CTI-TC Monthly Meeting: Session #1 & #2

Meeting Date: **May 18, 2023**

Time: **Session #1 & #2 Notes + Attendance**

Purpose: **Monthly CTI TC Meeting**

Recordings: **Meeting Recordings Link(This meeting was not recorded)**

Attendees: **TC Member Event Link (requires login)**

Company	Name	Role
National Security Agency	Carroll, Sean	Voting Member
Siemens AG	Caselli, Marco	Voting Member
Mitre Corporation	Desai, Kartikey	Voting Member
CIRCL	Dulaunoy, Alexandre	Chair
Cyber Threat Intelligence Network, Inc. (C...	Ginn, Jane	Voting Member
Cyber Threat Intelligence Network, Inc. (C...	Hunt, Christian	Voting Member
IBM	Lee, Chenta	Voting Member
AT&T	Maroney, Patrick	Voting Member
Fujitsu Limited	Masuoka, Ryusuke	Voting Member
US Department of Defense (DoD)	Mates, Jeffrey	Voting Member
Google Inc.	O'Brien, Chris	Voting Member
Mitre Corporation	Piazza, Richard	Voting Member
IBM	Ratliff, Emily	Voting Member
Peraton	Relitz, Stephan	Voting Member
Financial Services Information Sharing and...	Ricard, Chris	Voting Member
National Security Agency	Rosa, Michael	Voting Member
Fujitsu Limited	Satomi, Toshitaka	Voting Member
sFractal Consulting LLC	Sparrell, Duncan	Member
CIRCL	Studer, Christian	Voting Member
DHS Cybersecurity and Infrastructure Secur...	Taylor, Marlon	Chair
Australia and New Zealand Banking Group (A...	Thompson, Dean	Voting Member

Agenda

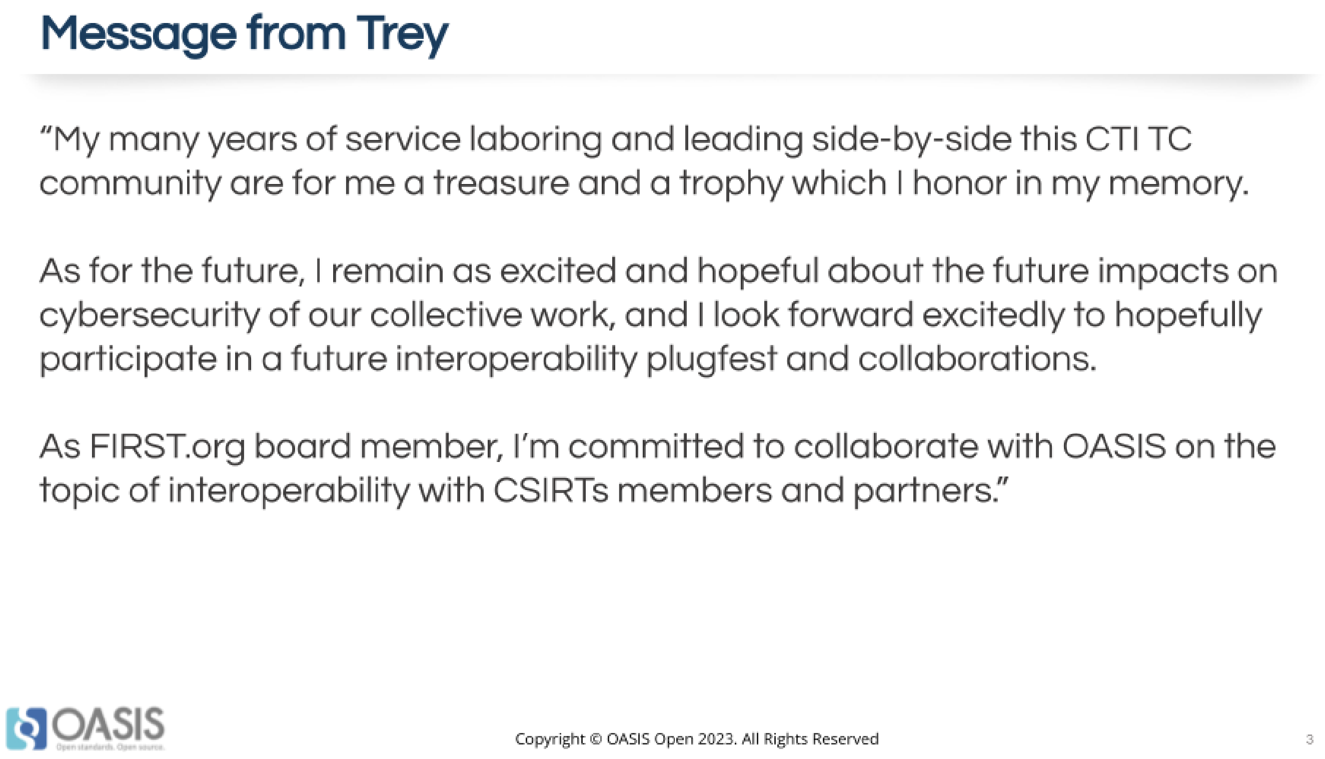
- Welcome
  - New Co-Chairs
- ITU Cross-Standardization Update
- TC Updates
  - STIX SC
  - Interop SC
- Q&A

Meeting Summary

Trey Darley and Robert Coderre gave their thanks and encouragement as the TC transitioned to new Co-Chairs (Alexandre Dulaunoy and Marlon Taylor). Marlon and Alexandre also thanked Trey and Rob for their service to the TC over the years. Marlon and Alexandre shared goals for the TC including (1) Broader Awareness, Participation, and Adoption (2) Enhancement to Specifications and Documentation and (3) More Streamlined and Transparent Processes.

