eclectic iq

EclecticIQ Platform integrations

Integrate with external tools in your cyber security ecosystem

Last generated: January 12, 2018

Last generated on Jan 12, 2018

Table of contents

EclecticIQ Platform integrations

EclecticIQ Platform integrations with third-party products and systems to leverage external intel sources and improve collaboration.

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
Cisco OpenDNS integration	Integrate EclecticIQ Platform with Cisco OpenDNS through OpenResolve by OpenDNS to retrieve reverse DNS lookup information.
Flashpoint integration	Integrate EclecticIQ Platform with Flashpoint AggregINT, Flashpoint Blueprint, and Flashpoint Thresher through the Flashpoint API.
Splunk integration	EclecticIQ Platform App for Splunk Enterprise enables Splunk users to ingest large quantities of threat intelligence by integrating EclecticIQ Platform feeds with Splunk Enterprise.

Feedback

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

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

The Product Team

Cisco OpenDNS integration

Integrate EclecticIQ Platform with Cisco OpenDNS through OpenResolve by OpenDNS to retrieve reverse DNS lookup information.

Cisco OpenDNS OpenResolve	**integration**
Integration	OpenDNS OpenResolve
Type	enricher
API endpoint	`http://api.openresolve.com/{}/{}`
Input	domain, host, ipv4, ipv6
Output	Enriches supported observable types with reverse-DNS lookup information.
Description	OpenResolve by OpenDNS offers a REST API to use DNS resolvers and to retrieve reverse-DNS lookup information.

EclecticIQ Platform integrates with Cisco OpenDNS solutions to use them as intel sources. The platform integrates with the Cisco OpenDNS OpenResolve API through an enricher.

To enable the Cisco OpenDNS integration you configure the Cisco OpenDNS/OpenResolve enricher as needed, and then activate it or run it manually to poll the intel source.

Configure the enricher

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 enrichment information.
  Data sources you can enrich are incoming feeds, other enrichers, and groups.
- Within the selected platform data sources, the entity type(s) to augment with enrichment information.
- The enrichers to use to fetch 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.

Observables

Observables augment the entities they are related to by providing additional context that can help discover indirect relationships or spawn new relationships between entities.
Observables are atomic and factual: an observable represents one discrete piece of information that describes a fact. For example, an IP address, a hash value, the name of a location or an actor.

Configure enricher tasks

To configure or to edit an enricher task, do the following:

- On the top navigation bar click **Data configuration > Enrichers**.
- On the enricher overview page click the tile corresponding to the enricher you want to configure or modify.
- On the enricher detail page click the **Edit** button.

✓ Input fields marked with an asterisk are required.

- **Observable types**: select one or more observable types you want to enrich with data retrieved through the Cisco OpenDNS enricher.
  Supported observable types:
  - *domain*
  - *host*
  - *ipv4*
  - *ipv6*

The Cisco OpenDNS enricher has no specific parameters to configure.

- To modify the general options for the enricher, click **Edit**.
- Click **Save** to store your changes, or **Cancel** to discard them.

Configure enricher rules

Add enricher rules

To add a new enricher rule, do the following:

- On the top navigation bar click **Data configuration > Rules > 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 ✚ icon.

> ✓ Input fields marked with an asterisk are required.

On the **Create enrichment rule** 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, enricher, or group whose entities and observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity types 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 the current data by clicking **Save**, you can also click the downward-pointing arrow on the **Save** button to display a context menu with additional save options:

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar click **Data configuration > Rules > 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 rule detail pane click **Actions > 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**.

✔ 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, enricher, or group whose entities and observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity types 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 **Data configuration > Rules > 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 delete a specific rule, do the following:

- 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.
- On the rule detail pane click **Actions > Delete**.

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.

Run the enricher

Automatically

To automatically enrich entities, make sure enricher tasks are active, and the necessary enrichment rules are configured.

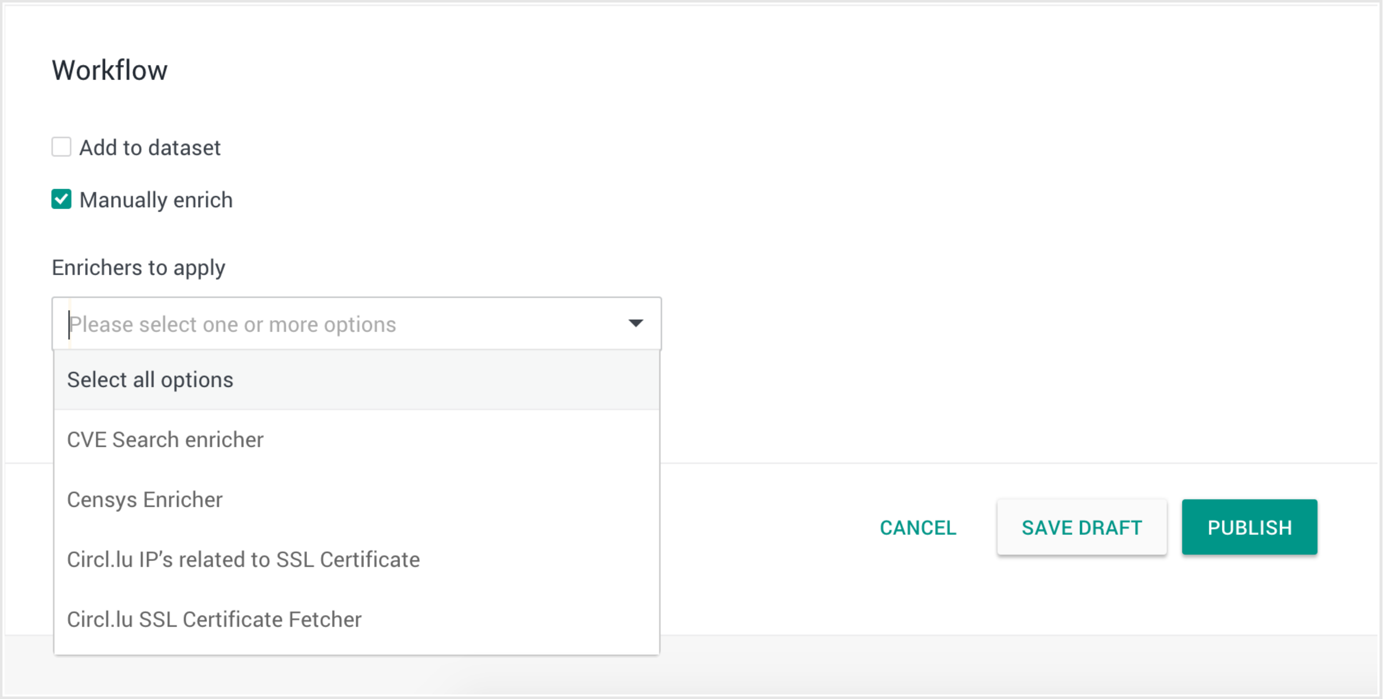
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment observable data, as well as route it to other devices that enforce cyber threat detection or prevention.

To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.
If it is deselected, check it, and then click **Save**.

Manually

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

- 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.

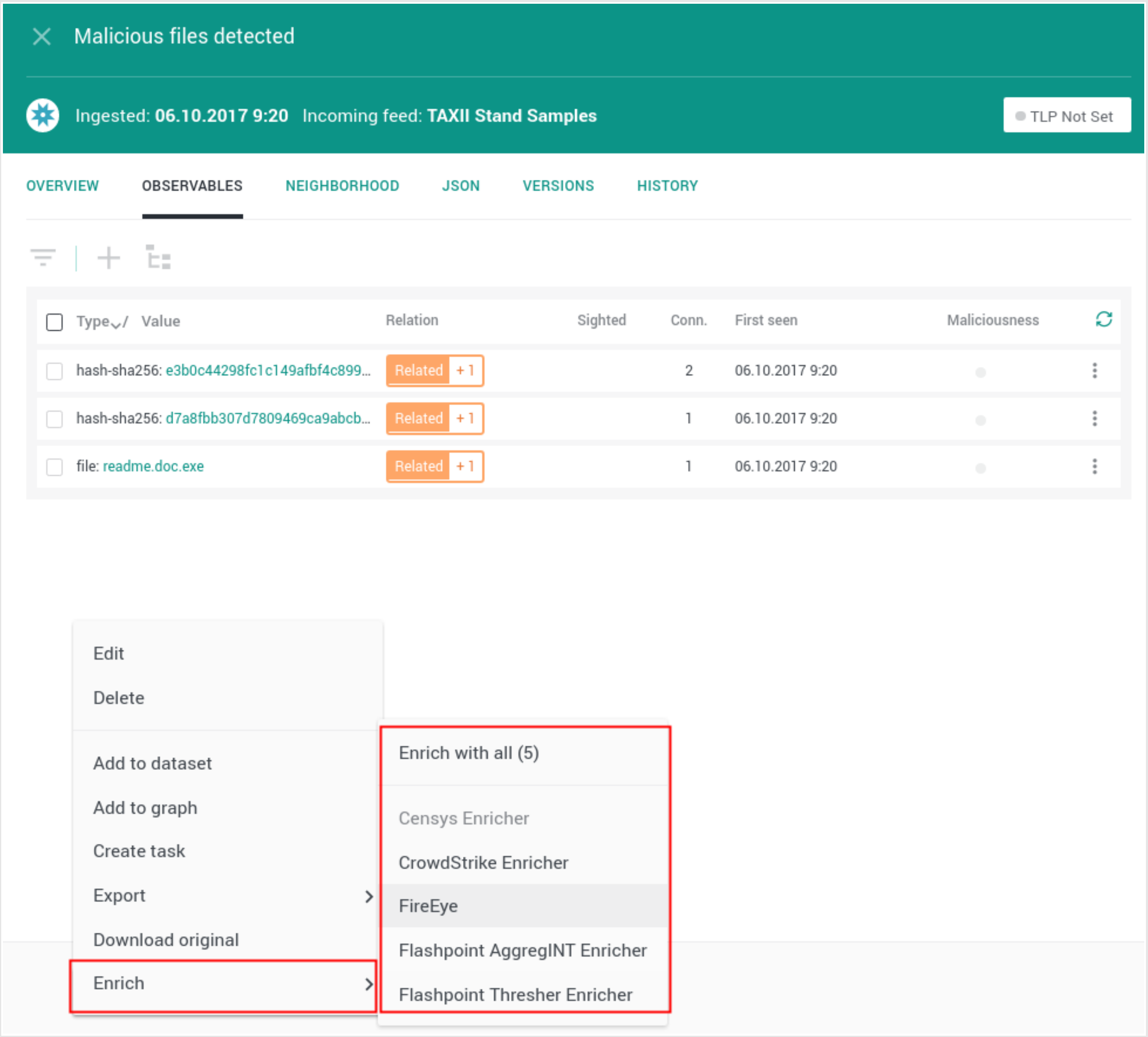
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

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 **Actions** pop-up menu, select **Enrich > Enrich with all**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



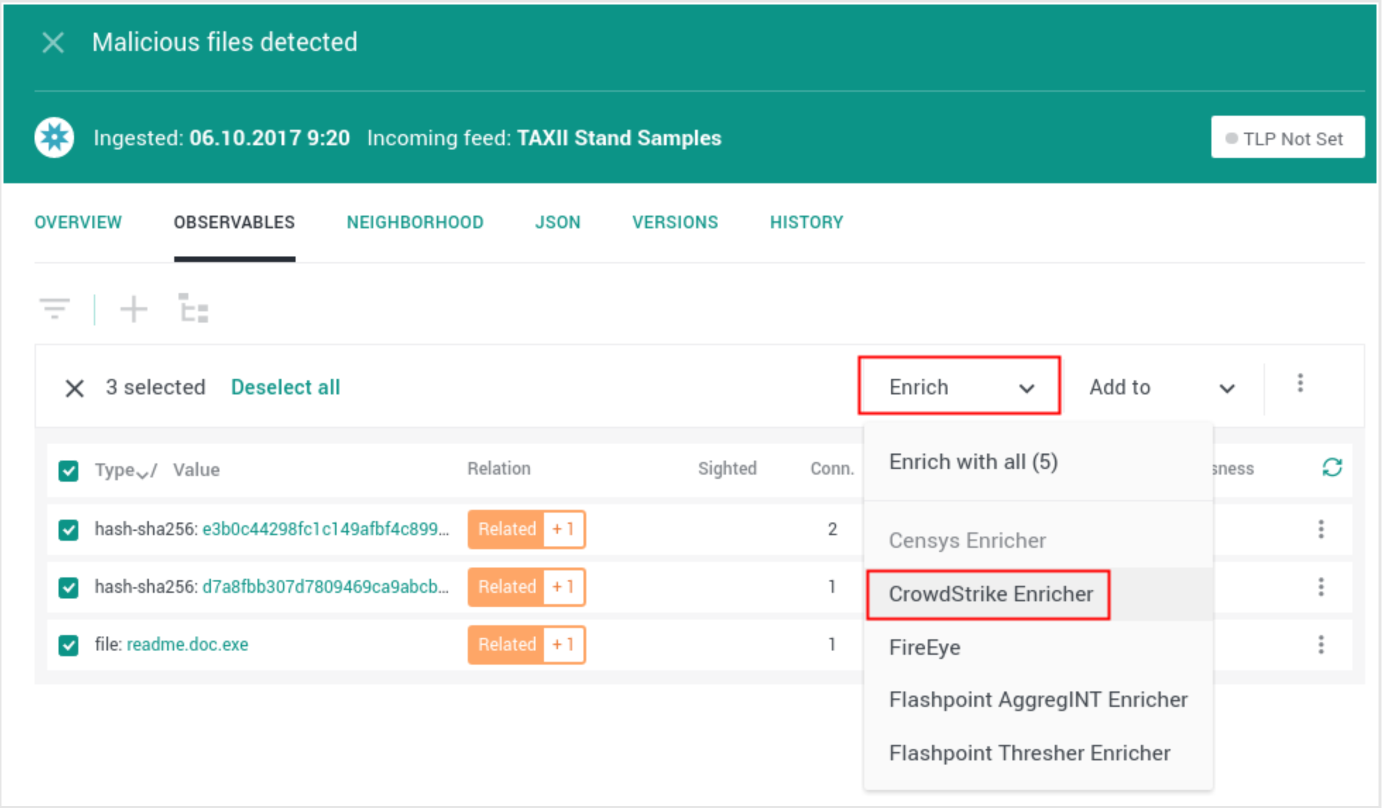
Malicious files detected

Ingested: **06.10.2017 9:20** Incoming feed: **TAXII Stand Samples**

Type / Value	Relation	Sighted	Conn.	First seen	Maliciousness
hash-sha256: e3b0c44298fc1c149afbf4c899...	Related +1		2	06.10.2017 9:20	
hash-sha256: d7a8fbb307d7809469ca9abcb...	Related +1		1	06.10.2017 9:20	
file: readme.doc.exe	Related +1		1	06.10.2017 9:20	

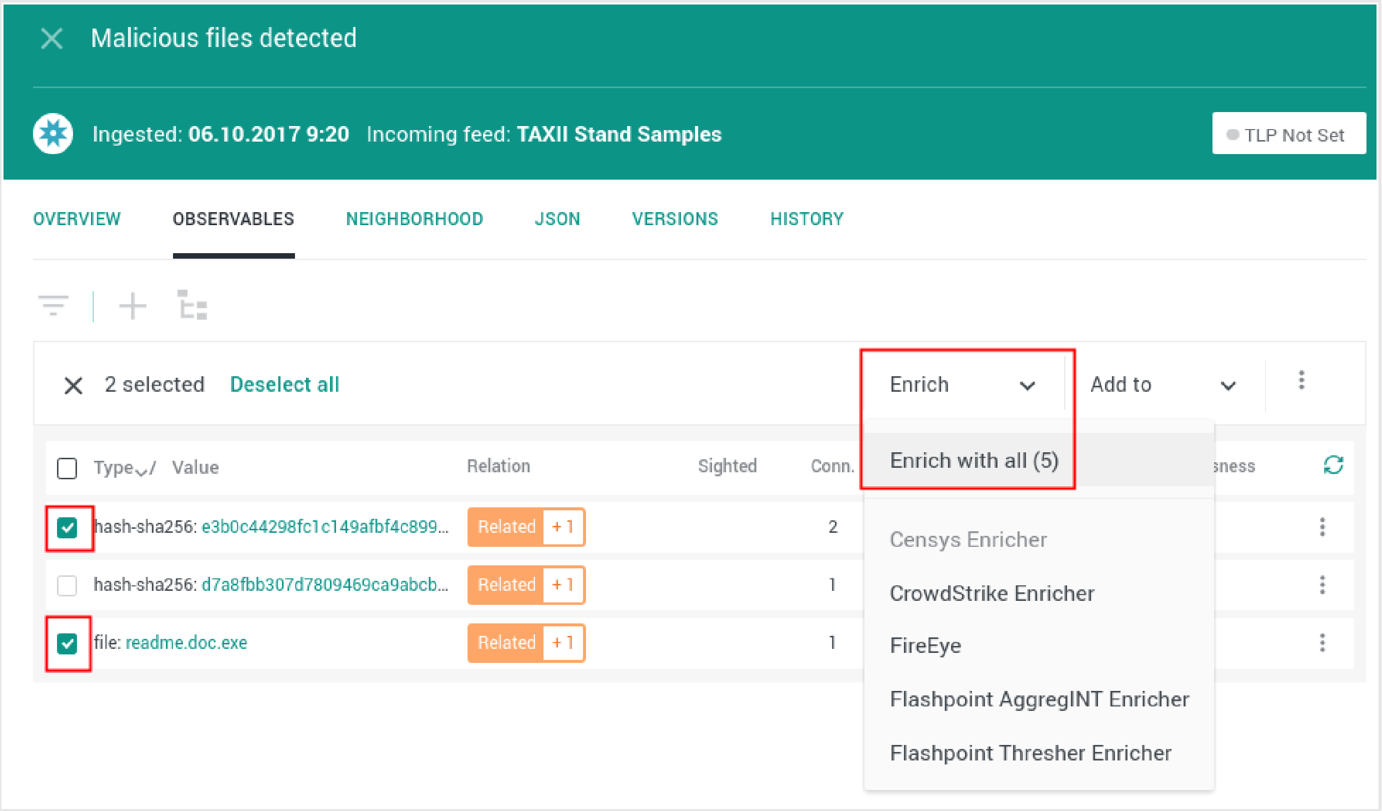
To poll a specific enricher:

- From the **Actions** pop-up menu, select **Enrich**, and then click the specific enricher whose task run you want to trigger.
- The platform polls the specified enricher for the entity, and it enriches all supported 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 with all**.
- 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.

