EclecticIQ Platform user guide

Build threat models with entities and observables — 2/4

Last generated: January 12, 2018

Table of contents

User guide to EclecticIQ Platform

This user guide helps you configure the main options of the platform, as well as familiarize with EclecticIQ Platform, so that you can start collecting and analyzing potential threats efficiently.

Scope

The user guide to EclecticIQ Platform aims at providing clear and to-the-point help to get you acquainted with the threat intelligence platform, so that you can configure it as needed, and you can use it to collect and analyze intelligence on potential threats, as well as share it and collaborate with other analysts.

Although it is not a complete reference manual, this guide shows end-users how they can use the platform and its rich feature set to collect data, to analyze and investigate potential threats, and to collaborate and share intelligence with other analysts.

Goal

Learn how to incorporate the platform in your daily workflow as a poweful tool to:

- Automate data ingestion
- View, edit, create, and delete platform entities
- Enrich entities with additional contextual details
- Analyze entities on the graph to identify potential threats and their relationships
- Search, filter, and slice data using rules
- Share your findings and collaborate

Audience

This document targets the following audience:

- Cyber threat intelligence analysts
- Cyber threat intelligence specialists

Feedback

No one reads manuals, ever. We know.
Yet, we strive to give you clear, concise, and complete documentation that helps you get stuff done neatly.

We are committed to crafting good documentation, because life is too short for bad doc.
We appreciate your comments, and we'd love to hear from you: if you have questions or suggestions, drop us a line and share your thoughts with us!

The Product Team

About entities

In the platform entities represent the standard STIX objects defining different types of cyber threat information.

About entities

Entities are the reference unit of measurement and the main data model in the platform. The platform tranforms ingested data to entities. An entity is a distinct data unit that represents a specific concept.

For example, indicators of compromise, observables, sightings, and relationships all live inside the platform as entities. This approach allows you to handle and manipulate distinct data chunks like objects during an analysis or an investigation.

Platform entities are mapped to the corresponding standard **STIX types** (https://stixproject.github.io/data-model/1.2/), and they represent the same type of information.

Entity types

Entity type	Description
Campaign (https://stixproject.github.io/data-model/1.2/campaign/campaigntype/)	A campaign is a series of planned actions aiming at achieving a specific goal. It groups a set of related threat actors, TTPs, and incidents sharing a common intent or goal.
Course of action (https://stixproject.github.io/data-model/1.2/coa/courseofactiontype/)	A course of action details a set of clear, specific recommendations and measures to mitigate an incident, address affected exploit targets, and effectively respond to a cyber threat.
Exploit target (https://stixproject.github.io/data-model/1.2/et/exploittargettype/)	An exploit target is a vulnerability or a weakness in software, hardware, systems, or networks that a threat actor can leverage and take advantage of to intrude or carry out an attack.
Incident (https://stixproject.github.io/data-model/1.2/incident/incidenttype/)	An incident describes a specific occurrence of one or more indicators affecting an organization. It includes information on threat actors, tools or skills, timeframes, techniques, as well as impact assessment and the recommended response course of action.
Indicator (https://stixproject.github.io/data-model/1.2/indicator/indicatortype/)	An occurrence or a sign that an incident may have occurred or may be in progress. See also the definition provided in the **Cybersecurity Information Sharing Act of 2015 (CISA)** (https://www.congress.gov/bill/114th-congress/senate-bill/754/text).

Entity type	Description
Report (https://stixproject.github.io/data-model/1.2/report/reporttype/)	A detailed account of an indicator of compromise (IOC), a threat, a campaign or other threat activity as a result of an investigation or an analysis. A report tells a story about a piece of threat intelligence by providing background, context, and by pulling threads together to weave a clear and meaningful description of a security breach, a cyber attack, or a series of attacks.
Sighting ()	A sighting records a discrete instance of an observed indicator of compromise inside their own environment — for example, an entry in a log file — the malicious item is sighted, and the organization environment is compromised. For example, it can record the occurrence of a malicious IP address at a specific date and time.
Threat actor (https://stixproject.github.io/data-model/1.2/ta/threatactortype/)	An individual or a group carrying out or planning to execute malicious activities. Threat actors include information on their identity, suspected motivation, and suspected intended effect.
TTP (https://stixproject.github.io/data-model/1.2/ttp/ttptype/)	Tactics, Techniques and Procedures. Sometimes referred to also as Tools, Techniques, Procedures. TTPs describe the behavior of cyber adversaries. Tactics describe *"the employment and ordered arrangement of forces in relation to each other"*. Techniques are *"non-prescriptive ways or methods used to perform missions, functions, or tasks."* Procedures are *"standard, detailed steps that prescribe how to perform specific tasks."* (definitions from *"Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (as amended through 15 February 2016)"*)
Package (https://stixproject.github.io/data-model/1.2/stix/stixtype/)	A package is a wrapper containing one or more STIX objects such as indicators, threat actors, TTPs, and so on. When the platform ingests packages, it extracts the STIX objects and it converts them to its internal JSON data model.

In the platform you can create the following entity types:

- Create a campaign
- Create a course of action
- Create an exploit target
- Create an incident
- Create an indicator
- Create a report
- Create a sighting
- Create a threat actor
- Create a TTP

Create a campaign

A campaign details a threat actor pursuing a goal, as observed through incidents and sightings, as well as attack patterns and TTPs.

About campaigns

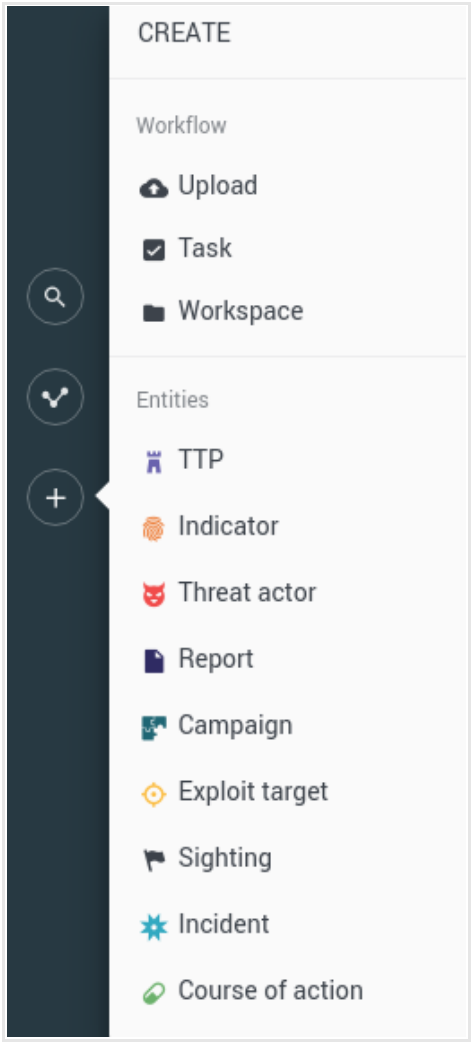
A campaign details instances of a threat actor aiming at reaching an intended effect on a targeted victim and/or an exploit target by applying a set of attack patterns and other (malicious) behaviors over time. The observation of indicators, observables, sightings, and incidents helps identify specific attack patterns and TTPs defining the threat actor's modus operandi.

Create a campaign

✔ Input fields marked with an asterisk are required.

To create a **campaign** (`https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part8-campaign/stix-v1.2.1-csprd01-part8-campaign.html`) in the platform to tie together a threat actor, their goals, their behavior, and their activities and effects on a targeted victim, do the following:

- On the left-hand navigation sidebar click **✚ > Campaign**.



The entity editor opens at **Create Campaign**, and you can start populating the input fields with content and details about the campaign you are creating.

Define the general options

- **Title**: assign the new campaign entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
- **Confidence**: it flags the **estimated level of confidence** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605) to assess the accuracy and trustworthiness of the entity information.
- **Intended effects**: from the drop-down menu select one or more options to define the **goals the threat actors aims at achieving** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440615).
- **Status**: from the drop-down menu select an option to indicate if the campaign is **currently active, if it supposed to occur sometime in the future, or if it happened in the past** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440600).

- **Name**: a campaign may be known under different names. Enter one alias for the campaign per input field.
  To confirm the current input and to display a new input field, press **ENTER**.

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > +**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click **+ (Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.

- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

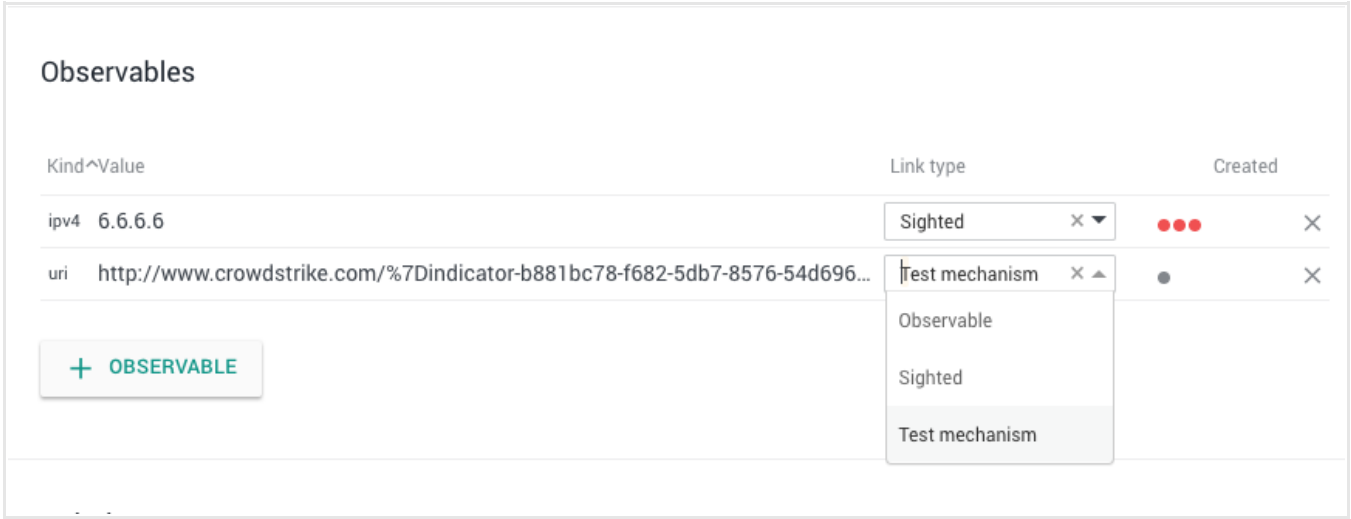
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the campaign entity:

- N/A. Campaign-related observables do not have link types.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.

For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the campaign.

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Activity**: select this option to add details about any actions the defender and/or targeted victim took, is taking, or is planning to take concerning the campaign.
  You can add as many activities as you need.
  - **Description**: describe the type of activity — for example, prevention, mitigation, deter, or defeat activities.
    Add a short description of the actions, the equipment, the tactics and techniques implemented and deployed in the activity.
  - **Date/Time**: click the icon to set a date and time for the activity.
  - **Date time precision**: from the drop-down menu select an option to provide an estimation of how accurate the activity date is: from **second** (dead-on accurate) to **year** (inaccurate).

Add relationships

You can add relationships to associate the campaign to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

You can refine the displayed results by specifying a search string in the filter input field.
Alternatively, click one of the available filter options to select and filter by specific:

- **Entity types**
- **Source**
- **Date**
- **Datasets**

- Click **Select**.

- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the campaign
Associated campaigns	Outgoing relationship — Relates the campaign to the selected campaign(s) on the **Search an entity** dialog.
Attributions	Outgoing relationship — Relates the campaign to the selected threat-actor(s) on the **Search an entity** dialog.
Related incidents	Outgoing relationship — Relates the campaign to the selected incident(s) on the **Search an entity** dialog.
Related TTPs	Outgoing relationship — Relates the campaign to the selected TTP(s) on the **Search an entity** dialog.
Indicator → Related campaigns	Incoming relationship — Relates the selected indicator(s) on the **Search an entity** dialog to the campaign.
Report → Campaigns	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the campaign.
Threat actor → Associated campaigns	Incoming relationship — Relates the selected threat-actor(s) on the **Search an entity** dialog to the campaign.
Sighting → Campaign	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the campaign.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field. When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/campaign — or outgoing — from the current origin campaign/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.

- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the campaign.
- **References**: enter a URL pointing to relevant reference information on the campaign, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the campaign to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create a course of action

A course of action describes specific measures and actions to address a cyber threat such as defeating or mitigating an incident, or correcting or preventing an exploit.

About courses of action

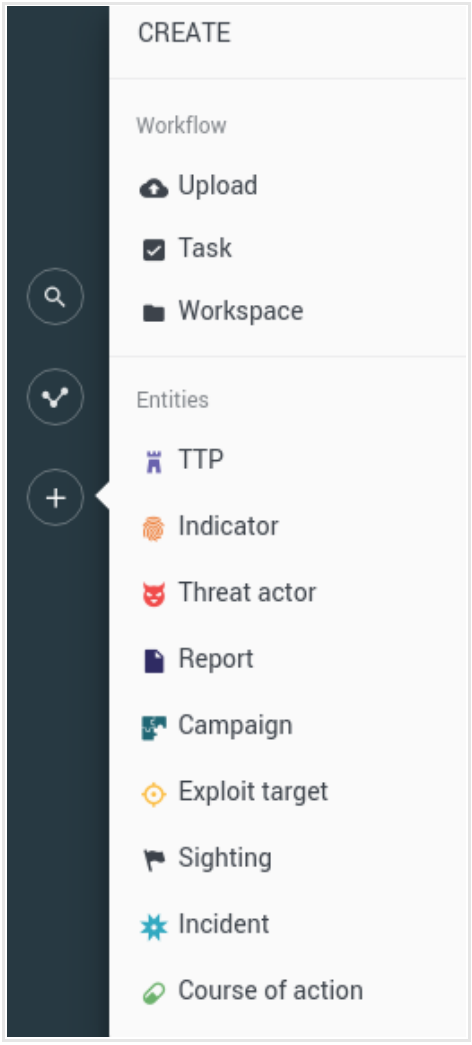
A course of action describes a specific set of actions, procedures and processes to efficiently address a threat.
The goal of a course of action can be preventing the potential occurrence of an incident, correcting a vulnerability so that it cannot be exploited, mitigating the consequences of an attack, or defeating an adversary.
Regardless the goal, a course of action suggests the recommended actions to take in order to achieve the intended effect.

Create a course of action

✔ Input fields marked with an asterisk are required.

To create a **course of action** (`https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html`) in the platform to outline a set of recommended tasks, processes and procedures to prevent a potential incident or to counter an adversary, do the following:

- On the left-hand navigation sidebar click **✚ > Course of action**.



The entity editor opens at **Create Course of action**, and you can start populating the input fields with content and details about the course of action you are creating.

Define the general options

- **Title**: assign the new course of action entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the course of action.

Under **Characteristics** click **+ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- ✚ **Characteristic > Type**: from the drop-down menu select an option to describe the **type of course of action** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440602), that is, the main line of action characterizing the course of action.
- ✚ **Characteristic > Stage**: from the drop-down menu select an option to indicate if the course of action is **proactive or reactive** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440601), that is, if it takes steps to *prevent* a potential incident or attack to occur in the future (**Remedy**), or if it is a *response* to an attack by an adversary (**Response**).
- ✚ **Characteristic > Objective**: select this option to describe the goal, the purpose, or the intended effect the course of action should achieve. ()
  - **Description**: provide a short free-text **description** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part9-coa/stix-v1.2.1-csprd01-part9-coa.html#_toc440440097) of the intended end result you want to achieve by implementing the course of action.
    Example: *Restore full availability of the affected data and services.*
  - **Applicability confidence**: from the drop-down menu select an option to assess the **level of confidence** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part9-coa/stix-v1.2.1-csprd01-part9-coa.html#_toc440440097) in the course of action being a realistic, feasible, and pragmatic approach to produce the desired results.
- ✚ **Characteristic > Impact**: select this option to describe the **consequences** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part9-coa/stix-v1.2.1-csprd01-part9-coa.html#_toc440440094) that can derive from implementing the course of action.
  - **Impact value**: from the drop-down menu select an option assess the **level of the impact** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605).
    It answers the question: “How much is the suggested course of action going to affect the organization in terms of consequences, side effects, and repercussions?”
  - **Confidence**: from the drop-down menu select an option to estimate the **level of confidence** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605) in the impact value assessment.
    It answers the question: “How reasonably reliable is the impact assessment?”
  - **Description**: enter a short description to provide additional context or extra details.
- ✚ **Characteristic > Cost**: select this option to appraise the **estimated cost** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part9-coa/stix-v1.2.1-csprd01-part9-coa.html#_toc440440094) of the course of action implementation.
  - **Cost value**: from the drop-down menu select an option to assess the **expected cost** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605) of the course of action.
    It answers the question: “How much is the suggested course of action going to cost if we implement it?”
  - **Confidence**: from the drop-down menu select an option to estimate the **level of confidence** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605) in the cost assessment.
    It answers the question: “How reasonably accurate is the cost assessment for the course of action?”
  - **Description**: enter a short description to provide additional context or extra details.

- ✚ **Characteristic > Efficacy**: select this option assess the **likeliness of a "happy scenario", that is, a positive outcome** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part9-coa/stix-v1.2.1-csprd01-part9-coa.html#_toc440440094) of the course of action and the achievement of the intended results.
  - **Efficacy value**: from the drop-down menu select an option to estimate the **effectiveness** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605) of the course of action.
    It answers the question: "How suitable or adequate is the course of action to achieve the intended results?"
  - **Confidence**: from the drop-down menu select an option to estimate the **level of confidence** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605) in the effectiveness assessment.
    It answers the question: "How likely is it that the suggested course of action is the most effective approach to achieve the intended results?"
  - **Description**: enter a short description to provide additional context or extra details.

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ✪ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click ✚ **(Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.

- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

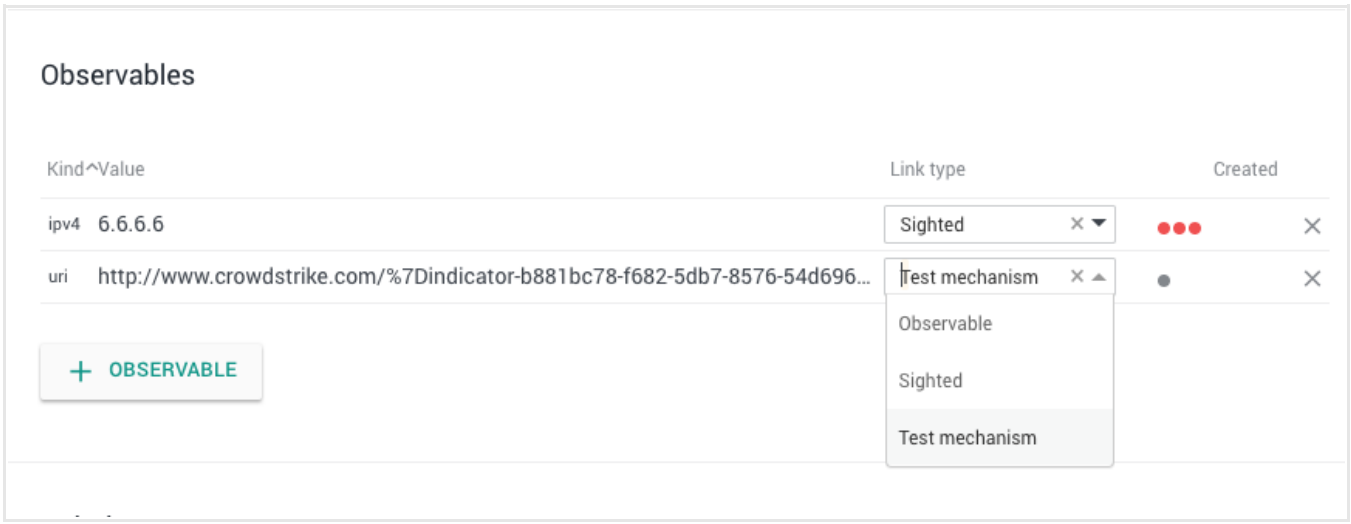
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the course of action entity:

- **Parameter**: it is the only link name option available for course of action entities.
  It enables defining specific technical parameters, settings, and configurations related to the course of action using the CybOX Language.

  You can set parameters for a course of action to define automated courses of action designed to to carry out follow-up actions. It can be a detection follow-up; for example, it can trigger adjusting the settings of a malware detection application accordingly. It can be a prevention follow-up; for example, it can instrument a third-party system to block a range of malicious IP addresses or domain names. Or it can produce a community follow-up; for example, creating and publishing a report to notify other parties about the possible threat the entity represents.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*

- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the course of action to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the course of action
Related exploit targets	Outgoing relationship — Relates the course of action to the selected exploit target(s) on the **Search an entity** dialog.
Related incidents	Outgoing relationship — Relates the course of action to the selected incident(s) on the **Search an entity** dialog.

Select this option…	… to create this relationship for the course of action
Related courses of action	Outgoing relationship — Relates the course of action to the selected course(s) of action on the **Search an entity** dialog.
Exploit target → Potential courses of action	Incoming relationship — Relates the selected exploit target(s) on the **Search an entity** dialog to the course of action.
Indicator → Suggested courses of action	Incoming relationship — Relates the selected indicator(s) on the **Search an entity** dialog to the course of action. Recommends carrying out a course of action to respond to an indicator.
Incident → Courses of action requested	Incoming relationship — Relates the selected indicator(s) on the **Search an entity** dialog to the course of action. Requests to carry out a course of action to respond to an incident.
Incident → Courses of action taken	Incoming relationship — Relates the selected indicator(s) on the **Search an entity** dialog to the course of action. Reports the course of action carried out as a response to an incident.
Report → Courses of action	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the course of action.
Sighting → Course of action	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the course of action.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field.
When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either ➔ or ➔, indicates that the relationship is either incoming — from the related entity to the current one/course of action — or outgoing — from the current origin course of action/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.

- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the course of action.
- **References**: enter a URL pointing to relevant reference information on the course of action, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the course of action to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create an exploit target

An exploit target details a vulnerability in software, systems, networks or configurations a threat actor leverages to gain access and/or control through a set of TTPs.

About exploit targets

An exploit target represents a vulnerability or a weakness in a software or hardware product or system, in a network, or in a configuration that allows a threat actor to use it as an entry point to access your assets and resources, and eventually to take control over them. Like a window that is left open upon leaving the house, it is a security hole in your ecosystem or infrastructure that malicious actors can leverage to get in and pursue their objectives.

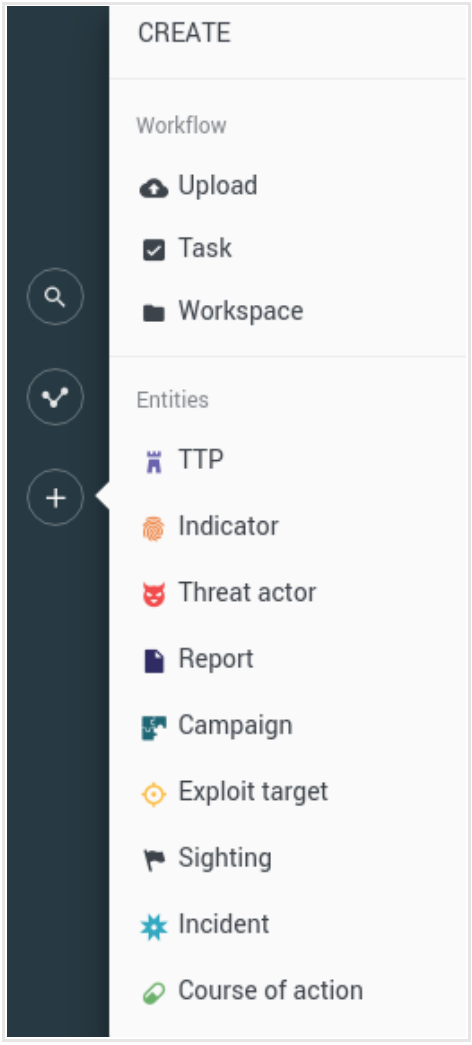
In the context of a broader cyber threat scenario, a threat actor implements TTP to hit an exploit target, and to attack a targeted victim.
A distinct occurrence is an incident. A series of structured attacks sharing similar characteristics — for example, they are carried out by the same threat actor and they hit the same exploit target — over a period of time is a campaign.
Any footprints or signatures the intruder leaves behind are indicators.

Create an exploit target

✔ Input fields marked with an asterisk are required.

To create an **exploit target** (`https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part10-exploit-target/stix-v1.2.1-csprd01-part10-exploit-target.html`) in the platform to describe a security hole, a vulnerability, or a weakness in your organization or environment, do the following:

- On the left-hand navigation sidebar click **✚ > Exploit target**.



The entity editor opens at **Create Exploit target**, and you can start populating the input fields with content and details about the exploit target you are creating.

Define the general options

- **Title**: assign the new exploit target entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the exploit target.

- **Vulnerability**: describes the **vulnerability type** (https://stixproject.github.io/data-model/1.2/et/vulnerabilitytype/) being exploited.
  The vulnerability editor is based on the **STIX CVRF InstanceType** (https://stixproject.github.io/data-model/1.2/stix-cvrf/cvrf1.1instancetype/) and the **Common Vulnerability Reporting Framework (CVRF)** (http://www.icasi.org/cvrf/).
- **Weakness**: describes the **type of weakness** (https://stixproject.github.io/data-model/1.2/et/weaknesstype/), flaw, imperfection, or defect causing th vulnerability that the threat actor is exploiting.
- **Configuration**: provides information on the exploited configuration, and on the security issues that allow it to be used as an exploit target.

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Vulnerability**: select this option to add details about the vulnerability the threat actor exploits to attack the exploit target.
  - **Title**: enter a name to define the vulnerability.
  - **Is known**: select this checkbox to indicate that the vulnerability is already known to exist.
    If you leave the checkbox deselected, it means that you are describing a *zero-day* vulnerability.
  - **Is publicly acknowledged**: select this checkbox to indicate whether the affected product vendor officially acknowledged the vulnerability.
  - **Description**: describe the vulnerability and its effects — for example, if it causes a denial of service, if it can arbitrarily run code, if it a flavor of XSS, and so on.
  - **Source**: enter the origin of the acquired information about the vulnerability — for example:
    - **Common Vulnerabilities and Exposures** (https://cve.mitre.org/)
    - **National Vulnerability Database** (https://nvd.nist.gov/)
    - **CVE Details** (https://www.cvedetails.com/)
  - **Discovered date/time**: click the 🗓 icon to set a date and time for the discovery of the vulnerability.
  - **Discovered date/time precision**: from the drop-down menu select an option to provide an estimation of how accurate the vulnerability discovery time is: from **second** (dead-on accurate) to **year** (inaccurate).
  - **Published date/time**: click the 🗓 icon to set a date and time for the publication of the information about the vulnerability.
  - **Published date/time precision**: from the drop-down menu select an option to provide an estimation of how accurate the vulnerability publication time is: from **second** (dead-on accurate) to **year** (inaccurate).
  - **CVE-ID**: enter the **unique** (https://cve.mitre.org/cve/identifiers/) CVE **identifier** (https://en.wikipedia.org/wiki/common_vulnerabilities_and_exposures#cve_identifiers) to reference the vulnerability.
    Example: ***CVE-2017-6394* on CVE** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-6394) or ***CVE-2017-6394* on NVD** (https://web.nvd.nist.gov/view/vuln/detail?vulnid=cve-2017-6394).
  - **OSVDB-ID**: enter the **unique** (https://en.wikipedia.org/wiki/open_source_vulnerability_database) Open Source Vulnerability Database (OSVDB) identifier to reference the vulnerability.
    Note: the database was **shut down** (https://blog.osvdb.org/2016/04/05/osvdb-fin/) in April 2016, whereas the OSVDB blog is still active.
  - **CVSS score**: enter the **Common Vulnerability Scoring System (CVSS)** (https://en.wikipedia.org/wiki/cvss) value to assess the **severity of the vulnerability** (https://www.first.org/cvss).
    You can use an **online calculator** (https://www.first.org/cvss/calculator/3.0) to calculate the CVSS score of the vulnerability.
  - **Overall score**: global score assessing the severity of the vulnerability.