The TC is seeking individual(s) for Secretary. STIX and TAXII are in the process for adoption within the ITU SG17 with the next formal meeting occurring August 29 - September 08 2023. TC members, with representation within the ITU, were encouraged to coordinate with their ITU representatives to show support for STIX and TAXII within the ITU. The STIX subcommittee briefed their use of AsciiDocs for transparency and consistency in specification documentation. The STIX subcommittee also provided an update on the STIX Incident Extension effort which now includes new SDOs (Event, Task, and Impact). The Interop subcommittee recapped lessons-learned actions from previous plugfest and continuation on interop compliance efforts.

Slides



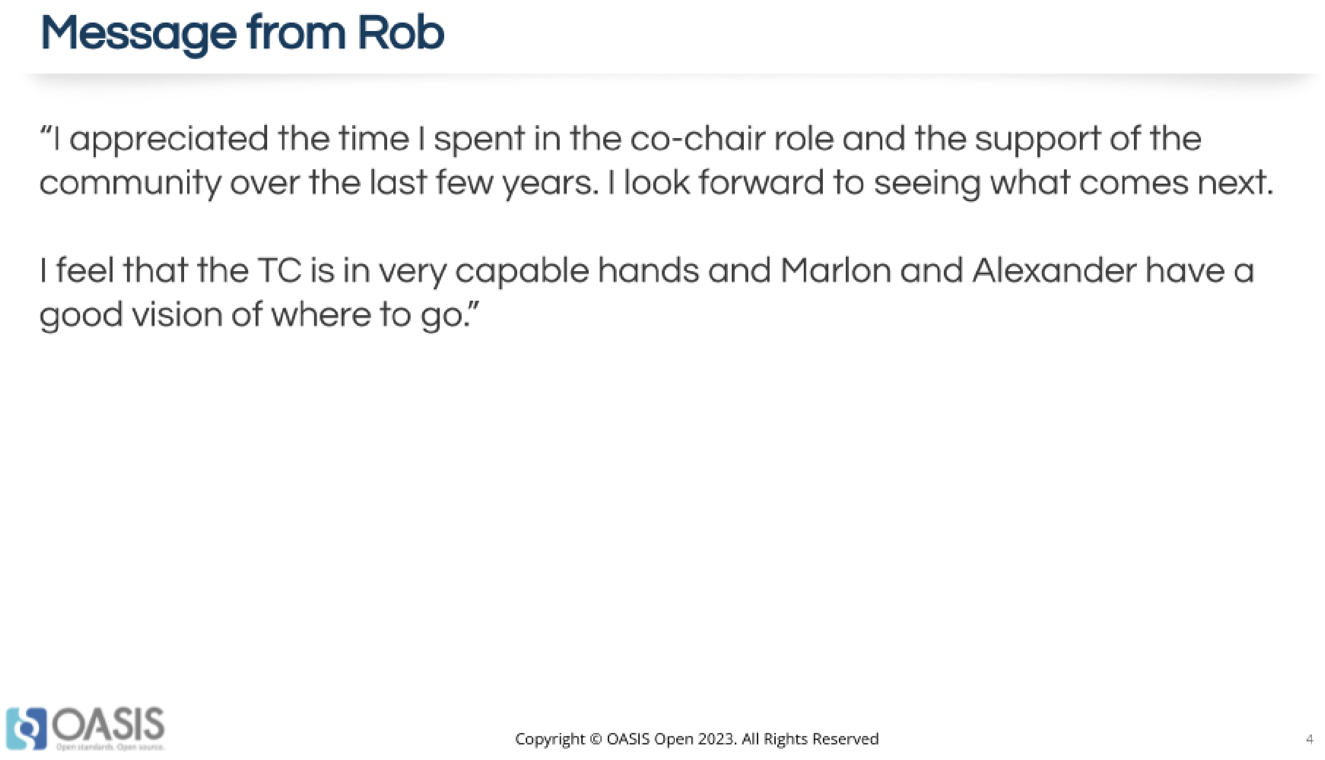
Message from Trey

“My many years of service laboring and leading side-by-side this CTI TC community are for me a treasure and a trophy which I honor in my memory.

As for the future, I remain as excited and hopeful about the future impacts on cybersecurity of our collective work, and I look forward excitedly to hopefully participate in a future interoperability plugfest and collaborations.

As FIRST.org board member, I’m committed to collaborate with OASIS on the topic of interoperability with CSIRTs members and partners.”

