STIX 1.x Extensions

Final

9 September 2021

​MITRE

​Editors:

Rich Piazza (rpiazza@mitre.org), MITRE Corporation

Additional artifacts:

* STIX™ Version 2.1 - OASIS Specification

Related work:

This specification replaces or supersedes:

* *N/A*

Abstract:

The stix-elevator will convert as faithfully as possible STIX 1.x content to STIX 2.1. The elevator will use the extension mechanism (defined in section 7.3 of the STIX 2.1 specification) to represent some or all of the properties in a STIX 1.x object type in STIX 2.1 content. This documentation describes the extensions used by the elevator.

Table of Contents

[1 Campaign Extension 3](#_Toc126752538)

[1.1 Extension Definition object 3](#_Toc126752539)

[1.2 Campaign Type Extension 4](#_Toc126752540)

[1.3 Intended Effect Statement Type 4](#_Toc126752541)

[1.4 Intended Effect Open Vocabulary 4](#_Toc126752542)

[1.5 Properties not in the Specification or the Extension 6](#_Toc126752543)

[1.6 Properties represented by SROs 6](#_Toc126752544)

[2 Course of Action Extension 6](#_Toc126752545)

[2.1 Extension Definition object 6](#_Toc126752546)

[2.2 Course of Action Type Extension 6](#_Toc126752547)

[2.3 High/Medium/Low Statement Type 7](#_Toc126752548)

[2.4 High-Medium-Low Open Vocabulary 8](#_Toc126752549)

[2.5 COA Stage Open Vocabulary 8](#_Toc126752550)

[2.6 Properties not in the Specification or the Extension 8](#_Toc126752551)

[2.7 Properties represented by SROs 9](#_Toc126752552)

[2.8 Example 9](#_Toc126752553)

[3 Email Message Extension 9](#_Toc126752554)

[3.1 Extension Definition Object 9](#_Toc126752555)

[3.2 Email Message Type Extension 10](#_Toc126752556)

[3.3 Properties not in the Specification or the Extension 10](#_Toc126752557)

[3.4 Example 10](#_Toc126752558)

[4 Identity Extension (CIQ sub-schema) 11](#_Toc126752559)

[4.1 Extension Definition Object 11](#_Toc126752560)

[4.2 Identity Type Extension 11](#_Toc126752561)

[4.3 Properties not in the Specification or the Extension 12](#_Toc126752562)

[4.4 Example 12](#_Toc126752563)

[5 Identity Extension (as a Victim Target) 12](#_Toc126752564)

[5.1 Extension Definition Object 12](#_Toc126752565)

[5.2 Identity Type Extension 13](#_Toc126752566)

[5.3 Properties not in the Specification or the Extension 13](#_Toc126752567)

[5.4 Example 13](#_Toc126752568)

[6 Incident Extension 14](#_Toc126752569)

[6.1 Extension Definition Object 14](#_Toc126752570)

[6.2 ​ Incident Type Extension 14](#_Toc126752571)

[6.3 Discover Method Open Vocabulary 17](#_Toc126752572)

[6.4 Incident Status Open Vocabulary 18](#_Toc126752573)

[6.5 Security Compromise Open Vocabulary 18](#_Toc126752574)

[6.6 Properties not in the Specification or the Extension 19](#_Toc126752575)

[6.7 Properties represented by SROs 19](#_Toc126752576)

[6.8 Example 19](#_Toc126752577)

[7 Indicator 20](#_Toc126752578)

[7.1 Extension Definition Object 20](#_Toc126752579)

[7.2 Indicator Type Extension 21](#_Toc126752580)

[7.3 Properties not in the Specification or the Extension 21](#_Toc126752581)

[7.4 Properties represented by SROs 21](#_Toc126752582)

[7.5 Examples 22](#_Toc126752583)

[8 Network Traffic icmp-ext Extension 22](#_Toc126752584)

[8.1 Extension Definition Object 22](#_Toc126752585)

[8.2 icmp-ext Type Extension 23](#_Toc126752586)

[8.3 Properties not in the Specification or the Extension 23](#_Toc126752587)

[8.4 Examples 23](#_Toc126752588)

[9 Network Traffic socket-ext Extension 23](#_Toc126752589)

[9.1 Extension Definition Object 23](#_Toc126752590)

[9.2 socket-ext Type Extension 24](#_Toc126752591)

[9.3 Properties not in the Specification or the Extension 24](#_Toc126752592)

