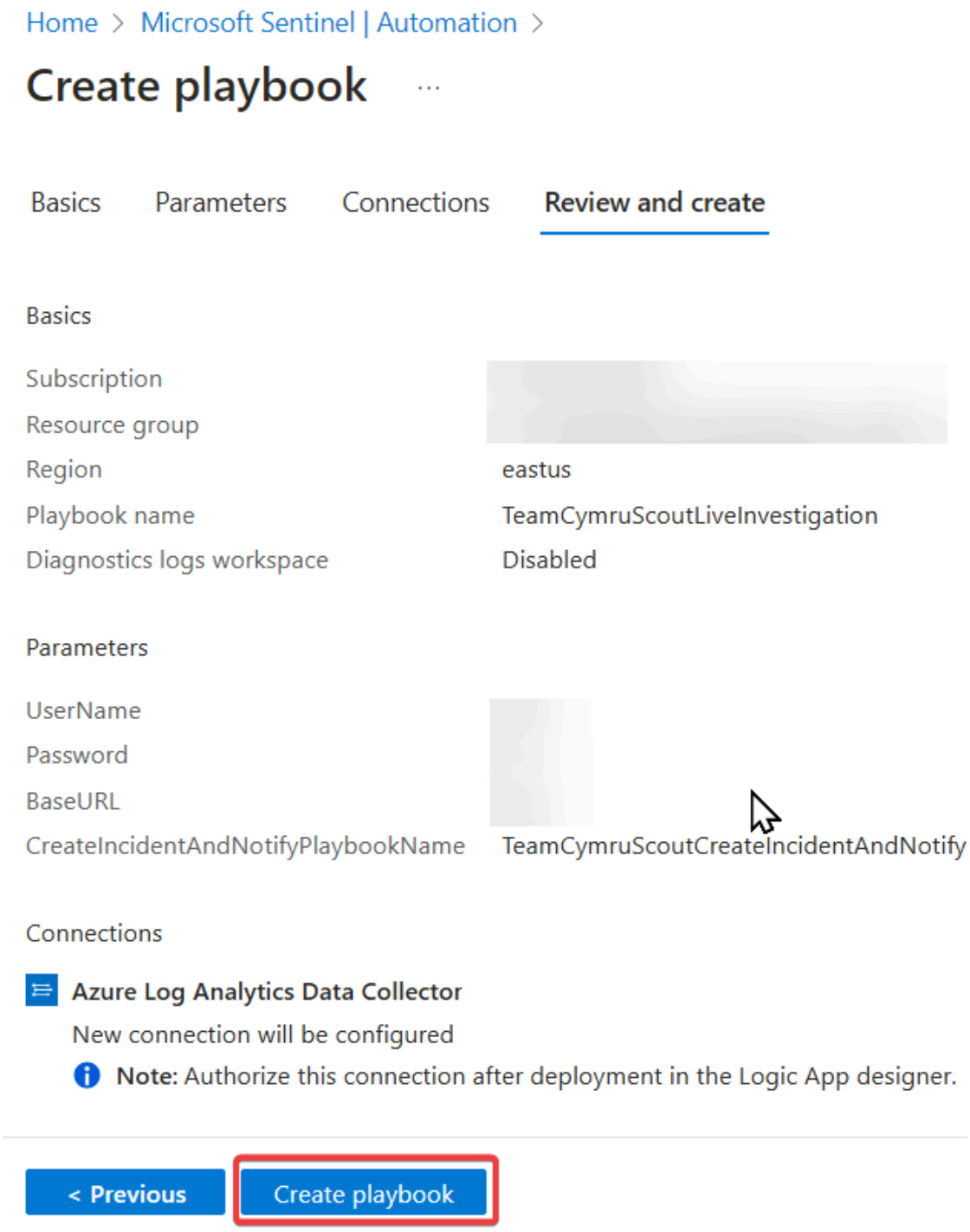
NOTE: Please do **not update Playbook name** else you won't be able to run it from the Indicator Overview tab of Workbook.

5. In the **Parameters** tab, enter the required details:
    - **EmailId:** Enter valid, comma-separated email addresses of recipients without spaces (e.g., person1@gmail.com,person2@gmail.com). Then notification via mail sent to these recipients on Malicious data.
    - **WorkspaceName:** Enter the name of the **Log Analytics Workspace** where the incident should be created.
6. Click on **Next:Connections**



7. Click on **Next: Review+Create**

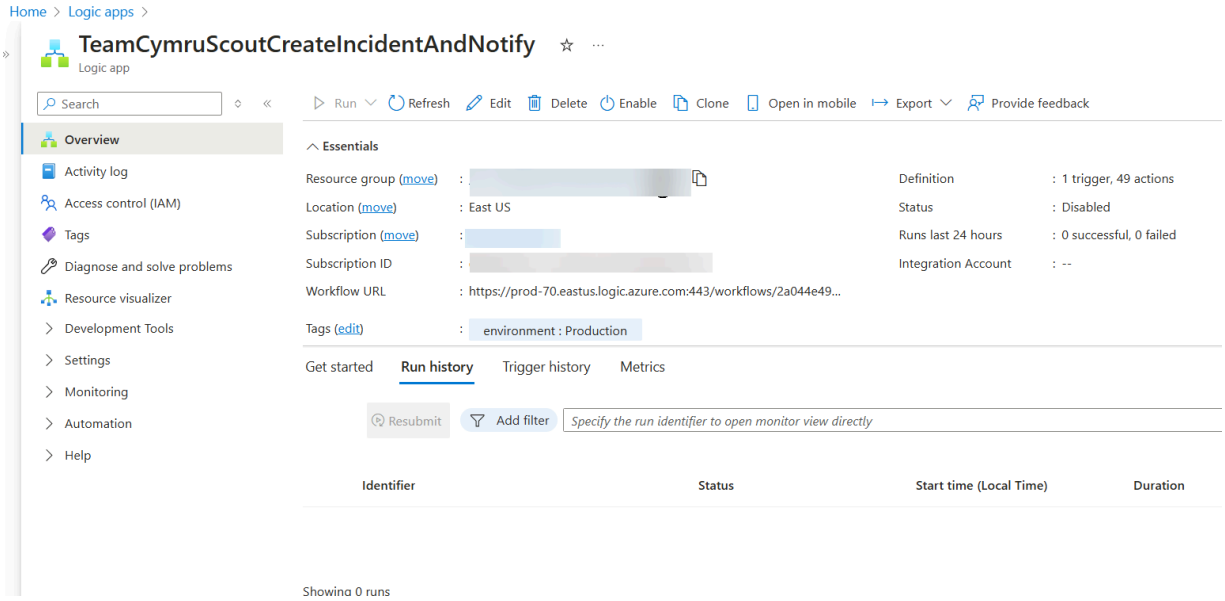
8. Click on **Create Playbook**



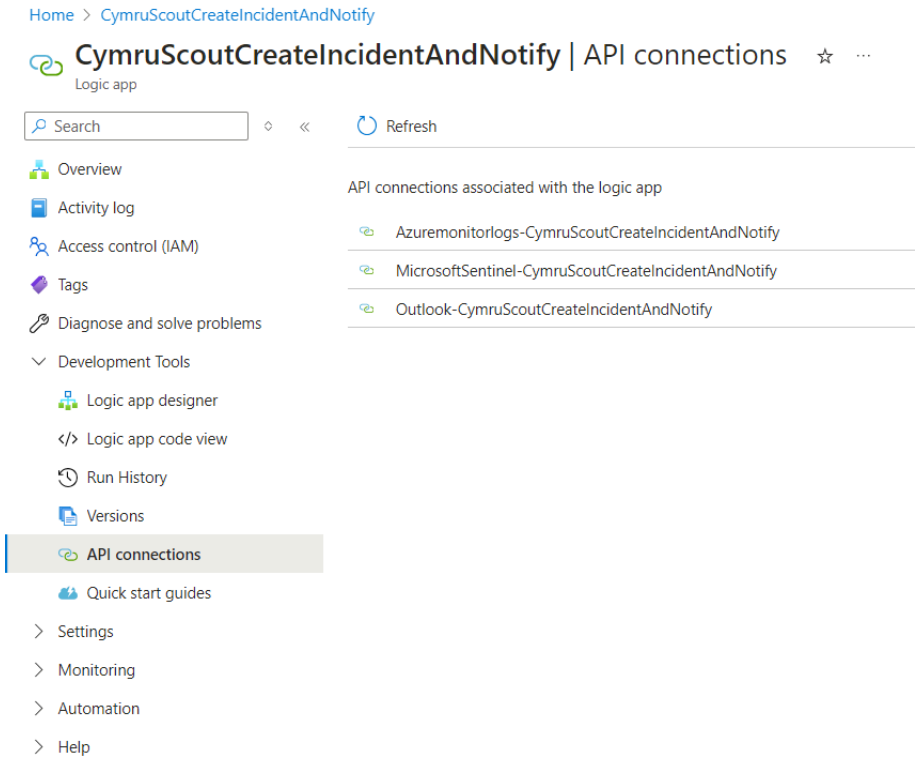
9. Once the playbook is successfully deployed, complete the **post-deployment steps** to authorize each required connection to ensure the playbook executes successfully.

Authorize API Connection

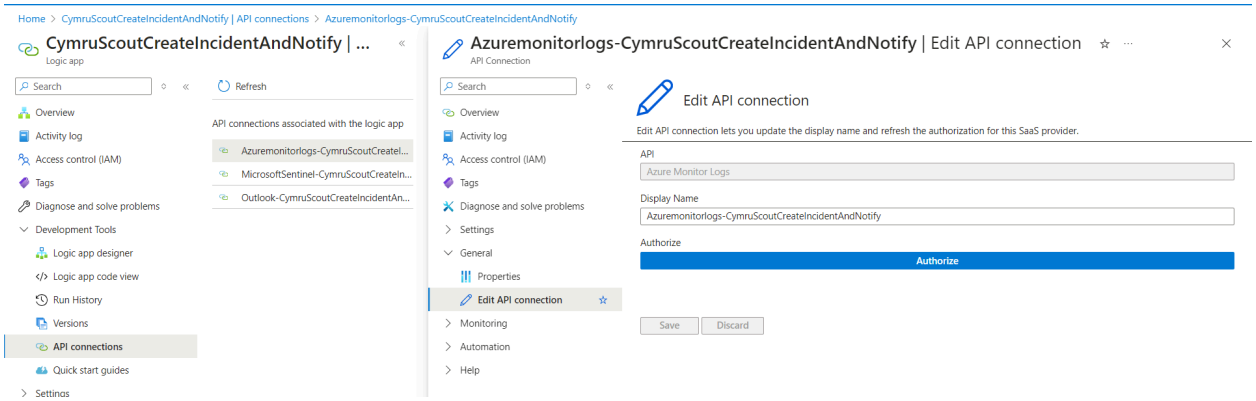
1. Search for **Logic App** and navigate to the configured playbook (**TeamCymruScoutCreateIncidentAndNotify**).



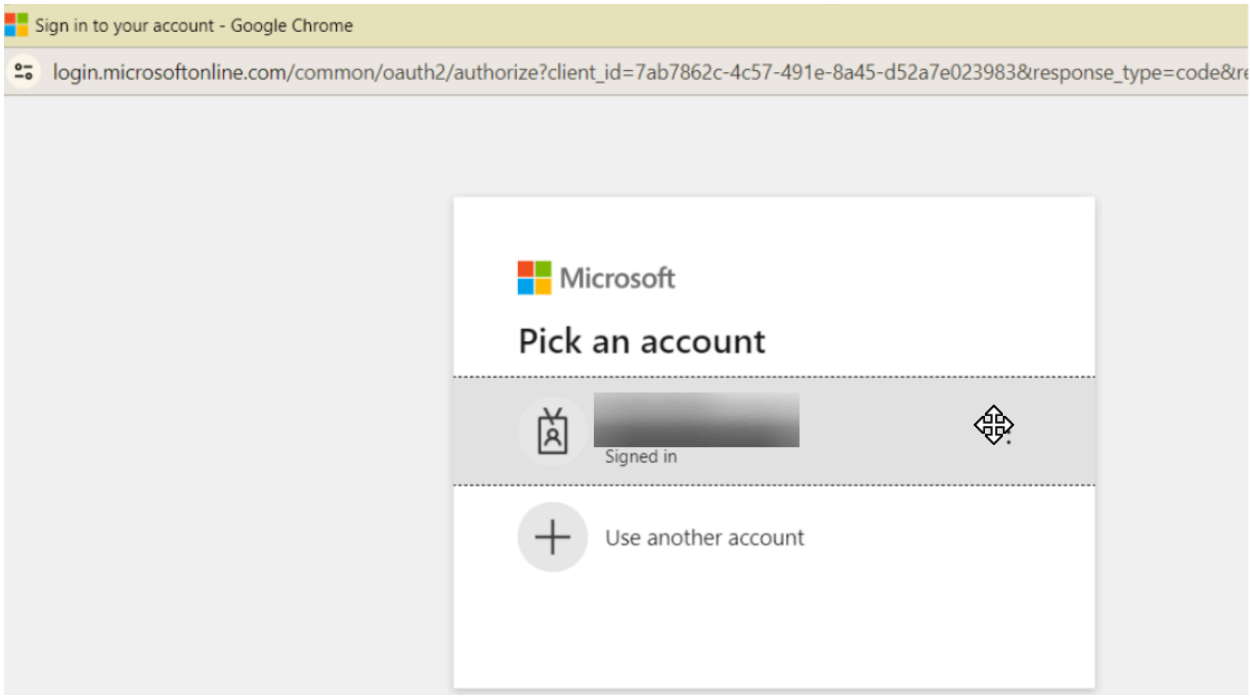
2. Go to **API connections**



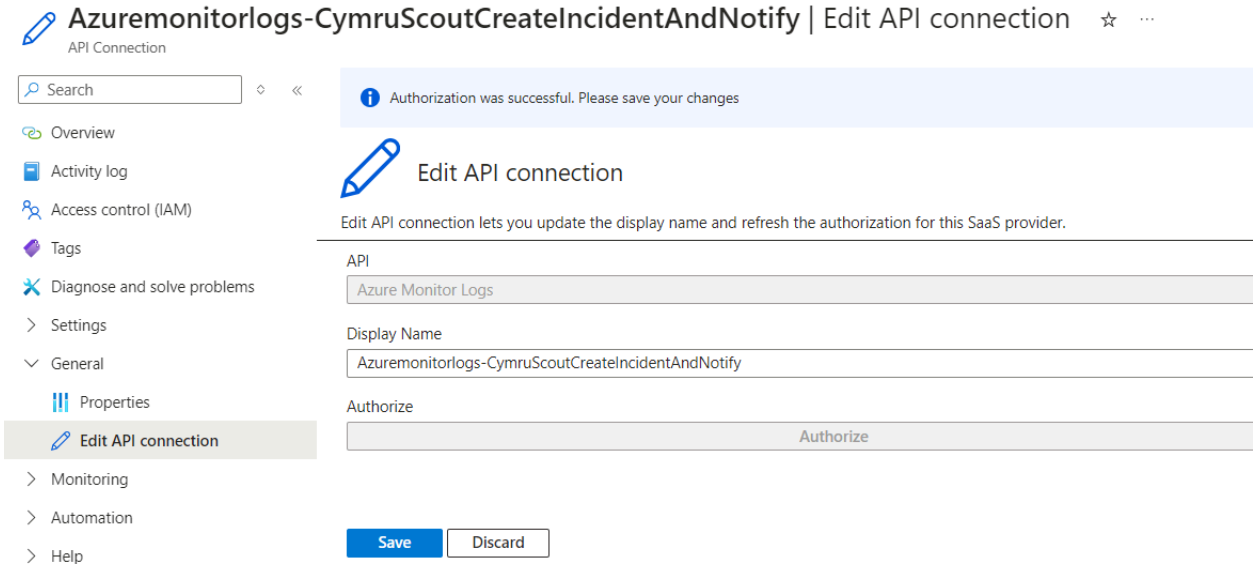
3. Click on **AzureMonitorLogs-CymruScoutCreateIncidentAndNotify API Connection** and **select Edit API Connection.**



4. Click the **Authorize** button, which will open an **Azure Portal login** popup. Sign in using your **Azure Portal credentials** for authentication.