3

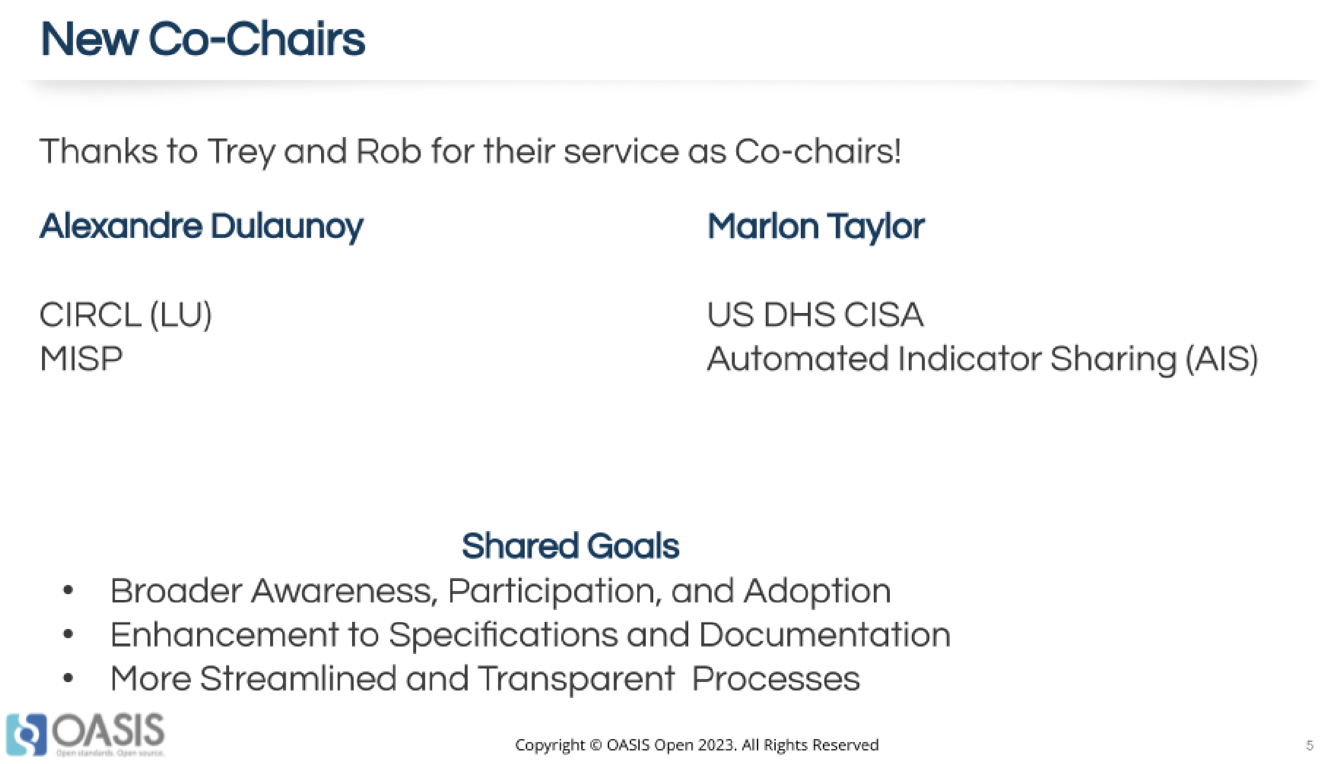


Message from Rob

“I appreciated the time I spent in the co-chair role and the support of the community over the last few years. I look forward to seeing what comes next.

I feel that the TC is in very capable hands and Marlon and Alexander have a good vision of where to go.”

4



New Co-Chairs

Thanks to Trey and Rob for their service as Co-chairs!

Alexandre Dulaunoy

CIRCL (LU)
MISP

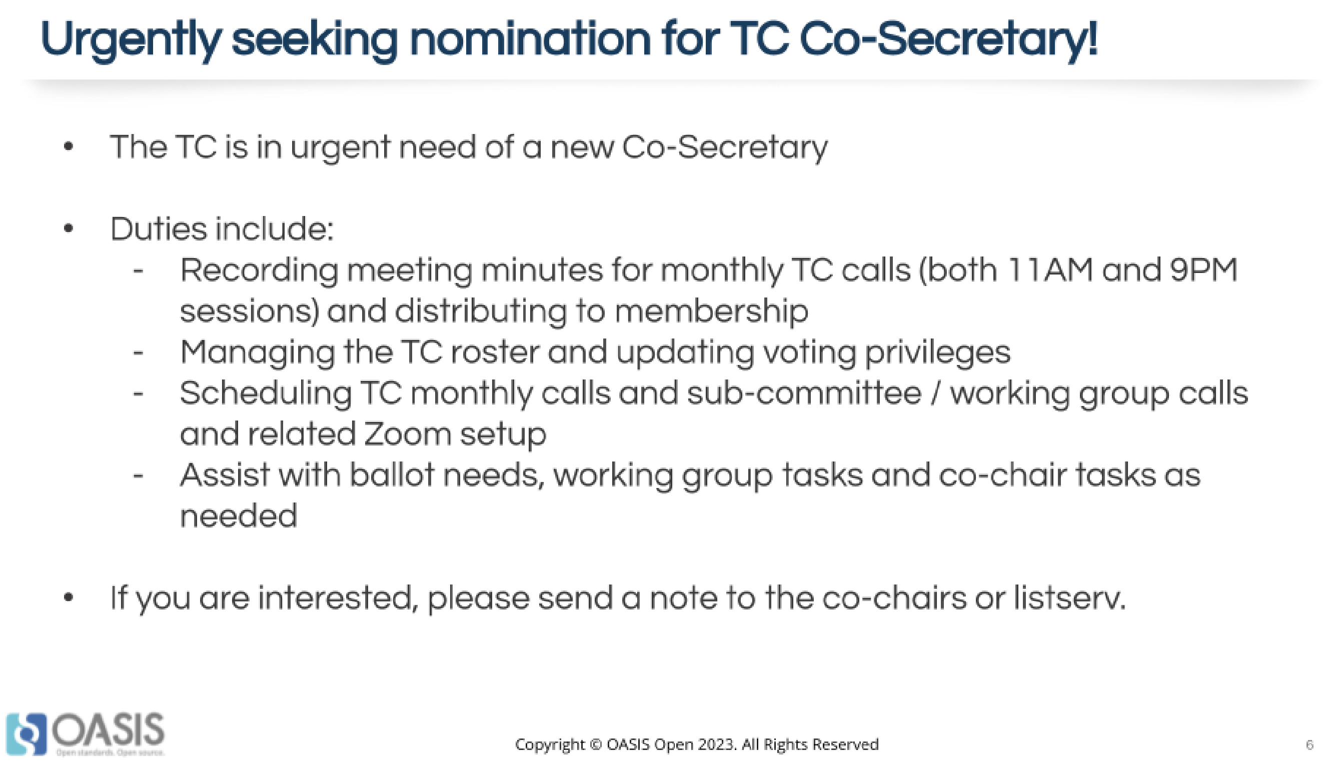
Marlon Taylor

US DHS CISA
Automated Indicator Sharing (AIS)

Shared Goals

- Broader Awareness, Participation, and Adoption
- Enhancement to Specifications and Documentation
- More Streamlined and Transparent Processes

5



Urgently seeking nomination for TC Co-Secretary!