Review enrichment observables

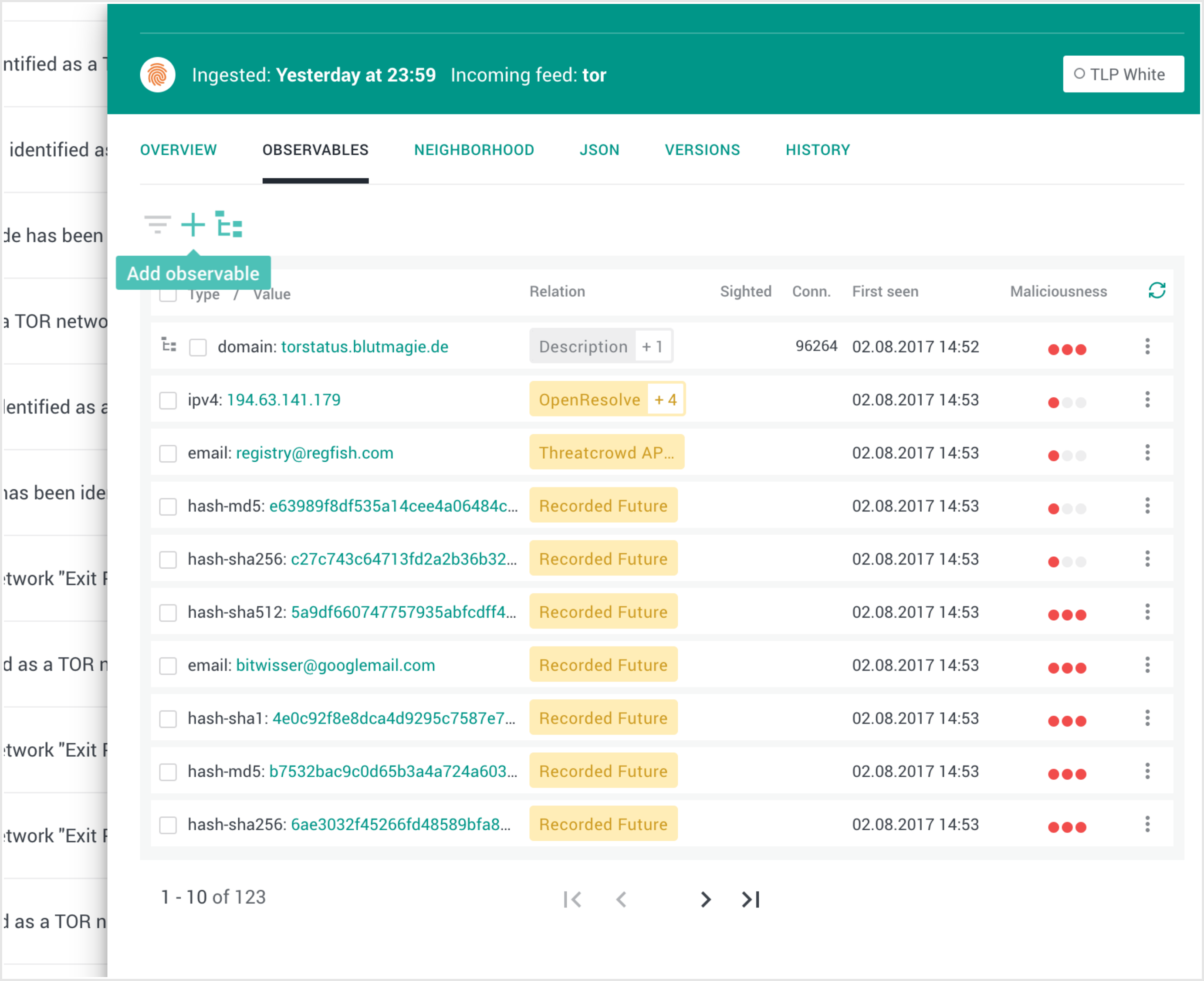
The Cisco OpenDNS enricher can take the following observable types as input:

- *domain, host, ipv4, ipv6*

The enricher uses these input data types to look for additional information to enrich existing observables with. Any entity types supporting these observable types can be enriched with OpenDNS OpenResolve.

To view enrichment information on the entity detail pane, do the following:

- Select an entity; 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.



Ingested: **Yesterday at 23:59** Incoming feed: **tor**

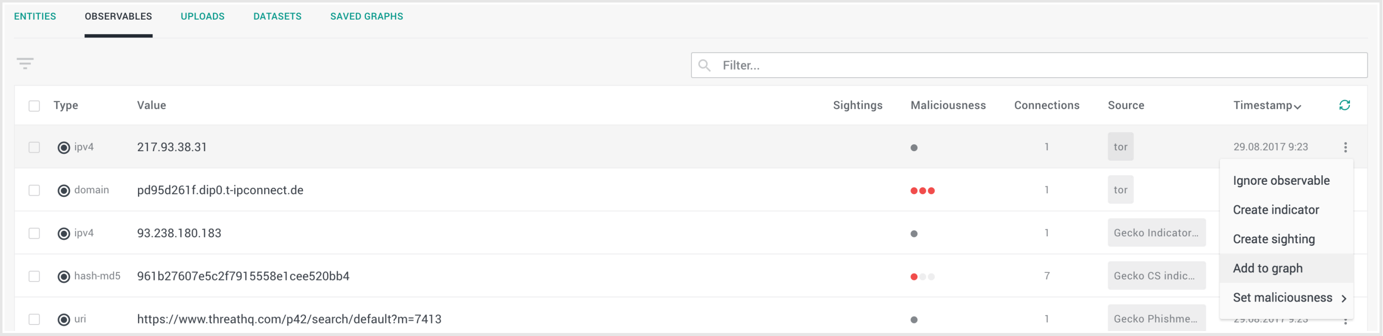
☐ Type / Value	Relation	Sighted	Conn.	First seen	Maliciousness
☐ domain: torstatus.blutmagie.de	Description + 1		96264	02.08.2017 14:52	●●●
☐ ipv4: 194.63.141.179	OpenResolve + 4			02.08.2017 14:53	●○○
☐ email: registry@regfish.com	Threatcrowd AP...			02.08.2017 14:53	●○○
☐ hash-md5: e63989f8df535a14cee4a06484c...	Recorded Future			02.08.2017 14:53	●○○
☐ hash-sha256: c27c743c64713fd2a2b36b32...	Recorded Future			02.08.2017 14:53	●○○
☐ hash-sha512: 5a9df660747757935abfcdff4...	Recorded Future			02.08.2017 14:53	●●●
☐ email: bitwisser@googlemail.com	Recorded Future			02.08.2017 14:53	●●●
☐ hash-sha1: 4e0c92f8e8dca4d9295c7587e7...	Recorded Future			02.08.2017 14:53	●●●
☐ hash-md5: b7532bac9c0d65b3a4a724a603...	Recorded Future			02.08.2017 14:53	●●●
☐ hash-sha256: 6ae3032f45266fd48589bfa8...	Recorded Future			02.08.2017 14:53	●●●

1 - 10 of 123

Review enrichment observables on the graph

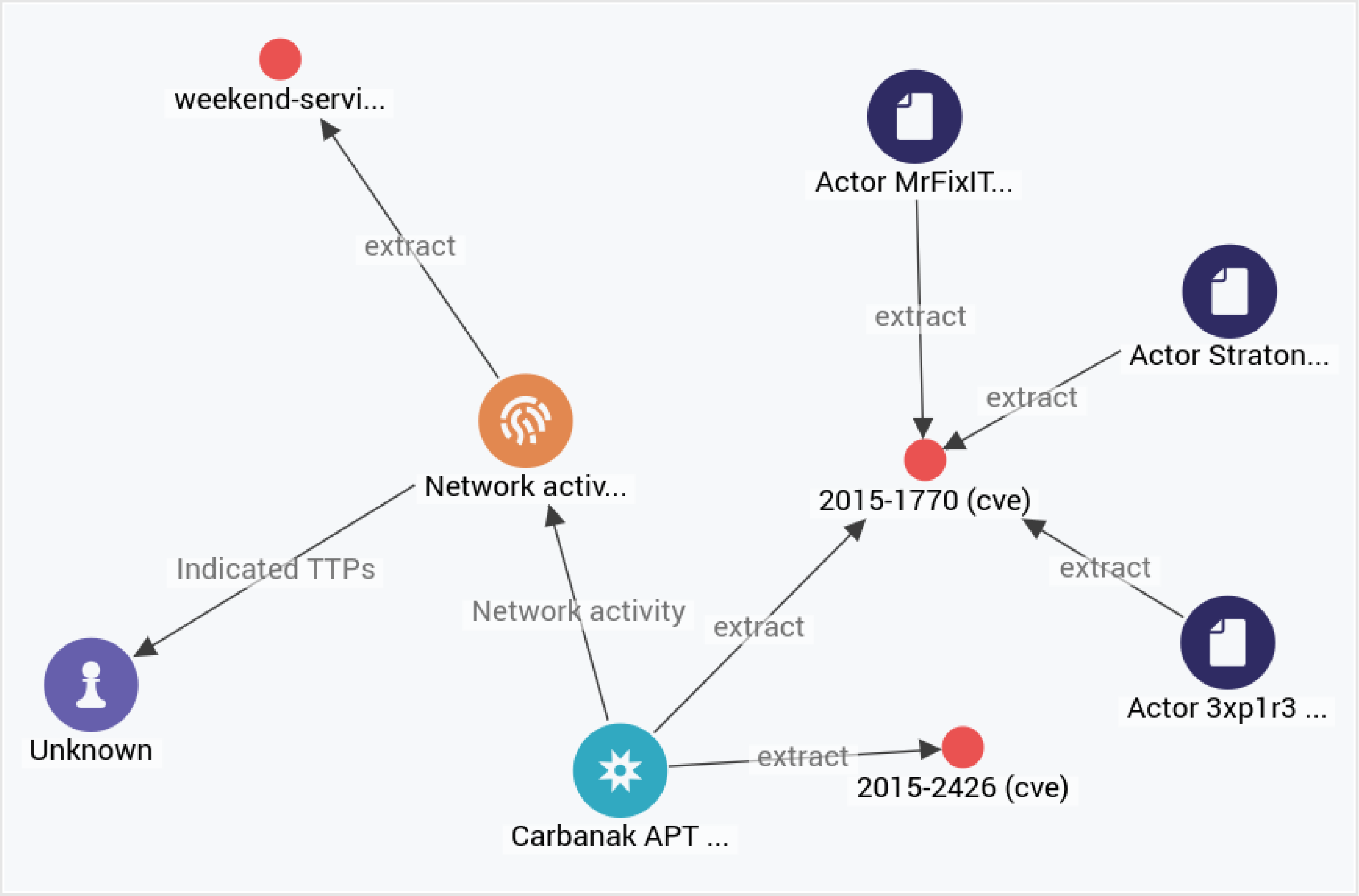
To view enrichment data and their connections with other entities and observables on the graph, do the following:

- On the row corresponding to the observable you want to load on the graph, click the ⋮ icon, and then select **Add to graph**.

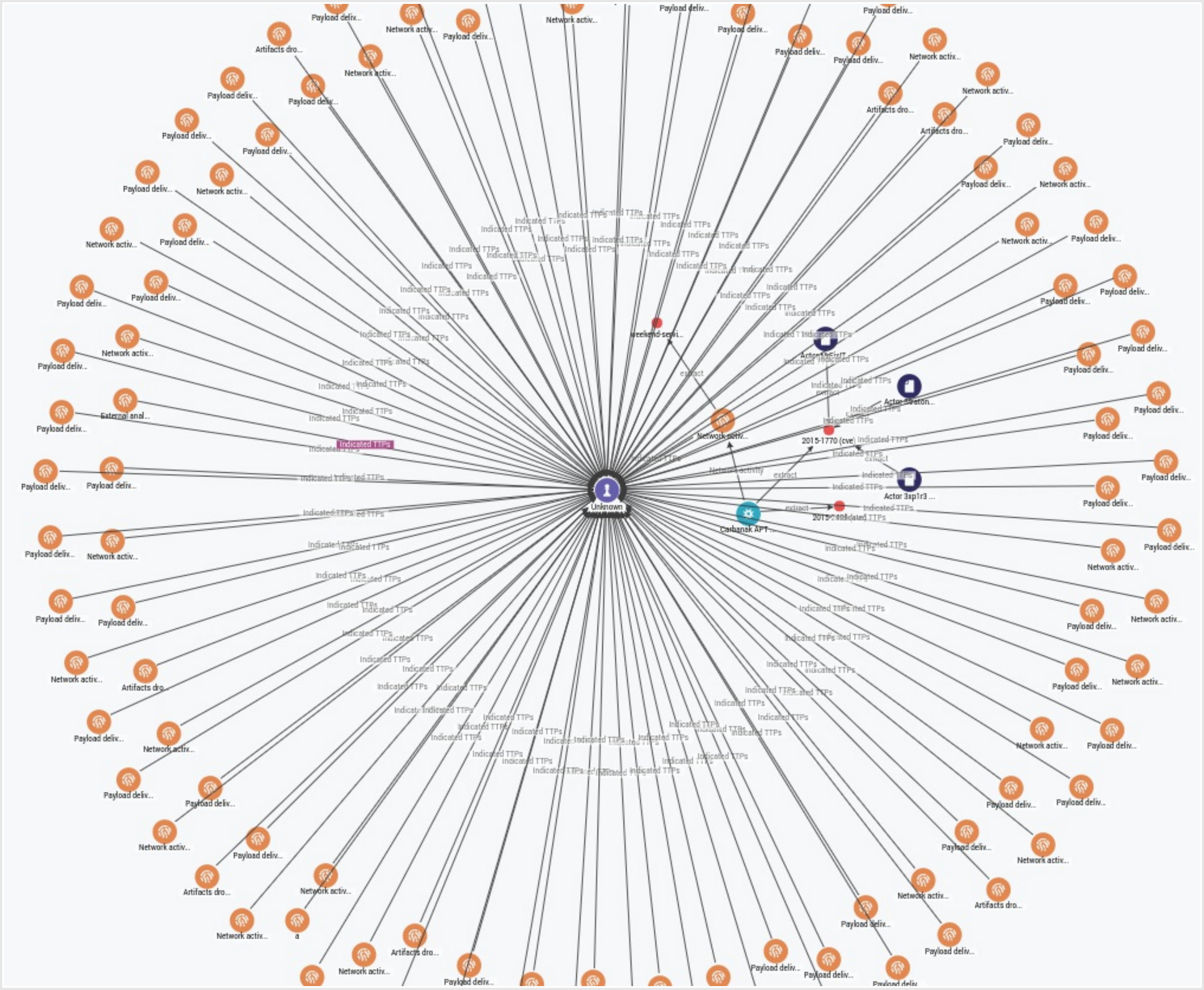


☐	Type	Value	Sightings	Maliciousness	Connections	Source	Timestamp
☐	ipv4	217.93.38.31		●	1	tor	29.08.2017 9:23
☐	domain	pd95d261f.dip0.t-ipconnect.de		●●●	1	tor	
☐	ipv4	93.238.180.183		●	1	Gecko Indicator...	
☐	hash-md5	961b27607e5c2f7915558e1cee520bb4		●○○	7	Gecko CS indic...	
☐	uri	https://www.threathq.com/p42/search/default?m=7413		●	1	Gecko Phishme...	

- To load the parent entity whose detail pane you are viewing, instead of its observables, from the pop-up **Actions** menu at the bottom of the pane select **Add to graph**.
- Click the graph thumbnail on the lower side of the screen to expand it.
- On the graph, right-click the entity you want to inspect, and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .

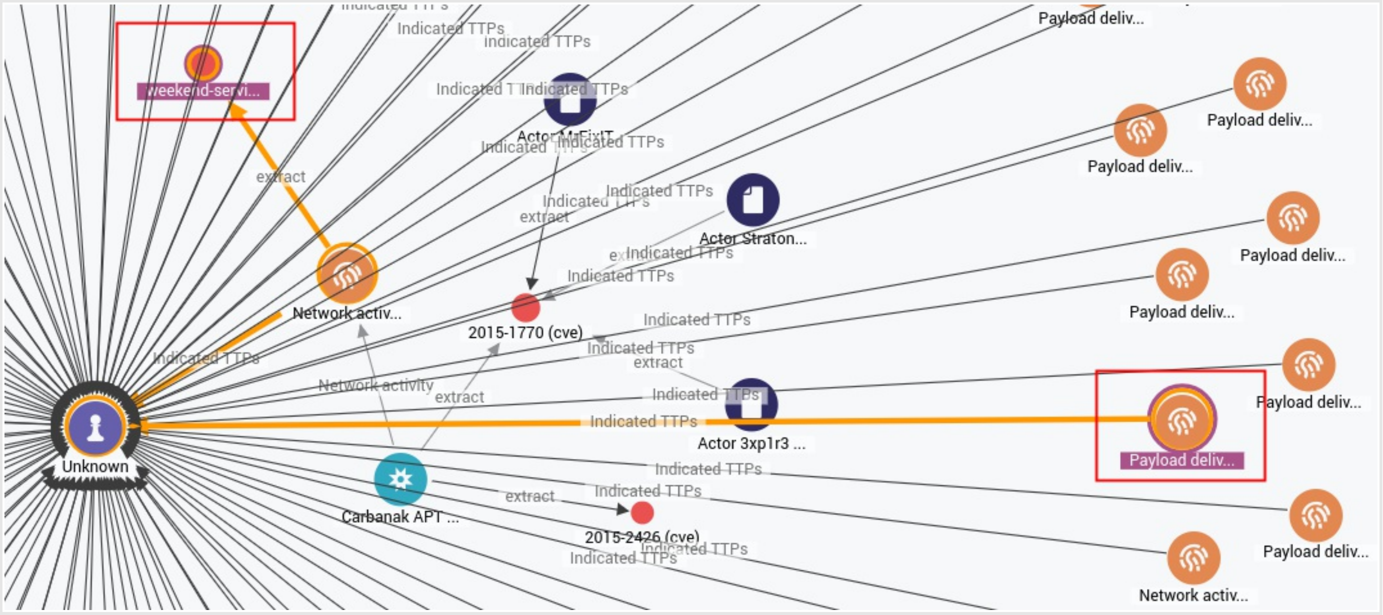


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



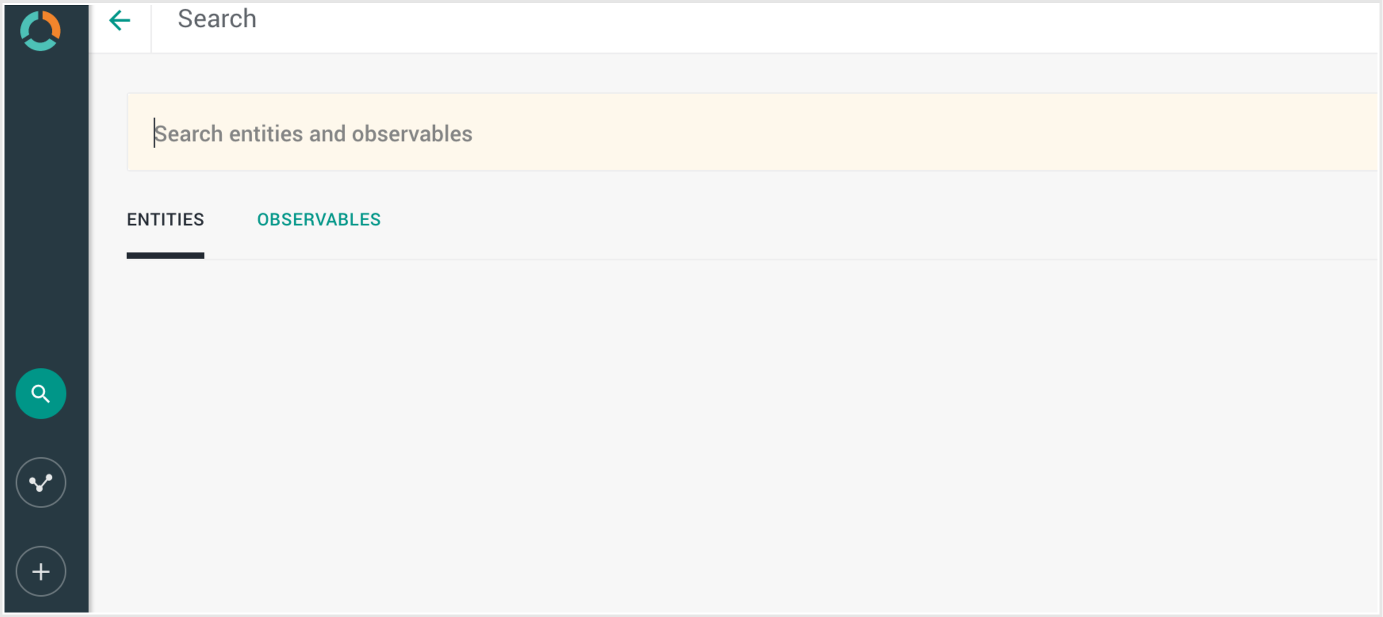
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight asn existing path on the graph.
- If a path does exist, the selected nodes and all the intermediate ones are highlighted on the graph to show the path that links them.



