STIX Version 1.2.1 Part 6: Incident

Working Draft 01

31 August 2015

Technical Committee:

[OASIS Cyber Threat Intelligence (CTI) TC](https://www.oasis-open.org/committees/cti/)

Chair:

Richard Struse ([Richard.Struse@HQ.DHS.GOV](mailto:Richard.Struse@HQ.DHS.GOV)), [DHS Office of Cybersecurity and Communications (CS&C)](http://www.dhs.gov/office-cybersecurity-and-communications)

Editors:

Sean Barnum ([sbarnum@mitre.org](mailto:sbarnum@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

Desiree Beck ([dbeck@mitre.org](mailto:dbeck@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

Aharon Chernin ([achernin@soltra.com](mailto:achernin@soltra.com)), [Soltra](http://www.soltra.com/)

Rich Piazza ([rpiazza@mitre.org](mailto:rpiazza@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

Additional artifacts:

This prose specification is one component of a Work Product which consists of:

* *STIX Version 1.2.1 Part 1: Overview*. [URI – added during publication]
* *STIX Version 1.2.1 Part 2: Common*. [URI]
* *STIX Version 1.2.1 Part 3: Core*. [URI]
* *STIX Version 1.2.1 Part 4: Indicator*. [URI]
* *STIX Version 1.2.1 Part 5: TTP*. [URI]
* *STIX Version 1.2.1 Part 6: Incident*. (this document)
* *STIX Version 1.2.1 Part 7: Threat Actor*. [URI]
* *STIX Version 1.2.1 Part 8: Campaign*. [URI]
* *STIX Version 1.2.1 Part 9: Course of Action*. [URI]
* *STIX Version 1.2.1 Part 10: Exploit Target*. [URI]
* *STIX Version 1.2.1 Part 11: Report*. [URI]
* *STIX Version 1.2.1 Part 12: Default Extensions*. [URI]
* *STIX Version 1.2.1 Part 13: Data Marking*. [URI]
* *STIX Version 1.2.1 Part 14: Vocabularies*. [URI]
* *STIX Version 1.2.1 Part 15: UML Model*. [URI]

Related work:

This specification is related to:

* *CybOX Version 2.1.1 (placeholder)*

Abstract:

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 Incident construct, which captures discrete instances of a specific set of observed events or properties affecting an organization.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

URI patterns:

Initial publication URI:  
http://docs.oasis-open.org/cti/stix/v1.2.1/csd01/part6-incident/stix-v1.2.1-csd01-part6-incident.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part6-incident.docx

(Managed by OASIS TC Administration; please don’t modify.)

Copyright © OASIS Open 2015. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

[1 Introduction 5](#_Toc429495724)

[1.1 STIX Specification Documents 5](#_Toc429495725)

[1.2 Document Conventions 6](#_Toc429495726)

[1.2.1 Fonts 6](#_Toc429495727)

[1.2.2 UML Package References 6](#_Toc429495728)

[1.2.3 UML Diagrams 7](#_Toc429495729)

[1.2.3.1 Class Properties 7](#_Toc429495730)

[1.2.3.2 Diagram Icons and Arrow Types 7](#_Toc429495731)

[1.2.3.3 Color Coding 8](#_Toc429495732)

[1.2.4 Property Table Notation 8](#_Toc429495733)

[1.2.5 Property and Class Descriptions 8](#_Toc429495734)

[1.3 Terminology 9](#_Toc429495735)

[1.4 Normative References 9](#_Toc429495736)

[2 Background 10](#_Toc429495737)

[2.1 Incident-Related Component Data Models 10](#_Toc429495738)

[3 STIX Incident Data Model 12](#_Toc429495739)

[3.1 IncidentVersionType Enumeration 18](#_Toc429495740)

[3.2 ExternalIDType Class 18](#_Toc429495741)

[3.3 TimeType Class 19](#_Toc429495742)

[3.4 CategoriesType Class 20](#_Toc429495743)

[3.5 AffectedAssetsType Class 20](#_Toc429495744)

[3.5.1 AffectedAssetType Class 21](#_Toc429495745)

[3.5.1.1 AssetTypeType Class 24](#_Toc429495746)

[3.5.2 NatureOfSecurityEffectType Class 24](#_Toc429495747)

[3.5.2.1 PropertyAffectedType Class 25](#_Toc429495748)

[3.6 ImpactAssessmentType Class 27](#_Toc429495749)

[3.6.1 DirectImpactSummaryType Class 30](#_Toc429495750)

[3.6.2 IndirectImpactSummaryType Class 32](#_Toc429495751)

[3.6.3 TotalLossEstimationType Class 33](#_Toc429495752)

[3.6.3.1 LossEstimationType Class 34](#_Toc429495753)

[3.6.4 EffectsType Class 34](#_Toc429495754)

[3.6.5 ExternalImpactAssessmentModelType Class 35](#_Toc429495755)

[3.7 RelatedIndicatorsType Class 35](#_Toc429495756)

[3.8 RelatedObservablesType Class 36](#_Toc429495757)

[3.9 LeveragedTTPsType Class 37](#_Toc429495758)

[3.10 AttributedThreatActorsType Class 39](#_Toc429495759)

[3.11 RelatedIncidentsType Class 40](#_Toc429495760)

[3.12 COATakenType Class and COARequestedType Class 42](#_Toc429495761)

[3.12.1 ContributorsType Class 43](#_Toc429495762)

[3.12.2 COATimeType Class 43](#_Toc429495763)

[3.13 HistoryType Class 44](#_Toc429495764)

[3.13.1 HistoryItemType Class 46](#_Toc429495765)

[3.13.1.1 JournalEntryType Class 46](#_Toc429495766)

[4 # Conformance 47](#_Toc429495767)

[Appendix A. Acknowledgments 48](#_Toc429495768)

[Appendix B. Revision History 50](#_Toc429495769)

# Introduction

[All text is normative unless otherwise labeled]

The Structured Threat Information Expression (STIX) framework defines nine top-level component data models: Observable[[1]](#endnote-1), Indicator, Incident, TTP, ExploitTarget, CourseOfAction, Campaign, ThreatActor, and Report. This document serves as the specification for the STIX Incident data model.