- The TC is in urgent need of a new Co-Secretary

- Duties include:
  - Recording meeting minutes for monthly TC calls (both 11AM and 9PM sessions) and distributing to membership
  - Managing the TC roster and updating voting privileges
  - Scheduling TC monthly calls and sub-committee / working group calls and related Zoom setup
  - Assist with ballot needs, working group tasks and co-chair tasks as needed

- If you are interested, please send a note to the co-chairs or listserv.

6

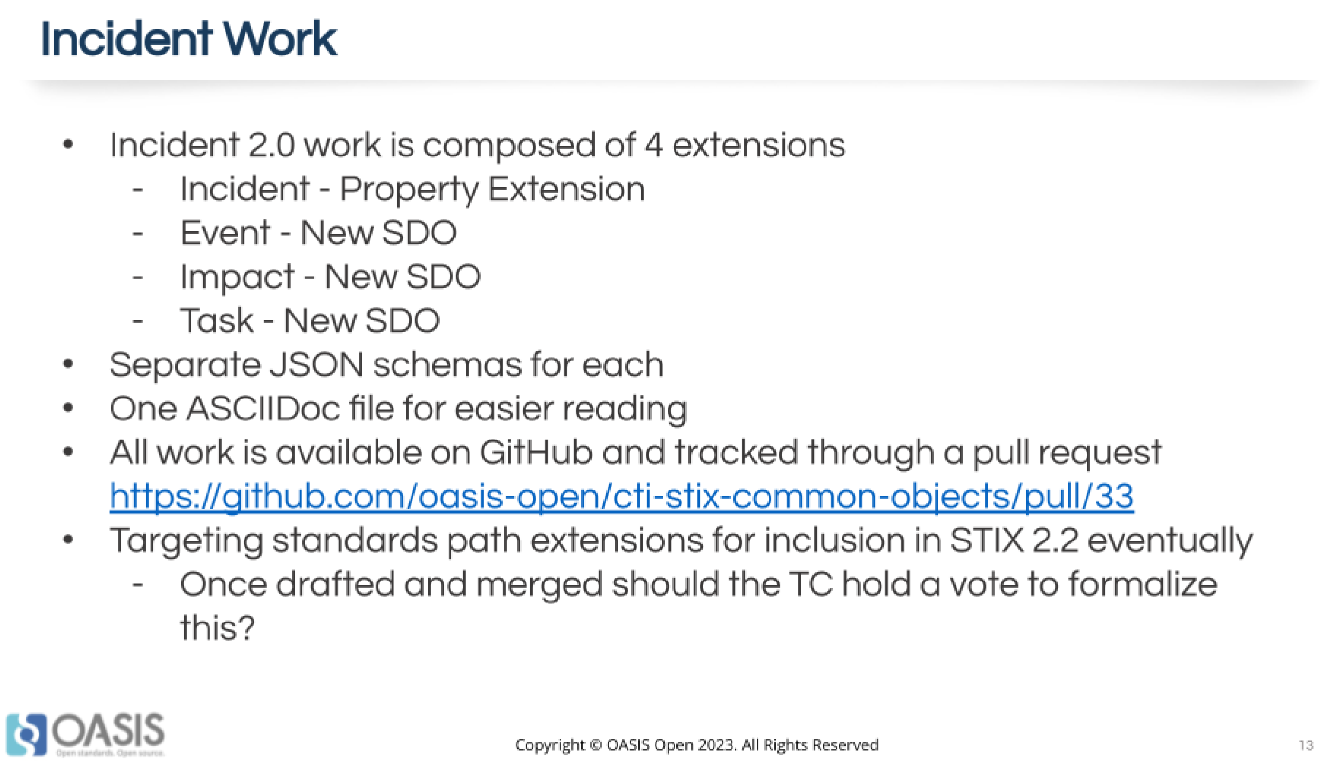
ITU-T Cross-Standardization Update

STIX Update

Experiment in git flow for specification editing - asciidoc

