www.oasis-open.org

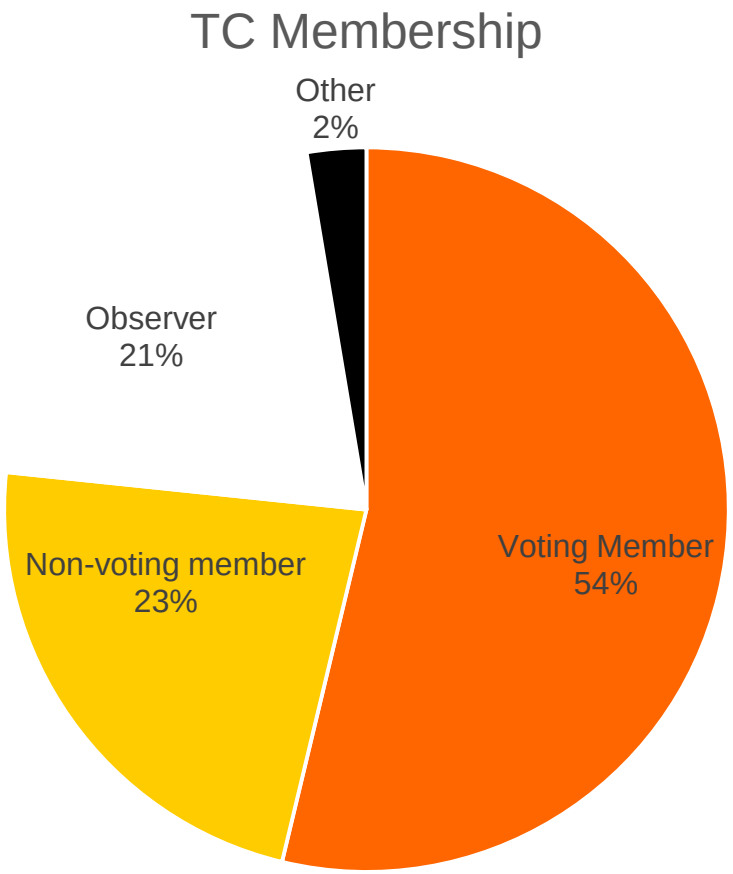
Cyber Threat Intelligence (CTI) Technical Committee (TC)

Face-to-Face
January 14-15, 2016

Richard Struse
TC Chair

Chief Advanced Technology Officer
NCCIC
US Department of Homeland Security

Largest TC in OASIS – 227 people



What's the Purpose of a F2F?

- High-bandwidth discussions of knotty technical issues
  - Lots of drawing on whiteboards
- Get to know each other – build relationships and trust, aka "community"

A F2F is NOT

- A substitute for electronic ballots on work-products
- The time to discuss things we could easily do on the list or slack

Where are we at now?

- A large and vibrant community (more people at this F2F than are in many/most other TC's!)
- Significant adoption/implementation/operational use
  - Example: STIX/TAXII are the foundation for the US Government's automated indicator sharing initiative and are being used to satisfy the requirements of the US Cybersecurity Information Sharing Act of 2015
- We understand that STIX, TAXII and CybOX all have room for improvement and we are making those improvements
  - Example: JSON as the MTI serialization
- Key inflection point – send a message to the global community that we remain responsive and agile after the transition to OASIS

Goals

- Leave on Friday afternoon with:
  - A shared understanding of a ***Minimally-Viable Product*** (MVP) for STIX 2.0, TAXII 2.0 and CybOX 3.0
  - A high-level roadmap for the development of the specifications and supporting materials (e.g. documentation, API's) – *with target dates*
  - Consensus on the approach to key issues in all three specification families
- Be nice and have fun ☺

Principles/Key Points

- Build on the incredible knowledge and experience in the TC to take a fresh look at how we solve key problems
- Use the next major release to create a stable foundation – i.e. break stuff *once* in order to allow stability moving forward
- Focus on defining the MVP – know that we can and will make non-breaking changes/additions in dot releases (every six months?)
- Understand that it will not be perfect or 100% complete
- STIX 1.2.1, TAXII 1.1 and CybOX 2.1 **ARE NOT GOING AWAY** – the standards, API's, documentation, etc. will remain in perpetuity
- Consensus is *not* unanimity

STIX Issue Prioritization

The co-chairs thoroughly reviewed the entire STIX Github tracker twice, and triaged each issue. As a result, the co-chairs have provided a starting point for the community determination of what should constitute a minimally viable product (MVP) for STIX 2.0

- There are currently 167 open issues in the STIX schemas repository
- 81 of these were flagged **2.0-Yes**
- 27 were flagged **2.0-Maybe**
- 28 were flagged **2.0-No**
- Rough time estimates were applied to the 2.0-Yes items.

STIX Issue Time Estimates

- 8 issues were flagged **Effort-weeks**
- 24 were flagged **Effort-days**
- 49 were flagged **Effort-hours**

Other things to be aware of / remember

- This and all TC discussions will be archived and publically accessible
- Only CTI TC members can directly participate in TC discussions
- We *will* remain on schedule ☺
- Passion for the topic is great – but we are *all* going to remain cordial and professional