



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
TEAM CYMRU. COPYRIGHT © 2025. ALL RIGHTS RESERVED

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	9
Usage	9
Prerequisites	9
App Registration steps for the Application in Microsoft Entra ID	9
Add a client secret for application in Microsoft Entra ID	10
Assign role of Microsoft Sentinel Contributor to application in Microsoft Entra ID	11
Upload Indicators csv in Watchlists to get data related to ip/domain from Team Cymru Scout	12
Get Object ID of your application in Microsoft Entra ID	13
Configuration of Data Connector	16
Steps to Configure Playbook (Logic Apps)	23
Team Cymru Scout Create Incident And Notify Playbook	23
Usage	23
Configuration	23
Authorize API Connection	28
Assign Role to Add Comment in Incident	32
Team Cymru Scout Live Investigation Playbook	35
Usage	35
Configuration	35
Authorize API Connection	39
Team Cymru Scout Enrich Incident Playbook	40
Usage	40
Configuration	40
Authorize API Connection	44
Assign Role to Add Comment in Incident	45
Steps to Configure the Team Cymru Scout Parsers	48
Usage	48
Steps to Configure the Team Cymru Scout Workbook (Dashboards)	50
Indicator Overview	52
Usage	52
Live Investigation	53
Usage	53
Correlation Overview	54

Usage	54
Steps to Deploy ASIM Parsers	56
Troubleshooting Steps	57
Steps to check invocation details of the function in Team Cymru Scout function app	57
Steps to check the data in Log Analytic Workspace table	57
Steps to verify or edit the environment variables of function app	58
Steps to find the exact action where playbook execution failed	59
Case #1 - Indicators Overview Dashboard not showing data in any panel	60
Case #2 - The function app invocation logs are showing "No ip/domain values found for watchlist"	61
Case #3 -The Account Usage tab in the workbook does not immediately show the latest API usage count.	61
Case #4 - Getting Connection error in the logic app	61
Case #5 - Getting Microsoft Outlook account connection error in TeamCymruScoutCreateIncidentAndNotify Logic app	62
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	62
Case #7 - The Live Investigation tab of workbook not populating data in panels	63
Case #8 - The Data Connector showing the Not Connected status on the data connector UI page	63
Case #9 - The Correlation Overview dashboard not populating data in any panel	63

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.

Home >

Custom deployment

Deploy from a custom template

Select a template Basics Review + create

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. [Learn more about template deployment ↗](#)



Build your own template in the editor

Common templates

- Create a Linux virtual machine
- Create a Windows virtual machine
- Create a web app
- Create a SQL database
- Azure landing zone

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

The screenshot shows the 'Edit template' page in the Azure portal. At the top, there are navigation links: 'Home > Custom deployment > ...'. Below that is the title 'Edit template' and a sub-instruction 'Edit your Azure Resource Manager template'. A toolbar contains buttons for '+ Add resource', 'Quickstart template', 'Load file' (which is highlighted with a red box), and 'Download'. To the left, a sidebar lists 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main area displays a JSON template with line numbers 1 through 6:

```
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {},
5   "resources": []
6 }
```

At the bottom of the editor are two buttons: 'Save' (blue) and 'Discard'.

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**".

Home >

Custom deployment ...

Deploy from a custom template

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

Select a template **Basics** Review + create

Template

 Customized template 
60 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 * 

Location 

Workspace-location 

Workspace 

Workbook1-name 

Watchlist1-id 

Watchlist2-id 

[Previous](#)

[Next](#)

Review + create

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

Home >

 Microsoft.Template-20250326103837 | Overview

Deployment

Search X << Delete Cancel Redeploy Download Refresh

Overview

Your deployment is complete

Deployment name : Microsoft.Template-20250326103837
Subscription :
Resource group :
Start time : [redacted]
Correlation ID : [redacted]

Inputs Outputs Template

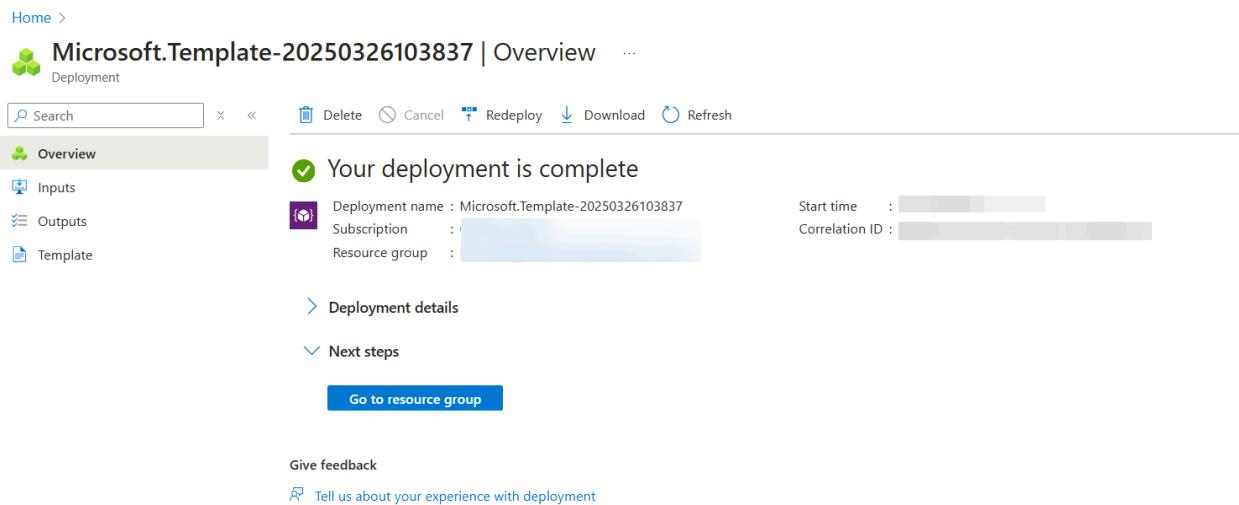
> Deployment details

< Next steps

Go to resource group

Give feedback

Tell us about your experience with deployment



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**

The screenshot shows the Azure Active Directory portal for 'CREST DATA SYSTEMS PRIVATE LIMITED'. In the left sidebar under 'Manage', the 'App registrations' link is highlighted with a red box. At the top of the main content area, there is a red box around the '+ New registration' button. The 'Owned applications' tab is selected, and the message 'This account isn't listed as an owner of any applications in this directory.' is displayed.

