

kaspersky

Kaspersky Threat Intelligence Data Feeds for Microsoft Sentinel

Configuration Guide

Version 1.0

Kaspersky Threat Intelligence Data Feeds

Basics of Kaspersky Threat Data Feeds

First-tier security vendors and enterprises use time-tested and authoritative Kaspersky Threat Data Feeds to produce premium security solutions or to protect their business.

Cyber attacks happen every day. Cyber threats are constantly growing in frequency, complexity, and obfuscation, as they try to compromise your defenses. Adversaries currently use complicated intrusion kill chains, campaigns, and customized Tactics, Techniques, and Procedures (TTPs) to disrupt business or damage clients.

Kaspersky offers continuously updated Threat Data Feeds to inform your business or clients about risks and implications associated with cyber threats, helping you to mitigate threats more effectively and defend against attacks even before they are launched.

Kaspersky Threat Data Feeds contain thoroughly vetted threat indicator data sourced from the real world in real time.

In order to be used in Microsoft Sentinel, Kaspersky Threat Data Feeds are provided via TAXII collections (additionally the feeds can be delivered in JSON via HTTPS, for more information please contact intelligence@kaspersky.com).

Available TAXII collections

At the time of writing, the following collections are supported:

Collection description	Collection name	Collection ID ¹
Malicious URL Data Feed - a set of URLs that cover malicious websites and web pages.	TAXII_Malicious_URL_Data_Feed_Indicators	c11ae81e813b2f630b4139c8452d1e36
Phishing URL Data Feed - a set of URLs that cover phishing websites and web pages.	TAXII_Phishing_URL_Data_Feed_Indicators	a8b13dcb35e66276b4f84ea5116731da
Botnet CnC URL Data Feed - a set of URLs and hashes that cover desktop botnet C&C servers and related malicious objects.	TAXII_Botnet_CnC_URL_Data_Feed_Indicators	db92fd382b6b81b84af7e7dc0d4fbe64
IP Reputation Data Feed - a set of IP addresses that cover different categories of malicious hosts.	TAXII_IP_Reputation_Data_Feed_Indicators	e3b0eab15fd0b2063d2c741c990f8393
IP Reputation Data Feed - a set of high confidence IP addresses that cover different categories of malicious hosts.	TAXII_IP_Reputation_Data_Feed_Indicators_High_Confidence	b2d222813d61096390bc8c3e6e0746b5

¹ Collection ID may change

Malicious Hash Data Feed - a set of file hashes that cover the most dangerous, prevalent, or emerging malware.	TAXII_Malicious_Hash_Data_Feed_Indicators	68e6d1051c70ab988a6d95ed5c2bdfd0
--	---	----------------------------------

Configuration of Kaspersky Threat Intelligence Data Feeds in Microsoft Sentinel

To import Kaspersky Threat Intelligence Data Feeds into Microsoft Sentinel as TAXII Threat Intelligence source:

1. Create Log Analytics workspace in your Microsoft Azure Account.
2. Add Microsoft Sentinel into your workspace.
3. Open the “Threat Intelligence – TAXII” connector:

The screenshot shows the Microsoft Sentinel 'Data connectors' page. The breadcrumb path is 'Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel'. The page title is 'Microsoft Sentinel | Data connectors' with a sub-header 'Selected workspace: 'TAXIIfeeds''. There is a search bar with 'taxii' entered, and filters for 'Providers: All', 'Data Types: All', and 'Status: All'. A summary shows 123 connectors and 0 connected. A table lists the 'Threat intelligence - TAXII' connector by Microsoft.

Status	Connector name ↑
	Threat intelligence - TAXII Microsoft

The screenshot shows the Microsoft Azure portal interface for configuring the Threat intelligence - TAXII connector. The top navigation bar includes 'Microsoft Azure' and a search bar. The breadcrumb trail is 'Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel > Threat intelligence - TAXII'. The main content area is split into two columns. The left column displays the connector's status as 'Not connected', a description of its functionality, and a chart showing 'Total data received' (0) over time. The right column, titled 'Instructions', contains 'Prerequisites' (Workspace permissions and TAXII Server URI/ID) and a 'Configuration' section with a form for entering server details.

4. Configure the connector as follows:

Friendly name: <Specify the friendly name of the TAXII server>

API Root URL: <https://taxii.tip.kaspersky.com/v2/>

Collection ID: Specify the Collection ID for one of the supported collections².

You can check the ID of the specified collection by sending the following request:

```
curl -v -k -H "Accept: application/taxii+json;version=2.1" -u taxii:<TOKEN> https://taxii.tip.kaspersky.com/v2/collections/
```

Username: taxii

Password: Specify your token. To obtain a trial or commercial token, please contact intelligence@kaspersky.com

Import indicators: Select an appropriate option (e.g. 'All available')

Polling frequency: Select an appropriate option (e.g. 'Once per hour')

² See section 'Available TAXII collections'.

For example:

Instructions

Next steps

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:

Polling frequency

Add

List of configured TAXII servers

Friendly name ↑↓

TAXII server ↑↓

Collection ID ↑↓

No results

5. Click "Add".

After the indicators are pulled, you can use Kaspersky Threat Intelligence in Microsoft Sentinel:

Microsoft Sentinel | Overview Selected workspace: 'taxiifeeds'

Search (Ctrl+/) Refresh Last 24 hours

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

138.3K Events 138.3K 0 Alerts 0 Incidents

Incidents by status: New (0) Active (0) Closed (True Positive) (0)

Events and alerts over time

Alerts: 0
THREATINTELLIGENCE: 138.3K
USAGE: 2

Microsoft Sentinel | Threat intelligence Selected workspace: 'taxiifeeds'

Search (Ctrl+/) Refresh Add new Add tags Delete Columns Threat intelligence workbook Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics
- Watchlist
- Automation
- Settings

0 TI alerts 136.8K TI Indicators 1 TI sources

Search by name, values, description or tags Type: All Source: All Threat Type: All More (2)

Name	Values	Types	Source	Confidence
IP	94.101.179.215	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	117.57.29.254	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	175.150.105.225	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	177.75.42.68	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	186.216.182.148	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	78.96.87.205	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	111.179.93.151	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	121.205.231.169	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	94.203.202.195	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	18.176.196.9	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	140.250.146.65	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	146.70.59.150	ipv4-addr	Kaspersky-IP-Reputati...	80
IP	175.165.160.234	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	185.180.12.33	ipv4-addr	Kaspersky-IP-Reputati...	80
IP	182.204.158.232	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	182.179.157.191	ipv4-addr	Kaspersky-IP-Reputati...	74
IP	143.0.224.108	ipv4-addr	Kaspersky-IP-Reputati...	74

IP

74 Confidence Alerts

Tags: ipv4-addr

Values: ipv4-addr: 94.101.179.215

Threat types: Name: IP, Description: Revoked

Confidence: 74, Source: Kaspersky-IP-Reputation

Pattern: [ipv4-addr]value = '94.101.179.215', Kill chains

Created: Fri, Jul 8, 2022, 1:51:04 AM GMT+3, Valid from: Fri, Jul 8, 2022, 1:51:04 AM GMT+3

Valid until: Fri, Jan 1, 2100, 3:00:00 AM GMT+3, Modified: Fri, Jul 8, 2022, 2:34:31 PM GMT+3

Created by: -