Notes taken by Jon Baker of MITRE.

For each session on the agenda, I have included a summary of the discussion. I attempted to capture areas of consensus and areas where further research or discussion in needed. Slides were made available to the TC so I did not capture the contents of the slides.

Day 1

Roadmap

- Consensus - we should aim for a fall release for STIX 2.1.
- Based upon experience with 2.0, the TC needs to plan for up to two months to finalize the documents.
- Beyond STIX 2.1, the TC will aim for a 6 - 8 month release cadence, but there was general agreement that the release cadence will likely change as STIX becomes more mature and there are fewer needed capabilities.
- Features will be included in the release based on time available, value of the item, and whether or not a TC member is willing to develop the concepts.
- In later releases, we may need to take a feature based approach, like focusing on developing support for mobile cyber observables or OT.
- For targeting, we might need to develop a way to use patterns to express ranges of software versions.

Intel Notes for 2.1

- Consensus - supporting the addition of Intel notes as an SDO in STIX 2.1.
- The primary reason for making it an SDO was to allow intel notes to have their own lifecycle, independent of the thing that the note applies to.
- Most seemed to favor a new SDO with an embedded reference to the thing that the note applied to.
- One issue considered was whether or not to allow the note to apply to a SRO.
- To enable automation, there was a request for additional contextual information to be added to the proposed object. Need to identify specific use cases and supporting properties.

Confidence for 2.1

- Consensus - support object level confidence in STIX 2.1 and field level confidence will not be included in STIX 2.1. Confidence will be a property that is set by the object creator to allow the creator to indicate their confidence in the data that they create. Confidence will be a scale of 0 - 100.
- When developing the specification for confidence, we need to ensure that it is given only one meaning regardless of where it appears (i.e. no special meaning on indicators). Confidence will allow creators to express their opinion of how accurate the data is.
    - later, the STIX SC should consider adding an indicator severity property
- A suggestion was made to allow object level confidence on all objects. The room seemed to favor this approach rather than identifying just a subset of SDOs and SROs.

- Later releases can develop an approach like granular markings for field level confidence if needed. (Note that on day 2 a proposal to use the granular marking capability to support multiple languages in one object was well received by the room. This same approach could be used for field level confidence assertions.)
- A suggestion was made to look at the names of the proposed Intel Notes, Confidence, and Opinion objects and ensure that the name clearly aligns with the intended use. Consider using "creator confidence" instead of confidence.
- It was undecided if the specification needed normative mappings between STIX 0-100 confidence scale and other scales. This could be in a specification as normative language, non-normative language, or simply included in other supporting documentation.
- Confidence in the information source was discussed as well. While there was general agreement that this is an import aspect of confidence, it will not be addressed by this proposal. This proposal is focused on creator confidence and not consumer confidence.

Opinion Object

- Consensus - support the Opinion Object as an SDO in STIX 2.1
- General agreement that TAXII may need a feature to allow filtering out of opinion information or Intel Notes?
- Again, intel notes and opinion might need renaming to differentiate.
- Consider allowing the object_ref to be a list of ids rather than just one id.
- Consider adding documentation to an implementers guide to help disambiguate the intel notes and opinion objects.

Greg Back - Open Source Tool Demos

- A suggestion was made to create an open repository to allow people to post prose based threat intel reports and tie associated stix structured representations to those reports.

Incident + Event

- Consensus - Events should be included as an SDO in STIX 2.1.
- Event object should have a mechanism for flagging or marking a given instance as an Incident.
    - STIX does not need to define what is and is not an incident. The solution might be a set of labels applied to an Event.
- The event object might support several different use cases or needs:
    - changes in domain registration by an adversary could be an event
    - clicking a link in a phishing email / receiving the phishing email could all be separate events
    - the combination of smaller events that occurred in a successful phishing attack could be expresses as one event
    - sharing basic event information vs. very detailed information within an organization to support IR
    - sharing detailed event information with a CIRT could be supported in the event object

    - The discussion of these different use cases for the event object led to the agreement that the TC needs to define a set of more targeted use cases and focus on modeling them.
- The TC needs to determine how to represent group of related events.
    - do we need a chain of events?
    - do we need to model an event lifecycle?
- The proposed properties on the Event SDO seemed to span many use cases. There was general concern about the diversity of use cases supported by one object.
- Consensus - The definition of the proposed SDO needs to be rewritten. Events are not tied to indicators.
- Consensus - further development needs to be done on the event proposal to make sure it is flexible enough to address common use cases without being over defined.

