STIX Block #2: Quick Wins

January 14, 2016

Session objective

- See if we can quickly nail down some quick wins
- VERY briefly describe apparent consensus on 10 issues/proposals
- Confirm/Refute that consensus holds among F2F attendees
  - VERY briefly identify any areas of non-consensus as open questions
- Post-F2F, post proposals to list (with 1 week window) to achieve formal consensus or discuss open questions
- Ideally identify JSON Schema snippets from TWIGS and add them to proposals

Make IDs required (RM#5) (Prop#2)

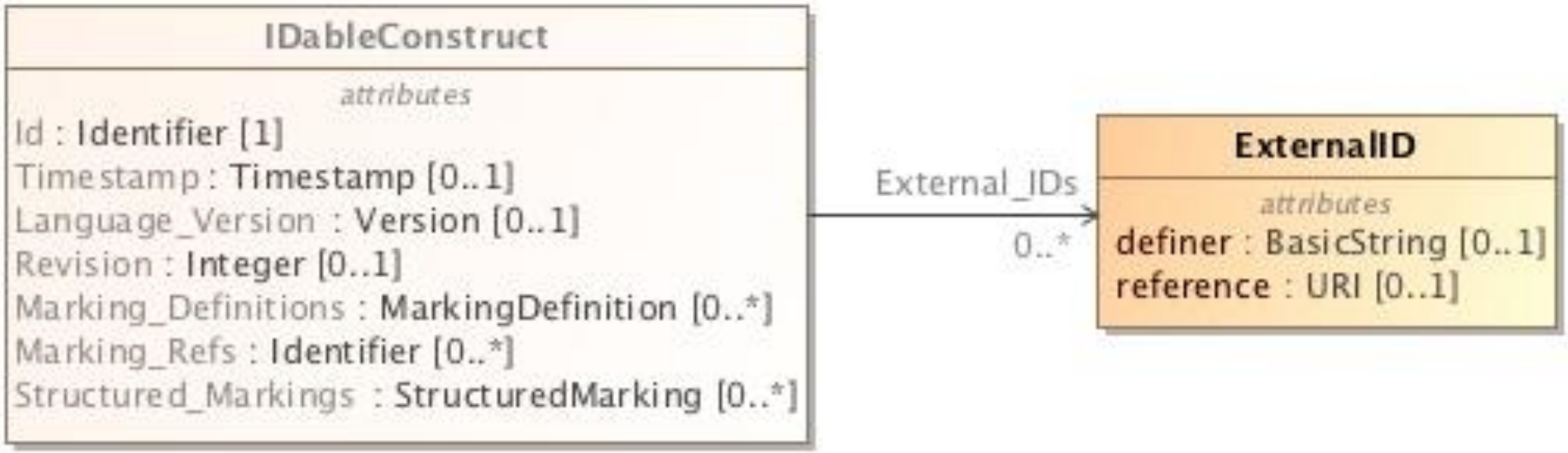
- Quick summary of consensus
  - Both “strawmen” agree that the ID property should be required on all constructs that support it
- Any objections to this consensus?

Remove Short_Description (prop#4)

- Quick summary of consensus
  - Both “strawmen” agree with removing this field as unnecessary
- Any objections to this consensus?

External_IDs (prop#3)

