

# Configuring the Microsoft Sentinel Threat Intelligence - TAXII Connector

[Configuring the Microsoft Sentinel Threat Intelligence Connector](#)

[Changelog](#)

[Introduction](#)

[Threat Intelligence Solution Installation](#)

[TAXII Data Connector Configuration](#)

[Data Connector Configuration Details](#)

[Additional support](#)

## Changelog

Version	Description
2.0	Updated instructions to match new Microsoft Sentinel solution installation process

## Introduction

The ReversingLabs Early Detection of Ransomware Threat Intelligence feed has been designed to seamlessly integrate with Microsoft Sentinel. This document describes how to configure a Microsoft Sentinel instance to use this feed, which can be summarized as:

1. Install the "Threat Intelligence" solution in the Microsoft Sentinel content hub
2. Configure the "Threat Intelligence - TAXII" data connector from within the solution manager with your credentials and the details provided below
3. Verify that new indicators are delivered to Microsoft Sentinel

## Threat Intelligence Solution Installation

Microsoft provides a solution for Microsoft Sentinel named "Threat Intelligence" containing the required data connectors and related content. To install this solution, navigate to the Microsoft Sentinel content hub and search for "threat intelligence":

### Solutions (3)

The screenshot shows three solution cards in a grid. The first card, 'Threat Intelligence', is highlighted with a red border. It features a shield icon, 'FEATURED' and 'PREVIEW' tags, the text 'Threat Intelligence', 'Microsoft Sentinel, Microsoft Corporation', 'Security - Threat Intelligence', and tags for 'Analytics rule (38)', 'Data connector (4)', and '+2'. A green checkmark and the word 'Installed' are at the bottom. The second card is 'Cybersixgill Actionable Alerts' by Cybersixgill, with a blue star icon, 'Security - Threat Intelligence', and tags for 'Data connector' and 'Hunting query +2'. The third card is 'Digital Shadows SearchLight' by Digital Shadows, with a 'digital shadows' logo, 'Security - Threat Intelligence', and tags for 'Analytics rule (2)' and 'Data connector +2'.

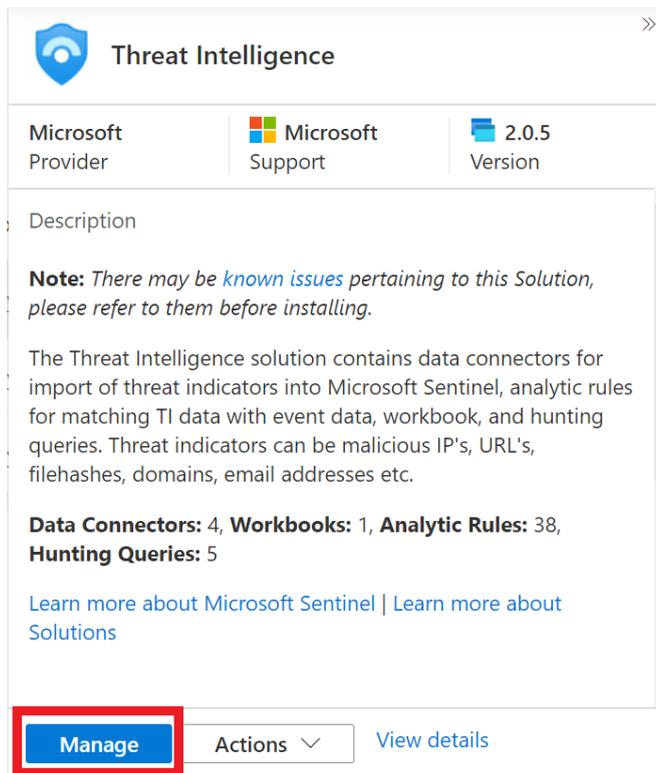
Select the solution, then click the “install” button in the fly-out menu:

The screenshot shows the 'Threat Intelligence' solution details fly-out menu. It has a title bar with the solution icon and name. Below the title bar, it lists 'Microsoft Provider', 'Microsoft Support', and '2.0.5 Version'. A 'Description' section contains a note: 'Note: There may be known issues pertaining to this Solution, please refer to them before installing.' followed by a paragraph: 'The Threat Intelligence solution contains data connectors for import of threat indicators into Microsoft Sentinel, analytic rules for matching TI data with event data, workbook, and hunting queries. Threat indicators can be malicious IP's, URL's, filehashes, domains, email addresses etc.' Below this, it lists 'Data Connectors: 4, Workbooks: 1, Analytic Rules: 38, Hunting Queries: 5'. At the bottom, there are links for 'Learn more about Microsoft Sentinel' and 'Learn more about Solutions', and an 'Install' button next to a 'View details' link.