- **Base score**: the partial score resulting from the analysis and calculation of the ***Base Score* factors** (https://www.first.org/cvss/calculator/3.0).
- **Base vector**: the **attack vector** (https://www.first.org/cvss/calculator/3.0) defines how close the threat actor needs to be to attack the vilnerability. The further away the threat actor is from the exploit target, the higher the base scroe and the seriousness of the vulnerability.
- **Temporal score**: the partial score resulting from the analysis and calculation of the ***Temporal Score* factors** (https://www.first.org/cvss/calculator/3.0).
- **Temporal vector**: the **temporal score factors** (https://www.first.org/cvss/calculator/3.0) help assess the target's ability to respond to the vulnerability attack. They take into account aspects such as the availability of the exploit code, of a fix to patch the vulnerability, as well as the confidence level in the existence of the vulnerability.
- **Environmental score**: the partial score resulting from the analysis and calculation of the ***Environmental Score* factors** (https://www.first.org/cvss/calculator/3.0).
- **Environmental vector**: the **environmental score factors** (https://www.first.org/cvss/calculator/3.0) help assess the seriousness of the vulnerability in the specific context of the target environment and its assets. They take into account aspects such as data breach, loss of privacy or confidentiality, as well as reduced performance and availability.
- **Affected software**: this section holds details about the software product affected by the vulnerability.
- **Product**: enter the standard/commercial name of the software product.
  Example: *Prez-o-matic-fantastic*
- **Edition**: enter the flavor of the software product.
  Example: *PE*, *Home*, *Pro*.
- **Language**: enter the locale of the software product.
  Example: *English (US)*, *Portuguese (BR)*
- **Update**: enter any updates or service packs applied to the software product.
  Example: *SP1*
- **Vendor**: enter the vendor name of the software product.
  Example: *Ecorp*
- **Version**: enter the version name of the software product.
  Example: *4.2.1*
- **Device manufacturer**: if the vulnerability affects a hardware device, enter the name of the manufacturer.
  Example: *Omni Consumer Products*
- **Device model**: enter the model of the device.
  Example: *ED-209*
- **Device serial number**: enter the serial number of the device.
  Example: *OCP-ED-209-PK1580FF20SEC*
- **Device firmware version**: enter the version number of the device firmware.
  Example: *1.0.2*
- **Device system OS**: enter the name of the operating system the device is equipped with.
  Example: *TempleOS*
- **References**: enter a URL pointing to relevant reference information on the exploit target, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

- ✚ **Characteristic > Weakness**: select this option to add details about the specific weakness or flaw causing a vulnerability in the software product or the hardware device.
  The taxonomy and the categorization follow the **Common Weakness Enumeration (CWE)** `(https://cwe.mitre.org/)` list.
  - **Description**: describe the weakness and its effects — for example, ***Use of Non-Canonical URL Paths for Authorization Decisions*** `(https://cwe.mitre.org/data/definitions/647.html)`.
  - **CWE-ID**: enter the **CWE identifier** `(https://cwe.mitre.org/about/faq.html#b.2)` to reference the **weakness** `(https://nvd.nist.gov/cwe.cfm)`.
    The CWE ID format is *CWE-${int}*.
    Example: *CWE-647*
- ✚ **Characteristic > Configuration**: select this option to add details about the specific configuration of the software product or hardware device that causes a vulnerability.
  The taxonomy and the categorization follow the **Common Configuration Enumeration (CCE)** `(https://nvd.nist.gov/cce/index.cfm)` list.
  - **Description**: describe the affected configuration — for example, ***The Java Security Manager (JSM) should be enabled or disabled as appropriate.*** `(https://nvd.nist.gov/feeds/cce/cce-tomcat6-5.20130214.xls)`.
  - **CCE-ID**: enter the **CCE identifier** `(https://cce.mitre.org/about/faqs.html#b2)` to reference the **configuration** `(https://nvd.nist.gov/cce.cfm)`.
    The CCE ID format is *CCE-${random_integer}-${Luhn_algorithm_check_digit}*.
    Example: *CCE-26789-8*

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ✪ **> Observable**

  or:
- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:
- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click ✚ **(Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.
- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

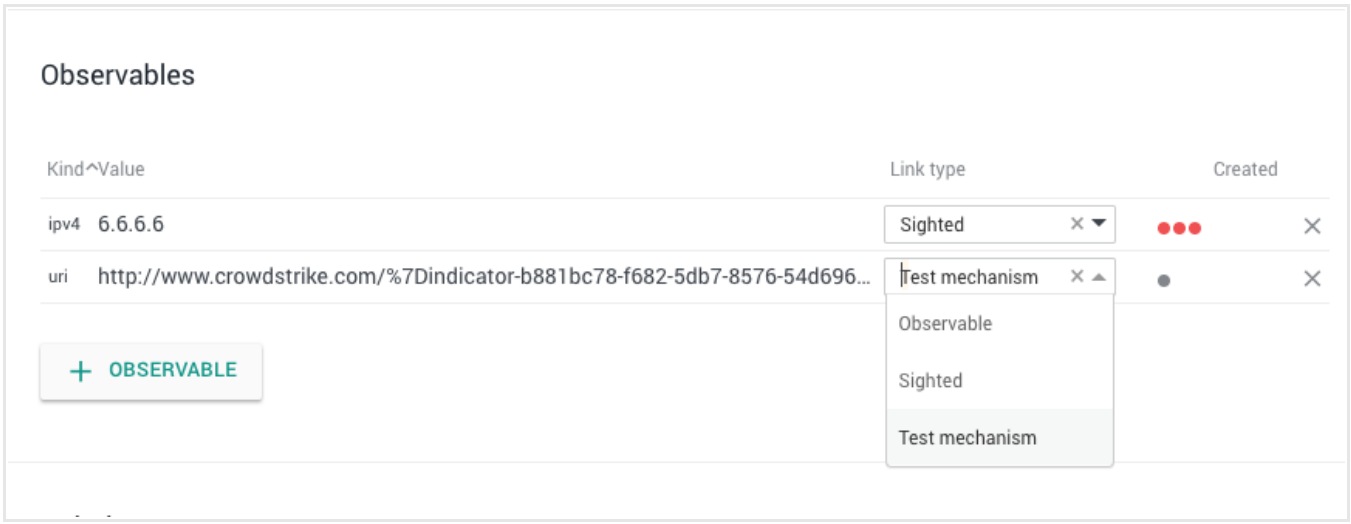
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the exploit target entity:

- **Affected**: describes an affected, impacted resource.
- **Configuration**: enter the **Common Configuration Enumeration (CCE)** `(https://nvd.nist.gov/config/cce/index)` code defining a specific security system configuration issue, as well as the related configuration guidance statement containing preferred or required settings or policies for the system configuration it refers to.
  Example: *CCE-5770-3*
- **Vulnerability**: enter the **Common Vulnerabilities and exposures (CVE)** `(https://cve.mitre.org/cve/identifiers/)` **identifier** `(https://en.wikipedia.org/wiki/common_vulnerabilities_and_exposures#cve_identifiers)` to reference the security threat.
  Example: ***CVE-2017-6394* on CVE** `(https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-6394)` or ***CVE-2017-6394* on NVD** `(https://web.nvd.nist.gov/view/vuln/detail?vulnid=cve-2017-6394)`.

- **Weakness**: enter the **Common Weakness Enumeration (CWE)** `(https://cwe.mitre.org/)` **identifier** `(https://en.wikipedia.org/wiki/common_weakness_enumeration)` to reference the software security weakness. Example: ***CWE-319*** `(http://cwe.mitre.org/data/definitions/319.html)`, ***CWE-642*** `(http://cwe.mitre.org/data/definitions/642.html)`.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the exploit target to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the exploit target
Potential courses of action	Outgoing relationship — Relates the exploit target to the selected potential course(s) of action on the **Search an entity** dialog
Related exploit targets	Outgoing relationship — Relates the exploit target to the selected exploit target(s) on the **Search an entity** dialog
Course of action → Related exploit targets	Incoming relationship — Relates the selected course(s) of action on the **Search an entity** dialog to the exploit target.
Report → Exploit targets	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the exploit target.
TTP → Exploit targets	Incoming relationship — Relates the selected TTP(s) on the **Search an entity** dialog to the exploit target.
Sighting → Exploit target	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the exploit target.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field. When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/exploit target — or outgoing — from the current origin exploit target/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.

- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the exploit target.
- **References**: enter a URL pointing to relevant reference information on the exploit target, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the exploit target to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create an incident

An incident describes a specific occurrence of indicators or observables affecting your organization or environment.

About incidents

An incident records a specific occurrence of indicators of compromise or observables affecting your organization or your system. An incident includes context information about the event such as start and end times, affected assets and resources, impact and seriousness assessment, any known threat actors and targeted victims involved, TTPs, related indicators and observables, and so on.

An incident leverages the following STIX entities:

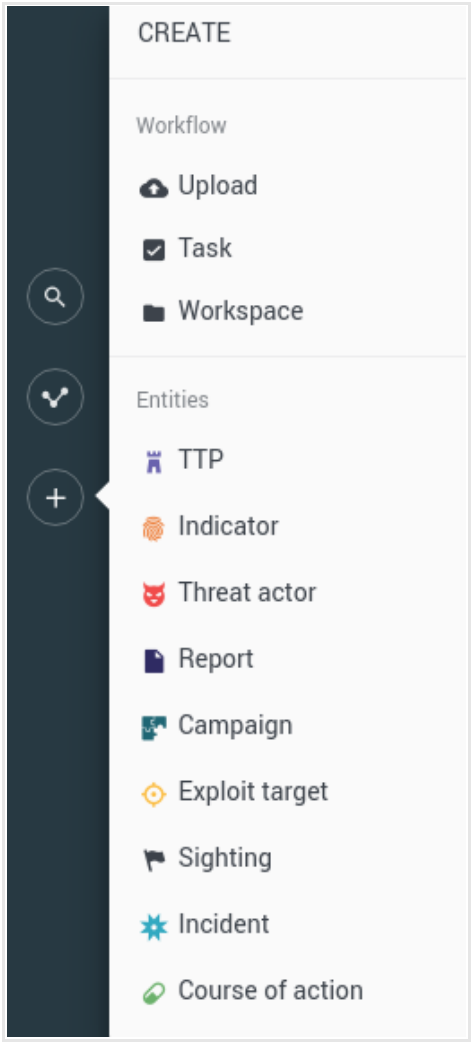
- Indicator
- Observable
- Threat actor
- TTP
- Course of action

Create an incident

✔ Input fields marked with an asterisk are required.

To create an **incident** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html)` in the platform to describe a discrete instance of an observable or an indicator affecting your organization or your system, do the following:

- On the left-hand navigation sidebar click **✚ > Incident**.



The entity editor opens at **Create Incident**, and you can start populating the input fields with content and details about the incident you are creating.

Define the general options

- **Title**: assign the new incident entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
- **Status**: from the drop-down menu select an option to indicate the current **status the incident is in** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440610)`.
- **Categories**: from the drop-down menu select one or more entries, as applicable, to describe the **type of incident** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440608)` amd the type of action or artifact that caused it.
- **Confidence**: it flags the **estimated level of confidence** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605)` to assess the accuracy and trustworthiness of the entity information.

- **Intended effects**: from the drop-down menu select one or more entries, as applicable, to describe what you reasonably assume to be the goal the threat actor implementing the TTP strives to achieve.
  Intended effects (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440615) range from personal advantage, to theft, to fraud or extortion. They all aim at damaging the target victim or system.
- **Security compromise**: from the drop-down menu select an option to report whether the incident **compromised security** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440629).
- **Discovery methods**: from the drop-down menu select an option to report how the **incident was detected** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440603).

Define the characteristics

Characteristics — This section holds structured, more detailed information about the incident.

- **Time coordinates**: sets a timeline and a timeframe for the incident.
- **Reporter**: identifies the source that **notified** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439807) the incident.
  It also clarifies **role** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613) of the reporter.
- **Coordinator**: identifies the individual, team, organization, entity or solution responsible for **managing, containing, and responding** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439807) to the incident.
  It also clarifies **role** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613) of the coordinator.
- **Responder**: identifies the individual, team, organization, entity or solution performing responsive or reactive tasks and procedures to defuse the incident. (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439807).
  It also clarifies **role** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613) of the responder.
- **Contact**: identifies the individual, team, organization, entity or solution acting as a point of contact and a source of information about the incident.
  It also clarifies **role** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613) of the contact.
- **Affected asset**: identifies and categorizies the **assets and resources** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439807) the incident targeted.
- **Impact**: assesses, quantifies, and qualifies the **impact and the damage** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439815) the incident caused.
- **Victim**: identifies the individual, team, organization, entity or artifact the incident **targeted and attacked** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439807).

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Time coordinates**: select this option to draw a timeline marking crucial events in the incident

history.

- **First malicious action**: click the 🗓 icon to set a date and time for the initial/first occurrence of a **malicious action** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
  A malicious action is any unathorized attempt to access the targeted assets. For example, probing, port scans, the beginning of a brute-force attach or a DDoS attack.
- **Time first malicious action precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **Initial compromise**: click the 🗓 icon to set a date and time for the occurrence of the **initial compromise** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810) of the targeted system, assets, resources or organization.
  It records the point in time when a security attribute of the targeted assets was compromised. For example: confidentiality, integrity, availability.
- **Time initial compromise precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **First data exfiltration**: click the 🗓 icon to set a date and time for the initial/first occurrence of an **unauthorized data grab** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810) from the targeted system, assets, resources or organization.
- **Time first data exfiltration precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **Incident discovery**: click the 🗓 icon to set a date and time marking the moment when the incident was **detected and discovered** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
- **Time incident discovery precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **Incident opened**: click the 🗓 icon to set a date and time marking the moment when the incident was **officially opened** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
- **Time incident opened precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **Containment achieved**: click the 🗓 icon to set a date and time marking the moment when the incident was **contained and kept under control** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
- **Time containment achieved precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **Restoration achieved**: click the 🗓 icon to set a date and time marking the moment when the assets and resources the incident targeted were **restored and brought back to normal operation** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
- **Time restoration achieved precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).
- **Incident reported**: click the 🗓 icon to set a date and time marking the moment when the incident was **officially recorded, registered, or logged** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
- **Time incident reported precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).

- **Incident closed**: click the icon to set a date and time marking the moment when the incident was **officially closed** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439810).
- **Time incident closed precision**: from the drop-down menu select an option to provide an estimation of how accurate the time estimation is: from **second** (dead-on accurate) to **year** (inaccurate).

- **✚ Characteristic > Reporter**: select this option to add details about the individual, the organization, or the resources related to the incident reporter's identity.

  The **Reporter** editor is based on the **CIQ standard** (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq) and its **specifications** (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html). The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.

  - **Name**: specify the name of the incident reporter. It should be descriptive and easy to remember.
    The reporter is the individual, team, organization, entity, system or mechanism that officially registers and communicates the occurrence of the incident.
  - **Roles**: from the drop-down menu select one or more options to specify the incident reporter's **role** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613).
    The role defines the function of the reporter concerning information tasks such as authoring, editing, updating, handling, and processing.
  - **Description**: enter a short description to provide additional context or extra details.

Under **✚ Characteristic > Reporter > Specification** you can define additional information related to the reporter such as payment accounts, individuals, organizations, and email addresses.

- Click **✚ Fields**.
  From the drop-down menu select an option to add the reporter-related details:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the reporter.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*
- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*

Key	Value
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*
- **✚ Characteristic > Coordinator**: select this option to add details about the individual, the organization, or the resources related to the incident coordinator's identity.

  The **Coordinator** editor is based on the **CIQ standard** `(https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq)` and its **specifications** `(http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html)`. The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.
  - **Name**: specify the name of the incident coordinator. It should be descriptive and easy to remember.
    The coordinator is the individual, team, organization, entity, system or mechanism that officially handles, manages, and orchestrates tasks and efforts to mititgate and contain the incident.
  - **Roles**: from the drop-down menu select one or more options to specify the incident coordinator's **role** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)`.
    The role defines the function of the coordinator concerning information tasks such as authoring, editing, updating, handling, and processing.
  - **Description**: enter a short description to provide additional context or extra details.

Under **✚ Characteristic > Coordinator > Specification** you can define additional information related to the coordinator such as payment accounts, individuals, organizations, and email addresses.

- Click **✚ Fields**.
  From the drop-down menu select an option to add the coordinator-related details:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the coordinator.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*
- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*

Key	Value
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*
- **✚ Characteristic > Responder**: select this option to add details about the individual, the organization, or the resources related to the incident responder's identity.

  The **Responder** editor is based on the **CIQ standard** `(https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq)` and its **specifications** `(http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html)`. The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.
  - **Name**: specify the name of the incident responder. It should be descriptive and easy to remember.
    The responder is the individual, team, organization, entity, system or mechanism that immediately takes action to react to the incident.
  - **Roles**: from the drop-down menu select one or more options to specify the incident responder's **role** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)`.
    The role defines the function of the responder concerning information tasks such as authoring, editing, updating, handling, and processing.
  - **Description**: enter a short description to provide additional context or extra details.

Under **✚ Characteristic > Responder > Specification** you can define additional information related to the responder such as payment accounts, individuals, organizations, and email addresses.

- Click **✚ Fields**.
  From the drop-down menu select an option to add the responder-related details:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the responder.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*
- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*

Key	Value
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*
- **✚ Characteristic > Contact**: select this option to add details about the individual, the organization, or the resources related to the incident contact's identity.

  The **Coordinator** editor is based on the **CIQ standard** (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq) and its **specifications** (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html). The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.
  - **Name**: specify the name of the incident contact. It should be descriptive and easy to remember.
    The contact is the individual, team, organization, entity, system or mechanism that acts as the official point of contact liasing with the different parties involved in the incident response.
  - **Roles**: from the drop-down menu select one or more options to specify the incident contact's **role** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613).
    The role defines the function of the contact concerning information tasks such as authoring, editing, updating, handling, and processing.
  - **Description**: enter a short description to provide additional context or extra details.

Under **✚ Characteristic > Contact > Specification** you can define additional information related to the contact such as payment accounts, individuals, organizations, and email addresses.

- Click **✚ Fields**.
  From the drop-down menu select an option to add the contact-related details:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the contact.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*
- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*

Key	Value
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*
- ✚ **Characteristic > Affected asset** : select this option to add details about the **affected assets and resources** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part6-incident/stix-v1.2.1-csprd01-part6-incident.html#_toc440439812) the incident targeted/is targeting.
  - **Description**: enter a short description to provide additional context or extra details about the impacted assets.
  - **Asset type**: from the drop-down menu select an option to specify the **type of asset** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440595) the incident impacted.
  - **Ownership class**: from the drop-down menu select an option to define the **owner of the affected assets** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440624).
  - **Management class**: from the drop-down menu select an option to identify the individual, team, group or entity responsible for **managing the affected assets** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440620).
  - **Location class**: from the drop-down menu select an option to define the **place where the affected assets reside** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440616).
  - **Business function or role**: enter a short free-text description of the tasks or processes the affected assets perform.
    Example: *Customer support ticketing workflow manager*, *Indexing server and service*

- Under **Properties affected**, you can specify which security attributes the incident compromised.
  - **Property**: from the drop-down menu select an option to specify **which security attribute** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440618) the incident compromised.
  - **Type of availability loss**: from the drop-down menu select an option to specify how exactly the incident compromised **asset and/or resource availability** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440598).
  - **Duration of availability loss**: from the drop-down menu select an option to provide an estimation of **how long the availability loss** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440617) is likely to last as a consequence of the incident.
  - **Non public data compromised**: from the drop-down menu select an option to indicate if the security breach compromised assets and/or resources that were until the incident occurrence **undisclosed and not publicly accessible** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440629).
  - **Description of effect**: enter a short free-text description of the effects resulting from the security attributes being compromised.
    Example: *Security breach exfiltrated sensitive data and blocked automated order processing.*

    Click **✚ Add** or **✚ More** to add new rows/new input fields as needed.
    To confirm the current input and to display a new input field, press **ENTER**.
- **✚ Characteristic > Impact**: select this option to add details about the effects and the consequences of the damage resulting from the .
  - **Effects**: from the drop-down menu select one or more options to specify **which type of assets or resources** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440609) the incident impacted and damaged.
  - **Direct impact summary**: this section assesses the immediate damage that is a direct consequence of the incident.
    - **Asset losses**: from the drop-down menu select an option to estimate the **extent of the damage** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440607) the incident caused.
    - **Business mission disruption**: from the drop-down menu select an option to estimate how much the incident **affected the smooth flow of business** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440607).
    - **Response and recovery costs**: from the drop-down menu select an option to estimate the **necessary costs** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440607) to respond to, contain, and recover from the incident.

- **Indirect impact summary**: this section assesses the damage that occurred as a side effect in the chain of events related to the incident.
  - **Loss of competitive advantage**: from the drop-down menu select an option to indicate if the incident compromised the ability of the organization to **remain competitive on the market** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440629).
  - **Brand and market damage**: from the drop-down menu select an option to indicate if the incident produced a negative effect on **brand perception and market position** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440629).
  - **Increased operating costs**: from the drop-down menu select an option to indicate if the incident made **normal business operations more expensive** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440629).
  - **Legal and regulatory costs**: from the drop-down menu select an option to indicate if the incident brought in **costs related to legal services** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440629).
  - **Impact qualification**: from the drop-down menu select an option to estimate the **severity of the consecquences** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440606) the incident caused.
- **Total loss estimation**: this section provides an estimate of the financial damage the incident caused.
  - **Initial reported**: temporary estimate following the discovery and notification of the incident.
    - **Amount**: enter a numerical value to indicate the currency amount. Use a dot (**.**) as a decimal separator. Example: *3141.59*
    - **Currency**: enter the currency code in **ISO 4217 format** (https://en.wikipedia.org/wiki/iso_4217). Example: *EUR*, *JPY*, *GBP*
  - **Actual**: accurate estimate following an inventory of the affected assets and resources, as well as collateral damage.
    - **Amount**: enter a numerical value to indicate the currency amount. Use a dot (**.**) as a decimal separator. Example: *3141.59*
    - **Currency**: enter the currency code in **ISO 4217 format** (https://en.wikipedia.org/wiki/iso_4217). Example: *EUR*, *JPY*, *GBP*

- **✚ Characteristic > Victim**: select this option to add details about the individual, the organization, or the resources related to the incident coordinator's identity.

  The **Victim** editor is based on the **CIQ standard** (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq) and its **specifications** (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html). The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.

  - **Name**: specify the name of the victim the incident targeted/is targeting. It should be descriptive and easy to remember.

Under **✚ Characteristic > Victim > Specification** you can define the type of victim under attack. You can describe affected individuals, organizations, and assets.

- Click ✚ **Fields**.
  From the drop-down menu select an option to define the type of victim:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the victim.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*
- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click ✚ **Add** or ✚ **More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click ✚ **Add** or ✚ **More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*

Key	Value
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ⊕ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click **✚ (Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.
- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

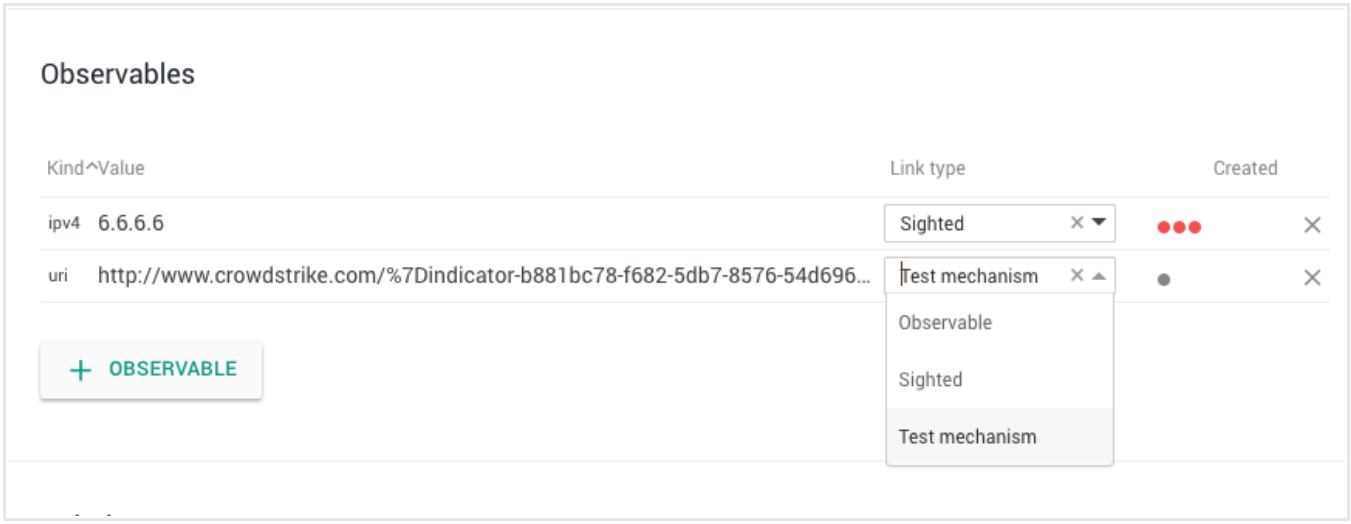
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the incident entity:

- **Affected asset**: defines an affected, impacted resource or **asset type** (`https://stixproject.github.io/data-model/1.2/stixvocabs/assettypevocab-1.0/`).
- **Related**: holds one or more observables that are related to this one.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the incident to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the incident
Related indicators	Outgoing relationship — Relates the incident to the selected indicator(s) on the **Search an entity** dialog.
Leveraged TTPs	Outgoing relationship — Relates the incident to the selected TTP(s) on the **Search an entity** dialog.
Attributed threat actors	Outgoing relationship — Relates the incident to the selected threat-actor(s) on the **Search an entity** dialog.
Related incidents	Outgoing relationship — Relates the incident to the selected incident(s) on the **Search an entity** dialog.
Courses of action requested	Outgoing relationship — Relates the incident to the selected course(s) of action on the **Search an entity** dialog to respond to the incident.
Courses of action taken	Outgoing relationship — Relates the incident to the selected course(s) of action on the **Search an entity** dialog that are carried out as a response to the incident.
Campaign → Related incidents	Incoming relationship — Relates the selected campaign(s) on the **Search an entity** dialog to the incident.
Course of action → Related incidents	Incoming relationship — Relates the selected course(s) of action on the **Search an entity** dialog to the incident.
Report → Incidents	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the incident.
Sighting → Incident	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the incident.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field. When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/incident — or outgoing — from the current origin incident/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the incident.
- **References**: enter a URL pointing to relevant reference information on the incident, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP (`https://www.us-cert.gov/tlp`) provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the incident to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.

- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create an indicator

An indicator identifies specific observable patterns, links them to TTPs, and provides additional context to the cyber threat scenario under investigation.

About indicators

An indicator, or an **indicator of compromise (IOC)** (https://en.wikipedia.org/wiki/indicator_of_compromise), is a footprint or a fingerprint an intruder **leaves behind** (https://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/) in a targeted system. It is a ripple in the “all systems running normally” pond indicating anomalous or unusual activity or behavior in the system.

For example, you can spot indicators in logs, call stacks, tracebacks, network stream, and responses to request calls — look for unexpected data:

- Unusual spikes in incoming or outgoing network traffic
- Access from IP addresses in unexpected geographic locations
- Anomalous DNS requests
- Access across security zones
- Connections on unusual ports or protocols
- Hosts systematically failing to connect to a target
- High counts of failed login attempts
- Unusual database activity
- Suspicious file or registry changes

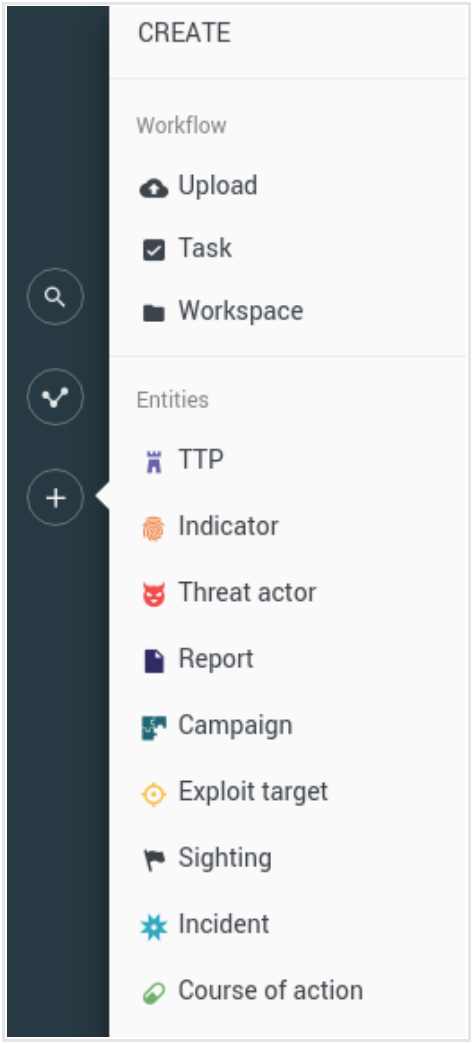
Indicators help you identify patterns to link observables and TTPs, so that you can react with an appropiate course of action, as well as implement preventive measures.

Create an indicator

✔ Input fields marked with an asterisk are required.

To create an indicator in the platform to record an anomalous artifact or event, do the following:

- On the left-hand navigation sidebar click **+ > Indicator**.



The entity editor opens at **Create Indicator**, and you can start populating the input fields with content and details about the indicator you are creating.

Define the general options

- **Title**: assign the new indicator entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
- **Types**: from the drop-down menu select an option to define the **indicator type** `(https://stixproject.github.io/data-model/1.2/stixvocabs/indicatortypevocab-1.1/)` whose effects you want to describe.
- **Confidence**: it flags the **estimated level of confidence** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605)` to assess the accuracy and trustworthiness of the entity information.
- **Likely impact**: from the drop-down menu select an option to assess the estimated **impact** `(https://stixproject.github.io/data-model/1.2/stixvocabs/highmediumlowvocab-1.0/)` of the intrusion on the targeted system or organization.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the indicator.

- **Time window**: define a start and an end date to record a specific time interval for the anomalous artifact or event activity.
- **Test mechanism**: a **test mechanism** (https://stixproject.github.io/data-model/1.2/indicator/testmechanismtype/) enables the platform to share entity information with external tools and systems. In particular, it is useful to send indicator information to an **IDS/HIDS/NIDS** (https://en.wikipedia.org/wiki/intrusion_detection_system) to test it against a tool-specific rule. When matching hits are returned, you can either analyze them further, or include them in an automation workflow; for example, to generate sightings.
  - **Generic**: **generic test mechanism** (https://stixproject.github.io/data-model/1.2/genericm/generictestmechanismtype/) to interact with a generic system supporting plain text format as an input.
  - **Snort**: **Snort test mechanism** (https://stixproject.github.io/data-model/1.2/snorttm/snorttestmechanismtype/).
    You can include the indicator in an outgoing feed to a Snort instance. The Snort rules in the indicator are used to look for **matching patterns** (https://stixproject.github.io/documentation/idioms/snort-test-mechanism/) in the Snort logs. You can configure Snort so that matching hits trigger a follow-up action. For example, creating a sighting or adding a malicious entry to a blocklist.
  - **YARA**: **YARA test mechanism** (https://stixproject.github.io/data-model/1.2/yaratm/yaratestmechanismtype/).
    You can include the indicator in an outgoing feed to a YARA instance. YARA uses the rules in the indicator to look for **matching patterns** (https://stixproject.github.io/documentation/idioms/yara-test-mechanism/) in the target files or locations you specify in YARA.
    You can feed indicators from the platform to YARA to look for, identify, and classify malware samples.
- **Sighting**: a sighting characteristic means that you observed a distinct occurrence of the indicator in your environment.

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Time window** : select this option to define a time period when the anomalous artifact or event activity took place.
  - **Start time**: click the 📅 icon to select the date marking the beginning of the time period.
  - **Start precision**: from the drop-down menu select an option to provide an estimation of how accurate the start date is: from **second** (dead-on accurate) to **year** (inaccurate).
  - **End time**: click the 📅 icon to select the date marking the end of the time period.
  - **End precision**: from the drop-down menu select an option to provide an estimation of how accurate the end date is: from **second** (dead-on accurate) to **year** (inaccurate).
- **✚ Characteristic > Test mechanism > Snort** : select this option to define a **Snort test mechanism** (https://stixproject.github.io/documentation/idioms/snort-test-mechanism/) to search Snort logs for matching patterns, based on the specified **Snort rules** (https://www.snort.org/documents/snort-rule-infographic).

- **Type**: from the drop-down menu select **Snort**.

- **Efficacy**: from the drop-down menu select an option to assess the **effectiveness of the test mechanism** (https://stixproject.github.io/data-model/1.2/stixvocabs/highmediumlowvocab-1.0/) at detecting the targeted observables.
- **Product name**: enter the name of the Snort-compatible tool used to author the rules. Specify a **CPE name** (https://nvd.nist.gov/cpe.cfm), if available.
- **Version**: enter the version of the Snort-compatible tool used to author the rules.
- **Signature (rule)**: enter the **Snort rule** (http://commons.oreilly.com/wiki/index.php/snort_cookbook/rules_and_signatures) you want to use to look for malicious patterns and behaviors. The rule needs to be complete and in the Snort rule native format.
- **Event filters**: **event filtering** (http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node19.html) helps you reduce data noise. It sets a threshold to limit the number of times an event gets logged during a specified time period.
  - Click **✚ Add** or **✚ More** to add new rows/new input fields as needed.
  - To confirm the current input and to display a new input field, press **ENTER**.
- **Rate filters**: **rate filters** (http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node19.html) change rule behavior. They can trigger a follow-up action in Snort when the rule exceeds a predefined amount of matches in a specified time interval.
  - Click **✚ Add** or **✚ More** to add new rows/new input fields as needed.
  - To confirm the current input and to display a new input field, press **ENTER**.
- **Event suppressions**: **event suppression** (http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node19.html) disables logging for irrelevant events, based on an IP list.
  - Click **✚ Add** or **✚ More** to add new rows/new input fields as needed.
  - To confirm the current input and to display a new input field, press **ENTER**.
- **Producer — Identity — Name**: enter the name of the producer who authored the rules. This value identifies the source of the rules.
- **Producer — Time — Start**: click the 📅 icon to select the date marking the beginning of the **relevant time period** (https://stixproject.github.io/data-model/1.2/cyboxcommon/timetype/) the data refers to.
- **Producer — Time — Start precision**: from the drop-down menu select an option to provide an estimation of how accurate the start date is: from **second** (dead-on accurate) to **year** (inaccurate)..
  If you do not set precision, the default value is **second**.
- **Producer — Time — End**: click the 📅 icon to select the date marking the end of the relevant time period the data refers to.

- **Producer — Time — End precision**: from the drop-down menu select an option to provide an estimation of how accurate the end date is from: **second** (dead-on accurate) to **year** (inaccurate).
  If you do not set precision, the default value is **second**.
- **Producer — Time — Received**: click the 📅 icon to select the date when you obtained the data.
- **Producer — Time — Received precision**: from the drop-down menu select an option to provide an estimation of how accurate the received date is: from **second** (dead-on accurate) to **year** (inaccurate).
  If you do not set precision, the default value is **second**.
- **Producer — References — Reference back URL** : enter a URL pointing to relevant reference information on the indicator, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

- ✚ **Characteristic > Test mechanism > YARA** : select this option to define a **YARA** (https://virustotal.github.io/yara/) test mechanism to use **YARA** (https://yara.readthedocs.io/) pattern matching functionality to look for, identify, and classify malware samples based on the specified **YARA rules** (http://yara-generator.net/).
  - **Type**: from the drop-down menu select **YARA**.

  - **Efficacy**: from the drop-down menu select an option to assess the **effectiveness of the test mechanism** (https://stixproject.github.io/data-model/1.2/stixvocabs/highmediumlowvocab-1.0/) at detecting the targeted malware samples.
  - **Signature (rule)**: enter the **YARA rule** (https://github.com/neo23x0/yargen) you want to use to look for malicious patterns. The **rule** (https://github.com/yara-rules/rules) needs to be complete and in the YARA rule native format.
  - **Producer — Identity — Name**: enter the name of the producer who authored the rules. This value identifies the source of the rules.
  - **Producer — Time — Start**: click the 🗓 icon to select the date marking the beginning of the **relevant time period** (https://stixproject.github.io/data-model/1.2/cyboxcommon/timetype/) the data refers to.
  - **Producer — Time — Start precision**: from the drop-down menu select an option to provide an estimation of how accurate the start date is: from **second** (dead-on accurate) to **year** (inaccurate)..
    If you do not set precision, the default value is **second**.
  - **Producer — Time — End**: click the 🗓 icon to select the date marking the end of the relevant time period the data refers to.
  - **Producer — Time — End precision**: from the drop-down menu select an option to provide an estimation of how accurate the end date is from: **second** (dead-on accurate) to **year** (inaccurate).
    If you do not set precision, the default value is **second**.
  - **Producer — Time — Received**: click the 🗓 icon to select the date when you obtained the data.
  - **Producer — Time — Received precision**: from the drop-down menu select an option to provide an estimation of how accurate the received date is: from **second** (dead-on accurate) to **year** (inaccurate).
    If you do not set precision, the default value is **second**.
  - **Producer — References — Reference back URL** : enter a URL pointing to relevant reference information on the indicator, if available.
    - The field takes only URLs as input. Enter one URL per field.
      To confirm the current input and to display a new input field, press **ENTER**.
    - To remove an input field from this section, click the corresponding ✖ icon.

- ✚ **Characteristic > Test mechanism > Generic** : select this option to define a **generic test mechanism** (https://stixproject.github.io/data-model/1.2/generictm/generictestmechanismtype/) to use, for example, rule or regex-enabled pattern matching functionality to look for anomalous events, actions, behavior, or potentially malicious artifacts.
  - **Type**: from the drop-down menu select **Generic**.

  - **Efficacy**: from the drop-down menu select an option to assess the **effectiveness of the test mechanism** (https://stixproject.github.io/data-model/1.2/stixvocabs/highmediumlowvocab-1.0/) at detecting the targeted malware samples.
  - **Description**: enter a short description to provide additional context or extra details about the mechanism, the authoring tool or the rule format. Specify a **CPE name** (https://nvd.nist.gov/cpe.cfm), if available.
  - **Specification**: enter the mechanism you want to use to look for anomalies or malicious artifacts. For example, a rule or a regex.
  - **Producer — Identity — Name**: enter the name of the producer who authored the rules. This value identifies the source of the rules.
  - **Producer — Time — Start**: click the 🗓 icon to select the date marking the beginning of the **relevant time period** (https://stixproject.github.io/data-model/1.2/cyboxcommon/timetype/) the data refers to.
  - **Producer — Time — Start precision**: from the drop-down menu select an option to provide an estimation of how accurate the start date is: from **second** (dead-on accurate) to **year** (inaccurate)..
    If you do not set precision, the default value is **second**.
  - **Producer — Time — End**: click the 🗓 icon to select the date marking the end of the relevant time period the data refers to.
  - **Producer — Time — End precision**: from the drop-down menu select an option to provide an estimation of how accurate the end date is from: **second** (dead-on accurate) to **year** (inaccurate).
    If you do not set precision, the default value is **second**.
  - **Producer — Time — Received**: click the 🗓 icon to select the date when you obtained the data.
  - **Producer — Time — Received precision**: from the drop-down menu select an option to provide an estimation of how accurate the received date is: from **second** (dead-on accurate) to **year** (inaccurate).
    If you do not set precision, the default value is **second**.
  - **Producer — References — Reference back URL** : enter a URL pointing to relevant reference information on the indicator, if available.
    - The field takes only URLs as input. Enter one URL per field.
      To confirm the current input and to display a new input field, press **ENTER**.
    - To remove an input field from this section, click the corresponding ✖ icon.
- ✚ **Characteristic > Sighting**: select this option to notify a specific occurrence of the indicator in your environment.

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ✪ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click **✚ (Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.

- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

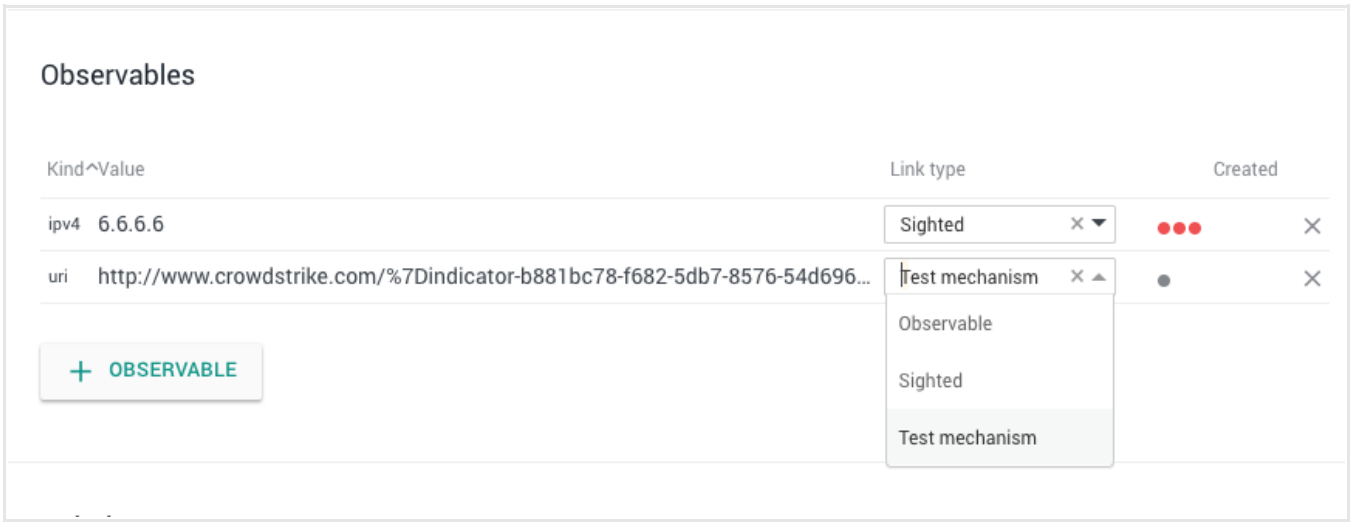
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the indicator entity:

- **Observable**: the observable related to the entity is an embedded CybOX observable object.
  It has been detected *outside* the organization.
- **Sighted**: the observable related to the entity is an embedded CybOX observable object.
  At least one specific occurrence of the observable related to the entity has been detected, that is, sighted, *inside* the organization.

- **Test mechanism**: a **test mechanism** (https://stixproject.github.io/data-model/1.2/indicator/testmechanismtype/) enables the platform to share entity information with external tools and systems. In particular, it is useful to send information to an **IDS/HIDS/NIDS** (https://en.wikipedia.org/wiki/intrusion_detection_system) to test it against a tool-specific rule.

  For example, an observable with a **Test mechanism** link name can trigger follow-up actions in external systems:

  - **Rule**: **generic test mechanism** (https://stixproject.github.io/data-model/1.2/genericm/genericmtestmechanismtype/) to interact with a generic system supporting plain text format as an input.
  - **Snort**: **Snort test mechanism** (https://stixproject.github.io/data-model/1.2/snorttm/snorttestmechanismtype/).
    You can include the observable in an outgoing feed to a Snort instance. The Snort rules in the indicator are used to look for **matching patterns** (https://stixproject.github.io/documentation/idioms/snort-test-mechanism/) in the Snort logs. You can configure Snort so that matching hits trigger a follow-up action. For example, creating a sighting or adding a malicious entry to a blocklist.
  - **YARA**: **YARA test mechanism** (https://stixproject.github.io/data-model/1.2/yaratm/yaratestmechanismtype/).
    You can include the observable in an outgoing feed to a YARA instance. YARA uses the rules in the indicator to look for **matching patterns** (https://stixproject.github.io/documentation/idioms/yara-test-mechanism/) in the target files or locations you specify in YARA.
    You can feed indicators from the platform to YARA to look for, identify, and classify malware samples.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the indicator to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the indicator
Indicated TTPs	Outgoing relationship — Relates the indicator to the selected TTPs(s) on the **Search an entity** dialog.
Suggested courses of action	Outgoing relationship — Relates the indicator to the selected course(s) of action on the **Search an entity** dialog. Recommends carrying out a course of action to respond to the indicator.
Related indicators	Outgoing relationship — Relates the indicator to the selected indicator(s) on the **Search an entity** dialog.
Related campaigns	Outgoing relationship — Relates the indicator to the selected campaign(s) on the **Search an entity** dialog.
Incident → Related indicators	Incoming relationship — Relates the selected incident(s) on the **Search an entity** dialog to the indicator.
Report → Indicators	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the indicator.
Sighting → Indicator	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the indicator.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field.
When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don’t know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/indicator — or outgoing — from the current origin indicator/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the indicator.

- **References**: enter a URL pointing to relevant reference information on the indicator, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP (`https://www.us-cert.gov/tlp`) provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the indicator to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.

- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create a report

A report wraps around different pieces of threat intelligence to weave a common story into a consistent narrative.

About reports

During an analysis or an investigation, analysts use a number of sources to gather many bits of information. They sift through the data to separate the wheat from the chaff, and then they start connecting the dots to gain a broader perspective and add meaning to the data.

By exploring entity relationships and by gaining extra context through enrichment, they can weave a solid narrative to accurately and objectively describe the threat scenario under investigation.

Intel reports provide a suitable format to structure and to organize this type of content: analysts can include their analysis of the threat scenario, make mitigation recommendations, as well as include links to entities, observables, and relationships in the platform. They can also add relevant attachments such as samples or PDF documents. Moreover, they can specify metadata such as the time ranges defining the start and and time of the observed threat, and the time of observation. Last but not least, tags help organize and categorize the intelligence.

Intel reports give their intended recipients a rich and sharp picture of the cyber threat landscape they may need to act on. They can follow links to further explore the reported threat relationships with other potentially malicious elements such as campaigns, C2 infrastructure, or threat actors.

Intel reports implement **microdata** `(https://www.w3.org/tr/microdata/#overview)` to add machine-readable semantic relevance to the content. Analysts can leverage microdata to reference any entities, relationships, and observables they include in the reports.

Analysts can publish reports in HTML format through outgoing feeds using any of the supported transport types. When they choose to make reports available by email, the HTML reports are attached to the email messages before sending them to the intended recipients.

About content

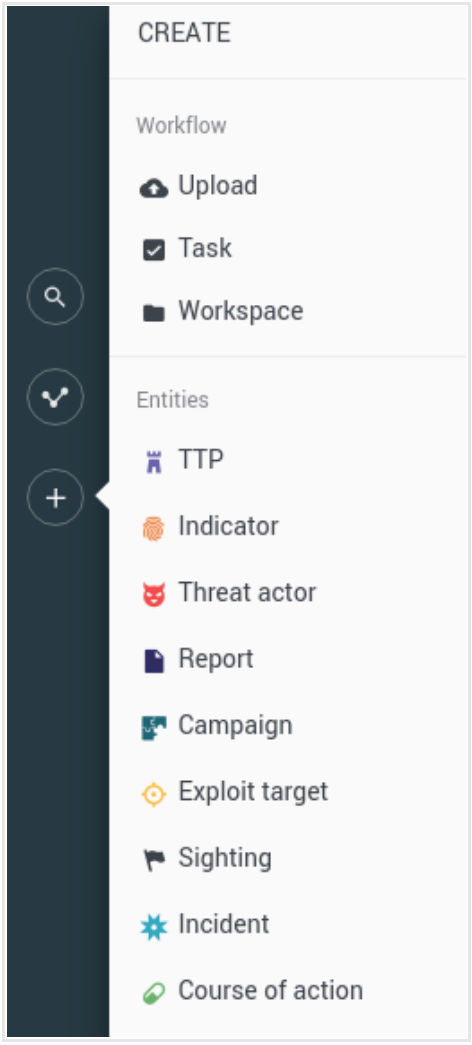
When the platform ingests unstructured content — either through an incoming feed or a manual file upload — to produce a report entity, the original unstructured source is attached in its original format to the resulting report entity. In this way, when analysts modify or update the the resulting report entity, they can always refer back to the original information.

Create a report

✔ Input fields marked with an asterisk are required.

To create a report in the platform, do the following:

- On the left-hand navigation sidebar click **✚ > Report**.



The entity editor opens at **Create Report**, and you can start populating the input fields with content and details about the report you are creating.

Define the general options

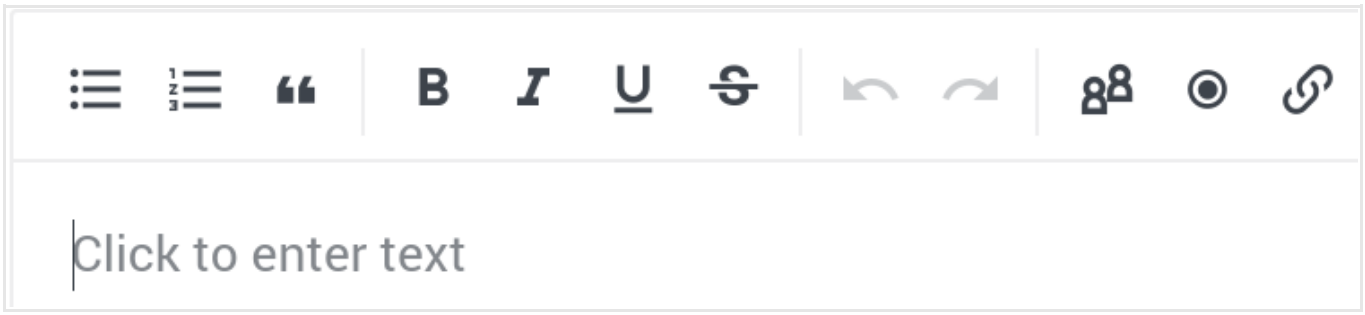
- **Title**: assign the new **report** `(https://stixproject.github.io/data-model/1.2/report/reporttype/)` entity a clear and descriptive title.
  The title name appears also on the entity detail pane header section.

- Click ✚ **Section** to add a content section to the report:
  - **Summary**: write a short summary to highlight the main points and/or the core concepts discussed in the report.
  - **Analysis**: in this section you weave your story to clearly communicate the core message of the report: organize your information to set the stage (background details and context), unfold the timeframe of the events the report describes, and introduce the characters such as threat actors, targeted victims, as well as any malicious sidekicks such as (money) mules. These are the foundations shaping the threat scenario under analysis.

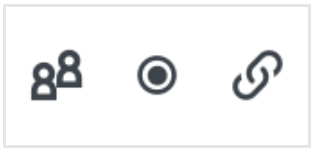
    Proceed to describe motives and intentions, behaviors, strategies, tactics, and techniques. Include any relevant details about resources and infrastructure, be it a C2 server or targeted assets.

    In short, this is where analysts use their story-telling skills to make their point to the stakeholders who will read the report and who may or may not decide to (re)act on the basis of the intelligence value of the report.
  - **Recommendations**: after the analysis, formulate a set of recommendations to reduce risk and to mitigate possible or likely damage.
    You can make recommendations on areas such as prevention, detection, and response.

When you position the cursor inside the **Summary**, **Analysis** or **Recommendations** field, a rich text editor becomes available to help you format content:



You can format text, create ordered/numbered and unordered/bulleted lists, undo and redo actions, as well as insert relationships, observables, and references:



- **Insert relationship**: add a relationship to existing entities describing actors, victims, targets, and other roles and resources that are relevant to the report narrative.
- **Insert observable**: create a new observable on the fly and add it to the report to reference specific bits of information that are relevant to the report narrative, such as an address, an IP address, or a credit card number.
- **Insert reference**: enter a URL pointing to relevant reference information on the report, if available.
  Reference should provide more context to get a sharper picture of the threat scenario.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

When you publish the report, any inserted relationships, observables and references are indexed and made searchable. You can click these links to open the detail pane of the selected relationship or observable, or to follow a link to a reference.

- **Intents**: from the drop-down menu select one or more options to define the main **purpose** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440628) of the report, that is, the main item(s) discussed in the report, and the main topic(s) it focuses on.

- **Information source**: provide details about the source of the information included in the report.
  - **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
  - **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
  - **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the report.
  - **References**: enter a URL pointing to relevant reference information on the report, if available.
    - The field takes only URLs as input. Enter one URL per field.
      To confirm the current input and to display a new input field, press **ENTER**.
    - To remove an input field from this section, click the corresponding ✖ icon.
- **Attachment**: you can attach relevant files by dragging and dropping them onto the highlighted upload area. Alternatively, click anywhere on the upload area, browse to the location where the file you want to upload is stored, and then select it.