Search for enrichment observables

You can use the search box to look for enrichment observables. You can find the search box on the sidebar:



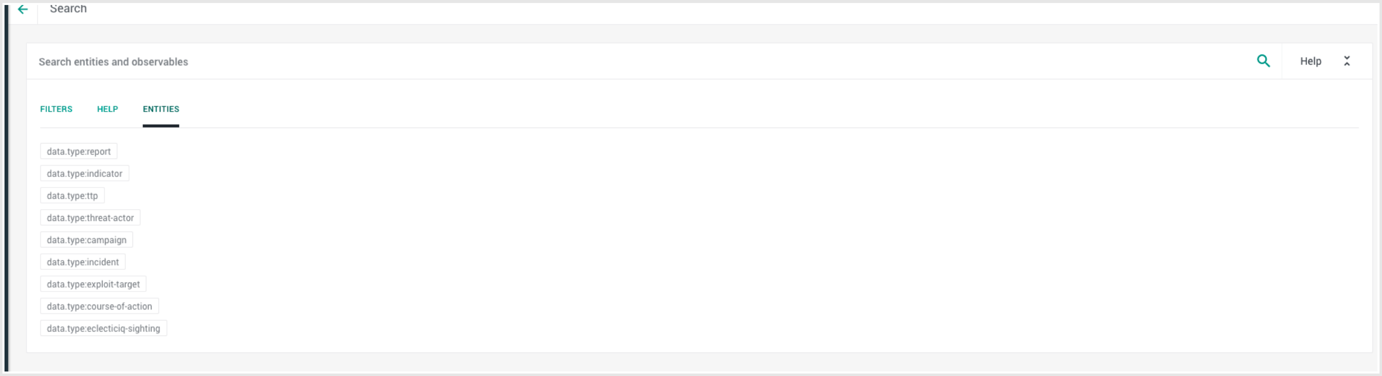
Quick search: Hover over the magnifier and enter search queries. Click the search icon to run the search.

Specific search: click the magnifier and enter search terms and search queries. Then click **ENTER** or click the search icon to run the search.
Searches you run through this search box are executed platform-wide.

The search functionality uses **Elasticsearch query syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html).`

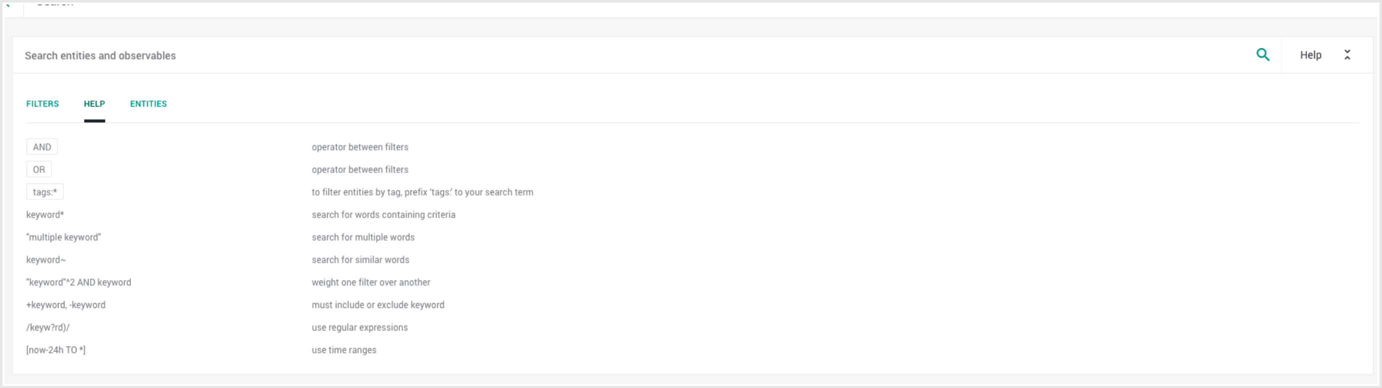
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **Filters**: examples of quick search filters.
- **Help**: examples of regex, Boolean, wildcards, and tag search usage.
- **Entities**: examples of searchable entity types.



data.type:report
data.type:indicator
data.type:ttp
data.type:threat-actor
data.type:campaign
data.type:incident
data.type:exploit-target
data.type:course-of-action
data.type:eclecticiq-sighting

Besides full text search, you can use Boolean operators, wildcards, regex, and you can combine these filtering options to create more refined searches.



AND	operator between filters
OR	operator between filters
tags:*	to filter entities by tag, prefix 'tags:' to your search term
keyword*	search for words containing criteria
"multiple keyword"	search for multiple words
keyword~	search for similar words
"keyword"^2 AND keyword	weight one filter over another
+keyword, -keyword	must include or exclude keyword
/keyw?rd)/	use regular expressions
[now-24h TO *]	use time ranges

Use operators to combine multiple quick filters and create a more complex search query.
Example:

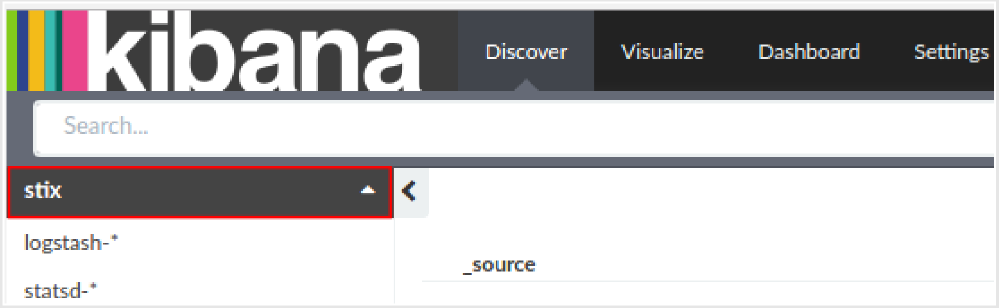
enrichment_extracts.kind:domain AND enrichment_extracts.meta.classification:high

Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean — An observable is blacklisted when it is included in the results returned by an *ignore* extraction rule. Allowed values: `true`, `false`.	`true`

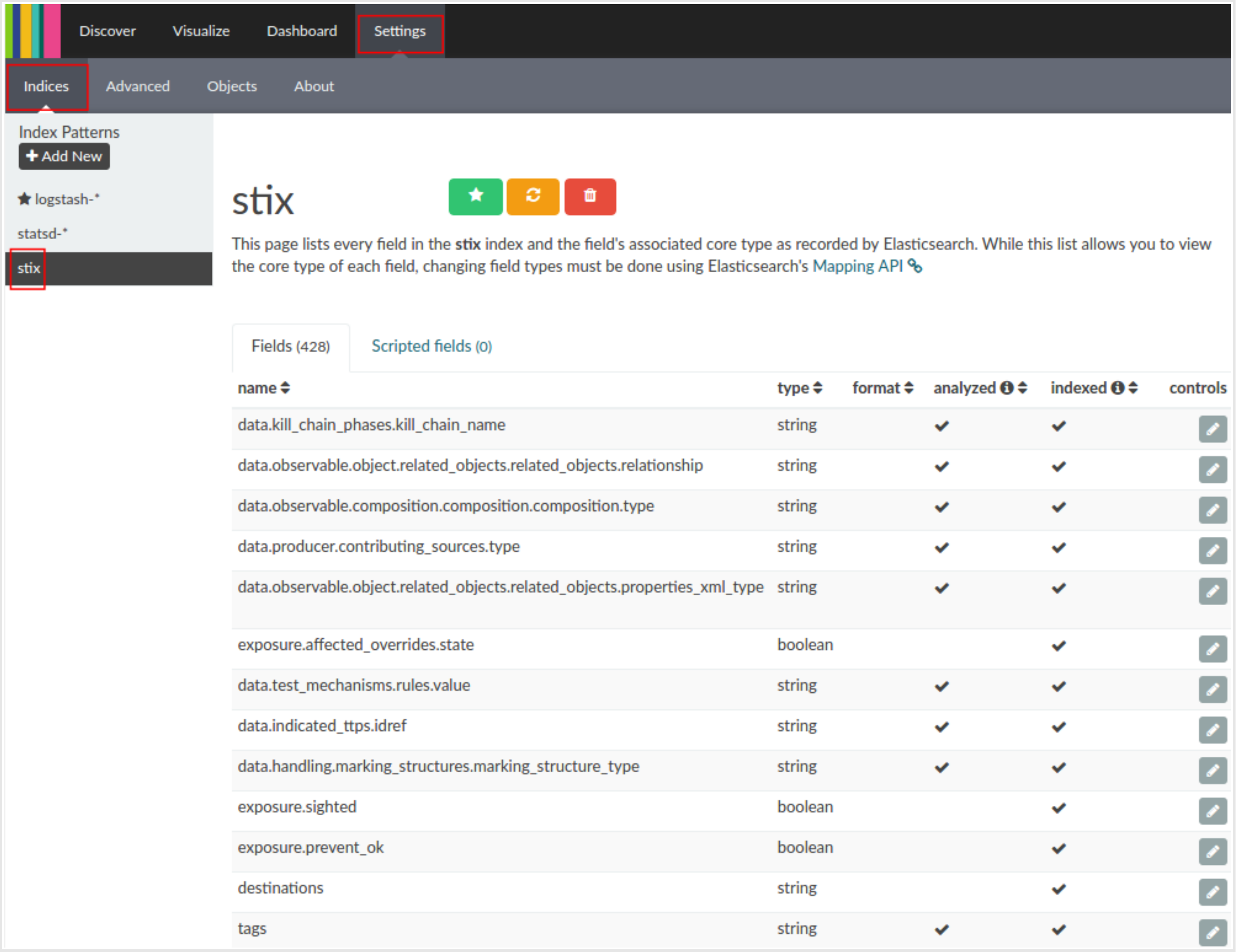
Field	Description	Example
enrichment_extracts.meta.classification	string — This value is defined in **Rules** by selecting appropriate options under **Action** and **Confidence**. Allowed classification metadata values are `good`, `bad`, and `unknown`.	`good`
enrichment_extracts.meta.confidence	string — This value is defined in **Rules** by selecting the appropriate option under **Action** and **Confidence**. The selected action must be **Mark as malicious** for the **Confidence** drop-down list to become available. Allowed confidence metadata values are `low`, `medium`, and `high`.	`high`
enrichment_extracts.value	string — The actual value of the enrichment observable, based on the enrichment observable data type.	`doom.dismay.biz`

For reference, you can look up a complete list of all available search query fields in Kibana:

- To access Kibana, in the web browser address bar enter a URL with the following format:
  https://${platform_host}/private/kibana/app/kibana#
  Keep the trailing **#**
  Example: *https://${platform_host}.com/private/kibana/app/kibana#*
- Select the **stix** index field:



- On the main menu bar, select **Settings**:



stix

This page lists every field in the **stix** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API

name	type	format	analyzed	indexed	controls
data.kill_chain_phases.kill_chain_name	string		✓	✓	✎
data.observable.object.related_objects.related_objects.relationship	string		✓	✓	✎
data.observable.composition.composition.composition.type	string		✓	✓	✎
data.producer.contributing_sources.type	string		✓	✓	✎
data.observable.object.related_objects.related_objects.properties_xml_type	string		✓	✓	✎
exposure.affected_overrides.state	boolean			✓	✎
data.test_mechanisms.rules.value	string		✓	✓	✎
data.indicated_ttps.idref	string		✓	✓	✎
data.handling.marking_structures.marking_structure_type	string		✓	✓	✎
exposure.sighted	boolean			✓	✎
exposure.prevent_ok	boolean			✓	✎
destinations	string			✓	✎
tags	string		✓	✓	✎

Flashpoint integration

Integrate EclecticIQ Platform with Flashpoint AggregINT, Flashpoint Blueprint, and Flashpoint Thresher through the Flashpoint API.

Configure the enrichers

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 enrichment information.
  Data sources you can enrich are incoming feeds, other enrichers, and groups.
- Within the selected platform data sources, the entity type(s) to augment with enrichment information.
- The enrichers to use to fetch 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.

Observables

Observables augment the entities they are related to by providing additional context that can help discover indirect relationships or spawn new relationships between entities.
Observables are atomic and factual: an observable represents one discrete piece of information that describes a fact.
For example, an IP address, a hash value, the name of a location or an actor.

The Flashpoint AggregINT, Flashpoint Blueprint, and Flashpoint Thresher enrichers share almost identical configuration options, the only differences being the number and the type of available Flashpoint datasets per enricher.

Configure enricher tasks

To configure or to edit an enricher task, do the following:

- On the top navigation bar click **Data configuration > Enrichers** .

- On the enricher overview page click the tile corresponding to the enricher you want to configure or modify.
- On the enricher detail page click the **Edit** button.

✓ 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 feed or enricher content with a predefined reliability value to help other users assess how trustworthy the data 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 enricher or the rule is executed automatically.
  If you deselect it, you need to manually run the enricher or the rule.
- Under **Parameters**, define the specific configuration options for the selected enricher, where applicable.
- Click **Save** to store your changes, or **Cancel** to discard them.

Configure enricher rules

Add enricher rules

To add a new enricher rule, do the following:

- On the top navigation bar click **Data configuration > Rules > 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 ✚ icon.

✓ Input fields marked with an asterisk are required.

On the **Create enrichment rule** 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, enricher, or group whose entities and observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity types 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 the current data by clicking **Save**, you can also click the downward-pointing arrow on the **Save** button to display a context menu with additional save options:

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar click **Data configuration > Rules > 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 rule detail pane click **Actions > 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**.

> ✔ 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, enricher, or group whose entities and observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity types 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 **Data configuration > Rules > 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 delete a specific rule, do the following:

- 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.
- On the rule detail pane click **Actions > Delete**.

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.

Run the enricher

Automatically

To automatically enrich entities, make sure enricher tasks are active, and the necessary enrichment rules are configured.

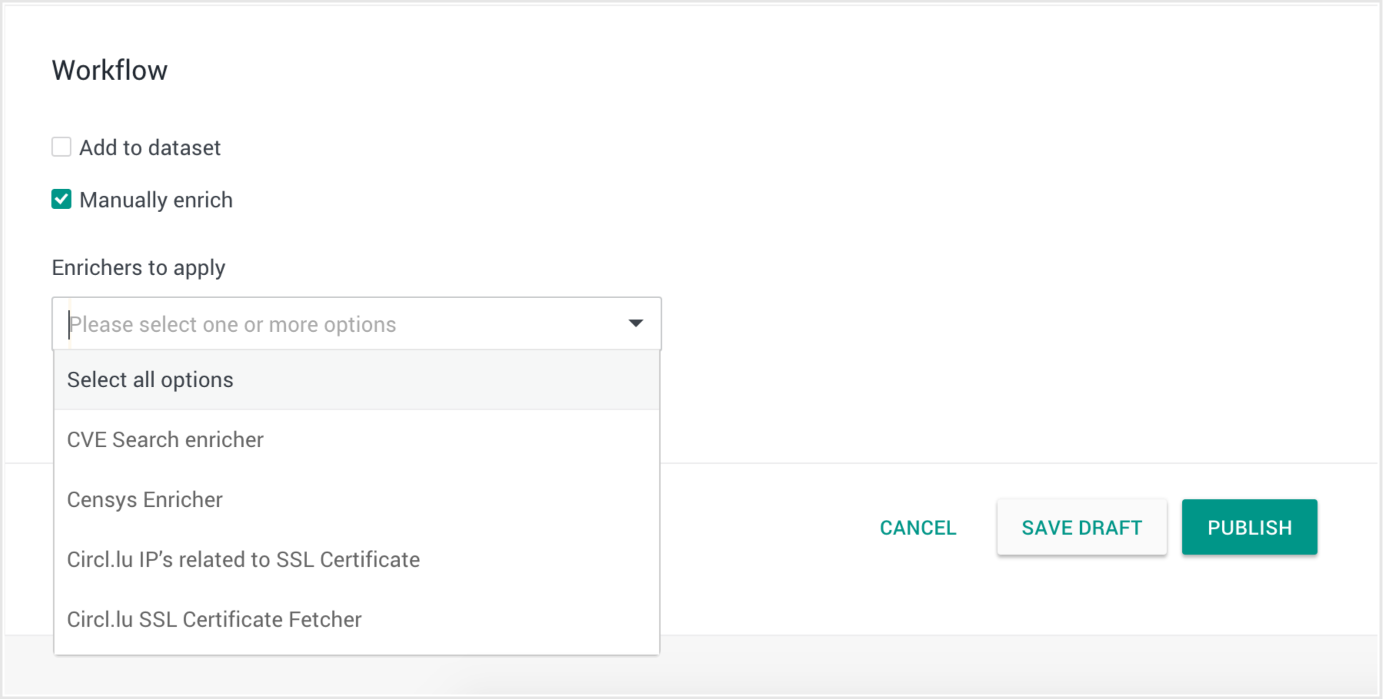
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment observable data, as well as route it to other devices that enforce cyber threat detection or prevention.

To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.
If it is deselected, check it, and then click **Save**.

Manually

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
CVE Search enricher
Censys Enricher
Circl.lu IP's related to SSL Certificate
Circl.lu SSL Certificate Fetcher
CANCEL
SAVE DRAFT
PUBLISH

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

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.

