

# How-tos for EclecticIQ Platform

Hands-on articles on specific platform features

Last generated: July 21, 2017



©2017 EclecticIQ

All rights reserved. No part of this document may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without written permission from the author, except in the case of a reviewer, who may quote brief passages embodied in critical articles or in a review.

Trademarked names appear throughout this book. Rather than use a trademark symbol with every occurrence of a trademarked name, names are used in an editorial fashion, with no intention of infringement of the respective owner's trademark.

The information in this book is distributed on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this work, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this book.

©2017 by EclecticIQ BV. All rights reserved.  
Last generated on Jul 21, 2017

## Table of contents

Table of contents	2
How to work with enrichers	5
How to work with the Censys enricher	8
Work with the Censys enricher	8
Configure the Censys enricher	8
Configure enricher rules	10
Add enricher rules	10
Save options	11
Edit enricher rules	11
Delete enricher rules	12
Run the enricher	12
Automatically	12
Manually	13
Review enrichment observables	16
Review enrichment observables on the graph	17
Search for enrichment observables	20
How to work with the Crowdstrike Falcon Intelligence Indicator enricher	25
Work with the Crowdstrike Falcon Intelligence Indicator enricher	25
Configure the Crowdstrike Falcon Intelligence Indicator enricher	25
Configure enricher rules	26
Add enricher rules	26
Save options	27
Edit enricher rules	27
Delete enricher rules	28
Run the enricher	28
Automatically	28
Manually	29
Review enrichment observables	32
Review enrichment observables on the graph	33
Search for enrichment observables	36
How to work with the Farsight DNSDB enricher	41
Work with the Farsight DNSDB enricher	41
Configure the Farsight DNSDB enricher	41
Configure enricher rules	42
Add enricher rules	42
Save options	43
Edit enricher rules	43
Delete enricher rules	44
Run the enricher	45
Automatically	45
Manually	45
Review enrichment observables	48
Review enrichment observables on the graph	49
Search for enrichment observables	52
How to work with the Flashpoint AggregINT enricher	57
Work with the Flashpoint AggregINT enricher	57
Configure the Flashpoint AggregINT enricher	57
Configure enricher rules	58
Add enricher rules	58
Save options	59
Edit enricher rules	59
Delete enricher rules	60
Run the enricher	61
Automatically	61
Manually	61
Review enrichment observables	64
Review enrichment observables on the graph	65
Search for enrichment observables	68

How to work with the Flashpoint Blueprint enricher	73
Work with the Flashpoint Blueprint enricher	73
Configure the Flashpoint Blueprint enricher	73
How to work with the Flashpoint Thresher enricher	75
Work with the Flashpoint Thresher enricher	75
Configure the Flashpoint Thresher enricher	75
How to work with the DomainTools Hosted Domains enricher	77
Work with the DomainTools Hosted Domains enricher	77
Configure the DomainTools Hosted Domains enricher	77
Configure enricher rules	78
Add enricher rules	78
Save options	79
Edit enricher rules	79
Delete enricher rules	80
Run the enricher	80
Automatically	80
Manually	81
Review enrichment observables	84
Review enrichment observables on the graph	85
Search for enrichment observables	88
How to work with the DomainTools Malicious Server Domains enricher	93
Work with the DomainTools Malicious Server Domains enricher	93
Configure the DomainTools Malicious Server Domains enricher	93
Configure enricher rules	94
Add enricher rules	94
Save options	95
Edit enricher rules	95
Delete enricher rules	96
Run the enricher	97
Automatically	97
Manually	97
Review enrichment observables	100
Review enrichment observables on the graph	101
Search for enrichment observables	104
How to work with the DomainTools Reputation enricher	109
Work with the DomainTools Reputation enricher	109
Configure the DomainTools Reputation enricher	109
Configure enricher rules	110
Add enricher rules	110
Save options	111
Edit enricher rules	111
Delete enricher rules	112
Run the enricher	113
Automatically	113
Manually	113
Review enrichment observables	116
Review enrichment observables on the graph	117
Search for enrichment observables	120
How to work with the DomainTools Retrieve Parsed Whois Observables enricher	125
Work with the DomainTools Retrieve Parsed Whois Observables enricher	125
Configure the DomainTools Retrieve Parsed Whois Observables enricher	125
Configure enricher rules	126
Add enricher rules	126
Save options	127
Edit enricher rules	127
Delete enricher rules	128
Run the enricher	128
Automatically	129
Manually	129
Review enrichment observables	132



Review enrichment observables on the graph	133
Search for enrichment observables	136
How to work with the DomainTools Suspicious Domains enricher	141
Work with the DomainTools Suspicious Domains enricher	141
Configure the DomainTools Suspicious Domains enricher	141
Configure enricher rules	142
Add enricher rules	142
Save options	143
Edit enricher rules	143
Delete enricher rules	144
Run the enricher	145
Automatically	145
Manually	145
Review enrichment observables	148
Review enrichment observables on the graph	149
Search for enrichment observables	152
How to work with the Elasticsearch sightings enricher	157
Work with the Elasticsearch sightings enricher	160
Configure the enricher	160
Configure enricher rules	162
Add enricher rules	162
Save options	163
Edit enricher rules	163
Delete enricher rules	164
Run the enricher	165
Automatically	165
Manually	165
Review enrichment observables	168
Review enrichment observables on the graph	169
Search for enrichment observables	172

# 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 addresses, 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 addresses, 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 addresses 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 addresses, 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 addresses, 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	<code>https://censys.io/api/v1/search/ipv4</code>
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 <b>ASN</b> ( <code>https://en.wikipedia.org/wiki/autonomous_system_(internet)</code> ) details.
Description	Returns relevant contextual information about the submitted observable types to augment their intelligence value with geographic and geolocation details, hashes, and <b>ASN</b> ( <code>https://en.wikipedia.org/wiki/autonomous_system_(internet)</code> ) 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.

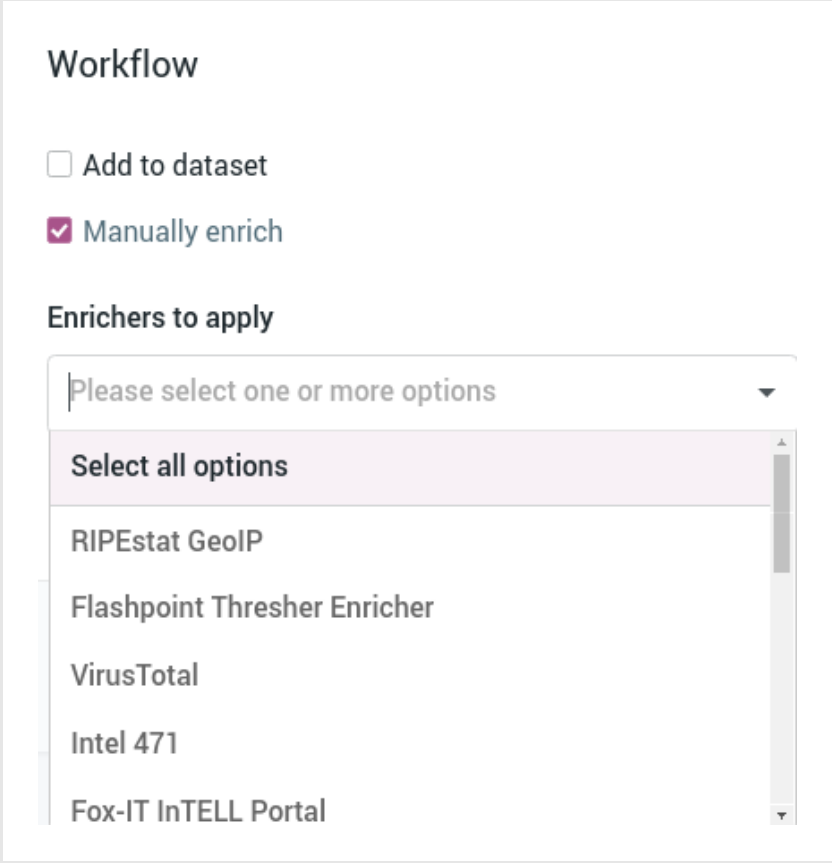
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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

Select all options

RIPEstat GeoIP

Flashpoint Thresher Enricher

VirusTotal

Intel 471

Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

The screenshot shows the interface for a sighting of a URI. The header bar is teal and contains the text "Sighting of uri: http://www.panazan.ro/o..." with a pencil icon and a close button. Below the header, there is a status bar with a flag icon, the text "Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes...", and a "TLP None" button. The main content area has a navigation bar with tabs: OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The OBSERVABLES tab is selected. Below the navigation bar, there is a dropdown menu labeled "Enrich" with a downward arrow. The dropdown menu is open, showing options: "Enrich all observables", "Enrich selected observables", "Elastic Sightings Enricher", and "OpenResolve". The "Enrich all observables" option is highlighted with a red box. To the right of the dropdown menu is a button labeled "ADD OBSERVABLE". Below the dropdown menu, there is a table with columns: Origin, Maliciousness, Date, Lv, Conn, Origins, and Created. The table has two rows of data. The first row has a value of "100.210.00.200" in the Origin column. The second row has a value of "100.210.00.200" in the Origin column. The "Created" column has a value of "14 days ago" and a refresh icon (a circular arrow) which is highlighted with a red box.

