CybOXTM Version 2.1.1 Part 89: Win Task Object

Working Draft 01

15 December 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:

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

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:ikirillov@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 01: Overview*. [URI]
* *CybOX™ Version 2.1.1 Part 02: Common*. [URI]
* *CybOX™ Version 2.1.1 Part 03: Core*. [URI]
* *CybOX™ Version 2.1.1 Part 04: Default Extensions*. [URI]
* *CybOX™ Version 2.1.1 Part 05: Default Vocabularies*. [URI]
* *CybOX™ Version 2.1.1 Part 06: UML Model*. [URI]
* *CybOX™ Version 2.1.1 Part 07: API Object*. [URI]
* *CybOX™ Version 2.1.1 Part 08: ARP Cache Object*. [URI]
* *CybOX™ Version 2.1.1 Part 09: AS Object*. [URI]
* *CybOXTM Version 2.1.1 Part 10: Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 11: Address Object*. [URI]
* *CybOXTM Version 2.1.1 Part 12: Archive File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 13: Artifact Object*. [URI]
* *CybOXTM Version 2.1.1 Part 14: Code Object*. [URI]
* *CybOXTM Version 2.1.1 Part 15: Custom Object*. [URI]
* *CybOXTM Version 2.1.1 Part 16: DNS Cache Object*. [URI]
* *CybOXTM Version 2.1.1 Part 17: DNS Query Object*. [URI]
* *CybOXTM Version 2.1.1 Part 18: DNS Record Object*. [URI]
* *CybOXTM Version 2.1.1 Part 19: Device Object*. [URI]
* *CybOXTM Version 2.1.1 Part 20: Disk Object*. [URI]
* *CybOXTM Version 2.1.1 Part 21: Disk Partition Object*. [URI]
* *CybOXTM Version 2.1.1 Part 22: Domain Name Object*. [URI]
* *CybOXTM Version 2.1.1 Part 23: Email Message Object*. [URI]
* *CybOXTM Version 2.1.1 Part 24: File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 25: GUI Dialogbox Object*. [URI]
* *CybOXTM Version 2.1.1 Part 26: GUI Object*. [URI]
* *CybOXTM Version 2.1.1 Part 27: GUI Window Object*. [URI]
* *CybOXTM Version 2.1.1 Part 28: HTTP Session Object*. [URI]
* *CybOXTM Version 2.1.1 Part 29: Hostname Object*. [URI]
* *CybOXTM Version 2.1.1 Part 30: Image File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 31: Library File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 32: Link Object*. [URI]
* *CybOXTM Version 2.1.1 Part 33: Linux Package Object*. [URI]
* *CybOXTM Version 2.1.1 Part 34: Memory Object*. [URI]
* *CybOXTM Version 2.1.1 Part 35: Mutex Object*. [URI]
* *CybOXTM Version 2.1.1 Part 36: Network Connection Object*. [URI]
* *CybOXTM Version 2.1.1 Part 37: Network Flow Object*. [URI]
* *CybOXTM Version 2.1.1 Part 38: Network Packet Object*. [URI]
* *CybOXTM Version 2.1.1 Part 39: Network Route Entry Object*. [URI]
* *CybOXTM Version 2.1.1 Part 40: Network Route Object*. [URI]
* *CybOXTM Version 2.1.1 Part 41: Network Socket Object*. [URI]
* *CybOXTM Version 2.1.1 Part 42: Network Subnet Object*. [URI]
* *CybOXTM Version 2.1.1 Part 43: PDF File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 44: Pipe Object*. [URI]
* *CybOXTM Version 2.1.1 Part 45: Port Object*. [URI]
* *CybOXTM Version 2.1.1 Part 46: Process Object*. [URI]
* *CybOXTM Version 2.1.1 Part 47: Product Object*. [URI]
* *CybOXTM Version 2.1.1 Part 48: SMS Message Object*. [URI]
* *CybOXTM Version 2.1.1 Part 49: Semaphore Object*. [URI]
* *CybOXTM Version 2.1.1 Part 50: Socket Address Object*. [URI]
* *CybOXTM Version 2.1.1 Part 51: System Object*. [URI]
* *CybOXTM Version 2.1.1 Part 52: URI Object*. [URI]
* *CybOXTM Version 2.1.1 Part 53: URL History Object*. [URI]
* *CybOXTM Version 2.1.1 Part 54: Unix File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 55: Unix Network Route Entry Object*. [URI]
* *CybOXTM Version 2.1.1 Part 56: Unix Pipe Object*. [URI]
* *CybOXTM Version 2.1.1 Part 57: Unix Process Object*. [URI]
* *CybOXTM Version 2.1.1 Part 58: Unix User Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 59: Unix Volume Object*. [URI]
* *CybOXTM Version 2.1.1 Part 60: User Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 61: User Session Object*. [URI]
* *CybOXTM Version 2.1.1 Part 62: Volume Object*. [URI]
* *CybOXTM Version 2.1.1 Part 63: Whois Object*. [URI]
* *CybOXTM Version 2.1.1 Part 64: Win Computer Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 65: Win Critical Section Object*. [URI]
* *CybOXTM Version 2.1.1 Part 66: Win Driver Object*. [URI]
* *CybOXTM Version 2.1.1 Part 67: Win Event Log Object*. [URI]
* *CybOXTM Version 2.1.1 Part 68: Win Event Object*. [URI]
* *CybOXTM Version 2.1.1 Part 69: Win Executable File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 70: Win File Object*. [URI]
* *CybOXTM Version 2.1.1 Part 71: Win Filemapping Object*. [URI]
* *CybOXTM Version 2.1.1 Part 72: Win Handle Object*. [URI]
* *CybOXTM Version 2.1.1 Part 73: Win Hook Object*. [URI]
* *CybOXTM Version 2.1.1 Part 74: Win Kernel Hook Object*. [URI]
* *CybOXTM Version 2.1.1 Part 75: Win Kernel Object*. [URI]
* *CybOXTM Version 2.1.1 Part 76: Win Mailslot Object*. [URI]
* *CybOXTM Version 2.1.1 Part 77: Win Memory Page Region Object*. [URI]
* *CybOXTM Version 2.1.1 Part 78: Win Mutex Object*. [URI]
* *CybOXTM Version 2.1.1 Part 79: Win Network Route Entry Object*. [URI]
* *CybOXTM Version 2.1.1 Part 80: Win Network Share Object*. [URI]
* *CybOXTM Version 2.1.1 Part 81: Win Pipe Object*. [URI]
* *CybOXTM Version 2.1.1 Part 82: Win Prefetch Object*. [URI]
* *CybOXTM Version 2.1.1 Part 83: Win Process Object*. [URI]
* *CybOXTM Version 2.1.1 Part 84: Win Registry Key Object*. [URI]
* *CybOXTM Version 2.1.1 Part 85: Win Semaphore Object*. [URI]
* *CybOXTM Version 2.1.1 Part 86: Win Service Object*. [URI]
* *CybOXTM Version 2.1.1 Part 87: Win System Object*. [URI]
* *CybOXTM Version 2.1.1 Part 88: Win System Restore Object*. [URI]
* *CybOXTM Version 2.1.1 Part 89: Win Task Object*. (this document)
* *CybOXTM Version 2.1.1 Part 90: Win Thread Object*. [URI]
* *CybOXTM Version 2.1.1 Part 91: Win User Account Object*. [URI]
* *CybOXTM Version 2.1.1 Part 92: Win Volume Object*. [URI]
* *CybOXTM Version 2.1.1 Part 93: Win Waitable Timer Object*. [URI]
* *CybOXTM Version 2.1.1 Part 94: X509 Certificate Object*. [URI]