  To remove an uploaded file from the attachment list, click **Remove file**: the attachment is instantly removed, without prompting you to confirm the action.

> If you publish reports with attachments through an outgoing feed, *attachments are excluded from the feed*. Only the report entity *without attachments* is included in the outgoing feed.

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ⊕ **> Observable**

  or:
- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:
- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.

- On the entity detail pane, click the **Observables** tab.
- On the active view, click **+ (Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.
- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

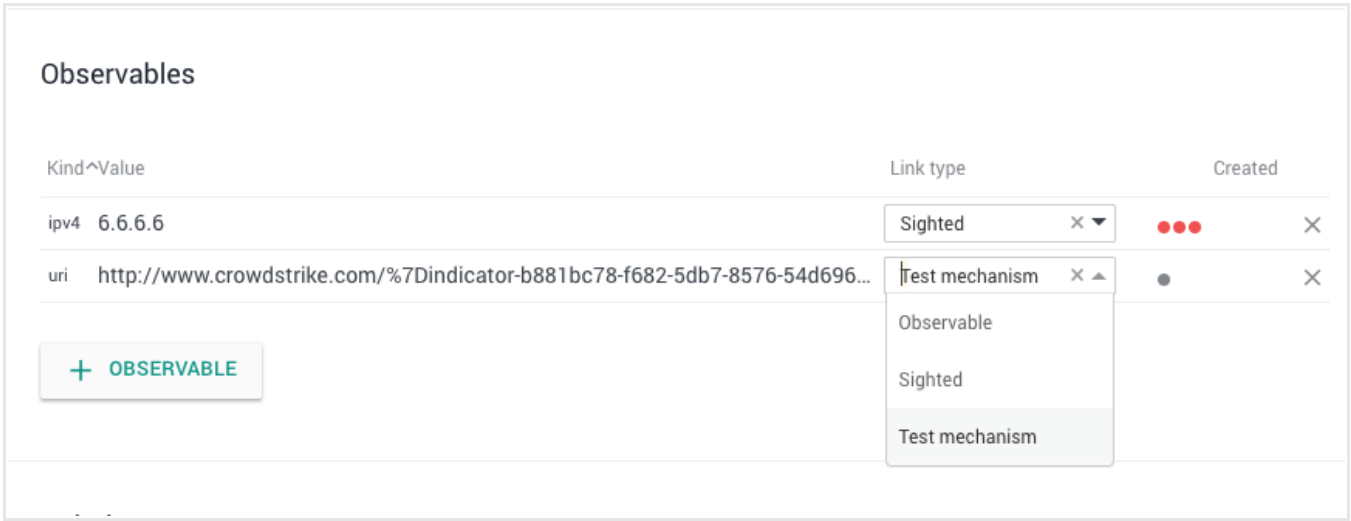
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the report entity:

- **Observable**: the observable related to the entity has been detected *outside* the organization.
  It represents a potential threat that may or may not impact your organization.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (,) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*

- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the report to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the report
Indicators	Outgoing relationship — Relates the report to the indicator(s) on the **Search an entity** dialog.
TTPs	Outgoing relationship — Relates the report to the selected TTP(s) on the **Search an entity** dialog. Recommends carrying out a course of action to respond to the report.

Select this option…	… to create this relationship for the report
Exploit targets	Outgoing relationship — Relates the report to the selected exploit target(s) on the **Search an entity** dialog.
Incidents	Outgoing relationship — Relates the report to the selected incident(s) on the **Search an entity** dialog.
Courses of action	Outgoing relationship — Relates the report to the selected course(s) of action on the **Search an entity** dialog.
Campaigns	Outgoing relationship — Relates the report to the selected campaign(s) on the **Search an entity** dialog.
Threat actors	Outgoing relationship — Relates the report to the selected threat actor(s) on the **Search an entity** dialog.
Sighting → Report	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the report.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field.
When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/report — or outgoing — from the current origin report/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.

- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the report.
- **References**: enter a URL pointing to relevant reference information on the report, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the report to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create a sighting

A sighting describes a specific occurrence of an observable or an indicator.

About sightings

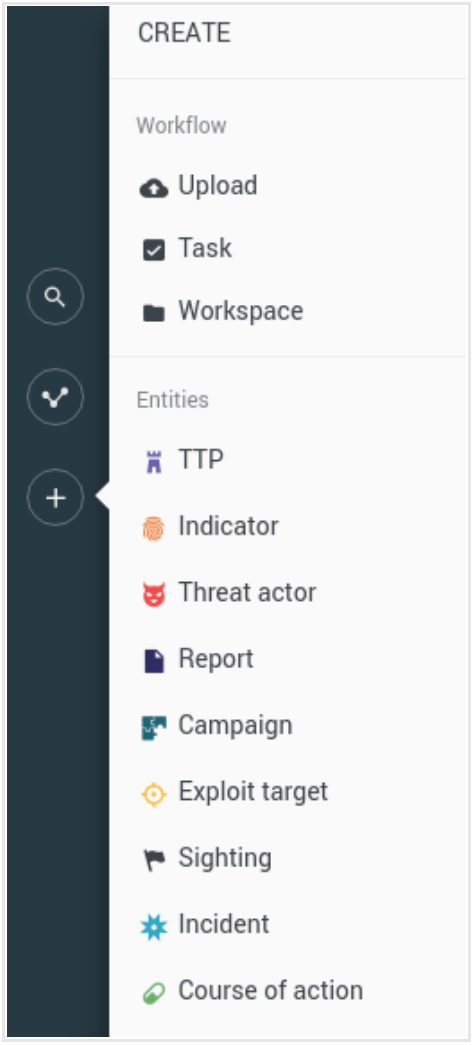
A sighting describes a specific occurrence of an indicator or an observable. It sets a date and a time when an instance of an indicator of compromise was observed in your organization or environment.

Create a sighting

✔ Input fields marked with an asterisk are required.

To create a **sighting** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part10-exploit-target/stix-v1.2.1-csprd01-part10-exploit-target.html) in the platform to describe a specific occurrence of an observable or an indicator in your organization or environment, do the following:

- On the left-hand navigation sidebar click **✚ > Sighting**.



The entity editor opens at **Create Sighting**, and you can start populating the input fields with content and details about the sighting you are creating.

Define the general options

- **Title**: assign the new **sighting** `(https://stixproject.github.io/data-model/1.2/indicator/sightingtype/)` entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
- **Confidence**: it flags the **estimated level of confidence** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605)` to assess the accuracy and trustworthiness of the entity information.
- **Impact**: from the drop-down menu select an option to assess the estimated **impact** `(https://stixproject.github.io/data-model/1.2/stixvocabs/highmediumlowvocab-1.0/)` of the sighted indicator of compromise on the targeted system or organization.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the sighting.

- **Related observables**: enables relating the sighting to one or more observables to create an association between the specific occurrence of the sighting and the potentially malicious objects observed during the sighting.
- **Security control**: describes the tools, systems, equipment, processes and procedures that are in place to manage and protect the confidentiality, integrity, and availability of the system and its data.
- **Raw events**: enables inserting raw event data related to the sighting.

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Related observables**: select this option to insert one or more observables you want to related to the sighting.
  - **Related observables — Kind**: from the drop-down menu select the type of observable you want to add.
    Example: *Domain*, *Ipv-4*, *City*, *Actor*
  - **Related observables —Value**: enter the value of the observable. The value and its format should match the specified observable type (kind).
    Insert one value entry per line.
    Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
  - Click **✚ Add** or **✚ More** to add new rows/new input fields as needed.
- **✚ Characteristic > Security control**: select this option to specify the security control tool, system, process or procedure that detected the sighting.
  - **Identity — Name**: enter the name of the security control acting as a data source for the sighting. It corresponds to the security control that detected the sighting.
  - **Time — Start**: click the 🗓 icon to select the date and time marking the beginning of the sighting observation period.
  - **Time — Start precision**: from the drop-down menu select an option to provide an estimation of how accurate the start date is: from **second** (dead-on accurate) to **year** (inaccurate).
  - **Time — End**: click the 🗓 icon to select the date and time marking the end of the sighting observation period.
  - **Time — End precision**: from the drop-down menu select an option to provide an estimation of how accurate the end date is: from **second** (dead-on accurate) to **year** (inaccurate).
  - **Time — Received**: click the 🗓 icon to select the date and time when a notification about the sighting was received.
  - **Time — Received precision**: from the drop-down menu select an option to provide an estimation of how accurate the sighting notification date is: from **second** (dead-on accurate) to **year** (inaccurate).
  - **References — Reference back URL**: enter a URL pointing to relevant reference information on the sighting, if available.
    - The field takes only URLs as input. Enter one URL per field.
      To confirm the current input and to display a new input field, press **ENTER**.
    - To remove an input field from this section, click the corresponding ✖ icon.
- **✚ Characteristic > Raw events**: select this option to paste raw event data related to the sighting.
  - **Raw events**: paste the raw event data as plain text in the input field.

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ✪ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click ✚ **(Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.

- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

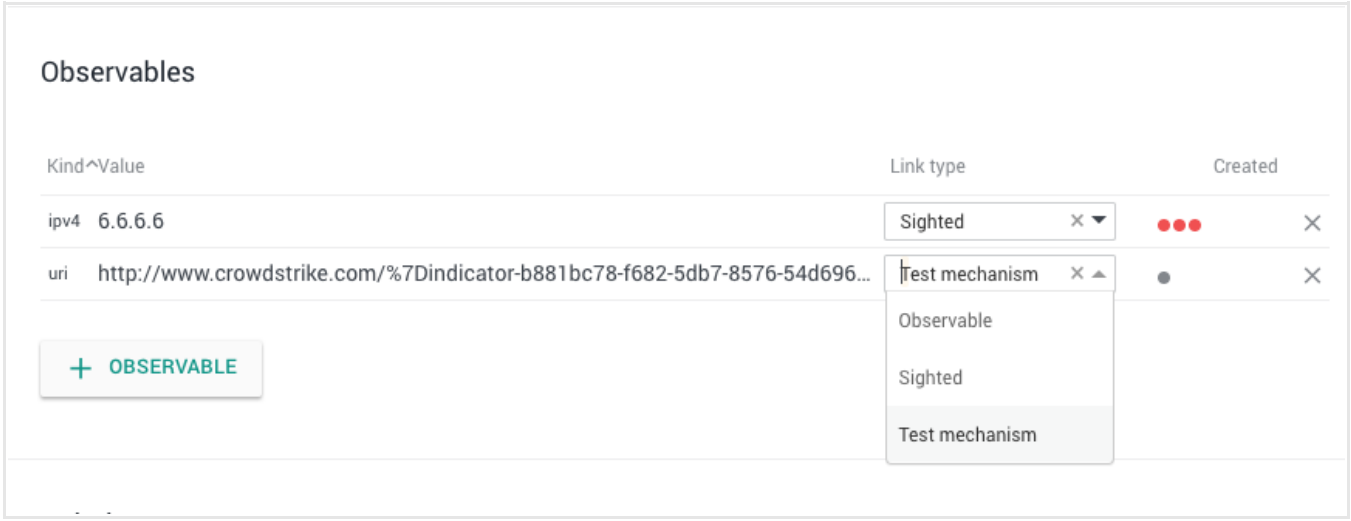
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the sighting entity:

- N/A. Campaign-related observables do not have link types.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.

For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the sighting to other entities:

- Under **Relationships** click **+ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

You can refine the displayed results by specifying a search string in the filter input field.
Alternatively, click one of the available filter options to select and filter by specific:

- **Entity types**
- **Source**
- **Date**
- **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the sighting
Campaign	Outgoing relationship — Relates the sighting to the selected campaign(s) on the **Search an entity** dialog.
Course of action	Outgoing relationship — Relates the sighting to the selected course(s) of action on the **Search an entity** dialog.
Exploit target	Outgoing relationship — Relates the sighting to the selected exploit target(s) on the **Search an entity** dialog.
Indicator	Outgoing relationship — Relates the sighting to the selected indicator(s) on the **Search an entity** dialog.
Incident	Outgoing relationship — Relates the sighting to the selected incident(s) on the **Search an entity** dialog.
Report	Outgoing relationship — Relates the sighting to the selected report(s) on the **Search an entity** dialog.

Select this option…	… to create this relationship for the sighting
Threat actor	Outgoing relationship — Relates the sighting to the threat actor(s) on the **Search an entity** dialog.
TTP	Outgoing relationship — Relates the sighting to the selected TTP(s) on the **Search an entity** dialog.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field.
When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/sighting — or outgoing — from the current origin sighting/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.

- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity. The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** (http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613) to the information in the sighting.
- **References**: enter a URL pointing to relevant reference information on the sighting, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP (https://www.us-cert.gov/tlp) provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the sighting to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create a threat actor

A threat actor identifies an adversary who is motivated to damage a targeted victim, usually for personal gain.

About threat actors

A threat actor is an adversary who is motivated to damage an individual, a group, an entity or an organization. Threat actors can be individuals, groups, or organizations; they can be nation-sponsored or nation-state actors; they can be external to the targeted victims, or they can be insider threats. The motivation that drives them ranges from economic, political, ideological, to revenge and bragging. The benefits they gain from attacking a targeted victim vary from financial, to reputation damage, to intellectual property theft, and so on.

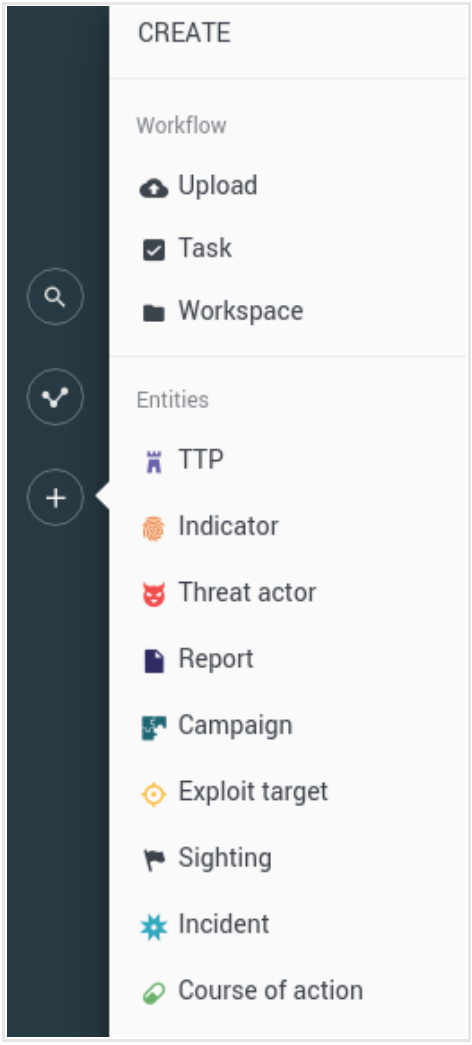
You can associate threat actors to TTPs and campaigns to understand how they plan and organize their attacks to the targeted victims. Indicators can help you track them, and relate them to observables and sightings. For example, an email address, an IP address, or a domain name associated with a real person's identity.

Create a threat actor

✔ Input fields marked with an asterisk are required.

To create a threat actor in the platform to record information that can help identfy them, do the following:

- On the left-hand navigation sidebar click **+ > Threat actor**.



The entity editor opens at **Create Threat actor**, and you can start populating the input fields with content and details about the threat actor you are creating.

Define the general options

- **Title**: assign the new threat actor entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
- **Types**: from the drop-down menu select an option to define the **threat actor type** `(https://stixproject.github.io/data-model/1.2/stixvocabs/threatactortypevocab-1.0/)` you want to describe and identify.
- **Confidence**: it flags the **estimated level of confidence** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605)` to assess the accuracy and trustworthiness of the entity information.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the threat actor.

- **Intent**: describes the threat actor's skill level, their motivations, the goals they intend to achieve, and the effects their actions may cause on the target.
- **Identity**: provides information that helps detect and identify the threat actor.

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Intent**: select this option to add details about the threat actor's level of expertise, their motivations, their intended goals, and any available planning or operation support they may need and use.
  - **Motivations**: from the drop-down menu select one or more options to define the threat actor's **motivation** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440621) to act against a victim.
  - **Sophistications**: from the drop-down menu select one or more options to define the threat actor's **level of expertise** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440631).
  - **Intended effects**: from the drop-down menu select one or more options to define the threat actor's **intended goals and the results** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440615) they may want to achieve.
  - **Planning and operational support**: from the drop-down menu select one or more options to define the **support functions** (https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440626) the threat actor may have access to and may need to plan and organize their actions.
- **✚ Characteristic > Identity**: select this option to add details about the individual, the organization, or the resources related to the threat actor's identity.

  The **Identity** editor is based on the **CIQ standard** (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq) and its **specifications** (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html). The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.
  - **Name**: specify the name of the threat actor. It should be descriptive and easy to remember.
    Example: *Spicy Panda*

Under **✚ Characteristic > Identity > Specification** you can define additional information relating and contributing to identify the threat actor such as credit and payment accounts, individuals, organizations, and email addresses.

- Click **✚ Fields**.
  From the drop-down menu select an option to add the threat actor-related details:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the threat actor.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*

- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ✪ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click ✚ **(Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.
- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

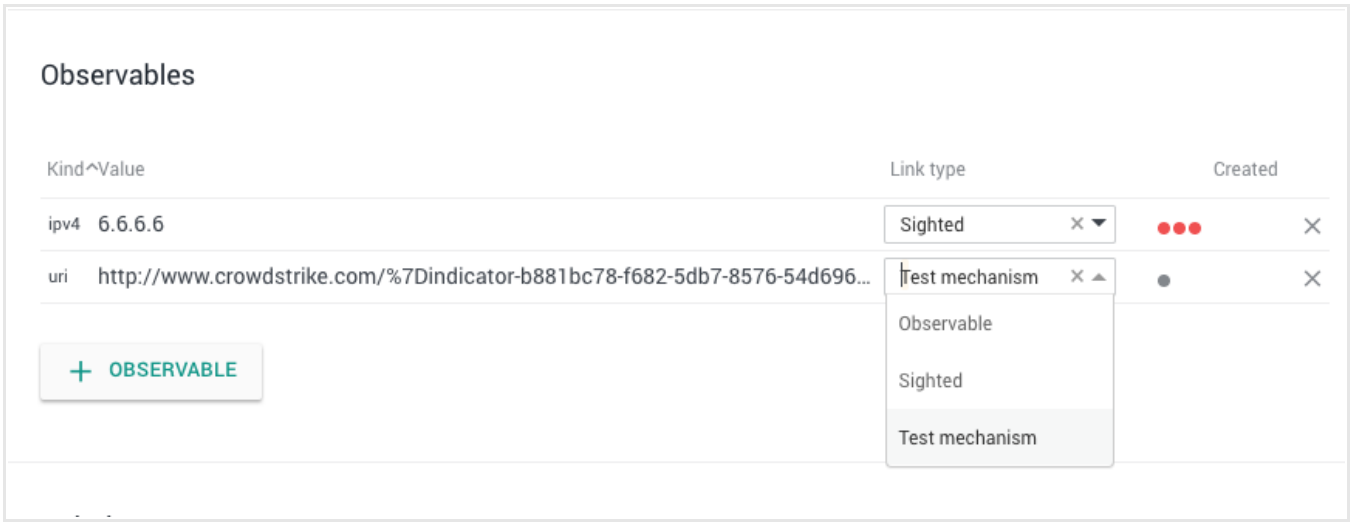
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the threat actor entity:

- N/A. Campaign-related observables do not have link types.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*

- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the threat actor to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the threat actor
Observed TTPs	Outgoing relationship — Relates the threat actor to the selected TTP(s) on the **Search an entity** dialog.
Associated campaigns	Outgoing relationship — Relates the threat actor to the selected campaign(s) on the **Search an entity** dialog.

Select this option…	… to create this relationship for the threat actor
Associated actors	Outgoing relationship — Relates the threat actor to the selected threat actor(s) on the **Search an entity** dialog.
Campaign → Attributions	Incoming relationship — Relates the selected campaign(s) on the **Search an entity** dialog to the threat actor.
Incident → Attributed threat actors	Incoming relationship — Relates the selected incident(s) on the **Search an entity** dialog to the threat actor.
Report → Threat actors	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the threat actor.
Sighting → Threat actor	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the threat actor.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field.
When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/threat actor — or outgoing — from the current origin threat actor/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.

- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the threat actor.
- **References**: enter a URL pointing to relevant reference information on the threat actor, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the threat actor to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Create a TTP

A TTP — Tactics, Techniques, and Procedures — describes a cyber adversary's behavior.

About TTPs

TTPs borrow their name and definition from military jargon:

- Tactics: *"the employment and ordered arrangement of forces in relation to each other."*
- Techniques: *"non-prescriptive ways or methods used to perform missions, functions, or tasks."*
- Procedures: *"standard, detailed steps that prescribe how to perform specific tasks."*

(Definitions from: *"Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (as amended through 15 February 2016)"*)

TTPs describe how an adversary behaves. The description of a cyber adversary's behavior should be as accurate as possible. For example, it should strive to include:

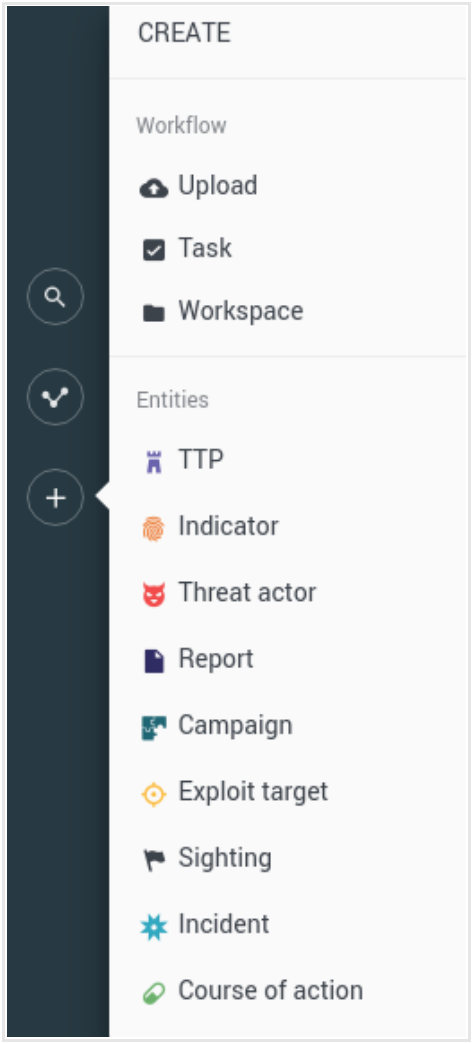
- The steps the adversary performs to achieve their goal.
- The equipment, gear, or tools they use. For example, software, hardware, USB sticks, forged ID badges, and so on.
- Information on any parties they associate with, or the victims they target, as well as on any exploit targets they may leverage to achieve their goals.
- How they act on, or react to the victim's behavior to avoid detection or defeat.
- The intended goals the adversary wants to achieve.

Create a TTP

✔ Input fields marked with an asterisk are required.

To create a TTP in the platform to describe the modus operandi of an adversary, do the following:

- On the left-hand navigation sidebar click **✚ > Ttp**.



The entity editor opens at **Create Ttp**, and you can start populating the input fields with content and details about the TTP you are creating.

Define the general options

- **Title**: assign the new TTP entity a clear and descriptive name.
  The name appears also on the entity detail pane header section.
- **Analysis**: it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
- **Confidence**: it flags the **estimated level of confidence** `(https://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440605)` to assess the accuracy and trustworthiness of the entity information.
- **Intended effects**: from the drop-down menu select one or more entries, as applicable, to describe what you reasonably assume to be the goal the threat actor implementing the TTP strives to achieve.
  Intended effects `(https://stixproject.github.io/data-model/1.2/stixvocabs/intendedeffectvocab-1.0/)` range from personal advantage, to theft, to fraud or extortion. They all aim at damaging the target victim or system.

Define the characteristics

Characteristics — This section holds structured, more detailed information about the TTP.

- **Behavior**: provides information on the practical procedures and processes the threat actor implements.
- **Resources**: provides information on the resources the threat actor uses, such as software or hardware equipments, as well as third-party associates.
- **Targeted victim**: provides information on the victim of the threat actor's actions.

Under **Characteristics** click **✚ Characteristic**, and then click an option from the drop-down menus to display additional fields in the editor where you can enter more details about the selected item.

- **✚ Characteristic > Behavior > Exploit** : select this option to add details about a vulnerability/weakness related to the TTP.
  - **Title**: assign a clear and descriptive name for the exploit. This is the vulnerable, weak spot the threat actor uses as an entry point.
    Example: *Open window*
  - **Description**: enter a short description to provide additional context or extra details.
    Example: *Open window on the ground floor, completely unlocked*
- **✚ Characteristic > Behavior > Malware** : select this option to add details about one or more pieces of malware related to the TTP.
  - **Name**: enter the common/standard name for the malware. Press **ENTER** to display additional fields to add more names.
    Example: *Mirai*
  - **Type**: from the drop-down menu select one or more entries, as applicable, to describe the purpose or the function of the malware.
    Example: *Bot — DDoS*
- **✚ Characteristic > Behavior > Attack pattern** : select this option to add details about an attack pattern related to the TTP.
  - **CAPEC**: enter the **CAPEC ID/CAPEC attack ID** `(https://capec.mitre.org/data/index.html)` corresponding to the attack pattern you want to describe here. (CAPEC: Common Attack Pattern Enumeration and Classification)

    Ingested data is processed and saved as **TTP entities** `(https://stixproject.github.io/data-model/1.2/ttp/ttptype/)`
    The STIX ID is based on the CAPEC ID — the default naming convention of a standard CAPEC-ingested TTP starts with the *[CAPEC-${numeric reference}]* prefix — and it is idempotent across uploads.

