

THE MITRE CORPORATION

# STIX™ 1.2

## VOCABULARIES SPECIFICATION

---

JULY 17, 2015

*The Structured Threat Information eXpression (STIX™) framework defines eight 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.*

## **Acknowledgements**

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

## **Trademark Information**

STIX, the STIX logo, and CybOX are trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners.

## **Warnings**

MITRE PROVIDES STIX "AS IS" AND MAKES NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, CAPABILITY, EFFICIENCY, MERCHANTABILITY, OR FUNCTIONING OF STIX. IN NO EVENT WILL MITRE BE LIABLE FOR ANY GENERAL, CONSEQUENTIAL, INDIRECT, INCIDENTAL, EXEMPLARY, OR SPECIAL DAMAGES, RELATED TO STIX OR ANY DERIVATIVE THEREOF, WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, OR TORT, EVEN IF MITRE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.<sup>1</sup>

## **Feedback**

The STIX development team welcomes any feedback regarding this document. Please send any comments, questions, or suggestions to [stix@mitre.org](mailto:stix@mitre.org).<sup>2</sup>

---

<sup>1</sup> For detailed information see [TOU].

<sup>2</sup> For more information about the STIX Language, please visit [STIX].

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	STIX Specification Documents .....	1
1.2	Document Conventions.....	2
1.2.1	Key Words .....	2
1.2.2	Fonts.....	2
1.2.3	UML Package References.....	3
1.2.4	UML Diagrams.....	3
1.2.4.1	Diagram Icons and Arrow Types.....	4
1.2.4.2	Color Coding .....	4
1.2.5	Enumeration Table Notation .....	4
<b>2</b>	<b>Background Information .....</b>	<b>5</b>
2.1.1	VocabularyStringType Data Type.....	6
2.1.2	UnenforcedVocabularyStringType Data Type .....	7
2.1.3	ControlledVocabularyStringType Data Type.....	7
<b>3</b>	<b>STIX Default Vocabularies Data Models .....</b>	<b>8</b>
3.1	AssetTypeVocab-1.0 Enumeration .....	8
3.2	AttackerInfrastructureTypeVocab-1.0 Enumeration .....	10
3.3	AttackerToolTypeVocab-1.0 Enumeration.....	11
3.4	AvailabilityLossTypeVocab-1.1.1 Enumeration.....	12
3.5	AvailabilityLossTypeVocab-1.0 Enumeration .....	12
3.6	CampaignStatusVocab-1.0 Enumeration .....	13
3.7	COAStageVocab-1.0 Enumeration .....	13
3.8	CourseOfActionTypeVocab-1.0 Enumeration .....	13
3.9	DiscoveryMethodVocab-1.0 Enumeration.....	14
3.10	HighMediumLowVocab-1.0 Enumeration .....	15
3.11	ImpactQualificationVocab-1.0 Enumeration.....	16
3.12	ImpactRatingVocab-1.0 Enumeration .....	17
3.13	IncidentCategoryVocab-1.0 Enumeration .....	17
3.14	IncidentEffectVocab-1.0 Enumeration .....	18
3.15	IncidentStatusVocab-1.0 Enumeration .....	18
3.16	IndicatorTypeVocab-1.1 Enumeration .....	19
3.17	IndicatorTypeVocab-1.0 Enumeration .....	20
3.18	InformationSourceRoleVocab-1.0 Enumeration .....	20
3.19	InformationTypeVocab-1.0 Enumeration.....	21
3.20	IntendedEffectVocab-1.0 Enumeration.....	21
3.21	LocationClassVocab-1.0 Enumeration.....	22
3.22	LossDurationVocab-1.0 Enumeration.....	23
3.23	LossPropertyVocab-1.0 Enumeration.....	23
3.24	MalwareTypeVocab-1.0 Enumeration.....	23
3.25	ManagementClassVocab-1.0 Enumeration .....	24
3.26	MotivationVocab-1.1 Enumeration .....	25
3.27	MotivationVocab-1.0.1 Enumeration .....	26
3.28	MotivationVocab-1.0 Enumeration .....	27

3.29 OwnershipClassVocab-1.0 Enumeration ..... 27

3.30 PackageIntentVocab-1.0 Enumeration..... 28

3.31 PlanningAndOperationalSupportVocab-1.0.1 Enumeration ..... 29

3.32 PlanningAndOperationalSupportVocab-1.0 Enumeration ..... 30

3.33 SecurityCompromiseVocab-1.0 Enumeration ..... 31

3.34 SystemTypeVocab-1.0 Enumeration ..... 31

3.35 ThreatActorSophisticationVocab-1.0 Enumeration ..... 33

3.36 ThreatActorTypeVocab-1.0 Enumeration ..... 33

**Appendix .....35**

**References.....37**

# 1 Introduction

The Structured Threat Information eXpression (STIX™) framework defines eight top-level component data models: Observable<sup>3</sup>, Indicator, Incident, TTP, ExploitTarget, CourseOfAction, Campaign, and ThreatActor. 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<sup>4</sup>. This specification covers default vocabularies that are relevant to STIX v1.2.

In Section 1.1 we list additional specification documents, and in Section 1.2 we provide document conventions. In Section 0, we give background information to help the reader better understand the specification details that are provided later in the document. We present the Vocabularies data model specification details in Section 0. References are provided in the final section.