[9.4 Examples 24](#_Toc126752593)

[10 Tool Extension 25](#_Toc126752594)

[10.1 Extension Definition Object 25](#_Toc126752595)

[10.2 Tool Type Extension 25](#_Toc126752596)

[10.3 Properties not in the Specification or the Extension 26](#_Toc126752597)

[10.4 Examples 26](#_Toc126752598)

# Campaign Extension

## Extension Definition object

{  
 **"id"**: **"extension-definition--d83fce45-ef58-4c6c-a3f4-1fbc32e98c6e"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x Campaigns"**,  
 **"** **"description": "This schema adds STIX 1.x Campaign properties not present in the STIX 2.1 Campaign object",**  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-12-12T00:00:00.000000Z"**,  
 **"created\_by\_ref"**:**"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## Campaign Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **intended\_effects** (optional) | list of type intended-effect-statement | This property specifies the suspected intended effect of this incident.  The values for this property **MUST** be of type intended-effect-statement. |
| **status** (optional) | open-vocab | The values for this property **SHOULD** come from the campaign-status-ov open vocabulary. |

## Intended Effect Statement Type

**Type Name:** intended-effect-statement-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **description** (optional) | string | This property contains a prose description of the intended effect. |
| **confidence** (optional) | integer | *See confidence common property definition in section 3.2 of the STIX 2.1 specification*. |
| **value** (required) | open-vocab | This property contains the intended effect.  The values for this property **SHOULD** come from the intended-effect-ov open vocabulary. |

## Intended Effect Open Vocabulary

**Type Name**: intended-effect-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| advantage |  |
| advantage-economic |  |
| advantage-military |  |
| advantage-political |  |
| theft |  |
| intellectual-property-theft |  |
| credential-theft |  |
| identity-theft |  |
| proprietary-information-theft |  |
| account-takeover |  |
| brand-damage |  |
| competitive-advantage |  |
| degradation-of-service |  |
| denial-and-deception |  |
| destruction |  |
| disruption |  |
| embarrassment |  |
| exposure |  |
| extortion |  |
| fraud |  |
| harassment |  |
| ics-control |  |
| traffic-diversion |  |
| unauthorized-access |  |

## Properties not in the Specification or the Extension

* activity

## Properties represented by SROs

|  |  |
| --- | --- |
| STIX 1.x Property | STIX 2.x Relationship Type |
| related-ttps | uses |
| related\_incidents | attributed-to |
| related\_indicators | indicates |
| attribution | attributed-to |
| associated\_campaigns | related-to |

# Course of Action Extension

## Extension Definition object

{  
 **"id"**: **"extension-definition--a46b18de-0b41-4a95-9d2d-67a360f2d859"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x Courses of Action"**,  
 **"description": "This schema adds STIX 1.x Courses of Action properties not present in the STIX 2.1 COA object",**  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-12-12T00:00:00.000000Z"**,  
 **"created\_by\_ref"**:**"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## Course of Action Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **stage** (optional) | open-vocab | This property specifies what stage in the cyber threat management lifecycle this CourseOfAction is relevant to (e.g. Remedy or Response).  The values for this property **MUST** come from the coa-stage-ov enumeration. |
| **objective** (optional) | string | The objective property characterizes the objective of this Course of Action. |
| **objective\_confidence** (optional) | string | The objective\_confidence property characterizes the level of confidence held in the applicability of this Course of Action for its targeted Objective. |
| **parameter\_expression**  (optional) | string | This property enables the specification of technical parameters to this Course of Action expressed as a STIX pattern |
| **impact** (optional) | hml-statement-type | This property characterizes the estimated impact of applying this Course of Action. |
| **cost** (optional) | hml-statement-type | This property characterizes the estimated cost for applying this C Course of Action. |
| **efficacy** (optional) | hml-statement-type | This property characterizes the effectiveness of this Course of Action in achieving its targeted Objective. |

## High/Medium/Low Statement Type

**Type Name:** hml-statement-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **description** (required) | string | This property contains a prose description of the statement. |
| **confidence** (optional) | integer | *See confidence common property definition in section 3.2 of the STIX 2.1 specification*. |
| **value** (required) | high-medium-low-ov | This property contains the level of the statement’s subject.  The values for this property **MUST** come from the high-medium-low-ov enumeration. |

