TAXII Working Call

2019-07-16

TAXII 2.1 Status

- TAXII 2.1 Working Draft 05 was approved as CSD02 on December 15, 2018
- TAXII 2.1 CSD02 went to public review from December 15th - End of January 2019
- TAXII 2.1 Working Draft 06 was released on January 24th, 2019
  - There was an objection due to not addressing the yet-to-be decided Cyber Observable changes
  - We added a change to address this in Working Draft 07
  - We are currently at TAXII 2.1 Working Draft 07

TAXII 2.1 Status

- During the last F2F basic querying functionality came back up, specifically about pivoting
- After we decide this, we can ship TAXII 2.1

Search / Query Proposals

- We have had three very different proposals
- Option 1: Jason’s and Terry’s proposal for a query resource object to allow full TAXII query
- Option 2: A lightweight TAXII endpoint to allow pivoting on relationships
- Option 3: Marlon’s proposal to expand the filtering URL parameters

Option 1 - Full Query

- Create one or more search endpoints like
  - {api-root}/collections/{id}/search/
  - {api-root}/search/
- These endpoints would accept some sort of “query or information-request object/resource”
- This object / resource would need to be fleshed out, including what types of queries would be allowed and how would they be structured.

Option 2 - Relationships

- Create an endpoint like:
  - {api-root}/collections/{id}/relationships/related/{stix-id}/
- This would result in a simple database query and URL filtering logic. This would follow the same URL filtering and path design we already have.
- Pseudo SQL code: select * from table-objects where type=relationship && (source_ref = stixid || target_ref = stixid)

TAXII Query Options SWOT

- Strengths
  - Option 1 - Might allow all of the query options that we would need in the future. Might work for TAXII Channels.
  - Option 2 - This is something we could do in a matter of days not months.
  - Option 3 - Somewhat straight forward, but we would need Marlon to present his idea again.

TAXII Query Options SWOT

- Weaknesses
  - Option 1 - It will take some time to get right (6-12 months) and we may still release something that needs to be refactored later on. This is also a big feature to add this late in the release cycle.
  - Option 2 - It does not address all of the things we need out of TAXII Query. It only solves one use case.
  - Option 3 - Similar to Option 2 but conflates filtering parameters with searching / query

TAXII Query Options SWOT

- Opportunities
  - We could address a key need in the market and give organizations a more useable version of TAXII
  - If we can address this sooner rather than later, we can get a more solid TAXII solution in to the market in the near term.

TAXII Query Options SWOT

- Threats / Risks
  - TAXII 2.1 without the ability to at least query for a relationship might be deemed as still not-yet-viable for production use.
  - TAXII 2.1 without full blow query might also be deemed as still not-yet-viable for production use.
  - This could put pressure to release TAXII 2.2 rapidly

TAXII Scheduling Options

- **A**: We do option 1 and delay TAXII 2.1
- **B**: We only do option 1 but do it in TAXII 2.2+
- **C**: We do option 2 now for TAXII 2.1 and look at option 1 later
- **D**: We do nothing now, ship TAXII 2.1, and address all of this at a later time
- **E**: Try to find a merged solution