STIX 1.1 Release Notes

This document provides a high-level summary of the changes between STIX 1.0.1 and 1.1. For additional information about the development of STIX v1.1, please refer to the STIX Release Planning wiki and the STIX v1.1 Issue Tracker.

Highlights

- Upgraded supported CybOX version from 2.0.1 to 2.1
- Added mechanism to support versioning of STIX content
- Added support for more flexible packaging of STIX packages, including nested packages, packages referring to other packages, and content referring to packages. Packages can now be thought of as "reports".

Other Major New Features

- Added the Terms of Use marking extension (thanks to: Terry MacDonald)
- Added consistent Title, Description, and Short_Description fields to all major constructs
- Added @id and @idref fields to TTP subcomponents (Attack Patterns, Malware, Exploits, and Infrastructure) and other constructs to allow referencing
- Added new Personas structure under TTP/Resources
- Improved Information_Source to allow complex (nested) document sources with derivations and roles
- Added mechanism to indicate which profile(s) are being conformed to for a given STIX package
- Added field to Threat Actor to characterize the sophistication of that actor (thanks to: iSight Partners, Inc.)

Minor New Features

- Added additional fields to Snort test mechanism to support event filters, rate filters, event suppression, and product name
- Renamed extension schemas to include the extension point (test mechanism, malware, etc.) in the filename to improve clarity
- Added LanguageCode field to STIXCIQIdentity3.0Type to allow for specification of language on identity elements
- Added mechanism to capture the precision of timestamps
- Added documentation strongly suggesting the deterministic specification of a timezone
- Added schema mechanisms to enforce unique IDs within an XML instance
- Added documentation stating that element content should be empty when using an @idref
- Changed multiplicity of Package_Intent to 0..many
- Added Related_Observables to Indicator Sightings (thanks to: Justin Borland)
- Added Technical_Targeting structure to VictimTargetingType to enable specification of Observable structures
- Added Parameter_Observables to COA, allowing machine-readable COA parameters

- Expanded the IndicatorType vocabulary
- Changed multiplicity on Controlled_Structure and Marking_Structure (in MarkingType) to allow for referenced Markings
- Added external ID field to incident
- Expanded VulnerabilityType in Exploit Target to support many new descriptive fields
- Made the Indicator/Sightings/Sighting element optional, allowing for specification of sightings_count without any sightings
- Changed multiplicity on Indicator/Type to allow multiple types for an indicator
- Added unstructured meta-data (description) field to Sighting
- Clarified precedence for data markings
- Added ability to express whether data lost was encrypted or not to Incident
- Created a default vocabulary for COA/Type

Bug Fixes

- Corrected the multiplicity of COA_Taken and COA_Requested in Incident to 0..many
- Corrected the Exploit_Targets element in TTP to use the standard STIX relationship pattern
- Corrected the AttackerToolTypeVocab so it is usable as expected for ToolType.
- Corrected the directionality of the Indicator ⇔ Campaign relationship
- Corrected regular expression pattern for CVEs to support 2014 syntax
- Specified the XML schema type of ActivityType/Date_Time
- Corrected a typo in MotivationVocab

Documentation

- Used multiple documentation elements rather than newlines in documentation for better tooling support
- Added annotations to Indicator element
- Clarified annotations for @negate (on Indicator)
- Clarified annotations on Valid_Time_Position (on Indicator)
- Clarified annotations on Composite_Indicator_Expression to more closely align with IndicatorType
- Clarified the intended usage of the id, phase_id, kill_chain_id fields on kill chain types
- Clarified redundant fields across KillChainPhaseReferenceType and KillChainPhaseType
- Corrected documentation on StructuredTextType to refer to STIX, not CybOX