



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

Contents

Contents	2
Prerequisites	4
Steps to Install the Team Cymru Scout MS Sentinel Integration	5
Steps to Install the Team Cymru Scout Data Connector	10
Usage	10
Prerequisites	10
App Registration steps for the Application in Microsoft Entra ID	10
Add a client secret for application in Microsoft Entra ID	11
Assign role of Microsoft Sentinel Contributor to application in Microsoft Entra ID	12
Upload Indicators csv in Watchlists to get data related to ip/domain from Team Cymru Scout	13
Configuration of Data Connector	15
Steps to Configure Playbook (Logic Apps)	22
Cymru Scout Create Incident And Notify Playbook	22
Usage	22
Configuration	22
Authorize API Connection	27
Assign Role to Add Comment in Incident	30
Cymru Scout Live Investigation Playbook	33
Usage	33
Configuration	33
Authorize API Connection	36
Steps to Configure the Team Cymru Scout Parsers	37
Usage	37
Steps to Configure the Team Cymru Scout Workbook (Dashboards)	39
Indicator Overview	41
Usage	41
Live Investigation	42
Usage	42
Correlation Overview	43
Usage	43
Steps to Deploy ASIM Parsers	44
Troubleshooting Steps	45
Steps to check invocation details of the function in Team Cymru Scout function app	45
Steps to check the data in Log Analytic Workspace table	45
Steps to verify or edit the environment variables of function app	46
Steps to find the exact action where playbook execution failed	47

Case #1 - Indicators Overview Dashboard not showing data in any panel	48
Case #2 - The function app invocation logs are showing “No ip/domain values found for watchlist”	48
Case #3 -The Account Usage tab in the workbook does not immediately show the latest API usage count.	48
Case #4 - Getting Connection error in the logic app	49
Case #5 - Getting Microsoft Outlook account connection error in TeamCymruScoutCreateIncidentAndNotify Logic app	49
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	49
Case #7 - The Live Investigation tab of workbook not populating data in panels	50
Case #8 - The Data Connector showing the Not Connected status on the data connector UI page	50
Case #9 - The Correlation Overview dashboard not populating data in any panel	50

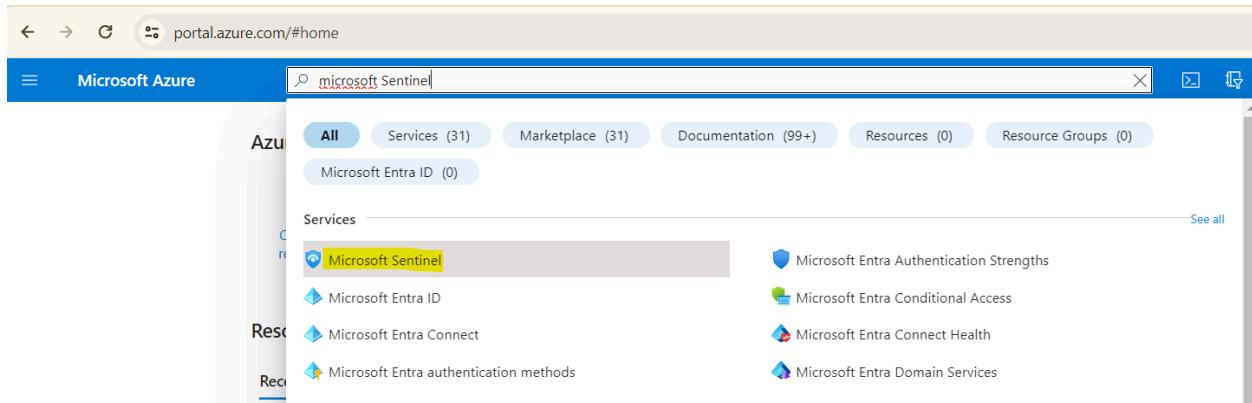
Prerequisites

The following requirements are essential for configuring all components:

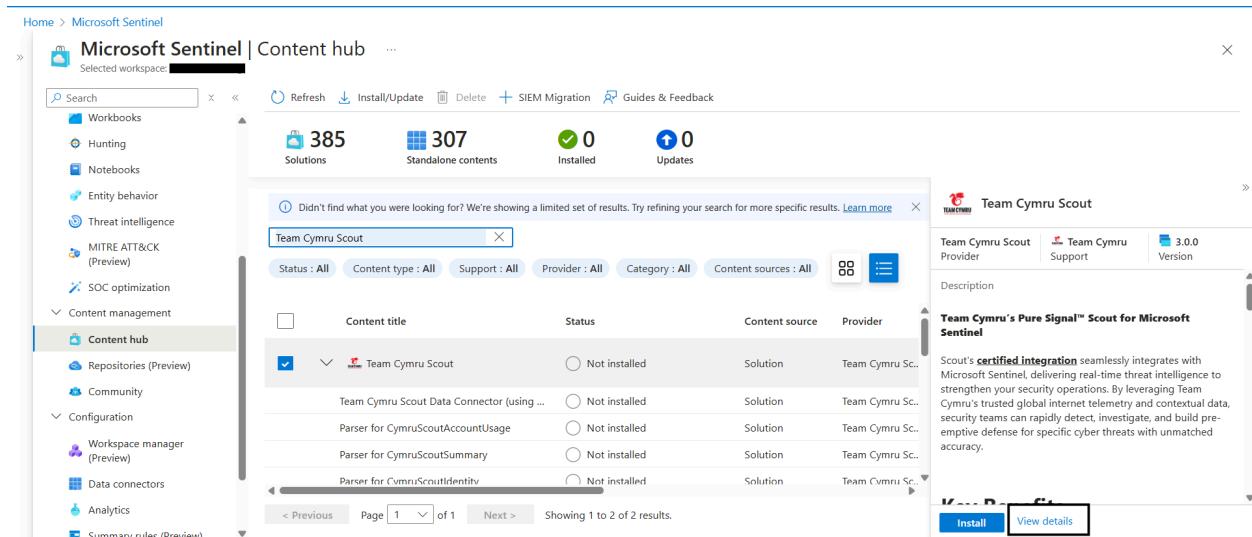
- Azure Account with subscription
- Resource Group
 - This requires **Microsoft Sentinel Contributor Role at Subscription Level**
- Microsoft EntraID Application
 - The Azure account user must have an **Application Developer or Application Owner** role at subscription level to create Microsoft EntraID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

Steps to Install the Team Cymru Scout MS Sentinel Integration

1. Login to the azure portal(<https://portal.azure.com/#home>), search for Microsoft Sentinel in the search bar and select Microsoft Sentinel service.



2. Now select your workspace and then go to **Content Hub** and search for Team Cymru Scout. After finding the solution **click on it** and **click on view details**.



3. After clicking on View Details you will see the screen like the image below. Click on the Create button.

[Home](#) > [Microsoft Sentinel | Content hub](#) >

Team Cymru Scout for Microsoft Sentinel

Team Cymru



...



Team Cymru Scout for Microsoft Sentinel

[Add to Favorites](#)

Team Cymru | Azure Application

Plan

Team Cymru Scout for Microsoft Sent...

Create

Overview

Plans

Usage Information + Support

Ratings + Reviews

4. Fill in the details of the workspace and resource group then click on **Review + Create**.

Create Team Cymru Scout for Microsoft Sentinel ...

- There may be [known issues](#) pertaining to this Solution, please refer to them before installing.

Team Cymru Scout brings the most advanced AI-powered real-time intelligence into Microsoft Sentinel. The Microsoft Sentinel Integration allows you to perform LiveInvestigation on Indicators like IP, Domain and perform Correlation of Team Cymru Scout Data with Other Sources. It also leverage the capability to generate incident and notify when malicious ip found.

Data Connectors: 1, **Parsers:** 17, **Workbooks:** 1, **Watchlists:** 2, **Playbooks:** 2

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="CDS_R15_Sub1"/>
Resource group *	<input type="text" value="████████████████"/> Create new

Instance details

Workspace *	<input type="text" value="████████"/>
-------------	---------------------------------------

[Previous](#)

[Next](#)

Review + create

5. Then click on the **Create** button.

Create Team Cymru Scout for Microsoft Sentinel

...

policy

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Preferred e-mail address

Preferred phone number

Basics

Subscription

CDS_R15_Sub1

Resource group

[REDACTED]

Workspace

[REDACTED]

[Previous](#)

[Next](#)

[Create](#)

6. It will install the solution into the Microsoft Sentinel.

Home >



team-cymru.teamcymruscout_sentinel-20250407145927 | Overview

...

