STIX^{TM} Version 1.2.1. Part 14: Vocabularies

Committee Specification 01

05 May 2016

Specification URIs

This version:

http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part14-vocabularies/stix-v1.2.1-cs01-part14-vocabularies.doc (Authoritative)
http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part14-vocabularies/stix-v1.2.1-cs01-part14-vocabularies.html
http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part14-vocabularies/stix-v1.2.1-cs01-part14-vocabularies.pdf

Previous version:

http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.doc (Authoritative)
http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html
http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.pdf

Latest version:

http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part14-vocabularies.doc (Authoritative)
http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part14-vocabularies.html
http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part14-vocabularies.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:

Sean Barnum (sbarnum@mitre.org), MITRE Corporation
Desiree Beck (dbeck@mitre.org), MITRE Corporation
Aharon Chernin (achernin@soltra.com), Soltra
Rich Piazza (rpiazza@mitre.org), MITRE Corporation

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

- *STIX Version 1.2.1. Part 1: Overview*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part1-overview/stix-v1.2.1-cs01-part1-overview.html
- *STIX Version 1.2.1. Part 2: Common*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part2-common/stix-v1.2.1-cs01-part2-common.html
- *STIX Version 1.2.1. Part 3: Core*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part3-core/stix-v1.2.1-cs01-part3-core.html
- *STIX Version 1.2.1. Part 4: Indicator*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part4-indicator/stix-v1.2.1-cs01-part4-indicator.html
- *STIX Version 1.2.1. Part 5: TTP*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part5-ttp/stix-v1.2.1-cs01-part5-ttp.html

- *STIX Version 1.2.1. Part 6: Incident*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part6-incident/stix-v1.2.1-cs01-part6-incident.html
- *STIX Version 1.2.1. Part 7: Threat Actor*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part7-threat-actor/stix-v1.2.1-cs01-part7-threat-actor.html
- *STIX Version 1.2.1. Part 8: Campaign*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part8-campaign/stix-v1.2.1-cs01-part8-campaign.html
- *STIX Version 1.2.1. Part 9: Course of Action*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part9-coa/stix-v1.2.1-cs01-part9-coa.html
- *STIX Version 1.2.1. Part 10: Exploit Target*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part10-exploit-target/stix-v1.2.1-cs01-part10-exploit-target.html
- *STIX Version 1.2.1. Part 11: Report*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part11-report/stix-v1.2.1-cs01-part11-report.html
- *STIX Version 1.2.1. Part 12: Default Extensions*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part12-extensions/stix-v1.2.1-cs01-part12-extensions.html
- *STIX Version 1.2.1. Part 13: Data Marking*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part13-data-marking/stix-v1.2.1-cs01-part13-data-marking.html
- *STIX Version 1.2.1. Part 14: Vocabularies* (this document). http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part14-vocabularies/stix-v1.2.1-cs01-part14-vocabularies.html
- *STIX Version 1.2.1. Part 15: UML Model*. http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/part15-uml-model/stix-v1.2.1-cs01-part15-uml-model.html
- UML Model Serialization: http://docs.oasis-open.org/cti/stix/v1.2.1/cs01/uml-model/

Related work:

This specification replaces or supersedes:

- *STIX^TM 1.2 Vocabularies Specification* https://github.com/STIXProject/specifications/blob/version1.2/documents/pdf%20versions/STIX_Vocab_Draft.pdf

This specification is related to:

- *CybOX^TM Version 2.1.1.* Work in progress. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti-cybox
- *CybOX^TM 2.1.* https://cyboxproject.github.io/

Abstract:

The Structured Threat Information Expression (STIX) framework defines nine core constructs and the relationships between them for the purposes of modeling cyber threat information and enabling cyber threat information analysis and sharing. This specification document defines the Vocabularies data model, which includes definitions for default constrained enumerations of values for specific properties in other STIX data models.

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:

[STIX-v1.2.1-Vocabularies]

STIX^{TM} Version 1.2.1. Part 14: Vocabularies. 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/part14-vocabularies/stix-v1.2.1-cs01-part14-vocabularies.html. Latest version: http://docs.oasis-open.org/cti/stix/v1.2.1/stix-v1.2.1-part14-vocabularies.html.

Notices

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 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.

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

[All text is normative unless otherwise labeled]

The Structured Threat Information Expression (STIX[TM]) framework defines nine top-level component data models: Observable[1], Indicator, Incident, TTP, ExploitTarget, CourseOfAction, Campaign, ThreatActor, and Report. In addition, it defines a cross-cutting data model for expressing string-based properties as constrained by specific vocabularies. As part of this model, it defines numerous default vocabularies - defined lists of values to choose from when specifying certain properties in other STIX data models. These vocabularies are provided as the default lists, but the STIX data models also allow users to define their own vocabularies or even use values outside of any constrained vocabulary. Each default vocabulary in the Vocabularies data model is versioned separately (this is discussed further in Section **3**). This specification covers default vocabularies that are relevant to STIX v1.2.1.

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

1.1 STIX[TM] Specification Documents

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

The *STIX Version 1.2.1 Part 1: Overview* document provides a comprehensive overview of the full set of STIX data models, which in addition to the nine top-level data models mentioned in the Introduction, includes a core data model, a common data model, a cross-cutting data marking data model, various extension data models, and a vocabularies data model including a set of default controlled vocabularies. *STIX Version 1.2.1 Part 1: Overview* also summarizes the relationship of STIX to other languages and outlines general STIX data model conventions.

Figure 1-1 illustrates the set of specification documents are available. The color black is used to indicate the specification overview document, altered shading differentiates the overarching Core and Common data models from the supporting data models (vocabularies, data marking, and default extensions), and the color white indicates the component data models. The solid grey color denotes the overall STIX Language UML model. This STIX Vocabularies specification document is highlighted in its associated color (see Section **1.2.3.1**). For a list of all STIX documents and related information sources, please see *STIX Version 1.2.1 Part 1: Overview*.
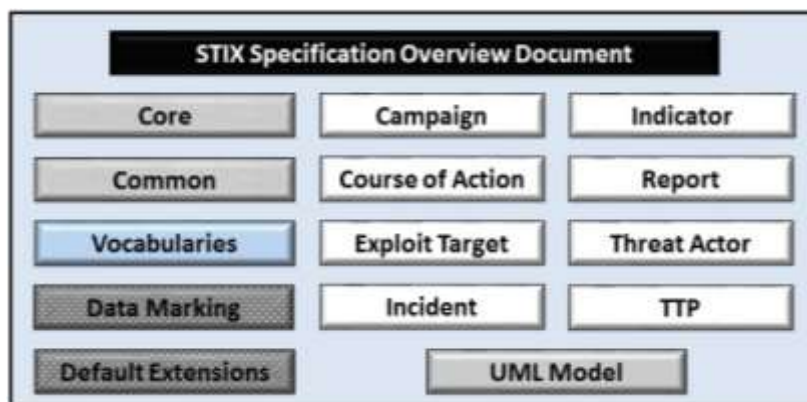
Figure 1-1. STIX^{TM} Language v1.2.1 specification documents

1.2 Document Conventions

The following conventions are used in this document.

