TAXII Working Call

2018-02-20

Editor Needed

- I made a call to the list for a volunteer to help me do editorial work on the TAXII specification

Update JSON Reference #43

- TAXII 2.0 references RFC 7159 for JSON. It was obsoleted by RFC 8259
- TAXII 2.1 should reference RFC 8259. Additionally, RFC 8259 changes course on Character Encoding, moving away from non-UTF-8 payloads.
- What do we need to do here? What changes to UTF-8?
  - JSON content MUST be encoded using UTF-8

Issue 43

	The JSON MTI serialization uses the JSON array type [RFC7159], which is an ordered list of zero or more values.

`string`	The `string` data type represents a finite-length string of valid characters from the Unicode coded character set [ISO10646] that are encoded in UTF-8. Unicode incorporates ASCII [RFC0020] and the characters of many other international character sets.

Returning the number of results is not explicitly clear #42

- In the 2.0 specification we talk about the server returning the total number of results. It is felt that this is not super clear. Does this mean the number of records in the collection or the number of records that match a certain query. All it says is "in a result set". If we keep this in our new pagination style, when that is designed, it should probably be made to be optional and it should probably be the total number of objects / items in the collection, not the number of objects that match the current filtered query.

- For example: "items 10-49/500", "500" represents the total number of items available.

Trailing-slash normative requirement for resource identifiers is missing #41

- All of the examples and resource definitions call out that the TAXII resources have a trailing slash. However, we forgot to add a normative statement saying as much. I propose we add a simple normative statement that says "All TAXII resources MUST have a trailing slash, as shown in their definitions." Or something like that.

Add Delete Capability to Object Endpoints #38

- We need to discuss how a client that has posted content to the TAXII server can delete the objects from the server collections.
- Currently, there is no easy way to do that and using revoke of an object has problems.

Add clarifying text around the types of errors you should get and when #22

- We probably need to add a bit more clarifying text to the spec to say what should happen under the following conditions, so that people implement this the same way:
  - If no data is returned for a filter
  - If the filter parameters are wrong
  - If some of the filter parameters are right and some are wrong

The X headers are not clear about which date #19

- In the spec we defined two headers X-TAXII-Date-Added-First and X-TAXII-Date-Added-Last.
- Should this be the time the object was added to the server or the time it was added to the collection that you are pulling from...
- When I wrote this originally, I was thinking about the time it was added to the server. But now that I have working code and am trying to implement this feature, there is a difference between when an object is added to a server and when it was put in a collection. Some times these will be the same time, other times, an object may be added to a collection after some sort of analysis, which means it was already in the server.

Issue 19

Custom Headers	
`X-TAXII-Date-Added-First`	The X-TAXII-Date-Added-First header is an extension header. It indicates the **`date_added`** timestamp of the first object of the response from ~~a~~the requested collection. This timestamp is collection specific. This header SHOULD only be present on responses to the **<api-root>**/collections/**<id>**/ and **<api-root>**/collections/**<id>**/objects/ endpoints. Behaviour of this header on any other endpoint, is not defined. The value of this header **MUST** be a `timestamp`. All HTTP 200 and 206 responses to the following Endpoints **MUST** include the `X-TAXII-Date-Added-First` header: • GET <api-root>/collections/objects/ • GET <api-root>/collections/manifest/
`X-TAXII-Date-Added-Last`	The X-TAXII-Date-Added-Last header is an extension header. It indicates the **`date_added`** timestamp of the last object of the response from ~~a~~the requested collection. This timestamp is collection specific. This header SHOULD only be present on responses to the **<api-root>**/collections/**<id>**/ and **<api-root>**/collections/**<id>**/objects/ endpoints. Behaviour of this header on any other endpoint, is not defined. The value of this header **MUST** be a `timestamp`. All HTTP 200 and 206 responses to the following Endpoints **MUST** include the `X-TAXII-Date-Added-Last` header: • GET <api-root>/collections/objects/ • GET <api-root>/collections/manifest/

Review Proposed Breaking Changes

TAXII Discovery URL Collides With Existing Product URLs #18

- During interoperability testing, the CTI TC learned that the /taxii/ URL conflicts with existing product URLs. The conflict prevents effective implementation of TAXII2 for existing products, which is undesirable.
- Proposal: change the DiscoveryURL from /taxii/ to /taxii2/.

Need to change the media type for STIX and TAXII per OASIS / IETF / IANA #29

- Need to make a change to the media types as IANA will not approve us using the vendor tree, we need to use the standards tree.
- Proposal: We discussed this at the F2F and the consensus is that we need to make a change. There is an open question about using a single media type to represent both STIX and TAXII or keep using two.

Manifest Resource Cannot Accurately Specify All Media Types and Version Combinations #36

- The manifest resource specifies a list of versions and a list of media types. However, not all version and media type combinations are necessarily valid and pagination problems exist when versions are added much later in the dataset.
- Proposal: Change manifest resource from "one manifest for all versions of an object" to "one manifest per object version and media type"

Item Based Pagination is Unusable for Rapidly Changing Datasets #23

- When a resource changes faster than a client can page through it, pagination becomes unpredictable.
- Single database transaction forces millions of records to have the same date_added timestamp.
- Proposal: Investigate and verify in code a solution to replace Item based pagination. One option is to sub-sort content with same date_added value by ID and then add an id_after URL parameter.

New Topics

Dereference Objects

- TAXII should support the ability to automatically dereference objects. Meaning, if you request a STIX indicator and the client says auto-dereference the object, then the TAXII server should send the identity object that is linked via the created_by_ref at the same time.

Find Objects Using an ID

- One should be able to find objects that relate to a given ID, either embedded or external relationship.
- For example: Given an Indicator STIX ID, give all relationships that list that ID in one of the fields.

Resolve to Some Depth

- TAXII should support the ability for a client to tell it to automatically send external relationship objects and their end points to some depth level. This depth level should be configurable on the server and probably advertised either at the api-root level, server level, or maybe even collection level.