

THE MITRE CORPORATION

STIX™ 1.2

COMMON SPECIFICATION (v1.2)

JULY 23, 2015

The Structured Threat Information eXpression (STIX™) framework defines nine core constructs and the relationships between them for the purposes of modeling cyber threat information and enabling cyber threat information analysis and sharing. This specification document defines the Common data model, which defines base classes that are extended or leveraged by the core components, relationship-oriented classes, content aggregation classes, vocabulary-related classes, kill chain-related classes, and other classes shared by the core constructs.

Acknowledgements

The authors would like to thank the STIX Community for its input and help in reviewing this document.

Trademark Information

STIX, the STIX logo, and CybOX are trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners.

Warnings

MITRE PROVIDES STIX "AS IS" AND MAKES NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, CAPABILITY, EFFICIENCY, MERCHANTABILITY, OR FUNCTIONING OF STIX. IN NO EVENT WILL MITRE BE LIABLE FOR ANY GENERAL, CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY, OR SPECIAL DAMAGES, RELATED TO STIX OR ANY DERIVATIVE THEREOF, WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, OR TORT, EVEN IF MITRE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.¹

Feedback

The STIX development team welcomes any feedback regarding this document. Please send any comments, questions, or suggestions to stix@mitre.org.²

¹ For detailed information see [TOU].

² For more information about the STIX Language, please visit [STIX].

Table of Contents

1	Introduction	1
1.1	STIX Specification Documents	1
1.2	Document Conventions	2
1.2.1	Keywords	2
1.2.2	Fonts	2
1.2.3	UML Package References	3
1.2.4	UML Diagrams	3
1.2.4.1	Class Properties	3
1.2.4.2	Diagram Icons and Arrow Types	4
1.2.4.3	Color Coding	4
1.2.5	Property Table Notation	5
1.2.6	Property and Class Descriptions	5
2	Background Information	7
3	STIX Common Data Model	8
3.1	Component Base Classes	8
3.1.1	CampaignBaseType Class	9
3.1.2	CourseOfActionBaseType Class	10
3.1.3	ExploitTargetBaseType Class	11
3.1.4	IncidentBaseType Class	12
3.1.5	IndicatorBaseType Class	13
3.1.6	ThreatActorBaseType Class	14
3.1.7	TTPBaseType Class	15
3.1.8	ReportBaseType Class	16
3.2	Relationship-Oriented Classes	17
3.2.1	GenericRelationshipType Class	17
3.2.2	RelatedCampaignType Class	18
3.2.3	RelatedCampaignReferenceType Class	20
3.2.3.1	CampaignReferenceType Class	21
3.2.4	RelatedCourseOfActionType Class	21
3.2.5	RelatedExploitTargetType Class	23
3.2.6	RelatedIdentityType Class	24
3.2.7	RelatedIncidentType Class	25
3.2.8	RelatedIndicatorType Class	27
3.2.9	RelatedObservableType Class	28
3.2.10	RelatedPackageRefType Class	29
3.2.11	RelatedReportType Class	30
3.2.12	RelatedThreatActorType Class	32
3.2.13	RelatedTTPType Class	33
3.3	Content Aggregation Classes	35
3.3.1	GenericRelationshipListType	35
3.3.2	ConfidenceAssertionChainType Class	36

3.3.3	ContributingSourcesType Class.....	37
3.3.4	ExploitTargetsType Class.....	38
3.3.5	NamesType Class	39
3.3.6	ProfilesType Class	39
3.3.7	ReferencesType Class.....	40
3.3.8	RelatedIdentitiesType Class	40
3.3.9	RelatedPackageRefsType Class	41
3.4	Kill Chains	41
3.4.1	KillChainsType Class	41
3.4.1.1	KillChainType Class	42
3.4.2	KillChainPhasesReferenceType Class	43
3.4.2.1	KillChainPhaseReferenceType Class	44
3.5	General Shared Classes	44
3.5.1	ActivityType Class.....	45
3.5.2	AddressAbstractType Class	45
3.5.3	ConfidenceType Class	46
3.5.4	IdentityType Class	47
3.5.5	InformationSourceType Class	48
3.5.6	StatementType Class.....	50
3.5.7	ToolInformationType Class	51
3.6	General Data Types	52
3.6.1	DateTimeWithPrecisionType Data Type	52
3.6.2	NativeFormatStringType Data Type.....	53
3.6.3	StructuredTextType Data Type	54
3.7	Vocabulary Data Types.....	55
3.7.1	VocabularyStringType Data Type.....	58
3.7.2	UnenforcedVocabularyStringType Data Type	58
3.7.3	ControlledVocabularyStringType Data Type.....	58
3.8	Enumerations	59
3.8.1	DateTimePrecisionEnum Enumeration.....	59
3.8.2	RelationshipScopeEnum	60
References		61

1 Introduction

The Structured Threat Information eXpression (STIX™) framework defines nine top-level component data models: Observable³, Indicator, Incident, TTP, ExploitTarget, CourseOfAction, Campaign, ThreatActor, and Report. In addition, it defines a common data model that defines base classes that are extended or leveraged by the core components, relationship-oriented classes, content aggregation classes, kill chain-related classes, and other classes shared by the core constructs. This document serves as the specification for the STIX Common Version 1.2 data model.

The STIX Common data model defines object classes that are shared across the various STIX data models. For clarity in the document, the classes are divided into five types: component base classes (Section 3.1), relationship-oriented classes (Section 3.1.8), content aggregation classes (Section 3.3), kill chain-related classes (Section 3.4), and general shared classes (Section 3.5). We also list general data types (Section 3.6), vocabulary-related data types (Section 3.7), and enumerations separately (Section 3.8).

In Section 1.1 we discuss STIX specification documents, and in Section 1.2 we give document conventions. In Section 2, we give background information necessary to fully understand the Common data model, and we present the Common data model specification details in Section 3. References are provided in the final section.

1.1 STIX Specification Documents

The STIX specification consists of a formal UML model and a set of textual specification documents that explain the UML model. Specification documents have been written for each of the key data models that compose the full STIX UML model.

The STIX specification overview document provides a comprehensive overview of the full set of STIX data models [STIX_o], which in addition to the nine top-level component data models mentioned in the Introduction, includes a core data model, a common data model, a cross-cutting data marking data model, various extension data models and a set of default controlled vocabularies. [STIX_o] also summarizes the relationship of STIX to other languages and outlines general STIX data model conventions.

Figure 1-1 illustrates the set of specification documents that are available. The color black is used to indicate the specification overview document, altered shading differentiates the overarching Core data model from the supporting data models (default vocabularies, data marking, and extensions), and the color white indicates the component data models. The Observable component data model is shown as an oval shape to indicate that it is defined

³ The CybOX Observable data model is actually defined in the CybOX Language, not in STIX; but it is included in the list because it is referenced often from STIX.

as a CybOX specification (see [STIX₀] for details). This Common specification document is highlighted in its associated color (see Section 1.2.4.3). For a list of all STIX documents and related information sources, please see [STIX₀].

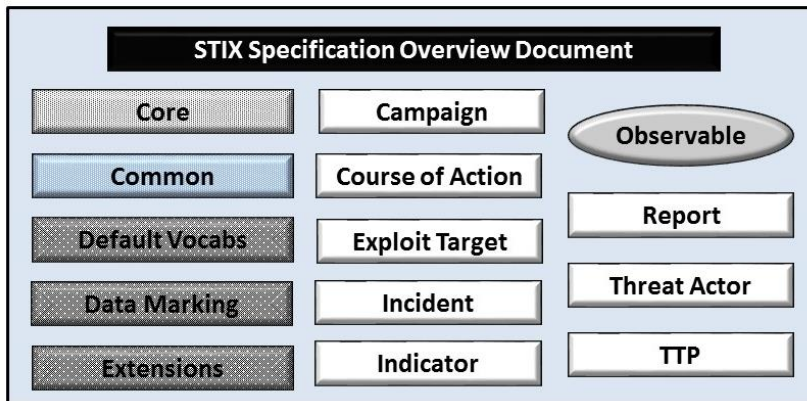


Figure 1-1. STIX Language v1.2 specification documents

All specification documents can be found on this STIX Website [STIX-SPECS].

1.2 Document Conventions

The following conventions are used in this document.

1.2.1 Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in *RFC 2119* [RFC2119].

1.2.2 Fonts

The following font and font style conventions are used in the document:

- Capitalization is used for STIX high level concepts, which are defined in the STIX Specification Overview [STIX₀].

Examples: Indicator, Course of Action, Threat Actor

- The Courier New font is used for writing UML objects.

Examples: RelatedIndicatorsType, stixCommon:StatementType

Note that all high level concepts have a corresponding UML object. For example, the Course of Action high level concept is associated with a UML class named, CourseOfActionType.

- The '*italic*' font (with single quotes) is used for noting actual, explicit values for STIX Language properties. The *italic* font (without quotes) is used for noting example values.

Example: '*PackageIntentVocab-1.0*,' *high*, *medium*, *low*

1.2.3 UML Package References

Each STIX data model is captured in a different UML package (e.g., Core package, Campaign package, etc.) where the packages together compose the full STIX UML model. To refer to a particular class of a specific package, we use the format `package_prefix:class`, where `package_prefix` corresponds to the appropriate UML package. The STIX 1.2 Specification Overview document [STIX₀] contains a list of the packages used by the Common data model, along with the associated prefix notations, descriptions, examples.

Note that in this specification document, we do not explicitly specify the package prefix for any classes that originate from the Common data model.

1.2.4 UML Diagrams

This specification makes use of UML diagrams to visually depict relationships between STIX Language constructs. Note that the diagrams have been extracted directly from the full UML model for STIX; they have not been constructed purely for inclusion in the specification documents. Typically, diagrams are included for the primary class of a data model, and for any other class where the visualization of its relationships between other classes would be useful. This implies that there will be very few diagrams for classes whose only properties are data types. Other diagrams that are included correspond to classes that specialize a superclass and abstract or generalized classes that are extended by one or more subclasses.

In UML diagrams, classes are often presented with their attributes elided, to avoid clutter. The fully described class can usually be found in a related diagram. A class presented with an empty section at the bottom of the icon indicates that there are no attributes other than those that are visualized using associations.

1.2.4.1 Class Properties

Generally, a class property can be shown in a UML diagram as either an attribute or an association (i.e., the distinction between attributes and associations is somewhat subjective). In order to make the size of UML diagrams in the specifications manageable, we have chosen to capture most properties as attributes and to capture only higher level properties as associations, especially in the main top-level component diagrams. In particular, we will always capture properties of UML data types as attributes. For example, properties of a class that are identifiers, titles, and timestamps will be represented as attributes.

1.2.4.2 Diagram Icons and Arrow Types

Diagram icons are used in a UML diagram to indicate whether a shape is a class, enumeration or data type, and decorative icons are used to indicate whether an element is an attribute of a class or an enumeration literal. In addition, two different arrow styles indicate either a directed association relationship (regular arrowhead) or a generalization relationship (triangle-shaped arrowhead). The icons and arrow styles we use are shown and described in Table 1-1.

Table 1-1. UML diagram icons

Icon	Description
	This diagram icon indicates a class. If the name is in italics, it is an abstract class.
	This diagram icon indicates an enumeration.
	This diagram icon indicates a data type.
	This decorator icon indicates an attribute of a class. The green circle means its visibility is public. If the circle is red or yellow, it means its visibility is private or protected.
	This decorator icon indicates an enumeration literal.
	This arrow type indicates a directed association relationship.
	This arrow type indicates a generalization relationship.

1.2.4.3 Color Coding

The shapes of the UML diagrams are color coded to indicate the data model associated with a class. The colors used in the Common specification are illustrated via exemplars in Figure 1-2.

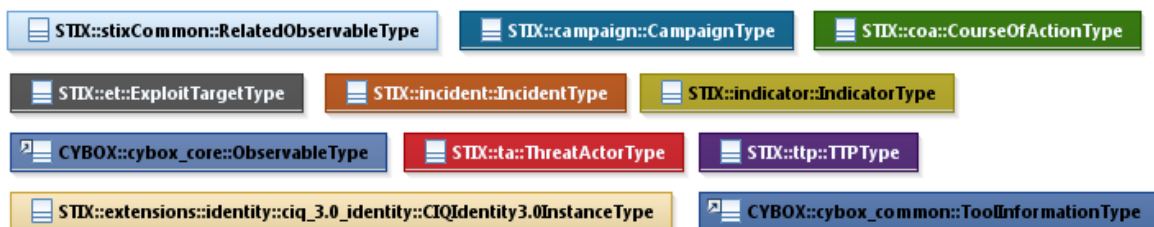


Figure 1-2. Data model color coding

1.2.5 Property Table Notation

Throughout Section 3, tables are used to describe the properties of each data model class. Each property table consists of a column of names to identify the property, a type column to reflect the datatype of the property, a multiplicity column to reflect the allowed number of occurrences of the property, and a description column that describes the property. Package prefixes are provided for classes outside of the Common data model (see Section 1.2.3).

Note that if a class is a specialization of a superclass, only the properties that constitute the specialization are shown in the property table (i.e., properties of the superclass will not be shown). However, details of the superclass may be shown in the UML diagram.

In addition, properties that are part of a “choice” relationship (e.g., Prop1 OR Prop2 is used but not both) will be denoted by a unique letter subscript (e.g., API_Call_A, Code_B) and single logic expression in the Multiplicity column. For example, if there is a choice of property API_Call_A and Code_B, the expression “A(1)|B(0..1)” will indicate that the API_Call property can be chosen with multiplicity 1 or the Code property can be chosen with multiplicity 0 or 1.