## 1.1 STIX Specification Documents

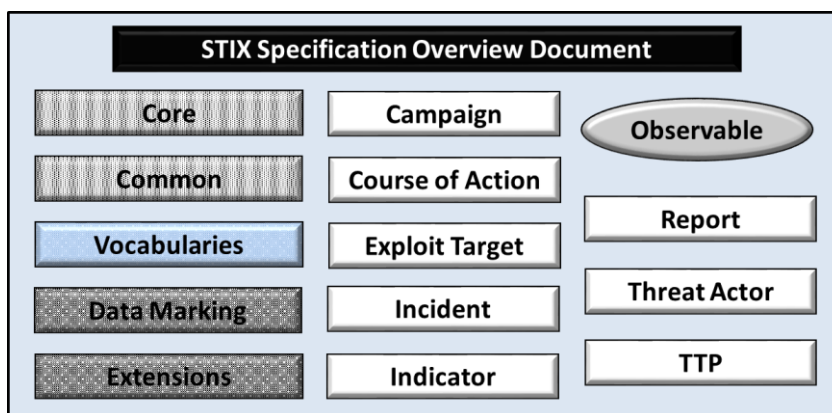
The STIX specification consists of a formal UML model and a set of textual specification documents that explain the UML model. Specification documents have been written for each of the key individual data models that compose the full STIX UML model.

The STIX specification overview document provides a comprehensive overview of the full set of STIX data models [STIX<sub>0</sub>], which in addition to the eight 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<sub>0</sub>] 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 (default vocabularies, data marking, and extensions), and the color white indicates the component data models. The Observable component data model is shown as an oval shape to indicate that it is defined as a CybOX specification (see [STIX<sub>0</sub>] for details). This STIX Vocabularies specification document is highlighted in its associated color (see Section 1.2.4.1). For a list of all STIX documents and related information sources, please see [STIX<sub>0</sub>].

<sup>3</sup> The CybOX Observable data model is actually defined in the CybOX Language, not in STIX.

<sup>4</sup> This is discussed further in Section 3.



**Figure 1-1.** STIX Language v1.2 specification documents

All specification documents can be found on this STIX Website [STIX-SPECS].

## 1.2 Document Conventions

The following conventions are used in this document.

### 1.2.1 Key Words

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 *RFC 2119* [RFC2119].

### 1.2.2 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 the STIX Specification Overview [STIX<sub>0</sub>].

Examples: Indicator, Course of Action, Threat Actor

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

Examples: `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, with single quotes'* font is used for noting explicit values for STIX Language properties.








Example: *'STIX Default Package Intent Vocabulary'*

### 1.2.3 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™ 1.2 Specification Overview document [STIX<sub>0</sub>] 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.

**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 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.

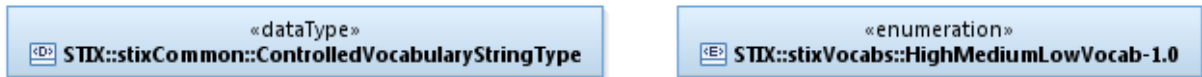
In UML diagrams, classes are often presented with their attributes elided, to avoid clutter. A class presented with an empty section at the bottom of the icon indicates that there are no attributes other than those that are visualized using associations.

#### 1.2.4.1 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.

#### 1.2.4.2 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 Report 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

#### 1.2.5 Enumeration Table Notation

Throughout Section 0, 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.



## 2 Background Information

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 0.

There are three vocabulary-related UML data types defined in the Common data model [STIX<sub>COM</sub>], and together they provide a content creator with four choices for defining content,<sup>5</sup> 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

---

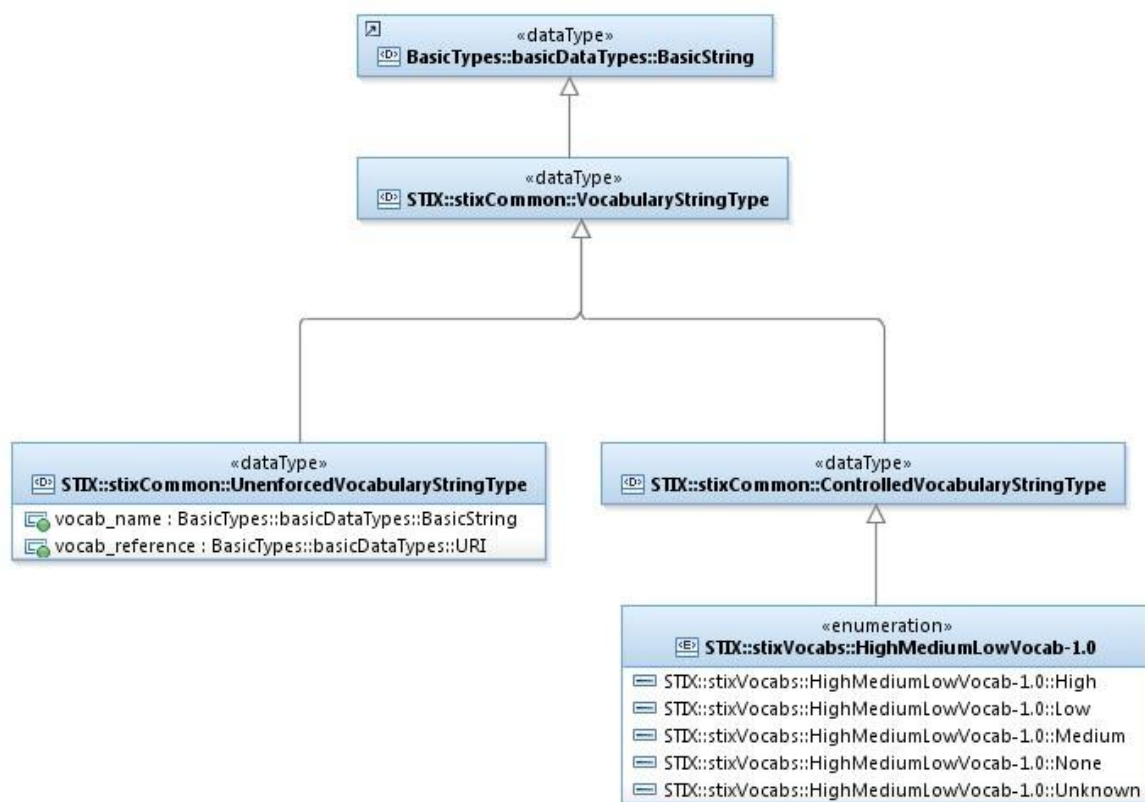
<sup>5</sup> The vocabulary-related data types discussed here are different than those defined for vocabularies in the STIX 1.2 XSD implementation.