- 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 interface for managing application registrations. On the left, there's a sidebar with various options like Overview, Quickstart, Integration assistant, Diagnose and solve problems, Manage (with Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), Support + Troubleshooting, and New support request. The 'Certificates & secrets' option is highlighted with a red box. On the right, a modal window titled 'Add a client secret' is open. It has fields for 'Description' (with a placeholder 'Enter a description for this client secret') and 'Expires' (set to 'Recommended: 180 days (6 months)'). Below these, a table lists a single client secret: 'MSSentinel' with an expiration date of '11/12/2026' and a value starting with 'oIT*****'. At the bottom of the modal are 'Add' and 'Cancel' buttons, with 'Add' also being 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

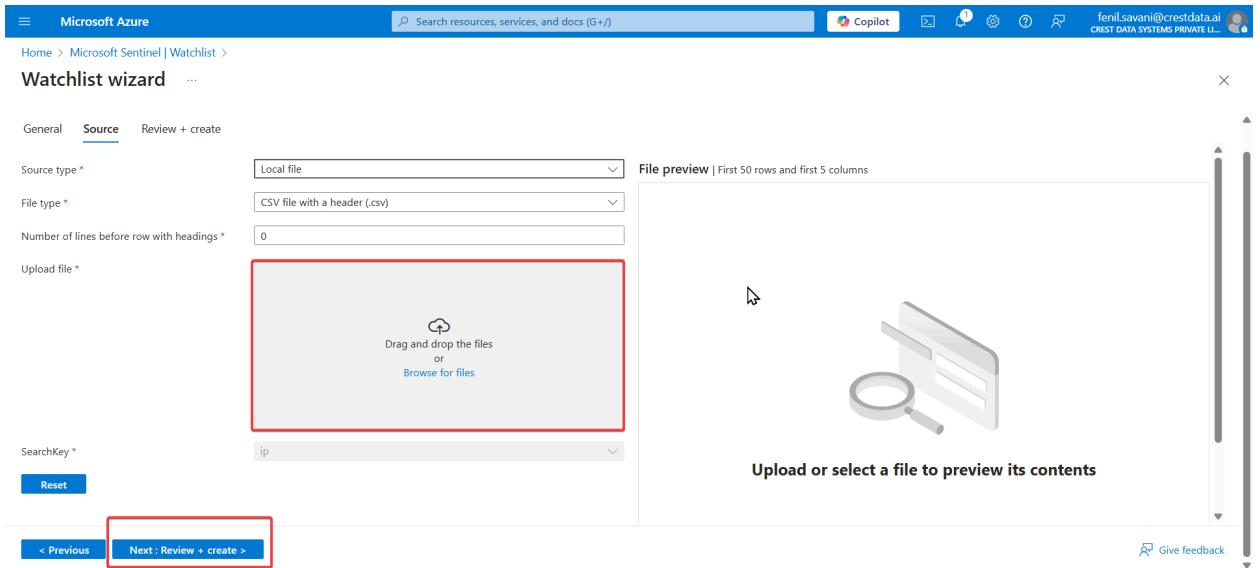
Follow the steps in this section to upload csv containing indicators in watchlist:

- 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 Azure 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. The table below shows two entries: 'TeamCymruScoutIPData' and 'TeamCymruScoutDomainData'. The 'TeamCymruScoutDomainData' entry has a checked checkbox next to its name.

Name	Alias	Source	Created time	Last u...
TeamCymruScoutIPData	TeamCymruScoutIPData	ip_indicator.csv	3/25/2025, 2:12:28 PM	3/25/2025
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](#)

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.

Home >

CREST DATA SYSTEMS PRIVATE LIMIT

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with options like 'Overview', 'Preview features', 'Diagnose and solve problems', 'Manage' (with sub-options for 'Users', 'Groups', 'External Identities', 'Roles and administrators', 'Administrative units', 'Delegated admin partners', and 'Enterprise applications'). The 'Enterprise applications' option is highlighted with a red box. To the right, there's a main content area with tabs for 'Overview' (which is selected), 'Monitoring', and a search bar. Below the tabs, there are sections for 'Basic information' (Name, Tenant ID, Primary domain), 'License', and a summary table.

Category	Value
Name	CREST DATA SYSTEMS PRIVATE LIMITED
Tenant ID	00000000-0000-0000-0000-000000000000
Primary domain	cymru.com
License	Standard

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

The screenshot shows the 'Enterprise applications' list page. The top navigation bar includes 'New application', 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?'. The left sidebar has 'Overview', 'Manage', and 'All applications' (which is selected). The main content area displays a table of applications with columns for 'Name', 'Type', 'Status', 'Last modified', and 'Actions'. A search bar at the bottom allows filtering by application name or object ID, application type (set to 'Enterprise Applications'), and application ID starts with. The message '112 applications found' is displayed at the bottom.

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

The screenshot shows the Azure portal interface for managing enterprise applications. At the top, the navigation bar includes 'Home', 'CREST DATA SYSTEMS PRIVATE LIMITED | Enterprise applications', 'Enterprise applications | All applications', and a back arrow. Below the navigation is a breadcrumb trail: 'Enterprise Application' > 'Overview'. The main content area has a left sidebar with links like 'Overview', 'Deployment Plan', 'Diagnose and solve problems', 'Manage', 'Security', 'Activity', and 'Troubleshooting + Support'. The right side is titled 'Properties' and contains fields for 'Name' (with a placeholder 'New application'), 'Application ID', and 'Object ID'. The 'Object ID' field is specifically highlighted with a red rectangular box. Below the properties section is a 'Getting Started' section.

- 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**.

The screenshot shows the Microsoft Sentinel Data connectors page. On the left, there's a navigation sidebar with links 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' link is highlighted with a red box. The main area shows a summary of connectors: 1 Connected (1). Below this, a search bar and filters (Providers: Team Cymru Scout, Data Types: All, Status: Connected (1)) are present. A list of connectors includes 'Team Cymru Scout Data Connector (using Azure Functions)'. On the right, detailed information for this connector is shown: Provider (Team Cymru Scout), Status (Connected), Last Log Receive (8 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.), and a 'Content source' section. A blue '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. It displays basic connector details: Connected Status, Team Cymru Scout Provider, and Last Log Received (14 Minutes Ago). Below this, there's a 'Description' section and a 'Last data received' timestamp (3/25/2025, 6:30:05 PM). Under 'Content source', it shows Team Cymru Scout (Version 1.0.0). The 'Author' is Team Cymru. Related content includes 1 Workbooks, 14 Queries, and 0 Analytics rules templates. On the right, under 'STEP 6 - Choose ONE from the following two deployment options to deploy the connector and the associated Azure Function', there's an 'IMPORTANT' note about workspace ID and primary key. It shows fields for 'Workspace ID' and 'Primary Key'. Below this, 'Option 1 - Azure Resource Manager (ARM) Template' is described, along with steps 1 and 2: 1. Click the 'Deploy to Azure' button below, and 2. Select the preferred Subscription, Resource Group and Location. A blue '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 * [①](#) [▼](#)

Resource group * [①](#) [▼](#)
[Create new](#)

Instance details

Region * [①](#) [East US](#) [▼](#)

Function Name [CymruScout](#)