5. Once authentication is successful, the **Save** button will be enabled. Click **Save** to store the authorized connection.

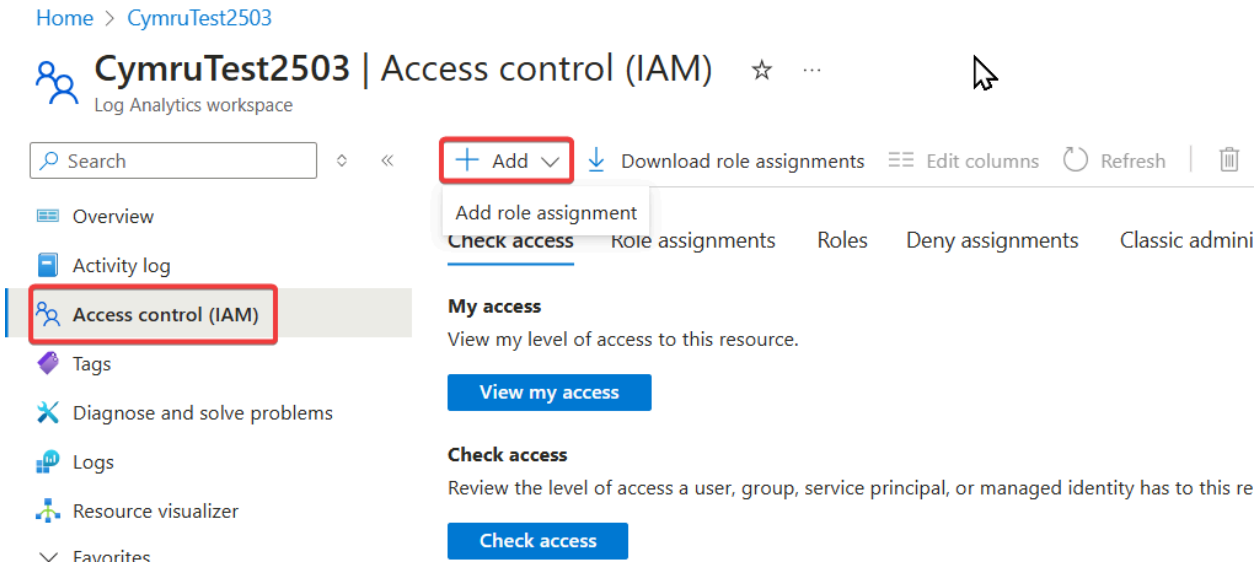


6. Similarly, authorize the connection for **Outlook**.

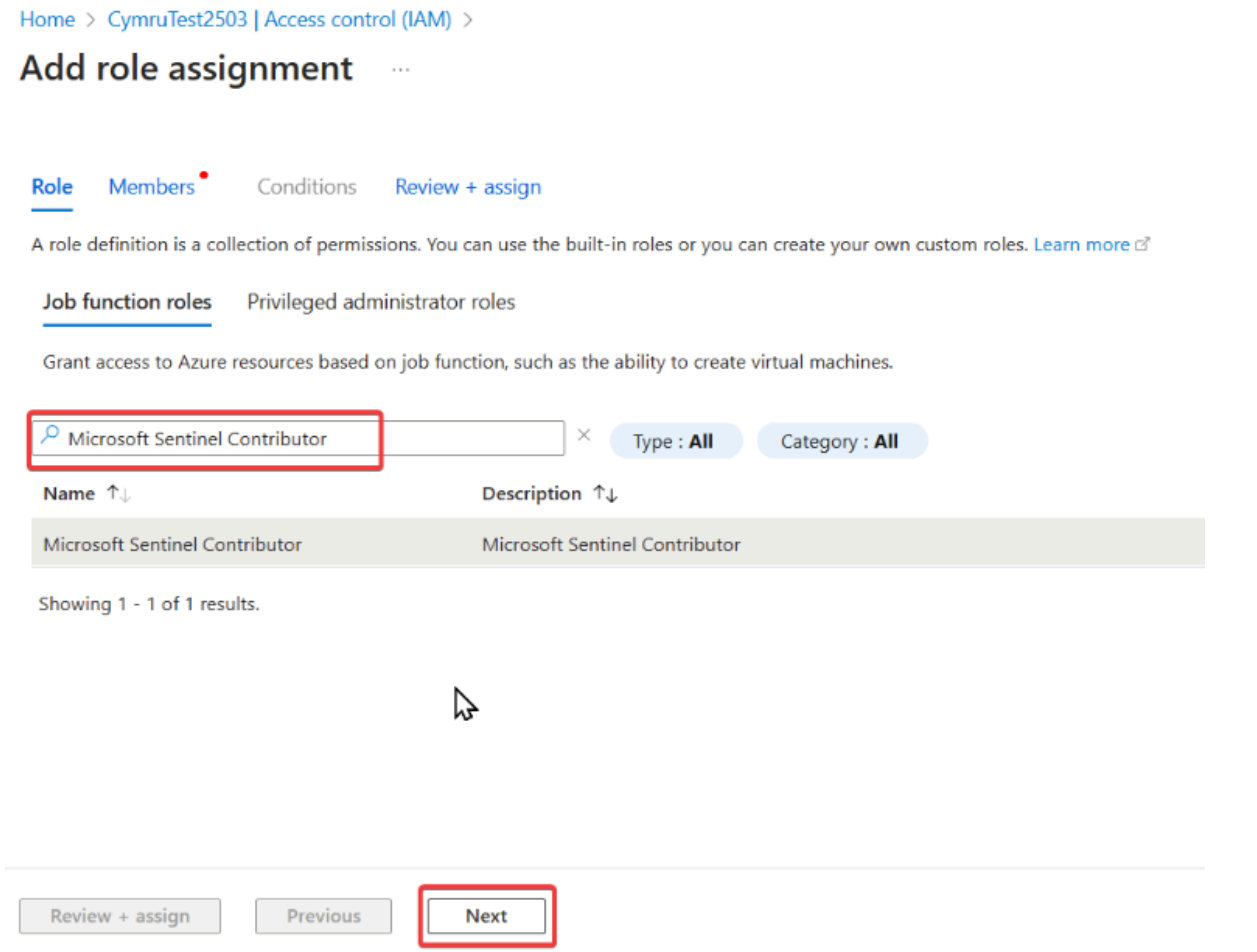
NOTE: You must authorize Outlook connection using your Outlook email ID only.

Assign Role to Add Comment in Incident

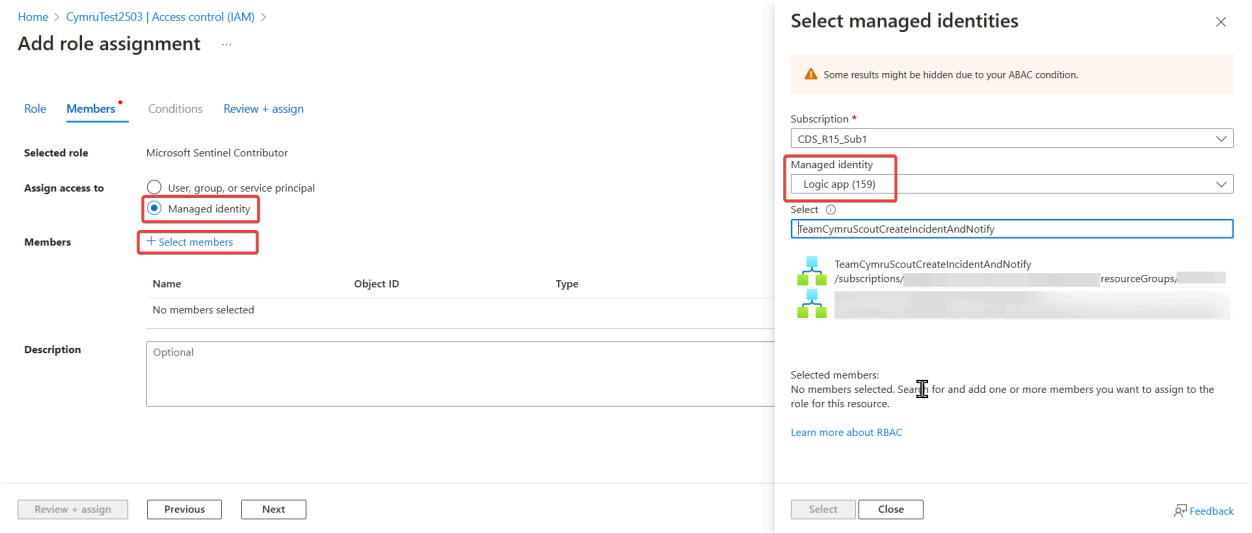
1. Navigate to **Log Analytics Workspace → {your workspace} → Access Control (IAM)**.
2. Click on **Add → Add role assignment**.

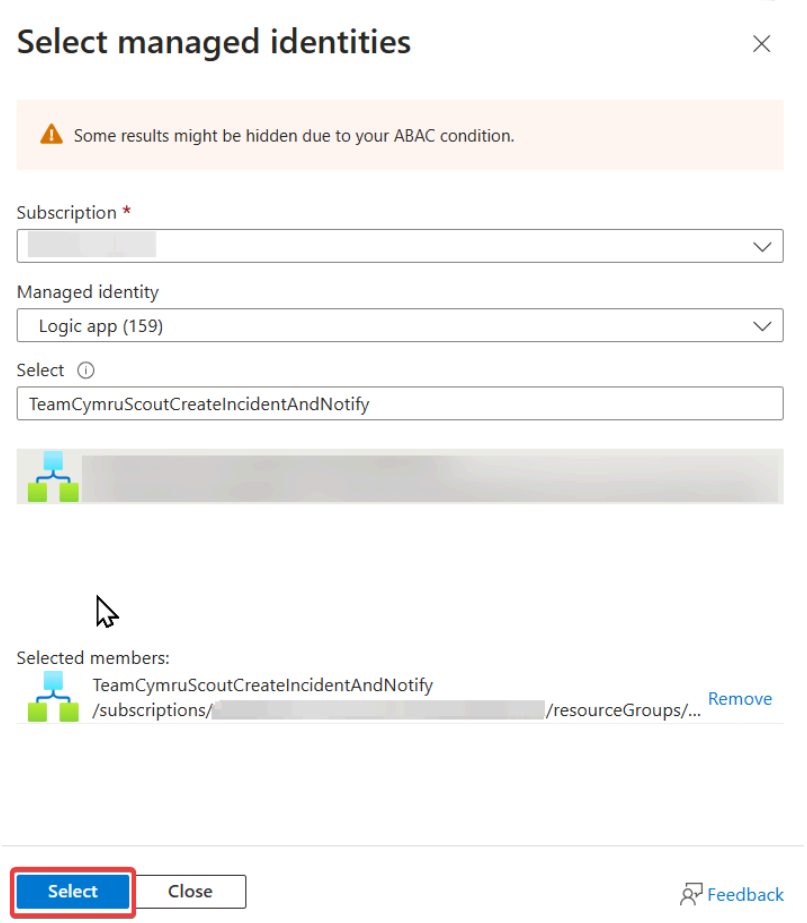


3. Under **Assignment type**, select **Job function roles**.
4. Search for **Microsoft Sentinel Contributor** and click **Next**.

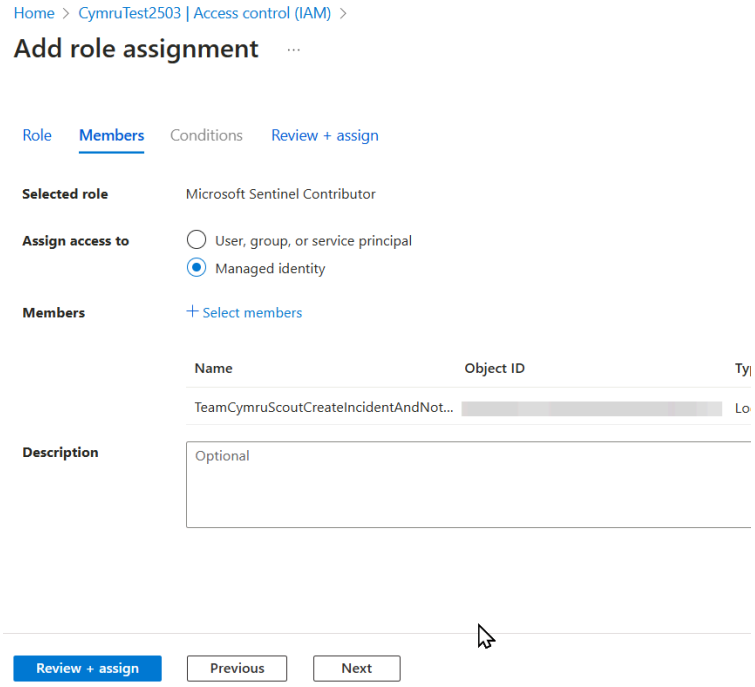


5. In the **Members** section, choose **Managed identity** for assigned access.
6. Click **Select members**, then add your **Logic App** as a member.





