Incident Core Extension Version 1.1 for STIX™ Version 2.1

27 October 2022

Incident Mini Group

​Editors:

IMG – Incident Mini Group

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 extension 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

Incident objects represent events that have occurred and require further consideration or investigation. The Incident object should have sufficient properties to represent the current state of the Incident with respect to impact to the enterprise. For example, an incident may (or may not) have an impact that justifies the cost of immediate remediation or mitigation.

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 additional types within the Incident Core Extension are defined below. As this is not a top-level object, fields such as identifier are not present.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **determination** (required) | enum | A high level determination on the outcome of this incident. This **SHOULD** be suspected until enough information is available to provide a well researched result.  Some automated tools may flag results as blocked or low-value automatically depending on the tool type or activity. A tool that blocks a series of phishing emails may create an incident with a blocked determination automatically.  The values of this property **MUST** come from the incident-determination-enum enumeration. |
| **extension\_type** (required) | string | The value of this property **MUST** be property-extension |
| **investigation\_status** (required) | open-vocab | The current status of the incident investigation.  The values of this property **MUST** come from the incident-investigation-ov enumeration. |
| **attacker\_activities** (optional) | list of type attacker-activity | A list of attacker focused activities associated with the Incident including information about when these occurred. |
| **availability\_impact** (optional) | integer | The availability / functional impact of the incident on operations.  This value **MUST** bebetween 0 to 100. This can be translated into qualitative values as described in Appendix B. |
| **confidentiality\_impacts** (optional) | list of type confidentiality-impact | Information that has been stolen, compromised, or that may have been stolen or compromised as part of this incident.  Multiple items can be entered here as an incident can include multiple forms of data theft. |
| **criticality** (optional) | integer | The criticality of the incident. This value **MUST** bebetween 0 to 100. This can be translated into qualitative values as described in Appendix A. |
| **defender\_activities** (optional) | list of type defender-activity | 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) | list of type open-vocab | A list of strings containing what was used to detect the activity, e.g., 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. |
| **impacted\_entity\_counts** (optional) | entity-count | An optional listing of the entity types that were impacted and how many of each were affected.    If this field is not present it should be assumed that this information is not being shared, not that there were no impacted entities. |
| **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. |
| **integrity\_impacts** (optional) | list of type integrity-impact | Information that has been altered or destroyed as part of this incident.  Multiple items can be entered here as an incident can include multiple forms of data tampering and destruction. |
| **monetary\_impacts** (optional) | list of type monetary-impact | A list of monetary impacts that can affect an organization’s ability to remain viable.  Multiple items can be entered here as an incident can include multiple forms of costly damage. |
| **physical\_impacts** (optional) | list of type physical-impact | A list of physical impacts for this incident. This can include physically damaged or destroyed property or systems. |
| **recoverability** (optional) | enum | The recoverability of this particular Incident with respect to feasibility and required time and resources.  The values of this property **MUST** come from the recoverability-enum enumeration |
| **scores** (optional) | list of type incident-score | A list of scores from various automated or manual mechanisms along with optional descriptions. |
| **traceability\_impact** (optional) | enum | The impact of this incident on a system or organization’s ability to perform audits or provide non-repudiation.  The values of this property **MUST** come from the traceability-enum enumeration |