1.2.1 Fonts

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

- Capitalization is used for STIX high level concepts, which are defined in *STIX Version 1.2.1 Part 1: Overview*.

  <u>Examples</u>: Indicator, Course of Action, Threat Actor

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

  <u>Examples</u>: `RelatedIndicatorsType`, `stixCommon:StatementType`

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

- The '*italic'* font (with single quotes) is used for noting actual, explicit values for STIX Language properties.

  <u>Example</u>: *'STIX Default Package Intent Vocabulary'*

1.2.2 UML Package References

Each STIX data model is captured in a different UML package (e.g., Core package, Campaign package, etc.) where the packages together compose the full STIX UML model. To refer to a particular class of a specific package, we use the format `package_prefix:class`, where `package_prefix` corresponds to the appropriate UML package. *STIX Version 1.2.1 Part 1: Overview* contains a list of the packages used by the Vocabularies data model, along with the associated prefix notations, descriptions, examples.

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

1.2.3 UML Diagrams

This specification makes use of UML diagrams to visually depict relationships between STIX Language constructs. Note that the diagrams have been extracted directly from the full UML model for STIX; they have not been constructed purely for inclusion in the specification documents. Due to the nature of the Vocabularies data model, which mostly consists of UML enumerations, there are few diagrams included in this document.

In UML diagrams, classes are often presented with their attributes elided, to avoid clutter. 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 Diagram Icons and Arrow Types

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

Table 1-1. UML diagram icons

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

1.2.3.2 Color Coding

The shapes of the UML diagrams are color coded to indicate the data model associated with a class. The colors used in the Vocabularies specification are illustrated via exemplars in **Figure 1-2**. Note that this data model uses UML stereotypes datatype and enumeration.

Figure 1-2. Data model color coding

1.2.4 Enumeration Table Notation

Throughout Section **3**, tables are used to describe the list of defined values for each default vocabulary. Each property table consists of a column of literal names, and a description column that describes the literal name, if needed.

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

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

There are three vocabulary-related UML data types defined in *STIX Version 1.2.1 Part 2: Common*, and together they provide a content creator with four choices for defining content, listed below in order of formality.

- Leverage a formally defined default vocabulary extended from the `stixCommon:ControlledVocabularyStringType` data type. STIX v1.2 defines a collection of default vocabularies and associated enumerations that are based on input from the STIX community; however, not all vocabulary properties have an assigned formally defined default vocabulary.

- Formally define a custom vocabulary by extending the `stixCommon:ControlledVocabularyStringType` data type. Because this is an extension of the STIX Vocabularies data model, producers and consumers MUST have access to the addition to the data model for successful use in the sharing of STIX documents.

- Reference an externally-defined, custom vocabulary using the `stixCommon:UnenforcedVocabularyStringType` data type to constrain the set of values. Externally-defined vocabularies are explicitly defined, but have not been included as formally specified vocabularies within the STIX Vocabularies data model using the `stixCommon:ControlledVocabularyStringType` data type. In this case, it is sufficient to specify the name of the vocabulary and a URL to a definition of that vocabulary.

- Choose an arbitrary and unconstrained value using the `stixCommon:VocabularyStringType` data type.

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

If a formally defined vocabulary is not sufficient for a content producer's purposes, the STIX Vocabularies data model allows the two alternatives listed above: externally defined custom vocabularies and arbitrary string values, which dispense with enumerated vocabularies altogether. If a custom vocabulary is not formally added to the Vocabularies data model then no enforcement policy of appropriate values is specified.

The UML diagram shown in **Figure 2-1** illustrates the relationships between the three vocabulary data types as defined in the STIX Common data model. As illustrated, all controlled vocabularies formally defined within the STIX Vocabularies data model are defined using an enumeration derived from the `ControlledVocabularyStringType` data type.

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

Further details of each vocabulary class are provided in Subsections **2.1.1** through **2.1.3**.

Figure 2-1. UML diagram of the STIX^{TM} Vocabularies data model

2.1.1 VocabularyStringType Data Type

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

2.1.2 UnenforcedVocabularyStringType Data Type

The `stixCommon:UnenforcedVocabularyStringType` data type specifies custom vocabulary values via a definition outside of the STIX Vocabularies data model. It extends the `stixCommon:VocabularyStringType` data type. Note that the STIX vocabularies data model does not define any enforcement policy for this data type.

2.1.3 ControlledVocabularyStringType Data Type

The `stixCommon:ControlledVocabularyStringType` data type specifies a formally defined vocabulary. It is an abstract data type so it MUST be extended via an enumeration defined according to the STIX Vocabularies data model (see Section **3**). This enables appropriate enumeration values to be enforced for any property asserting a given formally defined vocabulary.

3 STIX^{TM} Default Vocabularies Data Models

The STIX Vocabularies data model is defined as one UML package, but can be thought of as a collection of separate data models, each containing one UML enumeration. Each vocabulary will be specified using a separate version number, which is appended to the enumeration name. This facilitates adding literals to the enumeration without the need to update the version number of any of the other STIX data models or the version number of the full STIX specification.

3.1 AssetTypeVocab-1.0 Enumeration

The `AssetTypeVocab` enumeration is used to define the default STIX vocabulary for expressing the type of an asset. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Access reader	A device that protects an access point, using credentials. Both the access point and the credentials themselves can be virtual (password) or physical (access card).
Administrator	
ATM	An automatic teller machine.
Auditor	
Auth token	A token used during authenication of an object, such as a user or system.
Backup	A copy of data on a different storage device to be available in the case of destruction of the original data.
Broadband	
Call center	A group of individuals that handles telephone inquiries for an organization
Camera	A device for taking a photograph or video
Cashier	A cashier is a person who handles the cash register at various locations such as the point of sale in a retail store.
Customer	An individual or organization that purchases a product or service.
Database	Software for efficiently storing large amounts of data.
DCS	A distributed control system (DCS) is a control system for a process or plant, where elements are distributed throughout the system.
Desktop	A personal computer that generally isn't portable.
Developer	An individual that develops hadware, software, etc.
DHCP	Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
Directory	A file system artifact for storing a collection of other file system artifacts, including other directories

Disk drive	A device used to store data on a disk medium
Disk media	
DNS	Domain name system (DNS) is a collection of names of a computer hardware and/or software artifacts on a computer network
Documents	
End-user	
Executive	
File	A file system artifact for storing data in a particular format
Finance	
Firewall	A network security system that limits access to trusted traffic
Flash drive	A solid state data storage device that does not contain any moving parts.
Former employee	An individual who was previously employee by an organization
Gas terminal	An internet enabled gasoline dispencing device.
Guard	An individual who secures a particular device or location
Helpdesk	A resource for users of a product to troubleshoot problems
HSM	A hardware security model (HSM) is a device that securely stores a digital cryptographic key.
Human resources	A department in an organization that performs personnel management.
IDS	An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station
Kiosk	
LAN	A local area network (LAN)
Laptop	A portable personal computer.
Log	A digital recording of the activity of a device or process
Mail	
Mainframe	
Maintenance	
Manager	
Media	An object used to store and deliver data
Mobile phone	A portable telephone that communicates over a cellular network
Network	A collection of devices that are connected either physically or virtually
Partner	
Payment card	