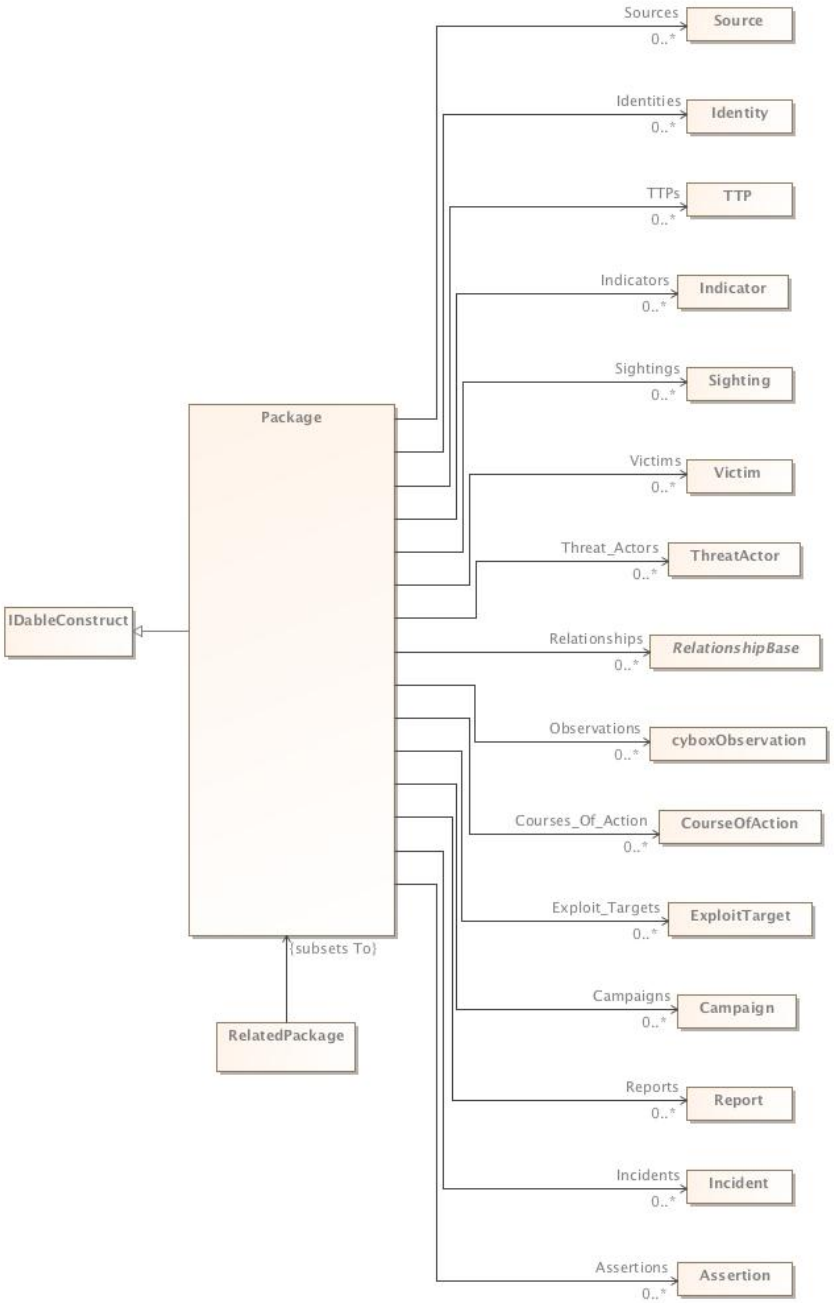
- Quick summary of consensus
  - Both “strawmen” agree that all IDable constructs should support an “External_IDs” property that:
    - Lets you specify an ID (as a string) from some external source/system
    - Provides an optional simple string “Definer” subproperty to specify who/what the ID is from
    - Provides an optional simple URI “Reference” subproperty to specify an URI to the actual ID’d content within the external system/environment
- Any objections to this consensus?


IDableConstruct
attributes
Id : Identifier [1]
Timestamp : Timestamp [0..1]
Language_Version : Version [0..1]
Revision : Integer [0..1]
Marking_Definitions : MarkingDefinition [0..*]
Marking_Refs : Identifier [0..*]
Structured_Markings : StructuredMarking [0..*]
External_IDs
0..*
ExternalID
attributes
definer : BasicString [0..1]
reference : URI [0..1]

Flatten Package lists (prop#14)

- Quick summary of consensus
  - Both “strawmen” agree that the current 2-layer approach for component lists within Package should be flattened to a single layer containing 0..* of each component.

- Any objections to this consensus?