Deployment

Search X <>

Delete Cancel Redeploy Download Refresh

Overview Inputs Outputs Template

Your deployment is complete

Deployment name : team-cymru.teamcymruscout_sentinel-202504071459... Start time : [REDACTED]
Subscription : CDS_R15_Sub1 Correlation ID : 94163782-afc1-446c-bc77-e7cca7ef2537
Resource group : [REDACTED]

Deployment details

Next steps

Go to resource group

7. Go to Microsoft Sentinel, then go to **Content Hub**, and search for the solution that you have installed and click on **Manage**.

The screenshot shows the Microsoft Sentinel Content hub interface. On the left, there's a navigation sidebar with options like Threat management, Content hub (which is selected and highlighted in blue), and Configuration. The main area displays statistics: 385 Solutions, 307 Standalone contents, 1 Installed, and 0 Updates. A search bar at the top has 'Team Cymru Scout' typed into it. Below the search bar, there are filters for Status (All), Content type (All), Support (All), Provider (All), Category (All), and Content sources (All). A table lists two results: 'Team Cymru Scout' (Status: Installed, Provider: Team Cymru Scout) and 'Microsoft Teams' (Status: Not installed, Provider: Microsoft). To the right of the table is a detailed description of the integration, mentioning its certified integration with Microsoft Sentinel and its ability to deliver real-time threat intelligence. At the bottom right of the table area is a 'Manage' button.

8. After clicking on manage you can see the list of components associated with this integration.

This screenshot shows the 'Team Cymru Scout' integration details page. At the top, it displays '21 Installed content items' and '3 Configuration needed'. Below this, there's a summary section with the provider information: Team Cymru Scout (Provider), Team Cymru Support (Support), and Version 3.0.0. A 'Description' section contains the text: 'Scout's certified integration seamlessly integrates with Microsoft Sentinel, delivering real-time threat intelligence to strengthen your security operations. By leveraging Team Cymru's trusted global internet telemetry and contextual data, security teams can rapidly detect, investigate, and build pre-emptive defense for specific cyber threats with unmatched accuracy.' A 'Key Benefits' section is also present. On the right side, there's a large list of installed content items, each with a preview icon, a name, and a status indicating '1 item'. The list includes: Team Cymru Scout Data Connector (using Azure Functions), Parser for CymruScoutAccountUsage, Parser for CymruScoutCorrelate, Parser for CymruScoutDomain, Parser for CymruScoutDomainData, Parser for CymruScoutIdentity, Parser for CymruScoutIP, Parser for CymruScoutProtoByIP, Parser for CymruScoutSummary, and Parser for CymruScoutSummaryTopCerts.

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.

The screenshot shows the Azure portal's 'Certificates & secrets' page for an app registration. The left sidebar has a 'Certificates & secrets' item highlighted with a red box. In the main content area, there's a 'Client secrets' tab also highlighted with a red box. Below it, a table lists a single client secret named 'MSSentinel'. The 'Add' button at the bottom right of the table is also highlighted with a red box.

- 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.

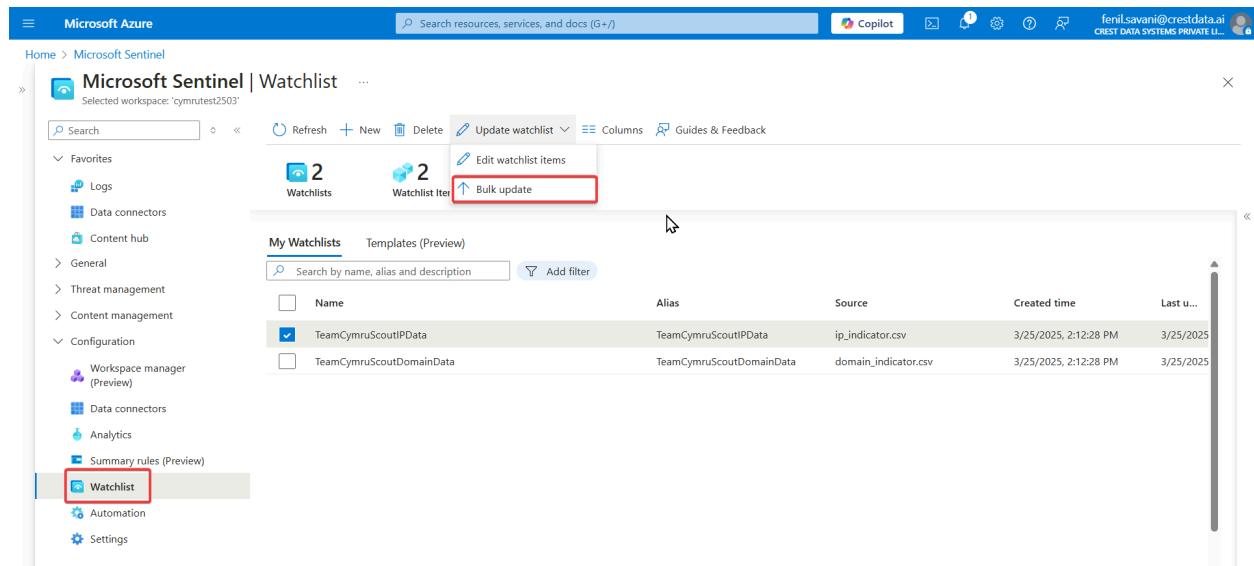
Reference link:

<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:

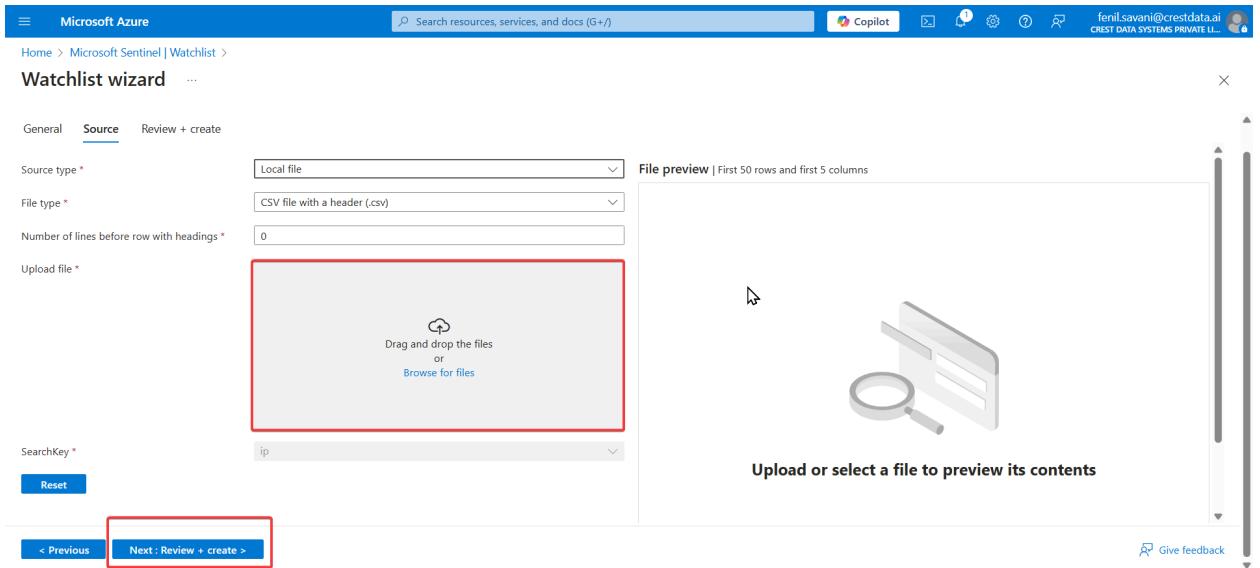
- In the Azure portal, Go to **Microsoft Sentinel** and select your workspace.
- Go to **Watchlist** under the Configuration section from the left panel.
- Click on **TeamCymruScoutDomainData**, and then select **Bulk update** from **Update watchlist**



The screenshot shows the Microsoft Sentinel Watchlist interface. On the left sidebar, the 'Watchlist' item is selected and highlighted with a red box. In the main content area, there is a 'Bulk update' button highlighted with a red box. A tooltip above the button says 'Edit watchlist items'. Below the button, a table lists two watchlists: 'TeamCymruScoutIPData' and 'TeamCymruScoutDomainData'. The table columns include Name, Alias, Source, Created time, and Last u... . The 'TeamCymruScoutIPData' row has a checked checkbox in the Name column.

