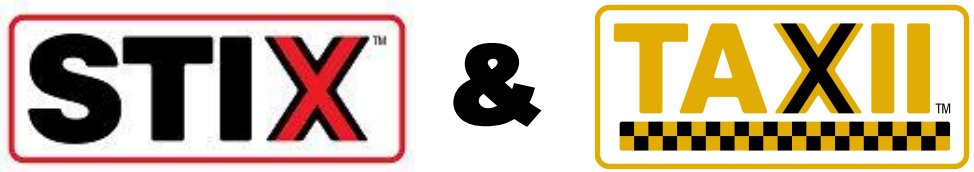
Cyber Threat Intelligence: Technical Committee (CTI TC)

Monthly Meetings – 26 October
Session #1 & Session #2



Agenda

Moderating: Richard Struse - Chair, CTI TC

- STIX 2.0 CS
- Where are we after the F2F?
  - Changes that we're making
  - Roadmap/timing
- STIX update
- Observables update
- TAXII update
- Interop update

STIX 2.0 Committee Specification

- We're DONE! :)
- Being finalized by OASIS staff as we speak
- Secured another trademark waiver from the OASIS board
- Trademark discussions with DHS will continue

Where are we after the F2F?

- Good progress made towards completing 2.1 in the near term
- Identified an issue with too many meetings and general cadence of work
- Implementing changes to address these concerns - some immediate, others to follow

STIX Subcommittee Update

John Wunder and Sarah Kelley – Co-Chairs

- **Most 2.1 additions are nearing done or done**
- **Aiming for a STIX 2.1 release in the near-term**
  - Some discussion at the F2F of taking a slow, deliberative approach to 2.2
- **Focusing on 3 topics with defined timelines**

STIX SC Update

Assessment/Risk/Classification

John Wunder and Sarah Kelley – Co-Chairs

- **Timeline**: 2-3 weeks, if no consensus defer
- **Approach**: minimal capability for producers to provide risk scores and classifications for their own objects
  - Property on indicator and observed data
  - Focus on "threat level"
  - Tackle feedback and peer-provided ratings in a later release
- **Status**: Jason developing updated proposal to discuss
  - **Action**: Review updated proposal

STIX SC Update

Incident/Event/Alert/Grouping

John Wunder and Sarah Kelley – Co-Chairs

- **Timeline**: 1-2 weeks to get minimal capability
- **Approach**: pursuing support for suspicious events via the Grouping object
  - Additional "context" field indicates what type of grouping (suspicious-activity, etc.)
  - Tackle broader structured fields in later releases
  - Same object as used for "MISP Events"
- **Status**: finalizing vocabulary and confirming consensus
  - **Action:** Review and respond to Sean's e-mail

STIX SC Update

Infrastructure

John Wunder and Sarah Kelley – Co-Chairs

- **Timeline**: 2-3 weeks

- **Approach**: several options, remain minimal
  - Option 1: nothing, use observed data with assertions to categorize
  - Option 2: new infrastructure object
  - Option 3: something else

- **Status**: modeling
  - **Action:** Submit reports to model
  - **Action:** Model reports in different options

STIX Subcommittee Update

Course of Action

John Wunder and Sarah Kelley – Co-Chairs

- **Timeline**: still in mini-group, timeline unclear
  - If there is consensus by 2.1 release, include
  - If not, defer to 2.2
- **Approach**: staged capability roadmap starting with basic sequential actions and ending with more complete capabilities
- **Status**: Mini-group, available for review
  - **Action:** Review proposal if interested in COA

STIX Subcommittee Update

Malware

John Wunder and Sarah Kelley – Co-Chairs

- **Timeline**: essentially complete, a few small open questions remain
- **Approach**: send email to list discussing open questions. Once resolved, motion to move into STIX 2.1
- **Status**: Mini-group, available for review
  - **Action:** Review proposal

Cyber Observables Subcommittee Update

Trey Darley & Ivan Kirillov – Co-Chairs

- **Socket Address Object - Needs Review**

Property Name	Type	Description
type (required)	`string`	The value of this property **MUST** be `socket-addr`.
address (optional)	`object-ref`	Specifies a reference to an IP address associated with the socket address. The object referenced **MUST** be of type `ipv4-addr` or `ipv6-addr`.
port (optional)	`integer`	Specifies a port number associated with the socket address.
protocol (optional)	`string`	Specifies the OSI Layer 3 or Layer 4 protocol associated with the socket address. The protocol name **SHOULD** come from the service names defined in the Service Name column of the IANA Service Name and Port Number Registry [Port Numbers]. In cases where there is variance in the name of a network protocol not included in the IANA Registry, content producers should exercise their best judgement, and it is recommended that lowercase names be used for consistency with the IANA registry.

