eclectic iq

How-tos for EclecticIQ Platform

Hands-on articles on specific platform features

Last generated: July 21, 2017

Table of contents

How to configure incoming feeds

This summary page gives you an overview of the available how-to and tutorial articles about incoming feeds. They describe how to configure content types, transport types, and all the required options you need to set when you create incoming feeds to ingest cyber threat intelligence into EclecticIQ Platform.

Browse the table for the topics you want to look up.
You can also use the drop-down menu on the left-hand navigation sidebar to access the articles or to go to a different section.

Title	Excerpt
How to configure Anubis Cyberfeed incoming feeds	Set up and configure AnubisNetworks Infections Detection Cyberfeed incoming feeds.
How to configure BFK incoming feeds	Set up and configure transport and content types for BFK incoming feeds to retrieve and process reports on cyber threats and activities, as well as information on NIDs (Network Intrusion Detections).
How to configure Crowdstrike Falcon Intelligence Indicator incoming feeds	Set up and configure transport and content types for Crowdstrike Falcon Intelligence Indicator incoming feeds to retrieve and process information on indicators, such as compromised devices, malicio...
How to configure Group-IB accounts incoming feeds	Set up and configure Group-IB accounts incoming feeds.
How to configure Group-IB cards incoming feeds	Set up and configure Group-IB cards incoming feeds.
How to configure Group-IB IMEIs incoming feeds	Set up and configure Group-IB IMEIs incoming feeds.
How to configure Intel 471 incoming feeds	Set up and configure Intel 471 incoming feeds.
How to configure EclecticIQ JSON incoming feeds	Set up and configure EclecticIQ JSON incoming feeds.
How to configure PDF incoming feeds	Set up and configure PDF incoming feeds.
How to configure STIX incoming feeds	Set up and configure STIX 1.0, 1.1, 1.1.1 and 1.2 incoming feeds.
How to configure text incoming feeds	Set up and configure plain text incoming feeds.

Title	Excerpt
How to configure ThreatGRID incoming feeds	Set up and configure ThreatGRID incoming feeds.
How to configure Threat Recon incoming feeds	Set up and configure Threat Recon incoming feeds.
How to split MISP STIX packages	Split MISP STIX packages into their corresponding embedded STIX packages by using the splitter command line utility.

How to configure Anubis Cyberfeed incoming feeds

Set up and configure AnubisNetworks Infections Detection Cyberfeed incoming feeds.

This article describes how to configure **Anubis Cyberfeed** incoming feeds for ingestion into EclecticIQ Platform.

This intel provider/intel source enables intelligence ingestion through the following channels:

Feed	Ingested data	Processed data
Infection detection Bank Trojans	Metadata from communication involving Trojan-infected machines.	An ID reference to the TTP containing information on the identified Trojan family.
		An indicator related with ID reference to the TTP, containing the Command and Control system address as server name or server address, as well as the first and last time the threat was sighted.
		A sighting related to the indicator, containing the IP address or the domain name of the compromised machine, HTTP request details like request method, cookies, HTTP user agent, the client IP address passed on to the server via a XFF HTTP header, any additionl arguments, as well as the first and last time the threat was sighted.
Infection detection DNS malware	Metadata from communication involving Trojan-infected DNS servers.	An ID reference to the TTP containing information on the identified Trojan family.
		An indicator related with ID reference to the TTP, containing the Command and Control system address as server name or server address.
		A sighting related to the indicator, containing the IP address of the compromised machine, and the **DNS query type** `(https://en.wikipedia.org/wiki/list_of_dns_record_types)`.
Compromised systems website analysis	Indicators of compromise concerning malware-infected web sites.	An indicator with the malware-targeted URL, a description, any available behavior signatures, as well as the first and last time the threat was sighted.
		Observables for any found IP addresses, domain names, or hashes.
Compromised systems malware analysis	Indicators of compromise concerning analyzed malware samples.	An indicator with details about the malware file, a description, any available behavior signatures, as well as the first and last time the threat was sighted.
		Observables for any found file sizes, file types, or file hashes.

By default, the entities the platform creates after processing the ingested data from Anubis Cyberfeed incoming feeds include the following properties:

Property	Default value	Entities
Confidence	*High*	TTPs, indicators, sightings
Likely impact	*High*	Indicators
Impact	*High*	Sightings

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ➕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **➕ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code**
  `(https://en.wikipedia.org/wiki/admiralty_code)`.

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Anubis Cyberfeed**.

Configure the transport type

Transport type	Allowed content types
Anubis Cyberfeed	Anubis Cyberfeed JSON

Anubis Cyberfeed

The source organization providing the data for the incoming feed is AnubisNetworks. From the **Transport type** drop-down list, select **Anubis Cyberfeed**.

Under **Transport configuration**, configure the following settings:

- **API URL**: the URL pointing to the API endpoint exposing the service that makes the data available for retrieval through the feed. Contact the intel provider of the incoming feed to obtain this information.

- **API key**: contact AnubisNetworks to receive an API key, and then enter it in the corresponding input field.

- **Infection detection bank trojans**: select this checkbox to fetch metadata from data flows between machines compromised with Trojans and the AnubisNetworks sinkhole platform.
  This channel provides information such as IP addresses, Trojan family, request metadata, request payload, and pattern verification.

- **Infection detection DNS malware**: select this checkbox to fetch metadata from DNS servers on Trojans trying to contact the AnubisNetworks sinkhole platform. This information allows to detect potential compromises when Command and Control communication is intercepted before it reaches the recipient Command and Control center.
  This channel provides information such as DNS request details, origin IP addresses, and Trojan family.

- **Compromised systems website analysis**: select this checkbox to fetch metadata to detect compromised web sites and servers on the specifed networks, to detect and profile compromised hosts, and to support mitigation by providing indicators and observables.

- **Compromised systems malware analysis**: select this checkbox to fetch metadata to detect malicious file infections on the specifed networks, and to support mitigation by providing indicators and observables.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure BFK incoming feeds

Set up and configure transport and content types for BFK incoming feeds to retrieve and process reports on cyber threats and activities, as well as information on NIDs (Network Intrusion Detections).

This article describes how to configure **BFK API** incoming feeds for ingestion into EclecticIQ Platform.

This intel provider/intel source enables intelligence ingestion through the following channels:

Feed	Ingested data	Processed data
BFK API	Reports and NIDs (Network Intrusion Detections).	Ingested reports are saved as report entities in the platform, whereas an ingested NID results in an entity with a linked TTP.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.
- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.
- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.
- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.
- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.
- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).
- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **BFK API**.

Configure the transport type

Transport type	Allowed content types
BFK API	BFK Threat Intelligence JSON

BFK API

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data.

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data.
  Contact the intelligence provider to subscribe to the service and to obtain the required authentication and authorization credentials.

- **Polling start time**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.
  The predefined max. amount of days in the past per each query/request is set to 60 days.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure Crowdstrike Falcon Intelligence Indicator incoming feeds

Set up and configure transport and content types for Crowdstrike Falcon Intelligence Indicator incoming feeds to retrieve and process information on indicators, such as compromised devices, malicious domains, hashes, and more.

This article describes how to configure **Crowdstrike Falcon Intelligence Indicator** incoming feeds for ingestion into EclecticIQ Platform.

This intel provider/intel source enables intelligence ingestion through the following channels:

Feed	Ingested data	Processed data
Crowdstrike Falcon Intelligence Indicator	Indicators found in their environment, related to entities such as threat actors or other indicators.	Indicators retrieved from the Falcon Intelligence platform such as compromised devices, malicious domains, hashes, and so on starting from the specified polling date.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.
- On the top-left corner of the page click the ➕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.
- On the ➕ **> Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.
- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.
- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.
- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Crowdstrike Falcon Intelligence Indicator Feed**.

Configure the transport type

Transport type	Allowed content types
Crowdstrike Falcon Intelligence Indicator Feed	Crowdstrike Indicator JSON

Crowdstrike Falcon Intelligence Indicator

- **API ID**: contact Crowdstrike to receive an API ID, and then enter it in the corresponding input field.
  You need a valid API ID and a corresponding API key as authentication credentials to access the Crowdstrike Falcon Intel API and to consume it.

- **API key**: contact Crowdstrike to receive an API key, and then enter it in the corresponding input field.

- **Polling start time**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.
  The predefined max. amount of days in the past per each query/request is set to 60 days.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure Group-IB accounts incoming feeds

Set up and configure Group-IB accounts incoming feeds.

This article describes how to configure **Group-IB accounts** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Group-IB accounts**.

Configure the transport type

Group-IB JSON API

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure Group-IB cards incoming feeds

Set up and configure Group-IB cards incoming feeds.

This article describes how to configure **Group-IB cards** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ● icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`.

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Group-IB cards**.

Configure the transport type

Group-IB JSON API

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** (https://www.us-cert.gov/tlp) color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure Group-IB IMEIs incoming feeds

Set up and configure Group-IB IMEIs incoming feeds.

This article describes how to configure **Group-IB IMEIs** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Group-IB IMEIs**.

Configure the transport type

Group-IB JSON API

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes. You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour. You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day. You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week. You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month. You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu. Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** (https://www.us-cert.gov/tlp) color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed. When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure Intel 471 incoming feeds

Set up and configure Intel 471 incoming feeds.

This article describes how to configure **Intel 471** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ➕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the ➕ **> Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Intel 471**.

⚠ **Warning:** You should set the **Override TLP** option to **Amber** for Intel 471 feed content, since this information should not be redistributed outside the organization.

Configure the transport type

Intel 471 API

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure EclecticIQ JSON incoming feeds

Set up and configure EclecticIQ JSON incoming feeds.

This article describes how to configure **EclecticIQ JSON** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code**
  `(https://en.wikipedia.org/wiki/admiralty_code)`.

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **EclecticIQ JSON**.

Configure the transport type

Transport type	Allowed content types
EclecticIQ JSON	FTP download
	HTTP download
	IMAP email fetcher
	Mount point download
	TAXII inbox
	TAXII poll

FTP download

If the source organization providing the incoming feed supports FTP download, from the **Transport type** drop-down list select **FTP download**.
Under **Transport configuration**, configure the following settings:

- **URL**: the `ftp://` endpoint URL that makes the feed available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **TLS**: select this checkbox if the FTP supports an additional layer for Transport Layer Security. The URL protocol for secure FTP is `ftps://`.

HTTP download

> ⚠️ **Warning:** The HTTP download transport type requires basic access authentication.

If the source organization providing the incoming feed supports HTTP download, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **URL**: the `http://` endpoint URL that makes the feed available for download.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)`.

- **Basic auth username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Basic auth password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Verify connection**: select this checkbox if you want to check the connection before starting downloading the feed.

- **Extra headers**: click the **✚ More** link to define any additional **HTTP headers** (
  `https://en.wikipedia.org/wiki/list_of_http_header_fields`) to send along with a request. Select an HTTP
  header from the drop-down list on the left, and then enter the corresponding value in the input field on the right.

IMAP email fetcher

If the source organization providing the incoming feed supports the email IMAP protocol, from the **Transport type** drop-down list select **IMAP email fetcher**.
Under **Transport configuration**, configure the following settings:

- **Host**: the domain name of the IMAP server handling email traffic for the email address you are going to use for the incoming feed.
  Usually, the standard format is `imap.<server_domain_name>` or `mail.<server_domain_name>`.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Use SSL**: select this checkbox if the email service provider supports Secure Sockets Layer.

- **To keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *To* email field, i.e. the recipient field.

- **From keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *From* email field, i.e. the sender field.

- **Subject keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *Subject* email field, i.e. the email header field.

Mount point download

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point download** option.

Under **Transport configuration**, configure the following settings:

- **Path**: enter the path to the local or network unit where the source data for the incoming feed is stored.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python**
  `(https://docs.python.org/3/library/re.html)` .

TAXII inbox

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII inbox**.

- Under **Transport configuration**, configure the following settings:

  - **Public**: by default, this checkbox is deselected. Select it if you allow access to the incoming feed to all users. Leave the default setting as is to keep the incoming feed private.

  - **Authorized groups**: this option defines the user groups that can access a private feed. If you leave the **Public** checkbox deselected, you need to choose at least one group from the drop-down menu.

TAXII poll

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII poll**.

- Under **Transport configuration**, configure the following settings:

    - **Polling service URL**: enter the URL exposing the service the platform polls to check for updated information in the incoming feed content. Contact the incoming feed service provider to obtain this information.

    - **Collection name**: specify a name to identify the incoming feed.

    - **TAXII version**: select the appropriate version of the TAXII poll service in use; either *1.0* (`https://taxiiproject.github.io/releases/1.0/`) or *1.1* (`https://taxiiproject.github.io/releases/1.1/`).

    - **Subscription URL**: enter the URL exposing the subscription service the platform uses to retrieve incoming feed content. Contact the incoming feed service provider to obtain this information.

    - **Ingest messages starting from**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.

    - **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
    Example:
    `https://<platform.host>/auth`

    - **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

    - **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

    - **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

    - **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.

    - **SSL key password**: enter here the password to unlock the SSL key.

    - **Verify SSL**: select this checkbox to verify the SSL credentials against a CA certificate store.

        - **SSL CA bundle file path**: enter the path to the CA bundle file containing root and intermediate certificates for the SSL authentication.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** (https://www.us-cert.gov/tlp) color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure PDF incoming feeds

Set up and configure PDF incoming feeds.

This article describes how to configure **PDF** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the ✚ **> Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`.

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **PDF**.

Configure the transport type

FTP download

If the source organization providing the incoming feed supports FTP download, from the **Transport type** drop-down list select **FTP download**.
Under **Transport configuration**, configure the following settings:

- **URL**: the `ftp://` endpoint URL that makes the feed available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **TLS**: select this checkbox if the FTP supports an additional layer for Transport Layer Security. The URL protocol for secure FTP is `ftps://`.

HTTP download

> ⚠️ **Warning:** The HTTP download transport type requires basic access authentication.

If the source organization providing the incoming feed supports HTTP download, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **URL**: the `http://` endpoint URL that makes the feed available for download.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)` .

- **Basic auth username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Basic auth password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Verify connection**: select this checkbox if you want to check the connection before starting downloading the feed.

- **Extra headers**: click the ✚ **More** link to define any additional **HTTP headers** (`https://en.wikipedia.org/wiki/list_of_http_header_fields`) to send along with a request. Select an HTTP header from the drop-down list on the left, and then enter the corresponding value in the input field on the right.

IMAP email fetcher

If the source organization providing the incoming feed supports the email IMAP protocol, from the **Transport type** drop-down list select **IMAP email fetcher**.
Under **Transport configuration**, configure the following settings:

- **Host**: the domain name of the IMAP server handling email traffic for the email address you are going to use for the incoming feed.
  Usually, the standard format is `imap.<server_domain_name>` or `mail.<server_domain_name>`.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Use SSL**: select this checkbox if the email service provider supports Secure Sockets Layer.

- **To keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *To* email field, i.e. the recipient field.

- **From keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *From* email field, i.e. the sender field.

- **Subject keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *Subject* email field, i.e. the email header field.

Mount point download

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point download** option.

Under **Transport configuration**, configure the following settings:

- **Path**: enter the path to the local or network unit where the source data for the incoming feed is stored.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)`.

TAXII inbox

> ⚠ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII inbox**.

- Under **Transport configuration**, configure the following settings:

  - **Public**: by default, this checkbox is deselected. Select it if you allow access to the incoming feed to all users. Leave the default setting as is to keep the incoming feed private.

  - **Authorized groups**: this option defines the user groups that can access a private feed. If you leave the **Public** checkbox deselected, you need to choose at least one group from the drop-down menu.

TAXII poll

> ⚠ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII poll**.

- Under **Transport configuration**, configure the following settings:

  - **Polling service URL**: enter the URL exposing the service the platform polls to check for updated information in the incoming feed content. Contact the incoming feed service provider to obtain this information.

  - **Collection name**: specify a name to identify the incoming feed.

  - **TAXII version**: select the appropriate version of the TAXII poll service in use; either *1.0* `(https://taxiiproject.github.io/releases/1.0/)` or *1.1* `(https://taxiiproject.github.io/releases/1.1/)`.

  - **Subscription URL**: enter the URL exposing the subscription service the platform uses to retrieve incoming feed content. Contact the incoming feed service provider to obtain this information.

  - **Ingest messages starting from**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.

  - **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
    Example:
    `https://<platform.host>/auth`

  - **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

  - **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

  - **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

  - **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.

  - **SSL key password**: enter here the password to unlock the SSL key.

  - **Verify SSL**: select this checkbox to verify the SSL credentials against a CA certificate store.

    - **SSL CA bundle file path**: enter the path to the CA bundle file containing root and intermediate certificates for the SSL authentication.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes. You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure STIX incoming feeds

Set up and configure STIX 1.0, 1.1, 1.1.1 and 1.2 incoming feeds.

This article describes how to configure **STIX** version **1.0** `(https://stixproject.github.io/data-model/1.0/)`, **1.1**
`(https://stixproject.github.io/data-model/1.1/)`, **1.1.1** `(https://stixproject.github.io/data-model/1.1.1/)`, and **1.2** `(https://stixproject.github.io/data-model/1.2/)` incoming feeds for ingestion the
EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code**
  `(https://en.wikipedia.org/wiki/admiralty_code)`.

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **STIX 1.0**, **STIX 1.1**, **STIX 1.1.1**, or **STIX 1.2**, depending on the available source data STIX version.

Configure the transport type

FTP download

If the source organization providing the incoming feed supports FTP download, from the **Transport type** drop-down list select **FTP download**.
Under **Transport configuration**, configure the following settings:

- **URL**: the `ftp://` endpoint URL that makes the feed available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **TLS**: select this checkbox if the FTP supports an additional layer for Transport Layer Security. The URL protocol for secure FTP is `ftps://`.

HTTP download

> ⚠ **Warning:** The HTTP download transport type requires basic access authentication.

If the source organization providing the incoming feed supports HTTP download, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **URL**: the `http://` endpoint URL that makes the feed available for download.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)`.

- **Basic auth username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Basic auth password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Verify connection**: select this checkbox if you want to check the connection before starting downloading the feed.

- **Extra headers**: click the ➕ **More** link to define any additional **HTTP headers** (`https://en.wikipedia.org/wiki/list_of_http_header_fields)` to send along with a request. Select an HTTP header from the drop-down list on the left, and then enter the corresponding value in the input field on the right.

IMAP email fetcher

If the source organization providing the incoming feed supports the email IMAP protocol, from the **Transport type** drop-down list select **IMAP email fetcher**.

Under **Transport configuration**, configure the following settings:

- **Host**: the domain name of the IMAP server handling email traffic for the email address you are going to use for the incoming feed.
  Usually, the standard format is `imap.<server_domain_name>` or `mail.<server_domain_name>`.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Use SSL**: select this checkbox if the email service provider supports Secure Sockets Layer.

- **To keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *To* email field, i.e. the recipient field.

- **From keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *From* email field, i.e. the sender field.

- **Subject keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *Subject* email field, i.e. the email header field.

Mount point download

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point download** option.

Under **Transport configuration**, configure the following settings:

- **Path**: enter the path to the local or network unit where the source data for the incoming feed is stored.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)`.

TAXII inbox

> ⚠ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII inbox**.

- Under **Transport configuration**, configure the following settings:

  - **Public**: by default, this checkbox is deselected. Select it if you allow access to the incoming feed to all users. Leave the default setting as is to keep the incoming feed private.

  - **Authorized groups**: this option defines the user groups that can access a private feed. If you leave the **Public** checkbox deselected, you need to choose at least one group from the drop-down menu.

TAXII poll

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII poll**.

- Under **Transport configuration**, configure the following settings:

  - **Polling service URL**: enter the URL exposing the service the platform polls to check for updated information in the incoming feed content. Contact the incoming feed service provider to obtain this information.

  - **Collection name**: specify a name to identify the incoming feed.

  - **TAXII version**: select the appropriate version of the TAXII poll service in use; either *1.0* (`https://taxiiproject.github.io/releases/1.0/`) or *1.1* (`https://taxiiproject.github.io/releases/1.1/`).

  - **Subscription URL**: enter the URL exposing the subscription service the platform uses to retrieve incoming feed content. Contact the incoming feed service provider to obtain this information.

  - **Ingest messages starting from**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.

  - **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
    Example:
    `https://<platform.host>/auth`

  - **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

  - **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

  - **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

  - **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.

  - **SSL key password**: enter here the password to unlock the SSL key.

  - **Verify SSL**: select this checkbox to verify the SSL credentials against a CA certificate store.

    - **SSL CA bundle file path**: enter the path to the CA bundle file containing root and intermediate certificates for the SSL authentication.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure text incoming feeds

Set up and configure plain text incoming feeds.

This article describes how to configure **Text** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **✚ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code**
  (https://en.wikipedia.org/wiki/admiralty_code).

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Text**.

Configure the transport type

FTP download

If the source organization providing the incoming feed supports FTP download, from the **Transport type** drop-down list select **FTP download**.

Under **Transport configuration**, configure the following settings:

- **URL**: the `ftp://` endpoint URL that makes the feed available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **TLS**: select this checkbox if the FTP supports an additional layer for Transport Layer Security. The URL protocol for secure FTP is `ftps://`.

HTTP download

> ⚠ **Warning:** The HTTP download transport type requires basic access authentication.

If the source organization providing the incoming feed supports HTTP download, from the **Transport type** drop-down list select **HTTP download**.

Under **Transport configuration**, configure the following settings:

- **URL**: the `http://` endpoint URL that makes the feed available for download.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)` .

- **Basic auth username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Basic auth password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

- **Verify connection**: select this checkbox if you want to check the connection before starting downloading the feed.

- **Extra headers**: click the ✚ **More** link to define any additional **HTTP headers** (`https://en.wikipedia.org/wiki/list_of_http_header_fields)` to send along with a request. Select an HTTP header from the drop-down list on the left, and then enter the corresponding value in the input field on the right.

IMAP email fetcher

If the source organization providing the incoming feed supports the email IMAP protocol, from the **Transport type** drop-down list select **IMAP email fetcher**.

Under **Transport configuration**, configure the following settings:

- **Host**: the domain name of the IMAP server handling email traffic for the email address you are going to use for the incoming feed.
  Usually, the standard format is `imap.<server_domain_name>` or `mail.<server_domain_name>`.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the designated email inbox to fetch the incoming feed from..

- **Use SSL**: select this checkbox if the email service provider supports Secure Sockets Layer.

- **To keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *To* email field, i.e. the recipient field.

- **From keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *From* email field, i.e. the sender field.

- **Subject keyword**: you can enter a keyword to filter feed text content, and to return only the parts that contain the specified term.
  The keyword defined here targets the *Subject* email field, i.e. the email header field.

Mount point download

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point download** option.