Cymru Scout Base URI * [①](#) [▼](#)

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

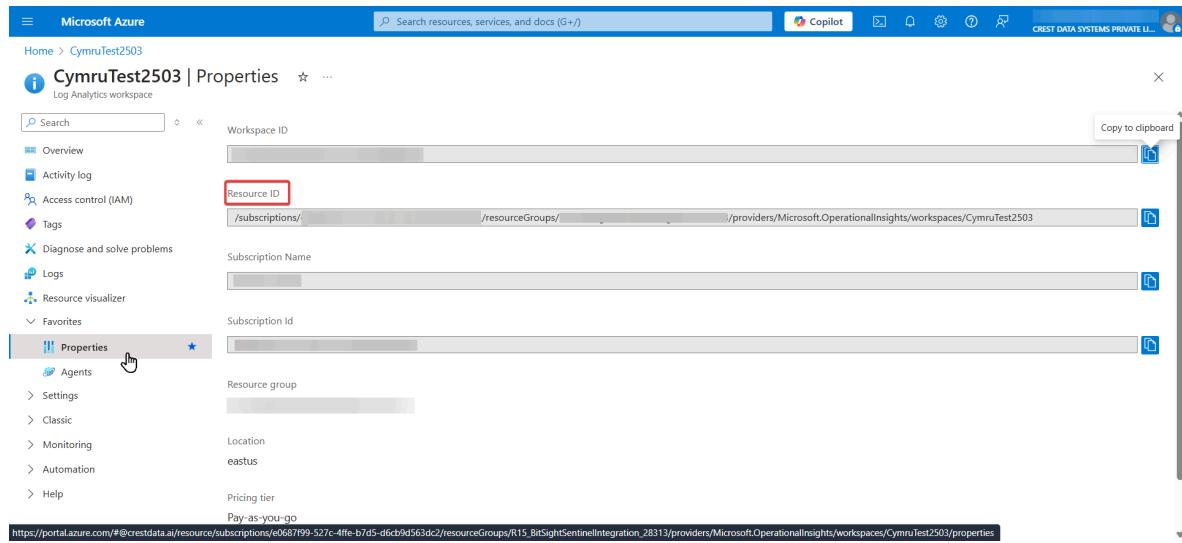
4. Enter the required **parameters** and click **Review + Create**.

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

Workspace Name	Name of the Log analytics workspace. 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**.



The screenshot shows the 'Properties' tab 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

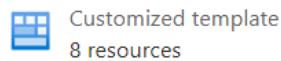
Home >

Custom deployment

Deploy from a custom template

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 start time of 7/17/2024, 3:45:29 PM and a correlation ID of 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 search results for "Function App". The search bar at the top has "Function App" typed in. Below the search bar, there are several categories: All, Services (43), Marketplace (1), Documentation (99+), Resources (0), and Resource Groups (0). Under the "Services" category, "Function App" is highlighted. 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 view. The search bar at the top has "cymruscout" typed in. Below the search bar, there are filter options: + Create, Manage view, Refresh, Export to CSV, Open query, Assign tags, Start, Restart, Stop, Delete. The search results show one record: "cymruscout" (Subscription equals all, Resource group equals all, Location equals all). The columns are Name, Status, Location, Pricing Tier, App Service Plan, Subscription, and App Type. The "App Type" column shows "Function App".

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

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and various navigation icons. Below the header, the URL 'cymruscoutnu3h5nfnsxa3w' is displayed, followed by a 'Function App' badge. On the left, a sidebar menu includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Microsoft Defender for Cloud', 'Events (preview)', 'Recommended services (preview)', 'Resource visualizer', and 'Favorites' (which contains 'Environment variables' and 'Configuration'). The main content area is titled 'Essentials' and shows resource details: Resource group (move) [REDACTED], Status: Running, Location: East US, Subscription (move) [REDACTED], Subscription ID [REDACTED], Default domain: cymruscoutnu3h5nfnsxa3w.azurewebsites.net, Operating System: Linux, App Service Plan: [REDACTED], and Runtime version: 4.1037.0.0. Below this, there's a 'Tags (edit)' section with a link to 'Add tags'. A 'Functions' tab is selected, showing three entries: 'AccountUsageDataCollector', 'DomainDataCollector', and 'IPDataCollector'. Each function entry includes a 'Name' column, a 'Trigger' column (all listed as 'Timer'), a 'Status' column (all listed as 'Enabled'), and a 'Monitor' column (all listed as 'Invocations and more'). There are also three horizontal ellipsis buttons for each function entry.

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

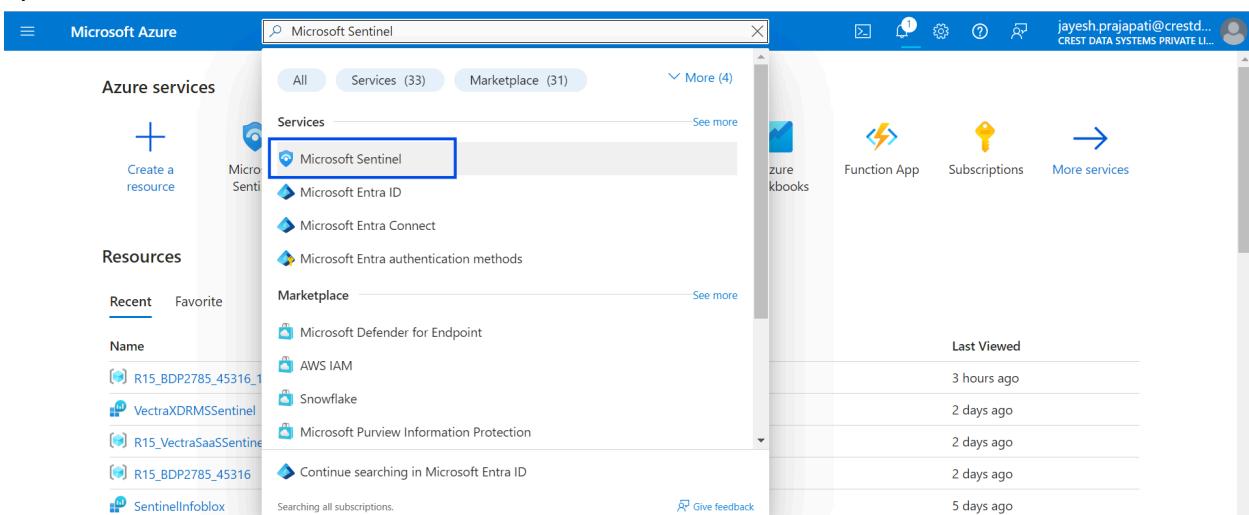
This **playbook** is triggered from two dashboards.

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**.