1.2.6 Property and Class Descriptions

Each class and property defined in STIX is described using the format, “The X property verb Y.” For example, in the specification for the STIX Indicator, we write, “The id property specifies a globally unique identifier for the kill chain instance.” In fact, the verb “specifies” could have been replaced by any number of alternatives: “defines,” “describes,” “contains,” “references,” etc.

However, we thought that using a wide variety of verb phrases might confuse a reader of a specification document because the meaning of each verb could be interpreted slightly differently. On the other hand, we didn’t want to use a single, generic verb, such as “describes,” because although the different verb choices may or may not be meaningful from an implementation standpoint, a distinction could be useful to those interested in the modeling aspect of STIX.

Consequently, we have chosen to use the three verbs, defined as follows, in class and property descriptions:

Verb	STIX Definition
<u>captures</u>	Used to record and preserve information without implying anything about the structure of a class or property. Often used for properties that encompass general content. This is the least precise of the three verbs.
	<i>Examples:</i> The Source property characterizes the source of the sighting information. Examples of details <u>captured</u> include identifying

	<p>characteristics, time-related attributes, and a list of the tools used to collect the information.</p> <p>The <code>Description</code> property <u>captures</u> a textual description of the Indicator.</p>
<u>characterizes</u>	<p>Describes the distinctive nature or features of a class or property. Often used to describe classes and properties that themselves comprise one or more other properties.</p>
	<p><i>Examples:</i></p> <p>The <code>Confidence</code> property <u>characterizes</u> the level of confidence in the accuracy of the overall content captured in the Incident.</p> <p>The <code>ActivityType</code> class <u>characterizes</u> basic information about an activity a defender might use in response to a Campaign.</p>
<u>specifies</u>	<p>Used to clearly and precisely identify particular instances or values associated with a property. Often used for properties that are defined by a controlled vocabulary or enumeration; typically used for properties that take on only a single value.</p>
	<p><i>Example:</i></p> <p>The <code>version</code> property <u>specifies</u> the version identifier of the STIX Campaign data model used to capture the information associated with the Campaign.</p>

2 Background Information

In this section, we provide high level information about the Common data model that is useful to fully understand the Common data model specification details given in Section 3.

The STIX Common data model defines object classes that are shared across the various STIX data models. There is a wide variety of class types, so to make the specification document content easier to reference and understand, we have organized the data model content into eight categories:

- **Component Base Classes** – defined for each of the top-level STIX components⁴: Campaign, Course of Action, Exploit Target, Incident, Indicator, Threat Actor, TTP and Report.
- **Relationship-oriented Classes** – capture relationships between STIX constructs.
- **Content Aggregation Classes** – capture a collection of one or more STIX objects.
- **Kill Chain-related Classes** – facilitate the use of a phase-based model to describe the stages of an attack.
- **General Shared Classes** – serve a variety of purposes and shared by the collection of STIX data models.
- **General Data Types** – support the classes defined in the STIX data models.
- **Vocabulary Data Types** – provide a content creator with choices for defining content.
- **Enumerations** – support the classes defined in the STIX data models.

Each category is contained in a separate subsection in Section 3.

⁴ There is currently no base class defined for the Observable component, which is defined in the CybOX Language [CybOX].

3 STIX Common Data Model

There is no primary class of the STIX Common UML package because the Common data model contains a collection of classes that are used by the other STIX Packages. We have separated the classes into six categories (Sections 3.1 through 3.5), and within each category, we primarily define the classes in alphabetical order below, except for the cases when one class (a superclass) is specialized by other classes, in which case the superclass is defined first. In addition, in the Shared Classes section, if a set of classes are related in concept, they are also grouped and are not necessarily in alphabetical order. We list data types and enumerations in Sections 3.6 and 3.7, respectively.

3.1 Component Base Classes

The STIX Common data model provides base classes (superclasses) for each of the top-level STIX components⁵: Campaign, Course of Action, Exploit Target, Incident, Indicator, Threat Actor, TTP, and Report. The STIX Common base classes are minimal and are intended to be extended by the corresponding STIX component defined in that specification. The use of base classes allows the STIX language to be modular: all of the STIX components are defined in separate data models rather than in one large data model to limit interdependence between STIX components.

The default and strongly recommended class for fully implementing each STIX component is the primary class defined in the STIX component's data model. For example, consider the STIX Common `CampaignBaseType` base class, which is specialized in the Campaign data model to define the `CampaignType` class. The corresponding UML diagram is shown in Figure 3-1.

⁵ There is currently no base class defined for the Observable component, which is defined in the CybOX Language [CybOX].

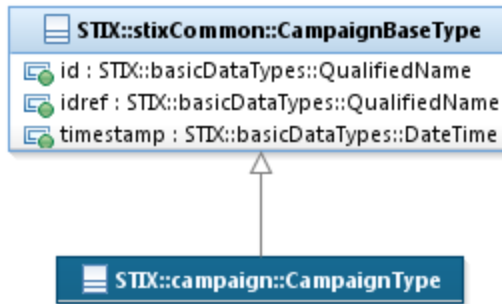


Figure 3-1. UML diagram showing the use of the `CampaignBaseType` base class

The collection of component base classes are defined in Sections 3.1.1 through 3.1.7; however, because all of the component superclasses are similar, UML diagrams analogous to Figure 3-1 are not included.

3.1.1 CampaignBaseType Class

The `CampaignBaseType` class is intended to be extended by a subclass, which characterizes a campaign. The decision to define base classes that are extended – like the `CampaignBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `CampaignBaseType` class is the `CampaignType` class in the Campaign data model [STIX_{CAM}].

The property table of the `CampaignBaseType` base class is given in Table 1-1.

Table 3-1. Properties of the `CampaignBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Campaign instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to a Campaign instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and

			timestamp should be specified.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of a Campaign. When used in conjunction with the <code>id</code> property, it specifies the definition time for the specific version of the Campaign instance; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of a Campaign instance defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.

3.1.2 CourseOfActionBaseType Class

The `CourseOfActionBaseType` class is intended to be extended by a subclass, which characterizes a course of action. The decision to define base classes that are extended – like the `CourseOfActionBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `CourseOfActionBaseType` class is the `CourseOfActionType` class in the Course of Action data model [STIX_{COA}]. The one case where the class SHOULD NOT be extended is when the `CourseOfActionBaseType` class is used as a reference via its `idref` property.

The property table of the `CourseOfActionBaseType` base class are given in Table 3-2.

Table 3-2. Properties of the `CourseOfActionBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Course of Action instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to a Course of Action instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.

timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of a Course of Action. When used in conjunction with the <code>id</code> property, it specifies the definition time for the specific version of the Course of Action instance; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of a Course of Action instance defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.
------------------	--------------------------------------	------	--

3.1.3 ExploitTargetBaseType Class

The `ExploitTargetBaseType` class is intended to be extended by a subclass, which characterizes an exploit target. The decision to define base classes that are extended – like the `ExploitTargetBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `ExploitTargetBaseType` class is the `ExploitTargetType` class in the Exploit Target data model [STIX_{ET}]. The one case where the class SHOULD NOT be extended is when the `ExploitTargetBaseType` class is used as a reference via its `idref` property.

The property table of the `ExploitTargetBaseType` base class is given in Table 3-3.

Table 3-3. Properties of the `ExploitTargetBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Exploit Target instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to an Exploit Target instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of an Exploit Target. When used in conjunction

			with the <code>id</code> property, it specifies the definition time for the specific version of the Exploit Target instance; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of an Exploit Target instance defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.
--	--	--	---

3.1.4 IncidentBaseType Class

The `IncidentBaseType` class is intended to be extended by a subclass, which characterizes an incident. The decision to define base classes that are extended – like the `IncidentBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `IncidentBaseType` class is the `IncidentType` class in the Incident data model [STIX_{INC}]. The one case where the class SHOULD NOT be extended is when the `IncidentBaseType` class is used as a reference via its `idref` property.

The property table of the `IncidentBaseType` base class is given in Table 3-4.

Table 3-4. Properties of the `IncidentBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Incident instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to an Incident instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of an Incident. When used in conjunction with the <code>id</code> property, it specifies the definition time for the specific version of the Incident instance; when used in conjunction with the <code>idref</code> property, it specifies the

			definition time for a specific version of an Incident instance defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.
--	--	--	--

3.1.5 IndicatorBaseType Class

The `IndicatorBaseType` class is intended to be extended by a subclass, which characterizes an indicator. The decision to define base classes that are extended – like the `IndicatorBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `IndicatorBaseType` class is the `IndicatorType` class in the Indicator data model [STIX_{IND}]. The one case where the class SHOULD NOT be extended is when the `IndicatorBaseType` class is used as a reference via its `idref` property.

The property table of the `IndicatorBaseType` base class is given in Table 3-5.

Table 3-5. Properties of the `IndicatorBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Indicator instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to an Indicator instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of an Indicator. When used in conjunction with the <code>id</code> property, it specifies the definition time for the specific version of the Indicator instance; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of an Indicator instance defined elsewhere. The <code>timestamp</code> property has no defined

			semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.
--	--	--	---

3.1.6 ThreatActorBaseType Class

The `ThreatActorBaseType` class is intended to be extended by a subclass, which characterizes a threat actor. The decision to define base classes that are extended – like the `ThreatActorBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `ThreatActorBaseType` class is the `ThreatActorType` class in the Threat Actor data model [STIX_{TA}]. The one case where the class SHOULD NOT be extended is when the `ThreatActorBaseType` class is used as a reference via its `idref` property.

The property table of the `ThreatActorBaseType` base class is given in Table 3-6.

Table 3-6. Properties of the `ThreatActorBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Threat Actor instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to a Threat Actor instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of a Threat Actor. When used in conjunction with the <code>id</code> property, it specifies the definition time for the specific version of the Threat Actor instance; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of a Threat Actor instance defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.

3.1.7 TTPBaseType Class

The `TTPBaseType` class is intended to be extended by a subclass, which characterizes a TTP. The decision to define base classes that are extended – like the `TTPBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `TTPBaseType` class is the `TTPType` class in the TTP data model [STIX_{TTP}]. The one case where the class SHOULD NOT be extended is when the `TTPBaseType` class is used as a reference via its `idref` property.

The property table of the `TTPBaseType` base class is given in Table 3-7.

Table 3-7. Properties of the `TTPBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the TTP instance.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to a TTP instance specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.
Timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the definition time of a specific version of a TTP. When used in conjunction with the <code>id</code> property, it specifies the definition time for the specific version of the TTP instance; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of a TTP instance defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.

3.1.8 ReportBaseType Class

The `ReportBaseType` class is intended to be extended by a subclass, which characterizes a report. The decision to define base classes that are extended – like the `ReportBaseType` class – was made to minimize interdependence between STIX components; it was not made to enable structural variation. The default and strongly RECOMMENDED subclass to extend the `ReportBaseType` class is the `ReportType` class in the Report data model [STIX_{REP}]. The one case where the class SHOULD NOT be extended is when the `ReportBaseType` class is used as a reference via its `idref` property.

The property table of the `ReportBaseType` base class is given in Table 3-8.

Table 3-8. Properties of the `ReportBaseType` base class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the Report.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies an identifier reference to a Report specified elsewhere. When the <code>idref</code> property is used, no properties other than <code>idref</code> and <code>timestamp</code> should be specified.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	When used in conjunction with the <code>id</code> property, the <code>timestamp</code> property specifies the definition time for the specific version of the Report; when used in conjunction with the <code>idref</code> property, it specifies the definition time for a specific version of a Report defined elsewhere. The <code>timestamp</code> property has no defined semantic meaning if it is used without either the <code>id</code> or <code>idref</code> property.

3.2 Relationship-Oriented Classes

The STIX Common data model defines a number of classes that capture relationships between STIX constructs through specialization of the `GenericRelationshipType` abstract class, which is defined first.

3.2.1 GenericRelationshipType Class

The `GenericRelationshipType` class captures attributes associated with a relationship between a subject STIX construct and another STIX construct. It is an abstract class, and it **MUST** be extended via a subclass to specify the other STIX constructs. Use of the `GenericRelationshipType` class helps to define a consistent structure for relationships that go beyond a simple statement of “construct A is related to construct B.” Instead, additional properties of the relationship can be specified such as the nature of the relationship and the level of confidence in the presence and accuracy of the asserted relationship.

The property table of the `GenericRelationshipType` class is given in Table 3-9.

Table 3-9. Properties of the `GenericRelationshipType` class

Name	Type	Multiplicity	Description
Confidence	<code>ConfidenceType</code>	0..1	The <code>Confidence</code> property characterizes the level of confidence in the presence and accuracy of the asserted relationship.
Information_Source	<code>InformationSourceType</code>	0..1	The <code>Information_Source</code> property characterizes the source of the relationship information. Examples of details captured include identifying characteristics, time-related attributes, and a list of tools used to collect the information.
Relationship	<code>VocabularyStringType</code>	0..1	The <code>Relationship</code> property specifies the nature of the relationship between two STIX constructs. Examples of potential natures of relationship include <i>Updates - Revises</i> (for versioning of content), <i>Asserted Same</i> (for relating two Threat Actors), and <i>Leverages</i> (for relating two TTPs). These specific values are only provided to help explain the property: they are neither recommended values nor necessarily part of any existing vocabulary). The content creator may choose any arbitrary value or may constrain the set of possible values by referencing an externally-defined

			vocabulary or leveraging a formally defined vocabulary extending from the <code>ControlledVocabularyStringType</code> class. No default vocabulary is defined in STIX v1.2.
--	--	--	---

As an example of how the `GenericRelationshipType` class is used, consider the UML diagram shown in Figure 3-2, which shows the relationship between an Indicator and a TTP. As illustrated, the `GenericRelationshipType` class enables capture of information that further defines the relationship between the Indicator and the TTP. Namely, it specifies the level of confidence that the two constructs are related and the source of the relationship information, and it characterizes the nature of the relationship between the two constructs.