TAXII Subcommittee Update

Bret Jordan & Mark Davidson – Co-Chairs

Interoperability Subcommittee Updates

Allan Thomson & Jason Keirstead – Co-Chairs

- STIX Preferred Program
- Interoperability Test Document Update
- Plugfest Update

STIX Preferred

- ***Preferred*** conveys formal recognition that product meets a higher level of quality
  - Users will want to select products that have attained *Preferred* status; vendors will be incentivized to earn that credential

- Considerations ruled out:
  - *Certified, Verified, Guaranteed*, *Tested* (liability issues)
  - *Interoperable* (Implies verification that product has exchanged data with another product)
  - *Compliant* (tests do more than signify compliance with the specs)
  - *Gold, Bronze* (tests aren't that granular, though we may want to introduce these levels later)

STIX Badges

- OASIS Staff will create official STIX and TAXII badges for exclusive use by products that pass online tests
- Products will be granted right to use one of two badges:
  - STIX-only or
  - STIX-and-TAXII (TAXII test incorporates STIX)
- Badges will incorporate STIX and TAXII logos
- Must resolve trademark issues with DHS
- Current logos will be updated in a way that leverages current brand recognition but also conveys v2 changes
- Only major version numbers will be used in the badges, i.e., 'STIX 2' and 'STIX/TAXII 2'.

STIX Preferred Usage Rules

- When used by vendors online
  - badges will be linked to OASIS web page that explains meaning
  - details restrictions for use
  - lists all products authorized to use badge
  - provides instructions for how to earn the badge including link to online test

- Vendors who use badge without authorization will be asked to remove it from their collateral and advised on how to attain authorization

STIX Preferred Rollout

- Create OASIS CTI Self-Certification Portal
  - OASIS Staff will draft SLA terms and work through other operational issues with CTI Interop SC
  - OASIS Staff will work with SC to define process for orgs to self-certify and publish their results

- 'STIX 2 Preferred' and 'STIX TAXII 2 Preferred' badges will be professionally designed under supervision of OASIS staff

- *OASIS Staff will apply lessons learned from STIX/TAXII to propose self-certification programs to others: TOSCA, LegalXML*

STIX Interoperability Update

- Test Document Part 1: **TC Approved**

Description	Producer Personas	Respondent Personas
Indicator Sharing	DFP, TIP	TMS, TDS, TIP, SIEM
Sightings Sharing	DFP, TIP, TMS, TDS	TIP, SIEM
Versioning	All	All
Data Markings	All	All
Custom Objects & Properties	All	All
Course of Action Sharing	DFP, TIP	TIP, TMS, TDS

- Test Document Part 2: **Subcommittee complete**, further edits/changes paused until Plugfest in Jan

Description	Producer Personas	Respondent Personas
Common Connection and Error Handling	All	All
Basic Feed Sharing	DFP, TIP; SIEM	TMS, TDS, TIP, SIEM, TIS
Basic Intel Collaboration	DFP, TIP, TMS, TDS; SIEM	TIP, SIEM

STIX Plugfest Update

- PlugFest Target Date: January F2F (Tuesday 30th Jan before F2F)
- **Participant Planning Meeting: 1st Nov**
- PlugFest Goals
  - *Help companies improve current or in-development products to enable STIX 2 interoperability*
  - *Confidential* environment where engineers can exchange/debug issues
  - No formal MNDA

- Likely test cases will be focused on
  - Basic connectivity and verification
  - Basic data sharing of threat feeds with recipients
  - Builds on Part 1 tests
  - Most likely aligned with Part 2: Basic Feed Sharing

Q & A

Richard Struse – Chairman, CTI TC
Jane Ginn - Secretary, CTI TC

Cyber Threat Intelligence
Technical Committee