CybOX™ Version 2.1.1. Part 89: Win Task Object

Committee Specification Draft 01 / Public Review Draft 01

20 June 2016

Specification URIs

This version:

http://docs.oasis-open.org/cti/cybox/v2.1.1/csprd01/part89-win-task/cybox-v2.1.1-csprd01-part89-win-task.docx (Authoritative)
http://docs.oasis-open.org/cti/cybox/v2.1.1/csprd01/part89-win-task/cybox-v2.1.1-csprd01-part89-win-task.html
http://docs.oasis-open.org/cti/cybox/v2.1.1/csprd01/part89-win-task/cybox-v2.1.1-csprd01-part89-win-task.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/cti/cybox/v2.1.1/part89-win-task/cybox-v2.1.1-part89-win-task.docx (Authoritative)
http://docs.oasis-open.org/cti/cybox/v2.1.1/part89-win-task/cybox-v2.1.1-part89-win-task.html
http://docs.oasis-open.org/cti/cybox/v2.1.1/part89-win-task/cybox-v2.1.1-part89-win-task.pdf

Technical Committee:

OASIS Cyber Threat Intelligence (CTI) TC

Chair:

Richard Struse (Richard.Struse@HQ.DHS.GOV), DHS Office of Cybersecurity and Communications (CS&C)

Editors:

Desiree Beck (dbeck@mitre.org), MITRE Corporation
Trey Darley (trey@kingfisherops.com), Individual member
Ivan Kirillov (ikirillov@mitre.org), MITRE Corporation
Rich Piazza (rpiazza@mitre.org), MITRE Corporation

Additional artifacts:

This prose specification is one component of a Work Product whose components are listed in http://docs.oasis-open.org/cti/cybox/v2.1.1/csprd01/cybox-v2.1.1-csprd01-additional-artifacts.html.

Related work:

This specification is related to:

- *STIX™ Version 1.2.1*. Edited by Sean Barnum, Desiree Beck, Aharon Chernin, and Rich Piazza. 05 May 2016. OASIS Committee Specification 01. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part1-overview/stix-v1.2.1-cs01-part1-overview.html.

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 document was last revised or approved by the OASIS Cyber Threat Intelligence (CTI) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the TC's web page at https://www.oasis-open.org/committees/cti/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/cti/ipr.php).

Citation format:

When referencing this specification the following citation format should be used:

[CybOX-v2.1.1-win-task]

CybOX™ Version 2.1.1. Part 89: Win Task Object. Edited by Desiree Beck, Trey Darley, Ivan Kirillov, and Rich Piazza. 20 June 2016. OASIS Committee Specification Draft 01 / Public Review Draft 01. http://docs.oasis-open.org/cti/cybox/v2.1.1/csprd01/part89-win-task/cybox-v2.1.1-csprd01-part89-win-task.html. Latest version: http://docs.oasis-open.org/cti/cybox/v2.1.1/part89-win-task/cybox-v2.1.1-part89-win-task.html.

Notices

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 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.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

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

Table of Contents

1 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 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**.

1.1 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 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* 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* also summarizes the relationship of CybOX to other languages, and outlines general CybOX data model conventions.

1.2 Document Conventions

The following sections describe the conventions used in this document.

1.2.1 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*.

  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 (with single 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*

1.2.2 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.

1.2.3 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.

1.2.3.1 Class Properties

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

1.2.3.2 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
	This diagram icon indicates a class. If the name is in italics, it is an abstract class.
	This diagram icon indicates an enumeration.
	This diagram icon indicates a data type.
	This decorator icon indicates an attribute of a class. The green circle means its visibility is public. If the circle is red or yellow, it means its visibility is private or protected.
	This decorator icon indicates an enumeration literal.
	This arrow type indicates a directed association relationship.
	This arrow type indicates a generalization relationship.

1.2.4 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.

1.2.5 Property and Class Descriptions

Each class and property defined in CybOX is described using the format, “The X property verb Y.” 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.

1.3 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]**.

1.4 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.

2 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**.

2.1 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.

