Configuring the Microsoft Sentinel Threat Intelligence - TAXII Connector

Changelog

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

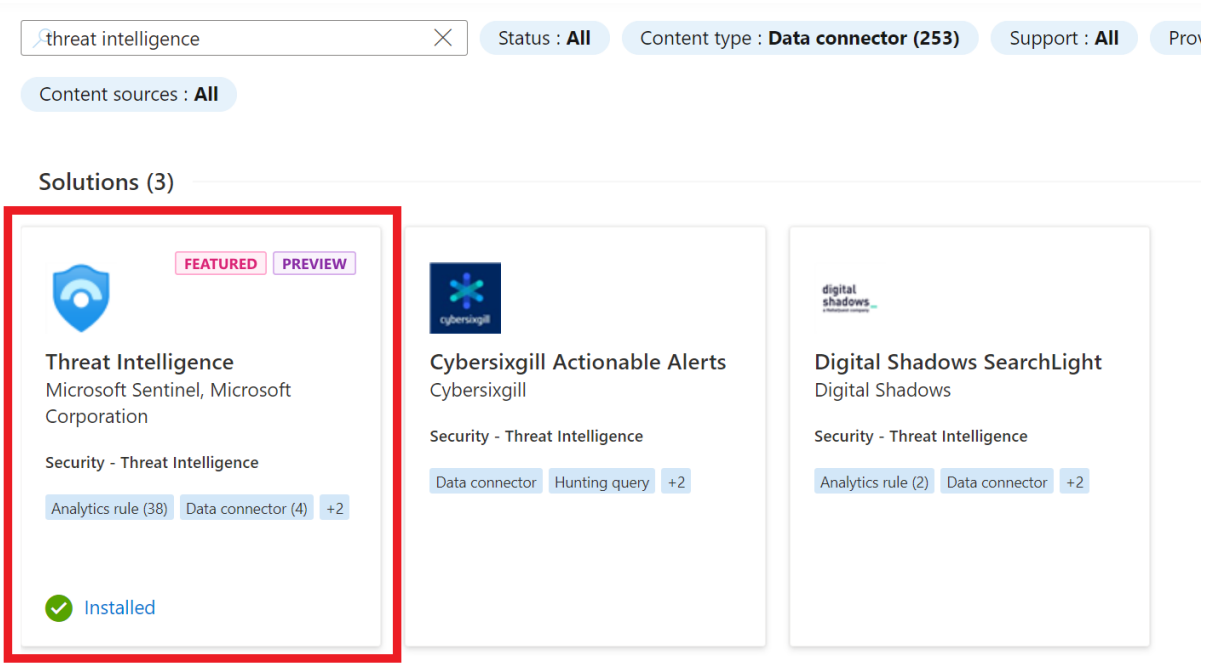
Introduction

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:

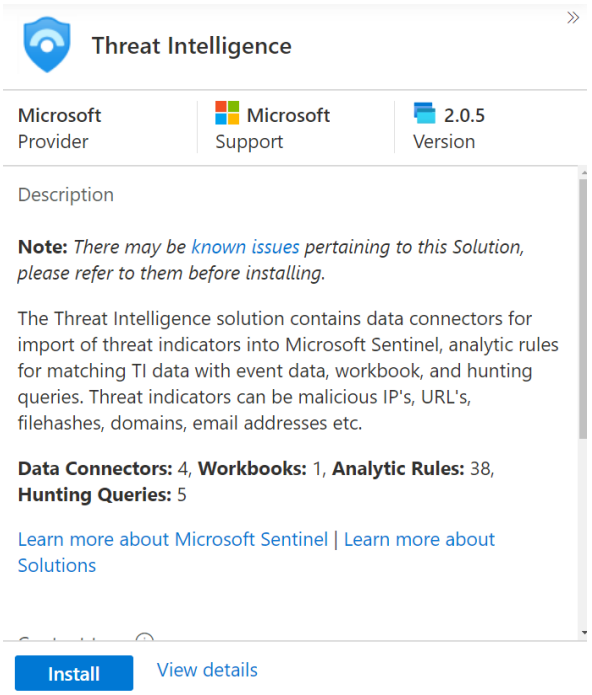
1. Install the “Threat Intelligence” solution in the Microsoft Sentinel content hub
2. Configure the “Threat Intelligence - TAXII” data connector from within the solution manager with your credentials and the details provided below
3. Verify that new indicators are delivered to Microsoft Sentinel

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”:



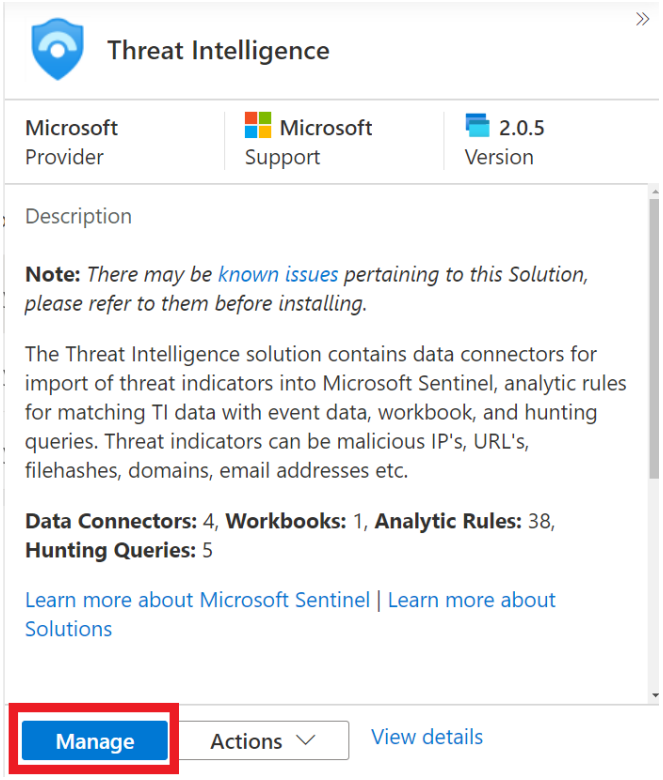
Select the solution, then click the “install” button in the fly-out menu:



