Incident Core Extension Version 1.0 for STIX™ Version 2.1

Draft

17 August 2021

Department of Defense Cyber Crime Center

​Editors:

(acronym) – (full name)

Additional artifacts:

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

* STIX™ Version 2.1 - OS

Related work:

This specification replaces or supersedes:

* *N/A*

Abstract:

The current STIX 2.1 Incident object exists as a stub in the hopes that future work would allow STIX Incidents to be more fully fleshed out using extensions, and that in time a set of core features could be defined to be migrated into a future version of the Incident object or the community could arrive at the consensus to continue to use these extensions.

This extension is focused on the core features of an incident across its life cycle by providing mechanisms to record the status of the incident, its impacts, attacker and defender activities, and related observables. This also provides both new means and examples of connections to a number of existing STIX Objects in order to facilitate highly interoperable verbose reporting that does not overburden analysts to initially generate or maintain.

# 1.​ Incidents in STIX

Incidents in STIX represent potential incidents that require investigation, confirmed incidents and items that were flagged as incidents but later dismissed as false positives. The incident core extension exists to allow a whole lifecycle approach for Incident response, reporting and tracking throughout its entire lifecycle while also allowing this information to be easily queried against at scale by systems that exchange STIX 2.1 Incident data.

### ​**2.****Incident Core Extension**

The properties and sub-objects within the Incident Core Extension are defined bellow. As this is not a top-level object fields such as identifier are not present.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **determination** (required) | incident-determination-enum | If the incident has been confirmed or is suspected. If it is determined to be benign it is considered a false-positive as defined by incident-status-enum. |
| **extension\_type** (required) | string | The value of this property **MUST** be property-extension |
| **investigation\_status** (required) | incident-investigation-enum | The current status of the incident investigation. This can be “new”, “open” or “closed” as defined by the investigation-status-enum. |
| **attacker\_activities** (optional) | list of type attacker-activity-type | A list of attacker focused activities associated with the Incident including information about when these occurred. |
| **criticality** (optional) | incident-criticality-enum | How important this incident is to operations. |
| **defender\_activities** (optional) | list of type defender-activity-type | A list of time relevant activities performed by the defender to the lifecycle of this incident, such as when it was first detected, when the investigation started, when remediation was started / completed. |
| **detection\_methods** (optional) | open-vocab | A list of strings containing what was used to detect the activity, ex. commercial tool names, techniques associated with proprietary solutions, human review, external sources, or other methods. This should draw from the detection-methods-ov. |
| **external\_impacts**  (optional) | list of type open-vocab | The scope of impact outside of the direct organization that should be drawn from external-impact-ov. |
| **functional\_impact** (optional) | functional-impact-enum | The functional impact of the incident on operations |
| **incident\_types** (optional) | list of type open-vocab | This property uses an Open Vocabulary that specifies the type of incident that occurred, if applicable. This is an open vocabulary and values SHOULD come from the incident-type-ov. |
| **information\_impacts** (optional) | list of type information-impact-type | If information has been lost, compromised or otherwise corrupted. Multiple items can be entered here as an incident can include multiple forms of data theft or destruction. |
| **mitigation** (optional) | string | A description of the steps taken to mitigate this incident.  If available this can be further detailed within defender activity, but this captures a high-level narrative of what has been done instead of a more step by step chain of action. |
| **observable\_refs** (optional) | list of type identifier | A list of all observed data that was part of this incident. This can relate directly to SCOs, but can also reference Sightings, Observables, and Indicators. |
| **recoverability** (optional) | recoverability-enum | The scope of impact required to recover from an incident. |

#### 2.1 Information Impact Object Type

**Type Name:** information-impact-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **impact** (required) | information-impact-enum | The impact experienced to the information defined by the type. |
| **type** (required) | string | The type of information being impacted by this. If more than one impact exists for the same type of information separate objects should be used for each combination.  This should be drawn from that should be drawn from information-impact-type-ov. |

#### 2.2 Defender Activity Object Type

**Type Name:** defender-activity-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **timestamp** (required) | timestamp | When this activity occurred. |
| **type** (required) | string | A general type for the timestamp for higher level rollups. This should be drawn from defender-activity-ov.  Timestamps types that mark the start or completion of a task should end with:  -started and -completed respectively. |
| **course\_of\_action\_ref** (optional) | identifier (of type course-of-action) | This property contains the date an original classification determination was made. |
| **description** (optional) | string | A description of the adversary activity that occurred. |
| **is\_projection** (optional) | boolean | If this is a projection of when a future event will occur for example when recovery is projected to be completed for an incident. |

#### 2.3 Attacker Activity Object Type

**Type Name:** attacker-activity-type

All properties in this object type are optional. However, either a type or pattern\_ref **MUST** be present. Both may be provided if desired, but in order to support mapping more general actions and milestones against a timeline that do not correspond with Attack Patterns the option to include a type value instead of a pattern\_ref is supported.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **type** (optional) | string | A general type for the timestamp for higher level rollups.  This is not necessary if a pattern\_ref is supplied, but is required if one is not present. |
| **description** (optional) | string | A description of adversary activity that occurred beyond what the type or associated attack pattern may provide. |
| **pattern\_ref** (optional) | identifier (of type attack-pattern) | A reference to an attack-pattern that details a TTP used during this time range. If the attacker used multiple attack patterns additional attacker activity objects should be used.  If this is present the type field is not required. |
| **start\_time** (optional) | timestamp | The date the activity was first recorded. If this is not present it is assumed to be unknown. |
| **end\_time** (optional) | timestamp | The date the activity was last recorded. If this is not present it is assumed to be unknown. |