As defined within the STIX language, an Incident construct captures discrete instances of a specific set of observed events or properties affecting an organization. More specifically, an Incident consists of properties such as observables, the parties involved, assets affected, impact assessment, leveraged TTPs, attributed threat actors, intended effects, nature of compromise, courses of action requested or taken, confidence in characterization, handling guidance, log of actions taken and source information.

In Section **1.1** we discuss additional specification documents, in Section **1.2** we provide document conventions, and in Section **1.3** we provide terminology. References are given in Section **1.4**. In Section **2**, we give background information to help the reader better understand the specification details that are provided later in the document. We present the Incident data model specification details in Section **3** and conformance information in Section **4**.

## 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 individual data models that compose the full STIX UML model.

The [*STIX Version 1.2.1 Part 1: Overview*](#AdditionalArtifacts) document provides a comprehensive overview of the full set of STIX data models, 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 Version 1.2.1 Part 1: Overview*](#AdditionalArtifacts) 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](#AdditionalArtifacts) are available. The color black is used to indicate the specification overview document, altered shading differentiates the overarching Core and Common data models 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 as a CybOX specification (see [*STIX Version 1.2.1 Part 1: Overview*](#AdditionalArtifacts) for details). This Incident specification document is highlighted in its associated color (see Section **1.2.3.3**). For a list of all STIX documents and related information sources, please see [*STIX Version 1.2.1 Part 1: Overview*](#AdditionalArtifacts).

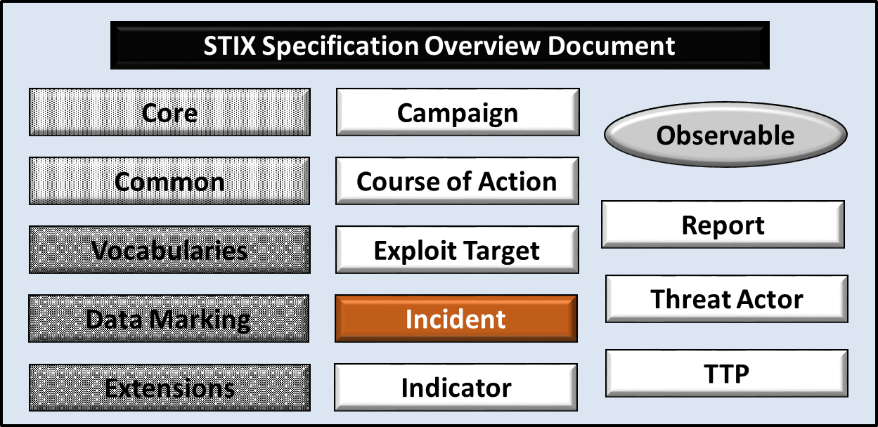


Figure ‑. STIX Language v1.2.1 specification documents

## Document Conventions

The following conventions are used in this document.

### 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 [*STIX Version 1.2.1 Part 1: Overview*](#AdditionalArtifacts).

Examples: Incident, Course of Action, Threat Actor

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

Examples: RelatedIncidentsType, 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 (withsingle 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.*

### 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. [*STIX Version 1.2.1 Part 1: Overview*](#AdditionalArtifacts) contains a list of the packages used by the Incident 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 Incident data model.

### 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 either a data type or a class from the STIX Common data model.  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.

#### 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.

#### 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 ‑. UML diagram icons

|  |  |
| --- | --- |
| **Icon** | **Description** |
| cid:image003.gif@01D05428.2B30AE20 | 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. |

#### 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 Incident specification are illustrated via exemplars in **Figure 1‑2**.



Figure ‑. Data model color coding

### Property Table Notation

Throughout Section **1**, 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 Indicator data model (see Section **1.2.2**).

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\_CallA, CodeB) and single logic expression in the Multiplicity column.  For example, if there is a choice of property API\_CallA and CodeB, 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.

### Property and Class Descriptions

Each class and property defined in STIX is described using the format, “The X property verbY.” 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** |
| captures | 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. |
|  | *Examples:*  The Source property characterizes the source of the sighting information. Examples of details captured include identitifying characteristics, time-related attributes, and a list of the tools used to collect the information.  The Description property captures a textual description of the Indicator. |
| characterizes | 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. |
|  | *Examples:*  The Confidence property characterizes the level of confidence in the accuracy of the overall content captured in the Incident.  The ActivityType class characterizes basic information about an activity a defender might use in response to a Campaign. |
| specifies | 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. |
|  | *Example:*  The version property specifies the version identifier of the STIX Campaign data model used to capture the information associated with the Campaign. |

## Terminology

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 [RFC2119].

## Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.

# Background

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

## Incident-Related Component Data Models

As will be explicitly detailed in Section **3**, a STIX Incident leverages five other top-level STIX constructs, namely Course of Action, Indicator, Threat Actor, Observable (as defined with the [CybOX Language](#RelatedWork)) and TTP (as indicated by the outward-oriented arrows). As stated in Section **1.1**, each of these components is defined in a separate specification document. **Figure 2‑1** illustrates the relationship between the Incident and the other core constructs.



Figure ‑. Highlevel view of the Incident data model

In this section, we give a high level summary of the relationship between the Incident data model and the other components to which an Incident may refer. We also make note of the fact that the Incident data model can be self-referential. Other relationships shown in the diagram are defined in the specification of the component that they originate from.

* **Course of Action**

A STIX [Course of Action](http://stixproject.github.io/data-model/1.1.1/coa/CourseOfActionType) (COA) is used to convey information about courses of action that may be taken either in response to an attack or as a preventative measure prior to an attack. A Course of Action component captures a variety of information such as the Course of Action’s objective, likely impact, efficacy, and cost. Please see [*STIX Version 1.2.1 Part 9: Course of Action*](#AdditionalArtifacts) for details.

The Incident data model references the Course of Action data model as a means to identify Courses of Action requested by the incident responders or Courses of Action that were actually taken in the process of responding to the Incident.

* **Incident**

The Incident data model is self-referential, enabling one Incident to reference other Incidents that are asserted to be related. Self-referential relationships between Incidents may indicate general associativity or can be used to indicate relationships beween different versions of the same Incident.

* **Indicator**

A STIX Indicator conveys specific Observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context. Please see [*STIX Version 1.2.1 Part 4: Indicator*](#AdditionalArtifacts) for details.

The Incident data model leverages the Indicator data model to specify indicators relevant to the Incident whether they were the triggers that initiated the incident response or they are a result of the incident investigation analysis and may be of value in detecting the adversary TTPs leveraged in the incident.