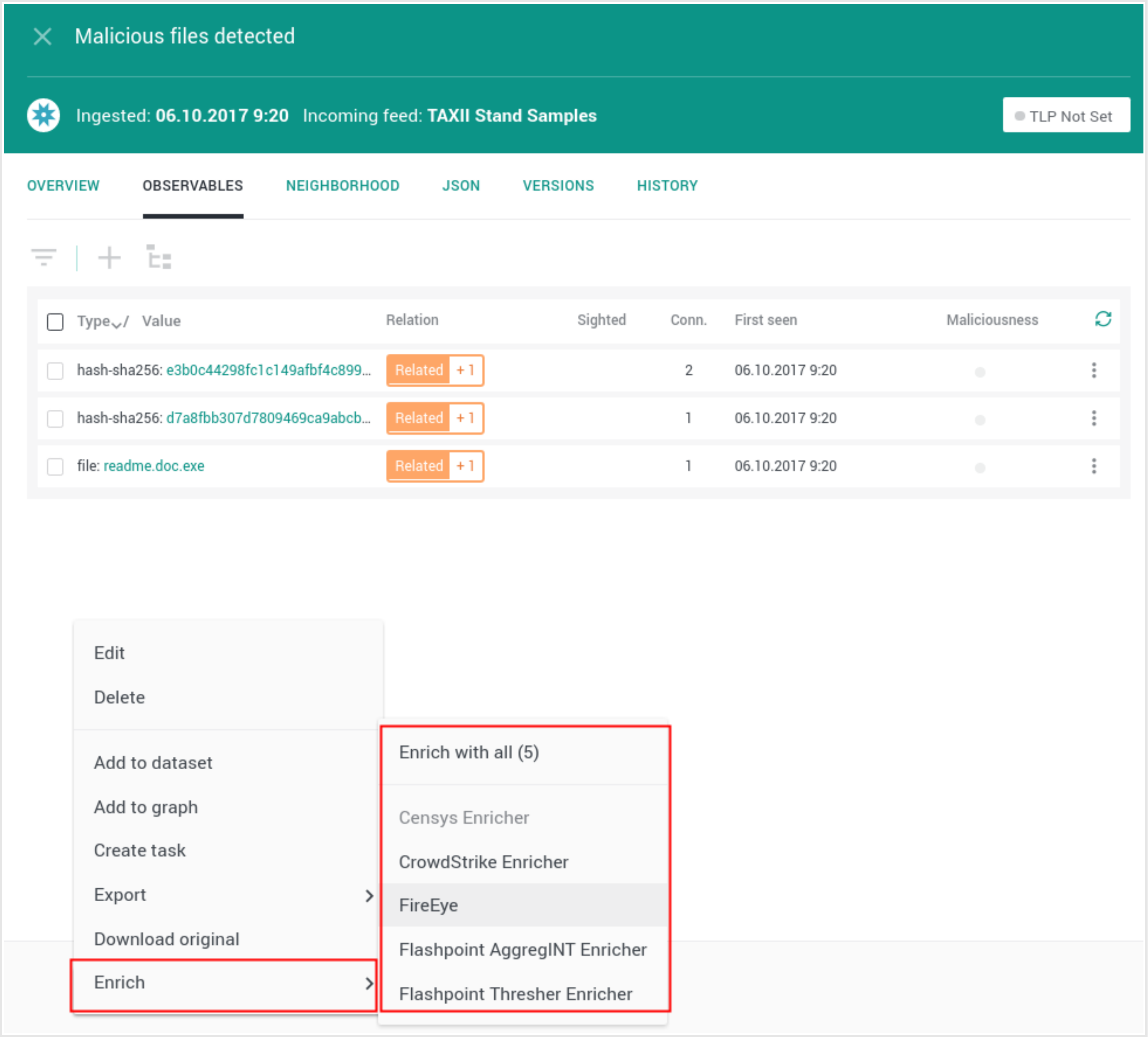
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

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 **Actions** pop-up menu, select **Enrich > Enrich with all**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



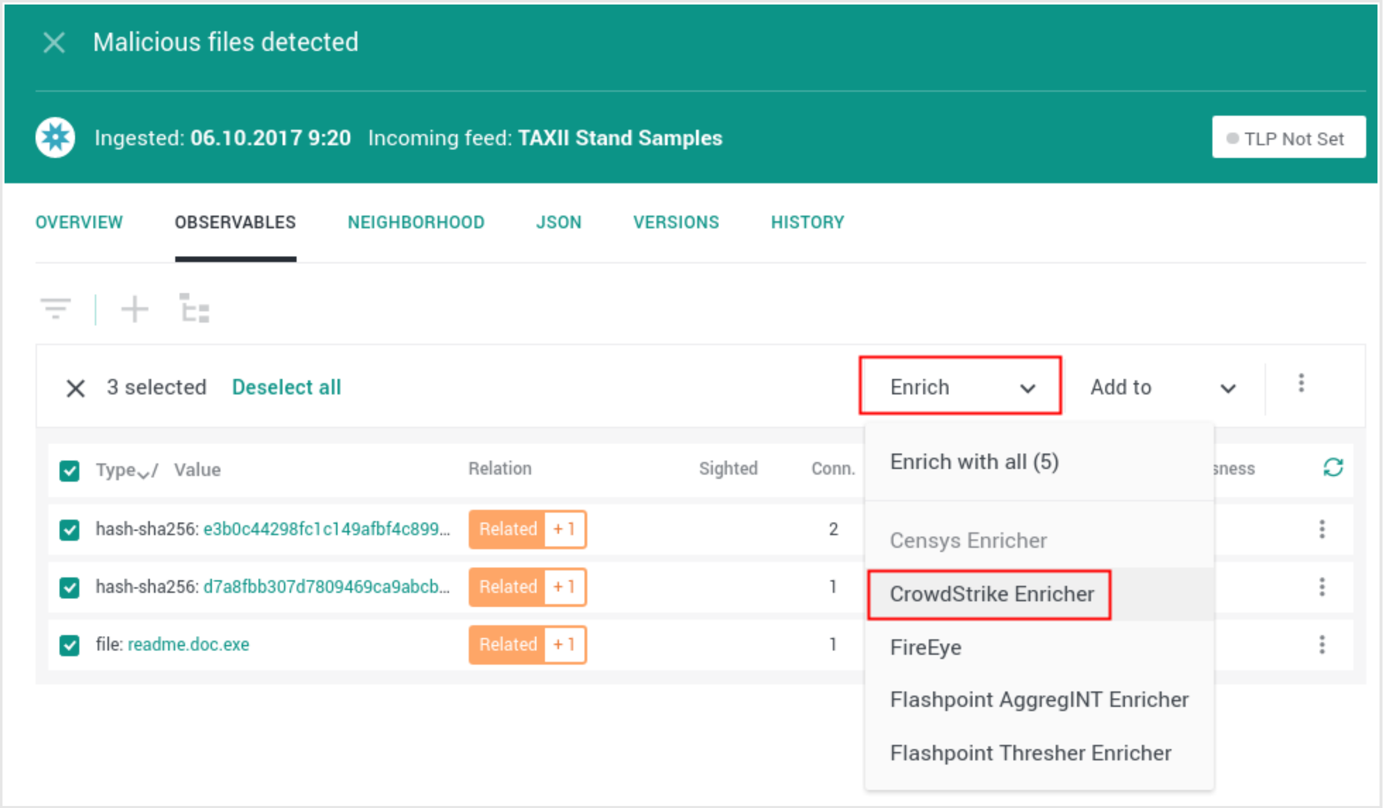
Malicious files detected

Ingested: **06.10.2017 9:20** Incoming feed: **TAXII Stand Samples**

☐ Type / Value	Relation	Sighted	Conn.	First seen	Maliciousness
☐ hash-sha256: e3b0c44298fc1c149afbf4c899…	Related +1		2	06.10.2017 9:20	
☐ hash-sha256: d7a8fbb307d7809469ca9abcb…	Related +1		1	06.10.2017 9:20	
☐ file: readme.doc.exe	Related +1		1	06.10.2017 9:20	

To poll a specific enricher:

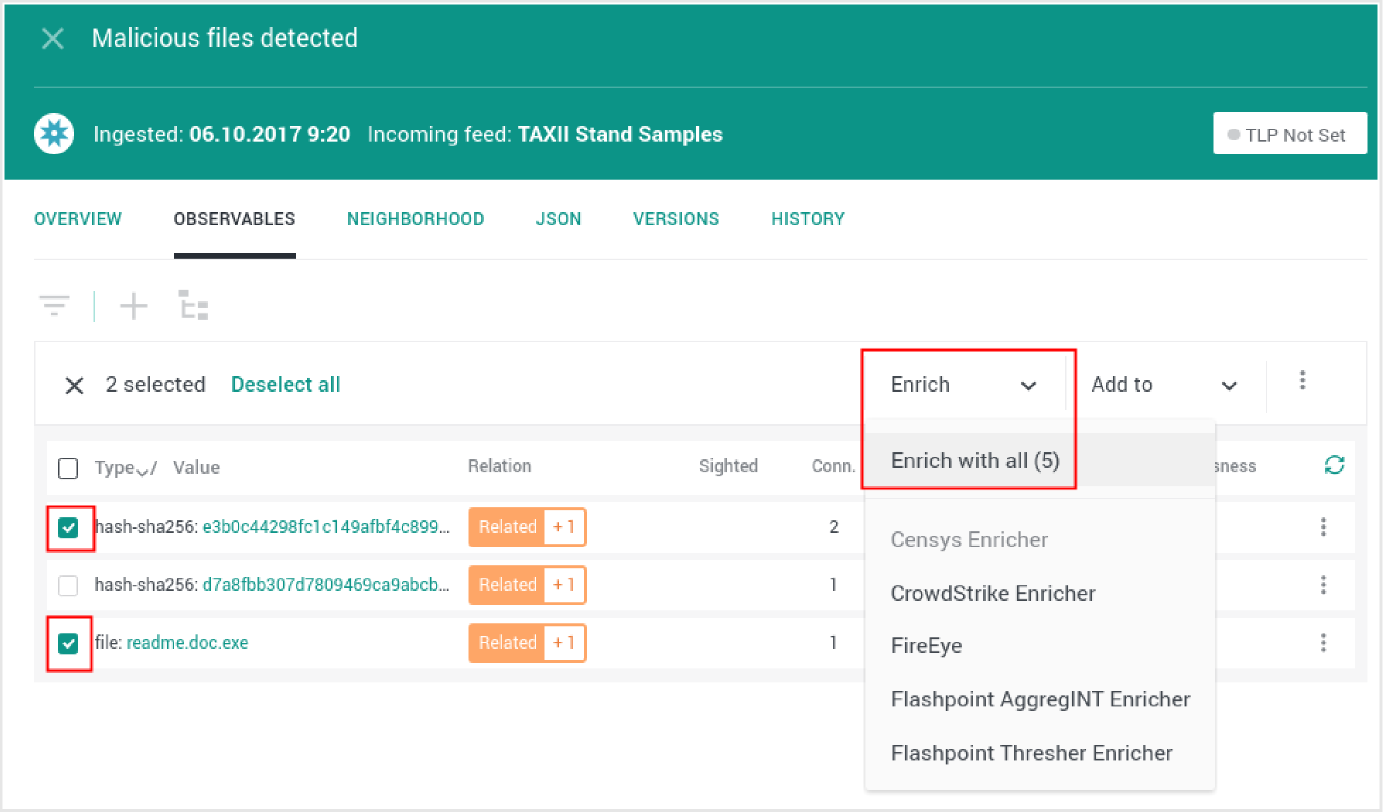
- From the **Actions** pop-up menu, select **Enrich**, and then click the specific enricher whose task run you want to trigger.
- The platform polls the specified enricher for the entity, and it enriches all supported entity observables with the retrieved data.



	Type / Value	Relation	Sighted	Conn.
☑	hash-sha256: e3b0c44298fc1c149afbf4c899...	Related +1		2
☑	hash-sha256: d7a8fbb307d7809469ca9abcb...	Related +1		1
☑	file: readme.doc.exe	Related +1		1

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 with all**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



	Type / Value	Relation	Sighted	Conn.
☑	hash-sha256: e3b0c44298fc1c149afbf4c899...	Related +1		2
☐	hash-sha256: d7a8fbb307d7809469ca9abcb...	Related +1		1
☑	file: readme.doc.exe	Related +1		1

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.

Review enrichment observables

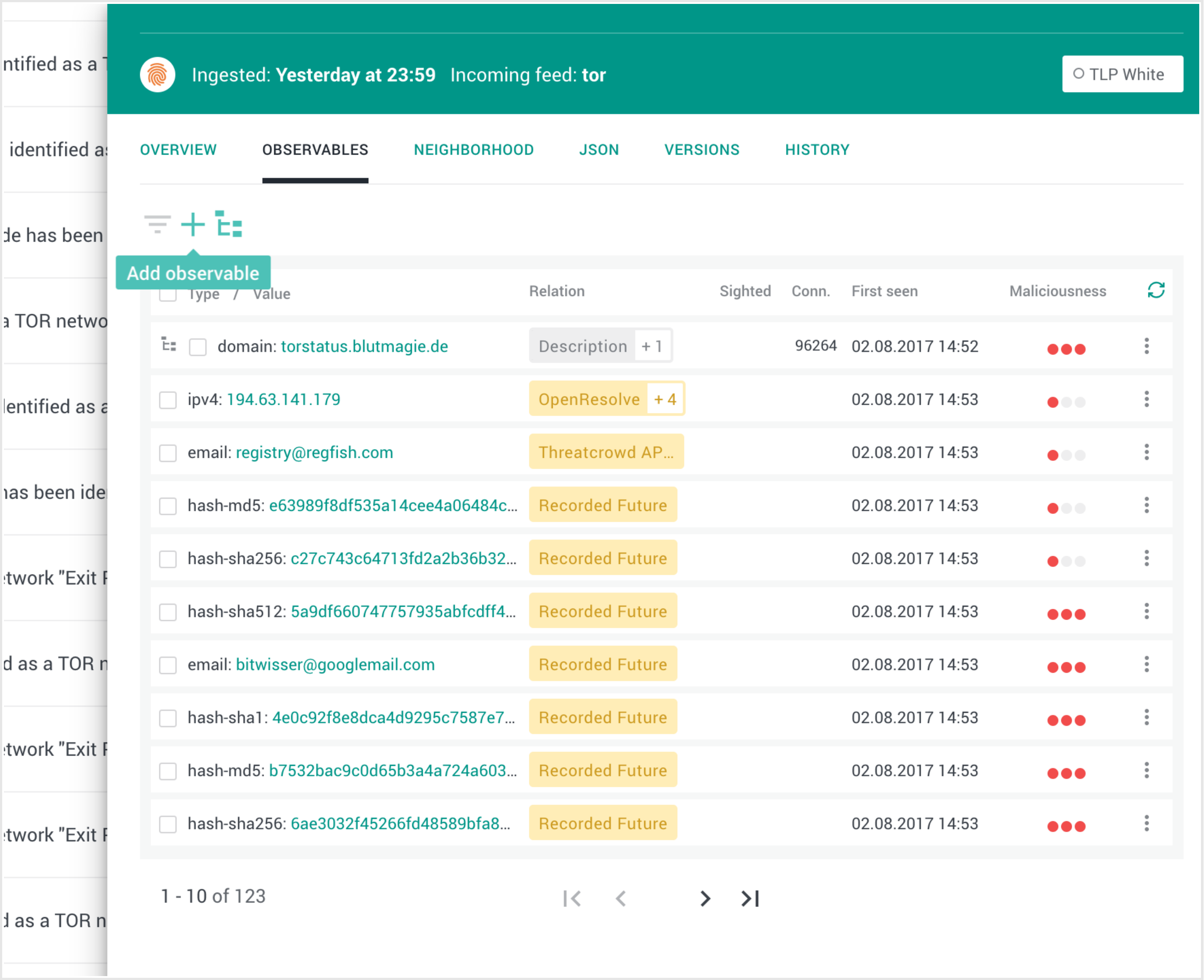
Flashpoint enrichers can take the following observable types as input:

- *actor-id, domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri*

The enrichers use these data types to look for additional information on observables. Any entity types supporting these observable types can be enriched with Flashpoint enrichers.

To view enrichment information on the entity detail pane, do the following:

- Select an entity; 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.



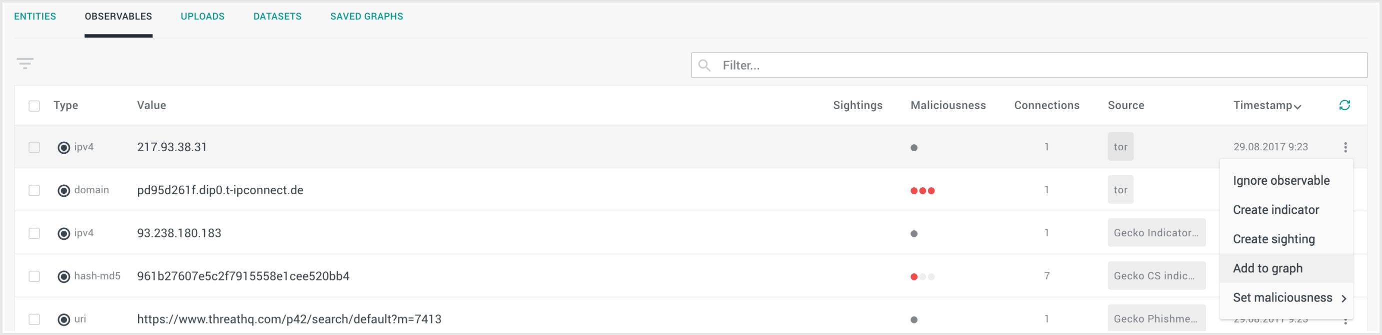
Type / Value	Relation	Sighted	Conn.	First seen	Maliciousness
domain: torstatus.blutmagie.de	Description + 1		96264	02.08.2017 14:52	●●●
ipv4: 194.63.141.179	OpenResolve + 4			02.08.2017 14:53	●○○
email: registry@regfish.com	Threatcrowd AP...			02.08.2017 14:53	●○○
hash-md5: e63989f8df535a14cee4a06484c...	Recorded Future			02.08.2017 14:53	●○○
hash-sha256: c27c743c64713fd2a2b36b32...	Recorded Future			02.08.2017 14:53	●○○
hash-sha512: 5a9df660747757935abfcdff4...	Recorded Future			02.08.2017 14:53	●●●
email: bitwisser@googlemail.com	Recorded Future			02.08.2017 14:53	●●●
hash-sha1: 4e0c92f8e8dca4d9295c7587e7...	Recorded Future			02.08.2017 14:53	●●●
hash-md5: b7532bac9c0d65b3a4a724a603...	Recorded Future			02.08.2017 14:53	●●●
hash-sha256: 6ae3032f45266fd48589bfa8...	Recorded Future			02.08.2017 14:53	●●●

1 - 10 of 123

Review enrichment observables on the graph

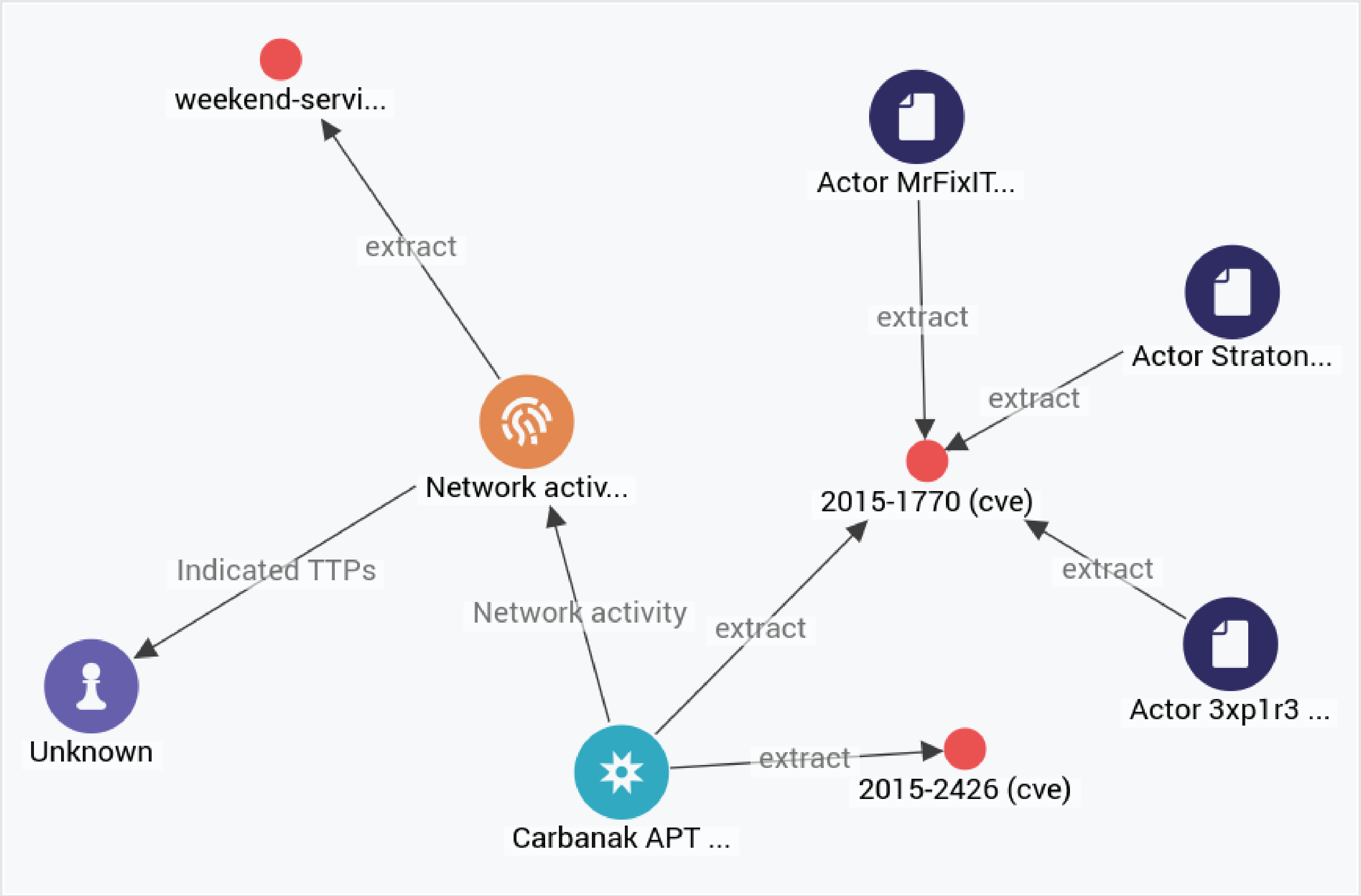
To view enrichment data and their connections with other entities and observables on the graph, do the following:

- On the row corresponding to the observable you want to load on the graph, click the ⋮ icon, and then select **Add to graph**.