Under **Transport configuration**, configure the following settings:

- **Path**: enter the path to the local or network unit where the source data for the incoming feed is stored.

- **Regex pattern**: you can define a regular expression to filter the text content in the feed, and to return only the parts that match the regex pattern. This field accepts normal regex syntax like the one **supported in Python** `(https://docs.python.org/3/library/re.html)`.

TAXII inbox

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII inbox**.

- Under **Transport configuration**, configure the following settings:

  - **Public**: by default, this checkbox is deselected. Select it if you allow access to the incoming feed to all users. Leave the default setting as is to keep the incoming feed private.

  - **Authorized groups**: this option defines the user groups that can access a private feed. If you leave the **Public** checkbox deselected, you need to choose at least one group from the drop-down menu.

TAXII poll

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.

- If the source organization providing the incoming feed makes the data available via a TAXII inbox service, from the **Transport type** drop-down list select **TAXII poll**.

- Under **Transport configuration**, configure the following settings:

  - **Polling service URL**: enter the URL exposing the service the platform polls to check for updated information in the incoming feed content. Contact the incoming feed service provider to obtain this information.

  - **Collection name**: specify a name to identify the incoming feed.

  - **TAXII version**: select the appropriate version of the TAXII poll service in use; either *1.0* (`https://taxiiproject.github.io/releases/1.0/`) or *1.1* (`https://taxiiproject.github.io/releases/1.1/`).

  - **Subscription URL**: enter the URL exposing the subscription service the platform uses to retrieve incoming feed content. Contact the incoming feed service provider to obtain this information.

  - **Ingest messages starting from**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.

  - **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
    Example:
    `https://<platform.host>/auth`

  - **Username**: a valid user name to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

  - **Password**: a valid password to authenticate and be granted the necessary authorization to access the data source and to download/ingest data..

  - **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

  - **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.

  - **SSL key password**: enter here the password to unlock the SSL key.

  - **Verify SSL**: select this checkbox to verify the SSL credentials against a CA certificate store.

    - **SSL CA bundle file path**: enter the path to the CA bundle file containing root and intermediate certificates for the SSL authentication.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes. You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour. You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day. You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week. You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month. You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu. Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure ThreatGRID incoming feeds

Set up and configure ThreatGRID incoming feeds.

This article describes how to configure **ThreatGRID** incoming feeds for ingestion into EclecticIQ Platform.

This intel provider/intel source enables intelligence ingestion through the following channels:

Feed	Ingested data
banking-dns	Banking Trojan network communications: (meta)data from communication involving Trojan-infected machines.
dll-hijacking-dns	Data obtained from the analysis of samples leveraging DLL sideloading and/or hijacking techniques
doc-net-com-dns	Document (PDF, Office) network communications: (meta)data from communication involving infected document files.
downloaded-pe-dns	Data obtained from the analysis of samples downloading executables over the network.
dynamic-dns	Data obtained from the analysis of samples leveraging dynamic DNS providers.
irc-dns	Data obtained from Internet Relay Chat (IRC) network communications.
modified-hosts-dns	Information about modified Windows hosts files.
parked-dns	Information about parked domains resolving to **RFC1918** `(https://tools.ietf.org/html/rfc1918)`, localhost and broadcast addresses.
public-ip-check-dns	Check For Public IP Address Network Communications.
ransomware-dns	Data obtained from the analysis of samples communicating with ransomware servers.
rat-dns	Information about remote access Trojans (RAT), and any communications with their Command and Control systems.
sinkholed-ip-dns	DNS entries obtained from the analysis of samples communicating with known DNS sinkholes.
stolen-cert-dns	DNS entries observed in samples signed with a stolen certificate.

The ingested data produce indicators with embedded observables, where each observable represents an indicator of compromise (IOC).

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.
- On the top-left corner of the page click the ⊕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **+ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code**
  `(https://en.wikipedia.org/wiki/admiralty_code)`.

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **ThreatGRID**.

Configure the transport type

ThreatGRID API

- **API URL**: the URL pointing to the API endpoint exposing the service that makes the data available for retrieval through the feed. Contact the intel provider of the incoming feed to obtain this information.

- **API key**: contact Cisco to receive an API key, and then enter it in the corresponding input field.

- **Feed type**: from the drop-down menu select the data source you want the incoming feed to retrieve data from. The available channels are:

  - **Banking Trojan Network Communications**

  - **Feed contains Domains communicated to by samples leveraging DLL Sideloading and/or hijacking techniques**

  - **Document (PDF, Office) Network Communications**

  - **Samples Downloading Executables Network Communications**

  - **Samples Leveraging Dynamic DNS Providers**

  - **Internet Relay Chat (IRC) Network Communications**

  - **Modified Windows Hosts File Network Communications**

  - **Parked Domains resolving to RFC1918, Localhost and Broadcast Addresses**

  - **Check For Public IP Address Network Communications**

  - **Samples Communicating with Ransomware Servers**

  - **Remote Access Trojan (RAT) Network Communications**

  - **DNS entries for samples communicating with a known dns sinkhole**

  - **DNS Entries observed from samples signed with a stolen certificate**

- **Ingest feed starting from**: select a date if you want to fetch content from the intel provider/data source starting from a specific date in the past.
  If you do not specify any start date, the default start date is 6 months in the past. This means that if you leave this field empty, the incoming feed will fetch data as old as 6 months until the present time.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to configure Threat Recon incoming feeds

Set up and configure Threat Recon incoming feeds.

This article describes how to configure **Threat Recon** incoming feeds for ingestion into EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

- On the top navigation bar, select **Configuration**, and then **Incoming feeds**.

- On the top-left corner of the page click the ➕ icon to open the incoming feed editor.

The **Incoming feeds** page displays an overview of the configured incoming feeds ingesting data from the specified intel providers and data sources.

- On the top-right corner of the screen, click the **+ Incoming feed** button.

- On the **➕ > Data management > Incoming feeds > Create** form you can populate the input fields to define the intel provider/data source for the feed, and the feed behavior.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- Under **Organization**, enter a name for the organization that serves as the intel provider for the incoming feed.

- Use **Source reliability** to flag the incoming feed with a value from the drop-down list to help oher users assess how trustworthy the feed source is deemed to be.
  This value has the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).

- **Extraction ignore levels**: from the drop-down menu select at least one option if you want to *exclude extracted content* from the ingested data.
  If you select at least one value, the filter excludes extracted data from ingestion, based on the direct or indirect relationship the data has with the entity it refers to.
  In other words, the filter ignores specific data, based on the data location in the entity data structure:

  - **Extraction ignore levels — 1**: the extracted data is inside a CybOX object. The ingestion process ignores and it does not include extracted data found inside observable CybOX objects embedded in STIX indicators.

  - **Extraction ignore levels — 2**: the extracted data is outside a CybOX object. The ingestion process ignores and it does not include extracted data found inside STIX fields. For example, STIX headers, titles or references.

- From the **Transport type** drop-down list, select **Threat Recon**.

Configure the transport type

Threat Recon JSON API

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

Override TLP overwrites the **TLP** (https://www.us-cert.gov/tlp) color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

Set half-life values

It represents the amount of time it takes an entity to lose half its intelligence value.
It corresponds to the number of days it takes the intelligence value of a malicious entity to decay by 50%.

When configuring an incoming or an outgoing feed, you can set a half-life value in days for the following entity properties:

- **Campaign**

- **Course of action**

- **Exploit target**

- **Incident**

- **Indicator**

- **TTP**

- **Threat actor**

- **Report**

To set a half-life for one or more of these properties, do the following::

- Enter a numerical value in the entity property input field(s) you want to flag with a half-life value in days.

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

Save options

Besides committing 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 creation work.

How to split MISP STIX packages

Split MISP STIX packages into their corresponding embedded STIX packages by using the splitter command line utility.

Issue

MISP XML files usually include multiple STIX XML packages. Each embedded STIX package holds data defining an entity object. The parent MISP XML file serves as a container for the embedded STIX packages. When a MISP XML file holds a large number of STIX packages, it may cause ingestion errors.

To address this issue and to correctly ingest all the valid STIX content, you can split the source MISP XML package into its constituent embedded STIX packages. This process removes the MISP XML container layer, and it outputs one XML file per STIX XML sub-package. The resulting STIX XML packages can then be ingested and processed by the platform.

Solution

The EclecticIQ Platform ships with a command line utility that splits the embedded STIX packages into separate XML files: `split-misp-stix-packages`.

The `split-misp-stix-packages` script is in the `.../platform-api/scripts` directory.

To run the script correctly, follow these recommendations:

- You need to run `split-misp-stix-packages` from within the CentOS virtual environment the platform runs on. Currently supported: **CentOS Linux 7 (1511)** `(https://lists.centos.org/pipermail/centos-announce/2015-december/021518.html)`.

- Explicitly point to the Python interpreter inside the virtual environment.
  Example:

```
# Python interpreter included with the
# virtual environment the platform runs on.
/opt/.../platform-api/venv/bin/python

# Directory in the platform virtual environment where the
# MISP XML splitter is located.
/opt/.../platform-api/scripts/split-misp-stix-packages
```

Usage

To view the built-in help, run the following command(s):

```
# Enter this command:
$ split-misp-stix-packages --help

# The help is displayed:
Usage: split-misp-stix-packages [OPTIONS] FILE.xml

Options:
  --output-directory DIRECTORY  Output directory  [required]
  --output-base-name TEXT       File name template to be used for output files
  --debug
  --help                        Show this message and exit.
```

Option	Description
`--output-directory`	*Required* — Defines the file splitter output directory the embedded STIX packages are saved to after extracting them from the MISP XML wrapper.
`--output-base-name`	*Optional* — By default, STIX packages are named `package-<int>.xml`, where `<int>` is a sequentially progressive numeric value starting at zero. If you want, you can specify a different name than `package`. It is not possible to modify the hyphen or the numeric part of the file name.
`--debug`	*Optional* — In case of errors, you can use this option to return a verbose output.
`--help`	*Optional* — Displays the built-in help.

Example

In this example, we are using the following dummy names for files and directories:

- `<platform_virtual_environment_username>`: user name to access the CentOS virtual environment the platform runs on. Currently supported: **CentOS Linux 7 (1511)** `(https://lists.centos.org/pipermail/centos-announce/2015-december/021518.html)`.

- `<platform_virtual_environment_password>`: password to access the CentOS virtual environment the platform runs on. Currently supported: **CentOS Linux 7 (1511)** `(https://lists.centos.org/pipermail/centos-announce/2015-december/021518.html)`.

- `misp-out misp-stix-package.xml`: example MISP XML file to extract the embedded STIX packages from.

- `temp`: directory where the source `misp-out misp-stix-package.xml` file is temporarily stored.

- `misp-out`: output directory where the embedded STIX packages, originally in the MISP XML file, are saved as separate XML files.

These are the main steps:

- To successfully execute several commands in the command line or in the terminal, you may need root-level access rights.
  To obtain admin rights, run the following command(s):

```
$ sudo su -
```

Alternatively:

- Grant admin rights to a specific user, who can then log in with their password to perform admin tasks:

```
$ su - {user_name}
```

Or:

- Prefix `sudo` to the command you want to run:

```
$ sudo {command}
```

- Create an output directory where the STIX packages can be saved as separate XML files.
- Go to the directory where the MISP XML file you want to split is located.
- Run the file splitter utility.

```
# SSH authentication in the EclecticIQ Platform virtual environment.
$ sudo su <platform_virtual_environment_username>
password: <platform_virtual_environment_password>

# Create a new directory; the MISP XML sub-packages will be saved here.
$ mkdir misp-out

# Go to the directory where you saved to source MISP STIX XML package.
# Example: "temp".
$ cd temp

# Run the split utility tool. Specify:
# - The output directory for the split sub-packages.
# - The source MISP STIX XML package you want to split.
$ split-misp-stix-packages --output-directory misp-out misp-stix-package.xml

# Log message at the end of a successful operation,
# where "%d" is an integer.
%d output files written
```

How to 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 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 look 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

> ✔ On the forms, 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 **✚ > 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 of the following 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. `data` is the default root of any JSON path expression defined here.
  The `data` root is implied. To point to the title or to the description fields of an entity, you only need to enter `title` or `description`, instead of `data.title` or `data.description`.

- **Content > Path**: based on the specified JSON path, the rule searches for a corresponding match in the JSON data structure representing entities in the platform.

  The JSON path root is the `data` field.
  The JSON path is a string that points to a location, that is, a field inside a JSON object. It tells the rule *where* in the entity structure it should go look for the corresponding data value.
  Think of it as a friend's address you scribble on the back of a postcard before dropping it into the mailbox.

  The JSON path format is a string where dots (`.`) define JSON parent-child relationships.
  Do not include square brackets (`[ ]`) in the path input: they are stripped during execution. It is not possible to use square brackets to point to specific array members.
  Wildcards are currently not supported.

  Examples:

  - Input string pattern example: `related_extracts.value`

  - The path matching the specified pattern points to any `value` key in the following array:

```
{
  "data": {

    "related_extracts": [

      {
        "kind": "domain",
        "value": "robohelptesting.biz"
      },

      {
        "kind": "ipv4",
        "value": "195.22.28.199"
      },

      {
        "kind": "ipv4",
        "value": "188.200.164.50"
      }
    ]

  }
}
```

💡 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 a regex to specify the data pattern the rule should apply to search for the desired content.

The regex tells the rule *what* to look for at the location the JSON path points to.
Think of it as the front of the postcard you're sending to a friend, the side with the picture of a very stereotypical landscape that can match a number of actual places.

Value 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 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 creation 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.

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.

> ✔ On the forms, 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 or 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@yahoo.com*
  - Skype: *<a_valid_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

Editor > Create ttp 👤

TTP

Title *

Money mule related to IBAN NLING000123456789

Analysis

Money mule seems to be receiving regular money transfers from IBAN NLING000123456789

Confidence *

High   ×   ▼

Intended effects *

× Fraud   ×   ▼

Targeted Victim ✕

Name

IBAN NL30INGB0123456789

Specification

Account ✕

Account type

Bank account

Account status

Active

Account specification (5)

✕

Type *

Account ID   ✕ ▾

Value *

NL30INGB0123456789

✕

Type *

Issuing Authority   ✕ ▾

Value *

ING Bank

✕

Type *

Account Type   ✕ ▾

Value *

Debit

✕

Type *

Account Branch   ✕ ▾

Value *

Utrecht center local branch

Specification

Account ✕

Account type

Account status

Account specification

+ add

Account specification

Type *

Please select one ▾

Value *

+ more

How to organize tags with taxonomies

The Taxonomy page displays an overview of the tags used to label entities in the platform. Besides using tags to organize entities, you can design taxonomies to structure the tags, and to create a controlled tag corpus to improve information retrieval.

Taxonomies are structured categories. Taxonomies make it easier for you to organize and maintain content, and they help other users find what they are looking for. They provide a hierarchical framework to structure tags and to describe parent-child relationships between tagged topics. Tag relationships provide a reference grid that makes content easier to navigate and to retrieve.

The main benefits of implementing a taxonomy are:

- Label information in a structured way to make it easier to navigate and to retrieve.

- Provide a reference framework to control entity tagging in the platform, so that tags remain meaningful and consistent.

- Deliver more accurate search results.

The Taxonomy feature

Platform taxonomies enable you to define specific categories to organize tagged entities. Besides the predefined ones, you can create as many taxonomies as you need to make it easier for users to discover meaningful information in the platform data corpus.

Predefined taxonomies

EclecticIQ Platform ships with the following predefined taxonomy sets:

- *Admiralty code*: based on the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`, it helps assess and categorize the reliability of a data source, and the accuracy of the information obtained through a data source.

- *Kill chain phases*: describes the different stages of an attack or an intrusion. By doing so, it helps identify the point(s) in the **kill chain** `(http://www.net-security.org/article.php?id=2220&p=1)` where it is possible to intervene with a mitigation action.

Admiralty code

Use the **Admiralty code** `(https://en.wikipedia.org/wiki/admiralty_code)` taxonomy to label entities with tags that define the level of reliability of the data source and the level of accuracy of the entity information. The Admiralty code taxonomy makes it easier to filter entities and information based on criteria such as relevance and credibility. It provides intuitive guidance to retrieve reliable and accurate information more easily, while leaving out unwanted data noise.

Data source reliability	Data accuracy
Completely reliable	Confirmed by other sources
Usually reliable	Probably True
Fairly reliable	Possibly True
Not usually reliable	Doubtful
Reliability cannot be judged	Improbable
Unreliable	Truth cannot be judged
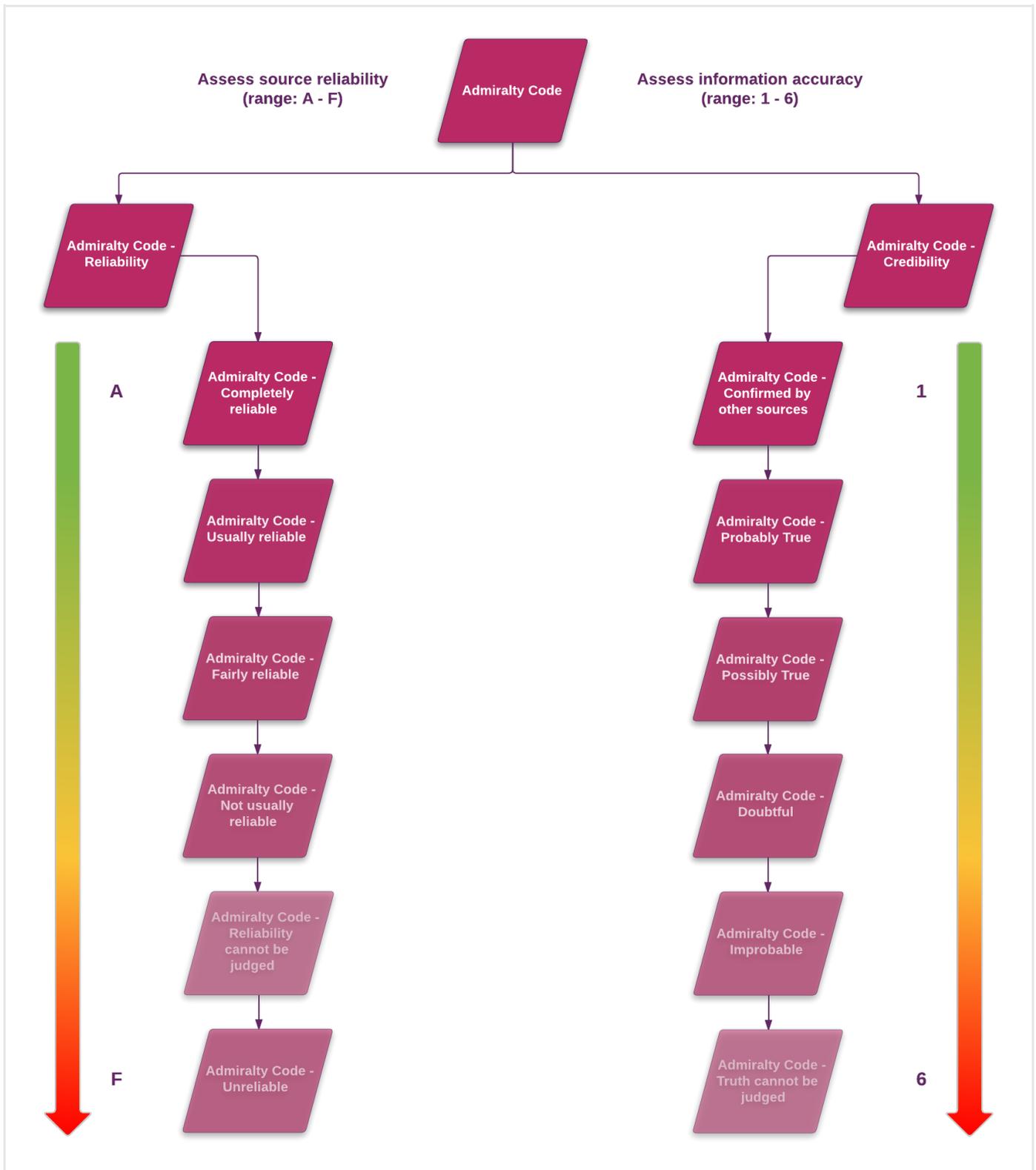
Kill chain

In the context of cyber threat defense, a **kill chain** `(https://en.wikipedia.org/wiki/kill_chain)` aims at encouraging proactive defense, and at implementing adequate courses of action as early as possible in the chain.

The kill chain provides a structured model to:

- Break down the actions of an adversary. This helps understand the TTPs the adversary is implementing.

- In case of an ongoing attack or intrusion, identify the current stage of the intrusion and quantify damage.

- Inspect the kill chain to identify the root cause of the attack or the intrusion.

- Plan a defensive course of action to neutralize the adversary.

Kill chain phase	Description
Reconnaissance	Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.
Weaponization	Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.
Delivery	Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.
Exploitation	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.
Installation	Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
Command and Control (C2)	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.
Actions on Objectives	Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

(Source: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* `(http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/lm-white-paper-intel-driven-defense.pdf)`, by Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D. Paper presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011.

Course of action	Description
Detect	Example: use analytics, auditing, logging tools, and intrusion detection systems (IDS) to detect the intrusion.
Deny	Example: use patching, firewall rules, access control lists (ACL), and intrusion prevention systems (IPS) to deny exploitation.
Disrupt	Example: use data execution prevention (DEP) and intrusion prevention systems to block or otherwise disturb exploitation.