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 **Error! Reference source not found.** 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 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<sup>6</sup> so it MUST be extended via an enumeration defined according to the STIX Vocabularies data model (see Section 0). This enables appropriate enumeration values to be enforced for any property asserting a given formally defined vocabulary.

---

<sup>6</sup> Note that in the XSD implementation, `ControlledVocabularyStringType` is not an abstract concept.

### 3 STIX Default Vocabularies Data Models<sup>7</sup>

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 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
<b>Access reader</b>	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).
<b>Administrator</b>	
<b>ATM</b>	An automatic teller machine.
<b>Auditor</b>	
<b>Auth token</b>	A token used during authentication of an object, such as a user or system.
<b>Backup</b>	A copy of data on a different storage device to be available in the case of destruction of the original data.
<b>Broadband</b>	
<b>Call center</b>	A group of individuals that handles telephone inquiries for an organization
<b>Camera</b>	A device for taking a photograph or video
<b>Cashier</b>	A cashier is a person who handles the cash register at various locations such as the point of sale in a retail store.
<b>Customer</b>	An individual or organization that purchases a product or service.
<b>Database</b>	Software for efficiently storing large amounts of data.
<b>DCS</b>	A distributed control system (DCS) is a control system for a process or plant, where elements are distributed throughout the system.
<b>Desktop</b>	A personal computer that generally isn't portable.
<b>Developer</b>	An individual that develops hardware, software, etc.
<b>DHCP</b>	Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such

<sup>7</sup> The descriptions of the enumeration literals found in this section are incomplete. Some are missing entirely, and the writing style is not consistent.

	as IP addresses for interfaces and services.
<b>Directory</b>	A file system artifact for storing a collection of other file system artifacts, including other directories
<b>Disk drive</b>	A device used to store data on a disk medium
<b>Disk media</b>	
<b>DNS</b>	Domain name system (DNS) is a collection of names of a computer hardware and/or software artifacts on a computer network
<b>Documents</b>	
<b>End-user</b>	
<b>Executive</b>	
<b>File</b>	A file system artifact for storing data in a particular format
<b>Finance</b>	
<b>Firewall</b>	A network security system that limits access to trusted traffic
<b>Flash drive</b>	A solid state data storage device that does not contain any moving parts.
<b>Former employee</b>	An individual who was previously employee by an organization
<b>Gas terminal</b>	An internet enabled gasoline dispensing device.
<b>Guard</b>	An individual who secures a particular device or location
<b>Helpdesk</b>	A resource for users of a product to troubleshoot problems
<b>HSM</b>	A hardware security model (HSM) is a device that securely stores a digital cryptographic key.
<b>Human resources</b>	A department in an organization that performs personnel management.
<b>IDS</b>	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
<b>Kiosk</b>	
<b>LAN</b>	A local area network (LAN)
<b>Laptop</b>	A portable personal computer.
<b>Log</b>	A digital recording of the activity of a device or process
<b>Mail</b>	
<b>Mainframe</b>	
<b>Maintenance</b>	
<b>Manager</b>	
<b>Media<sup>8</sup></b>	An object used to store and deliver data
<b>Mobile phone</b>	A portable telephone that communicates over a cellular network
<b>Network</b>	A collection of devices that are connected either physically or virtually
<b>Partner</b>	

---

<sup>8</sup> Appears twice in the vocabulary in error

<b>Payment card</b>	
<b>Payment switch</b>	
<b>PBX</b>	A private branch exchange (PBX) is a telephone switching system local to an organization
<b>PED pad</b>	
<b>Peripheral</b>	A device, which usually not logically or physically part of the main device, but connected physically or virtually.
<b>Person</b>	
<b>PLC</b>	A programmable logic controller (PLC) is a digital device used to control an electromechanical device.
<b>POS controller</b>	
<b>POS terminal</b>	
<b>Print</b>	
<b>Private WAN</b>	
<b>Proxy</b>	
<b>Public WAN</b>	
<b>Remote access</b>	
<b>Router or switch</b>	
<b>RTU</b>	Remote Terminal Unit (RTU)
<b>SAN</b>	
<b>SCADA</b>	
<b>Server</b>	
<b>Smart card</b>	
<b>Tablet</b>	A portable personal computer without a hardware keyboard
<b>Tapes</b>	A data media that uses spools of magnetic tape
<b>Telephone<sup>9</sup></b>	
<b>Unknown</b>	An unknown asset
<b>User Device</b>	
<b>VoIP adapter</b>	
<b>VoIP phone</b>	A telephone that communicates over voice internet protocol (VoIP)
<b>Web application</b>	A software application running on a server, which is accessed over the internet using a browser.
<b>WLAN</b>	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.