Payment switch	
PBX	A private branch exchange (PBX) is a telephone switching system local to an organization
PED pad	
Peripheral	A device, which usually not logically or physically part of the main device, but connected physically or virtually.
Person	
PLC	A programmable logic controller (PLC) is a digital device used to control an electomechanical device.
POS controller	
POS terminal	
Print	
Private WAN	
Proxy	
Public WAN	
Remote access	
Router or switch	
RTU	Remote Terminal Unit (RTU)
SAN	
SCADA	
Server	
Smart card	
Tablet	A portable personal computer without a hardware keyboard
Tapes	A data media that uses spools of magnetic tape
Telephone	
Unknown	An unknown asset
User Device	
VoIP adapter	
VoIP phone	A telephone that communicates over voice internet protocol (VoIP)
Web application	A software application running on a server, which is accessed over the internet using a browser.
WLAN	Wireless local area network (WLAN)

3.2 AttackerInfrastructureTypeVocab-1.0 Enumeration

The `AttackerInfrastructureTypeVocab` enumeration is used to define the default STIX vocabulary for expressing the type of infrastructure an attacker uses. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Anonymization	
Anonymization - Proxy	
Anonymization - TOR Network	
Anonymization - VPN	
Communications	
Communications - Blogs	
Communications - Forums	
Communications - Internet Relay Chat	
Communications - Micro-Blogs	
Communications – Mobile Communications	
Communications - Social Networks	
Communications – User-Generated Content Websites	
Domain Registration	
Domain Registration – Dynamic DNS Services	
Domain Registration – Legitimate Domain Registration Services	
Domain Registration – Malicious Domain Registrars	
Domain Registration – Top-Level Domain Registrars	
Electronic Payment Methods	
Hosting	
Hosting - Bulletproof / Rogue Hosting	
Hosting - Cloud Hosting	
Hosting - Compromised Server	
Hosting - Fast Flux Botnet Hosting	

Hosting - Legitimate Hosting	

3.3 AttackerToolTypeVocab-1.0 Enumeration

The `AttackerInfrastructureTypeVocab` enumeration is used to define the default STIX vocabulary for expressing the type of tools an attacker uses. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Application Scanner	
Malware	Software designed to be used to attack or gain access to a computer system
Password Cracking	The process of using a software application to recover a plain text password from its encrypted representation
Penetration Testing	The process of investigating a computer system to find security weaknesses.
Port Scanner	A software application that reports on the status of the ports available on a host computer
Traffic Scanner	A software application that monitors data transferred on a network
Vulnerability Scanner	A type of software application used to discover vulnerabilities on a host, a network, or in a software product.

3.4 AvailabilityLossTypeVocab-1.1.1 Enumeration

The `AvailabilityLossTypeVocab` class is used to define the default STIX vocabulary for expressing the type of loss to availability that occurred as part of an incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Destruction	The information was destroyed or wiped.
Loss	Availability to the information was lost.
Interruption	Availability to the information was interrupted.
Degradation	Availability to the information was degraded.
Acceleration	Availability loss type is acceleration.
Obscuration	Availability to the information is obscured.
Unknown	Nature of availability loss is not known.

3.5 AvailabilityLossTypeVocab-1.0 Enumeration

The `AvailabilityLossTypeVocab` enumeration is used to define the default STIX vocabulary for expressing the type of loss to availability that occurred as part of an incident. The associated enumeration literals are provided in the table below. NOTE: As of STIX Version 1.1.1, `AvailabilityLossTypeVocab-1.0` is deprecated. Please use version 1.1.1 instead (see section 3.4).

Enumeration Literal	Description
Destruction	The information was destroyed or wiped.
Loss	Availability to the information was lost.
Interruption	Availability to the information was interrupted.
Degredation[2]	Availability to the information was degraded.
Acceleration	Availability loss type is acceleration.
Obscuration	Availability to the information is obscured.
Unknown	Nature of availability loss is not known.

3.6 CampaignStatusVocab-1.0 Enumeration

The `CampaignStatusVocab` enumeration is used to define the default STIX vocabulary for expressing the status of a campaign. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Ongoing	This campaign is currently taking place.
Historic	This campaign occurred in the past and is currently not taking place.
Future	This campaign is expected to take place in the future.

3.7 COAStageVocab-1.0 Enumeration

The `COAStageVocab` enumeration is used to define the default STIX vocabulary for expressing the stages of the threat management lifecycle to which a COA is applicable. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Remedy	This COA is applicable to the "Remedy" stage of the threat management lifecycle, meaning it may be applied proactively to prevent future threats.
Response	This COA is applicable to the "Response" stage of the threat management lifecycle, meaning it may be applied as a reaction to an ongoing threat.

3.8 CourseOfActionTypeVocab-1.0 Enumeration

The `CourseOfActionTypeVocab` enumeration is used to define the default STIX vocabulary for expressing types of courses of action. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Diplomatic Actions	Engaging in communications and relationship building with threat actors to influence positive changes in behavior.
Eradication	Identifying, locating, and eliminating malware from the network.

Hardening	Securing a system by reducing its attack surface by removing unnecessary software, usernames or logins, and services.
Internal Blocking	Host-based blocking of traffic from an internal compromised source.
Logical Access Restrictions	Activities associated with restricting logical access to computing resources.
Monitoring	Setting up network or host-based sensors to detect the presence of a threat.
Other	Other actions not covered in this list.
Patching	A specific form of hardening, patching involves applying a code fix directly to the software with the vulnerability.
Perimeter Blocking	Perimeter-based blocking of traffic from a compromised source.
Physical Access Restrictions	Activities associated with restricting physical access to computing resources.
Policy Actions	Modifications to policy that reduce the attack surface or infection vectors of malware.
Public Disclosure	Informing the public of the existence and characteristics of the threat or threat actor to influence positive change in adversary behavior.
Rebuilding	Re-installing a computing resource from a known safe source in order to ensure that the malware is no longer present on the previously compromised resource.
Redirection	Re-routing of suspicious or known malicious traffic away from the intended target to an area where the threat can be more safely observed and analyzed.
Redirection (Honey Pot)	Setting up a decoy parallel network that is intended to attract adversaries to the honey pot and away from the real network assets.
Training	Training users and administrators how to identify and mitigate threats.

3.9 DiscoveryMethodVocab-2.0 Enumeration

The `DiscoveryMethodVocab` enumeration is used to define the default STIX vocabulary for expressing how an incident was discovered. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Agent Disclosure	The incident was disclosed by the threat agent (e.g. public brag, private blackmail).
External - Fraud Detection	The incident was discovered through external fraud detection means.
Monitoring Service	The incident was reported by a managed security event monitoring service.
Law Enforcement	The incident was reported by law enforcement.
Customer	The incident was reported by a customer or partner affected by the incident.