Course of action	Description
Degrade	Example: use queuing or a tarpit to hinder or otherwise reduce exploitation.
Deceive	Example: use DNS redirection or a honeypot to divert exploitation to a decoy.
Destroy	Take control of the attacker's system to neutralize it.
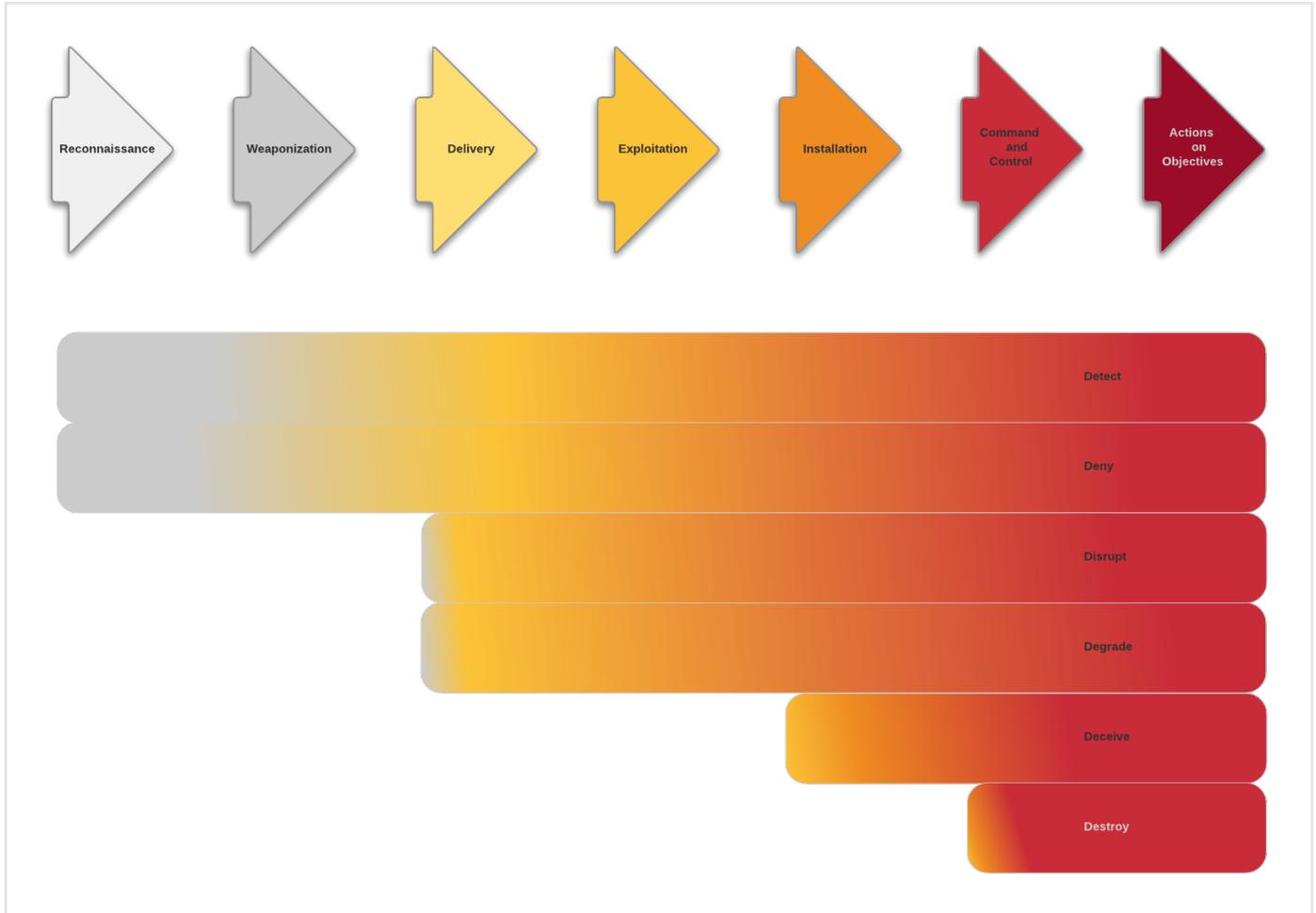
Create a taxonomy entry

✔ On the forms, input fields marked with an asterisk are required.

To create a new taxonomy entry to categorize entity tags, do the following:

- On the top navigation bar click **✚ > Data management > Taxonomy** .

Alternatively:

- On the top navigation bar click **✿ > Data management > Taxonomies > ✚ Taxonomy**.

- On the **Data management > Taxonomy > Create** page, fill out the input fields to define the new taxonomy entry:

  - **Name**: enter a name for the taxonomy entry. The name you specify here corresponds to the tag name you can assign to entities.

  - **Description**: enter a short explanation of what the entry represents or refers to.

  - **Parent**: you can structure taxonomy entries hierarchically by flagging them as either *parent* top-level entries, or subordinate *child* entries.

    - To create a parent entry, leave the field empty.

    - To create a child entry, from the drop-down menu select the parent entry you want to relate the child to. A child taxonomy entry can be the parent of another child entry nested one level beaneath.

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

Save options

Besides committing 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 creation work.

Edit a taxonomy entry

You can edit only user-created, custom taxonomy entries. You cannot edit the predefined Admiralty code and Kill chain taxonomies.

To edit an existing taxonomy entry, do the following:

- On the top navigation bar click ✿ **> Data management > Taxonomies** .
  The **Data management > Taxonomy** page displays an overview of the existing entries.
  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.

- On the overview table, click the ⋮ icon.

- From the drop-down menu select **Edit**.

NAME ∧	DESCRIPTION	PARENT	LAST MODIFIED	
Kill chain phase - Command and Control		Kill Chain Phases	01/26/2016	
Kill chain phase - Actions on Objectives		Kill Chain Phases	01/26/2016	
Ketchup	Test taxonomy entry - child	Vegetable	Today at 12:31 PM	⋯
Free_Form	Form		Yesterday at 9:14	Edit
For_dude_2	Desc	For_dude	02/01/2016	Delete

- On the **Data management > Taxonomy > Edit** page, edit the name, the description, or the parent-child hierarchy relationship as needed.

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

Delete a taxonomy entry

You can delete only user-created, custom taxonomy entries. You cannot delete the predefined Admiralty code and Kill chain taxonomies.

To delete an existing taxonomy entry, do the following:

- On the top navigation bar click ✿ **> Data management > Taxonomies** .
  The **Data management > Taxonomy** page displays an overview of the existing entries.
  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.

- On the overview table, click the ⋮ icon.

- From the drop-down menu select **Delete**.

NAME ▲	DESCRIPTION	PARENT	LAST MODIFIED	
Kill chain phase - Command and Control		Kill Chain Phases	01/26/2016	
Kill chain phase - Actions on Objectives		Kill Chain Phases	01/26/2016	
Ketchup	Test taxonomy entry - child	Vegetable	Today at 12:31 PM	•••
Free_Form	Form		Yesterday at 9:14 F	Edit Delete
For_dude_2	Desc	For_dude	02/01/2016	

- On the confirmation pop-up dialog, click **Delete** to confirm the action.

- The taxonomy entry is deleted.

If you delete a taxonomy entry that is a parent to one or more children entries, the children related to the removed parent remain available in the taxonomy. However, they lose the parent-child relationship, and they become top-level taxonomy entries.

How to work with relationships

The Neighborhood tab in the entity detail pane includes a small graph canvas showing close relationships of the entity to other entities, as well as related observables, datasets, workspaces, and tasks.

Go to the Neighborhood graph

During an analysis you may want to quickly inspect an entity to check relationships with other entities and observables. Normally, you would load the selected entity onto the graph, open the graph, and proceed with the inspection.

Without leaving the entity detail pane, the **Neighborhood** tab offers a faster alternative: click it to see a small graph displaying close-range relationships the entity has with nearby entities and observables.
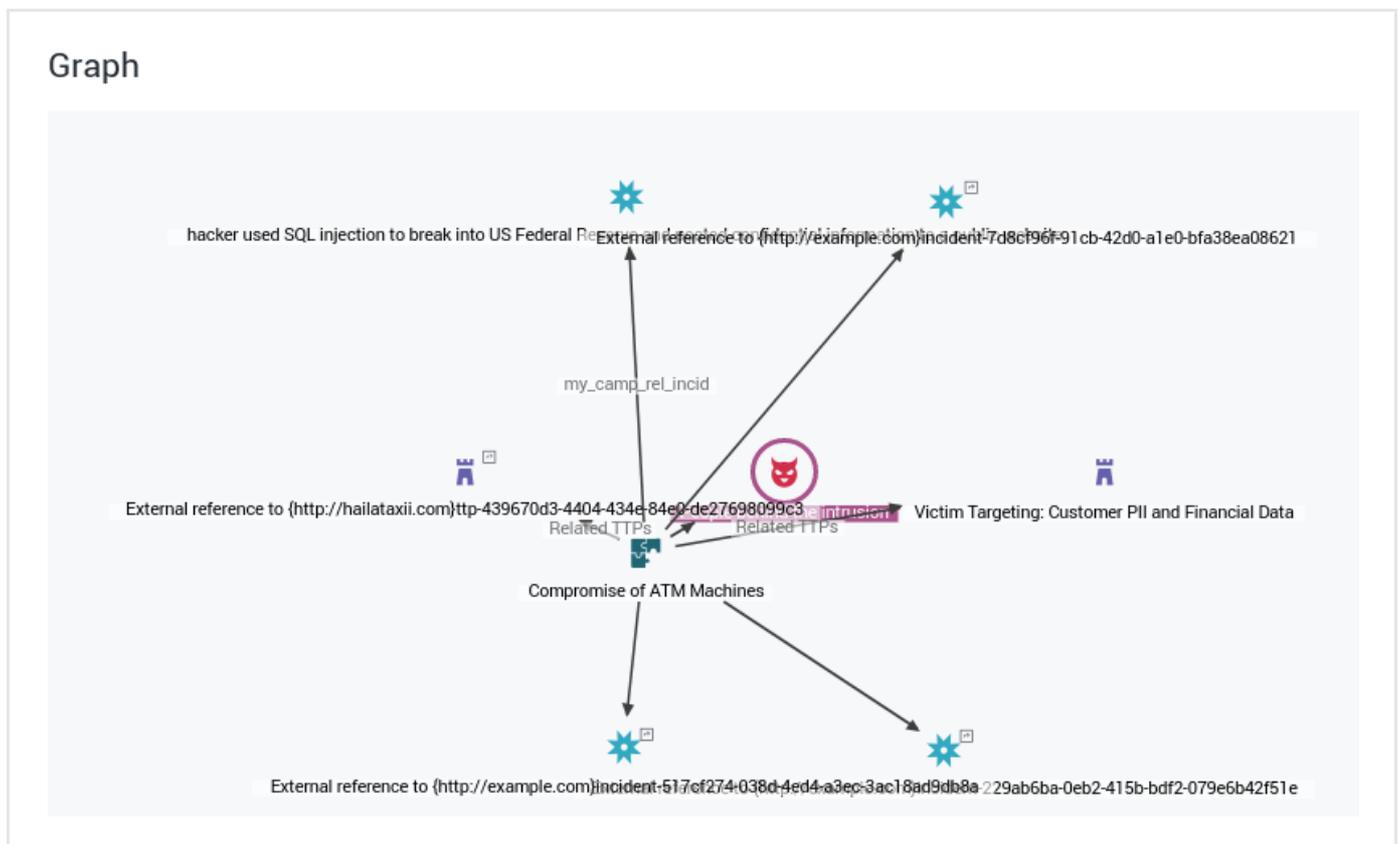
Click the embedded graph to load the entity and its neighborhood relationships onto the graph canvas, where you can further analyze the data.

The **Neighborhood** graph focuses on the immediate context around the entity. If the entity has more than 100 relationships, the **Neighborhood** graph displays only the 30 most recently created relationships. In this case, a notification message is displayed to inform the user:

> ℹ Too many items to show, showing only most relevant 30 items.

OVERVIEW   OBSERVABLES   **NEIGHBORHOOD**   JSON   VERSIONS   HISTORY

Graph
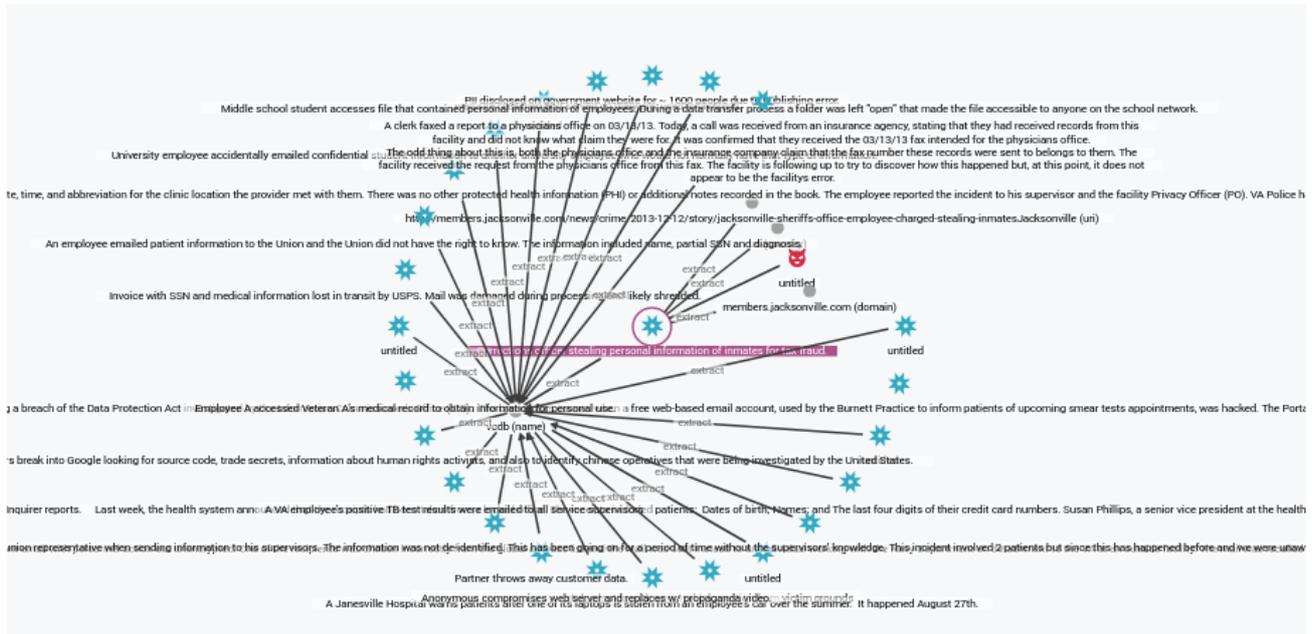
⚠ Too many items to show, showing only most relevant 30 items.   ✕

The embedded graph is a snapshot of the graph canvas view. The embedded snapshot is refreshed when accessing the **Neighborhood** tab, but it is not updated in real time. When the entity relationship landscape changes, for example, after adding or removing relationships, the embedded graph is not in sync anymore. In this case, a notification message is displayed to inform the user:

ℹ DATA PROCESSING IN PROGRESS — It may take some time before the latest entity data is available in the graph.
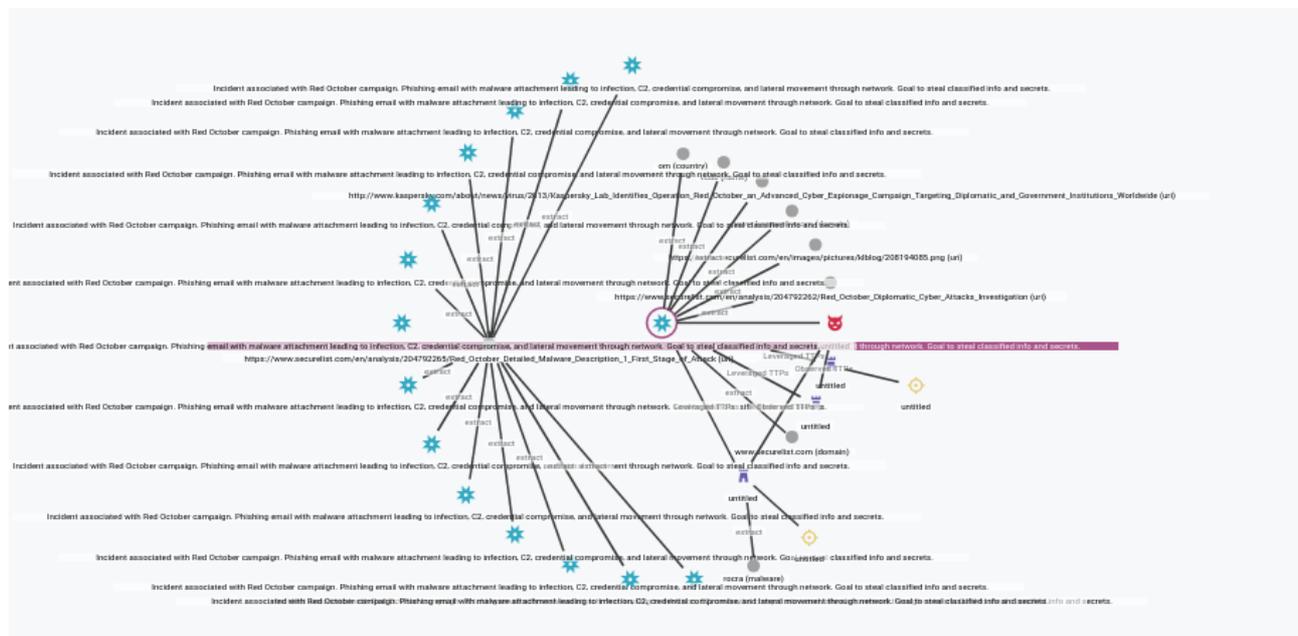
After the platform graph completes indexing, the embedded graph is back in sync. The time this task requires varies, depending on the size of the graph queue.

Explore the entity neighborhood

View relationships

On the graph view you can inspect any relationships the entity may have with other entities and observables in the platform. Relationships can be *direct* — the entities and/or observables are immediately related to each other — as well as *indirect* — the entities and/or observables are related through a shared entity or a shared observable.
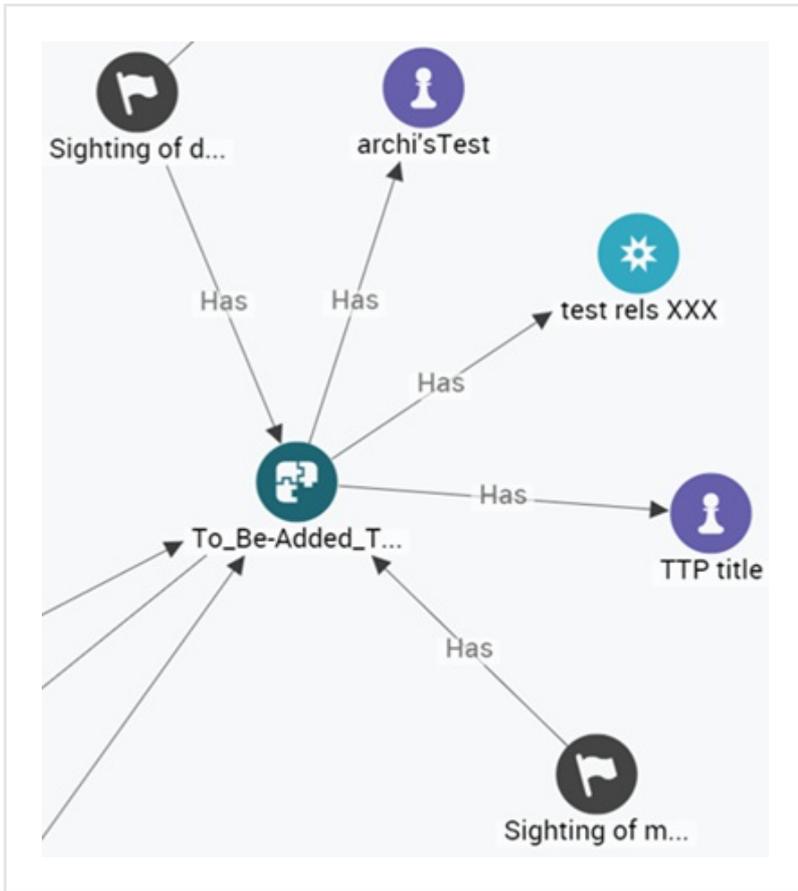
Entities with direct relationships
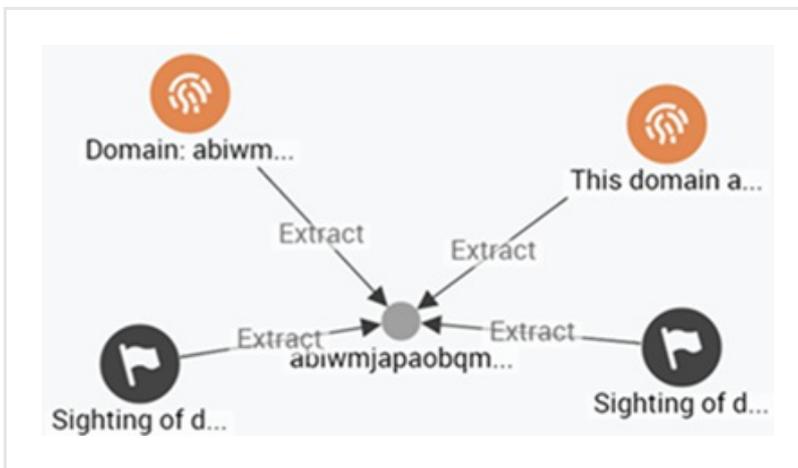
Entities with indirect relationships

To visually examine the entity more closely, click the small graph to launch the larger and feature-richer   graph.

Directly related entities

This section displays entities that are directly related to the active entity.
You can see the entity the current entity is related to, the relationship type, and the relationship direction, that is, if it
outgoing (from the current entity to the related one) or incoming (from the related entity to the current one).

Click an entity name to display the corresponding detail pane in full page format.
To edit entity relationships, click **Edit relationships**.

DIRECTLY RELATED ENTITIES

TITLE	TLP	INGESTED	⟳
⊕ Test_Exploit		09/10/2016 6:07 PM	
⊕ Heartbleed		08/18/2016 10:00 PM	
👤 Targeting: WhatsApp	○ White	09/16/2016 3:57 AM	
👤 External reference to {http:...	○ White	09/16/2016 3:59 AM	

Edit relationships

Entities related through observables

This section displays entities that are indirectly related to the active entity, that is, the relationship exists through an intermediate entity or observable.
Each entry reports entity name, entity TLP color code, if available, and entity ingestion time.
Click an entity name to display the corresponding detail pane in full page format.

ENTITIES RELATED THROUGH EXTRACTS

TYPE	TLP	INGESTED
🔘 This domain annoncodeal.com has been identifi	○ White	09/06/2016 2:04 AM
🔘 This domain thebodyclinic.com.sg has been ider	○ White	09/06/2016 2:04 AM
🔘 This domain fabsthings.com has been identified	○ White	09/06/2016 2:03 AM
🔘 This domain banchifutbol.com has been identifie	○ White	09/06/2016 2:03 AM
🔘 This domain cz.windowsswebs.com has been id	○ White	09/06/2016 2:00 AM
🔘 This domain promocaocartaoespecial.com has k	○ White	09/06/2016 1:59 AM
🔘 This domain acetraveljobs.com has been identifi	○ White	09/06/2016 1:57 AM
🔘 This domain cdinterior.com.sg has been identifie	○ White	09/06/2016 1:55 AM
🔘 This domain olangco.com has been identified as	○ White	09/06/2016 1:54 AM
🔘 This domain gma.gmail-act4024.com has been i	○ White	09/06/2016 1:53 AM

Edit relationships

You can update the entity information by adding and removing relationships. To do so, do the following:

- Under **Directly related entities** click **Edit relationships**.

- 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**.

- From the **Source** drop-down menu, select a data source for the entity or entities you are relating to the current one.
  You can select only one data source at a time, regardless the number of entities you choose on the **Search an entity** dialog.

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

- 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.

Edit relationships for a campaign

Select this menu option…	… to create this relationship
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.

Select this menu option…	… to create this relationship
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.