---

<sup>9</sup> Appears twice in the vocabulary in error

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

### 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
<b>Application Scanner</b>	
<b>Malware</b>	Software designed to be used to attack or gain access to a computer system
<b>Password Cracking</b>	The process of using a software application to recover a plain

	text password from its encrypted representation
<b>Penetration Testing</b>	The process of investigating a computer system to find security weaknesses.
<b>Port Scanner</b>	A software application that reports on the status of the ports available on a host computer
<b>Traffic Scanner</b>	A software application that monitors data transferred on a network
<b>Vulnerability Scanner</b>	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
<b>Destruction</b>	The information was destroyed or wiped.
<b>Loss</b>	Availability to the information was lost.
<b>Interruption</b>	Availability to the information was interrupted.
<b>Degradation</b>	Availability to the information was degraded.
<b>Acceleration</b>	Availability loss type is acceleration.
<b>Obscuration</b>	Availability to the information is obscured.
<b>Unknown</b>	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
<b>Destruction</b>	The information was destroyed or wiped.
<b>Loss</b>	Availability to the information was lost.
<b>Interruption</b>	Availability to the information was interrupted.
<b>Degradation</b> <sup>10</sup>	Availability to the information was degraded.
<b>Acceleration</b>	Availability loss type is acceleration.
<b>Obscuration</b>	Availability to the information is obscured.
<b>Unknown</b>	Nature of availability loss is not known.

<sup>10</sup> Corrected in `AvailabilityLossTypeVocab-1.1.1`



### 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
<b>Ongoing</b>	This campaign is currently taking place.
<b>Historic</b>	This campaign occurred in the past and is currently not taking place.
<b>Future</b>	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
<b>Remedy</b>	This COA is applicable to the "Remedy" stage of the threat management lifecycle, meaning it may be applied proactively to prevent future threats.
<b>Response</b>	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
<b>Diplomatic Actions</b>	Engaging in communications and relationship building with threat actors to influence positive changes in behavior.
<b>Eradication</b>	Identifying, locating, and eliminating malware from the network.
<b>Hardening</b>	Securing a system by reducing its attack surface by removing unnecessary software, usernames or logins, and services.
<b>Internal Blocking</b>	Host-based blocking of traffic from an internal compromised source.
<b>Logical Access Restrictions</b>	Activities associated with restricting logical access to computing resources.
<b>Monitoring</b>	Setting up network or host-based sensors to detect the presence of a threat.
<b>Other</b>	Other actions not covered in this list.

<b>Patching</b>	A specific form of hardening, patching involves applying a code fix directly to the software with the vulnerability.
<b>Perimeter Blocking</b>	Perimeter-based blocking of traffic from a compromised source.
<b>Physical Access Restrictions</b>	Activities associated with restricting physical access to computing resources.
<b>Policy Actions</b>	Modifications to policy that reduce the attack surface or infection vectors of malware.
<b>Public Disclosure</b>	Informing the public of the existence and characteristics of the threat or threat actor to influence positive change in adversary behavior.
<b>Rebuilding</b>	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.
<b>Redirection</b>	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.
<b>Redirection (Honey Pot)</b>	Setting up a decoy parallel network that is intended to attract adversaries to the honey pot and away from the real network assets.
<b>Training</b>	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
<b>Agent Disclosure</b>	The incident was disclosed by the threat agent (e.g. public brag, private blackmail).
<b>External - Fraud Detection</b>	The incident was discovered through external fraud detection means.
<b>Monitoring Service</b>	The incident was reported by a managed security event monitoring service.
<b>Law Enforcement</b>	The incident was reported by law enforcement.
<b>Customer</b>	The incident was reported by a customer or partner affected by the incident.
<b>Unrelated Party</b>	The incident was reported by an unrelated third party.
<b>Audit</b>	The incident was discovered during an external security audit or scan.
<b>Antivirus</b>	The incident was discovered by an antivirus system.
<b>Incident Response</b>	The incident was discovered in the course of investigating a

	separate incident.
<b>Financial Audit</b>	The incident was discovered in the course of a financial audit and/or reconciliation process.
<b>Fraud Detection</b>	The incident was discovered through internal fraud detection means.
<b>HIPS</b>	The incident was discovered a host-based IDS or file integrity monitoring.
<b>Internal - Fraud Detection</b>	The incident was discovered through internal fraud detection means.
<b>IT Audit</b>	The incident was discovered by an internal IT audit or scan.
<b>Log Review</b>	The incident was discovered during a log review process or by a SIEM.
<b>NIDS</b>	The incident was discovered by a network-based intrusion detection/prevention system (NIDS).
<b>Security Alarm</b>	The incident was discovered by a physical security alarm.
<b>User</b>	The incident was reported by a user.
<b>Unknown</b>	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
<b>Agent Disclosure</b>	The incident was disclosed by the threat agent (e.g. public brag, private blackmail).
<b>Fraud Detection</b>	The incident was discovered through external fraud detection means.
<b>Monitoring Service</b>	The incident was reported by a managed security event monitoring service.
<b>Law Enforcement</b>	The incident was reported by law enforcement.
<b>Customer</b>	The incident was reported by a customer or partner affected by the incident.
<b>Unrelated Party</b>	The incident was reported by an unrelated third party.
<b>Audit</b>	The incident was discovered during an external security audit or scan.
<b>Antivirus</b>	The incident was discovered by an antivirus system.
<b>Incident Response</b>	The incident was discovered in the course of investigating a separate incident.
<b>Financial Audit</b>	The incident was discovered in the course of a financial audit and/or reconciliation process.

