Connect threat indicators to Microsoft Sentinel

# Plan for threat intelligence connectors

Threat indicators boost our ability to detect and prioritise known threats. Several features from Sentinel then become available or are enhanced such as:

* Analytics includes a set of scheduled rule templates you can enable to generate alerts and incidents based on matches of log events from your threat indicators.
* Workbooks provide summarised information about the threat indicators imported into Microsoft Sentinel and any generated from analytics rules that match your threat indicators
* Hunting queries allow security investigators to use threat indicators within the context of common hunting scenarios.
* Notebooks can use threat indicators when you investigate anomalies and hunt for malicious behaviours.

We can stream threat indicators to Sentinel via Threat intelligence platform (TIP) products, connecting to TAXII servers or direct integration with Microsoft Graph Security Indicators API.

The two TI connectos are TAXIII and TIP; both write to the threatintelligenceidicator table.

# Connect the threat intelligence TAXII connector

Sentinel integrates with TAXII 2.0 and 2.1 data sources to enable monitoring, alerting and hunting using your TI. Threat indicators can include IP addresses, domains, URLs and file hashes.

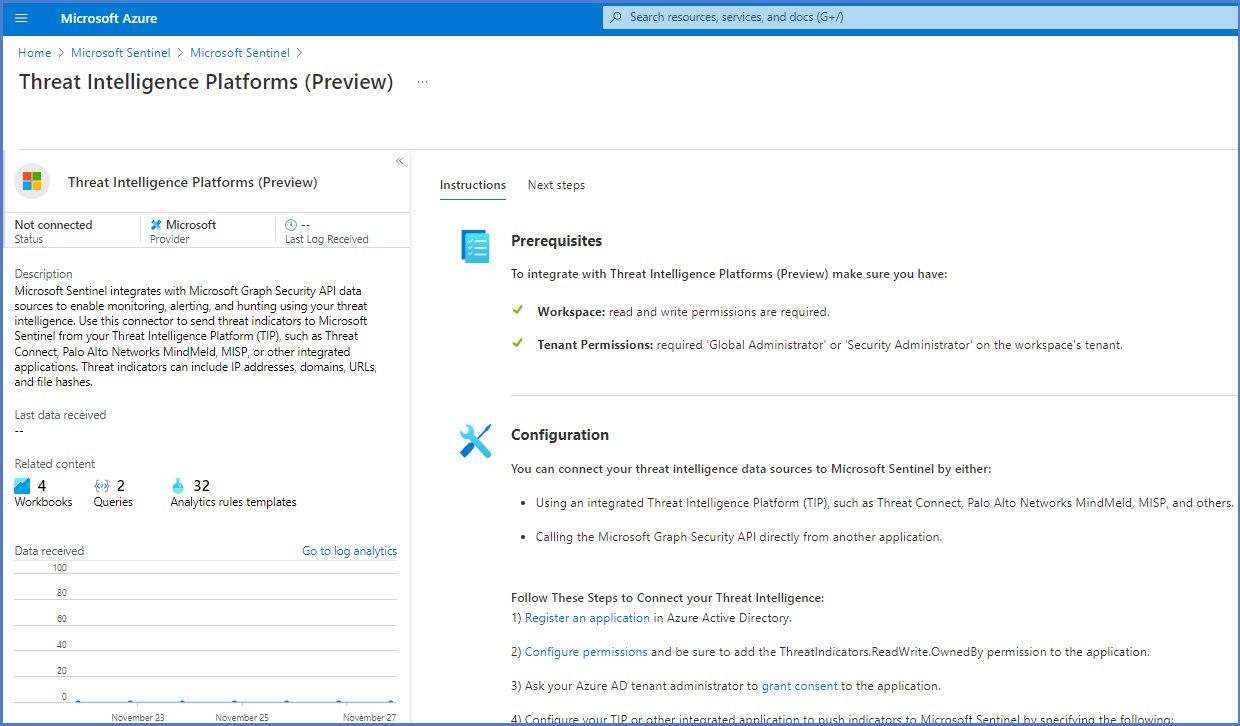
Graphical user interface, text, application, email

Description automatically generated

# Connect the threat intelligence platforms connector

1. Register an application in Azure Active Directory to get an application ID, application secret and Azure Active directory tenant ID. You need these values for when you configure your integrated TIP product or app that uses direct integration with Microsoft Graph Security tiIndicators API.
2. Configure API permissions for the registered application: Add the Microsoft Graph Application permission ThreatIndicators.ReadWrite.OwnedBy to your registered application.
3. Ask your AAD tenant administrator to grant admin consent to the registered application for your organisation. From the Azure Portal:  **AAD >- App registrations > <app name> > View API Permissions > Grant admin consent for <tenant name>.**
4. Configure your TIP product or app that uses direct integration with Microsoft Graph Security tiIndicators API to send indicators to Microsoft Sentinel by specifying the following:

* The values for the registered application’s ID, secret and tenant ID
* For the target product, specify Microsoft Sentinel
* For the action, specify alert



# View your threat indicators with KQL

The indicators reside in the ThreatIntelligenceIndicator table.