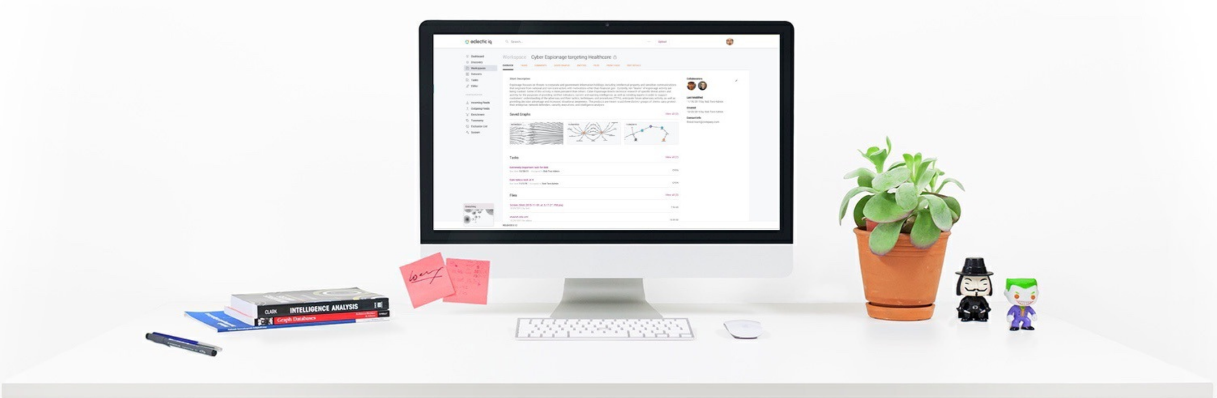
eclectic iq

How to create a money mule TTP

To analyze fraudulent activities and identify their actors

Last generated: March 06, 2018



Last generated on Mar 6, 2018

Table of contents

How to create a money mule TTP

Create a money mule TTP entity to investigate fraudulent activities and to identify the actors involved in them.

Money mules are middlemen who carry out illegal transactions on behalf of a criminal third party. Money mules may not always be aware that they are engaging in criminal activities aimed at committing fraud. They are part of a larger scheme designed to carry out fraudulent transactions involving money or goods.

In a fraudulent financial transaction, money mules are responsible for laundering the illicitly obtained money such as proceeds from phishing, malware or email scams. They transfer the money using money orders or cryptocurrencies, which provide an effective layer of obfuscation.

To identify and to track these actors and their behavioral patterns, fraud and risk teams can create TTP entities that describe the actors, their behaviors, and the victims. Analysts can add relationships with other entities on the fly, as well as let the platform process the data to generate meaningful intelligence providing valuable context to their investigation.

In the EclecticIQ Platform, you always record a money mule as a TTP entity where you need to include at least:

- An actor (the money mule).
  The TTP entity describes the money mule as a malicious actor by defining the context the money mule operates in as accurately as possible.
- A victim (for example, a bank account).
  You define and describe the victim of a money mule in the **Characteristics > Targeted Victim** section.
  A victim can be an individual, a commercial or financial entity, or an object like an email address.
- An intended effect of the criminal behavior (for example, fraud).
  You select the intended effect a money mule aims to achieve in the **Intended effects** section.
  Such an effect can be fraud, theft, money laundering, and so on.

Create a money mule TTP

To create a TTP entity describing a money mule, do the following:

- On the left-hand navigation sidebar, click **Editor**.
- On the editor page, click the **✚ Entity** button.
- From the drop-down menu select **TTP**.

The entity editor is displayed, and you can proceed to create the new TTP entity.

✔ Input fields marked with an asterisk are required.

Title

Specify the name of the new entity. It should be descriptive and easy to remember.
For example: *Money mule related to IBAN ${bank_account_number}*

Analysis

it is a free-text input field to include non-structured information such as additional context, references, links, and so on.
For example, you can add contextual details that can help identify the money mule or the location they operate in.

Confidence

From the drop-down menu select an option to assign the entity a confidence value.
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 an option to specify the purpose or the goal the cyber threat aims at achieving.
Fraud is a very common effect money mules and their associates intend to achieve.

Characteristics

This field allows you to add extra details to more accurately describe the entity; for example, by specifying the threat type, the resources it uses to spread and to reach the intended target, or any connections with other entities.
The one characteristic you want to include in a money mule TTP entity is **Targeted Victim**.

Create a targeted victim

Use the **Characteristics > Targeted Victim** section to record information about the individual, the organization, or the resources affected by the money mule's behavior:

- Under **Characteristics**, click **✚ Characteristic**, and then select **Targeted Victim**.
- The **Targeted Victim** editor opens. It 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.
  Apart from drop-down menus and checkboxes, where available, the editor input fields accept free-text as an input.
  No field is mandatory.