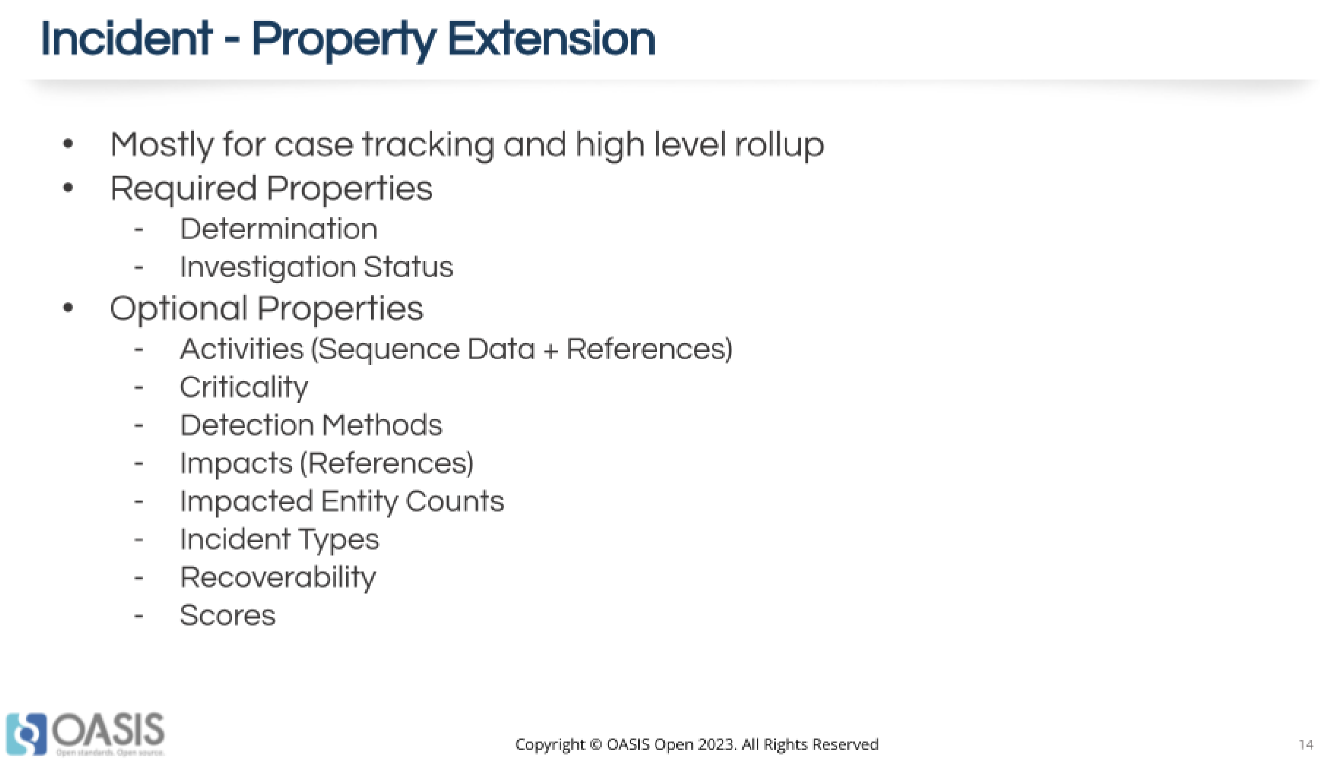
Updates to Extensions - Weekly meetings focused here

- Incident



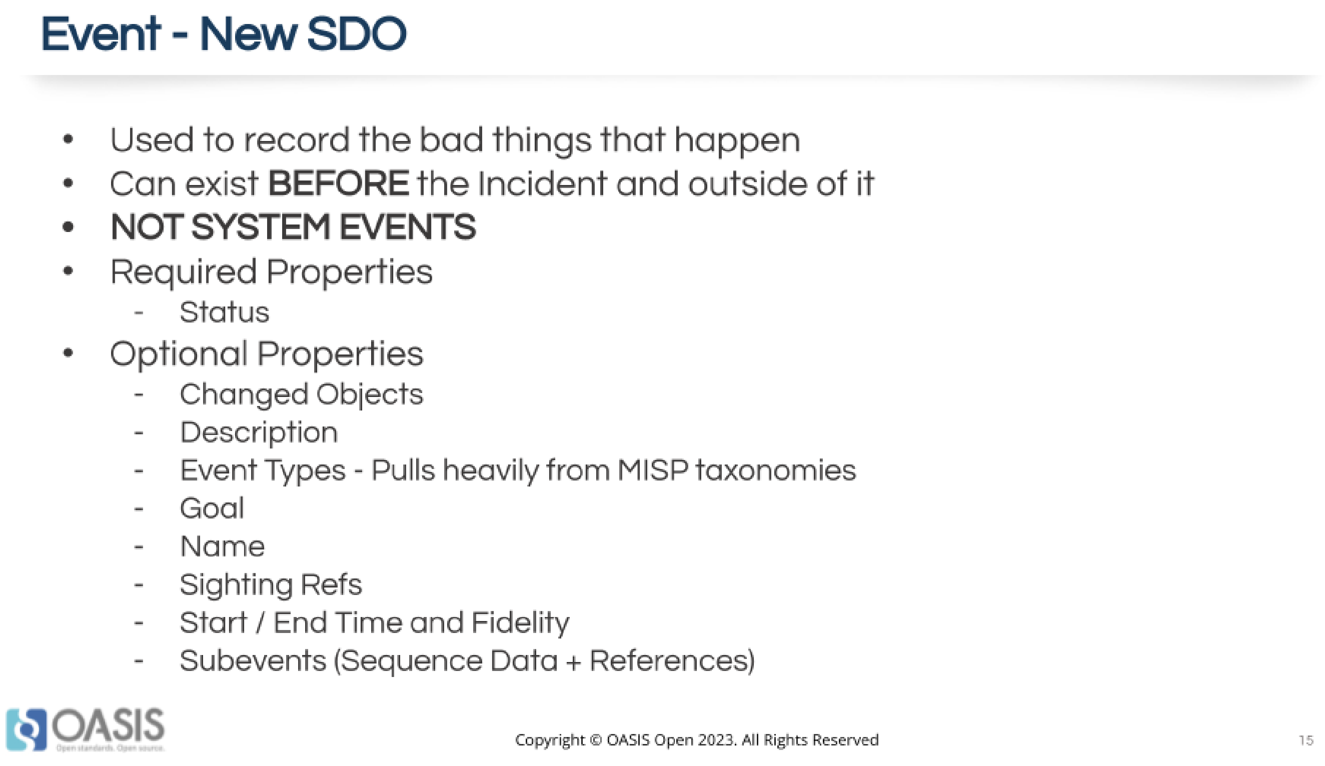
Incident Work

- Incident 2.0 work is composed of 4 extensions
  - Incident - Property Extension
  - Event - New SDO
  - Impact - New SDO
  - Task - New SDO
- Separate JSON schemas for each
- One ASCIIDoc file for easier reading
- All work is available on GitHub and tracked through a pull request https://github.com/oasis-open/cti-stix-common-objects/pull/33
- Targeting standards path extensions for inclusion in STIX 2.2 eventually
  - Once drafted and merged should the TC hold a vote to formalize this?