7. Click **Review + Assign** to complete the process.



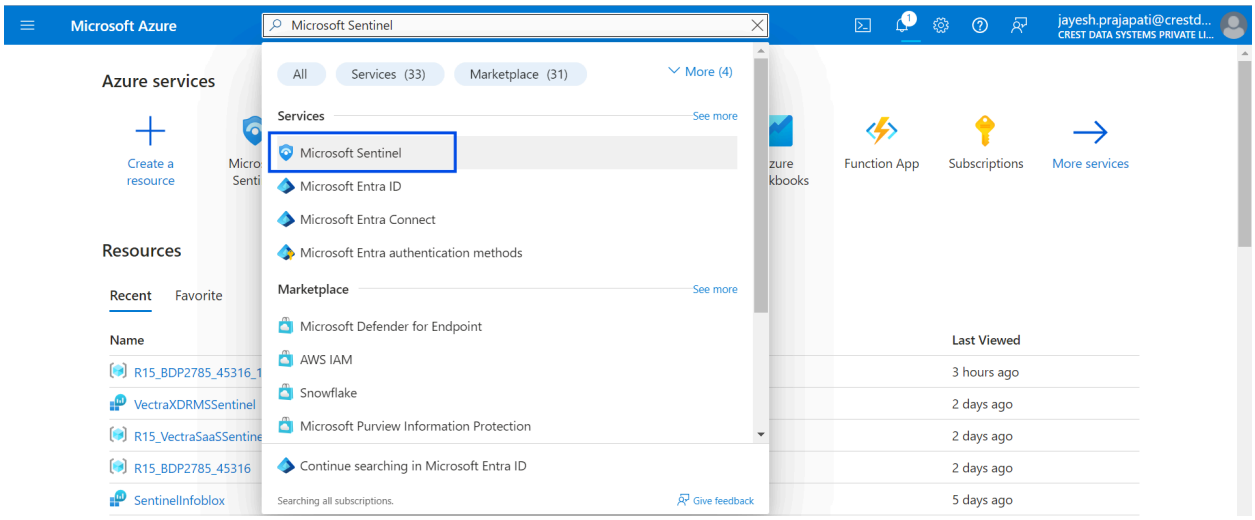
Team Cymru Scout Live Investigation Playbook

Usage

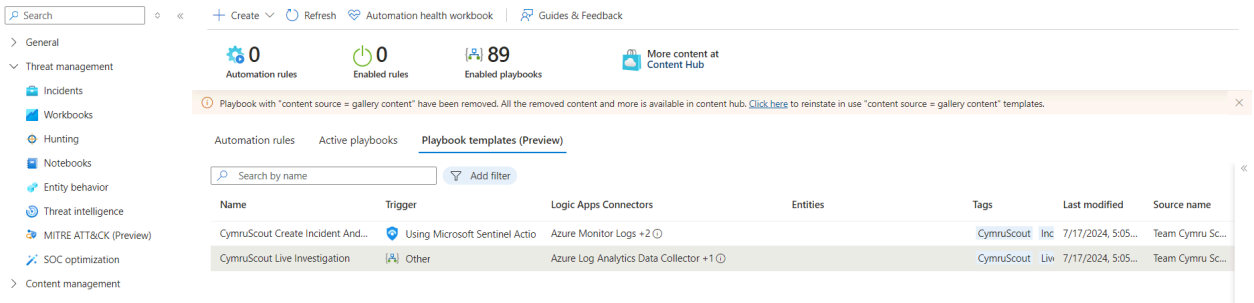
This **playbook** is triggered from the **Live Investigation** Dashboard. The **user** must provide input for an **IP or Domain value** from the **dashboard** to initiate the **live investigation**. It will **fetch live investigation data** for the specified **IP**(/api/scout/ip/{IP}/details) **or Domain**(/api/scout/search) from the **Scout API** and **store the information** in various **Microsoft Sentinel tables**.

Configuration

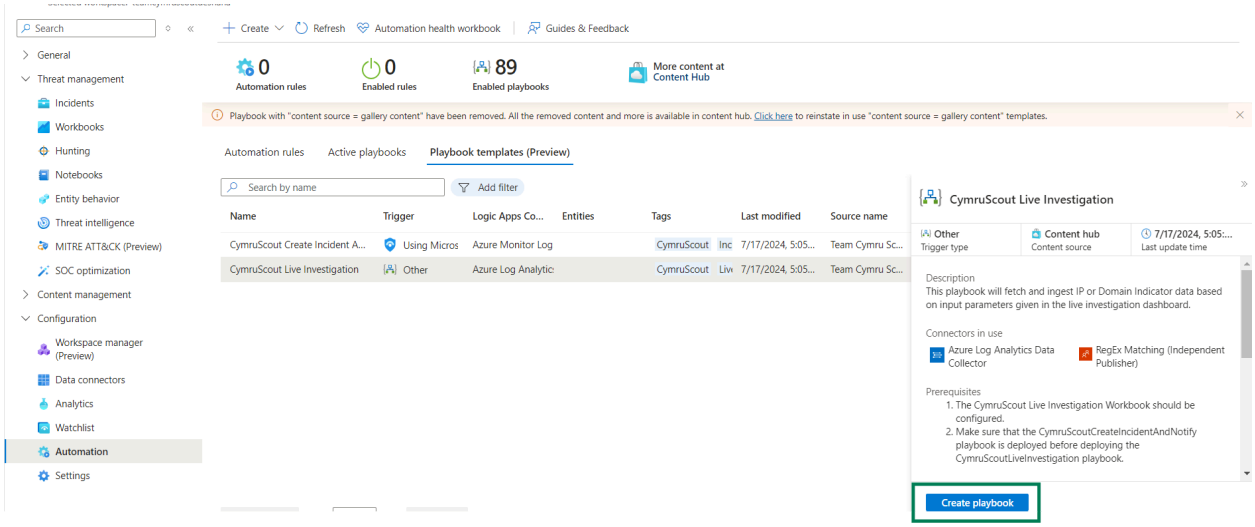
1. Go to Microsoft Sentinel



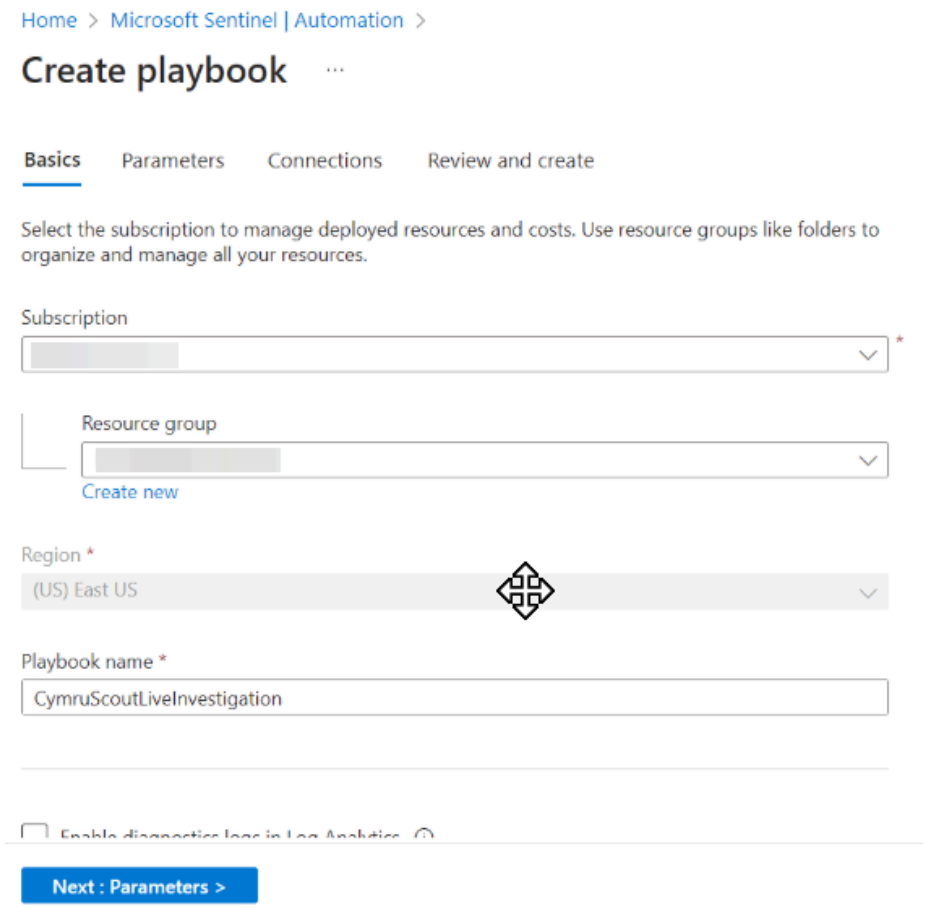
2. Navigate to the **Workspace** where the solution is installed, then go to **Automation → Playbook Templates (Preview)** and select the **"Team Cymru Scout Live Investigation"** playbook.



3. Click on the **Create Playbook** button.



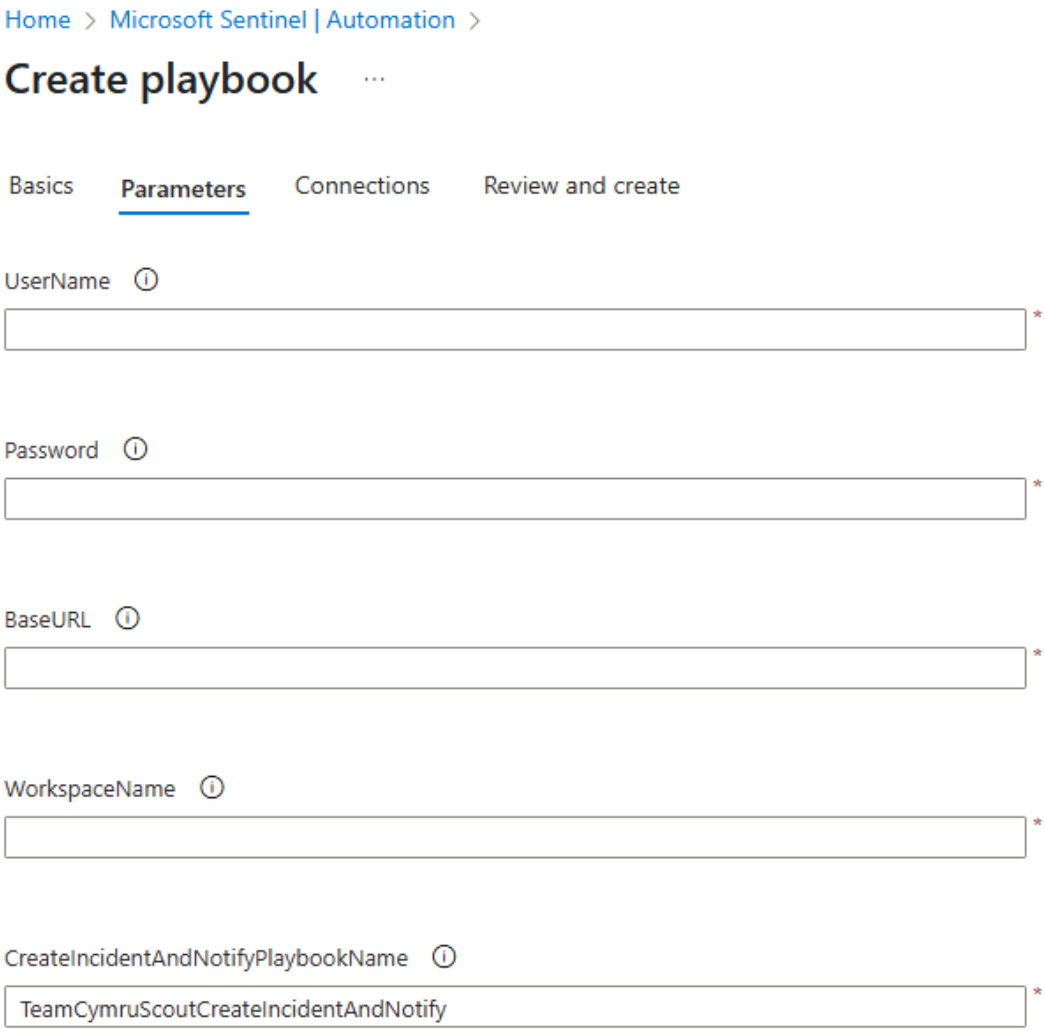
4. In the **Basic** tab, select the appropriate **Subscription** and **Resource Group**, then click **Next: Parameters**.



NOTE: Please do not modify the **Playbook name**, as this may prevent you from performing a **Live Investigation** from the **Workbook**.

5. In the **Parameters** tab, enter the following details:

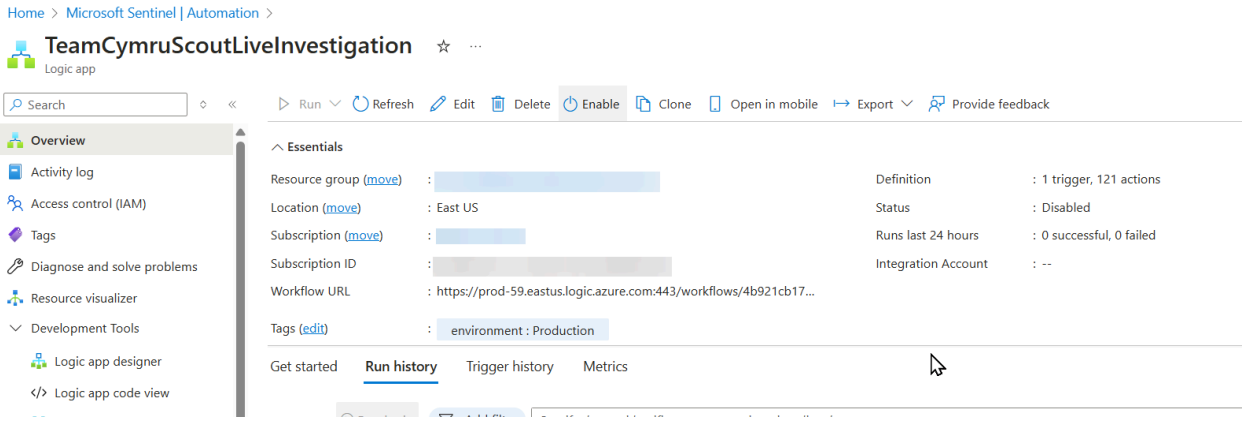
    - **UserName**: Provide the username for your **Team Cymru Scout** account.
    - **Password**: Enter the password for your **Team Cymru Scout** account.
    - **BaseURL**: Input the **Base URL** of your **Team Cymru Scout** account.
    - **CreateIncidentAndNotifyPlaybookName**: Enter the playbook name assigned during the deployment of **CymruScoutCreateIncidentAndNotify** (e.g., **CymruScoutCreateIncidentAndNotify**).
    - **WorkspaceName:** Enter workspace name in which you want to fetch or store your data.