Package
IDableConstruct
{subsets To}
RelatedPackage
Sources
0..*
Source
Identities
0..*
Identity
TTPs
0..*
TTP
Indicators
0..*
Indicator
Sightings
0..*
Sighting
Victims
0..*
Victim
Threat_Actors
0..*
ThreatActor
Relationships
0..*
RelationshipBase
Observations
0..*
cyboxObservation
Courses_Of_Action
0..*
CourseOfAction
Exploit_Targets
0..*
ExploitTarget
Campaigns
0..*
Campaign
Reports
0..*
Report
Incidents
0..*
Incident
Assertions
0..*
Assertion

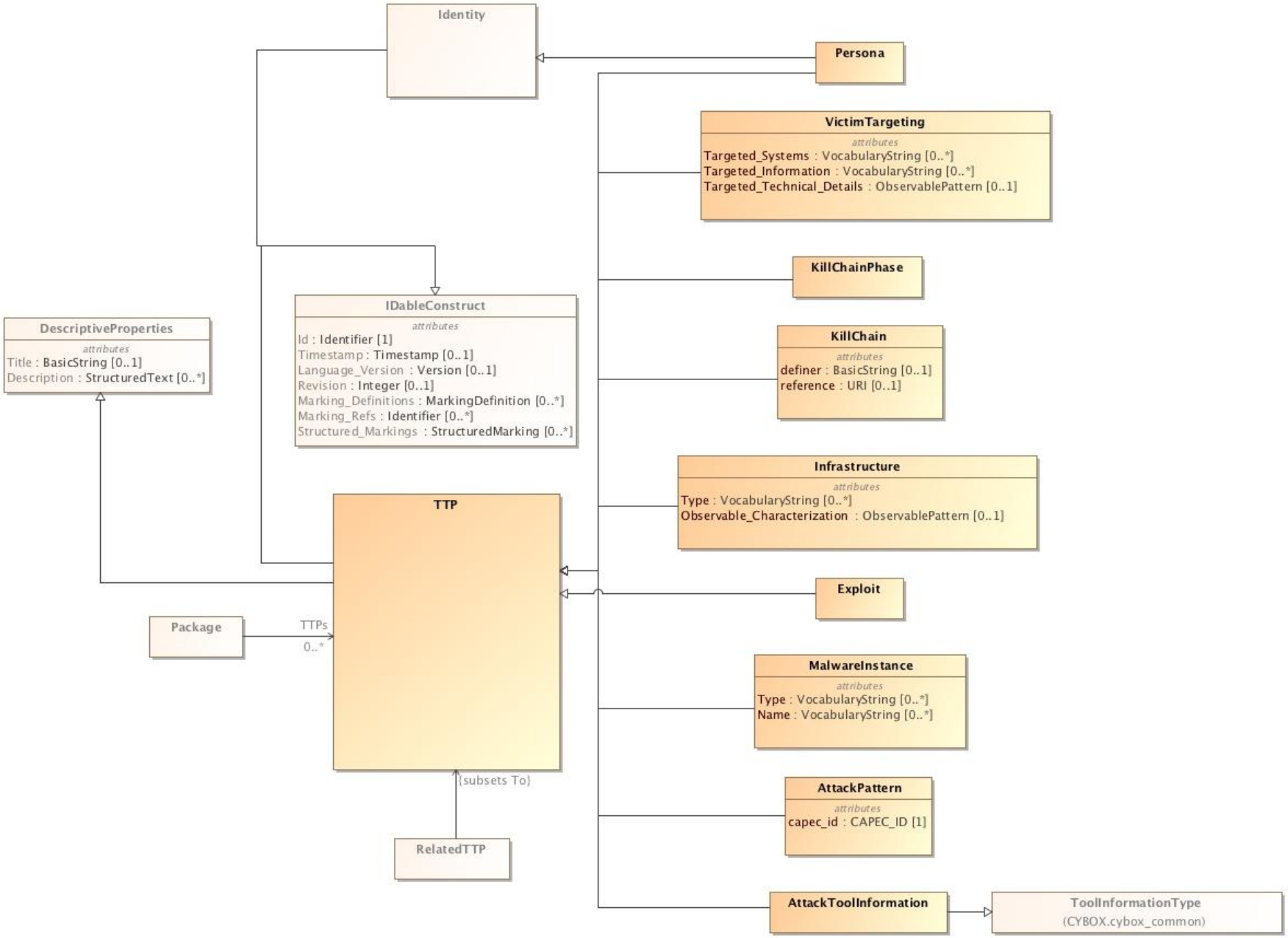
Remove abstract base types (prop#15)

- Quick summary of consensus
  - Both “strawmen” agree that the current abstract base types for the ”top-level” objects are superfluous and should be removed and the objects simply be defined on their own
- Any objections to this consensus?