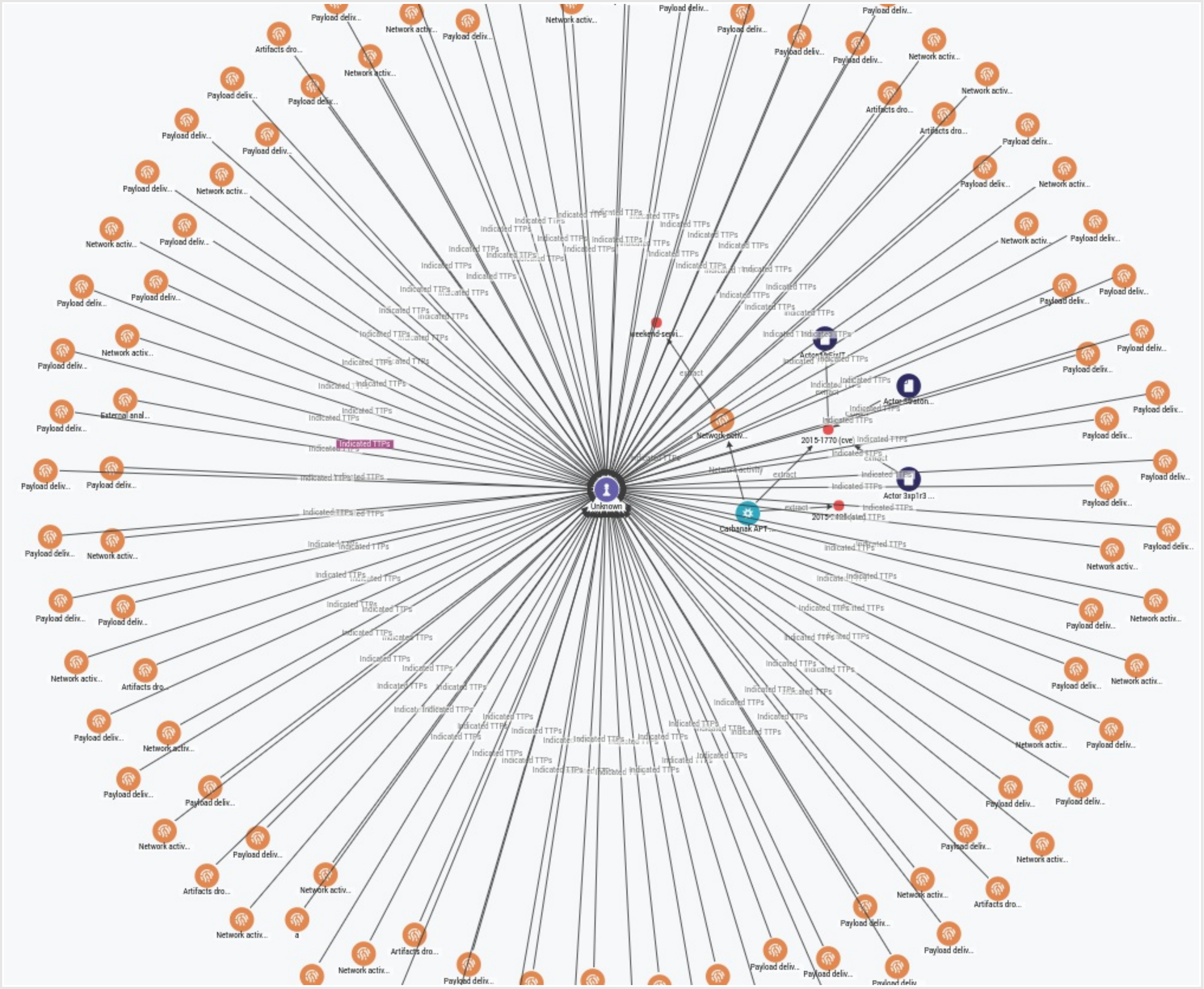


☐	Type	Value	Sightings	Maliciousness	Connections	Source	Timestamp
☐	ipv4	217.93.38.31		●	1	tor	29.08.2017 9:23
☐	domain	pd95d261f.dip0.t-ipconnect.de		●●●	1	tor	
☐	ipv4	93.238.180.183		●	1	Gecko Indicator...	
☐	hash-md5	961b27607e5c2f7915558e1cee520bb4		●○○	7	Gecko CS indic...	
☐	uri	https://www.threathq.com/p42/search/default?m=7413		●	1	Gecko Phishme...	

- To load the parent entity whose detail pane you are viewing, instead of its observables, from the pop-up **Actions** menu at the bottom of the pane select **Add to graph**.
- Click the graph thumbnail on the lower side of the screen to expand it.
- On the graph, right-click the entity you want to inspect, and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .

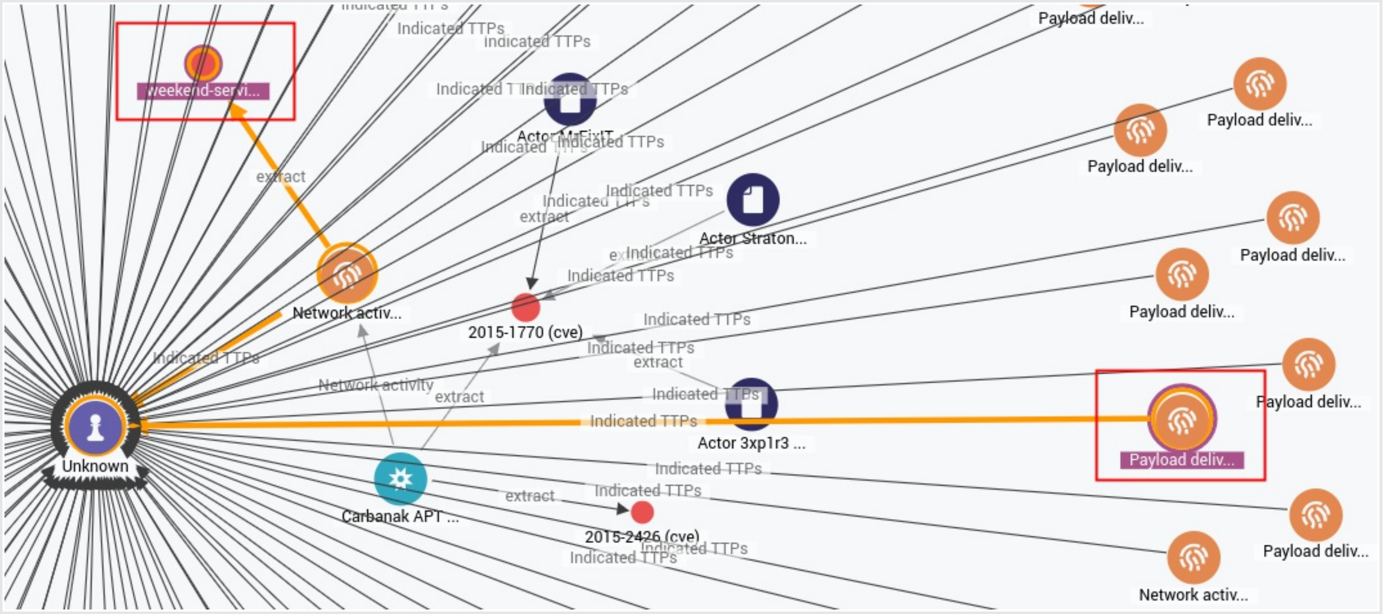


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



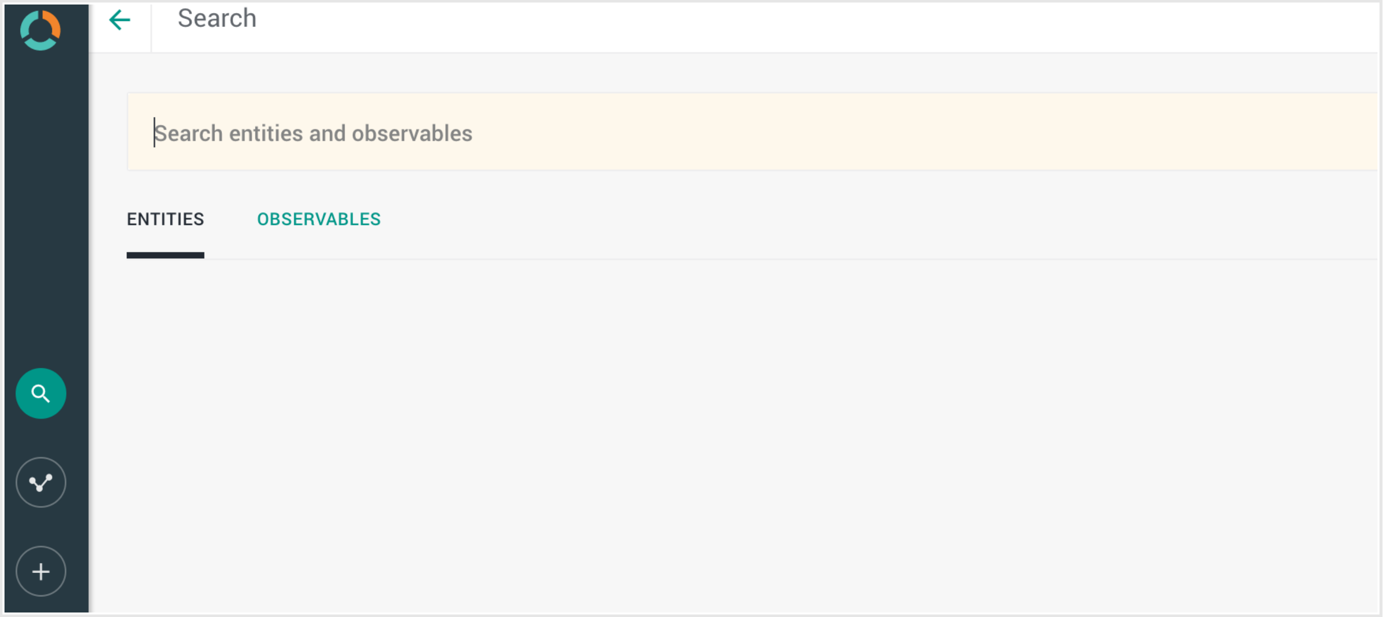
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight asn existing path on the graph.
- If a path does exist, the selected nodes and all the intermediate ones are highlighted on the graph to show the path that links them.



Search for enrichment observables

You can use the search box to look for enrichment observables. You can find the search box on the sidebar:



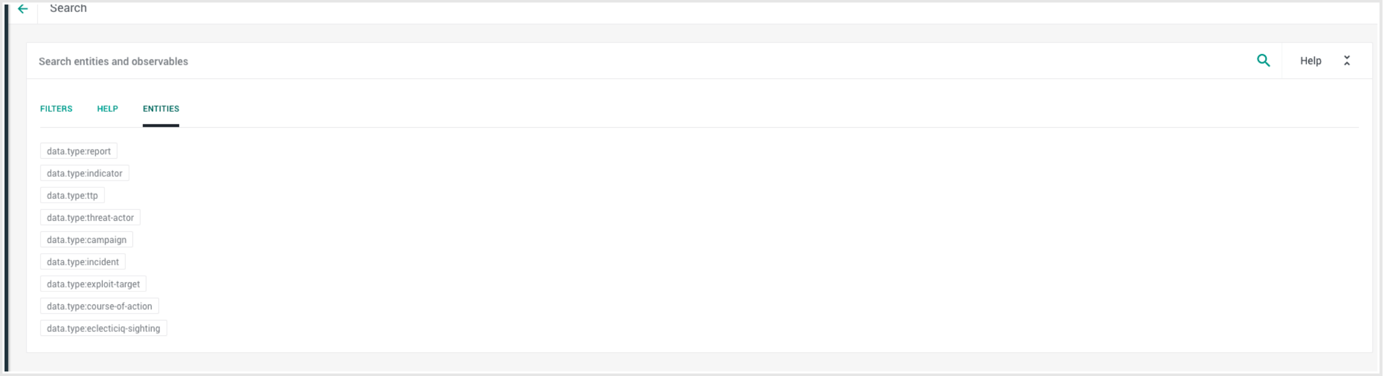
Quick search: Hover over the magnifier and enter search queries. Click the search icon to run the search.

Specific search: click the magnifier and enter search terms and search queries. Then click **ENTER** or click the search icon to run the search.
Searches you run through this search box are executed platform-wide.

The search functionality uses **Elasticsearch query syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html).`

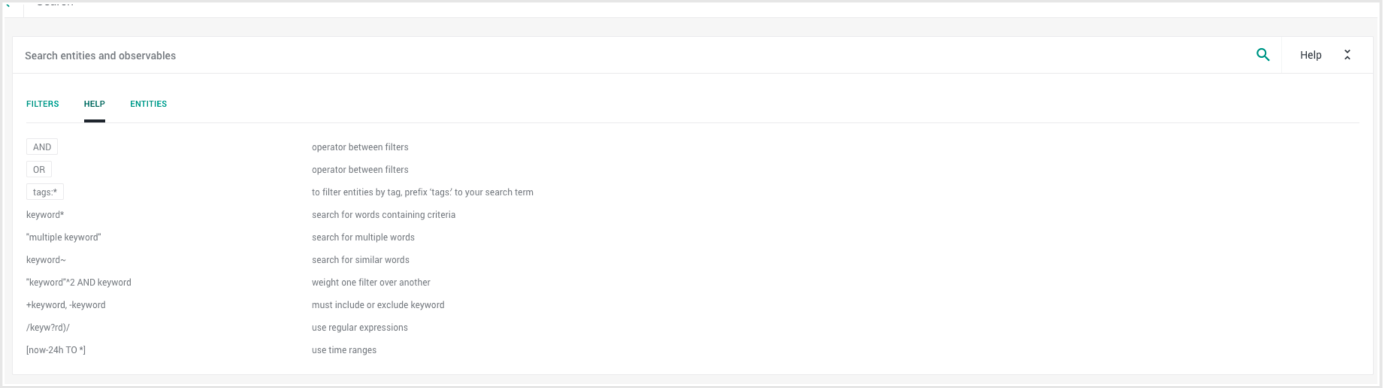
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **Filters**: examples of quick search filters.
- **Help**: examples of regex, Boolean, wildcards, and tag search usage.
- **Entities**: examples of searchable entity types.



data.type:report
data.type:indicator
data.type:ttp
data.type:threat-actor
data.type:campaign
data.type:incident
data.type:exploit-target
data.type:course-of-action
data.type:eclecticiq-sighting

Besides full text search, you can use Boolean operators, wildcards, regex, and you can combine these filtering options to create more refined searches.



AND	operator between filters
OR	operator between filters
tags:*	to filter entities by tag, prefix 'tags:' to your search term
keyword*	search for words containing criteria
"multiple keyword"	search for multiple words
keyword~	search for similar words
"keyword"^2 AND keyword	weight one filter over another
+keyword, -keyword	must include or exclude keyword
/keyw?rd)/	use regular expressions
[now-24h TO *]	use time ranges

Use operators to combine multiple quick filters and create a more complex search query.
Example:

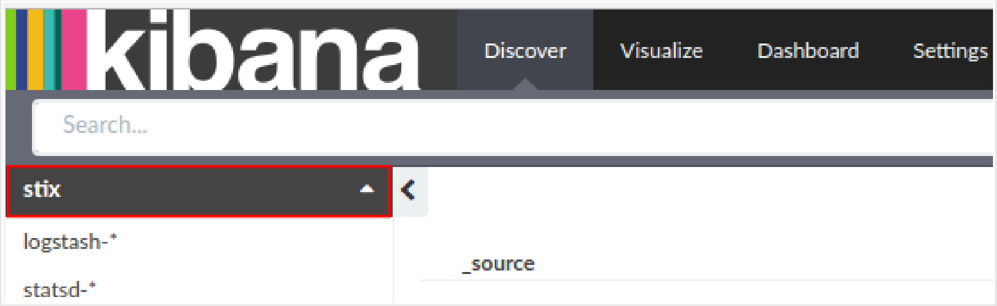
enrichment_extracts.kind:domain AND enrichment_extracts.meta.classification:high

Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean — An observable is blacklisted when it is included in the results returned by an *ignore* extraction rule. Allowed values: `true`, `false`.	`true`

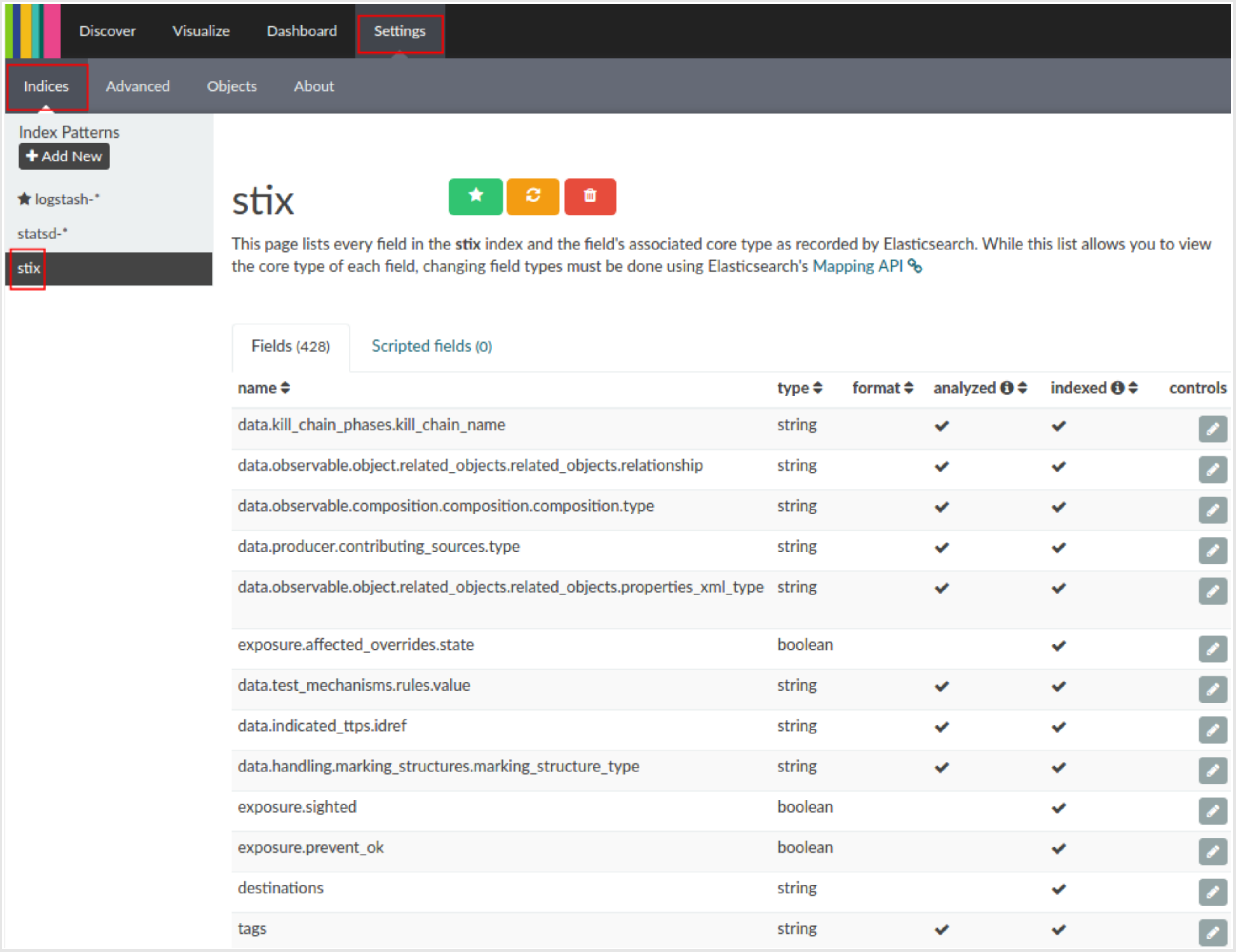
Field	Description	Example
enrichment_extracts.meta.classification	string — This value is defined in **Rules** by selecting appropriate options under **Action** and **Confidence**. Allowed classification metadata values are `good`, `bad`, and `unknown`.	`good`
enrichment_extracts.meta.confidence	string — This value is defined in **Rules** by selecting the appropriate option under **Action** and **Confidence**. The selected action must be **Mark as malicious** for the **Confidence** drop-down list to become available. Allowed confidence metadata values are `low`, `medium`, and `high`.	`high`
enrichment_extracts.value	string — The actual value of the enrichment observable, based on the enrichment observable data type.	`doom.dismay.biz`

For reference, you can look up a complete list of all available search query fields in Kibana:

- To access Kibana, in the web browser address bar enter a URL with the following format:
  https://${platform_host}/private/kibana/app/kibana#
  Keep the trailing **#**
  Example: *https://${platform_host}.com/private/kibana/app/kibana#*
- Select the **stix** index field:



- On the main menu bar, select **Settings**:



stix

This page lists every field in the **stix** index and the field's associated core type as recorded by Elasticsearch. While this list allows you to view the core type of each field, changing field types must be done using Elasticsearch's Mapping API

name	type	format	analyzed	indexed	controls
data.kill_chain_phases.kill_chain_name	string		✓	✓	✎
data.observable.object.related_objects.related_objects.relationship	string		✓	✓	✎
data.observable.composition.composition.composition.type	string		✓	✓	✎
data.producer.contributing_sources.type	string		✓	✓	✎
data.observable.object.related_objects.related_objects.properties_xml_type	string		✓	✓	✎
exposure.affected_overrides.state	boolean			✓	✎
data.test_mechanisms.rules.value	string		✓	✓	✎
data.indicated_ttps.idref	string		✓	✓	✎
data.handling.marking_structures.marking_structure_type	string		✓	✓	✎
exposure.sighted	boolean			✓	✎
exposure.prevent_ok	boolean			✓	✎
destinations	string			✓	✎
tags	string		✓	✓	✎

Splunk integration

EclecticIQ Platform App for Splunk Enterprise enables Splunk users to ingest large quantities of threat intelligence by integrating EclecticIQ Platform feeds with Splunk Enterprise.