## High-Medium-Low Open Vocabulary

**Type Name**: high-medium-low-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| high | It has been confirmed that this incident resulted in a security compromise. |
| medium | It is suspected that this incident resulted in a security compromise. |
| low | It has been confirmed that this incident did not result in a security compromise. |
| none |  |
| unknown |  |

## COA Stage Open Vocabulary

**Type Name**: coa-stage-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **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 an immediate reaction to an ongoing threat. |

## Properties not in the Specification or the Extension

* structured\_coa

## Properties represented by SROs

|  |  |
| --- | --- |
| STIX 1.x Property | STIX 2.x Relationship Type |
| related-coas | related-to |

## Example

{  
 **"created"**: **"2015-07-31T11:24:39.090Z"**,  
 **"extensions"**: {  
 **"extension-definition--a46b18de-0b41-4a95-9d2d-67a360f2d859"**: {  
 **"extension\_type"**: **"property-extension"**,  
 **"impact"**: {  
 **"description"**: **"Some description about the indicator."**,  
 **"value"**: **"medium"** },  
 **"objective"**: **"Block outbound traffic"**,  
 **"objective\_confidence"**: **"High"**,  
 **"stage"**: **"response"** }  
 },  
 **"id"**: **"course-of-action--3dbfccad-1fbb-4e9f-8307-f2d1a5c651cc"**,  
 **"labels"**: [  
 **"perimeter-blocking"** ],  
 **"modified"**: **"2015-07-31T11:24:39.090Z"**,  
 **"name"**: **"Block outbound traffic"**,  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"course-of-action"**}

# Email Message Extension

## Extension Definition Object

{  
 **"id"**: **"extension-definition--0d4dda28-1b6c-446a-be85-38b9d9cd297c"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x email-message"**,  
 **"description": "This schema adds STIX 1.x Email Messages properties not present in the STIX 2.1 Email Message object",**  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-12-12T00:00:00.000000Z"**,  
 **"created\_by\_ref"**:**"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x/"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## Email Message Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **link\_refs** (optional) | list of type identifier | This property identifies any URL that is found in the email message.  The objects referenced in this property **MUST** be of type url. |
| **message\_id** (optional) | string | This property specifies the automatically generated ID of the email message.  *This property is available in STIX 2.1* |

## Properties not in the Specification or the Extension

* email\_server
* raw\_header

## Example

{  
 **"additional\_header\_fields"**: {  
 **"X-Mailer"**: **"Microsoft Outlook Express 6.00.2800.1437"** },  
 **"extensions"**: {  
 **"extension-definition--0d4dda28-1b6c-446a-be85-38b9d9cd297c"**: {  
 **"extension\_type"**: **"property-extension"**,  
 **"link\_refs"**: [  
 **"url--85336f56-d406-530a-a485-f28a369e6b36"** ]  
 }  
 },  
 **"from\_ref"**: **"email-addr--b5c16ad8-a113-5b9b-82f9-1d54ddcae49b"**,  
 **"id"**: **"email-message--1a205fb0-7ab4-5786-bb7b-0e8bd60be8ae"**,  
 **"is\_multipart"**: **false**,  
 **"message\_id"**: **"201602112058.u1BKfrXh004925@mail-gw-01.oit.duke.edu"**,  
 **"raw\_email\_ref"**: **"artifact--9a975970-092c-56e0-9b23-e586774acb51"**,  
 **"subject"**: **"Fix The Error On Your Account."**,  
 **"type"**: **"email-message"**}

# Identity Extension (CIQ sub-schema)

## Extension Definition Object

{  
 **"id"**: **"extension-definition--ec1760d6-6e8a-4a13-8237-574e5bbcc785"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x CIQ Identities"**,  
 **"description"**: **"This schema adds STIX 1.x CIQ Identity properties not present in the STIX 2.1 Identity object",**  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-12-12T00:00:00.000000Z"**,  
 **"created\_by\_ref"**: **"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,

**"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: \_EXTENSION\_SCHEMA\_URL,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## Identity Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **information\_source\_roles** (optional) | list of type string | This property enables characterization of the sourcing role played by this identity.  The values **MAY** come from <https://stixproject.github.io/data-model/1.2/stixVocabs/InformationSourceRoleVocab-1.0/>  *The* **roles** *property is available in STIX 2.1* |
| **free\_text\_lines** (optional) | string | This property captures free text used to describe this identity.  The values **SHOULD** come from https://stixproject.github.io/data-model/1.2/stixVocabs/InformationTypeVocab-1.0/ |

## Properties not in the Specification or the Extension

The CIQ schema is extremely complex (see <http://www.oasis-open.org/committees/ciq>) most of which is not covered in the extension definition.