#### 

## 2.1 Attacker Activity Object Type

**Type Name:** attacker-activity

Attacker activity supports encoding both specific timestamp and relative sequence information for attacker activities when known or suspected. The sequence values for various attacker activities can overlap with each other when it is unknown what order the events took place in, or if it really was the case that multiple attacker activities were present at a time. When captured, these features are intended to allow mapping against complex sequence diagrams and attacker playbooks.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **outcome** (required) | activity-outcome-enum | The outcome of the attacker activity. |
| **description** (optional) | string | A description of adversary activity that occurred beyond what the type or associated attack pattern may provide. |
| **goal** (optional) | string | The attacker’s assumed objective when performing this activity. |
| **kill\_chain\_phases** (optional) | list of type kill-chain-phase | The kill chain phase(s) to which this attacker activity corresponds. |
| **pattern\_ref** (optional) | identifier of type attack-pattern | A reference to an attack-pattern that details a TTP used during this time range. This attack pattern **SHOULD** use MITRE ATT&CK whenever possible.  If the attacker used multiple attack patterns additional attacker activity objects **SHOULD** be used. |
| **start\_time** (optional) | timestamp | The date and time the activity was first recorded. If this is not present it is assumed to be unknown.  This property **SHOULD** be populated. |
| **start\_time\_fidelity** (optional) | integer | The level of fidelity that the start\_time is recorded in. This value **MUST** come from timestamp-fidelity-enum.  If no value is provided the timestamp should be considered to be accurate up to the number of decimals it includes. |
| **end\_time** (optional) | timestamp | The date and time the activity was last recorded. If this is not present it is assumed to be unknown. |
| **end\_time\_fidelity** (optional) | integer | The level of fidelity that the end\_time is recorded in. This value **MUST** come from timestamp-fidelity-enum.  If no value is provided the timestamp should be considered to be accurate up to the number of decimals it includes. |
| **impacted\_refs** (optional) | list of type identifier | A list of all impacted entities or infrastructure. This can relate directly to Infrastructure, SCOs, and other SDOs. |
| **observed\_refs** (optional) | list of type identifier | A list of all Indicators, Observed Data, Sightings, SCOs and other data that was part of this activity. This can relate directly to SDOs, SCOs, and Sightings. |
| **sequence\_start** (optional) | integer | An optional sequence number starting at 0 that shows the earliest point in an attack that this activity is believed to have occurred relative to other attacker activities.  This cannot exceed the sequence\_end value, but the two can be equal. |
| **sequence\_end** (optional) | integer | An optional sequence number starting at 0 that shows the last point in an attack that this activity is believed to have occurred relative to other attacker activities.  This cannot be less than the sequence\_start value, but the two can be equal. |

## 

## 2.2 Confidentiality Impact Object Type

**Type Name:** confidentiality-impact

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **description** (optional) | string | Additional details about this impact |
| **information\_type** (optional) | open-vocab | The type of information that had its confidentiality compromised. This can include control systems and other processes that can result in virtual or physical impacts.  This **SHOULD** be drawn from information-type-ov.  This value **MUST** be included if the loss\_type is not none. Including an entry with loss\_type of none and no information\_type indicates that no information had its confidentiality impacted by this incident. |
| **impacted\_refs** (optional) | list of type identifier | A list of all impacted entities or infrastructure. This can relate directly to Infrastructure, SCOs, and other SDOs. |
| **loss\_type** (required) | enum | The type of loss that occurred to the relevant information  The values of this property **MUST** come from the incident-confidentiality-loss-enum enumeration. |
| **record\_count** (optional) | integer | The number of records of this type that were compromised. The value of this property **MUST** not be negative. |
| **record\_size** (optional) | integer | The amount of data that was compromised in bytes. The value of this property **MUST** not be negative. |

## 

## 2.3 Defender Activity Object Type

**Type Name:** defender-activity

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **timestamp** (required) | timestamp | When this activity occurred. |
| **timestamp\_fidelity** (optional) | enum | The level of fidelity that the timestamp is recorded in. This value **MUST** come from timestamp-fidelity-enum.  If no value is provided the timestamp should be considered to be accurate up to the number of decimals it includes. |
| **activity\_type** (required) | open-vocab | A high level type for the defender activity in order to enable rollups and summaries. This should be drawn from defender-activity-ov.  Timestamp types that mark the start or completion of an activity type should end with:  -started and -completed respectively. |
| **description** (optional) | string | A description of the defender activity that occurred. |
| **identity\_refs** (optional) | list of identifier | A list of identities that were involved with this activity. For example a report was provided to specific identities at a given time. |
| **impacted\_refs** (optional) | list of type identifier | A list of all impacted entities or infrastructure. This can relate directly to Infrastructure, SCOs, and other SDOs. |
| **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. |
| **object\_ref** (optional) | identifier | A reference that **SHOULD** relate to a course of action, playbook or other object type that provides a structured description of specific actions that were performed. |

## 

## 2.4 Entity Count Type

**Type Name:** entity-count

The Entity Count type represents the count of one or more entity types. The name of each entity type **MUST** be specified as a key in the dictionary and **MUST** identify the count of the entity that corresponds to the value. Each key **SHOULD** come from identity-class-ov. This value **MUST** be an integer that is equal to or greater than zero.