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

Edit relationships for a course of action

Select this menu option…	… to create this relationship
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
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.

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

Edit relationships for an exploit target

Select this menu option…	… to create this relationship
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.

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

Edit relationships for an incident

Select this menu option…	… to create this relationship
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.

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

Edit relationships for an indicator

Select this menu option…	… to create this relationship
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.

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

Edit relationships for a report

Select this menu option…	… to create this relationship
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.
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.

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

Edit relationships for a sighting

Select this menu option…	… to create this relationship
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.
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.

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

Edit relationships for a threat actor

Select this menu option…	… to create this relationship
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.
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.

Select this menu option…	… to create this relationship
Sighting –> Threat actor	Incoming relationship — Relates the selected sighting(s) on the **Search an entity** dialog to the threat actor.

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

Edit relationships for a TTP

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.
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 report(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.

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

View related datasets

Related datasets

Entities can belong to one, more, or no datasets. If the entity is included in one or more datasets, they are listed here. Each entry reports the total amount of entities the corresponding dataset contains.

When a dataset is related to an entity, it shares data with it. Datasets and entities can be related in the following ways:

- The entity is included in the dataset.

- The entity and the dataset share common observables.

- The dataset contains an entity that bears a direct or indirect relationship with the active entity displayed on the entity detail pane.

Click a dataset name to display the corresponding detail pane in full page format where you can modify and edit it, if necessary.

View related workspaces

Related workspaces

Entities can belong to one, more, or no workspaces. If the entity belongs to one or more workspaces, they are listed here.

Each entry reports the most recent workspace modification date/time, and whether or not you are a collaborator of the workspace.

Click a workspace name to display the corresponding detail pane in full page format where you can modify and edit it, if necessary.

View related tasks

Related tasks

Any actionable user tasks associated to the entity are listed here.

You can create tasks and assign them to yourself or to other users to request follow-ups; for example, further investigation or a call to action.

This overview lists any actions that have been requested, are in progress, or have been carried out as a response or a follow-up action to the entity information. It shows what is being done to leverage the entity intelligence value.

Each entry reports task name, task progress status, task assignee, and task deadline.

Click a task name to display the corresponding detail pane where you can modify and edit it, if necessary.

Manipulate the entity

Click the **Actions** pop-up menu on the bottom half of the entity detail pane tab and select the desired option to manage the entity and act on it. You can:

- Edit it;

- Delete it;

- Add it to a dataset;

- Load it onto the graph for analysis;

- Create a follow-up task for the entity;

- Export it as JSON or STIX;

- Download it in its original data format; for example, the original STIX package containing the entity.

How to work with exposure

Exposure shows you what your organization is doing with the ingested cyber threat intelligence, so that you can evaluate its usage to define courses of actions and other preventive or reactive procedures within the organization.

What is exposure

In the 2004 Pixar movie **The Incredibles** `(http://www.imdb.com/title/tt0317705/)`, Helen Parr goes to see Edna Mode, only to find out her husband Bob Parr has resumed superhero work. And he's been gone from home for a few days. When Edna asks Helen *"Do you know where he is?"*, Helen cannot answer. Previously in the movie, she had witnessed some changes in her husband's behavior that should have alerted her, but she disregarded that information.

This is exposure in a nutshell.

When platform entities are flagged as exposed, your organization is not making the most of the available cyber threat intelligence (CTI) to drive effective courses of action. Intelligence is either underutilized, or it is ignored.

Exposure helps you assess how your organization uses and leverages CTI: how is CTI affecting the organization? Is the organization using CTI to drive processes to detect, deter, and defeat attacks and to minimize risk? What is working well, and what can be done to improve intel utilization?

Exposure gives you a comprehensive and user-friendly overview that helps you answer these questions by showing you how your organization uses existing CTI, and what it can do to use CTI more efficiently.

Configure exposure

You can configure Exposure to be as generic or as specific as you need:

- On the top navigation bar click **Exposure**.

- On the left-hand navigation sidebar click click **Settings**.

- On the **Exposure > Settings** page click **Edit exposure settings** to change exposure behavior.

On the configuration page you can define which entities you want to watch for exposure, as well as set filters to minimize unwanted data noise:

- **Entity types**: from the drop-down menu select Entity types to include one or more entity types in the exposure configuration.
  The entity types you add here are tracked to assess their exposure.

- **Observable types**: from the drop-down menu select one or more observable types.
  This option filters the selected entities to include in the exposure configuration only entities with at least one observable type matching the selection(s) you specify here.

- **Confidence values**: from the drop-down menu select one or more confidence values.
  This option filters the selected observable types to include in the exposure configuration only observables whose maliciousness confidence value matches at least one of the selections you specify here.
  Confidence corresponds to the value you set under **Rules > Observable > ✚ Rule > Action > Mark as malicious > Confidence**.

- **Entity age**: it defines a time interval ranging from now, that it, the current time, to a point in the past.
  It is an integer and it represents days.
  Only entities that fall inside this range and that are not older than the number of days specified here are tracked to assess their exposure.

- **Relevancy threshold**: *Relevancy* is a numerical value based on the current time and the estimated start time of the threat. You can use it to sort and filter entities. *0%* = low relevancy — *100%* = high relevancy. Its value is 100% when the current time (*now*) is included between the threat start and end times. Otherwise, its value is 0. If the estimated end time is not available, relevancy is calculated using the estimated start time and the half-life value.

- **Show enrichment observables**: if you select this checkbox, enrichment observables are included and displayed, when available.

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

After configuring exposure behavior, you should configure which outgoing feeds should share and distribute exposure information to external systems and devices, so that the data can trigger appropriate actions and responses as part of a concerted course of action.

- On the top navigation bar click **Exposure**.

- On the left-hand navigation sidebar click click **Outgoing feeds**.

On the **Exposure > Outgoing feeds** page you can define how to publish the ingested CTI to minimize exposure. For example, if you are publishing an outgoing feed to an external detection system, the feed data stream is used to detect potential threats.

On this page you map outgoing feeds to the purpose they serve in the context of an integration with external tools and systems.
Within exposure an unused outgoing feed, or a wrongly mapped outgoing feed — for example, an outgoing feed marked as **Detect** but used to distribute CTI to a relevant community, instead — is flagged as exposed.

For each outgoing feed in the overview, you can select one or more checkboxes to map feed usage as appropriate:

- **Detect**: the outgoing feed is published to an external detection system. The feed data is used to detect potential threats that have infiltrated your organization.

- **Prevent**: the outgoing feed is published to an external prevention system. The feed data is used to prevent potential threats from attacking your organization.

- **Community**: the outgoing feed is published to an external information distribution system. The feed is used to share CTI with other parties within or outside the organization.

- **N.A.**: the outgoing feed is not published to any external system.

View exposure

Exposed entities are ingested and processed. However, their intelligence value is not leveraged to produce follow-up actions.
For example, triggering a detection event in a malware detection application downstream in the system; or a prevention event such as creating a firewall rule; or a community event such as sending a notification message to inform other parties about the possible threat the entity represents.
The entities hold intelligence value that is not consumed.

> ℹ️ You first need to configure **Exposure** to specify the filtering criteria the platform should apply when flagging entities as exposed.
> After defining the exposure settings you can view exposed entities, basded on your configuration.

To view exposed entities, do the following:

- On the top navigation bar click **Exposure**.

- It shows an overview of all exposed entities.
  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.

- To enable the quick filters, click **Show filters**.

- To disable the quick filters, click **Hide filters**.

- On the left-hand navigation sidebar click a filter group name to expand the corresponding sub-nodes:

    - **Entity type**: select one or more checkboxes to view exposure details for the specified entity types.

    - **Date**: select a time interval to view exposure details for the entities ingested between the specified start and end dates.

    - **Dataset**: select one or more checkboxes to view exposure details for the entities belonging to the specified datasets.
      The **Dataset** filter is not available when the results do not include any entities belonging to at least a dataset.

You can stack and combine filters as you need.
For example, you can create a filter to view exposure details for indicators belonging to the X, Y, and Z datasets, ingested in the first two weeks of last month.

The **Exposure** view shows the following exposure-specific information:

- **Exposed**: the **Exposed** label indicates that the entity is exposed, that is, it is not used in any detection, prevention, or community integrations or processes.

- **Detection**: the entity and the intelligence value it holds are being consumed in an integration with an external system. In this case, with a detection system. If the dot is green, the entity information is used to carry out a follow-up action. 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.

- **Prevention**: the entity and the intelligence value it holds are being consumed in an integration with an external system. In this case, with a prevention system. If the dot is green, the entity information is used to carry out a follow-up action. 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.

- **Community**: the entity and the intelligence value it holds are being consumed in an integration with an external system. In this case, with an information distribution system. If the dot is green, the entity information is used to carry out a follow-up action. 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.

- **Sighting**: a **!** flag means that the entity has been seen in a secured domain, and there should be a sighting entity recording the occurrence.

- Click the ↻ icon to refresh and update the view.

> ✔ If an entity has been sighted, it is by default exposed no matter the level of integration with external detection, prevention or information distribution systems.

Override entity exposure

You can manually override the configured exposure settings for an entity. The **Override exposure** option allows you to reverse the **Detection**, **Prevention**, and **Sighting** exposure values, and to set them to their opposites.

The entity exposure override history is stored in reverse chronological order, based on the time when the change was applied.

To manually change the exposure state of an entity, do the following:

- On the top navigation bar click **Exposure**.

- On the **Exposure** page click the ⋮ icon on the row corresponding to the entity whose exposure settings you want to override.

- From the context menu select **Override exposure**.

- On the **Override exposure state** dialog window, select the **Override exposure state to** (**ON** or **OFF**, depending on the current exposure value) checkboxes to reverse the current exposure value — from **ON** to **OFF** or the other way around — of **Detection**, **Prevention**, and **Sighting**.

- If you want, you can specify a start date for the override value(s) to become effective: from the drop-down menu select select the desired start date.

- When you are done, close the dialog window. Your settings are automatically saved.

> ⓘ After confiming and saving a manual exposure override, the override value persists until new content is generated, and the entity is updated.

Edit entity exposure

You can manipulate entities by selecting one of the options available in the **Actions** menu above the table view. Apart from the extra **Override exposure** option, the **Actions** menu is the same as the corresponding menu on a workspace **Entities** tab.

Actions	
	Actions ˅ Entit Edit Delete Override exposure Add to Dataset Add to Graph Create a Task Export to JSON Export to CSV Download Original
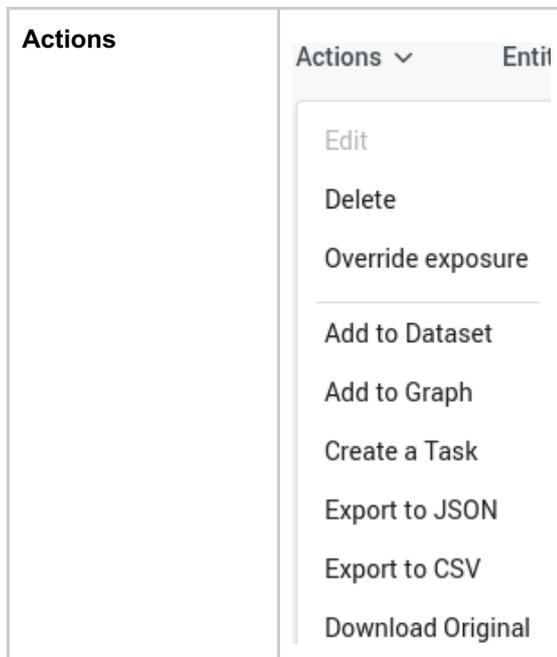
Filter exposure

You can refine the displayed results by specifying a search string in the filter input field.
Alternatively, click one or more quick filters to select and filter by specific:

- Entity types

- Worskpaces

- Datasets

- Date ranges

Entity Types	Entity Types ⌄ Wor ☐ 🌐 Campaign ☐ ✅ Course-Of-Action ☐ 🔶 Exploit-Target ☐ ⚙ Incident ☐ ⊗ Indicator ☐ 🅞 Report ☐ 😈 Threat-Actor ☐ ❶ Ttp
Workspaces	Workspaces ⌄ Datasets ⌄ ☐ 000000001 153 ☐ 000000001 69 ☐ 01 ☐ 1 ☐ And-T-Bug 186 ☐ And-T-Bug 187
Datasets	Datasets ⌄ Date ⌄ ☐ 0 Expo ☐ A ☐ A ☐ A_set ☐ ANdrei_Set ☐ ANdrei_Set_2 ☐ Another Set 6
Date	Date ⌄ From: To: [📅] [📅]

How to enrich entities with observables

Enrichment observables augment the quality of the intelligence you obtain from cyber data analysis. Enrich entities and integrate entity observables with additional raw data to access a broader context and gain deeper insight into threat scenarios.

Ingestion

Data ingestion into the platform is a multi-step process:
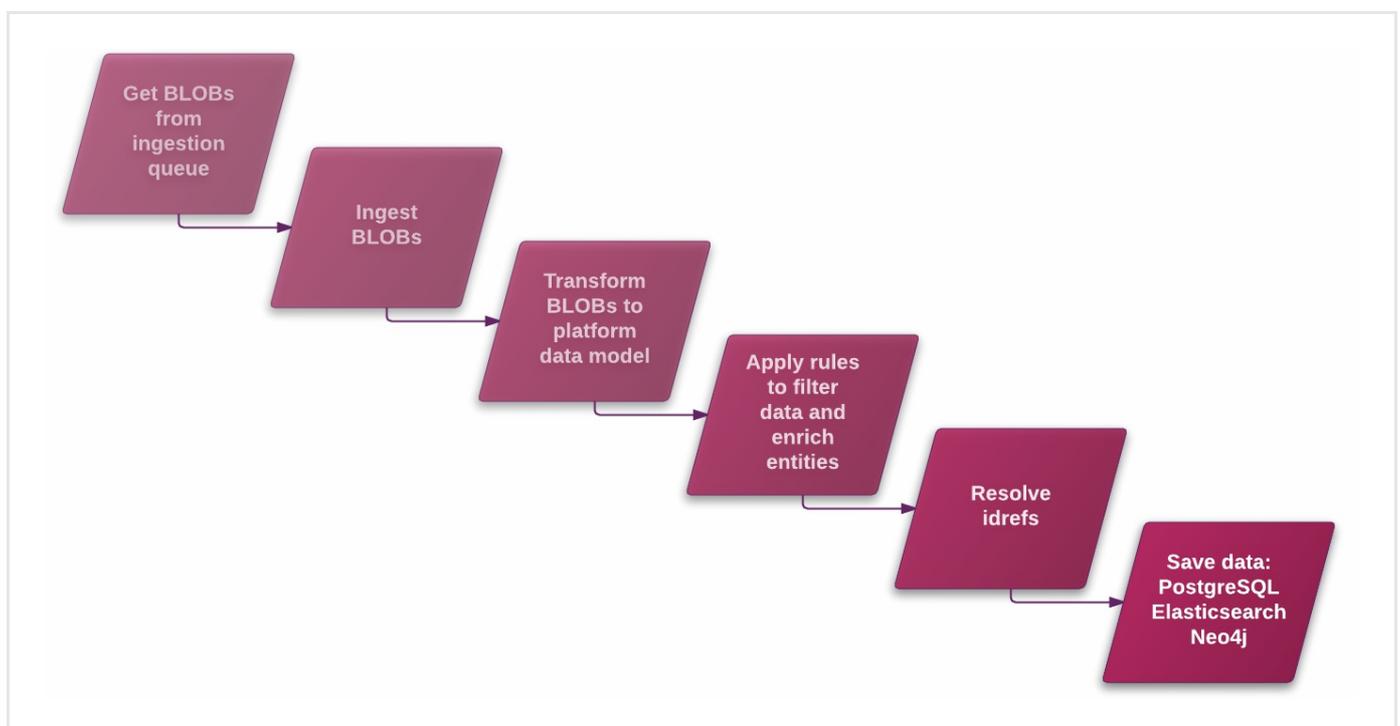
- Incoming data flows in and it is added to the ingestion queue.

- BLOBs are fetched from the ingestion queue to be processed.

- BLOBs are processed:

  - Data is deduplicated;

  - Data is normalized;

  - Data is transformed to the platform internal data model:

    - Entities

    - Observables

    - Relationships.

- Rules and filters enrich entities, create relationships, flag and tag entities, and so on.

- The platform tries to resolve ID references by looking for the data the IDs refer to.

- The ingested entities are saved to the databases.

Deduplication

When checking newly ingested entities vs. existing ones, entity-level deduplication handles the following scenarios:

- Multiple entities sharing the *same STIX ID* and having *identical content* are handled like identical copies.
  In this case, identical copies of the same entity are merged to one entity.

- Multiple entities sharing the *same STIX ID* and having *slightly different content* are handled like versions of the same entity.
  In this case, the most recent content is used to update the existing entity. This avoids creating redundant copies of the same entity in the system.

- Multiple entities sharing the *same STIX ID* and having *identical content*, but *different timestamps* are handled like chronological versions of the same entity.
  In this case, the existing entity timestamp is updated to the most recent value without creating a new version of the entity.

Before deduplication	After deduplication
Multiple entities	They are merged to one entity
Same STIX ID	
Identical content	
(identical copies)	
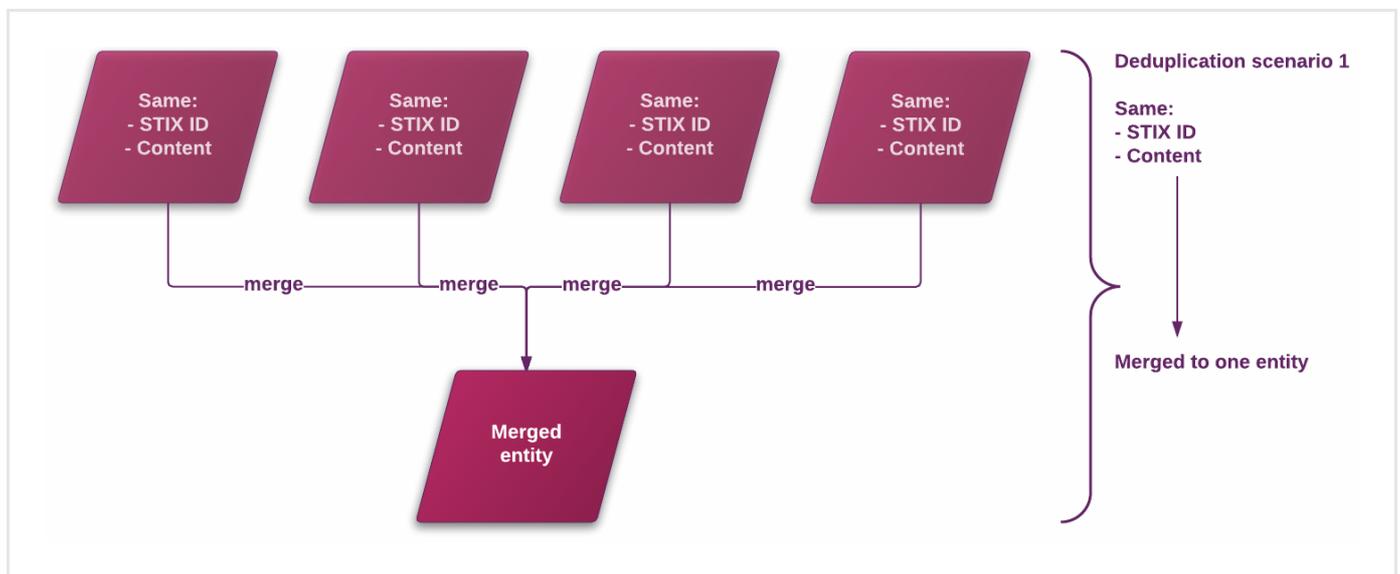
Before deduplication	After deduplication
Multiple entities	The existing entity is updated with the most recent content
Same STIX ID	
Slightly different content	

Before deduplication	After deduplication
(versions of the same entity)	
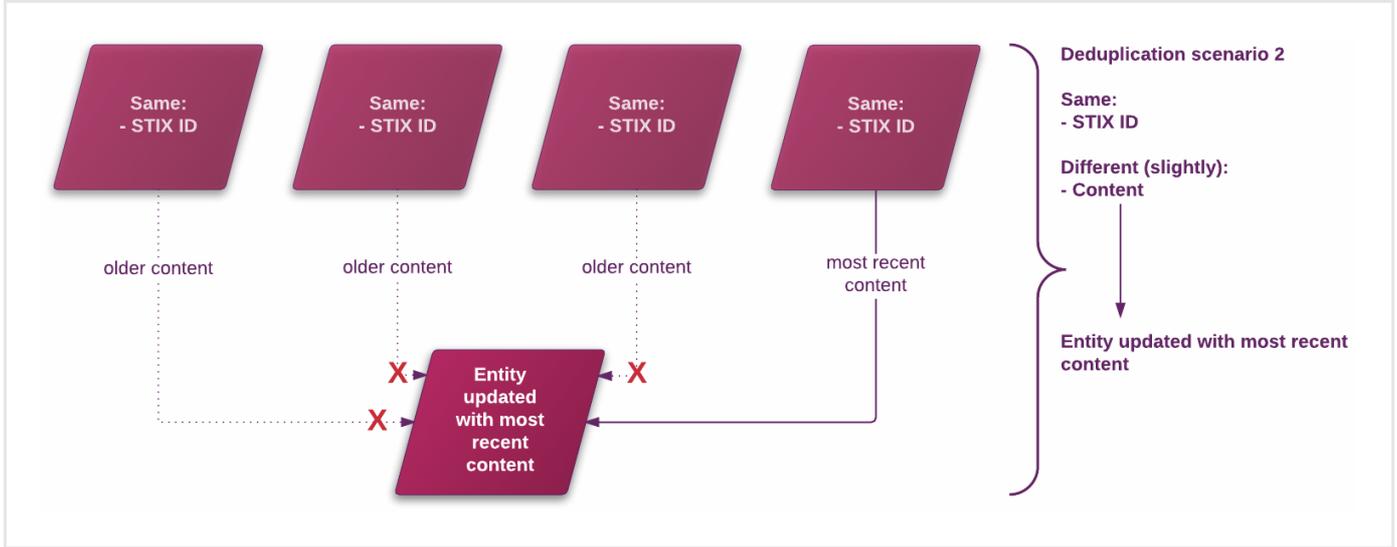
Deduplication scenario 2

Same:
- STIX ID

Different (slightly):
- Content

Entity updated with most recent content

Before deduplication	After deduplication
Multiple entities	The existing entity timestamp is updated to the most recent value
Same STIX ID	
Identical content	
Different timestamps	
(chronological versions of the same entity)	

Deduplication scenario 3

Same:
- STIX ID
- Content

Different:
- Timestamp

Entity updated with most recent timestamp value
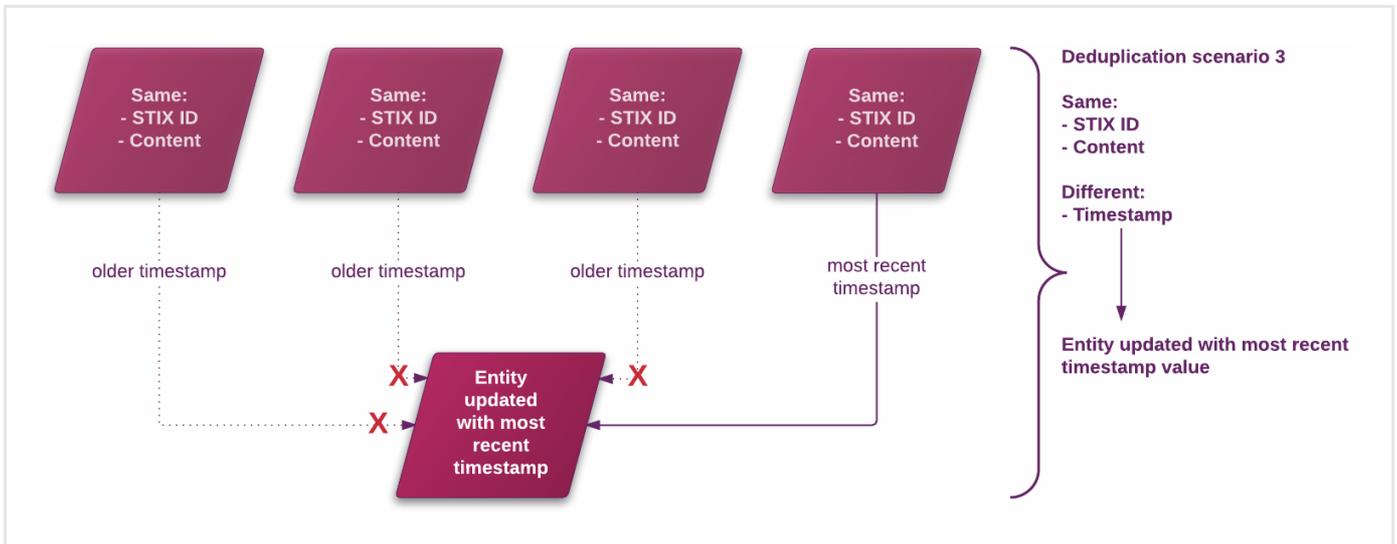
Filtering and enriching

Data extraction produces observables from data retrieved in embedded CybOX objects. This process contribute to data fusion across the whole platform dataset.