## Example

{  
 **"created"**: **"2015-05-15T09:00:00.000Z"**,  
 **"created\_by\_ref"**: **"identity--aeb57d1a-d038-4aab-9207-5004a6631c33"**,  
 **"extensions"**: {  
 **"extension-definition--ec1760d6-6e8a-4a13-8237-574e5bbcc785"**: {  
 **"extension\_type"**: **"property-extension"**,  
 **"free\_text\_lines"**: **" The group does not target industries systematically but\n\t\t\t\t\t\t\tmore likely steals from an enormous range of industries on a continuous\n\t\t\t\t\t\t\tbasis. Organizations in all industries related to China’s\n\t\t\t\t\t\t\tstrategic priorities are potential targets of APT1’s comprehensive cyber\n\t\t\t\t\t\t\tespionage campaign. "** }  
 },  
 **"id"**: **"identity--c63f31ac-871b-4846-aa25-de1926f4f3c8"**,  
 **"modified"**: **"2015-05-15T09:00:00.000Z"**,  
 **"name"**: **"APT1 Tactics, Techniques and Procedures"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--01d8ae23-a694-47c6-96a0-ef76d39a122f"** ],  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"identity"**}

# Identity Extension (as a Victim Target)

## Extension Definition Object

{  
 **"id"**: **"extension-definition--8f0b8ed7-c7ad-4650-babe-c4c45cac4a0b"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name": "Extension to support STIX 1.x Victim Targeting",**

**"description": "This schema adds STIX 1.x Victim Targeting properties not present in the STIX 2.1 Identity object",**

**"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-11-22T13:30:51.000000Z "**,  
 **"created\_by\_ref"**:**"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x/"**, **"**

**“version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## Identity Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **targeted\_systems** (optional) | list of type string | This property characterizes a type of systems that are targeted.  The values **SHOULD** come from https://stixproject.github.io/data-model/1.2/stixVocabs/SystemTypeVocab-1.0/. |
| **targeted\_information** (optional) | list of type string | This property characterizes a type of information that is targeted.  The values **SHOULD** come from https://stixproject.github.io/data-model/1.2/stixVocabs/InformationTypeVocab-1.0/ |

## Properties not in the Specification or the Extension

* targeted\_technical\_details

## Example

{  
 **"created"**: **"2014-08-08T15:50:10.983Z"**,  
 **"extensions"**: {  
 **"extension-definition--8f0b8ed7-c7ad-4650-babe-c4c45cac4a0b"**: {  
 **"extension\_type"**: **"property-extension"**,  
 **"targeted\_information"**: [  
 **"Information Assets - Financial Data"** ]  
 }  
 },  
 **"id"**: **"identity--2d1c6ab3-5e4e-48ac-a32b-f0c01c2836a8"**,  
 **"identity\_class"**: **"unknown"**,  
 **"modified"**: **"2014-08-08T15:50:10.983Z"**,  
 **"name"**: **"Victim Targeting: Customer PII and Financial Data"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"** ],  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"identity"**}