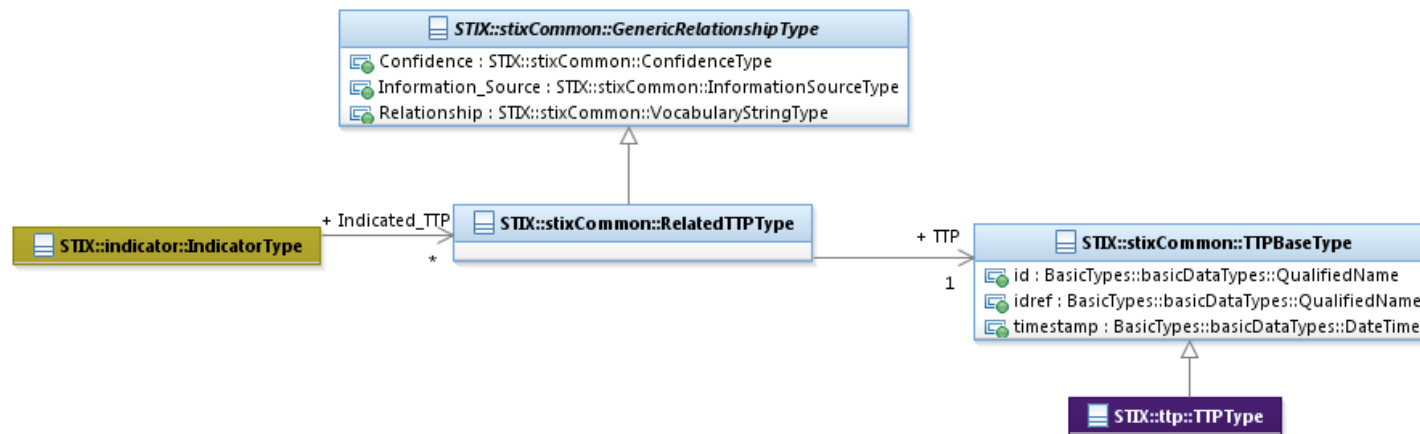


Figure 3-2. UML diagram of the Indicator/TTP relationship

3.2.2 RelatedCampaignType Class

The `RelatedCampaignType` class characterizes a relationship to a Campaign. It extends the `GenericRelationshipType` superclass by specifying the Campaign.

The UML diagram corresponding to the `RelatedCampaignType` class is shown in Figure 3-3.

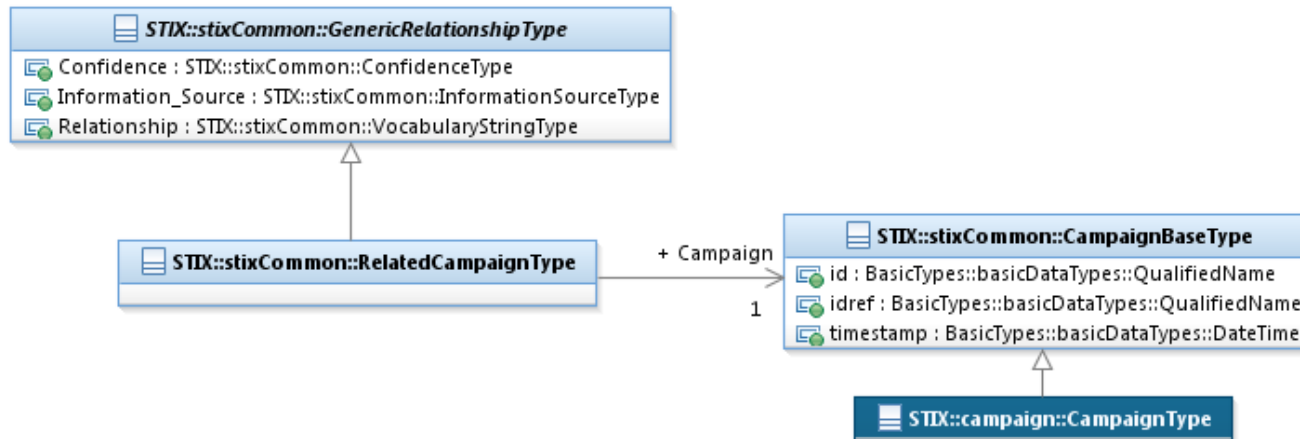


Figure 3-3. UML diagram of the RelatedCampaignType class

The property table given in Table 3-10 corresponds to the UML diagram shown in Figure 3-3.

Table 3-10. Properties of the RelatedCampaignType class

Name	Type	Multiplicity	Description
Campaign	CampaignBaseType	1	The Campaign property characterizes a cyber threat Campaign. The CampaignBaseType class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement a Campaign is the campaign: CampaignType class defined in [STIX _{CAM}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the idref property, a reference to a Campaign defined elsewhere can be specified via the direct use of the CampaignBaseType class.

3.2.3 RelatedCampaignReferenceType Class

The `RelatedCampaignReferenceType` class characterizes a relationship to a Campaign. It extends the `GenericRelationshipType` superclass by specifying a reference to the Campaign. Unlike most other relationships that are defined in STIX, the `RelatedCampaignReferenceType` class does not allow a Campaign to be embedded; an already-defined Campaign **MUST** be specified by its Name property and/or a reference to its identifier.

The UML diagram corresponding to the `RelatedCampaignReferenceType` class is shown in Figure 3-4.

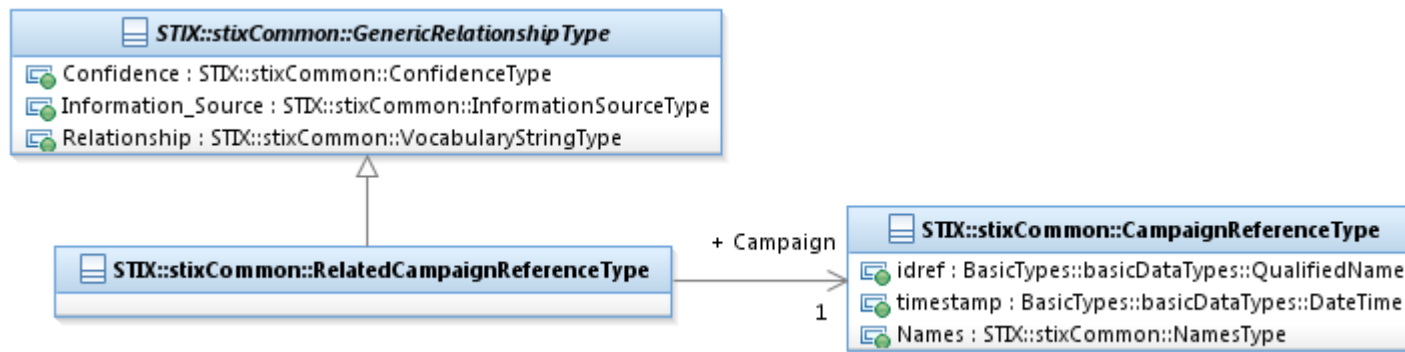


Figure 3-4. UML diagram of the `RelatedCampaignReferenceType` class

The property table given in Table 3-11 corresponds to the UML diagram shown in Figure 3-4.

Table 3-11. Properties of the `RelatedCampaignReferenceType` class

Name	Type	Multiplicity	Description
Campaign	<code>CampaignReferenceType</code>	0..1	The <code>Campaign</code> property captures a reference to the related Campaign.

The `RelatedCampaignReferenceType` class is defined in addition to the `RelatedCampaignType` class because in some cases it is not appropriate to define a Campaign *only* in the context of another construct, and in those cases, an otherwise defined

Campaign should be referenced. For example, a Campaign should not be defined only in the context of a single Indicator because the Indicator may be used across many Campaigns; a relationship between an Indicator and a Campaign should be a reference-only relationship (see the `Related_Campaigns` class defined in [STIX_{IND}]).

3.2.3.1 CampaignReferenceType Class

The `CampaignReferenceType` class captures a reference to a related Campaign.

The property table of the `CampaignReferenceType` class is given in Table 3-12.

Table 3-12. Properties of the `CampaignReferenceType` class

Name	Type	Multiplicity	Description
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies a globally unique identifier for a Campaign defined elsewhere.
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property, used in combination with the <code>idref</code> property, specifies a specific version of a Campaign defined elsewhere. To avoid ambiguity, all timestamps SHOULD include a specification of the time zone.
Names	<code>NamesType</code>	0..1	The <code>Names</code> property specifies a set of one or more names (i.e., aliases) used to identify a referenced Campaign (specified by an <code>idref</code> property). An organization may use names that are created internally or externally (outside the organization).

3.2.4 RelatedCourseOfActionType Class

The `RelatedCourseOfActionType` class characterizes a relationship to a Course of Action. It extends the `GenericRelationshipType` superclass by specifying a related Course of Action.

The UML diagram corresponding to the `RelatedCourseOfActionType` class is shown in Figure 3-5.

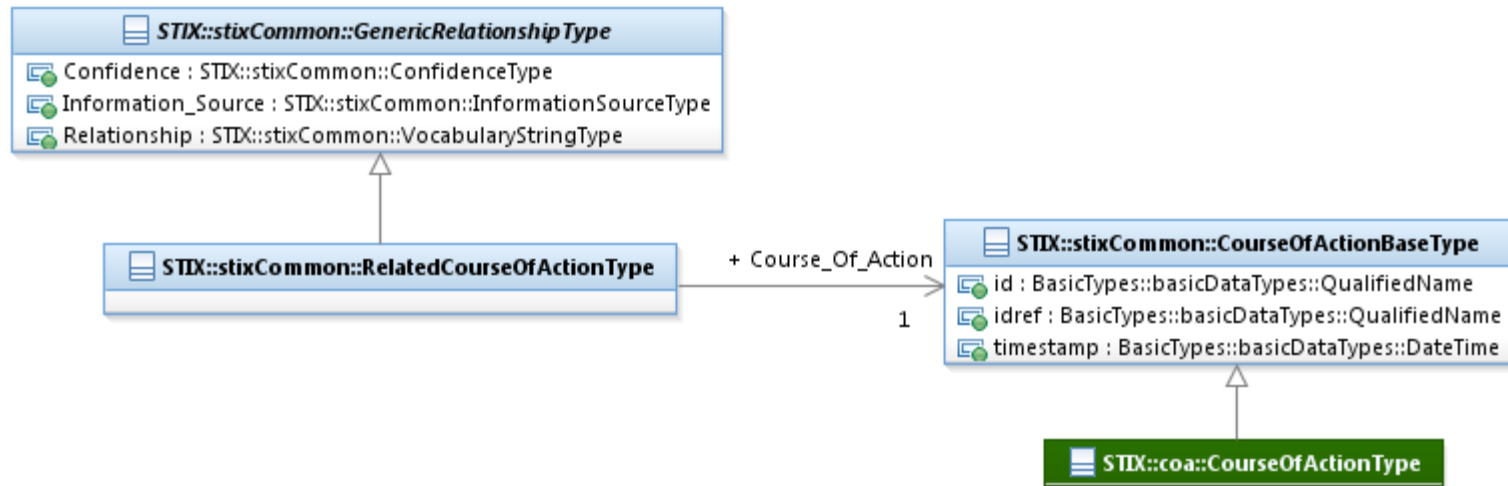


Figure 3-5. UML diagram of the `RelatedCourseOfActionType` class

The property table given in Table 3-13 corresponds to the UML diagram shown in Figure 3-5.

Table 3-13. Properties of the `RelatedCourseOfActionType` class

Name	Type	Multiplicity	Description
Course_Of_Action	<code>CourseOfActionBaseType</code>	1	The <code>Course_Of_Action</code> property characterizes a Course of Action that could be taken in regard to one or more cyber threats. The <code>CourseOfActionBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement a Course of Action is the <code>coa:CourseOfActionType</code> class defined in [STIX _{COA}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the

			idref property, a reference to a Course of Action defined elsewhere can be specified via the direct use of the <code>CourseOfActionBaseType</code> class.
--	--	--	---

3.2.5 RelatedExploitTargetType Class

The `RelatedExploitTargetType` class characterizes a relationship to an Exploit Target. It extends the `GenericRelationshipType` superclass by specifying a related Exploit Target.

The UML diagram corresponding to the `RelatedExploitTargetType` class is shown in Figure 3-6.