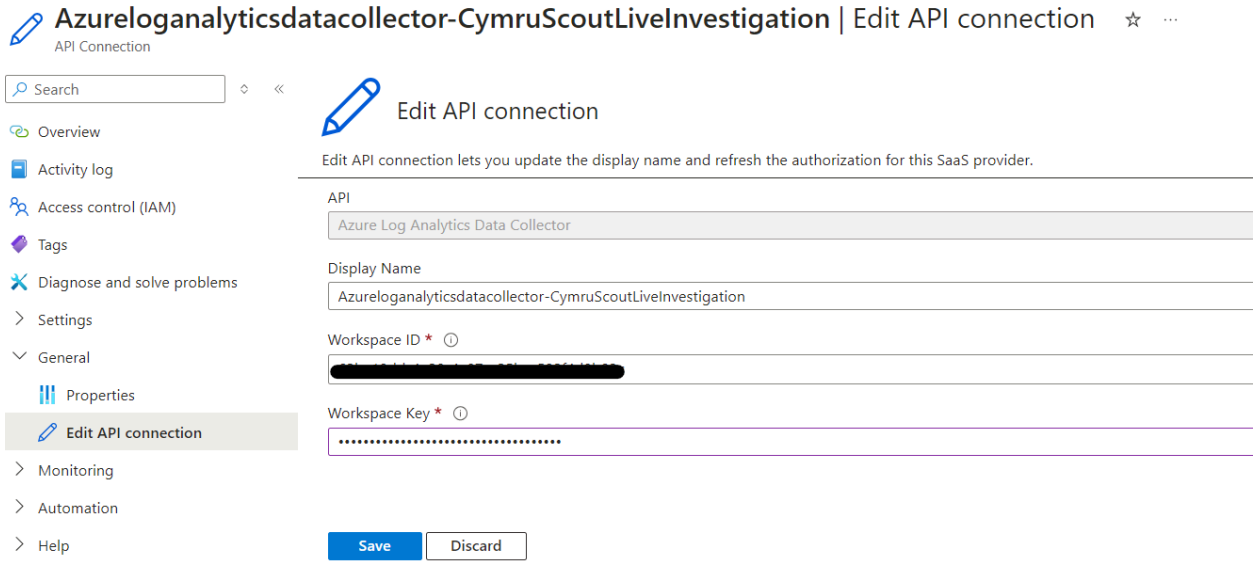
6. Click on **Next:Connections**
7. Click on **Next: Review+Create**
8. Click on **Create Playbook** and continue to the designer
9. After successfully deploying the playbook, complete the **post-deployment steps** to authorize all required connections, ensuring the playbook executes successfully.

Authorize API Connection

1. Search for **Logic App** and navigate to the configured playbook (**TeamCymruScoutLiveInvestigation**).



2. **Go to API Connections.**
3. Click on **AzureLogAnalyticsDataCollector-TeamCymruScoutLiveInvestigation API Connection** and select **Edit API Connection**.
4. Enter the **Workspace ID** and **Workspace Key** where your **Live Investigation Workbook** is available and where the data will be ingested.



5. Click **Save** to store the authorized connection.

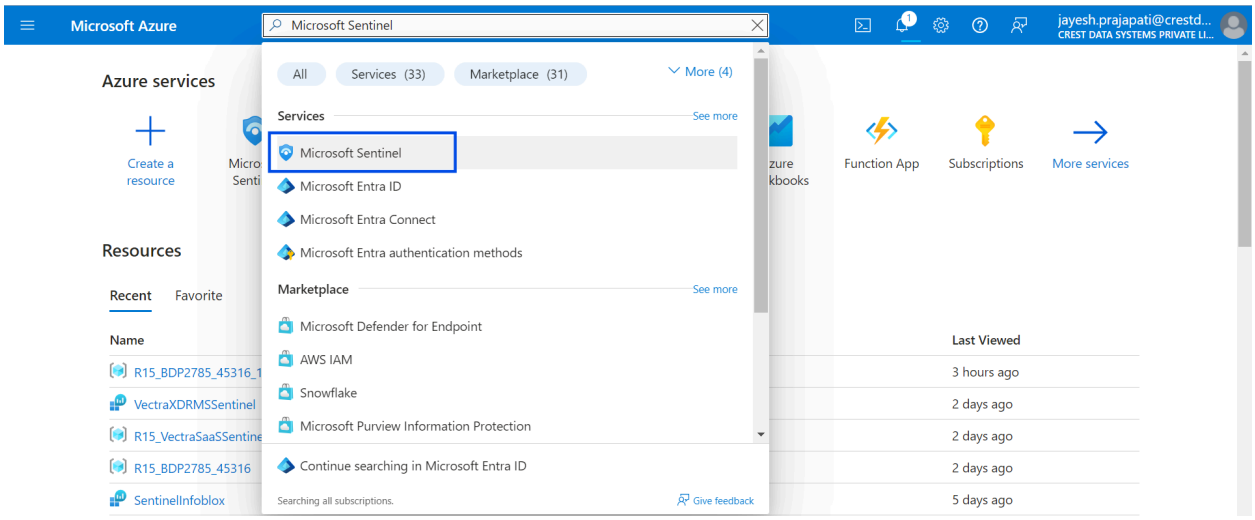
Team Cymru Scout Enrich Incident Playbook

Usage

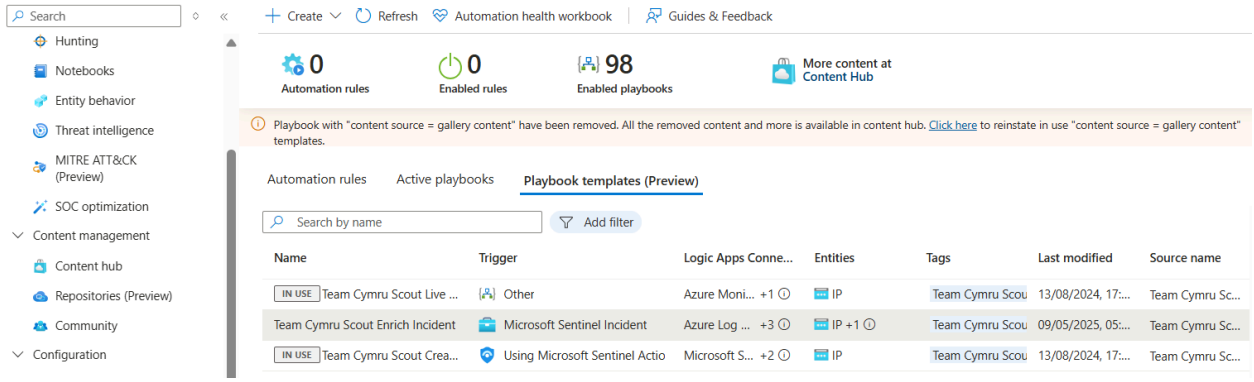
This **playbook** is triggered from the Microsoft Sentinel Incident. It will fetch IP and Domain List from mapped entities with Incident. It will **fetch investigation data** for the specified **IP**(/api/scout/ip/{IP}/details) **and Domain**(/api/scout/search) from the **Scout API** and **store the information** in various **Microsoft Sentinel tables**. It will process data from different sections and add into **Incident Comment**.Additionally, it will **send a notification** to a **predefined or user-customizable email ID**.

Configuration

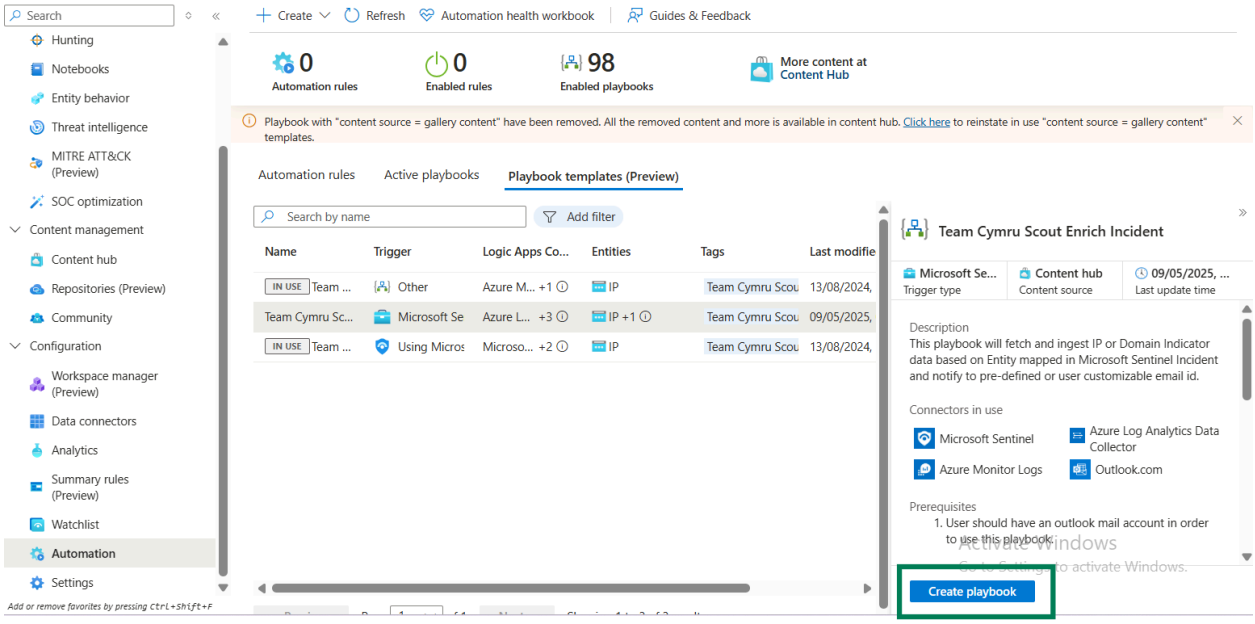
1. Go to Microsoft Sentinel



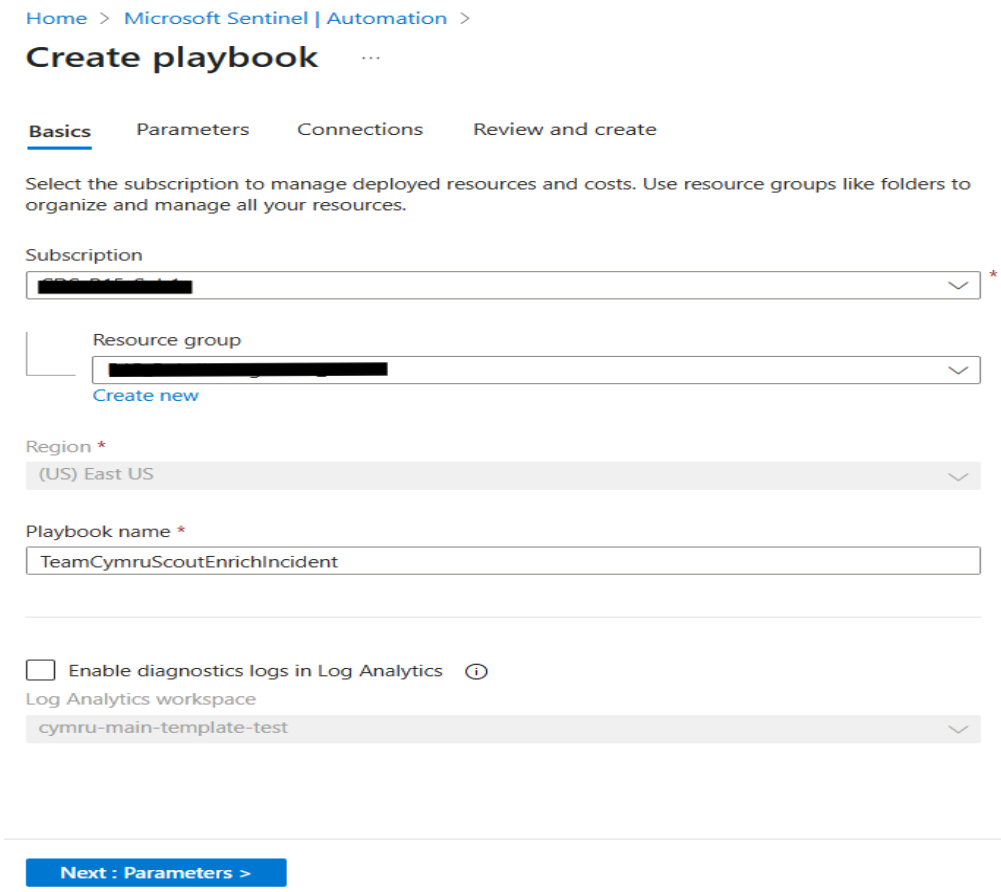
2. Navigate to the **Workspace** where the solution is installed, then go to **Automation** → **Playbook Templates (Preview)** and select the **"Team Cymru Scout Enrich Incident"** playbook.



3. Click on the **Create Playbook** button.

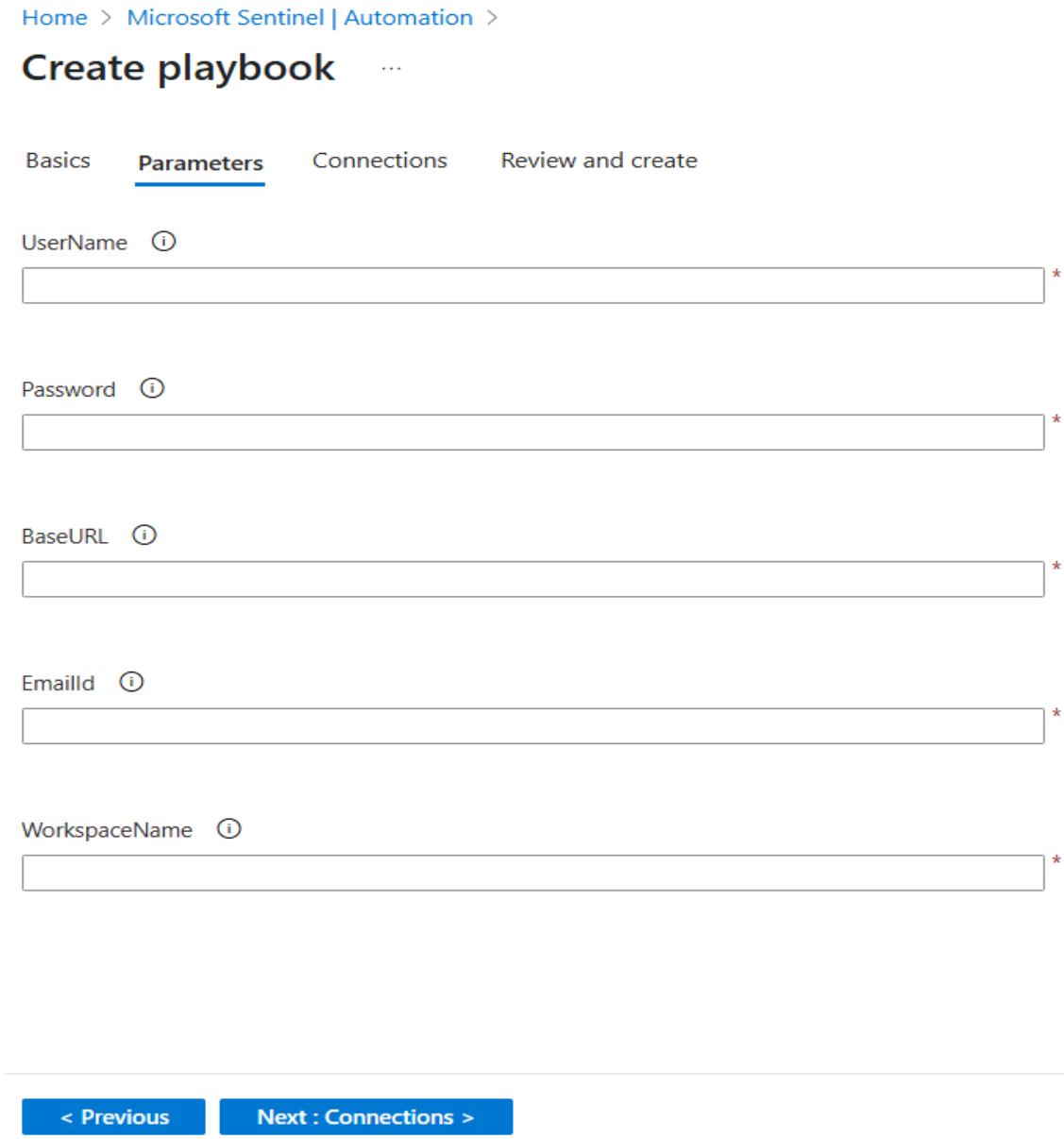


4. In the **Basic** tab, select the appropriate **Subscription** and **Resource Group**, then click **Next: Parameters**.