* **Observable**

A STIX Observable (as defined with the [CybOX Language](#RelatedWork)) represents stateful properties or measurable events pertinent to the operation of computers and networks. Implicit in this is a practical need for descriptive capability of two forms of observables: “observable instances” and “observable patterns.” Observable instances represent actual specific observations that took place in the cyber domain. The property details of this observation are specific and unambiguous. Observable patterns represent conditions for a potential observation that may occur in the future or may have already occurred and exists in a body of observable instances. These conditions may be anything from very specific concrete patterns that would match very specific observable instances to more abstract generalized patterns that have the potential to match against a broad range of potential observable instances.

The Incident data model leverages the Observable data model to specify the observable instances that were observed in relation to the Incident.

* **Tactics, Techniques and Procedures (TTP)**

A STIX Tactics, Techniques, and Procedures (TTP) is used to represent the behavior or modus operandi of cyber adversaries. Please see [*STIX Version 1.2.1 Part 5: TTP*](#AdditionalArtifacts) for details.

The Incident data model references the TTP data model as a means to identify sets of specific TTPs that are asserted as having been leveraged in the Incident.

* **Threat Actor**

A STIX Threat Actor is a characterization of a malicious actor (i.e., adversary) that represents a cyber attack threat. A variety of information can be captured in a Threat Actor construct, including identity, motivations, intended effect, and sophistication level. Please see [*STIX Version 1.2.1 Part 7: Threat Actor*](#AdditionalArtifacts) for details.

The Incident data model references the Threat Actor data model as a means to characterize the Threat Actors that have been attributed to the Incident.

# 

# STIX Incident Data Model

The primary class of the STIX Incident package is the IncidentType class, which characterizes a cyber threat Incident made up of sets of related security events affecting an organization, investigatory details of timing and personnel, as well as other characterizing information discovered or decisions reached during an incident response investigation. Similar to the primary classes of all of the component data models in STIX, the IncidentType class extends a base class defined in the STIX Common data model; more specifically, it specializes the IncidentBaseType base class, which provides the essential identifier (id) and identifier reference (idref) properties.

The relationship between the IncidentType class and the IncidentBaseType base class, as well as the properties of the IncidentType class, are illustrated in the UML diagram given in **Figure 3‑1**.



Figure ‑. UML diagram of the IncidentType class

The property table, which includes property descriptions and corresponds to the UML diagram above, is given in **Table 3‑1**.

All classes defined in the Incident data model are described in detail in Sections **3.1** through **3.13**. Details are not provided for classes defined in non-Incident data models; instead, the reader is refered to the corresponding data model specification as indicated by the package prefix specified in the Type column of the table.

Table ‑. Properties of the IncidentType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Documentation** |
| **version** | IncidentVersionType | 0..1 | The version property specifies the version identifier of the STIX Incident data model for STIX v1.2.1 used to capture the information associated with the Incident. |
| **URL** | basicDataTypes:URI | 0..1 | The URL property specifies a URL referencing the location for an external representation of the Incident (e.g. in an incident tracking system). |
| **Title** | basicDataTypes:  BasicString | 0..1 | The Title property provides a simple title for the Incident and reflects what the producer thinks the Incident as a whole should be called. Titles are typically used by humans to reference a particular Incident; however, titles are not meant to be used for correlation. |
| **External\_ID** | ExternalIDType | 0..\* | The External\_ID property captures an identifier for the Incident managed in an external non-STIX system. |
| **Time** | TimeType | 0..1 | The Time property specifies a variety of time values associated with the Incident (e.g., the time the Incident was officially opened). |
| **Description** | stixCommon:  StructuredTextType | 0..\* | The Description property captures a textual description of the Incident. Any length is permitted. Optional formatting is supported via the structuring\_format property of the StructuredTextType class. |
| **Short\_Description** | stixCommon:  StructuredTextType | 0..\* | The Short\_Description property captures a short textual description of the Incident.  This property is secondary and should only be used if the Description property is already populated and another, shorter description is available. |
| **Categories** | CategoriesType | 0..1 | The Categories property specifies a set of categorization labels for the Incident. |
| **Reporter** | stixCommon:  InformationSourceType | 0..1 | The Reporter property characterizes the entity that reported the Incident. |
| **Responder** | stixCommon:  InformationSourceType | 0..\* | The Responder property characterizes the entity playing the role of the responder for the Incident. |
| **Coordinator** | stixCommon:  InformationSourceType | 0..\* | The Coordinator property characterizes the entity playing the role of coordinator for the Incident. |
| **Victim** | stixCommon:  IdentityType | 0..\* | The Victim property chracterizes information about a victim of the Incident. For situations calling for more than a simple name, the underlying class may be extended using a more complete structure such as the CIQIdentity3.0InstanceType subclass as defined in [*STIX Version 1.2.1 Part 12: Default Extensions*](#AdditionalArtifacts). |
| **Affected\_Assets** | AffectedAssetsType | 0..1 | The Affected\_Assets property characterizes the assets affected during the Incident. |
| **Impact\_Assessment** | ImpactAssessmentType | 0..1 | The Impact\_Assessment property characterizes an assessment of impact for the Incident. |
| **Status** | stixCommon:  VocabularyStringType | 0..1 | The Status property specifies the state or disposition of the Incident. Examples of potential statuses are *new*, *open,* and *closed* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the Status property is ‘*IncidentStatusVocab-1.0*’. |
| **Related\_Indicators** | RelatedIndicatorsType | 0..1 | The Related\_Indicators property specifies a set of one or more other Indicators relevant to the Incident whether they were the triggers that initiated the incident response or they are a result of the incident investigation analysis and may be of value in detecting the adversary TTPs leveraged in the incident. |
| **Related\_Observables** | RelatedObservablesType | 0..1 | The Related\_Observables property specifies a set of one or more observable instances that were observed in relation to the Incident. |
| **Leveraged\_TTPs** | LeveragedTTPsType | 0..1 | The Leveraged\_TTPs property specifies a set of one or more TTPs that are asserted as having been leveraged in the Incident. |
| **Attributed\_Threat\_Actors** | AttributedThreatActorsType | 0..1 | The Attributed\_Threat\_Actors property specifies a set of one or more other Threat Actors that have been attributed to the Incident. |
| **Intended\_Effect** | stixCommon:  StatementType | 0..\* | The Intended\_Effect property characterizes the suspected intended effect of the Incident, which includes a Value property that specifies the type of the effect. Examples of potential types include *theft*, *disruption*, and *unauthorized access* (these specific values are only provided to help explain the Value 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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the Value property is ‘*IntendedEffectVocab-1.0*’ (which is different than the default vocabulary provided for the StatementType class). |
| **Security\_Compromise** | stixCommon:  VocabularyStringType | 0..1 | The Security\_Compromise property specifies an assertion of whether the Incident involved a compromise of security properties (e.g. confidentiality). Examples of potential assertions are *yes*, *no,* and *suspected* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is  *‘SecurityCompromiseVocab-1.0’.* |
| **Discovery\_Method** | stixCommon:  VocabularyStringType | 0..\* | The Discovery\_Method property specifies the method by which the Incident was discovered. Examples of potential methods are *audit*, *NIDS,* and *user* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is  *‘DiscoveryMethodVocab-2.0’.* |
| **Related\_Incidents** | RelatedIncidentsType | 0..1 | The Related\_Incidents property specifies a set of one or more Incidents related to this Incident. |
| **COA\_Requested** | COARequestedType | 0..\* | The COA\_Requested property specifies one or more Courses of Action for the Incident requested by the incident responders. This property is distinct from the COA\_Taken property due to the fact that while incident responders often have rich context for requesting particular courses of action, the authority to actually implement a course of action typically lies with other parties. |
| **COA\_Taken** | COATakenType | 0..\* | The COA\_Taken property specifies a Course of Action taken for the Incident. This property is distinct from the COA\_Requested property due to the fact that while incident responders often have rich context for requesting particular courses of action, the authority to actually implement a course of action typically lies with other parties. |
| **Confidence** | stixCommon:  ConfidenceType | 0..1 | The Confidence property characterizes the level of confidence in the accuracy of the overall content captured in the Incident. |
| **Contact** | stixCommon:  InformationSourceType | 0..\* | The Contact property characterizes a point of contact for the organizations and personnel involved in the Incident. |
| **History** | HistoryType | 0..1 | The History property captures a log of events or actions taken during the handling of the Incident. |
| **Information\_Source** | stixCommon:  InformationSourceType | 0..1 | The Information\_Source property characterizes the source of the Incident information. Examples of details captured include identitifying characteristics, time-related attributes, and a list of tools used to collect the information. |
| **Handling** | marking:MarkingType | 0..1 | The Handling property specifies the appropriate data handling markings for the properties of this Incident. The marking scope is limited to the Incident and the content is contains. Note that data handling markings can also be specified at a higher level. |
| **Related\_Packages** | stixCommon:  RelatedPackageRefsType | 0..1 | The Related\_Packages property specifies a set of one or more STIX Packages that are related to the Incident. |

