CybOX v1.0(draft) Release Notes

The Version 1.0(draft) release of CybOX is intended as a draft release of an initial major version of the CybOX language that could be utilized for practical operational use and integration into other standards efforts. This release consists of three primary components: a pair of formal language specifications for the core language content and defined objects content, a set of language implementation XML schemas (core, common_types and ~70 defined object schemas), and a small initial set of language utilities including an initial draft Snort->CybOX transform, an initial draft OpenIOC->CybOX transform and a set of CybOX language Python bindings. Recognizing that this is the first time that the formal language specifications will be available for review and as such will likely generate feedback from new stakeholders, this initial major version is being released as a “draft” v1.0 with the expectation of cycles of new feedback and revision before a final v1.0 is released.

The CybOX v1.0(draft) XML schemas include a significant number of changes from v0.7:

- to improve clarity, documentation and descriptive formality for reference and implementation by other standards and users
- to improve consistency, simplicity and efficiency
- to improve alignment (as appropriate) to existing normative references
- to improve the expressiveness of the schema to better support the broad set of use cases it targets (malware characterization, indicator and incident data sharing, event management, etc.) including the addition of an initial set of network-related defined objects

Summary of changes from CybOX_v0.7 to CybOX_v1.0(draft):

- Refinement of namespaces and schema locations for better effectiveness and flexibility going forward
- Normalized all content according to an established set of naming conventions
- Fully annotated all language items (types, attributes, elements, etc.)
- Moved several commonly leveraged types out of the core schema and into common_types
- Achieved full typing of entire schema structure such that all attributes and elements are definitively typed
- Changed all identifiers from ID & IDREF types to be QNames enabling globally unique identifiers and flexibility for domain-specific users of CybOX to define their own identifier syntax locally
- Reordered attributes and elements in numerous types to better reflect common usage and priority
- Added major_version and minor_version attributes for core schema
- Added capability to characterize source of overall observable package data and for individual observables

- Modified the logical composition structure such that any such compositions are now contained within a Observable_Composition element providing improved simplicity and modularity
- Removed the Delta element from ObservableType and relocated the appropriate portions (Change, Trend & Frequency) to appropriate locations under Stateful_Measure and Event
- Added a Domain_Specific_Object_Attributes field to Object utilizing an abstract type that will allow domain-specific use cases to add in their own domain-specific attributes for Objects
- Added a Tool-Specific_Data field to ToolInformationType utilizing an abstract type that will allow addition of tool-specific data
- Added an Indicators field to MeasureSourceType utilizing an abstract type that will allow characterizing differing formats or standards of indicators that may have led to the identification of the observable data
- Enhanced the Hash structure to capture full fuzzy hashes in addition to simple hashes
- Added a new ExtractedFeaturesType that can be used to adorn differing objects (e.g. files, memory, etc.) to capture extracted strings, imports, functions and code snippets
- Added a ByteRunsType to enable capture of byte runs within various objects
- Added object_reference attribute to DefinedObjectType to better support referencing of independently defined Objects from within another Object definition
- Added a generic DataSegmentType to provide a relatively abstract way of characterizing data segments that may be written/read/transmitted or otherwise utilized in actions or defined in objects.
- Added several new defined object schemas (*API, Code, Device, DNS_Record, Network_Flow, Network_Packet, Network_Route_Entry, Network_Subnet, Unix_Network_Route_Entry* **)** including an initial set of network-centric defined objects
- Modified every defined object schema with added annotations as well as minor and in some cases substantive changes to fix errors, improve consistency & alignment with existing normative references, and to improve expressiveness in support of the targeted use cases

Detailed changes from CybOX_v0.7 to CybOX_v1.0(draft):

- The level of changes within v1.0(draft) in the core schema, common_types and the defined object schemas is too great to list every change in these release notes. Detailed difference reports are available for each individual schema at http://cybox.mitre.org/XMLSchema/release_notes/cybox_v1.0(draft)_diff_reports.zip