    Example: *CAPEC-108* or *108*
  - **Title**: enter the official CAPEC name for the attack pattern, as listed on their web site .
    Example: *Command Line Execution through SQL Injection*
  - **Description**: enter a short description to provide additional context or extra details.
    Example: *Remember to sanitize SQL inputs*

- ✚ **Characteristic > Resources > Infrastructure** : select this option to add details about the basic necessary equipment and services related to the TTP.
  - **Title**: enter the name of the service, product, tool, or piece of equipment.
    Example: *The really evil hacker forum of doom*
  - **Description**: enter a short description to provide additional context or extra details.
    Example: *Forum used to recruit hack-for-hire individuals and groups*
  - **Types**: from the drop-down menu select **one or more entries** `(https://stixproject.github.io/data-model/1.2/stixvocabs/attackerinfrastructuretypevocab-1.0/)`, as applicable, to describe the purpose or the function of the piece of infrastructure.
    Example: *Communications — Forum*
- ✚ **Characteristic > Resources > Persona** : select this item to add details about a party related to the TTP — it can be an individual, a group, an organization, a web site, a brand or product — that the threat actor uses as a decoy to impersonate other parties.
  - **Name**: enter the name of the individual, organization, service, product, and so on the threat actor uses as a persona.
    Example: *Dread Pirate Roberts*
- ✚ **Characteristic > Resources > Tools** : select this item to add details about more specific software or hardware tools related to the TTP.
  - **Name**: enter the name of the service, product, tool, or piece of equipment.
    Example: *Wireshark*
  - **Types**: from the drop-down menu select **one or more entries** `(https://stixproject.github.io/data-model/1.2/stixvocabs/attackerinfrastructuretypevocab-1.0/)`, as applicable, to describe the purpose or the function of the specific software or hardware tools.
    Example: *Traffic scanner*
  - **Description**: enter a short description to provide additional context or extra details.
    Example: *Network protocol analyzer*
  - **Hash type**: from the drop-down menu select the hash type whose value you are going to include.
    Example: *MD5*
  - **Simple hash value**: enter the hash value corresponding to the specified hash type.
    Hash type and hash value pairs represent indicators of compromise related to the tool(s) the threat actor uses as part of their TTP. Example: *1340c4d7de06930cba7f37245aefa988*
  - Click ✚ **More** to add new rows where you can input additional hashes.

- **✚ Characteristic > Targeted victim**: select this option to add details about the individual, the organization, or the resources related to the TTP that the threat actor is hitting or trying to hit.

  The **Targeted victim** editor is based on the **CIQ standard** (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq) and its **specifications** (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html).
  The Customer Information Quality specification aims at providing an open and standard data model to accurately and consistently describe a party such as an individual or an organization, as well as attributes like roles and relationships. There are no mandatory fields.

  - **Name**: specify the name of the targeted victim. It should be descriptive and easy to remember.
    Example: *IBAN ${ludicrously_fat_bank_account_number}*
  - **Targeted systems**: from the drop-down menu select **one or more entries** (https://stixproject.github.io/data-model/1.2/stixvocabs/systemtypevocab-1.0/), as applicable, to describe the type of infrastructure, system or equipment affected by the threat actor's TTP.
    Example: *Enterprise Systems — Database Layer*
  - **Targeted information**: from the drop-down menu select **one or more entries** (https://stixproject.github.io/data-model/1.2/stixvocabs/informationtypevocab-1.0/), as applicable, to describe the type of information being handles or manipulated in the TTP.
    Example: *Information Assets — Financial Data*

Under **✚ Characteristic > Targeted victim > Specification** you can define the type of victim under attack. You can describe affected individuals, organizations, and assets.

- Click **✚ Fields**.
  From the drop-down menu select an option to define the type of targeted victim:
  - **Account**
  - **Person**
  - **Organization**
  - **Electronic address**

Account

- **Account type**: defines the type of account related to the victim.
  Example: *bank*, *online*
- **Account status**: defines the current status of the account.
  Example: *active*, *blocked*
- **Account specification**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click **✚ Add** or **✚ More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Account ID	The account number. Example: *NL30INGB0123456789*
Issuing Authority	The financial institution that issues the account. Example: *ABC Bank*
Account Type	The type of account. Example: *debit* or *savings*
Account Branch	The local branch office or the retail location of the bank responsible for issuing the account. Example: *Utrecht center*

Key	Value
Issuing Country Name	The name of country where the account was issued. Example: *The Netherlands*

Person

- **Person name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click ✚ **Add** or ✚ **More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Preceding Title	Example: *His*, *Her*
Title	Example: *Rogueness*, *Excellence*, *Pandit*, *Sheikh*
First Name	Example: *Peter*
Middle Name	Example: *Brandon*
Last Name	Example: *Quill*
OtherName Name	Example: *Guardian of the Galaxy*
Alias Name	Example: *Star-Lord*
Generation Identifier	Example: *Jr.*, *Sr.*, *The Younger*, *The Elder*, *XXVIII*
Degree	Example: *BSc Ethical Hacking*

Organization

- **Organization name**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

  Click ✚ **Add** or ✚ **More** to insert a new empty row below the current one, which you can populate with additional details.

Key	Value
Name Only	The name the organization is commonly referred to. Example: *Wey-Yu*
Type Only	The entity definition of the organization. Example: *Inc*, *LLC*, *Ltd*
Full Name	The full name of the organization. Example: *Weyland-Yutani Corporation, Inc.*

Electronic address

- **Electronic address**: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.
  - The key corresponds to the service provider, for example Google, Yahoo, Skype, ICQ, and so on.
  - The associated value needs to be a valid format for the selected service provider, for example:
    - Google: *larry@gmail.com*
    - Yahoo: *melinda-ex@yahoo.com*
    - Skype: ${skype_username}*

Add observables

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ⊕ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click ✚ **(Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.

- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

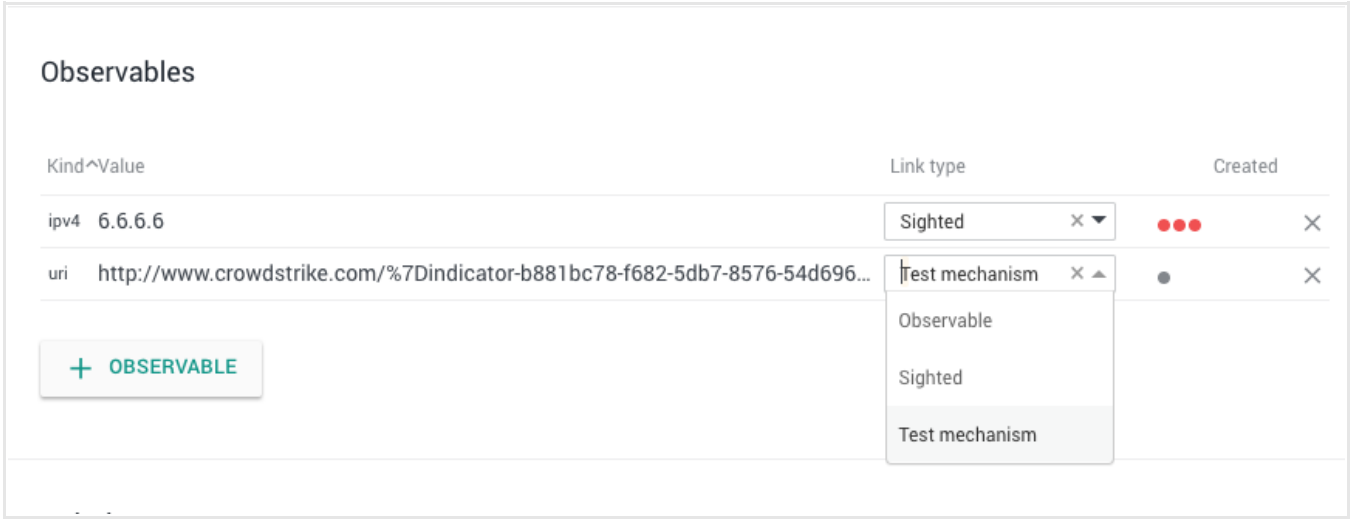
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



These are the supported entity-observable relationship link names for the TTP entity:

- **Malicious infrastructure**: describes a component of the infrastructure — gear, equipment, tools, software and hardware, services — used to carry out the malicious activities described in the TTP.
- **Targeted victim**: describes a component of the targeted victim's assets and resources.

After specifying the link name, you can move on to setting the observable value and its maliciousness confidence level:

- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*

- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > ✚ (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Add relationships

You can add relationships to associate the TTP to other entities:

- Under **Relationships** click **✚ Relationship**.
- From the drop-down menu select the option corresponding to the relationship you want to create.
- On the **Search an entity** dialog, click the checkbox(es) to select one or more entities to relate them to the current one.

> You can refine the displayed results by specifying a search string in the filter input field.
> Alternatively, click one of the available filter options to select and filter by specific:
>
> - **Entity types**
> - **Source**
> - **Date**
> - **Datasets**

- Click **Select**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Select this option…	… to create this relationship for the TTP
Exploit targets	Outgoing relationship — Relates the TTP to the selected exploit target(s) on the **Search an entity** dialog.
Related TTPs	Outgoing relationship — Relates the TTP to the selected TTP(s) on the **Search an entity** dialog.

Select this option…	… to create this relationship for the TTP
Campaign → Related TTPs	Incoming relationship — Relates the selected campaign(s) on the **Search an entity** dialog to the TTP.
Indicator → Indicated TTPs	Incoming relationship — Relates the selected indicator(s) on the **Search an entity** dialog to the TTP.
Incident → Leveraged TTPs	Incoming relationship — Relates the selected incident(s) on the **Search an entity** dialog to the TTP.
Report → TTPs	Incoming relationship — Relates the selected report(s) on the **Search an entity** dialog to the TTP.
Threat actor → Observed TTPs	Incoming relationship — Relates the selected threat actor(s) on the **Search an entity** dialog to the TTP
Sighting → TTP	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the TTP.

Under **Relationship type** you can choose an option from the drop-down menu to specify the type of entity relationship you established.
You can also enter custom definitions for the relationship by typing the desired relationship name in the empty input field.
When you assign a relationship a predefined or a custom name, it is visible in the graph view.
The predefined options are:

- **Indicates malware**
- **Is associated campaign to**
- **I don't know**
- **Could be anything**

The arrow orientation, either → or ←, indicates that the relationship is either incoming — from the related entity to the current one/TTP — or outgoing — from the current origin TTP/origin entity to the related one.

- To *remove* a relationship or a relationship type, click the ✖ icon on the row displaying the relationship or next to the relationship type you want to remove.
  The row and the corresponding relationship or the relationship type are removed.
  You cannot undo this action.

Add metadata information

- **Estimated observed time**: defines the point in time when the entity was first observed/detected.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat start time** : sets the estimated inception time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.
- **Estimated threat end time** : if the threat is no longer active, this field sets the estimated end time of the threat activity, based on observation, reports and other intelligence.
  If no start date is indicated, you can click the edit button for this field, select a start date, and save it.

- **Half life**: *Half life* is a numeric value representing the amount of time required to decrease the initial threat intelligence value of a malicious entity by 50%.
  In other words, it indicates how long it takes for a threat to cut its malicious potential by half.
  This value affects relevancy.
- **Tags**: select one or more tags to flag the entity with.
  Tags help you structure and categorize entities based on criteria like confidence and attack stage.
  Tags improve findability, and they represent quick reference pointers to place entities in a broader cyber threat context.
  You can select existing taxonomy tags from the drop-down list, as well as create tags on the fly by typing them in the input field.
  You can manage tags and their parent-child relationships under **Taxonomy**.
  To remove a tag from the input field, click the corresponding ✖ icon.
  To completely clear the **Tags** field, click the ✖ icon on the right-hand side of the field.
- **Source**: from the drop-down menu select the source of the threat information you are using to create the new entity.
  The available options are the names of the existing assigned user groups in the platform.
- **Source reliability**: from the drop-down menu select a value to assess how trustworthy and reliable the threat information data source is.

Add information source details

- **Description**: provide context and details to qualify the information source. For example, enter a job role, or the function of an institution.
- **Identity**: enter the name of the information source. For example, an individual's name or the official name of an entity such as an organization or government agency.
- **Roles**: from the drop-down menu select one or more options to define **how the information source contributed** `(http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part14-vocabularies/stix-v1.2.1-csprd01-part14-vocabularies.html#_toc440440613)` to the information in the TTP.
- **References**: enter a URL pointing to relevant reference information on the TTP, if available.
  - The field takes only URLs as input. Enter one URL per field.
    To confirm the current input and to display a new input field, press **ENTER**.
  - To remove an input field from this section, click the corresponding ✖ icon.

Define sharing and usage

- **TLP**: the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- **Terms of use**: enter any legal notes about fair use of the information about the entity.

Define a workflow

- **Add to dataset**: select this checkbox to include the TTP to one or more existing datasets.
  From the drop-down menu select the target datasets you want to add the entity to.
- **Manually enrich**: select this checkbox to manually enrich the entity with the enricher sources you select from the drop-down menu.

Save and publish

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Draft and published entities

Draft entities work like notepads or clipbooks: they hold your work in progress information, and they do not interact with other platform objects. Published entities are first-class platform citizens you can analyze, manipulate, and relate to other platform objects.

Draft entities

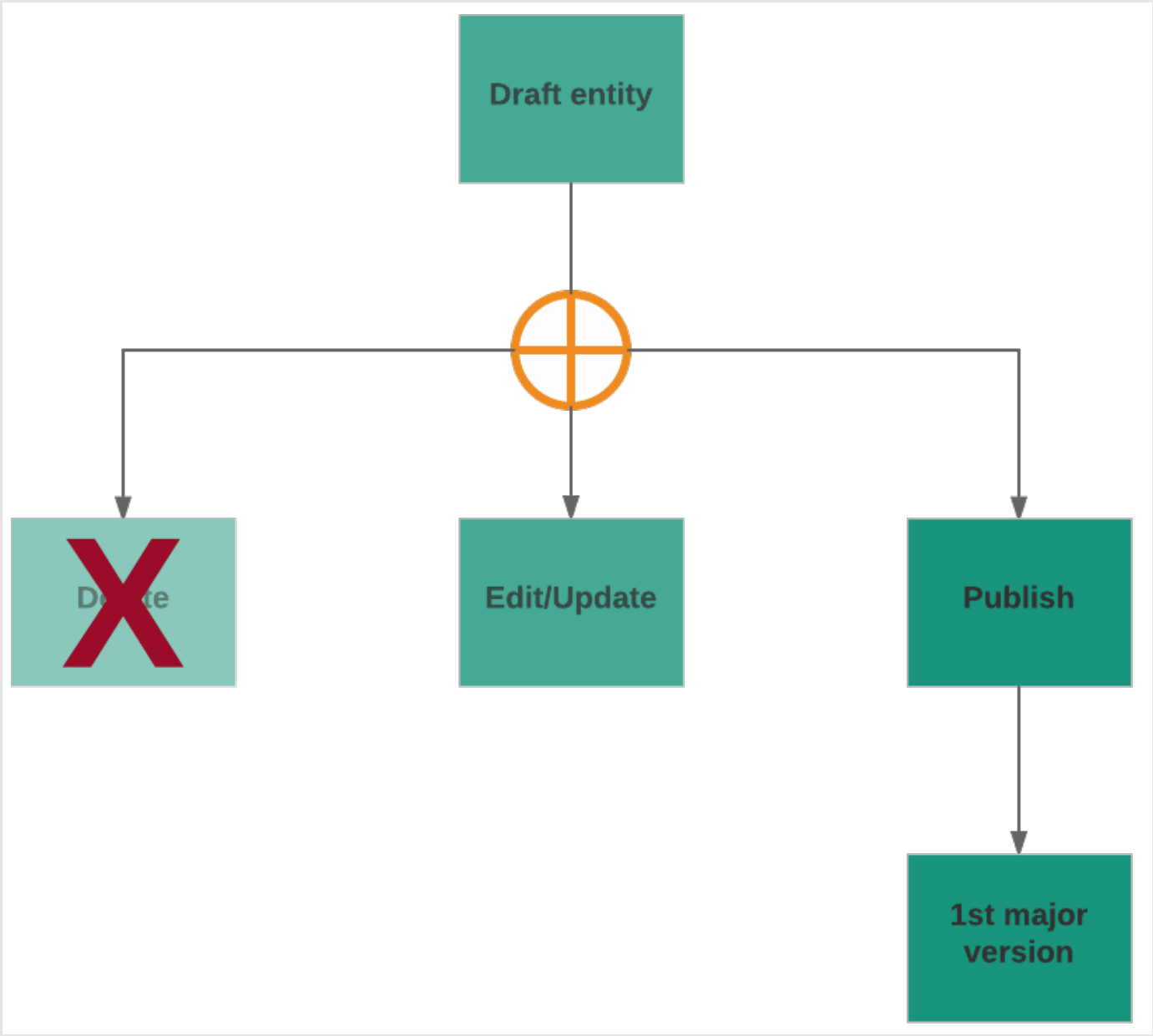
You can save entities as drafts only during the new entity creation step. After saving an entity for the first time you can update an existing draft, publish a draft, or update a published entity.

A draft entity is a not yet finalized work in progress:

- The platform does not index draft entities. Therefore:
  - You cannot search for draft entities.
  - You cannot add draft entities to datasets.
  - You cannot add draft entities to workspaces.
  - You cannot display draft entities on the graph.
- You can edit, update, download, and delete draft entities at any time without affecting other entities or existing relationships.

Draft entities are not versioned.
It is not possible to create multiple drafts of the same entity. This check avoids unnecessary data duplication. At any given time, there is only one draft version of an entity in the platform, which users can edit and update as often as needed.

The basic draft entity workflow allows deleting, editing, and publishing:



Published entities

When you publish and entity to the platform, upon publishing the system creates the first major version of the newly published entity. Subsequent save actions following editing or updating the entity generate minor bumped versions. You can review published entity versions in the entity history.

A published entity is a finalized item:

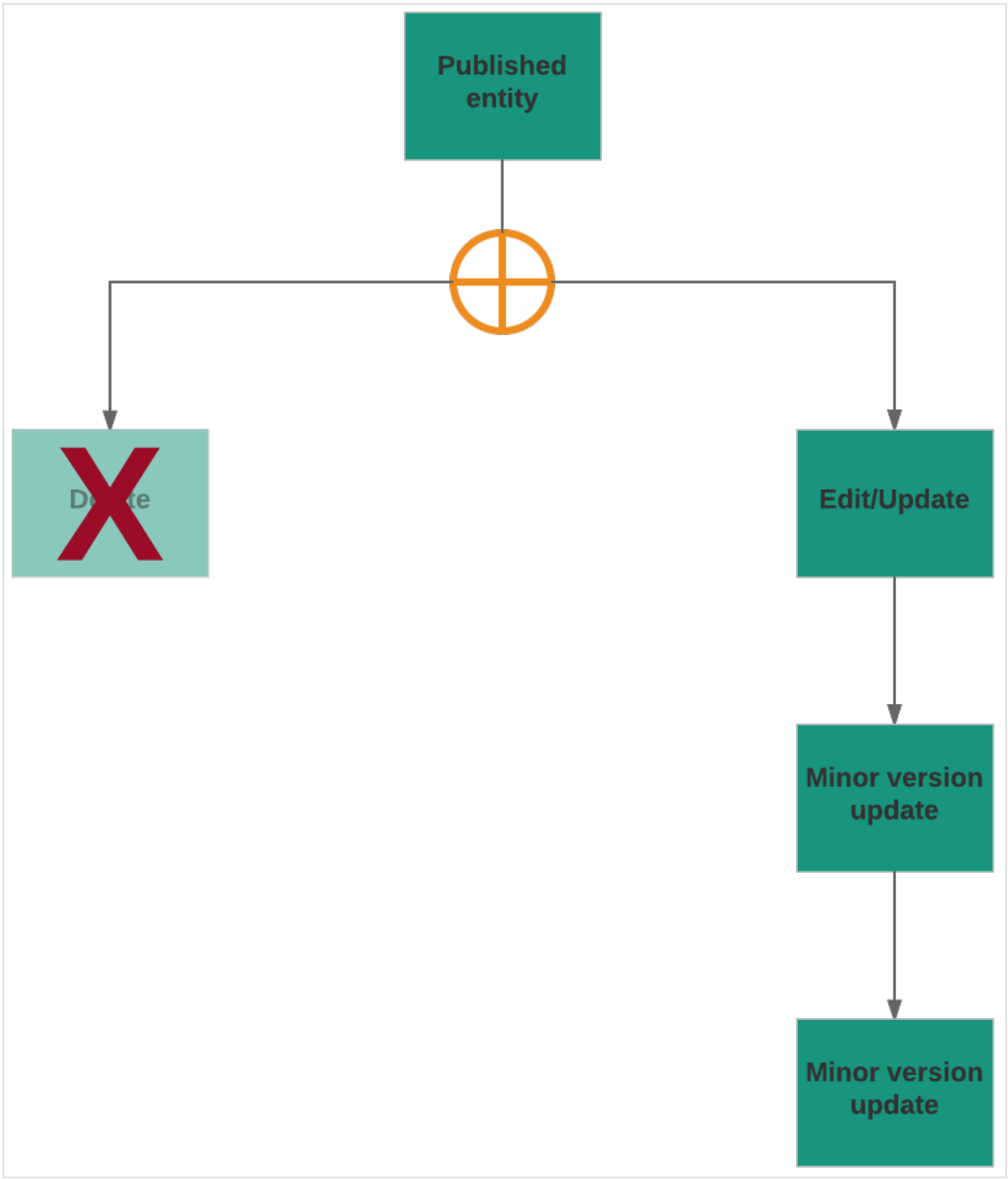
- The platform indexes published entities. Therefore:
  - You can search for published entities.
  - You can add published entities to datasets.
  - You can add published entities to workspaces.
  - You can display published entities on the graph.

- Published entities can have relationships. Therefore:
  - You can edit, update, and download published entities at any time. *However*:
  - You *cannot* revert a published entity back to draft.
  - You can delete a published entity only if it has *no existing relationships* with any other objects in the platform. If you try to delete a published entity with relationships, the action fails and an error message is displayed.

Deleting an entity fails in the following cases:

- The entity is available only as draft, that is, it has not been published yet.
  To delete it, you first need to publish it.
- The entity is included in one or more datasets.
  To delete it, you first need to remove it from the datasets it belongs to.
- The entity is included in one or more *public* workspaces.
  To delete it, you first need to remove it from the workspaces it belongs to.
- There are open or pending user tasks referring to the entity.
  To delete it, you first need to either complete and close, or delete the tasks that refer to the entity.
- Another user copied the entity, and the entity data is currently stored in the user's clipboard.
  To delete it, the copied entity data first needs to be removed from the user's clipboard.

The basic published entity workflow allows deleting and editing:



Save options

When you create a new entity in the editor, you can choose whether you want to save it as a draft, or if you want to publish it.

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.
- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Edit entities

Edit entities to update information on the fly or to add more context. Saving edits produces a new version of the entity.

About editing

You can open the entity editor to modify or update entity information from almost anywhere in the platform with a couple of clicks.
For quick edits on the fly, you can bypass the editor and apply inline edits directly on the entity detail pane.

You can edit acquired intelligence to update information, so that it remains accurate and reliable over time. At the same time, you want to keep the original intelligence as it was ingested. Versioning takes care of that.

When you edit an entity and save the changes, the platform creates a new version of the entity with the changes, and it archives the previous version without the changes. The new version receives a new ID value, it is published, and it becomes the current version of the entity. The previous version is not editable, not searchable, but it remains available for reference. To view a list with all existing versions of an entity, open the entity detail pane, and then click the **Version** tab.

Obsolete entity versions are flagged as ❗ **outdated**. You can click an entity version name to view the corresponding details, export it as JSON or STIX, add it to a dataset, or delete it. Other actions are disabled.

Edit entities in Browse

- On the top navigation bar click **Browse**. All the available entities are displayed
- You can choose to filter the display using the below options:
  - **Entity**: Select one more entity types you want to see.
  - **Source**: This lists the source the entity is derived from. Select one more sources to filter the display.
  - **TLP**: Filter based on the Traffic Light Protocol.
  - **Date**: Filter using a date range for entity creation.
  - **Dataset**: Filter using a dataset.

Edit from the context menu

- On the active view, browse to the entity you want to edit.
- Click the ⋮ icon on the row corresponding to the specified entity.
- From the drop-down menu select **Edit**.

The entity editor opens, and you can start editing the entity content in the form fields as needed.

Edit from the Actions menu

- On the active view, browse to the entity you want to edit.
- Click anywhere on the row corresponding to the entity you want to edit.
  The entity detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Edit**.

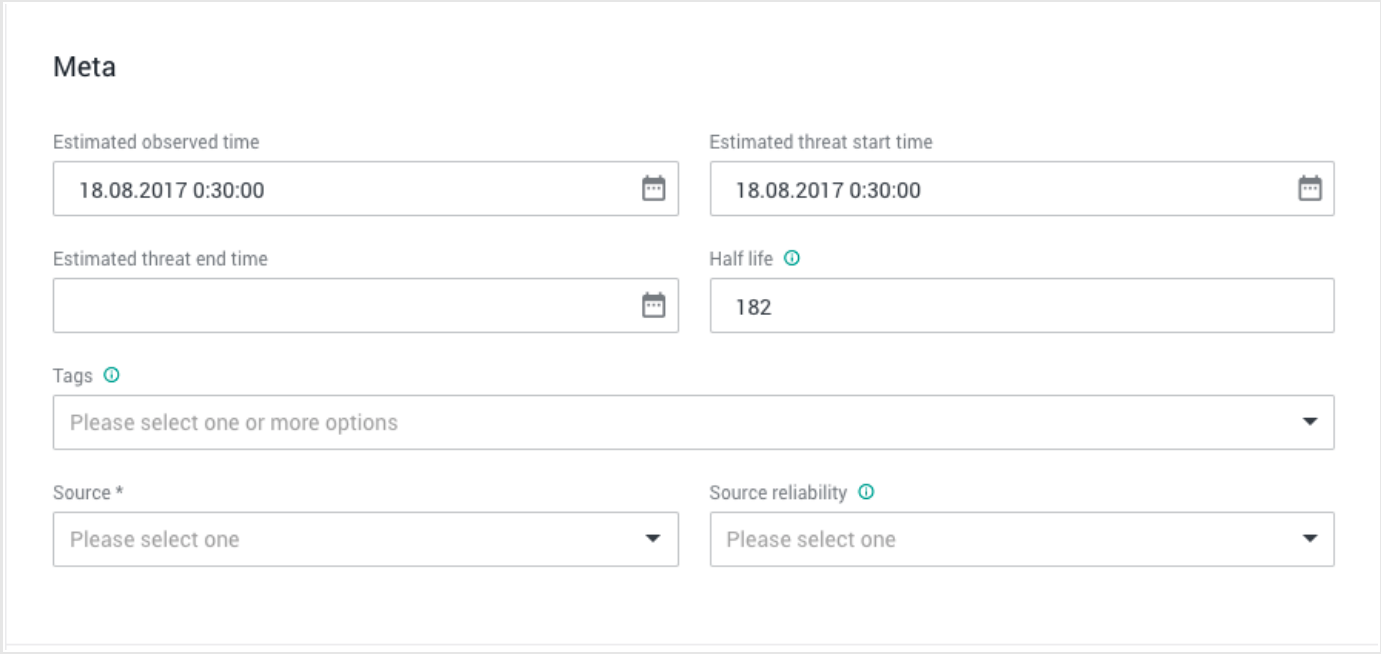
The entity editor opens, and you can start editing the entity content in the form fields as needed.

Edit entities on the detail pane

- On the active view, browse to the entity you want to edit.
- Click anywhere on the row corresponding to the entity you want to edit.
  The entity detail pane slides in from the side of the screen.

The detail pane includes a quick edit feature that enables you to apply inline edits on the fly: a ✎ pencil icon indicates the editable fields.

- Click the ✎ pencil icon corresponding to the field you want to edit, and apply the changes.
- Press **ENTER** or exit the field to save the updated content.