## IncidentVersionType Enumeration

The IncidentVersionType enumeration is an inventory of all versions of the Incident data model for STIX Version 1.2.1. The enumeration literals are given in **Table 3‑2**.

Table ‑. Literals of the IncidentVersionType enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **stix-1.2.1** | Incident data model for STIX v1.2.1 |

## ExternalIDType Class

The ExternalIDType provides a reference to an ID of an incident in a remote system.

The properties of the ExternalIDType class are given in **Table 3‑3**.

Table ‑. Properties of the ExternalIDType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **source** | basicDataTypes: NoEmbeddedQuotesString | 0..1 | The source property specifies the source of the External ID. |

## TimeType Class

The TimeType class characterizes key time points of interest for the Incident.

The properties of the TimeType class are given in **Table 3‑4**.

As specified in [*STIX Version 1.2.1 Part 2: Common*](#AdditionalArtifacts), all timestamps specified using the stixCommon:DateTimeWithPrecisionType SHOULD include a specification of the time zone. In addition to specifying a date and time, the Date\_Time property may also capture a precision property to specify the granularity with which the time should be considered, as specified by the DateTimePrecisionEnum 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.

Table ‑. Properties of the TimeType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **First\_Malicious\_Action** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The First\_Malicious\_Action property specifies the time that the first malicious action related to the Incident occured. |
| **Initial\_Compromise** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Initial\_Compromise property specifies the time that the initial compromise occured for the Incident. |
| **First\_Data\_Exfiltration** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The First\_Data\_Exfiltration property specifies the first time at which non-public data was taken from the victim environment. |
| **Incident\_Discovery** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Incident\_Discovery property specifies the first time at which the organization learned the Incident had occurred. |
| **Incident\_Opened** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Incident\_Opened property specifies the time at which the Incident was officially opened. |
| **Containment\_Achieved** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Containment\_Achieved property specifies the first time at which the Incident is contained (e.g., the “bleeding is stopped”). |
| **Restoration\_Achieved** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Restoration\_Achieved property specifies the first time at which the incident's assets are restored (e.g., fully functional). |
| **Incident\_Reported** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Incident\_Reported property specifies the time at which the Incident was reported. |
| **Incident\_Closed** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Incident\_Closed property specifies the time at which the Incident was officially closed. |

## CategoriesType Class

The CategoriesType class specifies one or more category labels for the Incident.

The properties of the TimeType class are given in **Table 3‑5**.

Table ‑. Properties of the CategoriesType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Category** | stixCommon:  VocabularyStringType | 1..\* | The Category property specifies a category label for the Incident. Examples of potential categories are *denial of service*, *improper usage*, and *scan* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is *‘IncidentCategoryVocab-1.0’.* |

## AffectedAssetsType Class

The AffectedAssetsType class specifies a list of one or more assets affected during the Incident.

The UML diagram corresponding to the AffectedAssetsType class is shown in **Figure 3‑2**.



Figure ‑. UML diagram of AffectedAssetsType class

The property table given in **Table 3‑6** corresponds to the UML diagram shown in **Figure 3‑2**.

Table ‑. Properties of the AffectedAssetsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Affected\_Asset** | AffectedAssetType | 0..\* | The Affected\_Asset property characterizes a particular asset affected during the Incident. |

### AffectedAssetType Class

The AffectedAssetType class characterizes various aspects of the asset negatively impacted by the Incident.

The UML diagram corresponding to the AffectedAssetsType class is shown in **Figure 3‑3**.



Figure ‑. UML diagram of AffectedAssetType class

The property tables given in **Table 3‑7**, **Table 3‑8**, **Table 3‑9**, **Table 3‑10** and **Table 3‑11** all correspond to the UML diagram shown in **Figure 3‑3**.