Name	Alias	Source	Created time	Last u...
<input checked="" type="checkbox"/> TeamCymruScoutIPData	TeamCymruScoutIPData	ip_indicator.csv	3/25/2025, 2:12:28 PM	3/25/2025
<input type="checkbox"/> TeamCymruScoutDomainData	TeamCymruScoutDomainData	domain_indicator.csv	3/25/2025, 2:12:28 PM	3/25/2025

- 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 watchlist](#)

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**.

The screenshot shows the Microsoft Sentinel Data connectors page. On the left, there's a navigation sidebar with sections like Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management (Content hub, Repositories (Preview), Community), Configuration (Workspace manager (Preview), Data connectors), Analytics, Summary rules (Preview), Watchlist, Automation, and The 'Data connectors' item is highlighted with a red box. The main area displays a summary of connectors: 1 Connected (Team Cymru Scout) and 1 More content at Content Hub. Below this, a table lists the 'Team Cymru Scout Data Connector (using Azure Functions)' with details: Provider: Team Cymru Scout, Data Types: All, Status: Connected (1). To the right, a detailed view of the connector is shown with tabs for Status, Connector name, and The Status tab shows 'Connected' status, 'Team Cymru... Provider', and '8 Minutes A Last Log Receive'. The Connector name tab shows 'Team Cymru Scout Data Connector (using Azure Functions)' and 'Team Cymru Scout'. The 'Open connector page' button is highlighted with a red box.

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

The screenshot shows the 'Team Cymru Scout Data Connector (using Azure Functions)' page. The left side contains basic information: Connected Status (Team Cymru Scout), Last data received (3/25/2025, 6:30:05 PM), Content source (Team Cymru Scout), Version (1.0.0), Author (Team Cymru), and Related content (1 Workbooks, 14 Queries, 0 Analytics rules templates). The right side has a 'STEP 6 - Choose ONE from the following two deployment options to deploy the connector and the associated Azure Function' section. It includes fields for Workspace ID and Primary Key. Below this, 'Option 1 - Azure Resource Manager (ARM) Template' is described with steps: 1. Click the Deploy to Azure button below, and 2. Select the preferred Subscription, Resource Group and Location. The 'Deploy to Azure' button is highlighted with a red box.

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

[Home >](#)

Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

[Basics](#) [Review + create](#)

Template



Customized template ↗

8 resources



Edit template



Edit parameters



Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

[Create new](#)

Instance details

Region * ⓘ

Function Name

Cymru Scout Base URL * ⓘ

[Previous](#)

[Next](#)

[Review + create](#)

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.
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.
Workspace ID	Provide Workspace ID of your log analytics workspace (Provide the same workspace where you have installed the solution)
Workspace Key	Provide Workspace Key of your log analytics workspace (Provide the same workspace where you have installed the solution)
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}'

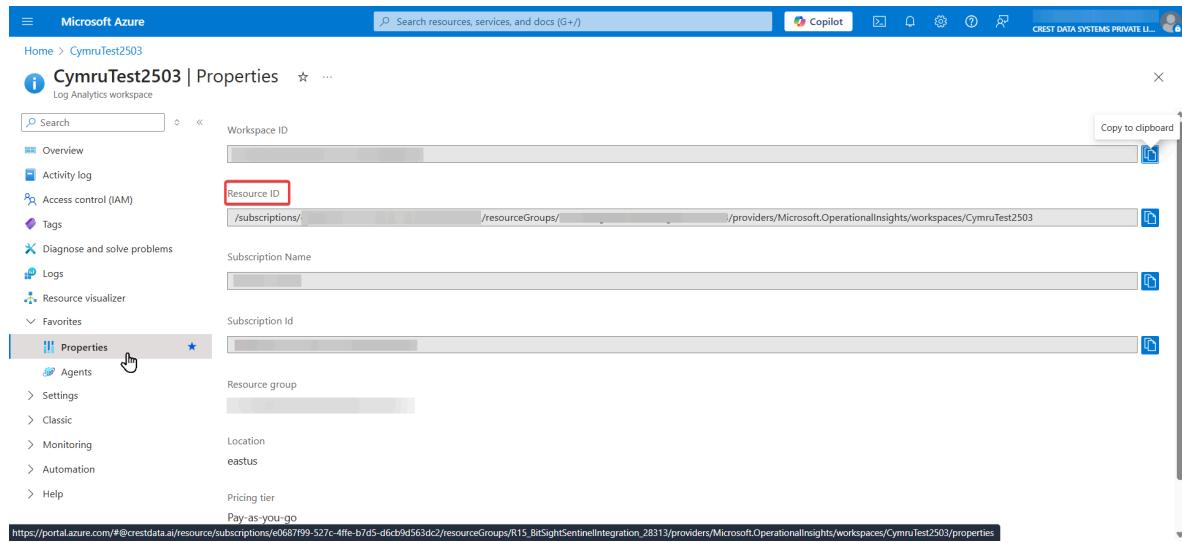
You can find **Workspace ID** and **Workspace Key** in the **Data Connector** page itself.

The screenshot shows the Microsoft Sentinel Data Connectors page. The URL is [Home > Microsoft Sentinel | Content hub > Team Cymru Scout > Data connectors > Team Cymru Scout Data Connector \(using Azure Functions\)](#). The connector details are as follows:

- Name:** Team Cymru Scout Data Connector (using Azure Functions)
- Status:** Connected
- Last Log Received:** 14 Minutes Ago
- Description:** The TeamCymruScout Data Connector allows users to bring Team Cymru Scout IP, domain and account usage data in Microsoft Sentinel for enrichment.
- Last data received:** 3/25/2025, 6:30:05 PM
- Content source:** Team Cymru Scout
- Version:** 1.0.0
- Author:** Team Cymru
- Supported by:** Team Cymru | Email
- Related content:** None

On the right side, there is a deployment section titled "STEP 6 - Choose ONE from the following two deployment options to deploy the connector and the associated A". It includes fields for "Workspace ID" and "Primary Key", both of which are highlighted with red boxes. Below these fields, there is an "Option 1 - Azure Resource Manager (ARM) Template" section with a "Deploy to Azure" button.

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



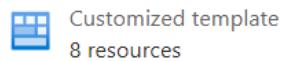
The screenshot shows the 'Properties' section of a Log Analytics workspace named 'CymruTest2503'. The 'Resource ID' field is highlighted with a red box. The URL at the bottom of the page is: https://portal.azure.com/#@crestdata.ai/resource/subscriptions/e0687f99-527c-4ffe-b7d5-d6cb9d563dc2/resourceGroups/R15_BitSightSentinelIntegration_28313/providers/Microsoft.OperationalInsights/workspaces/CymruTest2503/properties



The screenshot shows the 'Review + create' step of a custom deployment. It includes sections for 'Summary' (Customized template, 8 resources), 'Terms' (Azure Marketplace Terms, Azure Marketplace), legal terms, and deployment notes. At the bottom are 'Previous' and 'Next' buttons, and a large 'Create' button.

Basics Review + create

Summary



Terms

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the [Azure Marketplace](#); both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

Previous

Next

Create

- Click **Create** to install the **Data Connector**.
- After that, you will be able to see the deployment status, as shown in the image below.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "Microsoft.Template-20240717154512". The status is "Your deployment is complete". Deployment details include a deployment name, subscription, resource group, start time (7/17/2024, 3:45:29 PM), and correlation ID (1567dd3e-a631-4d36-be85-c56d658d0160). There are links for "Deployment details" and "Next steps", and a "Go to resource group" button.

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

The screenshot shows the Microsoft Azure portal search results for "Function App". The search bar at the top has "Function App" typed in. Below the search bar, there are tabs for "All", "Services (43)", "Marketplace (1)", "Documentation (99+)", "Resources (0)", and "Resource Groups (0)". The "Function App" service is highlighted in yellow. Other listed services include Microsoft Entra ID, App Services, Network Function Definitions, Network Function Definition Versions, Service catalog managed application definitions, VM application definitions, Definitions, and App Configuration.

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

The screenshot shows the Microsoft Azure Function App list page. The search bar at the top has "cymruscout" typed in. Below the search bar, there are filters for "Subscription equals all", "Resource group equals all", and "Location equals all". The table lists one record: "cymruscout" (Status: Stopped, Location: East US, Pricing Tier: Dynamic, App Service Plan: Microsoft Sentinel). The table has columns for Name, Status, Location, Pricing Tier, App Service Plan, Subscription, and App Type.

