CybOX Version 2.1.1 Part 1: Overview

Working Draft 01

28 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:

Trey Darley ([trey@soltra.com](mailto:trey@soltra.com)), [Soltra](http://www.soltra.com/)

Ivan Kirillov ([ikirillov@mitre.org](mailto:ikirillov@mitre.org)), [MITRE Corporation](http://www.mitre.org/)

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

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

Additional artifacts:

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

* *CybOX Version 2.1.1 Part 1: Overview*. (this document)
* *CybOX Version 2.1.1 Part 2: Common*. [URI]
* *CybOX Version 2.1.1 Part 3: Core*. [URI]
* *CybOX Version 2.1.1 Part 4: Default Extensions*. [URI]
* *CybOX Version 2.1.1 Part 5: Default Vocabularies*. [URI]
* *CybOX Version 2.1.1 Part 6: UML Model*. [URI]
* *CybOX Version 2.1.1 Part 7: API Object*. [URI]
* *CybOX Version 2.1.1 Part 8: ARP Cache Object*. [URI]
* *CybOX Version 2.1.1 Part 9: AS Object*. [URI]
* *CybOX Version 2.1.1 Part 10: Account Object*. [URI]
* *CybOX Version 2.1.1 Part 11: Address Object*. [URI]
* *CybOX Version 2.1.1 Part 12: Archive File Object*. [URI]
* *CybOX Version 2.1.1 Part 13: Artifact Object*. [URI]
* *CybOX Version 2.1.1 Part 14: Code Object*. [URI]
* *CybOX Version 2.1.1 Part 15: Custom Object*. [URI]
* *CybOX Version 2.1.1 Part 16: DNS Cache Object*. [URI]
* *CybOX Version 2.1.1 Part 17: DNS Query Object*. [URI]
* *CybOX Version 2.1.1 Part 18: DNS Record Object*. [URI]
* *CybOX Version 2.1.1 Part 19: Device Object*. [URI]
* *CybOX Version 2.1.1 Part 20: Disk Object*. [URI]
* *CybOX Version 2.1.1 Part 21: Disk Partition Object*. [URI]
* *CybOX Version 2.1.1 Part 22: Domain Name Object*. [URI]
* *CybOX Version 2.1.1 Part 23: Email Message Object*. [URI]
* *CybOX Version 2.1.1 Part 24: File Object*. [URI]
* *CybOX Version 2.1.1 Part 25: GUI Dialogbox Object*. [URI]
* *CybOX Version 2.1.1 Part 26: GUI Object*. [URI]
* *CybOX Version 2.1.1 Part 27: GUI Window Object*. [URI]
* *CybOX Version 2.1.1 Part 28: HTTP Session Object*. [URI]
* *CybOX Version 2.1.1 Part 29: Hostname Session Object*. [URI]
* *CybOX Version 2.1.1 Part 30: Image File Object*. [URI]
* *CybOX Version 2.1.1 Part 31: Library File Object*. [URI]
* *CybOX Version 2.1.1 Part 32: Link Object*. [URI]
* *CybOX Version 2.1.1 Part 33: Linux Package Object*. [URI]
* *CybOX Version 2.1.1 Part 34: Memory Object*. [URI]
* *CybOX Version 2.1.1 Part 35: Mutex Object*. [URI]
* *CybOX Version 2.1.1 Part 36: Network Connection Object*. [URI]
* *CybOX Version 2.1.1 Part 37: Network Flow Object*. [URI]
* *CybOX Version 2.1.1 Part 38: Network Packet Object*. [URI]
* *CybOX Version 2.1.1 Part 39: Network Route Entry Object*. [URI]
* *CybOX Version 2.1.1 Part 40: Network Route Object*. [URI]
* *CybOX Version 2.1.1 Part 41: Network Socket Object*. [URI]
* *CybOX Version 2.1.1 Part 42: Network Subnet Object*. [URI]
* *CybOX Version 2.1.1 Part 43: PDF File Object*. [URI]
* *CybOX Version 2.1.1 Part 44: Pipe Object*. [URI]
* *CybOX Version 2.1.1 Part 45: Port Object*. [URI]
* *CybOX Version 2.1.1 Part 46: Process Object*. [URI]
* *CybOX Version 2.1.1 Part 47: Product Object*. [URI]
* *CybOX Version 2.1.1 Part 48: SMS Message Object*. [URI]
* *CybOX Version 2.1.1 Part 49: Semaphore Object*. [URI]
* *CybOX Version 2.1.1 Part 50: Socket Address Object*. [URI]
* *CybOX Version 2.1.1 Part 51: System Object*. [URI]
* *CybOX Version 2.1.1 Part 52: URI Object*. [URI]
* *CybOX Version 2.1.1 Part 53: URL History Object*. [URI]
* *CybOX Version 2.1.1 Part 54: Unix File Object*. [URI]
* *CybOX Version 2.1.1 Part 55: Unix Network Route Entry Object*. [URI]
* *CybOX Version 2.1.1 Part 56: Unix Pipe Object*. [URI]
* *CybOX Version 2.1.1 Part 57: Unix Process Object*. [URI]
* *CybOX Version 2.1.1 Part 58: Unix User Account Object*. [URI]
* *CybOX Version 2.1.1 Part 59: Unix Volume Object*. [URI]
* *CybOX Version 2.1.1 Part 60: Unix Account Object*. [URI]
* *CybOX Version 2.1.1 Part 61: User Session Object*. [URI]
* *CybOX Version 2.1.1 Part 62: Volume Object*. [URI]
* *CybOX Version 2.1.1 Part 63: Whois Object*. [URI]
* *CybOX Version 2.1.1 Part 64: Win Computer Account Object*. [URI]
* *CybOX Version 2.1.1 Part 65: Win Critical Section Object*. [URI]
* *CybOX Version 2.1.1 Part 66: Win Driver Object*. [URI]
* *CybOX Version 2.1.1 Part 67: Win Event Log Object*. [URI]
* *CybOX Version 2.1.1 Part 68: Win Event Object*. [URI]
* *CybOX Version 2.1.1 Part 69: Win Executable File Object*. [URI]
* *CybOX Version 2.1.1 Part 70: Win File Object*. [URI]
* *CybOX Version 2.1.1 Part 71: Win Filemapping Object*. [URI]
* *CybOX Version 2.1.1 Part 72: Win Handle Object*. [URI]
* *CybOX Version 2.1.1 Part 73: Win Hook Object*. [URI]
* *CybOX Version 2.1.1 Part 74: Win Kernel Hook Object*. [URI]
* *CybOX Version 2.1.1 Part 75: Win Kernel Object*. [URI]
* *CybOX Version 2.1.1 Part 76: Win Mailslot Object*. [URI]
* *CybOX Version 2.1.1 Part 77: Win Memory Page Region Object*. [URI]
* *CybOX Version 2.1.1 Part 78: Win Mutex Object*. [URI]
* *CybOX Version 2.1.1 Part 79: Win Network Route Entry Object*. [URI]
* *CybOX Version 2.1.1 Part 80: Win Network Share Object*. [URI]
* *CybOX Version 2.1.1 Part 81: Win Pipe Object*. [URI]
* *CybOX Version 2.1.1 Part 82: Win Prefetch Object*. [URI]
* *CybOX Version 2.1.1 Part 83: Win Process Object*. [URI]
* *CybOX Version 2.1.1 Part 84: Win Registry Key Object*. [URI]
* *CybOX Version 2.1.1 Part 85: Win Semaphore Object*. [URI]
* *CybOX Version 2.1.1 Part 86: Win Service Object*. [URI]
* *CybOX Version 2.1.1 Part 87: Win System Object*. [URI]
* *CybOX Version 2.1.1 Part 88: Win System Restore Object*. [URI]
* *CybOX Version 2.1.1 Part 89: Win Task Object*. [URI]
* *CybOX Version 2.1.1 Part 90: Win Thread Object*. [URI]
* *CybOX Version 2.1.1 Part 91: Win User Account Object*. [URI]
* *CybOX Version 2.1.1 Part 92: Win Volume Object*. [URI]
* *CybOX Version 2.1.1 Part 93: Win Waitable Timer Object*. [URI]
* *CybOX Version 2.1.1 Part 94: X509 Certificate Object*. [URI]