Related work:

This specification is related to:

* *STIXTM 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 specification document defines the Win Task Object data model, which is one of the Object data models for CybOX content.

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/part1-overview/stix-v1.2.1-csd01-part1-overview.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part1-overview.docx

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

Copyright © OASIS Open 2016. 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.

Portions copyright © United States Government 2012-2016.  All Rights Reserved.  
  
STIX™, TAXII™, AND CybOX™ (STANDARD OR STANDARDS) AND THEIR COMPONENT PARTS ARE PROVIDED “AS IS” WITHOUT ANY WARRANTY OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY THAT THESE STANDARDS OR ANY OF THEIR COMPONENT PARTS WILL CONFORM TO SPECIFICATIONS, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR FREEDOM FROM INFRINGEMENT, ANY WARRANTY THAT THE STANDARDS OR THEIR COMPONENT PARTS WILL BE ERROR FREE, OR ANY WARRANTY THAT THE DOCUMENTATION, IF PROVIDED, WILL CONFORM TO THE STANDARDS OR THEIR COMPONENT PARTS. IN NO EVENT SHALL THE UNITED STATES GOVERNMENT OR ITS CONTRACTORS OR SUBCONTRACTORS BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF, RESULTING FROM, OR IN ANY WAY CONNECTED WITH THESE STANDARDS OR THEIR COMPONENT PARTS OR ANY PROVIDED DOCUMENTATION, WHETHER OR NOT BASED UPON WARRANTY, CONTRACT, TORT, OR OTHERWISE, WHETHER OR NOT INJURY WAS SUSTAINED BY PERSONS OR PROPERTY OR OTHERWISE, AND WHETHER OR NOT LOSS WAS SUSTAINED FROM, OR AROSE OUT OF THE RESULTS OF, OR USE OF, THE STANDARDS, THEIR COMPONENT PARTS, AND ANY PROVIDED DOCUMENTATION. THE UNITED STATES GOVERNMENT DISCLAIMS ALL WARRANTIES AND LIABILITIES REGARDING THE STANDARDS OR THEIR COMPONENT PARTS ATTRIBUTABLE TO ANY THIRD PARTY, IF PRESENT IN THE STANDARDS OR THEIR COMPONENT PARTS AND DISTRIBUTES IT OR THEM “AS IS.”