Unrelated Party	The incident was reported by an unrelated third party.
Audit	The incident was discovered during an external security audit or scan.
Antivirus	The incident was discovered by an antivirus system.
Incident Response	The incident was discovered in the course of investigating a separate incident.
Financial Audit	The incident was discovered in the course of a financial audit and/or reconciliation process.
Fraud Detection	The incident was discovered through internal fraud detection means.
HIPS	The incident was discovered a host-based IDS or file integrity monitoring.
Internal - Fraud Detection	The incident was discovered through internal fraud detection means.
IT Audit	The incident was discovered by an internal IT audit or scan.
Log Review	The incident was discovered during a log review process or by a SIEM.
NIDS	The incident was discovered by a network-based intrustion detection/prevention system (NIDS).
Security Alarm	The incident was discovered by a physical security alarm.
User	The incident was reported by a user.
Unknown	It is not known how this incident was discovered.

3.10 DiscoveryMethodVocab-1.0 Enumeration

The `DiscoveryMethodVocab` enumeration is used to define the default STIX vocabulary for expressing how an incident was discovered. The associated enumeration literals are provided in the table below. NOTE: As of STIX Version 1.2, `DiscoveryMethodVocab-1.0` is deprecated. Please use version 2.0 instead (see Section **3.9**)

Enumeration Literal	Description
Agent Disclosure	The incident was disclosed by the threat agent (e.g. public brag, private blackmail).
Fraud Detection	The incident was discovered through external fraud detection means.
Monitoring Service	The incident was reported by a managed security event monitoring service.
Law Enforcement	The incident was reported by law enforcement.
Customer	The incident was reported by a customer or partner affected by the incident.
Unrelated Party	The incident was reported by an unrelated third party.
Audit	The incident was discovered during an external security audit or scan.

Antivirus	The incident was discovered by an antivirus system.
Incident Response	The incident was discovered in the course of investigating a separate incident.
Financial Audit	The incident was discovered in the course of a financial audit and/or reconciliation process.
Fraud Detection	The incident was discovered through internal fraud detection means.
HIPS	The incident was discovered a host-based IDS or file integrity monitoring.
IT Audit	The incident was discovered by an internal IT audit or scan.
Log Review	The incident was discovered during a log review process or by a SIEM.
NIDS	The incident was discovered by a network-based intrustion detection/prevention system (NIDS).
Security Alarm	The incident was discovered by a physical security alarm.
User	The incident was reported by a user.
Unknown	It is not known how this incident was discovered.

3.11 HighMediumLowVocab-1.0 Enumeration

The `HighMediumLowVocab` enumeration is used to define the default STIX vocabulary for expressing basic values that may be high, medium, low, none, or unknown. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
High	
Medium	
Low	
None	
Unknown	

3.12 ImpactQualificationVocab-1.0 Enumeration

The `ImpactQualificationVocab` enumeration is used to define the default STIX vocabulary for expressing the subjective level of impact of an incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Insignificant	The impact is insignificant because it is absorbed by normal activities.
Distracting	There are limited "hard costs," but the impact is felt through having to deal with the incident rather than conducting normal duties.
Painful	Real, somewhat serious effect on the "bottom line".

Damaging	Real and serious effect on the "bottom line" and/or long-term ability to generate revenue.
Catastrophic	A business-ending event.
Unknown	The impact qualification is unknown.

3.13 ImpactRatingVocab-1.0 Enumeration

The `ImpactRatingVocab` enumeration is used to define the default STIX vocabulary for expressing the level of impact due to an incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
None	There was no impact.
Minor	There was a minor impact.
Moderate	There was a moderate impact.
Major	There was a major impact.
Unknown	The impact is not known.

3.14 IncidentCategoryVocab-1.0 Enumeration

The `IncidentCategoryVocab` enumeration is used to define the default STIX vocabulary for expressing possible categories of an incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Denial of Service	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
Improper Usage	A person violates acceptable computing use policies.
Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
Malicious Code	Installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.

3.15 IncidentEffectVocab-1.0 Enumeration

The `IncidentEffectVocab` enumeration is used to define the default STIX vocabulary for expressing the possible effects of an incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Brand or Image Degradation	The image or brand of the target related to the incident is damaged.
Data Breach or Compromise	The incident involved obtained or altered data.
Degradation of Service	The incident involved reducing the level of service of the target.
Destruction	The incident involved the destruction of a software or hardware system.
Disruption of Service / Operations	The incident involved terminating the service or operations of the target
Financial Loss	The incident involved a financial loss by the target
Loss of Competitive Advantage	The incident involved a non-specified loss of competitive advantage
Loss of Competitive Advantage - Economic	The incident involved an economic loss of competitive advantage
Loss of Competitive Advantage - Military	The incident involved a military loss of competitive advantage
Loss of Competitive Advantage - Political	The incident involved a political loss of competitive advantage
Loss of Confidential / **Proprietary Information or Intellectual Property**	During the incident proprietary information or intellectual property (IP) was obtained
Regulatory, Compliance or Legal Impact	The incident caused some violation of law, regulation, etc.
Unintended Access	
User Data Loss	During the incident, user data was obtained

3.16 IncidentStatusVocab-1.0 Enumeration

The `IncidentStatusVocab-1.0` enumeration is used to define the default STIX vocabulary for expressing the possible status of the incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
New	
Open	The incident is being investigated
Stalled	The investigation of the incident is open but progress is not being made.
Containment Achieved	Any negative impacts of the incident have been mitigated
Restoration Achieved	Any services or operations that were degradated or distrupted have been restored
Incident Reported	
Closed	The incident is no longer under investigation
Rejected	The incident was determined to be invalid
Deleted	The incident was marked as "deleted".

3.17 IndicatorTypeVocab-1.1 Enumeration

The `IndicatorTypeVocab` enumeration is used to define the default STIX vocabulary for expressing indicator types. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Malicious E-mail	The indicator describes suspected malicious e-mail (phishing, spear phishing, infected, etc.).
IP Watchlist	The indicator describes a set of suspected malicious IP addresses or IP blocks.
File Hash Watchlist	The indicator describes a set of hashes for suspected malicious files.
Domain Watchlist	The indicator describes a set of suspected malicious domains.
URL Watchlist	The indicator describes a set of suspected malicious URLs.
Malware Artifacts	The indicator describes the effects of suspected malware.
C2	The indicator describes suspected command and control activity or static indications.
Anonymization	The indicator describes suspected anonymization techniques (Proxy, TOR, VPN, etc.).
Exfiltration	The indicator describes suspected exfiltration techniques or behavior.
Host Characteristics	The indicator describes suspected malicious host characteristics.
Compromised PKI Certificate	The indicator describes a compromised PKI Certificate.
Login Name	The indicator describes a compromised Login Name.
IMEI Watchlist	The indicator describes a watchlist for IMEI (International Mobile

	Station Equipment Identity handset identifiers).
IMSI Watchlist	The indicator describes a watchlist for IMSI (International Mobile Subscriber Identity SIM card identifiers_.