5. In the **Parameters** tab, enter the following details:

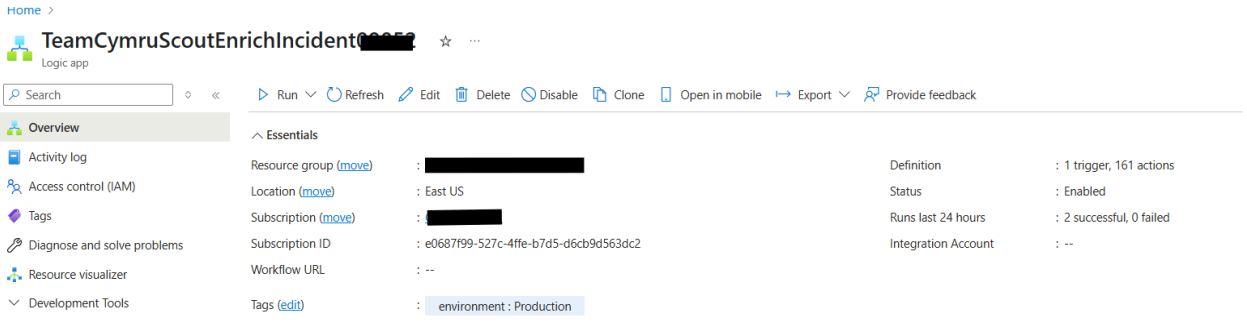
   - **UserName**: Provide the username for your **Team Cymru Scout** account.
   - **Password**: Enter the password for your **Team Cymru Scout** account.
   - **BaseURL**: Input the **Base URL** of your **Team Cymru Scout** account.
   - **EmailId:** Enter valid, comma-separated email addresses of recipients without spaces (e.g., person1@gmail.com,person2@gmail.com). Then notification via mail sent to these recipients on Malicious data.
   - **WorkspaceName:** Enter workspace name in which you want to fetch or store your data.



6. Click on **Next:Connections**
7. Click on **Next: Review+Create**
8. Click on **Create Playbook** and continue to the designer

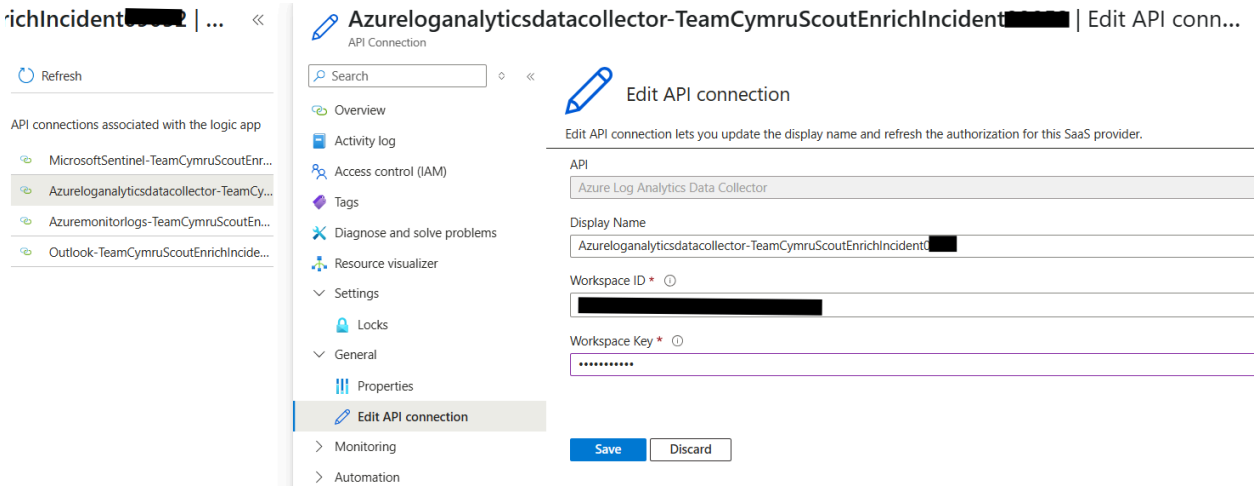
Authorize API Connection

1. Search for **Logic App** and navigate to the configured playbook (**TeamCymruScoutEnrichIncident**).



2. **Go to API Connections.**
3. Click on **AzureLogAnalyticsDataCollector-TeamCymruScoutEnrichIncident API Connection** and select **Edit API Connection**.

4. Enter the **Workspace ID** and **Workspace Key** where the data will be ingested.

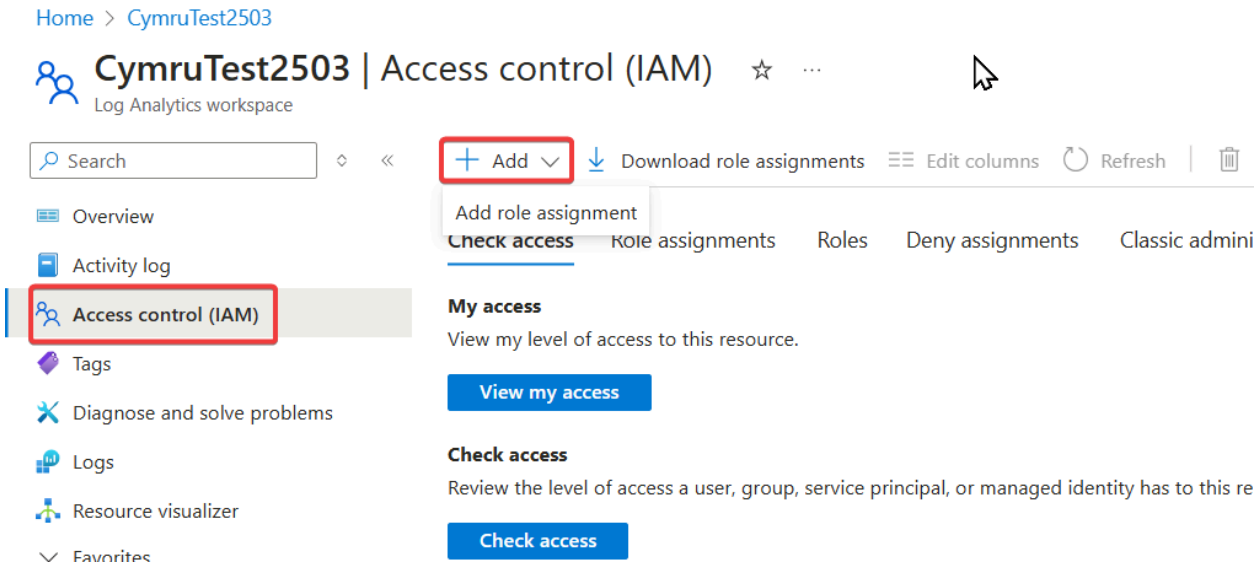


5. Click **Save** to store the authorized connection.
6. Similarly, authorize each connection.

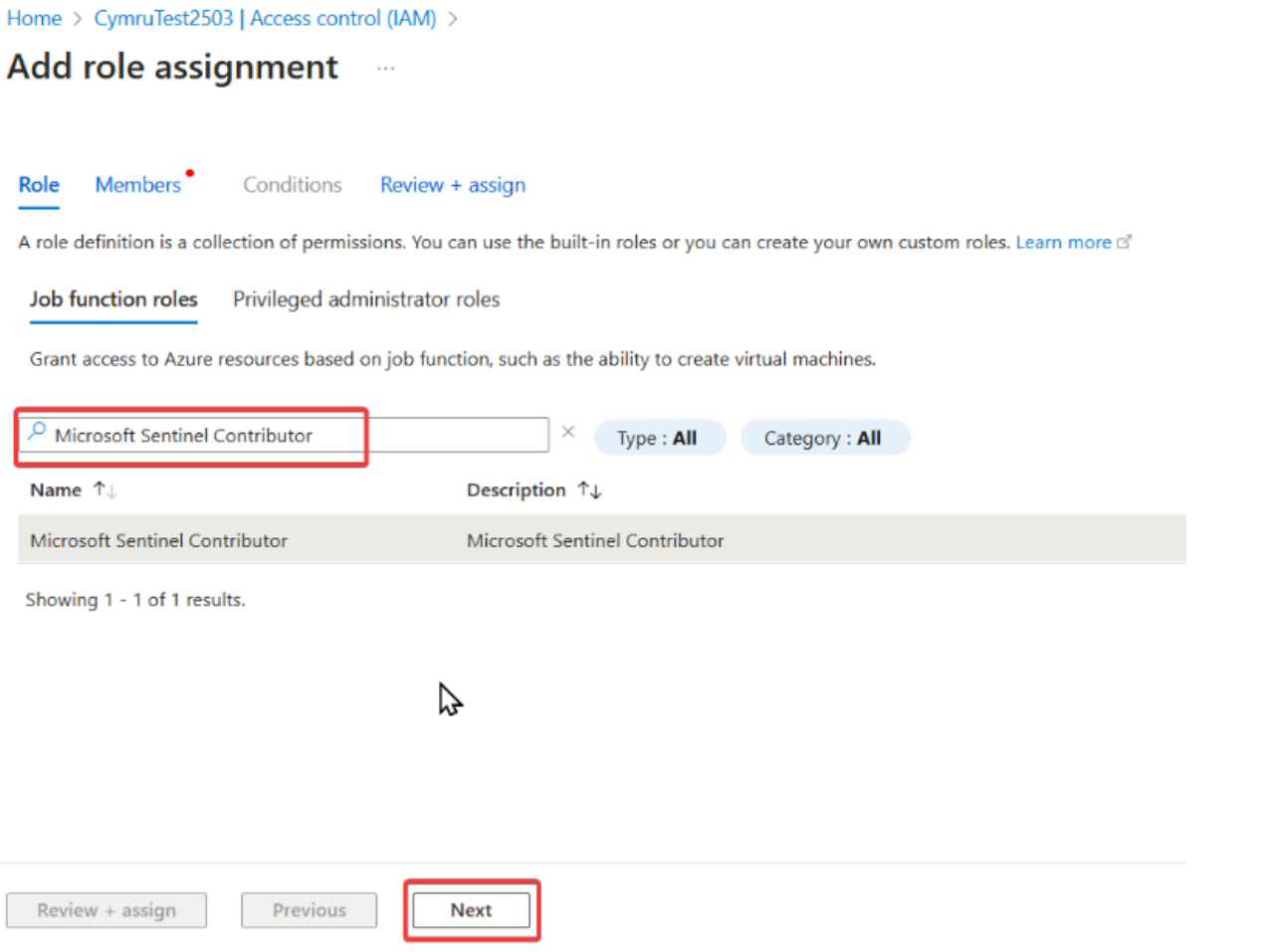
NOTE: You must authorize Outlook connection using your Outlook email ID only.

Assign Role to Add Comment in Incident

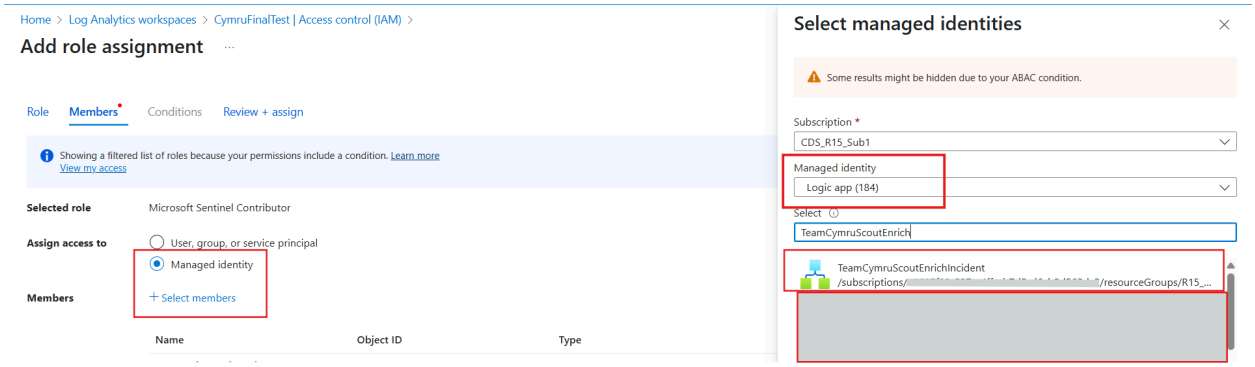
1. Navigate to **Log Analytics Workspace → {your workspace} → Access Control (IAM)**.
2. Click on **Add → Add role assignment**.



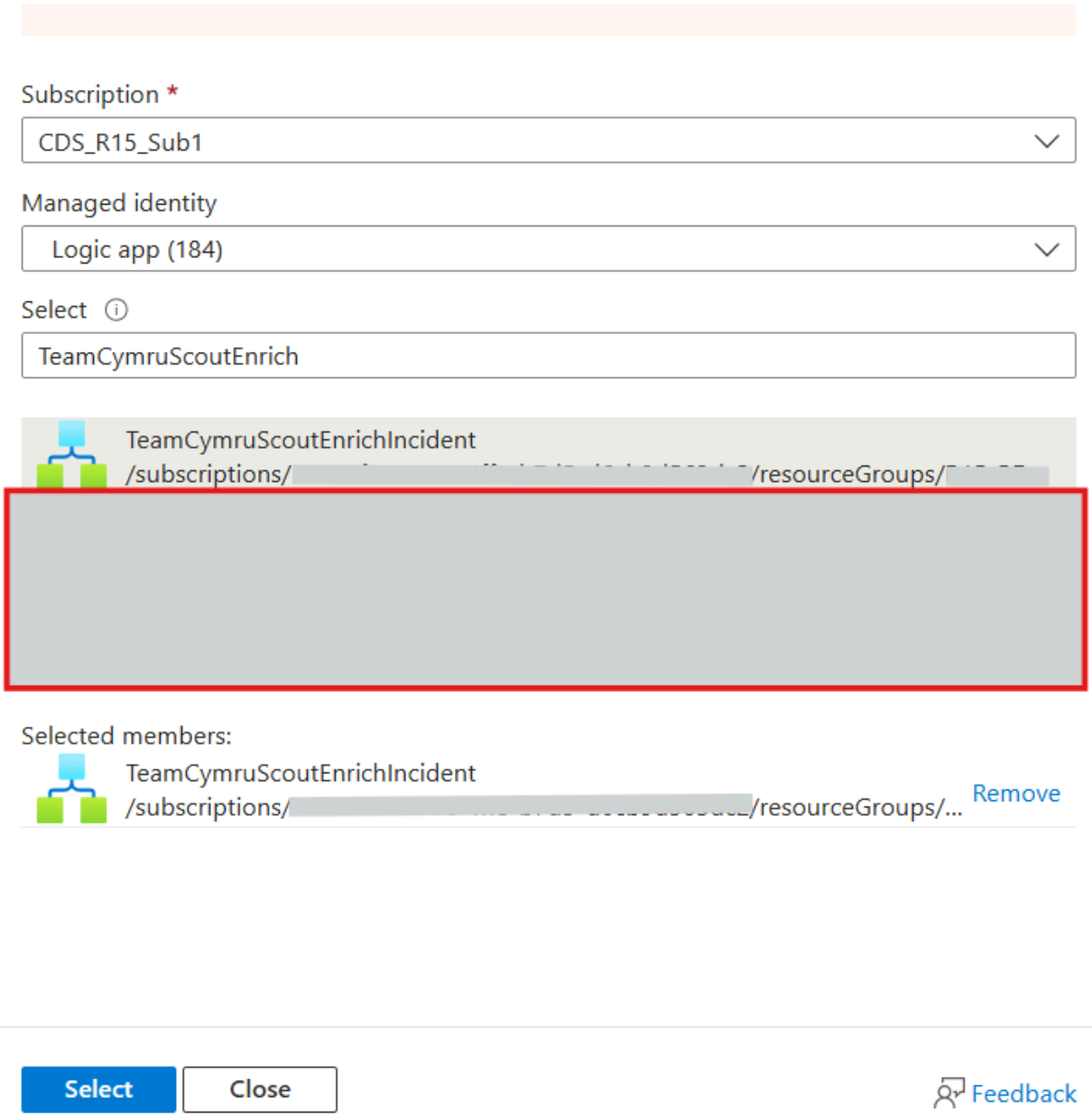
3. Under **Assignment type**, select **Job function roles**.
4. Search for **Microsoft Sentinel Contributor** and click **Next**.



