STIX and TAXII Working Call

2020-02-11

Agenda

- Sponsorship
  - Infrastructure is all done
    - COA will be reverted back to 2.0 tomorrow
- Review changes from last working call
- New STIX Issues
- Interoperability

Issue 204

- Clarify restrictions on property names
- We added the following text to section 3.1 first paragraph to address this issue. The text added is:
  - **Type names and property names MUST begin with a letter character (for example - in ASCII that would be a through z).**

Issue 216

- Clarify naming of custom extensions
- Added the following text to 11.3.1 as bullet point 3:
- **Custom Extension names MUST end with "-ext".**

Issue 210

- Add sample_ref property to malware analysis
- Added the following text to Malware Analysis

sample_ref (optional)	identifier	This property contains the reference to the SCO file, network traffic or artifact object that this malware analysis was performed against.

- Still trying to address a concern from Ivan

Issue 213

- Add AV Result Name to Malware Analysis
- Renamed the av_result property to just result and added the property result_name per the working call. The classification result as determined by the scanner or tool analysis process.

result_name (optional)	`string`	The classification result or name assigned to the malware instance by the scanner tool.
result (optional)	`open-vocab`	The classification result as determined by the scanner or tool analysis process. The value for this property **SHOULD** come from the `malware-result-ov` open vocabulary.

Issue 211

- Make Malware Types Optional
- This impacted the following
- Indicator (indicator_types), Infrastructure (infrastructure_type), Malware (malware_types), Report (report_types), Threat Actor (threat_actor_types), Tool (tool_types), Identity (identity_class). We did NOT change the Relationship (relationship_type) as that one has a slightly different meaning and is actually required to make sense of the relationship.
- We changed the following vocabulary entries to match the discussion on the working call. Infrastructure Vocab Undefined -> Unknown
Identity Vocab - Unspecified -> Unknown and then updated the description.

New Issues

- Make Hashes a SHOULD vs a MUST
- 192 - https://github.com/oasis-tcs/cti-stix2/issues/192

- Custom Properties at all Levels
- 215 - https://github.com/oasis-tcs/cti-stix2/issues/215

- It is not possible to reliably determine if a custom object is an SDO/SRO or an SCO
- 217 - https://github.com/oasis-tcs/cti-stix2/issues/217

More New Issues

- Is the constraint on SCO url's value too strict?
- 218 - https://github.com/oasis-tcs/cti-stix2/issues/218
- Should created and modified times be precise to exactly 3 digits after the decimal place in seconds?
- 219 - https://github.com/oasis-tcs/cti-stix2/issues/219
- Patterning
- 214 - https://github.com/oasis-tcs/cti-stix2/issues/214