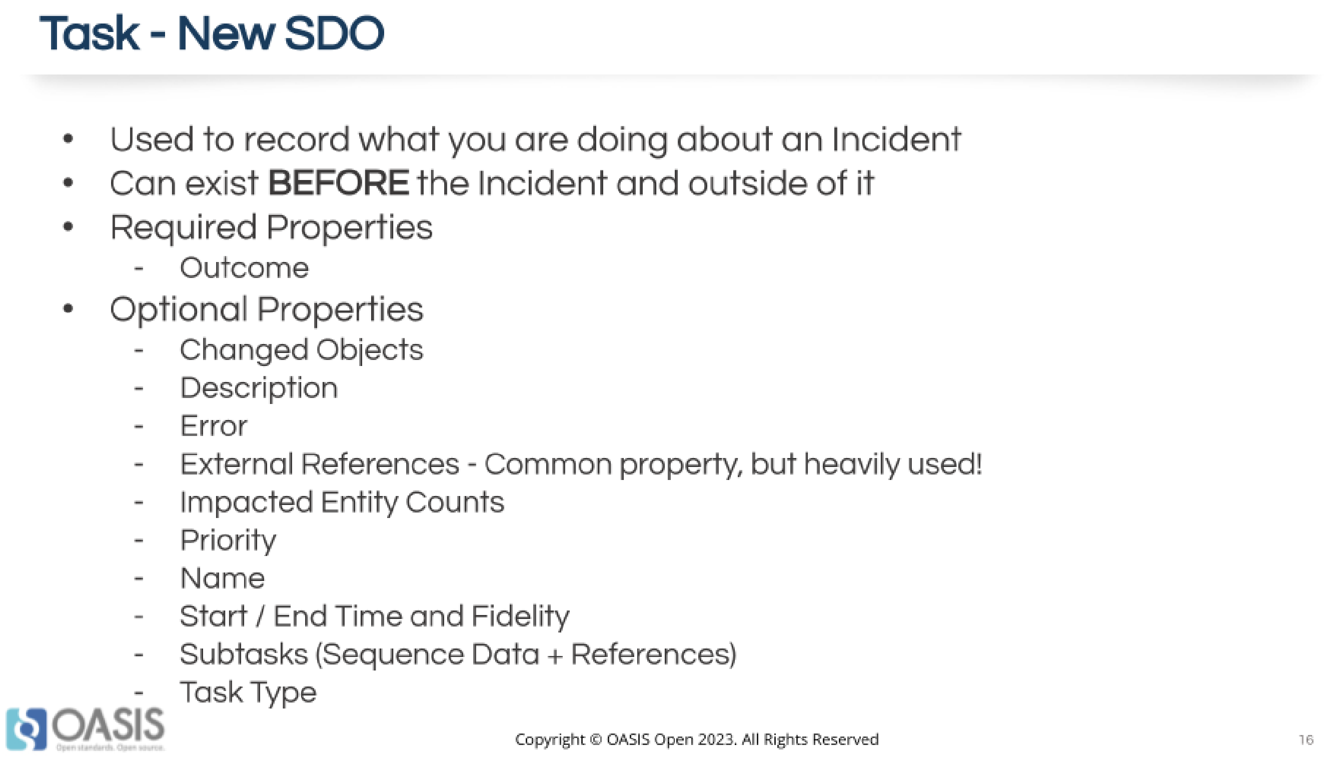
Incident - Property Extension

- Mostly for case tracking and high level rollup
- Required Properties
  - Determination
  - Investigation Status
- Optional Properties
  - Activities (Sequence Data + References)
  - Criticality
  - Detection Methods
  - Impacts (References)
  - Impacted Entity Counts
  - Incident Types
  - Recoverability
  - Scores