5. In the **Members** section, choose **Managed identity** for assigned access.
6. Click **Select members**, then add your **Logic App** as a member.



7. Click **Review + Assign** to complete the process

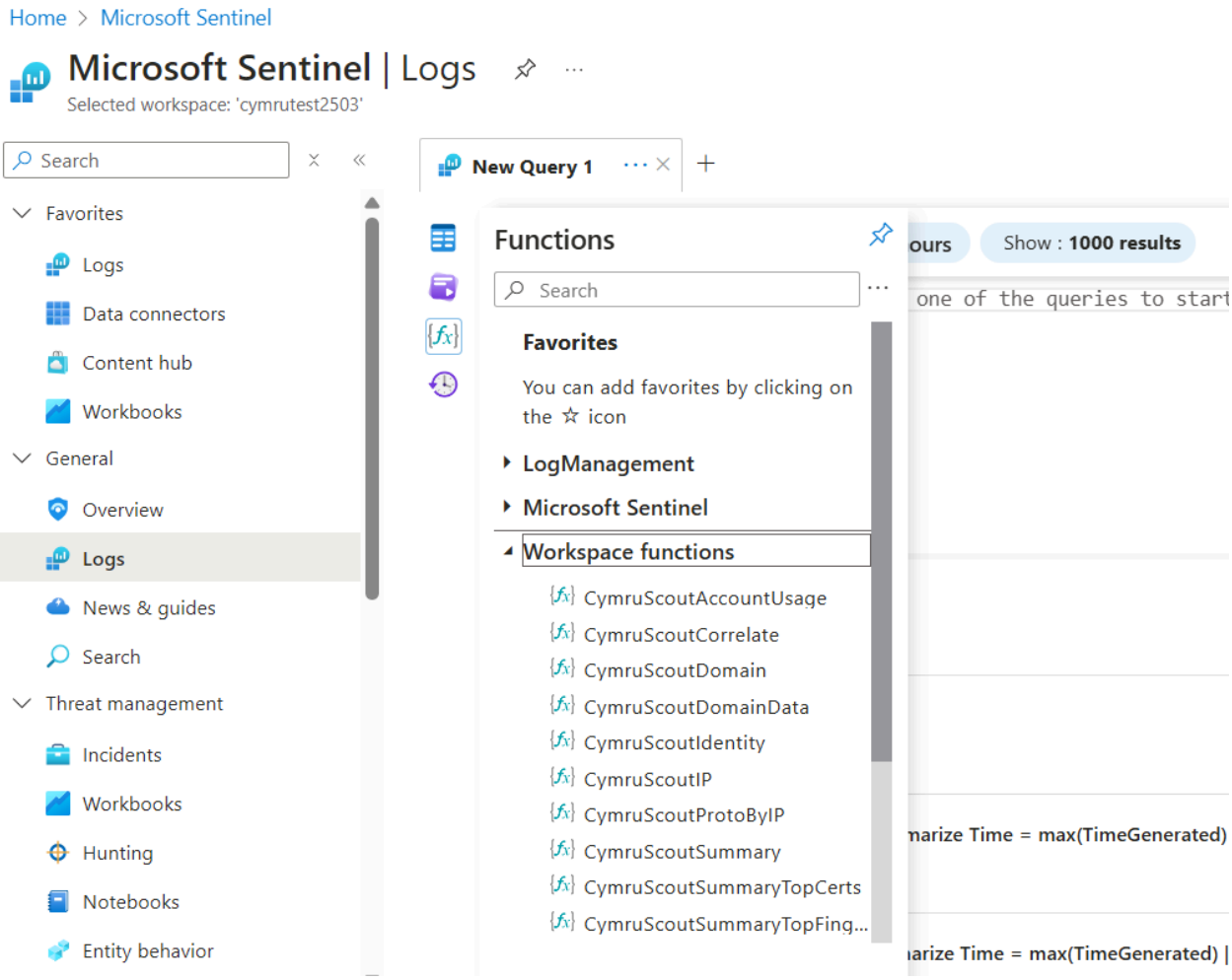


Steps to Configure the Team Cymru Scout Parsers

Usage

The **data connector** ingests scout **data** into **Microsoft Sentinel tables** within the **Log Analytics Workspace**. This **data** is then **visualized** in the **Workbook** using **KQL (Kusto Query Language)**. However, the **raw data** in the **table** requires **parsing** and **normalization** of fields before displaying those in the workbook. To achieve this, a **Kusto Function-based parser** is utilized. For **Team Cymru Scout**, it is essential that these **parsers** are available in the workspace.
Without these parsers, the **Workbook** will not be able to access the ingested data.

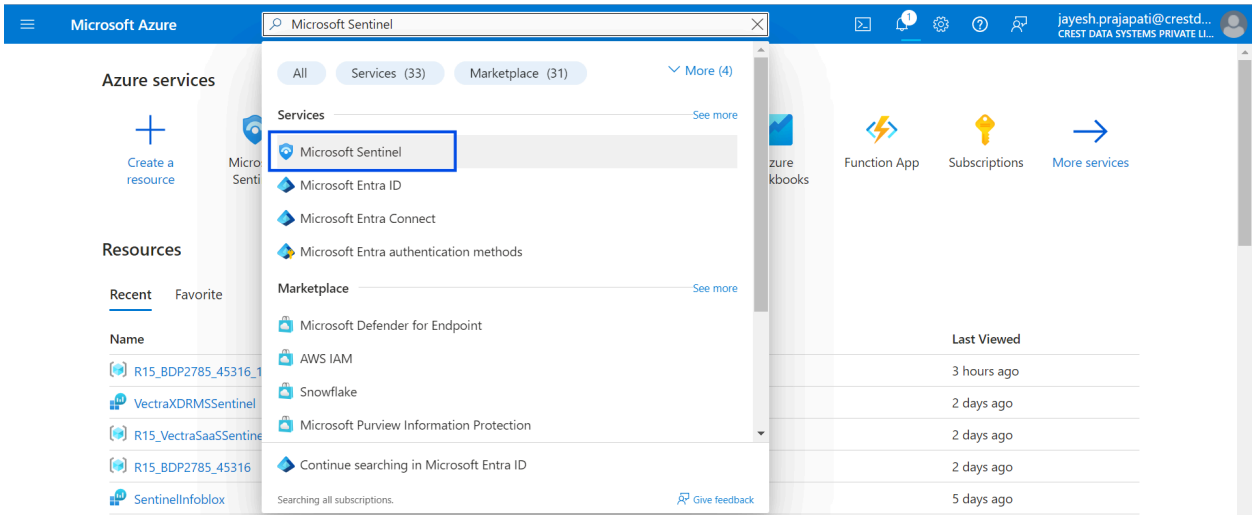
1. Once you install the **Team Cymru Scout** solution, the parsers are automatically installed to their correct location, so there is no need to install them separately.



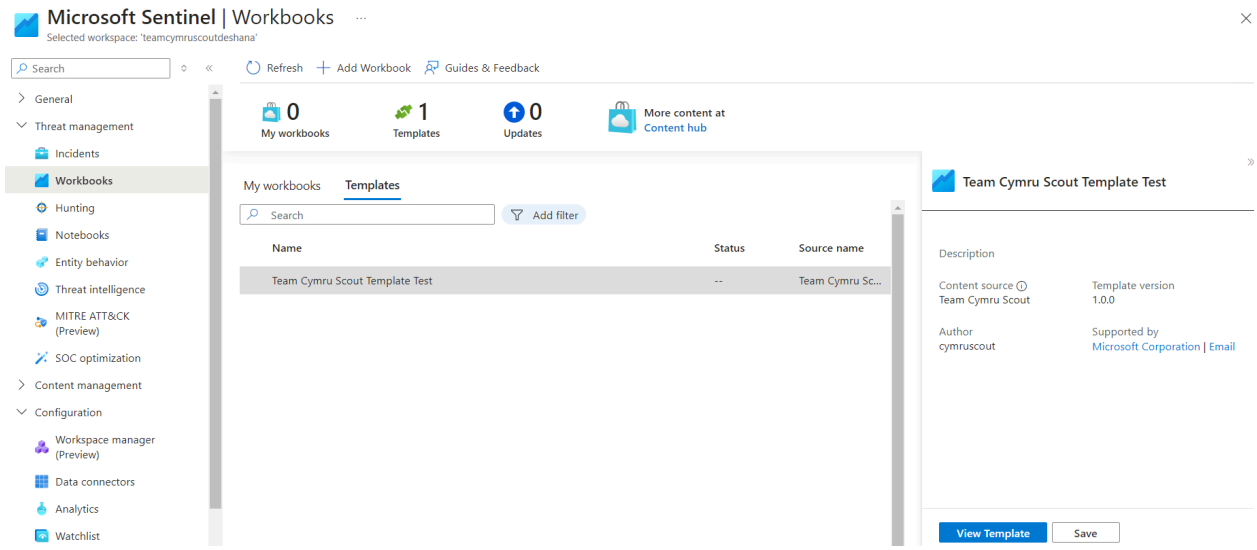
Steps to Configure the Team Cymru Scout Workbook (Dashboards)

Workbooks in Microsoft Sentinel provide a flexible canvas for data analysis and the creation of rich visual reports within the Microsoft Azure portal.

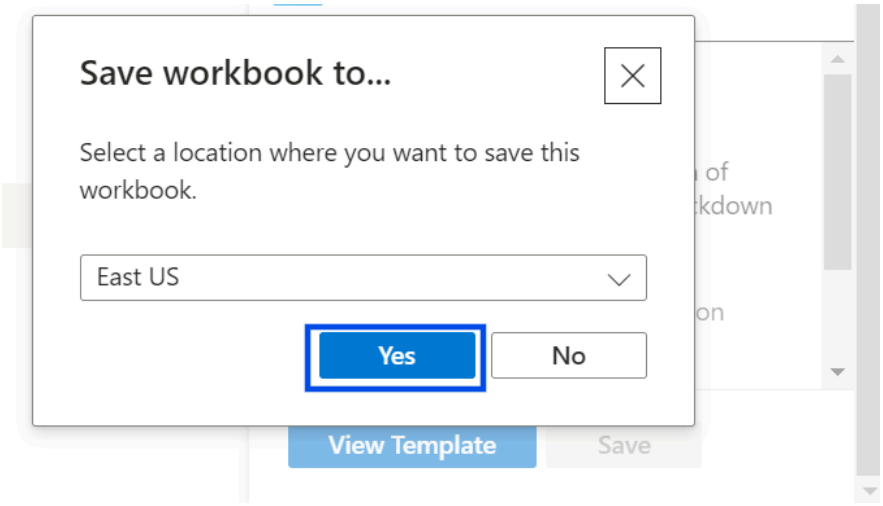
1. To install this workbook, start by navigating to the **Microsoft Sentinel** homepage:



2. Now go to Workspace in which you have installed the solution, go to **Workbooks**, go to template, search for **Team Cymru Scout** and click on the workbook that you want to install.
3. Click on **Save** button to save this workbook



4. Select the location of your Microsoft Sentinel Workspace and click on **Yes**.



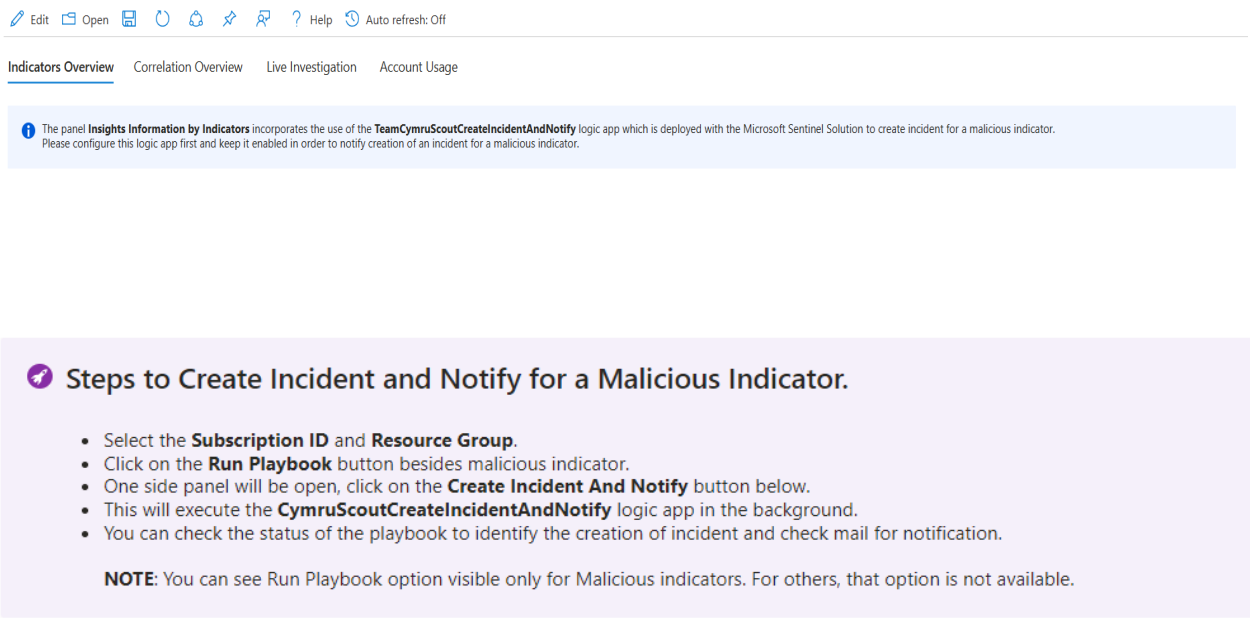
5. After successful completion, you will be able to see the “**View saved workbook**” button to see the configured workbook
   You can also now able to see workbook under the **“My workbooks”**

Indicator Overview

Usage

The **Indicator Overview Workbook** displays **indicator data** ingested via the **Data Connector** across multiple **panels**. Moreover, if an **IP is identified as malicious**, users can trigger the **Cymru Scout Create Incident and Notify Playbook** to **create an incident** in **MS Sentinel** and send a **notification email** to the user.