# Incident Extension

## Extension Definition Object

{  
 **"id"**: **"extension-definition--7a8eaf47-9b0f-487d-b280-1e6cc4cccee9"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x Incident"**,  
 **"description"**: **"This schema adds STIX 1.x Incident properties not present in the STIX 2.1 Incident stub object"**,  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-11-22T13:30:51.000000Z"**,  
 **"created\_by\_ref"**:**"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x/"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## ​Incident Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **contact\_refs** (optional) | list of type identifier | This property identifies and characterizes organizations or personnel involved in this Incident.  The objects referenced in this property **MUST** be of type identity. |
| **coordinator\_refs** (optional) | list of type identifier | This property is optional and details information about the assigned coordinator for this Incident.  The objects referenced in this property **MUST** be of type identity. |
| **discovery\_methods** (optional) | list of type open-vocab | This property identifies how the incident was discovered.  The values for this property **SHOULD** come from the discovery\_method-ov open vocabulary. |
| **reporter\_ref** (optional) | identifier | This property details information about the reporting source of this Incident.  The object referenced in this property **MUST** be of type identity. |
| **responder\_refs** (optional) | list of type identifier | This property details information about the assigned responder for this Incident.  The objects referenced in this property **MUST** be of type identity. |
| **security\_compromise** (optional) | open-vocab | This property specifies knowledge of whether the Incident involved a compromise of security properties.  The values for this property **SHOULD** come from the security-compromise-ov open vocabulary. |
| **status** (optional) | open-vocab | This property describes the current status (sometimes called "state" or "disposition") of the incident.  The values for this property **SHOULD** come from the incident-status-ov open vocabulary. |
| **victim\_refs** (optional) | list of type identifier | This property details information about a victim of this Incident.  The objects referenced in this property **MUST** be of type identity. |
| **intended\_effects** (optional) | list of type intended-effect-statement | This property specifies the suspected intended effect of this incident.  The values for this property **MUST** be of type intended-effect-statement. |
| **time\_of\_first\_malicious\_action** | timestamp | This property specifies the time that the first malicious action related to this Incident occurred. |
| **time\_of\_initial\_compromise** | timestamp | This property specifies the time that the initial compromise occurred for this Incident. |
| **time\_of\_first\_data\_exfiltration** | timestamp | This specifies the first time at which non-public data was taken from the victim environment. |
| **time\_of\_incident\_discovery** | timestamp | This property specifies the first time at which the organization learned the incident had occurred. |
| **time\_when\_incident\_opened** | timestamp | This property specifies the time at which the Incident was officially opened |
| **time\_when\_containment\_achieved** | timestamp | This property specifies the first time at which the incident is contained (e.g., the “bleeding is stopped”). |
| **time\_when\_restoration\_achieved** | timestamp | This property specifies the first time at which the incident's assets are restored (e.g., fully functional)”. |
| **time\_when\_incident\_reported** | timestamp | This property specifies the time at which the Incident was reported. |
| **time\_when\_incident\_closed** | timestamp | This property specifies the time at which the Incident was officially closed. |

## Discover Method Open Vocabulary

**Type Name**: discover-method-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| agent-disclosure | This incident was disclosed by the threat agent (e.g. public brag, private blackmail). |
| external-fraud-detection | This incident was discovered through external fraud detection means (e.g. CPP). |
| monitoring-service | This incident was reported by a managed security event monitoring service. |
| law-enforcement | This incident was reported by law enforcement. |
| customer | This incident was reported by a customer or partner affected by the incident. |
| unrelated-party | This incident was reported by an unrelated third party. |
| audit | This incident was discovered during an external security audit or scan. |
| antivirus | This incident was discovered by an antivirus system. |
| incident-response | This incident was discovered in the course of investigating a separate incident. |
| financial-audit | This incident was discovered in the course of a financial audit and/or reconciliation process. |
| internal-fraud-detection | This incident was discovered through internal fraud detection means. |
| hips | This incident was discovered a host-based IDS or file integrity monitoring. |
| it-audit | This incident was discovered by an internal IT audit or scan. |
| log-review | This incident was discovered during a log review process or by a SIEM. |
| nids | This incident was discovered by a network-based intrusion detection/prevention system. |
| security-alarm | This incident was discovered by a physical security alarm. |
| user | This incident was reported by a user. |
| unknown | It is not known how this incident was discovered. |

## Incident Status Open Vocabulary

**Type Name**: incident-status-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| new |  |
| open |  |
| stalled |  |
| containment-achieved |  |
| restoration-achieved |  |
| incident-reported |  |
| closed |  |
| rejected |  |
| deleted |  |

## Security Compromise Open Vocabulary

**Type Name**: security-compromise-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **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. |

## Properties not in the Specification or the Extension

* categories
* affected\_assets
* impact\_accessment

## Properties represented by SROs

|  |  |
| --- | --- |
| STIX 1.x Property | STIX 2.x Relationship Type |
| related\_observables | part-of |
| related\_indicators | indicates |
| leverged\_ttps | related-to |
| coa\_taken | used |
| coa\_requested | mitigates |
| attributed\_threat\_actors | attributed-to |