**Examples:**

*100 individuals*

{

“individual”: 100

}

*1000 systems, 10 organizations, 1 sector*

{

“organization”: 10,

“sector”: 1

“system”: 1000

}

*0 individuals*

{

“individual”: 0

}

## 

## 2.5 Incident Score Object Type

**Type Name:** incident-score

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **name** (required) | string | The name of the score. This is normally a system or process name or some combination of these such as [Tool Name] Automated Exposure Score. |
| **value** (required) | number | The numeric score. |
| **description** (optional) | string | An optional description about how this score was calculated at for systems that provide these. |

## 

## 2.6 Integrity Impact Object Type

**Type Name:** integrity-impact

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **alteration** (required) | enum | The type of alteration performed against the information\_type.  The values of this property **MUST** come from the integrity-alteration-enum enumeration. |
| **description** (optional) | string | Additional details about this impact |
| **impacted\_refs** (optional) | list of type identifier | A list of all impacted entities or infrastructure. This can relate directly to Infrastructure, SCOs, and other SDOs. |
| **information\_type** (optional) | open-vocab | The type of information that had its integrity compromised. This can include control systems and other processes that can result in virtual or physical impacts.  This **SHOULD** be drawn from information-type-ov.  This value **MUST** be included if the alternation is not none. Including an entry that with an alteration of none and no information\_type indicates that no information had its integrity impacted by this incident. |
| **record\_count** (optional) | integer | The number of records of this type that were compromised. The value of this property **MUST** not be negative. |
| **record\_size** (optional) | integer | The amount of data that was compromised in bytes. The value of this property **MUST** not be negative. |
| **recoverability** (optional) | enum | The recoverability of this particular integrity impact with respect to feasibility and required time and resources.  The values of this property **MUST** come from the recoverability-enum enumeration |

## 2.7 Monetary Impact Object Type

**Type Name:** monetary-impact

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **variety** (required) | open-vocab | The variety of this monetary impact.  The values of this property **SHOULD** come from the monetary-impact-type-ov. |
| **criticality** (optional) | integer | The criticality of this impact. This value **MUST** bebetween 0 to 100. This can be translated into qualitative values as described in Appendix A. |
| **currency** (optional) | string | The currency that the max\_amount and min\_amount fields use. This **MUST** be an ISO 4217 alpha currency code.  This value **MUST** be included if the min\_amount is included. |
| **description** (optional) | string | Additional details about this impact |
| **max\_amount** (optional) | number | The maximum damage estimate of this type in the provided currency. This value **MUST** be greater than zero.  This value **MUST** be included if the min\_amount is included. |
| **min\_amount** (optional) | number | The minimum damage estimate of this type in the provided currency. This value **MUST** be greater than zero.  This value **MUST** be included if the max\_amount is included. |

# 

## 2.8 Physical Impact Object Type

**Type Name:** physical-impact

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **impact\_type** (required) | enum | The type of physical impact that has occurred.  The values of this property **MUST** come from the physical-impact-enum enumeration. |
| **description** (optional) | string | Additional details about this impact |
| **asset\_type** (optional) | open-vocab | The type or property or system that was affected by this impact..  This **SHOULD** be drawn from asset-type-ov.  This value **MUST** be included if the impact\_type is not none. Including an entry with an impact\_type of none and no asset\_type indicates that no physical damage was caused by this incident. |
| **impacted\_refs** (optional) | list of type identifier | A list of locations or assets that this impact type applies to. |
| **recoverability** (optional) | enum | The recoverability of this particular integrity impact with respect to feasibility and required time and resources.  The values of this property **MUST** come from the recoverability-enum enumeration |