<b>Fraud Detection</b>	The incident was discovered through internal fraud detection means.
<b>HIPS</b>	The incident was discovered a host-based IDS or file integrity monitoring.
<b>IT Audit</b>	The incident was discovered by an internal IT audit or scan.
<b>Log Review</b>	The incident was discovered during a log review process or by a SIEM.
<b>NIDS</b>	The incident was discovered by a network-based intrusion detection/prevention system (NIDS).
<b>Security Alarm</b>	The incident was discovered by a physical security alarm.
<b>User</b>	The incident was reported by a user.
<b>Unknown</b>	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
<b>High</b>	
<b>Medium</b>	
<b>Low</b>	
<b>None</b>	
<b>Unknown</b>	

### 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
<b>Insignificant</b>	The impact is insignificant because it is absorbed by normal activities.
<b>Distracting</b>	There are limited “hard costs,” but the impact is felt through having to deal with the incident rather than conducting normal duties.
<b>Painful</b>	Real, somewhat serious effect on the “bottom line”.
<b>Damaging</b>	Real and serious effect on the “bottom line” and/or long-term ability to generate revenue.
<b>Catastrophic</b>	A business-ending event.
<b>Unknown</b>	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
<b>Denial of Service</b>	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
<b>Exercise/Network Defense Testing</b>	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
<b>Improper Usage</b>	A person violates acceptable computing use policies.
<b>Investigation</b>	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
<b>Malicious Code</b>	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.
<b>Scans/Probes/Attempted Access</b>	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.
<b>Unauthorized Access</b>	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
<b>Brand or Image Degradation</b>	The image or brand of the target related to the incident is damaged.
<b>Data Breach or Compromise</b>	The incident involved obtained or altered data.
<b>Degradation of Service</b>	The incident involved reducing the level of service of the target.
<b>Destruction</b>	The incident involved the destruction of a software or hardware system.
<b>Disruption of Service / Operations</b>	The incident involved terminating the service or operations of the target
<b>Financial Loss</b>	The incident involved a financial loss by the target
<b>Loss of Competitive Advantage</b>	The incident involved a non-specified loss of competitive advantage
<b>Loss of Competitive Advantage - Economic</b>	The incident involved an economic loss of competitive advantage
<b>Loss of Competitive Advantage - Military</b>	The incident involved a military loss of competitive advantage
<b>Loss of Competitive Advantage - Political</b>	The incident involved a political loss of competitive advantage
<b>Loss of Confidential / Proprietary Information or Intellectual Property</b>	During the incident proprietary information or intellectual property (IP) was obtained
<b>Regulatory, Compliance or Legal Impact</b>	The incident caused some violation of law, regulation, etc.
<b>Unintended Access</b>	
<b>User Data Loss</b>	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
<b>New</b>	

<b>Open</b>	The incident is being investigated
<b>Stalled</b>	The investigation of the incident is open but progress is not being made.
<b>Containment Achieved</b>	Any negative impacts of the incident have been mitigated
<b>Restoration Achieved</b>	Any services or operations that were degraded or distrusted have been restored
<b>Incident Reported</b>	
<b>Closed</b>	The incident is no longer under investigation
<b>Rejected</b>	The incident was determined to be invalid
<b>Deleted</b>	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
<b>Malicious E-mail</b>	The indicator describes suspected malicious e-mail (phishing, spear phishing, infected, etc.).
<b>IP Watchlist</b>	The indicator describes a set of suspected malicious IP addresses or IP blocks.
<b>File Hash Watchlist</b>	The indicator describes a set of hashes for suspected malicious files.
<b>Domain Watchlist</b>	The indicator describes a set of suspected malicious domains.
<b>URL Watchlist</b>	The indicator describes a set of suspected malicious URLs.
<b>Malware Artifacts</b>	The indicator describes the effects of suspected malware.
<b>C2</b>	The indicator describes suspected command and control activity or static indications.
<b>Anonymization</b>	The indicator describes suspected anonymization techniques (Proxy, TOR, VPN, etc.).
<b>Exfiltration</b>	The indicator describes suspected exfiltration techniques or behavior.
<b>Host Characteristics</b>	The indicator describes suspected malicious host characteristics.
<b>Compromised PKI Certificate</b>	The indicator describes a compromised PKI Certificate.
<b>Login Name</b>	The indicator describes a compromised Login Name.
<b>IMEI Watchlist</b>	The indicator describes a watchlist for IMEI (International Mobile Station Equipment Identity handset identifiers).
<b>IMSI Watchlist</b>	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
<b>Malicious E-mail</b>	The indicator describes suspected malicious e-mail (phishing, spear phishing, infected, etc.).
<b>IP Watchlist</b>	The indicator describes a set of suspected malicious IP addresses or IP blocks.
<b>File Hash Watchlist</b>	The indicator describes a set of hashes for suspected malicious files.
<b>Domain Watchlist</b>	The indicator describes a set of suspected malicious domains.
<b>URL Watchlist</b>	The indicator describes a set of suspected malicious URLs.
<b>Malware Artifacts</b>	The indicator describes the effects of suspected malware.
<b>C2</b>	The indicator describes suspected command and control activity or static indications.
<b>Anonymization</b>	The indicator describes suspected anonymization techniques (Proxy, TOR, VPN, etc.).
<b>Exfiltration</b>	The indicator describes suspected exfiltration techniques or behavior.
<b>Host Characteristics</b>	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
<b>Initial Author</b>	A party acting as the initial author/creator of a set of information.
<b>Content Enhancer/Refiner</b>	A party that enhances or refines a preexisting set of information.
<b>Aggregator</b>	A party that aggregates multiple different sets of information into one new set of information.
<b>Transformer/Translator</b>	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
<b>Information Assets</b>	Non-specific information
<b>Information Assets - Corporate Employee Information</b>	Data related to an employee, such as salary
<b>Information Assets - Customer PII</b>	Data related to a customer, such as their SSN
<b>Information Assets - Email Lists / Archives</b>	Email addresses collected by an organization
<b>Information Assets - Financial Data</b>	Information such as credit card numbers, bank accounts, etc.
<b>Information Assets - Intellectual Property</b>	
<b>Information Assets - Mobile Phone Contacts</b>	Information related to associates from a cell phone.
<b>Information Assets - User Credentials</b>	Username and/or passwords
<b>Authentication Cookies</b>	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
<b>Account Takeover</b>	The intended effect of the incident was for the attacker to obtain control over an account (financial, etc)
<b>Advantage</b>	The intended effect of the incident was for the attacker to obtain some advantage over the target
<b>Advantage - Economic</b>	The intended effect of the incident was for the attacker to obtain some economic advantage over the target
<b>Advantage - Military</b>	The intended effect of the incident was for the attacker to obtain some military advantage over the target