The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text "Microsoft Sentinel". Below the search bar, the "Azure services" section is visible, featuring a "Create a resource" button and a "Services" dropdown menu. The "Services" dropdown is open, and the item "Microsoft Sentinel" is highlighted with a blue rectangle. Other items in the dropdown include "Microsoft Entra ID", "Microsoft Entra Connect", and "Microsoft Entra authentication methods". To the right of the search bar, there are several navigation icons: "zure books", "Function App", "Subscriptions", and "More services". Below the search bar, there is a "Marketplace" section with a "See more" link. The "Resources" section shows a list of recent and favorite resources, including "R15_BDP2785_45316_1", "VectraXDRMSSentinel", "R15_VectraSaaSSENTINEL", "R15_BDP2785_45316", and "Sentinellnfblox". On the far right, there is a "Last Viewed" section listing resources last viewed at different times: "3 hours ago", "2 days ago", "2 days ago", "2 days ago", and "5 days ago".

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.

The screenshot shows the 'Playbook templates (Preview)' section of the Azure Automation portal. It displays two 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 'Basic' tab is selected, showing the following details:

- Subscription:** Using Microsoft Sentinel
- Resource Group:** Content hub
- Last update time:** 7/17/2024, 5:05...
- Description:** This playbook will create an incident for malicious ip and notify to pre-defined or user customizable email id.
- Connectors in use:** Microsoft Sentinel, Azure Monitor Logs, Outlook.com
- Prerequisites:** User should have an outlook mail account in order

A green box highlights the **Create playbook** button at the bottom right.

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 *

Playbook name *

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)

 *

WorkspaceName (i)

 *

< 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 (**TeamCymruScoutCreateIncidentAndNotify**).

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

- Logic app name:** TeamCymruScoutCreateIncidentAndNotify
- Location:** East US
- Subscription:** [redacted]
- Workflow URL:** https://prod-70.eastus.logic.azure.com:443/workflows/2a044e49...
- Tags:** environment : Production
- Run history tab:** The 'Run history' tab is selected, showing 0 runs.

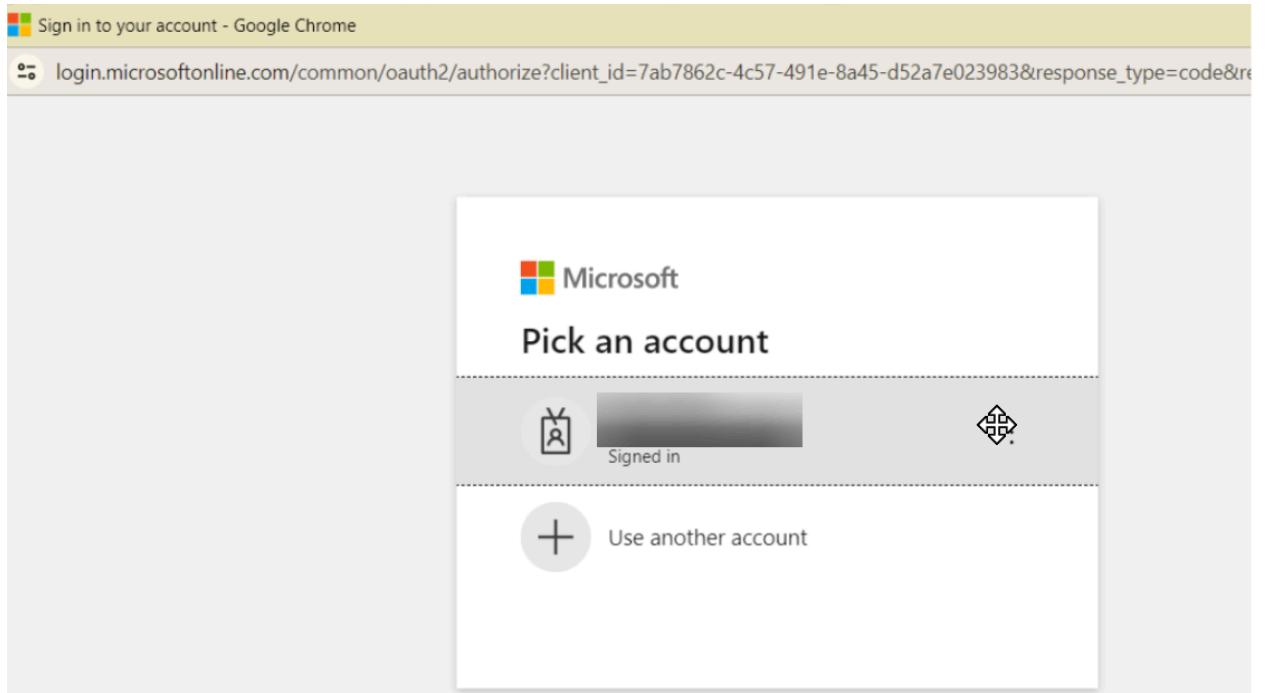
2. Go to API connections

The screenshot shows the Azure Logic App interface for the 'CymruScoutCreateIncidentAndNotify' app. The left sidebar has 'API connections' selected. The main area displays 'API connections associated with the logic app' with three entries: 'Azuremonitorlogs-CymruScoutCreateIncidentAndNotify', 'MicrosoftSentinel-CymruScoutCreateIncidentAndNotify', and 'Outlook-CymruScoutCreateIncidentAndNotify'. The 'Azuremonitorlogs-CymruScoutCreateIncidentAndNotify' entry is highlighted.

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

The screenshot shows the 'Edit API connection' dialog for the 'Azure Monitor Logs' connection. The dialog has tabs for 'General' and 'Properties'. The 'General' tab is selected, showing the 'Display Name' as 'Azuremonitorlogs-CymruScoutCreateIncidentAndNotify'. The 'Authorize' button is visible at the bottom right. The background shows the original Logic App interface with the 'API connections' page selected.

- 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.

The screenshot shows the Azure portal's 'Edit API connection' page for 'Azuremonitorlogs-CymruScoutCreateIncidentAndNotify'. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, General, Properties, Monitoring, Automation, and Help. The 'Edit API connection' option is selected. The main area displays the API connection details: 'API' set to 'Azure Monitor Logs', 'Display Name' set to 'Azuremonitorlogs-CymruScoutCreateIncidentAndNotify', and an 'Authorize' button. At the bottom are 'Save' and 'Discard' buttons, with 'Save' being highlighted in blue.

- 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' Log Analytics workspace. The left sidebar has a red box around the 'Access control (IAM)' option. The top navigation bar has a red box around the 'Add' button. The main content area includes sections for 'My access', 'Check access', and 'Role assignments'.

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'. The results table shows one result: 'Microsoft Sentinel Contributor'.

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

Some results might be hidden due to your ABAC condition.

Subscription * CDS_R15_Sub1

Managed identity Logic app (159)

Select TeamCymruScoutCreateIncidentAndNotify

TeamCymruScoutCreateIncidentAndNotify /subscriptions/.../resourceGroups/...