Name: specify the name of the targeted victim. It should be descriptive and easy to remember.
Example: *IBAN ${ludicrously_fat_bank_account_number}*

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**

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*

Specify the targeted victim type

- Under **Characteristics > Targeted Victim > Specification**, click ✚ **Fields**.
  The available types allow you to describe affected individuals, organizations, and assets.

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

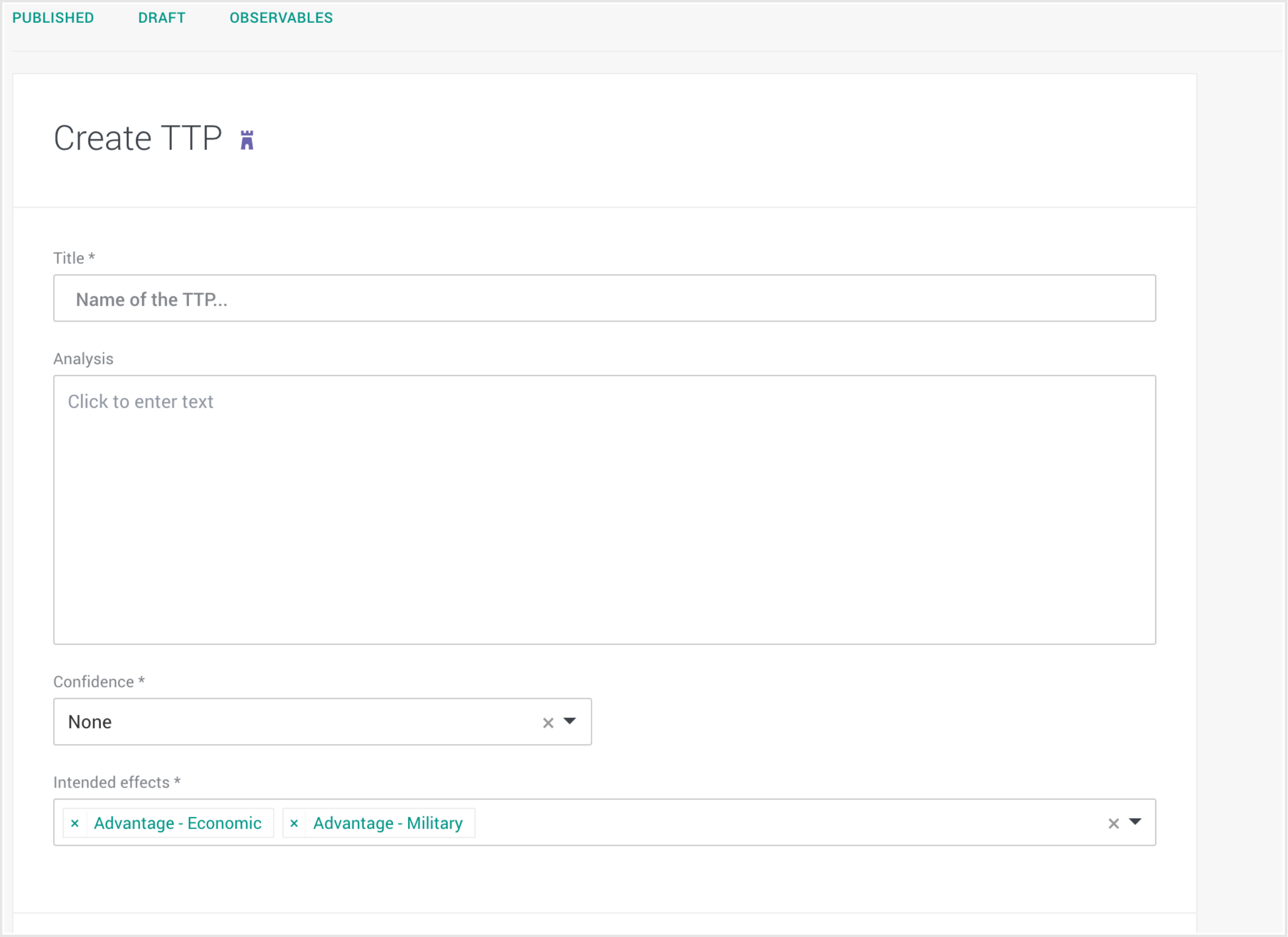
Electronic address: this section takes a set of predefined keys you can select from the drop-down menu, along with the corresponding values you enter as free-text in the input fields.