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

Essentials

Resource group (move)	: [REDACTED]	Default domain	: cymruscoutnu3h5nfnxsxa3w.azurewebsites.net
Status	: Running	Operating System	: Linux
Location (move)	: East US	App Service Plan	: [REDACTED]
Subscription (move)	: [REDACTED]	Runtime version	: 4.1037.0.0
Subscription ID	: [REDACTED]		

Tags (edit) : Add tags

Functions Metrics Properties Notifications (0)

Set up local environment Refresh

Name	Trigger	Status	Monitor
AccountUsageDataCollector	Timer	Enabled	Invocations and more
DomainDataCollector	Timer	Enabled	Invocations and more
IPDataCollector	Timer	Enabled	Invocations and more

- 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 **CymruScoutCreateIncidentAndNotify** Playbook, followed by the **CymruScoutLiveInvestigation** Playbook.

Cymru Scout Create Incident And Notify Playbook

Usage

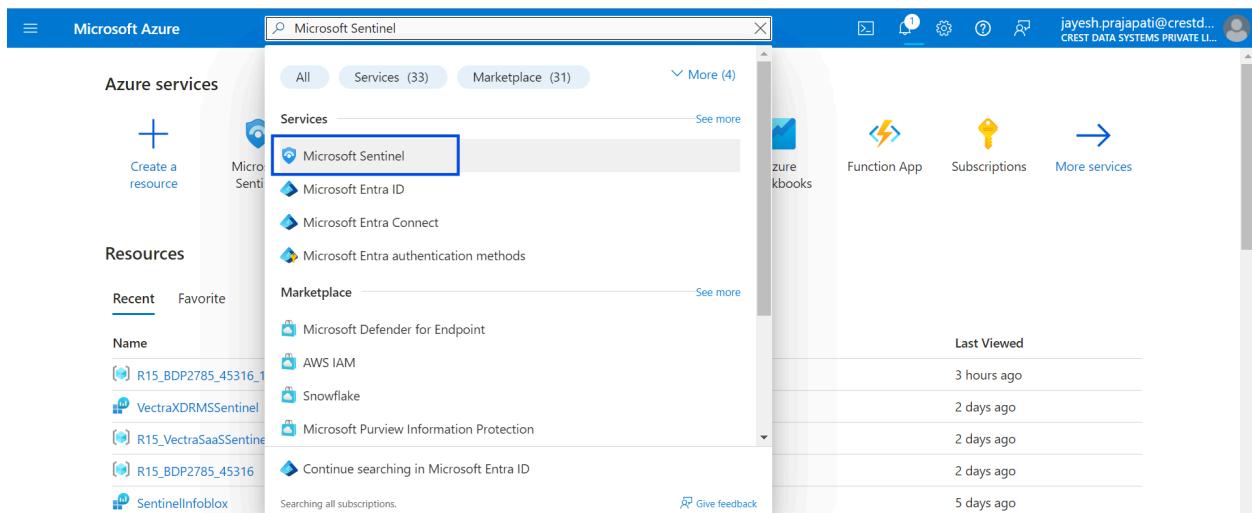
This **playbook** is triggered from two dashboards.

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 **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 "**Cymru Scout Create Incident And Notify**" playbook.

The screenshot shows the Microsoft Sentinel interface with the 'Playbook templates (Preview)' tab selected. The left sidebar includes sections for General, Threat management, Content management, Configuration, and SOC optimization. The main area displays two active playbooks:

Name	Trigger	Logic Apps Connectors	Entities	Tags	Last modified	Source name
CymruScout Create Incident And...	Using Microsoft Sentinel Action	Azure Monitor Logs +2		CymruScout Inc	7/17/2024, 5:05...	Team Cymru Sc...
CymruScout Live Investigation	Other	Azure Log Analytics Data Collector +1		CymruScout Liv	7/17/2024, 5:05...	Team Cymru Sc...

3. Click on **Create Playbook**.

The screenshot shows the 'Create Playbook' dialog for the 'CymruScout Create Incident And Notify' template. The dialog includes fields for Trigger type (Using Microsoft Sentinel Action), Content hub (Azure Monitor Log), and Last update time (7/17/2024, 5:05...). It also lists Connectors in use (Microsoft Sentinel, Azure Monitor Logs, Outlook.com) and Prerequisites (User should have an outlook mail account in order). A 'Create playbook' button is highlighted.

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

Create playbook

...

Basics Parameters Connections Review and create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription

*

Resource group

*

[Create new](#)

Region *

(US) East US

Playbook name *

CymruScoutCreateIncidentAndNotify

Enable diagnostic logs in Log Analytics [?](#)

[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**

Create playbook

...

Basics

Parameters

Connections

Review and create

EmailId (i)

nirali.shah@crestdata.ai

*

WorkspaceName (i)

[REDACTED]

*

< Previous

Next : Connections >

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

8. Click on **Create Playbook**

Home > Microsoft Sentinel | Automation >

Create playbook

Basics Parameters Connections **Review and create**

Basics

Subscription	
Resource group	
Region	eastus
Playbook name	TeamCymruScoutLiveInvestigation
Diagnostics logs workspace	Disabled

Parameters

UserName	
Password	
BaseUrl	
CreateIncidentAndNotifyPlaybookName	TeamCymruScoutCreateIncidentAndNotify

Connections

Azure Log Analytics Data Collector

New connection will be configured

i Note: Authorize this connection after deployment in the Logic App designer.

< Previous

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 (**CymruScoutCreateIncidentAndNotify**).

The screenshot shows the Azure Logic Apps portal. The top navigation bar includes 'Home > Logic apps >' followed by the logic app name 'TeamCymruScoutCreateIncidentAndNotify'. Below the navigation is a search bar and a toolbar with options like 'Run', 'Refresh', 'Edit', 'Delete', 'Enable', 'Clone', 'Open in mobile', 'Export', and 'Provide feedback'. The main area is titled 'Overview' and contains sections for 'Essentials' and 'Run history'. In the 'Essentials' section, details are provided: Resource group (move), Location (East US), Subscription (move), Subscription ID, Workflow URL, and Tags (environment : Production). The 'Run history' tab is selected, showing a table with columns 'Identifier', 'Status', 'Start time (Local Time)', and 'Duration'. A note at the bottom says 'Showing 0 runs'.