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

### 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
<b>Internally-Located</b>	The asset is located internally.
<b>Externally-Located</b>	The asset is located externally.
<b>Co-Located</b>	The asset is co-located.
<b>Mobile</b>	The asset is mobile.
<b>Unknown</b>	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
<b>Permanent</b>	The loss is permanent.
<b>Weeks</b>	The loss lasted for weeks.
<b>Days</b>	The loss lasted for days.
<b>Hours</b>	The loss lasted for hours.
<b>Minutes</b>	The loss lasted for minutes.
<b>Seconds</b>	The loss lasted for seconds.
<b>Unknown</b>	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
<b>Accountability</b>	
<b>Availability</b>	The availability of a computer system has been compromised
<b>Confidentiality</b>	Data can be obtained by an unauthorized user
<b>Integrity</b>	Data produced by a computer system is unreliable
<b>Non-Repudiation</b>	

### 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
<b>Automated Transfer Scripts</b>	
<b>Adware</b>	Any software that is funded by advertising. Adware may also gather sensitive user information from a system.

<b>Dialer</b>	A program to automatically dial a telephone
<b>Bot</b>	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.
<b>Bot - Credential Theft</b>	A bot for the specific purpose to steal credentials
<b>Bot - DDoS</b>	A bot for the specific purpose to
<b>Bot - Loader</b>	
<b>Bot - Spam</b>	A bot for the specific purpose to send out spam email
<b>DoS / DDoS</b>	
<b>DoS / DDoS - Participatory</b>	
<b>DoS / DDoS - Script</b>	
<b>DoS / DDoS - Stress Test Tools</b>	
<b>Exploit Kits</b>	A software toolkit to target common vulnerabilities
<b>POS / ATM Malware</b>	Malware that exclusively targets point of sale (POS) systems or automatic teller machines (ATMs)
<b>Ransomware</b>	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.
<b>Remote Access Trojan</b>	A remote access trojan program or RAT, is a trojan horse capable of controlling a machine through commands issue by a remote attacker.
<b>Rogue Antivirus</b>	A fake security product that demands money to clean phony infections.
<b>Rootkit</b>	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 root 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
<b>Internally-Managed</b>	The asset is managed internally.
<b>Externally-Management</b>	The asset is managed externally.
<b>Co-Management</b>	The asset is co-managed.
<b>Unknown</b>	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
<b>Ideological</b>	The threat actor is motivated by non-specific ideological reasons.
<b>Ideological - Anti-Corruption</b>	The threat actor is motivated to attack targets engaging in corruption.
<b>Ideological - Anti-Establishment</b>	The threat actor is motivated to attack established authority
<b>Ideological - Environmental</b>	The threat actor is motivated to attack targets engaging in actions detrimental to the environment.
<b>Ideological - Ethnic / Nationalist</b>	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
<b>Ideological - Information Freedom</b>	The threat actor is motivated by the belief in the freedom of information.
<b>Ideological - Religious</b>	The threat actor is motivated to attack targets associated with a religion.
<b>Ideological - Security Awareness</b>	
<b>Ideological - Human Rights</b>	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
<b>Ego</b>	The threat actor is motivated by enhancing their own self worth.
<b>Financial or Economic</b>	The threat actor is motivated by financial gain.
<b>Military</b>	The threat actor is motivated by the desire to exercise some military advantage.
<b>Opportunistic</b>	The threat actor is motivated by the relative vulnerability of the target
<b>Political</b>	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
<b>Ideological</b>	The threat actor is motivated by non-specific ideological reasons.
<b>Ideological - Anti-Corruption</b>	The threat actor is motivated to attack targets engaging in corruption.
<b>Ideological - Anti-Establishment</b>	The threat actor is motivated to attack established authority
<b>Ideological - Environmental</b>	The threat actor is motivated to attack targets engaging in actions detrimental to the environment.
<b>Ideological - Ethnic / Nationalist</b>	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
<b>Ideological - Information Freedom</b>	The threat actor is motivated by the belief in the freedom of information.
<b>Ideological - Religious</b>	The threat actor is motivated to attack targets associated with a religion.
<b>Ideological - Security Awareness</b>	
<b>Ideological - Human Rights</b>	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
<b>Ego</b>	The threat actor is motivated by enhancing their own self worth.
<b>Financial or Economic</b>	The threat actor is motivated by financial gain.
<b>Military</b>	The threat actor is motivated by the desire to exercise some military advantage.
<b>Opportunistic</b>	The threat actor is motivated by the relative vulnerability of the target
<b>Political<sup>11</sup></b>	The threat actor is motivated by the desire to exercise some political advantage.