The TLP override button at the top right of detail pane creates a new version of the entity if changed.

Edit entities in Discovery

- On the top navigation bar click **Discovery**. All the available entities are displayed.
- You can choose to filter the display using the below options:
  - **Entity**: Select one more entity types you want to see.
  - **Source**: This lists the source the entity is derived from. Select one more sources to filter the display.
  - **TLP**: Filter based on the Traffic Light Protocol.
  - **Date**: Filter using a date range for entity creation.
  - **Reliability**: Filter the entities by reliability. This is set while creating the entity based on how reliable the source is.
  - **Discovery rules**: If you have set any discovery rules, you can filter the entities using the Discovery filter.
  - **Dataset**: Filter using a dataset.
- On the active view, browse to the entity you want to edit, and click it.
- You can then proceed to edit the entity in one of the following ways:
  - Open the entity detail pane and select **Actions > Edit**, or
  - Apply inline edits on the fly on the entity detail pane.

Edit entities in Exposure

- On the top navigation bar click **Exposure** to display the exposed entity list.All the available entities are displayed.
- You can choose to filter the display using the below options:
  - **Entity**: Select one more entity types you want to see.
  - **Date**: Filter using a date range for entity creation.
  - **Dataset**: Filter using a dataset.
- On the active view, browse to the entity you want to edit.
- You can then proceed to edit the entity in one of the following ways:
  - Select the corresponding option in the context menu, or
  - Open the entity detail pane and select **Actions > Edit**, or
  - Apply inline edits on the fly on the entity detail pane.

Edit entities in a workspace

- On the top navigation bar click **Workspaces**.
- On the available workspace view, click the desired workspace to open it.
- In the Entities section, click the entity you want to edit. A detail pane with the entity details is displayed.

- You can then proceed to edit the entity in one of the following ways:
  - Select the corresponding option in the context menu, or
  - Open the entity detail pane and select **Actions > Edit**, or
  - Apply inline edits on the fly on the entity detail pane.
- If you are working on a graph, double-click the entity you want to edit and:
  - On the entity detail pane click Actions > Edit, or
  - Apply inline edits on the fly on the entity detail pane.

Edit entities on the graph

- On the graph double-click the entity you want to edit.
- You can then proceed to edit the entity in one of the following ways:
  - On the entity detail pane click **Actions > Edit**, or
  - Apply inline edits on the fly on the entity detail pane.

Edit entities in an incoming feed

- On the top navigation bar click **Data configuration**.
- On the left-hand navigation sidebar click **Incoming feeds** to display the incoming feed list.
- Click anywhere on the row corresponding to the incoming feed containing the entity you want to edit. The feed detail pane slides in from the side of the screen.
- Open the entity detail pane and select Actions > Edit, or
- On the feed detail pane click the Entities tab.
- On the active view, browse to the entity you want to edit, and click it.
- Apply inline edits on the fly on the entity detail pane.

Edit entities in a dataset

- On the top navigation bar click **Data configuration**.
- Go to **Browse > Datasets** to display the available dataset list.
- Click anywhere on the row corresponding to the dataset containing the entity you want to edit.

- You can then proceed to edit the entity in one of the following ways:
  - Select the corresponding option in the context menu, or
  - Open the entity detail pane and select **Actions > Edit**, or
  - Apply inline edits on the fly on the entity detail pane.

Edit uploaded entities

- On the top navigation bar click **Data configuration**.
- Go to **Browse -> Uploads** to display the available dataset list and scroll down to **Current uploads**.

You can edit only entities that are part of successfully uploaded files whose upload status is **Success**.

- Click the ⋮ icon on the row corresponding to the uploaded file originally containing the entity you want to edit.
- From the context menu select **View**.
  The page displays a list with the entities ingested through the uploaded file.
- On the active view, browse to the entity you want to edit.
- You can then proceed to edit the entity in one of the following ways:
  - Select the corresponding option in the context menu, or
  - Open the entity detail pane and select **Actions > Edit**, or
  - Apply inline edits on the fly on the entity detail pane.

Save options

Click **Save draft** to store your changes without publishing the entity, **Publish** to release the new version of the entity including your changes, or **Cancel** to discard the changes.

- Click **Save draft** to store your changes, or **Cancel** to discard them.
  The new entry is saved as a draft, but it is not published, i.e. it is inactive. It is available in the entity editor under **Draft entities**.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Save draft and new** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a new draft form in the editor.
- Alternatively, click the drop-down arrow and select **Save draft and duplicate** to:
  - Save the current populated form as a draft without publishing it to the platform;
  - Create and open a pre-populated copy of the draft entity in the editor to speed up the creation of a new entity of the same type.

- Click **Publish** to store your changes, or **Cancel** to discard them.
  The new entry is saved and published to the platform. As soon as it is indexed, it is available in the platform in the entity editor under **Published**.
  Published entities associated with a workspace or included in a dataset are available also through the corresponding workspace and dataset.
- If you are creating a new entity and you have not yet saved it for the first time, you can also click the drop-down arrow and select **Publish and new** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a new form in the editor.
- Alternatively, click the drop-down arrow and select **Publish and duplicate** to:
  - Save the current populated form and publish it to the platform;
  - Create and open a pre-populated copy of the newly published entity in the editor to speed up the creation of a new entity of the same type.

Merge entities

Merge almost identical entities into a master entity and rewire relationships to reduce data noise.

About merging

When the platform ingests data, it performs operations such as deduplication and idref resolution. This process consolidates and normalizes data, and it efficiently reduces unnecessary data.

However, some entities — typically, TTPs — can exist as multiple, distinct entities even if they share identical titles, descriptions, and types. They are identified and ingested as separate entities because they have different STIX IDs and timestamps. This can occur, for example, when the source feed data is not well formed.

Apart from STIX ID and timestamp, these entities hold identical information. Therefore, it may be a good idea to consolidate them to reduce data noise and unwanted redundancy. EclecticIQ Platform enables you to merge similar entities into a master entity to achieve a unified and consistent view of the data.

About entity merging

> **Warning:** Use entity merging with caution: it is not possible to undo a merge action.
> All merged entities disappear: they are not indexed, and therefore they are not searchable.
> However, they persist in the main data storage (PostgreSQL): you can still run a SQL query in PostgreSQL to search for them.

In this context, *similar entities* have the following characteristics:

- Identical content as for title, description, and other STIX data fields
- Different STIX ID
- Different timestamp.

From a point of view of information relevance and intelligence value, you can handle these entities like duplicates, and you can decide to merge similar entities into a master entity. You can manually create a new entity, as well as use an existing one as the master entity to merge similar entities into.

To control the merging process, you define a merge entity rule with a set of criteria and a merge action. Rules apply to new and to historical, that is, pre-existing, entities. Therefore, a merge rule merges new and historical entities into the selected master entity, based on the specified criteria.

When merging similar entities into a master entity, the merge rule handles similar/duplicate entities as follows:

- New similar entities, that is, processed but not yet saved to the database, are ignored because they are duplicates. Any incoming or outgoing relationships they may have are automatically rewired, so that they refer to the master entity.
- Historical, pre-existing similar entities are removed because they are duplicates.
  Any incoming or outgoing relationships they may have are automatically rewired, so that they refer to the master entity.
  Any existing workflow items merged historical entities may have — for example, workspaces or tasks — are also automatically rewired in the same way.

Merged entities are not deleted from the database, since the platform uses them for idref resolution. However, they are not indexed, and therefore not searchable in the platform.

You can still search for these entities by running SQL queries in PostgreSQL.

A successful merge action produces also an audit entry recording the main details of the operation.

Create a merge rule

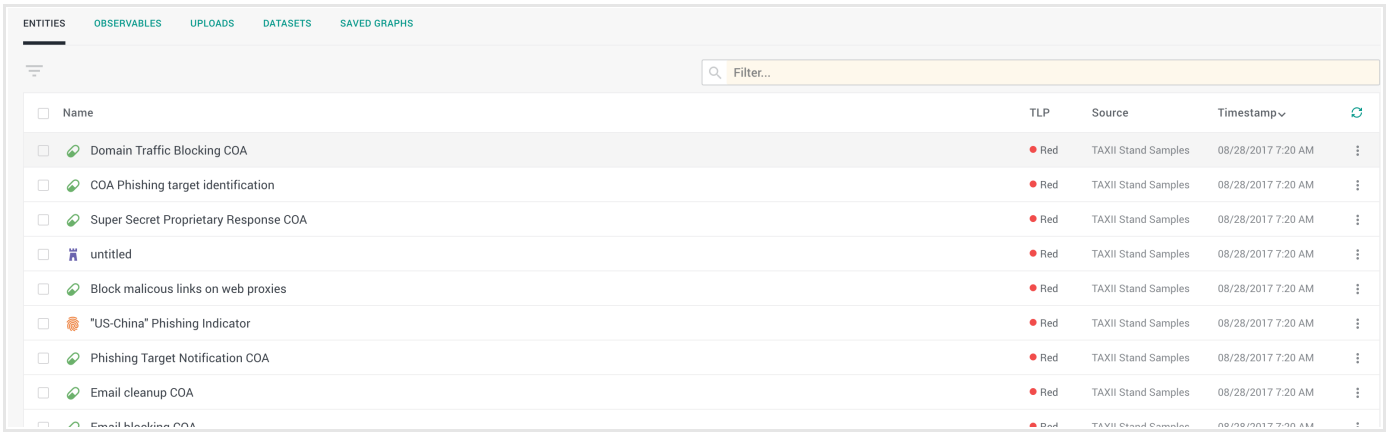
✔ Input fields marked with an asterisk are required.

To merge similar entities into a master entity, you define an entity merge rule.
To create a new entity merge rule, do the following:

- On the top navigation bar click **Data configuration > Rules > Entity**
- On the **Rules > Entity > Create** page, define the new rule criteria to automatically merge similar entities into a master entity:
- **Rule name**: enter a name to identify the rule. It should be descriptive and easy to remember.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.

Select the rule action

- **Actions**: from the drop-down menu select **Merge similar**.
- Under **Merge similar > Master entity**, click **+ add** to select the master entity where all similar entities should be merged to.
  On the pop-up search dialog, you can look for the desired master entity in several ways:
  - Click an entity from the list to select it as the master entity.
  - Enter search terms, quick filters or JSON paths in the search bar.
  - Apply filters to look for specific entity types; or entities from specific incoming feeds, enrichers, or datasets; or entities ingested within a given time range.
- To confirm your master entity selection, click **Select**.



Select the rule criteria

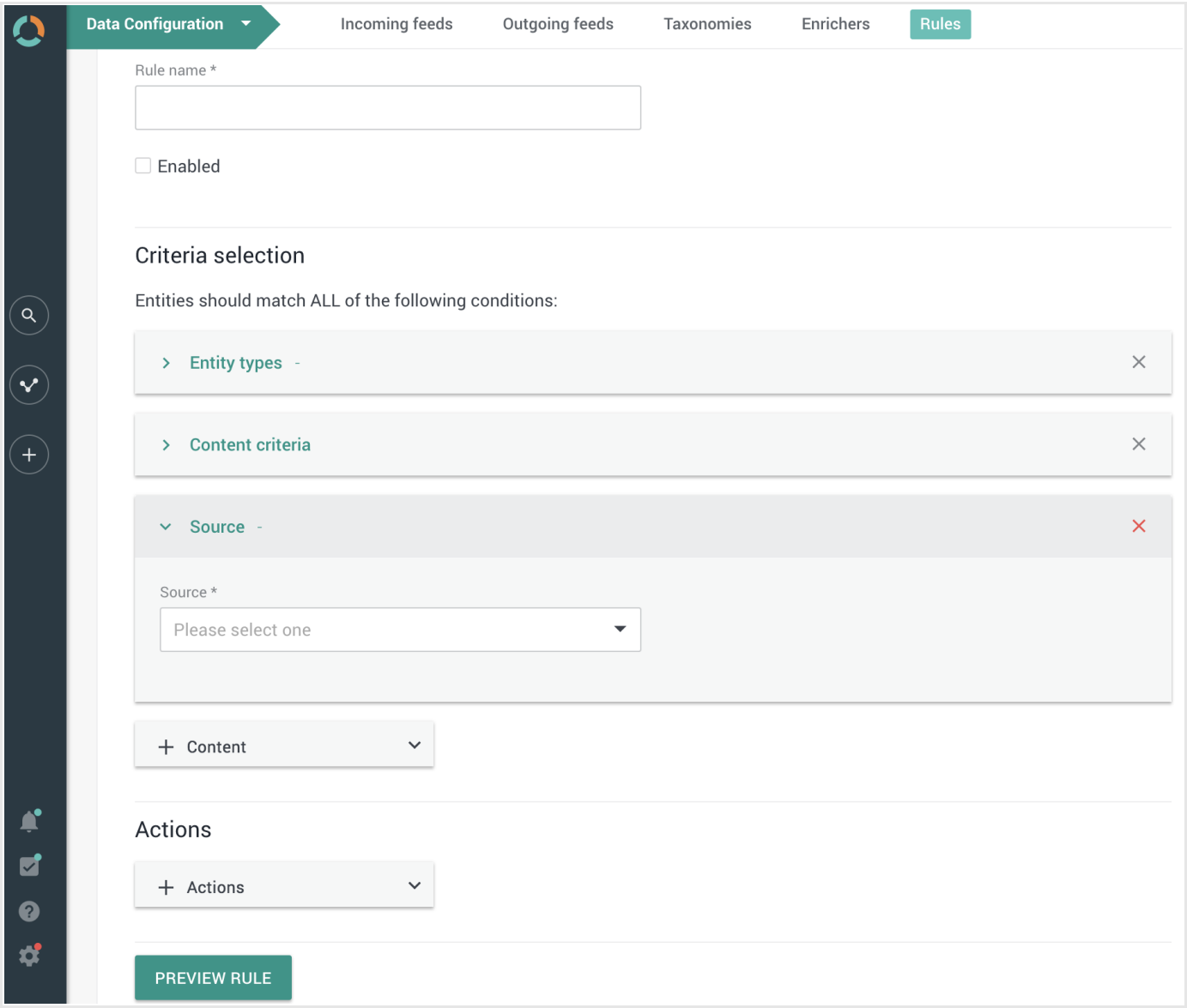
In this section you set the scope of the merge rule and the logical criteria of applicability of the merge rule.
You can define one or more conditions to target specific entity types, content inside entities, data sources, and TLP colors.

- A condition matches if *any* of the defined criteria match. Conditions allowing multiple criteria concatenate them with Boolean `OR`.
- A rule matches if *all* the defined conditions match. A rule using multiple conditions concatenates them with Boolean `AND`.

A valid rule needs to include a name, an action, and at least one condition, which you can select and configure under **Criteria selection**.
Click ✚ **Condition** to define one or more conditions:

- **Entity types**: from the drop-down menu select one or more entity types to apply the rule to.
  The rule applies the same action to all selected entity types.

To remove a selection from the input field, click the ✖ icon corresponding to the item(s) you want to remove.



- **Content criteria**: key/value pairs define the content criteria the rule should apply.
  The input format for the *key* field is a *JSON* path. It points to an entity field/entity location in the entity structure.
  The input format for the *value* field is a *regex*. It specifies the content pattern.
  By default, **Content criteria** JSON path expressions are relative to the `data` field, which is the root of the JSON path expression.
  The `data` root is implied. To point to the title or to the description fields of an entity, you only need to specify `title` or `description`, instead of `data.title` or `data.description`.
- **Content > Path**: from the drop-down menu select an option to define which field in the entity data structure you want to search for values in.

  The available options represent and map to corresponding JSON paths in the JSON data structure representing entities in the platform.
  The JSON path root is the top-level `data` field, and it is implicit in the JSON paths the menu options map to.

  Path defines the place in the entity data structure where you want to look for a specific data value that you want to exclude from publishing. This option works together with a specified regex to set the data pattern the rule should use to retrieve the desired matching value in the field defined in **Path**.

Path option	JSON path	Entity type
Information source, Identity	`information_source.identity`	All

Path option	JSON path	Entity type
Information source, References	`information_source.references[]`	All
Title	`title`	All
Affected assets, Properties affected	`affected_assets[].nature_of_security_effect_properties_affected`	Incident
Observables	`observable`	Indicator
Sightings	`sightings`	Indicator
Raw events	`raw_events`	Sightings
Security control, Identity	`security_control.identity`	Sightings
Security control, References	`security_control.references[]`	Sightings
Resources, Infrastructure	`resources.infrastructure`	TTP
Resources, Persona	`resources.persona`	TTP

To examine the JSON data structure of an entity:

- Go the entity detail pane, and then click the **JSON** tab.

Alternatively:

- On the selected entity detail pane, click **Actions > Export > JSON** to save the entity in JSON format.

- **Content > Value**: define one or more literals, where supported, or regexes to specify the data pattern(s) the rule should apply to search for the desired data values.
  If you specify multiple values, enter one value per line.
  Wildcards are currently not supported.

  The rule uses the literal value(s) or the regex pattern(s) defined here to look for matching values in the field(s) selected in **Paths**.

  This field supports only **Elasticsearch regular expression syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#regexp-syntax)`.
  The main peculiarities of the Elasticsearch query regex syntax are:

  - Anchors (`^` and `$`) are implied at the beginning and at the end of the regex. You do not need to include them in the regex you input.
  - If you insert explicit anchor characters in the **Value** field, they are interpreted as literal values.
  - You need to escape special characters (`.` `?` `+` `*` `|` `{` `}` `[` `]` `(` `)` `"` `\`).
    To escape a special character, prepend a backslash `\` to it. Example: `\{ \}`

✔ At this moment, Elasticsearch regular expression syntax **optional operators** (https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-regexp-query.html#_optional_operators) are not supported.

- Click **+ Add** or **+ More** to add new rows as needed, where you can enter additional criteria.
- **Source**: from the drop-down menu select an incoming feed or an enricher to use as a data source for the rule.
- **TLPs**: the TLP color code you want to use to filter data.
  TLP (https://www.us-cert.gov/tlp) provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

Besides committing the current data by clicking **Save**, you can also click the downward-pointing arrow on the **Save** button to display a context menu with additional save options:

- **Save and new**: saves the current data for the active item, and it allows you to start creating a new item of the same type right away. For example, a dataset, a feed, a rule, a workspace, or a task.
- **Save and duplicate**: saves the current data for the active item, and it creates a pre-populated copy of the same item, which you can use as a template to speed up manual work.

✔ Merge rules are a specific type of entity rule, but you can edit, delete, and filter them in the same way as other rules.

Delete entities

Manually delete redundant or unnecessary entities to limit unwanted data noise.

Warning:
You can delete a published entity only if it has *no existing relationships* with any other objects in the platform. If you try to delete a published entity with relationships, the action fails and an error message is displayed.

Deleting an entity fails in the following cases:

- The entity is available only as draft, that is, it has not been published yet.
  To delete it, you first need to publish it.
- The entity is included in one or more datasets.
  To delete it, you first need to remove it from the datasets it belongs to.
- The entity is included in one or more *public* workspaces.
  To delete it, you first need to remove it from the workspaces it belongs to.
- There are open or pending user tasks referring to the entity.
  To delete it, you first need to either complete and close, or delete the tasks that refer to the entity.
- Another user copied the entity, and the entity data is currently stored in the user's clipboard.
  To delete it, the copied entity data first needs to be removed from the user's clipboard.

You can manually delete an entity from almost anywhere in the platform.
To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse**, **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.

Delete a single entity

- On the active view, browse to the entity you want to delete.
- Click the ⋮ icon corresponding to the entity you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation dialog, click **Delete** to confirm the action.
- If the entity is in draft status or if it is a published entity without any relationships to other objects in the platform, the entity is successfully deleted.

Alternatively:

- On the active view, browse to the entity you want to delete.
- Click anywhere on the row corresponding to the entity you want to delete.
  The entity detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Delete**.

- On the confirmation dialog, click **Delete** to confirm the action.
- If the entity is in draft status or if it is a published entity without any relationships to other objects in the platform, the entity is successfully deleted.

Delete multiple entities

- On the active view, select the checkboxes corresponding to the entities you want to delete in bulk.
- Click the ⋮ icon on the top-right-corner of the table view, above the table header row.
- From the drop-down menu select **Delete**.
- On the confirmation dialog, click **Delete** to confirm the action.
- If *all* entities are in draft status or if they are *all* published entities without any relationships to other objects in the platform, they are successfully deleted.

Entity versions

If you delete an entity the previous versions of that entity are automatically removed from the platform. The platform does not allow you delete previous versions manually.

Export entities

Manually export entities to JSON or STIX for further analysis.

Export an entity

You can manually export an entity from almost anywhere in the platform.
To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.

- On the active view, browse to the entity you want to export.
- Click the ⋮ icon corresponding to the entity you want to export.
- From the drop-down menu select **Export**.
- Select the export format: either **JSON** or **STIX**.
- On the popup dialog, browse to the desired location you want to save the file to, and then confirm the action.
- The entity is exported and saved as a file in the specified format.

Alternatively:

- On the active view, browse to the entity you want to export.
- Click anywhere on the row corresponding to the entity you want to export.
  The entity detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Export**.
- Select the export format: either **JSON** or **STIX**.
- On the popup dialog, browse to the desired location you want to save the file to, and then confirm the action.
- The entity is exported and saved as a file in the specified format.

Download entities

Download entities in their original data format for further analysis.

Download an entity

You can manually download an entity from almost anywhere in the platform.
To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.

- On the active view, browse to the entity you want to download.
- Click the ⋮ icon corresponding to the entity you want to download.
- From the drop-down menu select **Download original**.
- On the popup dialog, browse to the desired location you want to save the file to, and then confirm the action.
- The entity is downloaded in its original data format to the specified location.

Alternatively:

- On the active view, browse to the entity you want to download.
- Click anywhere on the row corresponding to the entity you want to download.
  The entity detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Download original**.
- On the popup dialog, browse to the desired location you want to save the file to, and then confirm the action.
- The entity is downloaded in its original data format to the specified location.

Manually upload

Manually upload files and archives to the platform.

You can upload data files and compressed archives on the fly. The platform ingests and processes uploaded data, and it creates new entities after deduplicating and normalizing it.

About content

Structured content

For example: STIX, JSON, CSV
Machine-readable, easy to analyze, parse, and ingest as structured entities and observables.

Unstructured content

For example: PDF, email, (unstructured) text
Human-readable, more difficult to analyze, parse, and ingest as structured entities and observables.

When the platform ingests unstructured content — either through an incoming feed or a manual file upload — to produce a report entity, the original unstructured source is attached in its original format to the resulting report entity. In this way, when analysts modify or update the the resulting report entity, they can always refer back to the original information.

Content types

You can upload files in the following formats:

Content type	Description
Anubis Cyberfeed JSON	JSON format representing entity data as JSON objects.
ArcSight CEF	The Common Event Format is a text-based standard for log records proposed by ArcSight. It allows sharing, consuming, and parsing event information across devices such as SIEM platforms and Syslog servers.
Cisco Threat Grid Samples JSON	JSON format representing entity data as JSON objects.
EclecticIQ Entities CSV	Comma separated CSV format for tabular data representation of entities.
EclecticIQ Observables CSV	Comma separated CSV format for tabular data representation of observables.
EclecticIQ HTML Report	Default HTML format to publish EclecticIQ intel reports.
EclecticIQ HTML Report Digest	Default HTML format to publish EclecticIQ intel report digests.
EclecticIQ JSON	JSON format representing entity data as JSON objects.

Content type	Description
Intel 471	Intel 471 reports. Bundled observables are linked to the parent report entity. API endpoint: *https://api.intel471.com/v1/reports/{}*
PDF	Standard PDF format, preferably native (not scanned).
STIX 1.0	STIX data model **v. 1.0** `(http://stixproject.github.io/data-model/1.0/)`.
STIX 1.1	STIX data model **v. 1.1** `(http://stixproject.github.io/data-model/1.1/)`.
STIX 1.1.1	STIX data model **v. 1.1.1** `(http://stixproject.github.io/data-model/1.1.1/)`.
STIX 1.2	STIX data model **v. 1.2** `(http://stixproject.github.io/data-model/1.2/)`.
Text/Plain text value	Plain text format. This content type allows you to enter free text and literals, wildcards (where supported), as well as JSON paths to point to specific entity property fields, and regex patterns to filter data.
Threat Recon	Threat Recon JSON output returned by the **Threat Recon API** `(https://threatrecon.co/api)`. Threat Recon focuses on providiung information about indicators.
STIX 1.1.1	FireEye iSIGHT Intelligence Report API outputs reports in STIX 1.1.1 format. Reports concern threat topics such as vulnerabilities, malware, threat actors, stategies, tactics, and techniques.
BFK Threat Intelligence JSON	BFK reports and NIDs (Network Intrusion Detections) are saved as JSON report entities; they concern threat topics such as threat actors, targeted victims, tactics, and techniques.
Crowdstrike indicator JSON	Indicators retrieved from the Falcon Intelligence platform such as compromised devices, malicious domains, hashes, and so on starting from the specified polling date.
CAPEC XML	Categorizied and enumerated attack patterns, attack mechanisms, strategies, tactics and techniques retrieved from the **CAPEC** `(https://capec.mitre.org/about/index.html)` catalog.
Crowdstrike report JSON	Reports retrieved from the Falcon Intelligence platform in JSON format and as PDF attachments.
Crowdstrike actor JSON	Threat actor entities, related TTPs, indicators, and campaigns, as well as related observables to represent actor ID, target country, target industry, and targeted victim(s).
CVE Search JSON	Exploit target entities retrieved from **CIRCL CVE Search** `(https://www.circl.lu/services/cve-search/)`. The entity ID is derived from the **CVE ID** `(https://cve.circl.lu/)`. API endpoint: *https://cve.circl.lu/api/last*.
Intel 471 IOC Feed	Indicators of compromise such as IP addresses, malicious URLs, and MD5 and SHA-256 hashes. Intel 471 focuses on providing first-hand information related to threat actors and groups. API endpoint: *https://api.intel471.com/v1/search/{}*.
OpenPhish Feed Text	Phishing URLs are saved as indicators. The signaled phishing activities are saved as TTPs related to the corresponding indicators. API endpoint: *https://openphish.com/feed.txt*.
Proofpoint Message	Indicators and observables focusing on email threats such as phishing, spoofing, email malware, and impostor email/fraudulent messages API endpoint: *https://api.emaildefense.proofpoint.com/v1*.

Upload files

To manually upload files and archives to the platform, do the following:

- On the top navigation bar click **Intelligence > All intelligence > Browse > Uploads** .

Alternatively:

- On the top navigation bar click **Intelligence > All intelligence > Browse > Uploads** .
- **Content type**: from the drop-down menu select a content type corresponding to the file format you are about to upload. The available options on the list correspond to the allowed content type formats that the platform can ingest and process.
- **Require valid signature**: select this checkbox to enforce PGP signature validation of the incoming feed data.

  To work correctly, the source data provider needs to offer a PGP validation service based on a public and a private key.
  Moreover, you need to obtain a valid PGP public key from the source data provider, which you need to add to the platform trusted keys.