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

Select managed identities

Some results might be hidden due to your ABAC condition.

Subscription *

Managed identity Logic app (159)

Select TeamCymruScoutCreateIncidentAndNotify

TeamCymruScoutCreateIncidentAndNotify /subscriptions/.../resourceGroups/...

Selected members: TeamCymruScoutCreateIncidentAndNotify

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]	[REDACTED]

Description Optional

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



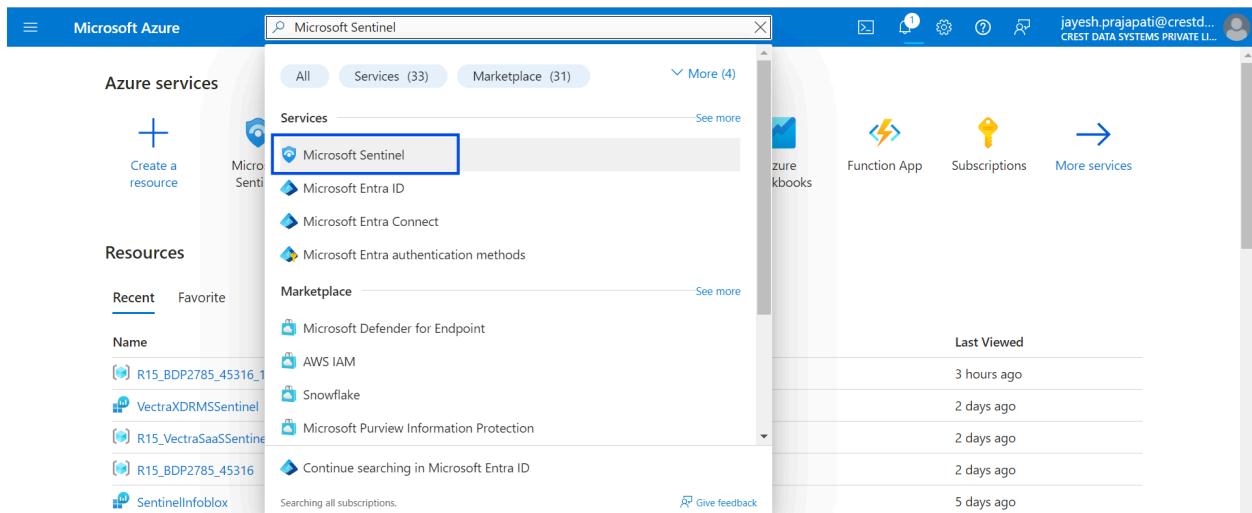
Team Cymru Scout Live Investigation Playbook

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**.

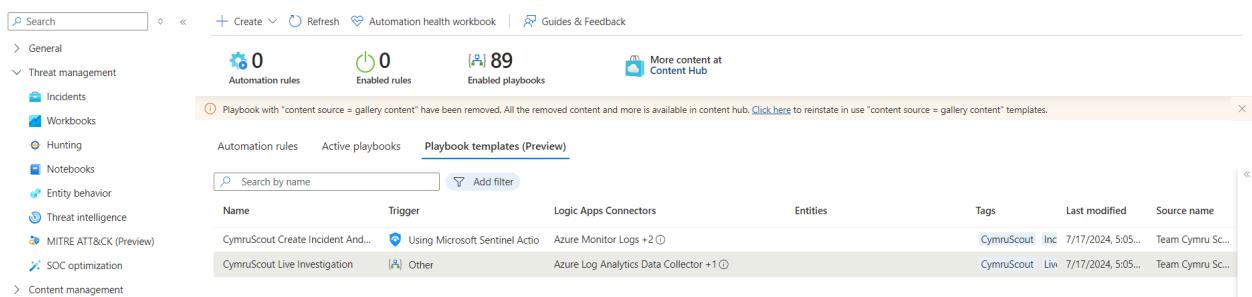
Configuration

1. Go to Microsoft Sentinel



The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains "Microsoft Sentinel". Below the search bar, the "Azure services" section is visible, with "Services" selected. A list of services is shown, and "Microsoft Sentinel" is highlighted with a blue box. To the right of the search bar, there are links for "Function App", "Subscriptions", and "More services". On the left, there's a sidebar with "Create a resource" and "Recent" and "Favorite" resources. The "Recent" section lists several resources, including "R15_BDP2785_45316_1", "VectraXDRMSentinel", "R15_VectraSaaSSENTINEL", "R15_BDP2785_45316", and "Sentinellnfolbox". On the right, there's a "Last Viewed" section with items like "zure kbooks", "3 hours ago", "2 days ago", etc.

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.



The screenshot shows the Microsoft Sentinel Automation blade. The left sidebar includes sections for General, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization), and Content management. The main area has tabs for "Automation rules", "Active playbooks", and "Playbook templates (Preview)". The "Playbook templates (Preview)" tab is selected. It displays a table with columns: Name, Trigger, Logic Apps Connectors, Entities, Tags, Last modified, and Source name. Two entries 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.

Name	Trigger	Logic Apps Co...	Entities	Tags	Last modified	Source name
CymruScout Create Incident A...	Using Micros	Azure Monitor Log	CymruScout Inc	7/17/2024, 5:05...	Team Cymru Sc...	
CymruScout Live Investigation	Other	Azure Log Analytic...	CymruScout Liv	7/17/2024, 5:05...	Team Cymru Sc...	

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 *

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**).
- **WorkspaceName:** Enter workspace name in which you want to fetch or store your data.

Create playbook ...

Basics **Parameters** Connections Review and create

UserName ⓘ *

Password ⓘ *

BaseURL ⓘ *

WorkspaceName ⓘ *

CreateIncidentAndNotifyPlaybookName ⓘ *
TeamCymruScoutCreateIncidentAndNotify

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**).

The screenshot shows the Azure Logic Apps portal. The top navigation bar includes 'Home', 'Microsoft Sentinel | Automation', and the logic app name 'TeamCymruScoutLiveInvestigation'. Below the navigation is a toolbar with 'Run', 'Refresh', 'Edit', 'Delete', 'Enable', 'Clone', 'Open in mobile', 'Export', and 'Provide feedback' buttons. The main area is titled 'Overview' and contains the following details:

Setting	Value	Definition	Status	Runs last 24 hours	Integration Account
Resource group (move)	[REDACTED]	: 1 trigger, 121 actions			
Location (move)	: East US		: Disabled		
Subscription (move)	[REDACTED]				
Subscription ID	[REDACTED]				
Workflow URL	: https://prod-59.eastus.logic.azure.com:443/workflows/4b921cb17...				
Tags (edit)	: environment : Production				

Below the details are tabs for 'Get started', 'Run history' (which is selected), 'Trigger history', and 'Metrics'. On the left, there's a sidebar with links like 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Development Tools' (with 'Logic app designer' and 'Logic app code view' options), and 'Help'.