- Make sure that **CymruScoutCreateIncidentAndNotify Playbook** is configured to run it from Indicator Overview from **Insights Information by Indicators** Panel where overall rating of IP is malicious.
  NOTE: *To perform SOAR action from Indicator Overview, follow the steps mentioned in the Indicator Overview tab of the workbook.*



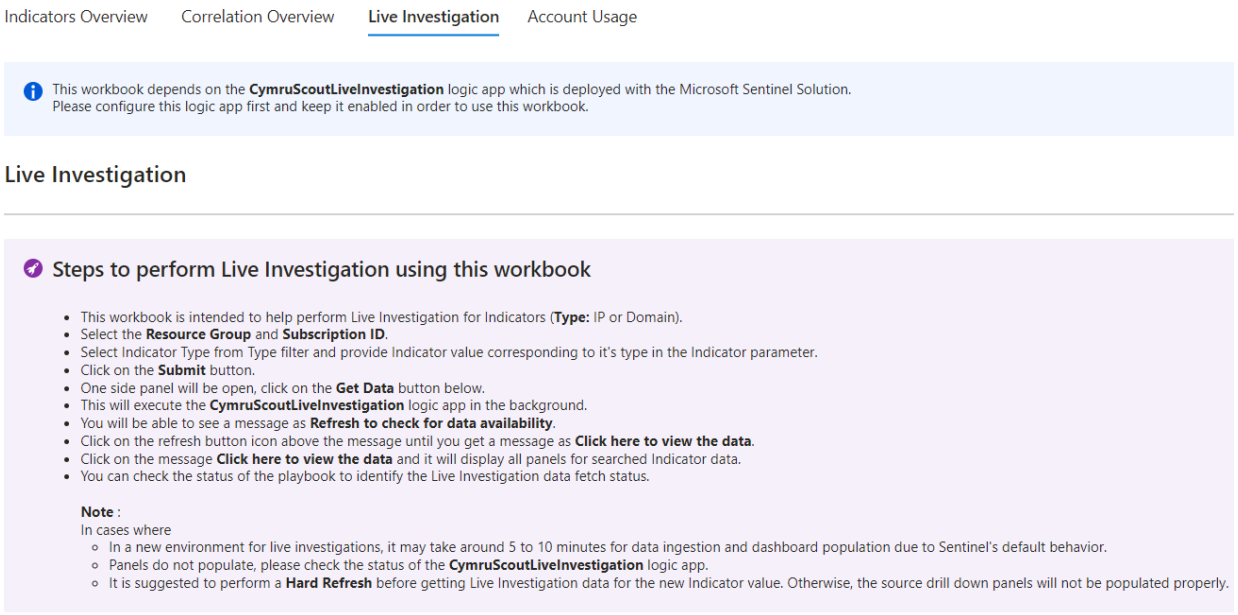
Live Investigation

Usage

The **Live Investigation Workbook** enables **on-demand investigation** of a specific **IP** or **Domain**, displaying the results across multiple **panels**. Users must enter specific **input parameters** given in the workbook, which then trigger the **Cymru Scout Live Investigation Playbook**. The **ingested data** from this **playbook** is subsequently **visualized** in various **panels**. Moreover, if the IP is found malicious in the live investigation, the **Cymru Scout Create Incident And Notify Playbook** will automatically be triggered from this workbook in order to create the incident in MS Sentinel and notify the user via email.

- Make sure that **TeamCymruScoutLiveInvestigation Playbook** is configured correctly.

  NOTE: *To perform Live Investigation, follow the steps mentioned in the Live Investigation tab of the workbook.*



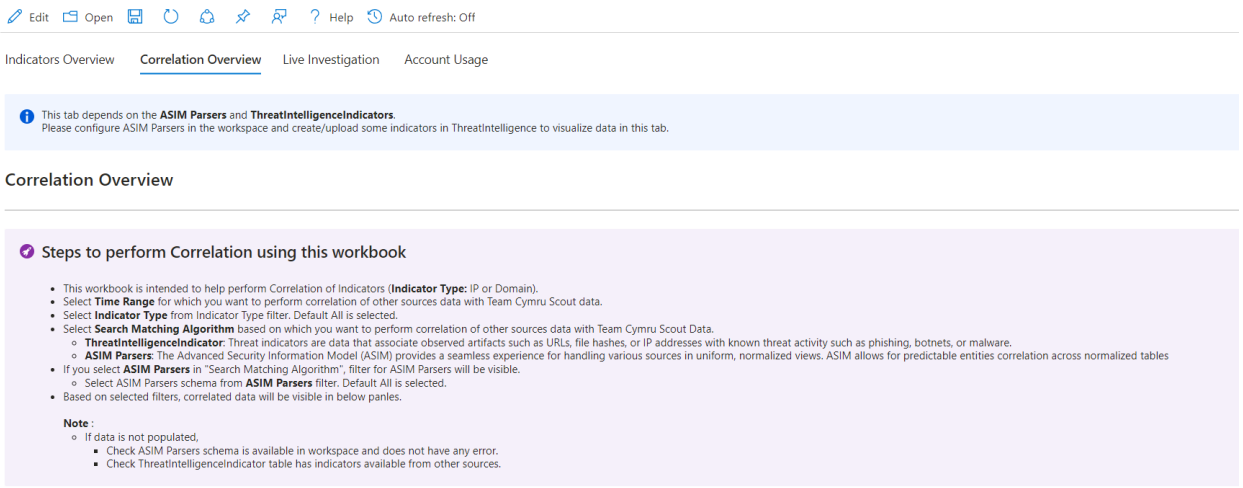
Usage

Correlation in **Microsoft Sentinel** means linking data from multiple sources to identify patterns, detect threats, and enhance security insights. By correlating logs, alerts, and threat intelligence, Sentinel helps in detecting complex attacks that might be missed in isolated data sources.

This workbook **correlates** IP and Domain data from ingested in the MS Sentinel table using the Scout API via the data connector, with the selected **ASIM Parser's schemas IP and Domain fields** and the **Threat Intelligence Indicator table's IP and Domain fields** to enhance detection and threat analysis.

- **ASIM Parser** (Advanced Security Information Model) normalizes security data across different sources, making it easier to query and analyze.
- **Threat Intelligence Indicator Table** stores threat data like malicious IPs, domains, and hashes, helping detect known threats in the environment.

- Make sure that **ASIM Parsers** are configured correctly in the workspace or **ThreatIntelligence indicators** are available.
  NOTE: *To perform Correlation of Other sources data with Team Cymru Scout data, follow the steps mentioned in the Correlation Overview tab of workbook.*

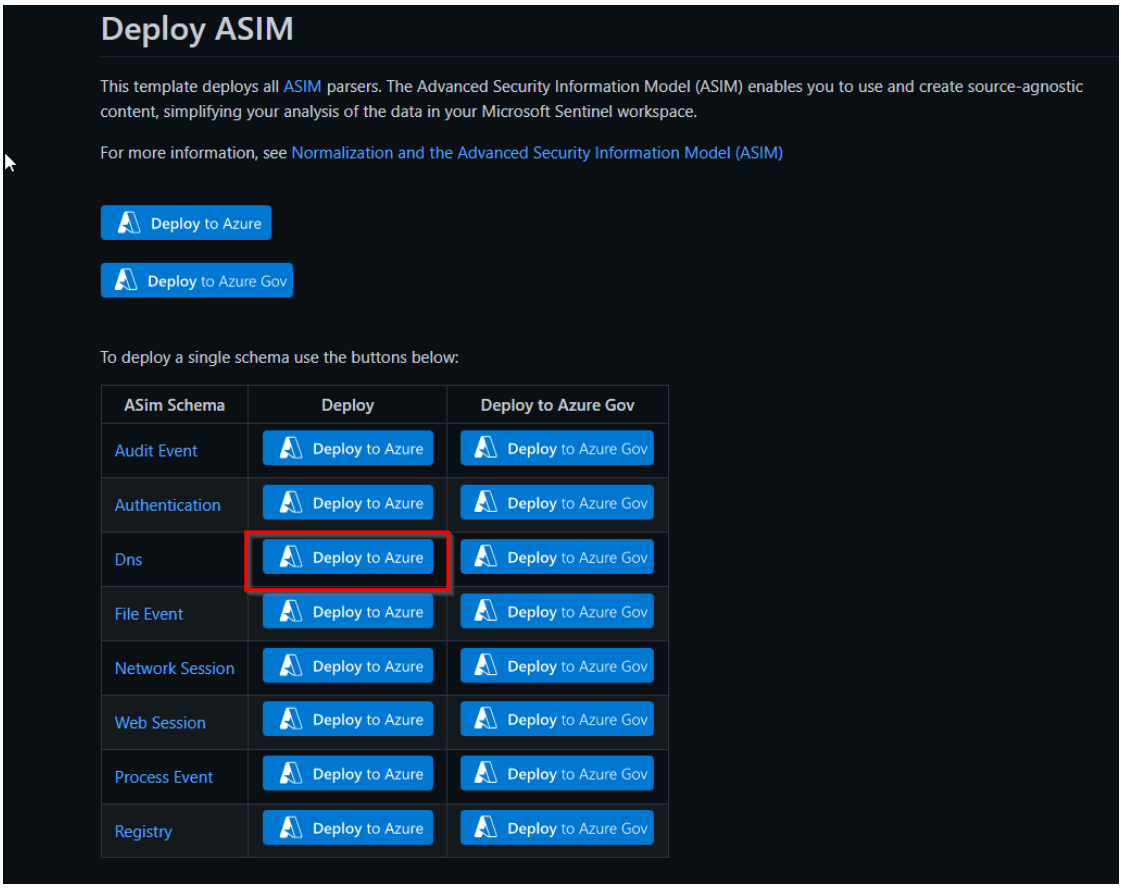


Steps to Deploy ASIM Parsers

In the Team Cymru Scout solution, we have used the ASIM Parsers in the **Correlation Overview Dashboard** for correlation with Team Cymru Scout data.

Follow these steps to deploy the ASIM Parser on Microsoft Sentinel Portal:

1. Go to https://github.com/Azure/Azure-Sentinel/tree/master/ASIM#deploy-asim
2. Click on **Deploy to Azure** for Dns Asim schema.

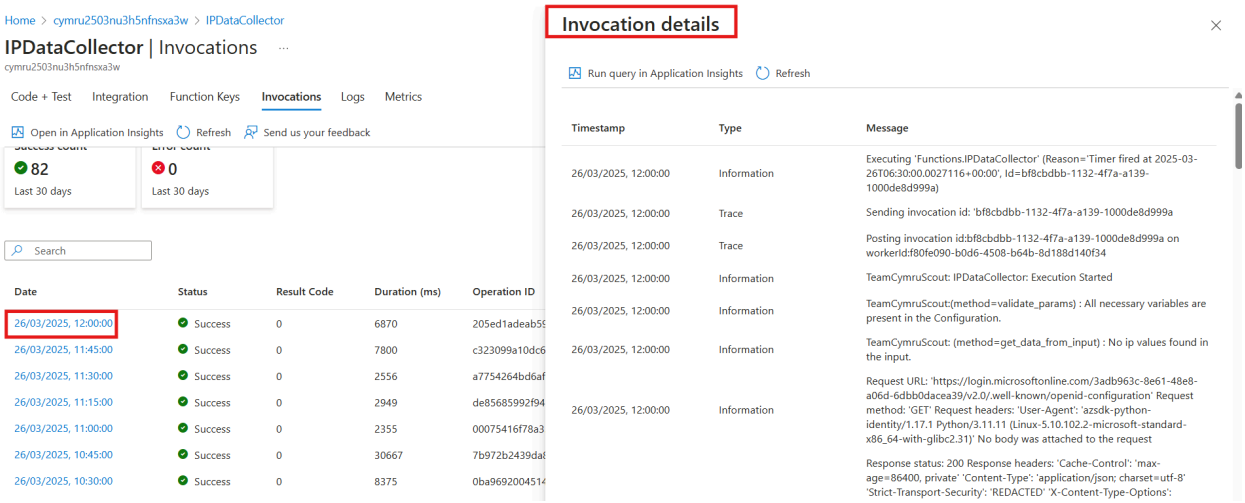


3. You will be redirected to the custom deployment page (same as other components) where you need to provide information including: **Resource Group**, **Region,** and Log **Analytic Workspace Name**.
4. Click on the **Review+Create** button.
5. Review the next dialog from Azure, and then click on **Create** to install the ASIM parser.
6. Similarly you need to deploy **WebSession, NetworkSession, DhcpEvent, AuditEvent,** and **Authentication parsers.**

Troubleshooting Steps

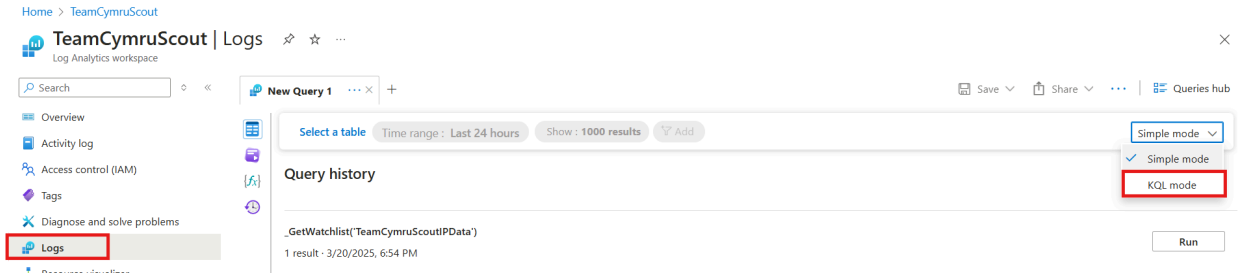
Steps to check invocation details of the function in Team Cymru Scout function app

1. Login to https://portal.azure.com .
2. Go to <your function app> → Functions → <FunctionName> → Invocations.
3. Click on the failed invocation to see the detailed logs.