# 

# 3. Vocabularies

## 3.1 Asset Type Vocabulary

**Type Name**: asset-type-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| building-doors | Doors within buildings or structures. |
| building-windows | The exterior or interior windows of buildings or structures. |
| buildings | Entire buildings or structures. |
| computers-mobile | Mobile devices such as smartphones. |
| computers-personal | Workstations or laptops owned by an organization. |
| computers-server | Servers owned by an organization. |
| environment | Land, environment or the ability of either to support humans or wildlife. |
| ics-actuator | Actuator for industrial control systems. |
| ics-engineering-workstation | Engineering workstation for industrial control systems. |
| ics-historian | Historian for industrial control systems. |
| ics-hmi | Human machine interfaces for industrial control systems. |
| ics-other | Other Industrial control systems. |
| ics-plc | Programmable logic controller for industrial control systems. |
| ics-safety-system | Safety system for industrial control systems. |
| ics-sensor | Sensor for industrial control systems. |
| inventory | Stocks of goods to be sold or consumed. |
| network-device | Switches, routers, and wireless communication towers. |
| private-infrastructure | Privately owned infrastructure such as roads, plumbing, railways, pipelines and electrical infrastructure. |
| public-infrastructure | Publicly owned infrastructure such as roads, plumbing, railways, pipelines and electrical infrastructure. |
| security-containers | Safes or other security containers. |
| vehicles | Vehicles of various types including cars, trains, and planes. |

## 3.2 Defender Activity Vocabulary

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

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| administrative | Perform an administrative action such as the introduction or change of a policy. |
| 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. |
| external-outreach | Reaching out to an external organization to gain support or information. |
| external-support | Acquire support from an external organization. |
| recovery-completed | When recovery was completed. |
| recovery-started | When recovery was started. |
| reported | When the incident was reported externally. |

## 3.3 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. |

## 3.4 External Impact Vocabulary

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

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

## 3.5 Incident Investigation Open Vocabulary

**Type Name**: incident-investigation-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| closed | All defender work on this incident has been concluded. In some cases, blue teams may make child Incidents of a closed Incident. In these cases, it is appropriate to mark an initial Incident as closed if 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. |

## 3.6 Incident Type Vocabulary

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

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| compromised-system | Attackers obtained control of a compromised system. |
| denial-of-service | The incident resulted in a loss of availability for a service or system.  Incidents of this **SHOULD** have an availability impact, but organizations may choose to not share the details of these impacts. |
| destruction | The incident destroyed data or systems.  Incidents of this **SHOULD** have an integrity impact, but organizations may choose to not share the details of these impacts. |
| equipment-loss | A loss of control of physical equipment that is not known to be theft. |
| equipment-theft | Theft of equipment. In general this should be paired with equipment-loss. |
| 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.  Incidents of this **SHOULD** have a confidentiality impact, but organizations may choose to not share the details of these impacts. |
| unauthorized-equipment | Usage of unauthorized devices as part of the incident |
| unauthorized-release | The unauthorized release of information.  Incidents of this **SHOULD** have a confidentiality impact, but organizations may choose to not share the details of these impacts. |
| unauthorized-use | The usage of information that falls outside of official purposes |

## 

## 3.7 Information Type Vocabulary

**Type Name**: information-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 e.g., intellectual property. |

# 

## 3.8 Monetary Impact Type Vocabulary

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

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| asset-and-fraud | Losses incurred due to loss of assets or fraud. |
| brand-damage | Losses incurred due to reputational or brand damage. |
| business-disruption | Losses incurred due to business disruptions. |
| competitive-advantage | Losses incurred due to theft of intellectual property, techniques or other capabilities that grant an advantage in the field. |
| legal-and-regulatory | Losses incurred due to legal or regulatory actions in response to the incident. |
| operating-costs | Losses incurred due to additional operating costs that have been incurred due to the incident. |
| response-and-recovery | Losses incurred due to response and recovery efforts for the incident. |
| uncategorized | Losses incurred that have not been categorized yet. |

# 

# 4. Enumerations

## 4.1 Activity Outcome Enumeration

**Type Name**: activity-outcome-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| blocked | The activity was blocked by pre-emptive measures including rate limiting or spam filters. |
| failed | The activity failed but not due to any affirmative defense.  For example: running a VisualBasic script failed because it was on a Linux machine. |
| ongoing | The activity is still occurring. |
| successful | The activity appears to have been successful. |
| unknown | The outcome of the activity is not yet known. |