3.18 IndicatorTypeVocab-1.0 Enumeration

The `IndicatorTypeVocab` enumeration is used to define the default STIX vocabulary for expressing indicator types. The associated enumeration literals are provided in the table below. NOTE: As of STIX Version 1.1.1 `IndicatorTypeVocab-1.0` is deprecated. Please use version 1.1 instead (see section 3.17).

Enumeration Literal	Description
Malicious E-mail	The indicator describes suspected malicious e-mail (phishing, spear phishing, infected, etc.).
IP Watchlist	The indicator describes a set of suspected malicious IP addresses or IP blocks.
File Hash Watchlist	The indicator describes a set of hashes for suspected malicious files.
Domain Watchlist	The indicator describes a set of suspected malicious domains.
URL Watchlist	The indicator describes a set of suspected malicious URLS.
Malware Artifacts	The indicator describes the effects of suspected malware.
C2	The indicator describes suspected command and control activity or static indications.
Anonymization	The indicator describes suspected anonymization techniques (Proxy, TOR, VPN, etc.).
Exfiltration	The indicator describes suspected exfiltration techniques or behavior.
Host Characteristics	The indicator describes suspected malicious host characteristics.

3.19 InformationSourceRoleVocab-1.0 Enumeration

The `InformationSourceRoleVocab-1.0` enumeration is used to define the default STIX vocabulary for expressing the role played by a given entity in the sourcing of the information. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Initial Author	A party acting as the initial author/creator of a set of information.
Content Enhancer/Refiner	A party that enhances or refines a preexisting set of information.
Aggregator	A party that aggregates multiple different sets of information into one new set of information.
Transformer/Translator	A party that transforms or translates a preexisting set of information into a different representation (e.g., translating an unstructured prose threat analysis report into STIX).

3.20 InformationTypeVocab-1.0 Enumeration

The `InformationTypeVocab` enumeration is used to define the default STIX vocabulary for expressing types of information. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Information Assets	Non-specific information
Information Assets - Corporate Employee Information	Data related to an employee, such as salary
Information Assets - Customer PII	Data related to a customer, such as their SSN
Information Assets - Email Lists / Archives	Email addresses collected by an organization
Information Assets - Financial Data	Information such as credit card numbers, bank accounts, etc.
Information Assets - Intellectual Property	
Information Assets - Mobile Phone Contacts	Information related to associates from a cell phone.
Information Assets - User Credentials	Username and/or passwords
Authentication Cookies	A small piece of data, usually stored to remember that a user has authenticated on a computer system.

3.21 IntendedEffectVocab-1.0 Enumeration

The `IntendedEffectVocab` enumeration is used to define the default STIX vocabulary for expressing possible intended effects of a malicious actor or activity. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Account Takeover	The intended effect of the incident was for the attacker to obtain control over an account (financial, etc)
Advantage	The intended effect of the incident was for the attacker to obtain some advantage over the target
Advantage - Economic	The intended effect of the incident was for the attacker to obtain some economic advantage over the target
Advantage - Military	The intended effect of the incident was for the attacker to obtain some military advantage over the target
Advantage - Political	The intended effect of the incident was for the attacker to obtain some political advantage over the target
Brand Damage	The intended effect of the incident was for the attacker to cause some brand damage on the target

Competitive Advantage	The intended effect of the incident was for the attacker to obtain some non-specific competitive advantage over the target
Degradation of Service	The intended effect of the incident was reducing the level of services provided by the target
Denial and Deception	
Destruction	The intended effect of the incident was to cause the destruction of a software or hardware system.
Disruption	
Embarrassment	The intended effect of the incident was to expose a socially unacceptable action by the target
Exposure	
Extortion	The intended effect of the incident was force the payment of some sort to prevent the attacker from taking some action.
Fraud	
Harassment	The intended effect of the incident was to pressure or intimidate the target
ICS Control	
Theft	The intended effect of the incident was to perpetrate a non-specific theft
Theft - Credential Theft	The intended effect of the incident was to perpetrate a theft of credentials
Theft - Identity Theft	The intended effect of the incident was to perpetrate a theft of the target's identity
Theft - Intellectual Property	The intended effect of the incident was to perpetrate a theft of intellectual property
Theft - Theft of Proprietary Information	The intended effect of the incident was to perpetrate a theft of proprietary information
Traffic Diversion	
Unauthorized Access	

3.22 LocationClassVocab-1.0 Enumeration

The LocationClassVocab enumeration is used to define the default STIX vocabulary for expressing the subjective location of an asset.

Enumeration Literal	Description
Internally-Located	The asset is located internally.
Externally-Located	The asset is located externally.

Co-Located	The asset is co-located.
Mobile	The asset is mobile.
Unknown	The asset location is unknown.

3.23 LossDurationVocab-1.0 Enumeration

The LossDurationVocab enumeration is used to define the default STIX vocabulary for expressing the approximate length of time of a loss as part of an incident. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Permanent	The loss is permanent.
Weeks	The loss lasted for weeks.
Days	The loss lasted for days.
Hours	The loss lasted for hours.
Minutes	The loss lasted for minutes.
Seconds	The loss lasted for seconds.
Unknown	The loss duration is not known.

3.24 LossPropertyVocab-1.0 Enumeration

The `LossPropertyVocab` enumeration is used to define the default STIX vocabulary for expressing the possible security properties affected as part of a loss in an incident.

Enumeration Literal	Description
Accountability	
Availability	The availability of a computer system has been compromised
Confidentiality	Data can be obtained by an unauthorized user
Integrity	Data produced by a computer system is unreliable
Non-Repudiation	

3.25 MalwareTypeVocab-1.0 Enumeration

The `MalwareTypeVocab` enumeration is used to define the default STIX vocabulary for expressing types of malware. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Automated Transfer Scripts	
Adware	Any software that is funded by advertising. Adware may also gather sensitive user information from a system.

Dialer	A program to automatically dial a telephone
Bot	A program that resides on an infected system, communicating with and forming part of a botnet. The bot may be implanted by a worm or trojan, which opens a backdoor. The bot then monitors the backdoor for further instructions.
Bot - Credential Theft	A bot for the specific purpose to steal credentials
Bot - DDoS	A bot for the specific purpose to
Bot - Loader	
Bot - Spam	A bot for the specific purpose to send out spam email
DoS / DDoS	
DoS / DDoS - Participatory	
DoS / DDoS - Script	
DoS / DDoS - Stress Test Tools	
Exploit Kits	A software toolkit to target common vulnerabilties
POS / ATM Malware	Malware that exclusively targets point of sale (POS) systems or automatic teller machines (ATMs)
Ransomware	A type of malware that encrypts files on a victim's system, demanding payment of ransom in return for the access codes required to unlock files.
Remote Access Trojan	A remote access trojan program or RAT, is a trojan horse capable of controlling a machine through commands issue by a remote attacker.
Rogue Antivirus	A fake security product that demands money to clean phony infections.
Rootkit	A method of hiding files or processes from normal methods of monitoring, and is often used by malware to conceal its presence and activities. Rootkits can operate at a number of levels, from the application level - simply replacing or adjusting the settings of system software to prevent the display of certain information - through hooking certain functions or inserting modules or drivers into the operating system kernel, to the deeper level of firmware or virtualization rook kits, which are activated before the operating system and thus even harder to detect while the system is running.