Table ‑. Properties of the AffectedAsset class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Type** | AssetTypeType | 0..1 | The Type property characterizes the type of the assets impacted by the Incident. |
| **Description** | stixCommon:  StructuredTextType | 0..\* | The Description property captures a textual description of the asset. Any length is permitted. Optional formatting is supported via the structuring\_format property of the StructuredTextType class. |
| **Business\_Function\_Or\_Role** | stixCommon:  StructuredTextType | 0..\* | The Business\_Function\_Or\_Role captures a textual description of the asset's role, function, and importance within the organization. Any length is permitted. Optional formatting is supported via the structuring\_format property of the StructuredTextType class. |
| **Ownership\_Class** | stixCommon:  VocabularyStringType | 0..1 | The Ownership\_Class property specifies who owns (or controls) this asset. Examples of potential values are *employee*, *customer* and *partner* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*OwnershipClassVocab-1.0*’. |
| **Management\_Class** | stixCommon:  VocabularyStringType | 0..1 | The Management\_Class property specifies a high-level characterization of who is responsible for the day-to-day management and administration of the asset. Examples of potential values are *internally*, *externally,* and *co-managed* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*ManagementClassVocab-1.0.’* |
| **Location\_Class** | stixCommon:  VocabularyStringType | 0..1 | The Location\_Class property specifies a high-level summarized characterization of the locality type for this asset Examples of potential values are *internal*, *external*, and *mobile* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*LocationClassVocab-1.0.’* |
| **Location** | stixCommon:  AddressAbstractType | 0..1 | The Location property characterizes the actual physical location of the affected asset. The underlying abstract class MUST be extended. The default and strongly RECOMMENDED subclass is CIQAddressInstanceType, as defined in [*STIX Version 1.2.1 Part 12: Default Extensions*](#AdditionalArtifacts). |
| **Nature\_Of\_Security\_Effect** | NatureOfSecurityEffectType | 0..1 | The Nature\_Of\_Security\_Effect property characterizes how the security properties of the asset were affected. |
| **Structured\_Description** | cybox:ObservablesType | 0..1 | The Structured\_Description property characterizes the asset through specification of a structured cyber Observables instance. |

#### AssetTypeType Class

The AssetTypeType class characterizes the type of the Affected Asset. Examples of asset types are *directory, firewall, PBX* and *cashier* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in this property is *'AssetTypeVocab-1.0'*.

The property of the AssetTypeType class is given in **Table 3‑8**.

Table ‑. Properties of the AssetTypeType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **count\_affected** | basicDataTypes:Integer | 0..1 | The count\_affected property specifies the number of assets of this type affected in the Incident. |

### NatureOfSecurityEffectType Class

The NatureOfSecurityEffectType class specifies a set of zero or more security properties affected by the Incident.

The property of the NatureOfSecurityEffectType class is given in **Table 3‑9**.

Table ‑. Properties of the NatureOfSecurityEffectType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Property\_Affected** | PropertyAffectedType | 0..\* | The Property\_Affected property characterizes how a particular security property of the asset was affected. |

#### PropertyAffectedType Class

The PropertyAffectedType class characterizes aspects of how security properties of an asset, such as Availability, Confidentiality, etc., were affected in this Incident.

The properties of the PropertyAffectedType class are given in **Table 3‑10**.

Table ‑. Properties of the PropertyAffectedType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Property** | stixCommon:  VocabularyStringType | 0..1 | The Property property specifies the security property that was affected by the incident. Examples of potential security properties are *confidentiality*, *integrity* and *availability* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*LossPropertyVocab-1.0.’* |
| **Description\_Of\_Effect** | stixCommon:  StructuredTextType | 0..\* | The Description\_Of\_Effect property captures a textual description of how the security property was affected.  Any length is permitted. Optional formatting is supported via the structuring\_format property of the StructuredTextType class. |
| **Type\_Of\_Availability\_Loss** | stixCommon:  VocabularyStringType | 0..1 | The Type\_Of\_Availability\_Loss property specifies in what manner the availability of the particular asset was affected. Examples of potential values are *destruction*, *deletion* and *interruption* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*AvailabilityLossTypeVocab-1.2’*. |
| **Duration\_Of\_Availability\_Loss** | stixCommon:  VocabularyStringType | 0..1 | The Duration\_Of\_Availability\_Loss property specifies the approximate length of time availability was affected. Examples of potential values are *permanent*, *seconds* and *days* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*LossDurationVocab-1.0’*. |
| **Non\_Public\_Data\_Compromised** | NonPublicDataCompromisedType | 0..1 | The Non\_Public\_Data\_Compromised property specifies whether non-public data was compromised or exposed and whether that data was encrypted or not. Examples of potential values are *yes, no* and *suspected* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the Non\_Public\_Data\_Compromised property is ‘*SecurityCompromiseVocab-1.0’*. |

##### NonPublicDataCompromisedType Class

The NonPublicDataCompromisedType class represents whether non-public data was compromised or exposed and whether that data was encrypted or not.

Table ‑. Properties of the NonPublicCompromisedType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **data\_encrypted** | basicDataTypes: Boolean | 0..1 | The data\_encrypted property specifies whether the data that was compromised was encrypted or not. |

## ImpactAssessmentType Class

The ImpactAssessmentType class characterizes a summary assessment of impact for this cyber threat Incident.

The UML diagram corresponding to the ImpactAssessmentType class is shown in **Figure 3‑3**.



Figure ‑. UML diagram of the ImpactAssessmentType class

The property tables given in **Table 3‑12**, **Table 3‑13**, **Table 3‑15**, **Table 3‑16**, **Table 3‑17** and **Table 3‑18** all correspond to the UML diagram shown in **Figure 3‑4**.

