



Threat Intelligence Platforms (Preview)

Last updated by | Hekmat Abuzahrah | Mar 30, 2023 at 8:35 AM CDT

Generic Information about the Connector and Security Graph API

1. Security Graph API can be accessed here: <https://developer.microsoft.com/en-us/graph/graph-explorer>  - AAD permissions are required so it can only be done via your Visual Studio subscription tenant
2. There is a ready to go command that can add a TI indicator to the Graph backend -> It will not work. Instead use the following Indicator as the body <https://docs.microsoft.com/en-us/graph/api/tiindicators-post?view=graph-rest-beta&tabs=http> 

Interesting Detail:

TI has retention time of 1 year. However, GSA serves TI by TenantID+AppID (the application ID that uploads the TI through GSA). If the TI are uploaded with one AppID but then queried with another AppID, the data will not be returned.

The idea is most TI info is owned by the TI provider. See 2 providers (with different application ID to upload TI) serve same customer (tenant ID), it will be bad if one provider can see the TI uploaded by another provider.

This means that, if the TI are fetched via an automated process using an APP registered in AAD, and then the user tries to get those TI by sending an API request using the auth token of their AAD user the return will be empty.