Splunk	**integration**
App	EclecticIQ Platform App for Splunk
Version	1.0.3
Compatibility	Splunk Enterprise 6.3 and later
Last changed	November 2017
Authors	SOC Prime, EclecticIQ
Type	SIEM integration
Integration	app/bidirectional
Description	The app integrates EclecticIQ Platform feeds with Splunk Enterprise. Outgoing feeds transmit relevant data to Splunk for analysis and further filtering to identify potential threats that may target your organization.
Download	**Splunkbase** `(https://splunkbase.splunk.com/app/3408/)`

Release notes

Version 1.0.3 — Several known issues were addressed.

Contact

If you want to send us your feedback or if you need any support with the app, you can contact EclecticIQ at splunk@eclecticiq.com.

To request further documentation, contact EclecticIQ at splunk@eclecticiq.com.
To suggest a feature request and to report bugs, send an email to splunk@eclecticiq.com.

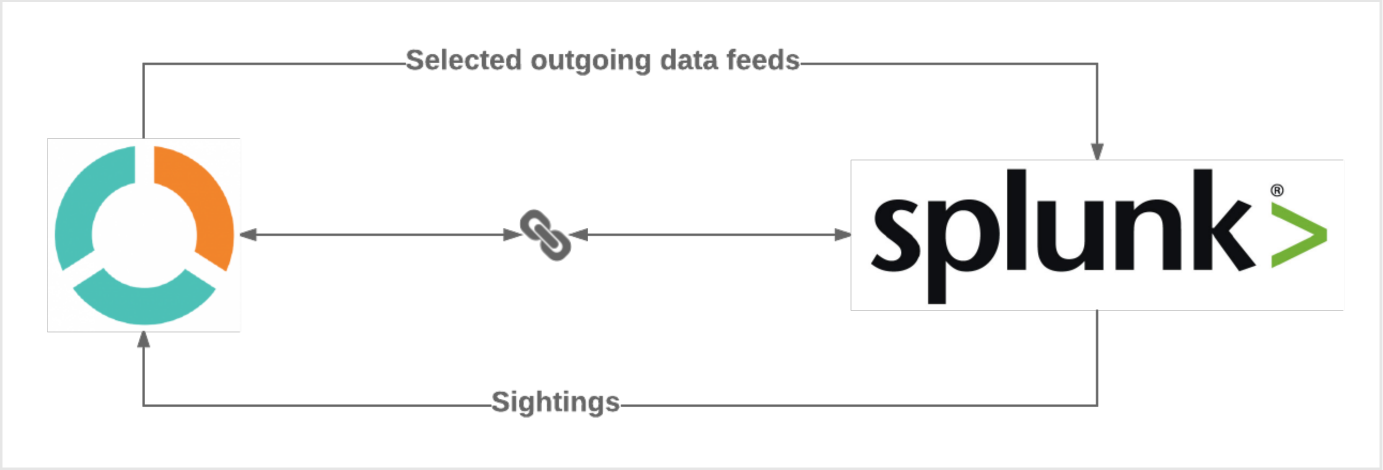
About EclecticIQ Platform App for Splunk

EclecticIQ Platform App for Splunk is an app for Splunk Enterprise. It enables Splunk users to ingest large quantities of threat intelligence by integrating EclecticIQ Platform feeds with Splunk.

EclecticIQ Platform ingests cyber threat data in different formats from multiple sources. The platform deduplicates, normalizes, and enriches source data with additional contextual details, and then it uses outgoing feeds to output relevant information to Splunk, where it can be analyzed and filtered by a set of rules to identify matching threats that may target your organization.

This process generates sightings and alerts that Splunk feeds back to EclecticIQ Platform, providing a rich threat intelligence dataset that allows you to efficiently tune your SIEM prevention and detection system.

EclecticIQ Platform App for Splunk ships with a default set of dashboard gauges to make it easier for Splunk users to monitor feed data collection, as well as to analyze and triage any *indicators of compromise* (IOCs) the data analysis process may yield.



Quick start guide

Compatibility

Splunk Enterprise 6.3 and later — EclecticIQ Platform App for Splunk 1.0.3

- EclecticIQ Platform App for Splunk 1.0.3
- Supports Splunk Enterprise 6.3 and later.
- Supports Python 2.6.6 or higher 2.x.x version.
  Not supported: Python 3.x.x.
- Required Python libraries: **argparse** `(https://pypi.python.org/pypi/argparse)`, **requests** `(https://pypi.python.org/pypi/requests)`.

Install

EclecticIQ Platform App for Splunk is developed specifically for Splunk Enterprise.
Everything you need to use the app is bundled with the installation package and the related files.
If you are using Splunk Enterprise, you do not need to install the script and configuration files.

- Verify that the Splunk Enterprise server you want to install EclecticIQ Platform App for Splunk on is compatible with the app.
- Verify that the required necessary Python libraries are installed.

- In the Splunk management console go to **Apps > Manage Apps**, and then click **Install app from file**.
- Browse to the location where the *eclecticiq-platform-app-for-splunk-${version_number}.tgz* file is stored, and then click **Upload**.
- After successfully completing the upload and the installation, restart Splunk.

Configure

After restarting Splunk, you can proceed to configuring EclecticIQ Platform App for Splunk.

- In the Splunk management console go to **Apps**.
- From the app list select **EclecticIQ Platform App for Splunk**.
- On the displayed dialog window click **Continue to app setup page**.

On the EclecticIQ Platform App for Splunk configuration screen, define the following options:

- **Feeds setup**: enter the feed ID of the EclecticIQ Platform outgoing feeds whose content you want to send to Splunk. If you enter multiple feed IDs use a comma (**,**) as a separator.
- **Input setup**: define the indexes and the source types you are using as data sources for this integration:
  - **Indexes**: enter the name of the **Splunk indexes** `(http://docs.splunk.com/splexicon:index)` you want to include as sources. If you enter multiple indexes, use a comma (**,**) as a separator.
  - **Sourcetypes**: enter the name of the **Splunk source types** `(https://docs.splunk.com/splexicon:sourcetype)` you want to include. If you enter multiple source type names, use a comma (**,**) as a separator.
- **Select the type of Sighting to send to EclecticIQ Platform**: select all applicable checkboxes corresponding to the data types you want to use to generate the sightings that are subsequently sent for ingestion to EclecticIQ Platform.
- **EclecticIQ platform URL**: enter the URL corresponding to the address of the EclecticIQ Platform host.
- **Verify SSL Connection**: select this checkbox to enable SSL verification for the connection, if applicable.
- **EclecticIQ source group name**: enter the name of the group you want to use as a source.
- **EclecticIQ platform authentication**: enter a valid user name and a password to authenticate and to sign in to the platform.
- Click **Save** to save and store your configuration.
- By default, a script is configured to run and collect outgoing feeds once every 2 hours at *hour:00 mins*; that is, at 00:00, 02:00, 04:00, and so on.
- By default, a script is configured to push sightings once a day at 01:00 AM.
- You can change the job schedules in the following configuration file: *$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/default/inputs.conf*
  - *eiq_collect_feeds.py* is the script that collects outgoing feed data from EclecticIQ Platform.
  - *eiq_send_sightings.py* is the script that sends sightings to EclecticIQ Platform.

After correctly configuring EclecticIQ Platform App for Splunk to integrate and work with Splunk, the corresponding dashboard view should become populated with relevant results.

Uninstall

To uninstall EclecticIQ Platform App for Splunk, run the following command(s):

```
$ SPLUNK_HOME/bin/splunk remove app eclecticiq-platform-app-for-splunk
```

Install and configure Python

To check which Python version is installed on the target server, run the following command(s):

```
$ python -V
```

- If you need to install the required Python version, **download it** `(https://www.python.org/downloads/source/)`, and then follow the **installation instructions** `(https://docs.python.org/2/using/unix.html)`.
- If the required Python version is installed, check if *pip* is available on the server:

```
$ pip -V
```

- If you need to install pip, **download get-pip.py** `(https://bootstrap.pypa.io/get-pip.py)`, and then follow the **installation instructions** `(https://pip.pypa.io/en/latest/installing.html)`:

```
# get pip
$ wget https://bootstrap.pypa.io/get-pip.py

# install pip
$ python get-pip.py
```

- Use pip to check that the necessary libraries are available:

```
$ pip list
```

- If the *argparse* and the *requests* libraries are missing, install them:

```
$ pip install argparse
$ pip install requests
```

End of the EclecticIQ Platform App for Splunk quick start guide

---

Beginning of the EclecticIQ Platform App for Splunk integration guide

EclecticIQ Platform integration with Splunk

(Through EclecticIQ Platform App for Splunk)

Before you start

Before you start installing the app, take a moment to review the preliminary requirements and the main steps of the process.

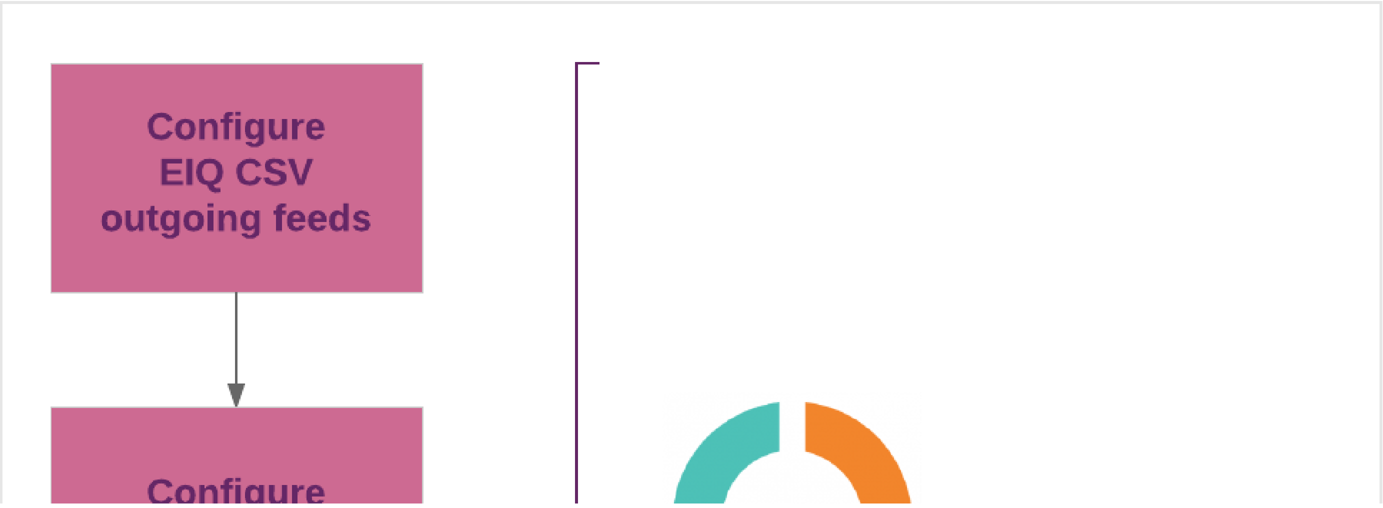
Requirements

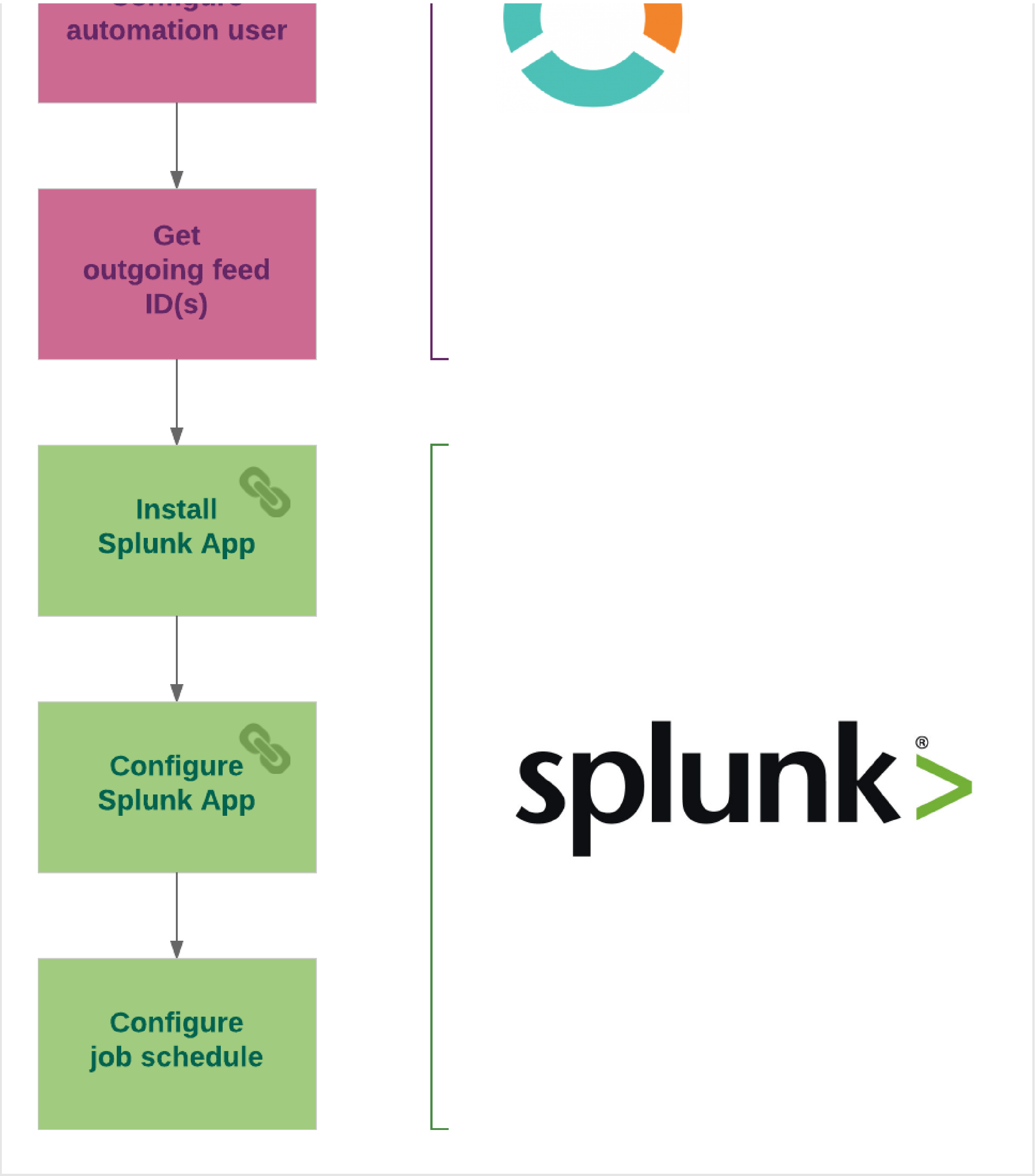
- An EclecticIQ Platform installation.
- A Splunk server installation.
- Splunk **Common Information Model (CIM)** `(https://splunkbase.splunk.com/app/1621/)` add-on needs to be **installed** `(https://docs.splunk.com/documentation/cim/latest/user/install)` on the Splunk server.
- Install and set up EclecticIQ Platform App for Splunk on a Splunk server that has network access to the EclecticIQ Platform server: these servers need to communicate and exchange data.
- Supports Splunk Enterprise 6.3 and later.
- Supports Python 2.6.6 or higher 2.x.x version.
  Not supported: Python 3.x.x.
- Required Python libraries:
  - **argparse** `(https://pypi.python.org/pypi/argparse)`
  - **requests** `(https://pypi.python.org/pypi/requests)`.

Process outline

The diagram sums up the main steps to set up and configure a platform integration with Splunk:

- First, you set up the outgoing feed sending data from the platform to Splunk.
- Then, you install and configure EclecticIQ Platform App for Splunk to enable the integration between the platform and Splunk.





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 section describes how to configure **EclecticIQ Entities CSV** and **EclecticIQ Observables CSV** outgoing feeds, so that you can distribute selected intelligence through EclecticIQ Platform.

Configure the general options

✔ Input fields marked with an asterisk are required.

- On the top navigation bar, select **Data configuration > Outgoing feeds**.
- On the top-left corner of the page click the ✚ icon to open the outgoing feed editor.

The **Outgoing feeds** page displays an overview of the configured outgoing feeds to publish and distribute selected intelligence from the platform to external parties, services, and systems.

On the **Create outgoing feed** 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.
- **Sign content with private key**: select this checkbox to automatically sign the content of the outgoing feed with a private PGP key.
  If you have not yet set a PGP private key in the platform, **Click here for the Private Key settings** to go to **System settings > Private key**, where you can set it before continuing with the feed configuration.

To set a PGP private key to sign outgoing feed content with, do the following:

- On the left-hand navigation sidebar, click ⚙ **> System settings > Private Key**.
- Click **Edit settings** to display the **Edit private key settings** page.
- In the **Private key** input field copy-paste the private PGP key you want to add to sign outgoing feed data packages with.
  Include in the pasted content the leading `-----BEGIN PGP PRIVATE KEY BLOCK-----` and the trailing `-----END PGP PRIVATE KEY BLOCK-----` lines.
- Click **Save** to store your changes, or **Cancel** to discard them.

To change PGP private key, you first need to remove the currently registered one:

- On the **Edit private key settings** page, browse to **Delete private key settings**, and then click **Delete settings**.
- On the confirmation dialog, click **Delete** to confirm the action.

Transport and content

Under **Transport type** and **Content type**, select the appropriate options to configure transport and content for the specified outgoing feed.