<sup>11</sup> Corrected in `MotivationVocab-1.1`

### 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 1.0.1 instead (see Section 3.27).

Enumeration Literal	Description
<b>Ideological</b>	The threat actor is motivated by non-specific ideological reasons.
<b>Ideological - Anti-Corruption</b>	The threat actor is motivated to attack targets engaging in corruption.
<b>Ideological - Anti-Establishment<sup>12</sup></b>	The threat actor is motivated to attack established authority
<b>Ideological - Environmental</b>	The threat actor is motivated to attack targets engaging in actions detrimental to the environment.
<b>Ideological - Ethnic / Nationalist</b>	The threat actor is motivated to attack targets engaging in actions either against or in favor of a nation state or ethnic group
<b>Ideological - Information Freedom</b>	The threat actor is motivated by the belief in the freedom of information.
<b>Ideological - Religious</b>	The threat actor is motivated to attack targets associated with a religion.
<b>Ideological - Security Awareness</b>	
<b>Ideological - Human Rights</b>	The threat actor is motivated to attack targets engaging in actions either in favor or against human rights.
<b>Ego</b>	The threat actor is motivated by enhancing their own self worth.
<b>Financial or Economic</b>	The threat actor is motivated by financial gain.
<b>Military</b>	The threat actor is motivated by the desire to exercise some military advantage.
<b>Opportunistic</b>	The threat actor is motivated by the relative vulnerability of the target
<b>Policial<sup>13</sup></b>	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.

<sup>12</sup> Corrected in `MotivationVocab-1.0.1`

<sup>13</sup> Corrected in `MotivationVocab-1.1`

Enumeration Literal	Description
<b>Internally-Owned</b>	The asset is owned internally.
<b>Employee-Owned</b>	The asset is owned by an employee.
<b>Partner-Owned</b>	The asset is owned by a partner.
<b>Customer-Owned</b>	The asset is owned by a customer.
<b>Unknown</b>	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
<b>Collective Threat Intelligence</b>	The package is intended to convey a broad characterization of a threat across multiple facets.
<b>Threat Report</b>	The package is intended to convey a broad characterization of a threat across multiple facets expressed as a cohesive report.
<b>Indicators</b>	The package is intended to convey mainly indicators.
<b>Indicators - Phishing</b>	The package is intended to convey mainly phishing indicators.
<b>Indicators - Watchlist</b>	The package is intended to convey mainly network watchlist indicators.
<b>Indicators - Malware Artifacts</b>	The package is intended to convey mainly malware artifact indicators.
<b>Indicators - Network Activity</b>	The package is intended to convey mainly network activity indicators.
<b>Indicators - Endpoint Characteristics</b>	The package is intended to convey mainly endpoint characteristics (hashes, registry values, installed software, known vulnerabilities, etc.) indicators.
<b>Campaign Characterization</b>	The package is intended to convey mainly a characterization of one or more campaigns.
<b>Threat Actor Characterization</b>	The package is intended to convey mainly a characterization of one or more threat actors.
<b>Exploit Characterization</b>	The package is intended to convey mainly a characterization of one or more exploits.
<b>Attack Pattern Characterization</b>	The package is intended to convey mainly a characterization of one or more attack patterns.
<b>Malware Characterization</b>	The package is intended to convey mainly a characterization of one or more malware instances.
<b>TTP - Infrastructure</b>	The package is intended to convey mainly a characterization



	of attacker infrastructure.
<b>TTP - Tools</b>	The package is intended to convey mainly a characterization of attacker tools.
<b>Courses of Action</b>	The package is intended to convey mainly a set of courses of action.
<b>Incident</b>	The package is intended to convey mainly information about one or more incidents.
<b>Observations</b>	The package is intended to convey mainly information about instancial observations (cyber observables).
<b>Observations - Email</b>	The package is intended to convey mainly information about instancial email observations (email cyber observables).
<b>Malware Samples</b>	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
<b>Data Exploitation</b>	
<b>Data Exploitation - Analytic Support</b>	
<b>Data Exploitation - Translation Support</b>	
<b>Financial Resources</b>	
<b>Financial Resources - Academic</b>	
<b>Financial Resources - Commercial</b>	
<b>Financial Resources - Government</b>	
<b>Financial Resources - Hacktivist or Grassroot</b>	
<b>Financial Resources - Non-Attributable Finance</b>	
<b>Planning</b>	
<b>Planning - Open-Source Intelligence (OSINT) Gathering</b>	
<b>Planning - Operational Cover Plan</b>	
<b>Planning - Pre-Operational Surveillance and Reconnaissance</b>	
<b>Planning - Target Selection</b>	
<b>Skill Development / Recruitment</b>	
<b>Skill Development / Recruitment - Contracting and Hiring</b>	
<b>Skill Development / Recruitment - Document Exploitation (DOCEX) Training</b>	
<b>Skill Development / Recruitment - Internal Training</b>	
<b>Skill Development / Recruitment - Military Programs</b>	
<b>Skill Development / Recruitment - Security / Hacker</b>	