Internationalization

- Consensus - Need an approach that does not break backwards compatibility
- This topic was further discussed as a sidebar at lunch on day 2. The day 2 discussion was very productive and led to general consensus around an approach that includes the following:
    - a top-level property in SDOs and SROs to capture whole object language
    - leveraging granular markings to allow for field level language designation when an object contains properties with different languages. Need to consider the implications of references to marking definitions in granular markings. Will this result in too much verbosity?
    - creating a translation object to allow for multiple language translations to refer to SDO/SROs
    - we need to double-check the semantics around the notional translation_of` relationship(s).

Mark Davidson - TAXII 2.0 prototype

- TAXII / STIX works well with popular libraries. An end to end prototype can be developed significantly easier than in STIX 1 and TAXII 1

Aharon Chernin - Perch Demo

- consider adding asset to a sighting
- consider adding geolocation to asset
- sharing asset with geolocation as a component of sightings

Allen Thompson – News Reports

- looking for an object to capture more general threat alerting like news reports and us-cert alerts.

Interop

- Consensus - There was general support for the charter with a revision to clarify that the purpose is to enable testing and validation of implementations.

COA Overview

- proposed two SDOs - COA and Playbook
    - playbook is more advanced and will reference COAs.

    - group expressed concerns about the broad scope of playbook
- Playbook
    - more advanced use cases look a lot like orchestration
    - Becomes very complex for an early implementation in STIX
- COAs are smaller and atomic actions
    - need a thing to pull together a set of COAs
    - is there a simple approach to do this that is not a full playbook?
- There is little shared understanding of the problem and little agreement on how to address the problems
- There was general support for leveraging openC2 and collaborating to develop COAs.
- There was general agreement that for STIX 2.1 the SC will focus on COA. Playbooks can be added later.

Closing Remarks – Debrief

- Short demo of IPA (http://www.ipa.go.jp/index-e.html) STIX TAXII implementation

Day 2

Observables

- Suggestion for SC to produce guidance to help mature proposals. Include topics like appropriate abstraction level. Goal is to make it easier for people to create high quality object proposals.
- Guiding thought: if we cannot easily define the object, then we probably don't have an easy way to use the object.
- When designing the Cyber Observable Object data models, we need to consider and think about the proper level of abstraction for complex Objects that may associated with multiple use cases
- the following existing object changes / additions were discussed:
    - windows handles
        - consider requiring access_mask
        - rename type to handle_type - make it an open vocabulary
        - Consensus - this object should be included in STIX 2.1
    - http response
        - Consensus - this object should be included in STIX 2.1
    - device
        - Consensus - this object should be included in STIX 2.1
        - needed for targeting, events, and infrastructure
        - Asset would be a STIX SDO that would reference the device object
        - what are the needed extensions and how do we avoid scope creep?
        - Consider a narrowly scoped device object. Carefully evaluate the use cases that we need to solve and be sure not to scope creep.
    - OS - skipped over for now
        - Device and and OS should be developed together
    - Credential Dump

        - Consensus that no support in the room for adding credential dump in stix 2.1 due to concerns about the sensitive of the data.
    - web page
        - proposal is based upon defining a property for each structure defined in the HTML 5 spec
        - Some people use YARA to pattern against HTML files
        - this approach loses the structure of the page
            - lacking structure undermines ability to analyze the data
            - consider artifact object to preserve the raw data.
        - consider developing an object that is focused on a minimal set of properties that are useful in a large number of contexts. What is useful for encoding in STIX and needs to be shared across boundaries.
        - explore using a dictionary approach rather than defining all properties based upon HTL 5 specification
    - Actions
        - about adding verbs to patterning
        - current list of MAEC actions is overwhelming.
        - Still need to think about abstraction issues - the more actions there are, the harder it is to implement and get correct.
    - General note: Cyber Observables should be more raw observable data collected from systems and networks vs. the interpretation of that data