TTP refactor for clarity (RM#10) (prop#12)

- Quick summary of consensus
  - Both “strawmen” agree that the current TTP structure where Attack_Pattern, Malware, Exploit, Infrastructure, Tools, Persona and VictimTargeting are listed as properties should be changed such that these are each subclasses of a general TTP structure.

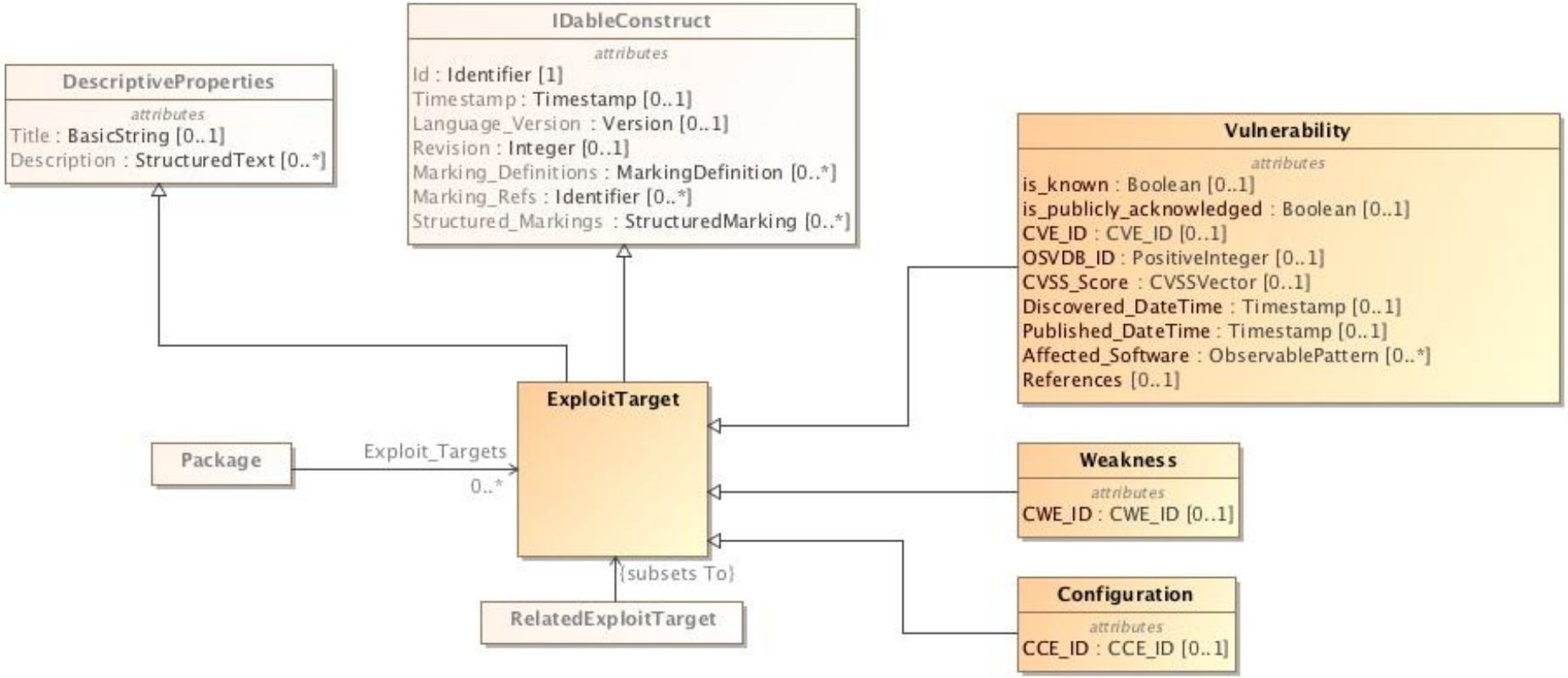
- Any objections to this consensus?