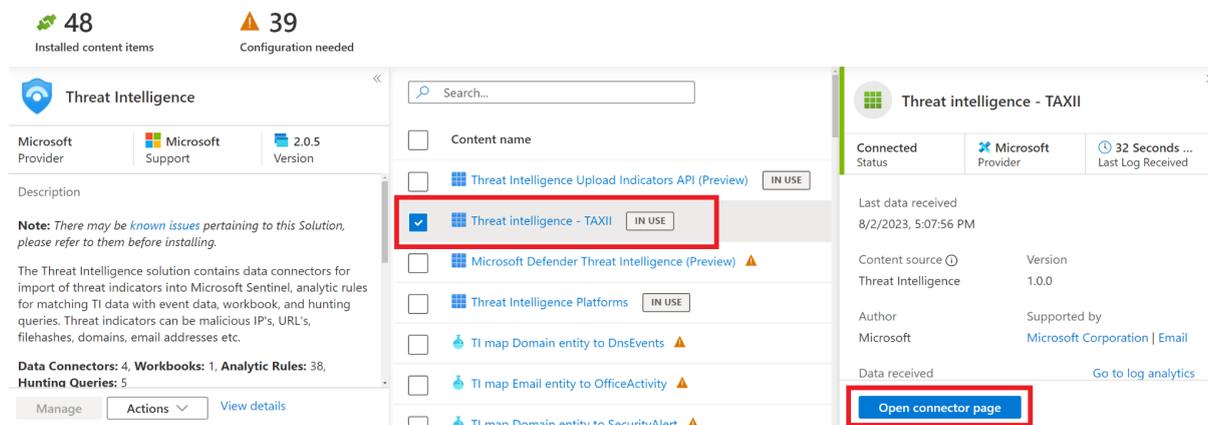
Once the solution has been installed, the relevant content should now be available as deployed templates.

# TAXII Data Connector Configuration

To begin configuring the data connector, select the Threat Intelligence solution and click the “manage” button:



In the solution management view, select the “Threat Intelligence - TAXII” data connector, then click the “Open connector page” button:



You will be redirected to the connector configuration page, where you will provide details such as your feed credentials and settings such as the polling frequency. The table below has been provided that describes the requirements:

Threat intelligence - TAXII

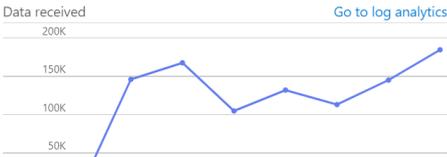
Connected Status
Microsoft Provider
32 seconds ago Last Log Received

**Description**  
 Microsoft Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting, and hunting using your threat intelligence. Use this connector to send threat indicators from TAXII servers to Microsoft Sentinel. Threat indicators can include IP addresses, domains, URLs, and file hashes.

Last data received  
 08/02/23, 05:09 PM

Related content  
2 Workbooks  
 2 Queries  
 35 Analytics rules templates

Data received Go to log analytics



**Instructions**

Configure TAXII servers to stream STIX 2.0 or 2.1 threat indicators to Microsoft Sentinel. You can connect your TAXII servers to Microsoft Sentinel using the built-in TAXII connector.

Enter the following information and select Add to configure your TAXII server.

Friendly name (for server) \*

API root URL \*

Collection ID \*

Username

Password

Import indicators:

All available
▼

Polling frequency

Once an hour
▼

Add

## Data Connector Configuration Details

Item	Parameter
Friendly name (for server)	<Name that you will recognize for this feed>
API root URL	<a href="https://data.reversinglabs.com/api/taxii/ransomware-api-root/">https://data.reversinglabs.com/api/taxii/ransomware-api-root/</a>
Collection ID	f0997a32-b823-562d-9856-c754ac5e1159
Username	<enter the username provided during the product activation>
Password	<enter the password provided during the product activation>
Import Indicators	<up to 30 days of indicators are stored on the server you can leave the default and import all 30 days or select a shorter time frame>
Polling Frequency	<we recommend the default of once per hour>

### Lost your password?

If you have lost or want to reset your password you can navigate to your SaaS resources in the Azure portal, find the subscription for ReversingLabs and then click the “Open SaaS Account on publisher’s site” link on the subscription details page.

# Additional support

Support can be obtained by contacting [support@reversinglabs.com](mailto:support@reversinglabs.com)