CTI-TC Working Group Meeting

Meeting Date: January 28, 2020
Time: 19:00 UTC
Purpose: Working group meeting on STIX & Interop

Attendees:
Alex Applegate
Bret Jordan
Chris Lenk
Drew Varner
Emmanuelle Vargas-Gonzalez
Emily Ratliff
Greg Reaume
Ivan Kirillov
Jason Keirstead
Jeff Mates
John Wunder
John-Mark Gurney
Justin Stewart
Marco Caselli
Mark Davidson
Patrick Maroney
Rich Piazza
Robert Keith
Roseann Guttierrez
Stephen Russett
Trey Darley

Action Items:

- [Chairs] Follow up with New Context on Infrastructure sponsorship
- [Chairs] Follow up on COA sponsorships
- [IK] Suggest language for restricting bundled malware and malware analysis objects from pointing to unrelated samples, as in GitHub issue 210
- [Editors] Update text to accept suggestions for GitHub issues 204, 210, 211, 213, and 216
- [Editors] Review text to see whether the pattern of “unknown” in an open vocab was present on other required fields (as in GitHub issue 211), example tool and indicator.
- [All] Request edit rights for Interop documents and start making suggestions
- [All] Let Interop Co-chairs know of intent to participate in the plugfest in May
- [Chairs] Work with TC secretaries to schedule bi-weekly meetings

Meeting Notes:
The working group reviewed the current state of sponsorship. COA is at risk of being removed. Looking Glass completed sponsorship for infrastructure and deterministic IDs. New Context has implemented COA.

The working group reviewed open GitHub issues:
204 - https://github.com/oasis-tcs/cti-stix2/issues/204
216 - https://github.com/oasis-tcs/cti-stix2/issues/216
210 - https://github.com/oasis-tcs/cti-stix2/issues/210

211 - https://github.com/oasis-tcs/cti-stix2/issues/211
213 - https://github.com/oasis-tcs/cti-stix2/issues/213

204
Consensus was to add clarifying text but to leave the name of body_multipart as is.

216
No objects were raised to accepting the suggestion to add -ext

210
Request for sample_refs to be added to malware analysis so that the sample analyzed can be clearly documents. This is especially useful when the result is benign, so no malware object exists to reference. Ivan pointed out that when malware and malware analysis are linked and malware is not a family, it would be odd to have the two objects point to different samples. He will suggest language to caution against doing this. Consensus was to add this embedded relationship.

213
Request to split analysis result from the analysis result name since this overloads av_result. Ivan suggested changing av_result to result because the result determination may have come from reverse engineering or one of the other allowed analysis techniques and not only av. Consensus was to make this split and use result rather than av_result.

211
malware_types is required but one of the possible values for the open vocab is “unknown”. The request was made to make malware_types optional rather than requiring “unknown” to be specified. The group felt that there is a different between not specifying malware_types and specifying malware_types as “unknown”, so the consensus was to make malware_types optional but leave “unknown” as an item in the open vocabulary. This pattern also exists in other object, for example tool and indicator so the editors will scan the spec to see if this pattern exists in additional objects.

[Interop]
Justin Stewart presented the current plan for the Interop Working Group. Copies of the 2.0 Interop documents for STIX and TAXII have been made and will be used as a starting point for the 2.1 interop documents. Editorial work has already begun. Links are on the CTI TC cover page. Working group members may request edit access and start making suggestions.

There will be a plugfest in May hosted by Mark Davidson from Celerium. CTI TC members who are planning to participate are requested to let the Interop Co-chairs know of their intention. Plugfest rules were reviewed.

Trey mentioned that in past plugfests there was a considerable amount of time spent on getting products to communicate rather than on interoperability. Trey recommended that each participant spend time on testing before attending the plugfest to attempt to reduce this non-productive time. Bret volunteered to update his test suite and revisit with the group in a couple of weeks whether it can be used to speed up this process.