3.26 ManagementClassVocab-1.0 Enumeration

The `ManagementClassVocab` enumeration is used to define the default STIX vocabulary for expressing the subjective type of management of an asset. The associated enumeration literals are provided in the table below.

Enumeration Literal	**Description**

Internally-Managed	The asset is managed internally.
Externally-Management	The asset is managed externally.
Co-Management	The asset is co-managed.
Unknown	The asset management class is unknown.

3.27 MotivationVocab-1.1 Enumeration

The `MotivationVocab` enumeration is used to define the default STIX vocabulary for expressing the motivation of a threat actor. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Ideological	The threat actor is motivated by non-specific ideological reasons.
Ideological - Anti-Corruption	The threat actor is motivated to attack targets engaging in corruption.
Ideological - Anti-Establishment	The threat actor is motivated to attack established authority
Ideological - Environmental	The threat actor is motivated to attack targets engaging in actions determental to the environment.
Ideological - Ethnic / Nationalist	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
Ideological - Information Freedom	The threat actor is motivated by the belief in the freedom of information.
Ideological - Religious	The threat actor is motivated to attack targets associated with a religion.
Ideological - Security Awareness	
Ideological - Human Rights	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
Ego	The threat actor is motivated by enhancing their own self worth.
Financial or Economic	The threat actor is motivated by financial gain.
Military	The threat actor is motivated by the desire to exercise some military advantage.
Opportunistic	The threat actor is motivated by the relative vulnerability of the target
Political	The threat actor is motivated by the desire to exercise some political advantage.

3.28 MotivationVocab-1.0.1 Enumeration

The `MotivationVocab` enumeration is used to define the default STIX vocabulary for expressing the motivation of a threat actor. The associated enumeration literals are provided in the table below. NOTE:

As of STIX Version 1.1, `MotivationVocab-1.0.1` is deprecated. Please use version 1.1 instead (see Section **3.27**).

Enumeration Literal	Description
Ideological	The threat actor is motivated by non-specific ideological reasons.
Ideological - Anti-Corruption	The threat actor is motivated to attack targets engaging in corruption.
Ideological - Anti-Establishment	The threat actor is motivated to attack established authority
Ideological - Environmental	The threat actor is motivated to attack targets engaging in actions determental to the environment.
Ideological - Ethnic / Nationalist	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
Ideological - Information Freedom	The threat actor is motivated by the belief in the freedom of information.
Ideological - Religious	The threat actor is motivated to attack targets associated with a religion.
Ideological - Security Awareness	
Ideological - Human Rights	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
Ego	The threat actor is motivated by enhancing their own self worth.
Financial or Economic	The threat actor is motivated by financial gain.
Military	The threat actor is motivated by the desire to exercise some military advantage.
Opportunistic	The threat actor is motivated by the relative vulnerability of the target
Policital[3]	The threat actor is motivated by the desire to exercise some political advantage.

3.29 MotivationVocab-1.0 Enumeration

The `MotivationVocab` enumeration is used to define the default STIX vocabulary for expressing the motivation of a threat actor. NOTE: As of STIX Version 1.0.1, `MotivationVocab-1.0` is deprecated. Please use version 1.1 instead (see Section **3.27**).

Enumeration Literal	Description
Ideological	The threat actor is motivated by non-specific ideological reasons.
Ideological - Anti-Corruption	The threat actor is motivated to attack targets engaging in

	corruption.
Ideological - Anti-Establisment[4]	The threat actor is motivated to attack established authority
Ideological - Environmental	The threat actor is motivated to attack targets engaging in actions determental to the environment.
Ideological - Ethnic / Nationalist	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
Ideological - Information Freedom	The threat actor is motivated by the belief in the freedom of information.
Ideological - Religious	The threat actor is motivated to attack targets associated with a religion.
Ideological - Security Awareness	
Ideological - Human Rights	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
Ego	The threat actor is motivated by enhancing their own self worth.
Financial or Economic	The threat actor is motivated by financial gain.
Military	The threat actor is motivated by the desire to exercise some military advantage.
Opportunistic	The threat actor is motivated by the relative vulnerability of the target
Policital[5]	The threat actor is motivated by the desire to exercise some political advantage.

3.30 OwnershipClassVocab-1.0 Enumeration

The `OwnershipClassVocab` enumeration is used to define the default STIX vocabulary for expressing the subjective type of ownership of an asset. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Internally-Owned	The asset is owned internally.
Employee-Owned	The asset is owned by an employee.
Partner-Owned	The asset is owned by a partner.
Customer-Owned	The asset is owned by a customer.
Unknown	The asset ownership class is unknown.

3.31 PackageIntentVocab-1.0 Enumeration

The `PackageIntentVocab` enumeration is used to define the default STIX vocabulary for the grouping intent of a set of STIX content. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Collective Threat Intelligence	The package is intended to convey a broad characterization of a threat across multiple facets.
Threat Report	The package is intended to convey a broad characterization of a threat across multiple facets expressed as a cohesive report.
Indicators	The package is intended to convey mainly indicators.
Indicators - Phishing	The package is intended to convey mainly phishing indicators.
Indicators - Watchlist	The package is intended to convey mainly network watchlist indicators.
Indicators - Malware Artifacts	The package is intended to convey mainly malware artifact indicators.
Indicators - Network Activity	The package is intended to convey mainly network activity indicators.
Indicators - Endpoint Characteristics	The package is intended to convey mainly endpoint characteristics (hashes, registry values, installed software, known vulnerabilities, etc.) indicators.
Campaign Characterization	The package is intended to convey mainly a characterization of one or more campaigns.
Threat Actor Characterization	The package is intended to convey mainly a characterization of one or more threat actors.
Exploit Characterization	The package is intended to convey mainly a characterization of one or more exploits.
Attack Pattern Characterization	The package is intended to convey mainly a characterization of one or more attack patterns.
Malware Characterization	The package is intended to convey mainly a characterization of one or more malware instances.
TTP - Infrastructure	The package is intended to convey mainly a characterization of attacker infrastructure.
TTP - Tools	The package is intended to convey mainly a characterization of attacker tools.
Courses of Action	The package is intended to convey mainly a set of courses of action.
Incident	The package is intended to convey mainly information about one or more incidents.
Observations	The package is intended to convey mainly information about instantial observations (cyber observables).
Observations - Email	The package is intended to convey mainly information about instantial email observations (email cyber

	observables).
Malware Samples	The package is intended to convey a set of malware samples.