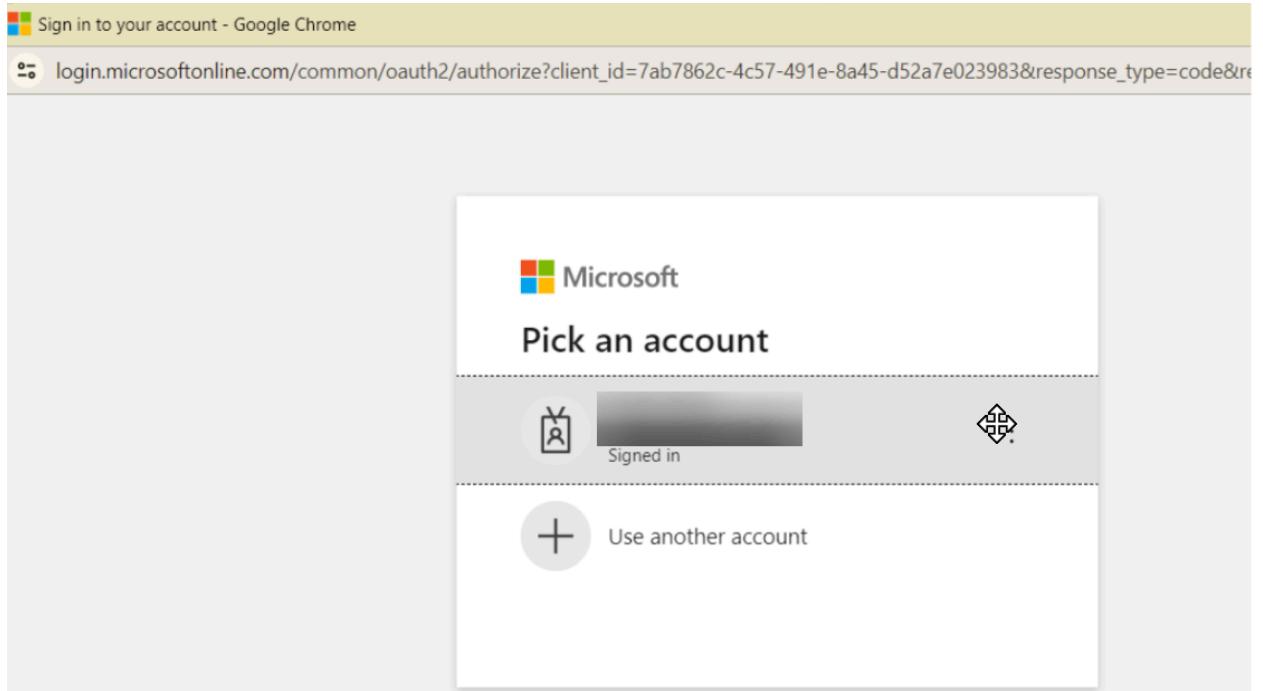
2. Go to **API connections**

The screenshot shows the 'API connections' tab for the logic app 'CymruScoutCreateIncidentAndNotify'. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Development Tools' (with 'Logic app designer' and 'Logic app code view'), 'Run History', 'Versions', and 'API connections' (which is selected and highlighted in blue). The main content area displays 'API connections associated with the logic app' and lists three entries: 'Azuremonitorlogs-CymruScoutCreateIncidentAndNotify', 'MicrosoftSentinel-CymruScoutCreateIncidentAndNotify', and 'Outlook-CymruScoutCreateIncidentAndNotify'.

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

The screenshot shows the Azure Logic App interface. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Development Tools (Logic app designer, Logic app code view, Run History, Versions), API connections (which is selected), Quick start guides, and Settings. The main area shows 'API connections associated with the logic app' with items like 'Azuremonitorlogs-CymruScoutCreate...', 'MicrosoftSentinel-CymruScoutCreateIn...', and 'Outlook-CymruScoutCreateIncidentAn...'. A modal window titled 'Edit API connection' is open over the main content. It has tabs for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, General, Properties, and Edit API connection (which is selected). The 'Edit API connection' tab has sections for API (set to 'Azure Monitor Logs'), Display Name ('Azuremonitorlogs-CymruScoutCreateIncidentAndNotify'), and Authorize (which is the current tab). At the bottom of the modal are 'Save' and 'Discard' buttons.

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



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

Azuremonitorlogs-CymruScoutCreateIncidentAndNotify | Edit API connection

API Connection

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

General

Properties

Edit API connection

Monitoring

Automation

Help

Authorization was successful. Please save your changes

Edit API connection

Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.

API

Azure Monitor Logs

Display Name

Azuremonitorlogs-CymruScoutCreateIncidentAndNotify

Authorize

Authorize

Save

Discard

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**.

The screenshot shows the 'Access control (IAM)' page for the 'CymruTest2503' workspace. The left sidebar has a red box around the 'Access control (IAM)' item. The top navigation bar has a red box around the '+ Add' button. The main content area shows sections for 'My access' and 'Check access', with the 'Check access' section having a red box around its 'Check access' button.

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

The screenshot shows the 'Add role assignment' page. The 'Members' tab is selected. A search bar at the top contains 'Microsoft Sentinel Contributor'. Below the search bar, there is a table with one result: 'Microsoft Sentinel Contributor' listed under both 'Name' and 'Description'. At the bottom, it says 'Showing 1 - 1 of 1 results.'



Next

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

Home > CymruTest2503 | Access control (IAM) >

Add role assignment ...

Role **Members** * **Conditions** **Review + assign**

Selected role Microsoft Sentinel Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
No members selected		

Description Optional

[Review + assign](#) [Previous](#) [Next](#)

Select managed identities

⚠ Some results might be hidden due to your ABAC condition.

Subscription * CDS_R15_Sub1

Managed identity Logic app (159)

Select TeamCymruScoutCreateIncidentAndNotify

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

[Learn more about RBAC](#)

[Select](#) [Close](#)

[Feedback](#)

Selected members:
 TeamCymruScoutCreateIncidentAndNotify
[/subscriptions/.../resourceGroups/.../remove](#)

[Select](#) [Close](#)

[Feedback](#)

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

Home > CymruTest2503 | Access control (IAM) >

Add role assignment

... [Edit](#) [Delete](#)

[Role](#) [Members](#) [Conditions](#) [Review + assign](#)

Selected role Microsoft Sentinel Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
TeamCymruScoutCreateIncidentAndNot...	[REDACTED]	Role

Description

[Review + assign](#) [Previous](#) [Next](#)

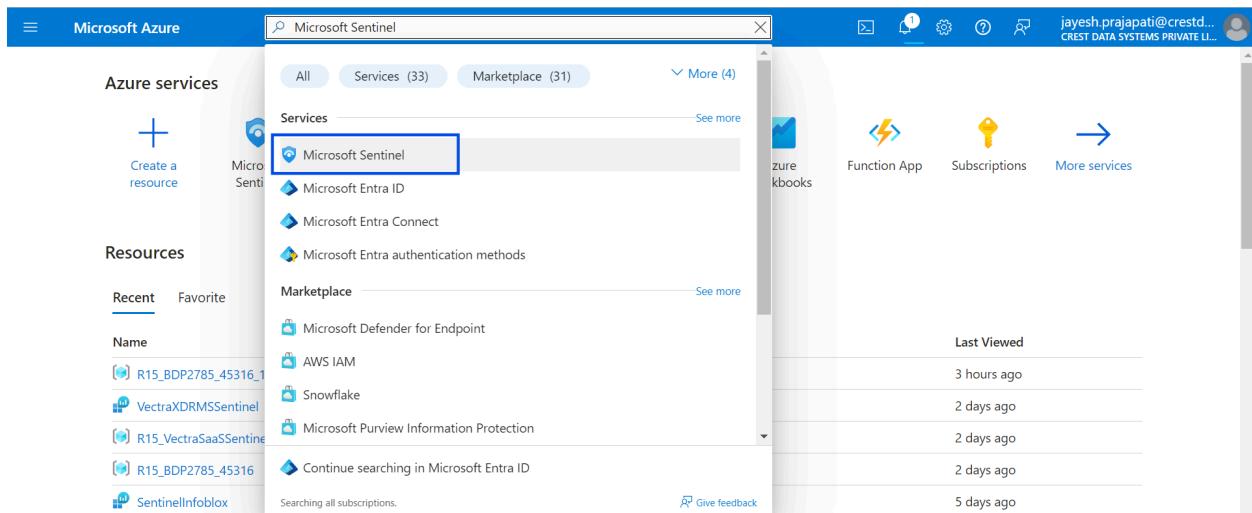
Cymru Scout Live Investigation Playbook

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**.

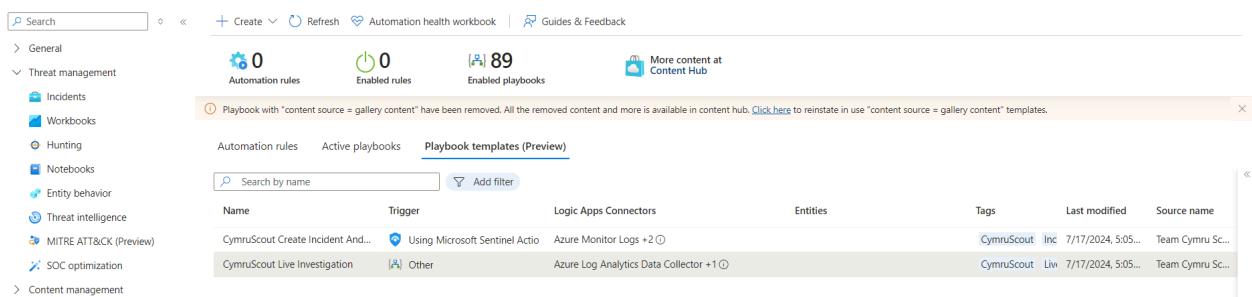
Configuration

1. Go to Microsoft Sentinel



The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar with 'Microsoft Sentinel' typed in. Below the search bar, the 'Azure services' section has a 'Services' tab selected, showing a list of services. 'Microsoft Sentinel' is highlighted with a blue box. Other listed services include Microsoft Entra ID, Microsoft Entra Connect, and Microsoft Entra authentication methods. To the right of the service list, there are links for 'Function App', 'Subscriptions', and 'More services'. Below the service list, there's a 'Last Viewed' section with a list of recently viewed items, each with a timestamp.