Echo Detection

- Goal is to enable the detection of duplicate content in a mesh ecosystem (i.e. an echo of content that you already sent out)
- semantically equivalent objects
    - how do you determine equivalence?
- independently submitted
    - semantically equivalent objects submitted by different creators
- proposal 1 - add property to SDO / SRO to capture source_ids as a list of UUIDs of the objects that were used in the creation of this property.
    - what about object bloat due to repeated information?
- proposal 2 - use a duplicate of relationship
    - issue - it does not work for sightings due to restriction on relationships referencing other relationships
- there was general interest in developing this use case and addressing it in STIX 2.1, but there was some confusion in the room about the use case.
- Consensus - this issue should be addressed, no real discussion of which proposal was preferred.

TAXII

- In TAXII 2, can I get STIX 1 content? yes
- In the definition of a TAXII Server, consider changing the name from client and server to router
- Distinguish between software that provides a service, and the service itself.

- Consensus definition - TAXII Server - software that supports the exchange of CTI and conforms to this specification.
- Conformance needs to explain what the exchange needs to look like
  - There are requirements in the spec that are unrelated to the protocol exchange
- TLS
  - need to balance requiring TLS with setting a requirement that is too high of a bar or counter to some organizational policies
- Should TAXII include authentication as MTI?
  - is the spec for the software or for an instance of the software. Can it be implemented and not used in deployment?
  - can we use an implementation best practices document to capture how implementers should do authentication
  - generally, people want to see lists of authentication mechanisms and not require an authentication mechanism.
- X509 - move to best practices
- DNS SRV records
  - consensus that service name must be TAXII
  - organizations MAY implement DNS SRV
- URL Paramaters
  - parameters can be used together
  - type param should allow a comma separated list
  - added_after
    - issue is focused on solving clock skew
    - suggest not addressing the timing issue and recommend that implementers use NTP.
- Conformance
  - gap here - I stepped away - sorry
- TAXII 2.1
  - ideal timeline for the release is to be aligned with STIX 2.1
  - focus will be on taxii query and taxii channels

Malware

- use cases
  - tracking and reporting on the evolution of malware over time
  - query/response on everything known about a piece of malware, or whether a binary is known to be malware
- open topics
  - how much observable data should be duplicated in the malware object?
    - avoid two ways of doing the same thing
    - consider implication on ability to write patterns. if not captured in observables, you cannot use patterning
    - how do timestamps in observed data work in this scenario
    - if we use observed data, it changes the meaning of observed data
    - focus on the core data elements that can be used to correlate malware
    - previous list consensus was to just embed the objects inside malware

        - need to be able to capture multiple file names.
            - suggest the simple approach is to just add the property directly to the malware object
        - malware instance object
            - hashes, size, name
        - malware family + name on
        - consensus in the room was largely around using cyber-observables container as a property on the malware instance object
            - increasingly necessary to describe behaviors of malware to identify the malware. this will allow us to build in this capability over time
- Representing Analysis
- Deep Dive
    - consensus MAEC-light be the basis for the malware object
        - pull fields that are established and mature from MAEC
    - no glaring omissions on malware instance object

Infrastructure

- consider as potential future SDO
- keep focused on stix as an exchange format
- question - what is the right level of granularity for infrastructure
    - one infrastructure object per IP address or an infrastructure object that encapsulates many IPs
    - analysts use one infrastructure object per IP address
- Consensus - infrastructure is just a name and a container for cyber observables

John Wunder - Unfetter Demo

- general take away that stix 2 is significantly easier to implement
- demonstrated use of stix beyond usual indicator focus
- jsonAPI worked very well with the STIX json schemas