Table of Contents

[1 Introduction 6](#_Toc450042995)

[1.1 CybOXTM Specification Documents 6](#_Toc450042996)

[1.2 Document Conventions 6](#_Toc450042997)

[1.2.1 Fonts 6](#_Toc450042998)

[1.2.2 UML Package References 7](#_Toc450042999)

[1.2.3 UML Diagrams 7](#_Toc450043000)

[1.2.3.1 Class Properties 7](#_Toc450043001)

[1.2.3.2 Diagram Icons and Arrow Types 7](#_Toc450043002)

[1.2.4 Property Table Notation 8](#_Toc450043003)

[1.2.5 Property and Class Descriptions 8](#_Toc450043004)

[1.3 Terminology 9](#_Toc450043005)

[1.4 Normative References 9](#_Toc450043006)

[2 Background Information 10](#_Toc450043007)

[2.1 Cyber Observables 10](#_Toc450043008)

[2.2 Objects 10](#_Toc450043009)

[3 Data Model 11](#_Toc450043010)

[3.1 WindowsTaskObjectType Class 11](#_Toc450043011)

[3.2 TriggerListType Class 15](#_Toc450043012)

[3.3 TriggerType Class 15](#_Toc450043013)

[3.4 TaskActionListType Class 16](#_Toc450043014)

[3.5 TaskActionType Class 17](#_Toc450043015)

[3.6 IComHandlerActionType Class 18](#_Toc450043016)

[3.7 IExecActionType Class 18](#_Toc450043017)

[3.8 IShowMessageActionType Class 19](#_Toc450043018)

[3.9 TaskActionTypeType Data Type 19](#_Toc450043019)

[3.10 TaskFlagType Data Type 19](#_Toc450043020)

[3.11 TaskPriorityType Data Type 20](#_Toc450043021)

[3.12 TaskTriggerFrequencyType Data Type 20](#_Toc450043022)

[3.13 TaskTriggerType Data Type 20](#_Toc450043023)

[3.14 TaskStatusType Date Type 20](#_Toc450043024)

[3.15 TaskActionTypeEnum Enumeration 20](#_Toc450043025)

[3.16 TaskPriorityEnum Enumeration 21](#_Toc450043026)

[3.17 TriggerFrequencyEnum Enumeration 21](#_Toc450043027)

[3.18 TriggerTypeEnum Enumeration 22](#_Toc450043028)

[3.19 TaskStatusEnum Enumeration 23](#_Toc450043029)

[4 Conformance 25](#_Toc450043030)

[Appendix A. Acknowledgments 26](#_Toc450043031)

[Appendix B. Revision History 27](#_Toc450043032)

# Introduction

[All text is normative unless otherwise labeled]

The Cyber Observable Expression (CybOXTM) 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 Win Task Object Version 2.1.1 data model, which is one of eighty-eight CybOX Object data models.

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 necessary to fully understand the Win Task Object data model. We present the Win Task Object data model specification details in Section **3** and conformance information in Section **4**.

## CybOXTM 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 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 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. In addition to the Core, Common, and numerous Object data models, the full set of CybOX data models includes various extension data models and a vocabularies data model, which contains a set of default controlled vocabularies. [*CybOX Version 2.1.1 Part 1: Overview*](#AdditionalArtifacts) also summarizes the relationship of CybOX to other languages, and outlines general CybOX data model conventions.

## Document Conventions

The following sections describe the conventions 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. To refer to a particular class of a specific package, we use the format package\_prefix:class, where package\_prefix corresponds to the appropriate UML package.

The package\_prefix for the Windows Task data model is WinTaskObj. Note that in this specification document, we do not explicitly specify the package prefix for any classes that originate from the Win Task Object 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.

#### 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 ‑. UML diagram icons

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

### 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 Win Task Object 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.

### 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 preferred 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>.

# Background Information

In this section, we provide high level information about the Win Task Object 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

Cyber observable objects (Files, IP Addresses, etc) in CybOX are characterized with a combination of two levels of data models.

The first level is the Object data model which specifies a base set of properties universal to all types of Objects and enables them to integrate with the overall cyber observable framework specified in the CybOX Core data model.

The second level are the object property models which specify the properties of a particular type of Object via individual data models each focused on a particular cyber entity, such as a Windows registry key, or an Email Message. 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 compose the Object.

Any specific instance of an Object is represented utilizing the particular object properties data model within the general Object data model.

# Data Model

## WindowsTaskObjectType Class

The WindowsTaskObjectType class is intended to characterize Windows task scheduler tasks. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381311(v=vs.85).aspx>. The UML diagram corresponding to the WindowsTaskObjectType class is shown in **Figure 3‑1**.