Identity
Persona
VictimTargeting
attributes
Targeted_Systems : VocabularyString [0..*]
Targeted_Information : VocabularyString [0..*]
Targeted_Technical_Details : ObservablePattern [0..1]
KillChainPhase
IDableConstruct
attributes
Id : Identifier [1]
Timestamp : Timestamp [0..1]
Language_Version : Version [0..1]
Revision : Integer [0..1]
Marking_Definitions : MarkingDefinition [0..*]
Marking_Refs : Identifier [0..*]
Structured_Markings : StructuredMarking [0..*]
DescriptiveProperties
attributes
Title : BasicString [0..1]
Description : StructuredText [0..*]
KillChain
attributes
definer : BasicString [0..1]
reference : URI [0..1]
Infrastructure
attributes
Type : VocabularyString [0..*]
Observable_Characterization : ObservablePattern [0..1]
TTP
Exploit
Package
TTPs
0..*
MalwareInstance
attributes
Type : VocabularyString [0..*]
Name : VocabularyString [0..*]
{subsets To}
AttackPattern
attributes
capec_id : CAPEC_ID [1]
RelatedTTP
AttackToolInformation
ToolInformationType
(CYBOX.cybox_common)

ET refactor for clarity (prop#17)

- Quick summary of consensus
  - Both “strawmen” agree that the current ExploitTarget structure where Vulnerability, Weakness and Configuration are listed as properties should be changed such that these are each subclasses of a general ExploitTarget structure.

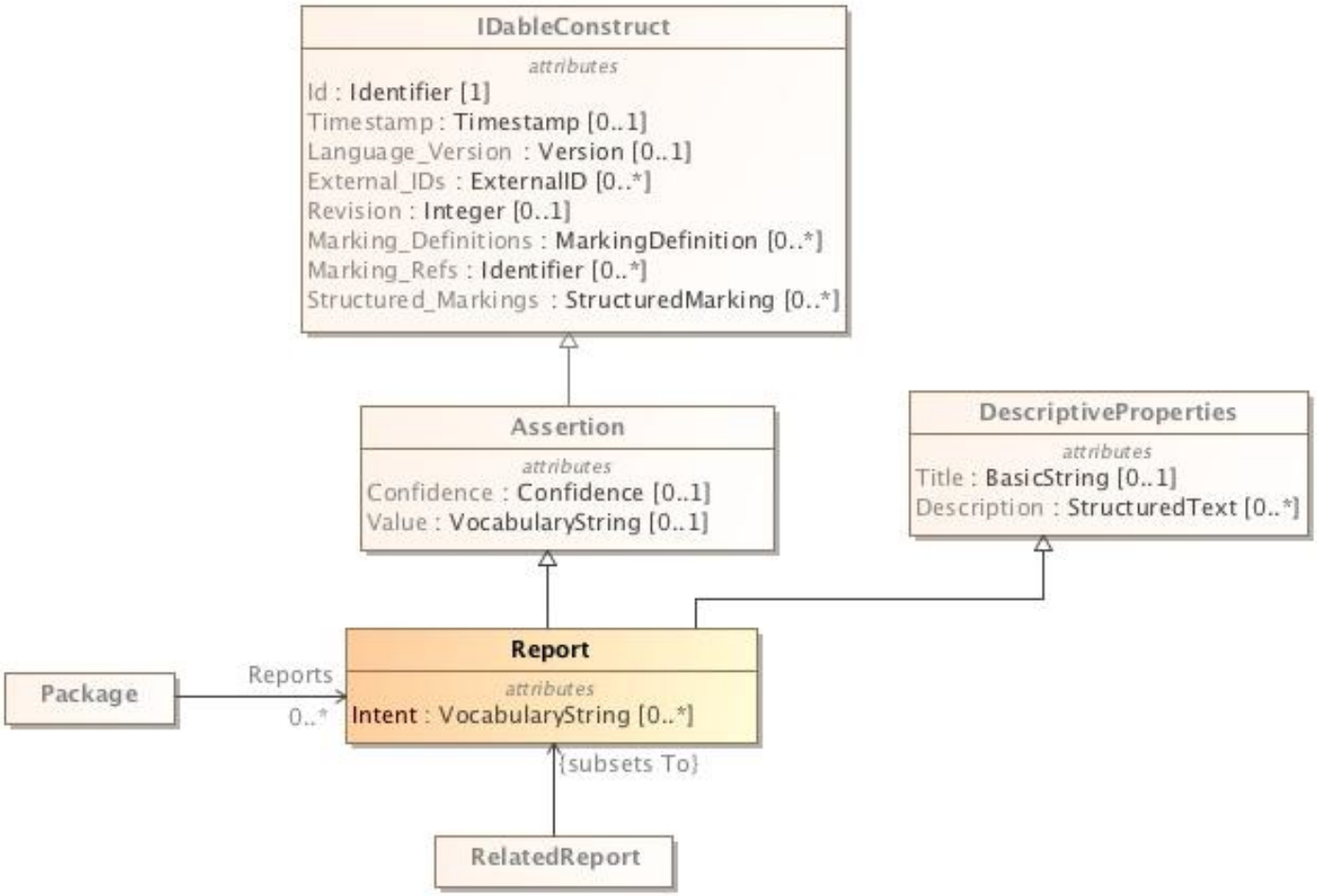
- Any objections to this consensus?