Related work:

This specification is related to:

* *STIX Version 1.2.1 (placeholder)*

Abstract:

The Cyber Observable Expression (CybOX) is a standardized language for encoding and communicating high-fidelity information about cyber observables, whether dynamic events or stateful measures that are observable in the operational cyber domain. By specifying a common structured schematic mechanism for these cyber observables, the intent is to enable the potential for detailed automatable sharing, mapping, detection and analysis heuristics. This document serves as an overview of those specifications and defines how they are used within the broader CybOX framework.

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/part9-coa/stix-v1.2.1-csd01-part9-coa.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part9-coa.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 4](#_Toc409437255)

[1.1 Terminology 4](#_Toc409437256)

[1.2 Normative References 4](#_Toc409437257)

[1.3 Non-Normative References 4](#_Toc409437258)

[2 Section Title 5](#_Toc409437259)

[2.1 Level 2 section title 5](#_Toc409437260)

[2.1.1 Level 3 section title 5](#_Toc409437261)

[2.1.1.1 Level 4 section title is usually deepest for Table of Contents 5](#_Toc409437262)

[3 # Conformance 6](#_Toc409437263)

[Appendix A. Acknowledgments 7](#_Toc409437264)

[Appendix B. Example Title 8](#_Toc409437265)

[B.1 Subsidiary section 8](#_Toc409437266)

[B.1.1 Sub-subsidiary section 8](#_Toc409437267)

[B.1.1.1 Sub-sub-subsidiary section 8](#_Toc409437268)

[Appendix C. Revision History 9](#_Toc409437269)

# Introduction

[All text is normative unless otherwise labeled]

The Cyber Observable Expression (CybOX) provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security. CybOX improves the consistency, efficiency, and interoperability of deployed tools and processes, and it increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics.