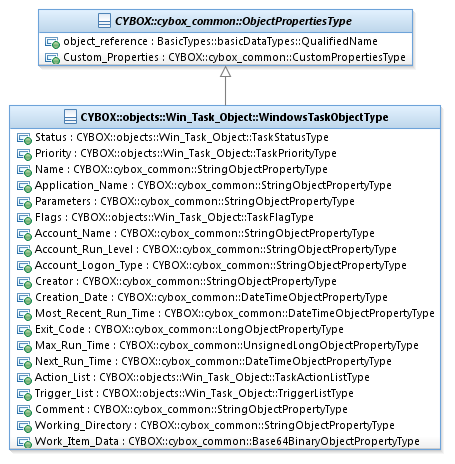


Figure ‑. UML diagram of the WindowsTaskObjectType class

The property table of the WindowsTaskObjectType class is given in **Table 3‑1**.

Table ‑. Properties of the WindowsTaskObjectType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Status** | TaskStatusType | 0..1 | The Status property specifies the current status of the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381263(v=vs.85).aspx>. |
| **Priority** | TaskPriorityType | 0..1 | The Priority property specifies the priority of the scheduled task. This can either be a free-form string or one the values in the TaskPriorityEnum enumeration. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381876(v=vs.85).aspx>. |
| **Name** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Name property specifies the image name for the task. |
| **Application\_Name** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Application\_Name property specifies the application name associated with the task. |
| **Parameters** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Parameters property specifies the command line parameters used to launch the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381875(v=vs.85).aspx>. |
| **Flags** | TaskFlagType | 0..1 | The Flags property specifies any flags that modify the behavior of the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381248(v=vs.85).aspx>. |
| **Account\_Name** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Account\_Name property specifies the name of the account used to run the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381228(v=vs.85).aspx>. |
| **Account\_Run\_Level** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Account\_Run\_Level property specifies the permission level of the account that the task will be run at. |
| **Account\_Logon\_Type** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Account\_Logon\_Type property specifies the security logon method required to run the tasks associated with the account. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa383013(v=vs.85).aspx>. |
| **Creator** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Creator property specifies the name of the creator of the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381235(v=vs.85).aspx>. |
| **Creation\_Date** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Creation\_Date property specifies the date and time that the task was registered. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa382623(v=vs.85).aspx>. |
| **Most\_Recent\_Run\_Time** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Most\_Recent\_Run\_Time property specifies the most recent run date/time of this scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381254(v=vs.85).aspx>. |
| **Exit\_Code** | cyboxCommon:  LongObjectPropertyType | 0..1 | The Exit\_Code property specifies the last exit code of the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381245(v=vs.85).aspx>. |
| **Max\_Run\_Time** | cyboxCommon:  UnsignedLongObjectPropertyType | 0..1 | The Max\_Run\_Time property specifies the maximum run time of the scheduled task before terminating, in milliseconds. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381874(v=vs.85).aspx>. |
| **Next\_Run\_Time** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Next\_Run\_Time property specifies the next run date/time of the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381257(v=vs.85).aspx>. |
| **Action\_List** | TaskActionListType | 0..1 | The Action\_List property specifies a list of actions to be performed by the scheduled task. |
| **Trigger\_List** | TriggerListType | 0..1 | The Trigger\_List property specifies a set of triggers used by the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa383264(v=vs.85).aspx>. |
| **Comment** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Comment property specifies a comment for the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381232(v=vs.85).aspx>. |
| **Working\_Directory** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Working\_Directory property specifies the working directory for the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381878(v=vs.85).aspx>. |
| **Work\_Item\_Data** | cyboxCommon:  Base64BinaryObjectPropertyType | 0..1 | The Work\_Item\_Data property specifies application defined data associated with the scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381271(v=vs.85).aspx>. |

## TriggerListType Class

The TriggerListType class specifies a set of triggers associated with the scheduled task.

The property table of the TriggerListType class is given in **Table 3‑2**.

Table ‑. Properties of the TriggerListType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Trigger** | TriggerType | 1..\* | The Trigger property specifies a trigger associated with this scheduled task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381264(v=vs.85).aspx>. |

## TriggerType Class

The TriggerType class characterizes task triggers. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa383868(v=vs.85).aspx>.

The property table of the TriggerType class is given in **Table 3‑3**.