- **Transport type**: from the drop-down menu select the appropriate transport type to publish data through the outgoing feed.
  You can implement this integration through the **HTTP download** and **Mount point upload** transport types.
- **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.

Set a schedule

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

- **None**: scheduled feed execution is disabled. You need to manually trigger the task to ingest or to publish data through an incoming or an outgoing feed, respectively.
- **Every [n] minutes**: the feed task runs automatically once 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.
- **Every hour, [n] minutes past the hour**: the feed task runs automatically once an hour every hour at the specified minute offset from the hour.
  You define how long in minutes after the beginning of an hour the task should run from the corresponding drop-down menu.
- **Every [n] hours**: the feed task runs automatically once every *[n]* hours, where *[n]* defines the time interval in hours between two consecutive feed task runs.
  You define how long the time interval between feed executions should be by selecting the number of hours from the corresponding drop-down menu.
- **Every day at [time]**: the feed task runs automatically once a day at the specified time.
  You define the time of the day when the task should run from the corresponding drop-down menus.
- **Every [n] days**: the feed task runs automatically once every *[n]* days, where *[n]* defines the time interval in days between two consecutive feed task runs.
  You define how long the time interval between feed executions should be by selecting the number of days from the corresponding drop-down menu.
- **Every week on [day of the week] at [time]**: the feed task runs automatically once a week on the designated day, at the specified time.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menus.
- **Every month on [day of the month] at [time]**: the feed task runs automatically once a month on the designated day of the month, at the specified time.
  You define the day of the week and time of the day when the task should run from the corresponding drop-down menus.
  Keep in mind that not all months of the year have 30 or 31 days.

Set a TLP override

- **Override TLP** overwrites the **TLP** `(https://www.us-cert.gov/tlp)` color code associated with 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 feed or enricher content with a predefined reliability value to help other users assess how trustworthy the data 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

Observable filters work independently of each other: there are no explicit or implicit Boolean `AND` or `OR` to join multiple filters into a serial pipeline.

- **Allowed observable states**: from the drop-down menu select one or more observable states to include in the outgoing feed content only entities whose observable states match at least one of the selections defined here.

- **Include only observables with link names** : from the drop-down menu select one or more link name options to include in the outgoing feed content only observables with the specified link name value(s) describing specific types of relationship between observables and their parent entities.

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

  Link name options vary, based on the relationship the observable has with the specific entity type it belongs to.
  This filter option does not apply to enrichment observables.
- **Include observables without a link type** : select this checkbox to include in the outgoing feed content also observables without a defined link type/link name. These observables may or may not have relationships with other entities or other observables; in the former case, the relationships are undefined; therefore, they have lower intelligence value than link-named ones.
  This filtering applies to bundled observables, that is, to observables that are included inside entities. It does not apply to enrichment observables.
- **Observable types**: from the drop-down menu select one or more observable types to include in the outgoing feed content only entities with observables whose 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 content only entities with enrichment observables whose types match at least one of the selections defined here.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Configure transport and content types

Transport types	**Allowed content types**
HTTP download	EclecticIQ Entities CSV
	EclecticIQ Observables CSV
Mount point upload	EclecticIQ Entities CSV
	EclecticIQ Observables CSV

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 intended 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.

After selecting **Transport type > Mount point upload** , set the origin location for the source data:

- **Mount point path**: enter the path to the local or network unit where the source data for the outgoing feed is stored.

Configure the content type

When you set up an outgoing feed from the platform to the destination Splunk instance, 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 menu, 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.

Create an automation user and group

It is a good idea to have one or more dedicated users and user groups, as necessary, to handle automation tasks that interact with external products or components of your system.
Automation groups bring together automation users, and they act as global controllers of the permissions the automation users require to operate.
Automation users handle automation and integration tasks such as authentication, data transmission through feeds and enrichers, or automatic entity creation as a follow-up action on a specific event.

Create an automation group

> ℹ The automation group should include all the data sources — incoming feeds, enrichers, and groups — the automation users in the group need to access.

To add an automation user group, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**.
- Under **User management > Groups**, click **+** *(Create group)*.
  The user group editor is displayed.

> ✔ Input fields marked with an asterisk are required.

- Under **Create group**, define the following configuration settings:
  - **Name**: a descriptive name for the automation user group.
    Example: *TAXII integration group*
  - **Description**: a short description of the automation user group and its purpose.
    Example: *Automation group for integrations through TAXII services*
  - **Allowed sources**: click **+ Add** or **+ More** to add new rows as needed, where you can enter additional criteria.
    - **Sources**: from the drop-down menu select one or more data sources the automation user group and its members can access to fetch data from.
      The data sources can be existing incoming feeds, enrichers, as well as other user groups.

      Whereas role-based permissions define what actions users are allowed to carry out, group-based **Allowed sources** define *what* users can act on, that is, what platform data they are allowed to access.
    - **TLP**: from the drop-down menu select a **Traffic Light Protocol** `(https://www.us-cert.gov/tlp)` color to filter data accordingly.
    - Click **+ Add** or **+ More** to add new rows as needed, where you can enter additional criteria.
  - **Source reliability**: from the drop-down menu select a value to filter data source reliability, so as to allow access only to data whose sources meet the specified reliability criteria.
  - Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Create an automation role

To add a new automation role, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**.
- Under **User management > Roles**, click ✚ *(Create role)*.
  The role editor is displayed.

✓ Input fields marked with an asterisk are required.

- Under **Create role**, define the following configuration settings:
  - **Name**: a descriptive name for the automation role.
    Example: *Systems integrator*
  - **Description**: a short description of the automation role and its purpose.
    Example: *Allows implementing data exchange interoperability between the platform and an external system.*
  - **Permissions**: from the drop-down menu select the actions the role is allowed to perform.

    Alternatively:
    - Start typing a permission name in the autocomplete text input field.
    - Select one or more filtered permissions from the list.
  - To revoke one or more permissions for the role, click the ✖ icon corresponding to the permission you want to remove, or the ✖ icon next to the drop-down arrow in the input field to remove all permissions at once.
  - Click **Save** to store your changes, or **Cancel** to discard them.

About permissions

- Permissions are associated with roles. Roles act as containers for sets of permissions defining the scope of actions of the corresponding roles.
- Permissions are predefined in the platform, and they are not editable or configurable. You can either grant them to roles, or revoke them.
- Permission names strive to be self-explanatory:
  Format: *${type of action} ${object of the action}*
  Example: *modify entities*

- Permissions allow two types of action:
    - **modify**: a modification permission that allows write operations.
    - **read**: a read permission that grants access to data without allowing any modifications.

To get an overview of the available permissions available on the platform, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**.
- Under **User management > Permissions**, the permission overview is displayed as a table, where each permission is assigned a row.
  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.

Whereas role-based permissions define what *actions* users are allowed to carry out, group-based **Allowed sources** define *what* users can act on, that is, what platform data they are allowed to access.

Create an automation user

To add an automation user, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**.
- Under **User management > User**, click ✚ *(Create user)*.
  The user editor is displayed.

✔ Input fields marked with an asterisk are required.

In the user editor define the following configuration settings:

- **First name**: enter a name that provides a short description of the automation user and its purpose.
- **Last name**: enter a name that provides a short description of the automation user and its purpose.
- **User name**: enter the designated user name to identify the user, when signed in to the platform.
  Choose a name that helps understand what the automation user does.
  Example: *platform-to-platform connector*
- **Email**: an email address associated with the automation user. You can use this address to send and to receive automated notifications.
- **Active**: select this checkbox to enable the user immediately after saving the newly created user profile.
  Active users can sign in to the platform and carry out actions, based on their permissions.
- **Administrator**: select this checkbox to elevate the user’s role to administrator.
  When the checkbox is selected, the user has full administrator rights and permissions.
- **Contact info**: n/a
- **PGP public key**: the user’s **PGP public key** `(https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp)`, if available.
- **Locale**: from the drop-down menu select the appropriate **locale** `(https://en.wikipedia.org/wiki/locale_(computer_software))` settings for the user interface.
- **Use system timezone**: select this checkbox to override any locale-specific time zone setting with the system-defined time zone.
  When this setting is enabled, the platform retrieves the time from the host server, and it displays it in the format defined in the host server configuration.

- **Preferred timezone**: this option is available when **Use system timezone** is deselected. From the drop-down menu select the preferred time zone you want to use as a reference to display date and time in the platform for the current user profile.
- **Groups**: from the drop-down menu select one or more groups to assign the new user to.
  Alternatively, search for a group by starting typing a group name in the autocomplete text input field.
- To remove the user from one or more groups, remove the relevant entries by clicking the ✖ corresponding to the group you want to remove the user from.
- **Roles**: it works like **Groups**, the only difference being that instead of adding the user to one or more groups, this option assigns one or more roles to the user.
- Click **Save** to store your changes, or **Cancel** to discard them.

Get the automation group meta.source ID

Platform entities include a `meta.source` property key/value pair to identify the platform group as a data source.
If you want to programmatically create entities in the platform, you need to pass a group `meta.source` ID value when you make the corresponding calls to the platform API.
Likewise, if you want to identify the platform source group an entity comes from when the platform transmits data to an external product or system, you can retrieve the `meta.source` property key/value pair.

To retrieve the correct `meta.source` ID value related to an automation group, do the following:

- Get the automation group ID.
- Pass the automation group ID to get the `meta.source` ID.

Step 1 of 2: get the group ID

To retrieve the automation group ID value you need, so that you can retrieve the `meta.source` ID you pass in the calls to the platform API, do the following:

- On the left-hand navigation sidebar click ⚙ **> User management**.
- Under **User management**, click **Groups**.
- On the platform group overview page, click the row corresponding to the automation group associated with the data source(s) you want to use as input *and* to the automation user making the API calls.
- The action returns a URL with the following format:
  https://${platform_host}/user-management/groups?detail=${int}
  Example: *https://${platform_host}/user-management/groups?detail=30*

In the example, the `detail` value is `30`. This is the group ID.
You need to pass this value in a call to a specific platform API endpoint to retrieve the `meta.source` ID.

Step 2 of 2: get the group source ID

To retrieve the `meta.source` ID to make calls to the platform API to programmatically create entities, do the following:

- Make an authentication call to the platform API to validate your user credentials and to receive a Bearer token.
- Make a call to the `/private/groups/${group_ID}` endpoint:
  - Include the Bearer token in a `Bearer` header in the call.
  - Include the group ID you previously retrieved as a trailing element in the URL.
    Example: `https://${platform_host}/private/groups/30`
- In the JSON response, look for the group object with the `"id" : ${int}` key/value pair matching the group ID you previously retrieved.
  Example: `"id" : 30,`

- In the same group object, look for the `"source" : "${UUID_string}"` key/value pair.
  This is the group `meta.source` ID you need to pass in API calls to programmatically create entities.

Get the automation group meta.source ID example

Get the group ID

- On the platform group overview page, click the row corresponding to the automation group associated with the data source(s) you want to use as input.

```
https://platform.example.com/user-management/groups?detail=30
```

cURL API request — fetches the group meta.source

```
$ curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/private/groups/30

# copy-paste version:
$ curl -X GET -v --insecure -i -H "Content-Type: application/json" -H "Accept: application/json"
-H "Authorization: Bearer ${token}" https://${platform_host}/private/groups/30
```

API response — returns the group meta.source

```
{
  // Number of returned user groups
  "count": 18,

  "data": [

    ...

    {
      "allowed_sources": [

        // Lists all allowed data sources configured in the group editor
        ...

      ],

      // Group id, same value as the 'detail=' URL param for the group
      "id": 30,

      // Group 'meta.source' ID you need to pass in API calls
      "source": "42c051f8-9f5b-4696-a629-b86c2ead955f",

      // Group 'meta.source_name', the group name defined in the group editor
      "name": "DomainTools automation group",

      "type": "groups",
      "users": [

      // Lists all users that are part of the group
      ...

      ]
    },

    ...

  ]
}
```

Authentication

The authentication mechanism is based on **JSON web tokens** `(http://jwt.io/)`.

By default, the token expires 30 minutes after successfully signing in to a platform user session. When the token expires, the corresponding session is terminated, and you need to sign back in to the platform.

When human interaction is detected — for example, keystrokes or mouse activity — the token is automatically refreshed every 60 seconds. This prevents the system from signing out users who may be working or saving data at that time.

Therefore, the default maximum amount of idle time without any human interaction before being automatically signed out equals to *session token validity - 1 minute*.

To authenticate and access the platform, do the following:

- Make a `POST` call.
- In the call, pass your authentication credentials as a JSON object to the `/auth` endpoint. The credential data is used to generate a token that is returned with the response.

You need to include the generated bearer token in the `Authorization` HTTP header with each subsequent API call. The `Authorization` HTTP header has the following format: `Authorization: Bearer ${token}`

Auth request

API endpoint	`/auth`
Auth method	`POST`
HTTP headers	`"Content-Type: application/json"`, `"Accept: application/json"`
API request	`POST` + `"Content-Type: application/json"` + `"Accept: application/json"` + `{ "username": "${username}", "password": "${password}" }` + `${platform_host}/api/auth`
API response	`{ "expires_at": "${expiration_timestamp}", "token": "${token}" }`

The following example uses cURL to authenticate:

```
# Public API auth endpoint
$ curl -X POST
       --insecure
       -H "Content-Type: application/json"
       -d '{ "username" : "${username}", "password" : "${password}" }'
       https://${platform_host}/api/auth
```

```
# copy-paste version:
$ curl -X POST --insecure -H "Content-Type: application/json" -d '{ "username" : "${username}",
"password" : "${password}" }' https://${platform_host}/api/auth
```

```
# Private API auth endpoint
$ curl -X POST
       --insecure
       -H "Content-Type: application/json"
       -d '{ "username" : "${username}", "password" : "${password}" }'
       https://${platform_host}/private/auth
```

```
# copy-paste version:
$ curl -X POST --insecure -H "Content-Type: application/json" -d '{ "username" : "${username}",
"password" : "${password}" }' https://${platform_host}/private/auth
```

Auth response

When the user name and password credential are valid, the `POST` call returns a JSON web token:

```
{
  "expires_at": "2016-03-30T12:11:40.078219+00:00",
  "token"     :
"abHpYXQiOjE0NTkzMzI3MDAsIm4TcCI6MTQ1OTMzOTkwMCwiYWxnIjoiSFMyNTYifQ.oyY1c2VyX2lkIjo1fQ.LQQ3NdUHp4s-
QCXsxq3feI0Dy6tf5XQX9DOML1RNIzQ"
}
```

You need to include the bearer token value in each subsequent API call. You pass the token by including an `Authorization` HTTP header in the API request.
The `Authorization` HTTP header has the following format: `Authorization: Bearer ${token}`

In the following example, you make a `GET` request to the `/api/` or the the `/private/` endpoint to retrieve a list of the available API endpoints and the corresponding methods for the public or the private API, respectively:

```
# GET list of public API endpoints
$ curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/api/
```

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

```
# GET list of private API endpoints
$ curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/private/
```

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

⚠ **Warning:**
About cURL calls

- If you make HTTPs cURL calls to the API *and* you have a self-signed or an invalid certificate, include the `-k` or the `--insecure` parameter in the cURL call to skip the SSL connection CA certificate check.
- Always append a `/` trailing slash at the end of an API URL endpoint. The only exception is `/auth`, which does not take a trailing forward slash.
- In the cURL call, the `-d` data payload with the entity information always needs to be flat JSON, not hierarchical JSON.
  If you want to pass a hierarchical JSON object, include the `--data-binary` parameter, followed by the path to the JSON file, for example `@/path/to/entity_file.json`.

Get the feed ID

You can access and download content from an outgoing feed by specifying its ID.
A feed ID is included in the outgoing feed URL as a URL parameter.

Get the feed ID through the GUI

To get the feed ID through the platform GUI, do the following:

- On the top navigation bar, select **Data configuration > Outgoing feeds** .
- On the top-left corner of the page click the ✚ icon to open the outgoing feed editor.
- On the **Outgoing feeds** overview, browse to the feed whose ID you need to retrieve, and then click the corresponding row.
- The outgoing feed URL is loaded on the web browser address bar. For example:
  `https://${platform_host}/#/configuration/outgoing-feeds?detail=78&tab=detail`
- The `detail` URL parameter holds the feed ID.
  In the example URL, `detail=78` indicates that the selected outgoing feed ID is `78`.
  When you make an API call to retrieve the feed content, you need to include the ID value in the API endpoint.

Get the feed ID through the API

Make an API call to download a list of all available public outgoing feeds.
This call returns a JSON object with an array listing all available public outgoing feeds with HTTP transport type.

API endpoint	`/open-outgoing-feed-download/`
API method	`GET`
HTTP headers	`"Content-Type: application/json"`, `"Accept: application/json"`, `"Authorization: Bearer ${token}"`
API request	`GET` + `"Content-Type: application/json"` + `"Accept: application/json"` + `"Authorization: Bearer ${token}"` + `${platform_host}/open-outgoing-feed-download/`
API response	`{ "data" : [ <open_outgoing_feed_array> ] }`

API request outgoing feeds

cURL call

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

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

API response outgoing feeds

```
{
  "data": [

    {
      "id": 1,
      "link": "/private/open-outgoing-feed-download/1",
      "name": "Default outgoing feed"
    },

    {
      "id": 16,
      "link": "/private/open-outgoing-feed-download/18",
      "name": "Public feed with electrolytes"
    },

    {
      "id": 25,
      "link": "/private/open-outgoing-feed-download/25",
      "name": "XYZ"
    }

  ]
}
```

Get a specific outgoing feed

Make an API call to download the details of a specific outgoing feed.
This call returns a JSON object containing the details of a specific public outgoing feed with HTTP transport type.
To select the public outgoing feed whose details you want to retrieve, include the feed ID in the API request endpoint.

API endpoint	`/open-outgoing-feed-download/${feed-id}/`
API method	`GET`
HTTP headers	`"Content-Type: application/json"`, `"Accept: application/json"`, `"Authorization: Bearer ${token}"`
API request	`GET` + `"Content-Type: application/json"` + `"Accept: application/json"` + `"Authorization: Bearer ${token}"` + `${platform_host}/open-outgoing-feed-download/${feed-id}/`
API response	`{ "data" : { ${specific_feed_details} } }`

API request specific outgoing feed

cURL call

```
$ curl -X GET
       -v
       --insecure
       -i
       -H "Content-Type: application/json"
       -H "Accept: application/json"
       -H "Authorization: Bearer ${token}"
       https://${platform_host}/private/open-outgoing-feed-download/18

# copy-paste version:
$ curl -X GET -v --insecure -i -H "Content-Type: application/json" -H "Accept: application/json"
-H "Authorization: Bearer ${token}" https://${platform_host}/private/open-outgoing-feed-
download/18
```

API response specific outgoing feed

The response details include an array listing the successful feed executions.

The paths in the `content_blocks` array have the following format:
`/private/open-outgoing-feed-download/${feed-id}/runs/${run-id}/content-blocks/${content-block-id}`

- A *run* is a feed execution to publish the feed content.
- A *content block* is a data blob whose format depends on the content type defined for the feed. For example, JSON, CSV or STIX.

```
{
  "data": {

    "content_blocks": [
      "/private/open-outgoing-feed-download/18/runs/0ad2edd4-8a7b-4894-b8b3-aee90a22ebaa/content-
blocks/32",
      "/private/open-outgoing-feed-download/18/runs/5fdeff71-93af-43a5-b94e-c4ab857a749c/content-
blocks/33",
      "/private/open-outgoing-feed-download/18/runs/40e31ada-06e6-4647-a287-4c9b54841619/content-
blocks/34",
      "/private/open-outgoing-feed-download/18/runs/0f56ec9c-cc1e-4aae-afd0-f693f412ad55/content-
blocks/35",
      "/private/open-outgoing-feed-download/18/runs/d842dd68-8ecf-4ecf-b073-a591d361cf26/content-
blocks/36",
      "/private/open-outgoing-feed-download/18/runs/eed28e1e-4352-42a5-8b1f-cfc918b0e0ab/content-
blocks/37",
      "/private/open-outgoing-feed-download/18/runs/f830aa7b-4ddc-4725-b13c-7cbe445f306d/content-
blocks/40",
      "/private/open-outgoing-feed-download/18/runs/a11bb585-720a-4c56-b650-90cb9d6a69e5/content-
blocks/41",
      "/private/open-outgoing-feed-download/18/runs/6e677f4b-c91d-49dd-9c39-70266987b863/content-
blocks/42"
    ],

    "id": 18,
    "name": "Public feed with electrolytes"
  }
}
```

Install and configure EclecticIQ Platform App for Splunk

EclecticIQ Platform App for Splunk is a native application that installs directly on your Splunk instance.
This section describes how to download and install EclecticIQ Platform App for Splunk, as well as how to configure Splunk to work with the app.