2.2 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.

3 Data Model

3.1 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**.

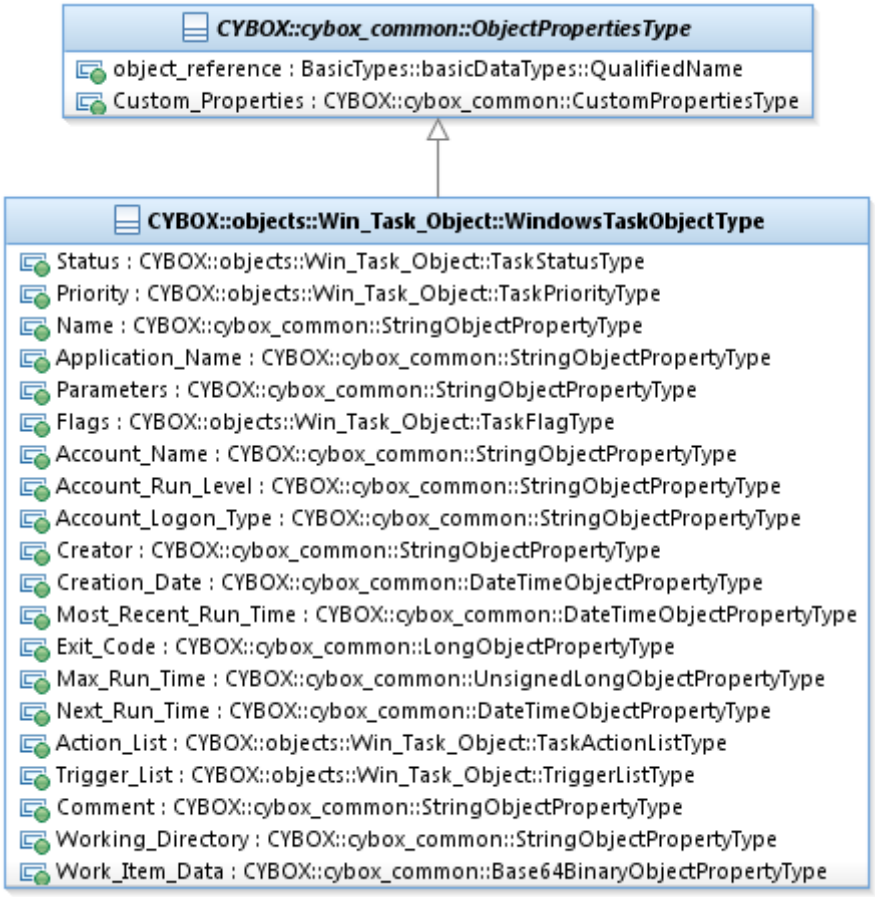

Figure 3-1. UML diagram of the `WindowsTaskObjectType` class

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

Table 3-1. 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.

3.2 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 3-2. 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.

3.3 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 3-3. 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:`	0..1	The `Trigger_Session_Change_Type` property specifies the type of Terminal Server session change

	StringObjectPropertyType		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.

3.4 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 3-4. 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.

3.5 TaskActionType Class

The TaskActionType class characterizes scheduled task actions.

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

Table 3-5. Properties of the TaskActionType class

Name	Type	Multiplicity	Description
Action_Type		0..1	The Action_Type property specifies the type of the action. See also: http://msdn.microsoft.com/en-

	TaskActionTypeType		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.

3.6 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 3-6. 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.

3.7 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 3-7. 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.

3.8 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 3-8. 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.

3.9 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.

3.10 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.

3.11 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.

3.12 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.

3.13 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.

3.14 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.

3.15 TaskActionTypeEnum Enumeration

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

Table 3-9. 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.

3.16 TaskPriorityEnum Enumeration

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

Table 3-10. 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).

3.17 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 3-11. 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.

3.18 TriggerTypeEnum Enumeration

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

Table 3-12. 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.

3.19 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 3-13. 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.

4 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.

Appendix A. 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

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

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

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.

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
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

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
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.

Appendix B. Revision History

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