**​2.1.​ Event**

**Type Name:** event

An event provides a SDO that represents a set of threat intelligence information captured that is used as input to further processing by systems and/or analysts.

An event may characterize a set of information to support the following use cases:

1. a set of observed data objects such as IP, Domains….etc that are transmitted by a system that has determined those network devices should be mitigated
2. a declaration that certain description or mitigation actions should be taken in response to particular scenario such as a malware outbreak where the scenario is described in textual form with potentially associated observed network/endpoint data

Events may or may not result in further analysis by machine or humans to determine if the data contained in the event represents an specific incident or contributes further context to other SDO such as a campaign, intrusion set, threat actor…..etc.

Events have lifecycles where those events are created, updated and transitioned through a variety of steps typical for handling threat intelligence ingest, correlation, analysis and response. Each stage of the lifecycle the event may be updated with additional context and the outcome of each stage may cause the event to be closed with a result or determination that the event does not require further processing in the workflow.

If further processing takes place, the disposition may be that an incident has occurred and the event object may be associated with other events and/or may be labelled as an Incident with appropriate status.. The term “Incident” is a frequently used term with a variety of definitions, some of them having a basis in law and requiring specific reporting; STIX does not require that any given definition be used. In STIX, an Event may result in being labelled an Incident when the producer of that Event says that it is.

The Event SDO is intended to capture information that is exchanged between tools wishing to distribute and exchange event information that helps support their threat intelligence workflows, such as incident response systems and threat intelligence platforms, or providers of threat intelligence to consumers of threat intelligence. It contains properties to capture information such as the name and description, contacts, important timestamps, activity that had been taken, and some categorizations. It has relationships to other SDOs that can be used to relate it to the attackers that might be responsible, what TTPs were leveraged to carry out the attack, who was impacted, what courses of action could or were taken, and related observable data (in activity).

**​2.1.1.​ Properties**

|  |  |  |
| --- | --- | --- |
| **Common Properties** | | |
| **type**, **id**, **created\_by\_ref**, **created**, **modified**, **revoked**, **labels**, **confidence**, **lang**, **external\_references**, **object\_marking\_refs**, **granular\_markings** | | |
| **Event Specific Properties** | | |
| **name**, **description**, **aliases**, **status**, **timestamps**, **contacts**, **objective**, **detection\_mechanism**, **counts**, **financial\_impact**, **financial\_impact\_currency**, **activity** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this property **MUST** be event |
| **labels** (required) | list of type string | This property is a list of classifications for the Event.  While no vocabulary has been defined, the value incident can be used to indicate that the producer considers this Event an incident. |
| **name** (required) | string | A name used to identify the Event. |
| **description** (optional) | string | A description that provides more details and context about the Event, potentially including a summary of what happened, what the results were, and other key characteristics.  For textual event information (such as CERT notifications) this property may be used to describe why the notification is being distributed |
| **~~aliases~~** ~~(optional)~~ | ~~list of type string~~ | ~~Additional names or titles for this event.~~ |
| **status** (required) | string | The current status of the event. The value of this property **MUST** be one of open, resolved, or rejected. Open indicates that the event is still being worked on, resolved that it was closed, and rejected that it was invalid (for example, was a false positive or incorrectly reported). More detailed status information can be captured in the timestamp (e.g., when the event was first detected). |
| **timestamps** (required) | dictionary | Points in time relevant to the lifecycle of this event, such as when it was first detected or when the activity first appeared. The keys of this dictionary **SHOULD** be values from the event-timestamp-ov open vocabulary. The values of this dictionary **MUST** be of type timestamp. |
| **contacts** (optional) | dictionary | Points of contact relevant to this event, such as who reported it and who is responding to it. The keys of this dictionary **SHOULD** be values from the event-contacts-ov open vocabulary. The values of this dictionary **MUST** eachbe a list of type string, where the values are the names of the contacts (either names of organizations or of people). |
| **objective** (optional) | string | If the event supports analysis that has determined the objective then this property may support what that objective was. For raw events where no objective is yet known or the event communicates basic network mitigation lists then this property may be left empty.  The primary goal, objective, desired outcome, or intended effect that the Threat Actor intended to accomplish. |
| **detection\_mechanism** (optional) | list of type open-vocab | Specifies how this event was detected.  This is an open vocabulary and values **SHOULD** come from the event-detection-mechanism-ov vocabulary.  As an example, an event detected by an external audit would have the values external, and audit. |
| **counts** (optional) | dictionary | If an event has been further analyzed and processed and the impact of that event has determined the overall coverage of users or systems impacted by the event.  A set of counts representing the number of users, systems, records, etc. that were impacted by this event. The keys of this dictionary **MAY** either be one of systems, users, or records or any other value to indicate counts of other things that were impacted. The values of these keys **MUST** be of type integer. |
| **~~activity~~** ~~(optional)~~ | ~~list of type event-activity~~ | ~~A journal of activity that has been taken during the lifetime of this event, in particular capturing when courses of action were taken or when data relevant to the event was collected.~~ |

