STIX 1.x Incident Extension

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 extension for the Incident object

# 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"**: **"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/stix1-incident/"**,  
 **"version"**: **"1.0.0"**,  
 **"extension\_types"**: [**"property-extension"**]  
}

### ​**2.****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. |

## 2.1 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. |

## 2.10 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. |

## 2.10 Incident Status Open Vocabulary

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

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

## 2.10 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 |  |

## 2.10 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. |

## 3. 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"**}

# ​