Table ‑. Properties of the ImpactAssessmentType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Direct\_Impact\_Summary** | DirectImpactSummaryType | 0..1 | The Direct\_Impact\_Summary property characterizes (at a high level) impact directly resulting from the Threat Actor's actions against organizational assets within the Incident. |
| **Indirect\_Impact\_Summary** | IndirectImpactSummaryType | 0..1 | The Indirect\_Impact\_Summary property characterizes (at a high level) impact from other stakeholder reactions to the Incident. |
| **Total\_Loss\_Estimation** | TotalLossEstimationType | 0..1 | The Total\_Loss\_Estimation property specifies the total estimated financial loss for the Incident. |
| **Impact\_Qualification** | stixCommon:  VocabularyStringType | 0..1 | The Impact\_Qualification property specifies the subjective level of impact of the Incident. Examples of potential values are *insignificant*, *catastrophic* and *damaging* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the Impact\_Qualification property is ‘*ImpactQualificationVocab-1.0*’. |
| **Effects** | EffectsType | 0..1 | The Effects property specifies a set of one or more effects of this incident. |
| **External\_Impact\_Assessment\_Model** | ExternalImpactAssessmentModelType | 0..1 | The External\_Impact\_Assessment\_Model property characterizes impact assessment details. It is defined utilizing an abstract class enabling the definition through extension of incident impact assessment models external to STIX. |

### DirectImpactSummaryType Class

The DirectImpactSummaryType class quantitatively characterizes (at a high level) the direct impact of the Incident, both financial and non-financial.

Table ‑. Properties of the DirectImpactSummaryType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Asset\_Losses** | stixCommon:  VocabularyStringType | 0..1 | The Asset\_Losses property specifies (at a high level) the level of asset-related losses that occured in the Incident, including lost or damaged assets, stolen funds, cash outlays, etc. Examples of potential levels are *minor*, *major* and *none* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*ImpactRatingVocab-1.0’.* |
| **Business-Mission\_Disruption** | stixCommon:  VocabularyStringType | 0..1 | The Business-Mission\_Disruption property specifies (at a high level) the level of business or mission disruption impact that occured in the Incident including unproductive man-hours, lost revenue from system downtime, etc.  Examples of potential levels are *minor*, *major* and *none* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*ImpactRatingVocab-1.0’.* |
| **Response\_And\_Recovery\_Costs** | stixCommon:  VocabularyStringType | 0..1 | The Response\_And\_Recovery\_Costs property specifies (at a high level) the level of response and recovery related costs that occured in the Incident including cost of response, investigation, remediation, restoration, etc.  Examples of potential levels are *minor*, *major* and *none* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is ‘*ImpactRatingVocab-1.0’.* |

### IndirectImpactSummaryType Class

The IndirectImpactSummaryType class qualitatively characterizes (at a high level) the indirect impact of the Incident, both financial and non-financial.

Table ‑. Properties of the IndirectImpactSummaryType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Loss\_Of\_Competitive\_Advantage** | stixCommon:  VocabularyStringType | 0..1 | The Loss\_Of\_Competitive\_Advantage if a loss of competitive advantage occured in the Incident. The impact could include: loss/damage/exposure of IP, corporate wisdom, ability to compete, key personnel, etc. Examples of potential statuses are *yes*, *no* and *suspected* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in the property is *‘SecurityCompromiseVocab-1.0’.* |
| **Brand\_And\_Market\_Damage** | stixCommon:  VocabularyStringType | 0..1 | The Brand\_And\_Market\_Damage property specifies the level of impact based on brand or market damage that occured in the Incident. The impact could include: lost customers or partners, decrease in market value or share, advertising, rebranding, etc. Examples of potential statuses are *yes*, *no* and *suspected* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in this property is *‘SecurityCompromiseVocab-1.0’.* |
| **Increased\_Operating\_Costs** | stixCommon:  VocabularyStringType | 0..1 | The Increased\_Operating\_Costs property specifies if increased operating costs occured in the Incident. The impact could include: cost of additional audits, new hires or training, mandatory action, higher insurance, etc. Examples of potential statuses are *yes*, *no* and *suspected* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in this property is *‘SecurityCompromiseVocab-1.0’.* |
| **Legal\_And\_Regulatory\_Costs** | stixCommon:  VocabularyStringType | 0..1 | The Legal\_And\_Regulatory\_Costs property specifies if legal and regulatory costs occured in the Incident. This includes legal fees, lawsuits, customer damages, contract violations, etc. Examples of potential statuses are *yes*, *no* and *suspected* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in this property is *‘SecurityCompromiseVocab-1.0’.* |

### TotalLossEstimationType Class

The TotalLossEstimationType class characterizes both the initial reported and actual estimated financial losses for this Incident.

Table ‑. Properties of the TotalLossEstimationType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Initial\_Reported\_Total\_Loss\_Estimation** | LossEstimationType | 0..1 | The Initial\_Reported\_Total\_Loss\_Estimation property specifies the initially reported level of total estimated financial loss for the Incident. |
| **Actual\_Total\_Loss\_Estimation** | LossEstimationType | 0..1 | The Actual\_Total\_Loss\_Estimation property specifies the actual level of total estimated financial loss for the Incident. |

#### LossEstimationType Class

The LossEstimationType class characterizes an estimated financial loss.

Table ‑. Properties of the LossEstimationType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **amount** | basicDataTypes:Decimal[[2]](#endnote-2) | 0..1 | The amount property specifies the estimated financial loss for the Incident. |
| **iso\_currency\_code** | basicDataTypes: NoEmbeddedQuotesString[[3]](#endnote-3) | 0..1 | The iso\_currency\_code property specifies the ISO 4217 currency code if other than USD. |

### EffectsType Class

The EffectsType class specifies one or more effects asserted as present for this Incident.

Table ‑. Properties of the EffectsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Effect** | stixCommon:  VocabularyStringType | 1..\* | The Effect property represents a single effect asserted as present for this Incident. Examples of potential statuses are *denial of service*, *improper usage* and *scan* (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 stixCommon:ControlledVocabularyStringType class. The STIX default vocabulary class for use in this property is  ‘*IncidentEffectVocab-1.0’*. |

### ExternalImpactAssessmentModelType Class

The ExternalImpactAssessmentModelType class is an abstract class enabling the definition through extension of incident impact assessment models external to STIX.

Table ‑. Properties of the ExternalImpactAssessmentModelType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **model\_name** | basicDataTypes: NoEmbeddedQuotesString | 0..1 | The model\_name property specifies the name of the externally defined impact assessment model. |
| **model\_reference** | BasicDataType:URI | 0..1 | The model\_reference property specifies a URI reference to the characterization of the externally defined impact assessment model. |

## RelatedIndicatorsType Class

The RelatedIndicatorsType class specifies one or more Indicators relevant to the Incident whether they were the triggers that initiated the incident response or they are a result of the incident investigation analysis and may be of value in detecting the adversary TTPs leveraged in the incident. It extends the GenericRelationShipListType superclass defined in the STIX Common data model, which specifies the scope (whether the elements of the set are related individually or as a group).