Table ‑. Properties of the TriggerType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **enabled** | basicDataTypes:Boolean | 0..1 | The enabled property specifies whether the trigger is enabled. |
| **Trigger\_Begin** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Trigger\_Begin property specifies the date/time that the trigger is activated. |
| **Trigger\_Delay** | cyboxCommon:  DurationObjectPropertyType | 0..1 | The Trigger\_Delay property specifies the delay that takes place between when the task is registered and when the task is started. |
| **Trigger\_End** | cyboxCommon:  DateTimeObjectPropertyType | 0..1 | The Trigger\_End property specifies the date/time that the trigger is deactivated. |
| **Trigger\_Frequency** | TaskTriggerFrequencyType | 0..1 | The Trigger\_Frequency property specifies the frequency at which the trigger repeats. |
| **Trigger\_Max\_Run\_Time** | cyboxCommon:  DurationObjectPropertyType | 0..1 | The Trigger\_Max\_Run\_Time property specifies the maximum amount of time that the task launched by the trigger is allowed to run. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa383868(v=vs.85).aspx>. |
| **Trigger\_Session\_Change\_Type** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Trigger\_Session\_Change\_Type property specifies the type of Terminal Server session change that would trigger a task launch. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381298(v=vs.85).aspx>. |
| **Trigger\_Type** | TaskTriggerType | 0..1 | The Trigger\_Type property specifies the type of the task trigger. |

## TaskActionListType Class

The TaskActionListType class specifies a list of task actions.

The property table of the TaskActionListType class is given in **Table 3‑4**.

Table ‑. Properties of the TaskActionListType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Action** | TaskActionType | 1..\* | The Action property specifies the work items (actions) performed by a task. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa383549(v=vs.85).aspx>. |

## TaskActionType Class

The TaskActionType class characterizes scheduled task actions.

The property table of the TaskActionType class is given in **Table 3‑5**.

Table ‑. Properties of the TaskActionType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Action\_Type** | TaskActionTypeType | 0..1 | The Action\_Type property specifies the type of the action. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa380596(v=vs.85).aspx>. |
| **Action\_ID** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Action\_ID property specifies the user-defined identifier for the action. This identifier is used by the Task Scheduler for logging purposes. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa380590(v=vs.85).aspx>. |
| **IEmailAction** | EmailMessageObj:  EmailMessageObjectType | 0..1 | The IEmail\_Action property specifies an action that sends an e-mail, which in this context refers to actual email message sent. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa380693(v=vs.85).aspx>. |
| **IComHandlerAction** | IComHandlerActionType | 0..1 | The IComHandlerAction property specifies an action that fires a handler. |
| **IExecAction** | IExecActionType | 0..1 | The IExecAction property specifies an action that executes a command-line operation. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa380715(v=vs.85).aspx>. |
| **IShowMessageAction** | IShowMessageActionType | 0..1 | The IShowMessageAction property specifies an action that shows a message box when a task is activated. See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381302(v=vs.85).aspx>. |

## IComHandlerActionType Class

The IComHandlerActionType class characterizes IComHandler actions.

See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa380613(v=vs.85).aspx>.

The property table of the IComHandlerActionType class is given in **Table 3‑6**.

Table ‑. Properties of the IComHandlerActionType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **COM\_Data** | cyboxCommon:  StringObjectPropertyType | 0..1 | The COM\_Data property specifies the data associated with the COM handler. |
| **COM\_Class\_ID** | cyboxCommon:  StringObjectPropertyType | 0..1 | The COM\_Class\_ID property specifies the ID of the COM action. |

## IExecActionType Class

The IExecActionType class characterizes IExec actions.

See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa380715(v=vs.85).aspx>

The property table of the IExecActionType class is given in **Table 3‑7**.

Table ‑. Properties of the IExecActionType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Exec\_Arguments** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Exec\_Arguments property specifies the arguments associated with the command-line operation launched by the action. |
| **Exec\_Program\_Path** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Exec\_Program\_Path property specifies the path to the executable file launched by the action. |
| **Exec\_Working\_Directory** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Exec\_Working\_Directory property specifies the directory that contains either the executable file or the files that are used by the executable file launched by the action. |
| **Exec\_Program\_Hashes** | cyboxCommon:HashListType | 0..1 | The Exec\_Program\_Hashes property specifies the hashes of the executable file launched by the action. |

## IShowMessageActionType Class

The IShowMessageActionType class characterizes IShowMessage actions.

See also: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa381302(v=vs.85).aspx>.

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

Table ‑. Properties of the IShowMessageActionType class

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Multiplicity** | **Description** |
| **Show\_Message\_Body** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Show\_Message\_Body property specifies the message text that is displayed in the body of the message box by the action. |
| **Show\_Message\_Title** | cyboxCommon:  StringObjectPropertyType | 0..1 | The Show\_Message\_Title property specifies the title of the message box shown by the action. |

## TaskActionTypeType Data Type

The TaskActionTypeType data type characterizes the specific type of task action. Its core value SHOULD be a literal from the TaskActionTypeEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e., regular-expression based) specifications.

## TaskFlagType Data Type

The TaskFlagType data type specifies the Windows Task flag type. Its core value SHOULD be a literal from the TaskFlagEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e., regular-expression based) specifications.

## TaskPriorityType Data Type

The TaskPriorityType data type specifies the Windows Task priority type. Its core value SHOULD be a literal from the TaskPriorityEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e., regular-expression based) specifications.