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



The screenshot shows the Microsoft Azure Automation blade. On the left, there's a navigation menu with sections like General, Threat management, and Content management. The main area is titled 'Playbook templates (Preview)' and contains a table of playbooks. The table has columns for Name, Trigger, Logic Apps Connectors, Entities, Tags, Last modified, and Source name. Two playbooks are listed: 'CymruScout Create Incident And...' and 'CymruScout Live Investigation'. A message at the top of the table area says: 'Playbook with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.'

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

The screenshot shows the Microsoft Sentinel Automation blade. On the left, there's a navigation menu with sections like General, Threat management, Content management, Configuration, and Automation (which is selected). The main area displays automation rules, enabled rules, and enabled playbooks. A prominent section is 'Playbook templates (Preview)', which lists two entries: 'CymruScout Create Incident A...' and 'CymruScout Live Investigation'. To the right of this list is a detailed view of the 'CymruScout Live Investigation' template, including its description, connectors in use (Azure Log Analytics Data Collector, RegEx Matching (Independent Publisher)), and prerequisites. A large blue button at the bottom right says 'Create playbook'.

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

Home > Microsoft Sentinel | Automation >

Create playbook ...

Basics **Parameters** **Connections** **Review and create**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription

Resource group

[Create new](#)

Region *

 (US) East US


Playbook name *

 CymruScoutLiveInvestigation

[Enable diagnostic logs in Log Analytics](#)

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**).

[Home](#) > [Microsoft Sentinel | Automation](#) >

Create playbook

[Basics](#) **Parameters** [Connections](#) [Review and create](#)

UserName ⓘ

*

Password ⓘ

*

BaseUrl ⓘ

*

CreateIncidentAndNotifyPlaybookName ⓘ

*

[< Previous](#)

[Next : Connections >](#)

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 (**CymruScoutLiveInvestigation**).

The screenshot shows the Azure Logic Apps portal with the following details:

- Resource group:** [REDACTED]
- Location:** East US
- Subscription:** [REDACTED]
- Subscription ID:** [REDACTED]
- Workflow URL:** <https://prod-59.eastus.logic.azure.com:443/workflows/4b921cb17...>
- Tags:** environment : Production

The navigation bar includes options like Run, Refresh, Edit, Delete, Enable, Clone, Open in mobile, Export, and Provide feedback.

2. **Go to API Connections.**
3. Click on **AzureLogAnalyticsDataCollector-CymruScoutLiveInvestigation 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.

The screenshot shows the 'Edit API connection' dialog for the 'AzureLogAnalyticsdatacollector-CymruScoutLiveInvestigation' connection. The dialog includes the following fields:

- API:** Azure Log Analytics Data Collector
- Display Name:** Azureloganalyticsdatacollector-CymruScoutLiveInvestigation
- Workspace ID ***: [REDACTED]
- Workspace Key ***: [REDACTED]

At the bottom, there are 'Save' and 'Discard' buttons.

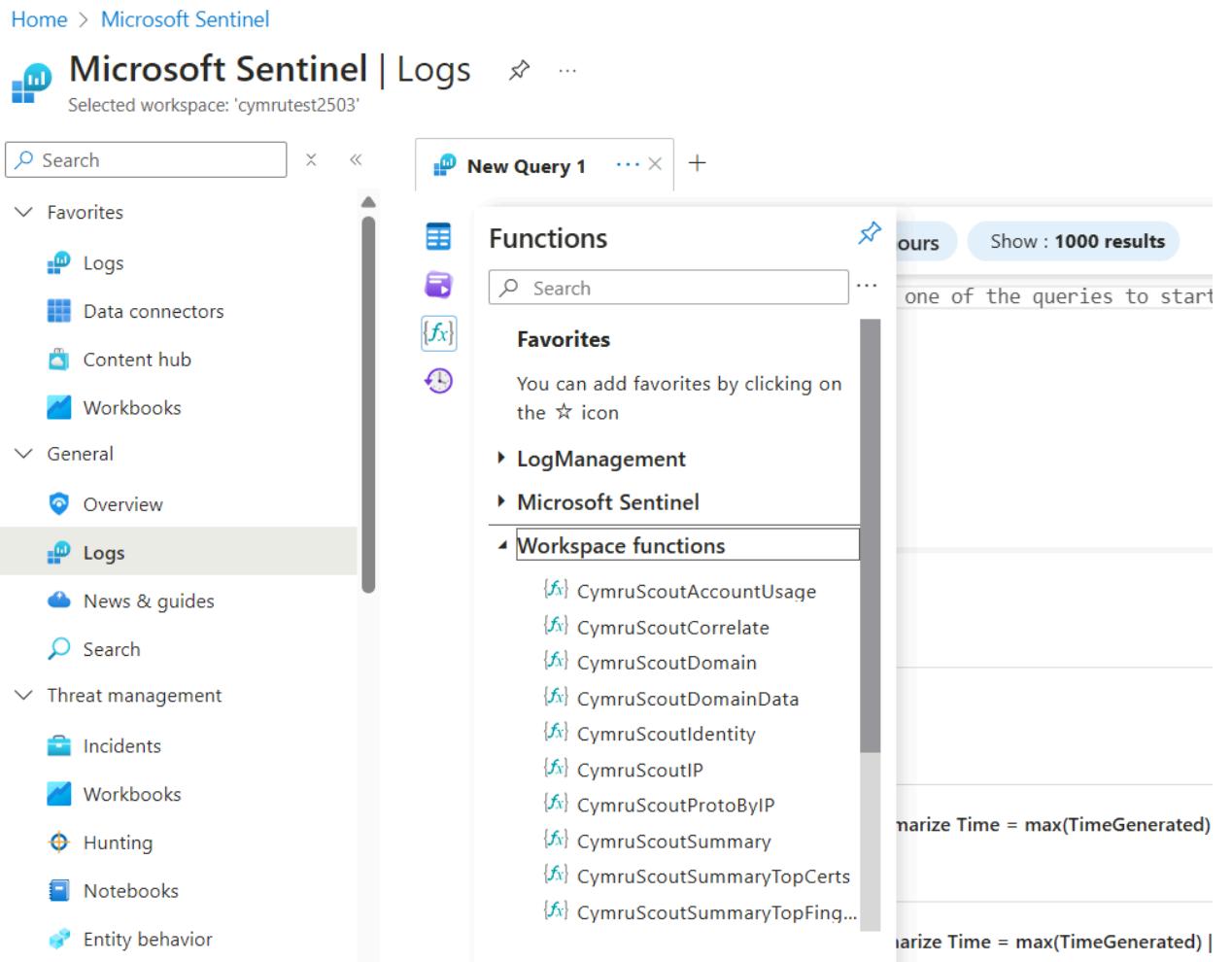
5. Click **Save** to store the authorized connection.

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.

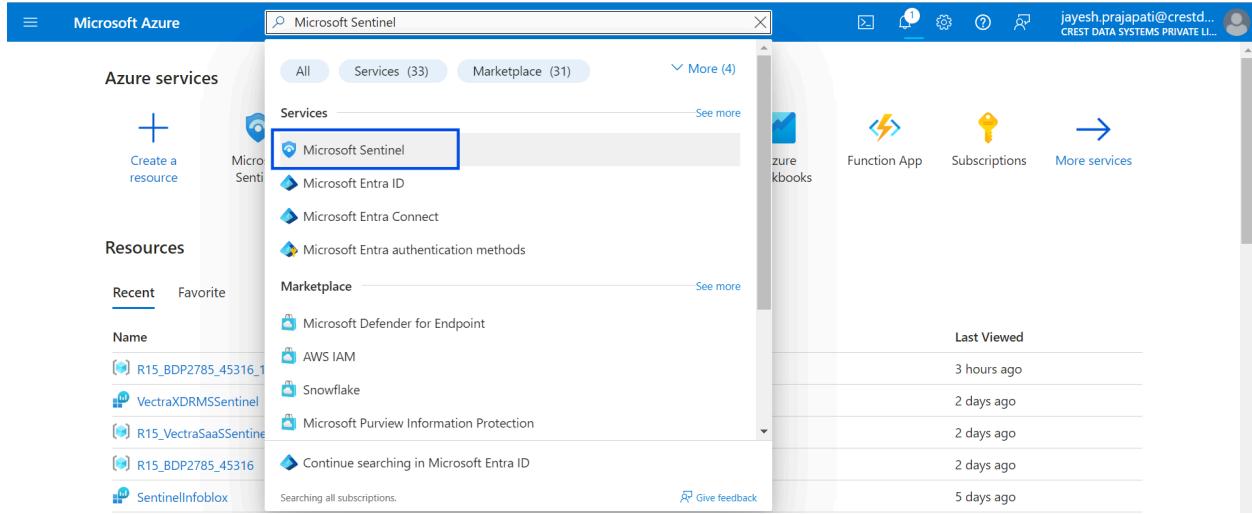
1. Once you install the **Team Cymru Scout** solution, the parsers are automatically installed to their correct location, so there is no need to install them separately.