**2.1.2. ~~Event Activity Type~~**

~~The Event Activity type captures specific steps taken during the lifecycle of the event.~~

|  |  |  |
| --- | --- | --- |
| **~~Property Name~~** | **~~Type~~** | **~~Description~~** |
| **~~activity\_date~~** ~~(required)~~ | ~~timestamp~~ | ~~The date and time the activity that is being described was recorded.~~ |
| **~~coa\_taken~~** ~~(optional)~~ | ~~identifier~~ | ~~The Course of Action that was taken during this activity.~~ |
| **~~Coa\_recommended (optional)~~** | ~~identifier~~ | ~~The Course of Action that is recommended by recipients of this event and if they have determined the event is related to their environment~~ |
| **~~collected\_data~~** ~~(optional)~~ | ~~identifier~~ | ~~The Observed Data that was collected or is being distributed related to this event or activity.~~ |
| **~~description~~** ~~(required)~~ | ~~string~~ | ~~A human-readable description of the activity that occurred or the outcome of the Course of Action that was taken or recommended~~ |

​​

**​2.1.3.​ Relationships**

These are the relationships explicitly defined between the Event object and other objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from the Event object by way of the Relationship object. The reverse relationships (relationships "to" the Event object) are included as a convenience. For their definitions, please see the objects for which they represent a "from" relationship.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship type or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | identifier (of type identity) | |
| **object\_marking\_refs** | | identifier (of type marking-definition) | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Relationship Type** | **Target** | **Description** |
| event | attributed-to | campaign, intrusion-set, threat-actor | This Relationship describes that the the related Campaign, Intrusion Set, or Threat Actor is responsible for the Event.  For example, an attributed-to Relationship from an Event at ACME Corporation to the Operation Aurora Campaign against technology companies in the United States means that the Event is a part of that Campaign. |
| event | targets | identity,  location | This Relationship describes that the related Location or Identity was targeted by the attacker as part of this Event.  For example, the targets relationship from an Event to an Identity representing ACME Corporation indicates that ACME corporation was targeted by the attacker. |
| event | part-of | event | This Relationship describes that this event is part of the related event.  For example, one broader case or investigation may be made up of several lower-level events. |
| event | recommends | course-of-action | This relationship describes the recommendations (if any) associated to responding to the event |
| event | reports-on | observed-data | This relationship describes the observed-data associated with this event that may represent related context to the event |
| event | Supported-by | Intel-note | This relationship describes any additional context that support the events |
| Event | Assessment-by | Opinion | This relationship describes any opinions from other systems on this particular event |
| **Reverse Relationships** | | | |
| course-of-action | mitigated | event | This relationship describes any course of action that occurred to respond to this event occurrence. |
| attack-pattern,  indicator,  infrastructure,  malware,  observed-data,  tool, vulnerability | triggered | event | See forward relationship for definition. |

**​2.2.​ 2.1 Event Timestamp Vocabulary**

**Type Name**: event-timestamp-ov

A non-exhaustive enumeration of possible event statuses.

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| contained | The event has been contained. |
| detected |  |
| opened | The event is currently in an open status. |
| mitigated | The event has been mitigated. |
| rejected | The event was closed and rejected, potentially as a false positive. |
| remediated | The event has been remediated. |
| reported |  |
| resolved | The event has been closed and resolved. |
| triaged | The event has been triaged. |
| started |  |

**​2.3.​ 2.1 Event Contacts Vocabulary**

**Type Name**: event-contacts-ov

A non-exhaustive list of contacts that are involved in the event.