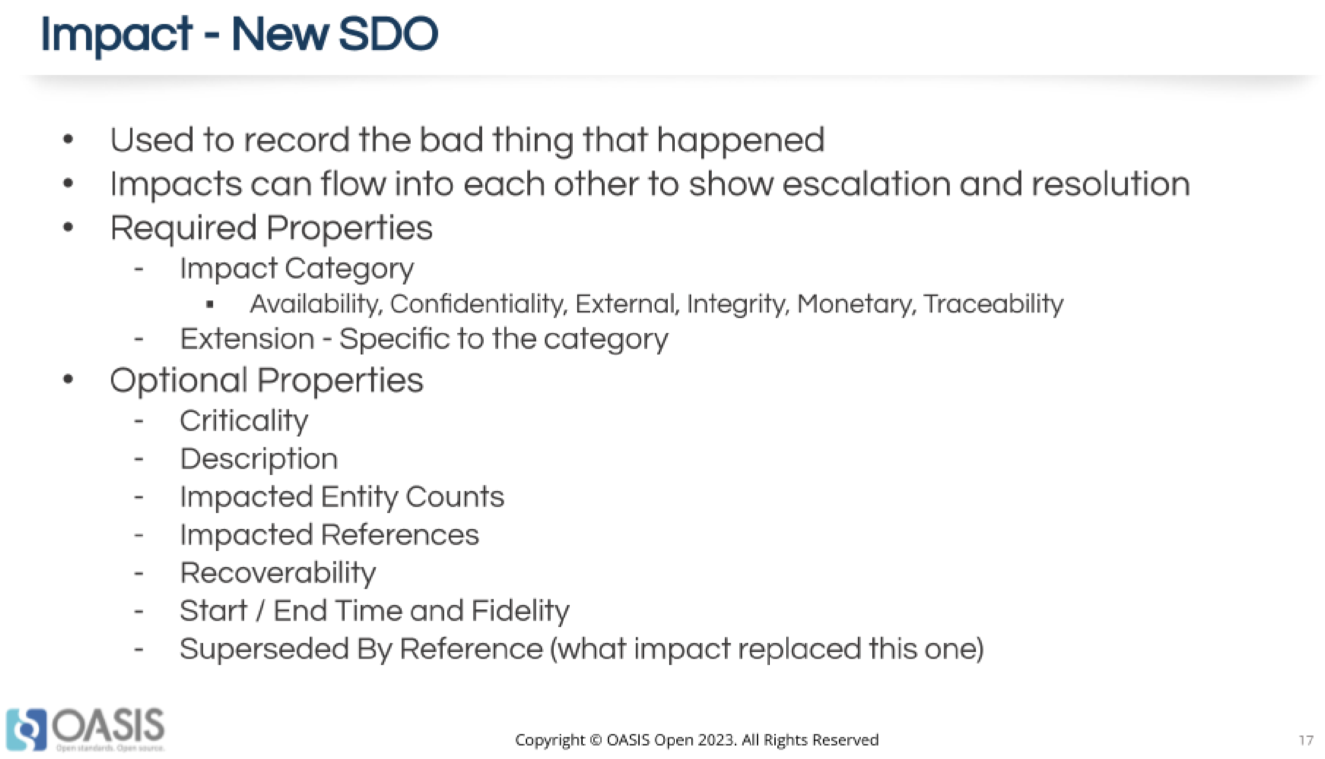
Event - New SDO

- Used to record the bad things that happen
- Can exist **BEFORE** the Incident and outside of it
- **NOT SYSTEM EVENTS**
- Required Properties
  - Status
- Optional Properties
  - Changed Objects
  - Description
  - Event Types - Pulls heavily from MISP taxonomies
  - Goal
  - Name
  - Sighting Refs
  - Start / End Time and Fidelity
  - Subevents (Sequence Data + References)



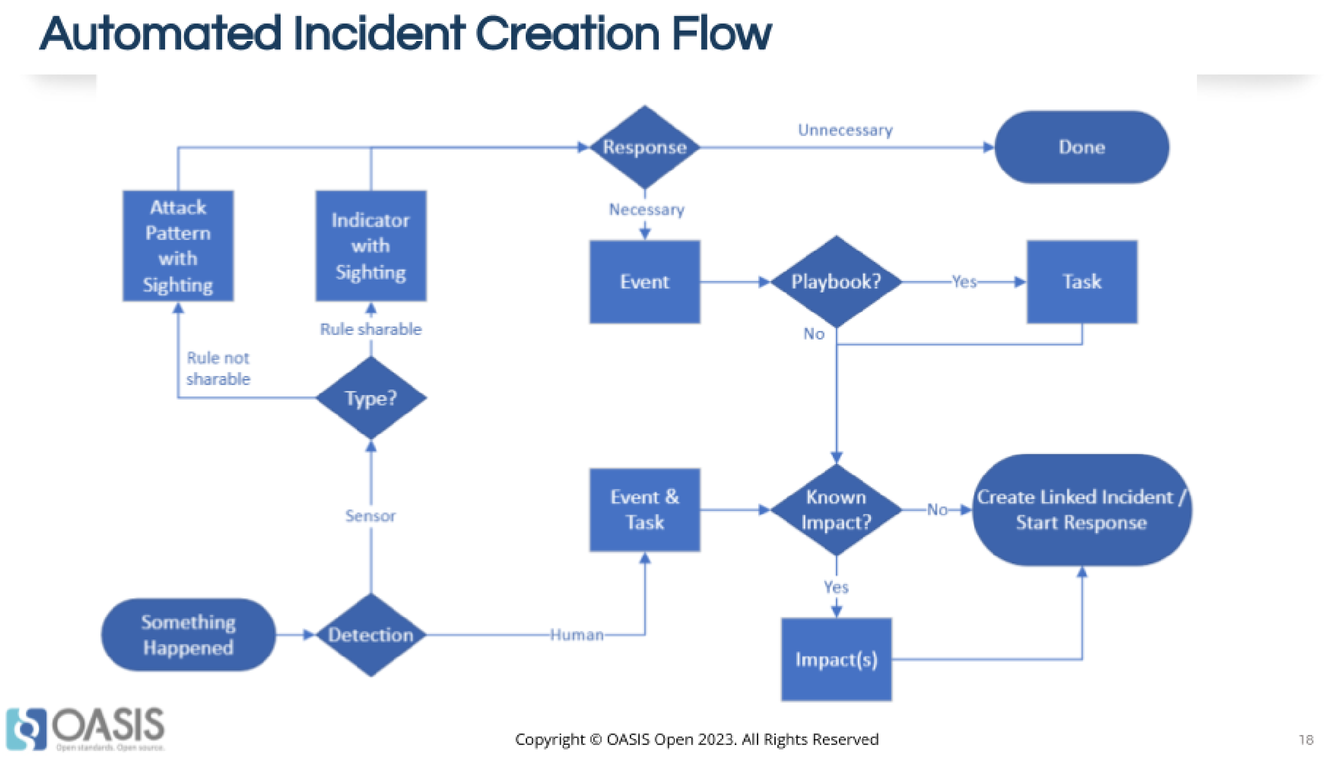
Task - New SDO

- Used to record what you are doing about an Incident
- Can exist **BEFORE** the Incident and outside of it
- Required Properties
  - Outcome
- Optional Properties
  - Changed Objects
  - Description
  - Error
  - External References - Common property, but heavily used!
  - Impacted Entity Counts
  - Priority
  - Name
  - Start / End Time and Fidelity
  - Subtasks (Sequence Data + References)
  - Task Type