- Enrichment rules sift through data to augment it with enrichment observables, that is, observables, obtained from the available enrichment sources, and to exclude specific data based on the defined filtering rules.

- You can further refine the quality of the extracted data by applying ad-hoc rules to classify observables as safe or malicious.

STIX and CyBOX objects can both include placeholder references to external objects and data in the `idref` field. By default, the platform attempts to resolve `idref`s at entity level and at nested object level by looking for the data matching the `idref` value.
If it finds matching data, it creates either a relationship between entities — entity-level, STIX `idref` resolution — or it replaces the `idref` placeholder value with the corresponding actual data — nested object-level, CybOX `idref` resolution.

idref resolution — Entity level

Entities and observables can reference external data through the STIX and CybOX `idref` field.
When the `idref --> id` reference is at entity level (STIX), the platform creates an entity relationship between the entities.

- When a STIX `idref` directly references an entity, the platform creates a direct relationship to associate the two entities.
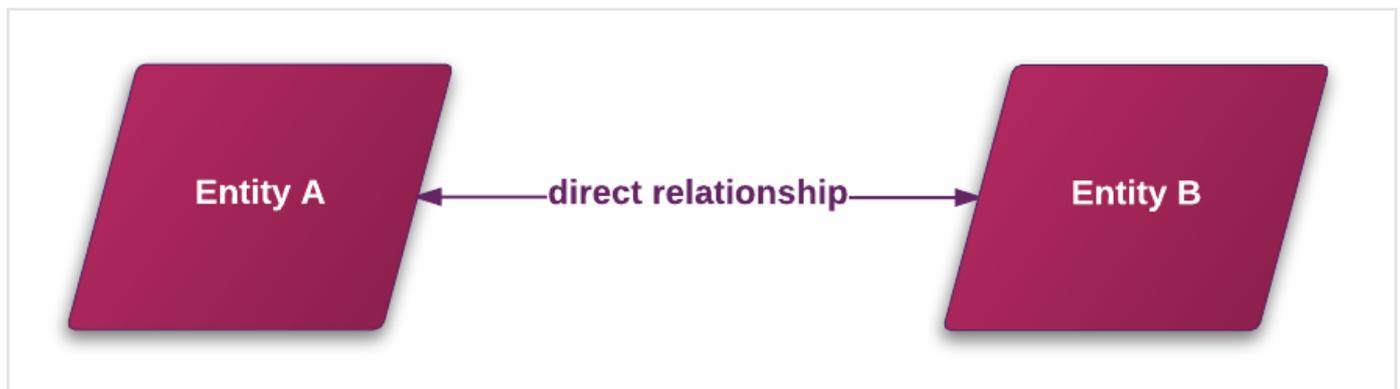
- When a STIX `idref` indirectly references an entity, for example by establishing a relationship with the target entity through a connecting entity or an observable, the platform creates an indirect relationship to associate the two entities.
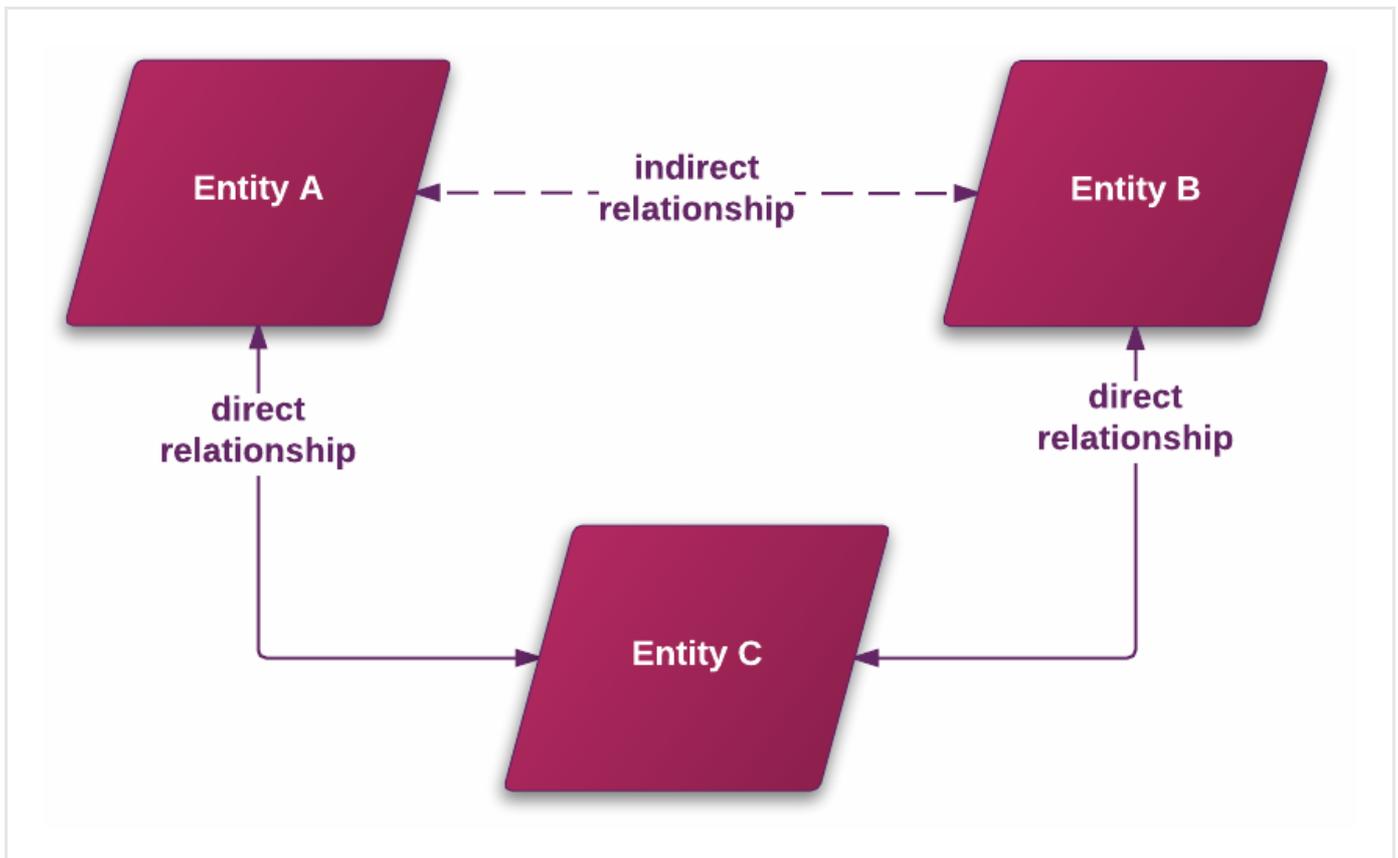
- When a STIX `idref` references an entity of the same type and content as the entity it belongs to, the only differences being either the timestamp, or the version reference values between the two entities, the platform processes the entity with the more recent timestamp or with the higher version value as an update of the other entity.
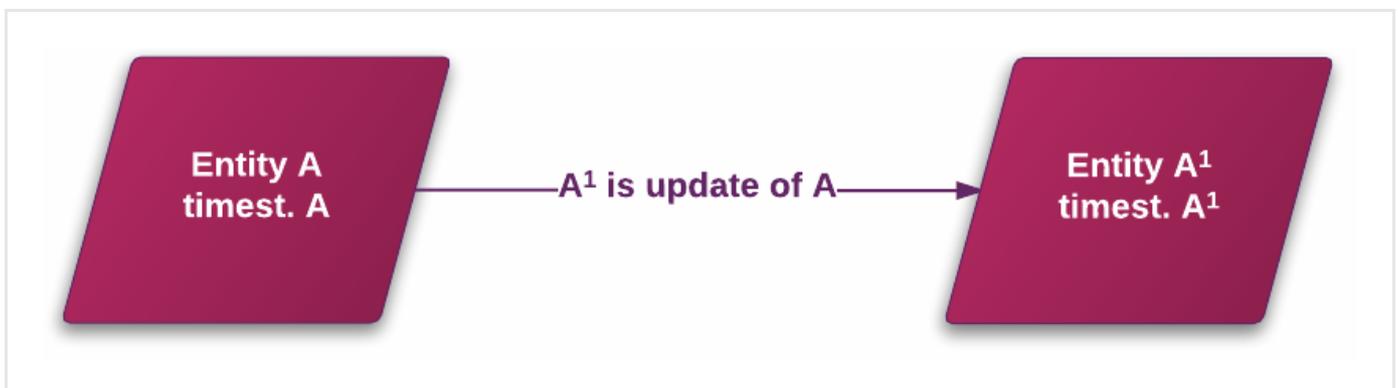
idref resolution — Nested objects

When the `idref --> id`reference is at nested object level (CybOX), that is, when an entity includes an embedded CybOX observable object with an `idref`, the platform attempts to resolve the CybOX `idref` by looking for the referenced data:

- If the CybOX `idref` references data available inside the same ingested package or data stored in the platform database, the newly ingested `idref` is removed and it is replaced with the existing referenced data.
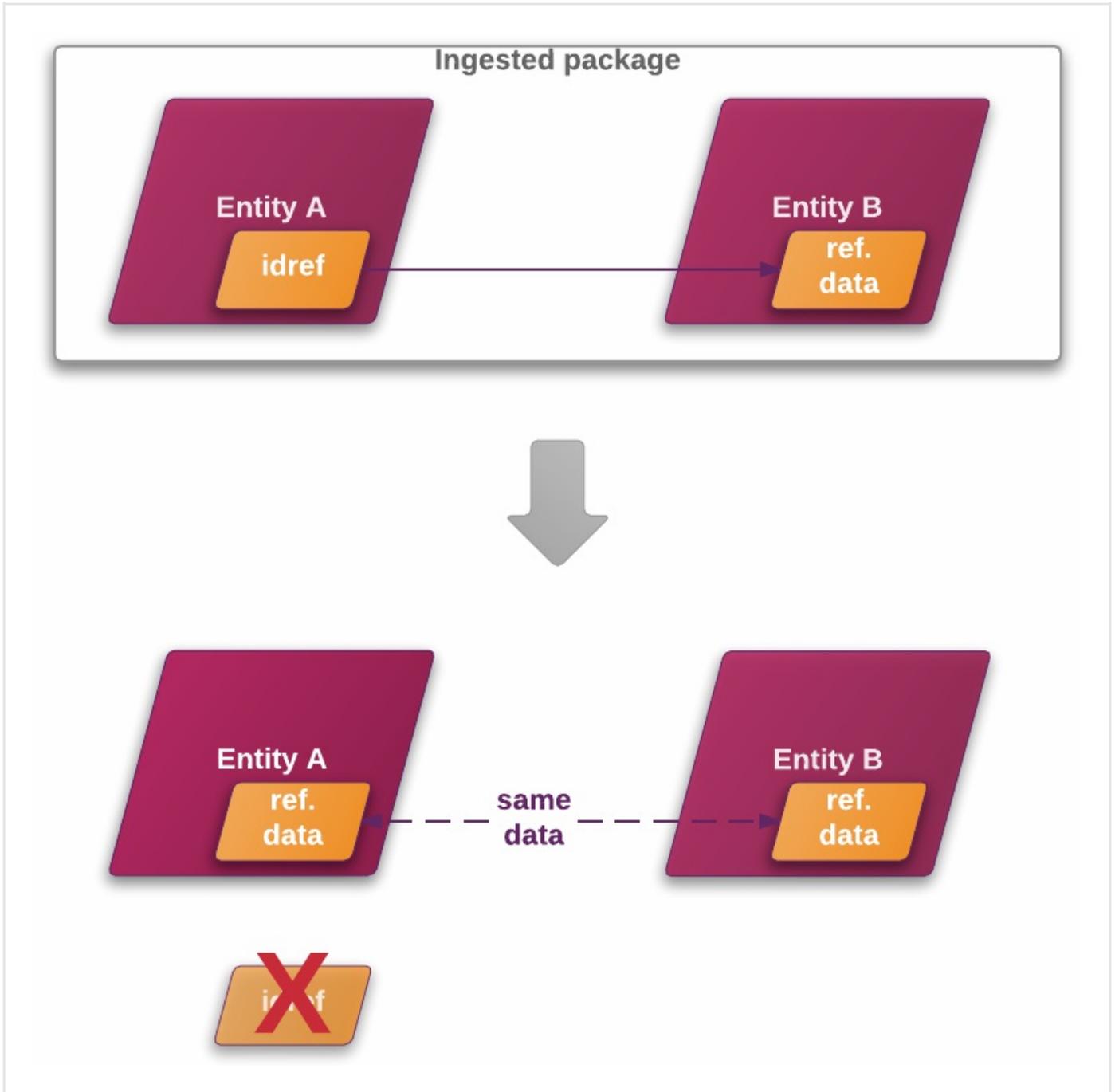
Referenced data is inside the same ingested package
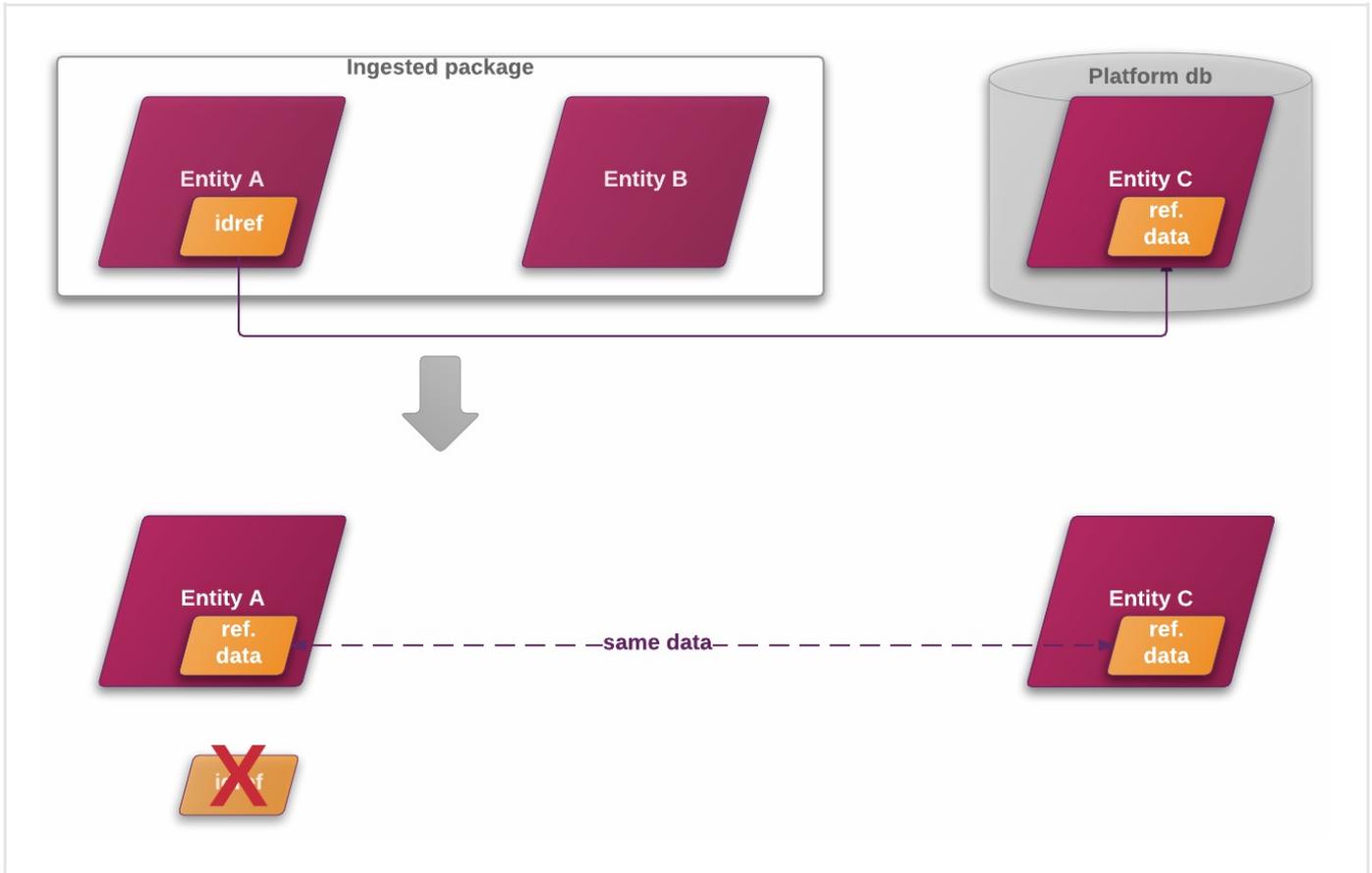
Referenced data is outside the same ingested package, but available in the platform database

- If the `idref` references unavailable data at the moment, the reference is resolved if/when the referenced data becomes available:

  - The `idref` is converted to an empty placeholder TTP or indicator entity that is populated when/if the originally referenced data becomes available.

  - The empty placeholder entity is indexed; therefore, it is searchable, and it can be loaded onto the graph.
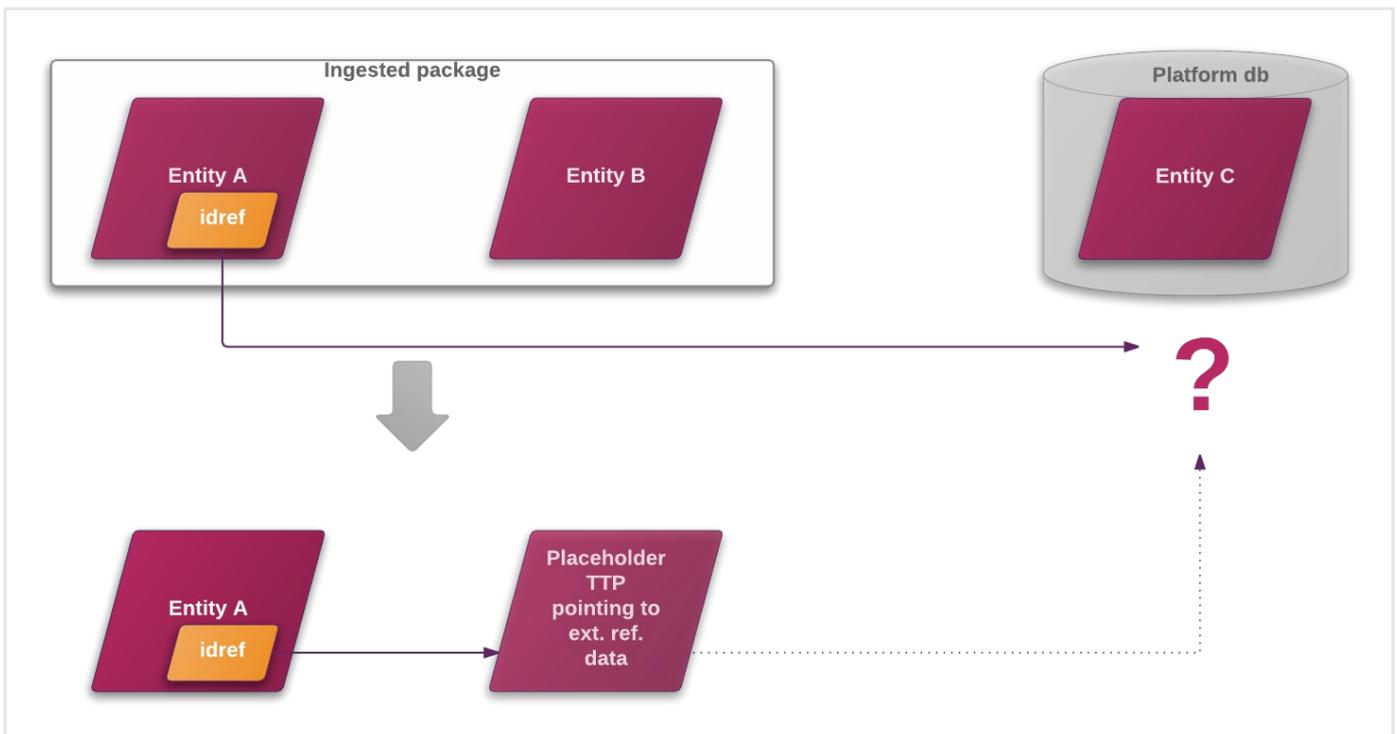
Referenced data is unavailable, an empty placeholder entity points to it in case it becomes available in the future

The process works identically in the opposite direction: if CybOX data is ingested, the platform looks for an existing `idref` pointing to it.