IDableConstruct
attributes
Id : Identifier [1]
Timestamp : Timestamp [0..1]
Language_Version : Version [0..1]
Revision : Integer [0..1]
Marking_Definitions : MarkingDefinition [0..*]
Marking_Refs : Identifier [0..*]
Structured_Markings : StructuredMarking [0..*]
DescriptiveProperties
attributes
Title : BasicString [0..1]
Description : StructuredText [0..*]
Vulnerability
attributes
is_known : Boolean [0..1]
is_publicly_acknowledged : Boolean [0..1]
CVE_ID : CVE_ID [0..1]
OSVDB_ID : PositiveInteger [0..1]
CVSS_Score : CVSSVector [0..1]
Discovered_DateTime : Timestamp [0..1]
Published_DateTime : Timestamp [0..1]
Affected_Software : ObservablePattern [0..*]
References [0..1]
ExploitTarget
Package
Exploit_Targets
0..*
Weakness
attributes
CWE_ID : CWE_ID [0..1]
{subsets To}
RelatedExploitTarget
Configuration
attributes
CCE_ID : CCE_ID [0..1]

Report refactor (prop#16)

- Quick summary of consensus
  - Both “strawmen” agree that due to the changes for no embedding of content and relationships as separate objects the Report object should be refactored to not contain definitions of or references to content but rather, acting as kind of a report cover sheet, all content relevant to the report would be asserted as separate relationship objects with a “Report Contains” nature