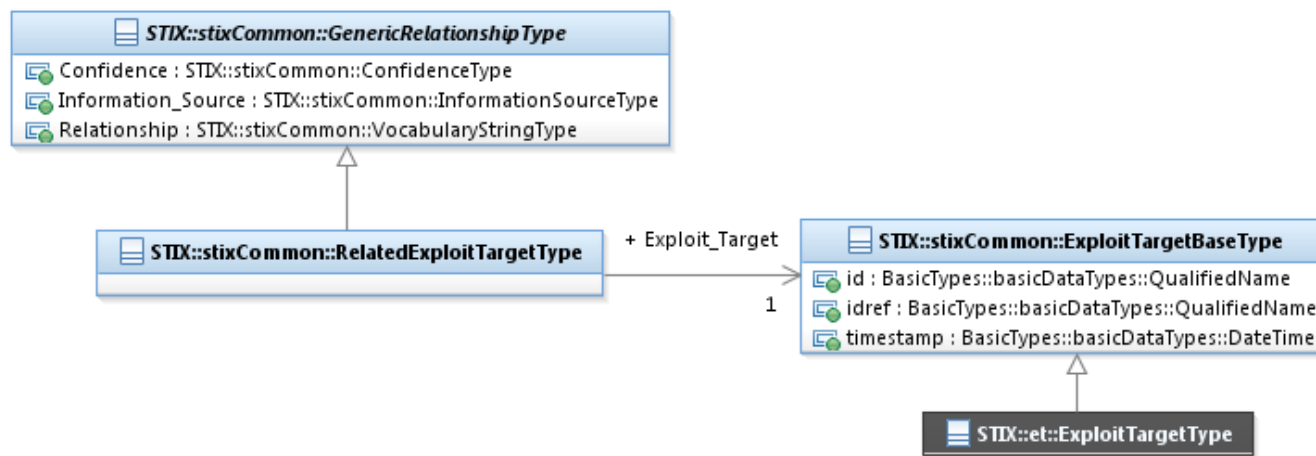


Figure 3-6. UML diagram of the `RelatedExploitTargetType` class

The property table given in Table 3-14 corresponds to the UML diagram shown in Figure 3-6.

Table 3-14. Properties of the `RelatedExploitTargetType` class

Name	Type	Multiplicity	Description
Exploit_Target	<code>ExploitTargetBaseType</code>	1	The <code>Exploit_Target</code> property characterizes an Exploit Target. The <code>ExploitTargetBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement an Exploit Target is the <code>et:ExploitTargetType</code> class defined in [STIX _{ET}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the <code>idref</code> property, a reference to an Exploit Target defined elsewhere can be specified via the direct use of the <code>ExploitTargetBaseType</code> class.

3.2.6 RelatedIdentityType Class

The `RelatedIdentityType` class characterizes a relationship to an identity. It extends the `GenericRelationshipType` superclass by specifying a related Identity.

The UML diagram corresponding to the `RelatedIdentityType` class is shown in Figure 3-7.

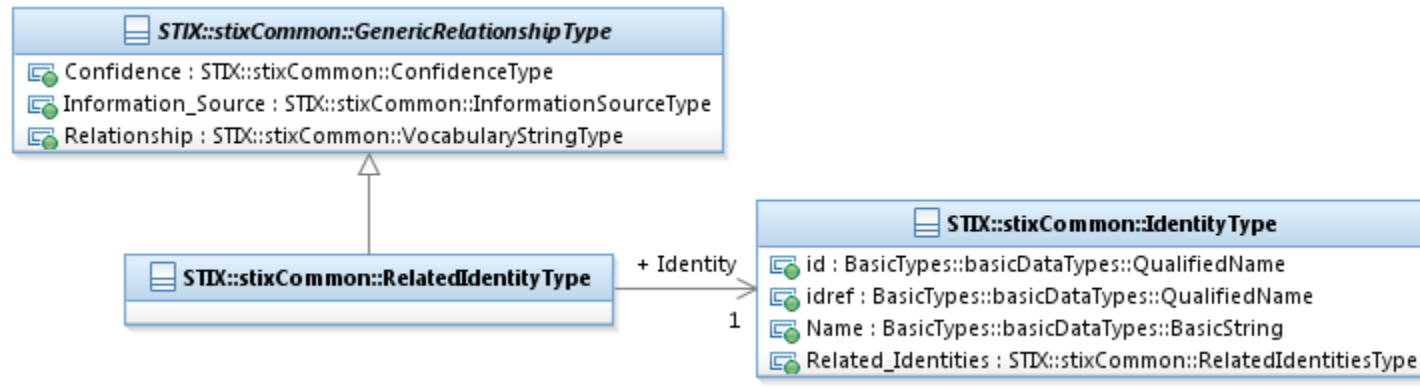


Figure 3-7. UML diagram of the `RelatedIdentityType` class

The property table given in Table 3-15 corresponds to the UML diagram shown in Figure 3-7.

Table 3-15. Properties of the `RelatedIdentityType` class

Name	Type	Multiplicity	Description
Identity	<code>IdentityType</code>	1	The <code>Identity</code> property characterizes the related identity. For situations calling for more than a simple name, the underlying class may be extended using a more complete structure such as the <code>CIQIdentity3.0InstanceType</code> subclass as defined in the “STIX Default Extensions Specification” document [STIX _{EXT}]. Through the use of the <code>idref</code> property, a reference to an <code>Identity</code> defined elsewhere can be specified via the direct use of the <code>IdentityType</code> class.

3.2.7 RelatedIncidentType Class

The `RelatedIncidentType` class characterizes a relationship to an Incident. It extends the `GenericRelationshipType` superclass by specifying a related Incident.

The UML diagram corresponding to the `RelatedIncidentType` class is shown in Figure 3-8.

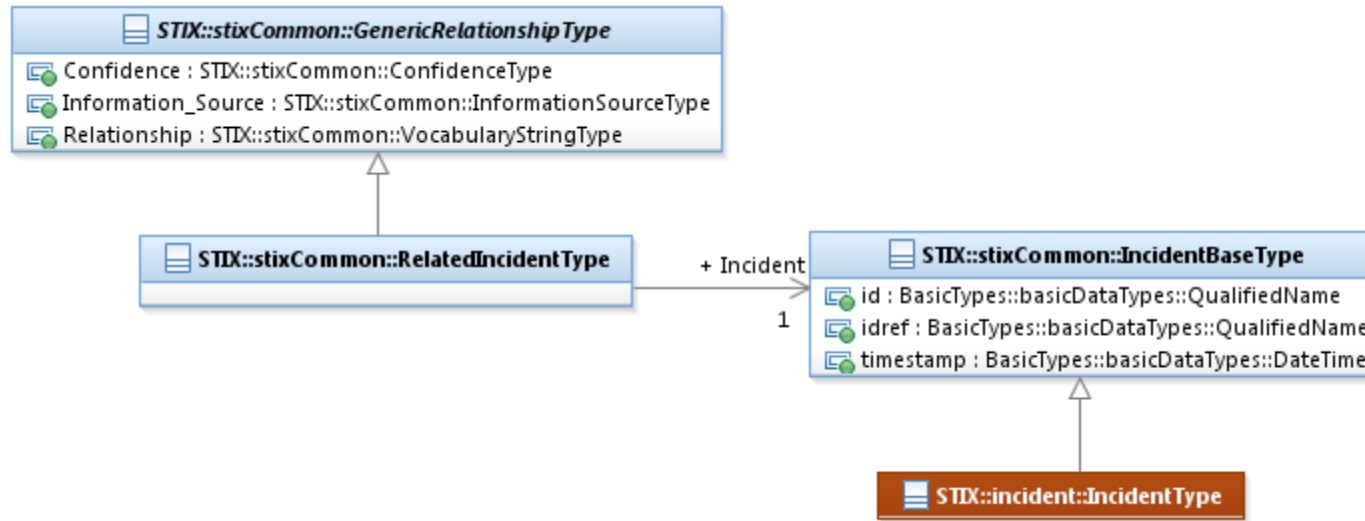


Figure 3-8. UML diagram of the `RelatedIncidentType` class

The property table given in Table 3-16 corresponds to the UML diagram shown in Figure 3-8.

Table 3-16. Properties of the `RelatedIncidentType` class

Name	Type	Multiplicity	Description
Incident	<code>IncidentBaseType</code>	1	The <code>Incident</code> property characterizes a cyber threat Incident. The <code>IncidentBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement an Incident is the <code>incident:IncidentType</code> class defined in [STIX _{INC}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the

			idref property, a reference to an Incident defined elsewhere can be specified via the direct use of the <code>IncidentBaseType</code> class.
--	--	--	--

3.2.8 RelatedIndicatorType Class

The `RelatedIndicatorType` class characterizes a relationship to an Indicator. It extends the `GenericRelationshipType` superclass by specifying a related Indicator.

The UML diagram corresponding to the `RelatedIndicatorType` class is shown in Figure 3-9.

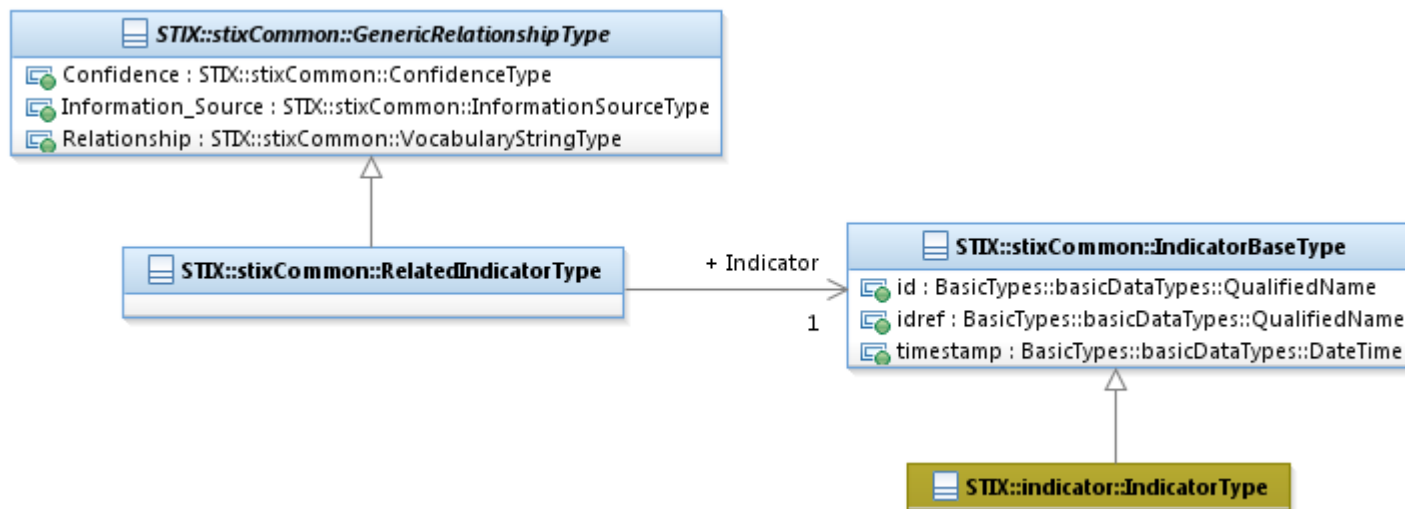


Figure 3-9. UML diagram of the `RelatedIndicatorType` class

The property table given in Table 3-17 corresponds to the UML diagram shown in Figure 3-9.

Table 3-17. Properties of the `RelatedIndicatorType` class

Name	Type	Multiplicity	Description
Indicator	<code>IndicatorBaseType</code>	1	The <code>Indicator</code> property characterizes a cyber threat Indicator. The <code>IndicatorBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement an Indicator is the <code>indicator:IndicatorType</code> class defined in [STIX _{IND}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the <code>idref</code> property, a reference to an Indicator defined elsewhere can be specified via the direct use of the <code>IndicatorBaseType</code> class.

3.2.9 RelatedObservableType Class

The `RelatedObservableType` class characterizes a relationship to a CybOX Observable. It extends the `GenericRelationshipType` superclass by specifying a related Observable.

The UML diagram corresponding to the `RelatedObservableType` class is shown in Figure 3-10.

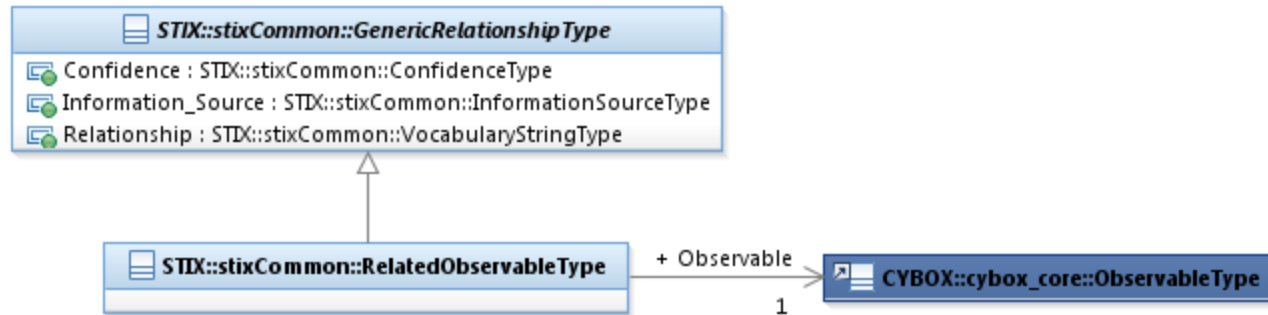


Figure 3-10. UML diagram of the `RelatedObservableType` class

The property table given in Table 3-18 corresponds to the UML diagram shown in Figure 3-10.

Table 3-18. Properties of the `RelatedObservableType` class

Name	Type	Multiplicity	Description
Observable	<code>cybox_core:ObservableType</code>	1	The <code>Observable</code> property characterizes the related cyber observable.

3.2.10 RelatedPackageRefType Class

The `RelatedPackageRefType` class characterizes a relationship to a STIX Package. It extends the `GenericRelationshipType` superclass by specifying the Package.