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.

The screenshot shows the Azure API Connections portal. The top navigation bar includes 'Home', 'Microsoft Sentinel | Automation', and the connection name 'AzureLogAnalyticsdatacollector-CymruScoutLiveInvestigation | Edit API connection'. Below the navigation is a toolbar with 'Edit API connection' (which is selected) and other options like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings', 'General', 'Properties', 'Monitoring', 'Automation', and 'Help'. The main area is titled 'Edit API connection' and contains the following fields:

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

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

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

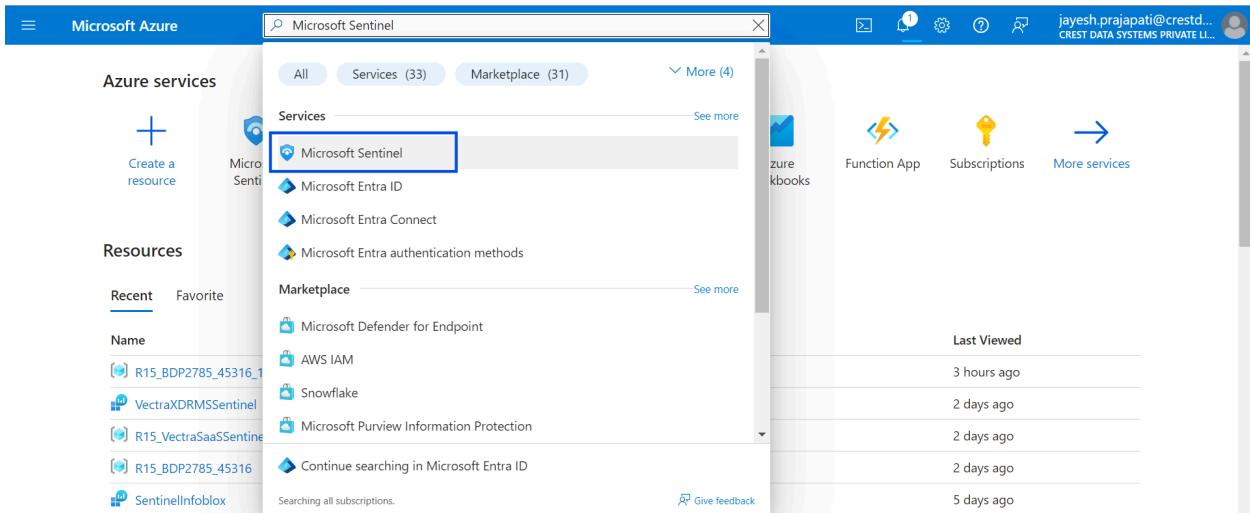
Team Cymru Scout Enrich Incident Playbook

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.

Automation rules Active playbooks **Playbook templates (Preview)**

Name	Trigger	Logic Apps Conn...	Entities	Tags	Last modified	Source name	
[IN USE] Team Cymru Scout Live ...	[A] Other	Azure Monit...	+1	[IP]	Team Cymru Scou	13/08/2024, 17...	Team Cymru Sc...
Team Cymru Scout Enrich Incident	Microsoft Sentinel Incident	Azure Log ...	+3	[IP +1]	Team Cymru Scou	09/05/2025, 05...	Team Cymru Sc...
[IN USE] Team Cymru Scout Crea...	Using Microsoft Sentinel Actio	Microsoft S...	+2	[IP]	Team Cymru Scou	13/08/2024, 17...	Team Cymru Sc...

3. Click on the Create Playbook button.

Automation rules Active playbooks **Playbook templates (Preview)**

Name	Trigger	Logic Apps Co...	Entities	Tags	Last modified	
[IN USE] Team ...	[A] Other	Azure M...	+1	[IP]	Team Cymru Scou	13/08/2024,
Team Cymru Sc...	Microsoft Se...	Azure L...	+3	[IP +1]	Team Cymru Scou	09/05/2025,
[IN USE] Team ...	Using Micros...	Microso...	+2	[IP]	Team Cymru Scou	13/08/2024,

Team Cymru Scout Enrich Incident

Trigger type: Microsoft Sentinel Incident

Content source: Content hub

Last update time: 09/05/2025, 05:00

Description: This playbook will fetch and ingest IP or Domain Indicator data based on Entity mapped in Microsoft Sentinel Incident and notify to pre-defined or user customizable email id.

Connectors in use:

- Microsoft Sentinel
- Azure Log Analytics Data Collector
- Azure Monitor Logs
- Outlook.com

Prerequisites:

- User should have an outlook mail account in order to use this playbook.

Activate Windows:

Get Started to activate Windows.

Create playbook

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 *

▼

Playbook name *

Enable diagnostics logs in Log Analytics i

Log Analytics workspace

▼

[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.

Create playbook

...

Basics

Parameters

Connections

Review and create

UserName (i)

*

Password (i)

*

BaseUrl (i)

*

EmailId (i)

*

WorkspaceName (i)

*

< Previous

Next : Connections >

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**).

The screenshot shows the Azure Logic Apps portal. The top navigation bar includes 'Home >', a search bar, and various action buttons like 'Run', 'Edit', 'Delete', 'Disable', 'Clone', 'Open in mobile', 'Export', and 'Provide feedback'. The main area is titled 'TeamCymruScoutEnrichIncident' with a status of 'Running'. The 'Overview' tab is selected, displaying details such as Resource group, Location, Subscription, Workflow URL, and Tags. A summary table on the right indicates 1 trigger, 161 actions, Enabled status, 2 successful, 0 failed runs, and the Integration Account.

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.

The screenshot shows the 'API connections associated with the logic app' section. It lists several connections, including 'MicrosoftSentinel-TeamCymruScoutEnr...', 'Azureloganalyticsdatacollector-TeamCymruScoutEnr...', 'Azuremonitorlogs-TeamCymruScoutEnr...', and 'Outlook-TeamCymruScoutEnrichIncide...'. The 'Edit API connection' dialog is open for the 'Azureloganalyticsdatacollector-TeamCymruScoutEnrichIncident' connection. The dialog title is 'Edit API connection' with a pencil icon. It contains fields for 'Display Name' (set to 'Azure Log Analytics Data Collector') and 'API' (set to 'Azure Log Analytics Data Collector'). Below these are fields for 'Workspace ID' (containing a redacted value) and 'Workspace Key' (containing a redacted value). At the bottom are 'Save' and 'Discard' buttons.

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**.

The screenshot shows the 'Access control (IAM)' page for a Log Analytics workspace named 'CymruTest2503'. 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. A dropdown menu is open over the '+ Add' button, with 'Add role assignment' highlighted.