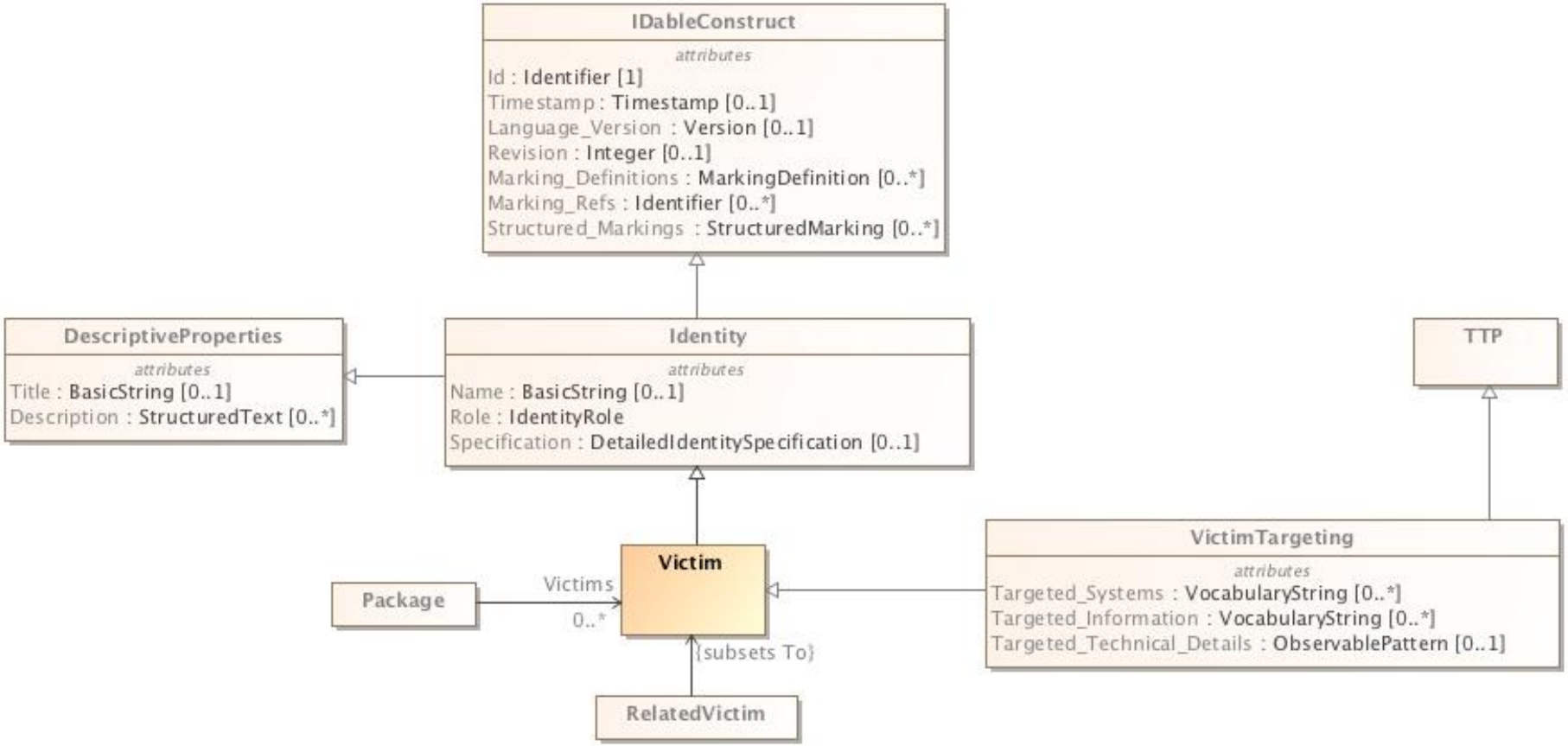
- Any objections to this consensus?


IDableConstruct
attributes
Id : Identifier [1]
Timestamp : Timestamp [0..1]
Language_Version : Version [0..1]
External_IDs : ExternalID [0..*]
Revision : Integer [0..1]
Marking_Definitions : MarkingDefinition [0..*]
Marking_Refs : Identifier [0..*]
Structured_Markings : StructuredMarking [0..*]
Assertion
attributes
Confidence : Confidence [0..1]
Value : VocabularyString [0..1]
DescriptiveProperties
attributes
Title : BasicString [0..1]
Description : StructuredText [0..*]
Report
attributes
Intent : VocabularyString [0..*]
Package
Reports
0..*
{subsets To}
RelatedReport

Abstract Victim to separate construct (prop#18)

- Quick summary of consensus
  - Both “strawmen” agree that a new Victim construct should be created as an Identity class, that this new class should be used for Victim characterization within Incidents, and that a VictimTargeting class should be created that is a subclass of both TTP and Victim with additional properties for Targeted_Systems, Targeted_Information and Targeted_Technical_Details.