Steps to Configure the Team Cymru Scout Workbook (Dashboards)

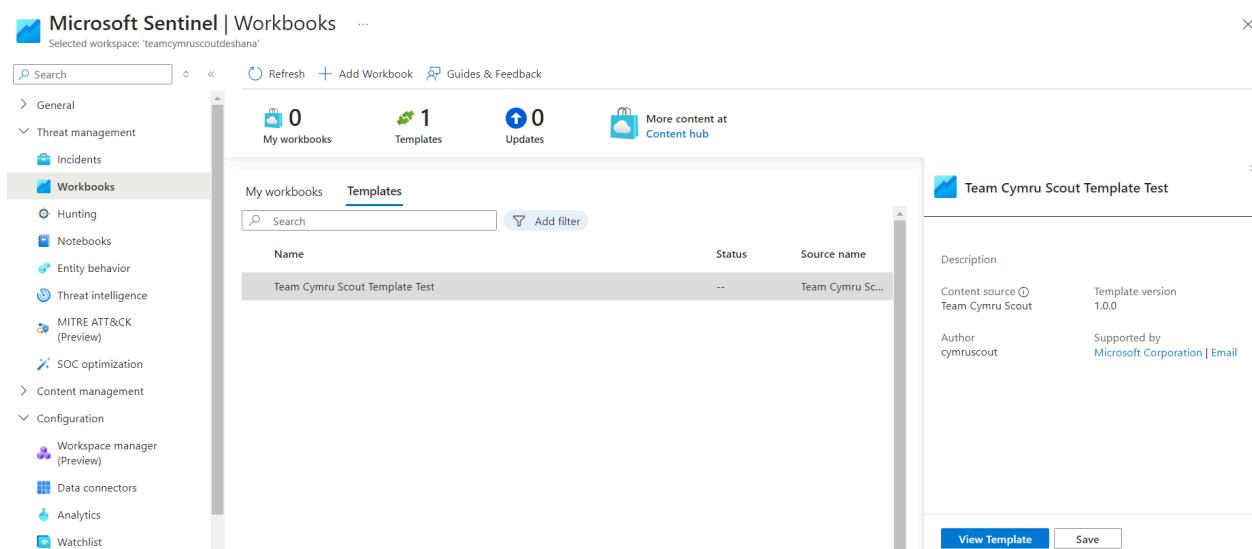
Workbooks in Microsoft Sentinel provide a flexible canvas for data analysis and the creation of rich visual reports within the Microsoft Azure portal.

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



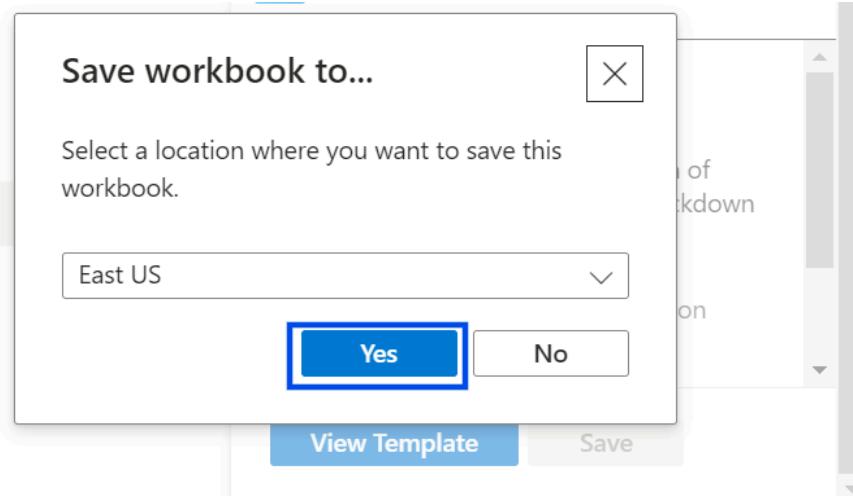
The screenshot shows the Microsoft Azure homepage with the search bar set to "Microsoft Sentinel". The "Services" section is expanded, showing "Microsoft Sentinel" highlighted with a blue box. Other services listed include Microsoft Entra ID, Microsoft Entra Connect, and Microsoft Entra authentication methods. The "Marketplace" section shows Microsoft Defender for Endpoint, AWS IAM, Snowflake, and Microsoft Purview Information Protection. The "Last Viewed" section lists recent resources like R15_BDP2785_45316_1, VectraXDRMSentinel, R15_VectraSaaSSENTINEL, R15_BDP2785_45316, and SentinelInfoblox. The "Recent" tab under "Resources" is selected, showing the same list of recent resources.

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



The screenshot shows the Microsoft Sentinel Workbooks page. The left sidebar is collapsed, and the main area shows the "Templates" tab selected. A search bar at the top right is empty. Below it, there are counts for "My workbooks" (0), "Templates" (1), and "Updates" (0). A "Content hub" link is also present. The main pane displays a table with one row: "Name" (Team Cymru Scout Template Test), "Status" (--), and "Source name" (Team Cymru Sc...). On the right side, a detailed view of the "Team Cymru Scout Template Test" template is shown, including its description, content source (Team Cymru Scout), template version (1.0.0), author (cymruscout), and support information (Supported by Microsoft Corporation | Email). At the bottom right of this panel are "View Template" and "Save" buttons.

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.

The screenshot shows the 'Insights Information by Indicators' panel in Microsoft Sentinel. At the top, there are navigation links: Edit, Open, Help, and Auto refresh: Off. Below these are tabs: Indicators Overview (which is selected), Correlation Overview, Live Investigation, and Account Usage. A tooltip message is displayed: 'The panel Insights Information by Indicators incorporates the use of the TeamCymruScoutCreateIncidentAndNotify logic app which is deployed with the Microsoft Sentinel Solution to create incident for a malicious indicator. Please configure this logic app first and keep it enabled in order to notify creation of an incident for a malicious indicator.' In the main pane, there is a section titled 'Steps to Create Incident and Notify for a Malicious Indicator.' with the following steps:

- Select the **Subscription ID** and **Resource Group**.
- Click on the **Run Playbook** button besides malicious indicator.
- One side panel will be open, click on the **Create Incident And Notify** button below.
- This will execute the **CymruScoutCreateIncidentAndNotify** logic app in the background.
- You can check the status of the playbook to identify the creation of incident and check mail for notification.

NOTE: You can see Run Playbook option visible only for Malicious indicators. For others, that option is not available.

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 **CymruScoutLiveInvestigation Playbook** is configured correctly.

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

Indicators Overview Correlation Overview **Live Investigation** Account Usage

i This workbook depends on the **CymruScoutLiveInvestigation** logic app which is deployed with the Microsoft Sentinel Solution. Please configure this logic app first and keep it enabled in order to use this workbook.

Live Investigation

⌚ Steps to perform Live Investigation using this workbook

- This workbook is intended to help perform Live Investigation for Indicators (**Type**: IP or Domain).
- Select the **Resource Group** and **Subscription ID**.
- Select Indicator Type from Type filter and provide Indicator value corresponding to its type in the Indicator parameter.
- Click on the **Submit** button.
- One side panel will be open, click on the **Get Data** button below.
- This will execute the **CymruScoutLiveInvestigation** logic app in the background.
- You will be able to see a message as **Refresh to check for data availability**.
- Click on the refresh icon above the message until you get a message as **Click here to view the data**.
- Click on the message **Click here to view the data** and it will display all panels for searched Indicator data.
- You can check the status of the playbook to identify the Live Investigation data fetch status.

Note :

In cases where

- In a new environment for live investigations, it may take around 5 to 10 minutes for data ingestion and dashboard population due to Sentinel's default behavior.
- Panels do not populate, please check the status of the **CymruScoutLiveInvestigation** logic app.
- It is suggested to perform a **Hard Refresh** before getting Live Investigation data for the new Indicator value. Otherwise, the source drill down panels will not be populated properly.

Correlation Overview

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.

This tab depends on the ASIM Parsers and ThreatIntelligenceIndicators. Please configure ASIM Parsers in the workspace and create/upload some indicators in ThreatIntelligence to visualize data in this tab.