- 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}*

Next steps

To complete the money mule TTP entity creation, follow the standard steps and procedures you normally use to create entities in the editor, tag them, add relationships, and enrich them with observables.

Example



Create TTP

Title *

Name of the TTP...

Analysis

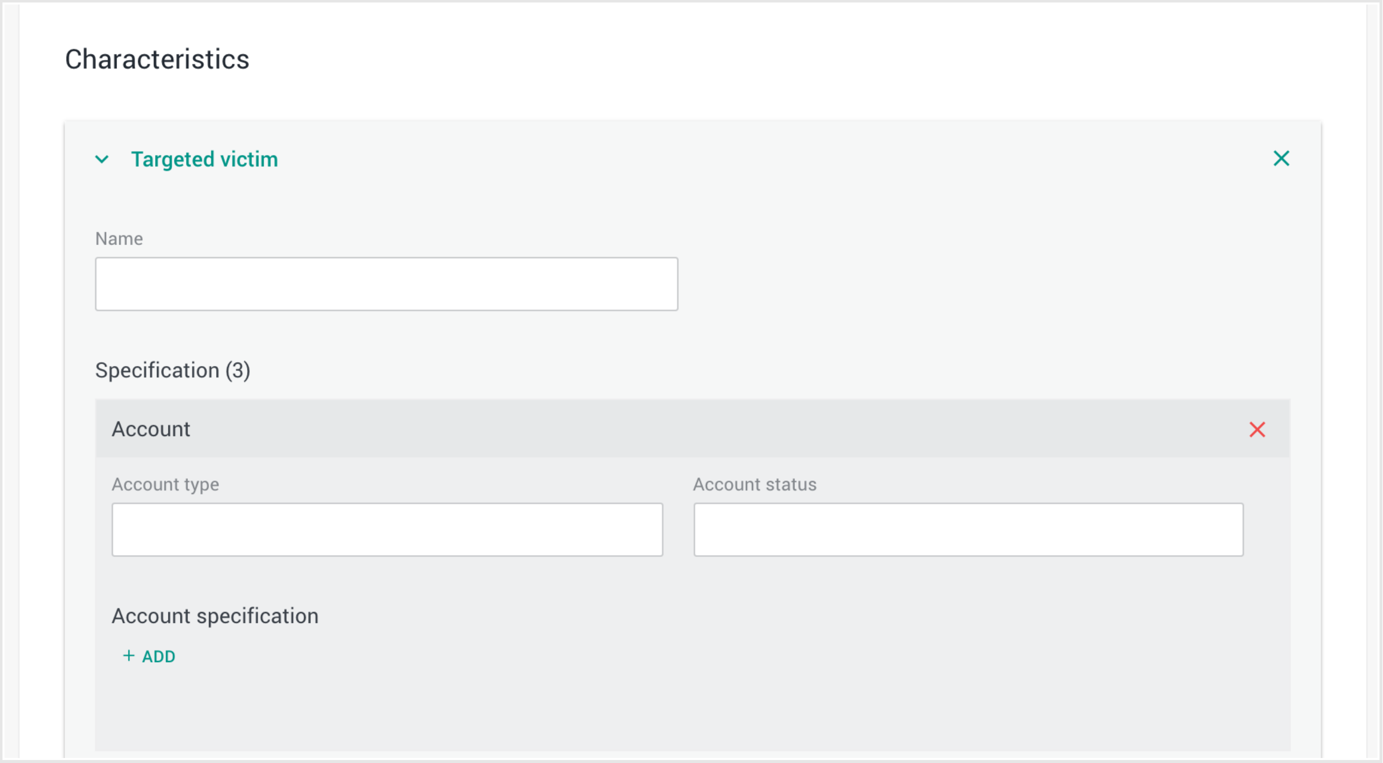
Click to enter text

Confidence *

None

Intended effects *

× Advantage - Economic × Advantage - Military