## TaskTriggerFrequencyType Data Type

The TaskTriggerFrequencyType data type specifies the Windows Task trigger frequency type. Its core value SHOULD be a literal from the TriggerFrequencyEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e., regular-expression based) specifications.

## TaskTriggerType Data Type

The TaskTriggerType data type specifies the Windows Task trigger type. Its core value SHOULD be a literal from the TriggerTypeEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e., regular-expression based) specifications.

## TaskStatusType Date Type

The TaskStatusType data type specifies the Windows Task state. Its core value SHOULD be a literal from the TaskStatusEnum enumeration. It extends the BaseObjectPropertyType data type, in order to permit complex (i.e., regular-expression based) specifications.

## TaskActionTypeEnum Enumeration

The literals of the TaskActionTypeEnum enumeration are given in **Table 3‑9**.

Table ‑. Literals of the TaskActionTypeEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **TASK\_ACTION\_EXEC** | This action performs a command-line operation. For example, the action could run a script, launch an executable, or, if the name of a document is provided, find its associated application and launch the application with the document. |
| **TASK\_ACTION\_COM\_HANDLER** | This action fires a handler. |
| **TASK\_ACTION\_SEND\_EMAIL** | This action sends an e-mail. |
| **TASK\_ACTION\_SHOW\_MESSAGE** | This action shows a message box. |

## TaskPriorityEnum Enumeration

The literals of the TaskPriorityEnum enumeration are given in **Table 3‑10**.

Table ‑. Literals of the TaskPriorityEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **HIGH\_PRIORITY\_CLASS** | A priority class of high (1). |
| **NORMAL\_PRIORITY\_CLASS** | A priority class of normal (4-6). |
| **IDLE\_PRIORITY\_CLASS** | A priority class of idle (9-10). |
| **REALTIME\_PRIORITY\_CLASS** | A priority class of realtime (0). |
| **ABOVE\_NORMAL\_PRIORITY\_CLASS** | A priority class of above normal (2-3). |
| **BELOW\_NORMAL\_PRIORITY\_CLASS** | A priority class of below normal (7-8). |

## TriggerFrequencyEnum Enumeration

The literals of the TriggerFrequencyEnum enumeration are given in **Table 3‑11**.

Also, see <https://msdn.microsoft.com/en-us/library/windows/desktop/aa383620%28v=vs.85%29.aspx>.

Table ‑. Literals of the TriggerFrequencyEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **TASK\_TIME\_TRIGGER\_ONCE** | The trigger is set to run the task a single time. |
| **TASK\_EVENT\_TRIGGER\_ON\_IDLE** | The trigger is set to run the task if the system remains idle for the amount of time specified by the idle wait time of the task. |
| **TASK\_EVENT\_TRIGGER\_AT\_SYSTEMSTART** | The trigger is set to run the task at system startup. |
| **TASK\_EVENT\_TRIGGER\_AT\_LOGON** | The trigger is set to run the task when a user logs on. |
| **TASK\_TIME\_TRIGGER\_DAILY** | The trigger is set to run the task on a daily interval. |
| **TASK\_TIME\_TRIGGER\_WEEKLY** | The trigger is set to run the work item on specific days of a specific week of a specific month. |
| **TASK\_TIME\_TRIGGER\_MONTHLYDATE** | The trigger is set to run the task on a specific day(s) of the month. |
| **TASK\_TIME\_TRIGGER\_MONTHLYDOW** | The trigger is set to run the task on specific days, weeks, and months. |

## TriggerTypeEnum Enumeration

The literals of the TriggerTypeEnum enumeration are given in **Table 3‑12**.

Table ‑. Literals of the TriggerTypeEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **TASK\_TRIGGER\_EVENT** | Triggers the task when a specific system event occurs. |
| **TASK\_TRIGGER\_TIME** | Triggers the task at a specific date and time. |
| **TASK\_TRIGGER\_IDLE** | Triggers the task when the computer enters an idle state. |
| **TASK\_TRIGGER\_REGISTRATION** | Triggers the task when the task is registered or updated. |
| **TASK\_TRIGGER\_BOOT** | Triggers the task when the system is booted. |
| **TASK\_TRIGGER\_LOGON** | Triggers the task when a user logs on. |
| **TASK\_TRIGGER\_SESSION\_STATE\_CHANGE** | Triggers the task when a Terminal Server session changes state. |

## TaskStatusEnum Enumeration

The literals of the TaskStatusEnum enumeration are given in **Table 3‑13**.

Also, see <https://msdn.microsoft.com/en-us/library/windows/desktop/aa383604%28v=vs.85%29.aspx>.