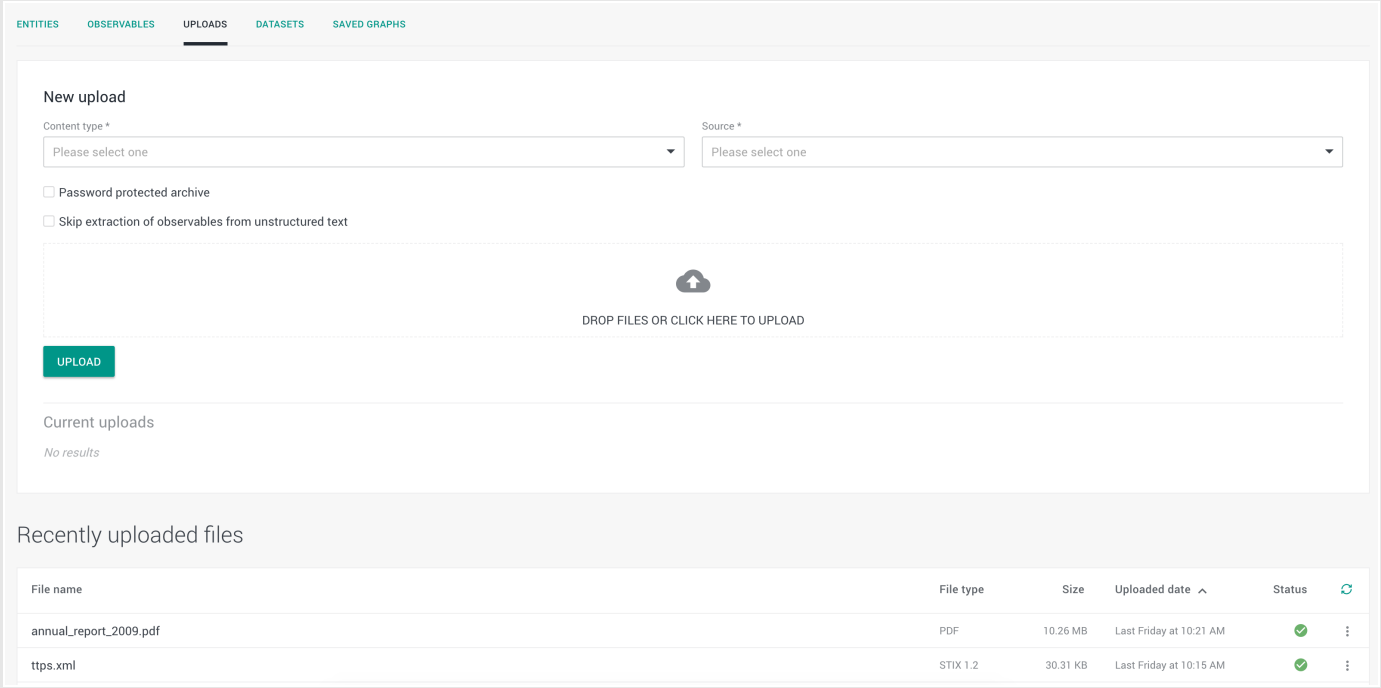
  To add a trusted key to the platform, do the following::

  - On the left-hand navigation sidebar click ⚙ **> System settings > Trusted keys > Edit settings** .
  - On the **Edit public trusted keys settings** page, click ✚ **Add** or ✚ **More** to add a new PGP public key:
    - **Key**: copy-paste into this field the public PGP key you want to add as a trusted key to verify the PGP signature of incoming data packages.
      Include in the pasted content the leading `-----BEGIN PGP PUBLIC KEY BLOCK-----` and the trailing `-----END PGP PUBLIC KEY BLOCK-----` lines.
    - **Description**: add a short description to help users understand the purpose of the PGP public key.
    - Click **Save** to store your changes, or **Cancel** to discard them.
- **Skip extraction of observables from unstructured text**: select this checkbox to exclude from ingestion observable data detected in unstructured content and without link names defining their relationships, if any.

  If you select the checkbox, the platform filters out any observable data detected inside titles, headers, descriptions, summaries, and other free-form, free text fields.
  Observable data inside unstructured text fields is usually not as relevant, and not as valuable in terms of intelligence, as observable data extracted from, for example, CybOX fields.
  In the same way, observables with relationships, but without any link names providing extra context and relevance, can add more noise than actual value to the platform data.
- **Archive**: select this checkbox if you are uploading one or more compressed archives.
  Supported archive formats: *.rar*, *.tar*, *.tar.bz2*, *.tar.gz*, *.tar.bz2*, *.tar.z*, *.zip*
  If the archives you are manually uploading are password-protected, select the **Password protected archive** checkbox, and then enter the password in the **Archive password** field. The specified password acts as a master password, and it is used to unlock all the archives included in the same upload operation.
- Drag and drop files onto the upload area, or click it to open a system file manager window, and browse to the desired file location.
- After selecting the appropriate file type and the file(s) you want to upload to the platform, click **Upload** to complete the action.
- Under **Current uploads** you can see the upload queue.
  File upload progress for each file is expressed as a percentage.
  A confirmation message notifies a successful file submission.

- To submit a new file for upload, click **New upload**.

> **About archives**
>
> - The archive(s) you want to upload should be in one of the following formats: *.rar*, *.tar*, *.tar.bz2*, *.tar.gz*, *.tar.bz2*, *.tar.z*, *.zip*.
> - When you prepare an archive for upload to the platform, you should not mix file types: to be correctly processed, all the files inclided in the archive need to share the same content type.
> - You can upload report documents in plain text *(txt)*, STIX or PDF format by including them in an archive, which you subsequently upload to the platform. Make sure all reports in the zipped archive share the same content type.
> - The platform automatically extracts and produces entities from successfully uploaded archive files.
> - The maximum file size you can upload is *10 MB*.



Review uploaded files

You can review a list of recently uploaded files under **Recently uploaded files**.
You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

- Click a **Status** icon to display further details about the corresponding file upload operation:

Pending	The selected file was added to the upload queue, and it is waiting to be uploaded.
Success	The selected file was successfully uploaded to the upload queue, and you can view it.

Error	The selected file was not uploaded. Click the status icon to view an error message and a traceback with more details about the failure. This information can be helpful to troubleshoot the issue.

- To display the content of a successfully uploaded file from the list, click the ⋮ icon, and then select **View**.

The upload fails because of a missing source

Scenario

The **New upload** page displays a **Source** input field with a drop-down menu.

Issue

- The **Source** field is marked as mandatory.
- The drop-down menu is empty. Therefore, it is not possible to make any valid selection.
- Since a mandatory field is left empty, the upload fails.

Cause

- Either no user groups are configured in the platform;
- Or the platform feayres one or more configured user groups, but the current user is not part of any existing group.

Solution

The current user needs to be part of a platform user group to be able to upload files manually.

If there are no configured user groups:

- Create a group.

- Add the current user to it.

If the current user is not part of any existing group:

- Add the current user to an existing group.

One you are done, proceed to manually upload the files again.

About observables

Observables are discrete pieces of information that represent properties, attributes, actions, and events. They do not carry any contextual information. If they are detected in a specific context or sighted within the organization, they can become indicators or sightings, respectively.

About observables

Observable

An observable records a distinct bit of information: it can be an item such as an IP address, a hash, as well as the name of a country, of a city, of an organization, or of an individual. It can also be an action such as the creation of a registry value, or a file deletion or modification.

An observable is atomic: the piece of information it records is complete and meaningful, but it cannot be split into smaller components without losing meaning and intelligence value.

An observable is factual: it records a bare fact as is, with no additional context or background.

Observable inside structured text

When you select **Skip extraction of observables from unstructured text** in the configuration of incoming feeds or a manual file upload, the platform filters and ingests *only* these higher-value observables.

Observables inside structured content are typically intelligence-richer, and therefore more valuable, than observables inside unstructured content.
Observables inside structured content are usually bundled with an entity when they are ingested; they are extracted from structured fields, or parsed from structured CybOX fields.

Observables whose values are retrieved from CybOX fields usually have higher intelligence value, and they are more relevant because they are directly related to the parent STIX entity they refer to.
In the same way, observables whose relationship to an entity has a link name value are likely to carry more meaning than observables without a link name: entity-observable relationships with a link name provide additional context, and they help understand, for example, how a specific resource is used, or the purpose it serves for an attacker.

You can leverage the intelligence value of these observables — for example, you may decide to (re)act by instrumenting your prevention/detection components to automatically block or blacklist them.

Example:

- A URI in a CybOX `URIObj` field: *http://www.evil.com/big/info.php*

Use cases:

- When you select **Skip Skip extraction of observables from unstructured text** in the configuration of an incoming feed or of a manual file upload, the platform filters and ingests only these higher-value observables.
- When you select **Include only observables with link names** in the configuration of an outgoing feed, the platform includes in the outgoing feed content only observables with the specified link name value(s) describing specific types of relationship between observables and their parent entities.
- When you select **Link types filter > Link types** in the configuration of an observable rule, the platform applies the rule only to observables with the specified link name value(s) describing specific types of relationship between observables and their parent entities.

Observable inside unstructured text

When you select **Skip extraction of observables from unstructured text** in the configuration of incoming feeds or a manual file upload, the platform *excludes* these lower-value observables from ingestion.
Deselect this option to include them and to ingest them along with any observables inside structured content.
These observables may be of low quality, and they may clutter, rather than enhance, the overall intelligence value of your platform data.

Observables inside unstructured text are typically not included in CybOX objects, and they usually do not have link names defining their relationships, if any.
They can be mentioned inside STIX fields such as headers, titles, descriptions, where they are included for reference.
These observables usually have lower intelligence value, and they are less relevant because they are indirectly related to the parent STIX entities they belong to.

Example:

- A URI in a STIX `Reference` field: *http://www.evil.com/big/info.php*

Use cases:

- When you leave **Skip Skip extraction of observables from unstructured text** deselected in the configuration of an incoming feed or of a manual file upload, the platform filters and ingests also observable data detected in unstructured content and without link names defining their relationships.
- When you select **Include observables without a link type** in the configuration of an outgoing feed, the platform includes in the outgoing feed content also observables with an undefined link type/link name.
- When you select **Link types filter > Include observables without a link type** in the configuration of an observable rule, the platform applies the rule also to observables with an undefined link type/link name.

Observable types

The available observable types are:

actor-id
address
asn
bank-account
card
card-owner
cce
city
company
country
country-code
cve

cwe
domain
email
email-subject
eui-64
file
forum-name
forum-room
forum-thread
fox-it-portal-uri
geo
geo-lat
geo-long
handle
hash-md5
hash-sha1
hash-sha256
hash-sha512
host
industry
inetnum
ipv4
ipv6
mac-48
malware
mutex
name
nationality
netname
organization
person

port
postcode
process
product
registrar
rule
snort
street
telephone
uri
uri-hash-sha256
winregistry
yara

Get observable types via API

You can retrieve a JSON response with all supported observable types by making an API call:

- Authenticate to obtain the token you pass with each API call.
- Send a request to the `/private/extracts/kinds/` (trailing slash included) API endpoint:

```
$ curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/private/extracts/kinds/
```

```
# copy-paste version:
$ curl -X GET -v --insecure -i -H "Content-Type: application/json" -H "Accept: application/json"
-H "Authorization: Bearer ${token}" https://${platform_host}/private/extracts/kinds/
```

- The response is a JSON array listing all the supported observable types:

```
{
 "data": [

  {
```

```
 "kind": "geo-lat"
},

{
 "kind": "company"
},

{
 "kind": "yara"
},

{
 "kind": "bank-account"
},

{
 "kind": "handle"
},

{
 "kind": "malware"
},

{
 "kind": "mutex"
},

{
 "kind": "winregistry"
},

{
 "kind": "fox-it-portal-uri"
},

{
 "kind": "port"
},

{
 "kind": "street"
},

{
 "kind": "hash-sha512"
},

{
 "kind": "city"
},

{
 "kind": "card"
},

{
 "kind": "uri-hash-sha256"
},

{
 "kind": "inetnum"
},

{
 "kind": "card-owner"
},
```

```
{
 "kind": "netname"
},

{
 "kind": "industry"
},

{
 "kind": "address"
},

{
 "kind": "ipv4"
},

{
 "kind": "hash-sha1"
},

{
 "kind": "mac-48"
},

{
 "kind": "nationality"
},

{
 "kind": "person"
},

{
 "kind": "process"
},

{
 "kind": "cve"
},

{
 "kind": "host"
},

{
 "kind": "name"
},

{
 "kind": "asn"
},

{
 "kind": "product"
},

{
 "kind": "country"
},

{
 "kind": "ipv6"
},

{
```

```
 "kind": "country-code"
},

{
 "kind": "domain"
},

{
 "kind": "forum-name"
},

{
 "kind": "registrar"
},

{
 "kind": "hash-sha256"
},

{
 "kind": "cce"
},

{
 "kind": "email"
},

{
 "kind": "postcode"
},

{
 "kind": "cwe"
},

{
 "kind": "uri"
},

{
 "kind": "hash-md5"
},

{
 "kind": "forum-thread"
},

{
 "kind": "eui-64"
},

{
 "kind": "telephone"
},

{
 "kind": "snort"
},

{
 "kind": "geo"
},

{
 "kind": "file"
```

```
  },

  {
   "kind": "organization"
  },

  {
   "kind": "email-subject"
  },

  {
   "kind": "geo-long"
  },

  {
   "kind": "forum-room"
  },

  {
   "kind": "actor-id"
  },

  {
   "kind": "rule"
  }

 ]
}
```

Add observables

You can manually add observables to entities to augment their intelligence value with additional context.

The platform uses enrichers to automatically retrieve data that augments an entity intelligence value by adding more context. These details are stored as discrete pieces of information, that is, they are saved as observables.

You can also manually add observables to entities. For example, to update the entity and to integrate newer or more accurate information about a related IP address, a domain name, a targeted victim, and so on.

Access observables

You can access observable details in one of the following ways:

Through the observable detail pane

- On the top navigation bar click:
  - Either **Intelligence > All intelligence > Browse > Observables**
  - Or **Intelligence > All intelligence > Production > Observables**
- On the active view, browse to the observable you want to inspect and click it.
  The observable detail pane slides in from the side of the screen.

Through the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

By clicking an observable name on the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.
- Browse to the observable whose details you want to inspect and click its name to display the corresponding detail pane.

Manually add observables

You can add observables on the fly to associate them with the corresponding entity, that is, either the current entity displayed on the entity detail pane, or an entity you are creating or editing.

You can add as many observables to an entity as you need.

To manually add an observable, do the following:

- On the left-hand navigation sidebar click ⊕ **> Observable**

  or:

- On the top navigation bar click **Intelligence > All intelligence > Production > Observables > ✚**

  or:

- On the top navigation bar click the **Browse**, **Production**, **Discovery**, or **Exposure** view.
- On the selected view, click an entity.
- On the entity detail pane, click the **Observables** tab.
- On the active view, click ✚ **(Create observable)** to create a new observable.

The observable editor opens, and you can start describing the new observable in the **Add observable** view:

- **Type**: from the drop-down menu select an observable type that describes the type of information you are storing in the observable.
  For example, a bank account number, a payment card number, an IP address, a domain name, a country or city name, and so on.

- **Link name**: from the drop-down menu select an option to define the type of relationship existing between the observable and the parent entity.

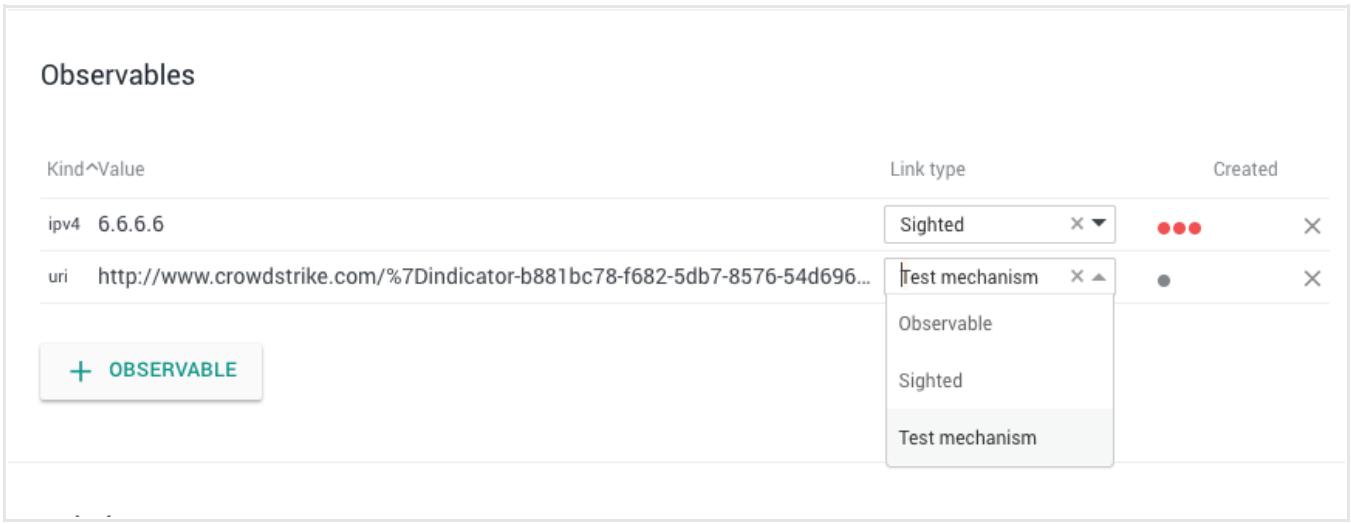
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.

  You can modify and update the link name value at any time to reflect changes in the entity-observable relationship:

  - On the entity edit page browse to the **Observables** section.
  - If the section is populated with observables, each of them has a **Link type** column.
  - Click the **Link type** drop-down menu for the observable whose relationship link name you want to update, and then select one of the available options.
  - If the **Link type** drop-down menu has no options, the selected the entity-observable relationship is undefined.

  Example:



- **Value(s)**: enter the value of the observable. The value and its format should match the specified observable type (kind).
  Insert one value entry per line.
  If you enter multiple values on one line, use a comma (**,**) as a separator.
  Example: *75.23.125.231*, *ipwnu.biz*, *Kansas City*, *1.37bn@rivercitymedia.com*, *Alvin Slocombe*
- **Maliciousness**: from the drop-down menu select a maliciousness confidence level to assess the likelihood the potential threat may or may not damage the organization.

  This option corresponds to the value you set under **Data configuration > Rules > Observable > + (Create rule) > Action > Mark as malicious > Confidence**.

  When you flag an observable with a maliciousness confidence level, it cannot transition back to *safe* or *ignore* anymore. It can only become more malicious, that is, it can only transition to a higher, never to a lower, maliciousness confidence level. Once an observable is flagged as harmful, it cannot go back to being safe or irrelevant anymore.

Define relationships with link names

When you manually add an observable to an existing entity through the entity detail pane, **Observables** tab, ✚ *(Add observable)*, you can select a **Link name** option to specify the type of relationship the observable has with the entity it refers to.

The available link name definitions vary, based on the relationship the observable has with the specific entity type it belongs to.

Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
For example, it can clarify that an observable describes a vulnerability or a weakness related to its parent exploit target entity.

Course of action

- **Parameter**: it is the only link name option available for observables entities.
  It enables defining specific technical parameters, settings, and configurations related to the observables using the CybOX Language.

  You can set parameters for a course of action to define automated courses of action designed to to carry out follow-up actions. It can be a detection follow-up; for example, it can trigger adjusting the settings of a malware detection application accordingly. It can be a prevention follow-up; for example, it can instrument a third-party system to block a range of malicious IP addresses or domain names. Or it can produce a community follow-up; for example, creating and publishing a report to notify other parties about the possible threat the entity represents.

Exploit target

- **Affected**: describes an affected, impacted resource.
- **Configuration**: enter the **Common Configuration Enumeration (CCE)** `(https://nvd.nist.gov/config/cce/index)` code defining a specific security system configuration issue, as well as the related configuration guidance statement containing preferred or required settings or policies for the system configuration it refers to.
  Example: *CCE-5770-3*
- **Vulnerability**: enter the **Common Vulnerabilities and exposures (CVE)** `(https://cve.mitre.org/cve/identifiers/)` **identifier** `(https://en.wikipedia.org/wiki/common_vulnerabilities_and_exposures#cve_identifiers)` to reference the security threat.
  Example: ***CVE-2017-6394* on CVE** `(https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-6394)` or ***CVE-2017-6394* on NVD** `(https://web.nvd.nist.gov/view/vuln/detail?vulnid=cve-2017-6394).`
- **Weakness**: enter the **Common Weakness Enumeration (CWE)** `(https://cwe.mitre.org/)` **identifier** `(https://en.wikipedia.org/wiki/common_weakness_enumeration)` to reference the software security weakness.
  Example: ***CWE-319*** `(http://cwe.mitre.org/data/definitions/319.html)`, ***CWE-642*** `(http://cwe.mitre.org/data/definitions/642.html).`

Incident

- **Affected asset**: defines an affected, impacted resource or **asset type** (https://stixproject.github.io/data-model/1.2/stixvocabs/assettypevocab-1.0/).
- **Related**: holds one or more observables that are related to this one.

Indicator

- **Observable**: the observable related to the entity is an embedded CybOX observable object.
  It has been detected *outside* the organization.
- **Sighted**: the observable related to the entity is an embedded CybOX observable object.
  At least one specific occurrence of the observable related to the entity has been detected, that is, sighted, *inside* the organization.
- **Test mechanism**: a **test mechanism** (https://stixproject.github.io/data-model/1.2/indicator/testmechanismtype/) enables the platform to share entity information with external tools and systems. In particular, it is useful to send information to an **IDS/HIDS/NIDS** (https://en.wikipedia.org/wiki/intrusion_detection_system) to test it against a tool-specific rule.

  For example, an observable with a **Test mechanism** link name can trigger follow-up actions in external systems:

  - **Rule**: **generic test mechanism** (https://stixproject.github.io/data-model/1.2/genericctm/genericctestmechanismtype/) to interact with a generic system supporting plain text format as an input.
  - **Snort**: **Snort test mechanism** (https://stixproject.github.io/data-model/1.2/snorttm/snorttestmechanismtype/).
    You can include the observable in an outgoing feed to a Snort instance. The Snort rules in the indicator are used to look for **matching patterns** (https://stixproject.github.io/documentation/idioms/snort-test-mechanism/) in the Snort logs. You can configure Snort so that matching hits trigger a follow-up action. For example, creating a sighting or adding a malicious entry to a blocklist.
  - **YARA**: **YARA test mechanism** (https://stixproject.github.io/data-model/1.2/yaratm/yaratestmechanismtype/).
    You can include the observable in an outgoing feed to a YARA instance. YARA uses the rules in the indicator to look for **matching patterns** (https://stixproject.github.io/documentation/idioms/yara-test-mechanism/) in the target files or locations you specify in YARA.
    You can feed indicators from the platform to YARA to look for, identify, and classify malware samples.

TTP

- **Malicious infrastructure**: describes a component of the infrastructure — gear, equipment, tools, software and hardware, services — used to carry out the malicious activities described in the TTP.
- **Targeted victim**: describes a component of the targeted victim's assets and resources.

Report

- **Observable**: the observable related to the entity has been detected *outside* the organization.
  It represents a potential threat that may or may not impact your organization.

Threat actor

- **Identity**: holds information that allows to identify the threat actor entity it is related to.
  For example, an individual's first and/or last name, or the denomination of an organization.

Campaign

- N/A. Campaign-related observables do not have link types.
- Click **Save** to store your changes, or **Cancel** to discard them.

> You can use the specified observable values to set up automation processes, so that the (potential) threat the entity represents can trigger an action in a security system or another device in the toolchain.
>
> For example, if the observable **Type** is *Email*, the **Link name** is *Parameter*, and the **Value(s)** are *scam@honestpaul-superdeals.com*, *info@honestpaul-superdeals.com*, and *support@honestpaul-superdeals.com*, create a rule in the email server to block all incoming messages from the *honestpaul-superdeals.com* email domain.

Search by link name

You can use link names to search for specific observables, based on the type of relationship they have with their parent entity.

For example, an analyst is working on a threat model where a threat actor exploits the **CVE-2017-8793** `(https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-8793)` vulnerability to gain access to the targeted victim's assets. The analyst may want to search the platform for any exploit target entities containing observables that are related to the parent exploit target because they describe a vulnerability. Pretend you are the analyst in question:

- On the left-hand navigation sidebar click 🔍
- In the search box at the top of the page, enter your search query:

```
data.type:exploit-target AND extracts.kind:domain AND
extracts.instance_meta.link_types:vulnerability
```

- Press **ENTER** to start the search.

In the search query example:

- `extracts.instance_meta.link_types` is the JSON path pointing to the JSON field in the entity data structure that holds the link name value

- `vulnerability` is the link name value, that is, the type of entity-observable relationship you are looking for.

If the link name value search string contains multiple words separated by spaces, wrap the search string in double quotes (example: `"my multiple word search string"`).
The platform search functionality uses the **Elasticsearch query syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html)`.

This table maps the link name values you can enter in a search query to the corresponding **Link name** options displayed in the GUI (campaign entities have no link names to define relationships with observables):

Search input value	GUI link name option	Entity
`parameter`	*Parameter*	Course of action
`affected`	*Affected*	Exploit target
`configuration`	*Configuration*	Exploit target
`vulnerability`	*Vulnerability*	Exploit target
`weakness`	*Weakness*	Exploit target
`affected-asset`	*Affected asset*	Incident
`related`	*Related*	Incident
`observed`	*Observable*	Indicator
`sighted`	*Sighted*	Indicator
`test-mechanism`	*Test mechanism*	Indicator
`malicious-infrastructure`	*Malicious infrastructure*	TTP
`targeted-victim`	*Targeted victim*	TTP
`observable`	*Observable*	Report
`identity`	*Identity*	Threat actor

Edit observables

Editing observables does not affect the information they hold, but rather the relationships they have with the entities they refer to, which can be direct or indirect.

Observables are atomic bits of information, they hold one piece of information. For example, an IP address, a domain name, an email address, a threat actor name, and so on.

Rather than the data value an observable holds, it is the way in which that information unit relates to other data objects, namely entities, that can change: direct vs indirect relationship, and non-malicious vs malicious. These attributes help assess threat severity and triage follow-up actions.

You can change the level of importance of the relationships observables have with entities; you can flag observables to be ignored or removed from the existing relationships entities have with other objects in the platform, as well as increase the level of confidence in the potential maliciousness observables may have.

Last but not least, you can load observables on the graph for analysis, and you can manually enrich them.

Access observables

You can access observable details in one of the following ways:

Through the observable detail pane

- On the top navigation bar click:
  - Either **Intelligence > All intelligence > Browse > Observables**
  - Or **Intelligence > All intelligence > Production > Observables**
- On the active view, browse to the observable you want to inspect and click it.
  The observable detail pane slides in from the side of the screen.