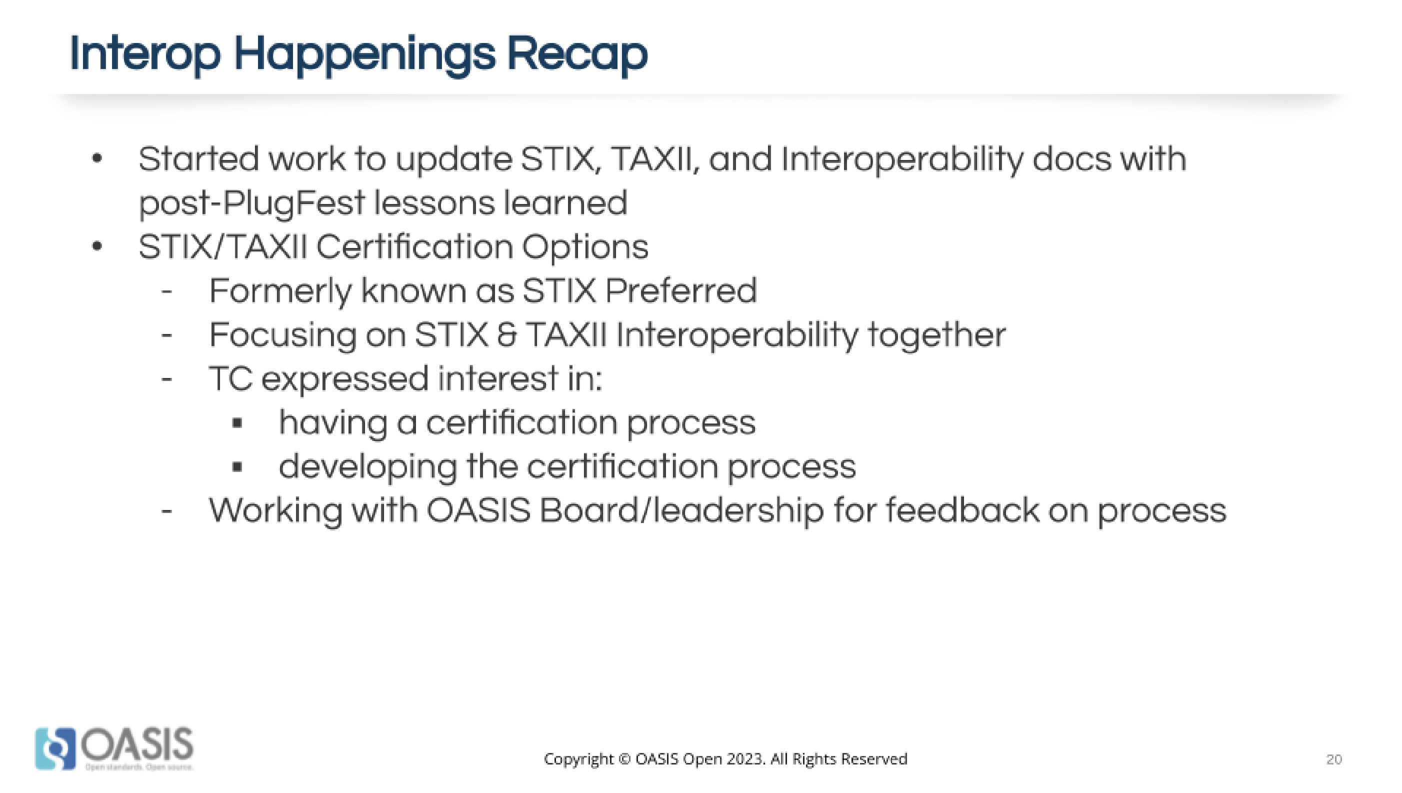
Impact - New SDO

- Used to record the bad thing that happened
- Impacts can flow into each other to show escalation and resolution
- Required Properties
  - Impact Category
    - Availability, Confidentiality, External, Integrity, Monetary, Traceability
  - Extension - Specific to the category
- Optional Properties
  - Criticality
  - Description
  - Impacted Entity Counts
  - Impacted References
  - Recoverability
  - Start / End Time and Fidelity
  - Superseded By Reference (what impact replaced this one)



Automated Incident Creation Flow

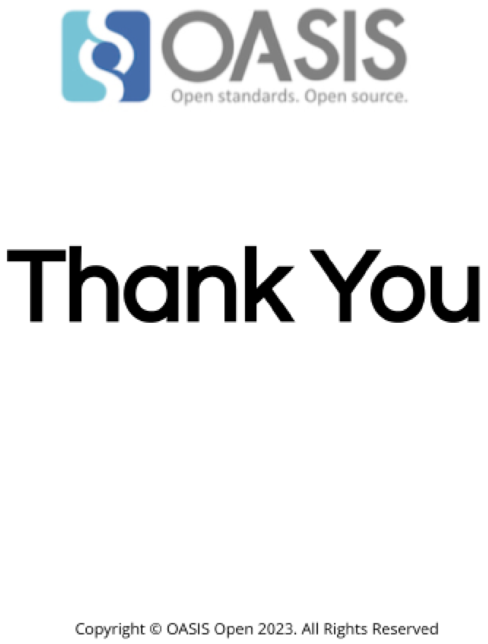
Interop SC Update



Interop Happenings Recap

- Started work to update STIX, TAXII, and Interoperability docs with post-PlugFest lessons learned
- STIX/TAXII Certification Options
  - Formerly known as STIX Preferred
  - Focusing on STIX & TAXII Interoperability together
  - TC expressed interest in:
    - having a certification process
    - developing the certification process
  - Working with OASIS Board/leadership for feedback on process

Questions or comments?



OASIS
Open standards. Open source.

Thank You

Meeting Terminated