<b>Conferences</b>	
<b>Skill Development / Recruitment - Underground Forums</b>	
<b>Skill Development / Recruitment - University Programs</b>	

### 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).

<b>Enumeration Literal</b>	<b>Description</b>
<b>Data Exploitation</b>	
<b>Data Exploitation - Analytic Support</b>	
<b>Data Exploitation - Translation Support</b>	
<b>Financial Resources</b>	
<b>Financial Resources - Academic</b>	
<b>Financial Resources - Commercial</b>	
<b>Financial Resources - Government</b>	
<b>Financial Resources - Hacktivist or Grassroot</b>	
<b>Financial Resources - Non-Attributable Finance</b>	
<b>Planning</b>	
<b>Planning - Open-Source Intelligence (OSINT) Gethering<sup>14</sup></b>	
<b>Planning - Operational Cover Plan</b>	
<b>Planning - Pre-Operational Surveillance and Reconnaissance</b>	
<b>Planning - Target Selection</b>	
<b>Skill Development / Recruitment</b>	
<b>Skill Development / Recruitment - Contracting and Hiring</b>	
<b>Skill Development / Recruitment – Document Exploitation (DOCEX) Training</b>	
<b>Skill Development / Recruitment - Internal Training</b>	
<b>Skill Development / Recruitment - Military Programs</b>	
<b>Skill Development / Recruitment - Security / Hacker Conferences</b>	
<b>Skill Development / Recruitment - Underground Forums</b>	
<b>Skill Development / Recruitment - University Programs</b>	

<sup>14</sup> Corrected in `PlanningAndOperationalSupportVocab-1.0.1`

### 3.34 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
<b>Yes</b>	It has been confirmed that this incident resulted in a security compromise.
<b>Suspected</b>	It is suspected that this incident resulted in a security compromise.
<b>No</b>	It has been confirmed that this incident did not result in a security compromise.
<b>Unknown</b>	It is not known whether this incident resulted in a security compromise.

### 3.35 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
<b>Enterprise Systems</b>	
<b>Enterprise Systems - Application Layer</b>	
<b>Enterprise Systems - Database Layer</b>	
<b>Enterprise Systems – Enterprise Technologies and Support Infrastructure</b>	
<b>Enterprise Systems - Network Systems</b>	
<b>Enterprise Systems - Networking Devices</b>	
<b>Enterprise Systems - Web Layer</b>	
<b>Enterprise Systems - VoIP</b>	
<b>Industrial Control Systems</b>	
<b>Industrial Control Systems – Equipment Under Control</b>	
<b>Industrial Control Systems – Operations Management</b>	
<b>Industrial Control Systems – Safety, Protection and Local Control</b>	
<b>Industrial Control Systems - Supervisory Control</b>	
<b>Mobile Systems</b>	
<b>Mobile Systems - Mobile Operating Systems</b>	
<b>Mobile Systems - Near Field Communications</b>	
<b>Mobile Systems - Mobile Devices</b>	
<b>Third-Party Services</b>	

<b>Third-Party Services - Application Stores</b>	
<b>Third-Party Services - Cloud Services</b>	
<b>Third-Party Services - Security Vendors</b>	
<b>Third-Party Services - Social Media</b>	
<b>Third-Party Services - Software Update</b>	
<b>Users</b>	
<b>Users - Application And Software</b>	
<b>Users - Workstation</b>	
<b>Users - Removable Media</b>	

### 3.36 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
<b>Innovator</b>	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.
<b>Expert</b>	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.
<b>Practitioner</b>	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.
<b>Novice</b>	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.

### 3.37 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
---------------------	-------------

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

### 3.38 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.

<b>Enumeration Literal</b>	<b>Description</b>
<b>Updates - Revises</b>	The new content represents a modified or expanded form of the previous content with existing information refined for improved quality or confidence.
<b>Updates - Corrects</b>	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.
<b>Revokes</b>	The previous content is asserted to be invalid and should not be considered for operational purposes.

## Appendix

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	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
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



## References

References made in this document are listed below.

- [CybOX<sub>COR</sub>] CybOX Core Specification (*not yet available*).
- [RFC2119] RFC 2119 – Key words for use in RFCs to Indicate Requirement Levels  
<http://www.ietf.org/rfc/rfc2119.txt>
- [STIX] STIX™ Web Site  
<https://stix.mitre.org>
- [STIX-SPECS] STIX™ Project Github Site  
<http://github.com/STIXProject/specifications>
- [STIX<sub>CAM</sub>] STIX™ 1.1.1 Campaign Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>COA</sub>] STIX™ 1.1.1 Course of Action (COA) Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>COM</sub>] STIX™ 1.1.1 Common Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>ET</sub>] STIX™ 1.1.1 Exploit Target Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>INC</sub>] STIX™ 1.1.1 Incident Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>IND</sub>] STIX™ 1.1.1 Indicator Specification (v2.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>O</sub>] STIX™ 1.1.1 Specification Overview  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>TA</sub>] STIX™ 1.1.1 Threat Actor Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>
- [STIX<sub>TTP</sub>] STIX™ 1.1.1 TTP Specification (v1.1.1)  
<http://stix.mitre.org/about/documents/XXXX.pdf>