- If it finds a matching `idref`, the existing `idref` is removed and it is replaced with the newly ingested referenced data.

- If no matching `idref` is available, nothing happens. If a matching `idref` becomes available at a later time, it will be resolved then by replacing it with the corresponding referenced data.

Example of an empty placeholder entity

This is an empty TTP placeholder, as shown in the entity detail pane:

This is the corresponding JSON representation:

```
{
  "entities": [

    ...

      "data": {
        "id": "{http://www.example.com/stix/1.0/}attack-d1273cc8b3e108h2e0971a27694fdd1e",
        "type": "ttp",
        "title": "External reference to {http://www.example.com/stix/1.0/}attack-
d1273cc8b3e108h2e0971a27694fdd1e"
      }
    }
  ],

    ...

}
```

Data saving

Last but not least, the platform saves the ingested entities to the databases in the following order:

- Entity store (PostgreSQL)

- Search store (Elasticsearch)

- Graph store (Neo4j)

Enriching entities with observables

The platform can ingest cyber threat intelligence through incoming feeds, by manually uploading one or more files, or by creating an entity in the entity editor.

After ingesting and saving entities to the database, you can integrate the existing information with additional details. The extra information is raw data that augments the entity intelligence value by adding more context and meaning to it. The data is extracted from different sources such as feeds, reports, database searches, curated intel distribution lists, and so on.

The platform uses enrichers to fetch and extract the data. Enricher rules sift through the data to link it to relevant entities as enrichment observables.
This process does not alter core entity data: each bit of enriching information is saved to observables, which are related to entities.
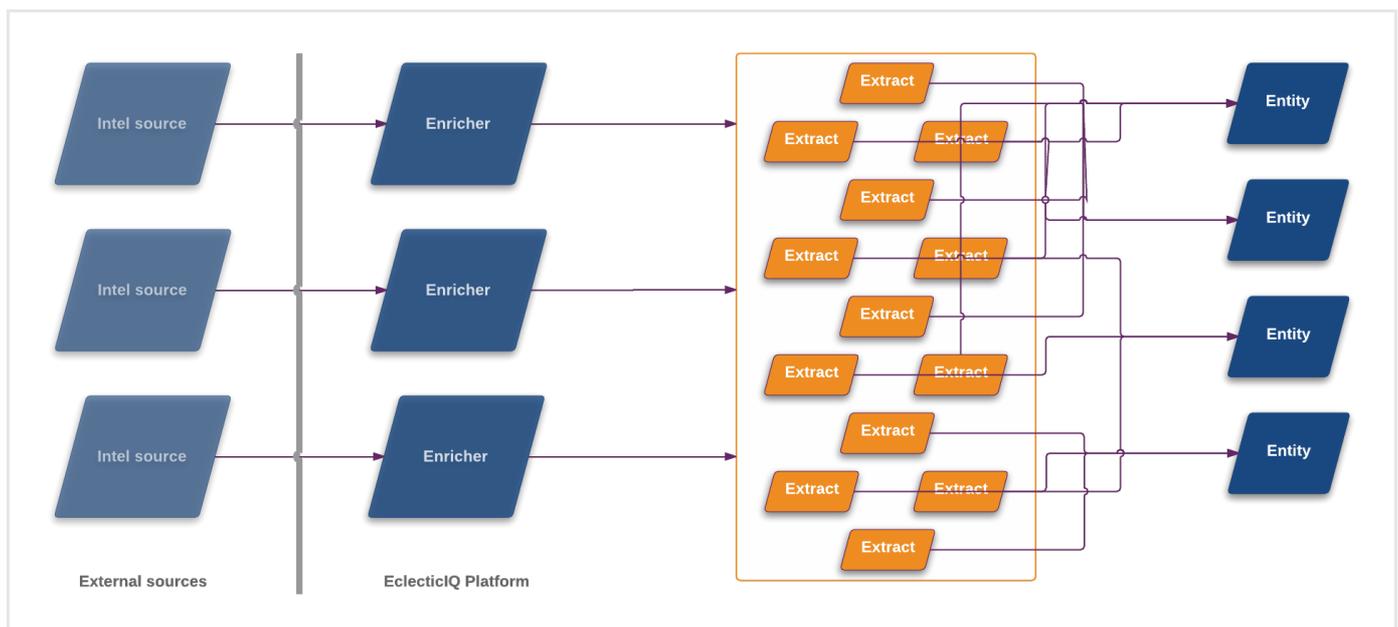
For example, let's assume a scenario where an analyst is investigating a threat actor entity. The entity includes some observables, and one of them is a DNS domain name.
The analyst looks up the domain name by running it through a whois service. The lookup results include an email address. During the investigation, the analyst retrieves also a file hash related to the domain name. An examination reveals that the hash is related to an incident. Information about the incident includes the same email address detail the DNS domain name returned.
There is an indirect relationship between the threat actor and the incident that would not have been noticeable without extra context, which in this example is provided by the hash.

Enrichments help get a broader and sharper picture: by adding meaningful context, they help discover broader, indirect relationships that are not immediately visible.
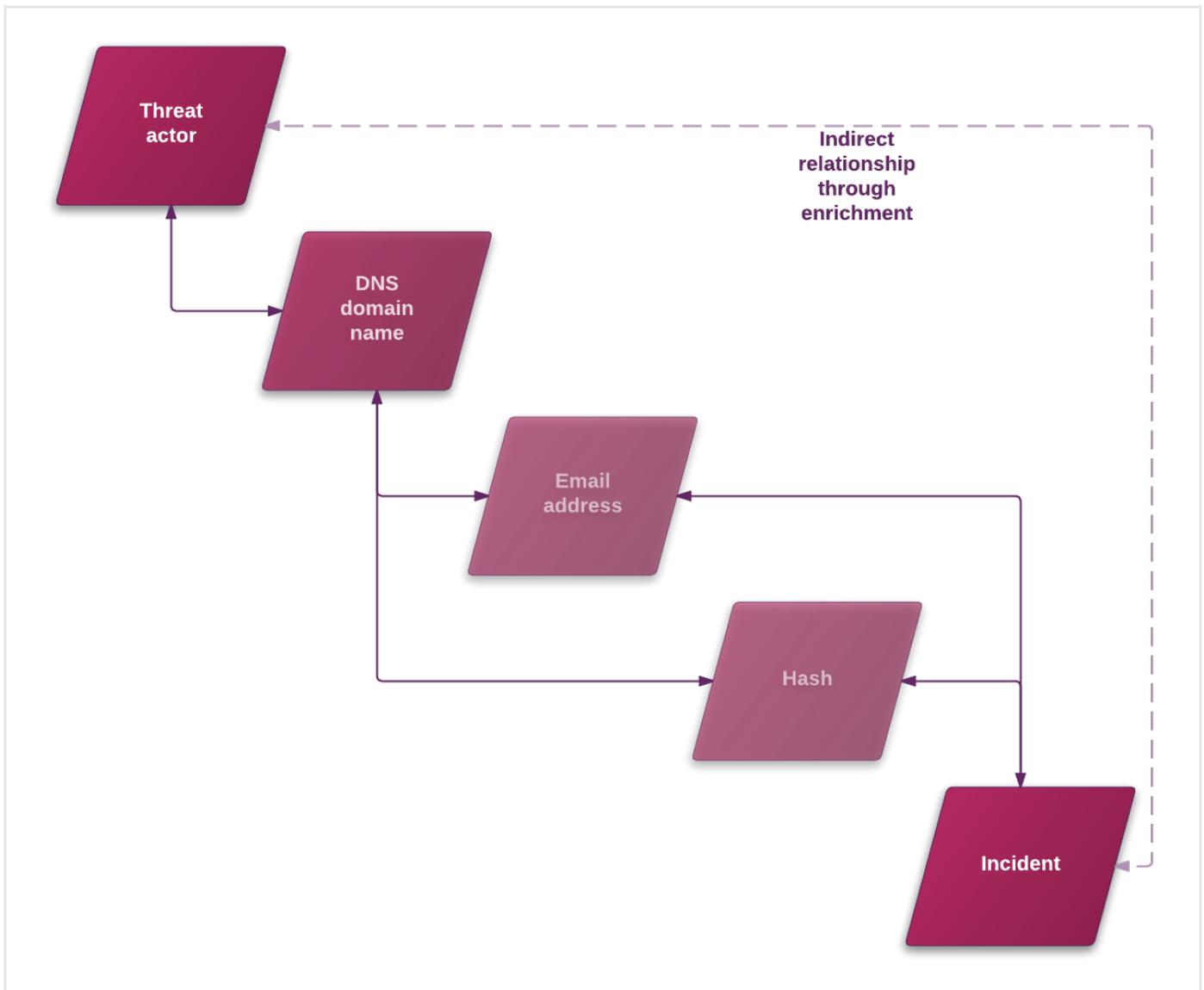
Enrichments augment observables with raw data information related to entities:
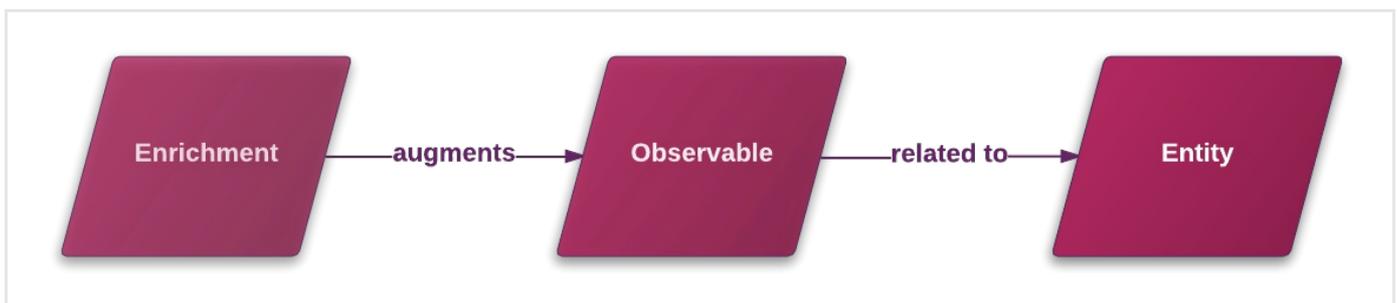
Observables from data URI and raw artifacts

The extracted entity data that is stored inside observables ranges from short, simple data such as email addresses, domain names, IP addresses, and so on, to binary data. When an entity contains binary data, the data can be included as either a *data URI* or a *CybOX raw artifact* element.

During ingestion, extraction logic handles binary data URI and raw artifact objects embedded in CybOX objects in the following way:

- **data URIs** (https://en.wikipedia.org/wiki/data_uri_scheme) are extracted and stored as entity attachments and new hash values:

    - The data URI value is recalculated to a new hash: `uri-hash-sha256`.
    The SHA-256 hash value for `uri-hash-sha256` is calculated over the UTF-8 encoding of the data URI string.
    The `uri-hash-sha256` hash substitute allows for entity correlation among entities containing the same data URI.

    - The binary data/raw content embedded in the data URI is decoded and processed:

        - The extracted binary data content is stored as an entity attachment similar to the CybOX `Raw_Artifact` object.

        - The extracted content is hashed using SHA-512, SHA-256, SHA-1, and MD5.
        Each resulting hash is added to the relevant entities as an observable.

Example

A data URI with image content nested inside a CybOX object generates the following output:

- 1 `uri-hash-sha256` hash to facilitate entity correlation

- 4 calculated hash observables: `hash-sha512`, `hash-sha256`, `hash-sha1`, and `hash-md5`

- 1 embedded JSON entity attachment (`raw-artifact`) with the extracted binary data

The following example shows a sample input along with the corresponding output.

```
dataUriExtractionSample(

    input={
        data:image/gif;base64,R0lGODlhAQABAAAAACH5BAEKAAEALAAAAAABAAEAAAICTAEAOw==
    },

    output={

        # Recalculated hash of the original URI:
        ('uri-hash-sha256:'
         'd16ae5d51dda6f58995171aa23c0fa5e'
         '6dcd9c777cf9c251c4be3b1d62fdf670'),

        # Multiple hashes of the decoded content:
        'hash-md5:3eacd0132310ea44cad756b378a3bc07',

        'hash-sha1:e2216a7e9b73f5cb0279351c78ce61c33475cea7',

        ('hash-sha256:'
         'bb229a48bee31f5d54ca12dc9bd960c6'
         '3a671f0d4be86a054c1d324a44499d96'),

        ('hash-sha512:'
         'bd9ab35dde3a5242b04c159187732e13'
         'b0a6da50ddcff7015dfb78cdd68743e1'
         '91eaf5cddedd49bef7d2d5a642c21727'
         '2a40e5ba603fe24ca676a53f8c417c5d'),

        # (Attachment) Raw artifact as embedded JSON with the content:
        ('raw-artifact:{"content": '
         '"R0lGODlhAQABAAAAACH5BAEKAAEALAAAAAABAAEAAAICTAEAOw==", '
         '"content_encoding": "base64", "type": "image/png"}'),
    }),
```

Enrichers

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Enrichers automatically augment all the entities that accept the enricher's content type as an observable. In other words, the observable types an entity supports define the applicable enrichers an entity can use.

Enricher types

Enricher	API endpoint	Descri
Elasticsearch sightings	`http://<elasticsearch_url>:9200/<schema_resource>`	Searches an external Elasticsearch in search criteria are processed to autom sightings.
Fox-IT InTELL Portal	`https://cybercrime-portal.fox-it.com/`	Based on Fox-IT InTELL, the portal ga a range of sources like forums and sit suspicious activity.
Intel 471	`https://api.intel471.com/v1/`	Besides data on compromised IP add Intel 471 focuses on providing first-ha and groups.
OpenDNS OpenResolve	`http://api.openresolve.com/{}/{}`	OpenResolve by OpenDNS offers a R to retrieve reverse-DNS lookup inform
PyDat	`http://10.0.1.60:8000/ (example)`	**PyDat** (`https://github.com/mitre` locally, and it can work together with a (`https://github.com/mitrecnd/wh with-elasticsearch`) to provide who passive DNS lookup information. Anal organization, country, city, street, ZIP
RIPEstat GeoIP	`https://stat.ripe.net/data/geoloc/data.json?resource={IP_address}`	Geolocation IP information from the R **API** (`https://stat.ripe.net/docs` longitude, country, and city.
RIPEstat Whois	`https://stat.ripe.net/data/whois/data.json?resource={IP_address}`	Whois information from the RIPEstat v **API** (`https://github.com/ripe-nc` including inet number, name, organiza telephone.
Cisco Threat Grid	`https://panacea.threatgrid.com/api/v2/`	Polls data from the Cisco Threat Grid range of cyber threat data like IP addr network streams, and hash files.

Enricher	API endpoint	Descri
VirusTotal	`https://www.virustotal.com/vtapi/v2/{}`	Polls data from the VirusTotal API. It p domains (passive DNS) and IP addres against 60+ antimalware products, res additional metadata information, wher
Flashpoint AggregINT	`https://endlesstunnel.info/v3`	Polls data from the Flashpoint API. It p hosts, domains, IP addresses, and ha thematic datasets focusing on hackers groups, communities in conflict, state **CBRN** `(https://en.wikipedia.org` produces enrichment observables like user name of the author of a post (as UTC date and time of a post in **ISO 86** `(https://en.wikipedia.org/wiki/` `(https://tools.ietf.org/html/rf`
Flashpoint Blueprint	`https://endlesstunnel.info/v3`	Polls data from the Flashpoint API. It p geolocation and IP ranges, as well as search thematic datasets focusing on supremacist groups, state actors invol `(https://en.wikipedia.org/wiki/` enrichment observables like city/coun latitude/longitude or IP address hit, fo a hit, user name uniquely matched to
Flashpoint Thresher	`https://endlesstunnel.info/v3`	Polls data from the Flashpoint API. Th datasets focusing on hackers, terroris and **CBRN** `(https://en.wikipedia` threats. It produces enrichment obser thresher data.
PassiveTotal Whois	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** `(https://api.passivetotal.org/a` `getv2whoisquery)`. It provides inform associated with an IP address or a do details. Analysts can retrieve registra telephone, and email details. They ca further queries to obtain, for example, the same individual or the same comp
PassiveTotal Passive DNS	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** `(https://api.passivetotal.org/a` `getv2dnspassivequery)`. It provides cross-referencing IP addresses to the over time. Analysts can examine how different IP addresses over time. They retrieve more domain names that may

Enricher	API endpoint	Descri
PassiveTotal IP/Domain	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** `(https://api.passivetotal.org/a getv2enrichmentquery)`. It provides queried IP address or domain name. I name, any sub-domains, inet details, a **(ASN)** `(https://en.wikipedia.org/wiki/` as well as geolocation information. An to look for further connections that ma investigation.
PassiveTotal Malware	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** `(https://api.passivetotal.org/a getv2enrichmentmalwarequery)`. It to the queried host or domain, such as sha1, hash-sha256, hash-sha512 — a malware entries are also tagged with `enrichment_extracts.meta.classi` to the value you set under **Rules > O Mark as malicious**; `enrichment_ext` it corresponds to the value you set un **> Confidence > Malicious - Low con**
Splunk sightings	`http://10.0.1.22:8089/ (example)`	Based on the search queries defined for matching data in the specified Splu extracted and saved to the platform a
DomainTools Hosted Domains	`http://api.domaintools.com/v1/{}/host-domains`	Enriches IPv4 observables by returnir and therefore related to, the input IP a
DomainTools Reputation	`http://api.domaintools.com/v1/reputation`	Enriches domain and host name obse information to assess maliciousness c defined threshold values.
DomainTools Suspicious Domains	`https://api.domaintools.com/v1/{}/host-domains`	Enriches IPv4 observables with suspi IP addresses. It includes configurable confidence levels to the processed IP malicious IPs.
FireEye iSIGHT	`https://api.isightpartners.com/search/{}`	Enriches platform observables with da related to areas such as critical infrast espionage, hacktivism, frauds, and vu
Recorded Future	`https://app.recordedfuture.com/live/sc/entity/{}`	The enricher returns additional data s addresses, and hashes related to the specified types, as well as maliciousn retrieved risk scores.
Unshorten-URL	`https://unshorten.me/s/{}`	It takes shortened URL as an input, a resolved original URLs, which can the discover relationships with other entiti

Enricher	API endpoint	Descri
Farsight DNSDB	`https://api.dnsdb.info/{}`	Historical passive DNS lookup enriche pointing to a specified IP address in th nameserver, domain names pointing t existing below a parent domain name
ThreatCrowd	`https://www.threatcrowd.org/{}`	Returns suspicious and potentially ma addresses, file hashes, and antivirus relationships between events, actors,
Censys	`https://censys.io/api/v1/search/ipv4`	Returns relevant contextual informatic types to augment their intelligence val details, hashes, and **ASN** `(https://en.wikipedia.org/wiki/` details. It makes it easier to discover actors, and targets.
DomainTools Malicious Server Domains	`http://api.domaintools.com/v1/{}/name-server-domains/`	Enriches domain and host observable domain names related to the same pri includes configurable thresholds to as levels to the processed domains and domains/hosts.
DomainTools Retrieve Parsed Whois Observables	`http://api.domaintools.com/v1/{}/whois/parsed`	Enriches domains, hosts, and IP addr JSON output includes the most recent domain or IP range, as well as parsed registrar, contacts, and so on. It helps referencing data in a set of Whois rec
Crowdstrike Falcon Intelligence Indicator	`https://intelapi.crowdstrike.com/indicator/v1/search/{}`	Enriches platform entities and observa IP addresses, domain names, email a

Enricher input

The overview shows the supported observable data types you can use as input for the enrichers.
These are the value types the *enrichment_extracts.kind* search query field returns.

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain

Enricher	Supported kinds (observable types)
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4

Enricher	Supported kinds (observable types)
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

Enricher output

Enrichers automatically augment all the entities that accept the enricher's content type as an observable. In other words, the observable types an entity supports define the applicable enrichers an entity can use.

The overview describes the output each enricher generates. The resulting enrichment observables are associated to the entities they bear relationships to.

Enricher	Generated output
Elasticsearch sightings	Creates sightings from matching results returned from a search in an external Elasticsearch instance.
Fox-IT InTELL Portal	Enriches the supported observable types with relevant contextual information from forums, chats, and IRC channels.
Intel 471	Enriches the supported observable types with data focusing on threat actor information.
OpenDNS OpenResolve	Enriches the supported observable types with reverse-DNS lookup information.
PyDat	Enriches the supported observable types with whois data, current IP resolution and passive DNS information.
RIPEstat GeoIP	Enriches the supported observable types with geolocation information related to IP addresses: coordinates, country, and city.
RIPEstat Whois	Enriches the supported observable types with whois information related to IP addresses.
Cisco Threat Grid	Enriches the supported observable types, as well as all found observables based on the enricher configuration, with information such as IP addresses, domains, host names, hashes, and Windows registry keys.
VirusTotal	Enriches the supported observable types with maliciousness confidence level information.
Flashpoint AggregINT	Enriches the supported observable types with information such as IP addresses, domains, host names, and hash files.
Flashpoint Blueprint	Enriches the supported observable types with information such as IP addresses, domains, host names, and URLs.
Flashpoint Thresher	Enriches the supported observable types with information such as IP addresses, domains, URLs, hashes, and files.
PassiveTotal Whois	Enriches the supported observable types with **whois** (https://www.riskiq.com/products/learn-threat-research-and-analysis/) information.

Enricher	Generated output
PassiveTotal Passive DNS	Enriches the supported observable types with **passive DNS** `(https://www.riskiq.com/products/learn-threat-research-and-analysis/)` information.
PassiveTotal IP/Domain	Enriches the supported observable types with **enrichment** `(https://passivetotal.readthedocs.io/en/latest/api.html#enrichment-request)` information.
PassiveTotal Malware	Enriches the supported observable types with **malware enrichment** `(https://passivetotal.readthedocs.io/en/latest/api.html?highlight=malware#enrichment-request)` information.
Splunk sightings	Creates sightings for matching input observables, based on the search result items retrieved in the specified Splunk instance.
DomainTools Hosted Domains	Enriches the supported observable types with domain and host name information.
DomainTools Reputation	Enriches the supported observable types with reputation information.
DomainTools Suspicious Domains	Enriches the supported observable types with suspicious domain and host name information.
FireEye iSIGHT	Enriches the supported observable types related to the matching input observable types.
Recorded Future	Enriches the supported observable types with pattern matching search results produced by the Recorded Future Temporal Analytics Engine.
Unshorten-URL	Original URL the submitted shortened one.
Farsight DNSDB	Enriches the supported observable types with passive DNS lookup information such as the name of the domain or host name owner, or the IP address a domain or host name points to.
ThreatCrowd	Enriches the supported observable types with suspicious and potentially malicious domains, IP addresses, email addresses, file hashes, and antivirus detections.
Censys	Enriches the supported observable types by providing additional context such as geolocation, country and city information, as well as **ASN** `(https://en.wikipedia.org/wiki/autonomous_system_(internet))` details.
DomainTools Malicious Server Domains	Enriches the supported observable types with malicious domain names that are served from the same name server.
DomainTools Retrieve Parsed Whois Observables	Enriches the supported observable types with structured Whois information.
Crowdstrike Falcon Intelligence Indicator	Enriches the supported observable types with information extracted from indicators.