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| reporter | The entities that reported the event to the organization. For example, an event might be reported by a law enforcement agency. |
| detector | The entities that first detected the event. For example, an event might be detected by a managed security services provider. |
| responder | The entities that is responding to the event. For example, an organization might hire an incident response company to respond. |
| coordinator | The entities that is coordinating the response to the event. For example, a national computer emergency response team might coordinate the response to an attack across the impacted organization, law enforcement, and the impacted users. |
| other | Other points of contact, such as related parties that are connected to the event but not filling one of the other roles. |
| reported\_to | The entities that the event was reported to, such as law enforcement or a national computer emergency response team. |

**​2.4.​ 2.1 Detection Mechanism Vocabulary**

**Type Name**: detection-mechanism-ov

A non-exhaustive enumeration of ways that organizations get alerted to events.

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| audit | The event was detected in the course of an audit. |
| external | The event was detected by an external organization or individual. |
| fraud-detection | The event was detected by fraud monitoring processes. |
| internal | The event was detected by the impacted organization itself. |
| law-enforcement | The event was detected by law enforcement. |
| service | The event was detected by a monitoring service, such as a managed security provider. |
| public-disclosure | The event was publicly disclosed. |
| tool | The event was detected by a network, endpoint, or other tool / sensor. |
| user | The event was reported by a user. |

**​2.4.1.​ Examples**

An event that represents an investigation

{

 "type": "event",

 "id": "event--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

 "created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

 "created": "2016-04-06T20:03:48.000Z",

 "modified": "2016-04-06T20:03:48.000Z",

 "labels": "investigation",

 "name": "Green Group Infiltration of Web Servers",

 "description": "Green group was able to infiltrate the web server infrastructure and caused sporadic and unpredictable content defacement issues."

 "timestamps": {

   "reported": "2016-04-06T20:03:48.000Z",

 },

 "status": "opened"

}

An event that represents a CERT notification

{

 "type": "event",

 "id": "event--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

 "created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

 "created": "2016-04-06T20:03:48.000Z",

 "modified": "2016-04-06T20:03:48.000Z",

 "labels": "CERT notification",

 "name": "FIRST Announcement: Malicious Chrome Extensions Stealing Roblox In-Game Currency, Sending Cookies via Discord",

“external-references”: [“<https://blog.malwarebytes.com/101/2017/08/4-steps-for-improving-employee-trust-securing/>”],

 "description": " Excerpt: With so many evolving threats from cybercriminals who employ a variety of tactics and techniques, there’s one element that many security pros consider to be the weak link in any security practice–humans. The challenge is to minimize the impact your users have on your well-laid plans to secure them. To help answer this question and inspire anyone else who is facing this same concern, I thought I’d share 4 key steps you can take within your business to help gain trust with your employees while accomplishing your mission."

 "timestamps": {

   "reported": "2016-04-06T20:03:48.000Z",

 },

 "status": "opened"

}

An event that represents a blacklist containing observed-data and recommended COA

{

 "type": "event",

 "id": "event--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

 "created\_by\_ref": "source--f431f809-377b-45e0-aa1c-6a4751cae5ff",

 "created": "2016-04-06T20:03:48.000Z",

 "modified": "2016-04-06T20:03:48.000Z",

 "labels": "Blacklist",

 "name": "Mitigation Blacklist 1010",

“external-references”: [“hxxps://blacklist.com/blacklist/1010 ”],

 "description": “Domain Blacklist to block on"

 "timestamps": {

   "reported": "2016-04-06T20:03:48.000Z",

 },

 "status": "opened"

}

  {

  "type": "relationship",

  "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",

  "created\_by\_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",

  "created": "2016-04-06T20:06:37.000Z",

  "modified": "2016-04-06T20:06:37.000Z",

  "source\_ref": "event--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

  "target\_ref": "observed-data--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

  "relationship\_type": "reports-on"

  },

{

“type” : “observed-data”

“id” : “observed-data-8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f”

…. Fields that identify a list of IPs or Domains

}

  {

  "type": "relationship",

  "id": "relationship--44298a74-ba52-4f0c-87a3-1824e67d7fad",

  "created\_by\_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",

  "created": "2016-04-06T20:06:37.000Z",

  "modified": "2016-04-06T20:06:37.000Z",

  "source\_ref": "event--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

  "target\_ref": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

  "relationship\_type": "recommends"

  },

{

“type” : “course-of-action”

“id” : “course-of-action-8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f”

…. Fields that describe ‘block and log’

}