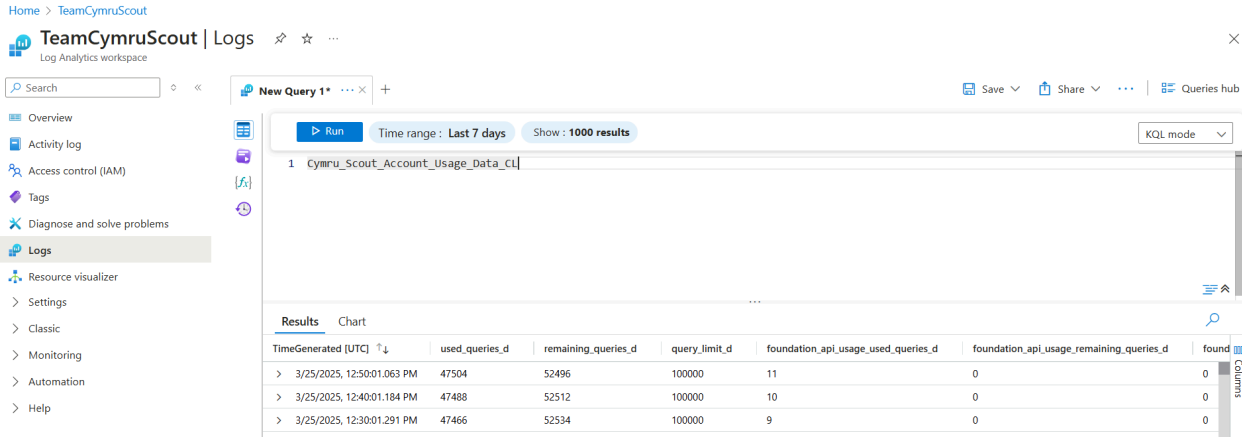
Steps to check the data in Log Analytic Workspace table

1. Go to Log Analytics Workspace → <your workspace>.
2. Go to Logs.
3. Change the mode from Simple mode to KQL mode.



4. Run the below KQL queries to verify that that data is available for that table or not.
    a. Cymru_Scout_Domain_Data_CL

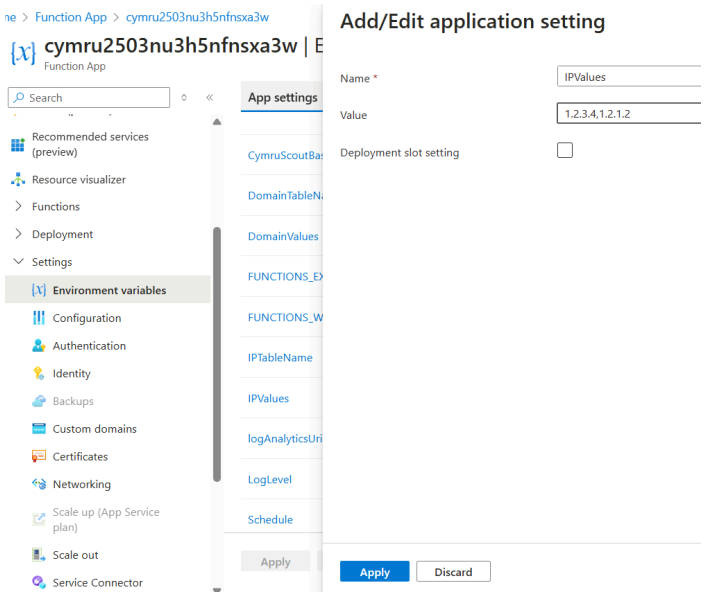
b. Cymru_Scout_IP_Data_Foundation_CL
    i. Data will be available in this table only if you have selected Foundation as **APIType** during Data Connector Configuration.
c. Cymru_Scout_IP_Data_Details_CL
    i. Data will be available in this table only if you have selected Details as **APIType** during Data Connector Configuration.
d. Cymru_Scout_Account_Usage_Data_CL



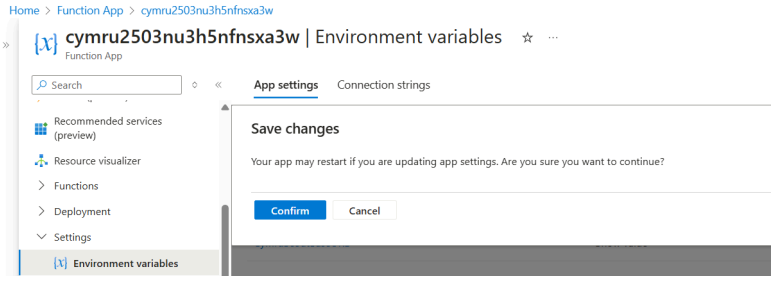
NOTE: If you have changed the table name while configuring the Data Connector, run the KQL query for that table.

Steps to verify or edit the environment variables of function app

1. Go to function apps → <function app>
2. Go to Environment variables under the Setting sections.
3. You can see the value of environment variables from here by clicking on Show value.
4. Check that values are provided in **any specific** variable.
5. To edit a particular variable,
    a. Click on the variable.
    b. Change the value.



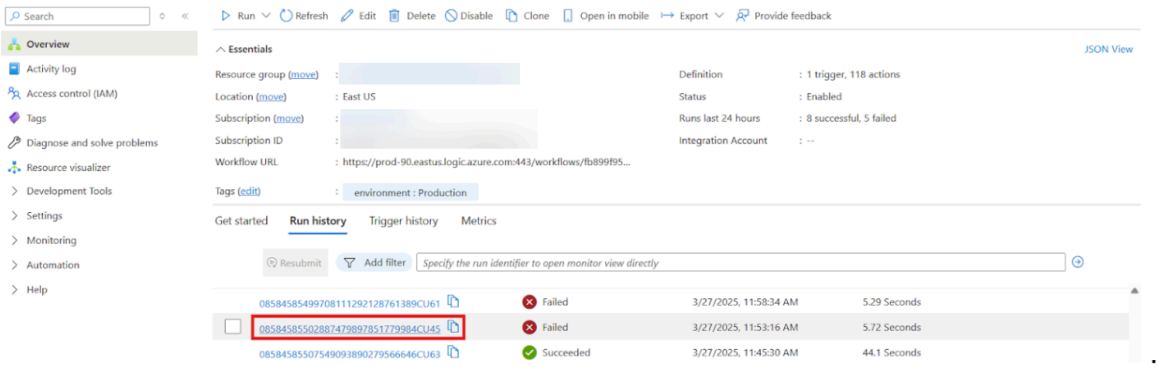
c. Click on Apply
d. Click on Apply at top to Save changes of all the variables.
e. Click on Confirm



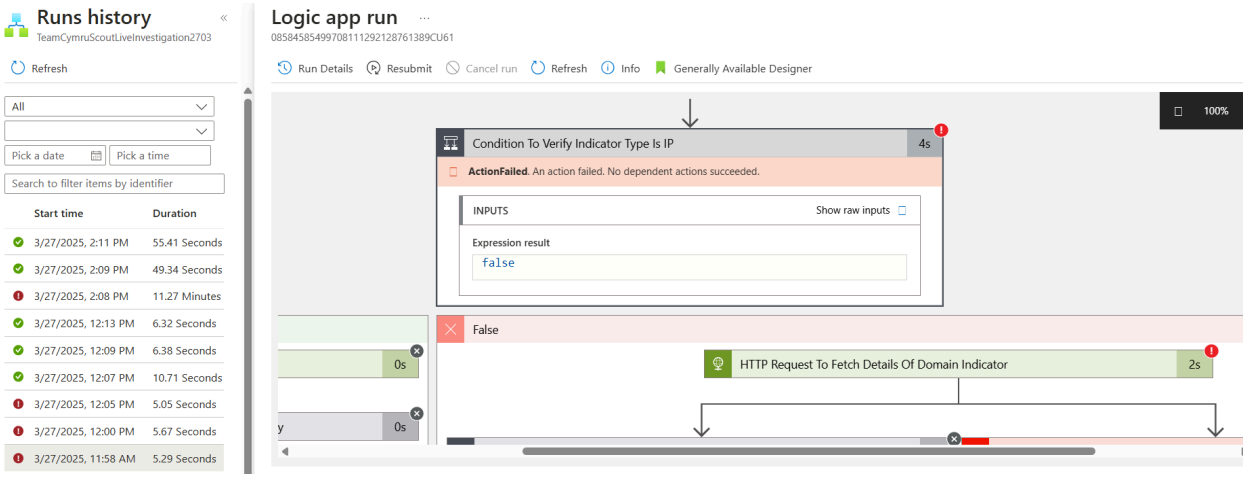
6. After editing any of the variables, you need to stop & start the function app to reflect the changes of the variables from next execution.

Steps to find the exact action where playbook execution failed

1. Go to Logic Apps → <your logic app>
2. In the Overview tab, Go to the Run history and select the failed execution.



3. Now, you can see the status of each action of that logic app for that invocation.
4. Find the action where it fails by checking the status of each action. You can identify the failed action by a red mark.



Case #1 - Indicators Overview Dashboard not showing data in any panel

Problem1: This can happen if inputs are provided for ip and domain neither in data connector configuration parameter nor in the watchlist.
Solution:

- Check the data connector configuration parameters by following the steps mentioned in the Steps to verify or edit the environment variables of function app.
- Verify that values are provided in **IPValues** and **DomainValues** are provided.

Problem2: The function app invocations logs are showing failed status.
Reason: The provided credentials in the data connector configuration are invalid.
Solution:

- Check the logs of function app invocation by following the step mentioned in Steps to check invocation details of the function in Team Cymru Scout function app:
    - If there are any failures related to **credentials**, use the previously provided steps to verify and update the credentials from the environment variables of the data connector.

Case #2 - The function app invocation logs are showing “No ip/domain values found for watchlist”

Problem1: This can occur if the data is added to the watchlist, but the Microsoft Entra ID application lacks the **Microsoft Sentinel Contributor** role at Resource Group level.
Solution:

- Follow the steps mentioned in the section, Assign Role of Contributor to application in Microsoft Entra ID

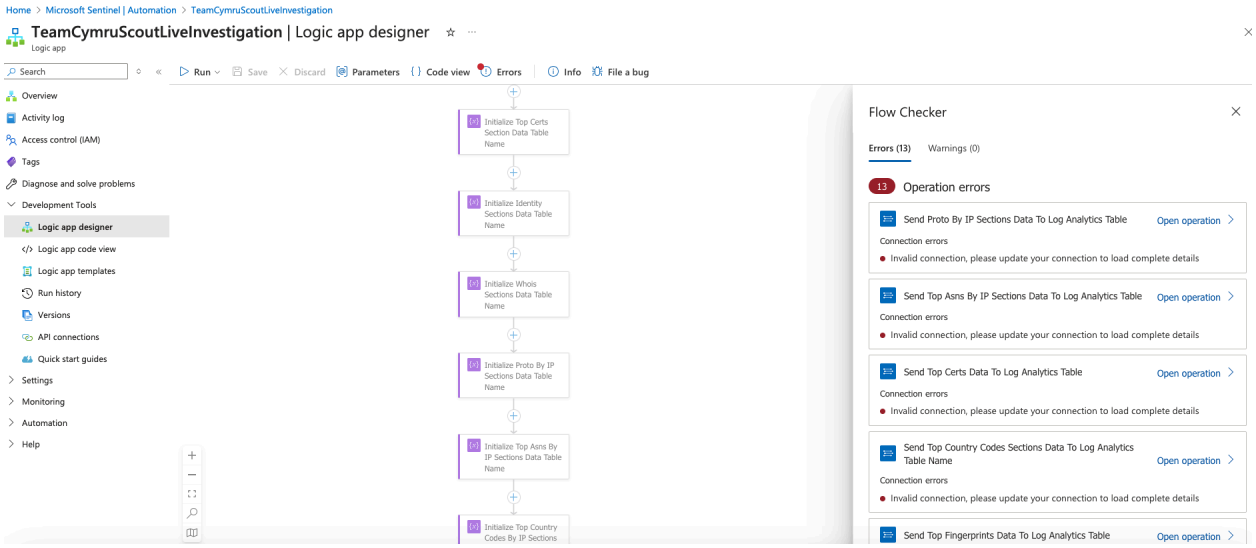
Case #3 -The Account Usage tab in the workbook does not immediately show the latest API usage count.

Problem1: This can occur because the default interval for the account usage function to retrieve data from the Scout API is set to **1 hour**.
Solution:

- To change the interval of the Account Usage function, follow the steps mentioned in this section Steps to verify or edit the environment variables of function app and update the cron expression in the **AccountUsageSchedule** parameter.
- Reference for cron expression: https://arminreiter.com/2017/02/azure-functions-time-trigger-cron-cheat-sheet/

Case #4 - Getting Connection error in the logic app

Problem1: While running the logic app, execution fails due to the connection error for any of the connections used in the logic app(except outlook email).



Reason: The user may not have followed the Authorized API Connections steps outlined in the playbook configuration.
Solution: Authorize required API Connections by following the steps mentioned in each playbook configuration steps.

- Authorize API Connection for Team Cymru Scout Live Investigation
- Authorize API Connection for Team Cymru Scout Create Incident And Notify

Case #5 - Getting Microsoft Outlook account connection error in TeamCymruScoutCreateIncidentAndNotify Logic app

Problem: User doesn't receive any notification via email related to malicious ip and logic app showcased the connection error for **Send an Email.**
Reason: Users have not authorized API connection **"Outlook-TeamCymruScoutCreateIncidentAndNotify"** using outlook email.
Solution: Create an outlook email account and authorize API Connection **"Outlook-TeamCymruScoutCreateIncidentAndNotify"** using the outlook email.

Case #6 - On the Indicators Overview tab in the workbook, the logic app to create incident from malicious ip was showing error while creating the incident

Problem: This logic app creates an incident for malicious ips found. For that, the logic app is missing the required role to create an incident in Microsoft Sentinel.
Solution:

- Follow the steps mentioned above to Assign Role to add comment in incident

Case #7 - The Live Investigation tab of workbook not populating data in panels

Reason: The live investigation dashboard provides detailed live investigation information for provided ip or domain. Initially, it may take some time to store data in various tables and populate the dashboard, aligning with Microsoft Sentinel's behavior. Even if the tables are already created—indicating that the live investigation has been performed—it still takes approximately 3-5 minutes to complete the playbook execution in the backend and populate the data in the workbook.

Problem2: The dashboard takes too long to populate the data and the playbooks are failing.

Solution:

- Follow the steps mentioned in Steps to find the exact action where playbook execution failed to identify the reason of failure for logic app.

Case #8 - The Data Connector showing the Not Connected status on the data connector UI page

Problem1: The data connector UI page will show **Connected** status only if there is any data available in the tables and the table names provided in the Data Connector configuration page are the same as written on the UI page.

Solution:

- Check function app invocation logs by following the steps mentioned in Steps to check invocation details of the function in Team Cymru Scout function app: to identify that the function app execution is successful or failed.
- To verify the data ingestion in the table, follow the steps mentioned in the section Steps to check the data in Log Analytic Workspace table

Case #9 - The Correlation Overview dashboard not populating data in any panel

Problem1: The Correlation Overview dashboard is not populating data in any panel, even after selecting the ASIM Parsers for the **Search Matching Algorithm** parameter.

Solution:

- Check that ASIM parsers are installed in the workspace by following the staps mentioned in the section Steps to Deploy ASIM Parsers.

- Since this dashboard provides correlation of Team Cymru Scout data with other data sources, data will only be populated if the selected ASIM parser data fields match the Scout API data, even if the ASIM parser is configured.

Problem2: The correlation overview dashboard is not populating data in any panel even after selecting the ThreatIntelligenceIndicator for the **Search Matching Algorithm** parameter.

Solution:

- Since this dashboard provides correlation of Team Cymru Scout data with other data sources, data will only be populated if data is available in ThreatIntelligenceIndicator and data matches with the Scout API data.