3.32 PlanningAndOperationalSupportVocab-1.0.1 Enumeration

The `PlanningAndOperationalSupportVocab` enumeration is used to define the default STIX vocabulary for expressing the planning and operational support functions available to a threat actor. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Data Exploitation	
Data Exploitation - Analytic Support	
Data Exploitation - Translation Support	
Financial Resources	
Financial Resources - Academic	
Financial Resources - Commercial	
Financial Resources - Government	
Financial Resources - Hacktivist or Grassroot	
Financial Resources - Non-Attributable Finance	
Planning	
Planning - Open-Source Intelligence (OSINT) Gathering	
Planning - Operational Cover Plan	
Planning - Pre-Operational Surveillance and Reconnaissance	
Planning - Target Selection	
Skill Development / Recruitment	
Skill Development / Recruitment - Contracting and Hiring	
Skill Development / Recruitment - Document Exploitation (DOCEX) Training	
Skill Development / Recruitment - Internal Training	
Skill Development / Recruitment - Military Programs	
Skill Development / Recruitment - Security / Hacker Conferences	
Skill Development / Recruitment - Underground Forums	
Skill Development / Recruitment - University Programs	

3.33 PlanningAndOperationalSupportVocab-1.0 Enumeration

The `PlanningAndOperationalSupportVocab` enumeration is used to define the default STIX vocabulary for expressing the planning and operational support functions available to a threat actor. The associated enumeration literals are provided in the table below.NOTE: As of STIX Version 1.0.1, `PlanningAndOperationalSupportVocab-1.0` is deprecated. Please use version 1.0.1 instead (see Section **3.32**).

Enumeration Literal	Description
Data Exploitation	
Data Exploitation - Analytic Support	
Data Exploitation - Translation Support	
Financial Resources	
Financial Resources - Academic	
Financial Resources - Commercial	
Financial Resources - Government	
Financial Resources - Hacktivist or Grassroot	
Financial Resources - Non-Attributable Finance	
Planning	
Planning - Open-Source Intelligence (OSINT) Gethering[6]	
Planning - Operational Cover Plan	
Planning - Pre-Operational Surveillance and Reconnaissance	
Planning - Target Selection	
Skill Development / Recruitment	
Skill Development / Recruitment - Contracting and Hiring	
Skill Development / Recruitment – Document Exploitation (DOCEX) Training	
Skill Development / Recruitment - Internal Training	
Skill Development / Recruitment - Military Programs	
Skill Development / Recruitment - Security / Hacker Conferences	
Skill Development / Recruitment - Underground Forums	
Skill Development / Recruitment - University Programs	

3.34 ReportIntentVocab-1.0 Enumeration

The `ReportIntentVocab` enumeration is used to define the default STIX vocabulary for the grouping intent of a STIX Report content. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Collective Threat Intelligence	The report is intended to convey a broad characterization of a threat across multiple facets.
Threat Report	The report is intended to convey a broad characterization of a threat across multiple facets expressed as a cohesive report.
Indicators	The report is intended to convey mainly indicators.
Indicators - Phishing	The report is intended to convey mainly phishing indicators.
Indicators - Watchlist	The report is intended to convey mainly network watchlist indicators.
Indicators - Malware Artifacts	The report is intended to convey mainly malware artifact indicators.
Indicators - Network Activity	The report is intended to convey mainly network activity indicators.
Indicators - Endpoint Characteristics	The report is intended to convey mainly endpoint characteristics (hashes, registry values, installed software, known vulnerabilities, etc.) indicators.
Campaign Characterization	The report is intended to convey mainly a characterization of one or more campaigns.
Threat Actor Characterization	The report is intended to convey mainly a characterization of one or more threat actors.
Exploit Characterization	The report is intended to convey mainly a characterization of one or more exploits.
Attack Pattern Characterization	The report is intended to convey mainly a characterization of one or more attack patterns.
Malware Characterization	The report is intended to convey mainly a characterization of one or more malware instances.
TTP - Infrastructure	The report is intended to convey mainly a characterization of attacker infrastructure.
TTP - Tools	The report is intended to convey mainly a characterization of attacker tools.
Courses of Action	The report is intended to convey mainly a set of courses of action.
Incident	The report is intended to convey mainly information about one or more incidents.
Observations	The report is intended to convey mainly information about instantial observations (cyber observables).
Observations - Email	The report is intended to convey mainly information about instantial email observations (email cyber observables).

Malware Samples	The report is intended to convey a set of malware samples.

3.35 SecurityCompromiseVocab-1.0 Enumeration

The `SecurityCompromiseVocab` enumeration is used to define the default STIX vocabulary for expressing whether or not an incident resulted in a security compromise. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Yes	It has been confirmed that this incident resulted in a security compromise.
Suspected	It is suspected that this incident resulted in a security compromise.
No	It has been confirmed that this incident did not result in a security compromise.
Unknown	It is not known whether this incident resulted in a security compromise.

3.36 SystemTypeVocab-1.0 Enumeration

The `SystemTypeVocab` enumeration is used to define the default STIX vocabulary for expressing the type of a system. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Enterprise Systems	
Enterprise Systems - Application Layer	
Enterprise Systems - Database Layer	
Enterprise Systems – Enterprise Technologies and Support Infrastructure	
Enterprise Systems - Network Systems	
Enterprise Systems - Networking Devices	
Enterprise Systems - Web Layer	
Enterprise Systems - VoIP	
Industrial Control Systems	
Industrial Control Systems – Equipment Under Control	
Industrial Control Systems – Operations Management	
Industrial Control Systems – Safety, Protection and Local Control	
Industrial Control Systems - Supervisory Control	

Mobile Systems	
Mobile Systems - Mobile Operating Systems	
Mobile Systems - Near Field Communications	
Mobile Systems - Mobile Devices	
Third-Party Services	
Third-Party Services - Application Stores	
Third-Party Services - Cloud Services	
Third-Party Services - Security Vendors	
Third-Party Services - Social Media	
Third-Party Services - Software Update	
Users	
Users - Application And Software	
Users - Workstation	
Users - Removable Media	

3.37 ThreatActorSophisticationVocab-1.0 Enumeration

The `ThreatActorSophisticationVocab` enumeration is used to define the default STIX vocabulary for expressing the subjective level of sophistication of a threat actor. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Innovator	Demonstrates sophisticated capability. An innovator has the ability to create and script unique programs and codes targeting virtually any form of technology. At this level, this actor has a deep knowledge of networks, operating systems, programming languages, firmware, and infrastructure topologies and will demonstrate operational security when conducting his activities. Innovators are largely responsible for the discovery of 0-day vulnerabilities and the development of new attack techniques.
Expert	Demonstrates advanced capability. An actor possessing expert capability has the ability to modify existing programs or codes but does not have the capability to script sophisticated programs from scratch. The expert has a working knowledge of networks, operating systems, and possibly even defensive techniques and will typically exhibit some operational security.
Practitioner	Has a demonstrated, albeit low, capability. A practitioner possesses low sophistication capability. He does not have the ability to identify or exploit known vulnerabilities without the use of automated tools. He is proficient in the basic uses of publicly available hacking tools, but is unable to write or alter such programs on his own.
Novice	Demonstrates a nascent capability. A novice has basic computer skills and likely requires the assistance of a Practitioner or higher to engage in hacking activity. He uses existing and frequently well known and easy-to-find

	techniques and programs or scripts to search for and exploit weaknesses in other computers on the Internet and lacks the ability to conduct his own reconnaissance and targeting research.