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

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▾ ADD OBSERVABLE

Enrich all observables

Enrich selected observables ▾

Elastic Sightings Enricher

OpenResolve

Origin ▾	Maliciousness ▾	Date ▾	Lv	Conn	Origins	Created ▾	↻
←	Enrichment (1)	14 days ago					⋮
←	Enrichment (1)	14 days ago					⋮

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 screenshot shows the Elastic Observables interface. At the top, a teal header bar displays the URL: `http://zebugtennis.com/wp-conte...` with a close button. Below the header, a status bar indicates the data was ingested on 09/15/2016 at 10:20 PM from the feed `guest.phishtank_c...`, with a TLP White label.

The main interface has tabs for OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The OBSERVABLES tab is active.

A dropdown menu is open under the 'Enrich' button, showing options: 'Enrich all observables', 'Enrich selected observables (6)' (highlighted with a red box), 'Elastic Sightings Enricher', and 'OpenResolve'.

Below the menu is a table of enrichment results. The first four rows are highlighted with a red box, indicating they are the selected observables:

	Origin	Maliciousness	Date
<input checked="" type="checkbox"/> uri <a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	2	2	Entity
<input checked="" type="checkbox"/> uri <a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	1	1	Direct
<input checked="" type="checkbox"/> hash-md5 <a href="#">a47a1906802faf32be76732366...</a>	1	2	Entity (1)
<input checked="" type="checkbox"/> domain <a href="#">zebugtennis.com</a>	1	10	Entity (3)

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.

OVERVIEW	OBSERVABLES	NEIGHBORHOOD	JSON	VERSIONS	HISTORY
<div>Enrich <span>▼</span> <span>Add observable</span></div>					
Actions <span>▼</span> Filters: Maliciousness <span>▼</span> Origin <span>▼</span> Kind <span>▼</span> Date <span>▼</span>					
<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED <span>▼</span>	<span>↻</span>
<input type="checkbox"/>	domain	t.esecurityplanet...	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	country	us	2 <span>+</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	uri	http://t.esecurit...	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	name	vcdb	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>

## 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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED <span>▼</span>	<span>↻</span>
<input type="checkbox"/>	domain	www.thestar.com.my	2 <span>+</span>	a month ago	<span>⋮</span>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2 <span>+</span>		
<input type="checkbox"/>	country	my	2 <span>+</span>		
<input type="checkbox"/>	uri	notes:the	2 <span>+</span>		
<input type="checkbox"/>	name	vcdb	2 <span>+</span>		

Ignore extract

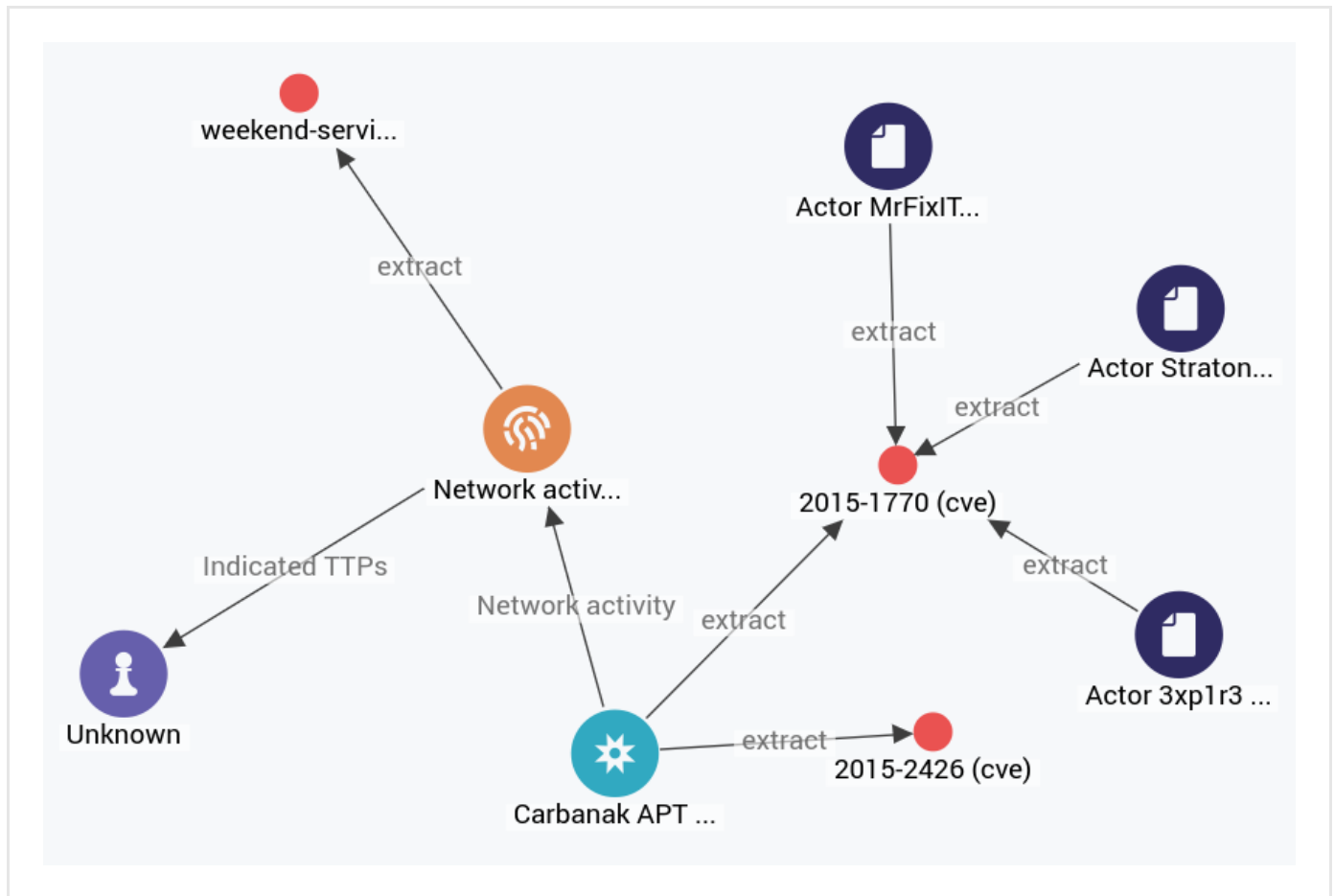
Create sighting

Add to graph

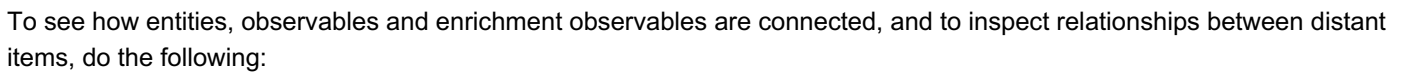
Set maliciousness >

- 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**.

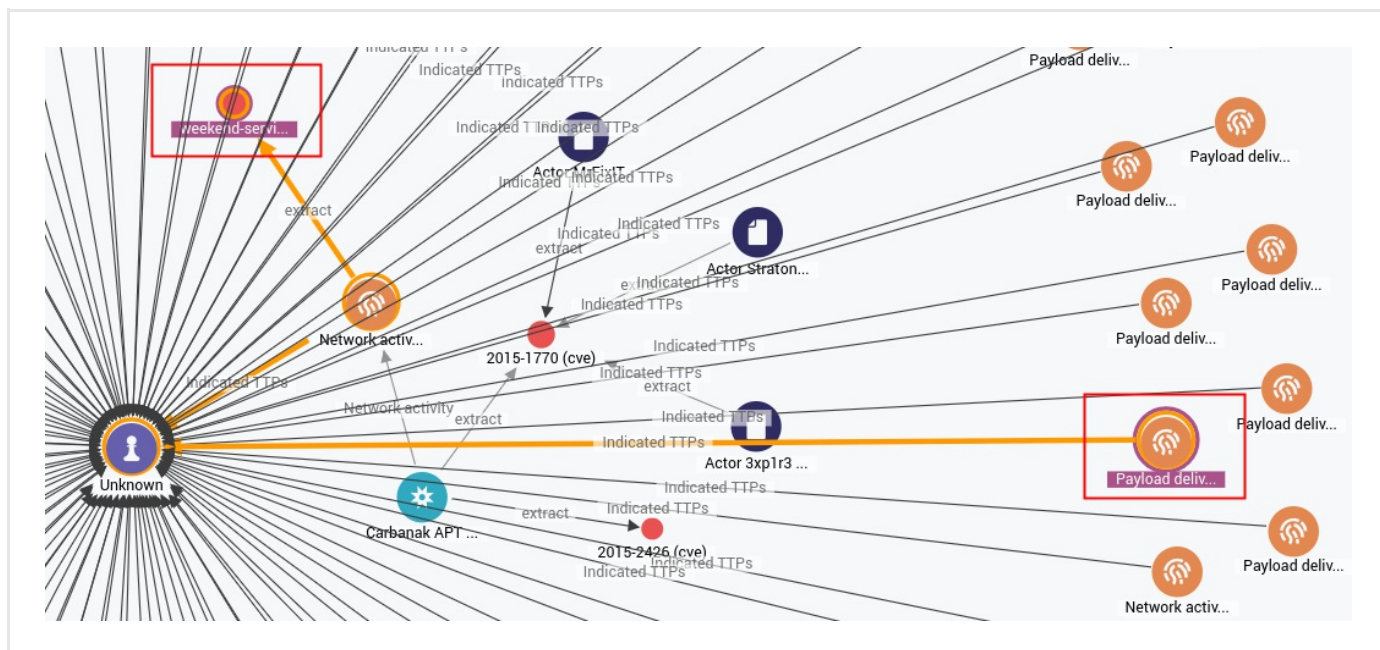


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



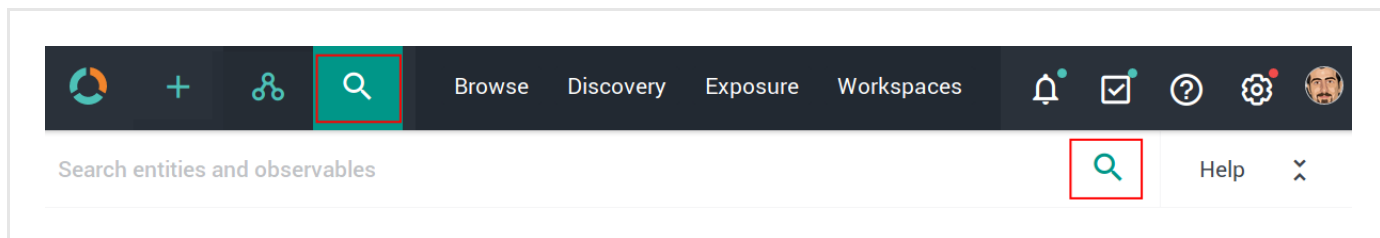
- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist, 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.

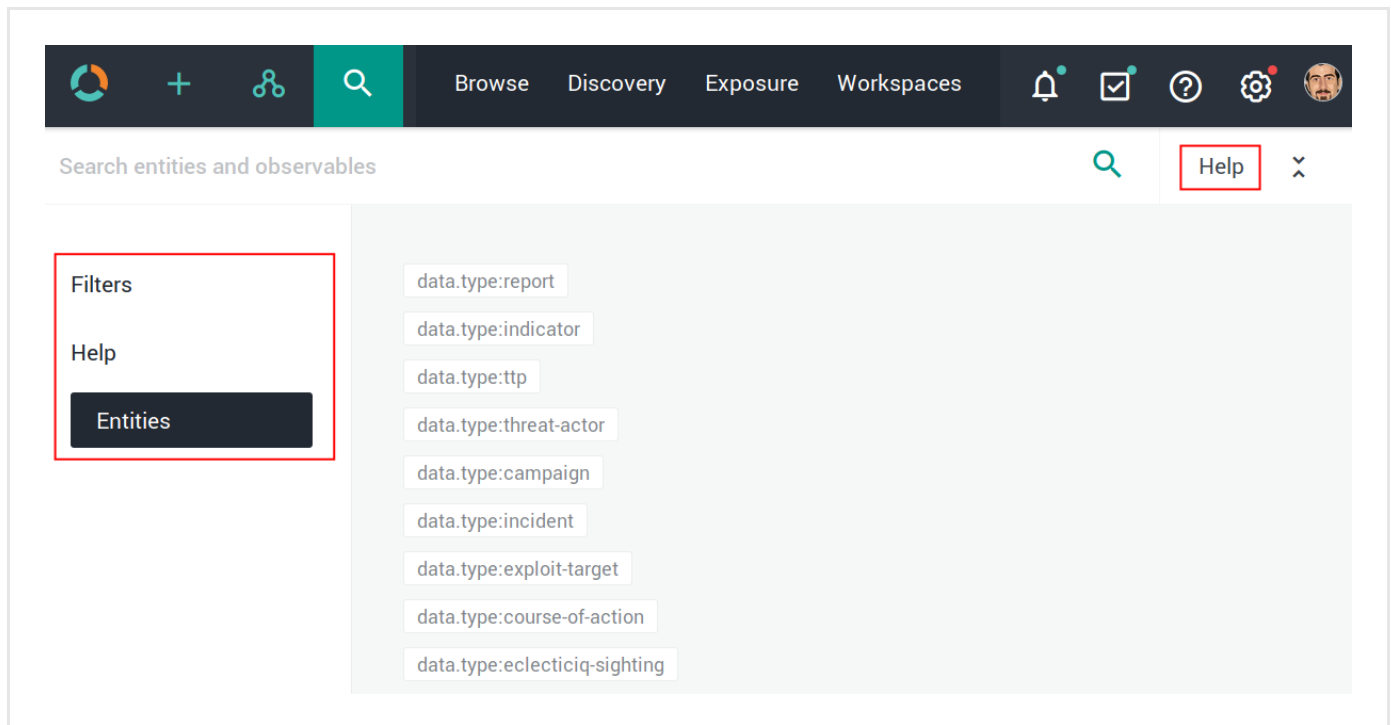


The search functionality uses **Elasticsearch query syntax**

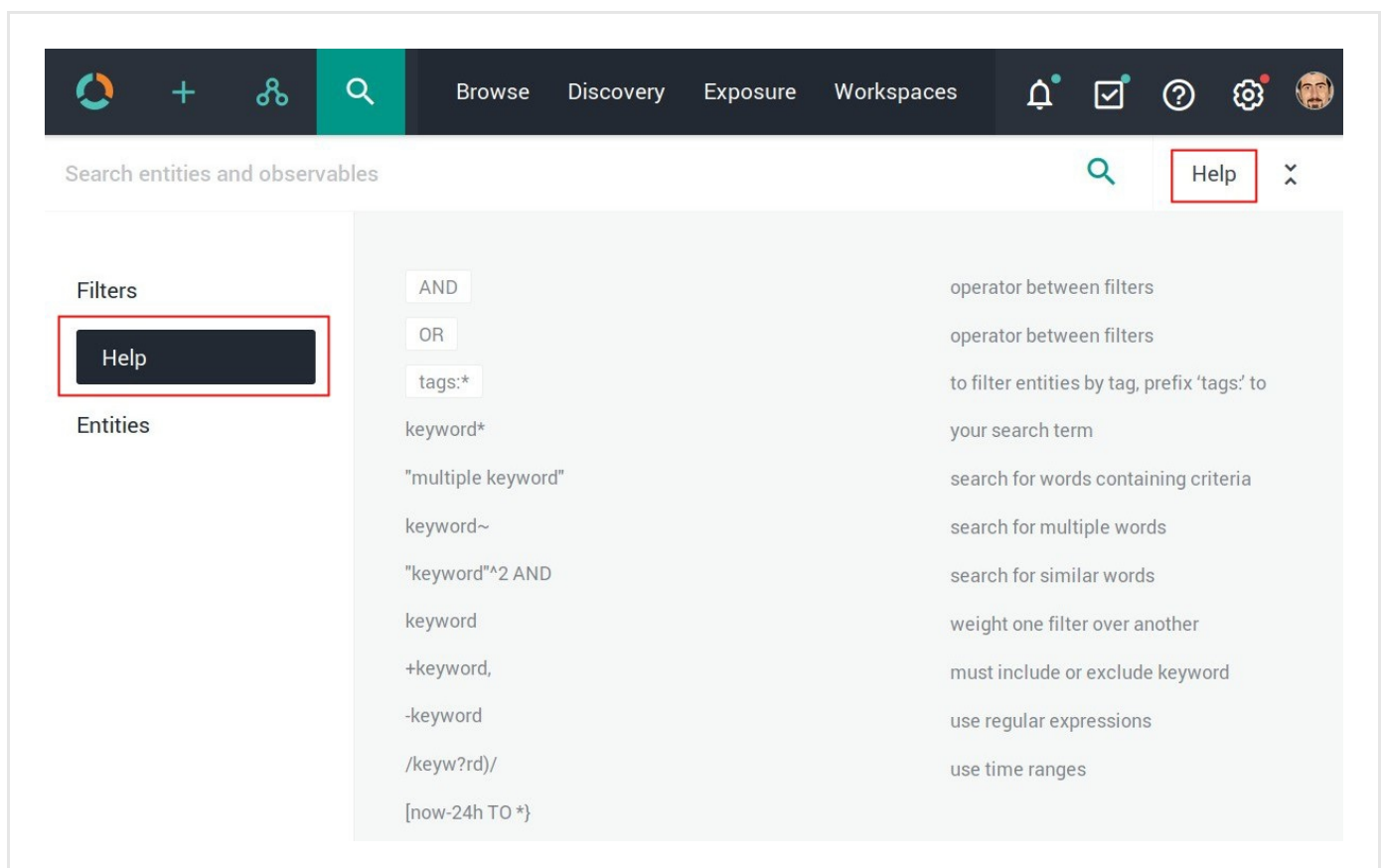
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
```

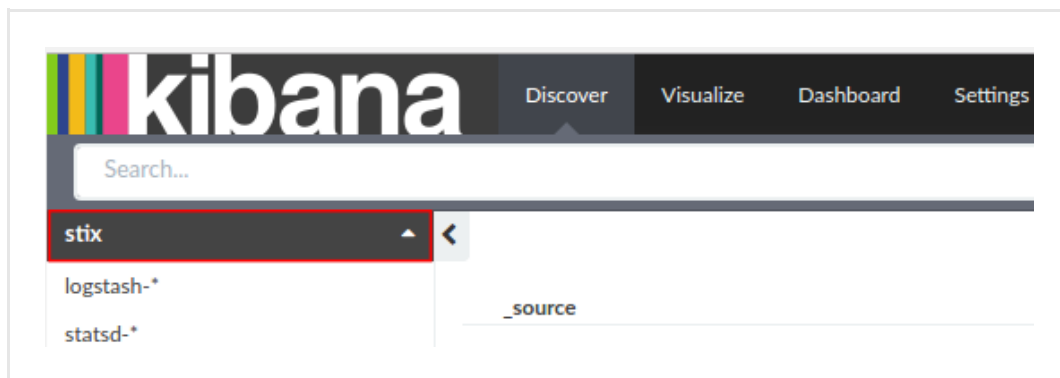
Field	Description	Example
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	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 GeolIP	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-sha512, 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**:

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](#).


<b>CrowdStrike Falcon Intelligence Indicator</b>	<b>enricher</b>
<b>Enricher name</b>	CrowdStrike Falcon Intelligence Indicator
<b>API endpoint</b>	<code>https://intelapi.crowdstrike.com/indicator/v1/search/{}</code>
<b>Input</b>	domain, email, email-subject, file, hash-md5, hash-sha1, hash-sha256, ipv4, ipv6, mutex, name, persona, port, uri
<b>Output</b>	Enriches the supported observable types with information extracted from indicators.
<b>Description</b>	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.

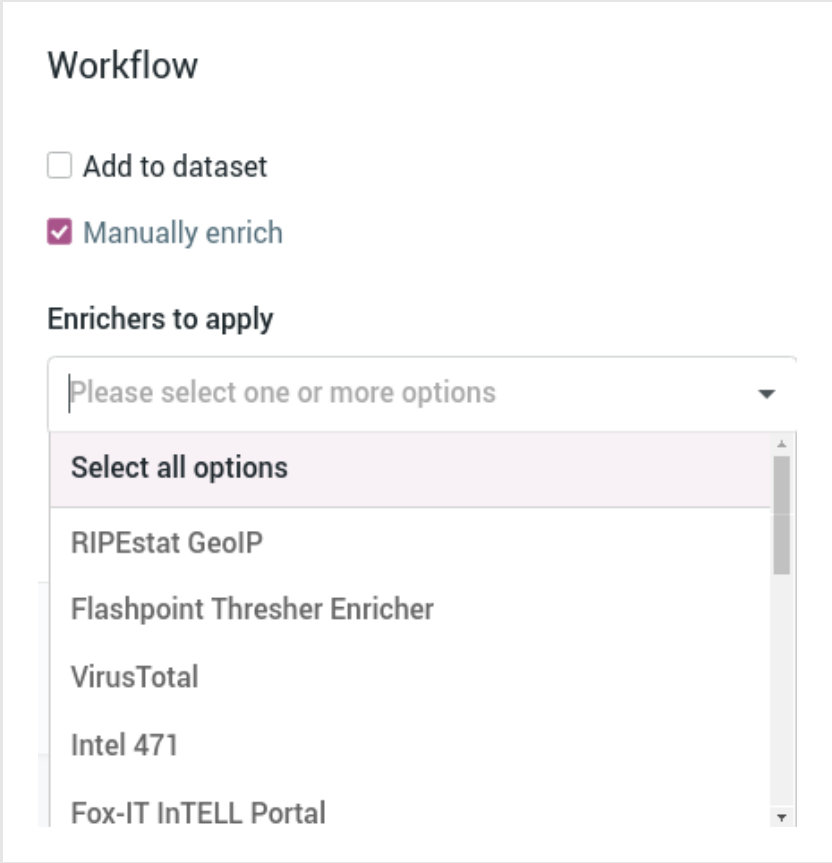
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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**

Please select one or more options

Select all options

RIPEstat GeoIP

Flashpoint Thresher Enricher

VirusTotal

Intel 471

Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.


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

To manually enrich the entity observables:

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

Alternatively:

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



The screenshot shows the 'Sighting of uri: http://www.panazan.ro/o...' entity detail pane. The 'OBSERVABLES' tab is selected. The 'Enrich' dropdown menu is open, showing options: 'Enrich', 'Enrich all observables', 'Enrich selected observables', 'Elastic Sightings Enricher', and 'OpenResolve'. The 'Enrich all observables' option is highlighted. A table of observables is displayed with columns: Origin, Maliciousness, Date, Lv, Conn, Origins, and Created. The 'Created' column has a refresh icon (circular arrow) next to it, which is highlighted with a red box. The table shows two rows of enrichment data, each with a status indicator (a circle) and a timestamp '14 days ago'.

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

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▾ ADD OBSERVABLE

Enrich all observables

Enrich selected observables ▾

Elastic Sightings Enricher

OpenResolve

Origin ▾	Maliciousness ▾	Date ▾
Lv	Conn	Origins
Created ▾		
←	Enrichment (1)	14 days ago
←	Enrichment (1)	14 days ago

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://zebugtennis.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	<a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	5 months ago
⌵	uri	<a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	5 months ago
⌵	hash-md5	<a href="#">a47a1906802faf32be76732366...</a>	5 months ago
⌵	domain	<a href="#">zebugtennis.com</a>	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.

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Add observable

Actions Filters: Maliciousness Origin Kind Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2		2 months ago
<input type="checkbox"/>	country	us	2		2 months ago
<input type="checkbox"/>	uri	http://t.esecurit...	2		2 months ago
<input type="checkbox"/>	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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdb	2		

Ignore extract

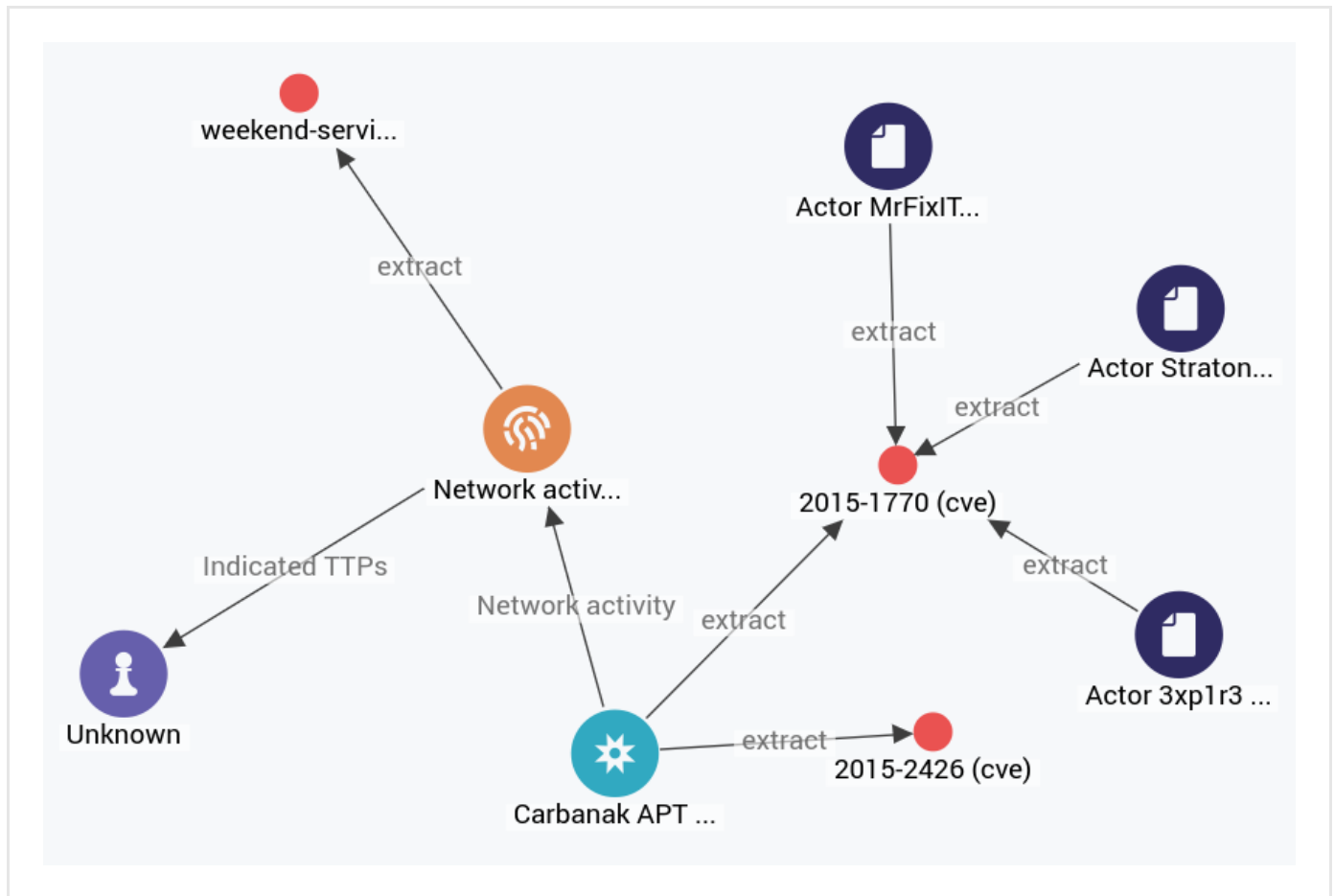
Create sighting

**Add to graph**

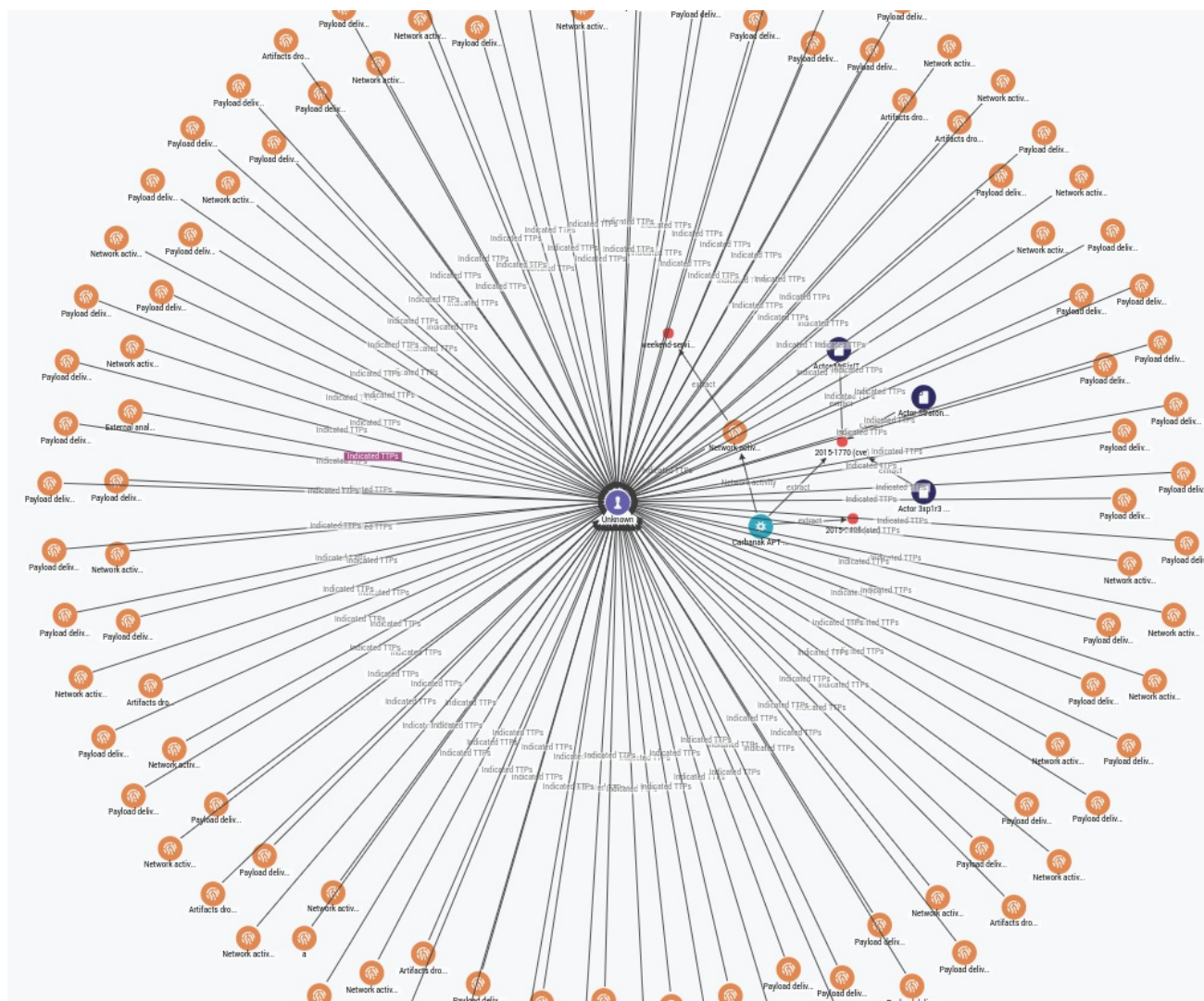
Set maliciousness >

- 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**.



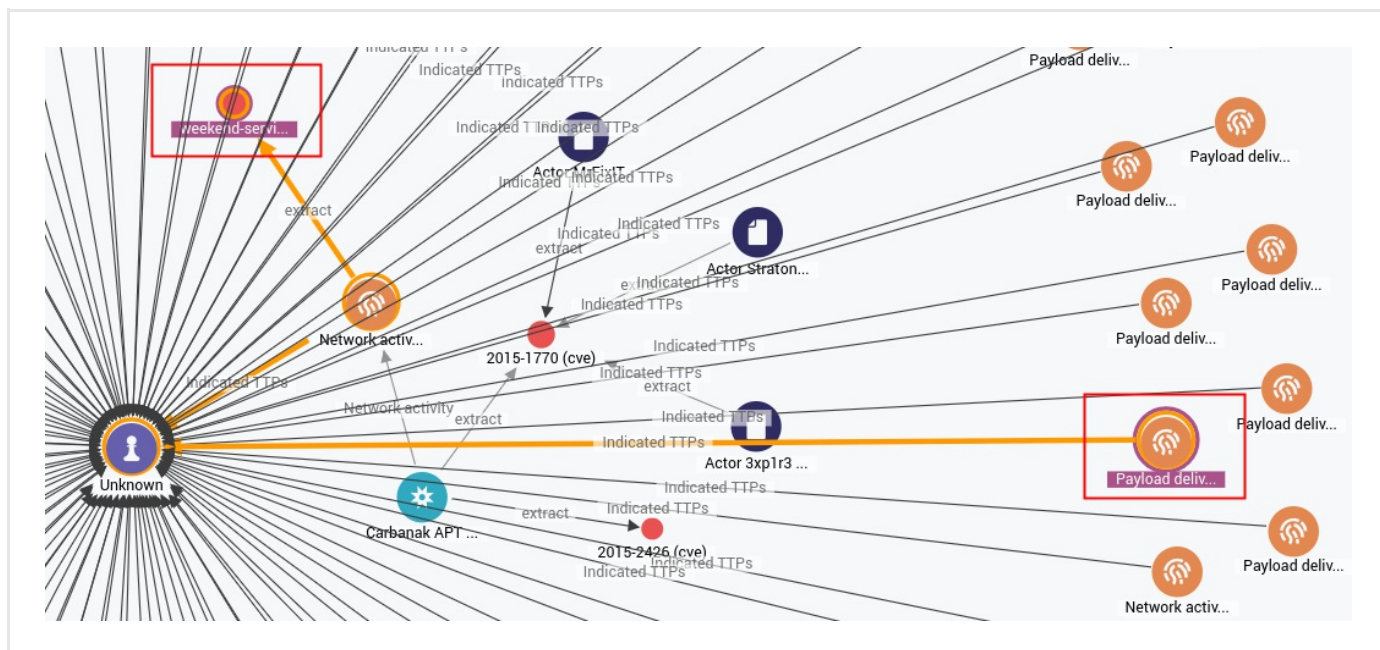
- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



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

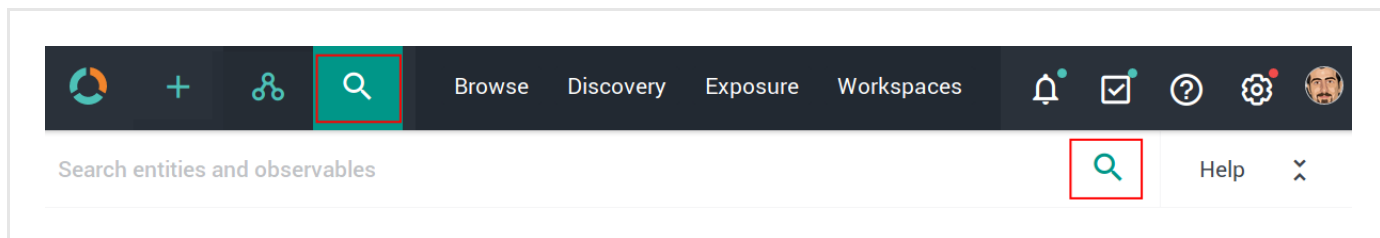
- **CTRL + click** two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist, 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.

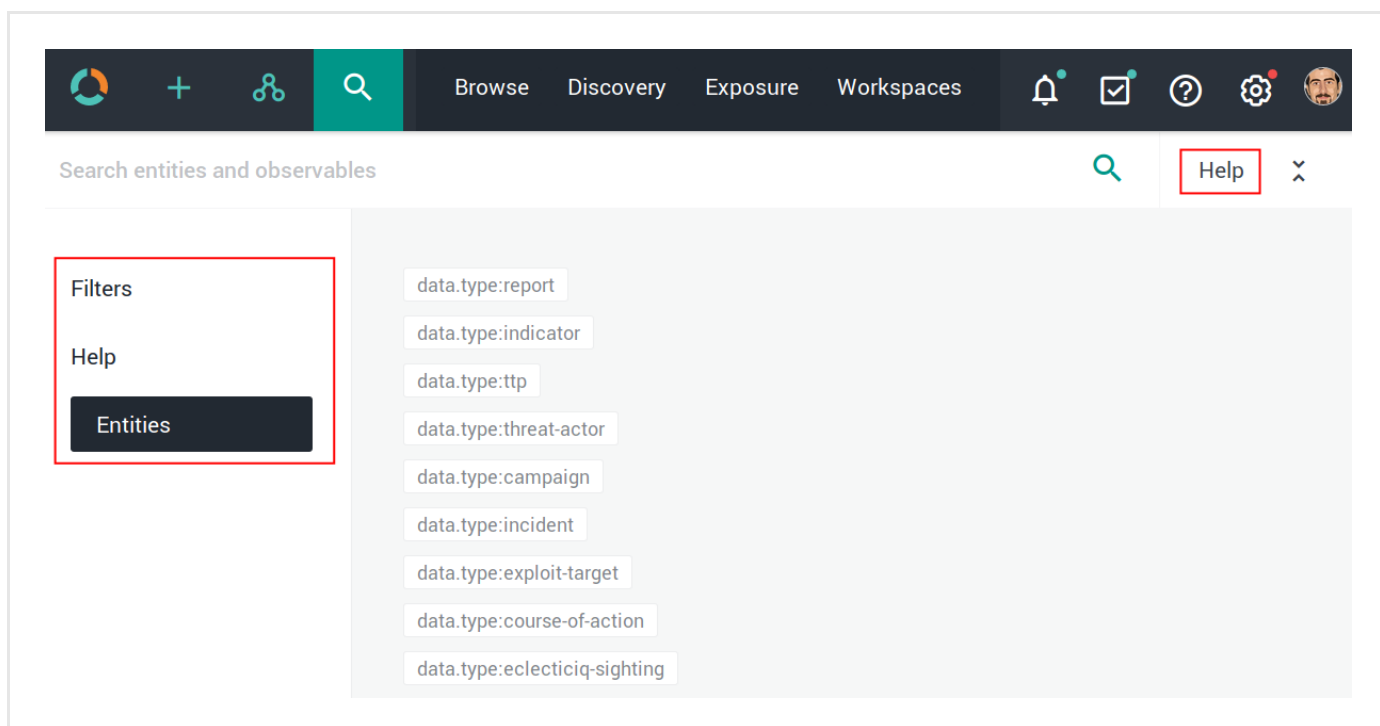


The search functionality uses **Elasticsearch query syntax**

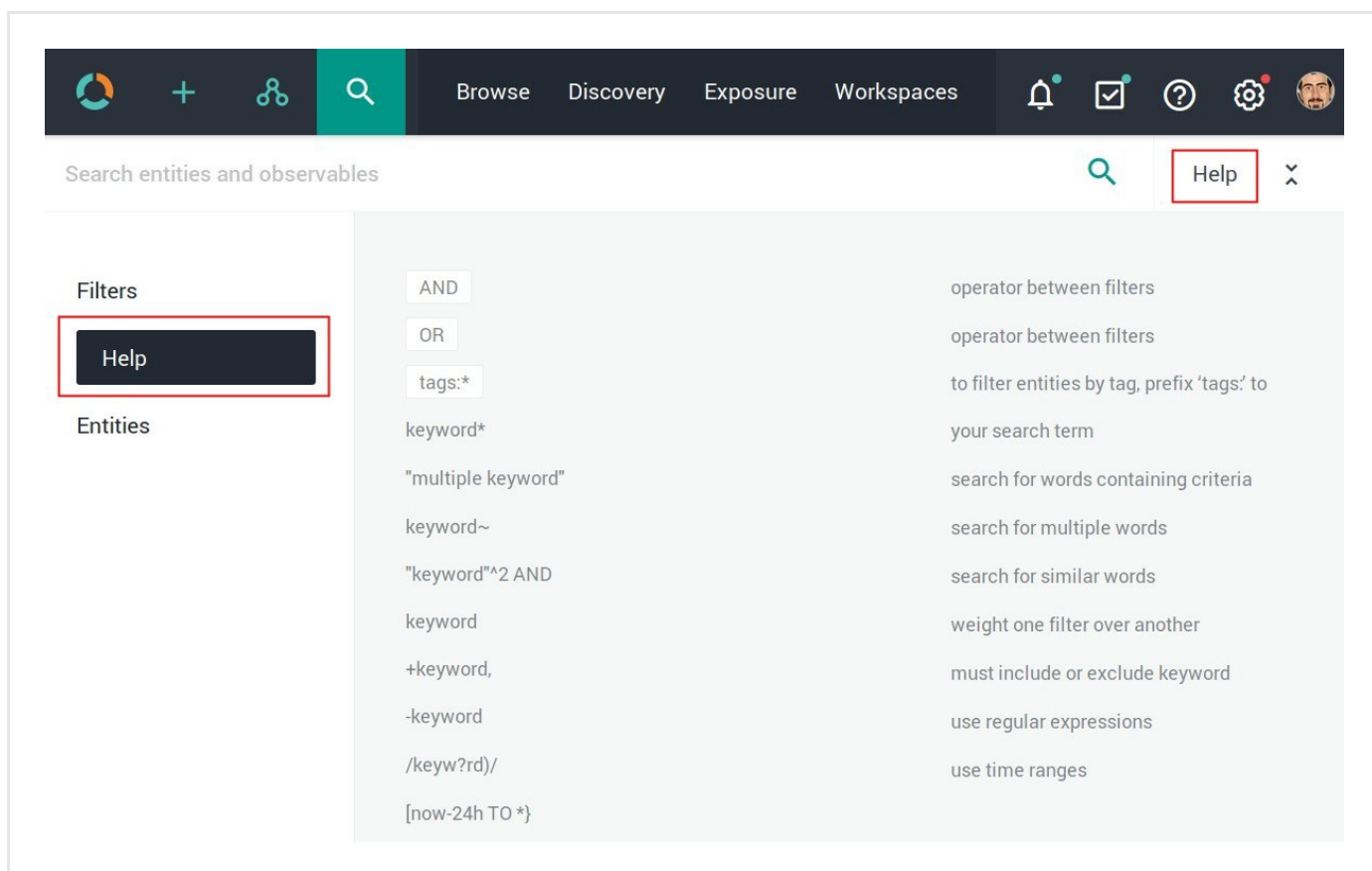
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
```

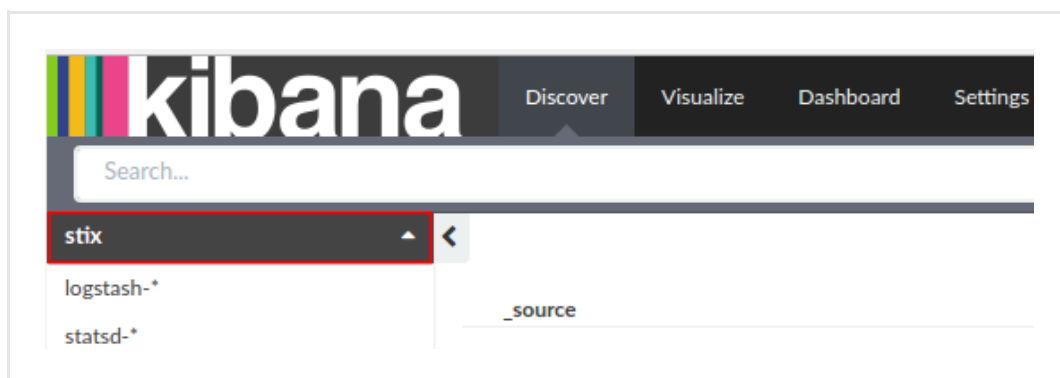
Field	Description	Example
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	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 GeolIP	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-sha512, 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**:

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 addresses 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	<code>https://api.dnsdb.info/{}</code>
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.

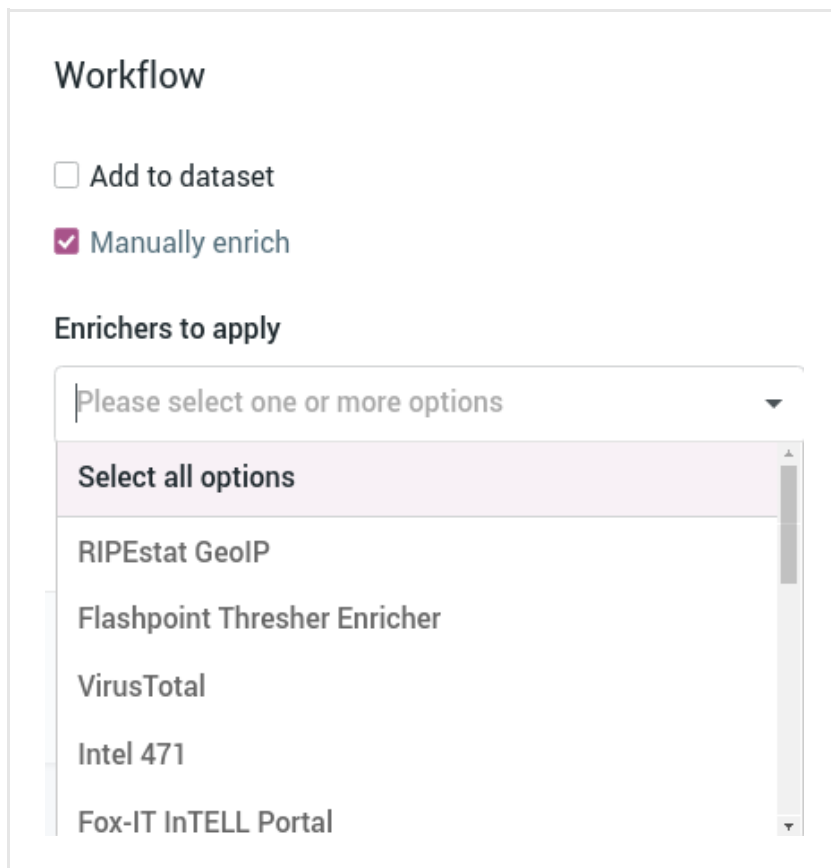
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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.