Table ‑. Literals of the TaskStatusEnum enumeration

|  |  |
| --- | --- |
| **Enumeration Literal** | **Description** |
| **SCHED\_S\_TASK\_READY** | The task is ready to run at its next scheduled time. |
| **SCHED\_S\_TASK\_RUNNING** | The task is currently running. |
| **SCHED\_S\_TASK\_NOT\_SCHEDULED** | One or more of the properties that are needed to run this task on a schedule have not been set. |
| **SCHED\_E\_SERVICE\_NOT\_RUNNING** | The Task Scheduler service is not running. |
| **SCHED\_E\_UNSUPPORTED\_ACCOUNT\_OPTION** | The task has been configured with an unsupported combination of account settings and run time options. |
| **SCHED\_E\_UNKNOWN\_OBJECT\_VERSION** | The task object version is either unsupported or invalid. |
| **SCHED\_E\_NO\_SECURITY\_SERVICES** | The Task Scheduler security services are available only on Windows NT. |
| **SCHED\_E\_ACCOUNT\_DBASE\_CORRUPT** | Corruption was detected in the Task Scheduler security database; the database has been reset. |
| **SCHED\_E\_ACCOUNT\_NAME\_NOT\_FOUND** | Unable to establish existence of the account specified. |
| **SCHED\_E\_ACCOUNT\_INFORMATION\_NOT\_SET** | No account information could be found in the Task Scheduler security database for the task indicated. |
| **SCHED\_E\_INVALID\_TASK** | The object either is an invalid task object or is not a task object. |
| **SCHED\_E\_CANNOT\_OPEN\_TASK** | The task object could not be opened. |
| **SCHED\_E\_SERVICE\_NOT\_INSTALLED** | The Task Scheduler service is not installed on this computer. |
| **SCHED\_E\_TASK\_NOT\_RUNNING** | There is no running instance of the task. |
| **SCHED\_E\_TASK\_NOT\_READY** | One or more of the properties required to run this task have not been set. |
| **SCHED\_E\_TRIGGER\_NOT\_FOUND** | A task's trigger is not found. |
| **SCHED\_S\_EVENT\_TRIGGER** | Event triggers do not have set run times. |
| **SCHED\_S\_TASK\_NO\_VALID\_TRIGGERS** | Either the task has no triggers or the existing triggers are disabled or not set. |
| **SCHED\_S\_TASK\_TERMINATED** | The last run of the task was terminated by the user. |
| **SCHED\_S\_TASK\_NO\_MORE\_RUNS** | There are no more runs scheduled for this task. |
| **SCHED\_S\_TASK\_HAS\_NOT\_RUN** | The task has not been run. This value is returned whenever the task has not been run, even if the task is ready to be run at the next scheduled time or the task is a recurring task. |
| **SCHED\_S\_TASK\_DISABLED** | The task will not run at the scheduled times because it has been disabled. |
| **TASK\_STATE\_UNKNOWN** | The state of the task is unknown. |
| **TASK\_STATE\_QUEUED** | Instances of the task are queued. |