3.38 ThreatActorTypeVocab-1.0 Enumeration

The `ThreatActorTypeVocab` enumeration is used to define the default STIX vocabulary for expressing the subjective type of a threat actor. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Cyber Espionage Operations	
Hacker	
Hacker - White hat	
Hacker - Gray hat	
Hacker - Black hat	
Hacktivist	
State Actor / Agency	
eCrime Actor - Credential Theft Botnet Operator	
eCrime Actor - Credential Theft Botnet Service	
eCrime Actor - Malware Developer	
eCrime Actor - Money Laundering Network	
eCrime Actor - Organized Crime Actor	
eCrime Actor - Spam Service	
eCrime Actor - Traffic Service	
eCrime Actor - Underground Call Service	
Insider Threat	
Disgruntled Customer / User	

3.39 VersioningVocab-1.0 Enumeration

The `VersioningVocab` enumeration is used to define the default STIX vocabulary for specifying the relationship between versions of STIX content. The associated enumeration literals are provided in the table below.

Enumeration Literal	Description
Updates - Revises	The new content represents a modified or expanded form of the previous content with existing information refined for improved quality or confidence.
Updates - Corrects	The new content represents a modified form of the previous content with corrections to errors in the existing information. The previous content should

	be considered invalid and the new content should be used in its place.
Revokes	The previous content is asserted to be invalid and should not be considered for operational purposes.

4 Conformance

Implementations have discretion over which parts (components, properties, extensions, controlled vocabularies, etc.) of STIX they implement (e.g., Indicator/Suggested_COAs).

[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 STIX they implement (e.g., Implementers of the entire TTP component must conform to all normative structural specifications of the UML model or additional normative statements within this document regarding the TTP component).

[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 STIX they implement (e.g., Non-implementers of any particular properties of the TTP component are free to ignore all normative structural specifications of the UML model or additional normative statements within this document regarding those properties of the TTP component).

The conformance section of this document is intentionally broad and attempts to reiterate what already exists in this document. The STIX 1.2 Specifications, which this specification is based on, did not have a conformance section. Instead, the STIX 1.2 Specifications relied on normative statements and the non-mandatory implementation of STIX profiles. STIX 1.2.1 represents a minimal change from STIX 1.2, and in that spirit no requirements have been added, modified, or removed by this section.

Appendix A. Suggested Default Vocabularies

This appendix shows the correspondence between properties in the STIX data model and the suggested default vocabularies which are described in the previous section. As discussed in Section **2**, there are many different options when using vocabulary terms in STIX. Default vocabularies should be used whenever possible to ensure the greatest level of compatibility between STIX users.

Enumeration	Package Prefix	Class	Properties
AssetTypeVocab-1.0	incident	AffectedAssetType	Type
AttackerInfrastructureTypeVocab-1.0	ttp	InfrastructureType	Type
AttackerToolTypeVocab-1.0	stixCommon	ToolInformationType	Type
AvailabilityLossTypeVocab-1.1.1(1.0)	incident	PropertyAffectedType	Type_Of_Availability_Loss
CampaignStatusVocab-1.0	campaign	CampaignType	Status
COAStageVocab-1.0	coa	CourseOfActionType	Stage
CourseOfActionTypeVocab-1.0	coa	CourseOfActionType	Type
DiscoveryMethodVocab-2.0 (1.0)	incident	IncidentType	incident:Discovery_Method
HighMediumLowVocab-1.0	stixCommon	StatementType	Value
ImpactQualificationVocab-1.0	incident	ImpactAssessmentType	Impact_Qualification
ImpactRatingVocab-1.0	incident	DirectImpactSummaryType	Asset_Losses Business-Mission_Disruption Response_And_Recovery_Costs
IncidentCategoryVocab-1.0	incident	CatgoriesType	Category
IncidentEffectVocab-1.0	incident	IncidentType	Effect
IncidentStatusVocab-1.0	incident	IncidentType	Status
IndicatorTypeVocab-1.1 (1.0)	indicator	IndicatorType	Type

InformationSourceRoleVocab-1.0	stixCommon	InformationSourceType	Role
InformationTypeVocab-1.0	ttp	VictimTargetingType	Targeted_Information
IntendedEffectVocab-1.0	incident	IncidentType	Intended_Effect/stixCommon:Value
LocationClassVocab-1.0	incident	AffectedAssetType	Location_Class
LossDurationVocab-1.0	incident	PropertyAffectedType	Duration_Of_Availability_Loss
LossPropertyVocab-1.0	incident	PropertyAffectedType	Property
MalwareTypeVocab-1.0	ttp	MalwareInstanceType	Type
ManagementClassVocab-1.0	incident	AffectedAssetType	Management_Class
MotivationVocab-1.1. (1.0.1, 1.0)	ta	ThreatActorType	Motivation/stixCommon:Value
OwnershipClassVocab-1.0	incident	AffectedAssetType	Ownership_Class
PackageIntentVocab-1.0	stix	STIXHeaderType	Package_Intent
PlanningAndOperationalSupportVocab-1.0.1 (1.0)	ta	ThreatActorType	Planning_And_Operational_Support/ stixCommon:Value
ReportIntentVocab-1.0	report	ReportHeaderType	Intent
SecurityCompromiseVocab-1.0	incident	ImpactAssessmentType IncidentType	Loss_Of_Competitive_Advantage Brand_And_Market_Damage Increased_Operating_Costs Legal_And_Regulatory_Costs Security_Compromise
SystemTypeVocab-1.0	ttp	VictimTargetingType	Targeted_Systems
ThreatActorSophisticationVocab-1.0	ta	ThreatActorType	Sophistication/stixCommon:Value
ThreatActorTypeVocab-1.0	ta	ThreatActorType	Type/stixCommon:Value
VersioningVocab-1.0	stixCommon	GenericRelationshipType	Relationship

Appendix B. Acknowledgments

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

Crystal Hayes, The Boeing Company
Brad Butts, U.S. Bank
Mona Magathan, U.S. Bank
Adam Cooper, United Kingdom Cabinet Office
Mike McLellan, United Kingdom Cabinet Office
Chris O'Brien, United Kingdom Cabinet Office
Julian White, United Kingdom Cabinet Office
Anthony Rutkowski, Yaana Technologies, LLC

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

Appendix C. Revision History

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

Notes ───────────────

[1] The CybOX Observable data model is actually defined in the CybOX Language, not in STIX.

[2] Corrected in `AvailabilityLossTypeVocab-1.1.1`.

[3] Corrected in `MotivationVocab-1.1`.

[4] Corrected in `MotivationVocab-1.0.1`.

[5] Corrected in `MotivationVocab-1.1`.

[6] Corrected in `PlanningAndOperationalSupportVocab-1.0.1`.