The UML diagram corresponding to the RelatedIndicatorsType class is shown in **Figure 3‑5**, and the specialized properties are shown in **Table 3‑19**.



Figure ‑. UML diagram of the RelatedIndicatorsType class

The property table given in **Table 3‑19** corresponds to the UML diagram given in **Figure 3‑5**.

Table ‑. Properties of the RelatedIndicatorsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Related\_Indicator** | stixCommon:RelatedIndicatorType | 1..\* | The Related\_Indicator property characterizes an Indicator asserted to be relevant to the Incident whether they were the triggers that initiated the incident response or they are a result of the incident investigation analysis and may be of value in detecting the adversary TTPs leveraged in the incident. To further characterize the relationship to the Indicator, information captured includes the level of confidence that the Indicator is relevant, the source of the relationship information, and type of the relationship. |

## RelatedObservablesType Class

The RelatedObservablesType class specifies one or more CybOX Observable instances that were observed in relation to the Incident. It extends the GenericRelationShipListType superclass defined in the STIX Common data model, which specifies the scope (whether the elements of the set are related individually or as a group).

The UML diagram corresponding to the RelatedObservablesType class is shown in **Figure 3‑6**, and the properties are shown in **Table 3‑20**.



Figure ‑. UML diagram of the RelatedObservablesType class

The property table given in **Table 3‑20** corresponds to the UML diagram shown in **Figure 3‑6**.

Table ‑. Properties of the RelatedObservablesType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Related\_Observable** | stixCommon:  RelatedObservableType | 1..\* | The Related\_Observable property captures the properties of a cyber Observable instance that was observed in relation to the Incident. In addition, the property characterizes the relationship between the Observable and the Incident by capturing additional information such as the level of confidence in the assertion that the Observable and the Incident are related, information on the source of the relationship information, and details on the type of the relationship between the Observable and the Incident. |

## LeveragedTTPsType Class

The LeveragedTTPsType class specifies one or more TTP that are asserted to have been leveraged during this Incident. It extends the GenericRelationShipListType superclass defined in the STIX Common data model, which specifies the scope (whether the elements of the set are related individually or as a group).

The UML digram corresponding to the LeveragedTTPsType class class is shown in **Figure 3‑7**.



Figure ‑. UML diagram of the LeveragedTTPsType class

The property table given in **Table 3‑21** corresponds to the UML diagram shown in **Figure 3‑7**.

Table ‑. Properties of the LeveragedTTPsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Leveraged\_TTP** | stixCommon:  RelatedTTPType | 1..\* | The Leveraged\_TTP property specifies a TTP asserted to have been leveraged in the Incident and characterizes the relationship between the Incident and the TTP by capturing information such as the level of confidence that the Incident and the TTP are related, the source of the relationship information, and the type of relationship. |

## AttributedThreatActorsType Class

The AttributedThreatActorsType class specifies a list of one or more Threat Actors that have been attributed to the Incident. It extends the GenericRelationShipListType superclass defined in the STIX Common data model, which specifies the scope (whether the elements of the set are related individually or as a group).

The UML digram corresponding to the AttributedThreatActorsType class is shown in **Figure 3‑8**.



Figure ‑. UML diagram of the AttributedThreatActorType class

The property table given in **Table 3‑22** corresponds to the UML diagram shown in **Figure 3‑8**.

Table ‑. Properties of the AttributedThreatActorsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Threat\_Actor** | stixCommon:  RelatedThreatActorType | 1..\* | The Threat\_Actor property captures a relationship to a Threat Actor that has been attributed to the Incident. To further characterize the relationship between the Incident and the Threat Actor, information captured includes the level of confidence that the Incident and the Threat Actor are related, the source of the relationship information, and type of the relationship. |

## RelatedIncidentsType Class

The RelatedIncidentsType class specifies a list of one or more other Incidents asserted as related to the Incident and therefore is a self-referential relationship. It extends the GenericRelationShipListType superclass defined in the STIX Common data model, which specifies the scope (whether the elements of the set are related individually or as a group).



Figure ‑. UML diagram of the RelatedIncidentsType class

The property table given in **Table 3‑23** corresponds to the UML diagram given in **Figure 3‑9**.

Table ‑. Properties of the RelatedIncidentsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Related\_Incident** | stixCommon:  RelatedIncidentType | 1..\* | The Related\_Incident property specifies another Incident associated with this Incident and characterizes the relationship between the Incidents by capturing information such as the level of confidence that the Incidents are related, the source of the relationship information, and type of the relationship. A relationship between Incidents may represent assertions of general associativity or different versions of the same Incident. |

## COATakenType Class and COARequestedType Class

The COATakenType class specifies a Course of Action for the Incident requested by the incident responders. The COARequestedType class specifies a Course of Action taken for the Incident. The UML diagram corresponding to the COATakenType andCOARequestedType classes is shown in **Figure 3‑10**.



Figure ‑. UML diagram of the COATakenType and COARequestedType classes

The property tables given in **Table 3‑24**, **Table 3‑25**, **Table 3‑26** and Error! Reference source not found. all correspond to the UML diagram given in **Figure 3‑10**.

Table ‑. Properties of the COATakenType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Time** | COATimeType | 0..1 | The Time property specifies when this Course of Action was taken (start and end). |
| **Contributors** | ContributorsType | 0..1 | The Contributors property specifies contributing actors for the Course of Action taken. |
| **Course\_Of\_Action** | stixCommon:  CourseOfActionBaseType | 0..1 | The Course\_Of\_Action property specifies the actual Course of Action taken. If a new Course of Action is defined (as opposed to an existing Course of Action referenced), the default and strongly RECOMMENDED method is to leverage the CourseOfActionType class from the Course Of Action data model (which extends the CourseOfActionBaseType superclass). |

Table ‑. Properties of the COARequestedType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **priority** | basicDataTypes:  NoEmbeddedQuotesString[[4]](#endnote-4) | 0..1 | The priority property characterizes a suggested level of priority to be applied to this requested COA. |

### ContributorsType Class

The ContributorType class characterizes the actors involved in a course of action.