Because it would not make sense to define a totally new STIX package in the context of any single STIX component, all relationships between a STIX Package and a component are reference type relationships using the `RelatedPackageRefType` class (i.e., a `RelatedPackageType` class is not defined).

The UML diagram associated with the `RelatedPackageRefType` class is shown in Figure 3-11.

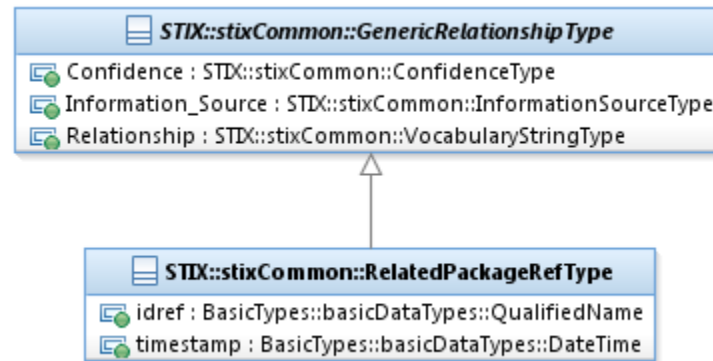


Figure 3-11. UML diagram of the RelatedPackageRefType class

The property table given in Table 3-19 corresponds to the UML diagram shown in Figure 3-11.

Table 3-19. Properties of the RelatedPackageRefType class

Name	Type	Multiplicity	Description
idref	basicDataTypes:QualifiedName	0..1	The <code>idref</code> property specifies a globally unique identifier of a STIX Package specified elsewhere.
timestamp	basicDataTypes:DateTime	0..1	The <code>timestamp</code> property, used in combination with the <code>idref</code> property, specifies a specific version of a Package defined elsewhere. To avoid ambiguity, all timestamps SHOULD include a specification of the time zone.

3.2.11 RelatedReportType Class

The RelatedReportType class characterizes a relationship to a Report. It extends the GenericRelationshipType superclass by specifying a related Report.

The UML diagram corresponding to the RelatedReportType class is shown in Figure 3-12.

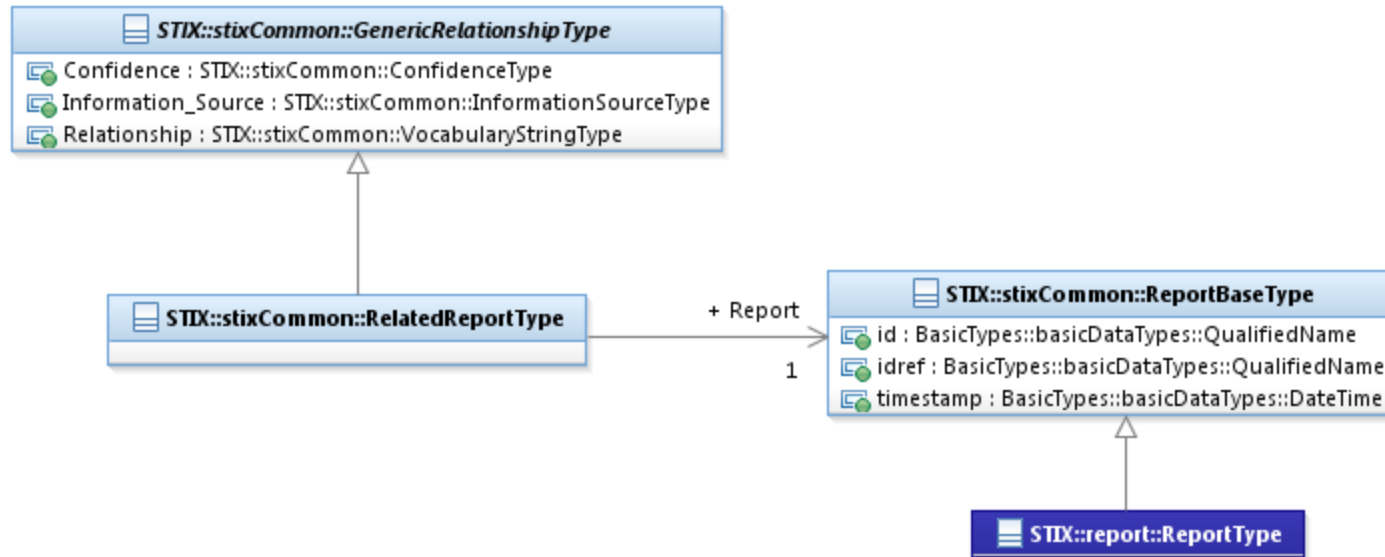


Figure 3-12. UML diagram of the `RelatedReportType` class

The property table given in Table 3-20 corresponds to the UML diagram shown in Figure 3-12.

Table 3-20. Properties of the `RelatedThreatActorType` class

Name	Type	Multiplicity	Description
Report	<code>ReportBaseType</code>	1	The <code>Report</code> property characterizes a STIX Report. The <code>ReportBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement a Report is the <code>report:ReportType</code> class defined in [STIX _{REP}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the <code>idref</code> property, a reference to a Report defined elsewhere can be specified via the direct use of the

			ReportBaseType class.
--	--	--	-----------------------

3.2.12 RelatedThreatActorType Class

The `RelatedThreatActorType` class characterizes a relationship to a Threat Actor. It extends the `GenericRelationshipType` superclass by specifying a related Threat Actor.

The UML diagram corresponding to the `RelatedThreatActorType` class is shown in Figure 3-13.

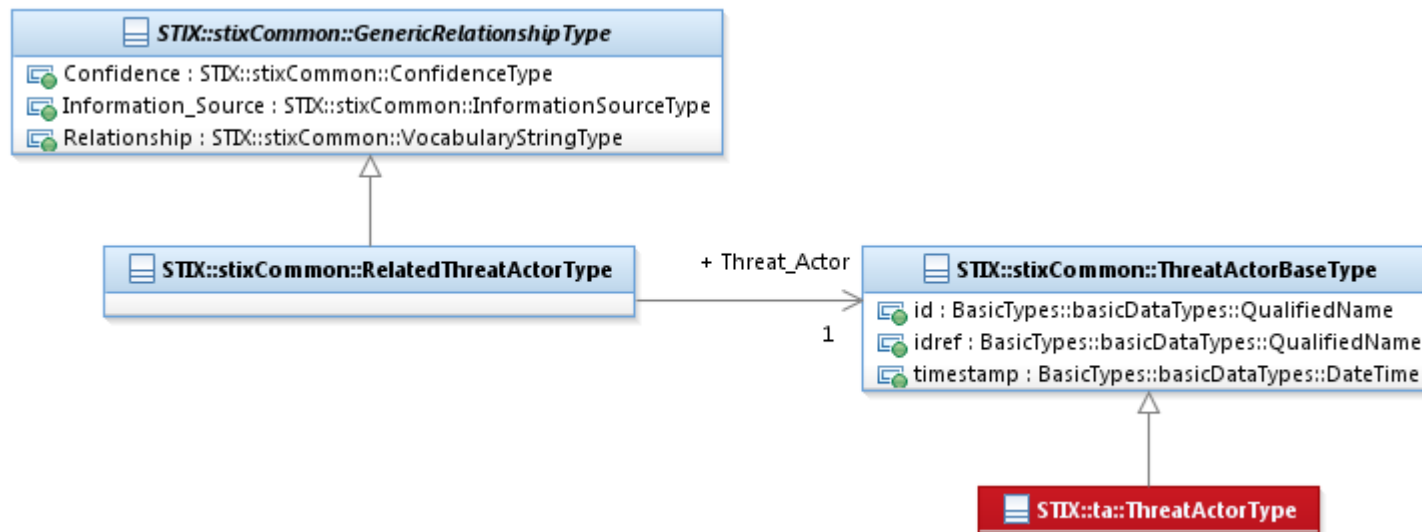


Figure 3-13. UML diagram of the `RelatedThreatActorType` class

The property table given in Table 3-21 corresponds to the UML diagram shown in Figure 3-13.

Table 3-21. Properties of the `RelatedThreatActorType` class

Name	Type	Multiplicity	Description
Threat_Actor	<code>ThreatActorBaseType</code>	1	The <code>ThreatActor</code> property characterizes a cyber Threat Actor. The <code>ThreatActorBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement an <code>ThreatActor</code> is the <code>ta:ThreatActorType</code> class defined in [STIX _{TA}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the <code>idref</code> property, a reference to a Threat Actor defined elsewhere can be specified via the direct use of the <code>ThreatActorBaseType</code> class.

3.2.13 RelatedTTPType Class

The `RelatedTTPType` class characterizes a relationship to a TTP. It extends the `GenericRelationshipType` superclass by specifying a related TTP.

The UML diagram corresponding to the `RelatedTTPType` class is shown in Figure 3-14.

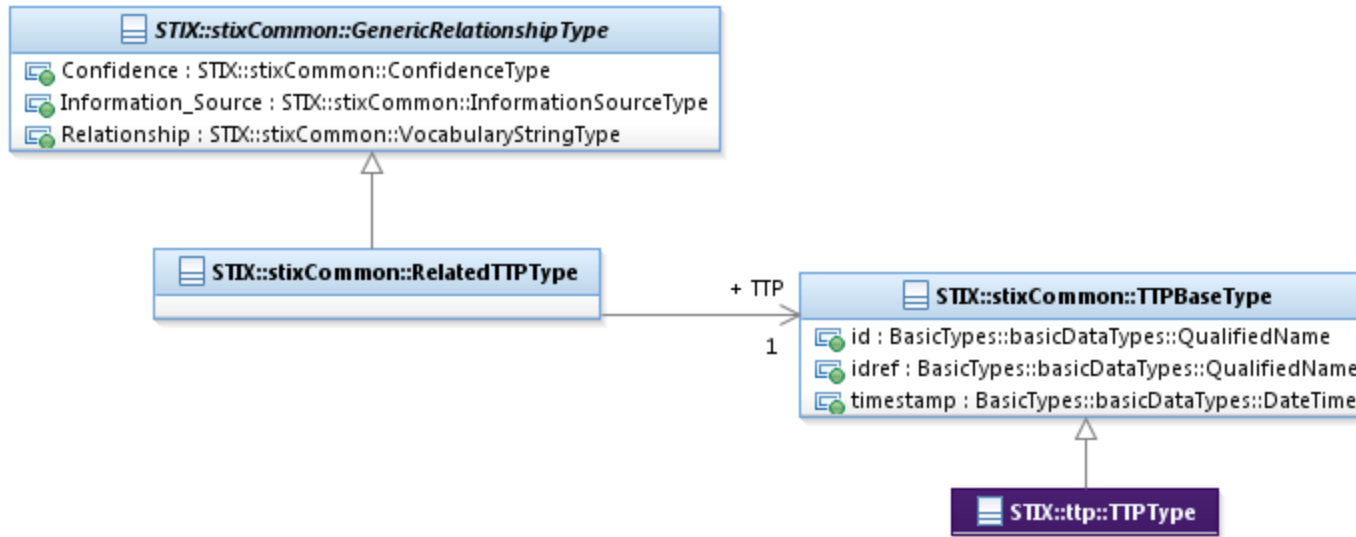


Figure 3-14. UML diagram of the RelatedTTPType class

The property table given in Table 3-22 corresponds to the UML diagram shown in Figure 3-14.

Table 3-22. Properties of the RelatedTTPType class

Name	Type	Multiplicity	Description
TTP	TTPBaseType	1	The TTP property characterizes a cyber threat adversary Tactic, Technique or Procedure (TTP). The TTPBaseType class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement a TTP is the ttp:TTPType class defined in [STIX _{TTP}]. Base classes are used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the idref property, a reference to a TTP defined elsewhere can be specified via the direct use of the TTPBaseType class.

3.3 Content Aggregation Classes

A content aggregation class captures a collection of one (or zero, in some cases) or more STIX objects. Some content aggregation classes are very straightforward and simply capture a set of objects. However, others such as the `GenericRelationshipListType` abstract class are intended to be extended (see Section 3.3.1).

3.3.1 `GenericRelationshipListType`

The `GenericRelationshipListType` class specifies how the relationships between a subject STIX construct and a set of one or more other STIX constructs should be interpreted. It is an abstract class, and it **MUST** be extended via a subclass to characterize the actual set of related constructs.

Classes that extend the `GenericRelationshipListType` class are used to *explicitly* represent the 1-to-many relationship between constructs. In this way, the model enables the ability to express a property of the set itself. Currently, the only property defined is the *scope* of the relationship – whether the elements of the set are related individually or as a group.

Examples of STIX classes that extend the `GenericRelationshipListType` class include the `AttributeType` class defined in the Campaign data model, the `RelatedIndicatorsType` class in the Incident data model, and the `ExploitTargetsType` class defined in the TTP data model (to name just a few). An explicit example is given in Figure 3-15, which illustrates how the `GenericRelationshipListType` class can be extended by the `RelatedIndicatorsType` class to associate a set of Indicators to an Incident.