## 4.2 Incident Confidentiality Loss Enumeration

**Type Name**: incident-confidentiality-loss-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| confirmed-loss | Information has been exfiltrated and is now available to the attacker, but it is unknown if it has been misused. |
| contained | Information’s confidentiality was compromised, but the spill was within an environment that allowed it to be effectively contained.  For example: a sensitive data spill occurred within a controlled network allowing it to be resolved before information exited the organization. |
| exploited-loss | Information has been exfiltrated and has been actively misused by the attacker. |
| none | This information type was not compromised based on the investigation that was performed. This option should be used to affirmatively supply this information when necessary. |
| suspected-loss | It is suspected but not confirmed that the attacker may have gained access to this information. |

## 4.3 Incident Determination Enumeration

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

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| blocked | The incident was blocked by pre-emptive measures including rate limiting or spam filters. |
| successful-attempt | An incident has been determined to have caused at least some harm. |
| 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. |
| false-positive | An incident was determined to have been triggered by a false alert and no action including automatically performed automated actions were needed to remediate the issue.  This should not be used when an incident was flagged correctly, but is of no importance. For findings of that nature low-value should be used. |
| low-value | An incident that has been deemed to be sufficiently unimportant for human intervention or may otherwise be considered noise. |
| suspected | An incident is suspected, but not yet confirmed. |

## 4.4 Integrity Alteration Enumeration

**Type Name**: integrity-alteration-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| potential-destruction | Information may have been destroyed within the system. |
| potential-modification | Information may have been modified within the system. |
| partial-destruction | Some data of this type has been destroyed, but sufficient data remains to allow partial functionality. |
| partial-modification | Some data in the system has been modified, but the remaining data is of an acceptable level of integrity for operations to continue. |
| full-destruction | Sufficient data of this type was destroyed to render the system inoperable until recovery can be completed. |
| full-modification | Sufficient data of this type was modified to render the system inoperable until recovery can be completed. |
| none | There is no evidence of destruction or modification of this data type in the system. |

## 4.5 Physical Impact Enumeration

**Type Name**: physical-impact-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| damaged-functional | The property, asset or system was damaged but still remains functional and repair may be possible. |
| damaged-nonfunctional | The property, asset or system was damaged and does not remain functional, but repair may be possible. |
| destruction | The property, asset or system was destroyed, cannot be repaired and no longer functions.  In some cases destroyed assets can be rebuilt, but doing so involves a similar amount of effort as the original construction. |
| none | No damage or destruction has occurred. |
| unknown | The degree of damage has not been determined yet. |

## 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. |

## 4.7 Timestamp Fidelity Enumeration

**Type Name**: timestamp-fidelity-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| day | The associated timestamp should be considered to represent a time within the one day period starting with the provided timestamp.  Hours and minutes should be understood to establish the timezone for this activity. |
| hour | The associated timestamp should be considered to represent a time within the one hour period starting with the provided timestamp. |
| minute | The associated timestamp should be considered to represent a time within the one minute period starting with the provided timestamp. |
| month | The associated timestamp should be considered to represent a time within the one month period starting with the provided timestamp.  Hours and minutes should be understood to establish the timezone for the activity. The day should always be listed as the first or the last day of the previous month if in a timezone that is offset before UTC. |
| second | The associated timestamp should be considered to represent a time within the one second period starting with the provided timestamp. |
| year | The associated timestamp should be considered to represent a time within the one year period starting with the provided timestamp.  Hours and minutes should be understood to establish the timezone for the activity. |

## 4.8 Traceability Enumeration

**Type Name**: traceability-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| accountability-lost | Traces used to retrieve accountability are lost or do not exist. |
| partial-accountability | Traces are present, but insufficient to have provable accountability. |
| provable-accountability | Accountability can be ensured from the traces that are present. |