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

The screenshot shows the 'Add role assignment' wizard. The 'Members' tab is selected. A search bar contains 'Microsoft Sentinel Contributor' with a red box around it. Below the search bar are 'Type : All' and 'Category : All' filters. The results table shows one entry: 'Microsoft Sentinel Contributor' with a description of 'Microsoft Sentinel Contributor'. At the bottom, there are 'Review + assign', 'Previous', and 'Next' buttons, with 'Next' highlighted by a red box.

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

The screenshot shows two overlapping windows. The top window is titled 'Select managed identities' and displays a list of identities under 'Subscription *'. One item, 'Logic app (184)' under 'Managed identity', is highlighted with a red box. The bottom window is titled 'Add role assignment' and shows the 'Members' tab selected. Under 'Assign access to', the 'Managed identity' option is selected and highlighted with a red box. A button '+ Select members' is also visible.

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

Subscription *

CDS_R15_Sub1



Managed identity

Logic app (184)



Select ⓘ

TeamCymruScoutEnrich

TeamCymruScoutEnrichIncident
/subscriptions/.../resourceGroups/...

Selected members:

TeamCymruScoutEnrichIncident
/subscriptions/.../resourceGroups/... [Remove](#)

Select

Close

Feedback

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.

Microsoft Sentinel | Logs

Selected workspace: 'cymrutest2503'

New Query 1 ... +

Search

Favorites

- Logs
- Data connectors
- Content hub
- Workbooks

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior

Functions

Search

Shows : 1000 results

one of the queries to start

Favorites

You can add favorites by clicking on the icon

LogManagement

Microsoft Sentinel

Workspace functions

- CymruScoutAccountUsage
- CymruScoutCorrelate
- CymruScoutDomain
- CymruScoutDomainData
- CymruScoutIdentity
- CymruScoutIP
- CymruScoutProtoByIP
- CymruScoutSummary
- CymruScoutSummaryTopCerts
- CymruScoutSummaryTopFing...

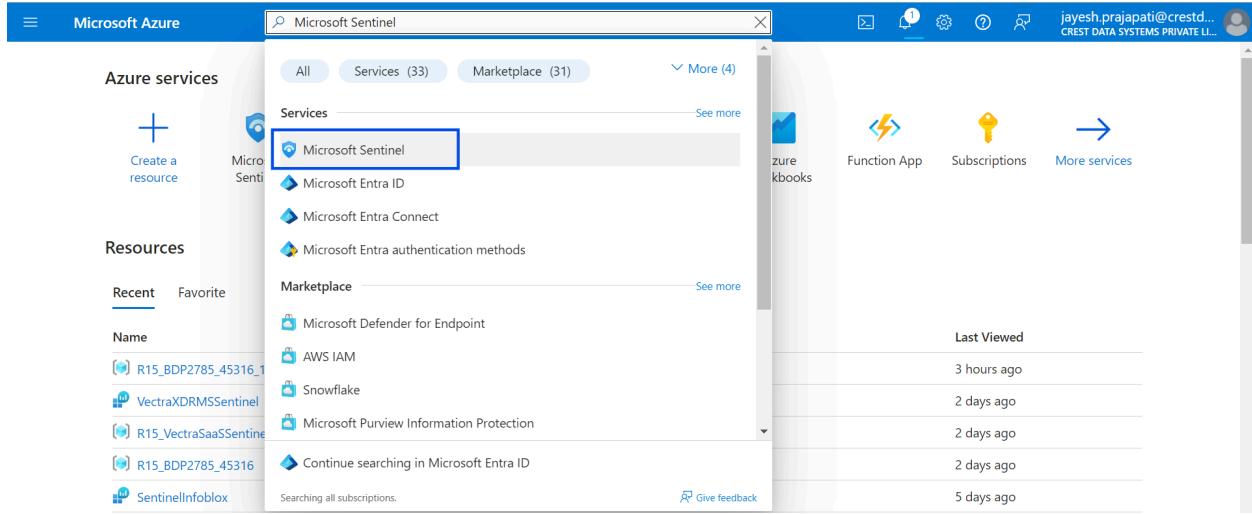
marize Time = max(TimeGenerated)

marize Time = max(TimeGenerated) |

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:

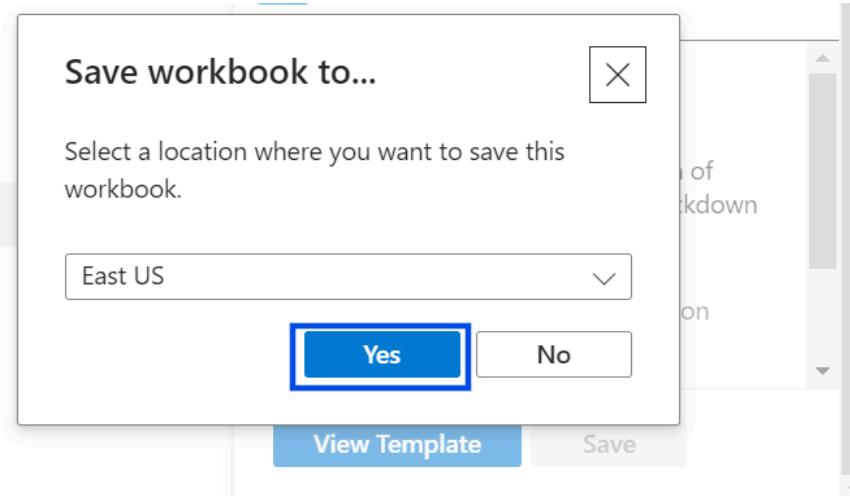


The screenshot shows the Microsoft Azure portal homepage. The search bar at the top contains the text "Microsoft Sentinel". Below the search bar, the "Services" section is expanded, showing a list of services. The "Microsoft Sentinel" service is highlighted with a blue border. Other listed services include 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". On the left side, there are sections for "Azure services" (with a "Create a resource" button) and "Resources" (Recent and Favorite items like R15_BDP2785_45316_1, VectraXDRMSentinel, R15_VectraSaaSSENTINEL, R15_BDP2785_45316, and SentinelInfoblox). On the right, there are sections for "Last Viewed" (3 hours ago, 2 days ago, 2 days ago, 2 days ago, 5 days ago) and "Marketplace" (listing Microsoft Defender for Endpoint, AWS IAM, Snowflake, and Microsoft Purview Information Protection).

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 interface. On the left, there's a navigation sidebar with various categories like General, Threat management, Workbooks, and Configuration. Under Workbooks, 'Templates' is selected. In the main area, there's a 'My workbooks' section with a count of 0 and a 'Templates' section with a count of 1. The template listed is 'Team Cymru Scout Template Test'. To the right, a detailed view of this template is shown, including its description, content source (Team Cymru Scout), template version (1.0.0), author (cymruscout), and supported by Microsoft Corporation. There are 'View Template' and 'Save' buttons at the bottom.

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 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.

Steps to Create Incident and Notify for a Malicious Indicator.