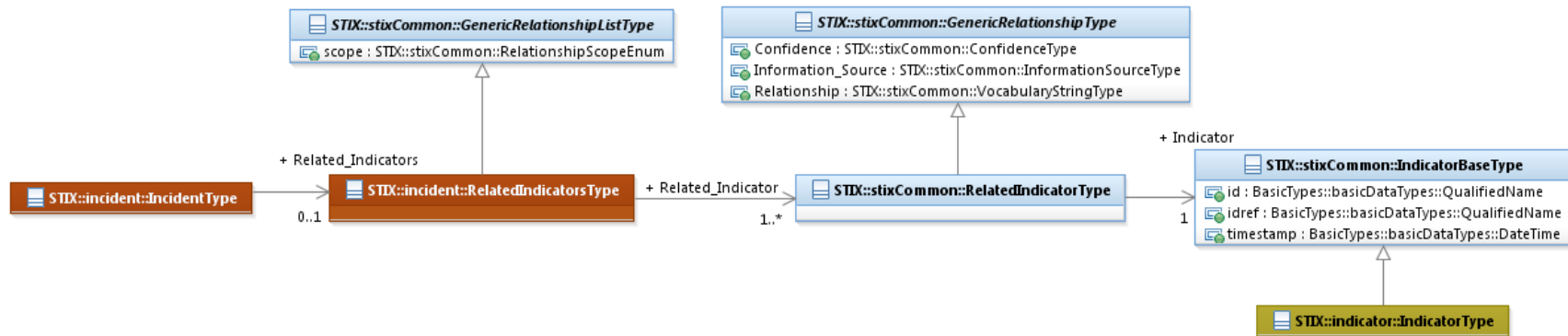


Figure 3-15. Example extension of the `GenericRelationshipListType` class

The property table given in Table 3-23 corresponds to the UML diagram shown in Figure 3-15.

Table 3-23. Properties of the `GenericRelationshipListType` class

Name	Type	Multiplicity	Description
scope	<code>RelationshipScopeEnum</code>	0..1	The <code>scope</code> property specifies how the set of relationships should be interpreted. Potential values are specified by the <code>ScopeEnum</code> enumeration. If ' <i>inclusive</i> ' is specified, then a single conceptual relationship is being defined between the subject construct and the combined collection of related constructs. If ' <i>exclusive</i> ' is specified (the default), then multiple relationships are being defined between the subject construct and each individual related construct.

3.3.2 ConfidenceAssertionChainType Class

The `ConfidenceAssertionChainType` class specifies a set of one or more related confidence levels in an assertion.

The property table of the `ConfidenceAssertionChainType` class is given in Table 3-24.

Table 3-24. Properties of the ConfidenceAssertionChainType class

Name	Type	Multiplicity	Description
Confidence_Assertion	ConfidenceType	1..*	The Confidence_Assertion property characterizes confidence in an assertion.

3.3.3 ContributingSourcesType Class

The ContributingSourcesType class specifies a set of one or more information sources contributing to the data entry.

The UML diagram corresponding to the ContributingSourcesType class is shown in Figure 3-16.

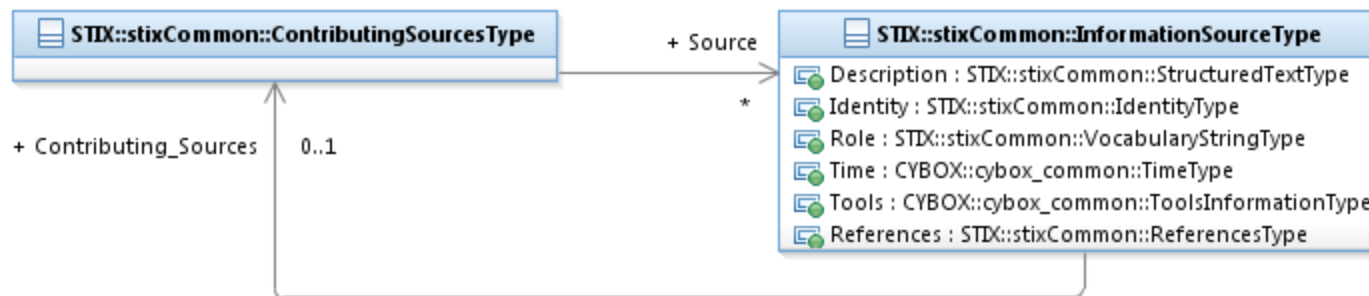


Figure 3-16. UML diagram of the ContributingSourcesType class

As illustrated in Figure 3-16, the ContributingSourcesType class exhibits a recursive, tree-like relationship between contributing sources (it is not simply a flat relationship): a contributing source instance captures its own contributing sources, along with other content such as a description and the role of the information source. Also, the Role property of the InformationSourceType class has increased relevance when characterizing a contributing source by capturing the details of how the source contributed to its parent source.

The property table given in Table 3-25 corresponds to the UML diagram shown in Figure 3-16.

Table 3-25. Properties of the `ContributingSourcesType` class

Name	Type	Multiplicity	Description
Source	<code>InformationSourceType</code>	0..*	The <code>Source</code> property characterizes the organization or tool that is the contributing source. Examples of details captured include identifying characteristics, time-related attributes, and a list of the tools used to collect the information.

3.3.4 ExploitTargetsType Class

The `ExploitTargetsType` class specifies a set of zero or more Exploit Targets⁶.

The property table of the `ExploitTargetsType` class is given in Table 3-26.

Table 3-26. Properties of the `ExploitTargetsType` class

Name	Type	Multiplicity	Description
Exploit_Target	<code>ExploitTargetBaseType</code>	0..*	The <code>Exploit_Target</code> property characterizes an Exploit Target to be considered with respect to one or more cyber threats. The <code>ExploitTargetBaseType</code> class is a minimal base class that is intended to be extended. The default and strongly RECOMMENDED class to fully implement an Exploit Target is the <code>et:ExploitTargetType</code> class defined in [STIX _{ET}]. Like the base classes defined in STIX Core data model, this class is used to minimize interdependence between STIX components, not to enable or encourage conflicting syntactic variation. Through the use of the <code>idref</code> property, a reference to an Exploit Target defined elsewhere can be specified

⁶ This class will eventually be moved to the STIX Core data model so that its location is consistent with similar classes (e.g., `IncidentsType`, `CoursesOfActionType`). The move will require a major version change because while instance content will not change, STIX bindings and APIs will need to import the class from another namespace and therefore may break.

			via the direct use of the <code>ExploitTargetBaseType</code> class.
--	--	--	---

3.3.5 NameType Class

The `NameType` class specifies a set of one or more names. Note that a similar class is defined in the Campaign data model (`campaign:NameType`), which will likely be removed in the next major version of STIX; Campaign names will be then defined exclusively via this STIX Common `NameType` class. For details on the use of the `NameType` class, see Section 3.2.3.1.

The property table of the `NameType` class is given in Table 3-27.

Table 3-27. Properties of the `NameType` class

Name	Type	Multiplicity	Description
Name	<code>VocabularyStringType</code>	1..*	The <code>Name</code> property specifies a name used to identify a construct, such as an alias name. The content creator may choose any arbitrary value or may constrain the set of possible values by referencing an externally-defined vocabulary or leveraging a formally defined vocabulary extending from the <code>ControlledVocabularyStringType</code> class. No default vocabulary is defined in STIX v1.2.

3.3.6 ProfilesType Class

The `ProfilesType` class specifies a list of one or more STIX Profiles (a STIX Profiles document will be available in the future).

The property table of the `ProfilesType` class is given in Table 3-28.

Table 3-28. Properties of the `ProfilesType` class

Name	Type	Multiplicity	Description
Profile	<code>basicDataTypes:URI</code>	1..*	The <code>Profile</code> property specifies a reference to one STIX profile using a Uniform Resource Identifier (URI).

3.3.7 ReferencesType Class

The `ReferencesType` class specifies a set of one or more references.

The property table of the `ReferencesType` class is given in Table 3-29.

Table 3-29. Properties of the `ReferencesType` class

Name	Type	Multiplicity	Description
Reference	<code>basicDataTypes:URI</code>	1..*	The <code>Reference</code> property specifies a reference associated with the data entry using a Uniform Resource Identifier (URI).

3.3.8 RelatedIdentitiesType Class

The `RelatedIdentitiesType` class specifies a set of one or more identities.

The property table of the `RelatedIdentitiesType` class is given Table 3-30.

Table 3-30. Properties of the `RelatedIdentitiesType` class

Name	Type	Multiplicity	Description
Related_Identity	<code>RelatedIdentityType</code>	1..*	The <code>Related_Identity</code> property specifies a related identity associated with the data entry using a Uniform Resource Identifier (URI).

3.3.9 RelatedPackageRefsType Class

The `RelatedPackageRefsType` class specifies a set of zero or more references to a related STIX Package.

The property table of the `RelatedPackageRefsType` class is given in Table 3-31.

Table 3-31. Properties of the `RelatedPackageRefsType` class

Name	Type	Multiplicity	Description
Package_Reference	<code>RelatedPackageRefType</code>	0..*	The <code>Package_Reference</code> property characterizes a relationship to a related STIX Package defined elsewhere.

3.4 Kill Chains

A cyber kill chain is a phase-based model to describe the stages of an attack. Kill chain-related classes are defined below.

3.4.1 KillChainsType Class

The `KillChainsType` class specifies a set of one or more specific kill chain definitions.

The property table of the `KillChainsType` class is given in Table 3-32.

Table 3-32. Properties of the `KillChainsType` class

Name	Type	Multiplicity	Description
Kill_Chain	<code>KillChainType</code>	1..*	A cyber kill chain is a phase-based model to describe the stages of an attack. The <code>Kill_Chain</code> property characterizes a single kill chain that may be referenced elsewhere; for example, from within a TTP or an Indicator component.

3.4.1.1 KillChainType Class

A cyber kill chain is a phase-based model to describe the stages of an attack. The `KillChainType` class characterizes a kill chain definition that may be referenced elsewhere; for example, from within a TTP or an Indicator component. Information captured includes a set of one or more kill chain phases that compose the kill chain.

The property table of the `KillChainType` class is given in Table 3-33.

Table 3-33. Properties of the `KillChainType` class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the kill chain definition.
name	<code>basicDataTypes: NoEmbeddedQuoteString</code>	0..1	The <code>name</code> property captures a simple name for the kill chain definition.
definer	<code>basicDataTypes: NoEmbeddedQuoteString</code>	0..1	The <code>definer</code> property specifies the organization or individual responsible for the kill chain definition.
reference	<code>basicDataTypes:URI</code>	0..1	The <code>reference</code> property specifies a reference associated with the kill chain using a Uniform Resource Identifier (URI).
number_of_phases	<code>basicDataTypes:Integer</code>	0..1	The <code>number_of_phases</code> property specifies the number of phases in the kill chain.
Kill_Chain_Phase	<code>KillChainPhaseType</code>	1..*	The <code>Kill_Chain_Phase</code> property characterizes an individual phase within the kill chain.

3.5.1.1.1 KillChainPhaseType Class

A cyber kill chain is a phase-based model to describe the stages of an attack, and a cyber kill chain phase is an individual phase within a kill chain definition. The `Kill_Chain_Phase` property characterizes an individual phase within a kill chain.

The property table of the `KillChainPhaseType` class is given in Table 3-34.

Table 3-34. Properties of the `KillChainPhaseType` class

Name	Type	Multiplicity	Description
phase_id	<code>basicDataTypes:</code> <code>QualifiedName</code>	0..1	The <code>phase_id</code> property specifies a globally unique identifier for the kill chain phase. When used within a kill chain definition (defined by the <code>KillChainType</code> class), it identifies the kill chain phase being defined. When used within a kill chain reference (defined by the <code>KillChainPhaseReferenceType</code> class), it must reference an existing kill chain <code>phase_id</code> property (note that this use is similar to the use of the <code>idref</code> property elsewhere in STIX.)
name	<code>basicDataTypes:</code> <code>NoEmbeddedQuoteString</code>	0..1	The <code>name</code> property captures a descriptive name of the kill chain phase. If the <code>KillChainPhaseType</code> class is extended by the <code>KillChainPhaseReferenceType</code> class, this attribute SHOULD be omitted, or if it is present, it MUST match the kill chain phase name used in the referenced kill chain.
ordinality	<code>basicDataTypes:</code> <code>Integer</code>	0..1	The <code>ordinality</code> property specifies the ordinality (e.g., '1', '2', or '3') of this phase within the kill chain definition. It should be omitted when the associated kill chain is being referenced (defined by the <code>KillChainPhaseReferenceType</code> class), but if the property is present, it MUST match the ordinality of the corresponding phase in the kill chain that is referenced.

3.4.2 KillChainPhasesReferenceType Class

A cyber kill chain is a phase-based model to describe the stages of an attack, and a cyber kill chain phase is an individual phase within a kill chain definition. The `KillChainPhasesReferenceType` class specifies a set of one or more kill chain phases.

The property table of the `KillChainPhasesReferenceType` class is given in Table 3-35.

Table 3-35. Properties of the `KillChainPhaseReferenceType` class

Name	Type	Multiplicity	Description
Kill_Chain_Phase	<code>KillChainPhaseReferenceType</code>	1..*	The <code>Kill_Chain_Phase</code> property specifies a single kill chain phase associated with this item.

3.4.2.1 KillChainPhaseReferenceType Class

The `KillChainPhaseReferenceType` class specifies a phase within a kill chain by extending the `KillChainPhaseType` superclass. A kill chain reference in an Indicator component indicates that the indicator detects malicious behavior at that phase of the kill chain. A kill chain reference in a TTP component indicates that the TTP is used (malware, infrastructure, etc.) at that phase of the kill chain.

The property table of the `KillChainPhaseReferenceType` class is given in Table 3-36.