Table ‑. Properties of the ContributorsType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Contributor** | cyboxCommon:ContributorType | 1..\* | The Contributor property characterizes an entity involved in this Course of Action. |

### COATimeType Class

The COATimeType class specifies the relevant time period for the execution of a courses of action were for this Incident.

Table ‑. Properties of the COATimeType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Start** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The Start property specifies the time in which the Course of Action was begun. To avoid ambiguity, timestamps SHOULD include a specification of the time zone. In addition to capturing a date and time, the Start property MAY also capture a precision property to specify the granularity with which the time should be considered, as specified by the DateTimePrecisionEnum enumeration (e.g., '*hour*,' '*minute*'). If the Start property is not present, then it is unknown when the Course of Action was started. |
| **End** | stixCommon:  DateTimeWithPrecisionType | 0..1 | The End field specifies the time at which the Course of Action was completed. In order to avoid ambiguity, it is strongly suggest that all timestamps include a specification of the timezone if it is known. In addition to capturing a date and time, the End property MAY also capture a precision property to specify the granularity with which the time should be considered, as specified by the DateTimePrecisionEnum enumeration (e.g., '*hour*,' '*minute*'). If the End property is not present, then it is unknown when the Course of Action ended, or the Course of Action is ongoing. |

## HistoryType Class

The HistoryType class captures a record of events or actions taken as well as information discovered during the handling of the Incident. This can include Courses of Action taken and general journal notes. The time that the note is written, or the Course of Action taken and the author or actors involved may be specified.



Figure ‑. UML diagram of the HistoryType class

The property tables given in Error! Reference source not found., Error! Reference source not found. and Error! Reference source not found. corresponds to the UML diagram given in Error! Reference source not found.. Also see tables in Section **3.12**.

Table ‑. Properties of the HistoryType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **History\_Item** | HistoryItemType | 0..\* | The History\_Item property captures a log entry of either an event or action taken during the handling of the Incident or a journal entry containing information discovered during the investigation of the Incident. |

### HistoryItemType Class

The HistoryItemType class specifies the choice of either an action or journal entry as an item in the Incident’s history.

Table ‑. Properties of the HistoryItemType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Action\_Entry** | COATakenType | 0..1 | The Action\_Entry property captures a record of a Course of Action taken during the handling of the Incident. |
| **Journal\_Entry** | JournalEntryType | 0..1 | The Journal\_Entry property captures journal notes for information discovered during the handling of the Incident. |

#### JournalEntryType Class

The JournalEntryType class captures journal notes for information discovered during the handling of the Incident. It is a subtype of BasicDataTypes:BasicString (see Error! Reference source not found.).

Table ‑. Properties of the JournalEntryType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **author** | basicDataTypes: NoEmbeddedQuotesString | 0..1 | The author property specifies the author of the JournalEntry note. |
| **time** | BasicDataTypes:DateTime | 0..1 | The time property specifies the date and time of the journal entry creation. To avoid ambiguity, all timestamps SHOULD include a specification of the time zone. |
| **time\_precision** | stixCommon:DateTimePrecisionEnum | 0..1 | The time\_precision property specifies the granularity with which the time property should be considered, as specified by the DateTimePrecisionEnum 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. |

# # Conformance

The last numbered section in the specification must be the Conformance section. Conformance Statements/Clauses go here. [Remove # marker]

1. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Dean Thompson, Australia and New Zealand Banking Group (ANZ Bank)

Bret Jordan, Blue Coat Systems, Inc.

Adnan Baykal, Center for Internet Security (CIS)

Jyoti Verma, Cisco Systems

Liron Schiff, Comilion (mobile) Ltd.

Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)

Richard Struse, DHS Office of Cybersecurity and Communications (CS&C)

Marlon Taylor, DHS Office of Cybersecurity and Communications (CS&C)

David Eilken, Financial Services Information Sharing and Analysis Center (FS-ISAC)

Sarah Brown, Fox-IT

Ryusuke Masuoka, Fujitsu Limited

Eric Burger, Georgetown University

Jason Keirstead, IBM

Paul Martini, iboss, Inc.

Jerome Athias, Individual

Terry MacDonald, Individual

Alex Pinto, Individual

Patrick Maroney, Integrated Networking Technologies, Inc.

Wouter Bolsterlee, Intelworks BV

Joep Gommers, Intelworks BV

Sergey Polzunov, Intelworks BV

Rutger Prins, Intelworks BV

Andrei Sîrghi, Intelworks BV

Raymon van der Velde, Intelworks BV

Jonathan Baker, MITRE Corporation

Sean Barnum, MITRE Corporation

Mark Davidson, MITRE Corporation

Ivan Kirillov, MITRE Corporation

Jon Salwen, MITRE Corporation

John Wunder, MITRE Corporation

Mike Boyle, National Security Agency

Jessica Fitzgerald-McKay, National Security Agency

Takahiro Kakumaru, NEC Corporation

John-Mark Gurney, New Context Services, Inc.

Christian Hunt, New Context Services, Inc.

Daniel Riedel, New Context Services, Inc.

Andrew Storms, New Context Services, Inc.

John Tolbert, Queralt, Inc.

Igor Baikalov, Securonix

Bernd Grobauer, Siemens AG

Jonathan Bush, Soltra

Aharon Chernin, Soltra

Trey Darley, Soltra

Paul Dion, Soltra

Ali Khan, Soltra

Natalie Suarez, Soltra

Cedric LeRoux, Splunk Inc.

Brian Luger, Splunk Inc.

Crystal Hayes, The Boeing Company

Brad Butts, U.S. Bank

Mona Magathan, U.S. Bank

Adam Cooper, United Kingdom Cabinet Office

Mike McLellan, United Kingdom Cabinet Office

Chris O'Brien, United Kingdom Cabinet Office

Julian White, United Kingdom Cabinet Office

Anthony Rutkowski, Yaana Technologies, LLC

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

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| wd01 | 21 August 2015 | Sean Barnum Desiree Beck Aharon Chernin Rich Piazza | Initial transfer to OASIS template |

1. The CybOX Observable data model is actually defined in the [CybOX Language](#RelatedWork), not in STIX. [↑](#endnote-ref-1)
2. The type of the amount property is suggested, not normative. [↑](#endnote-ref-2)
3. The type of the iso\_currency\_code property is suggested, not normative. [↑](#endnote-ref-3)
4. The type of the priority property is suggested, not normative. [↑](#endnote-ref-4)