Correlation Overview

Steps to perform Correlation using this workbook

- This workbook is intended to help perform Correlation of Indicators (**Indicator Type:** IP or Domain).
- Select **Time Range** for which you want to perform correlation of other sources data with Team Cymru Scout Data.
- Select **Indicator Type** from Indicator Type filter. Default All is selected.
- Select **Search Matching Algorithm** based on which you want to perform correlation of other sources data with Team Cymru Scout Data.
 - **ThreatIntelligenceIndicator:** Threat indicators are data that associate observed artifacts such as URLs, file hashes, or IP addresses with known threat activity such as phishing, botnets, or malware.
 - **ASIM Parsers:** The Advanced Security Information Model (ASIM) provides a seamless experience for handling various sources in uniform, normalized views. ASIM allows for predictable entities correlation across normalized tables.
- If you select **ASIM Parsers** in "Search Matching Algorithm", filter for ASIM Parsers will be visible.
 - Select ASIM Parsers schema from **ASIM Parsers** filter. Default All is selected.
- Based on selected filters, correlated data will be visible in below panes.

Note:

- If data is not populated,
 - Check ASIM Parsers schema is available in workspace and does not have any error.
 - Check ThreatIntelligenceIndicator table has indicators available from other sources.

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.

The screenshot shows a 'Deploy ASIM' interface. At the top, a message states: 'This template deploys all ASIM parsers. The Advanced Security Information Model (ASIM) enables you to use and create source-agnostic content, simplifying your analysis of the data in your Microsoft Sentinel workspace.' Below this is a link to 'Normalization and the Advanced Security Information Model (ASIM)'. Two large blue buttons are present: 'Deploy to Azure' and 'Deploy to Azure Gov'. A section titled 'To deploy a single schema use the buttons below:' contains a table:

ASim Schema	Deploy	Deploy to Azure Gov
Audit Event	Deploy to Azure	Deploy to Azure Gov
Authentication	Deploy to Azure	Deploy to Azure Gov
Dns	Deploy to Azure	Deploy to Azure Gov
File Event	Deploy to Azure	Deploy to Azure Gov
Network Session	Deploy to Azure	Deploy to Azure Gov
Web Session	Deploy to Azure	Deploy to Azure Gov
Process Event	Deploy to Azure	Deploy to Azure Gov
Registry	Deploy to Azure	Deploy to Azure Gov

The 'Dns' row is highlighted with a red box around the 'Deploy to Azure' button.

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.

The screenshot shows the Azure Functions Invocations page for the 'IPDataCollector' function. It displays a table of recent invocations with columns for Date, Status, Result Code, Duration (ms), and Operation ID. One invocation from March 26, 2025, at 12:00:00 is highlighted and selected. A modal window titled 'Invocation details' is open, showing detailed logs for this specific invocation. The logs include timestamp, type (Information, Trace), and message content, such as execution details and request headers.

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.

The screenshot shows the Log Analytics Workspace Logs page. The 'Logs' tab is selected. On the right, a 'New Query 1' pane is open, showing a dropdown menu for 'Simple mode' and 'KQL mode'. The 'KQL mode' option is highlighted with a red box. Below the query pane, a table named '_GetWatchlist('TeamCymruScoutIPData')' is shown with one result row.

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

The screenshot shows the Microsoft Log Analytics workspace interface. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs (which is selected), Resource visualizer, Settings, Classic, Monitoring, Automation, and Help. The main area has a search bar at the top. Below it, a 'New Query 1' card is open with the KQL query: `1 Cymru_Scout_Account_Usage_Data_CL`. The results pane shows a table with three rows of data:

TimeGenerated [UTC]	used_queries_d	remaining_queries_d	query_limit_d	foundation_api_usage_used_queries_d	foundation_api_usage_remaining_queries_d
> 3/25/2025, 12:50:01.063 PM	47504	52496	100000	11	0
> 3/25/2025, 12:40:01.184 PM	47488	52512	100000	10	0
> 3/25/2025, 12:30:01.291 PM	47466	52534	100000	9	0

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

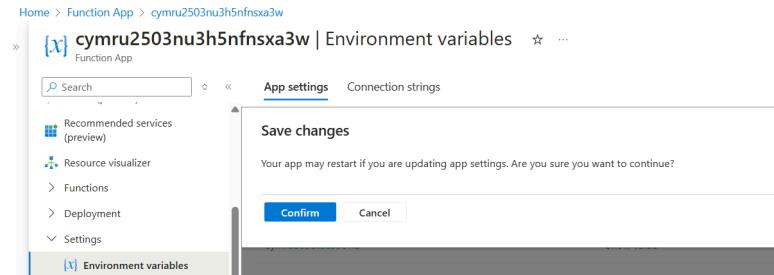
1. Go to function apps → <function app>
2. Go to Environment variables under the Setting sections.
3. You can see the value of environment variables from here by clicking on Show value.
4. Check that values are provided in **any specific** variable.
5. To edit a particular variable,
 - a. Click on the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

The screenshot shows the Azure Function App settings page for a function named 'cymru2503nu3h5nfnsxa3w'. The left sidebar lists various settings: Recommended services (preview), Resource visualizer, Functions, Deployment, Settings, and Environment variables (which is selected). The main pane shows the 'Add/Edit application setting' form for the 'Environment variables' section. It lists several environment variables with their current values:

Name *	Value
IPValues	1.2.3.4,1.2.1.2
CymruScoutBase	
DomainTableName	
DomainValues	
FUNCTIONS_D	
FUNCTIONS_W	
IPTableName	
IPValues	
logAnalyticsUri	
LogLevel	
Schedule	

At the bottom, there are 'Apply' and 'Discard' buttons.

- 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.

Run ID	Status	Timestamp	Duration
08545850288747989785177994CU45	Failed	3/27/2025, 11:53:16 AM	5.72 Seconds
0854585499708111292128761389CU61	Failed	3/27/2025, 11:58:34 AM	5.29 Seconds
085458507549093890279566646CU63	Succeeded	3/27/2025, 11:45:30 AM	44.1 Seconds

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.

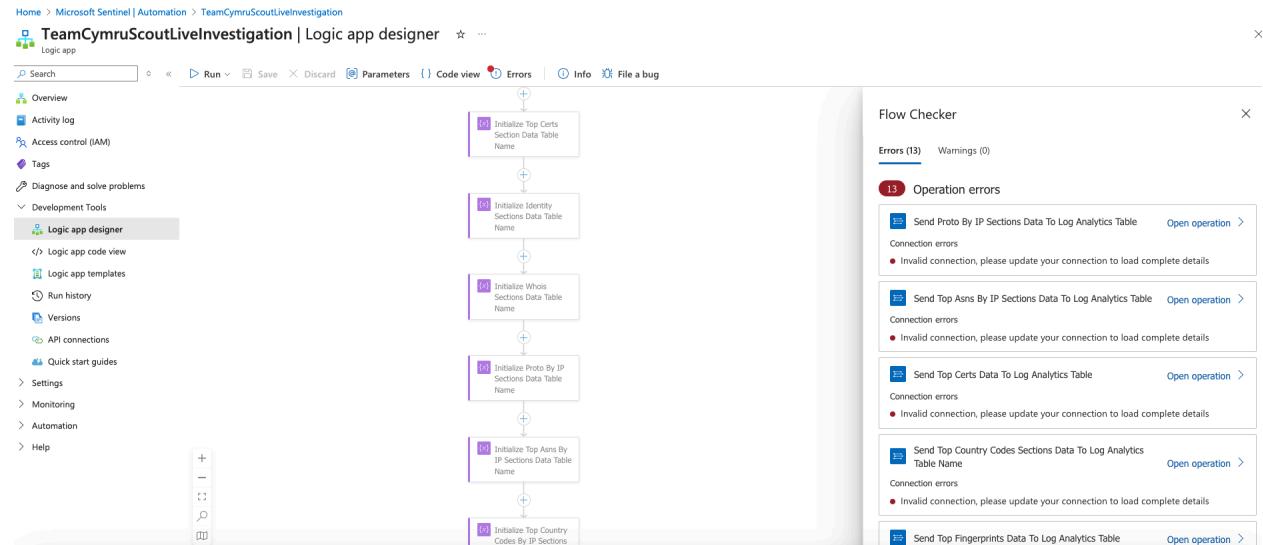
Problem1: This can occur because the default interval for the account usage function to retrieve data from the Scout API is set to **1 hour**.

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 steps 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.