## Example

{  
 **"created"**: **"2014-05-08T09:00:00.000Z"**,  
 **"id"**: **"identity--6e85a81b-5fd8-46c0-ba46-df128771f695"**,  
 **"modified"**: **"2014-05-08T09:00:00.000Z"**,  
 **"name"**: **"Fred"**,  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"identity"**},  
{  
 **"created"**: **"2014-05-08T09:00:00.000Z"**,  
 **"id"**: **"identity--c0cdd136-daa0-40ef-8957-a0e686fcd0d2"**,  
 **"modified"**: **"2014-05-08T09:00:00.000Z"**,  
 **"name"**: **"Barney"**,  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"identity"**},  
{  
 **"created"**: **"2014-05-08T09:00:00.000Z"**,  
 **"extensions"**: {  
 **"extension-definition--7a8eaf47-9b0f-487d-b280-1e6cc4cccee9"**: {  
 **"contact\_refs"**: [  
 **"identity--6e85a81b-5fd8-46c0-ba46-df128771f695"**,  
 **"identity--c0cdd136-daa0-40ef-8957-a0e686fcd0d2"** ],  
 **"discovery\_methods"**: [  
 **"log-review"**,  
 **"antivirus"** ],  
 **"extension\_type"**: **"property-extension"**,  
 **"intended\_effects"**: [  
 {  
 **"description"**: **"Bring down server"**,  
 **"value"**: **"degradation-of-service"** }  
 ],  
 **"security\_compromise"**: **"suspected"**,  
 **"status"**: **"containment-achieved"**,  
 **"time\_of\_incident\_discovery"**: **"2014-05-02T02:10:16.000000Z"**,  
 **"time\_when\_containment\_achieved"**: **"2014-05-07T08:00:00.000000Z"**,  
 **"time\_when\_incident\_reported"**: **"2014-05-07T02:00:00.000000Z"** }  
 },  
 **"external\_references"**: [  
 {  
 **"external\_id"**: **"81645723"**,  
 **"source\_name"**: **"JIRA"** }  
 ],  
 **"id"**: **"incident--1b75ee8f-44d6-419a-9729-09ab52c91fdb"**,  
 **"labels"**: [  
 **"denial-of-service"** ],  
 **"modified"**: **"2014-05-08T09:00:00.000Z"**,  
 **"name"**: **"Detected Poison Ivy beaconing through perimeter firewalls"**,  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"incident"**}

# Indicator

## Extension Definition Object

{  
 **"id"**: **"extension-definition--7c8ca481-f0e9-4389-94f5-90df472eb01d"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x Indicators"**,  
 **"description"**: **"This schema adds STIX 1.x Indicator properties not present in the STIX 2.1 Indicator object"**,  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-11-22T13:30:51.000000Z"**,  
 **"created\_by\_ref"**: **"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x/"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## **Indicator Type Extension**

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **likely\_impact** (optional) | hml-statement-type | Specifies the likely potential impact within the relevant context if this Indicator were to occur. This is typically local to an Indicator consumer and not typically shared. This field includes a Description of the likely potential impact within the relevant context if this Indicator were to occur and a Confidence held in the accuracy of this assertion.  See Section [1.3](#_High/Medium/Low_Statement_Type) for information on hml-statement-type |

## Properties not in the Specification or the Extension

n/a

## Properties represented by SROs

|  |  |
| --- | --- |
| STIX 1.x Property | STIX 2.x Relationship Type |
| Suggested\_coas | investigates |
| related\_campaigns | attributed-to |
| indicated\_ttps | indicates |
| related\_indicators | related-to |

## Examples

{  
 **"created"**: **"2020-12-30T16:03:21.950Z"**,  
 **"id"**: **"indicator--d81f86b9-975b-bc0b-775e-810c5ad45a4f"**,  
 **"indicator\_types"**: [  
 **"url-watchlist"** ],  
 **"modified"**: **"2020-12-30T16:03:21.950Z"**,  
 **"name"**: **"Malicious site hosting downloader"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--c0d0976c-76a1-4cf2-accd-19632991ac3f"** ],  
 **"pattern"**: **"[url:value = 'http://x4z9arb.cn/4712']"**,  
 **"pattern\_type"**: **"stix"**,  
 **"spec\_version"**: **"2.1"**,  
 **"type"**: **"indicator"**,  
 **"valid\_from"**: **"2020-12-30T16:03:21.950Z",**

**"extensions"**: {

**"extension-definition--7c8ca481-f0e9-4389-94f5-90df472eb01d"**: {

**"extension\_type"**: **"property-extension"**,

**"likely\_impact"**: {

**"description"**: **"really good"**,

**"value"**: **"high"**,

}

]}

# Network Traffic icmp-ext Extension

## Extension Definition Object

{  
 **"id"**: **"extension-definition--6f6973cb-70be-40cb-b1ac-15ed78cebe56"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name": "Extension to support STIX 1.x/CybOX 2.1 Network Packet ICMP IPV4 properties",**