Enrich entities

You can enrich entities in the following ways:

- Automatically, or

- Manually.

Enrichment rules and enrichment tasks drive the enrichment process to:

- Poll selected and trustworthy intelligence data sources;

- Retrieve relevant, accurate, and reliable data to augment platform entities with additional bits of information that provide additional context.

Rules

Enrichment rules define what to do with the retrieved enrichment data.
Rules act like filters, and they set the logical constraints defining:

- The platform data sources to augment with the enrichment information. Data sources can be incoming feeds, as well as other enrichers.

- Within the selected platform data sources, the entity type(s) to augment with the enrichment information.

- The enrichers to use to fetch the enrichment data.

Tasks

Enrichment tasks define process execution by setting the following options:

- The data fetching mechanism; for example, an API endpoint exposing the enrichment data service.

- Specific data sources; for example, datasets targeting threat actors like hackers and terrorist groups.

- Data rate limit and monthly execution cap values to control the amount of polled data.

- A source reliability flag for the incoming enrichment data to simplify assessing the quality of the retrieved data.

Automatically enrich entities

To automatically enrich entities, make sure enricher tasks are active, and the necessary enrichment rules are configured.

Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment observable data, as well as route it to other devices that enforce cyber threat detection or prevention.

Manually enrich entities

To adjust enrichment behavior to manually apply it to the entities you want to enrich, do the following:

- Open an entity in edit mode.
  For example, on the top navigation bar click **Browse > Published** to display an overview of the published entities available in the platform.

- On the row corresponding to the entity you want to manually enrich, click the ⋮ icon to display the context menu.

- From the drop-down menu select **Edit**.

- At the bottom of the entity editor page click the **Manually enrich** checkbox.
  A new input field with a drop-down menu becomes available.

- From the drop-down menu select one or more enrichers you want to apply to the entity.
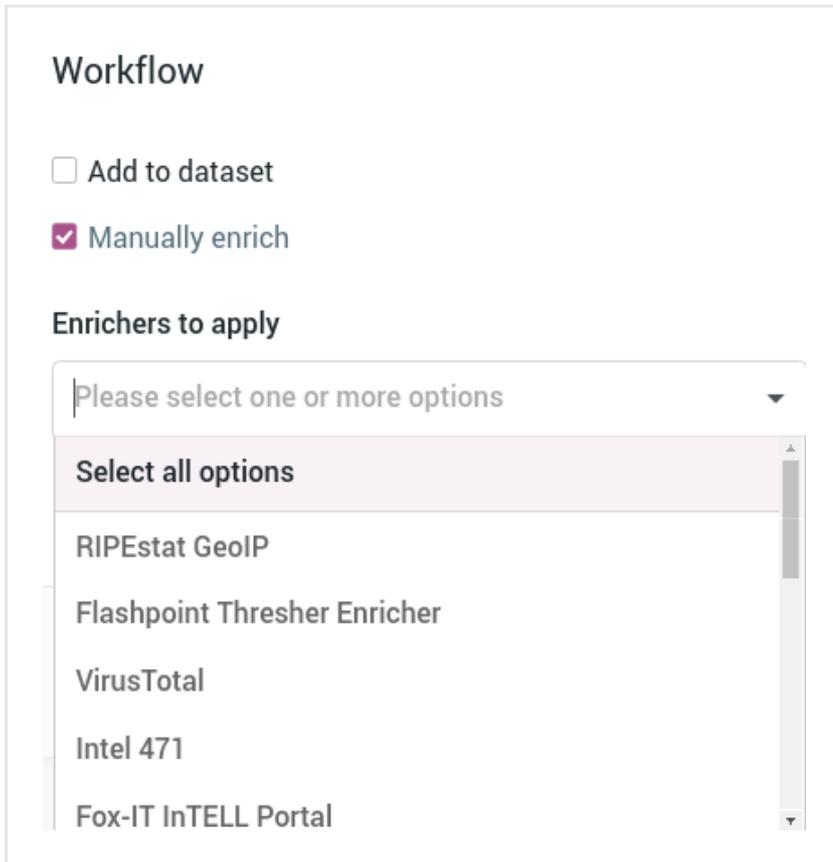
Workflow

☐ Add to dataset

☑ Manually enrich

Enrichers to apply

Please select one or more options ▾

Select all options

RIPEstat GeoIP

Flashpoint Thresher Enricher

VirusTotal

Intel 471

Fox-IT InTELL Portal

- 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.

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

- On the entity detail pane, click **Observables**.

- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the ⟳ refresh icon to trigger a task run that polls all the enrichers configured for the entity.

Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.

- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.

To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.

- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.

To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.

- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.

The available enricher tasks in the drop-down menu are automatically filtered to show only the applicable enrichers for the entity.

Enrichers automatically augment all the entities that accept the enricher's content type as an observable. In other words, the observable types an entity supports define the applicable enrichers an entity can use.

Enricher rules

View enricher rules

To view enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.

- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.

- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  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.

- To view the details of a specific rule, click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.

Add enricher rules

To add a new enricher rule, do the following:

- On the top navigation bar click **✚ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ✿ icon next to the user avatar image.

- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.

- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  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 the **+ Rule** button.

> ✔ On the forms, input fields marked with an asterisk are required.

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.

- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.

- Click **✚ Add** or **✚ More** to add a filtering option.

- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.

- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.

- **TLP**: from the drop-down menu select 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.

- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.

- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.

- Select the **Enabled** checkbox to enable the rule immediately after creating it.

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

Save options

Besides committing 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 creation work.

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.

- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.

- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  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.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.

- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.

- From the drop-down menu select **Edit**.

> ✔   On the forms, input fields marked with an asterisk are required.

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.

- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.

- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.

- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.

- **TLP**: from the drop-down menu select 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.

- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.

- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.

- Select the **Enabled** checkbox to enable the rule immediately after creating it.

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

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ✿ icon next to the user avatar image.

- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.

- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  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 an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.

- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.

- From the drop-down menu select **Delete**.

- On the confirmation pop-up dialog, click **Delete** to confirm the action.

- The rule is deleted.

Enricher tasks

View enricher tasks

To view enricher tasks, do the following:

- On the top navigation bar click ✚ **> Data management > Dataset > Enrichment** .

Alternatively:

- On the top navigation bar, click the ✿ icon next to the user avatar image.

- From the drop-down menu select **Data management**.

- On the left-hand navigation sidebar click **Enrichment**.

- Click the enricher you want to examine.

- On the enricher detail page, you can view all the details about the selected enricher, including the rules driving the enricher behavior, recently executed enriching tasks, and the state.

- You can click the state value or an enrichment rule to display additional information.

> 💡 When the state value returns **FAILURE**, click the link to view the task execution traceback and to begin troubleshooting.

The **Data management > Enrichment** view shows all configured enrichers polling third-party and/or external services to acquire additional information to integrate observables with, so that they can provide more context to the cyber threat entities they belong to.

RIPEstat GeoIP	RIPEstat Whois	OpenResolve	VirusTotal ❗	PyDat ❗	Cisco AMP Threat Grid ❗
☑ Active	☑ Active	☑ Active	☐ Active	☐ Active	☐ Active
4 runs this month	4 runs this month	47 runs this month	129 runs this month	0 runs this month	261 runs this month
Intel 471 ❗	Fox-IT InTELL Portal ❗	Elastic Sightings Enricher ❗	Flashpoint AggregINT Enri... ❗	Flashpoint Blueprint Enric...	Flashpoint Thresher Enricher ❗
☐ Active	☐ Active	☐ Active	☐ Active	☑ Active	☐ Active
398 runs this month	2 runs this month	2 runs this month	120 runs this month	112 runs this month	6 runs this month
PassiveTotal Whois Enricher ❗	PassiveTotal Passive DNS ... ❗	PassiveTotal IP/Domain En... ❗	PassiveTotal Malware Enri... ❗	Splunk Sightings Enricher ❗	
☐ Active	☐ Active	☐ Active	☐ Active	☐ Active	
42 runs this month	19 runs this month	78 runs this month	38 runs this month	0 runs this month	

Edit enricher tasks

To configure or to edit an enricher task, do the following:

- On the top navigation bar click ✚ **> Data management > Dataset > Enrichment** .

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.

- From the drop-down menu select **Data management**.

- On the left-hand navigation sidebar click **Enrichment**.

- Click the enricher you want to configure or modify.

- On the enricher detail page, click the **Edit** button.

> ✔ On the forms, input fields marked with an asterisk are required.

- **Name**: the name used to identify the enricher. It should be descriptive and easy to remember.

- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.

- **Cache validity (sec)**: defines for how long enrichment data remains stored in the cache. The value is expressed in seconds.

- **Rate limit (per sec)**: sets the maximum allowed number of requests/executions per second.

- **Monthly execution cap (executions)**: sets a maximum allowed number of requests/executions per month. Together with rate limiting, execution cap helps control data traffic for the enricher; for example, when the API or the service you are connecting to enforces usage limits.

- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
  Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).
  Example: *B - Usually reliable*

- **Enabled**: checkbox. Select the **Enabled** checkbox to enable the enricher task immediately after editing and saving it. If you select the checkbox, the rule is executed automatically. If you deselect it, you need to run the rule manually.

- Under **Parameters**, define the specific configuration options for the selected enricher, where applicable.

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

> ⚠ **Warning:**
> Some enricher tasks include an additional API key field where you specify the API key issued by the source of the enricher, along with the necessary authentication and authorization credentials.
> Contact the intel service provider whose data you want to use as a source for the enricher to request an API key and any other required credentials.
>
> You need to install and set up PyDat locally. The product does not work outside a local network.
> You need to configure the host before you can access PyDat features through the API endpoint.
> See also:
>
> - **Mitre blog on PyDat**
>   (http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/using-whois-and-passive-dns-for-intelligence)
>
> - **PyDat GitHub repo** (https://github.com/mitrecnd/whodat)

How to configure outgoing feeds

This summary page gives you an overview of the available how-to and tutorial articles about outgoing feeds. They describe how to configure content types, transport types, and all the required options you need to set when you create outgoing feeds to distribute and share acquired cyber threat intelligence through EclecticIQ Platform.

Browse the table for the topics you want to look up.
You can also use the drop-down menu on the left-hand navigation sidebar to access the articles or to go to a different section.

Title	Excerpt
How to configure ArcSight CEF outgoing feeds	Set up and configure ArcSight CEF outgoing feeds.
How to configure EclecticIQ CSV outgoing feeds	Set up and configure EclecticIQ CSV outgoing feeds.
How to configure EclecticIQ JSON outgoing feeds	Set up and configure EclecticIQ JSON outgoing feeds.
How to configure STIX 1.2 outgoing feeds	Set up and configure STIX 1.2 outgoing feeds.
How to retrieve outgoing feeds through the API	Fetch outgoing feeds either manually through the platform GUI or programmatically via the API.

How to configure ArcSight CEF outgoing feeds

Set up and configure ArcSight CEF outgoing feeds.

EclecticIQ Platform enables you to configure outgoing feeds to share and distribute cyber threat intelligence in several formats. Share knowledge and promote collaboration to support an ecosystem where partners work together to identify threats, and define an effective course of action to ensure their assets are protected.

This article describes how to configure **ArcSight CEF** outgoing feeds, so that you can distribute selected intelligence through EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

Under **Transport and content** you can define *what* you want to publish and *how*, that is, the data content type and the data transport type.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- **Transport type**: from the drop-down menu select the appropriate transport type to publish data through the outgoing feed. This can vary, based on the carrier used to distribute the data.

- Depending on the selected transport type, you may need to specify additional settings under **Transport configuration**. For example:

  - A URL endpoint corresponding to the API service exposing the data source for the incoming feed.

  - A valid API key to grant you access to the feed data source.

  - Any required login credentials to obtain access to the feed data source.

- **Content type**: from the drop-down menu select **ArcSight CEF** and configure the appropriate parameters under **Content configuration**, when applicable.

- **Dataset**: from the drop-down menu select one or more datasets as data sources for the outgoing feed.

- **Update strategy**: from the drop-down menu select the preferred method to update the data:

  - **Append**: every time the outgoing feed task runs, only new data from the latest task run, that is, only new entities, is appended to the existing data.
    When the outgoing feed task runs, it includes only new entities.

  - **Replace** every time the outgoing feed task runs, it publishes only new data.
    When the outgoing feed task runs, it produces new content that can include new, as well as existing entities.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes. You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour. You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day. You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week. You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month. You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu. Keep in mind that not all months of the year have 31 days.

Set a TLP override

- **Override TLP** overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

  You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed. When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences. For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

- The **Filter TLP color** options allow including in the feed data only an entity subset, based on the selected **TLP** `(https://www.us-cert.gov/tlp)` value. If you set a TLP color as a filter, the feed includes all the entities flagged with the selected TLP color code, as well as the entities whose TLP color indicates that they are suitable for progressively broader audiences. For example, if you select green, the feed includes entities with a TLP color set to green and entities with a TLP color set to white.

Set reliability and relevancy

- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is. Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`. Example: *B - Usually reliable*

- **Relevancy threshold (%)** allows you to set a filter to include in the feed only entities whose relevancy is higher than the value defined here.

Set observable filters

- **Allowed observable states**: from the drop-down menu select one or more observable states to include in the feed data only entities whose observable states match at least one of the selections defined here.

- **Observable types**: from the drop-down menu select one or more observable types to include in the outgoing feed only entities whose observable types match at least one of the selections defined here.

- **Enrichment observable types**: from the drop-down menu select one or more enrichment observable types to include in the outgoing feed only entities whose enrichment observable types match at least one of the selections defined here.

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

The filters work independently of each other: there are no Boolean `AND` or `OR` to join multiple filters into a serial pipeline.

Save options

Besides committing 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 creation work.

Configure the content type

When you select the **ArcSight CEF** content type for a feed, you need to configure the following content type parameters:

- **Observable types**: from the drop-down menu select one or more observable types to include in the feed data only entities whose observables match the selected types.

- **Enrichment observable types**: from the drop-down menu select one or more enrichment observable types to include in the feed data only entities whose enrichment observables match the selected types.

Configure the transport type

Content type	Allowed transport types
ArcSight CEF	FTP upload
	HTTP download
	Mount point upload
	Send email
	Syslog push

Content type	Allowed transport types
	TAXII inbox
	TAXII poll

FTP upload

If you want to make the outgoing feed data available through FTP, from the **Transport type** drop-down list select **FTP upload**.

Under **Transport configuration**, configure the following settings:

- **FTP server URL**: the target `ftp://` location to upload the outgoing feed content to, so as to make it available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

- **Password**: a valid password to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

HTTP download

> ℹ️ The HTTP download transport type requires basic access authentication.

If you want to make the outgoing feed data available through an HTTP URL, from the **Transport type** drop-down list select **HTTP download**.

Under **Transport configuration**, configure the following settings:

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

Mount point upload

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point upload** option.

Under **Transport configuration**, configure the following settings:

- **Mount point path**: the path to the local or network unit where the source data for the outgoing feed is stored.

Send email

> ⚠️ **Warning:** Email needs to be correctly configured in the platform system settings for this transport option to work.

If you want to make the outgoing feed data available by email, from the **Transport type** drop-down list select **Send email**. Under **Transport configuration**, configure the following settings:

- **Mail subject**: enter a short, descriptive subject for the outgoing email notifications.

- **Platform groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users. All the members of the selected group(s) will receive email notifications with the outgoing feed data.

- **Platform users**: if you want to further limit the outgoing feed email recipient targets, from the drop-down list you can select one or more users. In this case, only the selected users belonging to the designated groups will receive email notifications with the outgoing feed data.

Syslog push

If you want to make the outgoing feed data available through a syslog push service, from the **Transport type** drop-down list select **Syslog push**.
Under **Transport configuration**, configure the following settings:

- **Syslog server host**: specify the IP address or the host name of the server handling syslog message log communications.

- **Syslog server port**: specify the port number of the server handling syslog message log communications. Make sure the port is open, and that data traffic through the port is not blocked by, for example, a firewall.

  Typical port settings for the TCP protocol:

  - *601* for syslog-conn

  - *6514* for syslog over TCP with TLS

  Typical port settings for the UDP protocol:

  - *514* for syslog

- **Protocol**: from the drop-down menu select the transmission protocol, either **TCP** or **UDP**.

TAXII inbox

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII inbox** transport type requires Cabby. For further details, see the **official Cabby documentation** `(https://cabby.readthedocs.org/en/latest/)`, the **Cabby public repo on GitHub** `(https://github.com/eclecticiq/cabby)`, and the **Cabby download page** `(https://pypi.python.org/pypi/cabby/)`.

If you want to make the outgoing feed data available through a TAXII server and push email notifications to TAXII clients, from the **Transport type** drop-down list select **TAXII inbox**.
Under **Transport configuration**, configure the following settings:

- **Inbox service URL**: specify a valid URL address to determine the service location where the available **TAXII data collections** `(https://taxiiproject.github.io/documentation/sample-use/#data-collections)` are stored.
  Example:
  `https://example.com/taxii-inbox`

- **Destination collection name**: specify a valid collection as the source for the outgoing feed data.
  Example:
  `collection.Default`

- **Taxii version**: select the TAXII version your system supports:

  - Either **1.0** `(https://taxiiproject.github.io/releases/1.0/)`

  - Or **1.1** `(https://taxiiproject.github.io/releases/1.1/)`

- **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
  Example:
  `https://<platform.host>/auth`

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----`and `-----END CERTIFICATE-----` lines.

- **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----`and `-----END RSA PRIVATE KEY-----` lines.

- **SSL key password**: enter here the password to unlock the SSL key.

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

TAXII poll

> ⚠ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII poll** transport type requires Cabby. For further details, see the **official Cabby documentation** (https://cabby.readthedocs.org/en/latest/), the **Cabby public repo on GitHub** (https://github.com/eclecticiq/cabby), and the **Cabby download page** (https://pypi.python.org/pypi/cabby/).

If you want to make the outgoing feed data available through polling — where a TAXII client polls the TAXII server to request information and data updates — from the **Transport type** drop-down list select **TAXII poll**.

- Make sure that at least one dataset is selected under **Dataset** to allow TAXII clients to request information and updates about the specified **TAXII data collection(s)** (https://taxiiproject.github.io/documentation/sample-use/#data-collections).

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

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

How to configure EclecticIQ CSV outgoing feeds

Set up and configure EclecticIQ CSV outgoing feeds.

EclecticIQ Platform enables you to configure outgoing feeds to share and distribute cyber threat intelligence in several formats. Share knowledge and promote collaboration to support an ecosystem where partners work together to identify threats, and define an effective course of action to ensure their assets are protected.

This article describes how to configure **EclecticIQ CSV** outgoing feeds, so that you can distribute selected intelligence through EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

Under **Transport and content** you can define *what* you want to publish and *how*, that is, the data content type and the data transport type.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- **Transport type**: from the drop-down menu select the appropriate transport type to publish data through the outgoing feed. This can vary, based on the carrier used to distribute the data.

- Depending on the selected transport type, you may need to specify additional settings under **Transport configuration**. For example:

  - A URL endpoint corresponding to the API service exposing the data source for the incoming feed.

  - A valid API key to grant you access to the feed data source.

  - Any required login credentials to obtain access to the feed data source.

- **Content type**: from the drop-down menu select **EclecticIQ Entities CSV** or **EclecticIQ Observables CSV** and configure the appropriate parameters under **Content configuration**, when applicable.

- **Dataset**: from the drop-down menu select one or more datasets as data sources for the outgoing feed.

- **Update strategy**: from the drop-down menu select the preferred method to update the data:

  - **Append**: every time the outgoing feed task runs, only new data from the latest task run, that is, only new entities, is appended to the existing data.
  When the outgoing feed task runs, it includes only new entities.

  - **Replace** every time the outgoing feed task runs, it publishes only new data.
  When the outgoing feed task runs, it produces new content that can include new, as well as existing entities.

  - **Diff**: every time the outgoing feed task runs, new data is compared against existing data to identify any differences between the two datasets at observable-level — any observable added to or removed from the entities in the set — or at entity-level — any entities added to or removed from the set. Depending on the selected CSV content option, each row in the CSV output contains information about one entity or one observable.
  An extra diff column is added to the output to indicate if a row, and therefore either an entity or an observable, was added to or removed from the set.
  This option allows you to identify any changes in a feed between two task runs without downloading the whole feed every time.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes. You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

- **Override TLP** overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

  You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
  When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
  For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

- The **Filter TLP color** options allow including in the feed data only an entity subset, based on the selected **TLP** `(https://www.us-cert.gov/tlp)` value.
  If you set a TLP color as a filter, the feed includes all the entities flagged with the selected TLP color code, as well as the entities whose TLP color indicates that they are suitable for progressively broader audiences. For example, if you select green, the feed includes entities with a TLP color set to green and entities with a TLP color set to white.

Set reliability and relevancy

- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
  Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`.
  Example: *B - Usually reliable*

- **Relevancy threshold (%)** allows you to set a filter to include in the feed only entities whose relevancy is higher than the value defined here.

Set observable filters

- **Allowed observable states**: from the drop-down menu select one or more observable states to include in the feed data only entities whose observable states match at least one of the selections defined here.

- **Observable types**: from the drop-down menu select one or more observable types to include in the outgoing feed only entities whose observable types match at least one of the selections defined here.

- **Enrichment observable types**: from the drop-down menu select one or more enrichment observable types to include in the outgoing feed only entities whose enrichment observable types match at least one of the selections defined here.

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

The filters work independently of each other: there are no Boolean `AND` or `OR` to join multiple filters into a serial pipeline.

Save options

Besides committing 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 creation work.

Configure the content type

When you select the **EclecticIQ CSV** content type for a feed, you need to configure the following content type parameters.

From the drop-down menu select one of the following options to define the preferred structure for the output data and the resulting layout in the CSV output:

- **EclecticIQ Entities CSV**: in the resulting CSV with column headers, each row holds information referring to one entity. For example, an indicator, a TTP, and so on.

- **EclecticIQ Observables CSV**: in the resulting CSV with column headers, each row holds information referring to one observable.
  For example, an IP address, a hash, a geographic location name, and so on.

> ⚠️ **Warning:** If you select **EclecticIQ Observables CSV**, you need to choose at least one observable type from the **Observable types** drop-down list, and at least one enrichment observable type from the **Enrichment observable types** drop-down list.