# 

# 5.0 Relationships

|  |  |  |  |
| --- | --- | --- | --- |
| **Common Relationships** | | | |
| derived-from, duplicate-of, related-to | | | |
| **Source** | **Type** | **Target** | **Description** |
| incident | led-to | incident | One incident led to another. |
| incident | impacts | identity, infrastructure | An incident has an impact on the victim or specific infrastructure. |
| incident | attributed-to | intrusion-set, threat-actor | The incident has been attributed to the intrusion set or threat actor. |
| incident | targets | identity, infrastructure | An incident was targeted at the victim or specific infrastructure. |
| incident | located-at | location | The incident occurred at a specific location or locations. |
| **Reverse Relationships** | | | |
| campaign | associated-with | incident | The incident in question is part of the campaign that is associated with. |
| course-of-action | for-analysis-of | incident | A course of action can be used to help analyze an incident.\* |
| course-of-action | for-containment-of | incident | A course of action can be used to contain an incident.\* |
| course-of-action | for-detection-of | incident | A course of action can be used to detect an incident.\* |
| course-of-action | for-eradication-of | incident | A course of action can be used to eradicate an incident.  Course of action tag relationship tag information can be used to convey additional information on this action. |
| course-of-action | for-mitigation-of | incident | A course of action can be used to mitigate an incident.\* |
| course-of-action | for-prevention-of | incident | A course of action can be used to prevent this incident.\* |
| course-of-action | for-recovery-from | incident | A course of action can be used to recover from this incident.\* |
| identity | contact-for | incident | An identity should be considered a point of contact for an incident.  This can be used to supplement the created\_by\_ref in cases where external authorship would prevent using it for this purpose. |
| indicator | detected | incident | An indicator was responsible for detecting the incident. |
| \* Section 5.1 contains a list of labels that can be applied to relationships between courses of action and incidents to provide additional context for the status of these implementations. This is a temporary mechanism until a more formal extension can be created to better capture this information. | | | |

## 5.1 Relationship Labels

The following is a list of tags that can be applied to relationships in order to better capture the status of that relationship to an Incident. This provides a mechanism to indicate that a preventative measure that is being implemented is believed to be something that would have helped against an incident. It can also capture that a course of action failed to work, is planned to be implemented in the future along with several other possibilities.

If a defender is actively using a course of action as part of their response plan then it can be recorded directly into defender\_activities along with the time associated with starting this course of action. As such a separate relationship is not necessary in these scenarios.

Separate relationships and these labels should only be used to capture planned actions or controls, and ones that have been implemented in response to the incident.

This labeling mechanism should be considered temporary until a more formal extension can be provided that delivers this information in a focused manner.

|  |  |
| --- | --- |
| **Label** | **Description** |
| failed | The course of action did not achieve its desired effect.  This can be used to both say that a course of action taken as part of incident response failed, and that one intended to prevent an incident failed. |
| new-control | The course of action will be applying a new control in response to the incident, but was not applied against the incident directly. |
| not-attempted | The course of action was planned, but then not used. |
| planned | The course of action is planned for future use, but has not been used. The relationship start\_time and end\_time should be considered projections or goals in this case not statements of fact. |
| revised | If the course of action was changed from what was originally planned. |
| successful | The course of action achieved its desired effect.  This can be used to both say that a course of action taken as part of incident response succeeded, and that one intended to prevent an incident succeeded. |

# 

# ​Appendix A. Incident Criticality Mapping

This appendix defines mappings for criticality scales to be used by the criticality property. A value of "Not Specified" in the table below means that the criticality property is not present.

|  |  |  |
| --- | --- | --- |
| **5 Qualitative** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| False Positive | 0 | 0 |
| Low | 15 | 1-29 |
| Moderate | 40 | 30-49 |
| High | 70 | 50-89 |
| Extreme | 95 | 90-100 |

|  |  |  |
| --- | --- | --- |
| **Major / Minor** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| None | 0 | 0 |
| Minor | 25 | 1-49 |
| Major | 75 | 50-100 |

|  |  |  |
| --- | --- | --- |
| **Major / Minor / Critical** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| None | 0 | 0 |
| Minor | 25 | 1-49 |
| Major | 70 | 50-89 |
| Critical | 95 | 90-100 |

|  |  |  |
| --- | --- | --- |
| **None, Low, High, Extreme** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| None | 0 | 0 |
| Low | 20 | 1-39 |
| High | 65 | 40-89 |
| Extreme | 95 | 90-100 |