Table 3-36. Properties of the `KillChainPhaseReferenceType` class

Name	Type	Multiplicity	Description
kill_chain_id	<code>basicDataTypes:</code> <code>QualifiedName</code>	0..1	The <code>kill_chain_id</code> property specifies the globally unique identifier for the referenced kill chain instance.
kill_chain_name	<code>basicDataTypes:</code> <code>NoEmbeddedQuotesString</code>	0..1	The <code>kill_chain_name</code> property captures a descriptive name of the kill chain. If a kill chain is referenced by the <code>kill_chain_id</code> property, this attribute SHOULD be omitted, or if it is present, it MUST match the <code>name</code> property of the corresponding kill chain phase that is referenced.

3.5 General Shared Classes

Unlike the classes defined in the previous sections that shared similar roles, the following classes serve a variety of purposes and are shared by the collection of STIX data models.

3.5.1 ActivityType Class

The `ActivityType` class characterizes basic information about an activity a defender might use. It is an abstract class, so it **MUST** be extended via a subclass to express additional activity information. STIX does not define a default subclass. Note that an activity defined by the `ActivityType` class is fairly simple and includes only date/time information and a description. By contrast, a Course of Action construct contains detailed information such as the stage in the cyber threat management lifecycle to which the course of action is relevant, the impact and cost of applying the course of action, and efficacy of the course of action.

The property table for the `ActivityType` class is given in Table 3-37.

Table 3-37. Properties of the `ActivityType` class

Name	Type	Multiplicity	Description
Date_Time	<code>DateTimeWithPrecisionType</code>	1	The <code>Date_Time</code> property specifies the date and time at which the activity occurred. To avoid ambiguity, all timestamps SHOULD include a specification of the time zone. In addition to specifying a date and time, the <code>Date_Time</code> property may also capture a <code>precision</code> property to specify the granularity with which the time should be considered, as specified by the <code>DateTimePrecisionEnum</code> enumeration (e.g., <code>'hour'</code> , <code>'minute'</code>). If omitted, the default precision is <code>'second'</code> . Digits in a timestamp that are beyond the specified precision SHOULD be zeroed out.
Description	<code>StructuredTextType</code>	0..*	The <code>Description</code> property captures a textual description of the activity. Any length is permitted. Optional formatting is supported via the <code>structuring_format</code> property of the <code>StructuredTextType</code> class.

3.5.2 AddressAbstractType Class

The `AddressAbstractType` class characterizes geographic address information. It is an abstract class, so it **MUST** be extended via a subclass to capture an address. STIX v1.2 defines the `CIQAddress3.0InstanceType` subclass as a default extension to leverage the OASIS Customer Information Quality (CIQ) data model, which is a set of XML specifications for representing characteristic information about individuals and organizations. Details are provided in [STIX_{EXT}].

The `AddressAbstractType` class has no properties of its own (so there is no associated property table). Its UML diagram is illustrated in Figure 3-17.

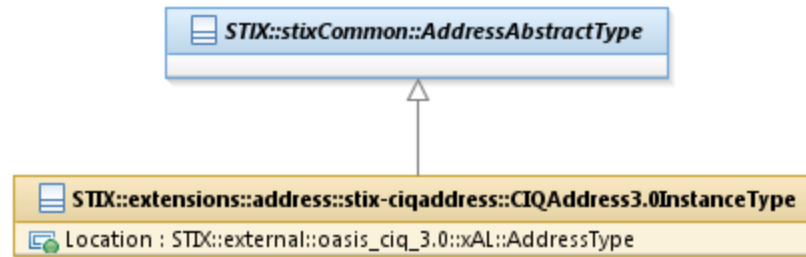


Figure 3-17. UML diagram of the `AddressAbstractType` class

3.5.3 ConfidenceType Class

The `ConfidenceType` class characterizes confidence in an assertion.

The property table of the `ConfidenceType` class is given in Table 3-38.

Table 3-38. Properties of the `ConfidenceType` class

Name	Type	Multiplicity	Description
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the date and time of the confidence assertion. To avoid ambiguity, all timestamps SHOULD include a specification of the time zone.
timestamp_precision	<code>DateTimePrecisionEnum</code>	0..1	The <code>timestamp_precision</code> property specifies the granularity with which the <code>timestamp</code> property should be considered, as specified by the <code>DateTimePrecisionEnum</code> enumeration (e.g., 'hour,' 'minute'). If omitted, the default precision is 'second.'

			Digits in a timestamp that are beyond the specified precision should be zeroed out.
Value	VocabularyStringType	0..1	The <code>Value</code> property specifies the level of confidence held in this direct assertion. Examples of potential levels include <i>high</i> , <i>medium</i> , and <i>low</i> (these specific values are only provided to help explain the property: they are neither recommended values nor necessarily part of any existing vocabulary). The content creator may choose any arbitrary value or may constrain the set of possible values by referencing an externally-defined vocabulary or leveraging a formally defined vocabulary extending from the <code>ControlledVocabularyStringType</code> class. The STIX default vocabulary class for use in the property is ' <i>HighMediumLowVocab-1.0</i> .'
Description	StructuredTextType	0..*	The <code>Description</code> property captures a textual description of the confidence assertion. Any length is permitted. Optional formatting is supported via the <code>structuring_format</code> property of the <code>StructuredTextType</code> class.
Source	InformationSourceType	0..1	The <code>Source</code> property characterizes the organization or tool that is the source of the confidence assertion. Examples of details captured include identifying characteristics, time-related attributes, and a list of the tools used to collect the information.
Confidence_Assertion_Chain	ConfidenceAssertionChainType	0..1	The <code>Confidence_Assertion_Chain</code> property specifies a set of one or more related confidence assertions.

3.5.4 IdentityType Class

The `IdentityType` class characterizes identity information for both individuals and organizations. The `IdentityType` class is intended to be extended via a subclass to capture the structured descriptions of identity information for both individuals and

organizations. STIX v1.2 defines a default extension to the `IdentityType` class to leverage the OASIS Customer Information Quality (CIQ) data model, which is a set of XML specifications for representing characteristic information about individuals and organizations (see [STIX_{EXT}]).

The property table of the `IdentityType` class is given in Table 3-39.

Table 3-39. Properties of the `IdentityType` class

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the identity.
idref	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>idref</code> property specifies a globally unique identifier for an identity specified elsewhere. When the <code>idref</code> property is used, the <code>id</code> property MUST NOT also be specified and the other properties of the <code>IdentityType</code> class SHOULD NOT hold any content.
Name	<code>basicDataTypes:BasicString</code>	0..1	The <code>Name</code> property captures a simple name for the identity.
Related_Identities	<code>RelatedIdentitiesType</code>	0..1	The <code>Related_Identities</code> property specifies a set of one or more identities related to this identity.

3.5.5 InformationSourceType Class

The `InformationSourceType` class specifies source information for the given STIX content.

The property table of the `InformationSourceType` class is given in Table 3-40.

Table 3-40. Properties of the `InformationSourceType` class

Name	Type	Multiplicity	Description
Description	<code>StructuredTextType</code>	0..*	The <code>Description</code> property captures a textual description of the information source. Any length is permitted. Optional formatting is supported via the <code>structuring_format</code> property of the <code>StructuredTextType</code> class.
Identity	<code>IdentityType</code>	0..1	The <code>Identity</code> property characterizes the identity of the information source. For situations calling for more than a simple name, the underlying class may be extended using a more complete structure such as the <code>CIQIdentity3.0InstanceType</code> subclass as defined in [STIX _{EXT}].
Role	<code>VocabularyStringType</code>	0..*	The <code>Role</code> property specifies a role played by the information source. Examples of potential roles include <i>initial author</i> , <i>aggregator</i> , and <i>transformer/translator</i> (these specific values are only provided to help explain the property: they are neither recommended values nor necessarily part of any existing vocabulary). The content creator may choose any arbitrary value or may constrain the set of possible values by referencing an externally-defined vocabulary or leveraging a formally defined vocabulary extending from the <code>ControlledVocabularyStringType</code> class. The STIX default vocabulary class for use in the property is ' <i>InformationSourceRoleVocab-1.0</i> '.
Contributing_Sources	<code>ContributingSourcesType</code>	0..1	The <code>Contributing_Sources</code> property specifies a set of zero or more individual sources contributing to the STIX content. Note that this property captures <i>secondary</i> sources of information.
Time	<code>TimeType</code>	0..1	The <code>Time</code> property characterizes the time-related attributes of the STIX content.
Tools	<code>cybox:ToolsInformationType</code>	0..1	The <code>Tools</code> property specifies a set of one or more tools contributing to the STIX content.

References	ReferencesType	0..1	The <code>References</code> property specifies a set of one or more references to information source material related to the STIX content.
-------------------	----------------	------	--

3.5.6 StatementType Class

The `StatementType` class characterizes a statement associated with STIX content.

The UML diagram corresponding to the `StatementType` class is shown in Figure 3-18.

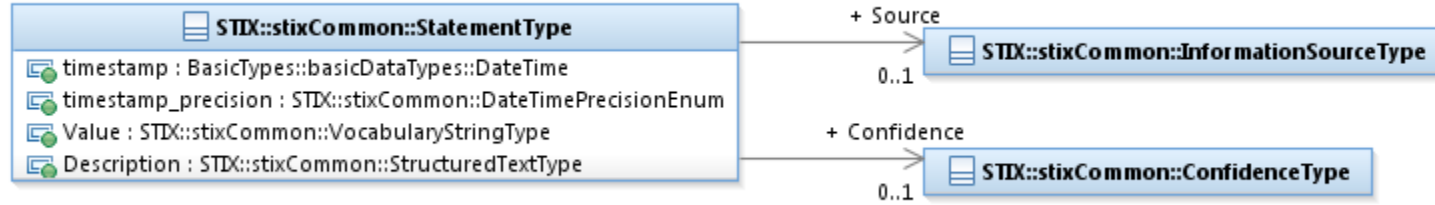


Figure 3-18. UML diagram of the `StatementType` class

The property table given in Table 3-41 corresponds to the UML diagram shown in Figure 3-18.

Table 3-41. Properties of the `StatementType` class

Name	Type	Multiplicity	Description
timestamp	<code>basicDataTypes:DateTime</code>	0..1	The <code>timestamp</code> property specifies the date and time of the statement. To avoid ambiguity, all timestamps SHOULD include a specification of the time zone.
timestamp_precision	<code>DateTimePrecisionEnum</code>	0..1	The <code>timestamp_precision</code> property specifies the granularity with which the <code>timestamp</code> property should be considered, as specified by the <code>DateTimePrecisionEnum</code> enumeration (e.g.,

			'hour,' 'minute'). If omitted, the default precision is 'second.' Digits in a timestamp that are beyond the specified precision SHOULD be zeroed out.
Value	VocabularyStringType	0..1	The Value property specifies the statement's level of importance. Examples of potential levels include <i>high</i> , <i>medium</i> , and <i>low</i> (these specific values are only provided to help explain the property: they are neither recommended values nor necessarily part of any existing vocabulary). The content creator may choose any arbitrary value or may constrain the set of possible values by referencing an externally-defined vocabulary or leveraging a formally defined vocabulary extending from the <code>ControlledVocabularyStringType</code> class. The STIX default vocabulary class for use in the property is ' <i>HighMediumLowVocab-1.0</i> '; however, when the <code>StatementType</code> class is used, this default vocabulary is often overwritten by a different vocabulary more suitable to the context.
Description	StructuredTextType	0..*	The Description property captures a textual description of the statement. Any length is permitted. Optional formatting is supported via the <code>structuring_format</code> property of the <code>StructuredTextType</code> class.
Source	InformationSourceType	0..1	The Source property characterizes the organization or tool that is the source of the statement. Examples of details captured include identifying characteristics, time-related attributes, and a list of the tools used to collect the information.
Confidence	ConfidenceType	0..1	The Confidence property characterizes the confidence in the statement.

3.5.7 ToolInformationType Class

The `ToolInformationType` class characterizes information about a hardware or software tool by extending the CybOX `ToolInformationType` superclass (note that both classes are named "ToolInformationType" but are in different UML packages).

The UML diagram corresponding to the `ToolInformationType` class is shown in Figure 3-19.

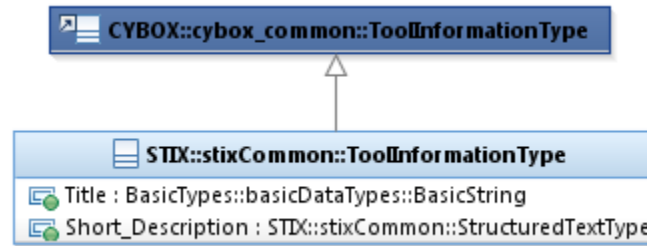


Figure 3-19. UML diagram of the `ToolInformationType` class

The property table given in Table 3-42 corresponds to the UML diagram shown in Figure 3-19.

Table 3-42. Properties of the `ToolInformationType` class

Name	Type	Multiplicity	Description
Title	<code>basicDataTypes:BasicString</code>	0..1	The <code>Title</code> property provides a simple title for the tool and reflects what the producer thinks the tool as a whole should be called. Titles are typically used by humans to reference a particular tool; however, titles are not meant to be used for correlation.
Short_Description	<code>StructuredTextType</code>	0..*	The <code>Short_Description</code> property captures a short textual description of the tool.

3.6 General Data Types

3.6.1 DateTimeWithPrecisionType Data Type

The `DateTimeWithPrecisionType` data type specializes the `basicDataTypes:DateTime` data type by capturing precision information.

The property table of the `DateTimeWithPrecisionType` data type is provided in Table 3-43.