Characteristics

Targeted victim

Name

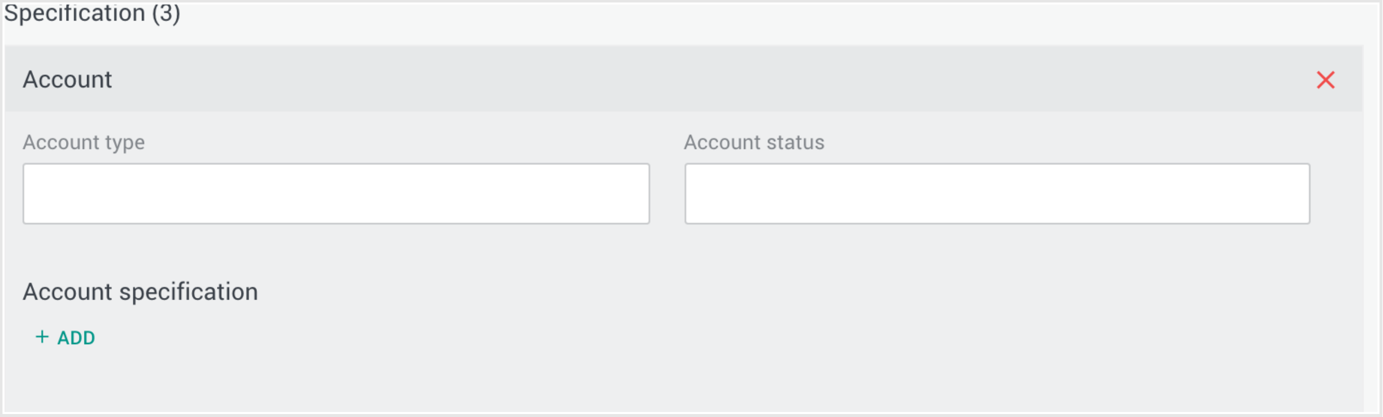
Specification (3)

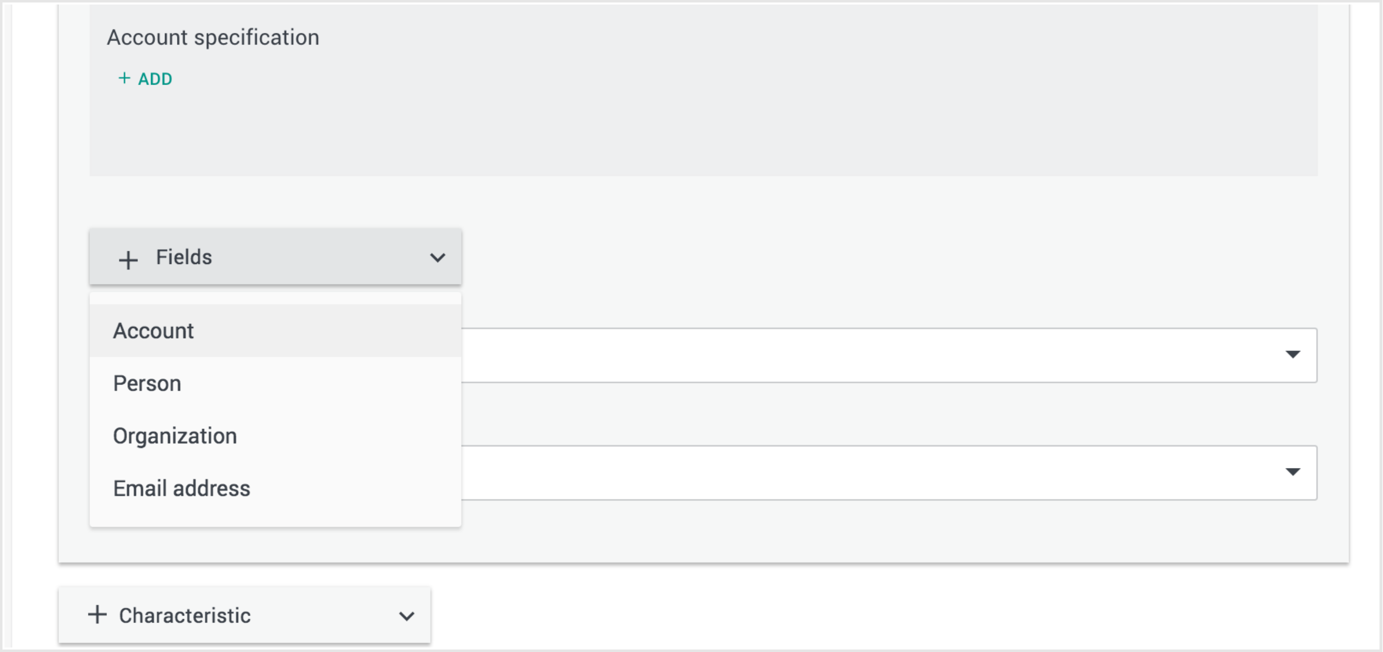
Account

Account type

Account status

Account specification


Specification (3)
Account
Account type
Account status
Account specification
+ ADD


Account specification
+ ADD
+ Fields
Account
Person
Organization
Email address
+ Characteristic

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:

