STIX Working Call

2019-05-21

Agenda

- Review Project Plan (1 minutes)

- Editorial Status Report (1 minutes)

- Items to Discuss (50* minutes)

- Action Items (2 minutes)

Editorial Status Review

* Only a few blockers left for us to resolve

* Today plus maybe one more working call, depending on how things go today

Identifiers in STIX

- Very loud and strong voices on all sides of this debate

- Common to hear things like "I strongly disagree" or "we can not or will not use STIX if this does or does not happen"

- We need to find a solution that works for everyone

- This means we need to have a lot of compromise

- The SCO changes hinge on some of these

Identifier Requirement

* Explosion of SCOs with same data

    * At the DC3 F2F the main objection to having SCOs be TLOs was the explosion of objects with the same data (e.g.. ip address 1.2.3.4).

    * At that point many said we could use deterministic IDs, but also at that point NO ONE had produced a solid proposal for how that could or should be done.

    * Thanks to Allan's works, we now have a solution that solves this problem.

    * The agreement for SCO changes hinges on the ability to have deterministic IDs for SCOs

Identifier Requirement

* Deterministic Comparison for SCOs

    * Some want to use deterministic IDs to try and figure out if content is the same or not

    * For this to happen, SCOs really need to have deterministic IDs

    * On the flip side, even if they are deterministic that does not mean products will always care

    * We can not force products to pay attention to or process the deterministic IDs they receive

Identifier Requirement

* No un-intended collections on IDs

    * It is super critical that we do not have un-intended collisions on IDs

    * The importances of this is carved in stone

    * Our whole versioning model and graph design hinges on this.

    * For SDOs, SROs, and Helper Objects, this is paramount

Identifier Requirement

* Transport / Interchange format

  * STIX is a transport language / interchange format NOT a database design or how your local product should store its data

* Bloat on the wire

  * There has been significant concern raised many times over about bloat on the wire for SCOs.

Proposals

* There are several proposals that have been floated around

* We need to remember that extreme flexibility and optionality is what killed STIX 1.X. Let us please not make those same mistakes

Proposals

* The main questions right now are:

    * Do we allow organizations to use a non-standard deterministic ID generation method?

    * If yes, do we require them to tell others how they made their IDs?

    * If yes, how best to do that?

Proposals

* Two pertinent elements from our TC design criteria are:

    * Extreme optionality is bad

    * Multiple ways of doing the same thing are bad

Discussion

- Discuss possible ideas

Other Topics

- \<TBD>