|  |  |  |
| --- | --- | --- |
| **VERIS** | **STIX Criticality Value** | **Range of Values** |
| Unknown | Not Specified | N/A |
| Insignificant | 10 | 0-19 |
| Distracting | 35 | 20-49 |
| Painful | 60 | 50-69 |
| Damaging | 80 | 70-90 |
| Catastrophic | 95 | 90-100 |

|  |  |  |
| --- | --- | --- |
| **0 to 10** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| 0 | 0 | 0-4 |
| 1 | 10 | 5-14 |
| 2 | 20 | 15-24 |
| 3 | 30 | 25-34 |
| 4 | 40 | 35-44 |
| 5 | 50 | 45-54 |
| 6 | 60 | 55-64 |
| 7 | 70 | 65-74 |
| 8 | 80 | 75-84 |
| 9 | 90 | 85-94 |
| 10 | 100 | 95-100 |

# 

# Appendix B. Incident Availability Impact Mapping

This appendix defines mappings for availability and functional scales to be used by the availability impact property. A value of "Not Specified" in the table below means that the criticality property is not present.

|  |  |  |
| --- | --- | --- |
| **US-CERT** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| No Impact | 0 | 0 |
| No Impact to Services | 5 | 1-9 |
| Minimal Impact to Non-Critical Services | 15 | 10-19 |
| Minimal Impact to Critical Services | 30 | 20-39 |
| Significant Impact to Non-Critical Services | 50 | 40-59 |
| Denial of Non-Critical Services | 65 | 60-69 |
| Significant Impact to Critical Services | 75 | 70-79 |
| Denial of Critical Services / Loss of Control | 90 | 80-100 |

|  |  |  |
| --- | --- | --- |
| **Simple Qualitative** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| None | 0 | 0 |
| Minimal | 20 | 1-39 |
| Significant | 50 | 40-59 |
| Denial | 75 | 60-89 |
| Loss of Control | 95 | 90-100 |

|  |  |  |
| --- | --- | --- |
| **0 to 10** | **STIX Criticality Value** | **Range of Values** |
| Not Specified | Not Specified | N/A |
| 0 | 0 | 0-4 |
| 1 | 10 | 5-14 |
| 2 | 20 | 15-24 |
| 3 | 30 | 25-34 |
| 4 | 40 | 35-44 |
| 5 | 50 | 45-54 |
| 6 | 60 | 55-64 |
| 7 | 70 | 65-74 |
| 8 | 80 | 75-84 |
| 9 | 90 | 85-94 |
| 10 | 100 | 95-100 |

# 

# Appendix C. Acknowledgements

**Primary Editor**

Jeffrey Mates, US Department of Defense (DoD)

**Contributors**

The following individuals were members of the OASIS CTI Technical Committee and contributed time and effort to ensure that this extension would be possible. Their contributions are gratefully acknowledged:

Alexandre Cabrol Perales, Sopra Steria Group

Ben Ottoman, Cyber Threat Intelligence Network, Inc. (CTIN)

Christian Hunt, Copado

Christopher Robinson, Cyber Threat Intelligence Network, Inc. (CTIN)

David Kemp, National Security Agency (NSA)

Duncan Sparrell, sFractal Consulting LLC

Emily Ratliff, IBM

Jane Ginn, Cyber Threat Intelligence Network, Inc. (CTIN)

Jason Keirstead, IBM

Jeremy Berthelet, Sopra Steria Group

Keven Ates, US Federal Bureau of Investigation

Margaux Quittelier, Sopra Steria Group

Michael Rosa, National Security Agency (NSA)

Richard Piazza, MITRE Corporation

Rob Coderre, Accenture

Robert Keith, Accenture

Ryan Hohimer, DarkLight, Inc.

Scott Robertson, Kaiser Permanente

Trey Darley, CCB/CERT.be

Vasileios Mavroeidis, University of Oslo

# 

# Appendix D. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| 01 | 2022-05-23 | Incident Mini Group | Initial Version |
| 02 | 2022-10-27 | Jeffrey Mates | Added “ongoing” to activity-outcome-enum. Removed normative text for attacker\_activity.pattern\_ref that indicated a field that does not exist can be excluded if it is present. |