Through the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

By clicking an observable name on the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

- Browse to the observable whose details you want to inspect and click its name to display the corresponding detail pane.

Add observables to the graph

On an observable view and on the detail pane **Observables** tab you can load one or more observables on the graph to analyze them and to examine their relationships.
To load an observable on the graph, do the following:

- On the row corresponding to the observable you want to load on the graph, click the ⋮ icon.
- From the drop-down menu select **Add to graph**.
- You can then proceed to open the graph, where you can start analyzing the observable.

Alternatively:

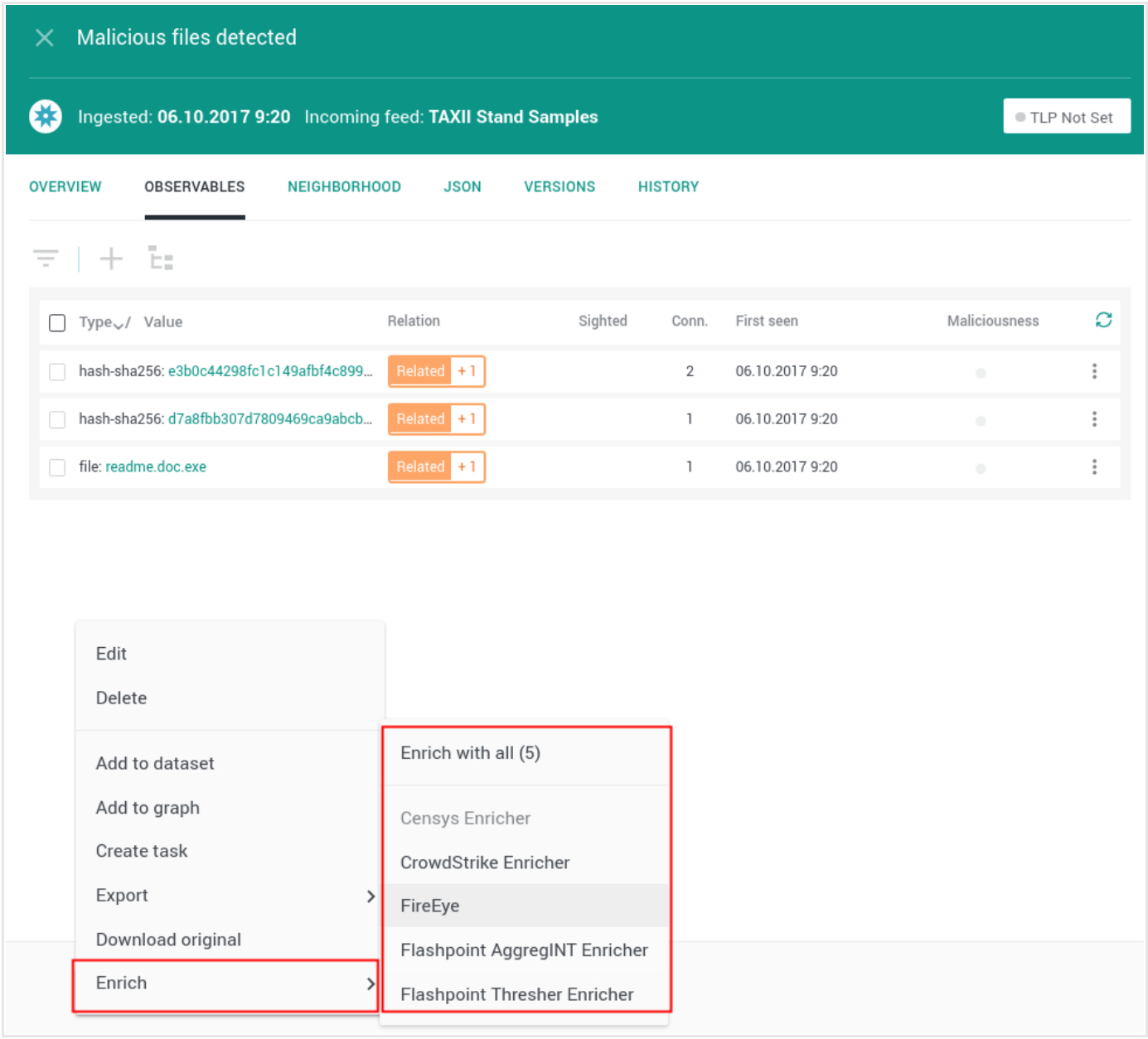
- Select the checkbox corresponding to the observable you want to load on the graph.
- From the **Actions** drop-down menu on the **Observables** tab click **Add to graph**.
- You can then proceed to open the graph, where you can start analyzing the observable.

> You can also select multiple observables, and then load them all on the graph by clicking **Add to > Graph** on the horizontal bar above the column header row.

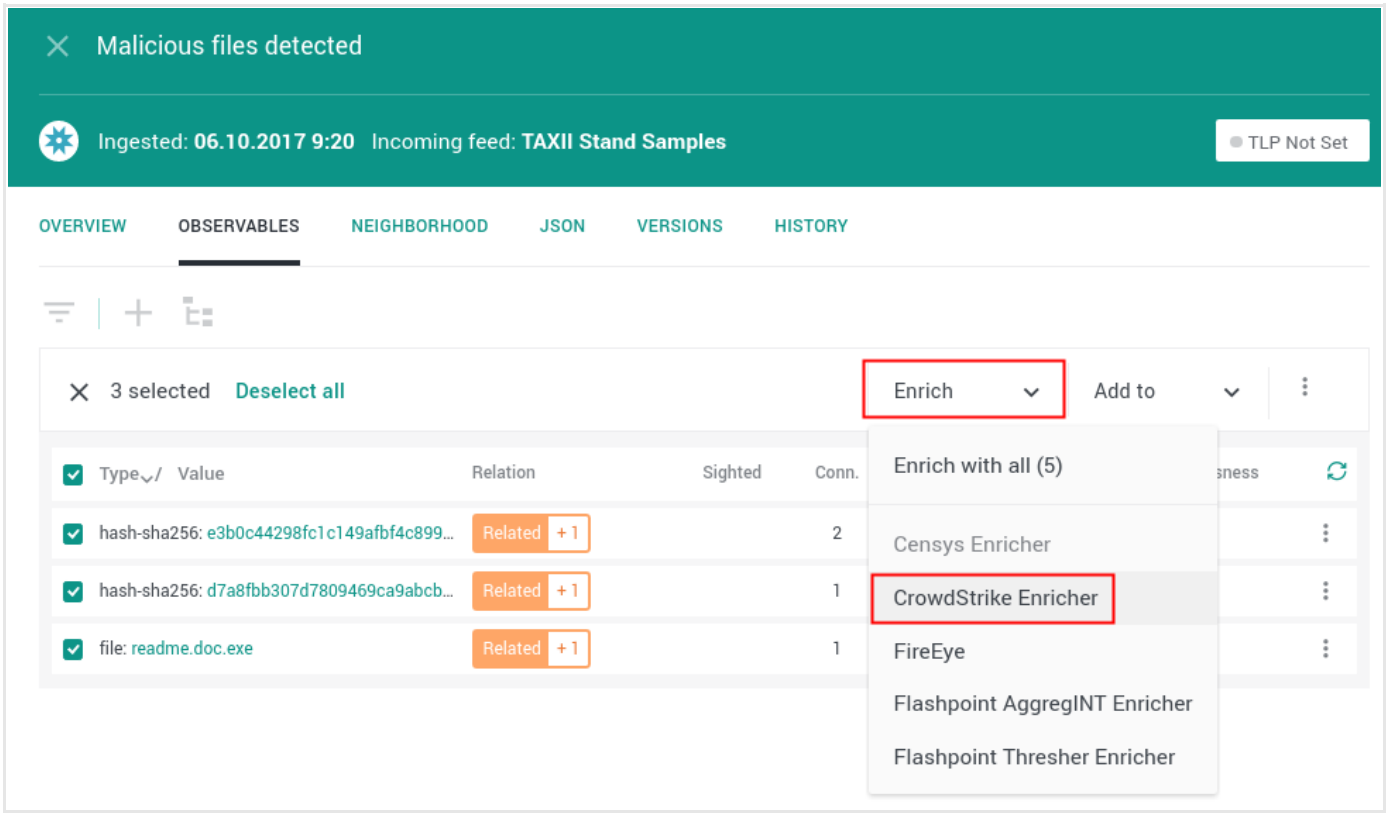
Manually enrich observables

You can manually enrich observables by:

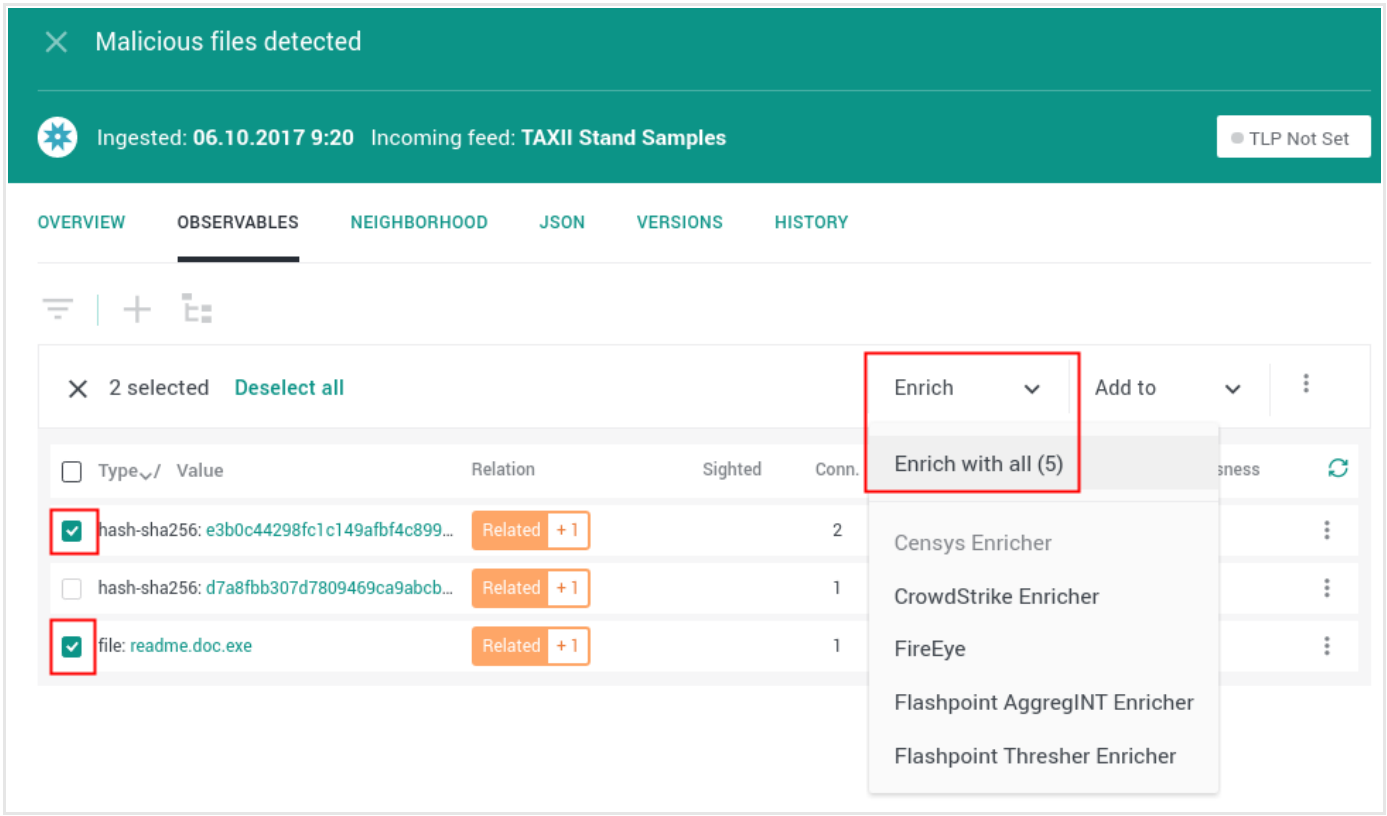
- Run all applicable enrichers for the entity to enrich all the observables it holds by selecting **Actions > Enrich > Enrich with all**:



- Select and run a specific enricher on all the observables listed on the tab by clicking all observable checkboxes, and then **Enrich > ${enricher_name}** on the horizontal bar above the column header row:



- Select some observables by clicking the corresponding checkboxes, and then run all applicable enrichers by clicking **Enrich > Enrich with all** on the horizontal bar above the column header row:



Delete observables

Flagging an observable to be ignored completely deletes it from the platform database. Removing it from the entity it relates to erases any relationships the observable has with the entity.

Access observables

You can access observable details in one of the following ways:

Through the observable detail pane

- On the top navigation bar click:
  - Either **Intelligence > All intelligence > Browse > Observables**
  - Or **Intelligence > All intelligence > Production > Observables**
- On the active view, browse to the observable you want to inspect and click it.
  The observable detail pane slides in from the side of the screen.

Through the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

By clicking an observable name on the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.
- Browse to the observable whose details you want to inspect and click its name to display the corresponding detail pane.

Ignore observables

You can ignore observables related to an entity when they add no intelligence value or when they introduce unwanted data noise. When you ignore an observable, the platform *permanently deletes it* from the database.

To ignore an observable related to an entity, do the following:

- Go to the **Observable** tab on the entity detail pane.
- On the row corresponding to the observable you want to ignore, click the ⋮ icon.
- From the drop-down menu select **Ignore observable**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.

To ignore an observable on the **Browse > Observables** overview, do the following:

- On the top navigation bar click **Browse > Observables**.
- On the active view, browse to the observable you want to ignore and click it.
  The observable detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Ignore observable**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.

Remove observables

You can remove observables related to an entity when they add no intelligence value or when they introduce unwanted data noise. When you remove an observable, the platform deletes any relationships between the observable and the entity. The observable remains stored in the database, but since it no longer has any relationships with the entity, it is not included in the **Observable** tab any longer.

To remove an observable related to an entity, do the following:

- Go to the **Observable** tab on the entity detail pane.
- On the row corresponding to the observable you want to ignore, click the ⋮ icon.
- From the drop-down menu select **Remove from entity**.
- You are not prompted to confirm the action, which is executed immediately.
  A notification message informs you about the outcome of the operation.

You can also select multiple observables, and then remove them from the entity in bulk.

To remove an observable on the **Browse > Observables** overview, do the following:

- On the top navigation bar click **Browse > Observables**.
- On the active view, browse to the observable you want to remove and click it.
  The observable detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Remove from entity**.
- You are not prompted to confirm the action, which is executed immediately.
  A notification message informs you about the outcome of the operation.

Remove unlinked observables

You can remove unlinked observables permanently following:

- Go to the **Observable** tab on the entity detail pane.
- On the row corresponding to the observable you want to ignore, click the ⋮ icon.
- From the drop-down menu select **Delete**.
- You are prompted to confirm the action, click **Delete**.

Set maliciousness

Set the maliciousness confidence level of an observable to prioritize threat severity and to filter relevant observables for follow-up actions.

Access observables

You can access observable details in one of the following ways:

Through the observable detail pane

- On the top navigation bar click:
  - Either **Intelligence > All intelligence > Browse > Observables**
  - Or **Intelligence > All intelligence > Production > Observables**
- On the active view, browse to the observable you want to inspect and click it.
  The observable detail pane slides in from the side of the screen.

Through the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

By clicking an observable name on the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.
- Browse to the observable whose details you want to inspect and click its name to display the corresponding detail pane.

Set observable maliciousness

Gauging maliciousness helps you assess how dangerous an observable threat potential can be. In the platform you can set a confidence level to estimate the likelihood of an observable being malicious or not. The maliciousness values you can set help you answer the following question:

“Based on the factual evidence and the intelligence gathered so far, how likely is it for the observable to be malicious?”

Maliciousness confidence level	Represented as	Meaning
Unknown	● (gray)	It is not possible to assess whether the observable is malicious or not.
Safe	● (green)	The observable is not malicious.
Malicious - Low confidence	● (red)	The observable might be malicious, but I am not sure.
Malicious - Medium confidence	● ● (red)	I am confident to a point that the observable may be malicious.
Malicious - High confidence	● ● ● (red)	I am confident that the observable is malicious.

Setting a maliciousness confidence level allows triaging and prioritizing threat severity.
You can set the maliciousness confidence level of an observable in one of the following ways:

On the observable overview page

- On the top navigation bar click **Browse > Observables**.
- On the row corresponding to the observable whose maliciousness confidence level you want to set, click the ⋮ icon, and then select **Set maliciousness**.
- From the sub-menu, click the maliciousness confidence level you want to assign to the observable.

On the observable detail pane

- Open the detail pane of the observable whose maliciousness confidence level you want to set.
- On the top half of the **Overview** tab under **Maliciousness** click **Edit**, and then select a maliciousness confidence level for the observable.
- Alternatively, on the bottom half of **Overview** tab, click **Actions > Set maliciousness** .
- From the sub-menu, click the maliciousness confidence level you want to assign to the observable.

On the Observable tab on the entity detail pane

- Go to the entity detail pane of the entity related to the observable whose maliciousness confidence level you want to set.
- On the entity detail pane, go to the **Observables** tab.
- On the row corresponding to the observable whose maliciousness confidence level you want to set, click the ⋮ icon.
- From the drop-down menu select **Set maliciousness**.
- From the sub-menu, click the maliciousness confidence level you want to assign to the observable.

Alternatively:

- Go to the entity detail pane of the entity related to the observable whose maliciousness confidence level you want to set.
- On the entity detail pane, go to the **Observables** tab.
- Select the checkbox corresponding to the observable whose maliciousness confidence level you want to set.
- From the **Actions** drop-down menu on the **Observables** tab click **Set maliciousness**.
- From the sub-menu, click the maliciousness confidence level you want to assign to the observable.

You can select multiple observables, and then you can assign the same maliciousness level to them clicking **Actions > Set malicioussness** .

You can configure the Cisco Threat Grid and the VirusTotal enrichers to automatically flag enriched observables with **Malicious - Low confidence** or **Malicious - High confidence**, based on predefined threshold values.

Automatic flagging with high/low confidence maliciousness through observables supports only the following observable types:

- *hash-sha1*
- *hash-sha256*
- *hash-md5*
- *uri*

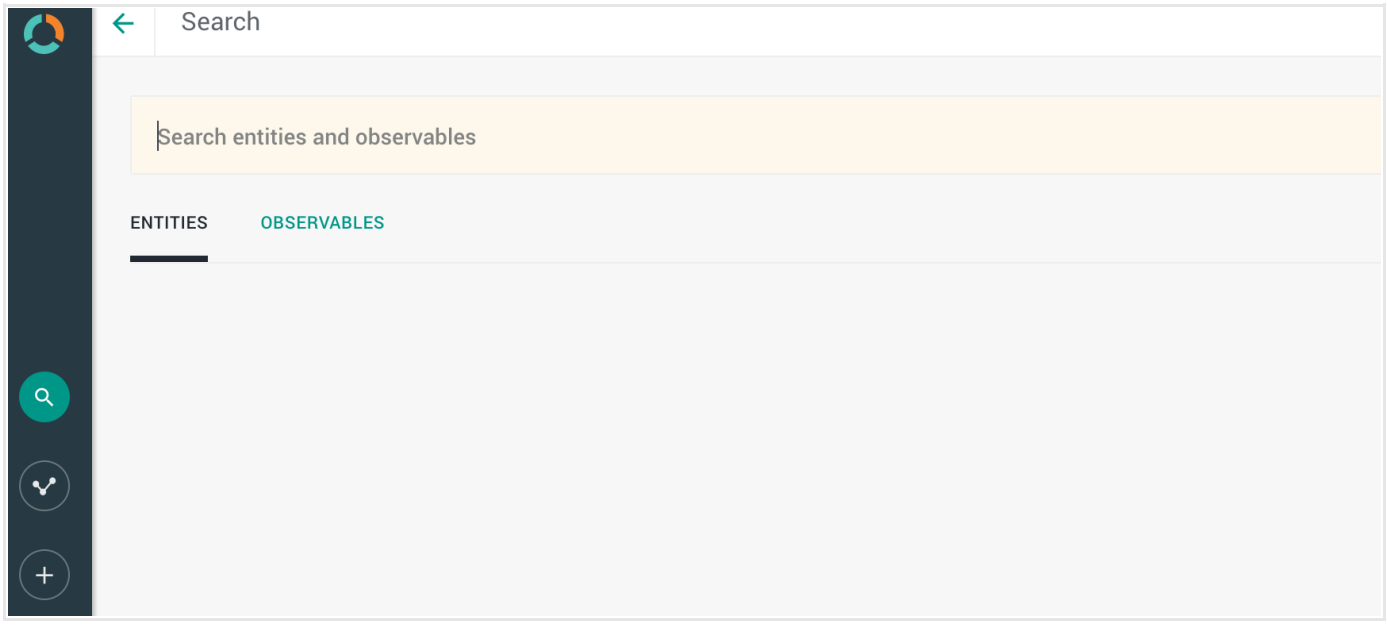
Filter observables by maliciousness

You can filter observables based on their maliciousness confidence level to retrieve a consistent observable data subset that you can further process.
For example, you can retrieve observables with a high maliciousness confidence level, and you can then route them to an external device to trigger an appropriate course of action, such as adding an IP address or a domain name to a blocklist, or closing a communication port.

Enter the following queries in the search box to obtain specific observable subsets:

Search query	Returns
data.confidence.value:high	Observables whose maliciousness confidence level is **Malicious - High confidence**.
data.confidence.value:medium	Observables whose maliciousness confidence level is **Malicious - High confidence**.
data.confidence.value:low	Observables whose maliciousness confidence level is **Malicious - High confidence**.
data.confidence.value:none	Observables with no maliciousness confidence level value.
data.confidence.value:unknown	Observables whose maliciousness confidence level is **Unknown**.

You can find the search box on the sidebar:



Quick search: Hover over the magnifier and enter search queries. Click the search icon to run the search.

Specific search: click the magnifier and enter search terms and search queries. Then click **ENTER** or click the search icon to run the search.
Searches you run through this search box are executed platform-wide.

The search functionality uses **Elasticsearch query syntax** (`https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html`).

Create an indicator

When an observable gains more context, you can transform it into an indicator to reflect the changes in the quantity and quality of the information, and to properly position it in the threat landscape under investigation.

Access observables

You can access observable details in one of the following ways:

Through the observable detail pane

- On the top navigation bar click:
  - Either **Intelligence > All intelligence > Browse > Observables**
  - Or **Intelligence > All intelligence > Production > Observables**
- On the active view, browse to the observable you want to inspect and click it.
  The observable detail pane slides in from the side of the screen.

Through the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

By clicking an observable name on the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.
- Browse to the observable whose details you want to inspect and click its name to display the corresponding detail pane.

Create an indicator from an observable

During an analysis, you may find out that an observable gains weight in the form of relevant contextual information that expands its intelligence value beyond the sheer statement of a fact such as an IP address, a hash value, or a threat actor's name. Therefore, you may want to consolidate, organize, and integrate this information in a consistent way; for example, by creating an indicator.

You can create an indicator from an observable by:

On the observable overview page

- On the top navigation bar click **Browse > Observables**.
- On the row corresponding to the observable you want to transform into a new indicator, click the ⋮ icon, and then select **Create indicator**.
  The entity editor opens and you can proceed to enter the relevant details to create the indicator.

On the observable detail pane

- On the top navigation bar click **Browse > Observables**.
- Click anywhere on the row corresponding to the observable you want to transform into a new indicator.
  The observable detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Create indicator**.
  The entity editor opens and you can proceed to enter the relevant details to create the indicator.

On the Observable tab on the entity detail pane

- Go to the entity detail pane of the entity related to the observable you want to transform into a new indicator.
- On the entity detail pane, go to the **Observables** tab.
- On the row corresponding to the observable you want to transform into a new indicator, click the ⋮ icon.
- From the drop-down menu select **Create indicator**.
  The entity editor opens and you can proceed to enter the relevant details to create the indicator.

Alternatively:

- Select the checkbox corresponding to the observable you want to transform into a new indicator.
- Click the **Actions** drop-down menu on the **Observables** tab, and then select **Create indicator**.
  The entity editor opens and you can proceed to enter the relevant details to create the indicator.

Create a sighting

When an observable is detected inside your organization, it is sighted, and security is compromised. You can transform the original observable into a sighting to reflect the changes in the quality of the information, and to properly position it in the threat landscape under investigation.

Access observables

You can access observable details in one of the following ways:

Through the observable detail pane

- On the top navigation bar click:
  - Either **Intelligence > All intelligence > Browse > Observables**
  - Or **Intelligence > All intelligence > Production > Observables**
- On the active view, browse to the observable you want to inspect and click it.
  The observable detail pane slides in from the side of the screen.

Through the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.

By clicking an observable name on the Observable tab on the entity detail pane

- To do so, go to an entity overview page. For example, by selecting **Intelligence > All intelligence > Browse** , **Production**, **Discovery** or **Exposure** on the top navigation bar, or by clicking **Intelligence > All Intelligence > Browse > Datasets > ${dataset_name}** or **Data configuration > Incoming feeds > ${incoming_feed_name} > Entities** tab on the feed detail pane.
- On the active view, browse to the entity you want to inspect and click it.
  The entity detail pane slides in from the side of the screen.
- On the entity detail pane click the **Observables** tab to display an overview listing any observables related to the entity.
- Browse to the observable whose details you want to inspect and click its name to display the corresponding detail pane.

Create a sighting from an observable

When an organization records a discrete instance of an observed indicator of compromise inside their own environment — for example, an entry in a log file — the malicious item is sighted, and the organization environment is compromised. To represent this scenario in the platform, you can create a sighting from the sighted observable.

You can create a sighting from an observable by:

On the observable overview page

- On the top navigation bar click **Browse > Observables**.
- On the row corresponding to the observable you want to transform into a new sighting, click the ⋮ icon, and then select **Create sighting**.
  The entity editor opens and you can proceed to enter the relevant details to create the sighting.

On the observable detail pane

- On the top navigation bar click **Browse > Observables**.
- Click anywhere on the row corresponding to the observable you want to transform into a new sighting.
  The observable detail pane slides in from the side of the screen.
- On the bottom half of the detail pane, click **Actions**.
- From the pop-up menu select **Create sighting**.
  The entity editor opens and you can proceed to enter the relevant details to create the sighting.

On the Observable tab on the entity detail pane

- Go to the entity detail pane of the entity related to the observable you want to transform into a new sighting.
- On the entity detail pane, go to the **Observables** tab.
- On the row corresponding to the observable you want to transform into a new sighting, click the ⋮ icon.
- From the drop-down menu select **Create sighting**.
  The entity editor opens and you can proceed to enter the relevant details to create the sighting.

Alternatively:

- Select the checkbox corresponding to the observable you want to transform into a new sighting.
- Click the **Actions** drop-down menu on the **Observables** tab, and then select **Create sighting**.
  The entity editor opens and you can proceed to enter the relevant details to create the sighting.