Cyber Threat Intelligence: Technical Committee (CTI TC)

Monthly Meeting – December 15, 2016

Session #1 & Session #2

Agenda

Welcome and Opening Remarks	Richard Struse
Interoperability Status & Way Forward	Richard Struse
Face-to-Face Meeting: S.F. Area January 17th & 18th - @ Google Meet-up – Jan. 17 - 6:00 p.m. – 9:00 p.m. Slack Channel: #2017-01_f2f	Richard Struse
STIX	John Wunder
Cyber Observables	Ivan Kirillov & Trey Darley
TAXII	Bret Jordan & Mark Davidson

STIX Update

STIX – RC4 Status

- Changes made since RC3
  - Bundle was flattened
  - Versioning was simplified
  - Timestamp precision removed (ballot pending)
  - Added last_seen to campaign and intrusion set
- Pending topics
  - Timestamp precision (ballot pending, please vote)
- Next Steps
  - RC4 released on 12/19, 1 week comment period
  - CSD ballot open

STIX 2.1 - Plan

- Join mini-groups on Slack to create proposals for F2F
  - Goal is to have proposals for F2F
- Proposals should include:
  - Normative text
  - Examples
  - Important decisions / alternatives (if applicable)
  - Open questions
- Proposals are due January 9

STIX 2.1 - Topics

- Active Now
  - Malware
  - Infrastructure
  - Location
  - Confidence
- Pending
  - Incident/Event
  - COA/Playbook
  - Internationalization
  - Intel Notes
- Miscellaneous
  - Org chart capability in identity
  - Missing relationships
  - Etc.

Cyber Observables Update

Specification Changes

- **Cyber Observables Core**
  - For capturing observed string encoding, removed _**bin** property (sibling of _**enc**)
    - Used for capturing the original binary representation of the observed string when it cannot be losslessly represented in Unicode
- **Patterning**
  - Added corresponding Observation Operator for “OR” equivalent of ALONGWITH
    - Originally called “OTHERWISE”
  - Based on community feedback, renamed ALONGWITH/OTHERWISE to AND/OR
    - `([file:name = 'foo.dll'] AND [win-registry-key:key = 'HKEY_LOCAL_MACHINE\\foo\\bar']) OR [process:name = 'fooproc' OR process:name = 'procfoo']`
  - Added prefix-based syntax around several constants for discerning between values
    - Binary: `b'ABI='`
    - Hex: `h'0012'`

STIX 2.1 & Cyber Observables I

- For STIX 2.1, there are a number of possible additions to Cyber Observables
  - New Objects
  - New Object Extensions
  - Non-Object Entities
- We need input from **you** (the community)
  - Help us determine what makes it into STIX 2.1 for Cyber Observables
    - Do you have any pressing needs that aren’t met by the current set of Objects?
    - Are there other things that you’d like Cyber Observables to cover?
  - Put together and submit a proposal around something you wish to add

STIX 2.1 & Cyber Observables II

- These are some initial thoughts on possibilities for Cyber Observables in STIX 2.1

Entity Type	Entity	Relative Complexity & Difficulty
New Objects	Device - Mobile Device Ext. - Mobile Phone Ext. - Virtualization Ext.	Unknown
	Operating System	Unknown
	WHOIS	Low
	SMS - MMS Ext.	Medium
	Network Share	Medium
New Object Extensions	Android APK (File Object Ext.)	Unknown
	Apple iOS (File Object Ext.)	Unknown
	EXT 3/4 (File Object Ext.)	Unknown
	Document Metadata (File Object Ext.)	Medium
	HTTP Response (Network Traffic Ext.)	Medium
Other Entities	Actions	High

TAXII Update

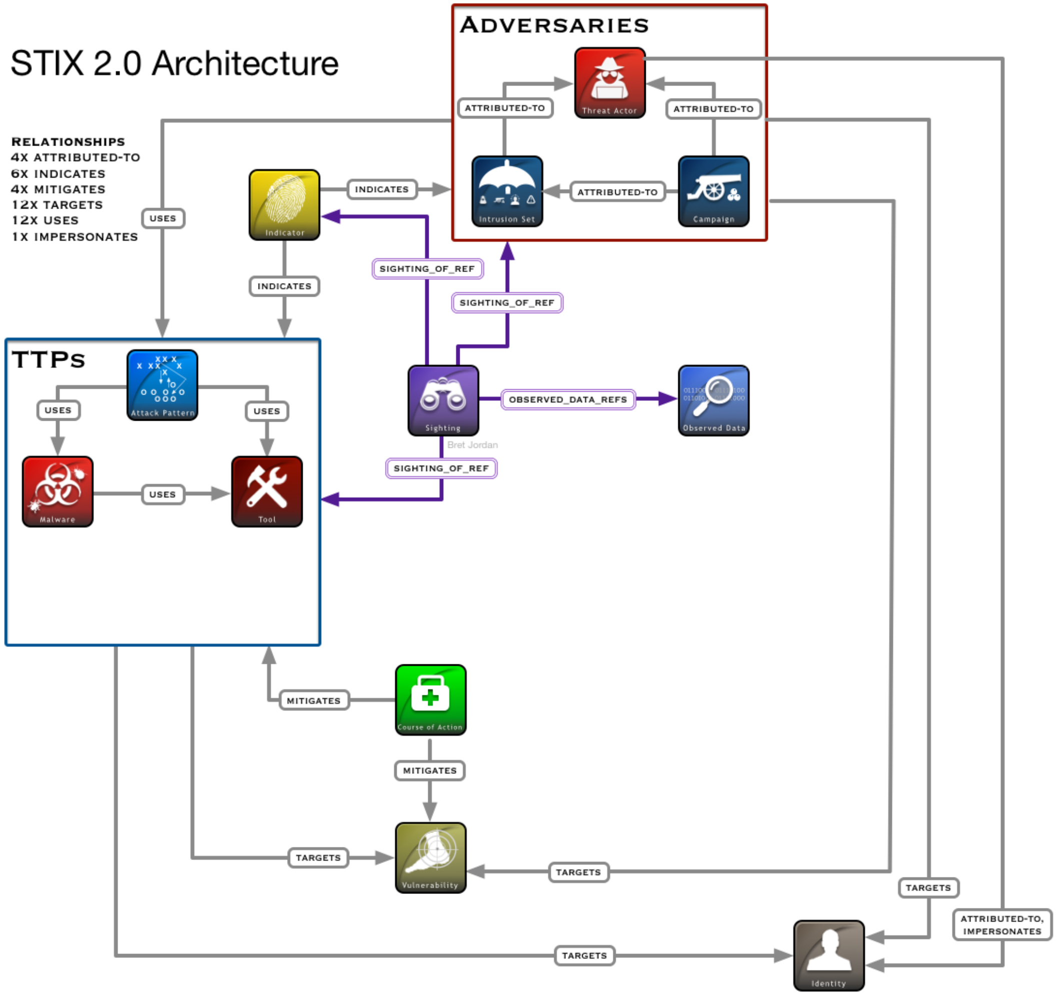
TAXII

- Draft 3 contains:
  - Support for Collections (support for Channels will be in a future release)
  - HTTPS
  - DNS SRV Records
  - Discovery API
  - API Roots (Trust Groups)
  - Content Negotiation

TAXII

- Plan to release Draft 4 / RC 1 before end of December
- Hope to have a CSD before the F2F

Q & A



STIX 2.0 Architecture

RELATIONSHIPS
4X ATTRIBUTED-TO
6X INDICATES
4X MITIGATES
12X TARGETS
12X USES
1X IMPERSONATES