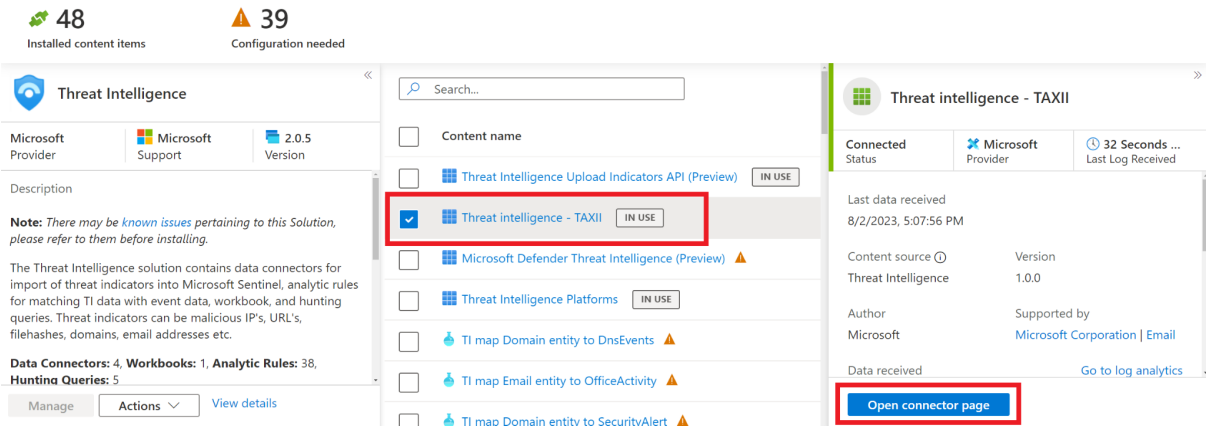
Once the solution has been installed, the relevant content should now be available as deployed templates.

TAXII Data Connector Configuration

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

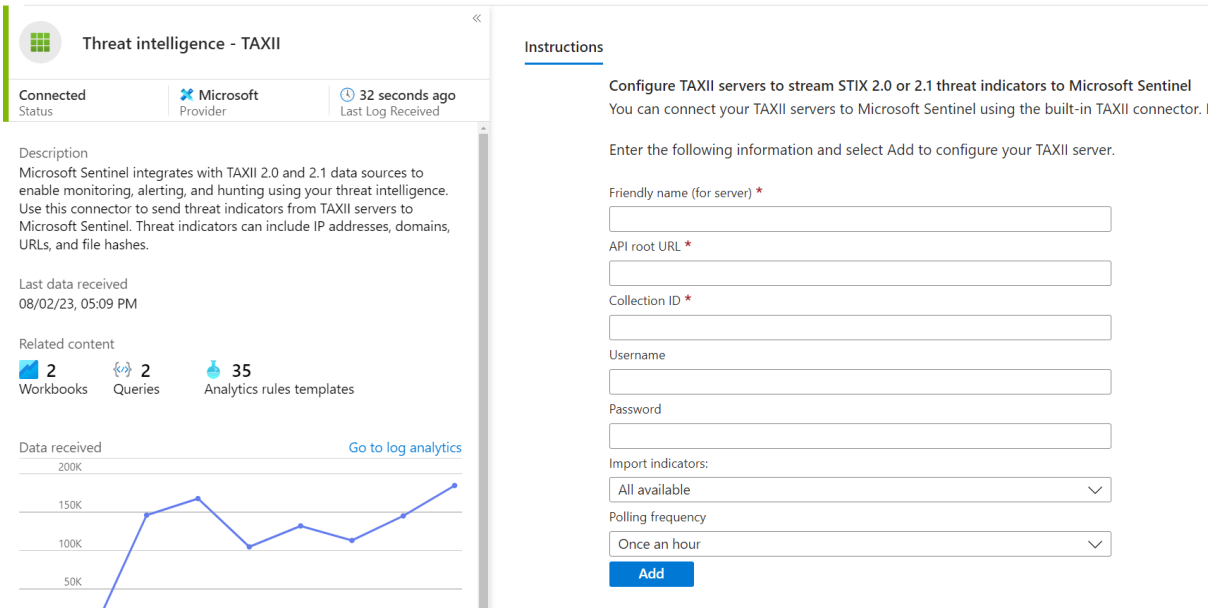


In the solution management view, select the “Threat Intelligence - TAXII” data connector, then click the “Open connector page” button:



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 ...



Data Connector Configuration Details

Item	Parameter
Friendly name (for server)	<Name that you will recognize for this feed>
API root URL	https://data.reversinglabs.com/api/taxii/ransomware-api-root/
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