## 3. Vocabularies

## 3.1 Defender Activity Vocabulary

**Type Name**: defender-activity-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| containment-completed | When containment was completed |
| containment-started | When containment was started |
| declared | When this was officially declared an incident |
| detected | When the incident was detected |
| eradication-completed | When eradication was completed |
| eradication-started | When eradication was started |
| escalated | When the incident was escalated to a major incident |
| recovery-completed | When recovery was completed |
| recovery-started | When recovery was started |
| reported | When the incident was reported externally |

## 3.2 Detection Methods Vocabulary

**Type Name**: detection-methods-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| automated-tool | An incident is detected by an automated tool. If this option is used it is generally useful to also include a separate entry for the tool itself. |
| human-review | An incident is detected by human threat hunting. |
| message-from-attacker | Notification comes from a message provided by the attacker including email, a note left of a message or popup message. |
| system-outage | An incident is detected because a system is no longer available. |
| user-reporting | One or more users report an incident. |

## 3.3 External Impact Vocabulary

**Type Name**: external-impact-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| civil-liberties | This incident is expected to impact the ability of citizens of one or more countries to exercise their civil liberties either directly, or indirectly by leaking information that can be used against them by public or private institutions. |
| economic | This incident is expected to have national or international economic impacts. |
| foreign-relations | This incident impacts international politics. |
| national-security | This incident impacts the national security of one or more nations. |
| public-confidence | This incident impacts the confidence in public or private institutions. |
| public-health | This incident impacts the public health of one or more nations. |

## 3.4 Incident Type Vocabulary

**Type Name**: incident-type-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| blocked | The incident was blocked by pre-emptive measures including rate limiting or spam filters. |
| compromised-system | Attackers obtained control of a compromised system |
| destruction | The incident destroyed data or systems. |
| equipment-loss | A loss of control of physical equipment. |
| failed-attempt | The incident didn't succeed but not due to any affirmative defense for example a password guesser failed but was also not rate limited. |
| major | The incident is classified as major based on the internal criteria within the organization or due to external reporting requirements. |
| supply-chain-customer | This incident used a vendor further up in the supply chain where the target was a customer. |
| supply-chain-vendor | This incident targeted a system or product that is supplied to others to enable further attacks. |
| unauthorized-access | Unauthorized access to information. |
| unauthorized-release | The unauthorized release of information. |
| under-investigation | The incident is still under investigation. |

## 3.5 Information Impact Type Vocabulary

**Type Name**: information-impact-type-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| classified-material | Data classified based on relevant government authorities |
| communication | Communication records including emails, chats and instant messages |
| credentials-admin | Administrative credential data |
| credentials-user | User credential data |
| financial | Financial records including purchasing activity and planned activities. |
| legal | Legal records that are not yet public including contracts under negotiation and documents protected under legal privilege |
| payment | Payment information |
| phi | Protected Health Information |
| pii | Personally Identifiable Information |
| proprietary | Proprietary information |

## 4. Enumerations

## 4.1 Functional Impact Enumeration

**Type Name**: functional-impact-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| denial | A critical system has been rendered unavailable |
| loss-of-control | The system is no longer under the control of the owner |
| minimal | A small impact to a system or service |
| none | No impact on functionality |
| significant | A significant impact to a system or service |

## 4.2 Incident Criticality Enumeration

**Type Name**: incident-criticality-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| critical | This incident impacts critical areas of operation. |
| deprecated | This incident impacts only deprecated systems that are not necessary for business operations. |
| non-critical | This incident impacts areas of operation, but not critical ones. |

## 4.3 Incident Determination Enumeration

**Type Name**: incident-determination-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| confirmed | An incident has been confirmed.  A confirmed incident does not indicate the attacker was successful. The success or failure of the attacker is mapped by other fields. |
| false-positive | An incident was determined to have been triggered by a false alert and not action including automatically performed automated actions were needed to remediate the issue. |
| suspected | An incident is suspected, but not yet confirmed. |

## 4.4 Incident Investigation Enumeration

**Type Name**: incident-investigation-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| closed | All defender work on this incident has been concluded. In some cases, blue teams may map child Incidents off of a closed Incident. In these cases, it is appropriate to mark an initial Incident as closed as long as the related child incidents that track this work are still open. |
| new | A new incident that has not begun the formal workflow on the defender’s network. |
| open | An open incident that is currently being worked. |

## 4.5 Information Impact Enumeration

**Type Name**: information-impact-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| destruction | The information in question has been destroyed or otherwise rendered permanently inaccessible. |
| loss | Information has been exfiltrated and is now available to the attacker. |
| major-loss | Information has been exfiltrated and is now available to the attacker, and given the nature and scale of this information loss this mandates higher-level reporting based on the laws or contracts that cover this type of information. |
| suspected | It is suspected but not confirmed that the attacker may have destroyed or gained access to this information. |

## 4.6 Recoverability Enumeration

**Type Name**: recoverability-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| extended | Time to recovery is unpredictable; additional resources and outside help are necessary. |
| not-applicable | No recovery is necessary. |
| not-recoverable | Recovery from the incident is not possible. |
| regular | Time to recovery is predictable with existing resources. |
| supplemented | Time to recovery is predictable with additional resources. |

# ​Appendix A. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| 01 | 2021-08-17 | Jeffrey Mates | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |