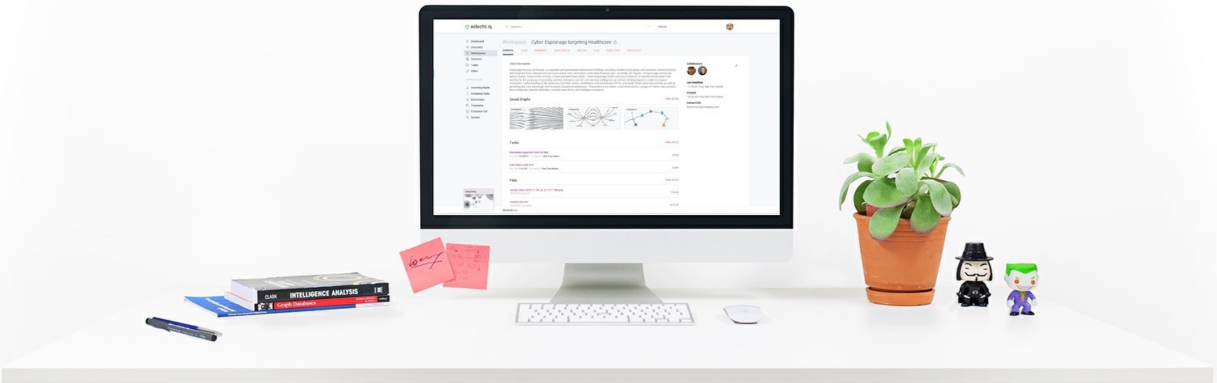
How-tos for EclecticIQ Platform

Hands-on articles on specific platform features

Last generated: July 21, 2017



Last generated on Jul 21, 2017

Table of contents

How to work with enrichers

This summary page offers an overview of the available how-to and tutorial articles about configuring and working with enrichers. They describe how to set up enricher rules and tasks, as well as how to review and search for enrichment observables.

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

Title	Excerpt
How to enrich entities with observables	Enrichment observables augment the quality of the intelligence you obtain from cyber data analysis. Enrich entities and integrate entity observables with additional raw data to access a broader context and gain deeper insight into threat scenarios.
How to work with the Censys enricher	The Censys enricher returns a wealth of information about IP addreses, from a network ASN to their geographic location, so that you can explore relationships between events, actors, and targets.
How to work with the Crowdstrike Falcon Intelligence Indicator enricher	The Crowdstrike Falcon Intelligence Indicator enricher returns observables extracted from indicators to provide additional context to existing platform intelligence.
How to work with the DomainTools Hosted Domains enricher	The Domaintools Hosted Domains enricher returns all domain names related to the specified input IP addresses.
How to work with the DomainTools Malicious Server Domains enricher	The DomainTools Malicious Server Domains enricher returns malicious domain names related to the same primary and/or secondary name servers, along with their risk scores to automatically flag server domains with an appropriate maliciousness confidence level.
How to work with the DomainTools Retrieve Parsed Whois Observables enricher	The DomainTools Retrieve Parsed Whois Observables enricher returns malicious domain names related to the same primary and/or secondary name servers.
How to work with the DomainTools Reputation enricher	The Domaintools Reputation enricher returns risk scores to assess the reputation of the specified input domain and host names.
How to work with the DomainTools Suspicious Domains enricher	The DomainTools Suspicious Domains enricher returns suspicious and potentially malicious domains related to the input IP addesses, along with their risk scores to automatically flag domains with an appropriate maliciousness confidence level.
How to work with the Elasticsearch sightings enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Elasticsearch sightings enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

Title	Excerpt
How to work with the Farsight DNSDB enricher	The Farsight DNSDB enricher provides historical passive DNS information to relate domain names with the IP addreses they point to, or IPs pointing to different domains over time.
How to work with the Flashpoint AggregINT enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Flashpoint AggregINT enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the Flashpoint Blueprint enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Flashpoint Blueprint enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the Flashpoint Thresher enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Flashpoint Thresher enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the Fox-IT InTELL Portal enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Fox-IT InTELL Portal enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the Intel 471 enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Intel 471 enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the OpenResolve enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the OpenResolve enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the PassiveTotal enrichers	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run PassiveTotal whois, passive DNS, IP and domain, and malware enrichers, view enrichment observables in the entity detail pane and on the graph, and search for enr...
How to work with the PyDat enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the PyDat enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the Recorded Future enricher	The Recorded Future enricher enables you to tap into the data stream generated by the Recorded Future Temporal Analytics Engine to retrieve search results potentially malicious IPs, domains, email addresses, and hashes related to the input observable types, along with their risk scores to automatically flag domains ...
How to work with the RIPEstat GeoIP enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the RIPEstat GeoIP enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

Title	Excerpt
How to work with the RIPEstat Whois enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the RIPEstat Whois enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the ThreatCrowd enricher	The ThreatCrowd enricher returns suspicious and potentially malicious domains, IP addreses, email addresses, file hashes, and antivirus detections, so that you can explore relationships between events, actors, and targets.
How to work with the ThreatGRID enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the ThreatGRID enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.
How to work with the Unshorten-URL enricher	The Unshorten-URL polls the specified URL shortener services to return the resolved original URLs corresponding to the submitted shortened ones.
How to work with the VirusTotal enricher	Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the VirusTotal enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

How to work with the Censys enricher

The Censys enricher returns a wealth of information about IP addreses, from a network ASN to their geographic location, so that you can explore relationships between events, actors, and targets.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the Censys enricher

This article describes how to configure the Censys enricher parameters.
To configure the general options for the Censys enricher, see Configure enrichers.

Censys	**enricher**
Enricher name	Censys
API endpoint	`https://censys.io/api/v1/search/ipv4`
Input	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
Output	Enriches the supported observable types by providing additional context such as geolocation, country and city information, as well as **ASN** `(https://en.wikipedia.org/wiki/autonomous_system_(internet))` details.
Description	Returns relevant contextual information about the submitted observable types to augment their intelligence value with geographic and geolocation details, hashes, and **ASN** `(https://en.wikipedia.org/wiki/autonomous_system_(internet))` details. It makes it easier to discover relationships between events, actors, and targets.

Configure the Censys enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.

- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the Censys enricher:

- **API URL**: the URL pointing to the API endpoint exposing the service that grants access to the enricher data source. Contact the intelligence provider to subscribe to the service and to obtain this information, as well as any required authentication and authorization credentials.
  The API URL for this enricher exposes the Censys **Search API** `(https://censys.io/api/v1/docs/search)`.
  The *ipv4* URL parameter allows sending requests to the IP address search index.
- **API ID**: **create an account** `(https://censys.io/register)` to receive the login credentials you need to authenticate and access the API service.
  Enter here your API user ID.
- **API secret**: enter the secret key associated to your API user profile, so that you can log in and consume the API service.
- **Observable queries**: from the drop-down menu select the observable type and the corresponding observable value the rule should look for.
  - In the first input field, from the drop-down menu select the *observable type* the rule should look for.
    Supported observable types:
    - *asn*
    - *city*
    - *company*
    - *country*
    - *country_code*
    - *geo-lat*
    - *geo-long*
    - *hash-md5*
    - *hash-sha1*
    - *hash-sha256*
    - *ipv4*
    - *postcode*
  - In the second input field, specify the *observable value* associated to the observable type that the rule should look for.
    You can use free text, wildcards, **Elasticsearch query syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html)`, as well as the *{kind}* and *{value}* placeholders to reference an observable type and value, respectively.
    When the query executes, the placeholders take the values from the input observable key (*{kind}*) and value (*{value}*) pairs, respectively.
    Example:
    The **@{value}* query searches for observable values matching the input observable values it is fed at runtime.
    Censys allows using **specific data fields** `(https://censys.io/overview)` to search for data related to IP hosts.
    You can combine these data definitions with the *{kind}* and *{value}* placeholders.
- Click **+ Add** or **+ More** to add a new filtering option. For example, to include in the search additional key/value pairs like IP addresses, hashes, or domains.

- 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 **✚ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **✚ Add** or **✚ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.

- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

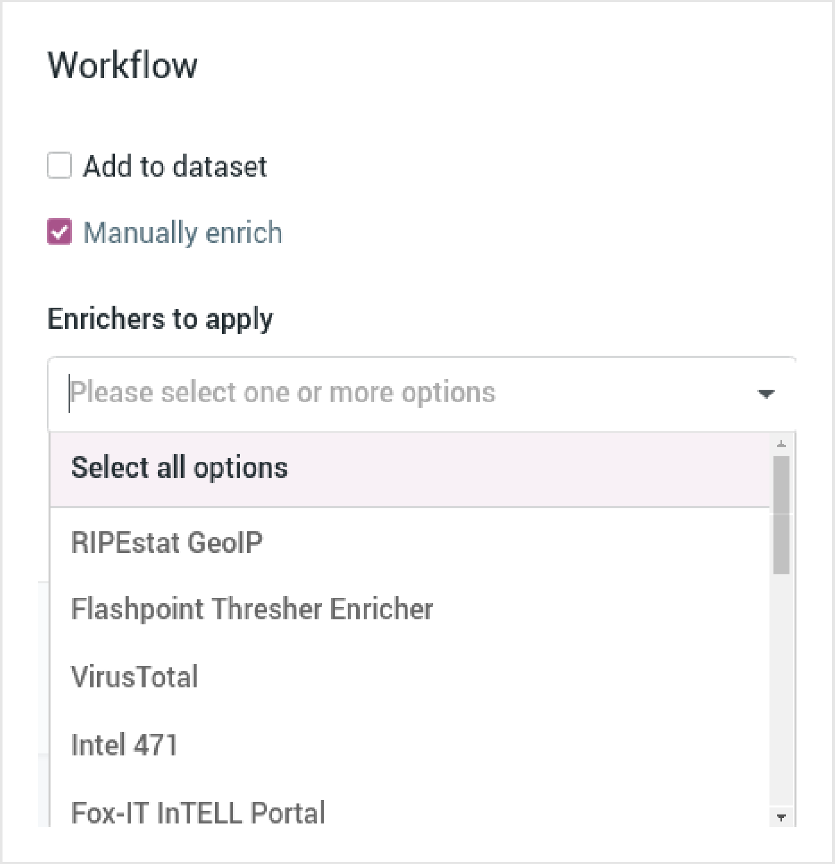
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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.

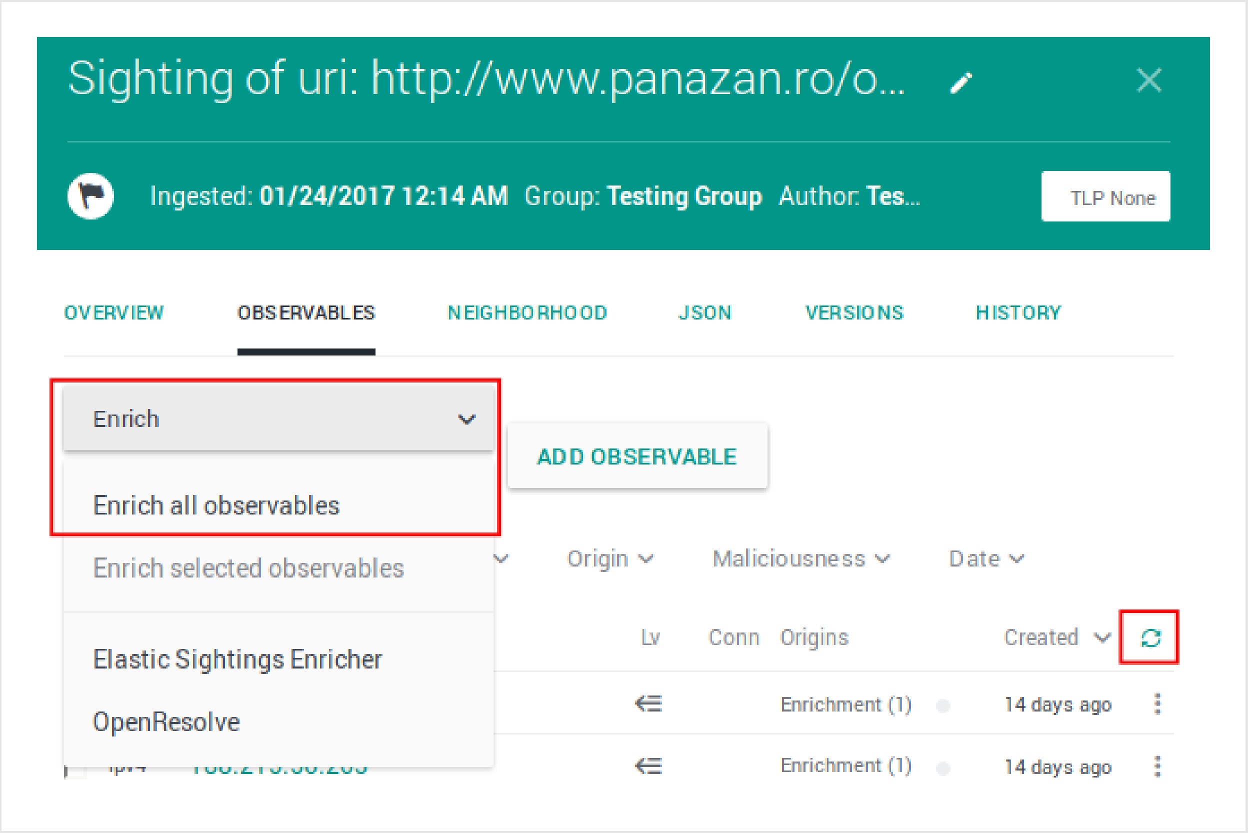
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the 🗘 refresh icon to trigger a task run that polls all the enrichers configured for the entity.

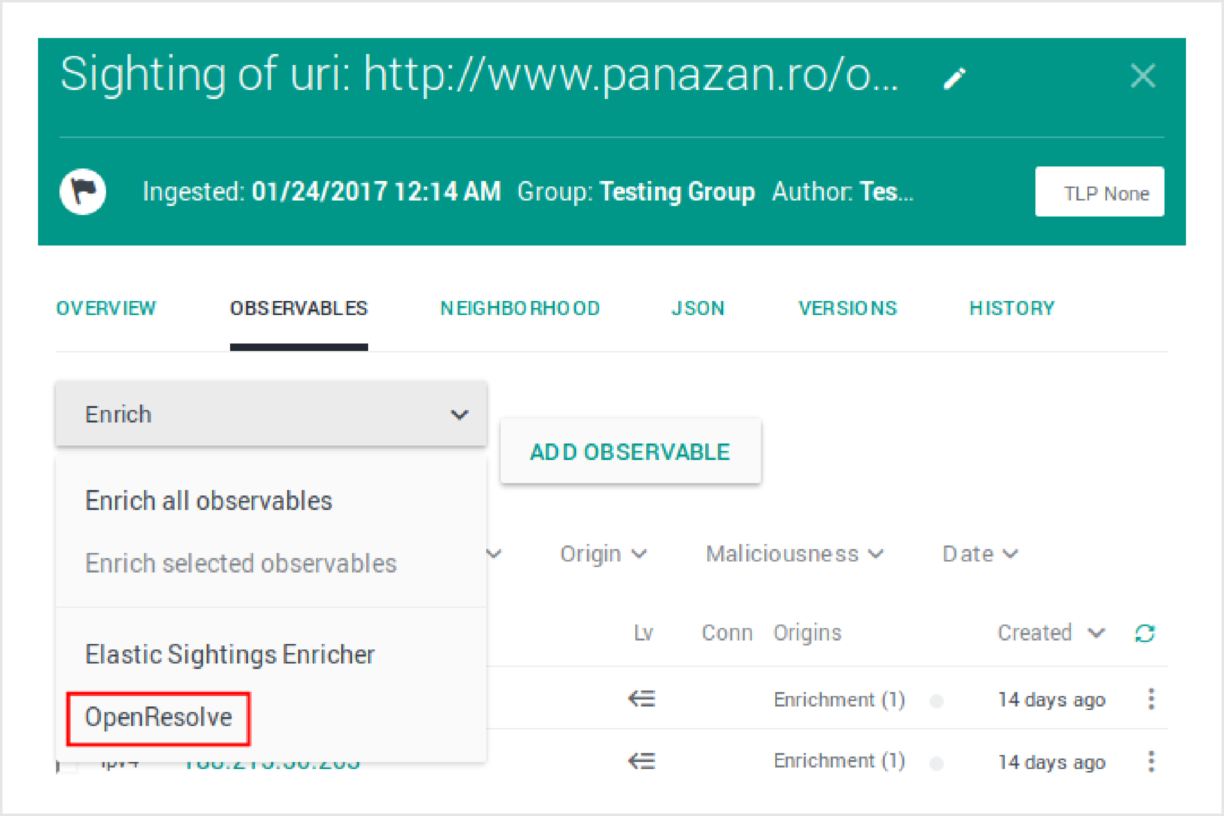
Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



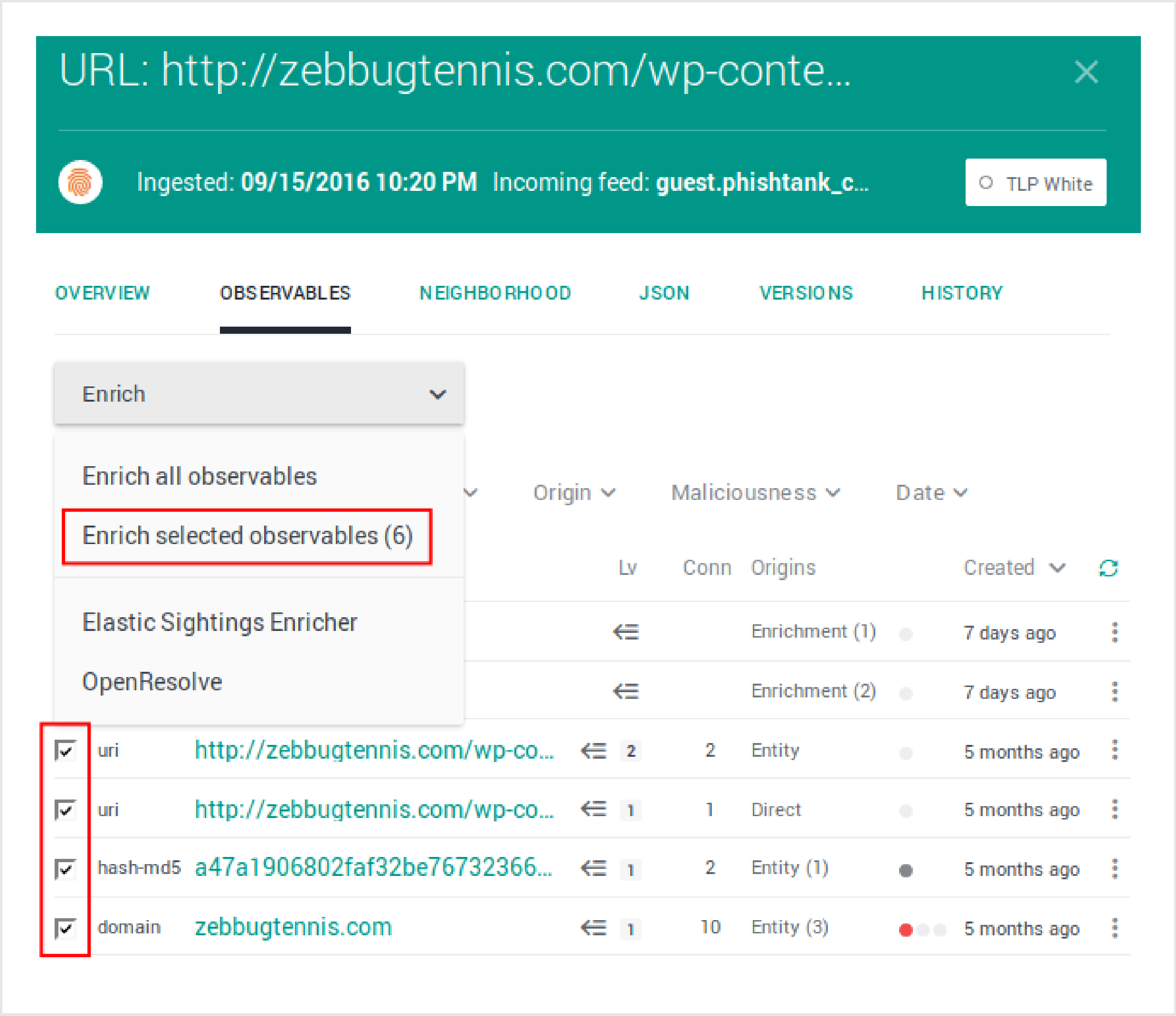
To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.
- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



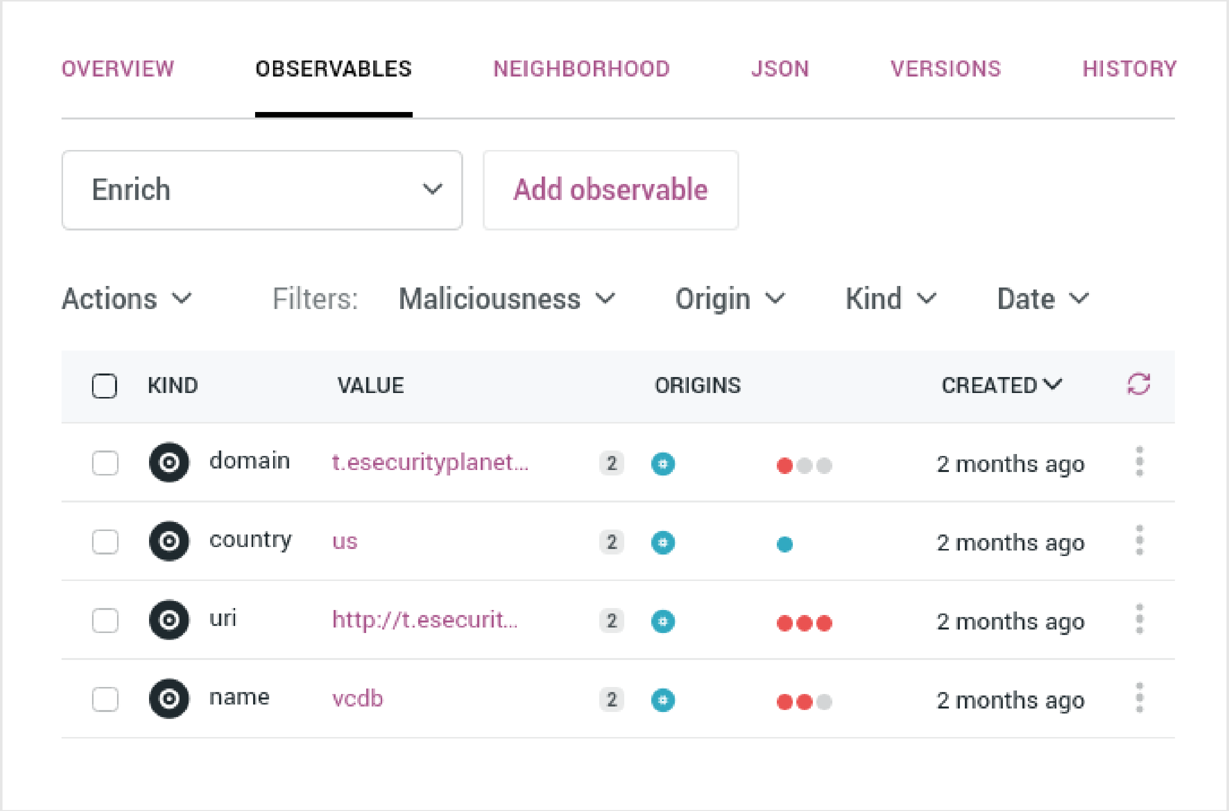
The available enricher tasks in the drop-down menu are automatically filtered to show only the applicable enrichers for the entity.

Enrichers automatically augment all the entities that accept the enricher's content type as an observable. In other words, the observable types an entity supports define the applicable enrichers an entity can use.

Review enrichment observables

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.

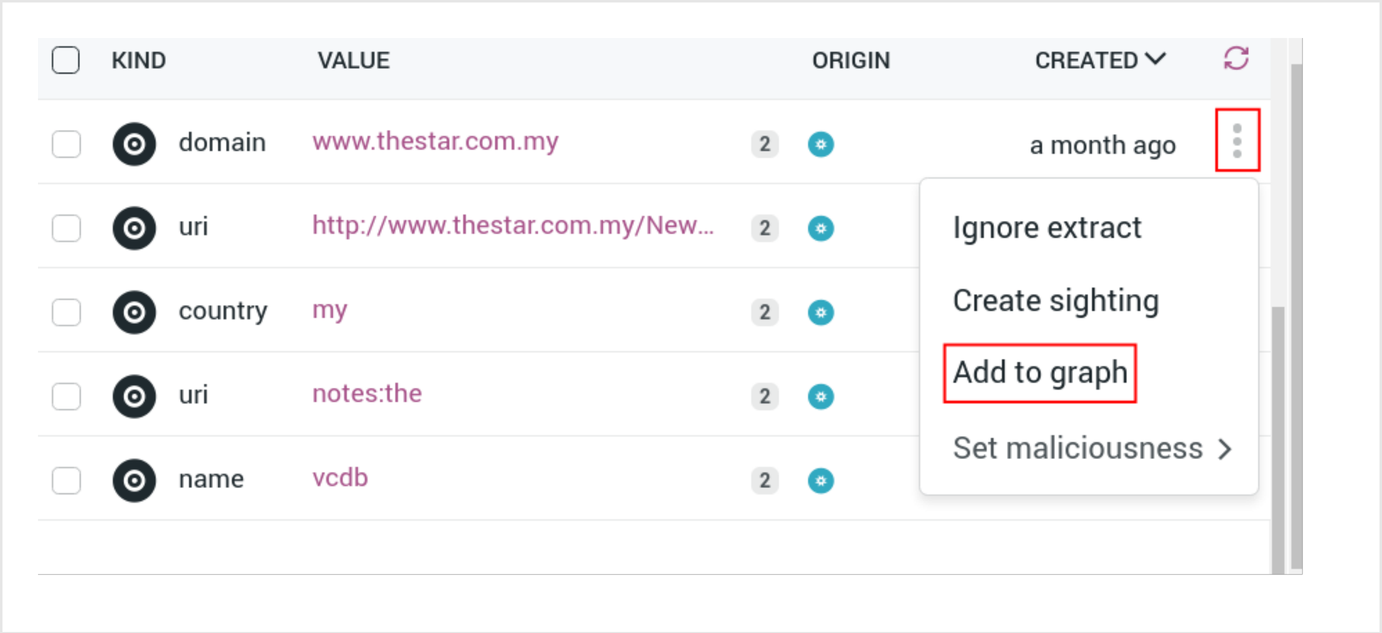


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

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

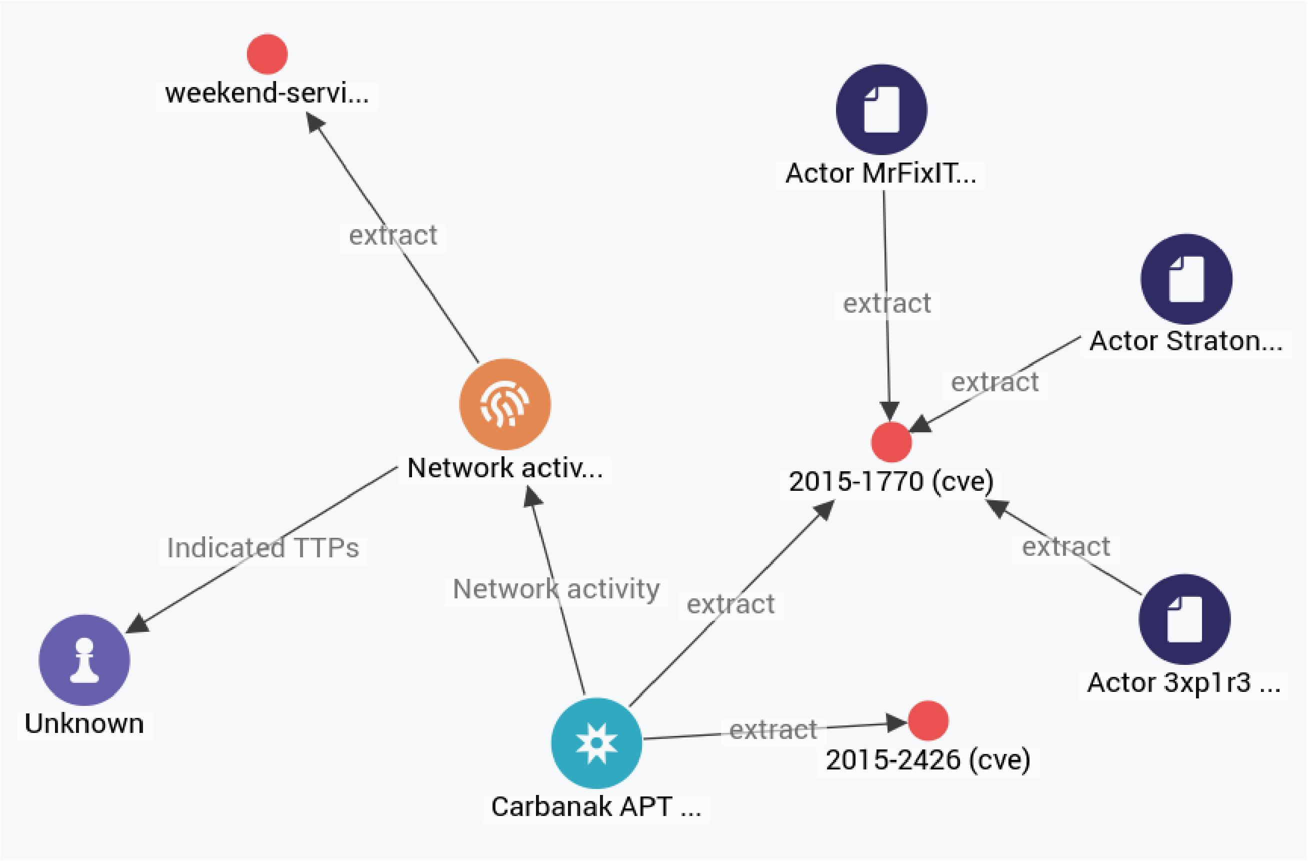
- On the row corresponding to the observable you want to load onto the graph, click the ⋮ icon, and then select **Add to graph**.



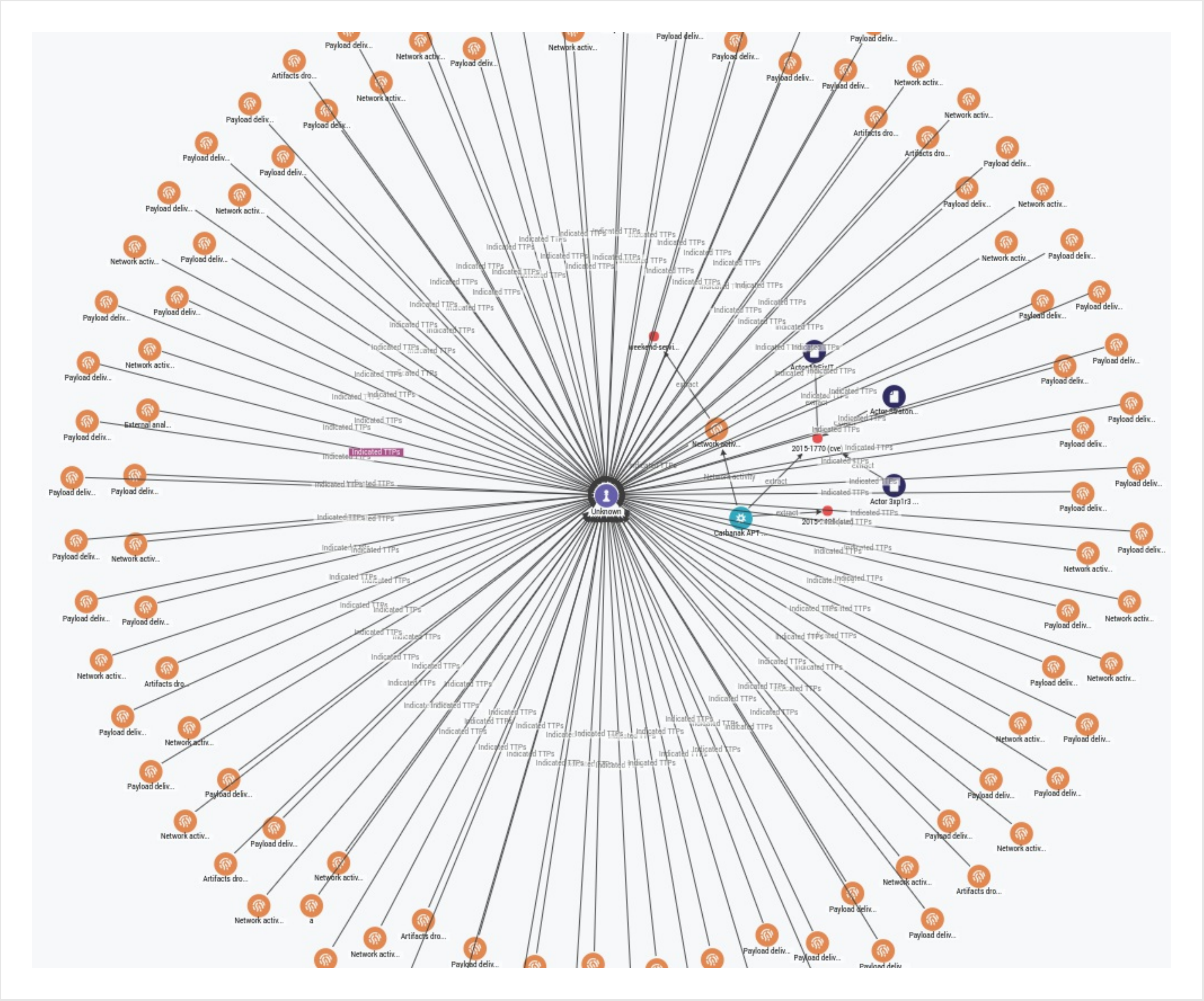
☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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**.

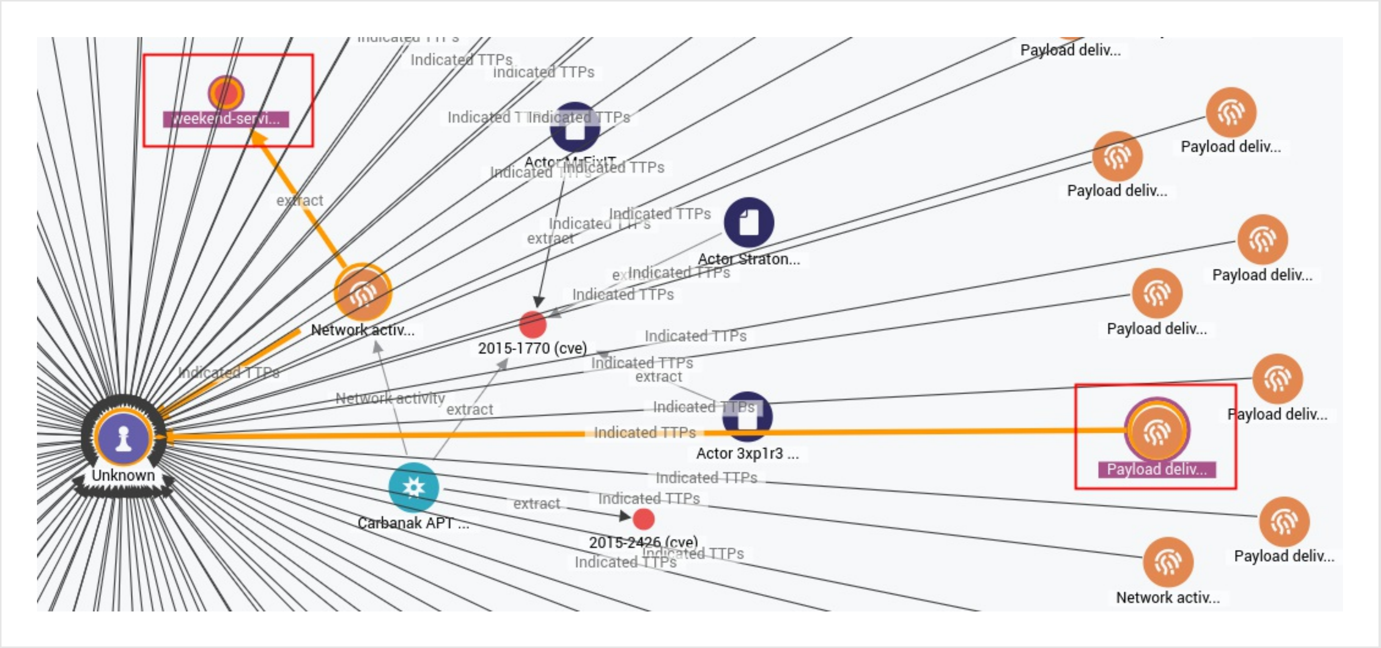


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



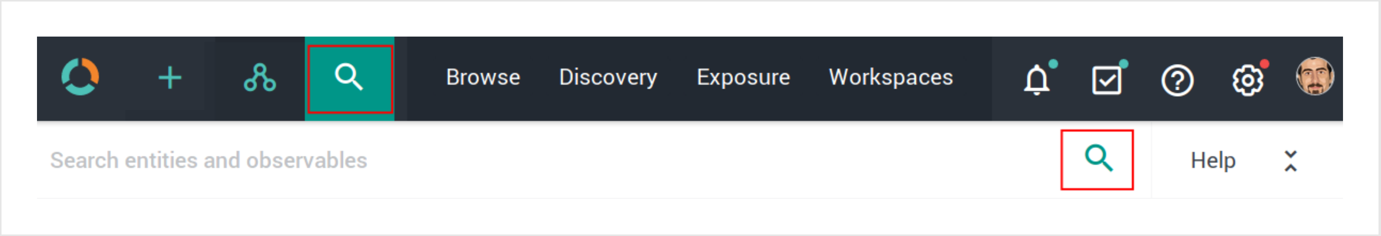
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

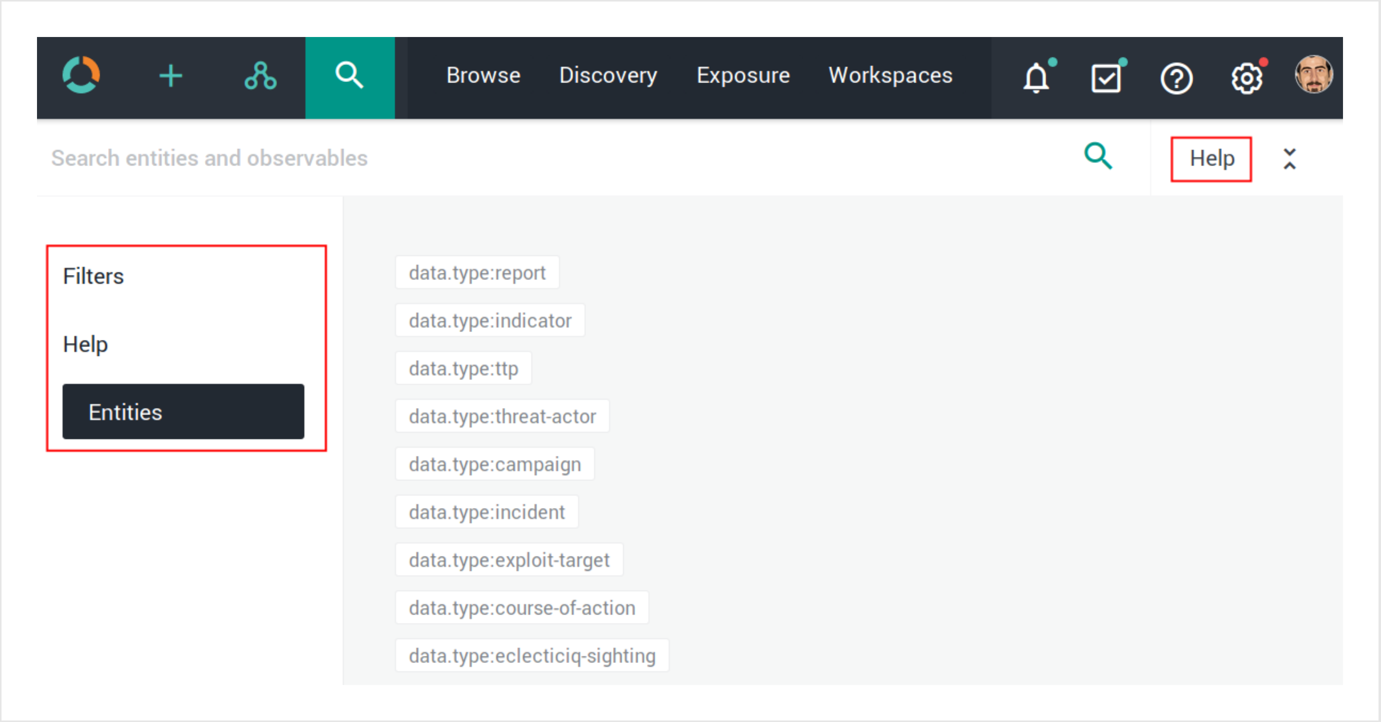


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

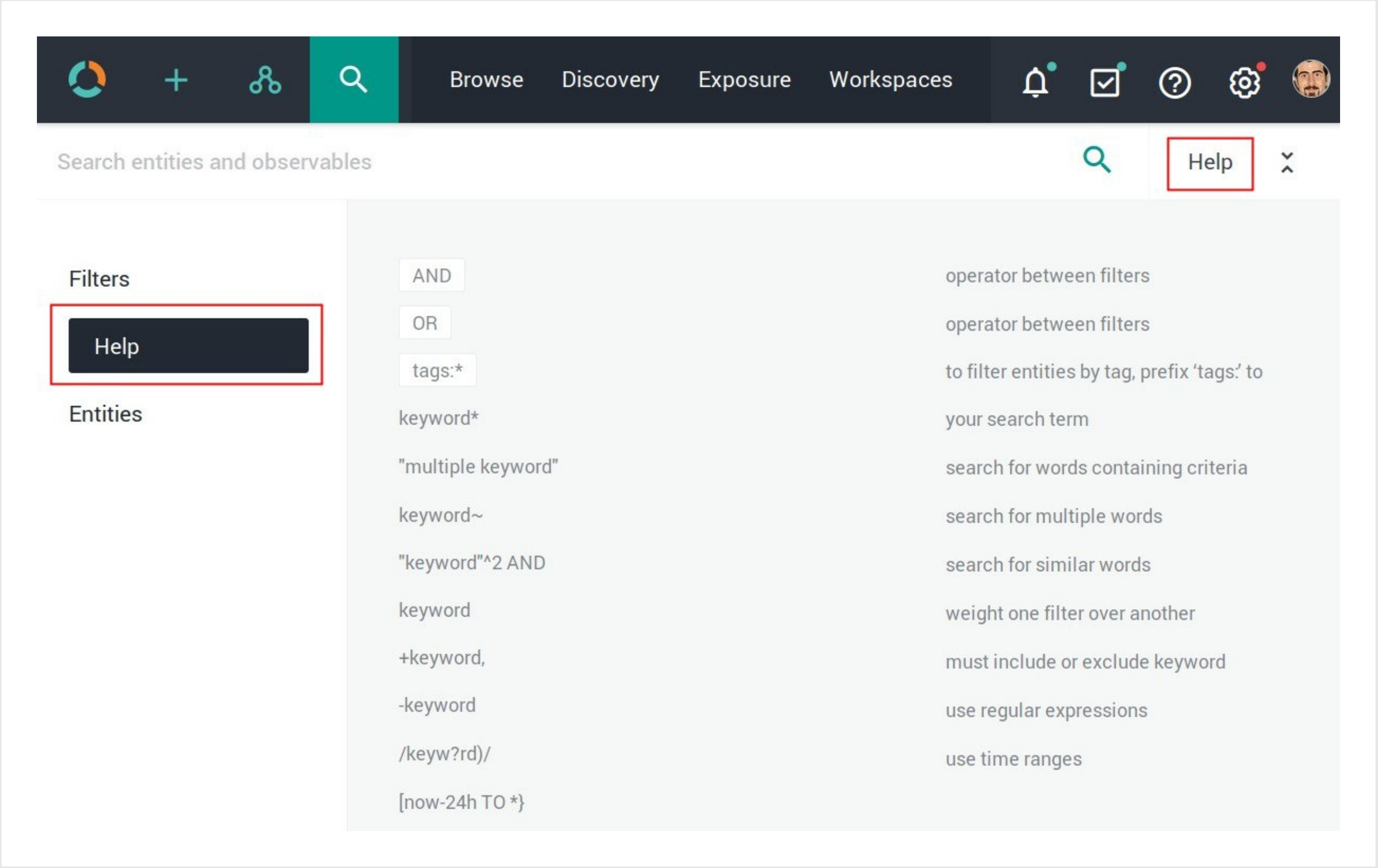
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

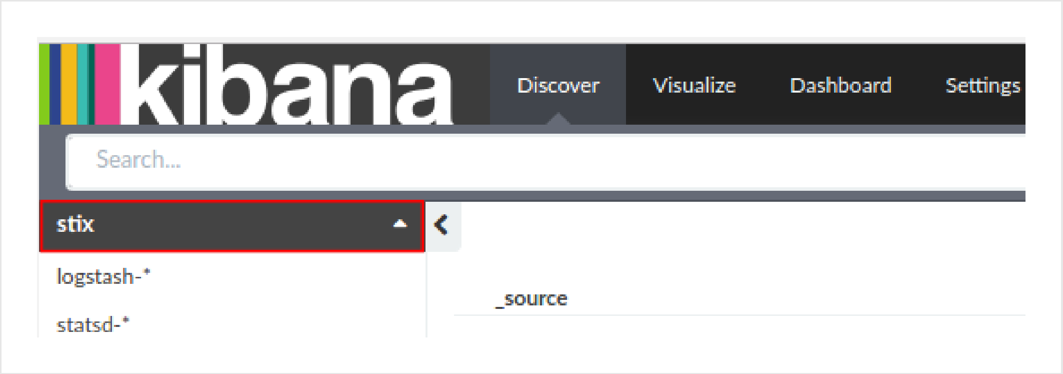
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

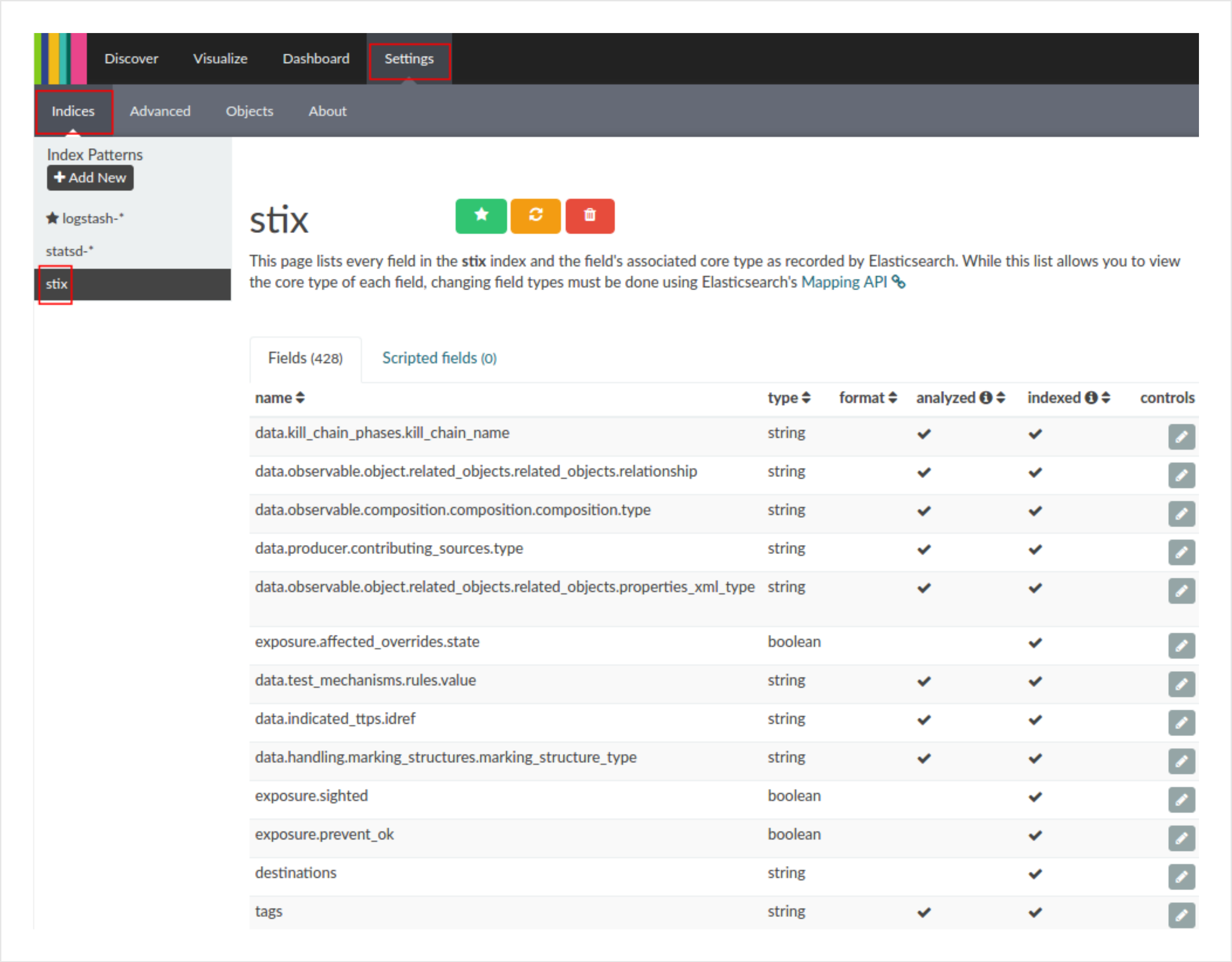
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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		✓	✓	✎

How to work with the Crowdstrike Falcon Intelligence Indicator enricher

The Crowdstrike Falcon Intelligence Indicator enricher returns observables extracted from indicators to provide additional context to existing platform intelligence.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the Crowdstrike Falcon Intelligence Indicator enricher

This article describes how to configure the Crowdstrike Falcon Intelligence Indicator enricher parameters.
To configure the general options for the Crowdstrike Falcon Intelligence Indicator enricher, see Configure enrichers.

Crowdstrike Falcon Intelligence Indicator	**enricher**
Enricher name	Crowdstrike Falcon Intelligence Indicator
API endpoint	`https://intelapi.crowdstrike.com/indicator/v1/search/{}`
Input	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri
Output	Enriches the supported observable types with information extracted from indicators.
Description	Enriches platform entities and observables with additional context such as IP addresses, domain names, email addresses, hashes, and more.

Configure the Crowdstrike Falcon Intelligence Indicator enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment.**
- Click the enricher you want to configure or modify.

- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the Crowdstrike Falcon Intelligence Indicator enricher:

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **+ Add** or **+ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.

- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.

- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

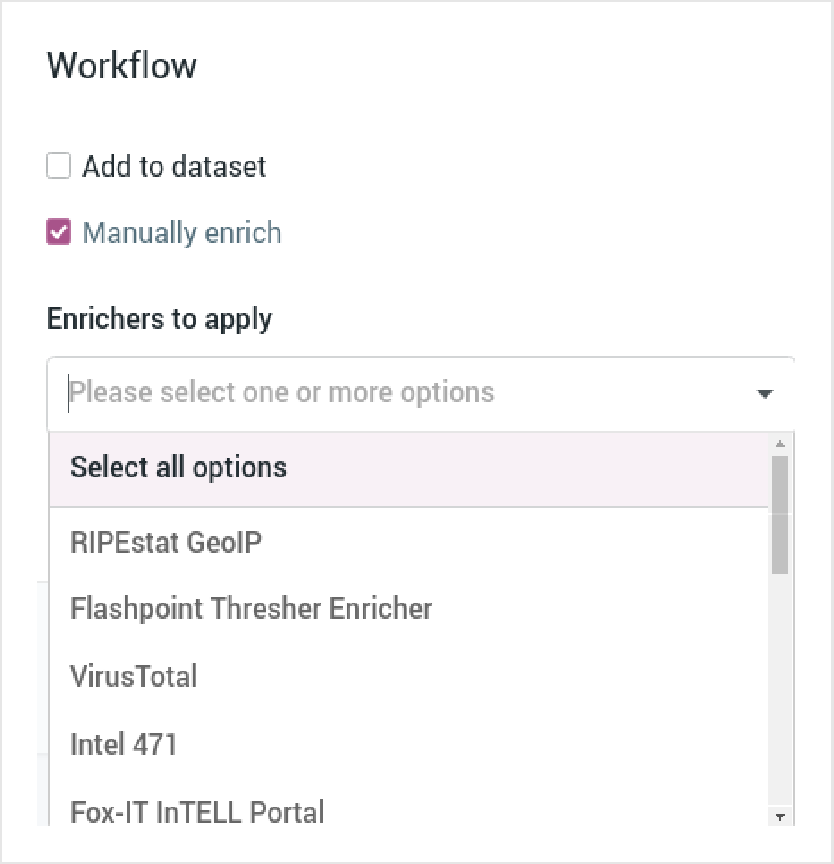
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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

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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

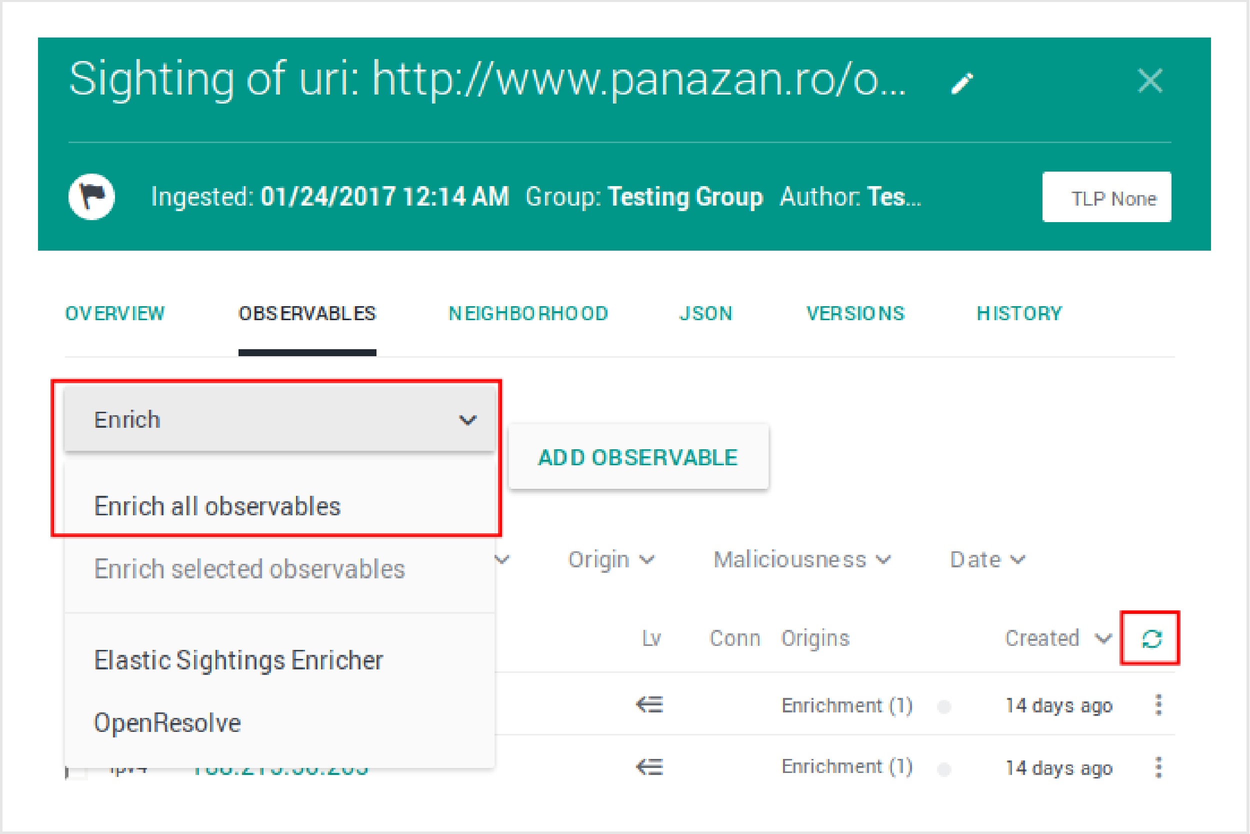
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the ⟳ refresh icon to trigger a task run that polls all the enrichers configured for the entity.

Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.

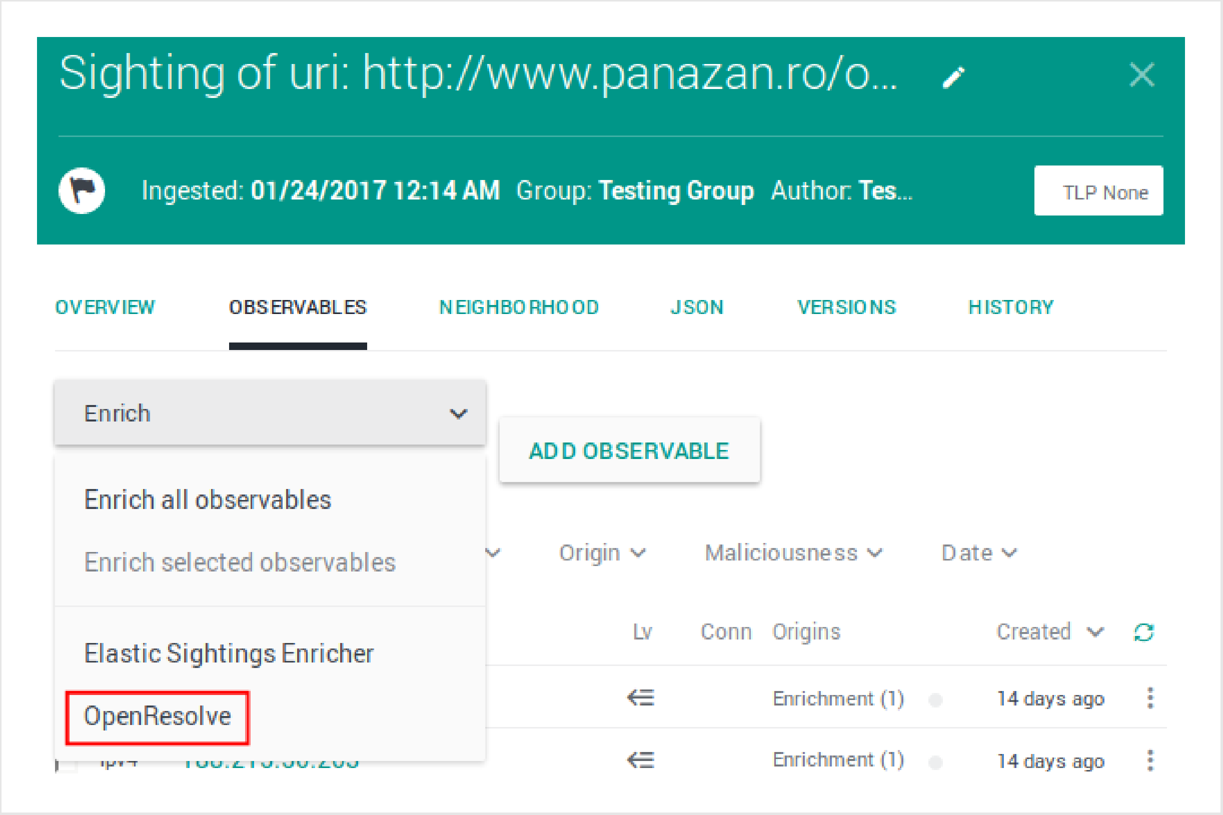


Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

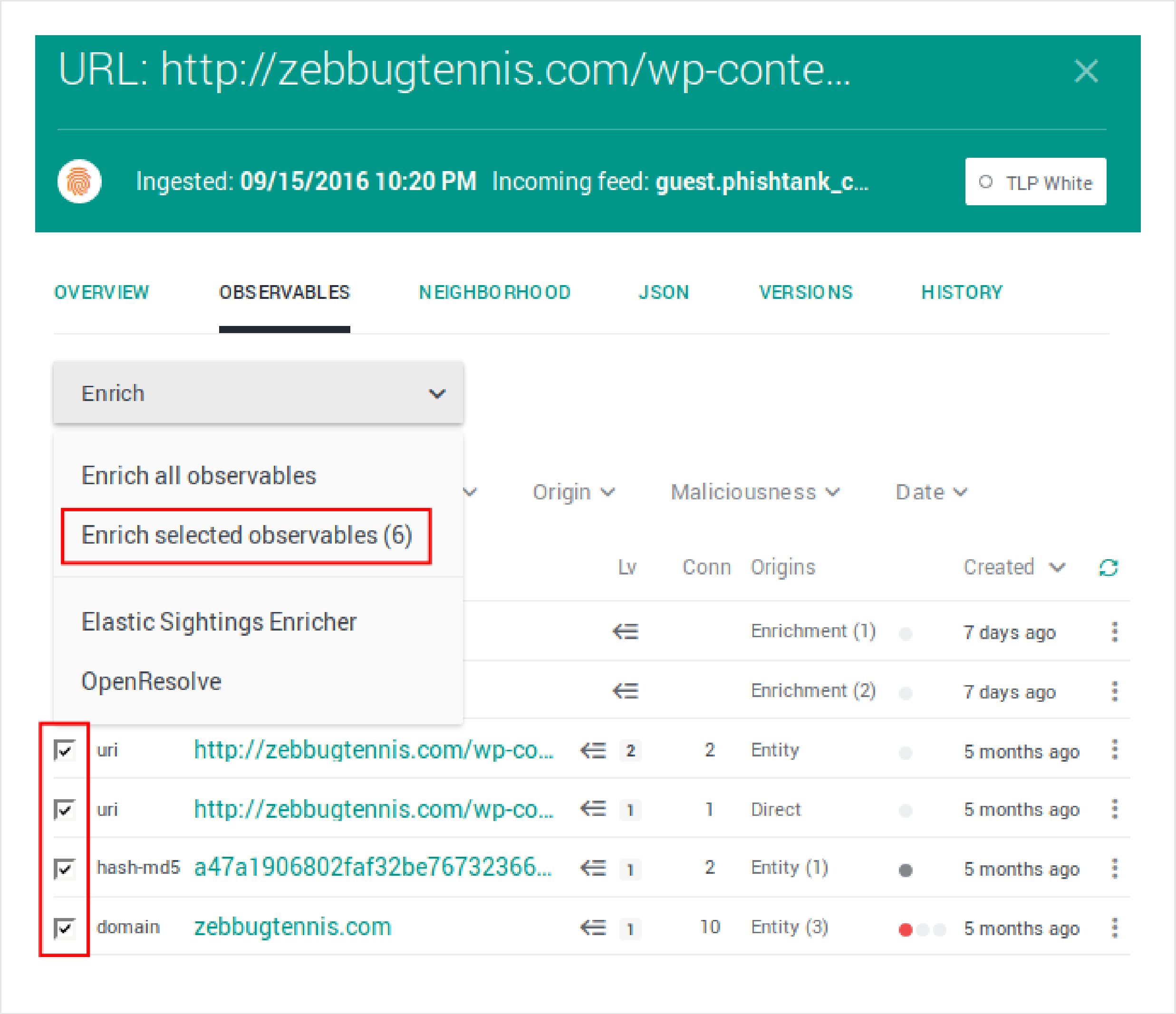
To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.
- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



URL: http://zebbugtennis.com/wp-conte...

Ingested: **09/15/2016 10:20 PM** Incoming feed: **guest.phishtank_c...**

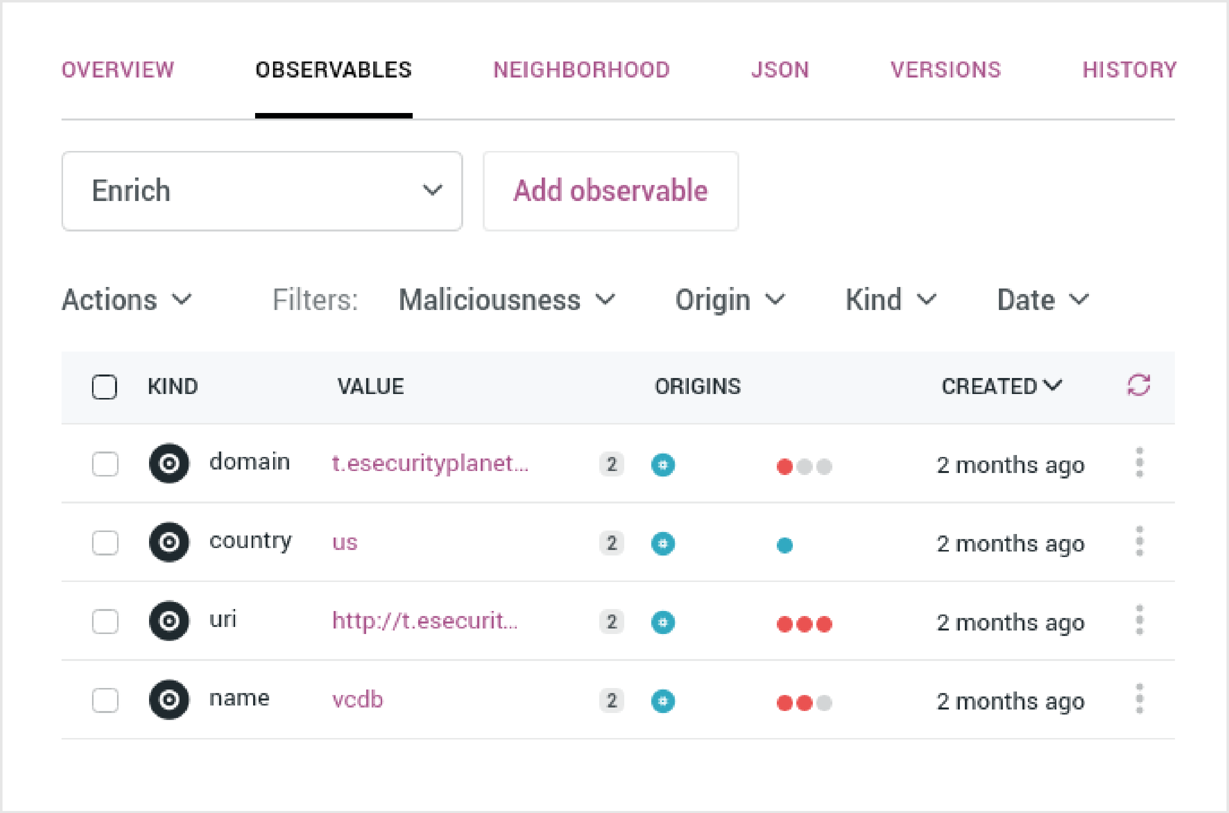
			Lv	Conn	Origins	Created
					Enrichment (1)	7 days ago
					Enrichment (2)	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	2	2	Entity	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	1	1	Direct	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	1	2	Entity (1)	5 months ago
☑	domain	zebbugtennis.com	1	10	Entity (3)	5 months ago

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

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.

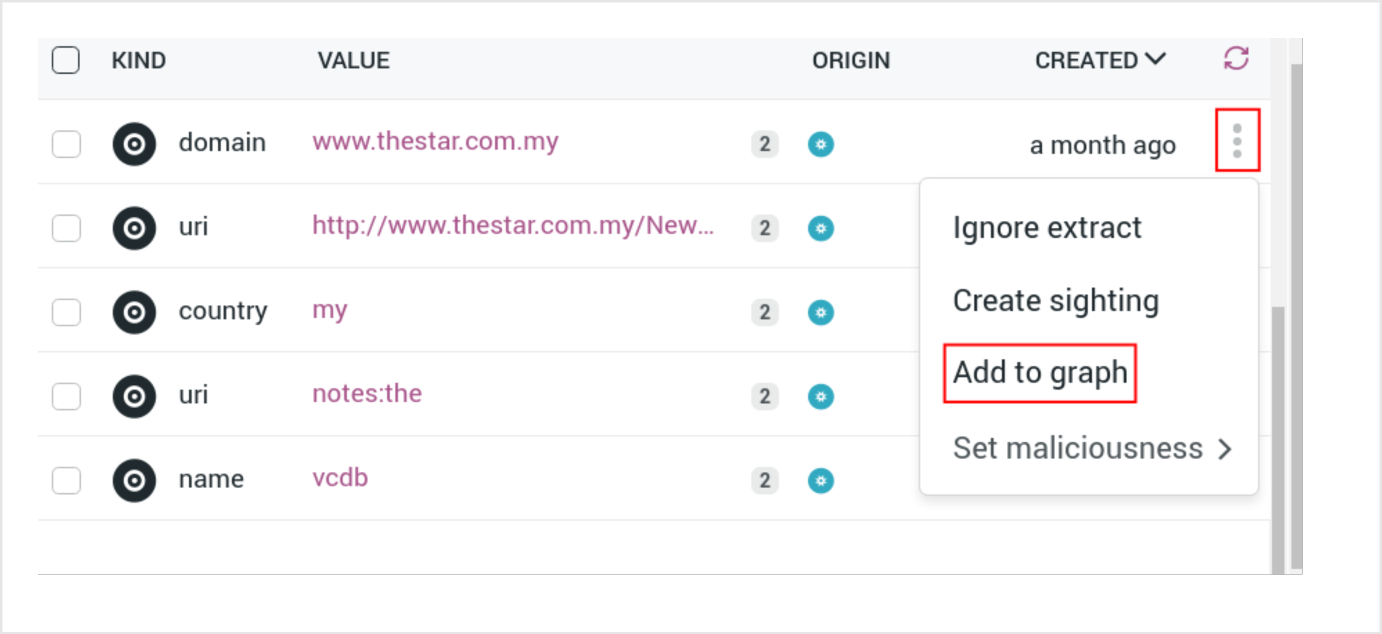


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

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

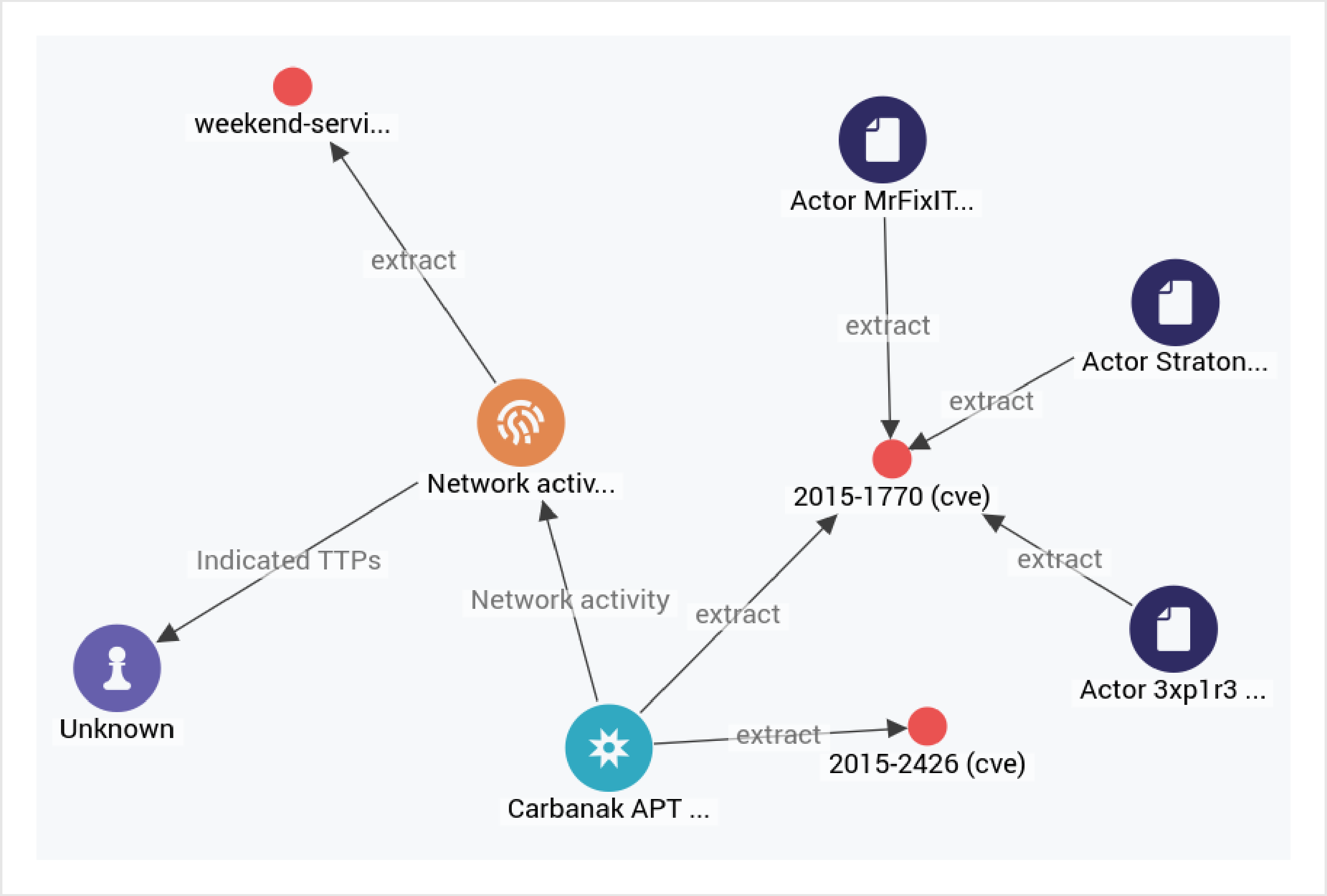
- On the row corresponding to the observable you want to load onto the graph, click the ⋮ icon, and then select **Add to graph**.



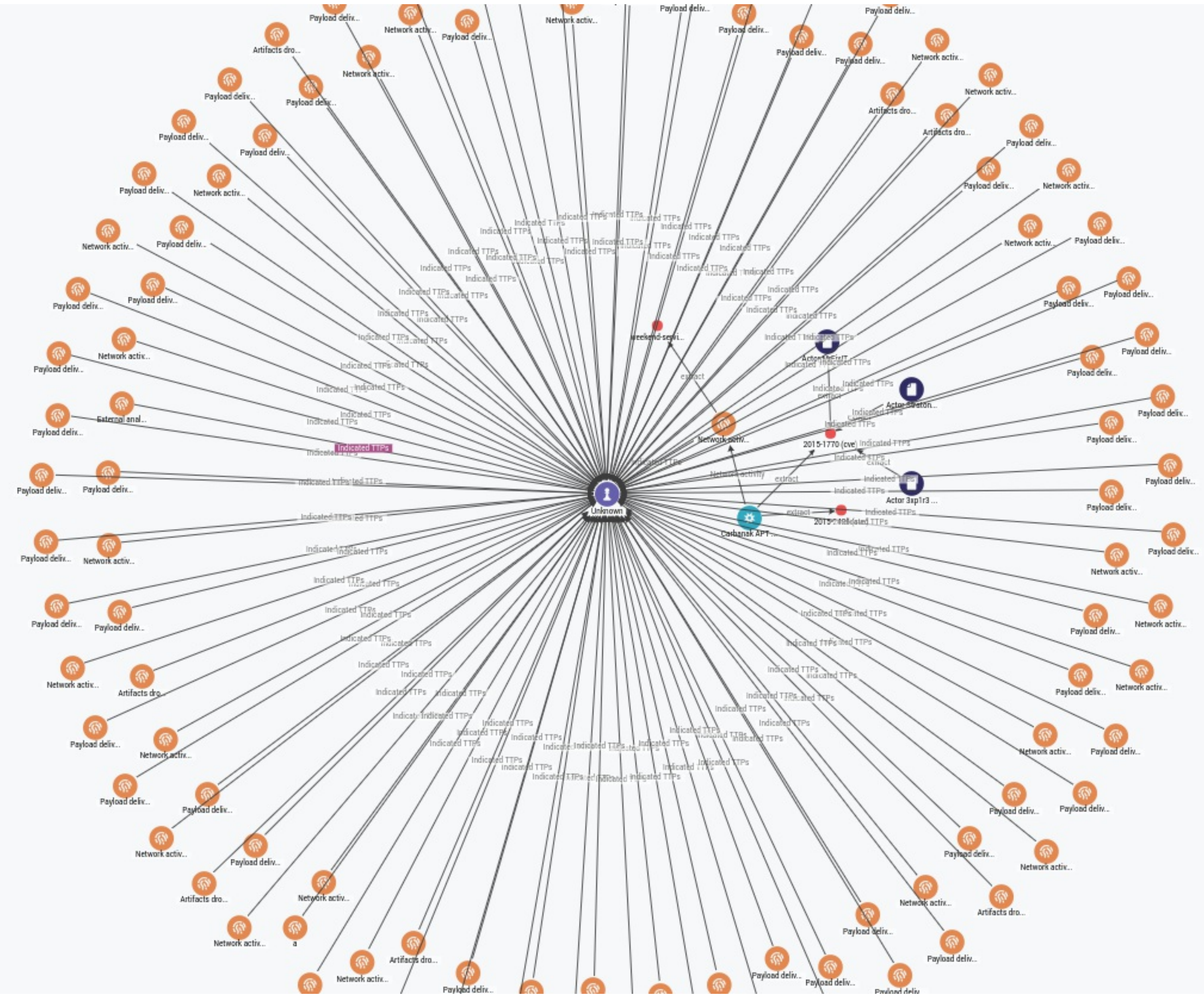
☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

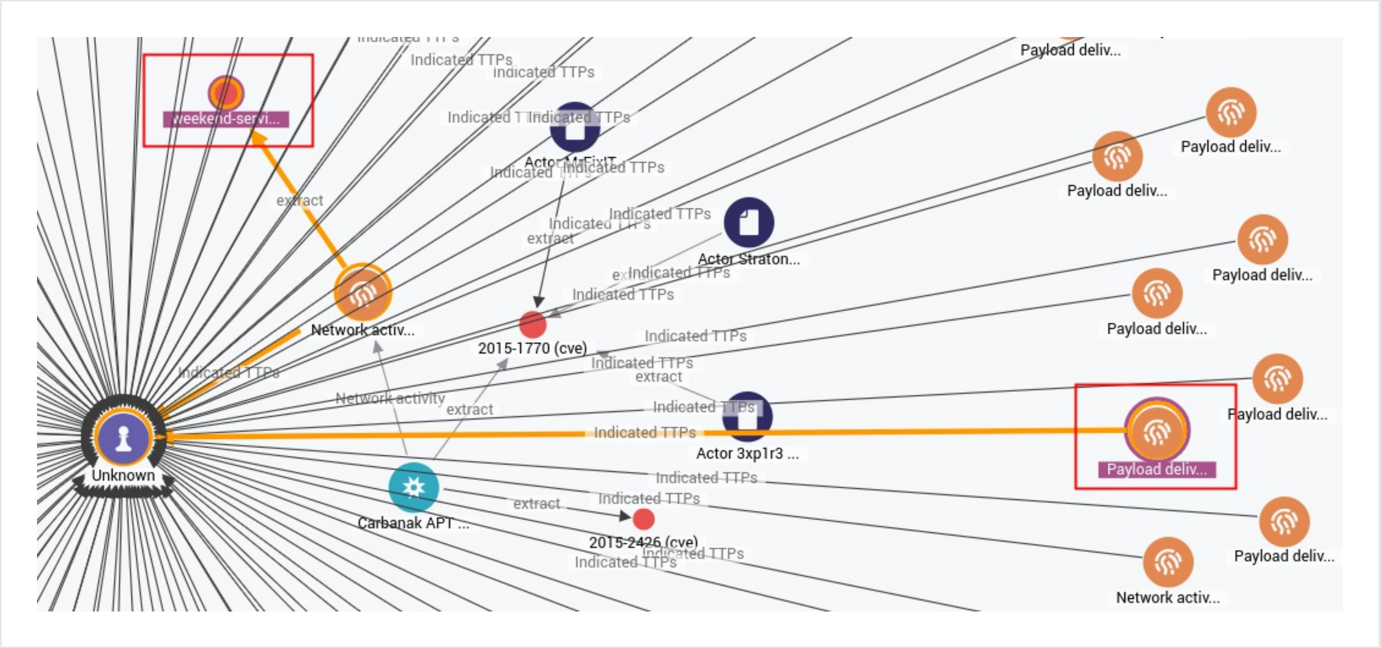


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



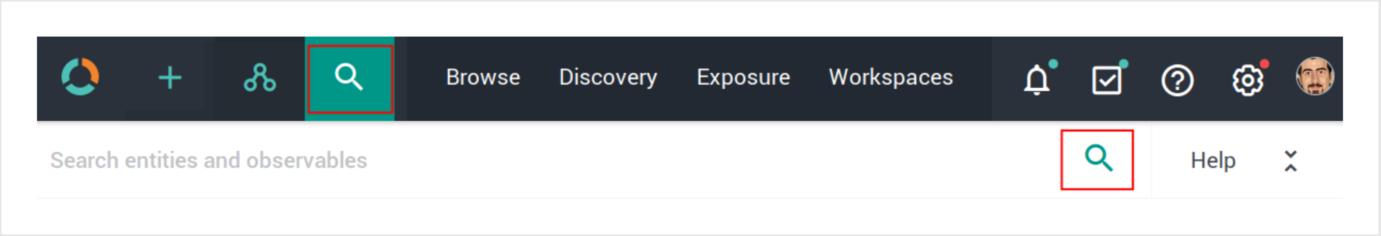
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

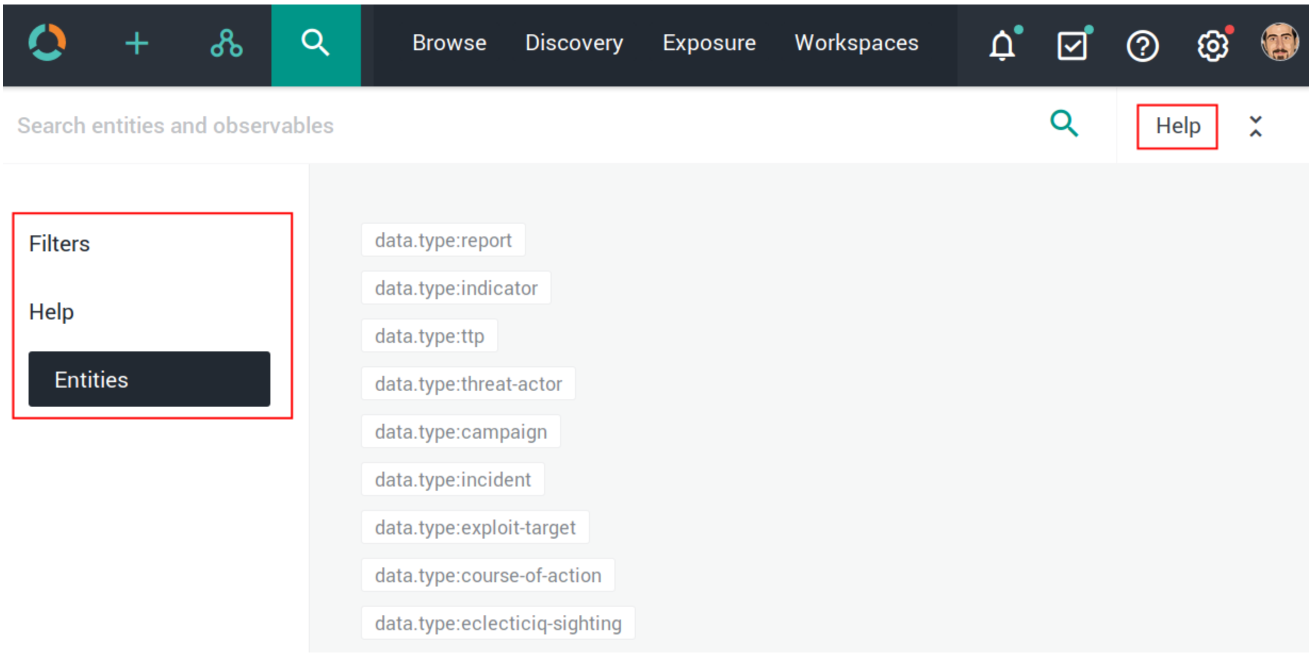


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

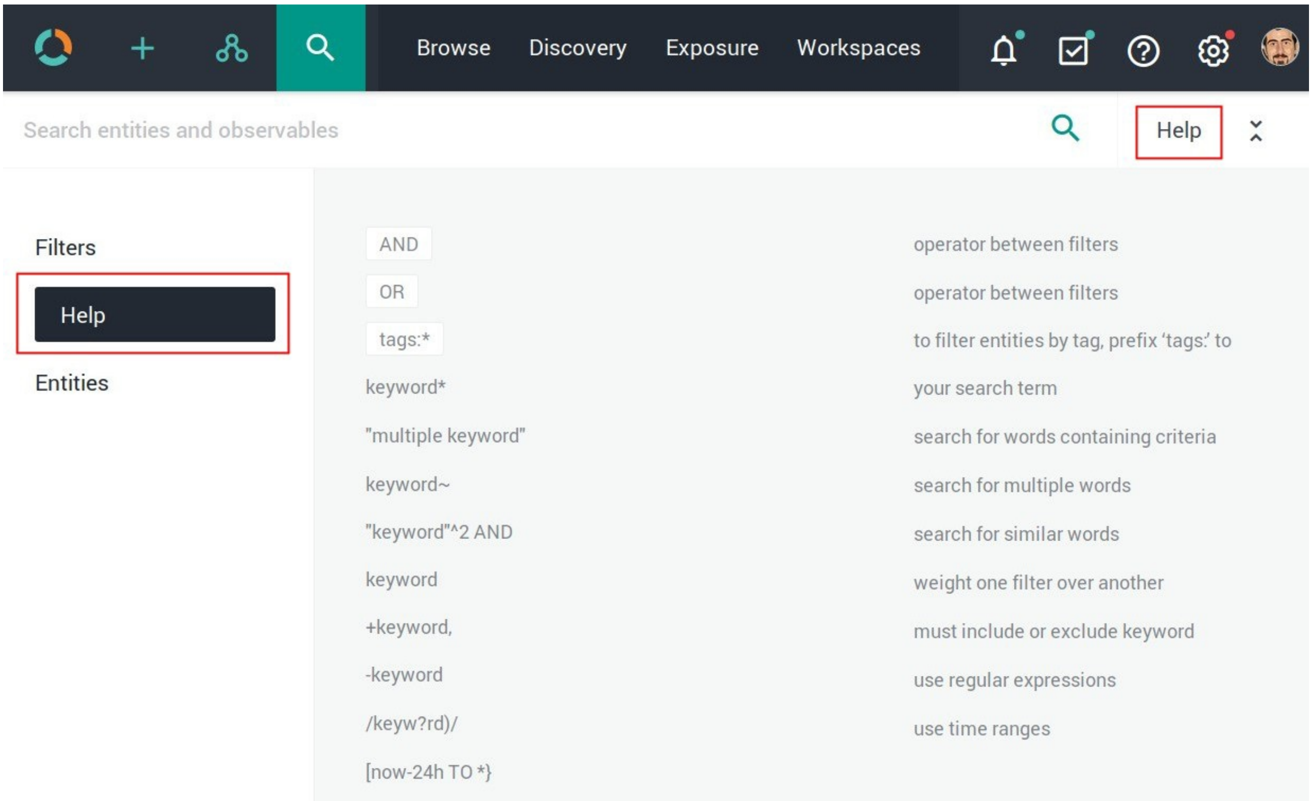
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

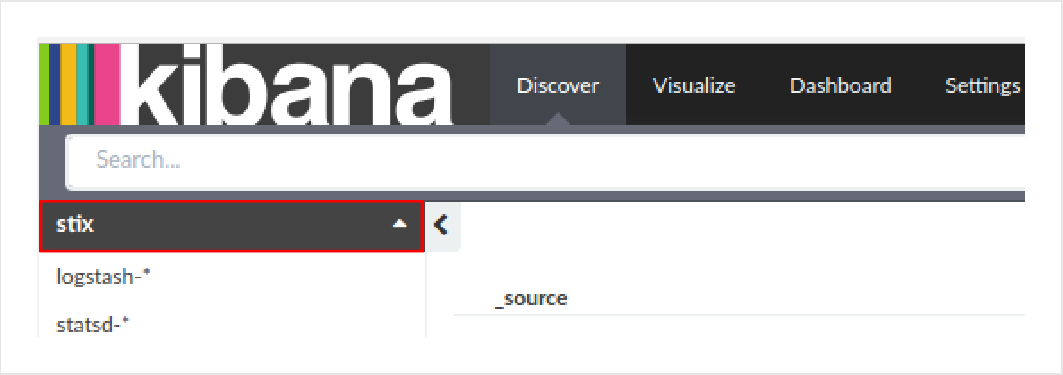
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

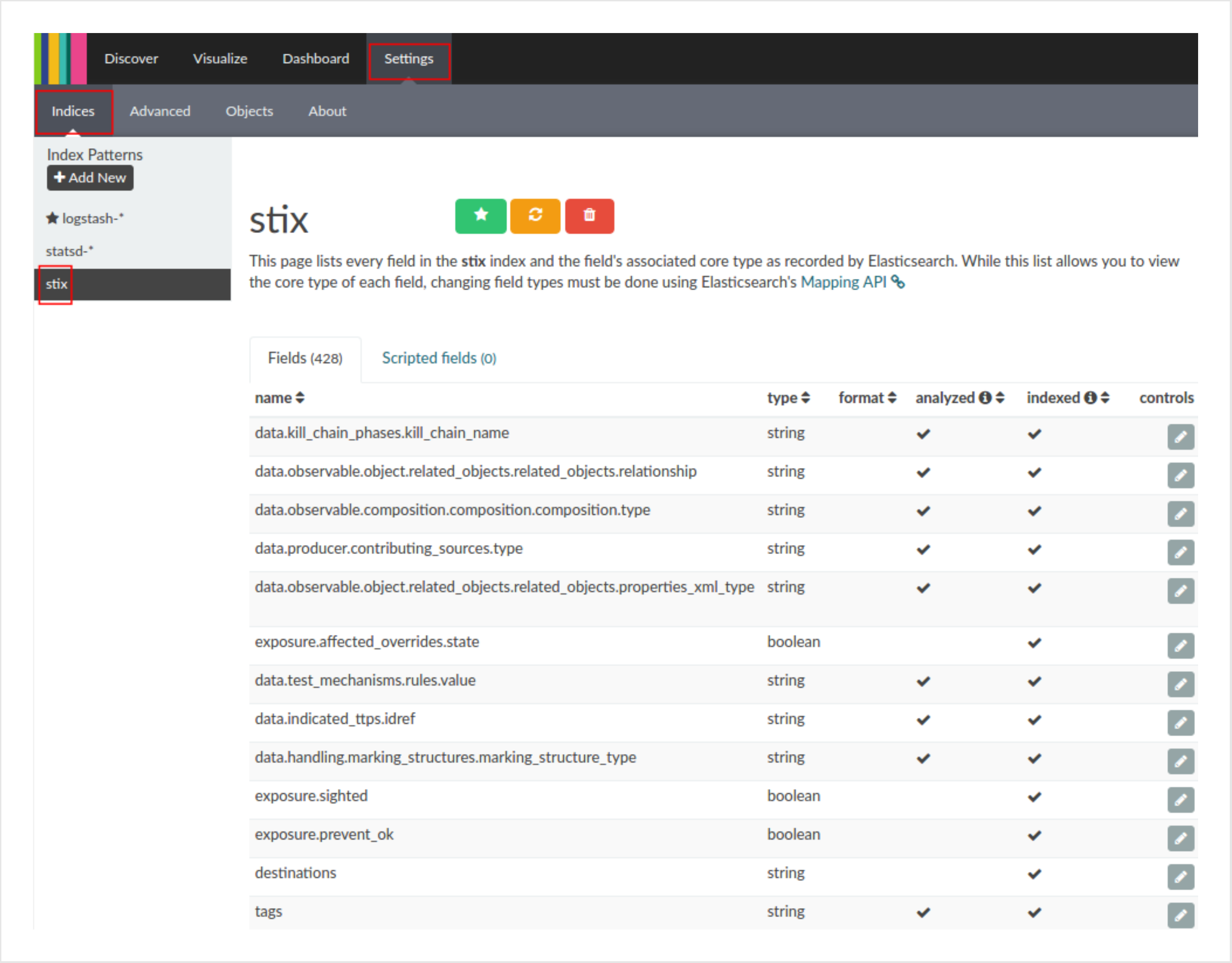
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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		✓	✓	✎

How to work with the Farsight DNSDB enricher

The Farsight DNSDB enricher provides historical passive DNS information to relate domain names with the IP addreses they point to, or IPs pointing to different domains over time.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the Farsight DNSDB enricher

This article describes how to configure the Farsight DNSDB enricher parameters.
To configure the general options for the Farsight DNSDB enricher, see Configure enrichers.

Farsight DNSDB	**enricher**
Enricher name	Farsight DNSDB
API endpoint	`https://api.dnsdb.info/{}`
Input	domain, host, ipv4, ipv6
Output	Enriches the supported observable types with passive DNS lookup information such as the name of the domain or host name owner, or the IP address a domain or host name points to.
Description	Historical passive DNS lookup enricher. It can retrieve previous domains pointing to a specified IP address in the past, domain names hosted by a nameserver, domain names pointing to an IP network, and subdomains existing below a parent domain name.

Configure the Farsight DNSDB enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment.**
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

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

Under **Parameters**, define the specific configuration options for the Farsight DNSDB enricher:

- **API URL**: the URL pointing to the API endpoint exposing the service that grants access to the enricher data source. Contact the intelligence provider to subscribe to the service and to obtain this information, as well as any required authentication and authorization credentials.
  The API URL to reach the Farsight DNSDB service is *https://api.dnsdb.info/{}*.
- **API key**: contact Farsight to receive an API key for the DNSDB service, and then enter it in the corresponding input field.
- **Search results limit**: enter an integer to limit the maximum amount of returned results.
  Default value: each time the enricher runs, it can return max. *1000* matches.
- **Time last seen**: enter an integer to set a starting point in the past to retrieve matches from. The number indicates the number of days in the past from the current time.
  Default value: *365* (each time the enricher runs, it looks for matches up to one year old)
- 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 **+** > **Rules** > **Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **✚ Add** or **✚ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data. **TLP** `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules. You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

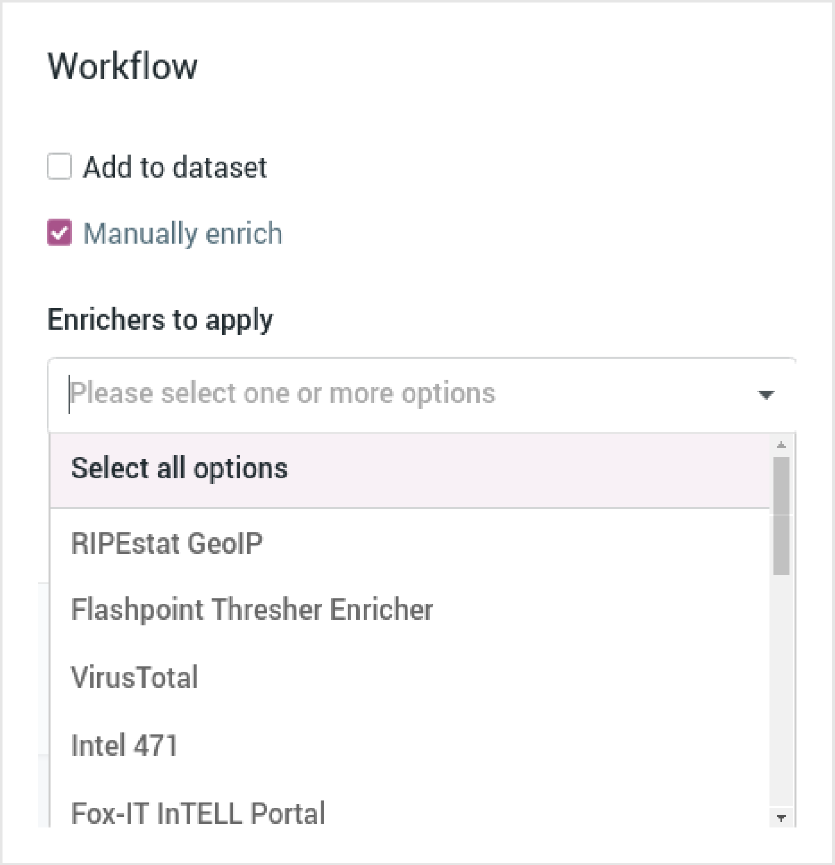
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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.



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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

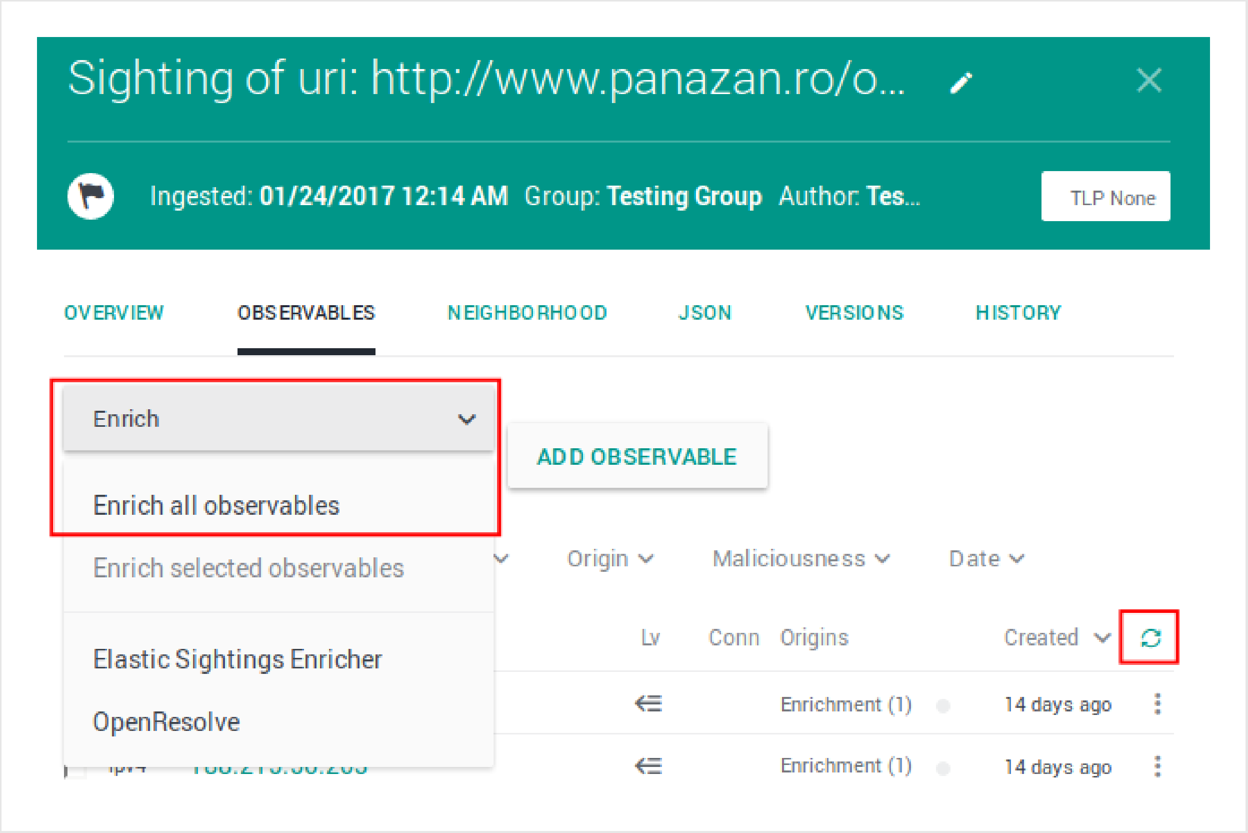
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the 🔄 refresh icon to trigger a task run that polls all the enrichers configured for the entity.

Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



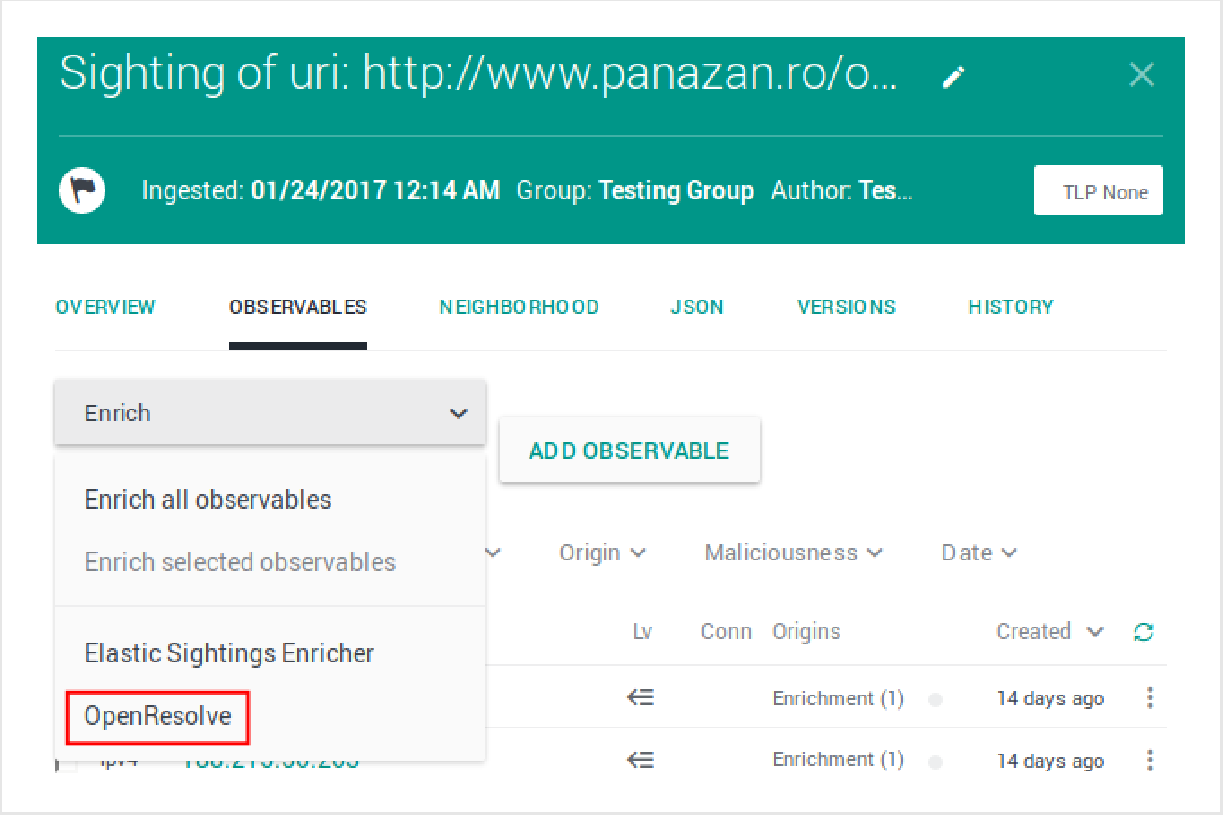
Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

TLP None

To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



Sighting of uri: http://www.panazan.ro/o...

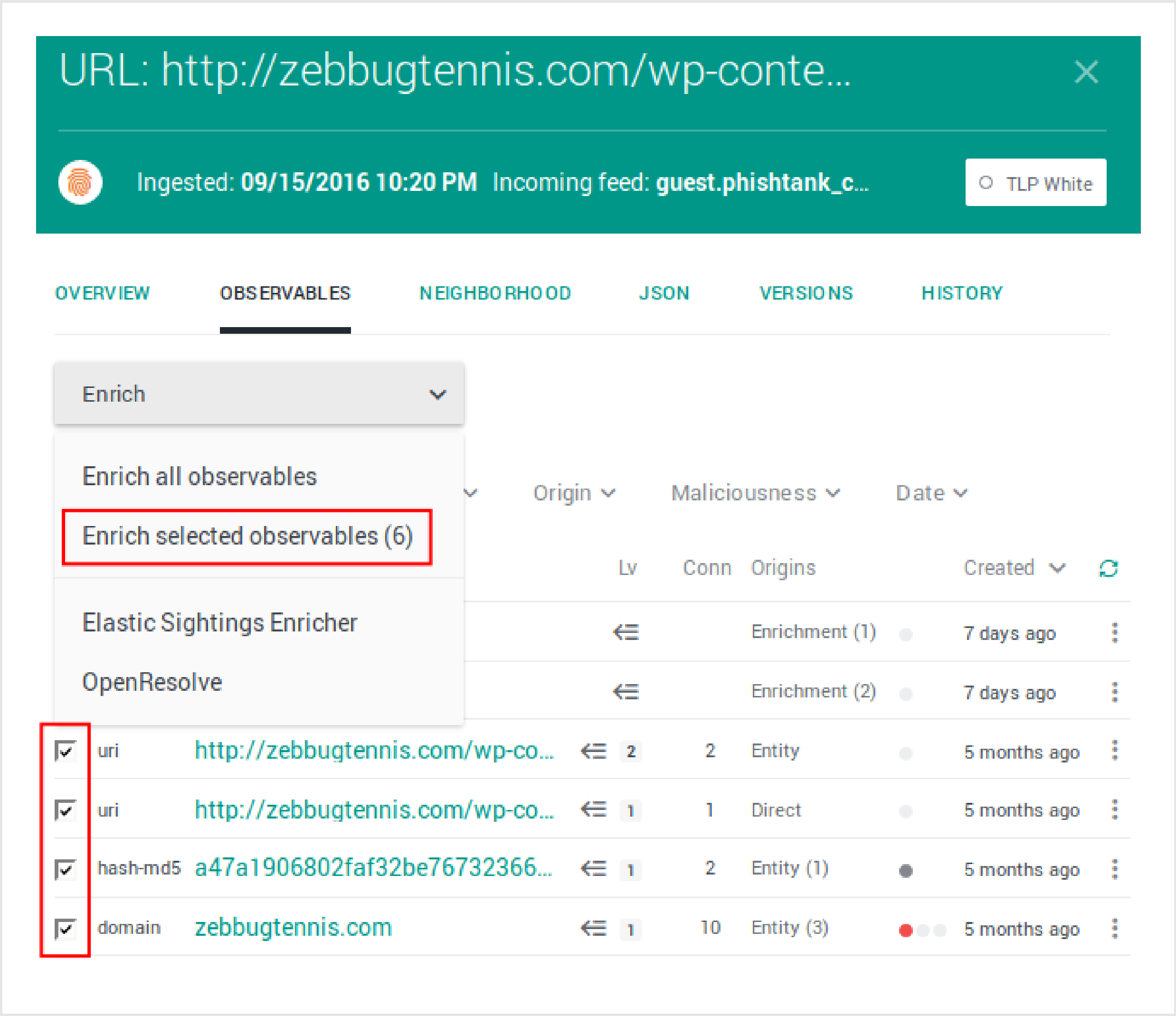
Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

TLP None

To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



URL: http://zebbugtennis.com/wp-conte...

Ingested: **09/15/2016 10:20 PM** Incoming feed: **guest.phishtank_c...**

			Lv	Conn	Origins		Created
			⇇		Enrichment (1)	●	7 days ago
			⇇		Enrichment (2)	●	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 2	2	Entity	●	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 1	1	Direct	●	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	⇇ 1	2	Entity (1)	●	5 months ago
☑	domain	zebbugtennis.com	⇇ 1	10	Entity (3)	● ● ●	5 months ago

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 Farsight DNSDB enricher can take the following observable types as input:

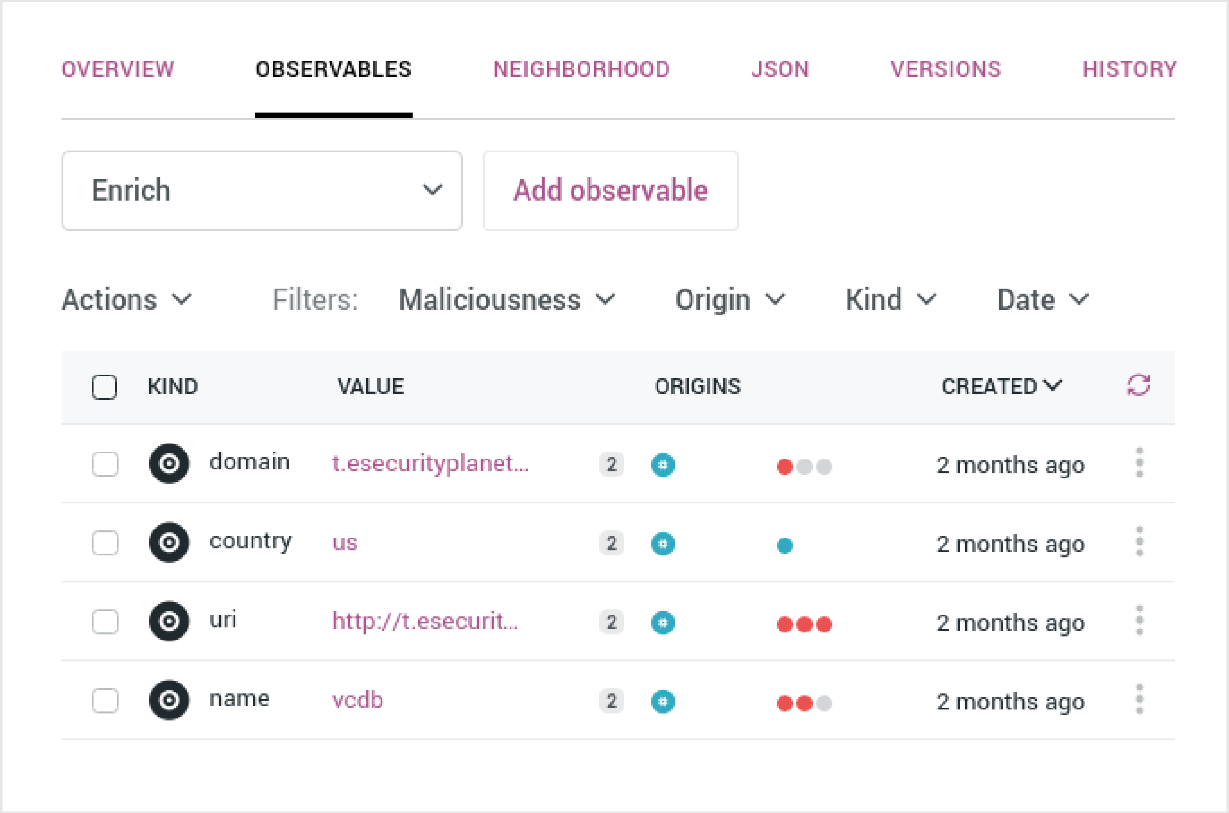
- *domain, host, ipv4, ipv6*

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 Farsight DNSDB.

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.

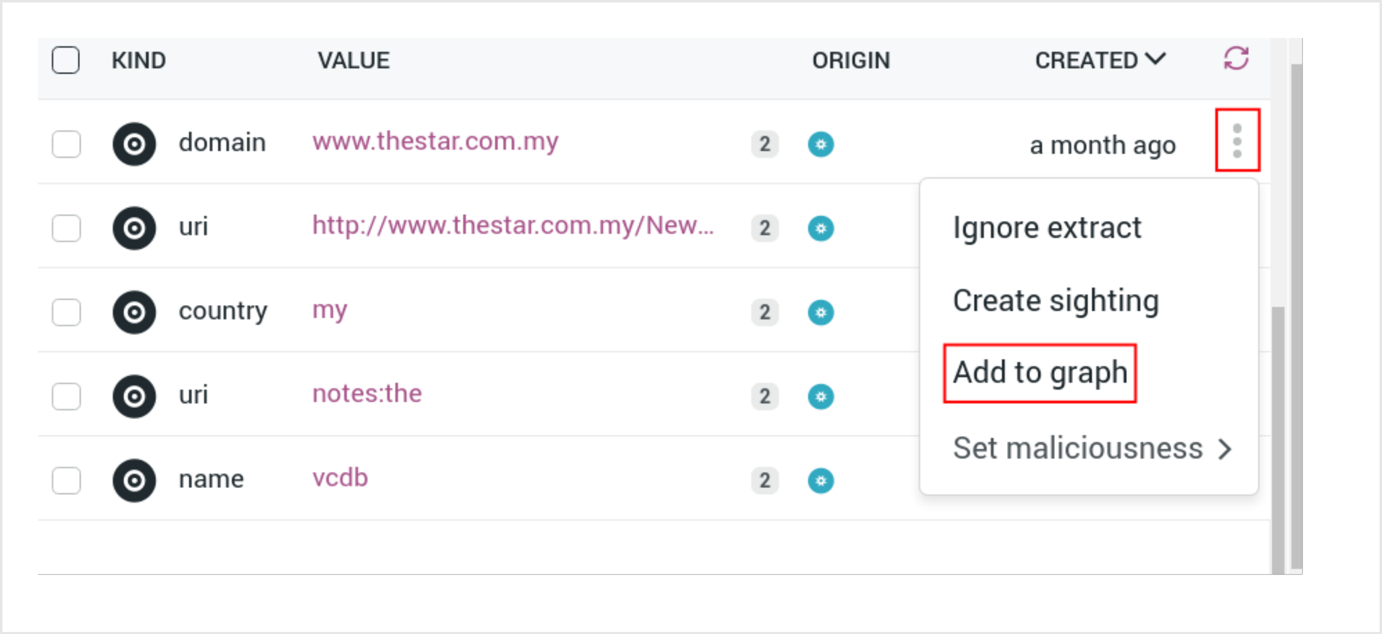


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

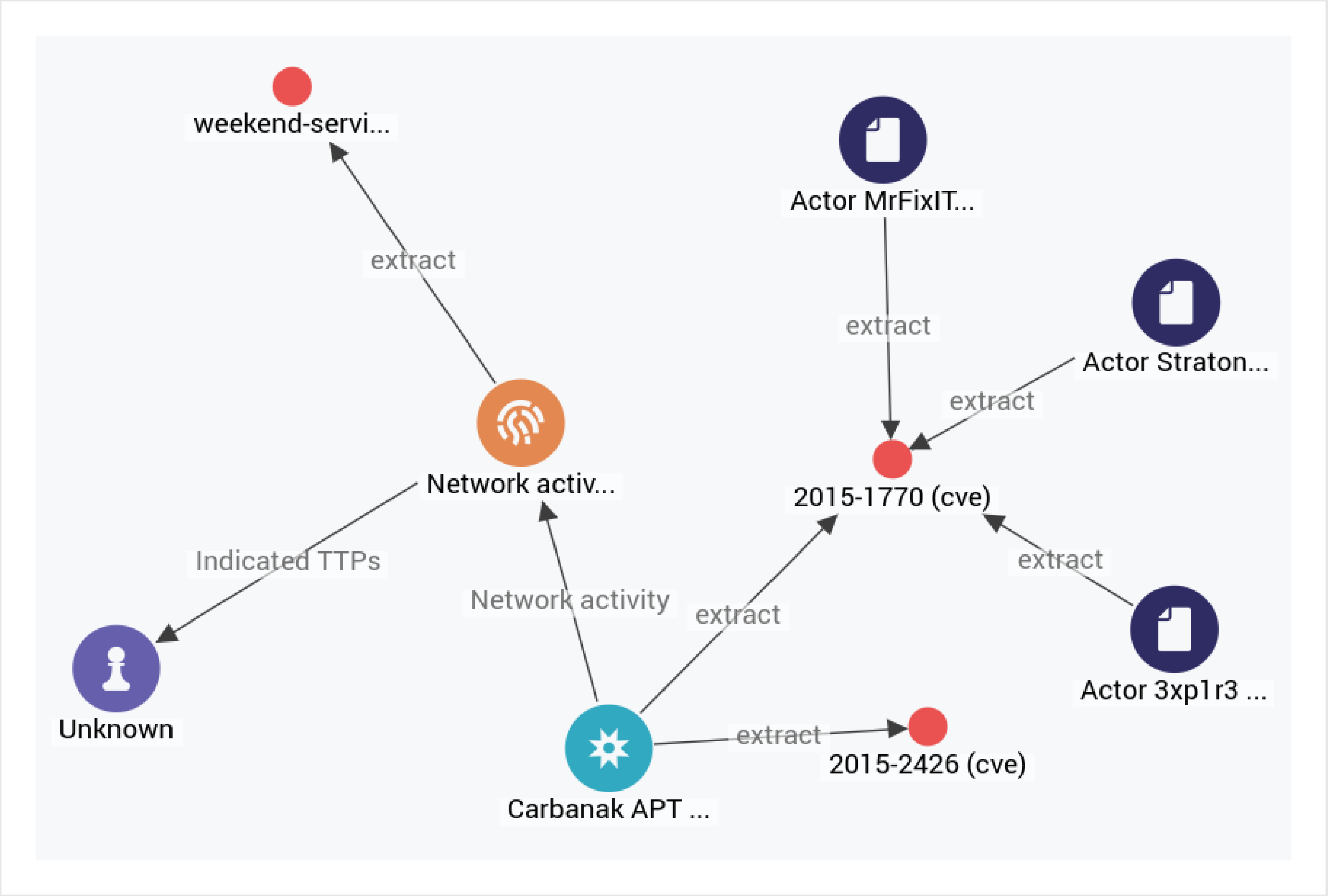
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

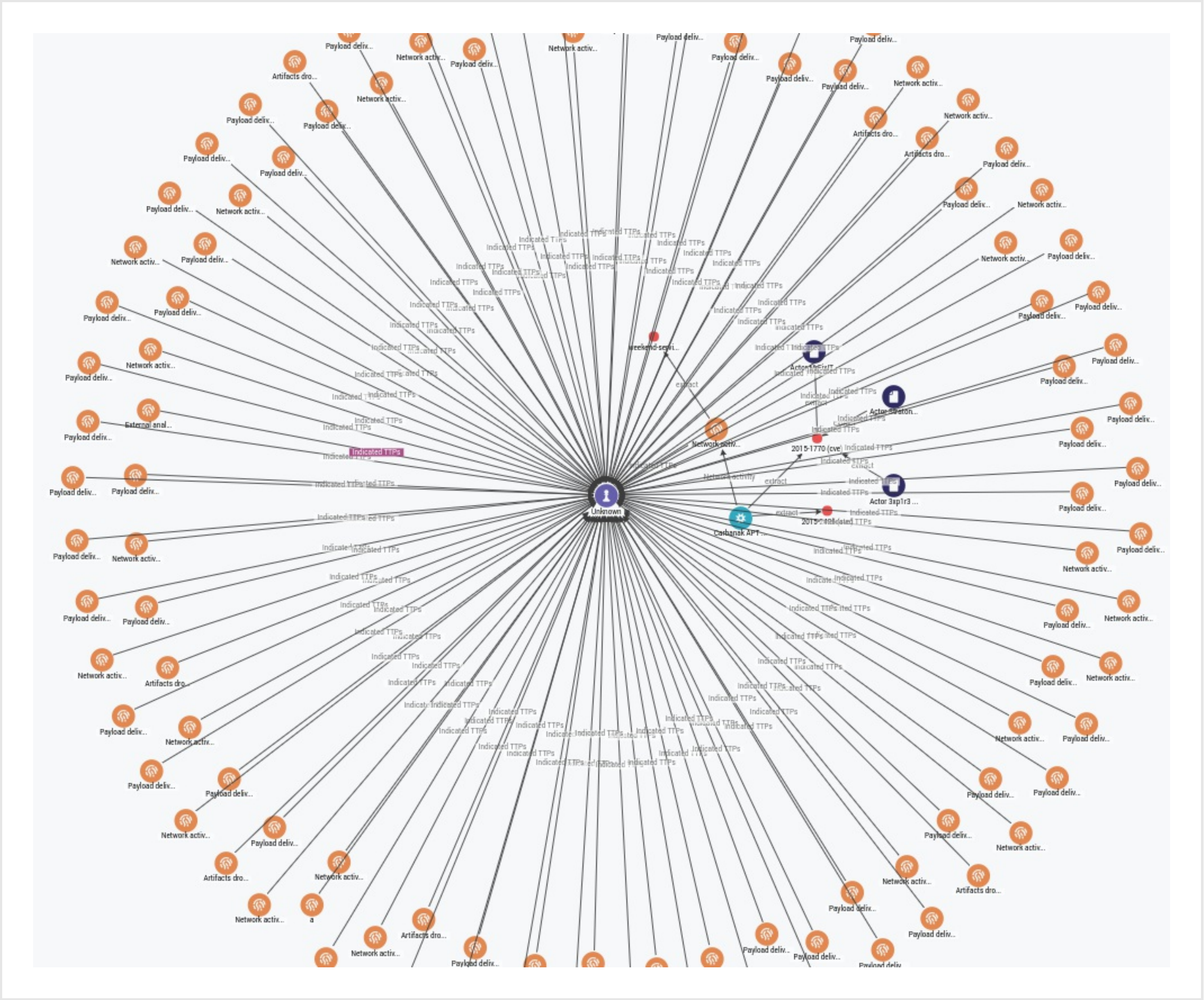


☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

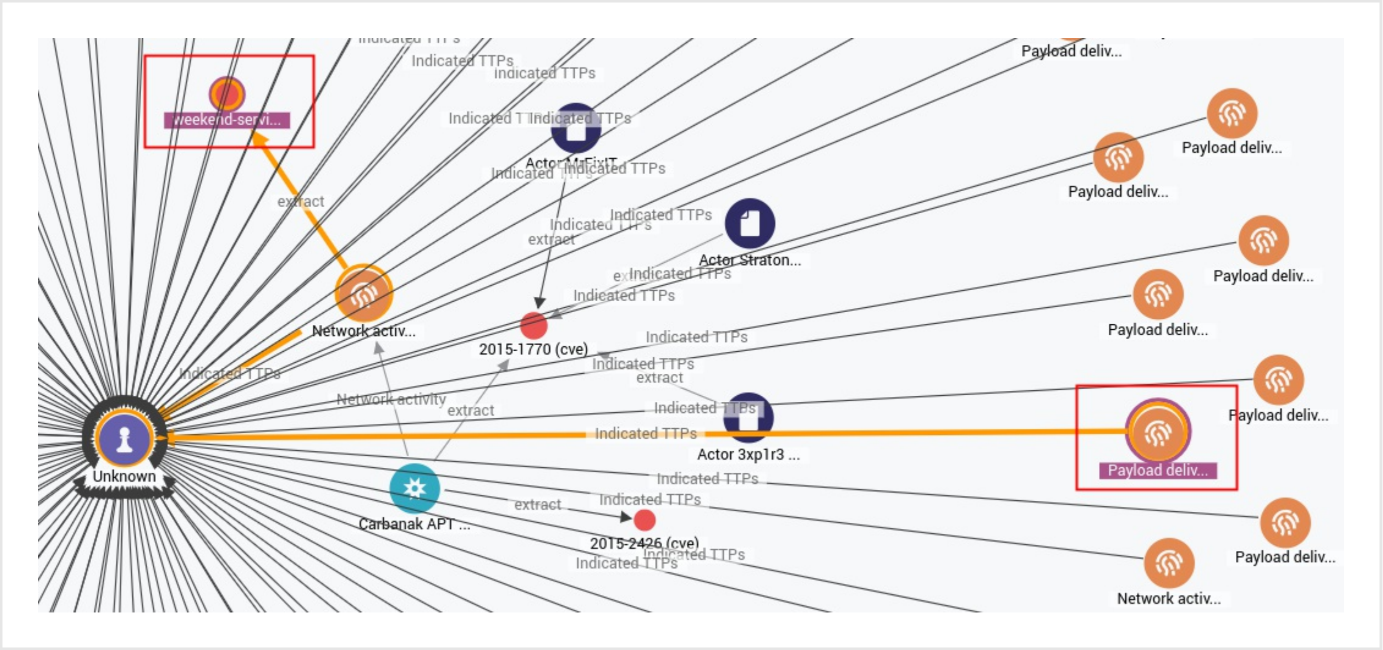


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



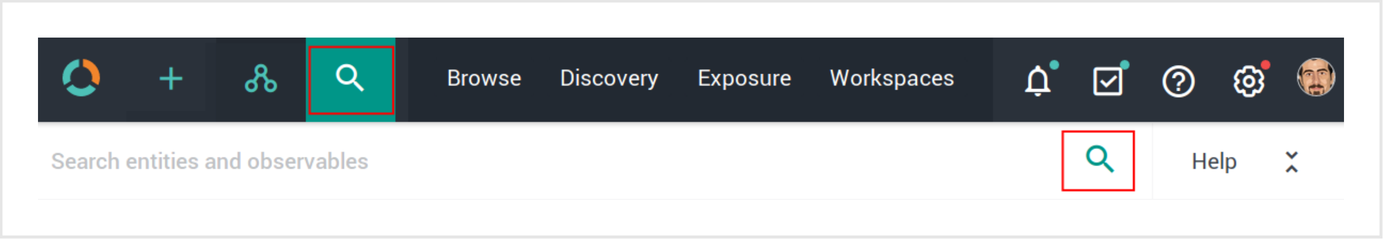
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

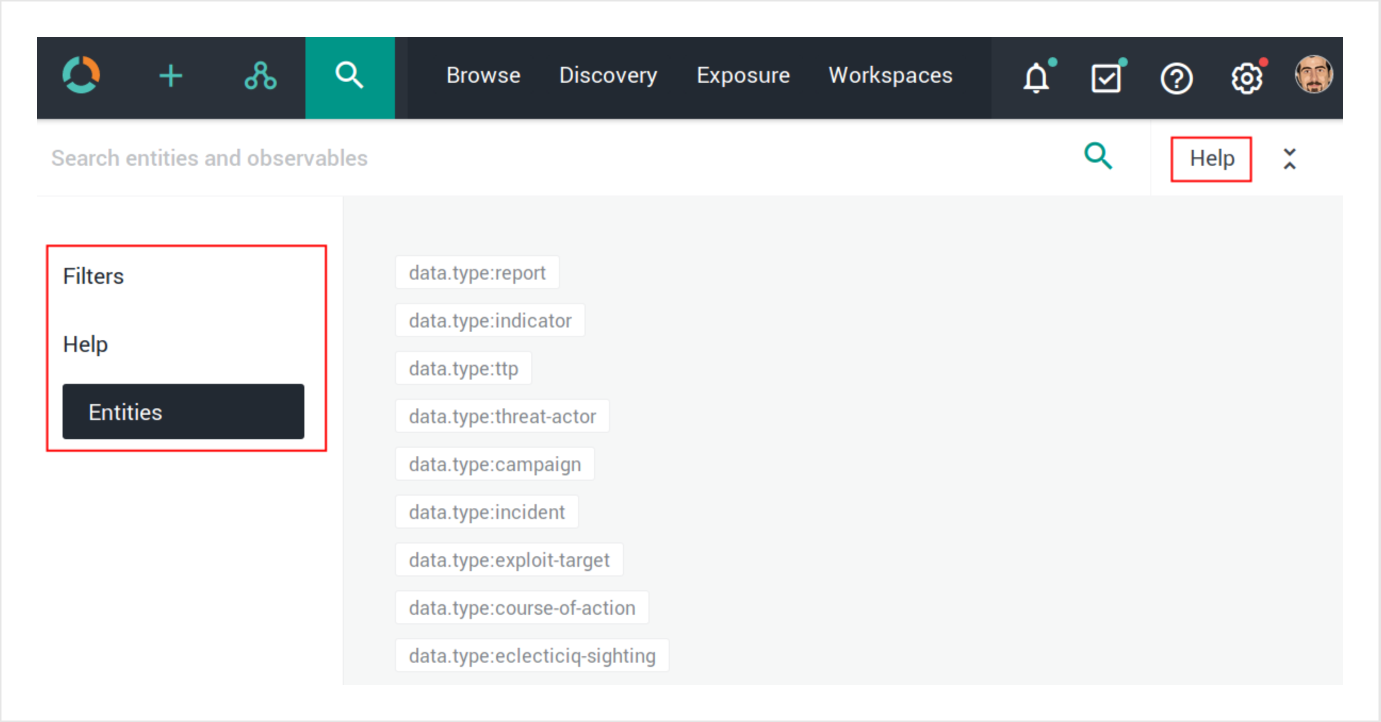


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

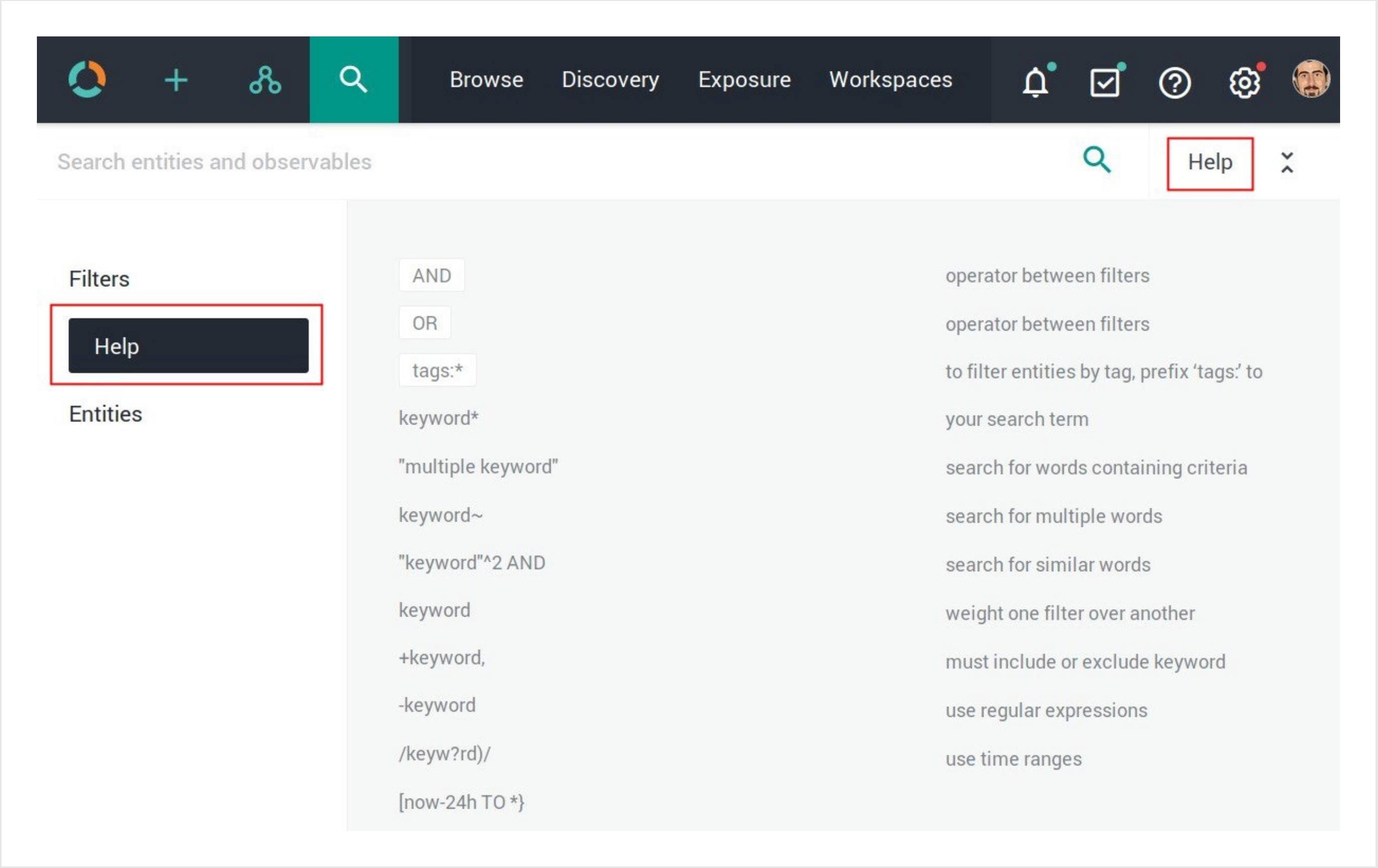
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

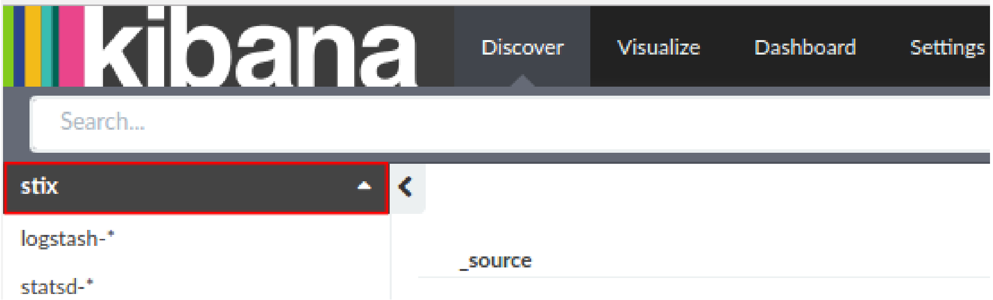
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

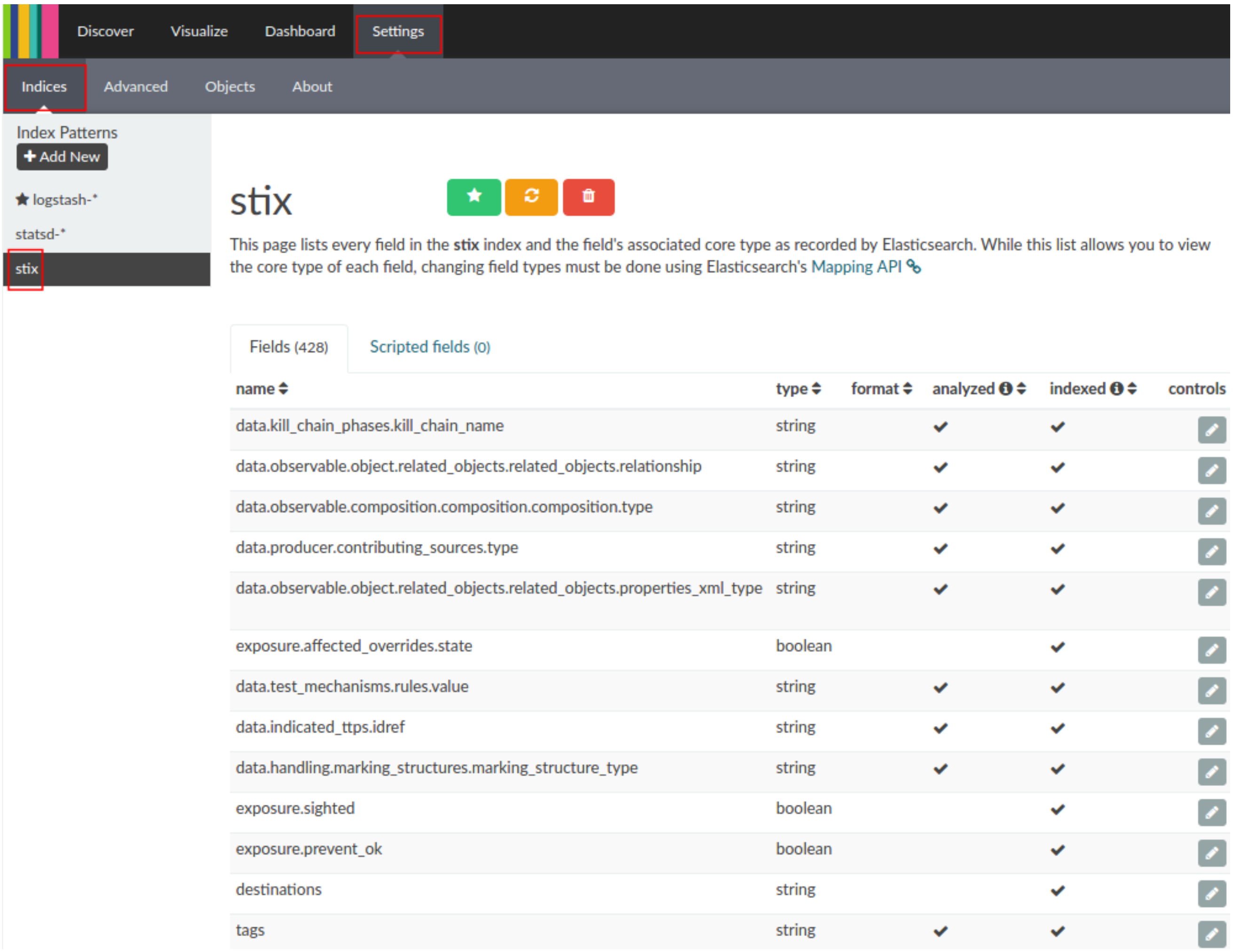
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/kibana/app/kibana#/`
- Select the **stix** index field:



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



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		✓	✓	✎

How to work with the Flashpoint AggregINT enricher

Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Flashpoint AggregINT enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the Flashpoint AggregINT enricher

This article describes how to configure the Flashpoint AggregINT enricher parameters.
To configure the general options for the Flashpoint AggregINT enricher, see Configure enrichers.

Flashpoint AggregINT	**enricher**
Enricher name	Flashpoint AggregINT
API endpoint	`https://endlesstunnel.info/v3`
Input	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Output	Enriches the supported observable types with information such as IP addresses, domains, host names, and hash files.
Description	Polls data from the Flashpoint API. It provides information on malware, hosts, domains, IP addresses, and hashed files. The enricher can search thematic datasets focusing on hackers, terrorist and white supremacist groups, communities in conflict, state actors involved in cyberwarfare, and **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats. It produces enrichment observables like forum name, forum room name, user name of the author of a post (as actor-id), post content, thread title, UTC date and time of a post in **ISO 8601** `(https://en.wikipedia.org/wiki/iso_8601)` **(RFC 3339)** `(https://tools.ietf.org/html/rfc3339)` format.

Configure the Flashpoint AggregINT enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.

- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the Flashpoint AggregINT enricher:

- **API URL**: the URL pointing to the API endpoint exposing the service that grants access to the enricher data source. Contact the intelligence provider to subscribe to the service and to obtain this information, as well as any required authentication and authorization credentials.
- **Username**: enter the user name associated to the Flashpoint AggregINT account to access and consume the Flashpoint AggregINT service.
- **Password**: enter the password associated to the Flashpoint AggregINT account to access and consume the Flashpoint AggregINT service.
- **Hacker dataset**: select this checkbox to search data on hacker groups and activities.
- **Terrorist dataset**: select this checkbox to search data on terrorist groups and activities.
- **White supermacist dataset**: select this checkbox to search data on white supremacist groups and activities.
- **CBRN dataset**: select this checkbox to search data on **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats.
- **State actor dataset**: select this checkbox to search data on state actors, that is, individuals who act on behalf of a governmental body, and their activities.
- **Communities in conflict dataset**: select this checkbox to search data on groups and communities currently in conflict with each other.
- 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 **+ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **✚ Add** or **✚ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data. **TLP** `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.

- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

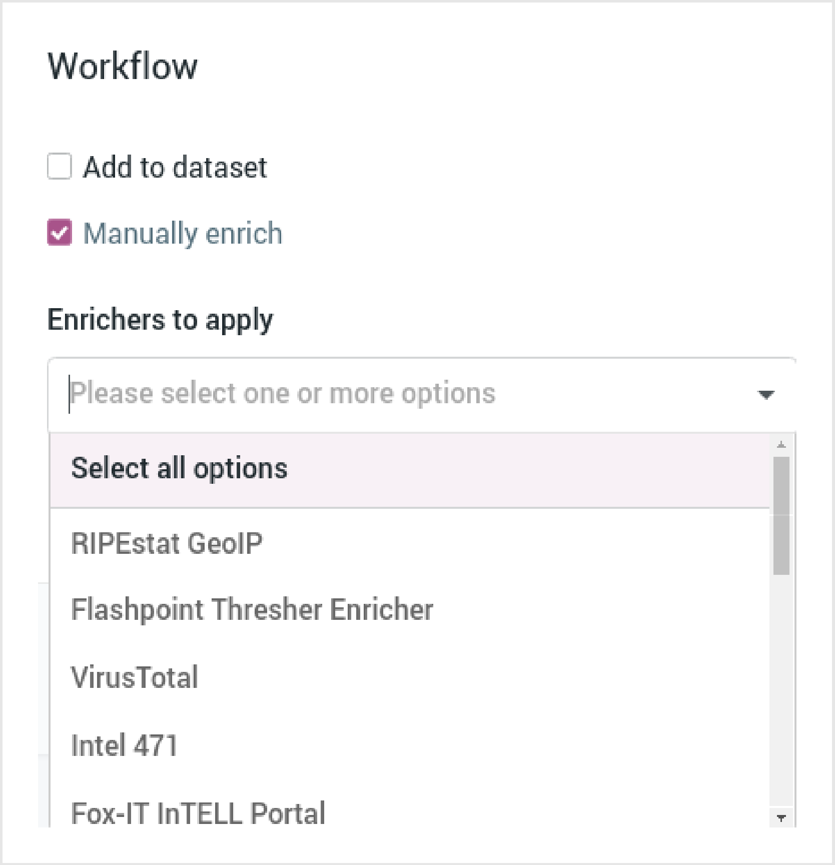
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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

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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

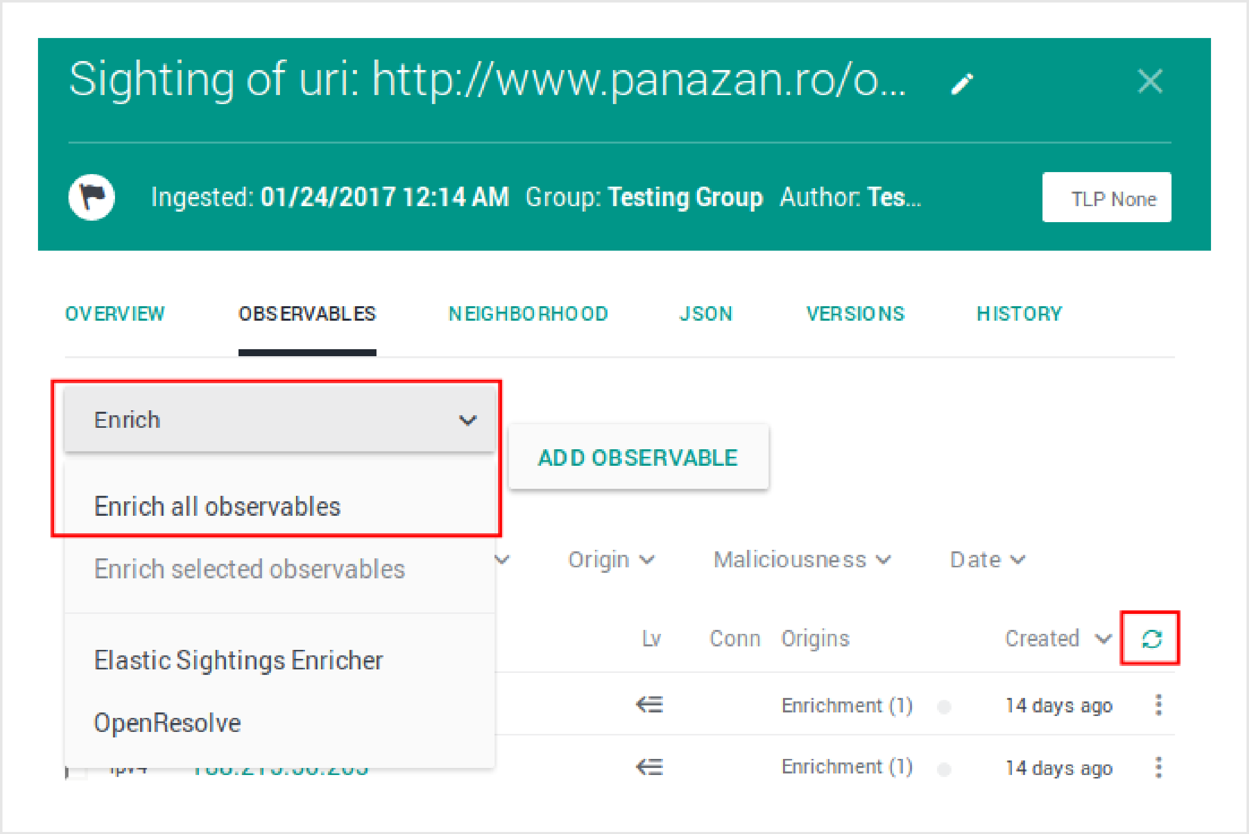
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the 🔄 refresh icon to trigger a task run that polls all the enrichers configured for the entity.

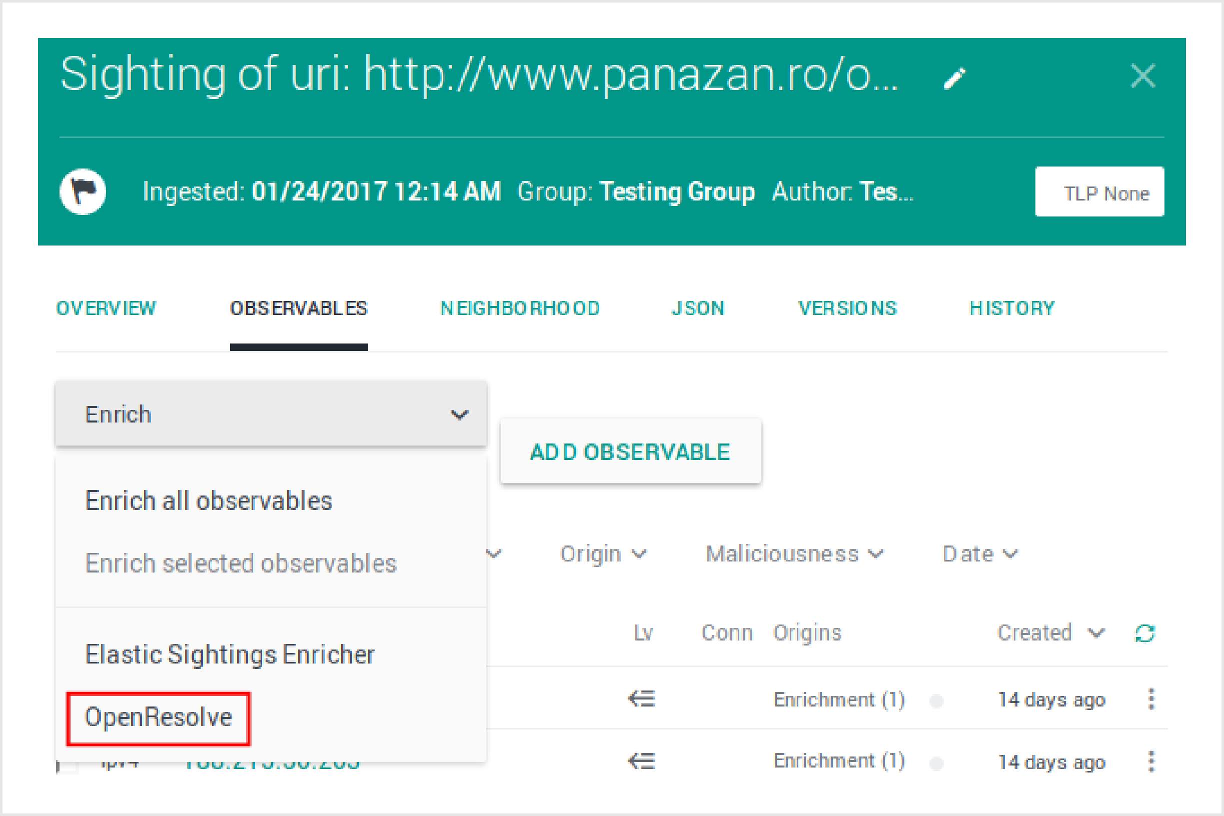
Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



To poll a specific enricher:

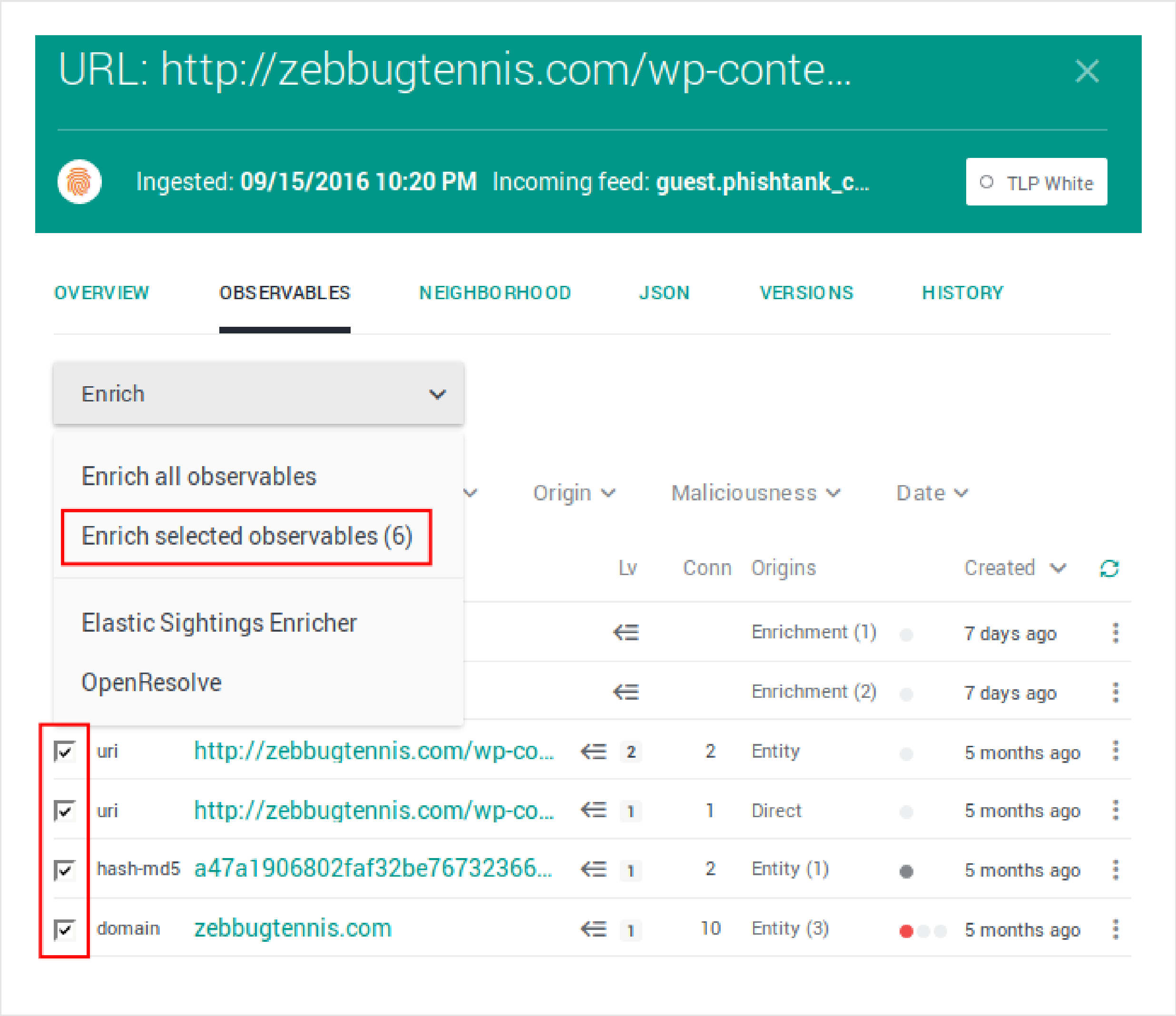
- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.


URL: http://zebbugtennis.com/wp-conte...
Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
TLP White
OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY
Enrich
Enrich all observables
Enrich selected observables (6)
Elastic Sightings Enricher
OpenResolve
Origin
Maliciousness
Date
Lv
Conn
Origins
Created
Enrichment (1) 7 days ago
Enrichment (2) 7 days ago
uri http://zebbugtennis.com/wp-co... 2 2 Entity 5 months ago
uri http://zebbugtennis.com/wp-co... 1 1 Direct 5 months ago
hash-md5 a47a1906802faf32be76732366... 1 2 Entity (1) 5 months ago
domain zebbugtennis.com 1 10 Entity (3) 5 months ago

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 Flashpoint AggregINT enricher can take the following observable types as input:

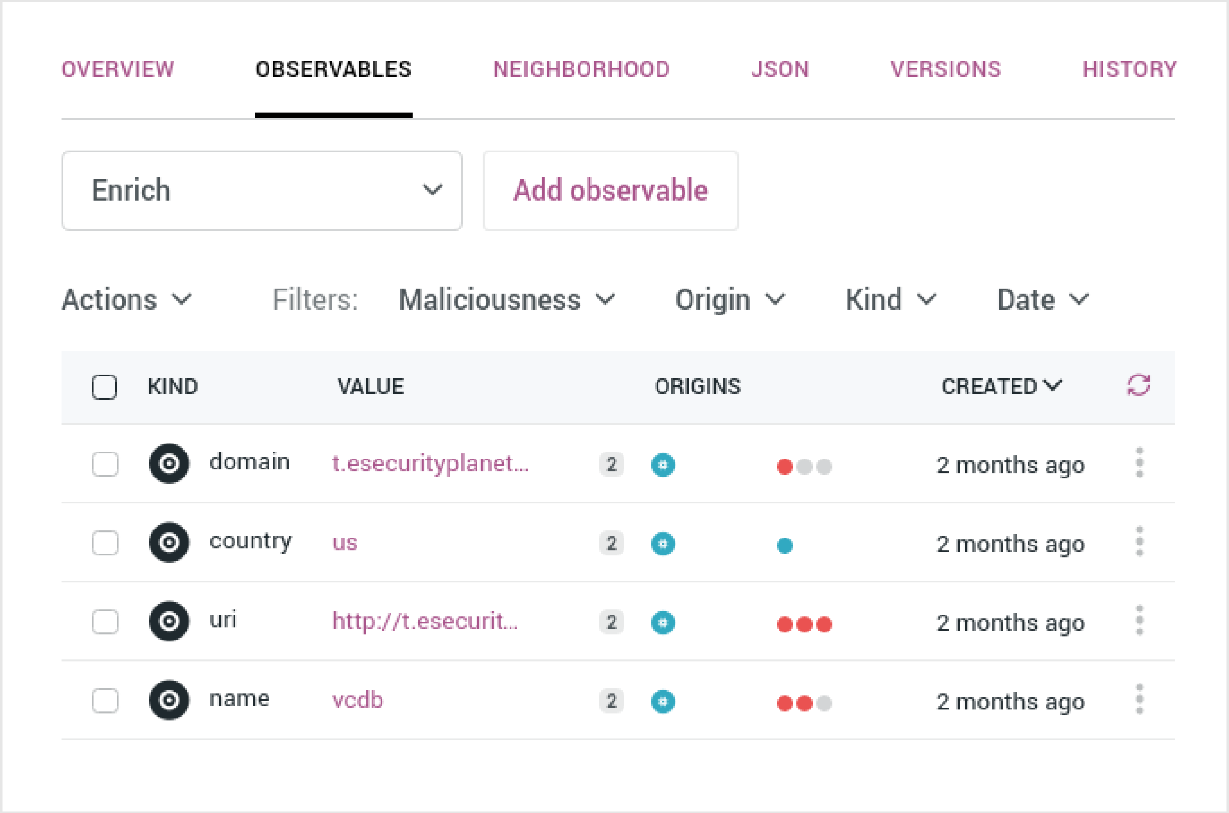
- *ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512*

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 Flashpoint AggregINT.

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.

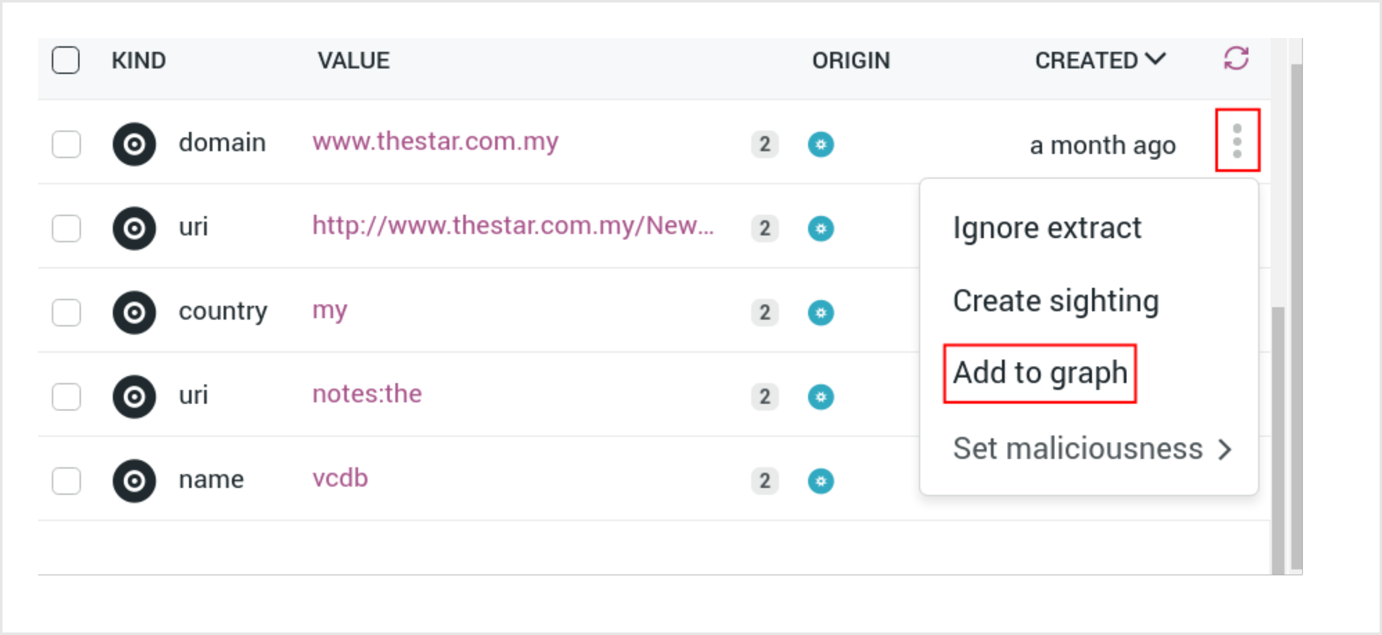


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

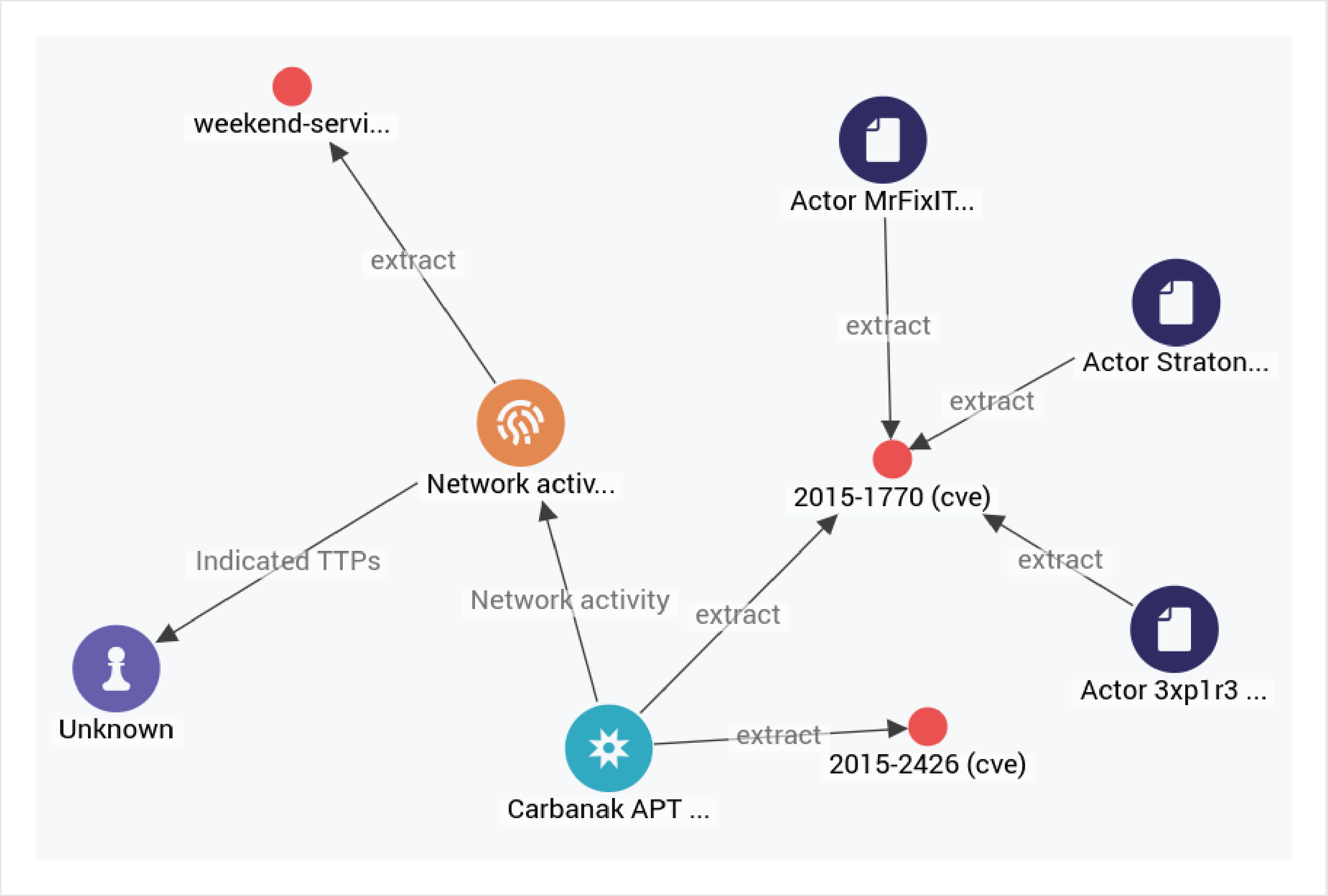
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

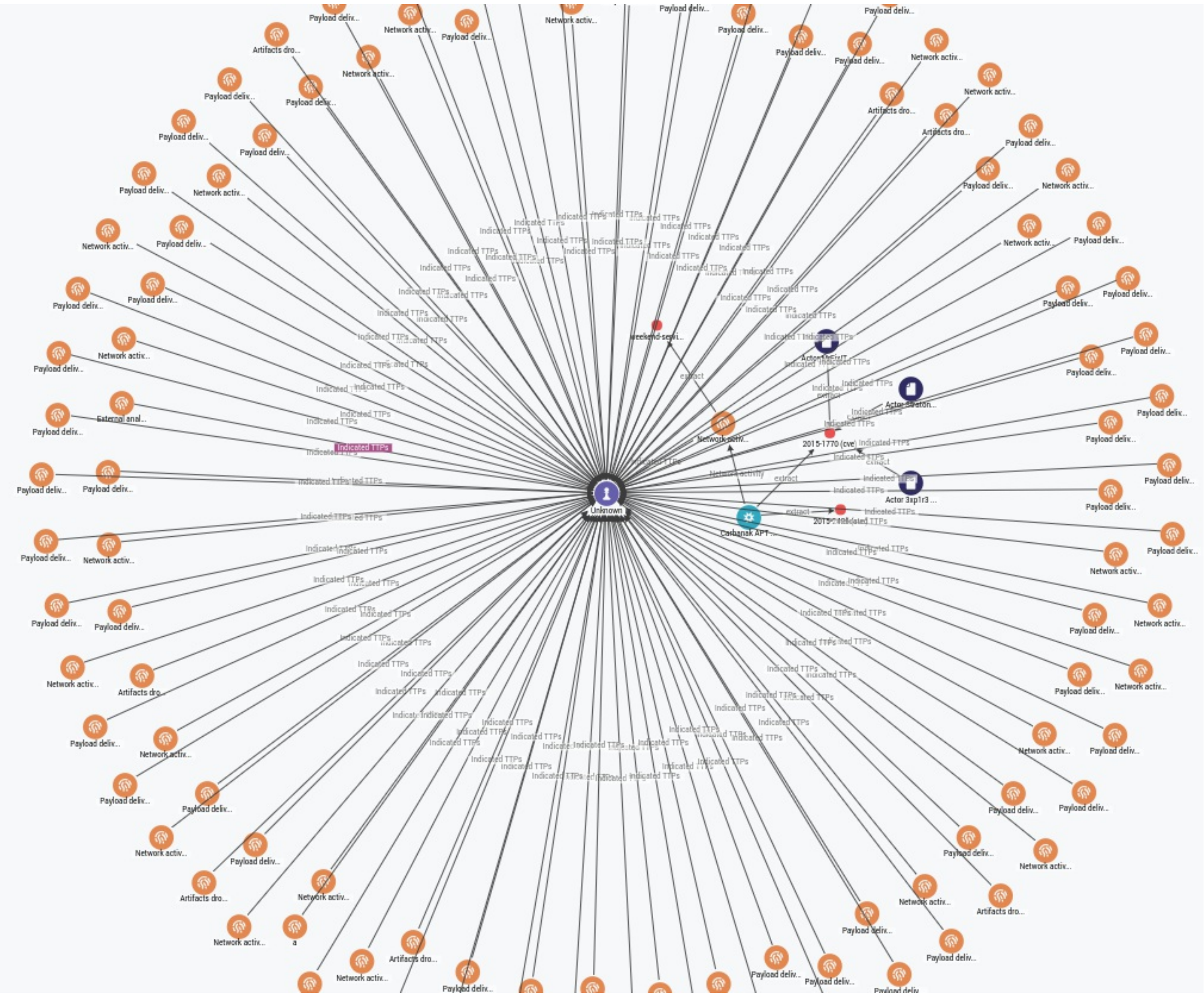


☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

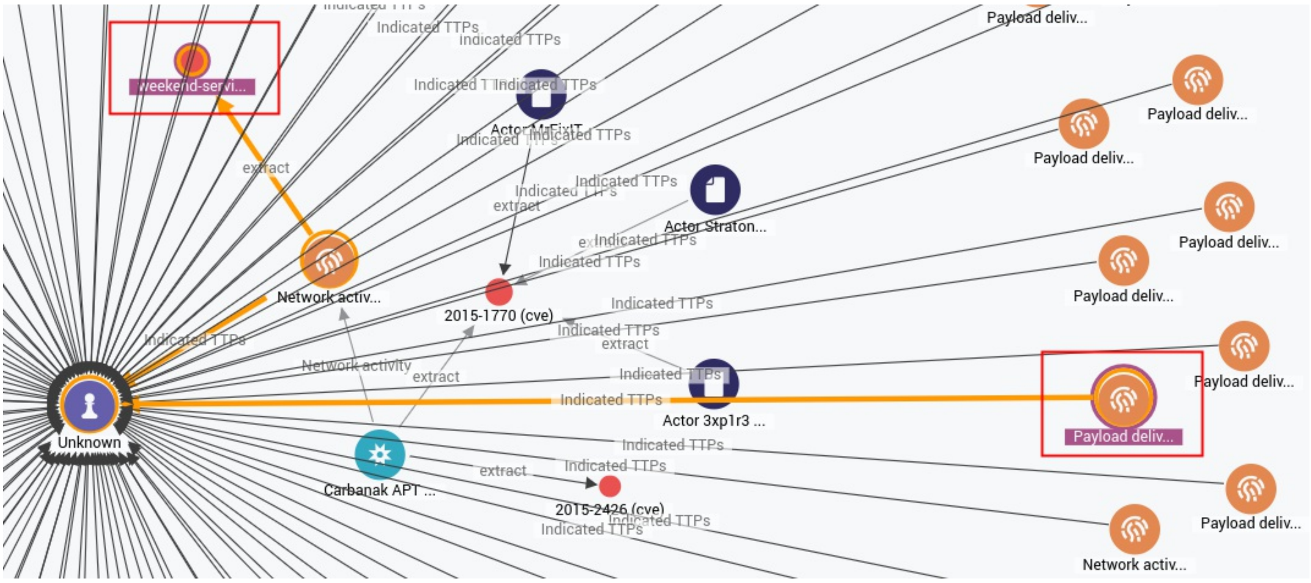


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



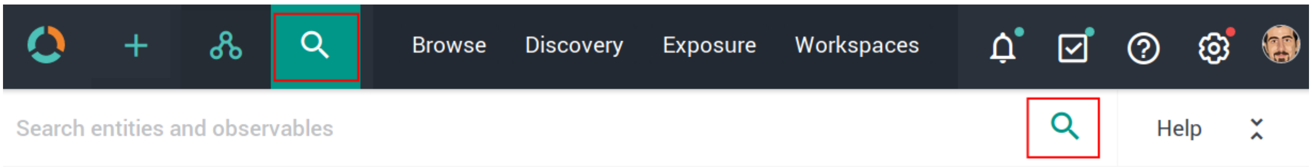
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

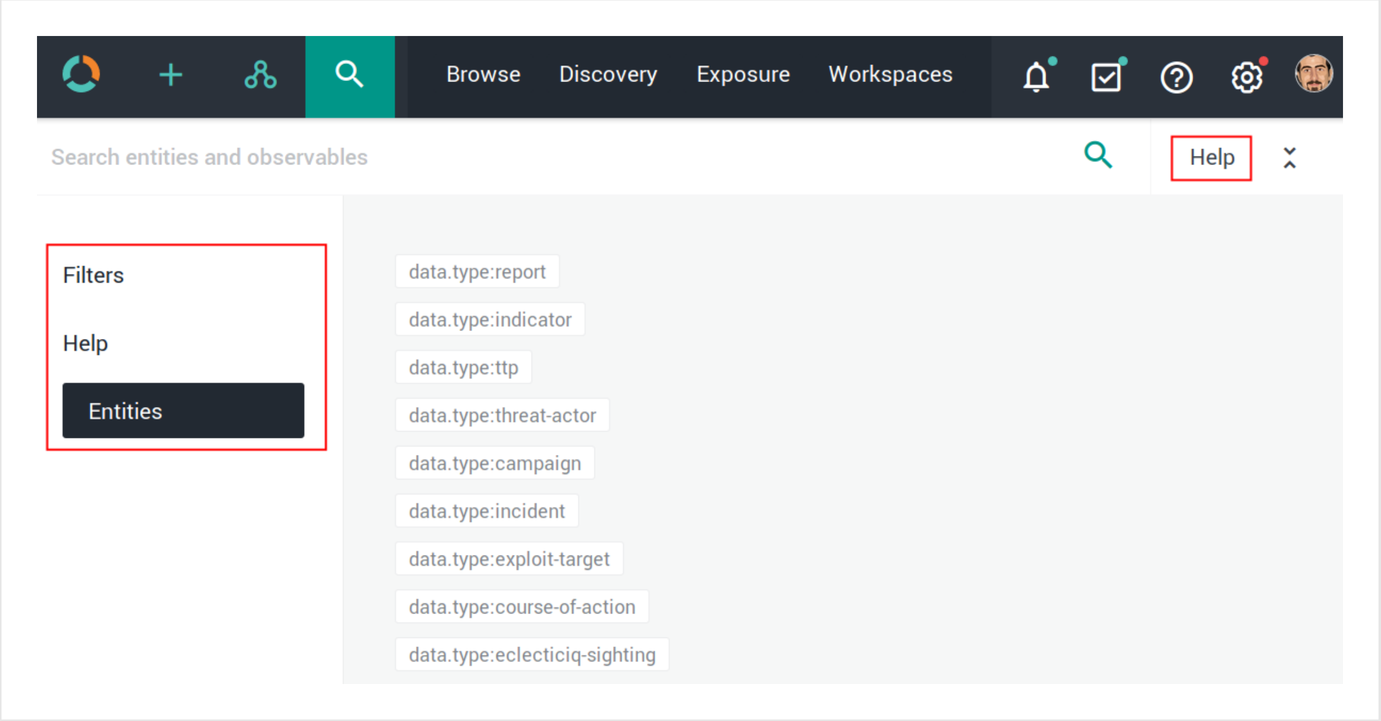


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

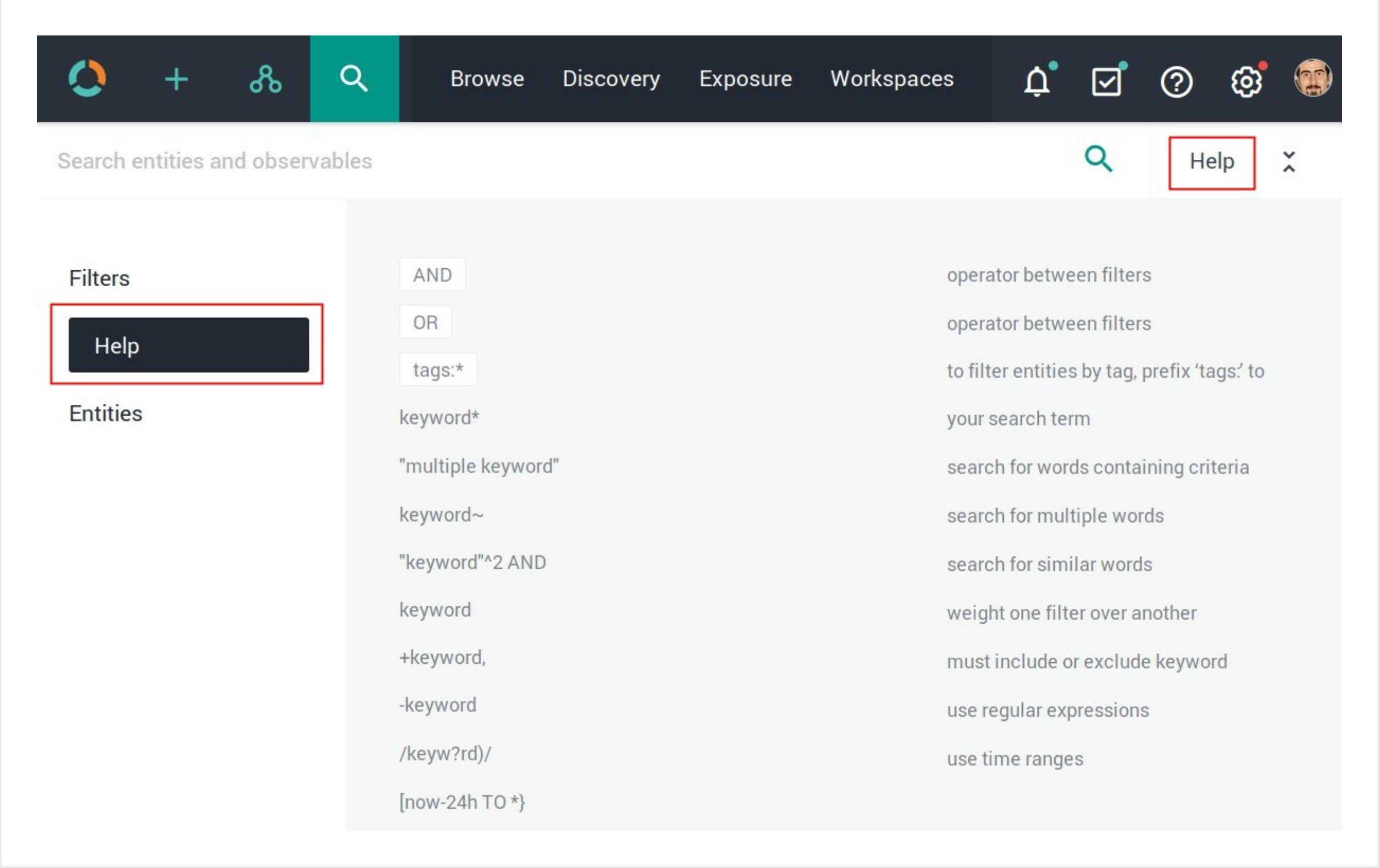
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

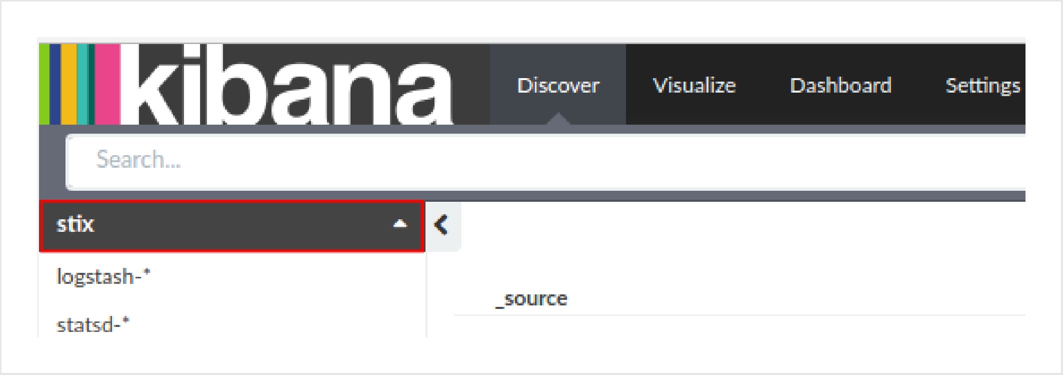
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

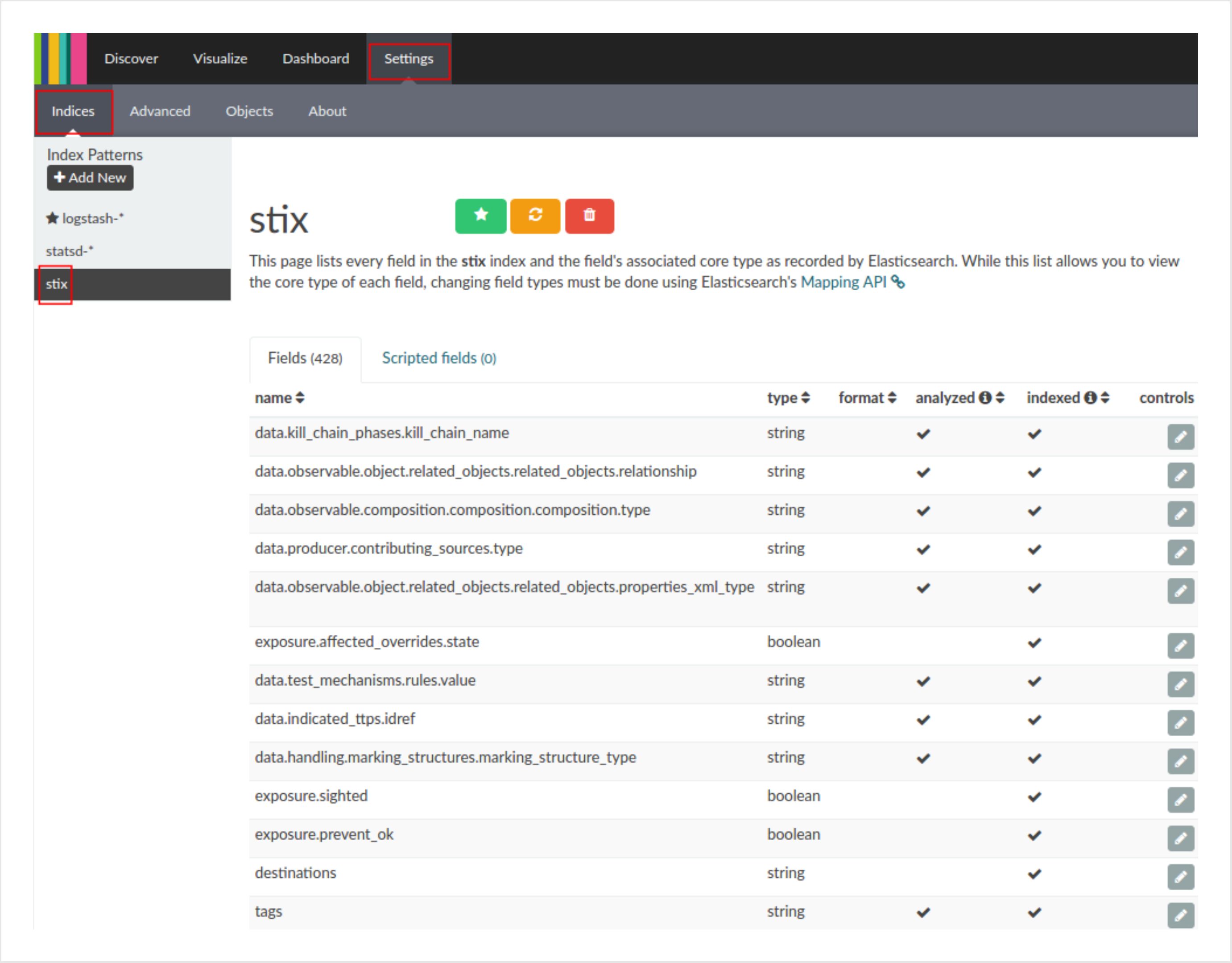
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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		✓	✓	✎

How to work with the Flashpoint Blueprint enricher

Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Flashpoint Blueprint enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the Flashpoint Blueprint enricher

This article describes how to configure the Flashpoint Blueprint enricher parameters.
To configure the general options for the Flashpoint Blueprint enricher, see Configure enrichers.

Flashpoint Blueprint	**enricher**
Enricher name	Flashpoint Blueprint
API endpoint	`https://endlesstunnel.info/v3`
Input	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Output	Enriches the supported observable types with information such as IP addresses, domains, host names, and URLs.
Description	Polls data from the Flashpoint API. It provides information based on geolocation and IP ranges, as well as on country scope. The enricher can search thematic datasets focusing on hackers, terrorist and white supremacist groups, state actors involved in cyberwarfare, and **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats. It produces enrichment observables like city/country name or IP address hit, latitude/longitude or IP address hit, forum name and thread title related to a hit, user name uniquely matched to an IP address hit.

Configure the Flashpoint Blueprint enricher

The Flashpoint Blueprint enricher is very similar to the Flashpoint AggregINT enricher.
The main configuration difference is that the available Flashpoint datasets vary among the Flashpoint enrichers.
To configure the Flashpoint Blueprint enricher, see Configure the Flashpoint AggregINT enricher, since both enrichers use the same configuration options.

How to work with the Flashpoint Thresher enricher

Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Flashpoint Thresher enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the Flashpoint Thresher enricher

This article describes how to configure the Flashpoint Thresher enricher parameters.
To configure the general options for the Flashpoint Thresher enricher, see Configure enrichers.

Flashpoint Thresher	**enricher**
Enricher name	Flashpoint Thresher
API endpoint	`https://endlesstunnel.info/v3`
Input	ipv4, domain, host, uri, hash-sha1, file
Output	Enriches the supported observable types with information such as IP addresses, domains, URLs, hashes, and files.
Description	Polls data from the Flashpoint API. The enricher can search thematic datasets focusing on hackers, terrorist and white supremacist groups, and **CBRN** `(https://en.wikipedia.org/wiki/cbrn_defense)` threats. It produces enrichment observables with Flashpoint torrent thresher data.

Configure the Flashpoint Thresher enricher

> ℹ The Flashpoint Thresher enricher is very similar to the Flashpoint AggregINT enricher.
> The main configuration difference is that the available Flashpoint datasets vary among the Flashpoint enrichers.
> To configure the Flashpoint Thresher enricher, see Configure the Flashpoint AggregINT enricher, since both enrichers use the same configuration options.

How to work with the DomainTools Hosted Domains enricher

The Domaintools Hosted Domains enricher returns all domain names related to the specified input IP addresses.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the DomainTools Hosted Domains enricher

This article describes how to configure the DomainTools Hosted Domains enricher parameters.
To configure the general options for the DomainTools Hosted Domains enricher, see Configure enrichers.

DomainTools Hosted Domains	enricher
Enricher name	DomainTools Hosted Domains
API endpoint	`http://api.domaintools.com/v1/{}/host-domains`
Input	ipv4
Output	Enriches the supported observable types with domain and host name information.
Description	Enriches IPv4 observables by returning all the domain names hosted on, and therefore related to, the input IP addresses.

Configure the DomainTools Hosted Domains enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the DomainTools Hosted Domains enricher:

- **API user name**: sign up and subscribe to the service to obtain the required API user name and API key credentials to access the API endpoint exposing the service.
- **API key**: contact DomainTools to receive an API key, and then enter it in the corresponding input field.
- 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 **+ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **+ Add** or **+ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.

- Click **+ Add** or **+ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.

- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

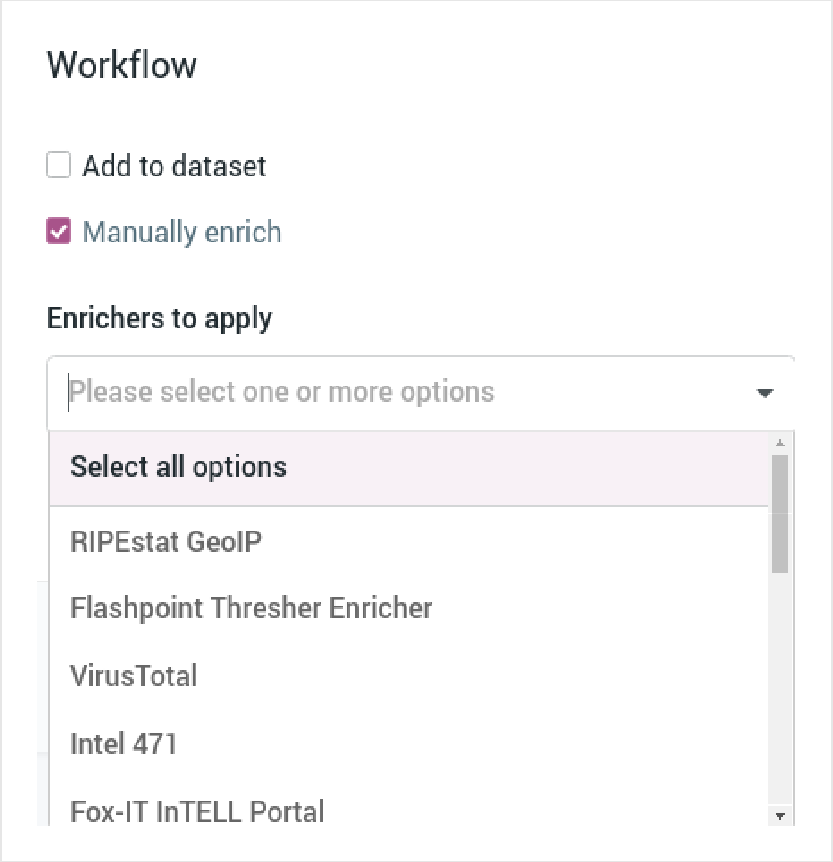
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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.

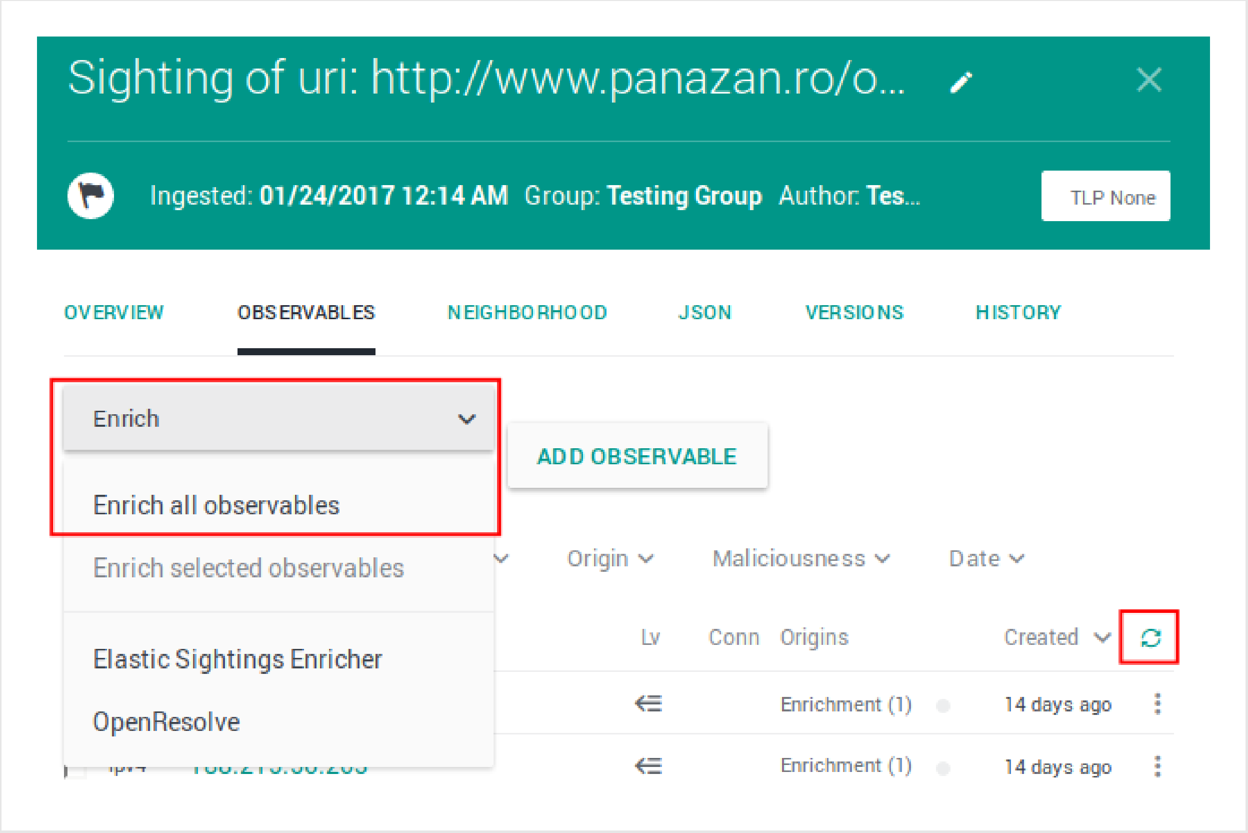
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

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 **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.

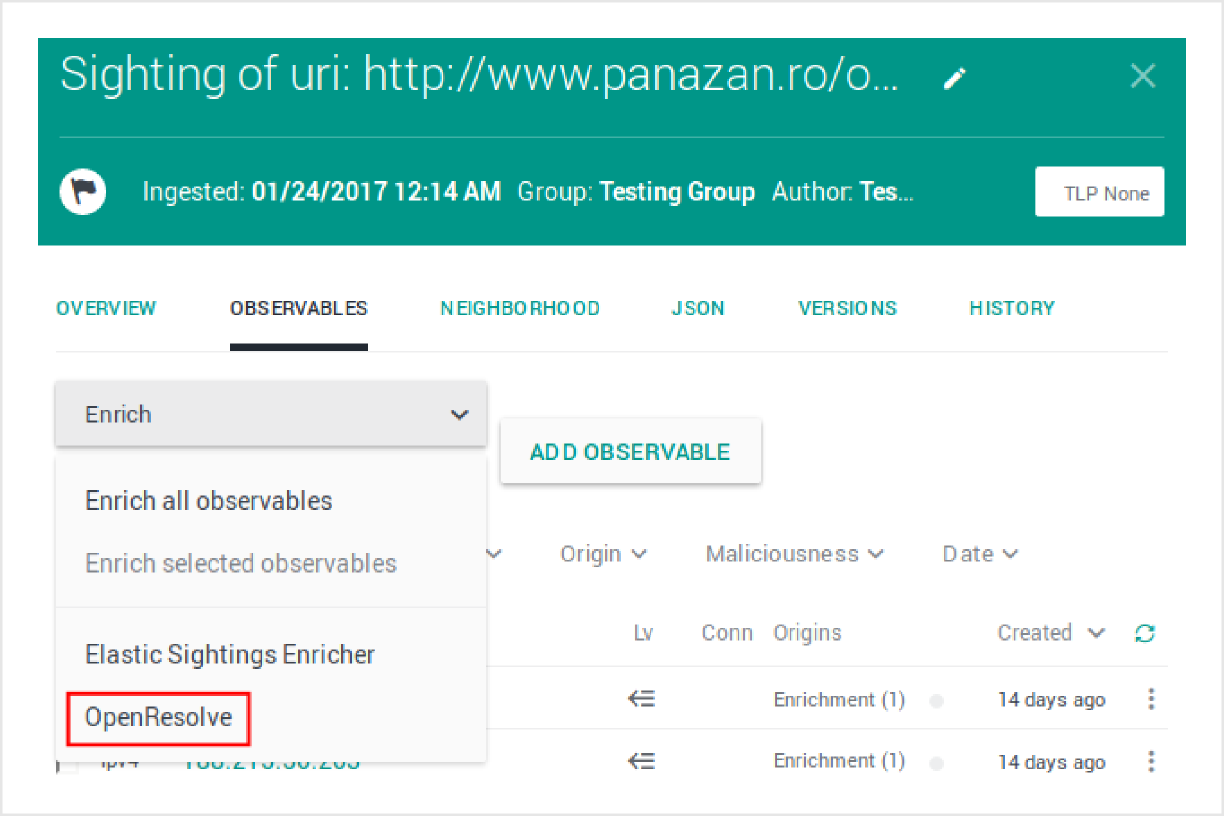


Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

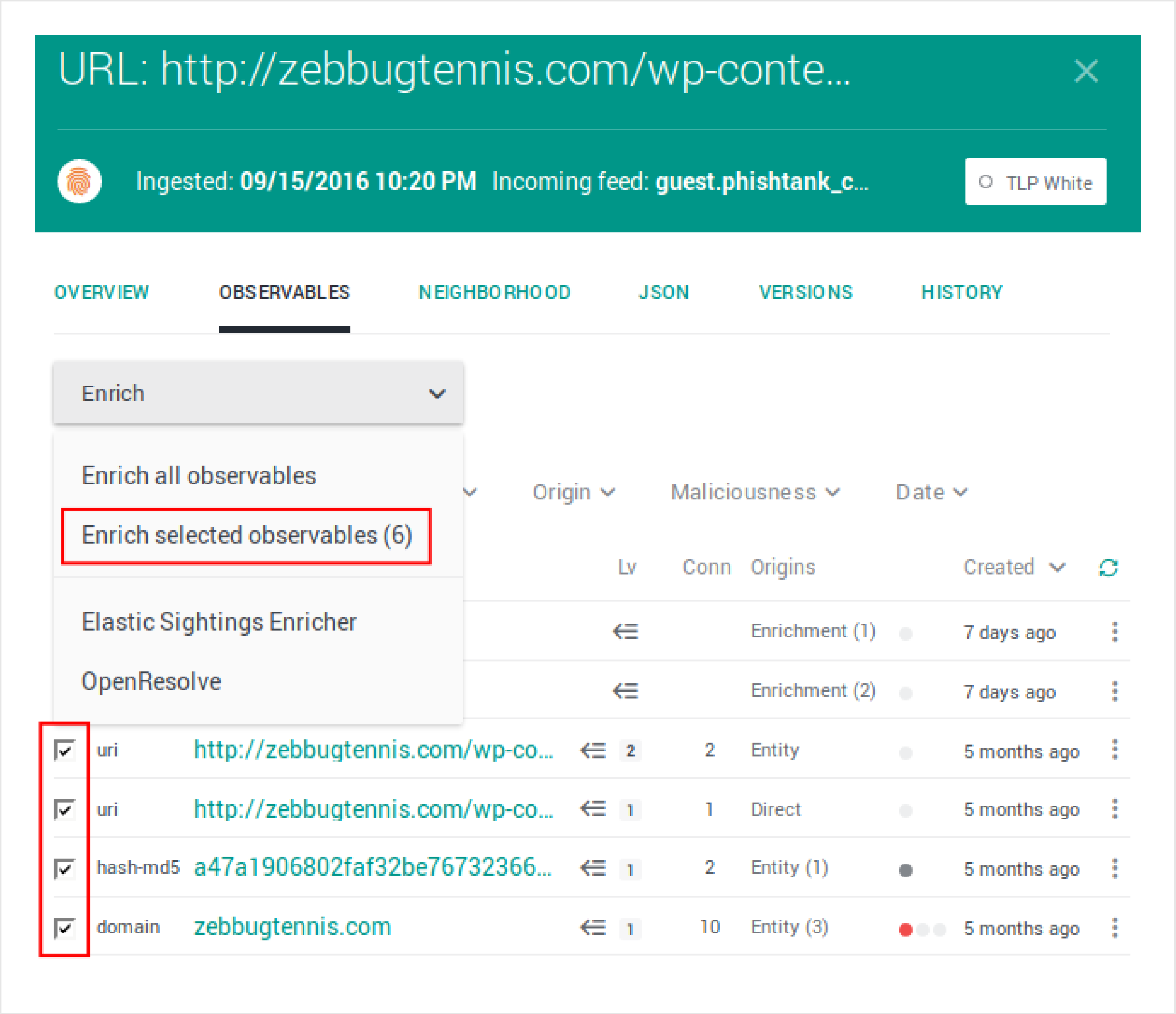
To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.
- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



URL: http://zebbugtennis.com/wp-conte...

Ingested: **09/15/2016 10:20 PM** Incoming feed: **guest.phishtank_c...**

			Lv	Conn	Origins		Created
					Enrichment (1)	●	7 days ago
					Enrichment (2)	●	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	2	2	Entity	●	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	1	1	Direct	●	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	1	2	Entity (1)	●	5 months ago
☑	domain	zebbugtennis.com	1	10	Entity (3)	●●●	5 months ago

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

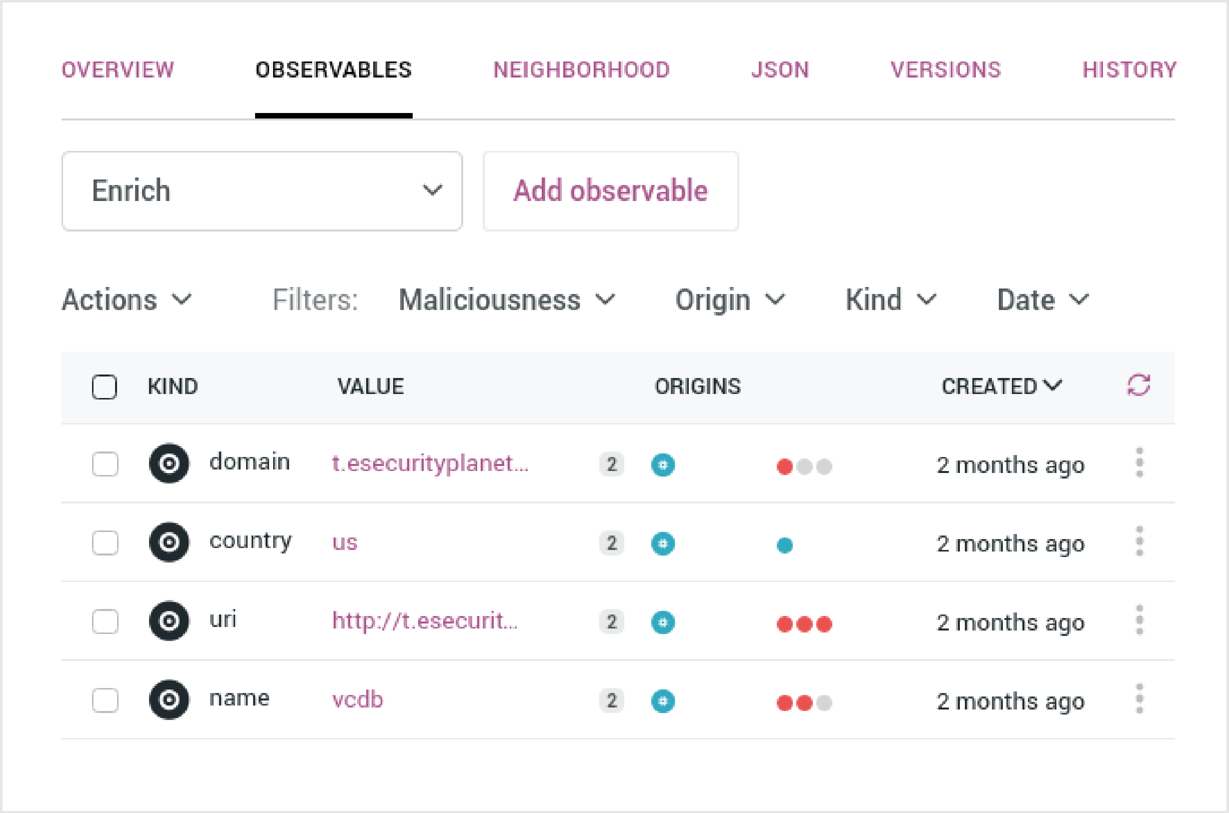
The DomainTools Hosted Domains enricher can take the following observable types as input:

- *ipv4*

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 DomainTools Hosted Domains.

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.

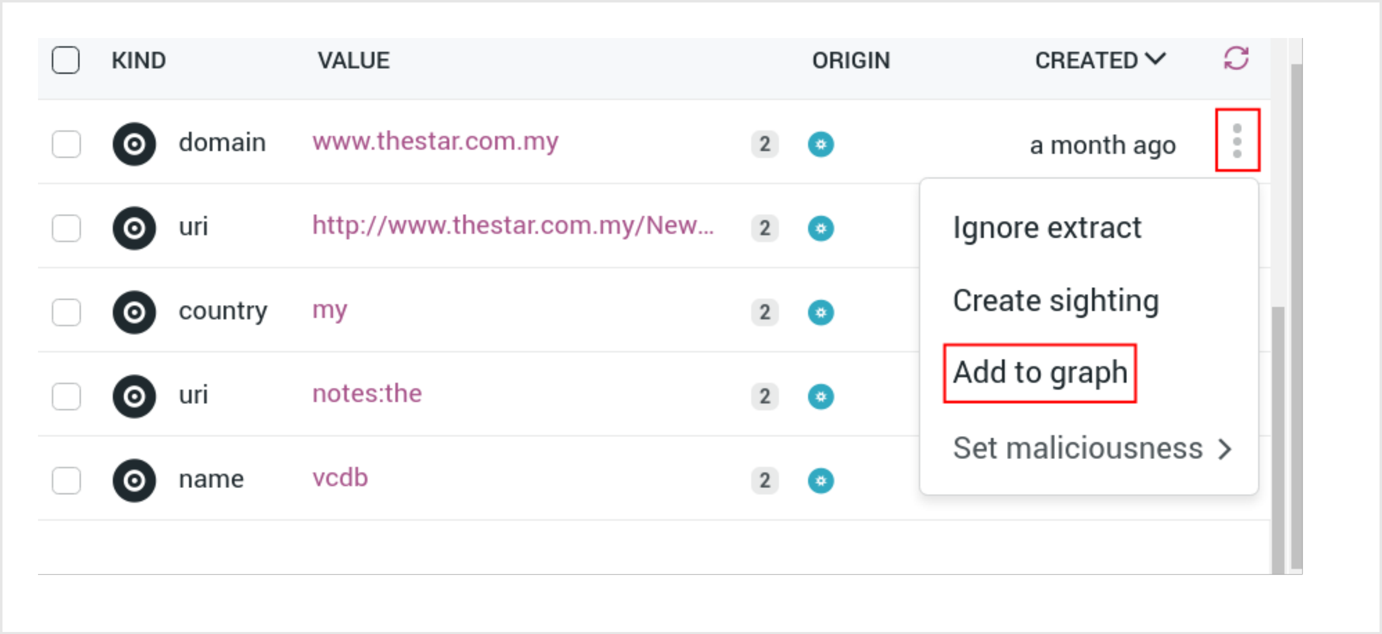


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●○○	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●○	2 months ago

Review enrichment observables on the graph

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

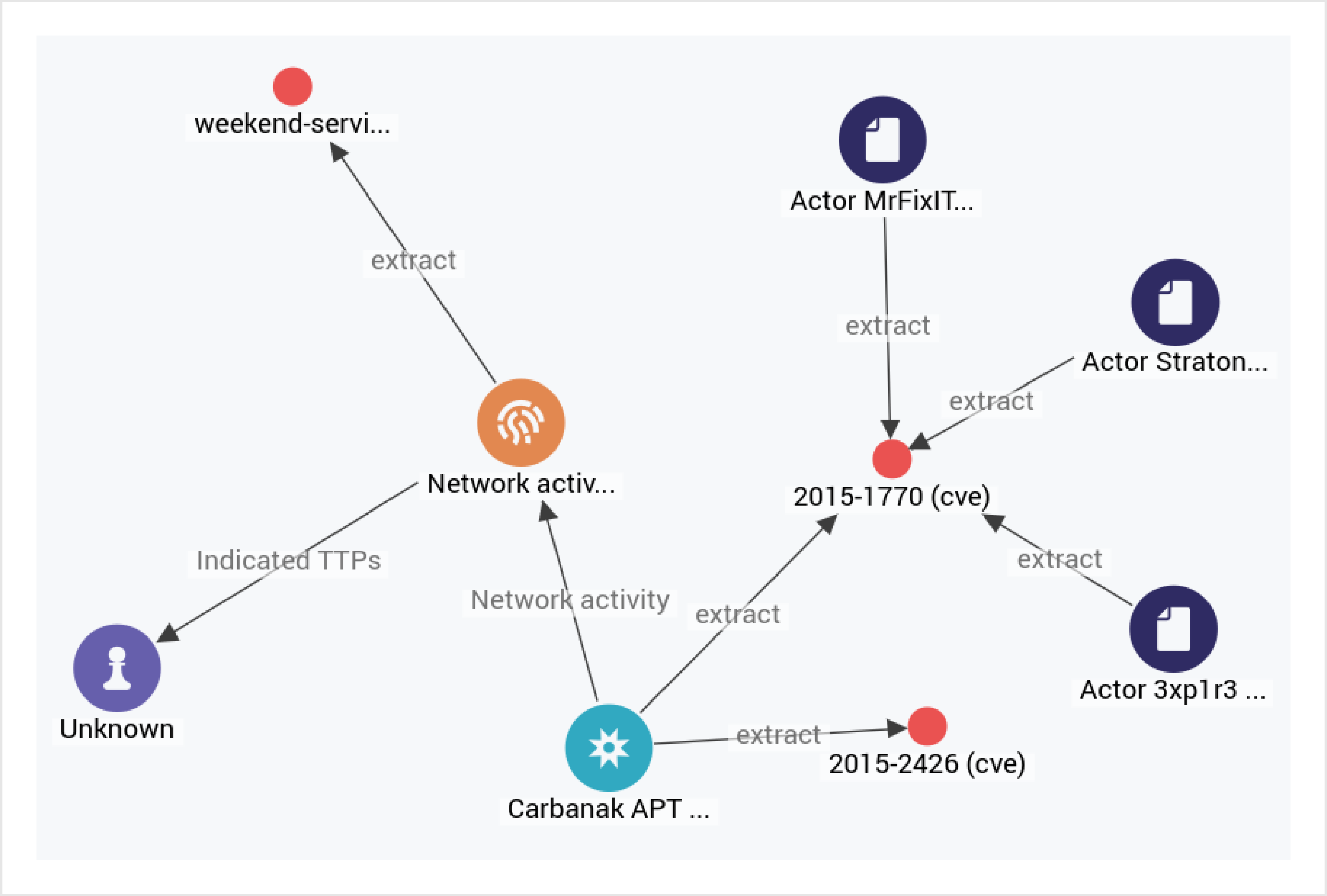
- On the row corresponding to the observable you want to load onto the graph, click the ⋮ icon, and then select **Add to graph**.



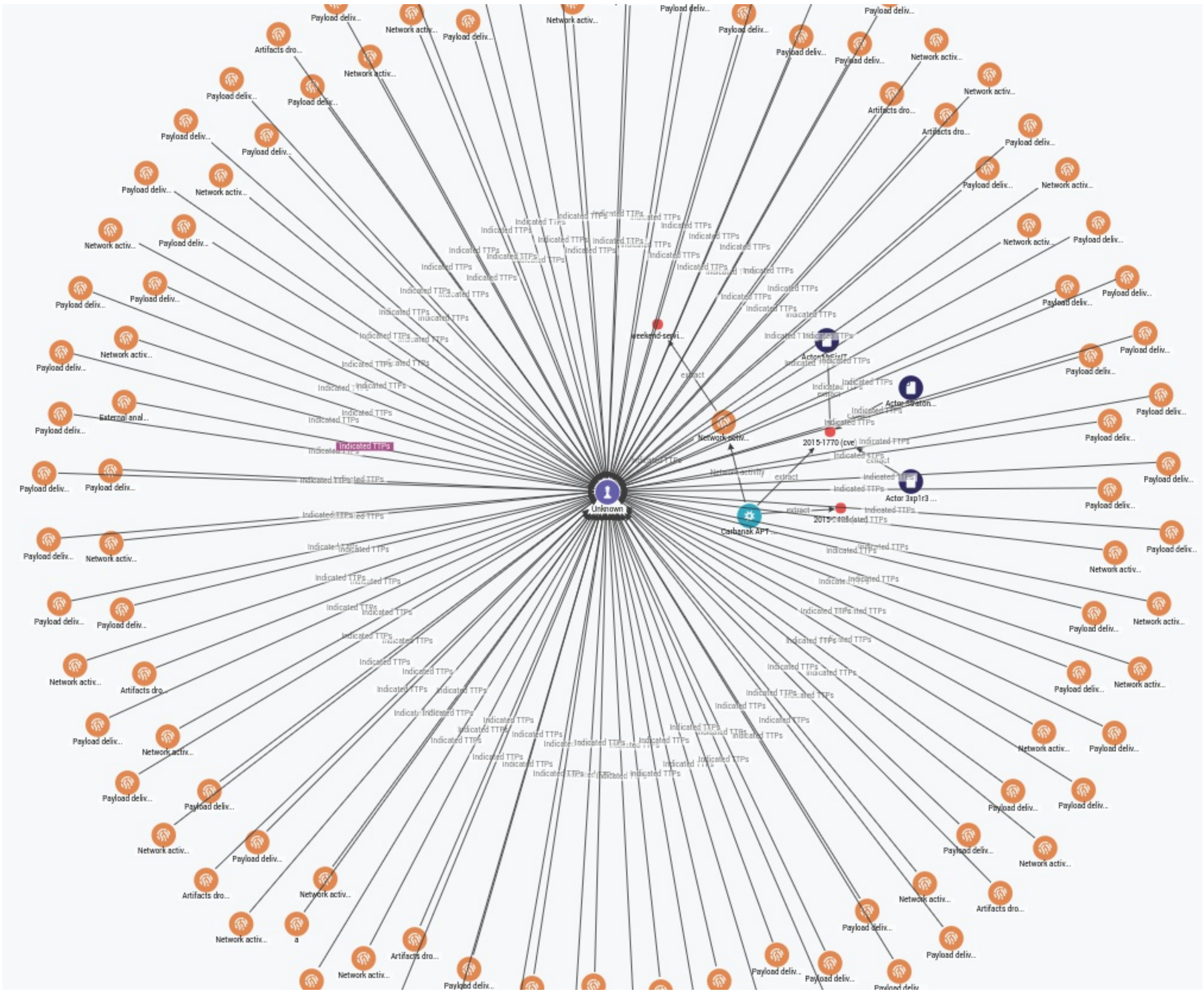
☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

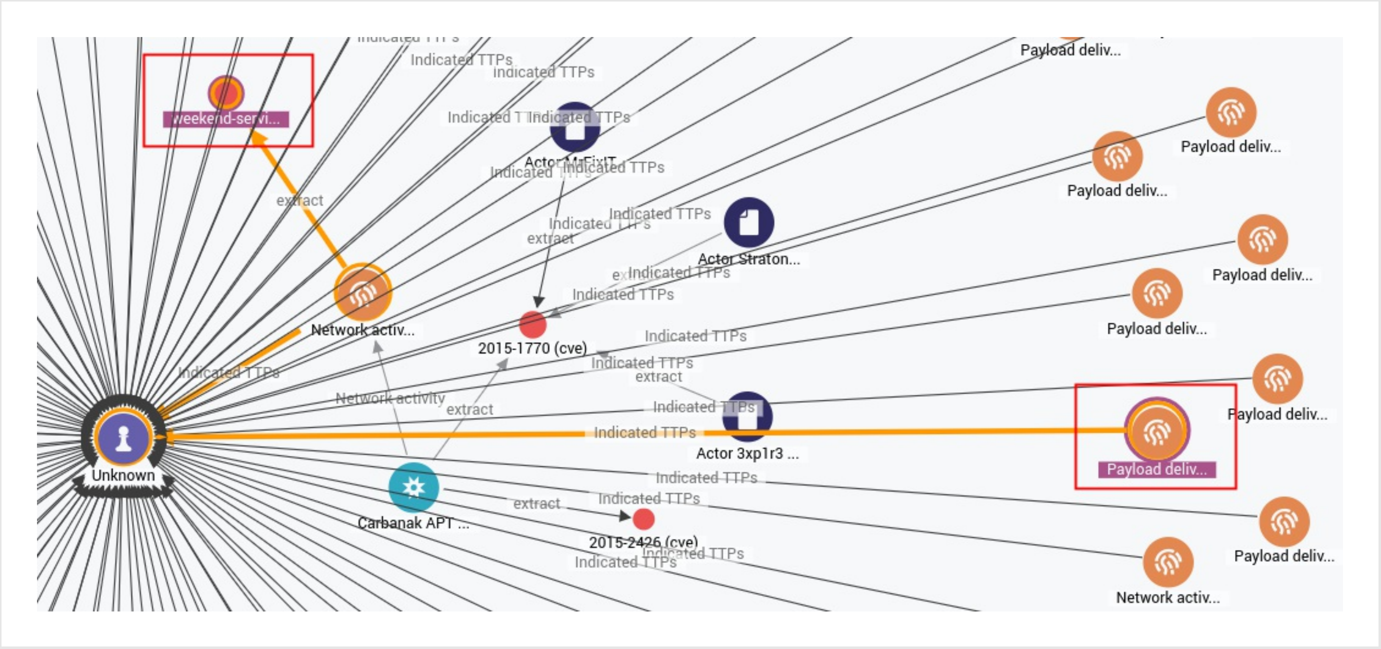


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



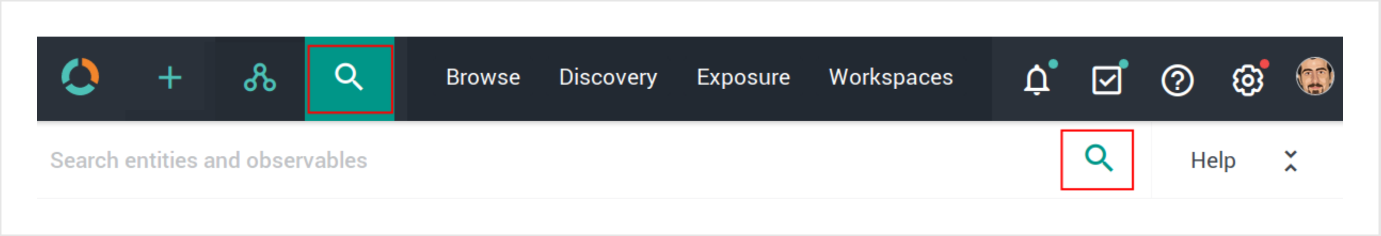
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

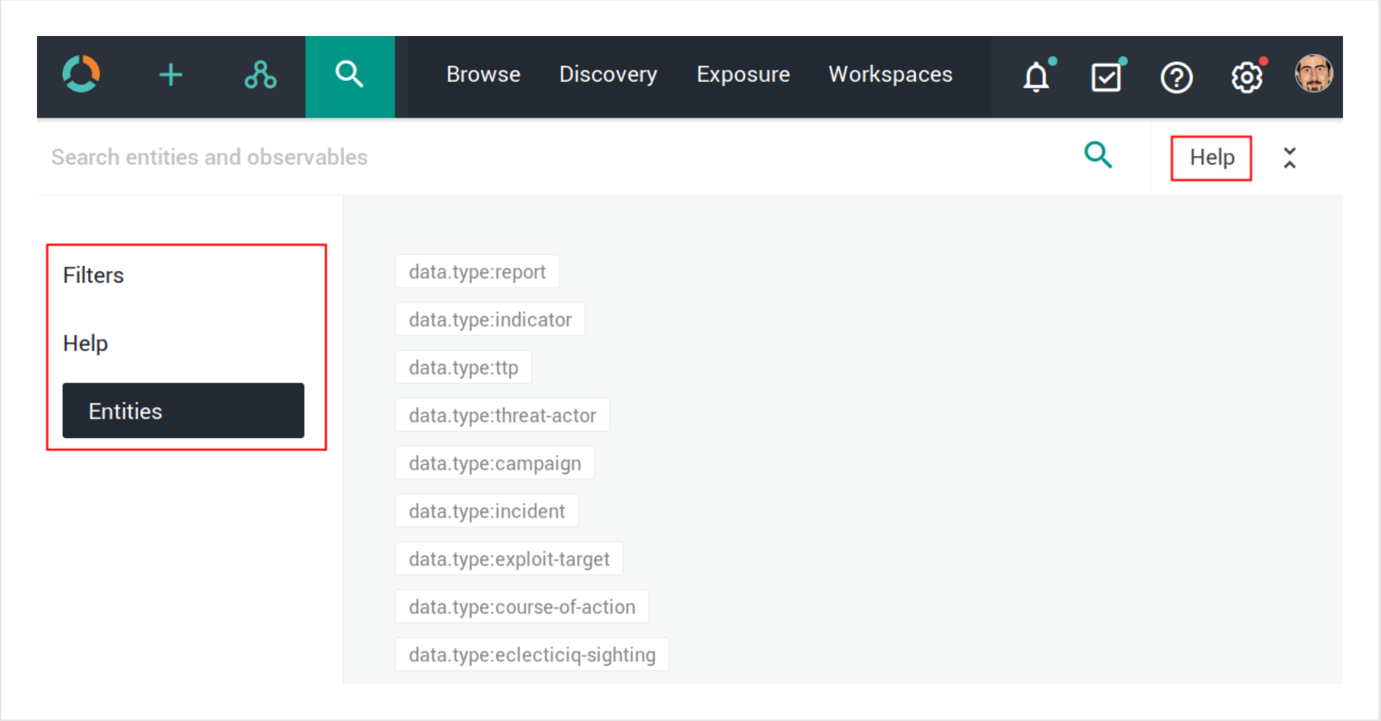


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

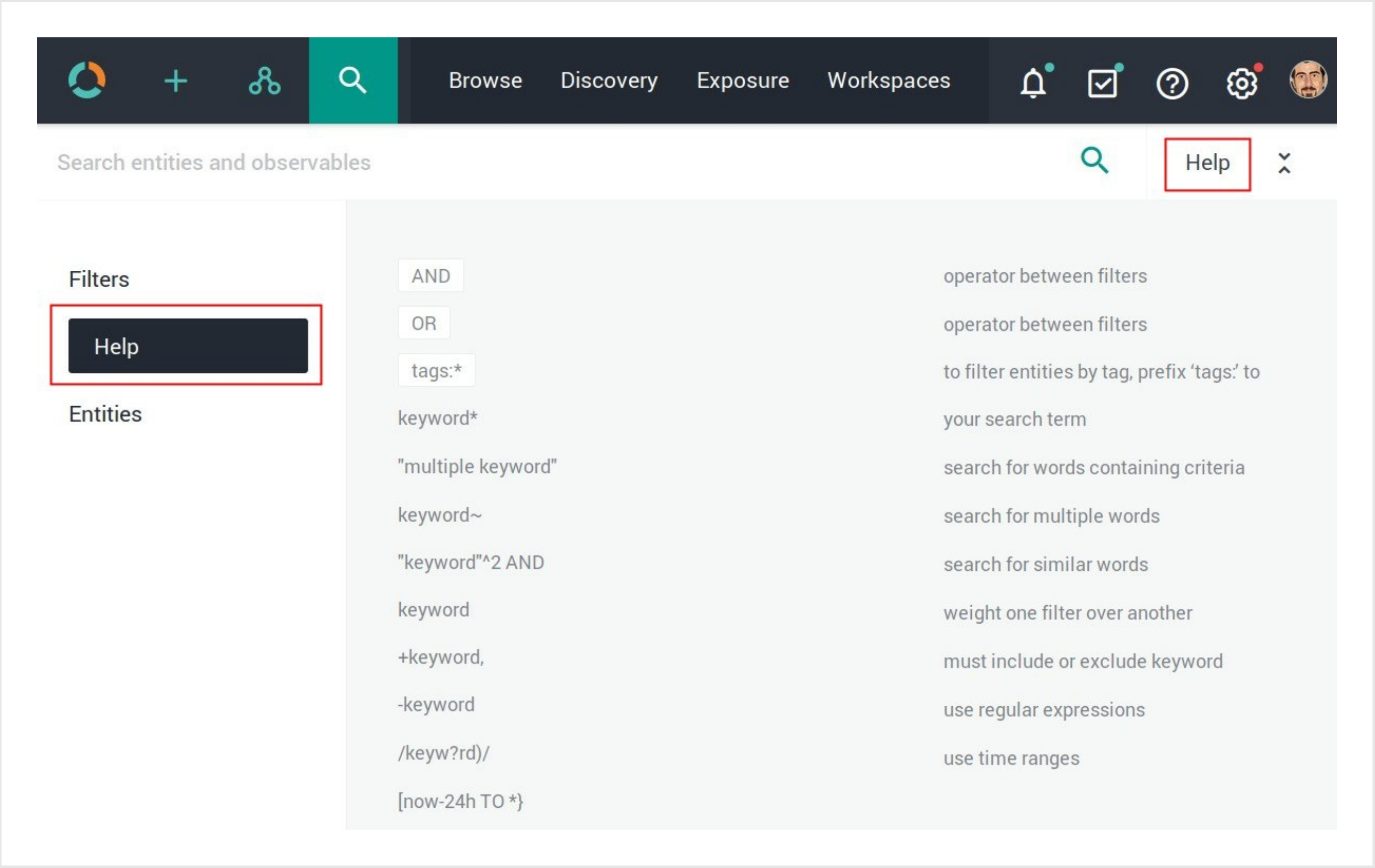
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

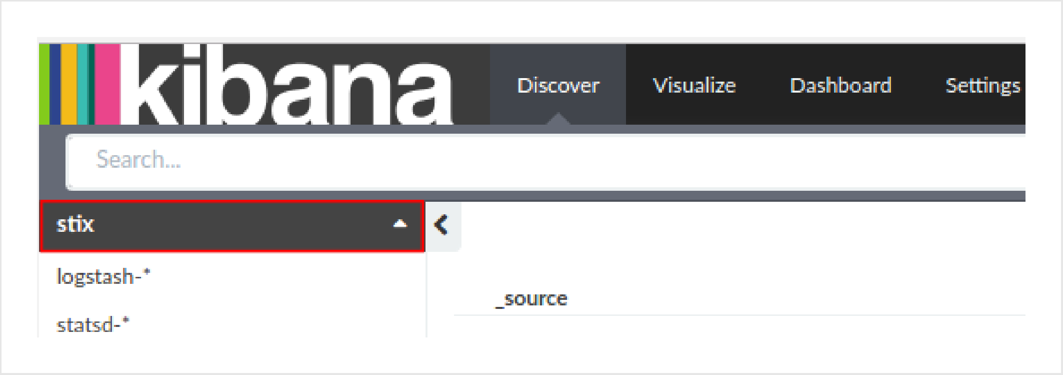
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

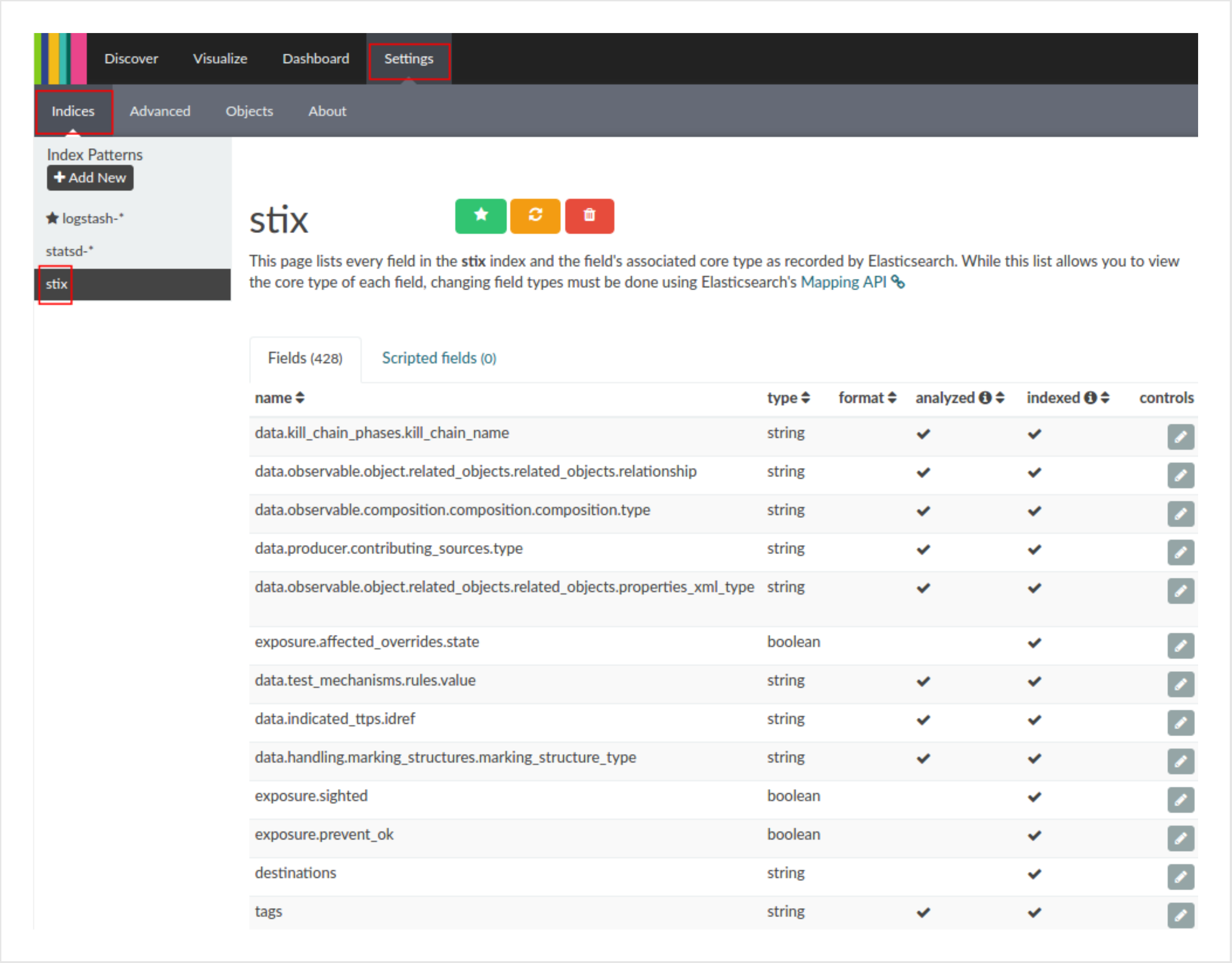
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format: `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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		✓	✓	✎

How to work with the DomainTools Malicious Server Domains enricher

The DomainTools Malicious Server Domains enricher returns malicious domain names related to the same primary and/or secondary name servers, along with their risk scores to automatically flag server domains with an appropriate maliciousness confidence level.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the DomainTools Malicious Server Domains enricher

This article describes how to configure the DomainTools Malicious Server Domains enricher parameters.
To configure the general options for the DomainTools Malicious Server Domains enricher, see Configure enrichers.

DomainTools Malicious Server Domains	**enricher**
Enricher name	DomainTools Malicious Server Domains
API endpoint	`http://api.domaintools.com/v1/{}/name-server-domains/`
Input	domain, host
Output	Enriches the supported observable types with malicious domain names that are served from the same name server.
Description	Enriches domain and host observable types with a list of malicious domain names related to the same primary or secondary name server. It includes configurable thresholds to assign maliciousness confidence levels to the processed domains and hosts, and to ignore non-malicious domains/hosts.

Configure the DomainTools Malicious Server Domains enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.

- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the DomainTools Malicious Server Domains enricher:

- **API user name**: sign up and subscribe to the service to obtain the required API user name and API key credentials to access the API endpoint exposing the service.
- **API key**: contact DomainTools to receive an API key, and then enter it in the corresponding input field.
- **Low maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - Low confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *low maliciousness threshold* and lower than the medium and high maliciousness thresholds are flagged with **Malicious - Low confidence**.
  - Enter a value between *0* and *99.99*.
  - Default value: *10*.
- **Medium maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - Medium confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *medium maliciousness threshold* and lower than the high maliciousness threshold are flagged with **Malicious - Medium confidence**.
  - Enter a value between *0* and *99.99*.
  - Default value: *40*.
- **High maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - High confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *high maliciousness threshold* are flagged with **Malicious - High confidence**.
  - Enter a value between *0* and *99.99*.
  - Default value: *80*.
- **Ignore non-malicious domains**: select this checkbox to to exclude from ingestion any domains and hosts whose reputation/risk score value is lower than the specified *low maliciousness threshold*.
- 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 **+ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **✚ Add** or **✚ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.

- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

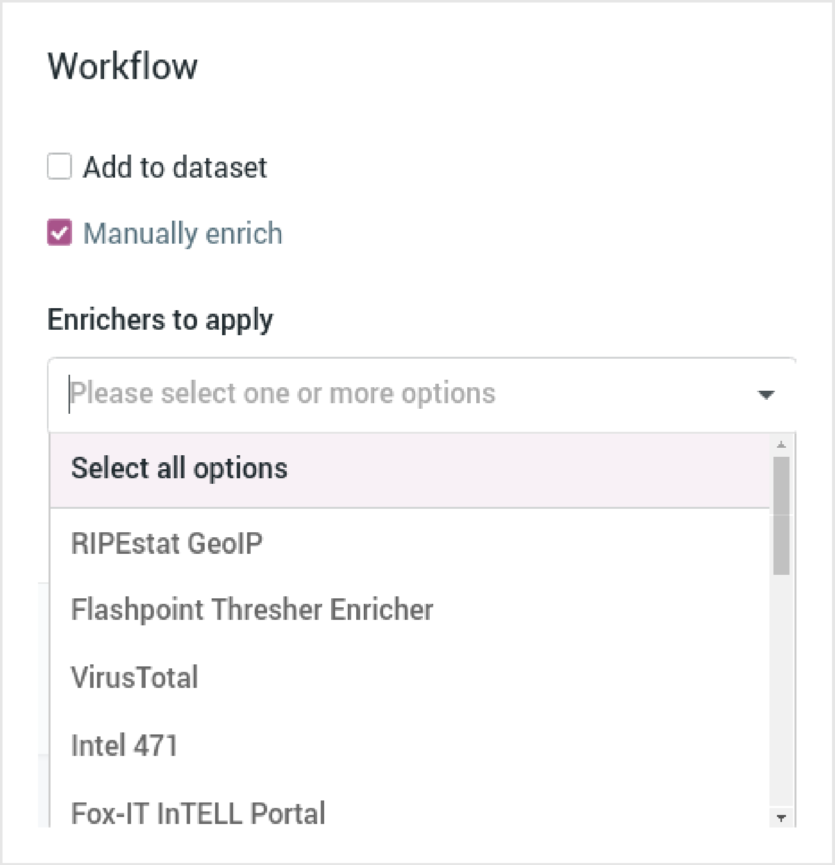
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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.

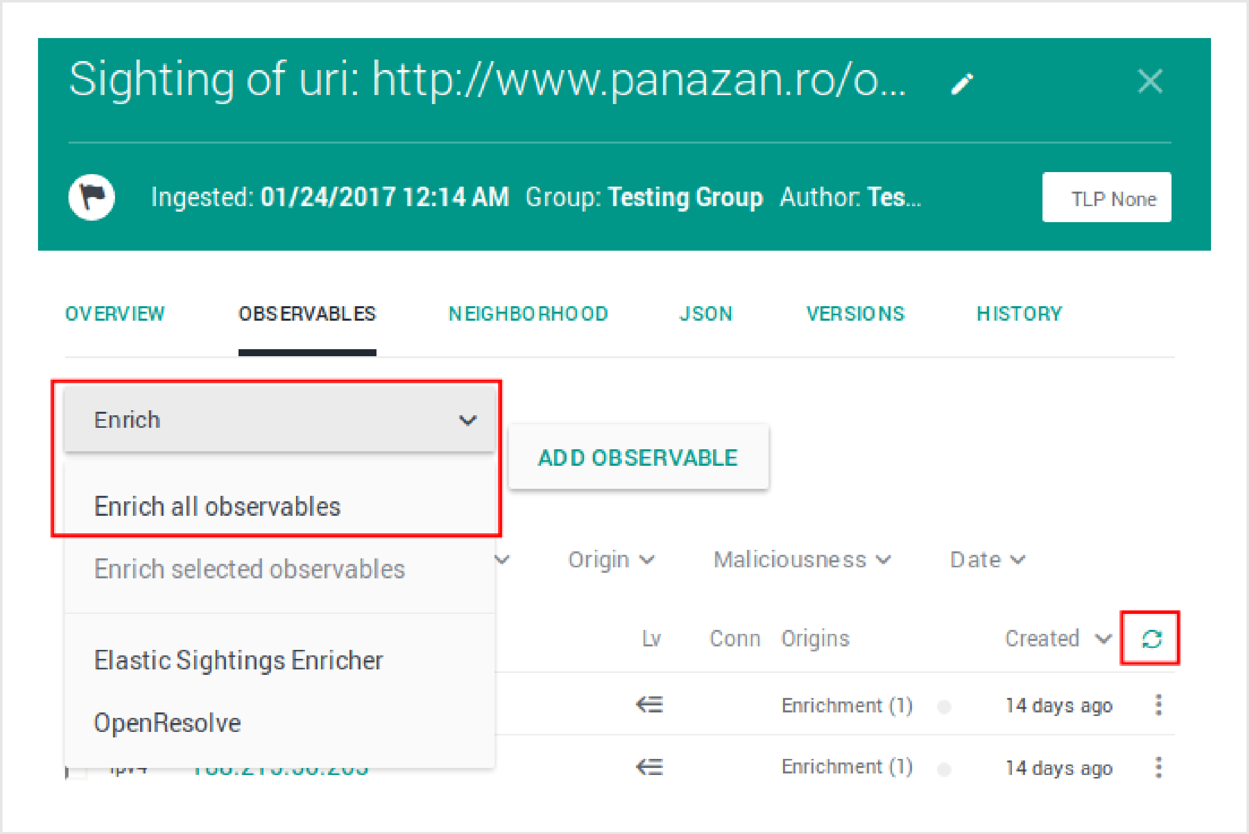
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

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 **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.

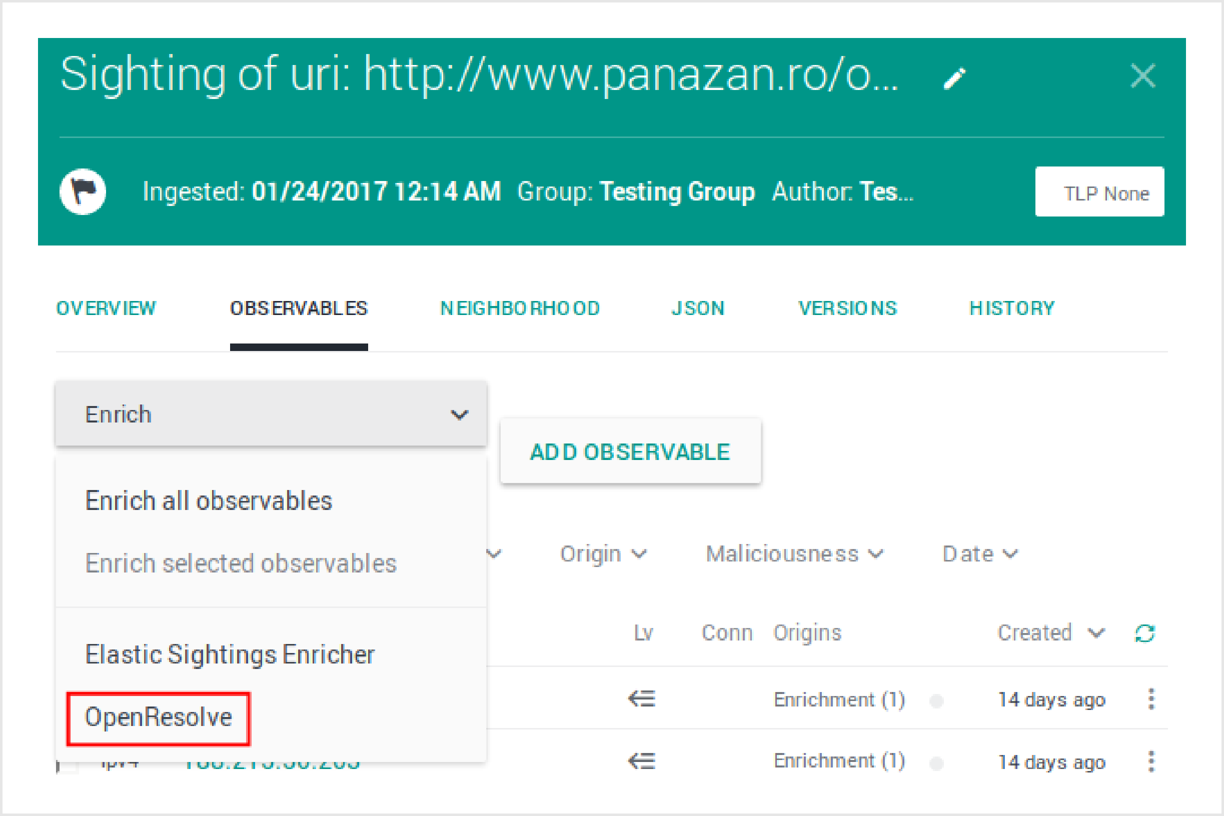


Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



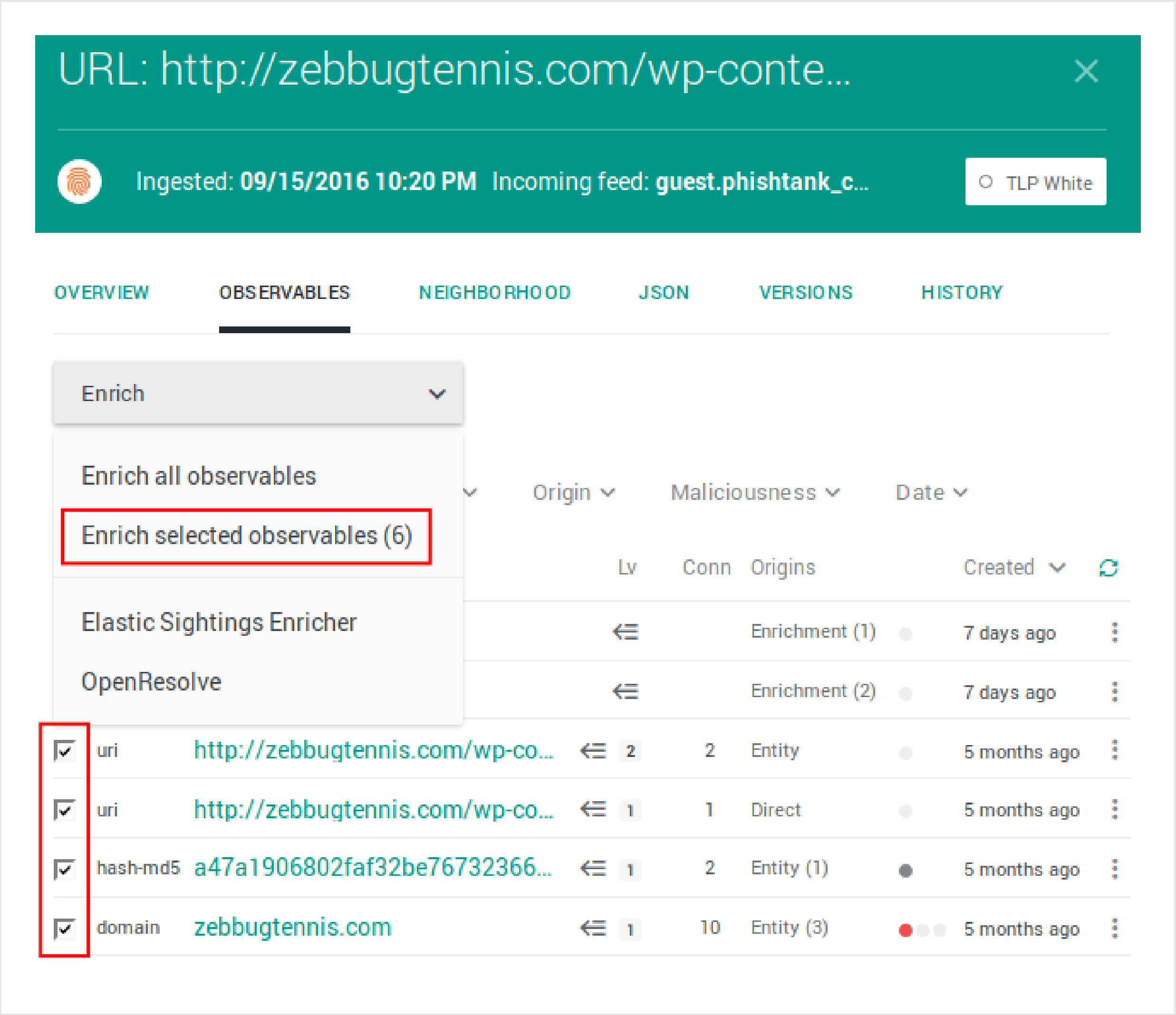
Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



Ingested: **09/15/2016 10:20 PM** Incoming feed: **guest.phishtank_c...**

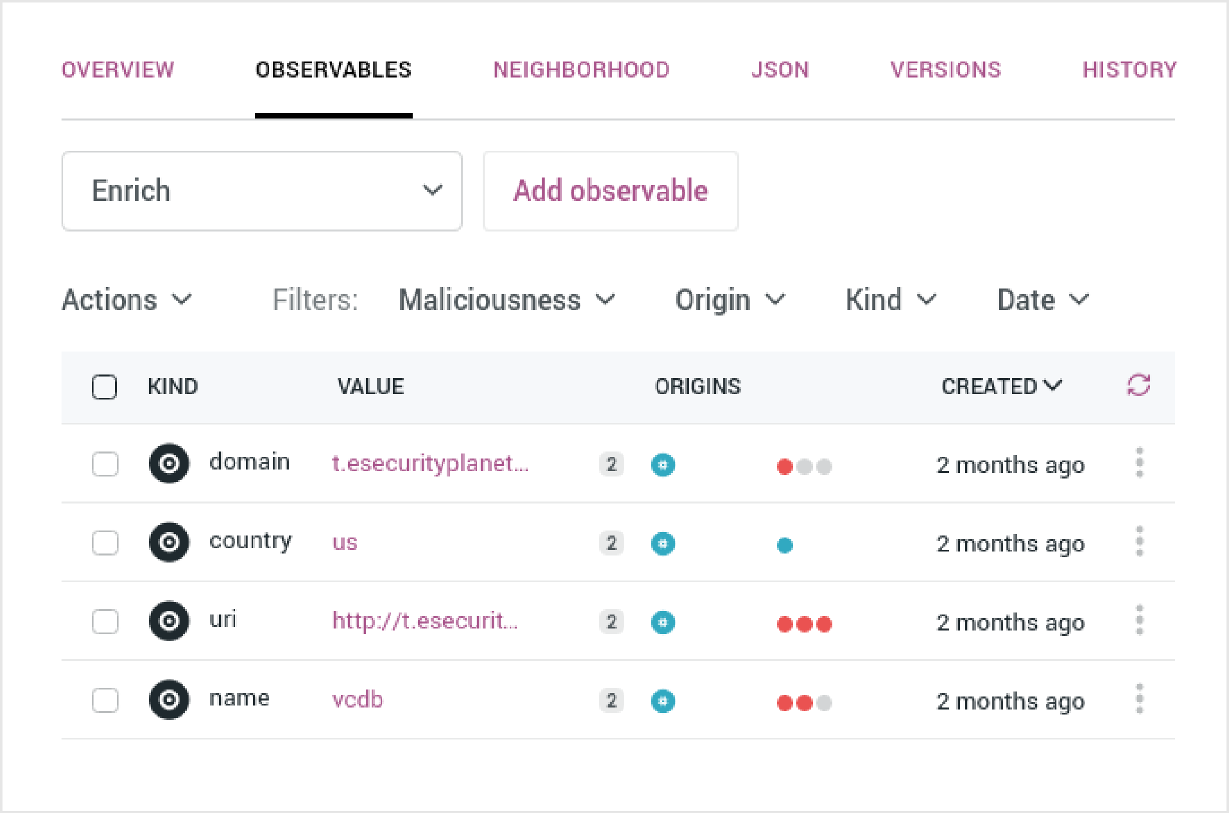
			Lv	Conn	Origins	Created
					Enrichment (1)	7 days ago
					Enrichment (2)	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	2	2	Entity	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	1	1	Direct	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	1	2	Entity (1)	5 months ago
☑	domain	zebbugtennis.com	1	10	Entity (3)	5 months ago

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

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.

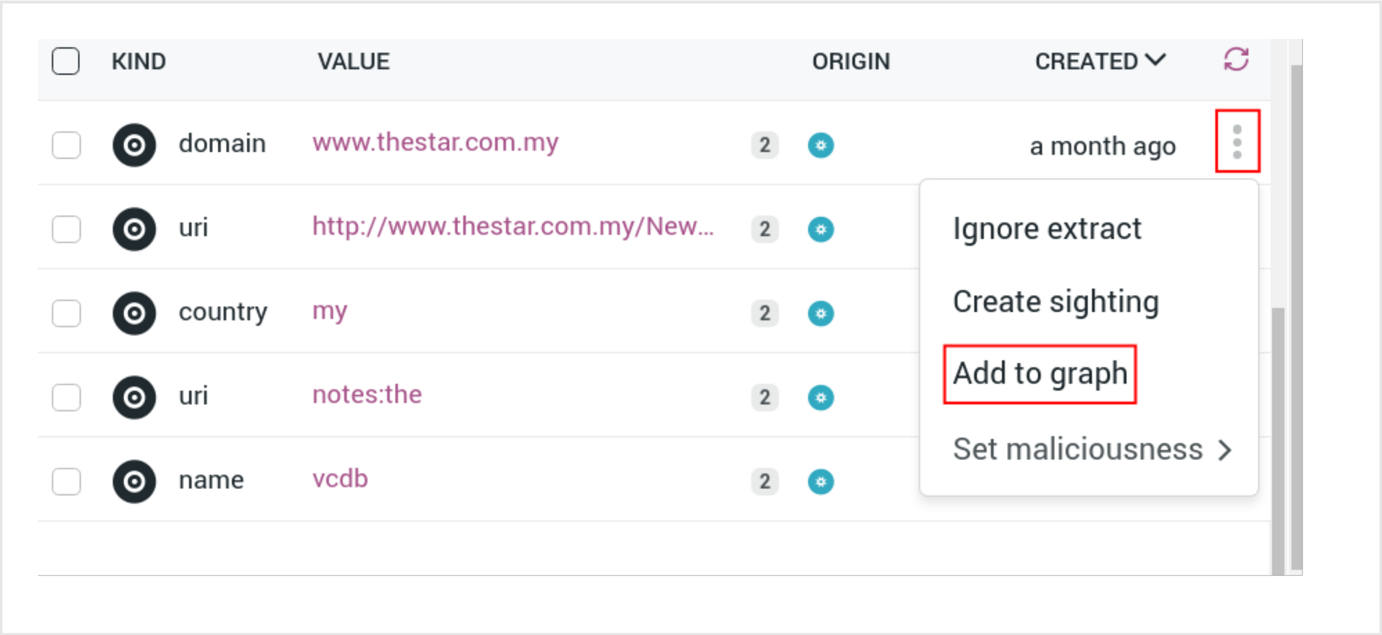


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

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

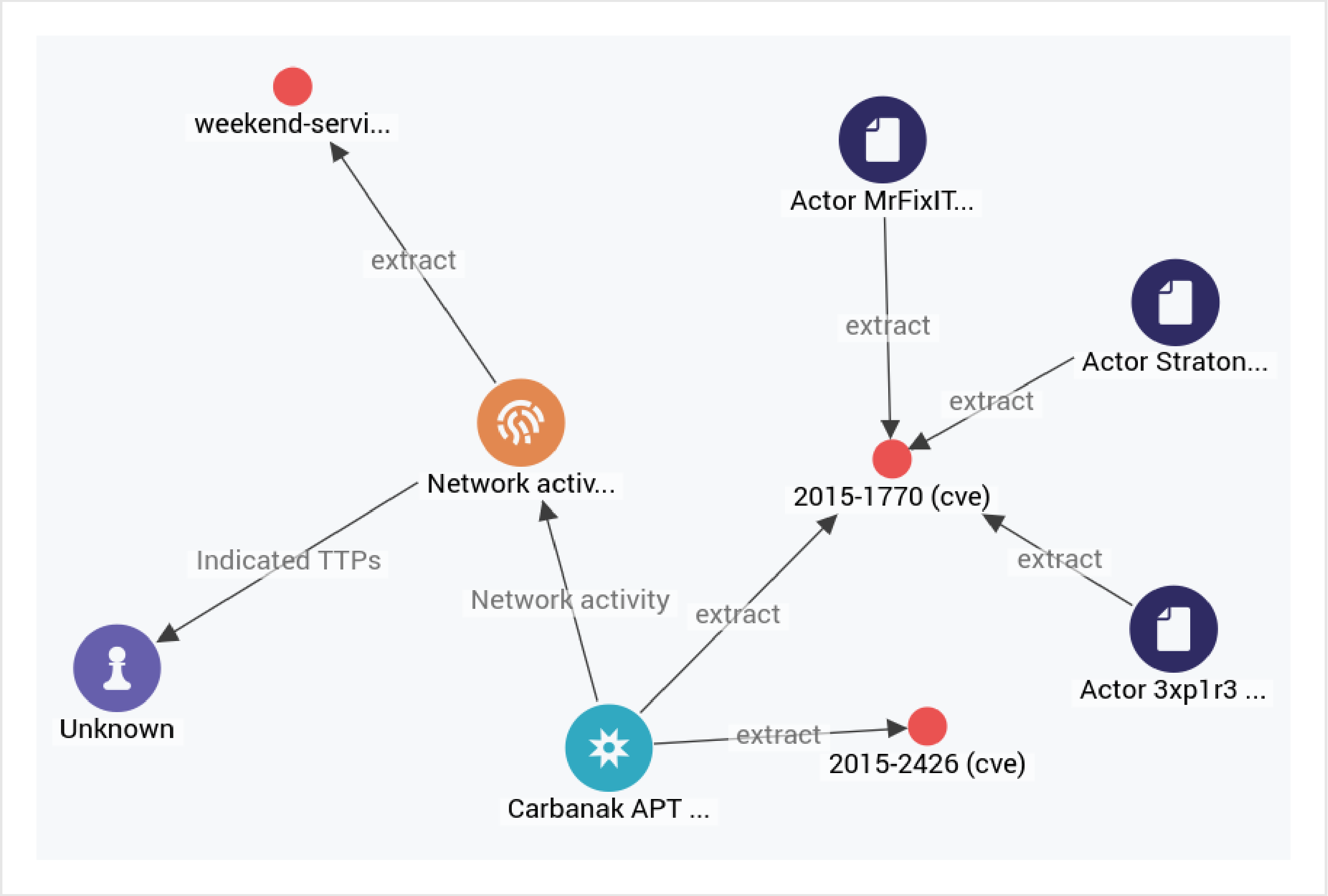
- On the row corresponding to the observable you want to load onto the graph, click the ⋮ icon, and then select **Add to graph**.



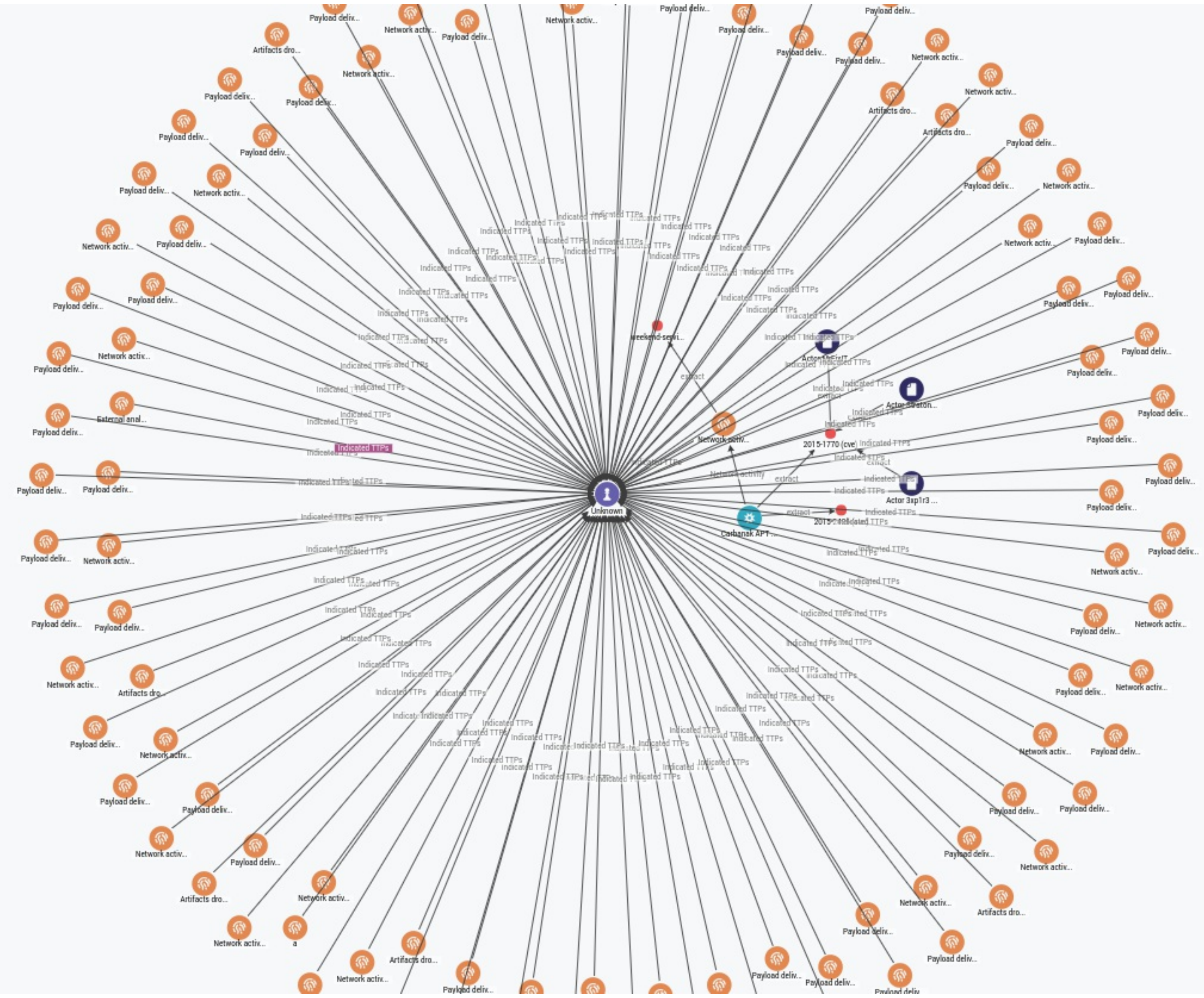
☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

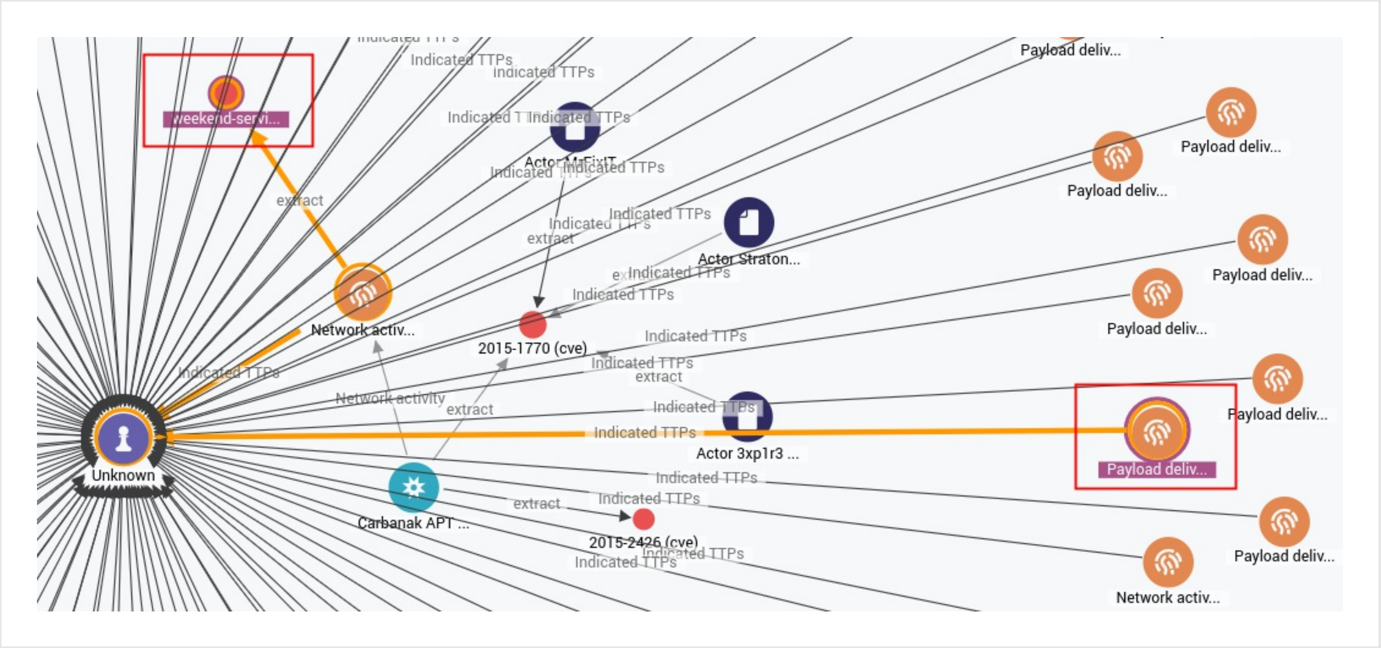


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



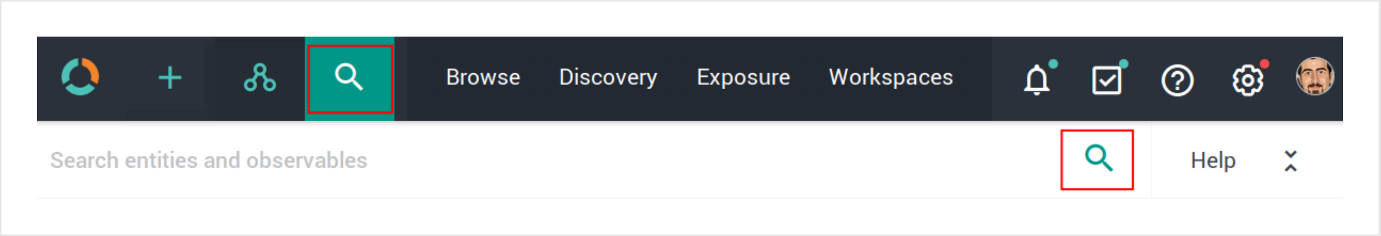
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

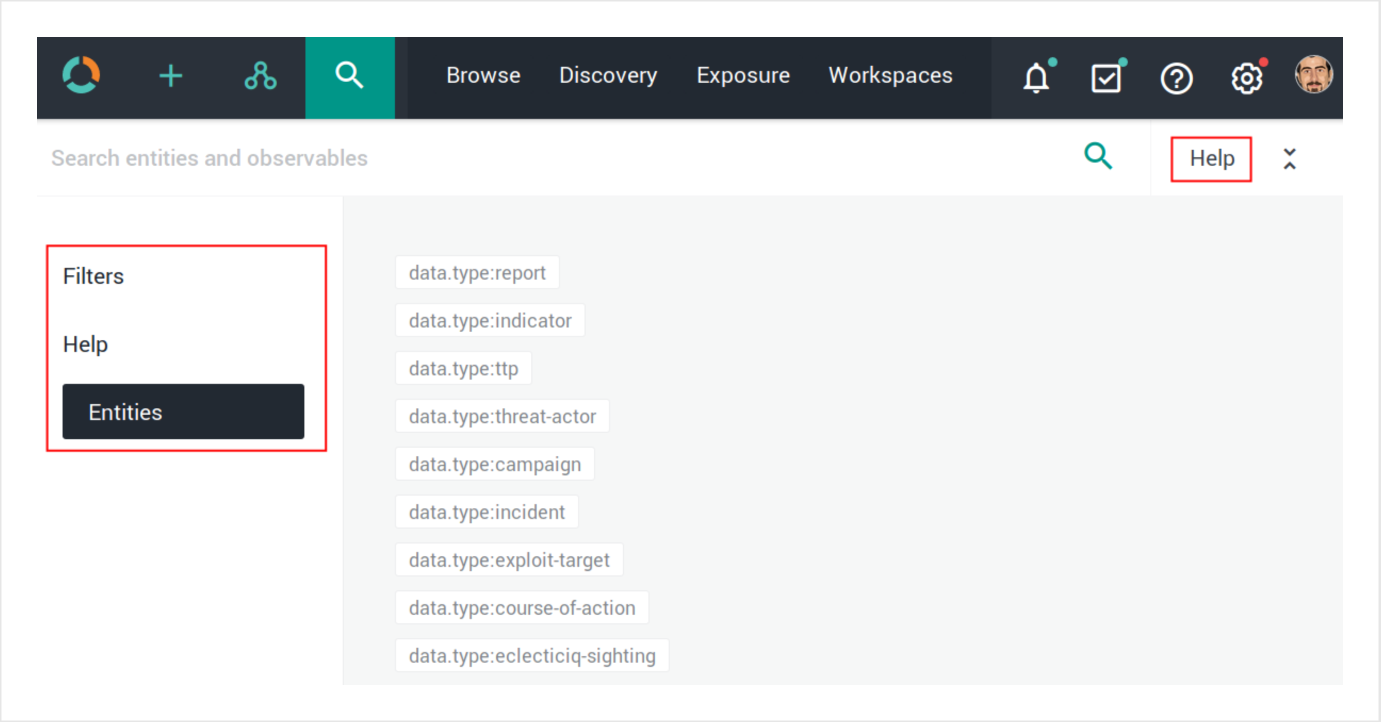


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

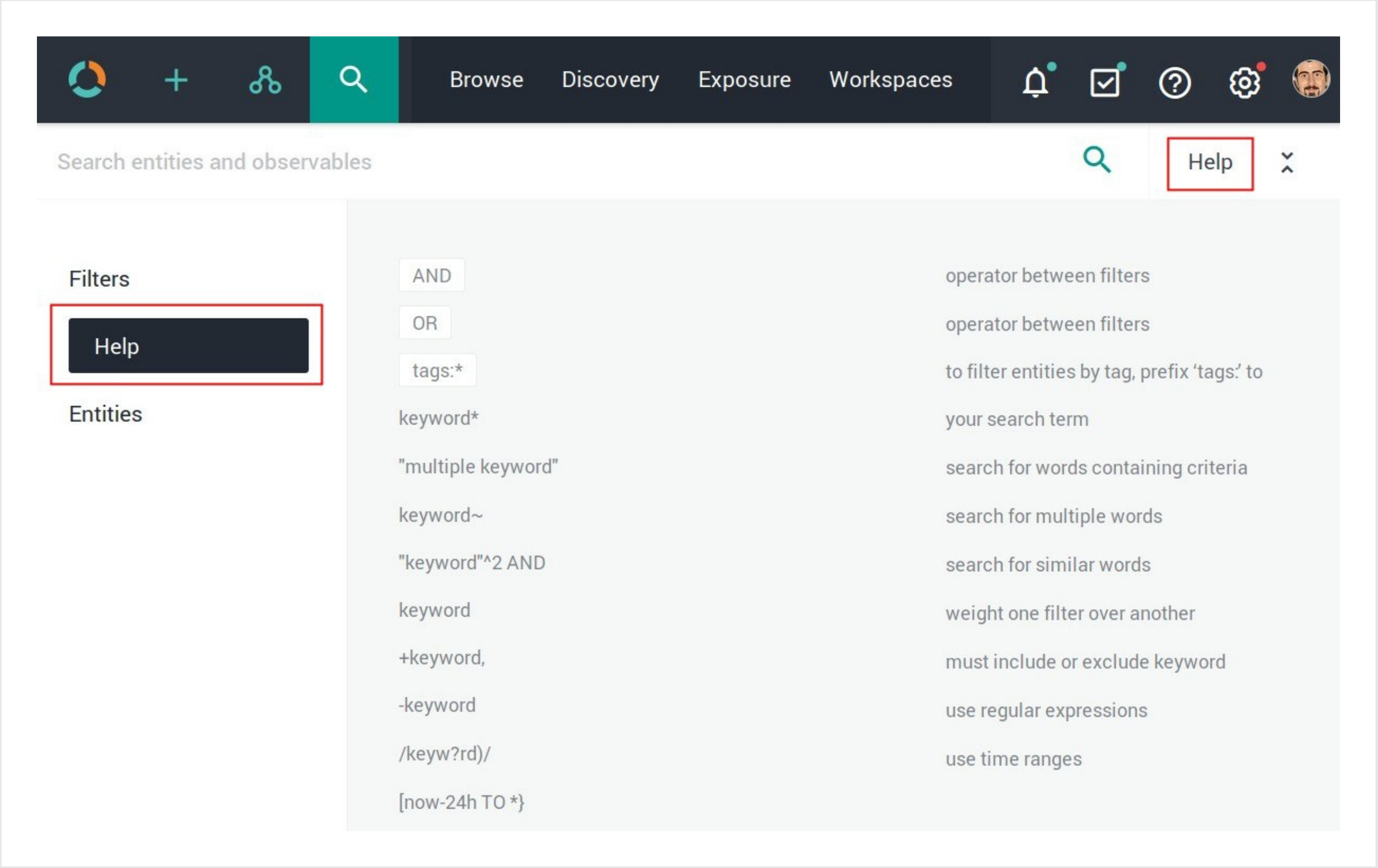
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

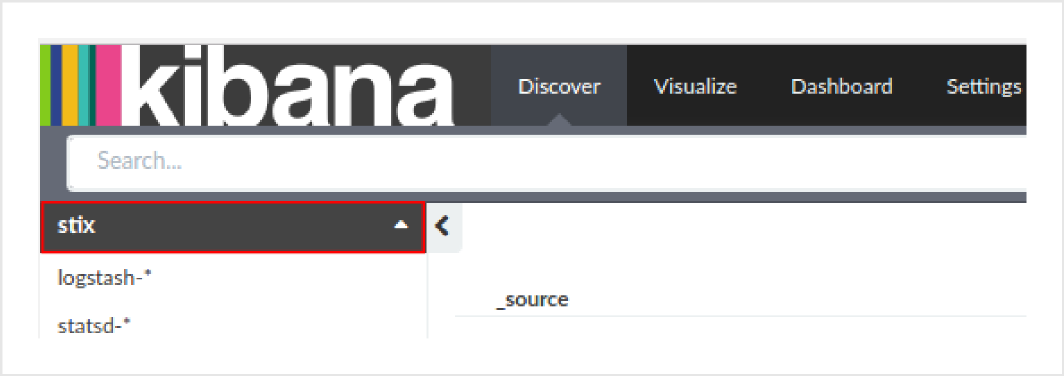
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

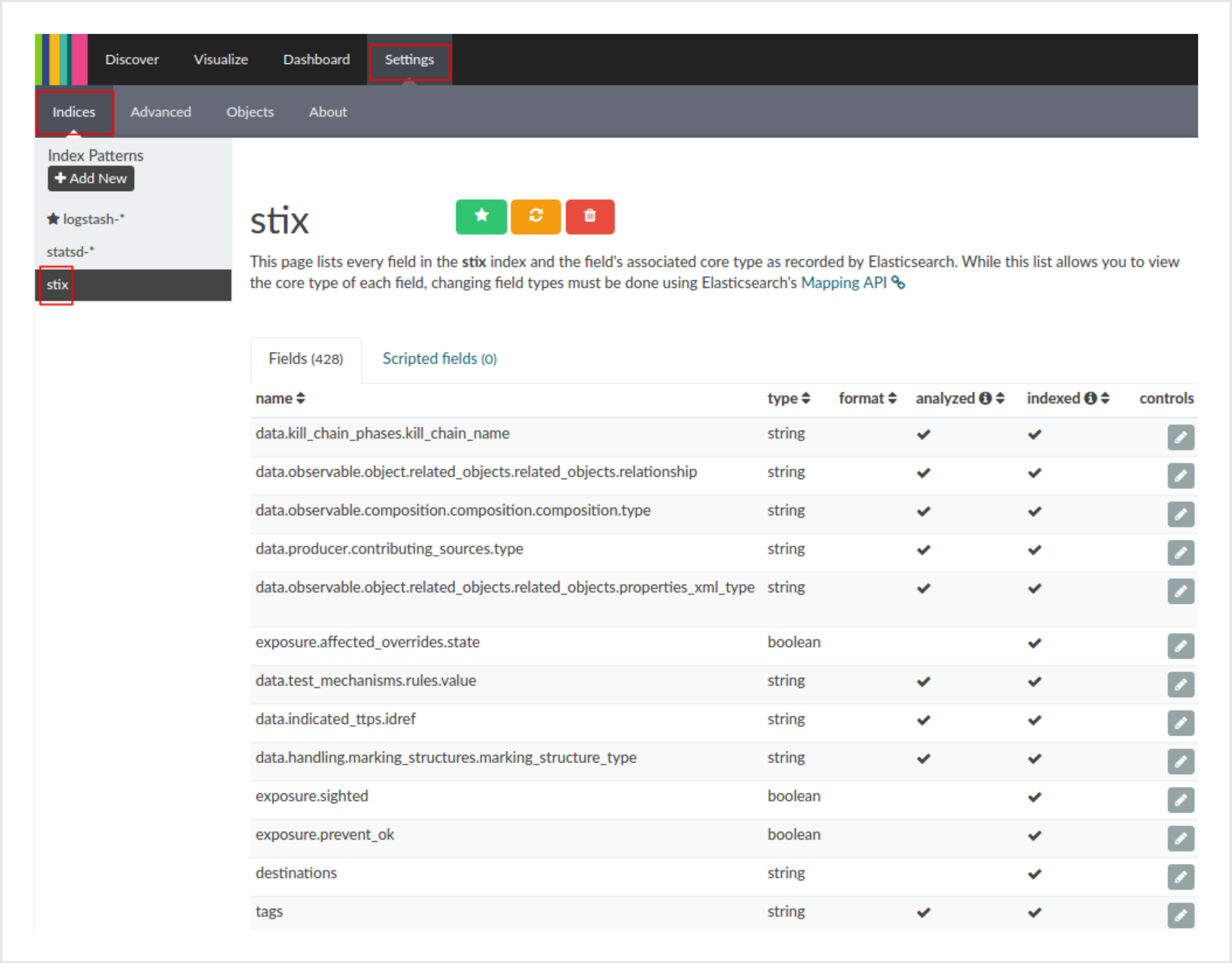
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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

Fields (428) Scripted fields (0)

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		✓	✓	

How to work with the DomainTools Reputation enricher

The Domaintools Reputation enricher returns risk scores to assess the reputation of the specified input domain and host names.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the DomainTools Reputation enricher

This article describes how to configure the DomainTools Reputation enricher parameters.
To configure the general options for the DomainTools Reputation enricher, see Configure enrichers.

DomainTools Reputation	**enricher**
Enricher name	DomainTools Reputation
API endpoint	`http://api.domaintools.com/v1/reputation`
Input	domain, host
Output	Enriches the supported observable types with reputation information.
Description	Enriches domain and host name observables with reputation/risk score information to assess maliciousness confidence levels, based on user-defined threshold values.

Configure the DomainTools Reputation enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

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

Under **Parameters**, define the specific configuration options for the DomainTools Reputation enricher:

- **API user name**: sign up and subscribe to the service to obtain the required API user name and API key credentials to access the API endpoint exposing the service.
- **API key**: contact DomainTools to receive an API key, and then enter it in the corresponding input field.
- **Low maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - Low confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *low maliciousness threshold* and lower than the medium and high maliciousness thresholds are flagged with **Malicious - Low confidence**.
    - Enter a value between *0* and *99.99*.
    - Default value: *10*.
- **Medium maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - Medium confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *medium maliciousness threshold* and lower than the high maliciousness threshold are flagged with **Malicious - Medium confidence**.
    - Enter a value between *0* and *99.99*.
    - Default value: *40*.
- **High maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - High confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *high maliciousness threshold* are flagged with **Malicious - High confidence**.
    - Enter a value between *0* and *99.99*.
    - Default value: *80*.
- 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 **✚ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.

- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **+ Add** or **+ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **+ Add** or **+ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.

- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

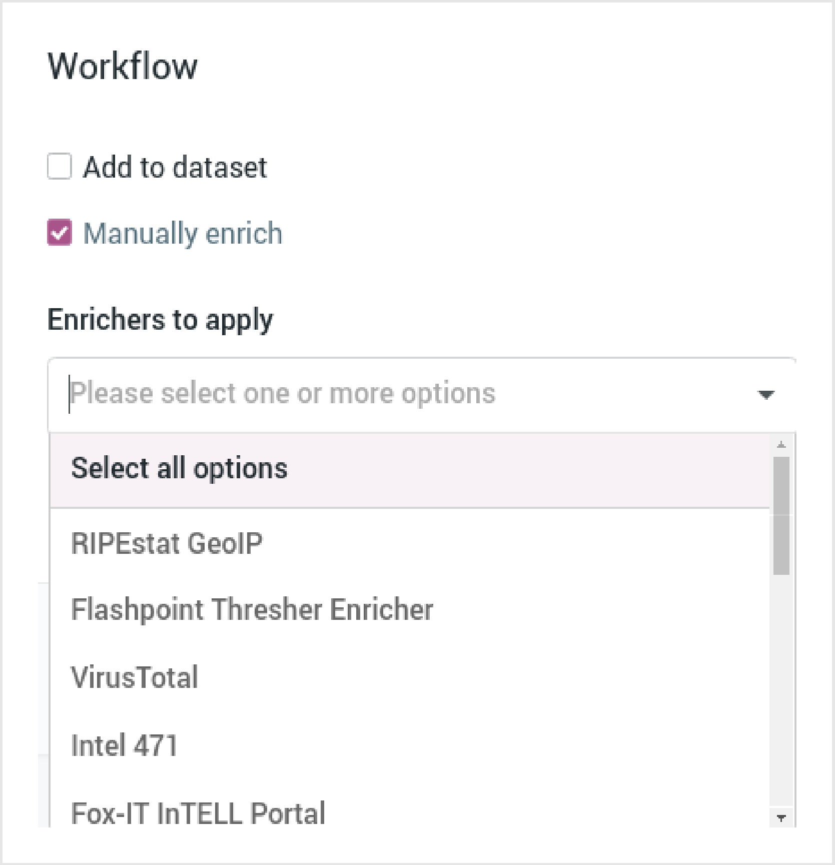
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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.



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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

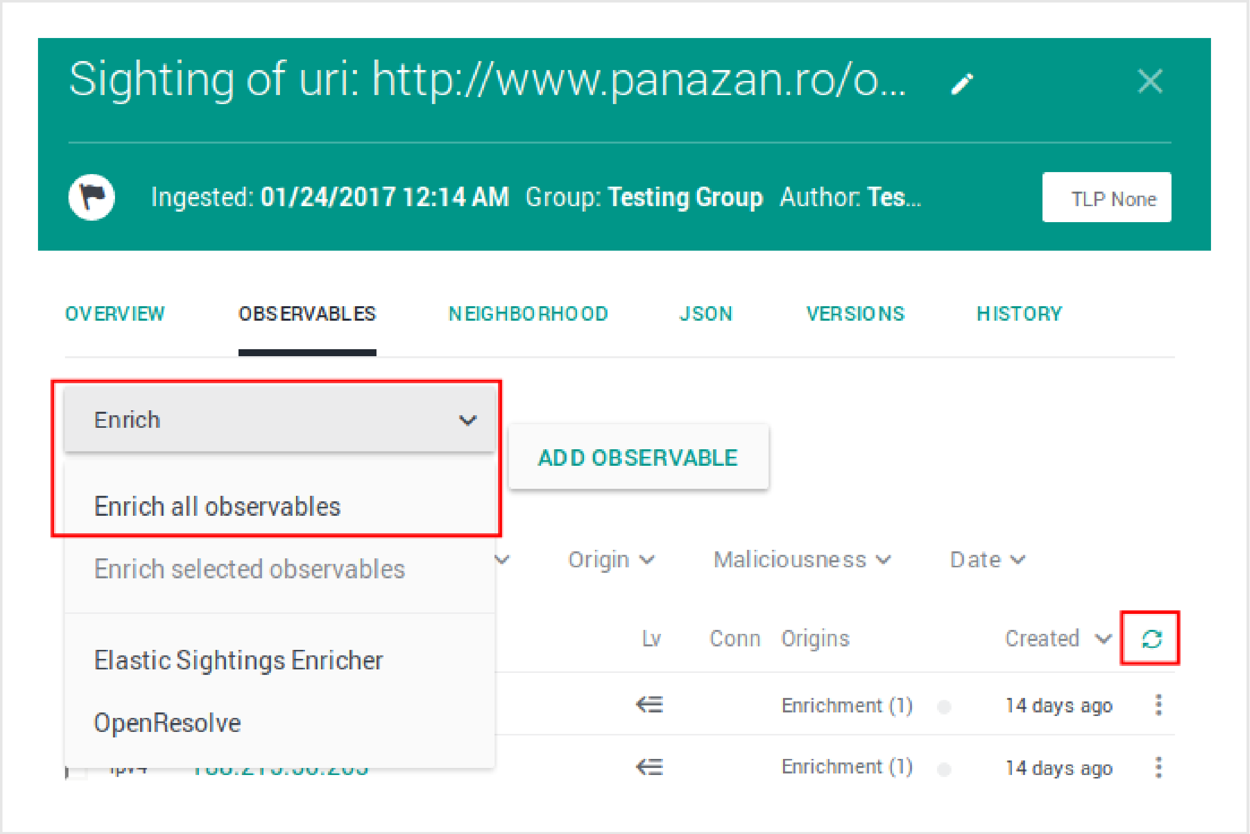
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the 🗘 refresh icon to trigger a task run that polls all the enrichers configured for the entity.

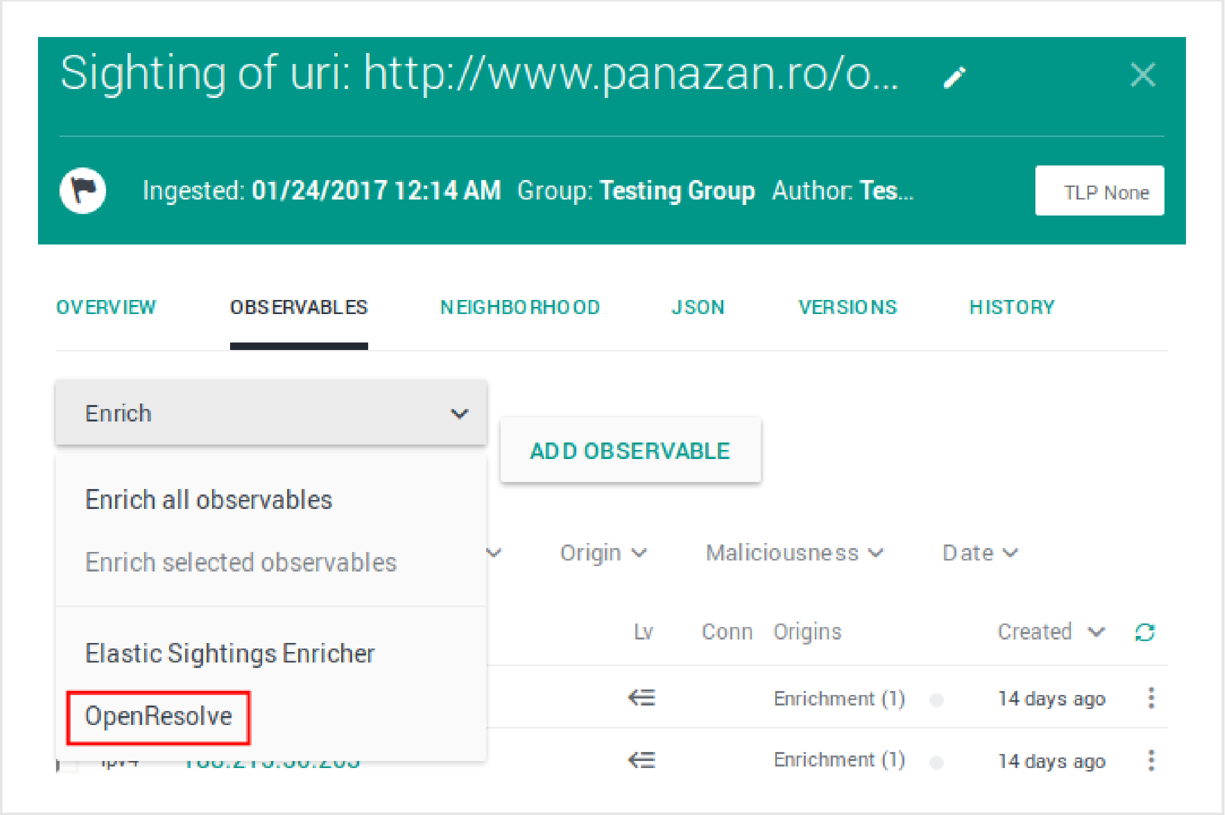
Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



To poll a specific enricher:

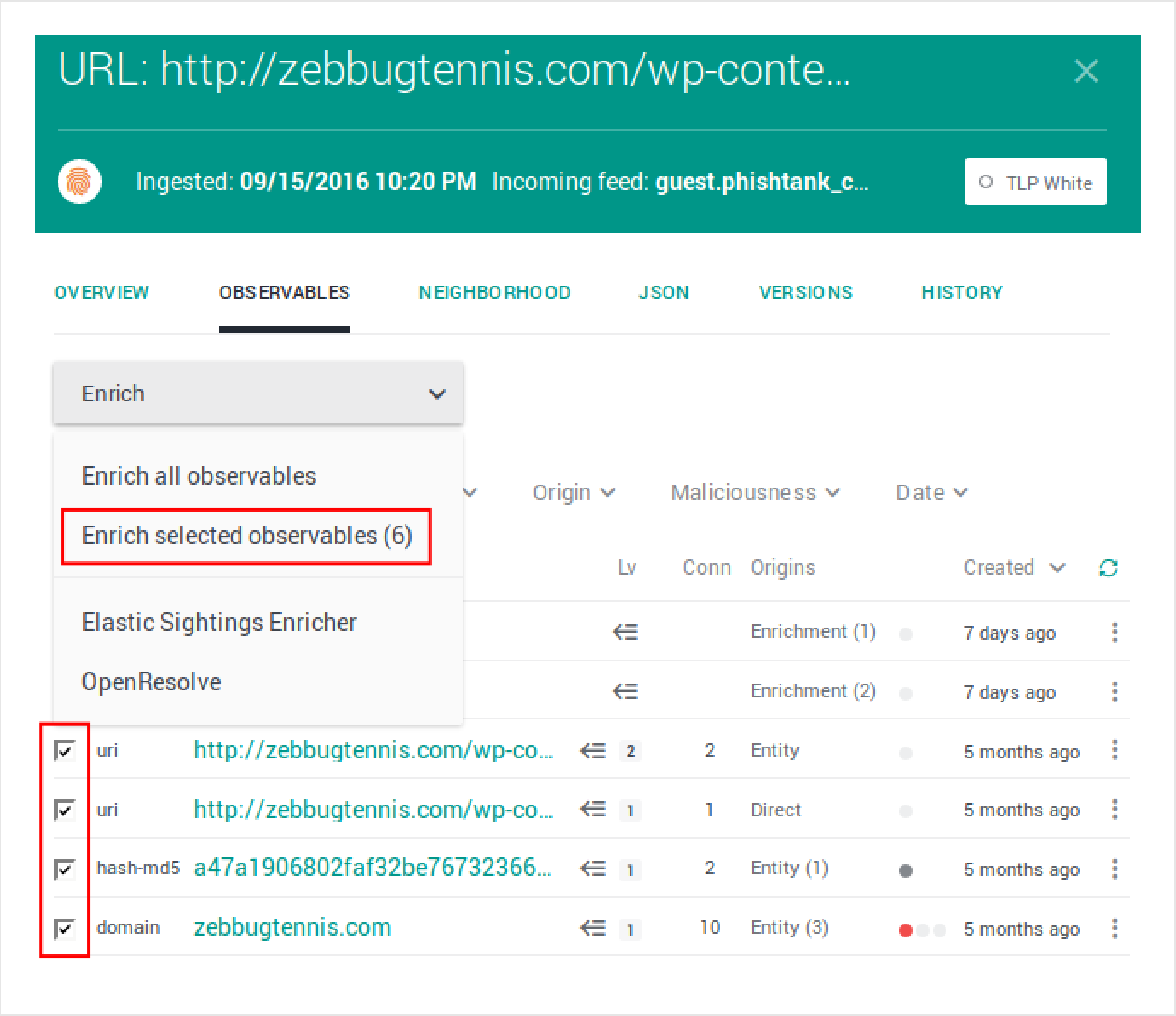
- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.


URL: http://zebbugtennis.com/wp-conte...
Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White
OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY
Enrich
Enrich all observables
Enrich selected observables (6)
Elastic Sightings Enricher
OpenResolve
Origin
Maliciousness
Date

			Lv	Conn	Origins		Created
			⇇		Enrichment (1)	●	7 days ago
			⇇		Enrichment (2)	●	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 2	2	Entity	●	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 1	1	Direct	●	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	⇇ 1	2	Entity (1)	●	5 months ago
☑	domain	zebbugtennis.com	⇇ 1	10	Entity (3)	●●●	5 months ago

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 DomainTools Reputation enricher can take the following observable types as input:

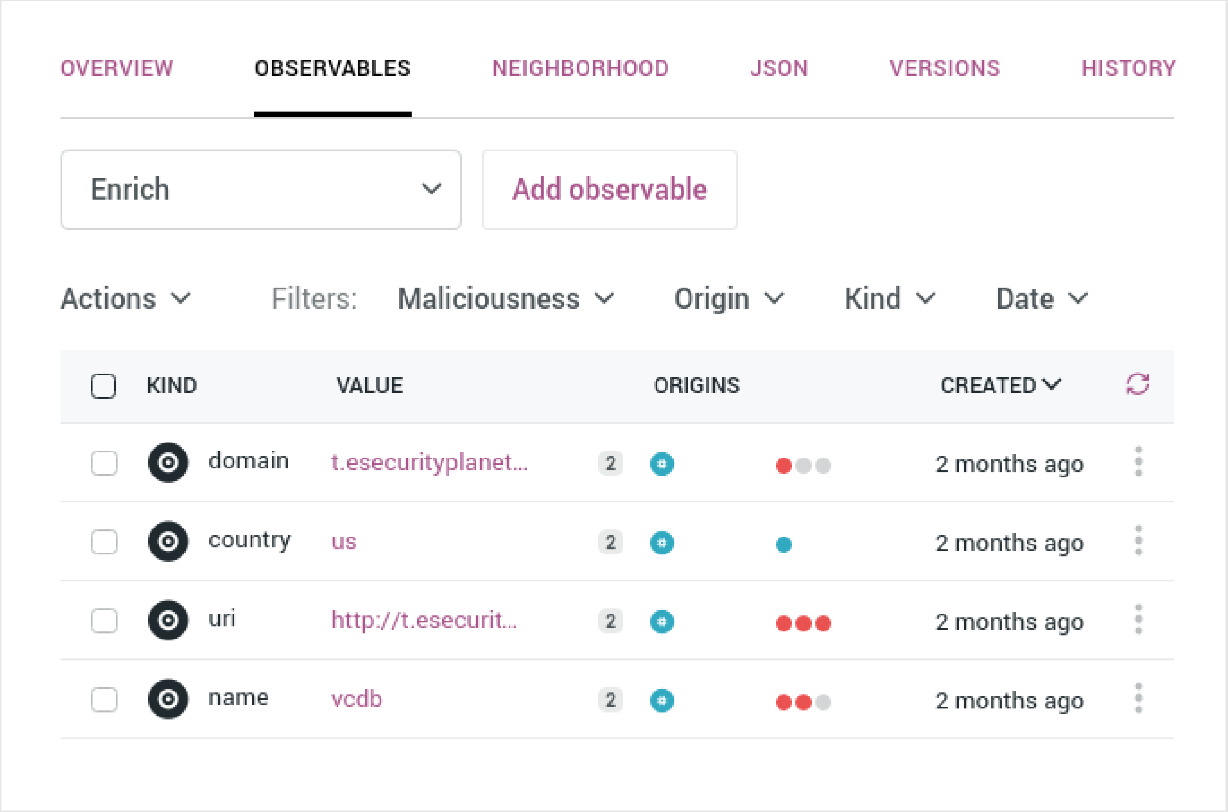
- *domain, host*

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 DomainTools Reputation.

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.

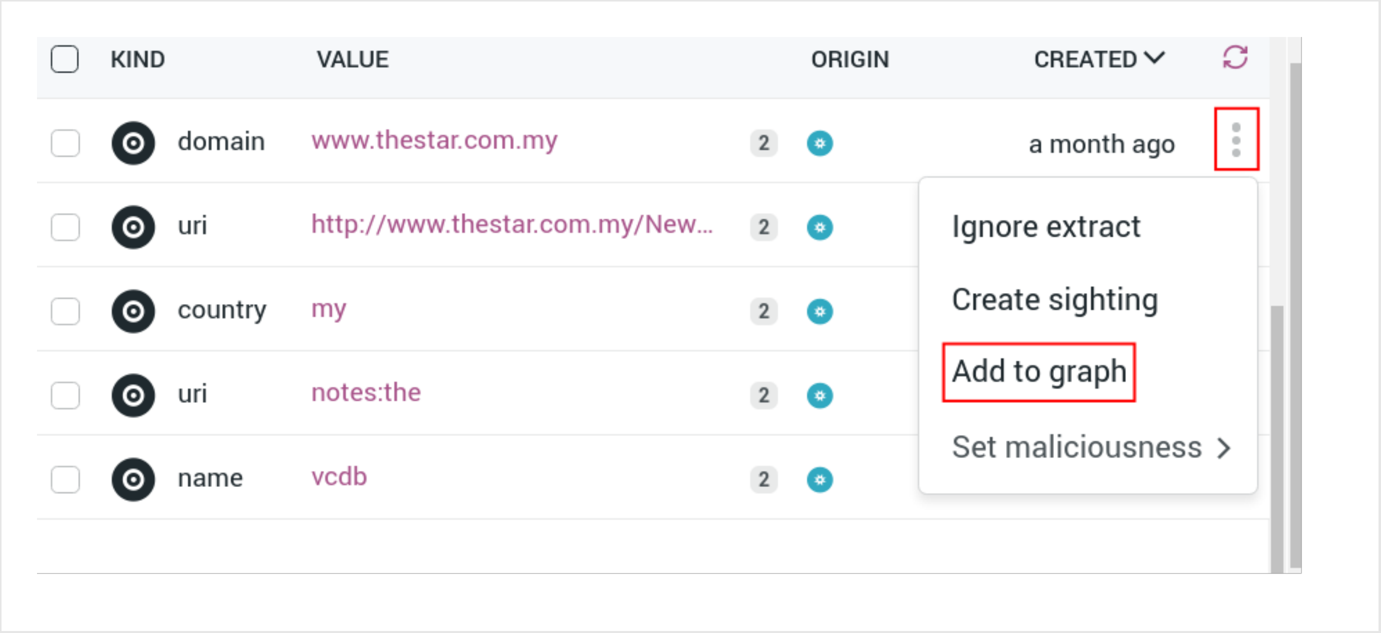


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●○○	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●○	2 months ago

Review enrichment observables on the graph

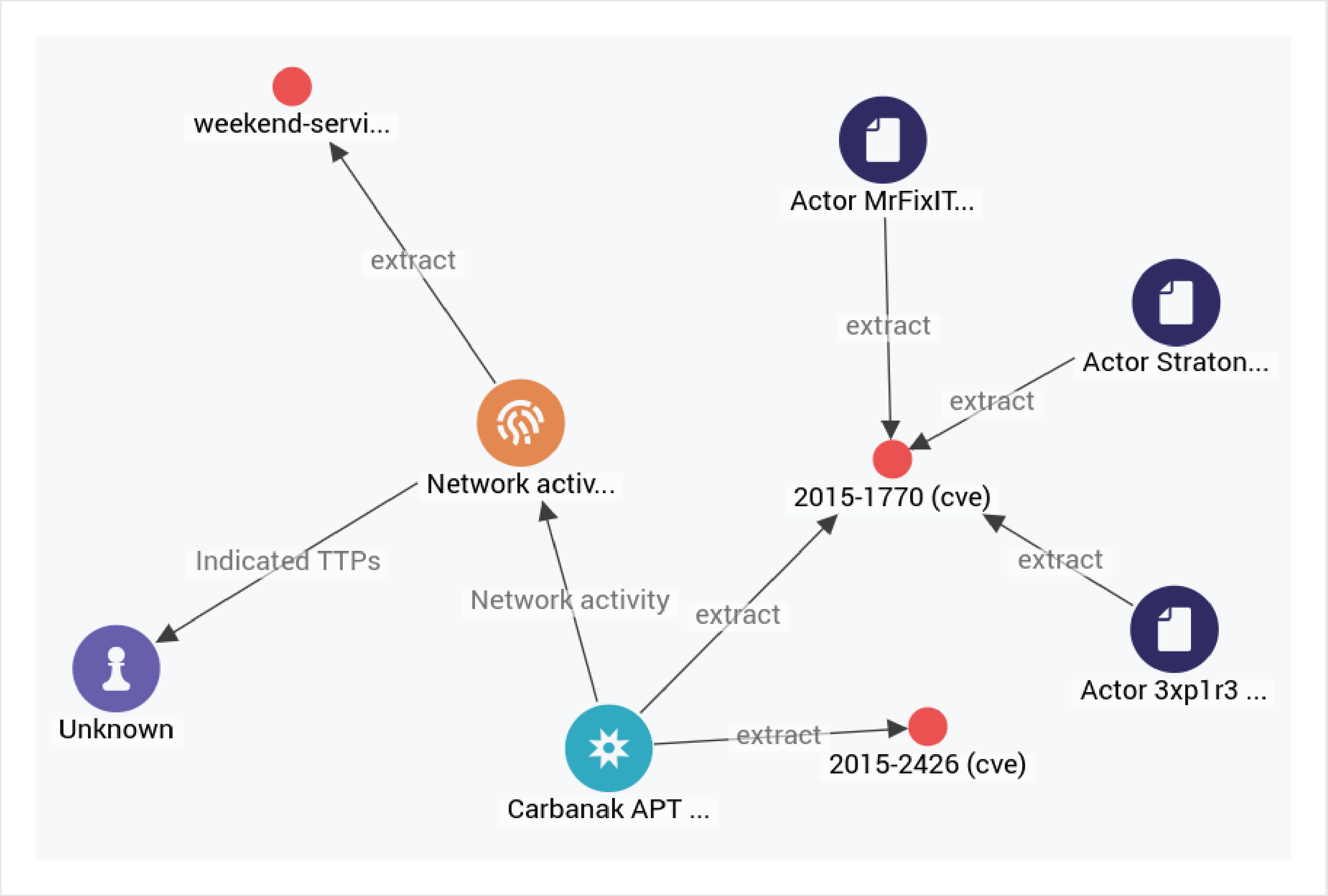
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

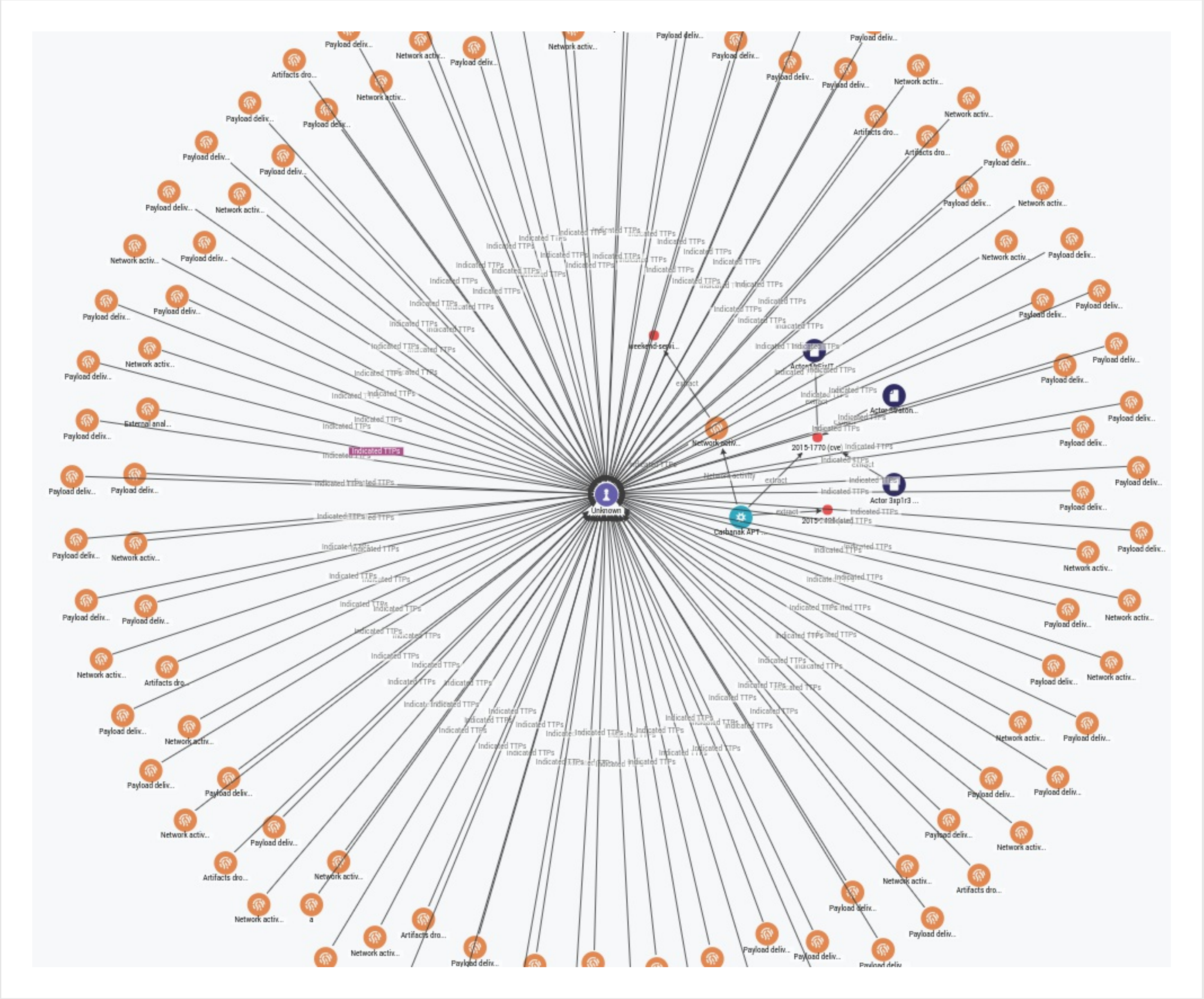


☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

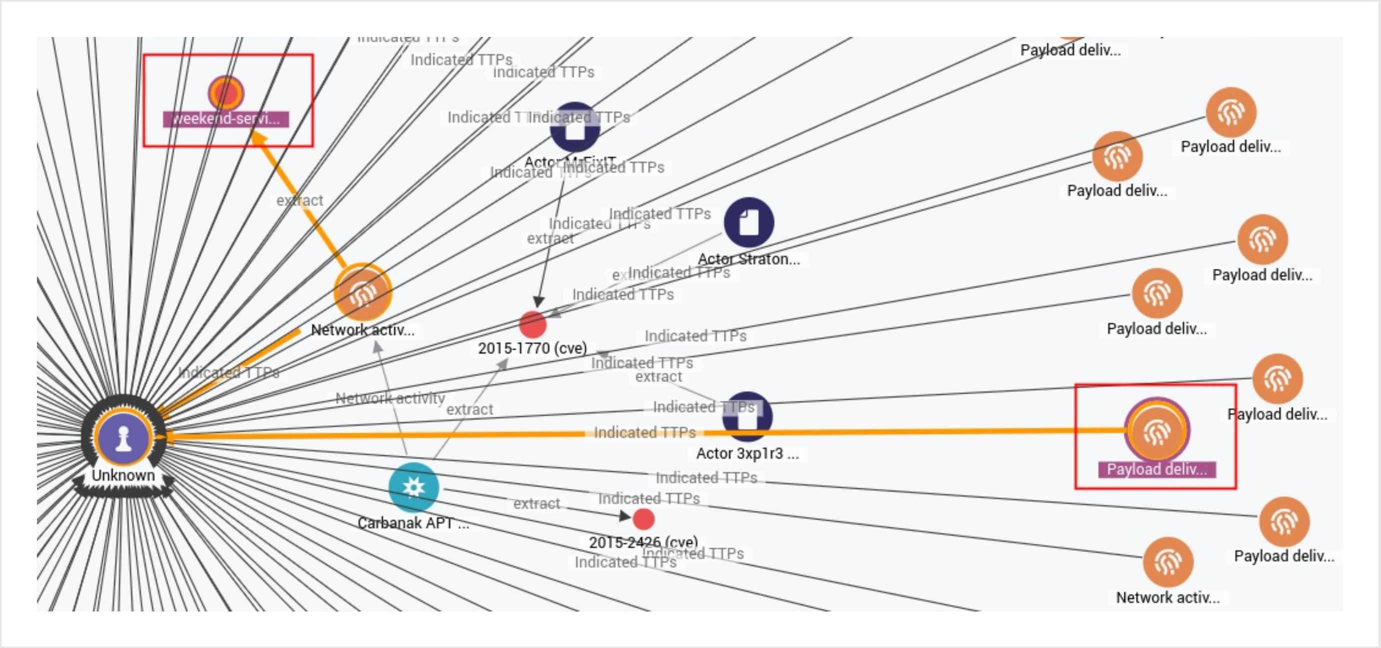


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



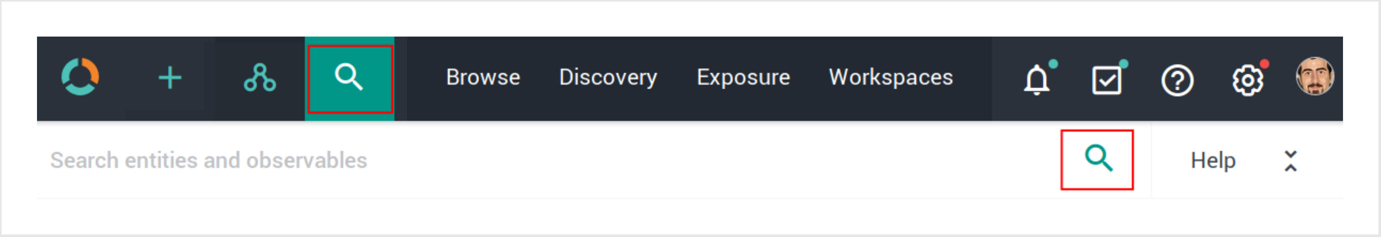
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

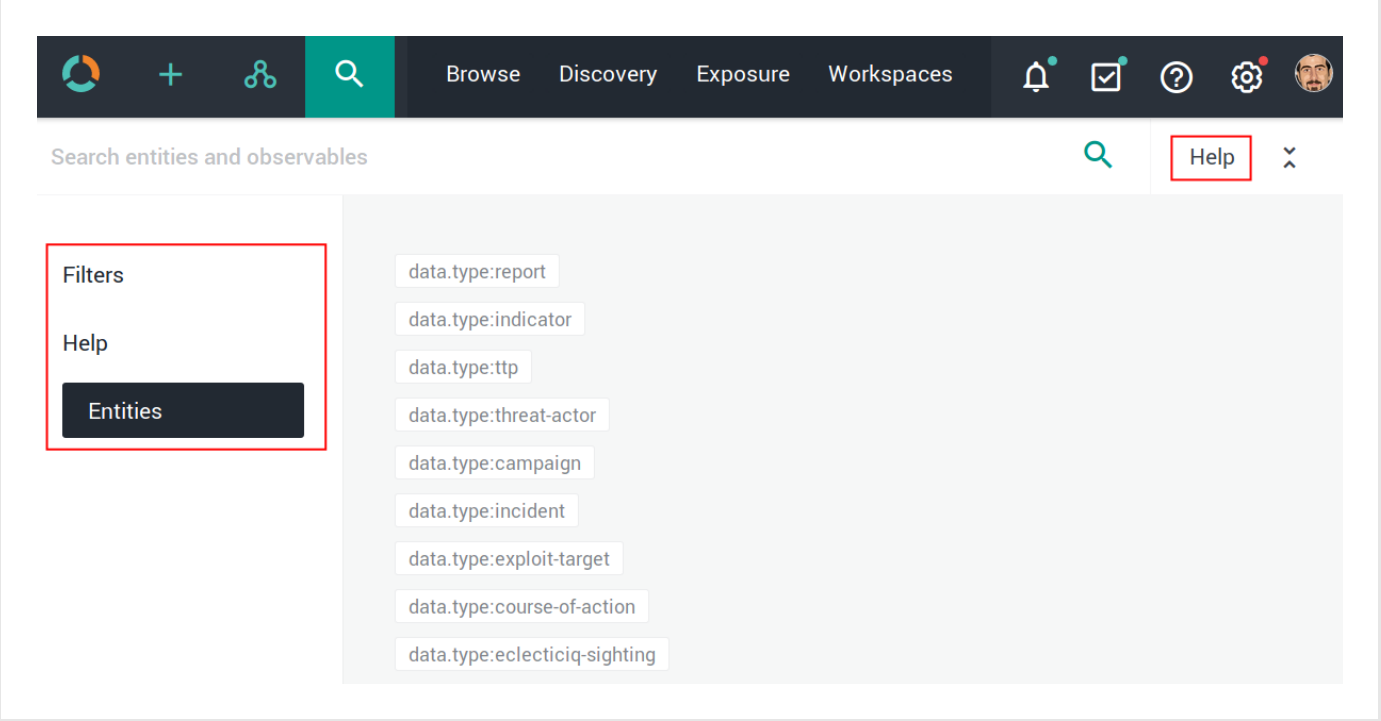


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

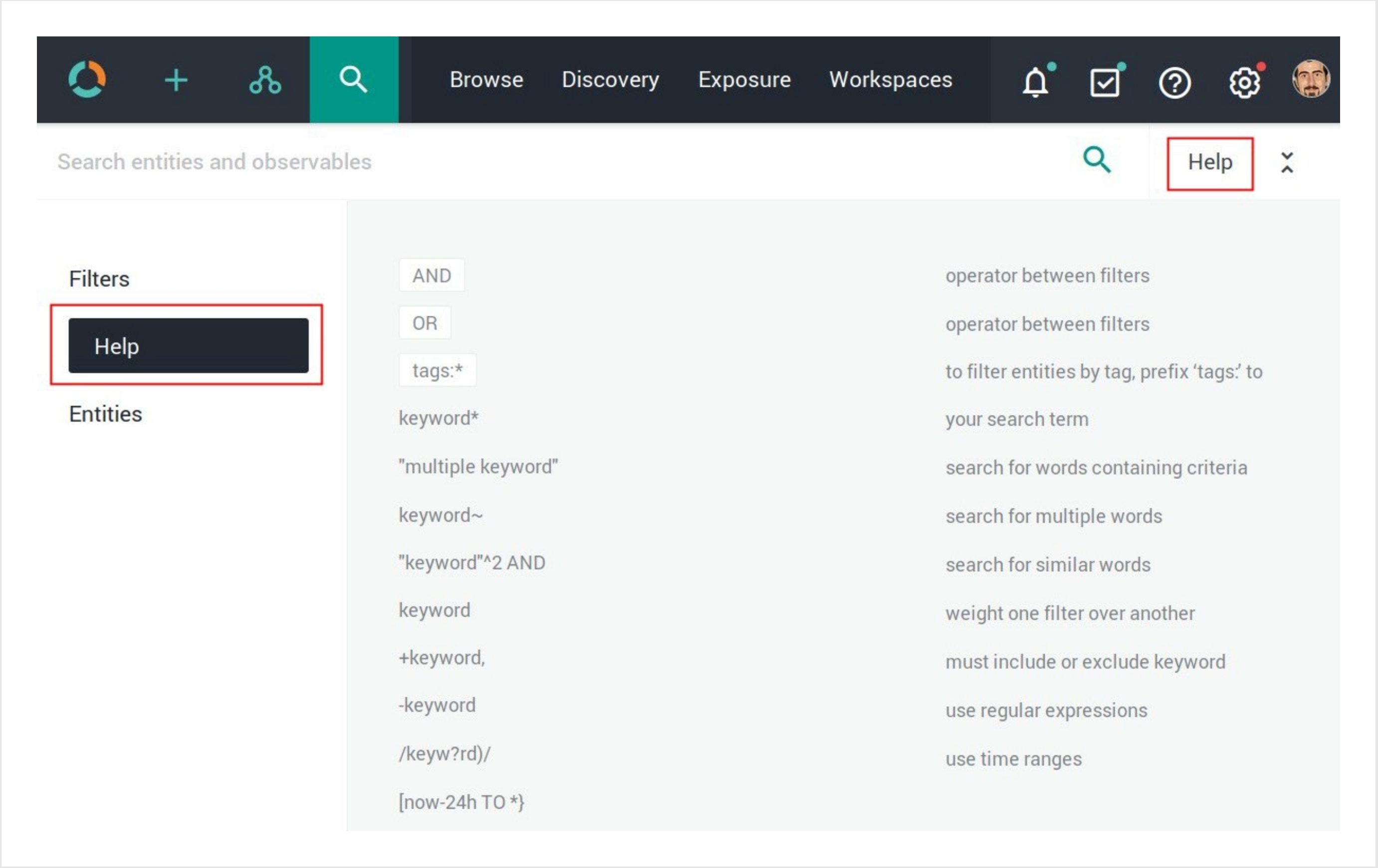
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

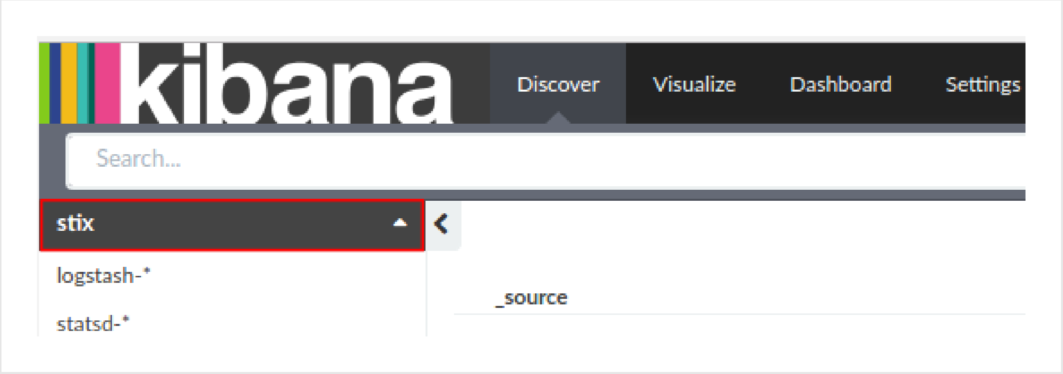
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

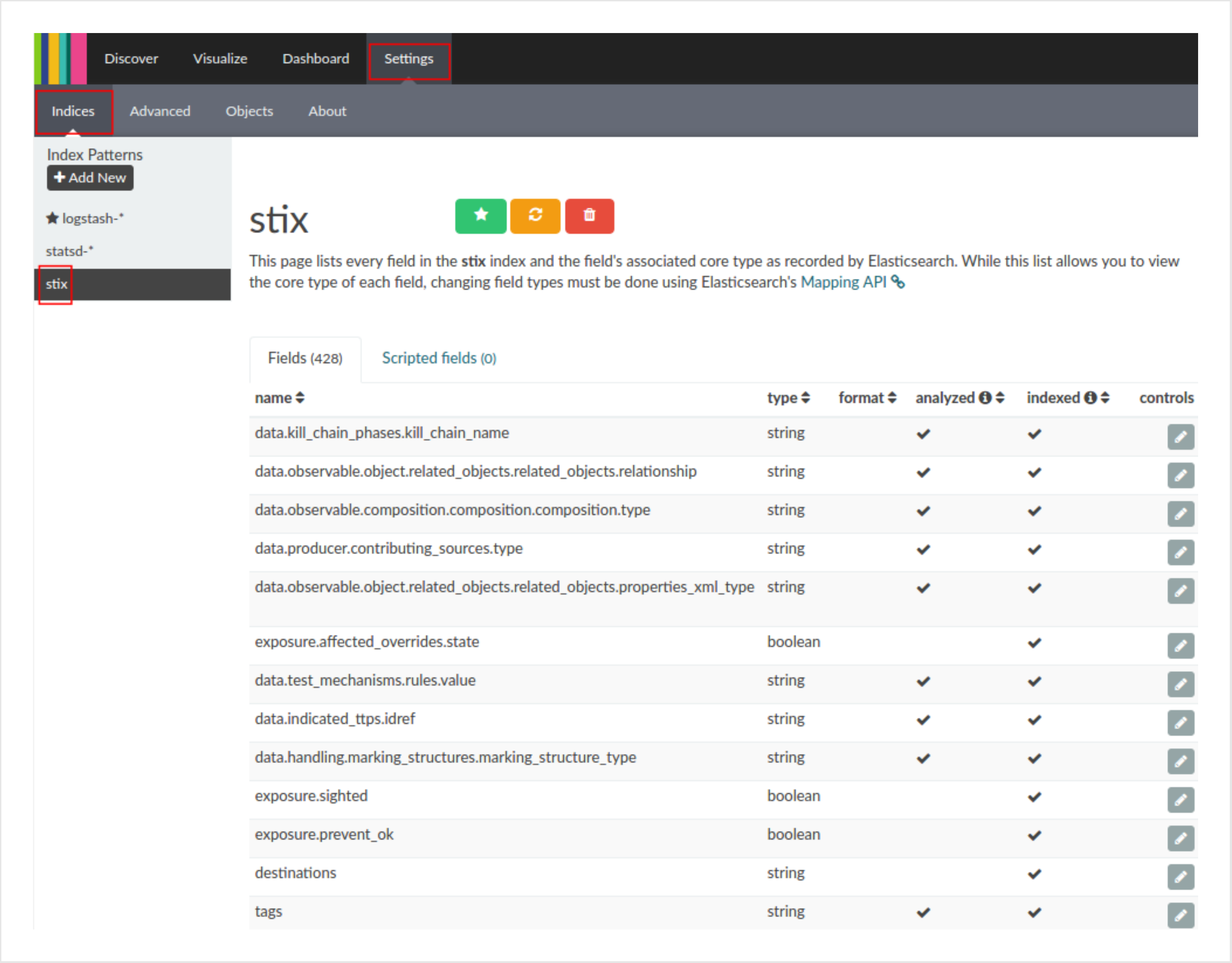
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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

Fields (428) Scripted fields (0)

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		✓	✓	✎

How to work with the DomainTools Retrieve Parsed Whois Observables enricher

The DomainTools Retrieve Parsed Whois Observables enricher returns malicious domain names related to the same primary and/or secondary name servers.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the DomainTools Retrieve Parsed Whois Observables enricher

This article describes how to configure the DomainTools Retrieve Parsed Whois Observables enricher parameters. To configure the general options for the DomainTools Retrieve Parsed Whois Observables enricher, see Configure enrichers.

DomainTools Retrieve Parsed Whois Observables	**enricher**
Enricher name	DomainTools Retrieve Parsed Whois Observables
API endpoint	`http://api.domaintools.com/v1/{}/whois/parsed`
Input	domain, host, ipv4
Output	Enriches the supported observable types with structured Whois information.
Description	Enriches domains, hosts, and IP addresses with Whois information. The JSON output includes the most recent Whois record for the requested domain or IP range, as well as parsed, structured data such as registrant, registrar, contacts, and so on. It helps searching for, indexing, and cross-referencing data in a set of Whois records.

Configure the DomainTools Retrieve Parsed Whois Observables enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.

- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the DomainTools Retrieve Parsed Whois Observables enricher:

- **API user name**: sign up and subscribe to the service to obtain the required API user name and API key credentials to access the API endpoint exposing the service.
- **API key**: contact DomainTools to receive an API key, and then enter it in the corresponding input field.
- 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 **✚ > Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **✚ Add** or **✚ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.

- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **✚ Add** or **✚ More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

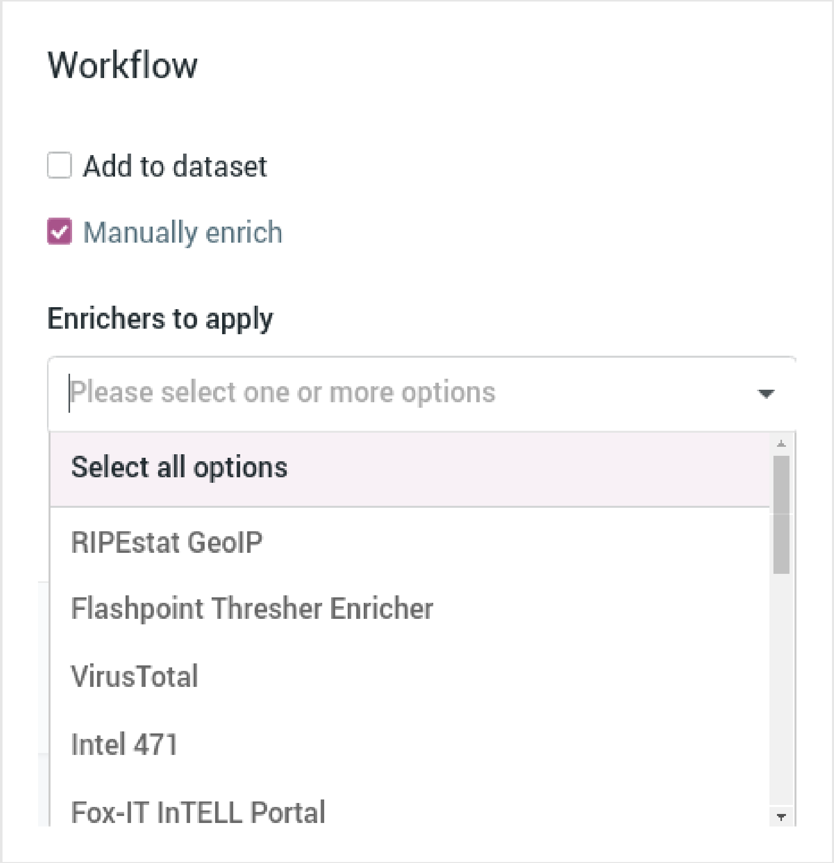
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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

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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

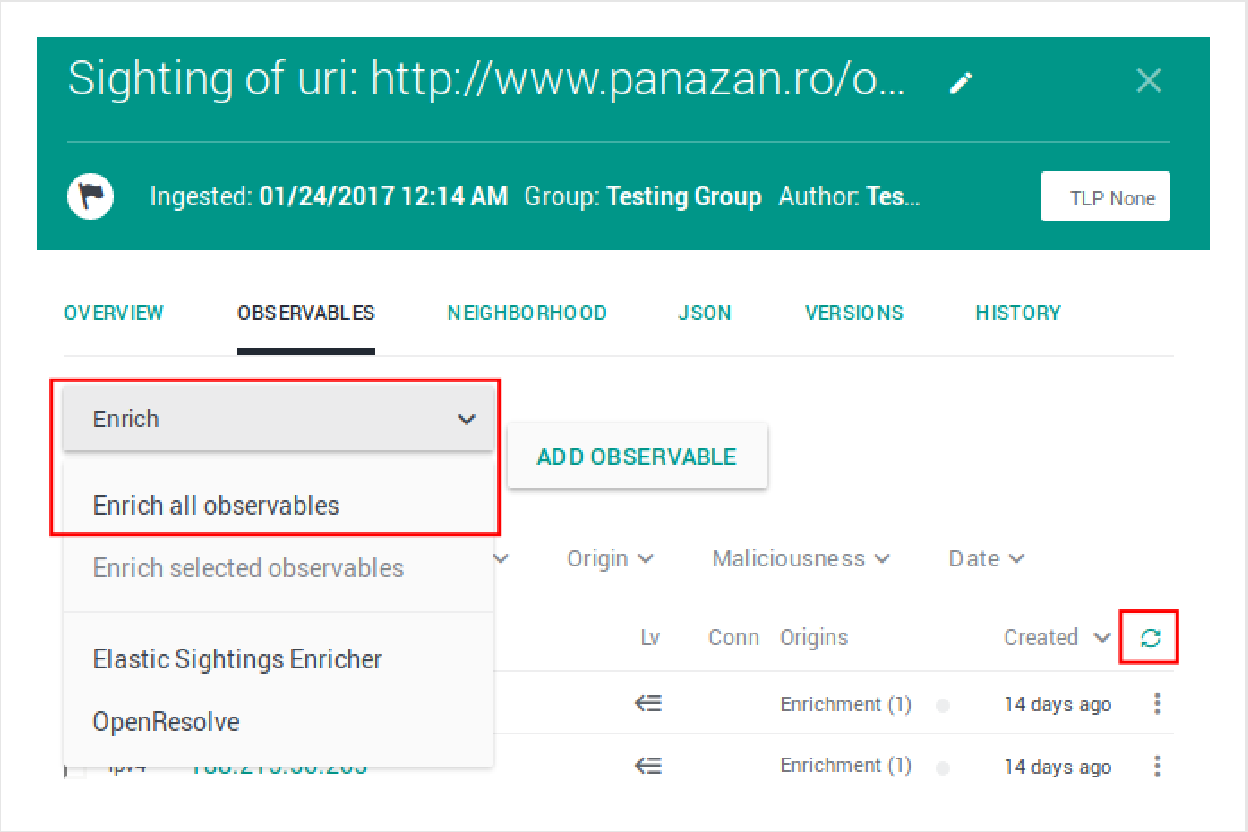
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the ⟳ refresh icon to trigger a task run that polls all the enrichers configured for the entity.

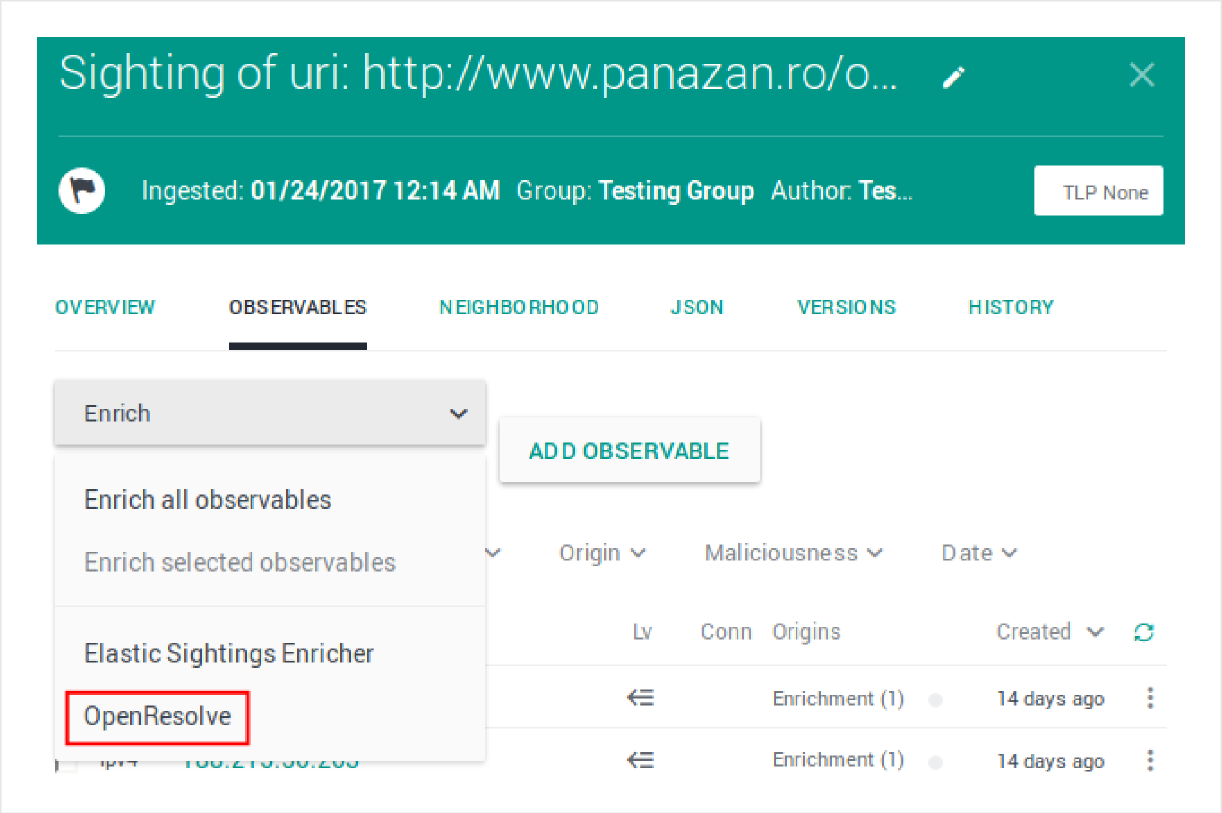
Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



To poll a specific enricher:

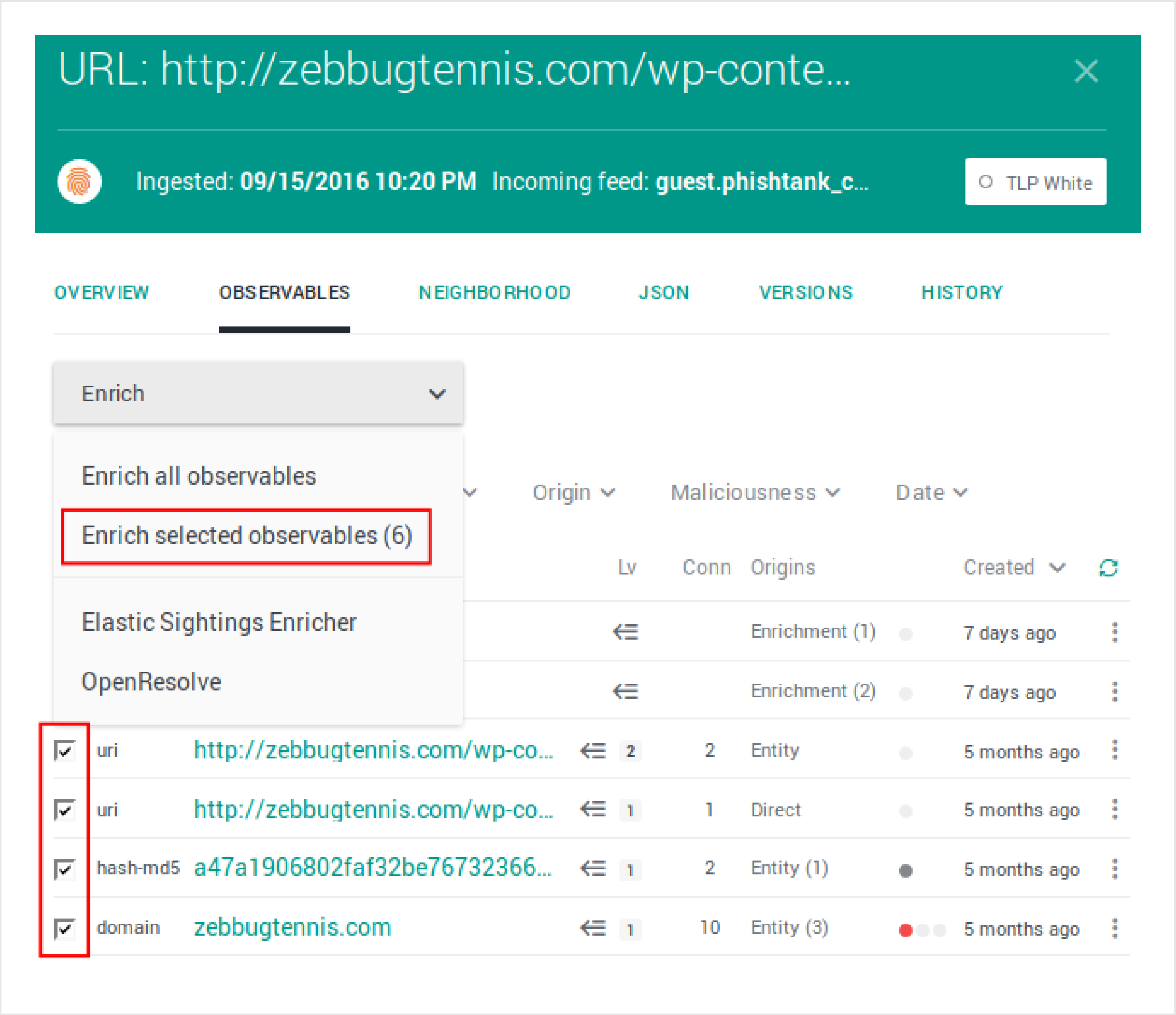
- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.


URL: http://zebbugtennis.com/wp-conte...
×
Ingested: 09/15/2016 10:20 PM
Incoming feed: guest.phishtank_c...
TLP White
OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY
Enrich
Enrich all observables
Enrich selected observables (6)
Elastic Sightings Enricher
OpenResolve
Origin
Maliciousness
Date

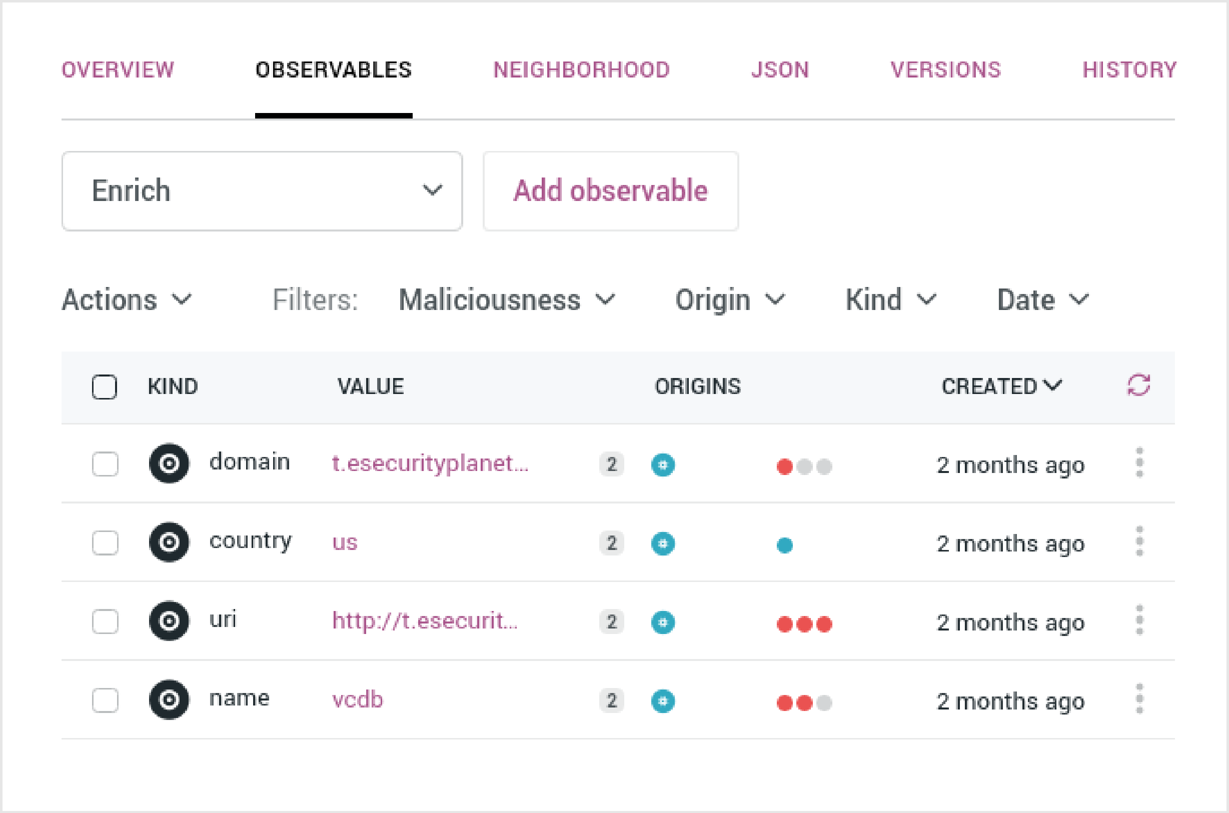
			Lv	Conn	Origins		Created
			⇚		Enrichment (1)	○	7 days ago
			⇚		Enrichment (2)	○	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	⇚ 2	2	Entity	○	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	⇚ 1	1	Direct	○	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	⇚ 1	2	Entity (1)	●	5 months ago
☑	domain	zebbugtennis.com	⇚ 1	10	Entity (3)	●○○	5 months ago

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

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.

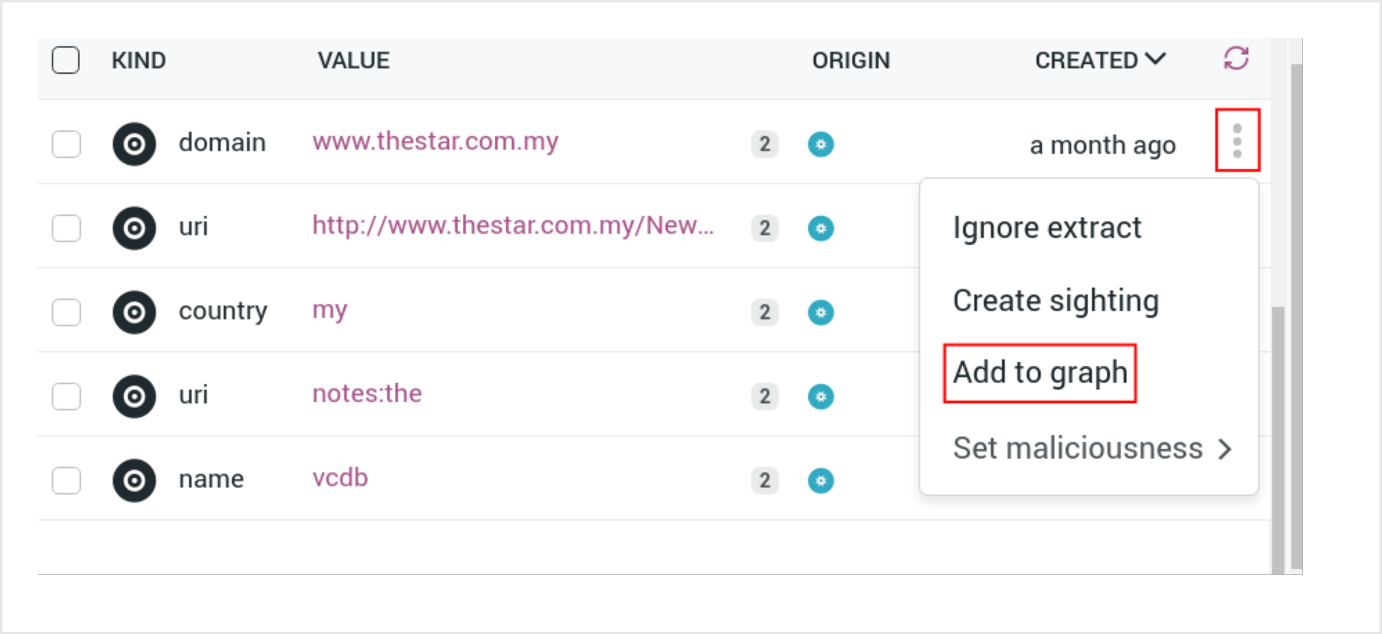


☐	KIND	VALUE		ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●	●●●	2 months ago
☐	country	us	2	●	●	2 months ago
☐	uri	http://t.esecurit...	2	●	●●●	2 months ago
☐	name	vcdb	2	●	●●●	2 months ago

Review enrichment observables on the graph

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

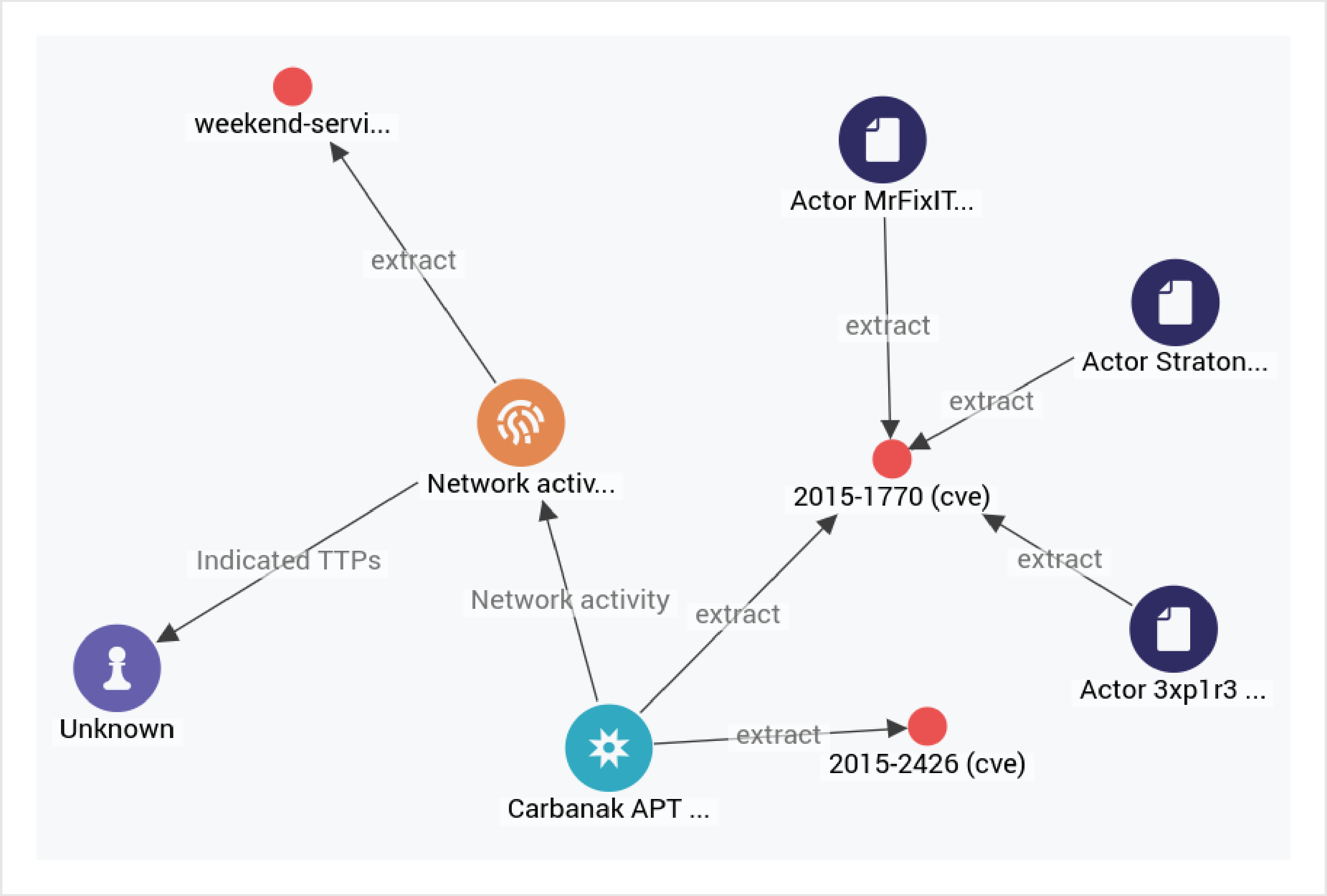
- On the row corresponding to the observable you want to load onto the graph, click the ⋮ icon, and then select **Add to graph**.



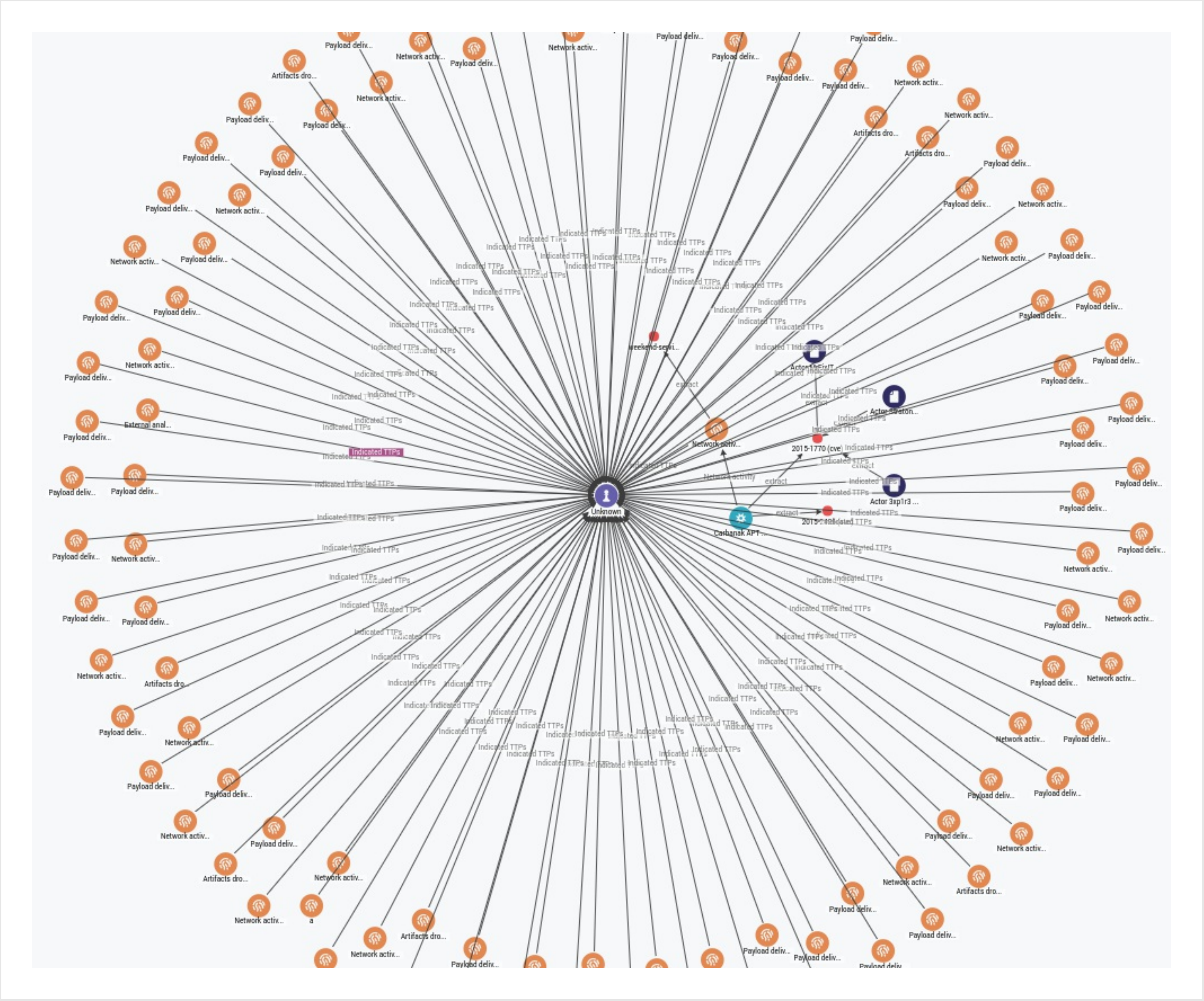
☐	KIND	VALUE		ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	●	a month ago
☐	uri	http://www.thestar.com.my/New...	2	●	
☐	country	my	2	●	
☐	uri	notes:the	2	●	
☐	name	vcdb	2	●	

- 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**.

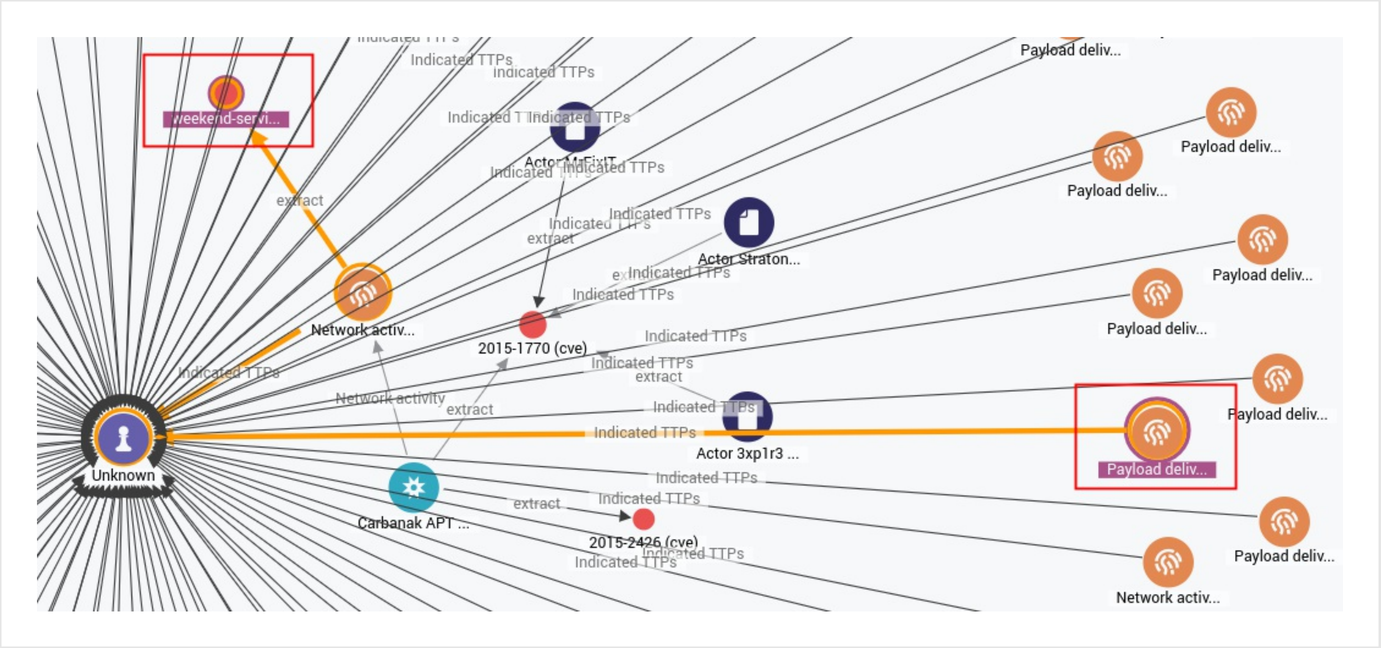


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



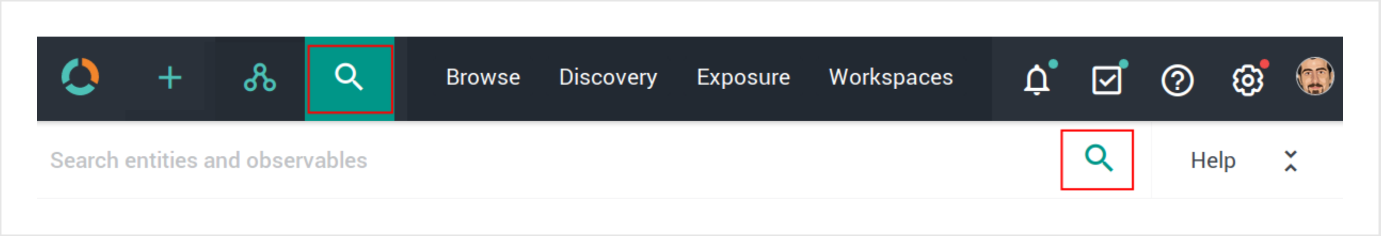
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

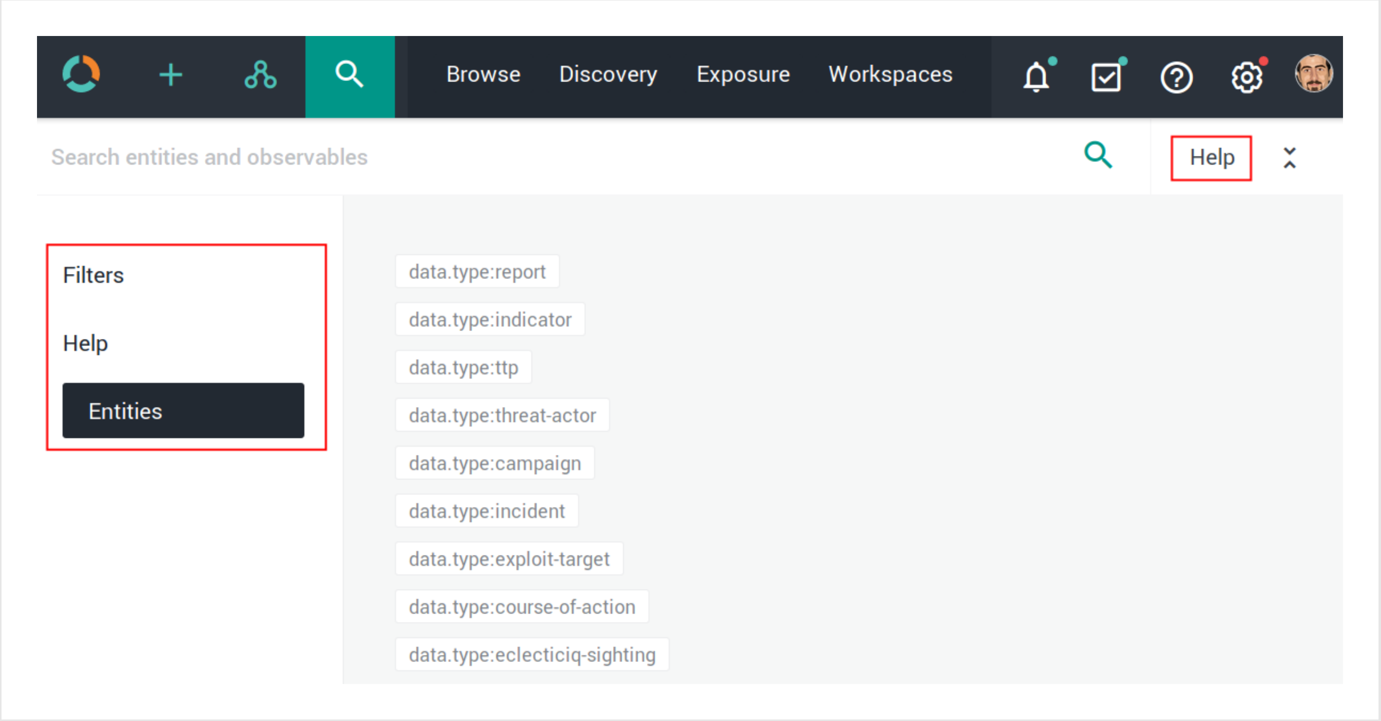


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

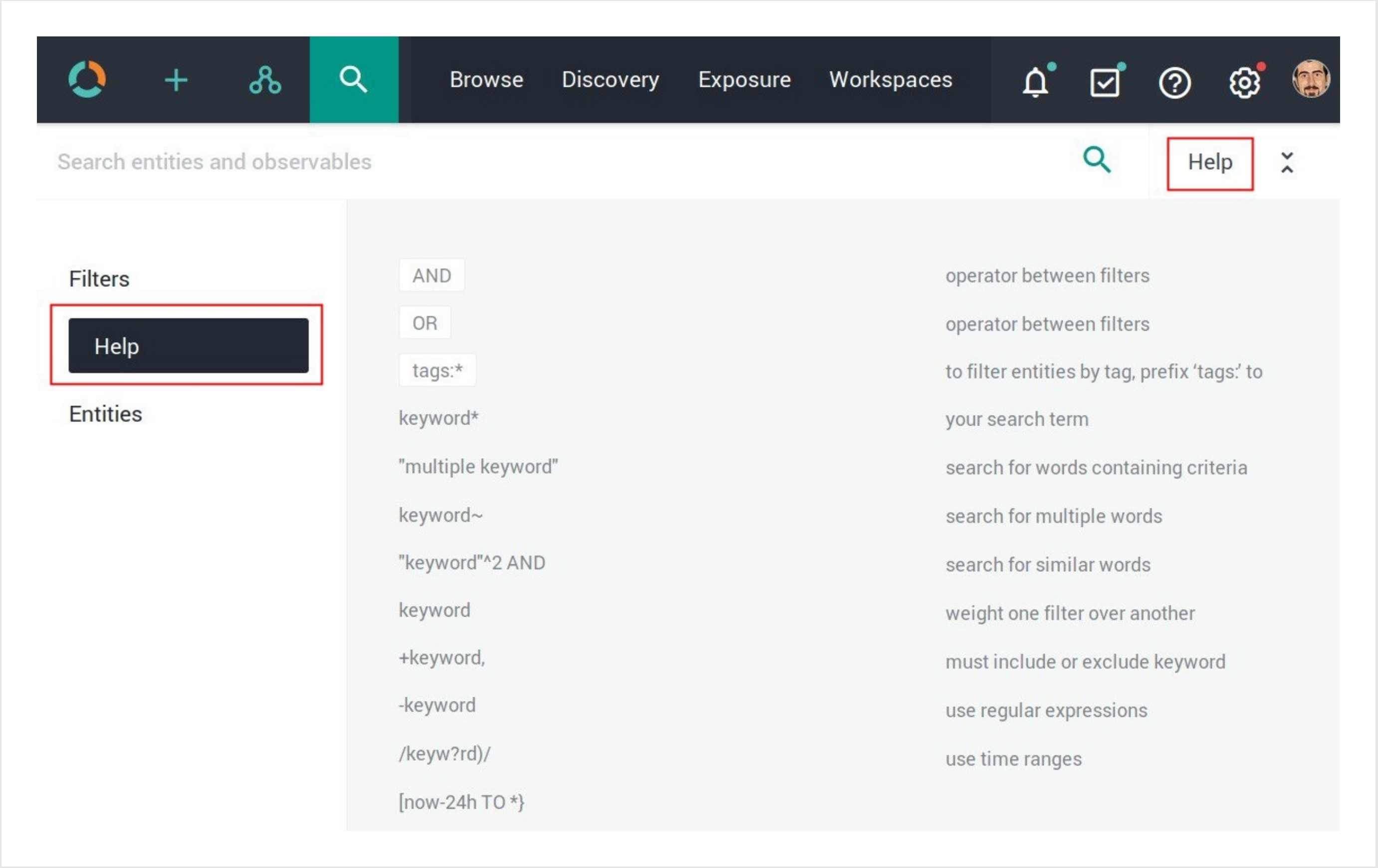
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

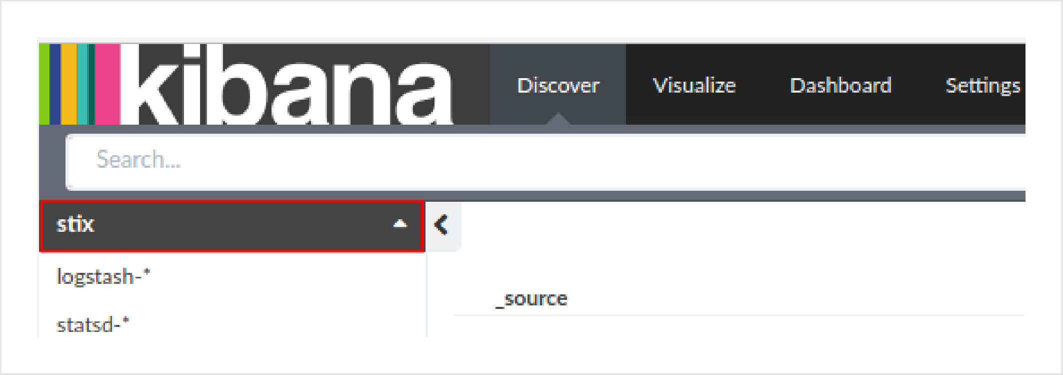
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

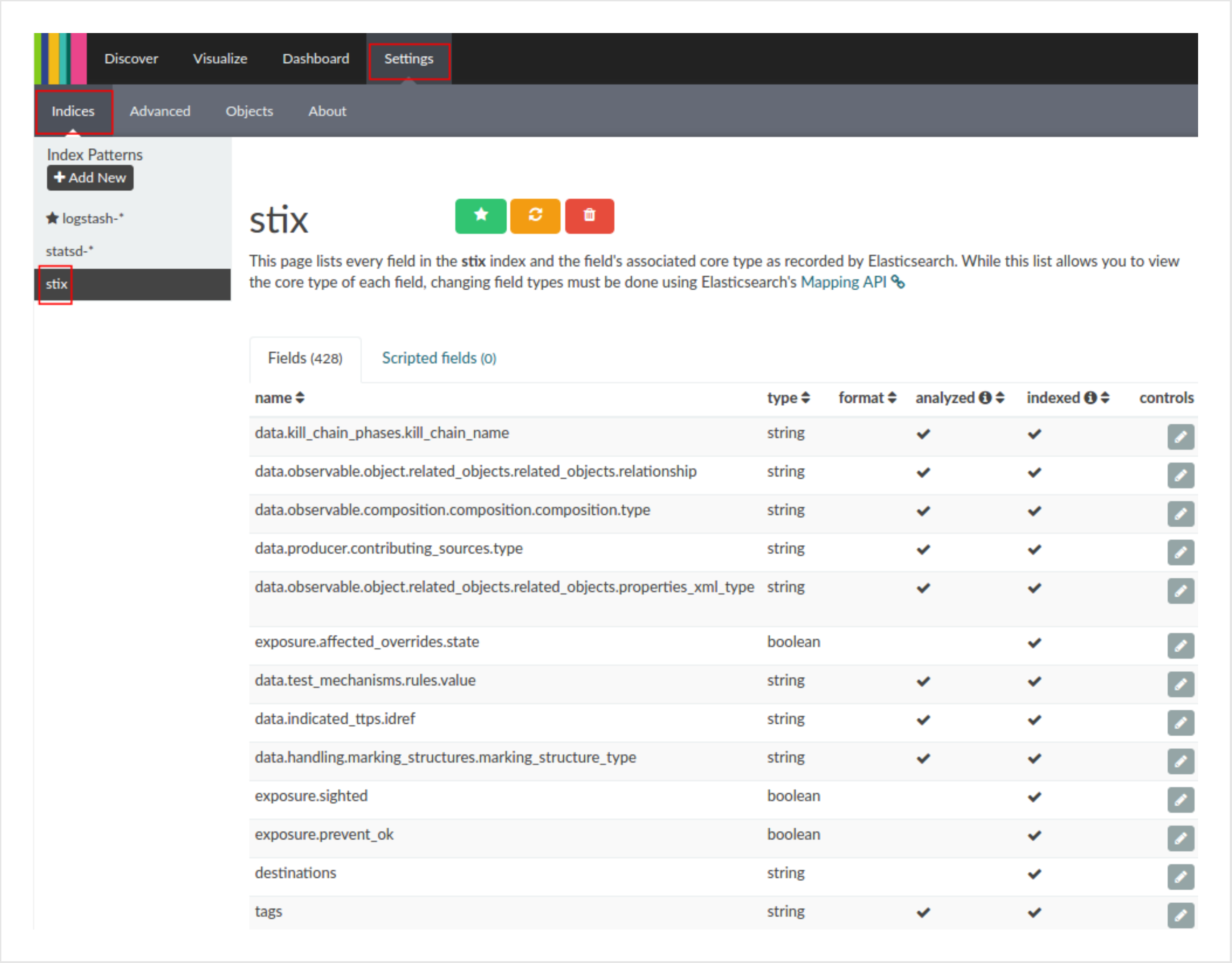
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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		✓	✓	✎

How to work with the DomainTools Suspicious Domains enricher

The DomainTools Suspicious Domains enricher returns suspicious and potentially malicious domains related to the input IP addesses, along with their risk scores to automatically flag domains with an appropriate maliciousness confidence level.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Work with the DomainTools Suspicious Domains enricher

This article describes how to configure the DomainTools Suspicious Domains enricher parameters.
To configure the general options for the DomainTools Suspicious Domains enricher, see Configure enrichers.

DomainTools Suspicious Domains	**enricher**
Enricher name	DomainTools Suspicious Domains
API endpoint	`https://api.domaintools.com/v1/{}/host-domains`
Input	ipv4
Output	Enriches the supported observable types with suspicious domain and host name information.
Description	Enriches IPv4 observables with suspicious domains related to the input IP addresses. It includes configurable thresholds to assign maliciousness confidence levels to the processed IP addresses, and to ignore non-malicious IPs.

Configure the DomainTools Suspicious Domains enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment.**
- Click the enricher you want to configure or modify.

- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the DomainTools Suspicious Domains enricher:

- **API user name**: sign up and subscribe to the service to obtain the required API user name and API key credentials to access the API endpoint exposing the service.
- **API key**: contact DomainTools to receive an API key, and then enter it in the corresponding input field.
- **Low maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - Low confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *low maliciousness threshold* and lower than the medium and high maliciousness thresholds are flagged with **Malicious - Low confidence**.
  - Enter a value between *0* and *99.99*.
  - Default value: *10*.
- **Medium maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - Medium confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *medium maliciousness threshold* and lower than the high maliciousness threshold are flagged with **Malicious - Medium confidence**.
  - Enter a value between *0* and *99.99*.
  - Default value: *40*.
- **High maliciousness threshold**: domain and host names with a higher DomainTools risk score than the value defined here are flagged with **Malicious - High confidence**.
  After completing the analysis, enriched domain and host names with a *higher* risk score than the *high maliciousness threshold* are flagged with **Malicious - High confidence**.
  - Enter a value between *0* and *99.99*.
  - Default value: *80*.
- **Ignore non-malicious domains**: select this checkbox to to exclude from ingestion any domains whose reputation/risk score value is lower than the specified *low maliciousness threshold*.
- 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 **+** > **Rules** > **Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **+ Add** or **+ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **+ Add** or **+ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

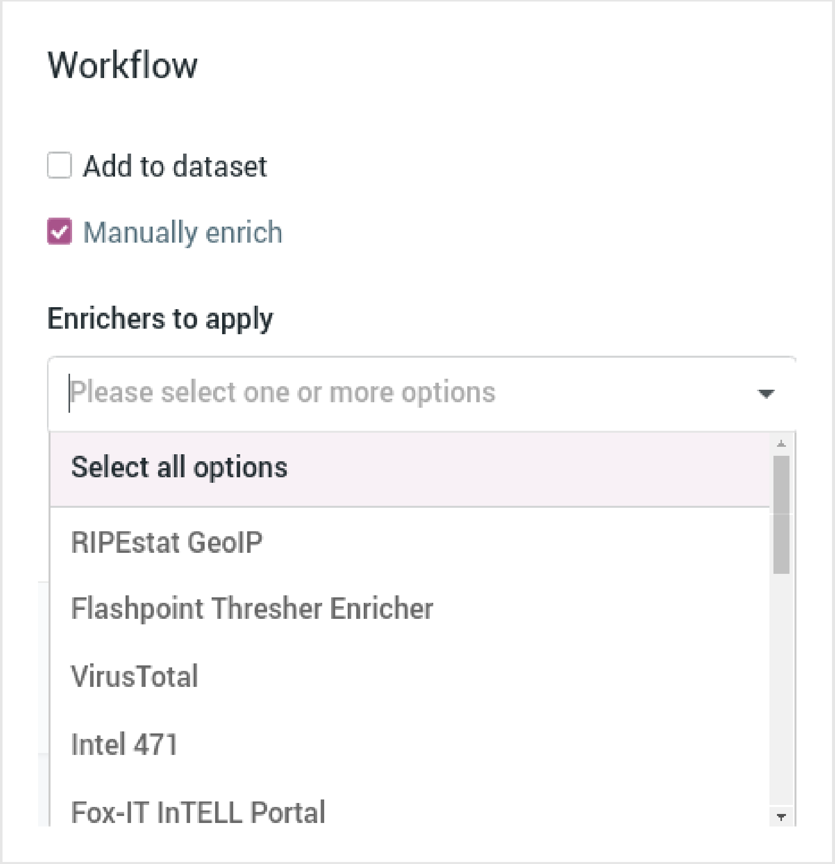
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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

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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

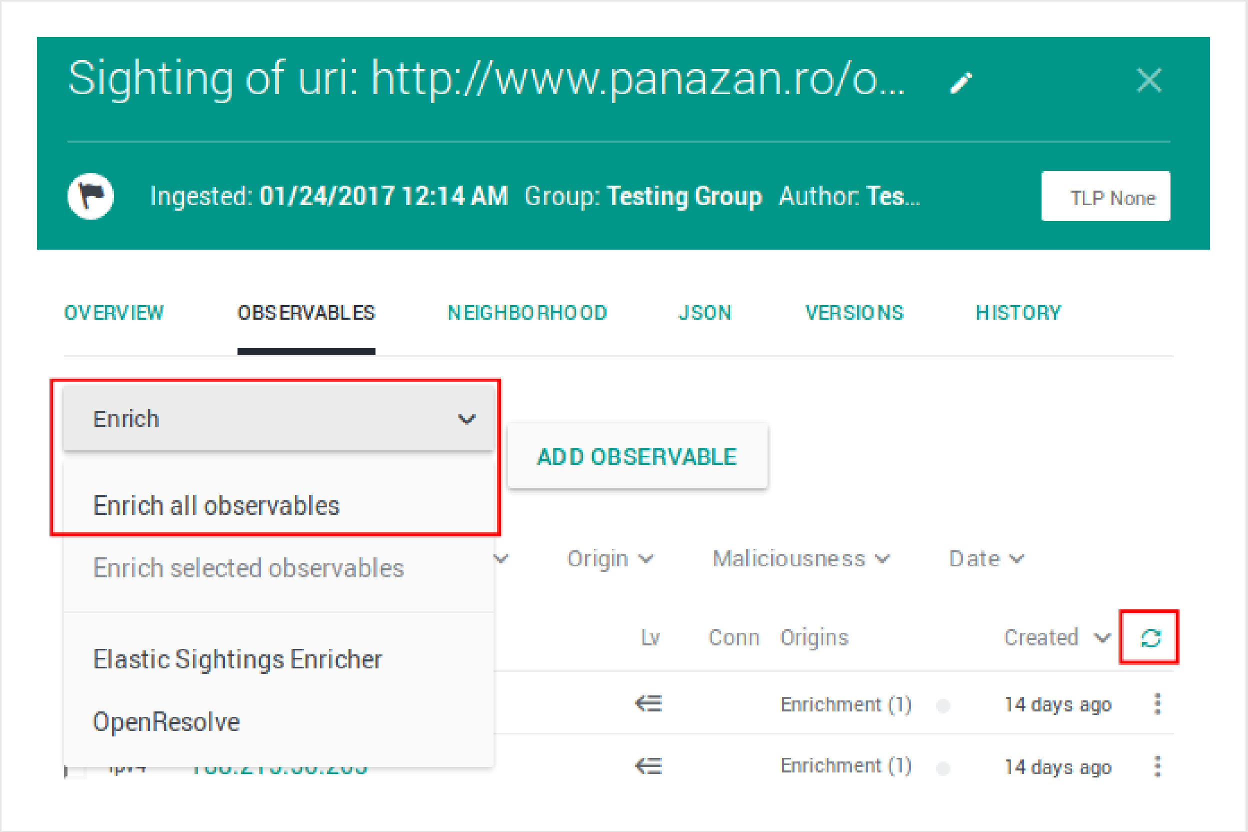
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the 🗘 refresh icon to trigger a task run that polls all the enrichers configured for the entity.

Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.

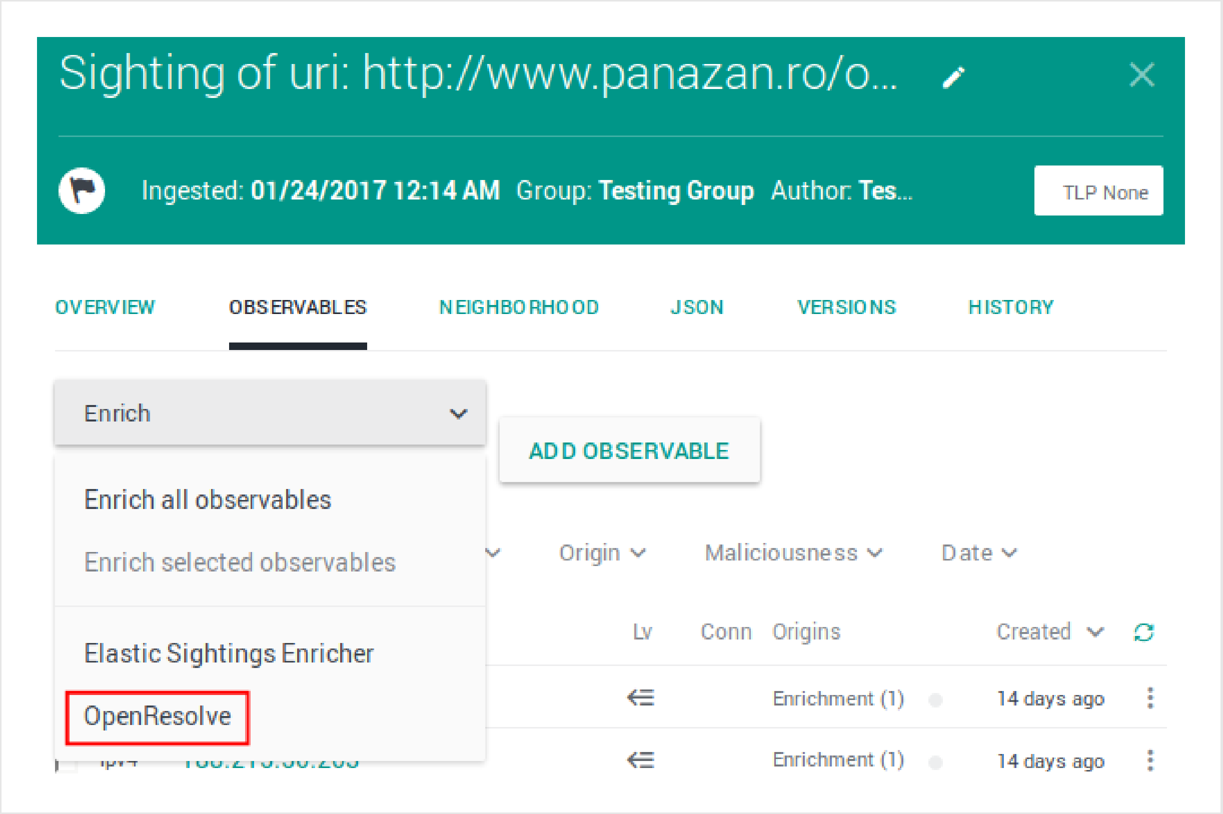


Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

To poll a specific enricher:

- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



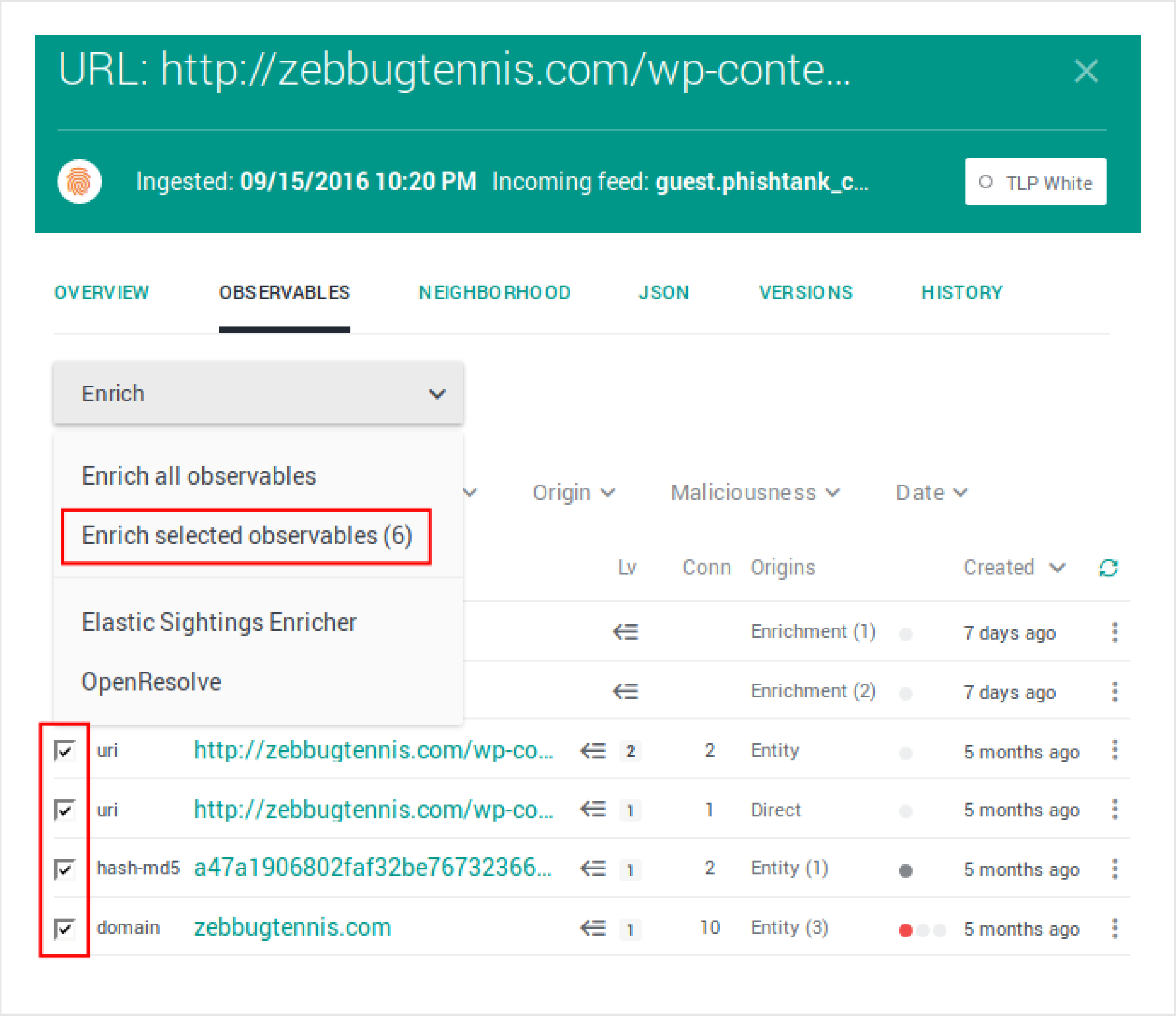
Sighting of uri: http://www.panazan.ro/o...

Ingested: **01/24/2017 12:14 AM** Group: **Testing Group** Author: **Tes...**

To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.


URL: http://zebbugtennis.com/wp-conte...
Ingested: 09/15/2016 10:20 PM
Incoming feed: guest.phishtank_c...
○ TLP White
OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY
Enrich
Enrich all observables
Enrich selected observables (6)
Elastic Sightings Enricher
OpenResolve
Origin
Maliciousness
Date

			Lv	Conn	Origins		Created
			⇇		Enrichment (1)	●	7 days ago
			⇇		Enrichment (2)	●	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 2	2	Entity	●	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 1	1	Direct	●	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	⇇ 1	2	Entity (1)	●	5 months ago
☑	domain	zebbugtennis.com	⇇ 1	10	Entity (3)	●●●	5 months ago

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 DomainTools Suspicious Domains enricher can take the following observable types as input:

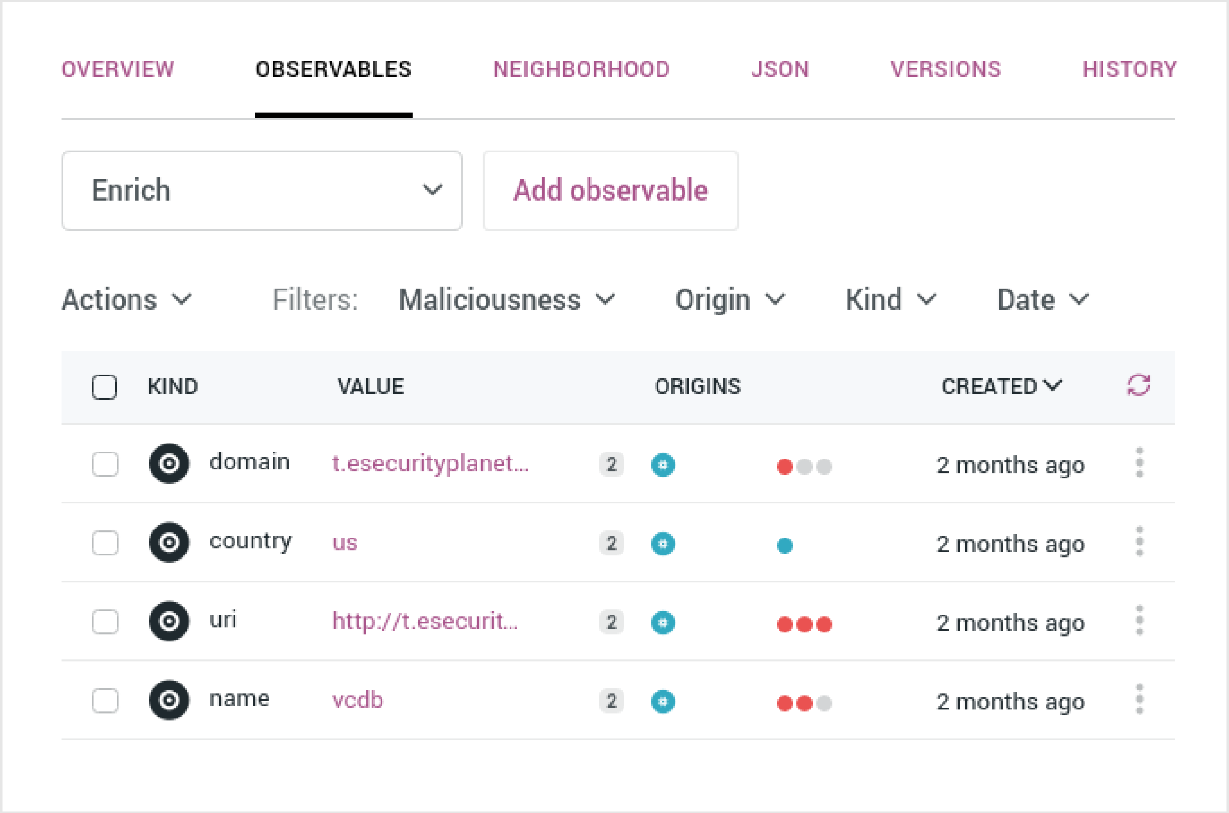
- *ipv4*

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 DomainTools Suspicious Domains.

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.

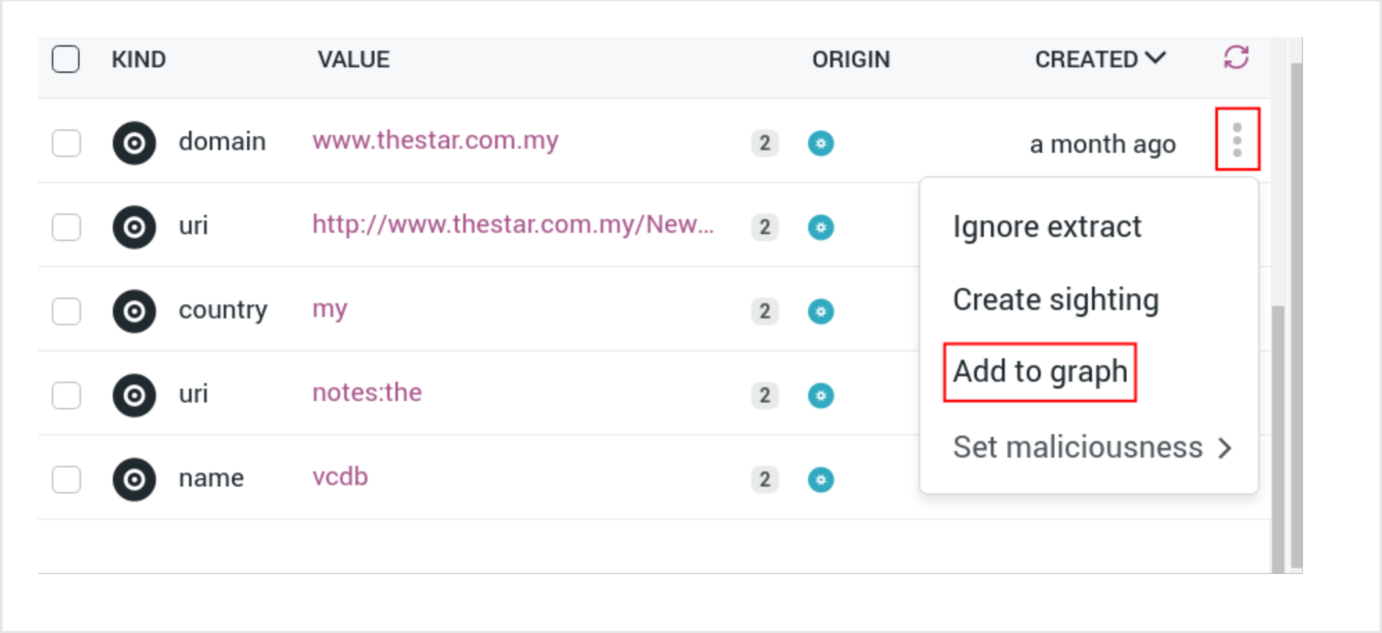


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

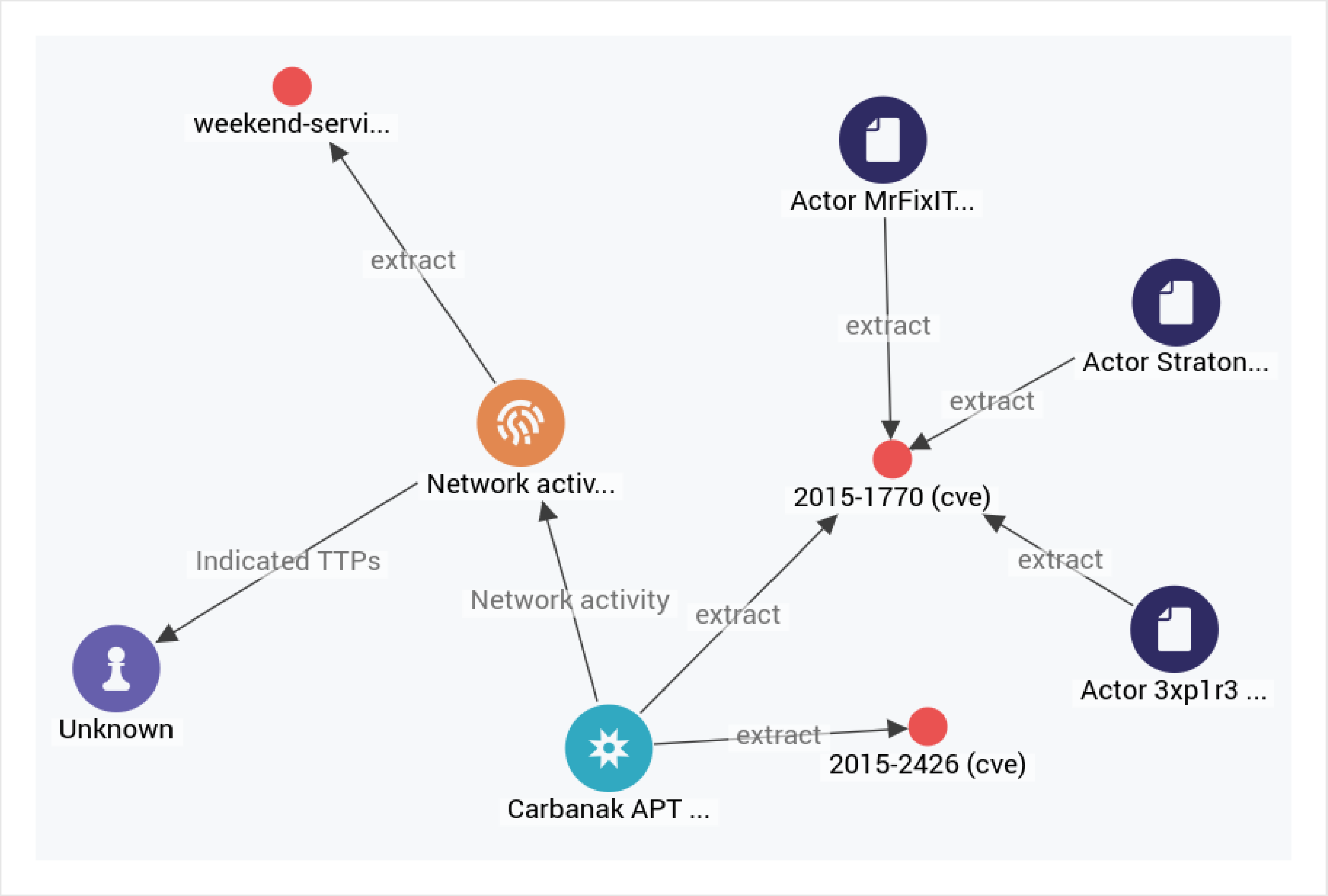
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

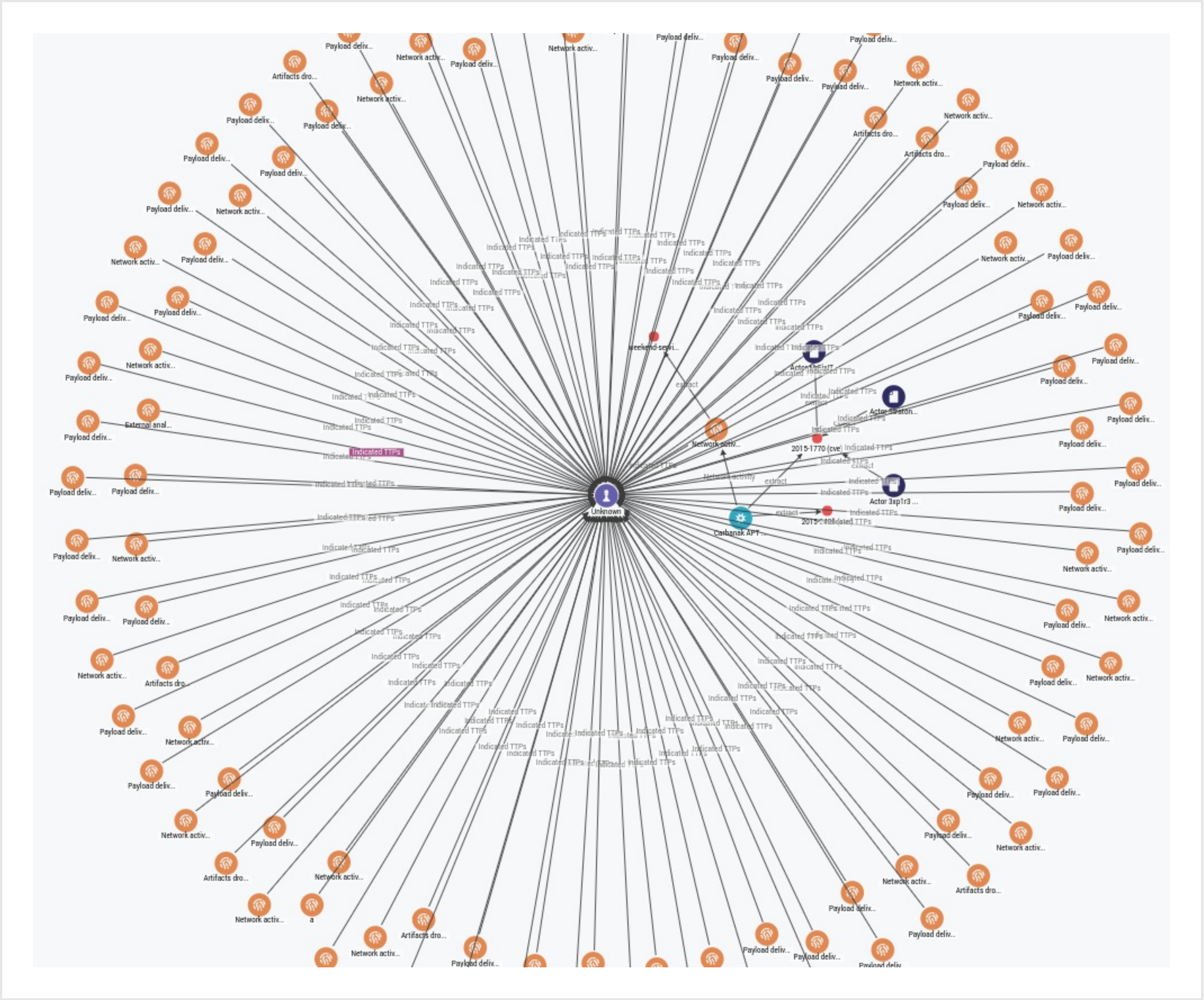


☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

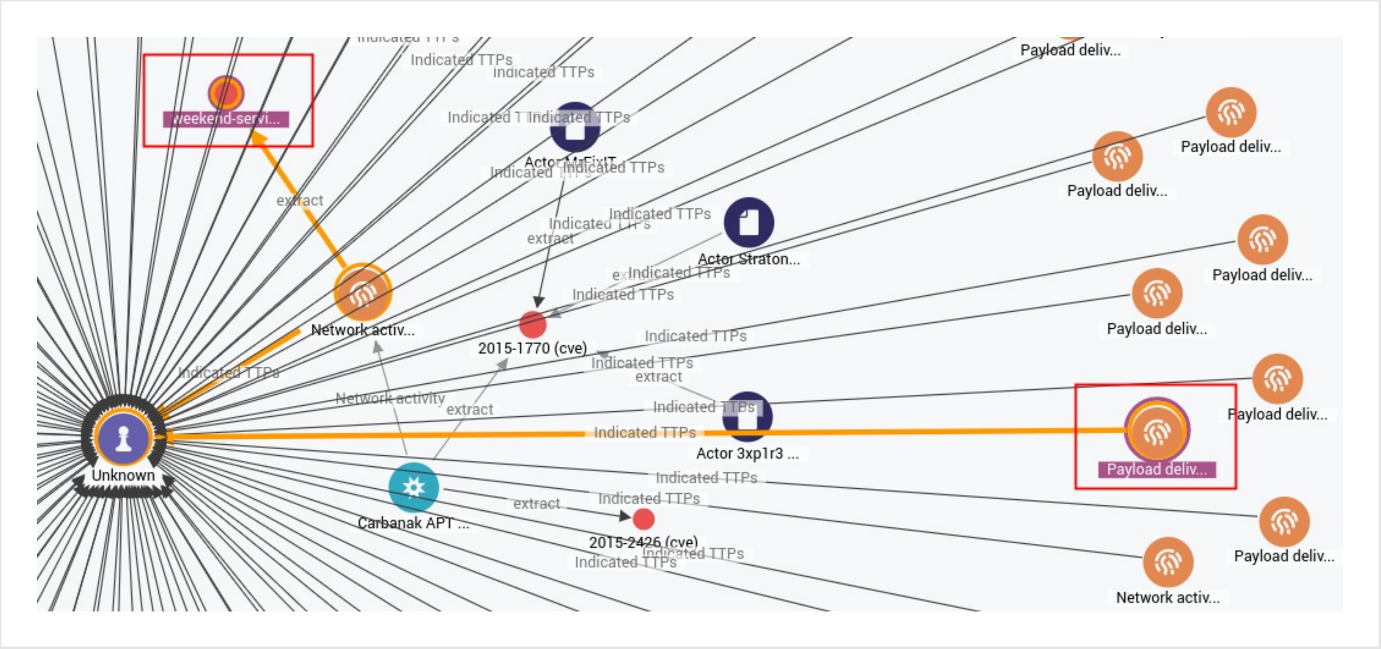


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



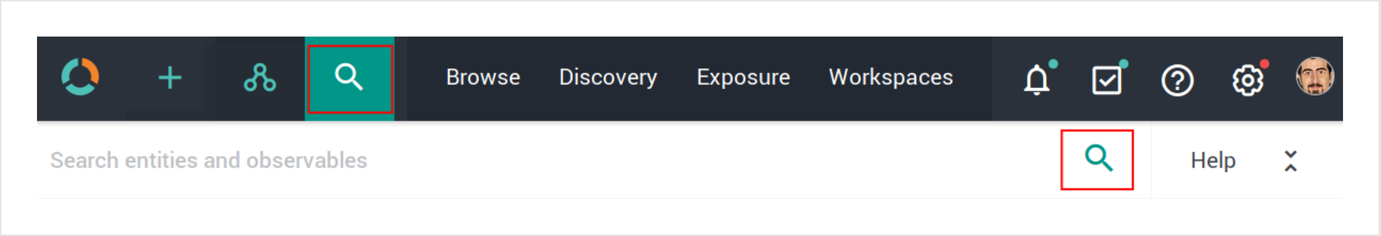
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

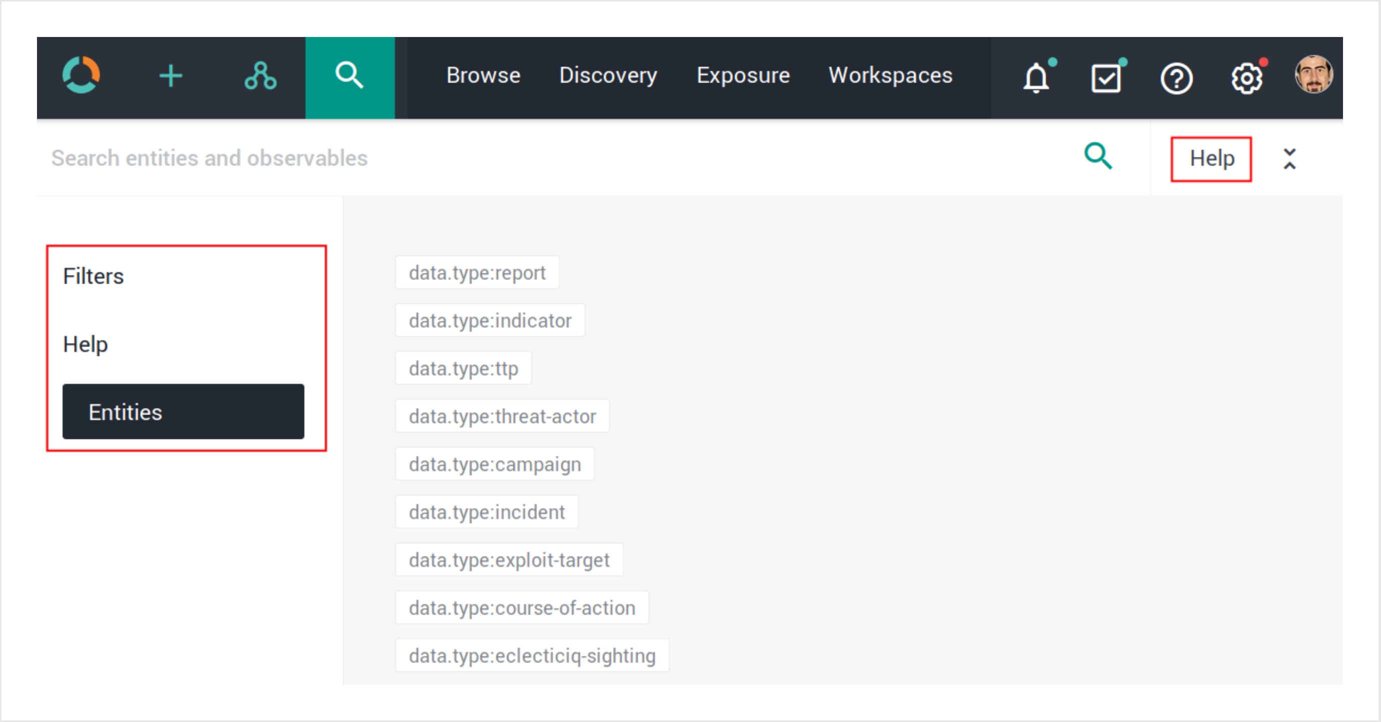


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

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

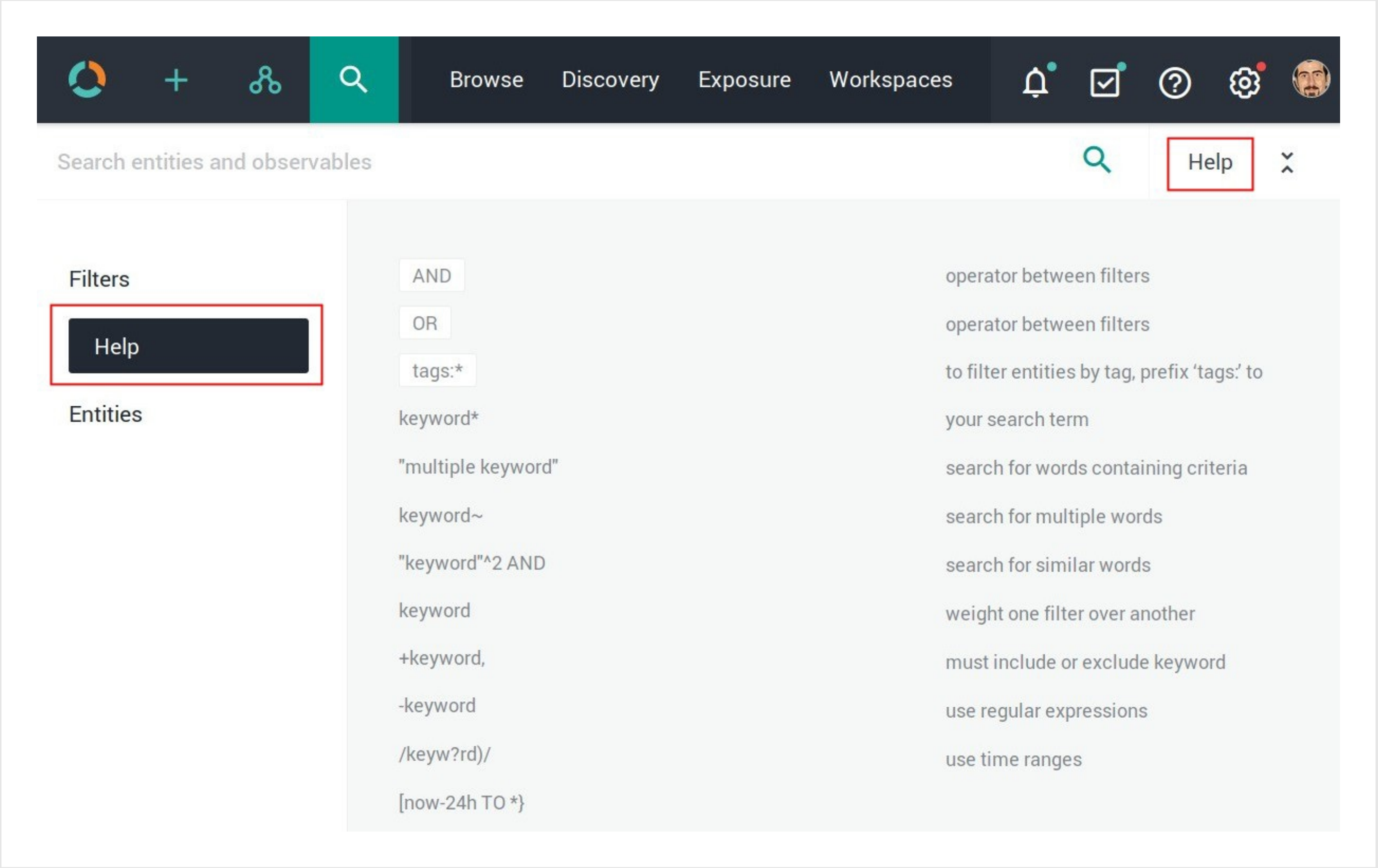
To access a cheatsheet with search examples using entity types, filters, and for help with the search syntax, click **Help** to display thematic drop-down lists with common search queries:

- **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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

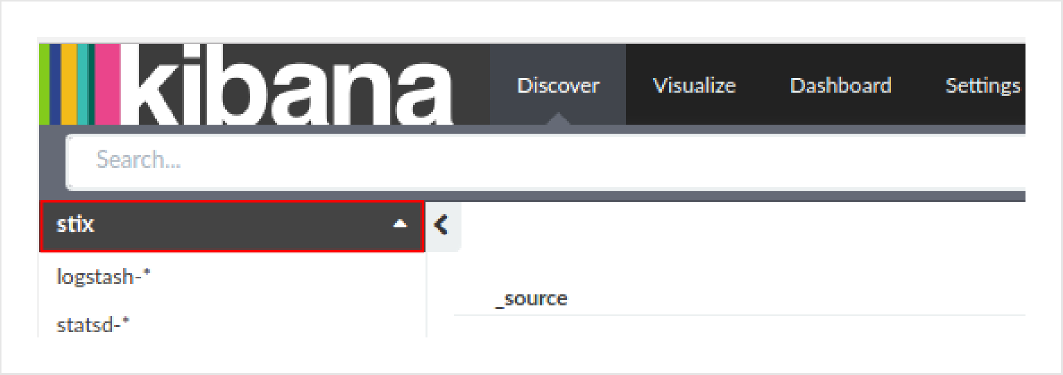
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

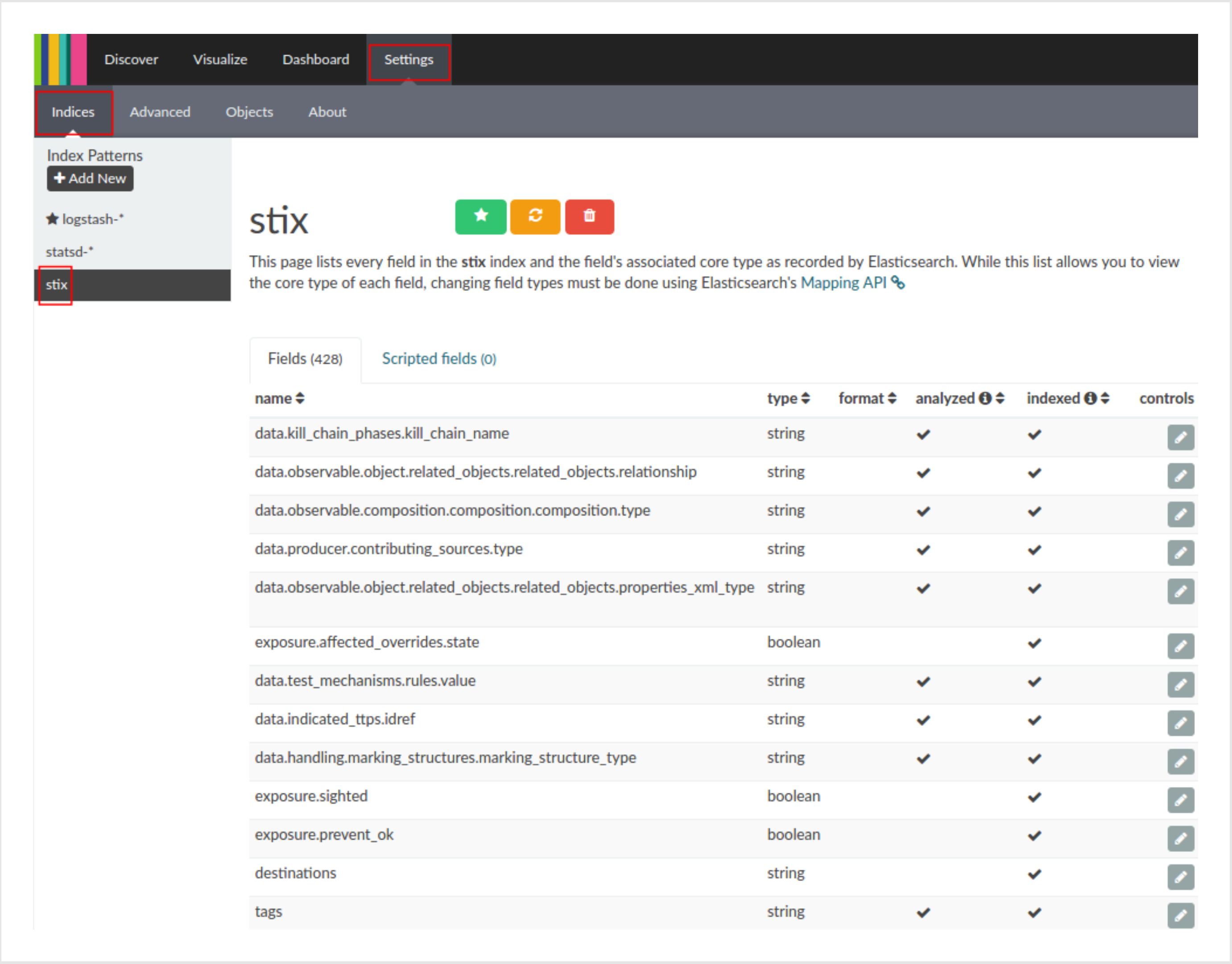
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format: `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/kibana/app/kibana#/`
- Select the **stix** index field:



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



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		✓	✓	

How to work with the Elasticsearch sightings enricher

Raw data enrichment observables improve the quality of the intelligence you obtain from external sources and use for cyber data analysis. Configure and run the Elasticsearch sightings enricher, view enrichment observables in the entity detail pane and on the graph, and search for enrichment observables using queries.

Enrichers poll external data sources to provide additional context and detail to augment — hence, enrich — the intelligence value of the entities stored in the platform.

The platform ships with several built-in, ready-to-use enrichers to obtain geolocation IP and whois details, DNS domain and malware information, as well as other relevant data to help analysts draw a sharper and more comprehensive picture of the cyber threat relationships and the cyber threat scenarios under investigation.

Enricher	API endpoint	Descri
Elasticsearch sightings	`http://<elasticsearch_url>:9200/<schema_resource>`	Searches an external Elasticsearch in search criteria are processed to auton sightings.
Fox-IT InTELL Portal	`https://cybercrime-portal.fox-it.com/`	Based on Fox-IT InTELL, the portal ga a range of sources like forums and sit suspicious activity.
Intel 471	`https://api.intel471.com/v1/`	Besides data on compromised IP add Intel 471 focuses on providing first-ha and groups.
OpenDNS OpenResolve	`http://api.openresolve.com/{}/{}`	OpenResolve by OpenDNS offers a R to retrieve reverse-DNS lookup inform
PyDat	`http://10.0.1.60:8000/ (example)`	**PyDat** `(https://github.com/mitre` locally, and it can work together with a `(https://github.com/mitrecnd/wh with-elasticsearch)` to provide who passive DNS lookup information. Anal organization, country, city, street, ZIP
RIPEstat GeoIP	`https://stat.ripe.net/data/geoloc/data.json?resource={IP_address}`	Geolocation IP information from the R **API** `(https://stat.ripe.net/docs` longitude, country, and city.
RIPEstat Whois	`https://stat.ripe.net/data/whois/data.json?resource={IP_address}`	Whois information from the RIPEstat \ **API** `(https://github.com/ripe-nc` including inet number, name, organiza telephone.
Cisco Threat Grid	`https://panacea.threatgrid.com/api/v2/`	Polls data from the Cisco Threat Grid range of cyber threat data like IP addr network streams, and hash files.
VirusTotal	`https://www.virustotal.com/vtapi/v2/{}`	Polls data from the VirusTotal API. It p domains (passive DNS) and IP addres against 60+ antimalware products, res additional metadata information, wher

Enricher	API endpoint	Descri
Flashpoint AggregINT	`https://endlesstunnel.info/v3`	Polls data from the Flashpoint API. It hosts, domains, IP addresses, and ha thematic datasets focusing on hacker groups, communities in conflict, state **CBRN** (https://en.wikipedia.or produces enrichment observables like user name of the author of a post (as UTC date and time of a post in **ISO 8** (https://en.wikipedia.org/wiki/ (https://tools.ietf.org/html/rf
Flashpoint Blueprint	`https://endlesstunnel.info/v3`	Polls data from the Flashpoint API. It geolocation and IP ranges, as well as search thematic datasets focusing on supremacist groups, state actors invol (https://en.wikipedia.org/wiki/ enrichment observables like city/coun latitude/longitude or IP address hit, fo a hit, user name uniquely matched to
Flashpoint Thresher	`https://endlesstunnel.info/v3`	Polls data from the Flashpoint API. Th datasets focusing on hackers, terroris and **CBRN** (https://en.wikipedia threats. It produces enrichment obser thresher data.
PassiveTotal Whois	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** (https://api.passivetotal.org/a getv2whoisquery). It provides inform associated with an IP address or a do details. Analysts can retrieve registrar telephone, and email details. They ca further queries to obtain, for example, the same individual or the same comp
PassiveTotal Passive DNS	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** (https://api.passivetotal.org/a getv2dnspassivequery). It provides cross-referencing IP addresses to the over time. Analysts can examine how different IP addresses over time. They retrieve more domain names that may
PassiveTotal IP/Domain	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** (https://api.passivetotal.org/a getv2enrichmentquery). It provides queried IP address or domain name. I name, any sub-domains, inet details, **(ASN)** (https://en.wikipedia.org/wiki/ as well as geolocation information. An to look for further connections that ma investigation.

Enricher	API endpoint	Descri
PassiveTotal Malware	`https://api.passivetotal.org/v2`	Polls data from the **PassiveTotal API** `(https://api.passivetotal.org/a` `getv2enrichmentmalwarequery)`. It to the queried host or domain, such sha1, hash-sha256, hash-sha512 — malware entries are also tagged with `enrichment_extracts.meta.classi` to the value you set under **Rules > O** **Mark as malicious**; `enrichment_ext` it corresponds to the value you set un **> Confidence > Malicious - Low cor**
Splunk sightings	`http://10.0.1.22:8089/ (example)`	Based on the search queries defined for matching data in the specified Splu extracted and saved to the platform a
DomainTools Hosted Domains	`http://api.domaintools.com/v1/{}/host-domains`	Enriches IPv4 observables by returni and therefore related to, the input IP
DomainTools Reputation	`http://api.domaintools.com/v1/reputation`	Enriches domain and host name obse information to assess maliciousness defined threshold values.
DomainTools Suspicious Domains	`https://api.domaintools.com/v1/{}/host-domains`	Enriches IPv4 observables with suspi IP addresses. It includes configurable confidence levels to the processed IP malicious IPs.
FireEye iSIGHT	`https://api.isightpartners.com/search/{}`	Enriches platform observables with d related to areas such as critical infras espionage, hacktivism, frauds, and vu
Recorded Future	`https://app.recordedfuture.com/live/sc/entity/{}`	The enricher returns additional data s addresses, and hashes related to the specified types, as well as maliciousn retrieved risk scores.
Unshorten-URL	`https://unshorten.me/s/{}`	It takes shortened URL as an input, a resolved original URLs, which can the discover relationships with other entiti
Farsight DNSDB	`https://api.dnsdb.info/{}`	Historical passive DNS lookup enriche pointing to a specified IP address in t nameserver, domain names pointing existing below a parent domain name
ThreatCrowd	`https://www.threatcrowd.org/{}`	Returns suspicious and potentially m addresses, file hashes, and antivirus relationships between events, actors,

Enricher	API endpoint	Descri
Censys	`https://censys.io/api/v1/search/ipv4`	Returns relevant contextual informatic types to augment their intelligence val details, hashes, and **ASN** `(https://en.wikipedia.org/wiki/` details. It makes it easier to discover r actors, and targets.
DomainTools Malicious Server Domains	`http://api.domaintools.com/v1/{}/name-server-domains/`	Enriches domain and host observable domain names related to the same pri includes configurable thresholds to as levels to the processed domains and l domains/hosts.
DomainTools Retrieve Parsed Whois Observables	`http://api.domaintools.com/v1/{}/whois/parsed`	Enriches domains, hosts, and IP addr JSON output includes the most recen domain or IP range, as well as parsed registrar, contacts, and so on. It helps referencing data in a set of Whois rec
Crowdstrike Falcon Intelligence Indicator	`https://intelapi.crowdstrike.com/indicator/v1/search/{}`	Enriches platform entities and observa IP addresses, domain names, email a

Work with the Elasticsearch sightings enricher

This article describes how to configure the Elasticsearch sightings enricher parameters.
To configure the general options for the Elasticsearch sightings enricher, see Configure enrichers.

Elasticsearch sightings	**enricher**
Enricher name	Elasticsearch sightings
API endpoint	`http://<elasticsearch_url>:9200/<schema_resource>`
Input	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Output	Creates sightings from matching results returned from a search in an external Elasticsearch instance.
Description	Searches an external Elasticsearch instance. Any hits matching the search criteria are processed to automatically generate corresponding sightings.

Configure the enricher

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

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

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Data management**.
- On the left-hand navigation sidebar click **Enrichment**.
- Click the enricher you want to configure or modify.
- On the enricher detail page, click the **Edit** button.

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

Under **Parameters**, define the specific configuration options for the Elasticsearch sightings enricher:

- **ElasticSearch URL**: enter the URL pointing to the external Elasticsearch instance you want to use as a source for the enricher, including the sub-resource pointing to the **data mapping schema** `(https://www.elastic.co/guide/en/elasticsearch/guide/current/mapping-intro.html).`
  Example: *http://localhost:9200/default*
  In a usage scenario, you may want to obtain data from an external Elasticsearch instance that acts as a centralized log aggregator to check for correlations with the platform observables, indicators, and other entities. If it is possible to establish a relationship between Elasticsearch data and a platform entity, a sighting is automatically created.
- **Username**: enter valid user name credentials to authenticate and to receive authorization to access the resource(s).
  Example: *nigeltufnel*.
- **Password**: enter valid password credentials to authenticate and to receive authorization to access the resource(s).
  Example: *thesegoto11*.

- **Observable queries**: from the drop-down menu select the observable type and the corresponding observable value the rule should look for.
    - In the first input field, from the drop-down menu select the *observable type* the rule should look for.
      Supported observable types:
        - *asn*
        - *city*
        - *company*
        - *country*
        - *country_code*
        - *geo-lat*
        - *geo-long*
        - *hash-md5*
        - *hash-sha1*
        - *hash-sha256*
        - *ipv4*
        - *postcode*
    - In the second input field, specify the *observable value* associated to the observable type that the rule should look for.
      You can use free text, wildcards, **Elasticsearch query syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html)`, as well as the *{kind}* and *{value}* placeholders to reference an observable type and value, respectively.
      When the query executes, the placeholders take the values from the input observable key (*{kind}*) and value (*{value}*) pairs, respectively.
      Example:
      The **@{value}* query searches for observable values matching the input observable values it is fed at runtime.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include in the search additional key/value pairs like IP addresses, hashes, or domains.
- **Search results limit**: if you want to limit the returned search results, so that the search result entries do not exceed a predefined amount, you can set a cap here.
  For example: *10*.
- 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 ✚ **> Rules > Enrichment**.

Alternatively:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.
- Click the **+ Rule** button.

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

On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **+ Add** or **+ More** to add a filtering option.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click **+ Add** or **+ More** to add a new filtering option. For example, to include another incoming feed or a different entity type. A filter can take only one source and one entity type at a time, but you can set up rules with as many filters as you need.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to.
  When a rule is applied to one or more enrichers, it filters the enrichment data polled from the enricher source, based on the specified rule filters and criteria.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Save options

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

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

Edit enricher rules

To edit enricher rules, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.

- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

To edit the details of a specific rule, do the following:

- Click an area on the row corresponding to the rule you want to examine. An overlay slides in from the side of the screen to display the rule detail pane.
- On the detail pane, click **Edit**.

Alternatively:

- Click the ⋮ icon on the row corresponding to the enricher you want to configure or modify.
- From the drop-down menu select **Edit**.

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

- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- **Source**: from the drop-down menu select the incoming feed or the enricher whose observables you want to augment with additional information.
- **Entity types**: from the drop-down menu select the entity type whose observables you want to enrich with additional information.
- **TLP**: from the drop-down menu select the TLP color code you want to use to filter enrichment data.
  TLP `(https://www.us-cert.gov/tlp)` provides an intuitive reference to assess how sensitive information is, focusing in particular on how serious it is, and whom it should or should not be shared with.
- Click ✚ **Add** or ✚ **More** to add a new filtering option. For example, to include another incoming feed or a different entity type.
- **Enrichers**: from the drop-down menu select one or more enrichers to apply the rule to. They are external data providers that are polled to obtain relevant enricher raw data; for example, whois lookup, reverse DNS, or GeoIP information.
- Select the **Enabled** checkbox to enable the rule immediately after creating it.
- Click **Save** to store your changes, or **Cancel** to discard them.

Delete enricher rules

To delete an enricher rule, do the following:

- On the top navigation bar, click the ⚙ icon next to the user avatar image.
- From the drop-down menu select **Rules**.
- On the left-hand navigation sidebar click **Enrichment**.
- The **Rules > Enrichment** page shows an overview of the configured enricher rules.
  You can sort the items on the view by column header. To do so, click the column header you want to base the data sorting on. An upward-pointing ▲ or a downward-pointing ▼ arrow in the header indicates ascending and descending sort order, respectively.

- Click an area on the row corresponding to the rule you want to delete. An overlay slides in from the side of the screen to display the rule detail pane.
- Click **Delete** on the rule detail pane.

Alternatively:

- Click the ⋮ icon on the row corresponding to the rule you want to delete.
- From the drop-down menu select **Delete**.
- On the confirmation pop-up dialog, click **Delete** to confirm the action.
- The rule is deleted.

Run the enricher

Automatically

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

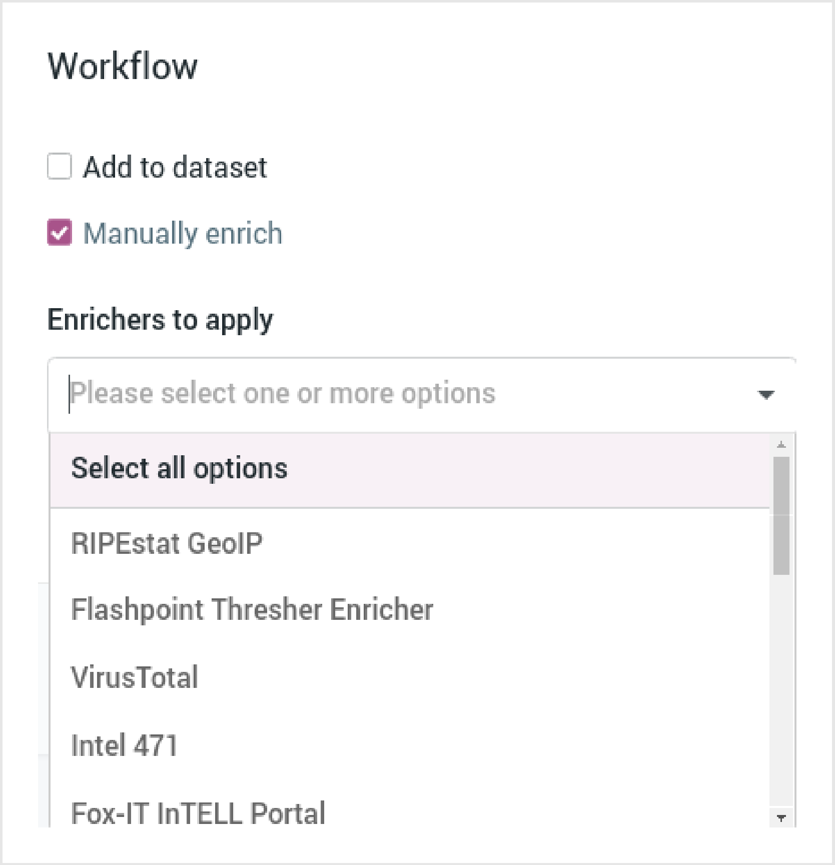
Rules give you control over the type of information you want to retrieve or exclude, and what you want to do with it. You can assign one or more enricher sources to specific observable types. You can set multiple filters to cover usage scenarios as needed. You can then examine the returned enrichment 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.

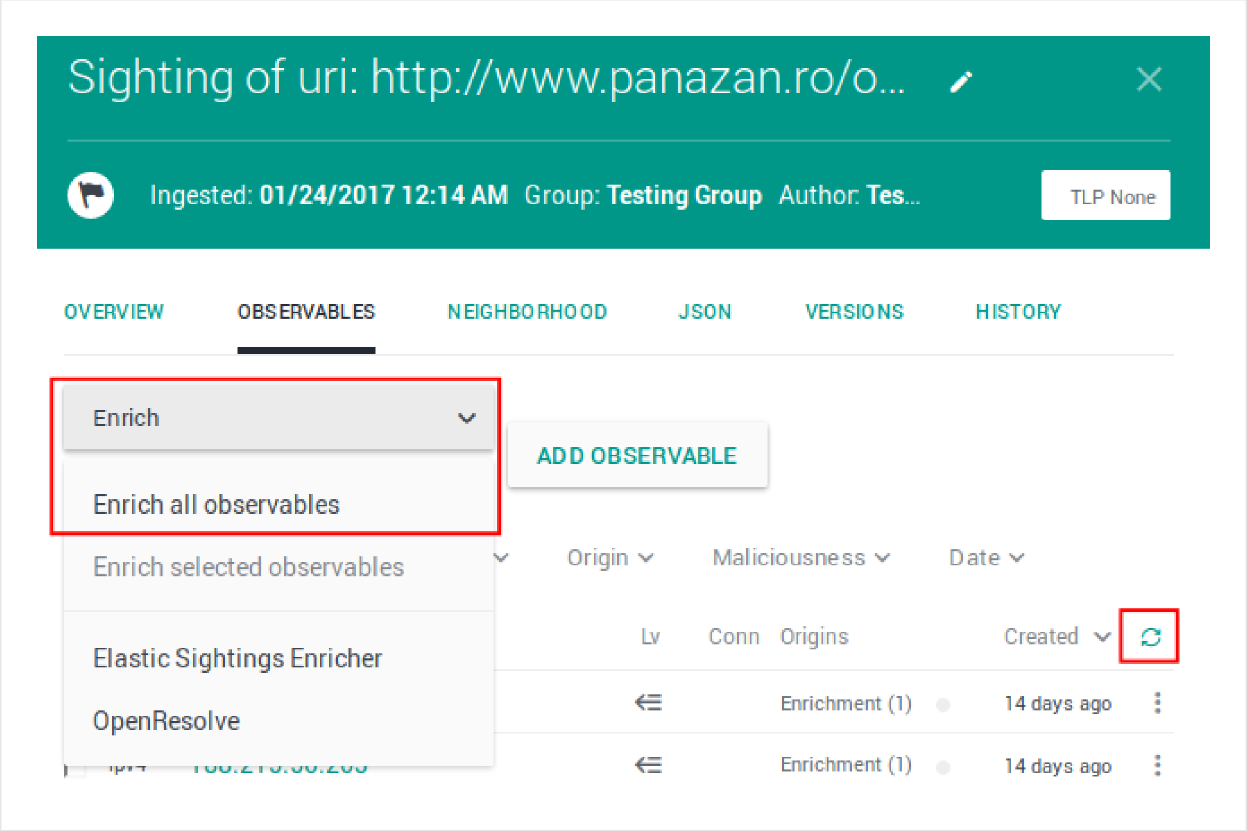
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.

To manually enrich the entity observables:

- Click the 🔄 refresh icon to trigger a task run that polls all the enrichers configured for the entity.

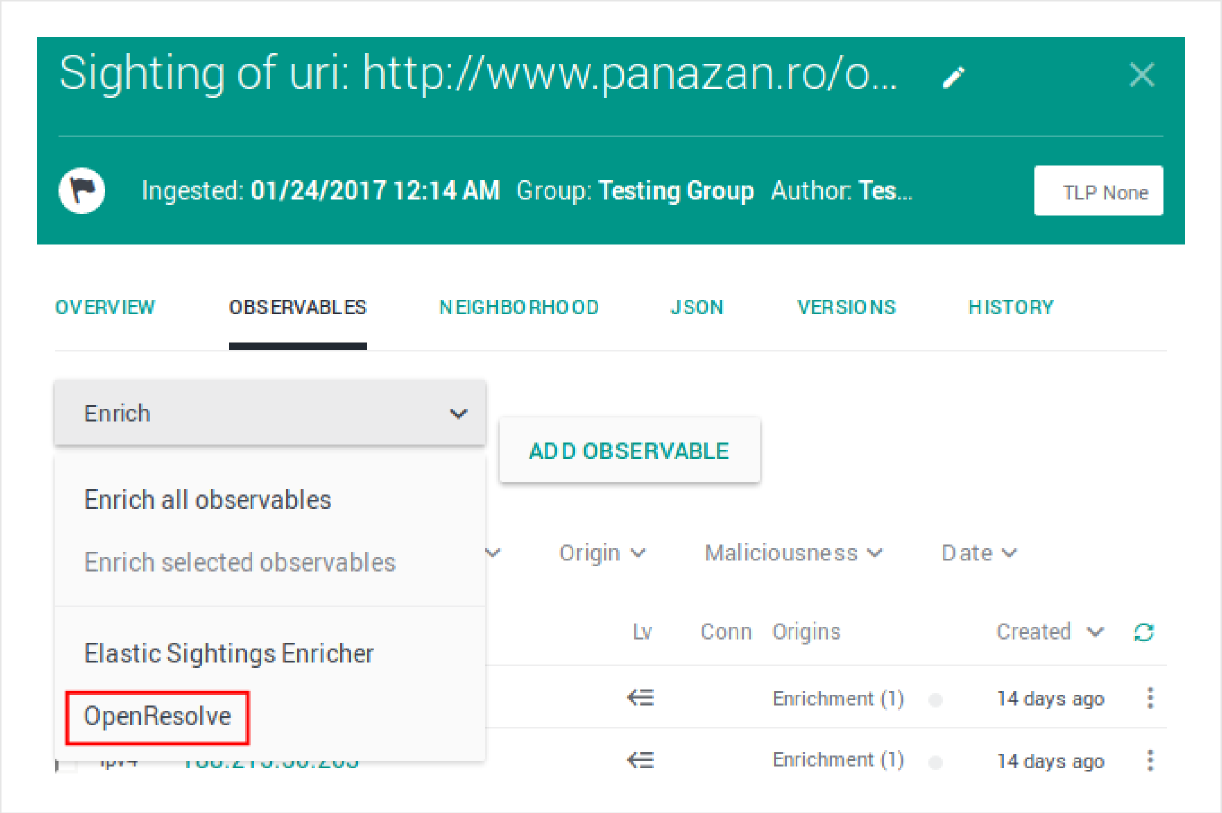
Alternatively:

- From the **Enrich** drop-down menu, select **Enrich all observables**.
- The platform polls all applicable enrichers for the entity, and it enriches all the entity observables with the retrieved data.



To poll a specific enricher:

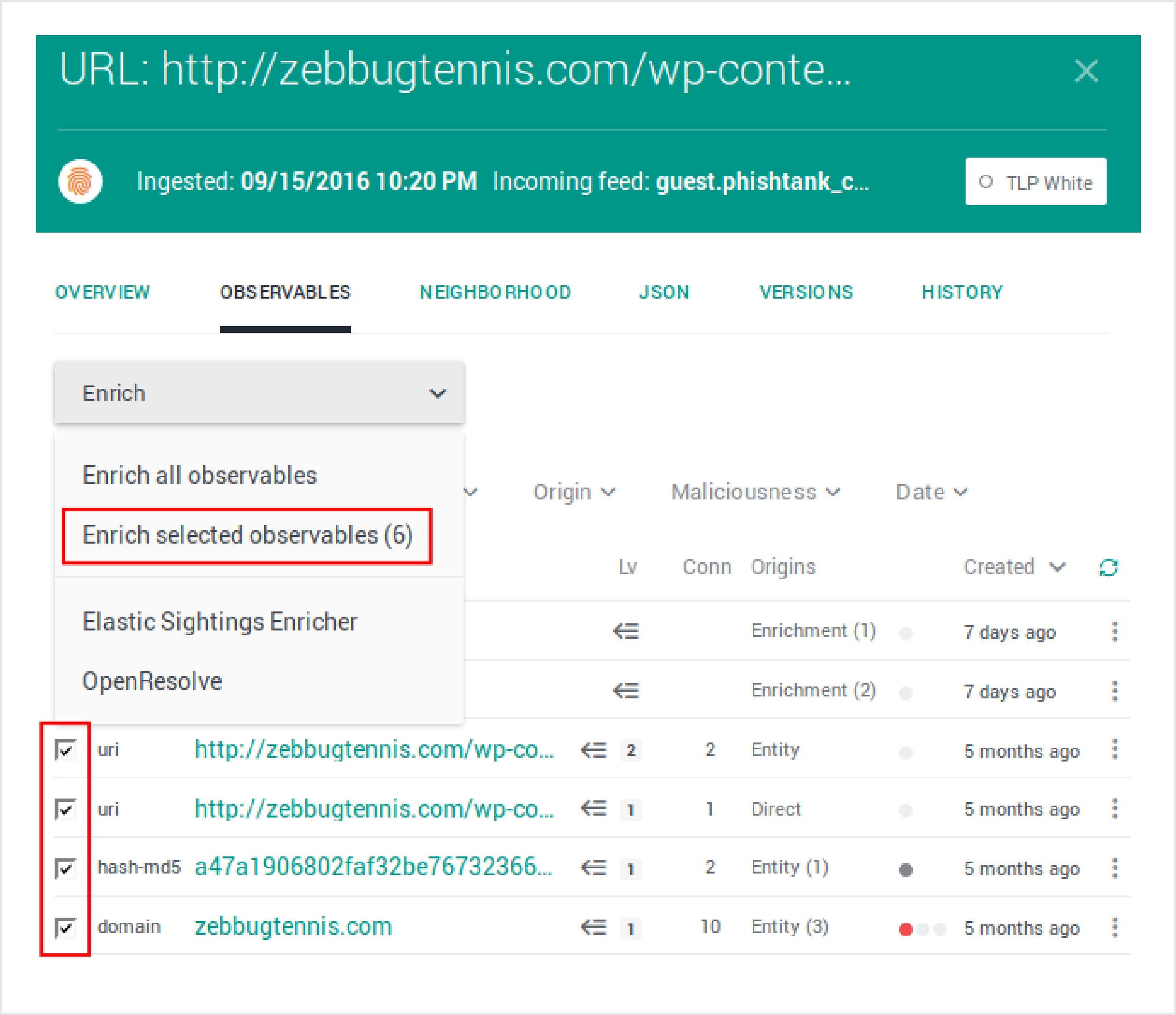
- Select it from the **Enrich** drop-down menu, and then click it.
- The platform polls the specified enricher for the entity, and it enriches all the entity observables with the retrieved data.



To enrich only specific observables:

- On the **Observables** tab, select the checkboxes corresponding to the observables you want to enrich.

- From the **Enrich** drop-down menu, select **Enrich selected observables**.
- The platform polls all applicable enrichers for the entity, and it enriches the selected entity observables with the retrieved data.



Ingested: **09/15/2016 10:20 PM** Incoming feed: **guest.phishtank_c...**

			Lv	Conn	Origins		Created
			⇇		Enrichment (1)	●	7 days ago
			⇇		Enrichment (2)	●	7 days ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 2	2	Entity	●	5 months ago
☑	uri	http://zebbugtennis.com/wp-co...	⇇ 1	1	Direct	●	5 months ago
☑	hash-md5	a47a1906802faf32be76732366...	⇇ 1	2	Entity (1)	●	5 months ago
☑	domain	zebbugtennis.com	⇇ 1	10	Entity (3)	●●●	5 months ago

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 Elasticsearch sightings enricher can take the following observable types as input:

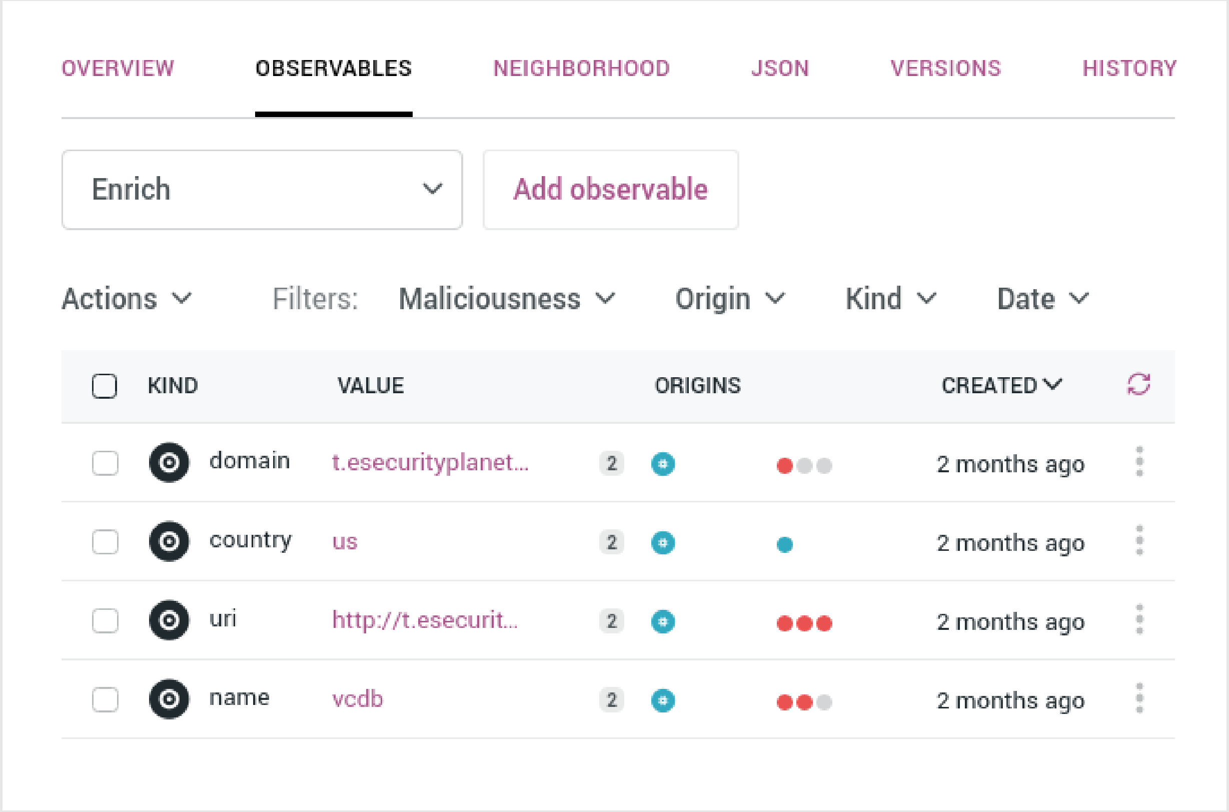
- *ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512*

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 Elasticsearch sightings.

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.

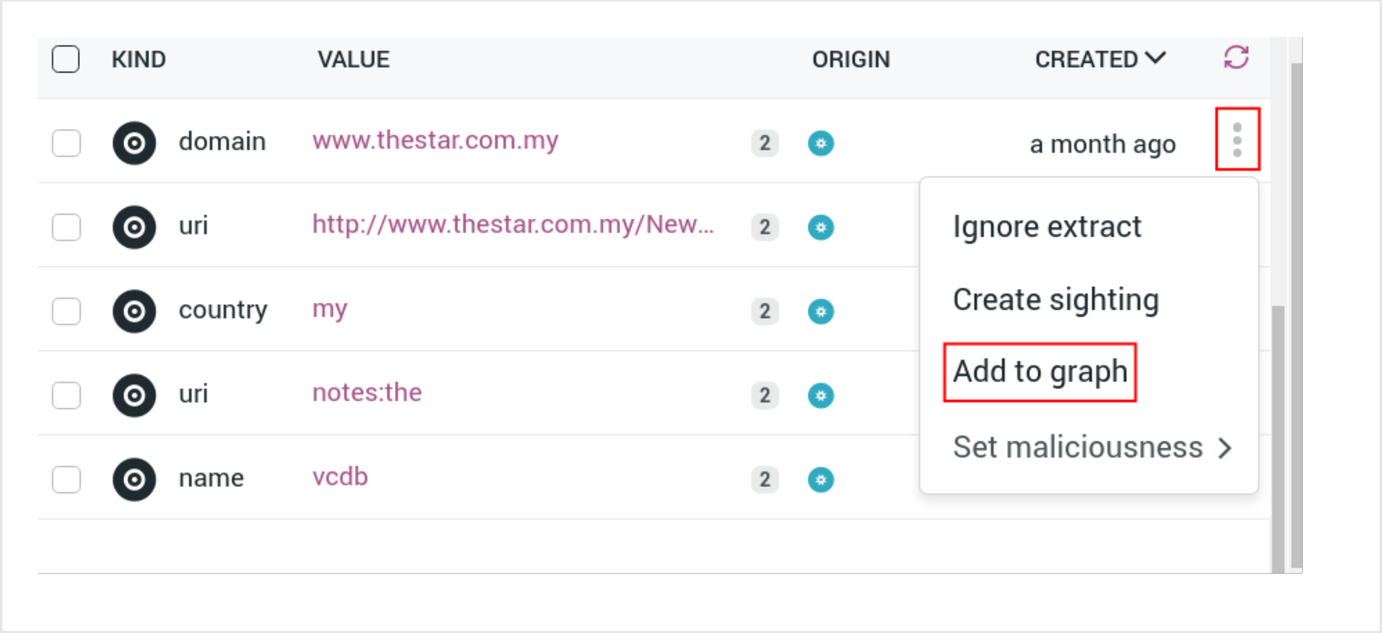


☐	KIND	VALUE	ORIGINS		CREATED
☐	domain	t.esecurityplanet...	2	●●●	2 months ago
☐	country	us	2	●	2 months ago
☐	uri	http://t.esecurit...	2	●●●	2 months ago
☐	name	vcdb	2	●●●	2 months ago

Review enrichment observables on the graph

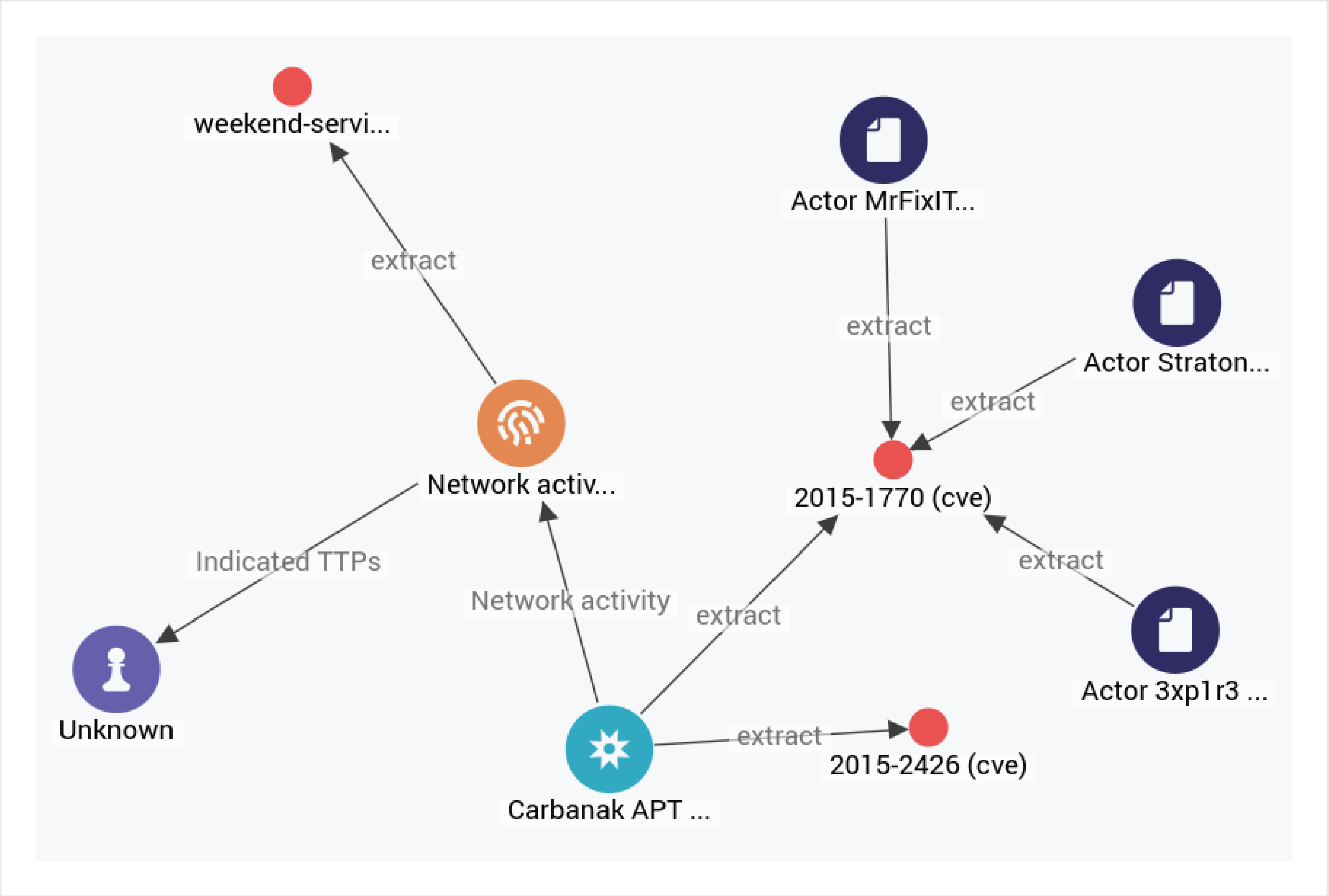
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

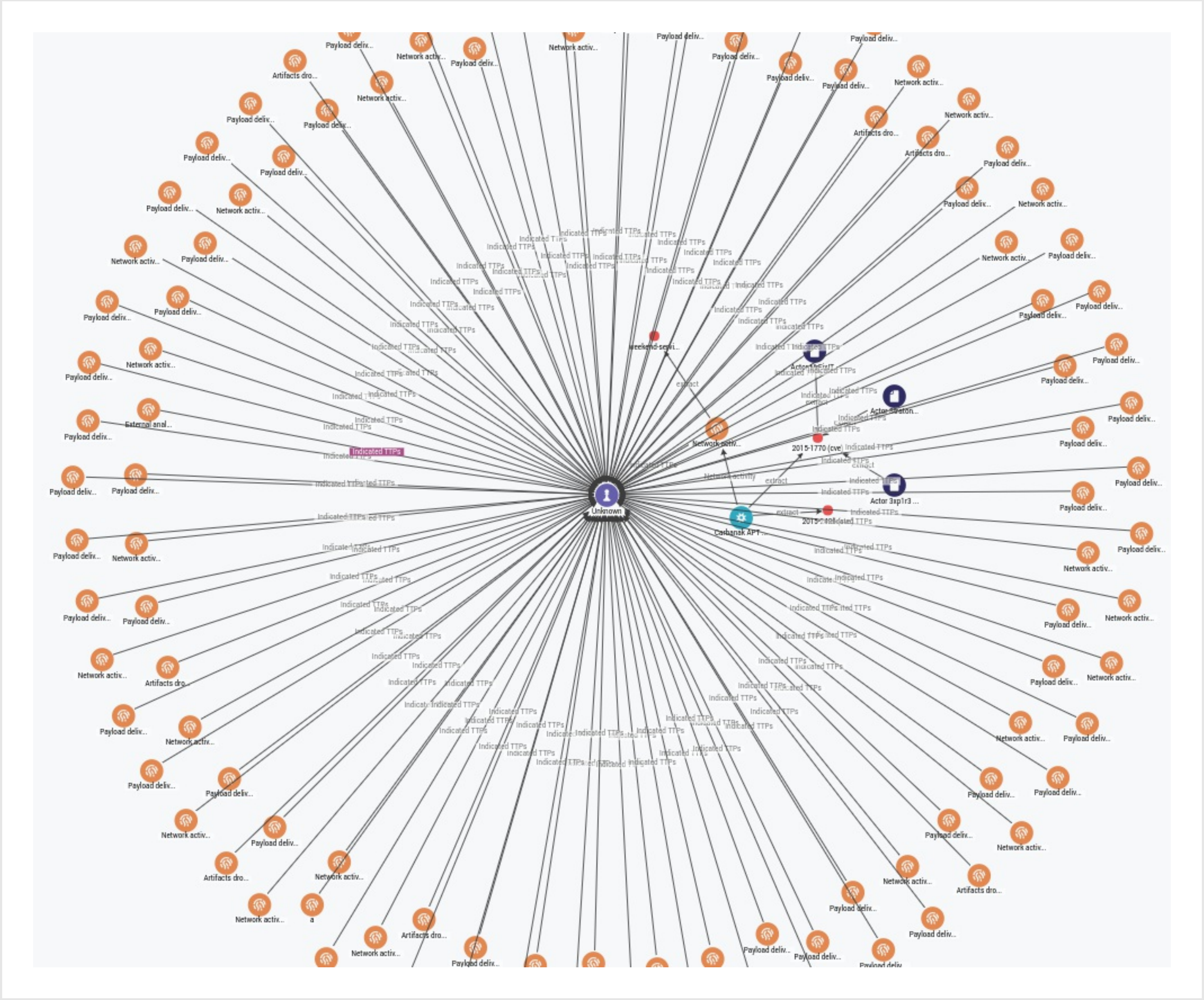


☐	KIND	VALUE	ORIGIN	CREATED
☐	domain	www.thestar.com.my	2	a month ago
☐	uri	http://www.thestar.com.my/New...	2	
☐	country	my	2	
☐	uri	notes:the	2	
☐	name	vcdb	2	

- 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** .

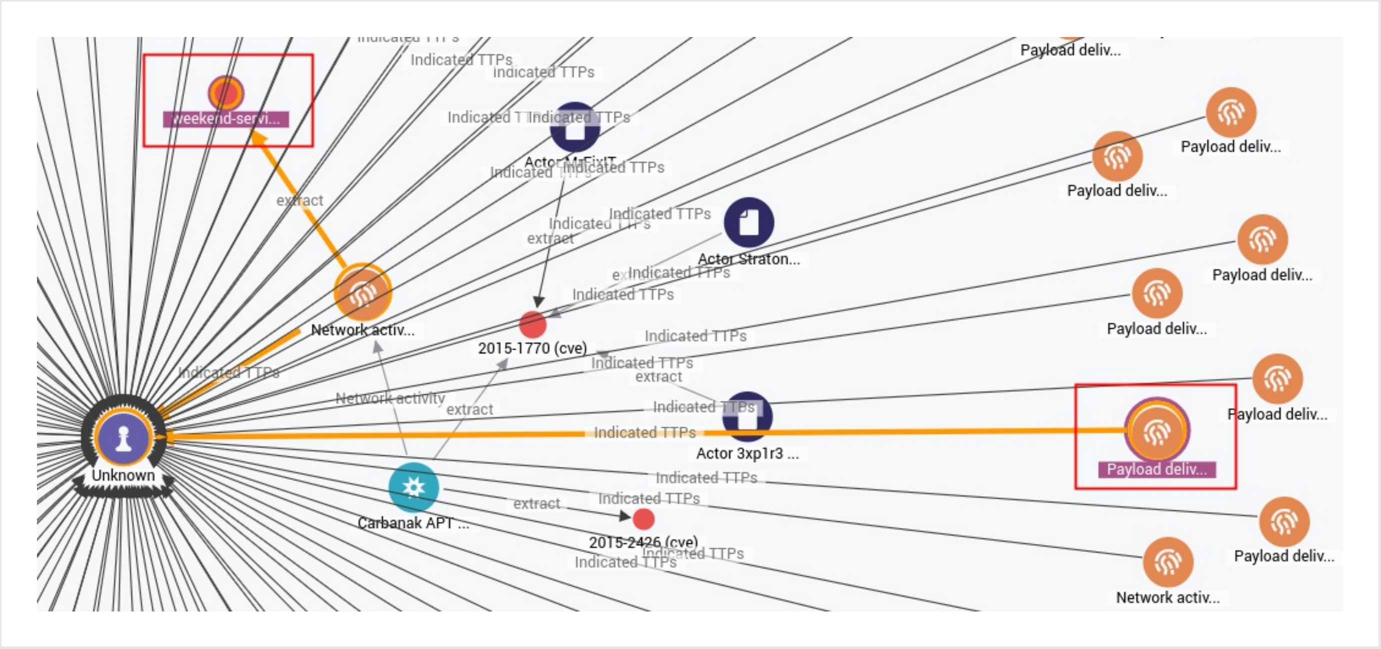


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All** .



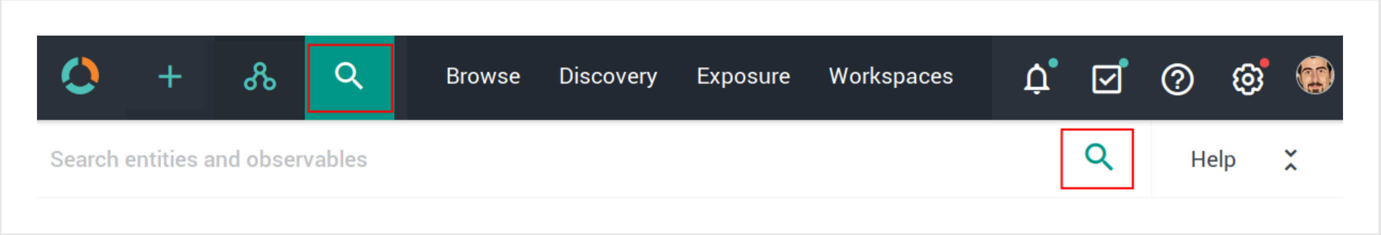
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 top bar:

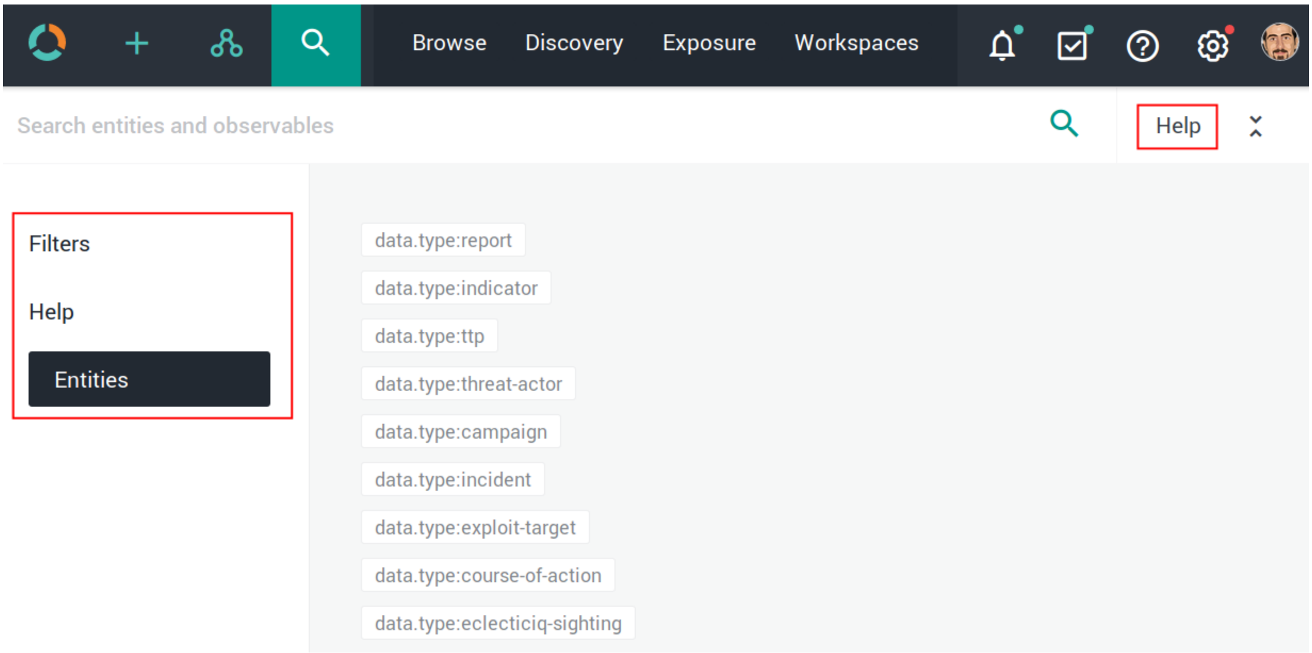


Enter search terms and search queries, and then press **ENTER** or click the search icon to run the search. Searches you run through this search box are executed platform-wide.

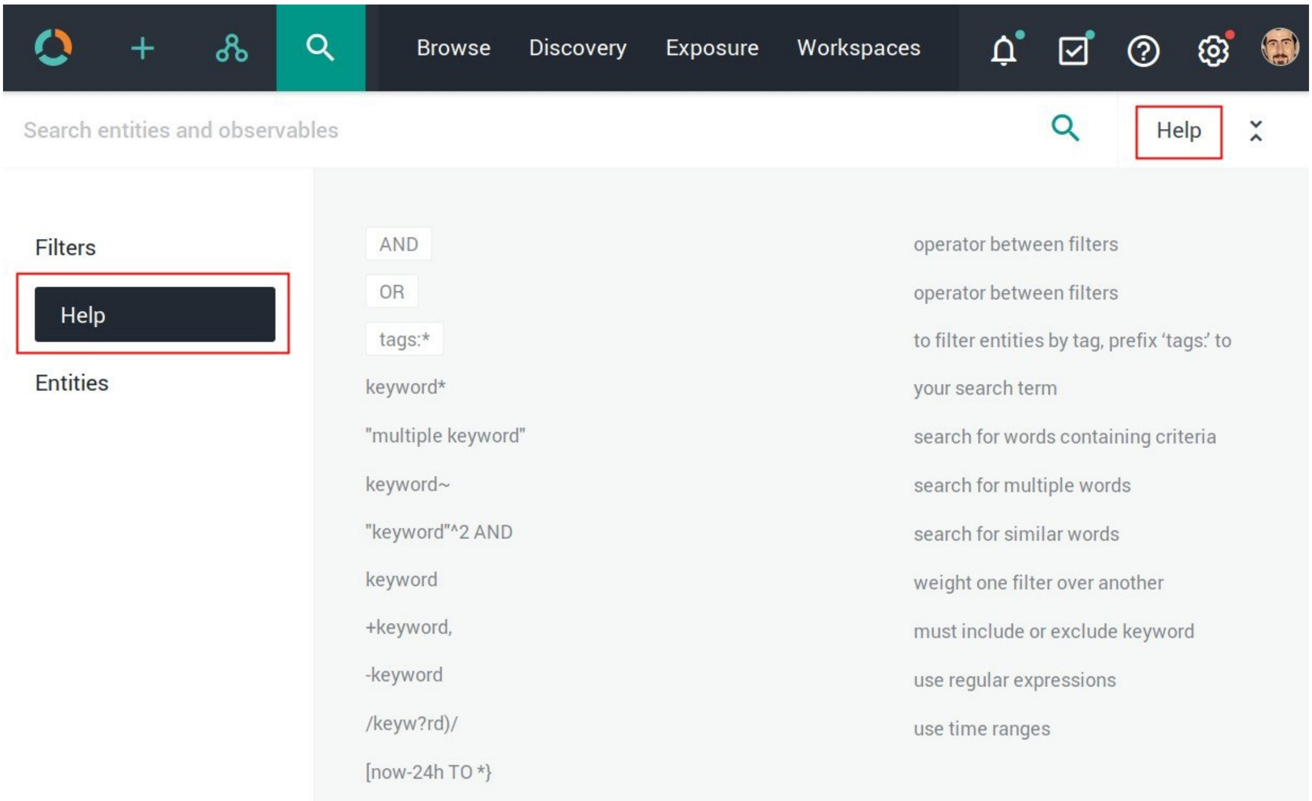
The search functionality uses **Elasticsearch query syntax** `(https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html)`.

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.



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
keyword*	your search term
"multiple keyword"	search for words containing criteria
keyword~	search for multiple words
"keyword"^2 AND	search for similar words
keyword	weight one filter over another
+keyword,	must include or exclude keyword
-keyword	use regular expressions
/keyw?rd)/	use time ranges
[now-24h TO *}	

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

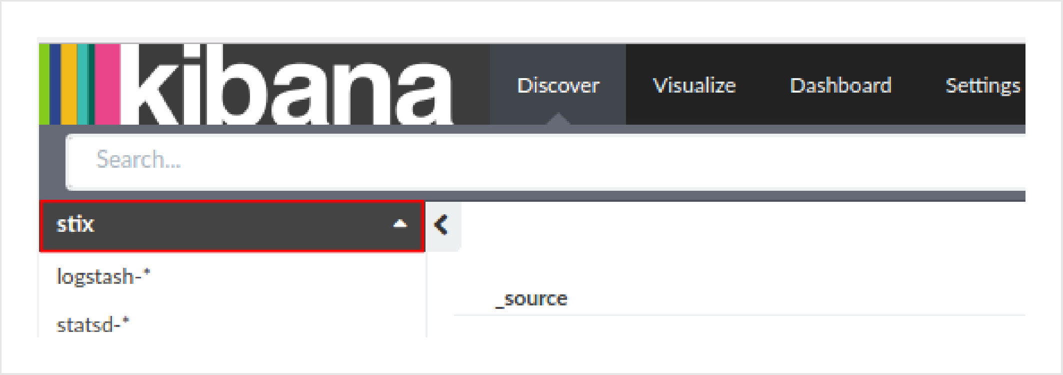
Field	Description	Example
enrichment_extracts.id	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	`01h12x45-01q2-1234-od01-123456h78h90`
enrichment_extracts.kind	string — The enrichment observable data type.	`domain`
enrichment_extracts.meta.blacklisted	Boolean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

Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeoIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host

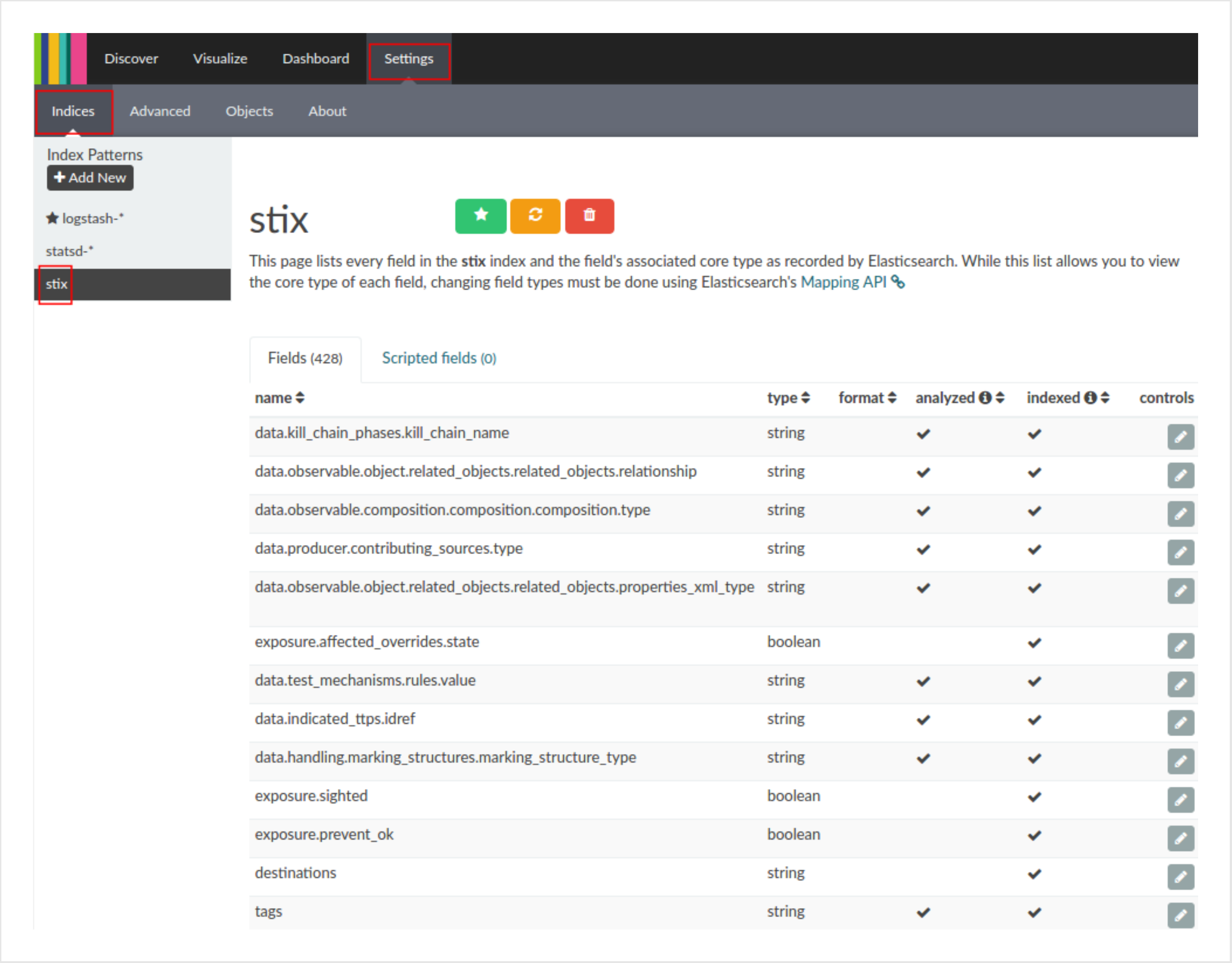
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye iSIGHT	asn, domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, host, ipv4, ipv6, uri
Recorded Future	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Unshorten-URL	uri
Farsight DNSDB	domain, host, ipv4, ipv6
ThreatCrowd	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, malware
Censys	asn, city, company, country, country_code, geo-lat, geo-long, hash-md5, hash-sha1, hash-sha256, ipv4, postcode
DomainTools Malicious Server Domains	domain, host
DomainTools Retrieve Parsed Whois Observables	domain, host, ipv4
Crowdstrike Falcon Intelligence Indicator	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri

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

- Sign in to the platform with your user credentials.
- To access Kibana, in the web browser address bar enter a URL with the following format:
  `<platform_host>/api/kibana/app/kibana#/`.
  Keep the trailing `/`.
  Example: `https://platform.host.com/api/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		✓	✓	✎