**"description": "This schema adds STIX 1.x/CybOX 2.1 Network Packet ICMP IPV4 properties in the STIX 2.x Network Traffic object", # noqa**  
 **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-12-12T00:00:00.000000Z"**,  
 **"created\_by\_ref"**: **"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## **icmp-ext Type Extension**

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **checksum\_hex** (optional) | hex | Specifies the ICMP checksum (16 bits) covers the ICMP message. |

## Properties not in the Specification or the Extension

n/a

## Examples

{  
 **"extensions"**: {  
 **"extension-definition--6f6973cb-70be-40cb-b1ac-15ed78cebe56"**: {  
 **"checksum\_hex"**: **"97c02164528d"**,  
 **"extension\_type"**: **"property-extension"** },  
 **"icmp-ext"**: {  
 **"icmp\_code\_hex"**: **"00"**,  
 **"icmp\_type\_hex"**: **"08"** }  
 },  
 **"id"**: **"network-traffic--8ef22721-8c32-5c85-81f9-cdfe162d1e72"**,  
 **"protocols"**: [  
 **"icmp"** ],  
 **"type"**: **"network-traffic"**}

# Network Traffic socket-ext Extension

## Extension Definition Object

{  
 **"id"**: **"extension-definition--005e229c-fffc-42b0-a912-84671ab2829d"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x/CybOX 2.1 Network Sockets"**,  
 **"description"**: **"This schema adds STIX 1.x/CybOX 2.1 Network Sockets properties not present in the STIX 2.1 Network Traffic object"**, *# noqa* **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"created\_by\_ref"**: **"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## **socket-ext Type Extension**

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **local\_address** (optional) | string | Specifies the IP address and port for the socket on the local machine |
| **protocol\_family** (optional) | string | Specifies the communication domain (PF\_\*) of the socket" |
| **remote\_address** (optional) | string | Specifies the IP address and port for the socket on the remote machine |

## Properties not in the Specification or the Extension

n/a

## Examples

{  
 **"extensions"**: {  
 **"extension-definition--005e229c-fffc-42b0-a912-84671ab2829d"**: {  
 **"extension\_type"**: **"property-extension"**,  
 **"local\_address"**: **"198.51.100.2"** },  
 **"socket-ext"**: {  
 **"address\_family"**: **"AF\_INET"**,  
 **"is\_listening"**: **true**,  
 **"options"**: {  
 **"IP\_MULTICAST\_LOOP"**: 1  
 }  
 }  
 },  
 **"id"**: **"network-traffic--d8301f41-2ed7-599a-9851-02c19eeaca42"**,  
 **"protocols"**: [  
 **"tcp"** ],  
 **"type"**: **"network-traffic"**}

# Tool Extension

## Extension Definition Object

{  
 **"id"**: **"extension-definition--683e2ed4-80fb-4910-a179-64e88ac6c259"**,  
 **"type"**: **"extension-definition"**,  
 **"spec\_version"**: **"2.1"**,  
 **"name"**: **"Extension to support STIX 1.x Tools"**,  
 **"description"**: **"This schema adds STIX 1.x Tool properties not present in the STIX 2.1 Tool object"**, *# noqa* **"created"**: **"2020-12-22T00:00:00.000000Z"**,  
 **"modified"**: **"2022-12-12T00:00:00.000000Z"**,  
 **"created\_by\_ref"**: **"identity--659e8342-f720-4d0d-b193-6a04fdfbb401"**,  
 **"object\_marking\_refs"**: [  
 **"marking-definition--3cd55916-d34b-4747-a8e0-dedec14b711b"**  
 ],  
 **"schema"**: **"https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/stix-1x"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

## Tool Type Extension

**Type Name:** n/a

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **vendor** (optional) | string | This property contains information identifying the vendor organization for this tool. |
| **service\_pack** (optional) | string | This property contains an appropriate service pack descriptor for this tool. |
| **title** (optional) | string | This property provides a simple title for a single tool leveraged.  *This property is only present if both the name and title fields are present in the STIX 1.x object.* |

## Properties not in the Specification or the Extension

* tool\_configration
* execution\_environment
* errors
* compensation\_model
* tool\_specific\_data
* tool\_hashes
* metadata

## Examples