Download the app

- Download the *eclecticiq-platform-app-for-splunk-${version_number}.tgz* file from **Splunkbase** `(https://splunkbase.splunk.com/app/3408/).`
- Save the archive locally.

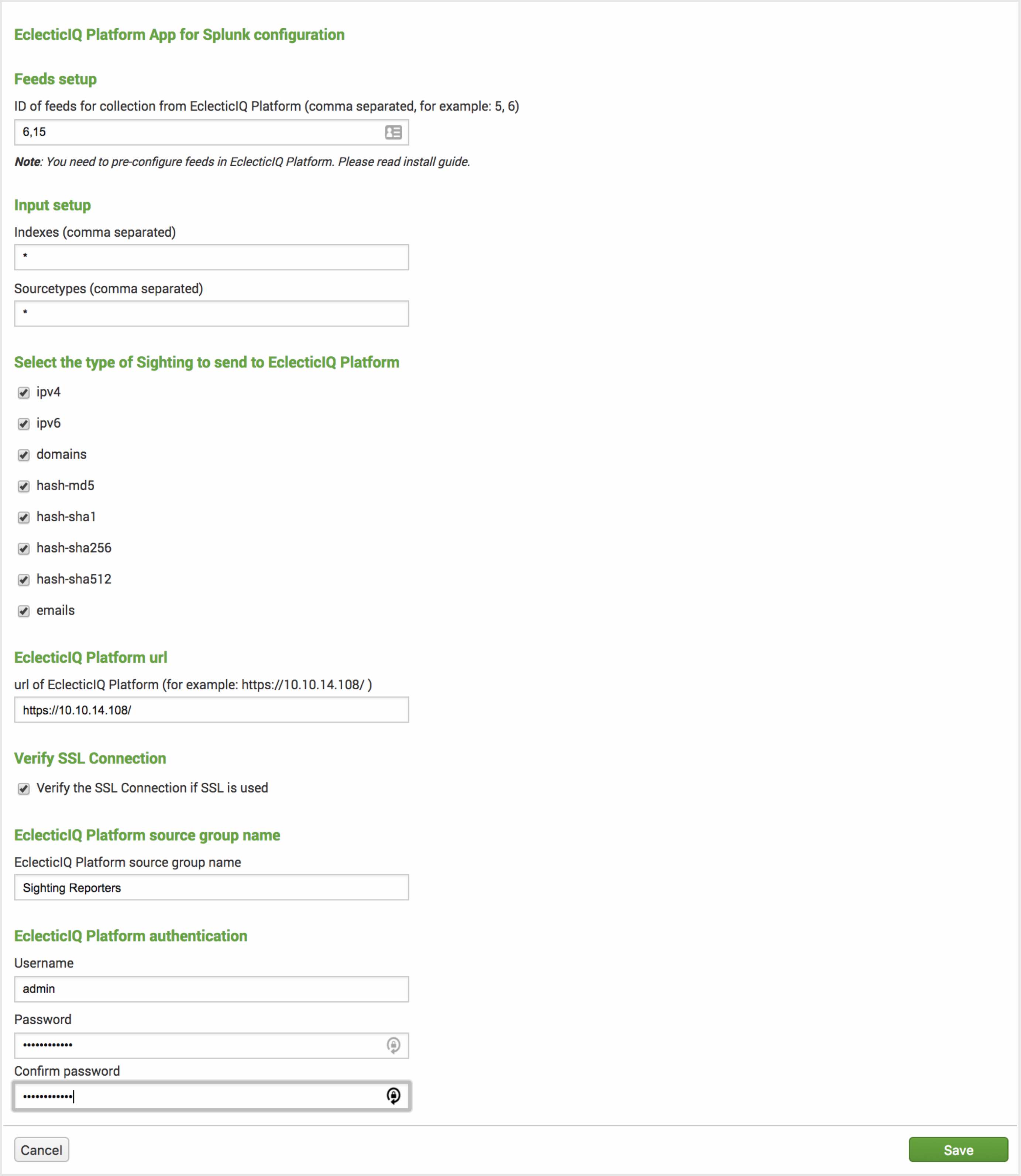
Install the app

- In the Splunk management console go to **Apps > Manage Apps**, and then click **Install app from file**.
- Browse to the location where the *eclecticiq-platform-app-for-splunk-${version_number}.tgz* file is stored, and then click **Upload**.
- After successfully completing the upload and the installation, restart Splunk.

Configure the app

After restarting Splunk, you can proceed to configuring EclecticIQ Platform App for Splunk.

- In the Splunk management console go to **Apps**.
- From the app list select **EclecticIQ Platform App for Splunk**.
- On the displayed dialog window click **Continue to app setup page**.



EclecticIQ Platform App for Splunk configuration

Feeds setup

ID of feeds for collection from EclecticIQ Platform (comma separated, for example: 5, 6)

6,15

***Note**: You need to pre-configure feeds in EclecticIQ Platform. Please read install guide.*

Input setup

Indexes (comma separated)

*

Sourcetypes (comma separated)

*

Select the type of Sighting to send to EclecticIQ Platform

☑ ipv4

☑ ipv6

☑ domains

☑ hash-md5

☑ hash-sha1

☑ hash-sha256

☑ hash-sha512

☑ emails

EclecticIQ Platform url

url of EclecticIQ Platform (for example: https://10.10.14.108/)

https://10.10.14.108/

Verify SSL Connection

☑ Verify the SSL Connection if SSL is used

EclecticIQ Platform source group name

EclecticIQ Platform source group name

Sighting Reporters

EclecticIQ Platform authentication

Username

admin

Password

••••••••••••

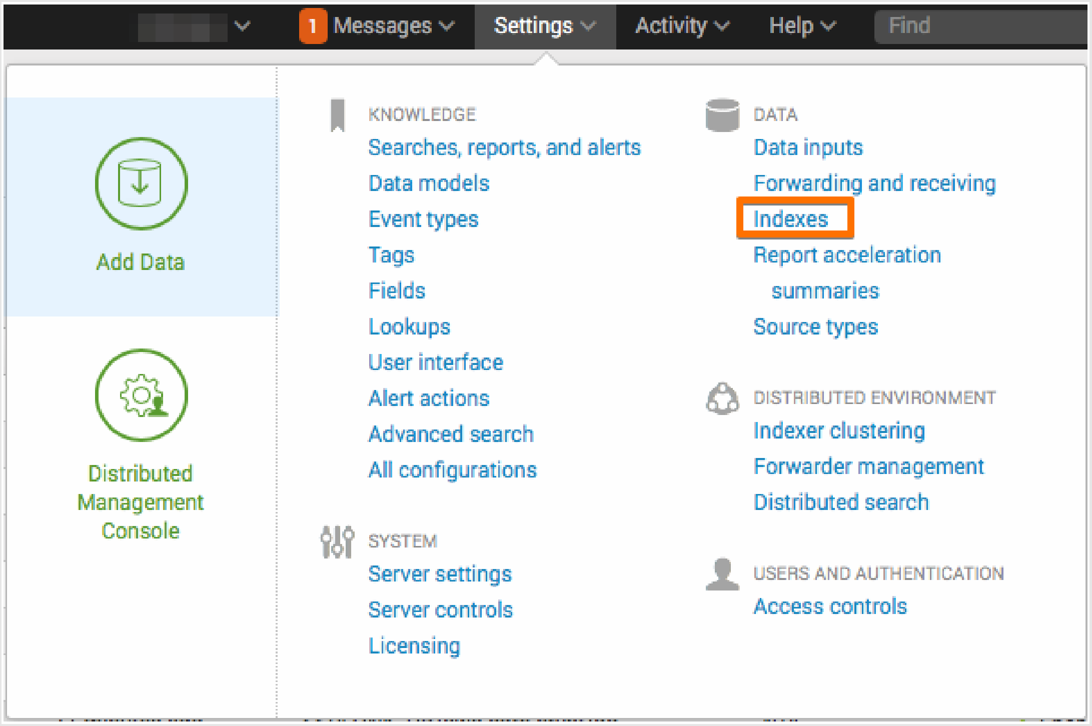
Confirm password

••••••••••••

On the EclecticIQ Platform App for Splunk configuration screen, define the following options:

- **Feeds setup**: enter the feed ID of the EclecticIQ Platform outgoing feeds whose content you want to send to Splunk. If you enter multiple feed IDs, use a comma (**,**) as a separator.
  Example: *4,18,74,88*

- **Input setup**: define the indexes and the source types you are using as data sources for this integration:
  - **Indexes**: enter the name of the **Splunk indexes** (http://docs.splunk.com/splexicon:index) you want to include as sources.
    Events included in the specified input indexes are searched for matches against the criteria defined in this configuration.
    Matching events are used to create sightings.
    If you enter multiple indexes, use a comma (**,**) as a separator.
    To view a list with the available Splunk indexes, in Splunk go to **Settings > Indexes**.
    Default value: * (asterisk, that is, all available Splunk indexes are included as sources)
  - **Sourcetypes**: enter the name of the **Splunk source types** (https://docs.splunk.com/splexicon:sourcetype) you want to include.
    Events whose data structure corresponds to the specified input source types are searched for matches against the criteria defined in this configuration.
    Matching events are used to create sightings.
    If you enter multiple source type names, use a comma (**,**) as a separator.
    Splunk includes a **built-in source type set** (http://docs.splunk.com/documentation/splunk/latest/data/listofpretrainedsourcetypes).
    Default value: * (asterisk, that is, all available source types are included as sources)
    Example: *access_combined,linux_messages_syslog*



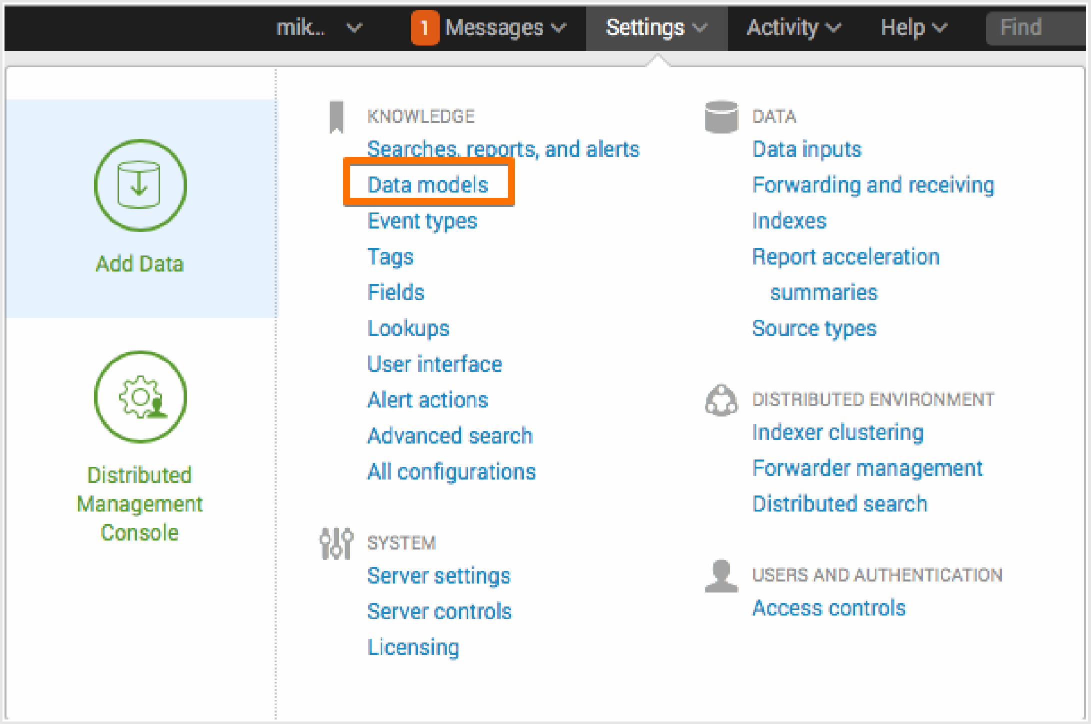
- **Select the type of Sighting to send to EclecticIQ Platform**: select all applicable checkboxes corresponding to the data types you want to use to generate the sightings that are subsequently sent for ingestion to EclecticIQ Platform. Supported types:
  - *ipv4*
  - *ipv6*
  - *domains*
  - *hash-md5*
  - *hash-1*
  - *hash-256*
  - *hash-512*
  - *email*
- **EclecticIQ platform URL**: enter the URL corresponding to the address of the EclecticIQ Platform host.
  Example: *https://10.10.10.10/ or https://platform.instance.org/*
- **Verify SSL Connection**: select this checkbox to enable SSL verification for the connection, if it uses SSL.
- **EclecticIQ source group name**: enter the name of the group you want to use as a source.
  A valid group name corresponds to the name of any available group configured in the platform.
  Example: *Sightingbusters*
- **EclecticIQ platform authentication**: enter valid credentials to authenticate and to sign in to the platform; that is, a valid user name and a password, which you need to confirm.
- Click **Save** to save and store your configuration.

Configure data model acceleration

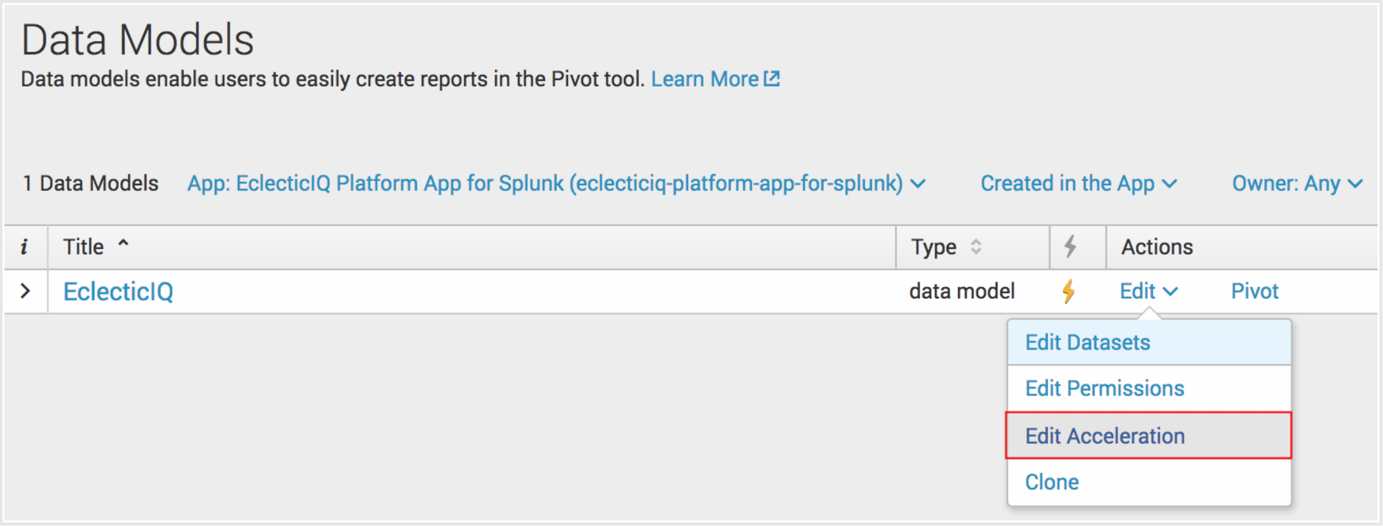
By default, **data model acceleration** `(https://docs.splunk.com/documentation/splunk/latest/knowledge/acceleratedatamodels)` is configured to speed up data models within 7 days.

To modify the data model acceleration settings, do the following:

- In Splunk, go to **Settings > Data models**.



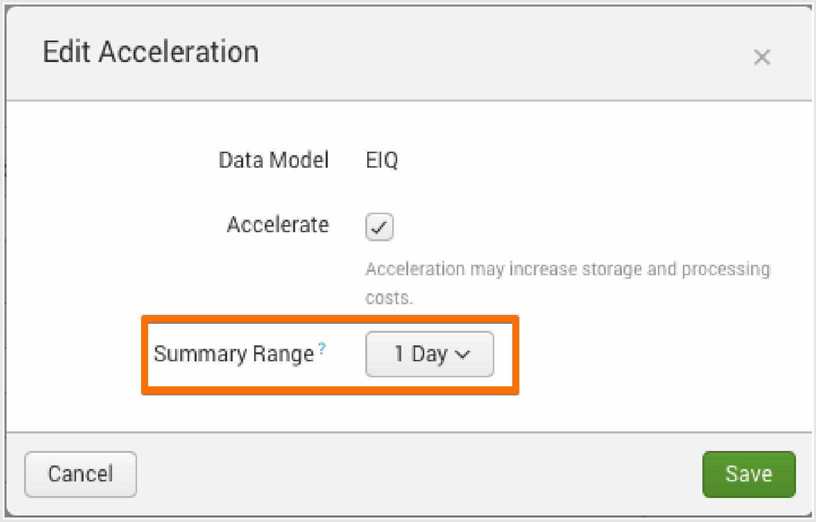
- Browse to the **EclecticIQ** row, and then select the **Edit > Edit Acceleration** menu option.



Data Models

Data models enable users to easily create reports in the Pivot tool. Learn More

- In the displayed dialog window, make sure the **Accelerate** checkbox is selected.
- From the **Summary Range** drop-down menu, select the time interval you want data to base acceleration on.



Edit Acceleration

Data Model EIQ

Accelerate ☑

Acceleration may increase storage and processing costs.

Summary Range 1 Day

- Click **Save** to save and store your edits.

Default job schedule

- By default, a script is configured to run and collect outgoing feeds once every 2 hours at *hour:00 mins*; that is, at 00:00, 02:00, 04:00, and so on.
- By default, a script is configured to push sightings once a day at 01:00 AM.

Customize the job schedule

You can change the job schedules in the following configuration file:
$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/default/inputs.conf

This is the default version of the file that ships with the app:

```
[default]

[script://$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/bin/eiq_send_sightings.py]
disabled = false
interval = 00 01 * * *

[script://$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/bin/eiq_collect_feeds.py]
disabled = false
interval = * */2 * * *

[script://$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/bin/eiq_setup_handler.py]
passAuth = splunk-system-user

[script://$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/bin/eiq_collect_feeds.py]
passAuth = splunk-system-user

[script://$SPLUNK_HOME/etc/apps/eclecticiq-platform-app-for-splunk/bin/eiq_send_sightings.py]
passAuth = splunk-system-user
```

- *eiq_collect_feeds.py* is the script that collects outgoing feed data from EclecticIQ Platform.
  To change the script execution schedule, edit the corresponding `interval` cron expression.
- *eiq_send_sightings.py* is the script that sends sightings to EclecticIQ Platform.
  To change the script execution schedule, edit the corresponding `interval` cron expression.

For further details on Splunk cron expressions, see the official **Splunk documentation on cron expressions** `(http://docs.splunk.com/documentation/splunk/latest/alert/definescheduledalerts#using_cron_expressions` and their **answers to common questions on cron expressions** `(https://answers.splunk.com/answers/120603/cron-expression-in-splunk.html).`

After correctly configuring EclecticIQ Platform App for Splunk to integrate and work with Splunk, the corresponding dashboard view should become populated with relevant results.