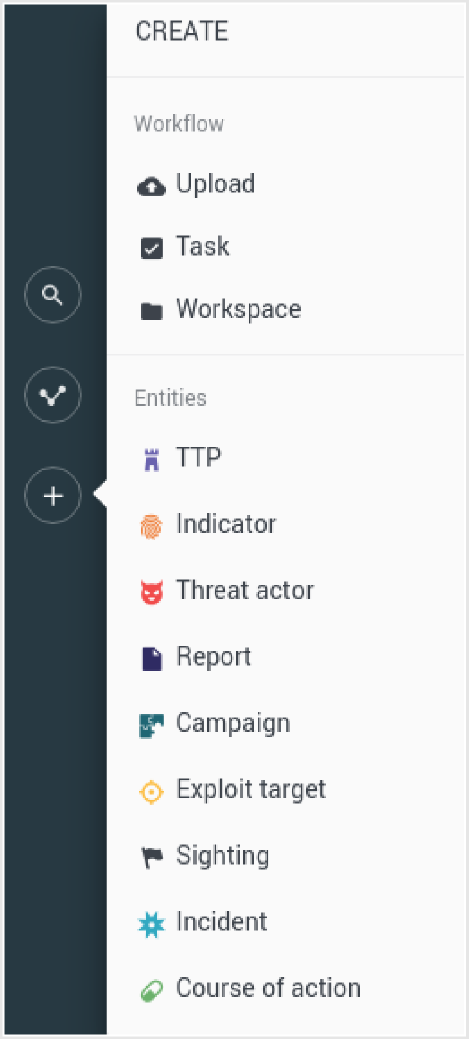
- The steps the adversary performs to achieve their goal.
- The equipment, gear, or tools they use. For example, software, hardware, USB sticks, forged ID badges, and so on.
- Information on any parties they associate with, or the victims they target, as well as on any exploit targets they may leverage 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.

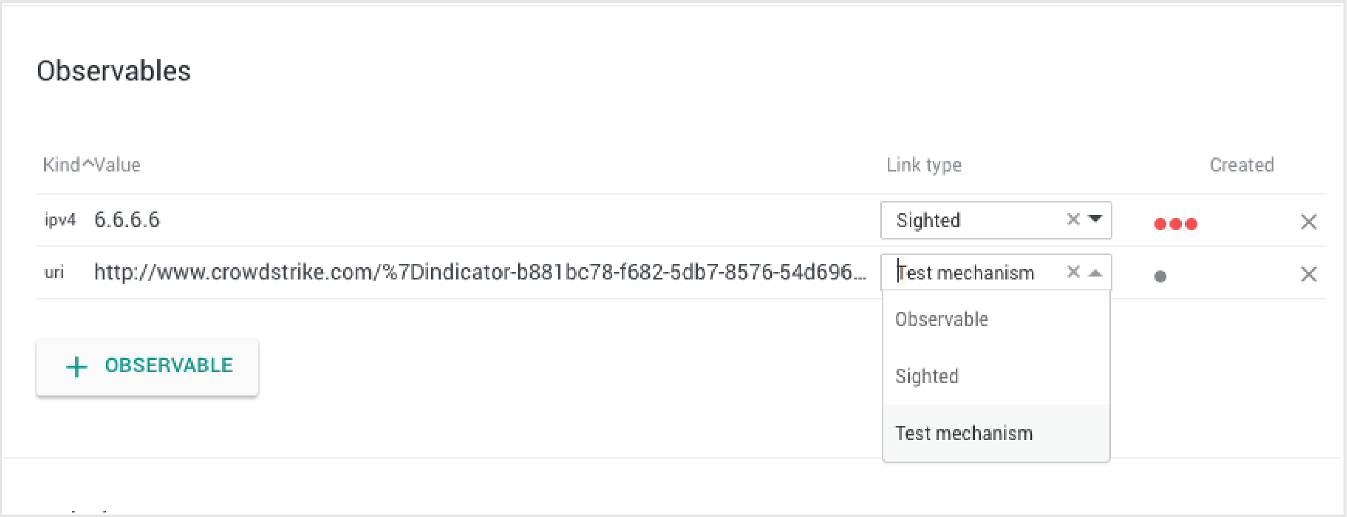
  Named relationships add intelligence value by describing *how* entities and observables are related. This information provides additional context, and it helps understand how a specific resource is used, or the purpose it serves for a potential attacker.
  For example, it can clarify that an observable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



Observables

Kind^Value		Link type	Created
ipv4	6.6.6.6	Sighted	
uri	http://www.crowdstrike.com/%7Dindicator-b881bc78-f682-5db7-8576-54d696...	Test mechanism	

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.