**Workflow**

☐ Add to dataset

☒ Manually enrich

**Enrichers to apply**

Please select one or more options

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv	Conn	Origins	Created	
←		Enrichment (1)	14 days ago	
←		Enrichment (1)	14 days ago	

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

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv	Conn	Origins	Created	
←		Enrichment (1)	14 days ago	
←		Enrichment (1)	14 days ago	

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 screenshot shows the EclecticIQ interface for a specific URL entity. At the top, a teal header bar displays the URL: `http://zebbugtennis.com/wp-conte...`. Below the header, a status bar indicates the entity was ingested on 09/15/2016 at 10:20 PM from the 'guest.phishtank\_c...' feed, with a 'TLP White' label.

The main interface has tabs for OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The 'OBSERVABLES' tab is active. On the left, an 'Enrich' dropdown menu is open, showing options: 'Enrich all observables', 'Enrich selected observables (6)' (highlighted with a red box), 'Elastic Sightings Enricher', and 'OpenResolve'.

Below the dropdown, a table lists the selected observables. The first column contains checkboxes, all of which are checked and highlighted with a red box. The table columns are: type, value, left arrow, count, conn, origins, status, and created time.

	uri	http://zebbugtennis.com/wp-co...	←	2	2	Entity	●	5 months ago	⋮
<input checked="" type="checkbox"/>	uri	http://zebbugtennis.com/wp-co...	←	1	1	Direct	●	5 months ago	⋮
<input checked="" type="checkbox"/>	hash-md5	a47a1906802faf32be76732366...	←	1	2	Entity (1)	●	5 months ago	⋮
<input checked="" type="checkbox"/>	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.

OVERVIEW

**OBSERVABLES**

NEIGHBORHOOD

JSON

VERSIONS

HISTORY

Enrich

Add observable

Actions 

Filters: Maliciousness

Origin


Kind

Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2	2 months ago	
<input type="checkbox"/>	country	us	2	2 months ago	
<input type="checkbox"/>	uri	http://t.esecurit...	2	2 months ago	
<input type="checkbox"/>	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

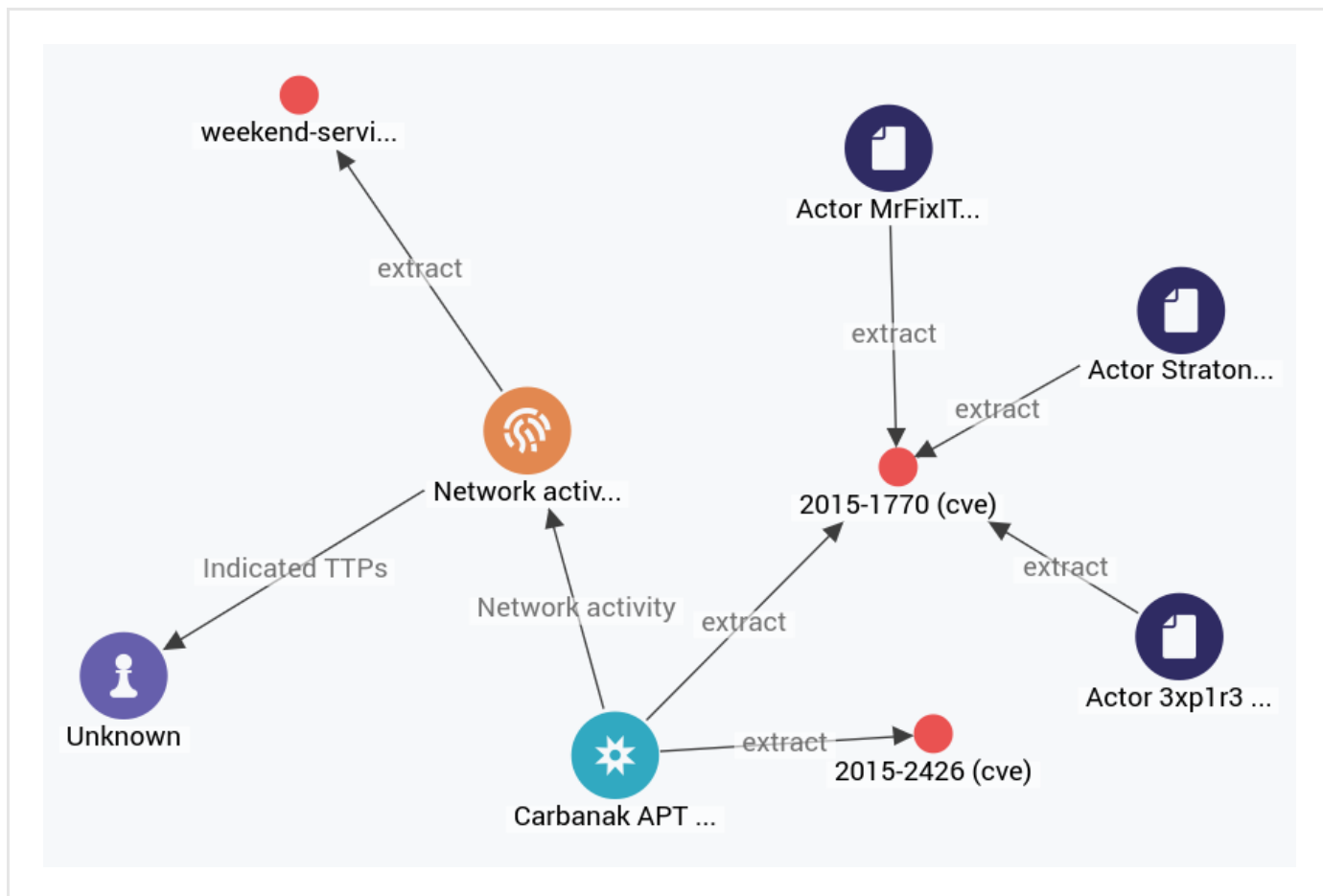
Ignore extract

Create sighting

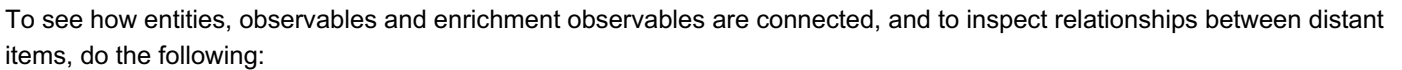
**Add to graph**

Set maliciousness >

- 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** .

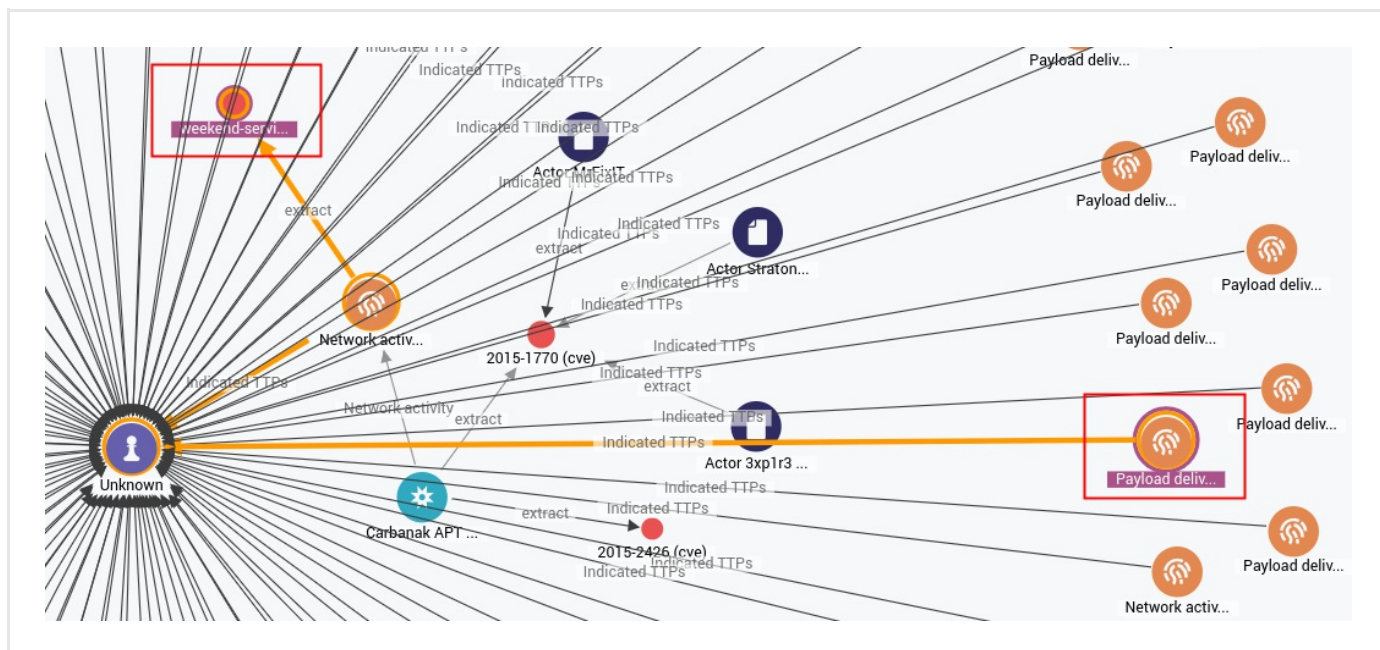


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All** , **Load observables > All** or **Load entities by extract > All** .