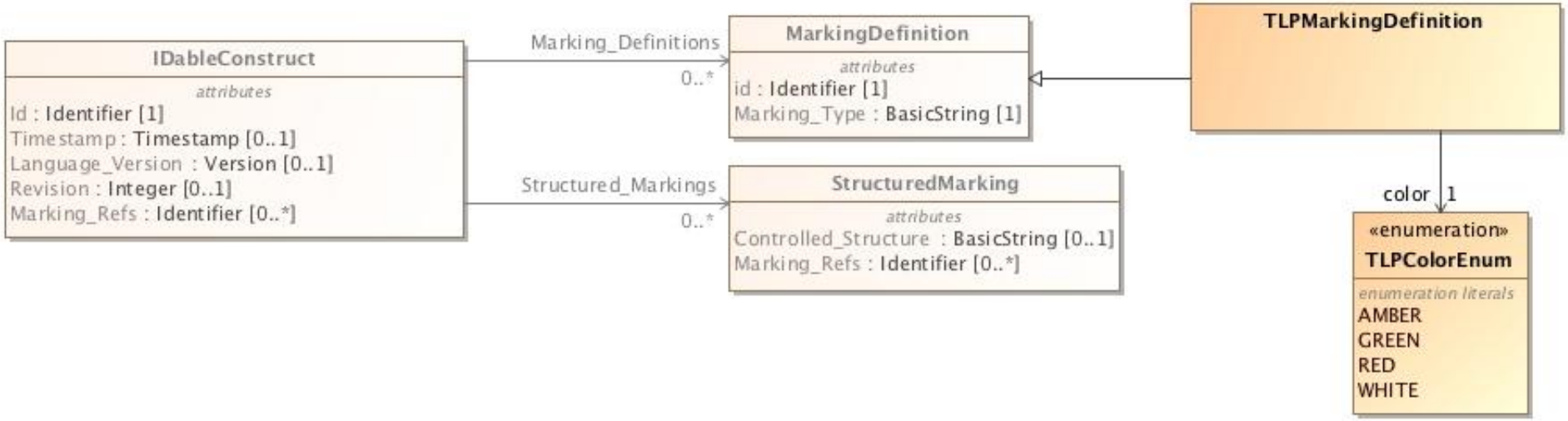
- Any objections to this consensus?


IDableConstruct
attributes
Id : Identifier [1]
Timestamp : Timestamp [0..1]
Language_Version : Version [0..1]
Revision : Integer [0..1]
Marking_Definitions : MarkingDefinition [0..*]
Marking_Refs : Identifier [0..*]
Structured_Markings : StructuredMarking [0..*]
DescriptiveProperties
attributes
Title : BasicString [0..1]
Description : StructuredText [0..*]
Identity
attributes
Name : BasicString [0..1]
Role : IdentityRole
Specification : DetailedIdentitySpecification [0..1]
TTP
Victim
Package
Victims
0..*
{subsets To}
RelatedVictim
VictimTargeting
attributes
Targeted_Systems : VocabularyString [0..*]
Targeted_Information : VocabularyString [0..*]
Targeted_Technical_Details : ObservablePattern [0..1]

DataMarkings application (RM#2)

- Quick summary of consensus
  - Both “strawmen” agree to the proposed and discussed approach utilizing Marking_Definitions, Marking_Refs (L1) and Structured_Markings (L2)

- Any objections to this consensus?


IDableConstruct
attributes
Id : Identifier [1]
Timestamp : Timestamp [0..1]
Language_Version : Version [0..1]
Revision : Integer [0..1]
Marking_Refs : Identifier [0..*]
Marking_Definitions
0..*
Structured_Markings
0..*
MarkingDefinition
attributes
id : Identifier [1]
Marking_Type : BasicString [1]
StructuredMarking
attributes
Controlled_Structure : BasicString [0..1]
Marking_Refs : Identifier [0..*]
TLPMarkingDefinition
color
1
«enumeration»
TLPColorEnum
enumeration literals
AMBER
GREEN
RED
WHITE

Summary out

- Consensus items

- Non-consensus items