This document serves as the specification for the CybOX Core Version 2.1.1 data model, which is one of two fundamental data models for CybOX content.

In Section **1.1** we discuss additional specification documents, in Section **1.2** we provide document conventions in, and in Section **1.3** we provide terminology. References are given in Sections **1.4** and **1.5**. In Section **2**, we give background information necessary to fully understand the Core data model. We present the Core data model specification details in Section **3** and conformance information in Section **4**.

## CybOX Specification Documents

The CybOX 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 CybOX UML model.

CybOX has a modular design comprising two fundamental data models and a collection of Object data models. The fundamental data models – CybOX Core and CybOX Common – provide essential CybOX structure and functionality. The CybOX Objects, defined in individual data models, are precise characterizations of particular types of observable cyber entities (e.g., HTTP session, Windows registry key, DNS query).

Use of the CybOX Core and Common data models is required; however, use of the CybOX Object data models is purely optional: users select and use only those Objects and corresponding data models that are needed. Importing the entire [CybOX suite of data models](#AdditionalArtifacts) is not necessary.

The [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts) document provides a comprehensive overview of the full set of CybOX data models, which in addition to the Core, Common, and numerous Object data models, includes a set of default controlled vocabularies. [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts) also summarizes the relationship of CybOX to other externally defined data models, and outlines general CybOX data model conventions.

## 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 CybOX high level concepts, which are defined in [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts).

Examples: Action, Object, Event, Property

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

Examples: ActionType, cyboxCommon:BaseObjectPropertyType

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

* The ‘*italic’* font (withsingle quotes) is used for noting actual, explicit values for CybOX Language properties. The *italic* font (without quotes) is used for noting example values.

Example:  *‘HashNameVocab-1.0,’ high, medium, low*

### UML Package References

Each CybOX data model is captured in a different UML package (e.g., Core package) where the packages together compose the full [CybOX UML model](#AdditionalArtifacts). 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. [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts)contains the full list of CybOX packages, along with the associated prefix notations, descriptions, and examples.

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

### UML Diagrams

This specification makes use of UML diagrams to visually depict relationships between CybOX Language constructs. Note that the diagrams have been extracted directly from the full UML model for CybOX; 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 CybOX 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 a 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** |
| 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 Core specification are illustrated via exemplars in **Figure 1‑1**.

[need diagram]

Figure 1‑1. Data model color coding

### 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 Core 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 CybOX is described using the format, “The X property verbY.” For example, in the specification for the CybOX Core data model, we write, “The id property specifies a globally unique identifier for the Action.” 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 CybOX.

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

|  |  |
| --- | --- |
| **Verb** | **CybOX 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 Observable\_Source property characterizes the source of the Observable information. Examples of details captured include identifying characteristics, time-related attributes, and a list of the tools used to collect the information.  The Description property captures a textual description of the Action. |
| 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 Action property characterizes a cyber observable Action.  The Obfuscation\_Technique property characterizes a technique an attacker could potentially leverage to obfuscate the Observable. |
| 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 cybox\_major\_version property specifies the major version of the CybOX language used for the set of Observables. |

## 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>.

## Non-Normative References

# Background Information

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

## Cyber Observables

A cyber observable is a dynamic event or a stateful property that occurs, or may occur, in the operational cyber domain. Examples of stateful properties include the value of a registry key, the MD5 hash of a file, and an IP address. Examples of events include the deletion of a file, the receipt of an HTTP GET request, and the creation of a remote thread.

A cyber observable is different than a cyber indicator. A cyber observable is a statement of fact, capturing what was observed or could be observed in the cyber operational domain. Cyber indicators are cyber observable patterns, such as a registry key value associated with a known bad actor or a spoofed email address used on a particular date.

## Objects

Objects in CybOX are individual data models for characterizing a particular cyber entity, such as a Windows registry key, or an Email Message, for example. Accordingly, each release of the CybOX language includes a particular set of Objects that are part of the release. The data model for each of these Objects is defined by its own specification that describes the context-specific classes and properties that comprise the Object.

# CybOX Core Data Model

# Conformance

Implementations have discretion over which parts (components, properties, extensions, controlled vocabularies, etc.) of CybOX they implement (e.g., Observable/Object).

[1] Conformant implementations must conform to all normative structural specifications of the UML model or additional normative statements within this document that apply to the portions of CybOX they implement (e.g., Implementers of the entire Observable class must conform to all normative structural specifications of the UML model regarding the Observable class or additional normative statements contained in the document that describes the Observable class).

[2] Conformant implementations are free to ignore normative structural specifications of the UML model or additional normative statements within this document that do not apply to the portions of CybOX they implement (e.g., Non-implementers of any particular properties of the Observable class are free to ignore all normative structural specifications of the UML model regarding those properties of the Observable class or additional normative statements contained in the document that describes the Observable class).

The conformance section of this document is intentionally broad and attempts to reiterate what already exists in this document.

1. Acknowledgments

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

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| wd01 | 28 August 2015 | Desiree Beck Trey Darley Ivan Kirillov Rich Piazza | Initial transfer to OASIS template |