Table 3-43. Properties of the `DateTimeWithPrecisionType` class

Name	Type	Multiplicity	Description
precision	<code>DateTimePrecisionEnum</code>	0..1	The <code>precision</code> property specifies the granularity with which a timestamp should be considered as specified by the <code>DateTimePrecisionEnum</code> enumeration (e.g., <code>'hour'</code> , <code>'minute'</code>). If omitted, the default precision is <code>'second'</code> . Digits in a timestamp that are beyond the specified precision SHOULD be zeroed out.

Some classes, such as the `ConfidenceType` and `StatementType` classes, have both a “timestamp” property (defined by the `basicDataTypes:DateTime` data type) and a “timestamp precision” property (defined by the `DateTimePrecisionEnum` enumeration). This is due to the evolution of the STIX language; a future major release could include the replacement of these two properties with a single property defined by the `DateTimeWithPrecisionType` class.

3.6.2 NativeFormatStringType Data Type

The `NativeFormatStringType` data type specializes the `basicDataTypes:BasicString` data type in order to capture data in the native format of some external language (see [STIX_{EXT}]). The data may be encoded in Base64 per [RFC4648]. Data encoded in Base64 must be denoted as such using the `encoded` property.

The property table of the `NativeFormatStringType` data type is provided in Table 3-44.

Table 3-44. Properties of the `NativeFormatStringType` class

Name	Type	Multiplicity	Description
encoded	<code>basicDataTypes:Boolean</code>	0..1	The <code>encoded</code> property specifies whether the data is Base64 encoded (<code>'true'</code>) or not encoded (<code>'false'</code>). The default value is <code>'false'</code> .

3.6.3 StructuredTextType Data Type

The `StructuredTextType` data type specializes the `basicDataTypes:BasicString` data type by capturing structuring format information. An identifier is captured to allow for differential data marking of distinct construct instances, and an ordinality property indicates the order of the instances if more than one is specified.

The property table of the `StructuredTextType` data type is provided in Table 3-45.

Table 3-45. Properties of the `StructuredTextType` data type

Name	Type	Multiplicity	Description
id	<code>basicDataTypes:QualifiedName</code>	0..1	The <code>id</code> property specifies a globally unique identifier for the construct instance.
ordinality	<code>basicDataTypes:PositiveInteger</code>	0..1	The <code>ordinality</code> property specifies the order (e.g., '1', '2', or '3') of this construct instance (e.g., Description) within a potential set of multiple peer construct instances. If only a single construct instance is present, its ordinality can be assumed to be 1. If multiple construct instances are present, the <code>ordinality</code> property SHOULD be specified with unique values for each instance.
structuring_format	<code>basicDataTypes:BasicString</code>	0..1	The <code>structuring_format</code> property specifies the structuring format used within an instance of the <code>StructuredTextType</code> class. If this property is absent, then markup MUST NOT be used.

3.7 Vocabulary Data Types

There are three vocabulary-related UML data types defined in the Common data model, and together they provide a content creator with four choices for defining content,⁷ listed below in order of formality. Please see [STIX_{voc}] for further information on STIX vocabularies.

- Leverage a default vocabulary using the `ControlledVocabularyStringType` data type. STIX v1.2 defines a collection of default vocabularies and associated enumerations that are based on input from the STIX community (see [STIX_{voc}]); however, not all vocabulary properties have an assigned default vocabulary.
- Formally define a custom vocabulary using the `ControlledVocabularyStringType` data type. To achieve value enforcement, a custom vocabulary must be formally added to the STIX Vocabulary data model. Because this is an extension of the STIX Vocabulary data model, producers and consumers MUST be aware of the addition to the data model for successful sharing of STIX documents.
- Reference an externally-defined, custom vocabulary using the `UnenforcedVocabularyStringType` data type to constrain the set of values. Externally-defined vocabularies are publically defined, but have not been included as formally specified vocabularies within the STIX Vocabulary data model using the `ControlledVocabularyStringType` data type. In this case, it is sufficient to specify the name of the vocabulary and a URL that defines that vocabulary.
- Choose an arbitrary and unconstrained value using the `VocabularyStringType` data type.

While not required by the general STIX language, default vocabularies should be used whenever possible to ensure the greatest level of compatibility between STIX users. If an appropriate default vocabulary is not available a formally defined custom vocabulary can be specified and leveraged. In addition to compatibility advantages, using formally defined vocabularies (whether default vocabularies or otherwise defined) enables enforced use of valid enumeration values; please see [STIX_{voc}] for the associated policy.

If a formally defined vocabulary is not sufficient for a content producer's purposes, the STIX Vocabulary data model allows the two alternatives listed above: externally defined custom vocabularies and arbitrary string values, which dispense with enumerated

⁷ The vocabulary-related data types defined here are different than those defined for vocabularies in the STIX 1.2 XSD implementation.

vocabularies altogether. If a custom vocabulary is not formally added to the Vocabulary data model then no enforcement policy of appropriate values is specified.

The UML diagram shown in Figure 3-20 illustrates the relationships between the three vocabulary data types defined in the STIX Common data model. As illustrated, all controlled vocabularies formally defined within the STIX Vocabulary data model are defined using an enumeration derived from the `ControlledVocabularyStringType` data type.

As shown, the `HighMediumLowVocab-1.0` enumeration (used as a defined controlled vocabulary exemplar) is defined as a specialization of the `ControlledVocabularyStringType` data type, and therefore it is also a specialization of the `VocabularyStringType` data type.

Further details of each vocabulary class are provided in Subsections 3.7.1 through 3.7.3.

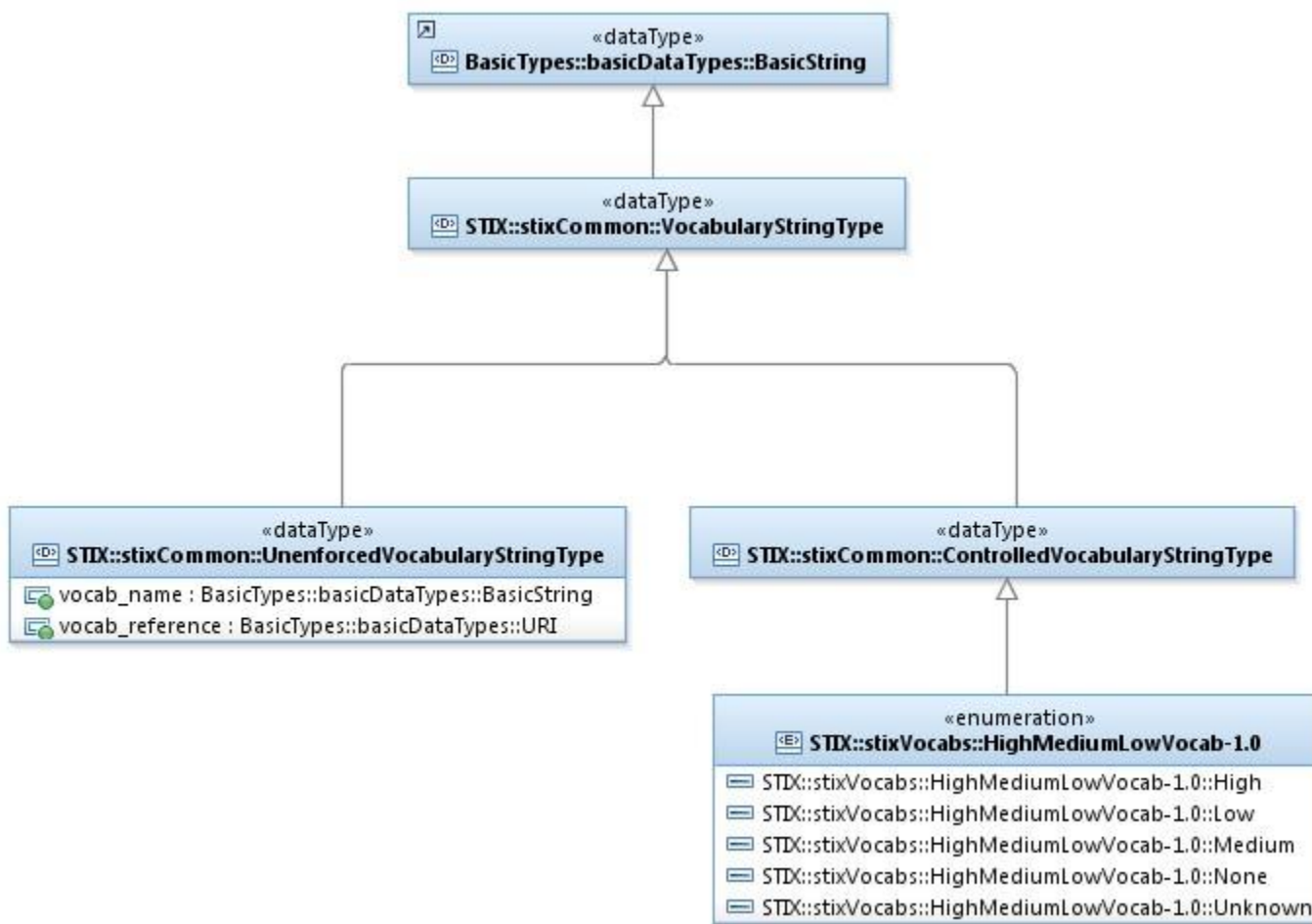


Figure 3-20. UML diagram of the STIX Vocabulary data model

3.7.1 VocabularyStringType Data Type

The `VocabularyStringType` data type is the basic data type of all vocabularies. Therefore, all properties in the collection of STIX data models that makes use of the Vocabulary data model must be defined to use the `VocabularyStringType` data type. Because this data type is a specialization of the `basicDataTypes:BasicString` data type, it can be used to support the arbitrary string option for vocabularies.

3.7.2 UnenforcedVocabularyStringType Data Type

The `UnenforcedVocabularyStringType` data type specifies custom vocabulary values via an enumeration defined outside of the STIX Vocabulary data model. It extends the `VocabularyStringType` data type. Note that the STIX vocabulary data model does not define any enforcement policy for this data type.

The property table of the `UnenforcedVocabularyStringType` data type is given in Table 3-46.

Table 3-46. Properties of the `UnenforcedVocabularyStringType` data type

Name	Type	Multiplicity	Description
vocab_name	<code>basicDataTypes:</code> <code>NoEmbeddedQuoteString</code>	0..1	The <code>vocab_name</code> property specifies the name of the externally defined vocabulary.
vocab_reference	<code>basicDataTypes:URI</code>	0..1	The <code>vocab_reference</code> property specifies the location of the externally defined vocabulary using a Uniform Resource Identifier (URI).

3.7.3 ControlledVocabularyStringType Data Type

The `ControlledVocabularyStringType` data type specifies a formally defined vocabulary. It is an abstract data type⁸ so it MUST be extended via an enumeration from the STIX Vocabulary data model (descriptions of all default vocabularies defined within

⁸ Note that in the XSD implementation, `ControlledVocabularyStringType` is not an abstract concept.

the STIX Vocabulary data model are found in [STIX_{VOC}]⁹). Any custom vocabulary must be defined via an enumeration added to the STIX Vocabulary data model, if appropriate enumeration values are to be enforced.

The `ControlledVocabularyStringType` class has no properties of its own, so there is no associated property table.

3.8 Enumerations

3.8.1 DateTimePrecisionEnum Enumeration

The `DateTimePrecisionEnum` enumeration is an inventory of values for representing time precision. The enumeration literals are given in Table 3-47.

Table 3-47. Literals of the `DateTimePrecisionEnum` enumeration

Enumeration Literals	Description
year	The given date/time is precise to the given year.
month	The given date/time is precise to the given month.
day	The given date/time is precise to the given day.
hour	The given date/time is precise to the given hour.
minute	The given date/time is precise to the given minute.
second	The given date/time is precise to the given second (including fractional seconds).

⁹ Note that all defined vocabulary enumerations have version numbers in their names to facilitate additions to the enumerations that are backward compatible.

3.8.2 RelationshipScopeEnum

The `RelationshipScopeEnum` enumeration is an inventory of types of relationship groupings between a subject and a collection of objects. The enumeration literals are given in Table 3-48.

Table 3-48. Literals of the `RelationshipScopeEnum` enumeration

Enumeration Literals	Description
inclusive	A single relationship is being defined between the subject and the collection of objects indicated by the related items.
exclusive	Multiple relationships are being defined between the subject and each object individually.

References

References made in this document are listed below.

- [CybOX_{COR}] CybOX Core Specification (*not yet available*).
- [RFC2119] RFC 2119 – Key words for use in RFCs to Indicate Requirement Levels
<http://www.ietf.org/rfc/rfc2119.txt>
- [STIX] STIX Web Site
<https://stix.mitre.org>
- [STIX-SPECS] STIX™ Project Github Site
<http://github.com/STIXProject/specifications>
- [STIX_{CAM}] STIX™ 1.2 Campaign Specification (v1.2)
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{COA}] STIX™ 1.2 Course of Action (COA) Specification (v1.2)
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{EXT}] STIX™ 1.2 Default Extensions Specification
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{INC}] STIX™ 1.2 Incident Specification (v1.2)
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{IND}] STIX™ 1.2 Indicator Specification (v2.2)
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{REP}] STIX 1.2 Report Specification (v1.2)
<https://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{TA}] STIX™ 1.2 Threat Actor Specification (v1.2)
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_{TTP}] STIX™ 1.2 TTP Specification (v1.2)
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX_O] STIX Specification Overview Version 1.2
<http://stix.mitre.org/about/documents/XXXX.pdf>