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:

<table>
<thead>
<tr>
<th>Collection description</th>
<th>Collection name</th>
<th>Collection ID</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious URL Data Feed - a set of URLs that cover malicious websites and web pages.</td>
<td>TAXII_Malicious_URL_Data_Feed_Indicators</td>
<td>c11ae81e813b2f630b4139c8452d1e36</td>
<td></td>
</tr>
<tr>
<td>Phishing URL Data Feed - a set of URLs that cover phishing websites and web pages.</td>
<td>TAXII_Phishing_URL_Data_Feed_Indicators</td>
<td>a8b13dcb35e66276b4f84ea5116731da</td>
<td></td>
</tr>
<tr>
<td>Botnet CnC URL Data Feed - a set of URLs and hashes that cover desktop botnet C&amp;C servers and related malicious objects.</td>
<td>TAXII_Botnet_CnC_URL_Data_Feed_Indicators</td>
<td>db92d382b6b81b84af7e7d0d4fbe64</td>
<td></td>
</tr>
<tr>
<td>IP Reputation Data Feed - a set of IP addresses that cover different categories of malicious hosts.</td>
<td>TAXII_IP_Reputation_Data_Feed_Indicators</td>
<td>e3b0e15f0b2063d2c741c990f8393</td>
<td></td>
</tr>
</tbody>
</table>

1 Collection ID may change
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 |

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

| TAXII_Malicious_Hash_Data_Feed_Indicators | 68e6d1051c70ab988a6d95ed5c2bdf0 |

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:
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:

   ```
   ```

   **Username**: taxi

   **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**

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)**:
  - Kaspersky-IP-Reputation

- **API root URL**:
  - https://taxii.tip.kaspersky.com/v2/

- **Collection ID**:
  - e3b0eab15fd0b2063d2c741c990f8393

- **Username**:
  - taxii

- **Password**:
  - <TOKEN>

- **Import indicators**:
  - All available

- **Polling frequency**:
  - Once an hour

- **Add**

**List of configured TAXII servers**

<table>
<thead>
<tr>
<th>Friendly name</th>
<th>TAXII server</th>
<th>Collection ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No results

5. Click “Add”.
After the indicators are pulled, you can use Kaspersky Threat Intelligence in Microsoft Sentinel:

www.kaspersky.com/
www.securelist.com

© 2022 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owners