

CTI TC

Monthly Meeting

May 16, 2019 | Session #1 & #2



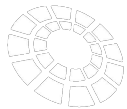
Agenda

- ❖ Introduction & Welcome
 - Admin Notes
- ❖ Subcommittee Updates
 - STIX 2.1 Updates
 - TAXII 2.1 Updates
- ❖ Community Development Corner
 - Call for Open Source Presentations

Need for CTI TC Support

Two Items Needed

- Co-Secretary
 - Contact Jane Ginn @ jg@ctin.us with questions
- Github Repo Maintainers
 - Reach out to Co-Chairs to Volunteer



LOOKINGGLASS

STIX SC Update

STIX Subcommittee Updates

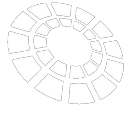
- Preparing to release Working Draft 04
- Does the following text resolve the issues that came out of the language-content sponsor's work
 - "If the property is not present, then the language of the content is en (English)."

STIX Subcommittee Updates

- Concepts included in this release: SCO Changes, Grouping, Malware, Malware Analysis, Infrastructure, and COA
- Action Items:
 - Review documents in detail

STIX Subcommittee Updates

- Topics that have been postponed
 - Versioning of SCOs
 - Additional Common Properties on SCOs
 - `spec_version`, `lang`, `revoked`, and `created_by_ref`
 - Deprecating some SCO embedded relationships
 - to be replaced by external relationships
 - Additional changes to the STIX IDs and SCO IDs / Deterministic IDs
 - Additional changes to new SCO ID properties
 - `id_method` and `id_method_details`

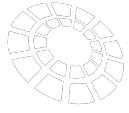


LOOKINGGLASS

TAXII SC Update

TAXII 2.1 Update

- **Waiting for STIX 2.1 Work Draft 04 to be released**
- **Once Working Draft 04 is out, we will address final issues**



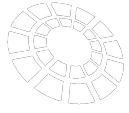
LOOKINGGLASS

Community Development Corner

John-Mark Gurney (New Context)

Two open-source projects:

- Idaho National Labs: Structured Threat Intelligence Graph (STIG):
<https://github.com/idaholab/STIG>
- New Context: Sample i18n STIX library:
<https://github.com/newcontext-oss/cti-stix-i18n>



LOOKINGGLASS

Questions or comments?



Thank You