# 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:

|  |  |
| --- | --- |
| **Aetna**  David Crawford  **AIT Austrian Institute of Technology**  Roman Fiedler  Florian Skopik  **Australia and New Zealand Banking Group (ANZ Bank)**  Dean Thompson  **Blue Coat Systems, Inc.**  Owen Johnson  Bret Jordan  **Century Link**  Cory Kennedy  **CIRCL**  Alexandre Dulaunoy  Andras Iklody  Raphaël Vinot  **Citrix Systems**  Joey Peloquin  **Dell**  Will Urbanski  Jeff Williams  **DTCC**  Dan Brown  Gordon Hundley  Chris Koutras  **EMC**  Robert Griffin  Jeff Odom  Ravi Sharda  **Financial Services Information Sharing and Analysis Center (FS-ISAC)**  David Eilken  Chris Ricard  **Fortinet Inc.**  Gavin Chow  Kenichi Terashita  **Fujitsu Limited**  Neil Edwards  Frederick Hirsch  Ryusuke Masuoka  Daisuke Murabayashi  **Google Inc.**  Mark Risher  **Hitachi, Ltd.**  Kazuo Noguchi  Akihito Sawada  Masato Terada  **iboss, Inc**.  Paul Martini  **Individual**  Jerome Athias  Peter Brown  Elysa Jones  Sanjiv Kalkar  Bar Lockwood  Terry MacDonald  Alex Pinto  **Intel Corporation**  Tim Casey  Kent Landfield  **JPMorgan Chase Bank, N.A.**  Terrence Driscoll  David Laurance  **LookingGlass**  Allan Thomson  Lee Vorthman  **Mitre Corporation**  Greg Back  Jonathan Baker  Sean Barnum  Desiree Beck  Nicole Gong  Jasen Jacobsen  Ivan Kirillov  Richard Piazza  Jon Salwen  Charles Schmidt  Emmanuelle Vargas-Gonzalez  John Wunder  **National Council of ISACs (NCI)**  Scott Algeier  Denise Anderson  Josh Poster  **NEC Corporation**  Takahiro Kakumaru  **North American Energy Standards Board**  David Darnell  **Object Management Group**  Cory Casanave  **Palo Alto Networks**  Vishaal Hariprasad  **Queralt, Inc**.  John Tolbert  **Resilient Systems, Inc.**  Ted Julian  **Securonix**  Igor Baikalov  **Siemens AG**  Bernd Grobauer  **Soltra**  John Anderson  Aishwarya Asok Kumar  Peter Ayasse  Jeff Beekman  Michael Butt  Cynthia Camacho  Aharon Chernin  Mark Clancy  Brady Cotton  Trey Darley  Mark Davidson  Paul Dion  Daniel Dye  Robert Hutto  Raymond Keckler  Ali Khan  Chris Kiehl  Clayton Long  Michael Pepin  Natalie Suarez  David Waters  Benjamin Yates  **Symantec Corp.**  Curtis Kostrosky  **The Boeing Company**  Crystal Hayes  **ThreatQuotient, Inc.**  Ryan Trost  **U.S. Bank**  Mark Angel  Brad Butts  Brian Fay  Mona Magathan  Yevgen Sautin  **US Department of Defense (DoD)**  James Bohling  Eoghan Casey  Gary Katz  Jeffrey Mates  **VeriSign**  Robert Coderre  Kyle Maxwell  Eric Osterweil | **Airbus Group SAS**  Joerg Eschweiler  Marcos Orallo  **Anomali**  Ryan Clough  Wei Huang  Hugh Njemanze  Katie Pelusi  Aaron Shelmire  Jason Trost  **Bank of America**  Alexander Foley  **Center for Internet Security (CIS)**  Sarah Kelley  **Check Point Software Technologies**  Ron Davidson  **Cisco Systems**  Syam Appala  Ted Bedwell  David McGrew  Pavan Reddy  Omar Santos  Jyoti Verma  **Cyber Threat Intelligence Network, Inc. (CTIN)**  Doug DePeppe  Jane Ginn  Ben Othman  **DHS Office of Cybersecurity and Communications (CS&C)**  Richard Struse  Marlon Taylor  **EclecticIQ**  Marko Dragoljevic  Joep Gommers  Sergey Polzunov  Rutger Prins  Andrei Sîrghi  Raymon van der Velde  **eSentire, Inc.**  Jacob Gajek  **FireEye, Inc.**  Phillip Boles  Pavan Gorakav  Anuj Kumar  Shyamal Pandya  Paul Patrick  Scott Shreve  **Fox-IT**  Sarah Brown  **Georgetown University**  Eric Burger  **Hewlett Packard Enterprise (HPE)**  Tomas Sander  **IBM**  Peter Allor  Eldan Ben-Haim  Sandra Hernandez  Jason Keirstead  John Morris  Laura Rusu  Ron Williams  **IID**  Chris Richardson  **Integrated Networking Technologies, Inc.**  Patrick Maroney  **Johns Hopkins University Applied Physics Laboratory**  Karin Marr  Julie Modlin  Mark Moss  Pamela Smith  **Kaiser Permanente**  Russell Culpepper  Beth Pumo  **Lumeta Corporation**  Brandon Hoffman  **MTG Management Consultants, LLC.**  James Cabral  **National Security Agency**  Mike Boyle  Jessica Fitzgerald-McKay  **New Context Services, Inc.**  John-Mark Gurney  Christian Hunt  James Moler  Daniel Riedel  Andrew Storms  **OASIS**  James Bryce Clark  Robin Cover  Chet Ensign  **Open Identity Exchange**  Don Thibeau  **PhishMe Inc.**  Josh Larkins  **Raytheon Company-SAS**  Daniel Wyschogrod  **Retail Cyber Intelligence Sharing Center (R-CISC)**  Brian Engle  **Semper Fortis Solutions**  Joseph Brand  **Splunk Inc.**  Cedric LeRoux  Brian Luger  Kathy Wang  **TELUS**  Greg Reaume  Alan Steer  **Threat Intelligence Pty Ltd**  Tyron Miller  Andrew van der Stock  **ThreatConnect, Inc.**  Wade Baker  Cole Iliff  Andrew Pendergast  Ben Schmoker  Jason Spies  **TruSTAR Technology**  Chris Roblee  **United Kingdom Cabinet Office**  Iain Brown  Adam Cooper  Mike McLellan  Chris O’Brien  James Penman  Howard Staple  Chris Taylor  Laurie Thomson  Alastair Treharne  Julian White  Bethany Yates  **US Department of Homeland Security**  Evette Maynard-Noel  Justin Stekervetz  **ViaSat, Inc.**  Lee Chieffalo  Wilson Figueroa  Andrew May  **Yaana Technologies, LLC**  Anthony Rutkowski |

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

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| wd01 | 15 December 2015 | Desiree Beck Trey Darley Ivan Kirillov Rich Piazza | Initial transfer to OASIS template |