OASIS CTI F2F – CybOX Session II

January 15, 2016

CybOX in Post-STIX v2.0

CybOX in Post-STIX v2.0

- Potential impacts to CybOX as a result of STIX v2.0-driven changes
  - **Top-level Relationships**
  - **Minimum Object Embedding**
  - **Patterning**
  - **CTI Common**

- CybOX could be used as a means of:
  - Expressing Observable Instances
    - Objects
    - Actions
    - Events (?)
  - Expressing Observable Patterns (?)

CybOX MVP

https://www.youtube.com/watch?v=zYUjIayCJSA

- Objects
  - *Address*
  - *File*
  - Device/System/Product
  - Network Connection
  - DNS Query/HTTP Session
  - Extension-based changes
  - Lots of minor tweaks

- Core/Common/Vocabularies
  - Observables Instances vs. Patterns
  - Object-based Patterning
  - Top-level relationships
  - Vocabulary tweaks

Where do we go from here?

- Things we have **good** coverage of
  - High/mid-level file system artifacts
  - Atomic network artifacts
  - Windows artifacts
- Things we have **poor** coverage of
  - Unix/Linux artifacts
  - Other domains
    - Mobile artifacts
    - ICS/SCADA artifacts
  - Mid-level/low-level network artifacts
  - Specific devices
- CybOX *3.1*
  - Mid/low-level network artifacts
    - Refactored Network Packet
    - Additional Layer 7 Objects
- CybOX *3.2*
  - Mobile artifacts
    - Android APK
    - iOS Binary
  - Mobile device/systems
- CybOX *3.3*
  - …