Taxii Connector TSG

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

Troubleshooting steps

Backend Telemetry:

```
cluster('SecurityInsights').database('SecurityInsightsProd').ServiceFabricDynamicOE
| where env_time > ago(10d)
//| where resultType == "Failure" or resultType=="ClientError"
| where customData contains "e6a8b789-4565-419e-b899-7d78990b5bbe" //workspace id
| where operationName contains "Sentinel.Connectors.ConnectorsService.Handlers.ConnectorTypeHandlers.TaxiiConn
| project env_time, operationName, resultType,  resultSignature, resultDescription, rootOperationId, customDat
```

Result example - API URLs invalid

```
{"x-ms-client-request-id":["460e0d78-4b23-4dbb-b9f8-31253fe6703b"],"workspaceRegion":"eastus","subscriptionId"
   at Microsoft.Azure.Sentinel.Connectors.Common.Clients.Interflow.TaxiiClient.AddTaxiiClientAsync(String tena
   at Microsoft.Azure.Sentinel.Connectors.ConnectorsService.Handlers.ConnectorTypeHandlers.TaxiiConnectorHandl
```

Taxii URL Structure:

Official taxii requirements: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html#_Toc31107529

Helpful Curl requests

```
If your TAXII Server implements TAXII 2.0
curl -u <username>:<password> <ApiRoot> -H "Accept: application/vnd.oasis.taxii+json; version=2.0"
curl -u <username>:<password> <ApiRoot>/collections/<CollectionId> -H "Accept: application/vnd.oasis.taxii+jso
curl -u <username>:<password> <ApiRoot>/collections/<CollectionId>/objects/ -H "Accept: application/vnd.oasis.



If your TAXII Server implements TAXII 2.1
curl -u <username>:<password> <ApiRoot> -H "Accept: application/taxii+json; version=2.1"
curl -u <username>:<password> <ApiRoot>/collections/<CollectionId> -H "Accept: application/taxii+json; version
curl -u <username>:<password> <ApiRoot>/collections/<CollectionId>/objects/?limit=1 -H "Accept: application/ta
```

Anomaly Deprecation statement:

https://www.anomali.com/resources/limo

Helpful ICMs:

1. https://portal.microsofticm.com/imp/v3/incidents/details/335462260/home
2. https://portal.microsofticm.com/imp/v3/incidents/details/328558056/home