- 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 **TeamCymruScoutLiveInvestigation 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 button 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.

The screenshot shows the 'Correlation Overview' tab selected in a top navigation bar. The main content area displays a note about dependencies on ASIM Parsers and ThreatIntelligence indicators, followed by a section titled 'Steps to perform Correlation using this workbook' with a bulleted list of instructions and a note section.

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.

www.cymru.com

901 International Parkway, Suite 350, Lake Mary, FL 32746, USA
TEAM CYMRU. COPYRIGHT © 2025. ALL RIGHTS RESERVED

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 dark-themed web page titled "Deploy ASIM". It contains a table with eight rows, each representing an ASim Schema. The columns are "ASim Schema", "Deploy", and "Deploy to Azure Gov". Each row has two buttons: "Deploy to Azure" and "Deploy to Azure Gov". The "Dns" row is highlighted with a red box around its "Deploy to Azure" button.

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

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 one entry for March 26, 2025, at 12:00:00 highlighted and its status set to 'Success'. A red box highlights this row. To the right, a detailed log pane titled 'Invocation details' is open, showing the execution of the 'IPDataCollector' function. The log entries include information about the execution reason, trace logs, and the response message, which indicates no IP values were found in the input.

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 for the 'TeamCymruScout' workspace. On the right side, there is a dropdown menu for selecting the query mode. The 'Simple mode' option is currently selected, indicated by a checked checkbox. A red box highlights the 'KQL mode' option, which is also available in the dropdown.

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 Azure Log Analytics workspace interface. On the left, there's a sidebar with navigation links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Logs (which is currently selected). The main area has a search bar at the top, followed by a 'New Query' button and a time range selector set to 'Last 7 days'. Below that, a table displays the results of a KQL query. The table has columns: TimeGenerated [UTC], used_queries_d, remaining_queries_d, query_limit_d, foundation_api_usage_used_queries_d, foundation_api_usage_remaining_queries_d, and found. There are 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	found
> 3/25/2025, 12:50:01.063 PM	47504	52496	100000	11	0	0
> 3/25/2025, 12:40:01.184 PM	47488	52512	100000	10	0	0
> 3/25/2025, 12:30:01.291 PM	47466	52534	100000	9	0	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.

Add/Edit application setting

Name *	IPValues
Value	1.2.3.4,1.2.1.2

Deployment slot setting

IPValues

FUNCTIONS_*

IPTableName

LogLevel

Schedule

Apply **Discard**

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

Save changes

Your app may restart if you are updating app settings. Are you sure you want to continue?

Confirm **Cancel**

- 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.

Resource group (move) : [REDACTED] Definition : 1 trigger, 118 actions
 Location (move) : East US Status : Enabled
 Subscription (move) : [REDACTED] Runs last 24 hours : 8 successful, 5 failed
 Subscription ID : [REDACTED] Integration Account : --
 Workflow URL : https://prod-90.eastus.logic.azure.com:443/workflows/fb899f95...
 Tags (edit) : environment : Production

Get started Run history Trigger history Metrics

Specify the run identifier to open monitor view directly

Run Identifier	Status	Timestamp	Duration
08584585499708111292128761389CU61	Failed	3/27/2025, 11:58:34 AM	5.29 Seconds
085845850288747997831779984CU45	Failed	3/27/2025, 11:53:16 AM	5.72 Seconds
08584585507549093890279566646CU63	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.

Runs history TeamCymruScoutLiveInvestigation2703

Refresh

All

Pick a date Pick a time

Search to filter items by identifier

Start time Duration

- 3/27/2025, 2:11 PM 55.41 Seconds
- 3/27/2025, 2:09 PM 49.34 Seconds
- 3/27/2025, 2:08 PM 11.27 Minutes
- 3/27/2025, 12:13 PM 6.32 Seconds
- 3/27/2025, 12:09 PM 6.38 Seconds
- 3/27/2025, 12:07 PM 10.71 Seconds
- 3/27/2025, 12:05 PM 5.05 Seconds
- 3/27/2025, 12:00 PM 5.67 Seconds
- 3/27/2025, 11:58 AM 5.29 Seconds

Logic app run ...

08584585499708111292128761389CU61

Run Details Resubmit Cancel run Refresh Info Generally Available Designer

Condition To Verify Indicator Type Is IP 4s

ActionFailed. An action failed. No dependent actions succeeded.

INPUTS Show raw inputs

Expression result false

False

HTTP Request To Fetch Details Of Domain Indicator 2s

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.

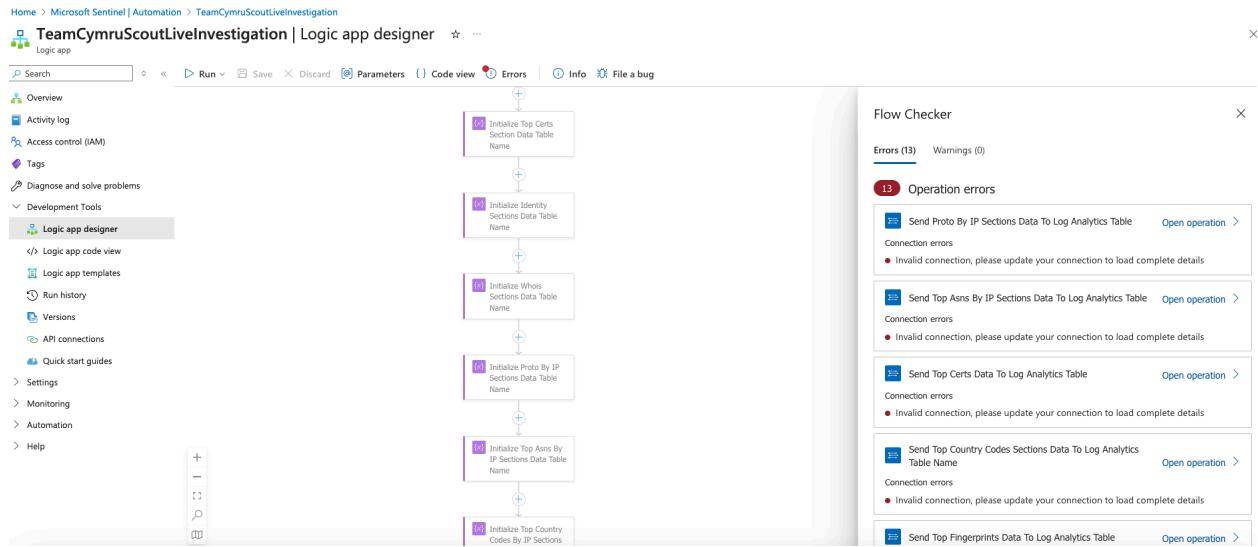
Problem1: This can occur because the default interval for the account usage function to retrieve data from the Scout API is set to **1 hour**.

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.