If you select **EclecticIQ Observables CSV**, by default the outgoing feed includes only *first level*, *original* observables:

- First level: the extracted data is inside a CybOX object.

- Original: the value is extracted as is, that is, the observable holds the actual value found in the CybOX object.

You can include also *second level*, *derived* observables by selecting one or both checkboxes under **Content configuration**:

- **Include derived observables**: the extracted data is the result of an analysis of the original value found inside a STIX field.

- **Include secondary observables**: the source of the extracted data is a value inside a STIX field, not a value inside a CybOX object.

Derivation and levels

Derivation — **Original** vs **Derived** observables — and levels — level **1** and level **2** observables — work together to make it easier to act efficiently on observables and to use them to trigger follow-up actions in your prevention/detection toolchain.

The platform can flag observables to automate processes such as:

- Add potentially malicious threats to a prevention and/or a detection system;

- Exclude non-malicious observables that do not represent a potential threat for the organization.

Rules handle the flags, and they can initiate actions on observables; for example, routing them to a prevention and/or a detection system, or marking them as ignorable and filter them out to reduce unwanted data noise.

Original + level 1

Derivation	**Original**
Level	**1**

- **Original / 1**: the extracted data is directly retrieved as is from a CybOX object embedded in a STIX indicator.

- **Original**: the value is extracted as is, that is, the observable holds the actual value found in the CybOX object.
  For example, a URI value extracted from:

```
<URIObj:Value condition="Equals">http://x4z9arb.cn/4712</URIObj:Value>
```

- **1**: the extracted data is inside a CybOX object.
  For example, a URI in a CybOX object embedded in a STIX indicator.

When the platform flags an observable as **Original / 1**, it handles it as follows:

- It assigns the observable an initially *low confidence maliciousness* level.

- It flags it as *level 1* extracted data to indicate that it originates from a CybOX object, it is directly related to its parent STIX entity, and it is probably relevant.

- It marks it as a potential threat that needs to be added to a detection and/or prevention system.

Derived + level 2

Derivation	**Derived**
Level	**2**

- **Derived / 2** : the source of the extracted data is a value inside a STIX field, not a value inside a CybOX object.

- **Derived**: the extracted data is the result of an analysis of the original value found inside a STIX field.
  For example, a domain name extracted from a URI:

```
<!-- The original observable value, in this example a URI -->
<stixCommon:Reference>https://technet.microsoft.com/library/security/2887505</stixCommon:Reference>


<!-- The derived observable obtained from the URI, that is, a domain -->
technet.microsoft.com
```

- **2**: the source of the extracted data is a value inside a STIX field, not a value inside a CybOX object.
  For example, a URI in a STIX field like a header, a title, or a reference.

When the platform flags an observable as **Derived / 2** , it handles it as follows:

- It does not assign the observable any maliciousness level.

- It flags it as *level 2* extracted data to indicate that it does not originate from a CybOX object, but from a STIX field; it is indirectly related to its source, and possibly less relevant.

- It does not mark it for inclusion in a detection and/or prevention system.

Configure the transport type

Content type	Allowed transport types
EclecticIQ CSV	FTP upload
	HTTP download
	Mount point upload
	Send email
	Syslog push
	TAXII inbox
	TAXII poll

FTP upload

If you want to make the outgoing feed data available through FTP, from the **Transport type** drop-down list select **FTP upload**.
Under **Transport configuration**, configure the following settings:

- **FTP server URL**: the target `ftp://` location to upload the outgoing feed content to, so as to make it available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

- **Password**: a valid password to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

HTTP download

> ℹ️ The HTTP download transport type requires basic access authentication.

If you want to make the outgoing feed data available through an HTTP URL, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

Mount point upload

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point upload** option.

Under **Transport configuration**, configure the following settings:

- **Mount point path**: the path to the local or network unit where the source data for the outgoing feed is stored.

Send email

> ⚠️ **Warning:** Email needs to be correctly configured in the platform system settings for this transport option to work.

If you want to make the outgoing feed data available by email, from the **Transport type** drop-down list select **Send email**. Under **Transport configuration**, configure the following settings:

- **Mail subject**: enter a short, descriptive subject for the outgoing email notifications.

- **Platform groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users. All the members of the selected group(s) will receive email notifications with the outgoing feed data.

- **Platform users**: if you want to further limit the outgoing feed email recipient targets, from the drop-down list you can select one or more users. In this case, only the selected users belonging to the designated groups will receive email notifications with the outgoing feed data.

TAXII inbox

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII inbox** transport type requires Cabby. For further details, see the **official Cabby documentation** `(https://cabby.readthedocs.org/en/latest/)`, the **Cabby public repo on GitHub** `(https://github.com/eclecticiq/cabby)`, and the **Cabby download page** `(https://pypi.python.org/pypi/cabby/)`.

If you want to make the outgoing feed data available through a TAXII server and push email notifications to TAXII clients, from the **Transport type** drop-down list select **TAXII inbox**.
Under **Transport configuration**, configure the following settings:

- **Inbox service URL**: specify a valid URL address to determine the service location where the available **TAXII data collections** `(https://taxiiproject.github.io/documentation/sample-use/#data-collections)` are stored.
  Example:
  `https://example.com/taxii-inbox`

- **Destination collection name**: specify a valid collection as the source for the outgoing feed data.
  Example:
  `collection.Default`

- **Taxii version**: select the TAXII version your system supports:

  - Either **1.0** `(https://taxiiproject.github.io/releases/1.0/)`

  - Or **1.1** `(https://taxiiproject.github.io/releases/1.1/)`

- **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
  Example:
  `https://<platform.host>/auth`

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----`and `-----END CERTIFICATE-----` lines.

- **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----`and `-----END RSA PRIVATE KEY-----` lines.

- **SSL key password**: enter here the password to unlock the SSL key.

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

TAXII poll

> ⚠ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII poll** transport type requires Cabby. For further details, see the **official Cabby documentation** (https://cabby.readthedocs.org/en/latest/), the **Cabby public repo on GitHub** (https://github.com/eclecticiq/cabby), and the **Cabby download page** (https://pypi.python.org/pypi/cabby/).

If you want to make the outgoing feed data available through polling — where a TAXII client polls the TAXII server to request information and data updates — from the **Transport type** drop-down list select **TAXII poll**.

- Make sure that at least one dataset is selected under **Dataset** to allow TAXII clients to request information and updates about the specified **TAXII data collection(s)** (https://taxiiproject.github.io/documentation/sample-use/#data-collections).

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

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

How to configure EclecticIQ JSON outgoing feeds

Set up and configure EclecticIQ JSON outgoing feeds.

EclecticIQ Platform enables you to configure outgoing feeds to share and distribute cyber threat intelligence in several formats. Share knowledge and promote collaboration to support an ecosystem where partners work together to identify threats, and define an effective course of action to ensure their assets are protected.

This article describes how to configure **EclecticIQ JSON** outgoing feeds, so that you can distribute selected intelligence through EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

Under **Transport and content** you can define *what* you want to publish and *how*, that is, the data content type and the data transport type.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- **Transport type**: from the drop-down menu select the appropriate transport type to publish data through the outgoing feed. This can vary, based on the carrier used to distribute the data.

- Depending on the selected transport type, you may need to specify additional settings under **Transport configuration**. For example:

    - A URL endpoint corresponding to the API service exposing the data source for the incoming feed.

    - A valid API key to grant you access to the feed data source.

    - Any required login credentials to obtain access to the feed data source.

- **Content type**: from the drop-down menu select **EclecticIQ JSON** and configure the appropriate parameters under **Content configuration**, when applicable.

- **Dataset**: from the drop-down menu select one or more datasets as data sources for the outgoing feed.

- **Update strategy**: from the drop-down menu select the preferred method to update the data:

    - **Append**: every time the outgoing feed task runs, only new data from the latest task run, that is, only new entities, is appended to the existing data.
      When the outgoing feed task runs, it includes only new entities.

    - **Replace** every time the outgoing feed task runs, it publishes only new data.
      When the outgoing feed task runs, it produces new content that can include new, as well as existing entities.

    - **Diff**: every time the outgoing feed task runs, new data is compared against existing data to identify any differences between the two datasets at observable-level — any observable added to or removed from the entities in the set — or at entity-level — any entities added to or removed from the set. Depending on the selected CSV content option, each row in the CSV output contains information about one entity or one observable.
      An extra diff column is added to the output to indicate if a row, and therefore either an entity or an observable, was added to or removed from the set.
      This option allows you to identify any changes in a feed between two task runs without downloading the whole feed every time.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes. You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

- **Override TLP** overwrites the **TLP** (https://www.us-cert.gov/tlp) color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

  You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
  When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
  For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

- The **Filter TLP color** options allow including in the feed data only an entity subset, based on the selected **TLP** (https://www.us-cert.gov/tlp) value.
  If you set a TLP color as a filter, the feed includes all the entities flagged with the selected TLP color code, as well as the entities whose TLP color indicates that they are suitable for progressively broader audiences. For example, if you select green, the feed includes entities with a TLP color set to green and entities with a TLP color set to white.

Set reliability and relevancy

- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
  Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`.
  Example: *B - Usually reliable*

- **Relevancy threshold (%)** allows you to set a filter to include in the feed only entities whose relevancy is higher than the value defined here.

Set observable filters

- **Allowed observable states**: from the drop-down menu select one or more observable states to include in the feed data only entities whose observable states match at least one of the selections defined here.

- **Observable types**: from the drop-down menu select one or more observable types to include in the outgoing feed only entities whose observable types match at least one of the selections defined here.

- **Enrichment observable types**: from the drop-down menu select one or more enrichment observable types to include in the outgoing feed only entities whose enrichment observable types match at least one of the selections defined here.

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

The filters work independently of each other: there are no Boolean `AND` or `OR` to join multiple filters into a serial pipeline.

Save options

Besides committing 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 creation work.

Configure the content type

When you select the **EclecticIQ JSON** content type for a feed, you need to configure the following content type parameters:

- **Override producer**: select this checkbox to replace the original producer identity with the one defined in the platform. Leave it deselected to include the original producer of the information.

Configure the transport type

Content type	Allowed transport types
EclecticIQ JSON	FTP upload

Content type	Allowed transport types
	HTTP download
	Mount point upload
	Send email
	TAXII inbox
	TAXII poll

FTP upload

If you want to make the outgoing feed data available through FTP, from the **Transport type** drop-down list select **FTP upload**.
Under **Transport configuration**, configure the following settings:

- **FTP server URL**: the target `ftp://` location to upload the outgoing feed content to, so as to make it available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

- **Password**: a valid password to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

HTTP download

> ⓘ The HTTP download transport type requires basic access authentication.

If you want to make the outgoing feed data available through an HTTP URL, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

Mount point upload

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point upload** option.

Under **Transport configuration**, configure the following settings:

- **Mount point path**: the path to the local or network unit where the source data for the outgoing feed is stored.

Send email

> ⚠️ **Warning:** Email needs to be correctly configured in the platform system settings for this transport option to work.

If you want to make the outgoing feed data available by email, from the **Transport type** drop-down list select **Send email**. Under **Transport configuration**, configure the following settings:

- **Mail subject**: enter a short, descriptive subject for the outgoing email notifications.

- **Platform groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users. All the members of the selected group(s) will receive email notifications with the outgoing feed data.

- **Platform users**: if you want to further limit the outgoing feed email recipient targets, from the drop-down list you can select one or more users. In this case, only the selected users belonging to the designated groups will receive email notifications with the outgoing feed data.

TAXII inbox

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII inbox** transport type requires Cabby. For further details, see the **official Cabby documentation** (https://cabby.readthedocs.org/en/latest/), the **Cabby public repo on GitHub** (https://github.com/eclecticiq/cabby), and the **Cabby download page** (https://pypi.python.org/pypi/cabby/).

If you want to make the outgoing feed data available through a TAXII server and push email notifications to TAXII clients, from the **Transport type** drop-down list select **TAXII inbox**.
Under **Transport configuration**, configure the following settings:

- **Inbox service URL**: specify a valid URL address to determine the service location where the available **TAXII data collections** (https://taxiiproject.github.io/documentation/sample-use/#data-collections) are stored.
  Example:
  `https://example.com/taxii-inbox`

- **Destination collection name**: specify a valid collection as the source for the outgoing feed data.
  Example:
  `collection.Default`

- **Taxii version**: select the TAXII version your system supports:

    - Either **1.0** `(https://taxiiproject.github.io/releases/1.0/)`

    - Or **1.1** `(https://taxiiproject.github.io/releases/1.1/)`

- **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
  Example:
  `https://<platform.host>/auth`

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----`and `-----END CERTIFICATE-----` lines.

- **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----`and `-----END RSA PRIVATE KEY-----` lines.

- **SSL key password**: enter here the password to unlock the SSL key.

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

TAXII poll

> ⚠ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII poll** transport type requires Cabby. For further details, see the **official Cabby documentation** `(https://cabby.readthedocs.org/en/latest/)`, the **Cabby public repo on GitHub** `(https://github.com/eclecticiq/cabby)`, and the **Cabby download page** `(https://pypi.python.org/pypi/cabby/)`.

If you want to make the outgoing feed data available through polling — where a TAXII client polls the TAXII server to request information and data updates — from the **Transport type** drop-down list select **TAXII poll**.

- Make sure that at least one dataset is selected under **Dataset** to allow TAXII clients to request information and updates about the specified **TAXII data collection(s)** `(https://taxiiproject.github.io/documentation/sample-use/#data-collections)`.

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

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

How to configure STIX 1.2 outgoing feeds

Set up and configure STIX 1.2 outgoing feeds.

EclecticIQ Platform enables you to configure outgoing feeds to share and distribute cyber threat intelligence in several formats. Share knowledge and promote collaboration to support an ecosystem where partners work together to identify threats, and define an effective course of action to ensure their assets are protected.

This article describes how to configure **STIX 1.2** version **1.2** `(https://stixproject.github.io/data-model/1.2/)` outgoing feeds, so that you can distribute selected intelligence through EclecticIQ Platform.

Configure the general options

> ✔ On the forms, input fields marked with an asterisk are required.

Under **Transport and content** you can define *what* you want to publish and *how*, that is, the data content type and the data transport type.

- Under **Feed name**, enter a name for the feed you are creating. It should be descriptive and easy to remember.

- **Transport type**: from the drop-down menu select the appropriate transport type to publish data through the outgoing feed. This can vary, based on the carrier used to distribute the data.

- Depending on the selected transport type, you may need to specify additional settings under **Transport configuration**. For example:

  - A URL endpoint corresponding to the API service exposing the data source for the incoming feed.

  - A valid API key to grant you access to the feed data source.

  - Any required login credentials to obtain access to the feed data source.

- **Content type**: from the drop-down menu select **STIX 1.2** and configure the appropriate parameters under **Content configuration**, when applicable.

- **Dataset**: from the drop-down menu select one or more datasets as data sources for the outgoing feed.

- **Update strategy**: from the drop-down menu select the preferred method to update the data:

  - **Append**: every time the outgoing feed task runs, only new data from the latest task run, that is, only new entities, is appended to the existing data.
    When the outgoing feed task runs, it includes only new entities.

  - **Replace** every time the outgoing feed task runs, it publishes only new data.
    When the outgoing feed task runs, it produces new content that can include new, as well as existing entities.

Set a schedule

Under **Execution schedule** you can define how often you want to run the feed task:

- **None**: no schedule is defined. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.

- **Minute**: the feed task runs automatically every *N* minutes, where *N* defines the selected time interval in minutes.
  You define the execution interval in 5-minute increments from the corresponding drop-down menu.

- **Hour**: the feed task runs automatically every hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.

- **Day**: the feed task runs automatically once a day.
  You define the time of the day when the task should run from the corresponding drop-down menu.

- **Week**: the feed task runs automatically once a week.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menu.

- **Month**: the feed task runs automatically once a month.
  You define the day of the calendar month and time of the day when the task should run from the corresponding drop-down menu.
  Keep in mind that not all months of the year have 31 days.

Set a TLP override

- **Override TLP** overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated to the feed entities with the one you set here. The selected TLP value is assigned to all the entities in the feed.

  You can override the original or the current TLP color code of an entity, an incoming feed, or an outgoing feed.
  When working as a filter, TLP colors select a decreasing range: if you set a TLP color as a filter the enricher, the feed, or the returned filtered results include all the entities flagged with the selected TLP color code, as well as all the entities whose TLP color indicates that they are progressively lower risk, less sensitive, and suitable for disclosure to broader audiences.
  For example, if you select green the filtered results include entities with a TLP color set to green, as well as entities with a TLP color set to white, and entities with no TLP color code flag.

- The **Filter TLP color** options allow including in the feed data only an entity subset, based on the selected **TLP** `(https://www.us-cert.gov/tlp)` value.
  If you set a TLP color as a filter, the feed includes all the entities flagged with the selected TLP color code, as well as the entities whose TLP color indicates that they are suitable for progressively broader audiences. For example, if you select green, the feed includes entities with a TLP color set to green and entities with a TLP color set to white.

Set reliability and relevancy

- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
  Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** `(https://en.wikipedia.org/wiki/admiralty_code)`.
  Example: *B - Usually reliable*

- **Relevancy threshold (%)** allows you to set a filter to include in the feed only entities whose relevancy is higher than the value defined here.

Set observable filters

- **Allowed observable states**: from the drop-down menu select one or more observable states to include in the feed data only entities whose observable states match at least one of the selections defined here.

- **Observable types**: from the drop-down menu select one or more observable types to include in the outgoing feed only entities whose observable types match at least one of the selections defined here.

- **Enrichment observable types**: from the drop-down menu select one or more enrichment observable types to include in the outgoing feed only entities whose enrichment observable types match at least one of the selections defined here.

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

The filters work independently of each other: there are no Boolean `AND` or `OR` to join multiple filters into a serial pipeline.

Save options

Besides committing 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 creation work.

Configure the content type

When you select the **STIX 1.2** content type for a feed, you need to configure the following content type parameters:

- **Override producer**: select this checkbox to replace the original producer identity with the one defined in the platform. Leave it deselected to include the original producer of the information.

Configure the transport type

Content type	Allowed transport types
STIX 1.2	FTP upload
	HTTP download
	Mount point upload
	Send email
	TAXII inbox
	TAXII poll

FTP upload

If you want to make the outgoing feed data available through FTP, from the **Transport type** drop-down list select **FTP upload**.
Under **Transport configuration**, configure the following settings:

- **FTP server URL**: the target `ftp://` location to upload the outgoing feed content to, so as to make it available for download.

- **Username**: a valid user name to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

- **Password**: a valid password to authenticate and be granted the necessary authorization to upload the outgoing feed content to the designated FTP server location.

HTTP download

> **ℹ** The HTTP download transport type requires basic access authentication.

If you want to make the outgoing feed data available through an HTTP URL, from the **Transport type** drop-down list select **HTTP download**.
Under **Transport configuration**, configure the following settings:

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

Mount point upload

If the source of the feed is located on a local or network unit, from the **Transport type** drop-down list select the **Mount point upload** option.

Under **Transport configuration**, configure the following settings:

- **Mount point path**: the path to the local or network unit where the source data for the outgoing feed is stored.

Send email

> ⚠️ **Warning:** Email needs to be correctly configured in the platform system settings for this transport option to work.

If you want to make the outgoing feed data available by email, from the **Transport type** drop-down list select **Send email**. Under **Transport configuration**, configure the following settings:

- **Mail subject**: enter a short, descriptive subject for the outgoing email notifications.

- **Platform groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users. All the members of the selected group(s) will receive email notifications with the outgoing feed data.

- **Platform users**: if you want to further limit the outgoing feed email recipient targets, from the drop-down list you can select one or more users. In this case, only the selected users belonging to the designated groups will receive email notifications with the outgoing feed data.

TAXII inbox

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII inbox** transport type requires Cabby. For further details, see the **official Cabby documentation** (https://cabby.readthedocs.org/en/latest/), the **Cabby public repo on GitHub** (https://github.com/eclecticiq/cabby), and the **Cabby download page** (https://pypi.python.org/pypi/cabby/).

If you want to make the outgoing feed data available through a TAXII server and push email notifications to TAXII clients, from the **Transport type** drop-down list select **TAXII inbox**.
Under **Transport configuration**, configure the following settings:

- **Inbox service URL**: specify a valid URL address to determine the service location where the available **TAXII data collections** (https://taxiiproject.github.io/documentation/sample-use/#data-collections) are stored.
  Example:
  `https://example.com/taxii-inbox`

- **Destination collection name**: specify a valid collection as the source for the outgoing feed data.
  Example:
  `collection.Default`

- **Taxii version**: select the TAXII version your system supports:
  - Either **1.0** (https://taxiiproject.github.io/releases/1.0/)
  - Or **1.1** (https://taxiiproject.github.io/releases/1.1/)

- **EclecticIQ authentication URL**: the URL exposing the platform authentication and authorization service. The platform autorization endpoint is `/auth`.
  Example:
  `https://<platform.host>/auth`

- **Username**: a valid user name to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **Password**: a valid password to authenticate and be granted the necessary authorization to access the location of the outgoing feed content.

- **SSL certificate**: paste here a valid SSL certificate, including the `-----BEGIN CERTIFICATE-----`and `-----END CERTIFICATE-----` lines.

- **SSL key**: paste here a valid SSL private key, including the `-----BEGIN RSA PRIVATE KEY-----`and `-----END RSA PRIVATE KEY-----` lines.

- **SSL key password**: enter here the password to unlock the SSL key.

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

TAXII poll

> ⚠️ **Warning:** Before configuring a TAXII transport type for an incoming or outgoing feed, make sure the appropriate TAXII service is correctly configured in the platform sysem settings.
>
> The **TAXII poll** transport type requires Cabby. For further details, see the **official Cabby documentation** `(https://cabby.readthedocs.org/en/latest/)`, the **Cabby public repo on GitHub** `(https://github.com/eclecticiq/cabby)`, and the **Cabby download page** `(https://pypi.python.org/pypi/cabby/)`.

If you want to make the outgoing feed data available through polling — where a TAXII client polls the TAXII server to request information and data updates — from the **Transport type** drop-down list select **TAXII poll**.

- Make sure that at least one dataset is selected under **Dataset** to allow TAXII clients to request information and updates about the specified **TAXII data collection(s)** `(https://taxiiproject.github.io/documentation/sample-use/#data-collections)`.

- **Public**: default setting: deselected.
  Select this checkbox to make the outgoing feed available to all platform groups and to all platform users.
  Leave it deselected to make the outgoing feed available only to specific groups. You can select the intenden recipient groups in the **Authorized groups** drop-down menu.

- **Authorized groups**: restricts access to the outgoing feed to the groups you select from the drop-down menu, and to their member users.
  The **Authorized groups** option is available only when the **Public** checkbox is deselected (default setting).

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