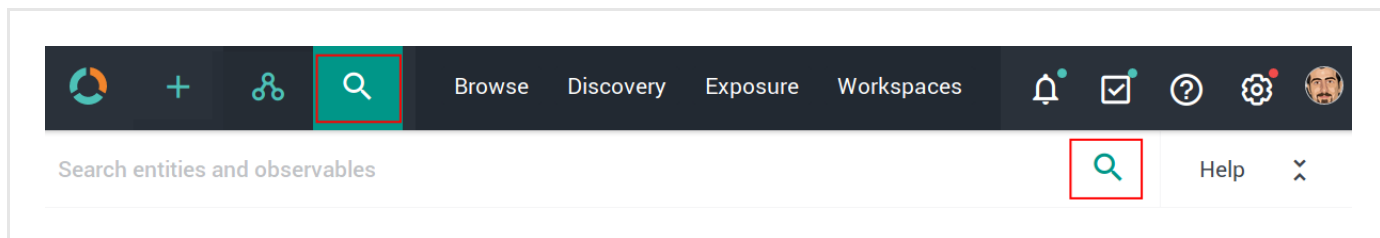
- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist, 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.

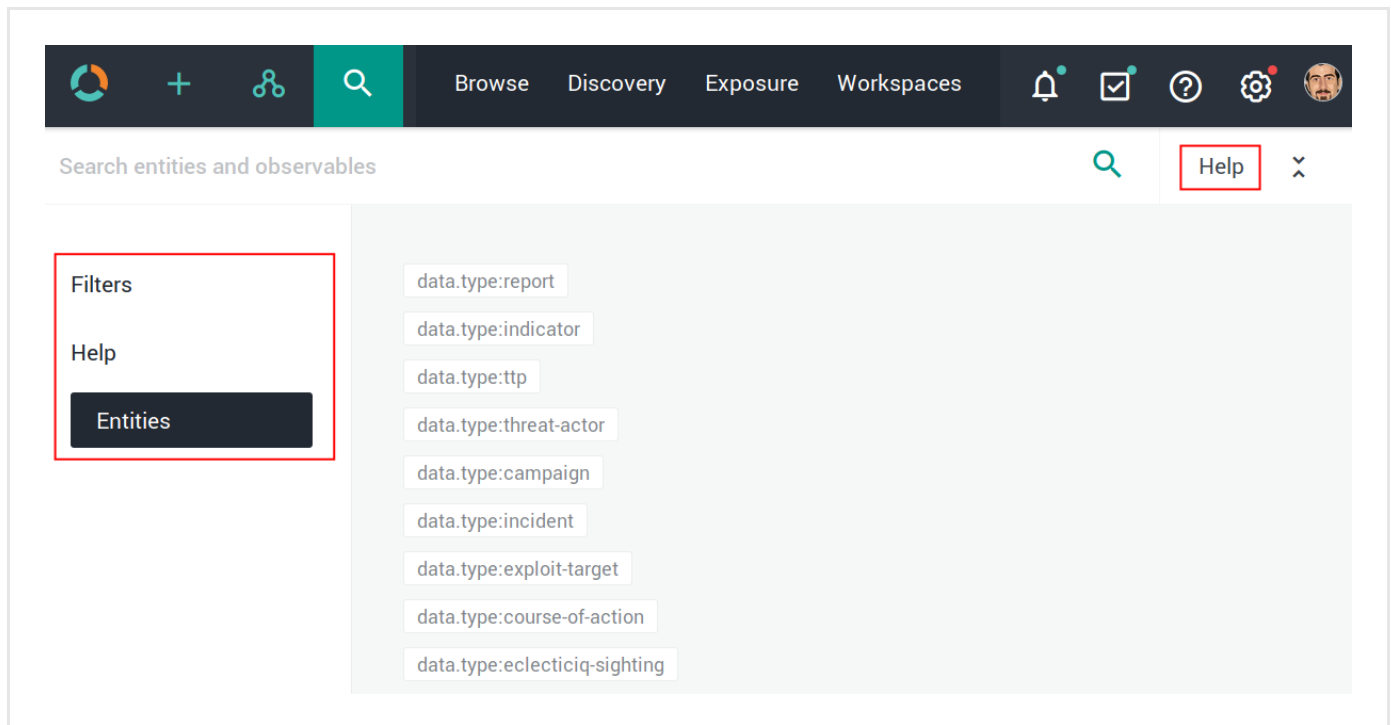


The search functionality uses **Elasticsearch query syntax**

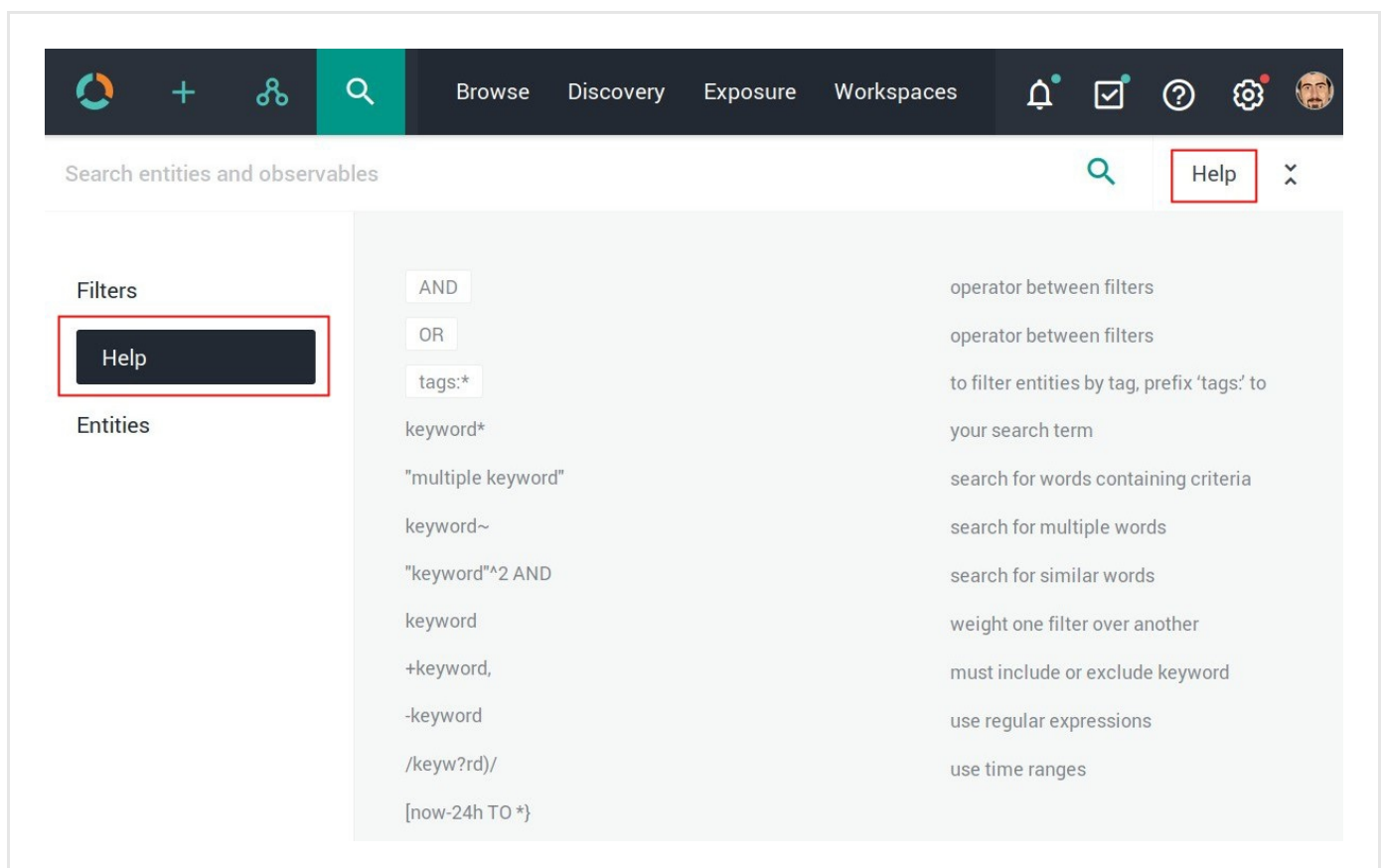
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
```

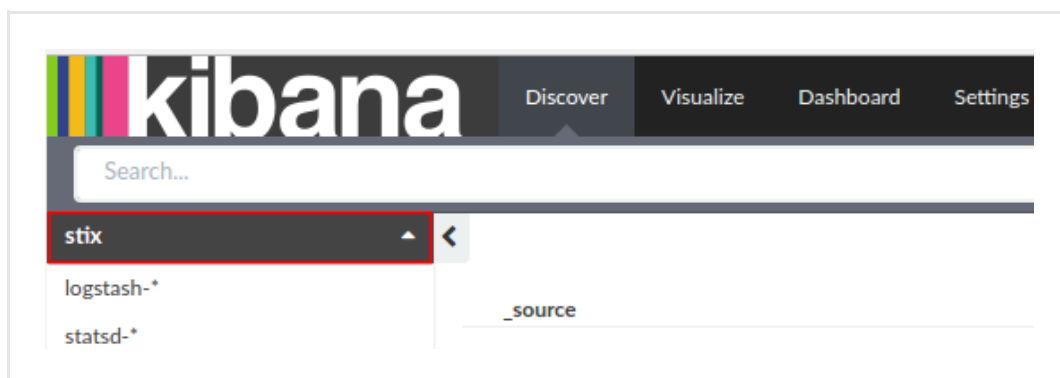
Field	Description	Example
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	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 GeolIP	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

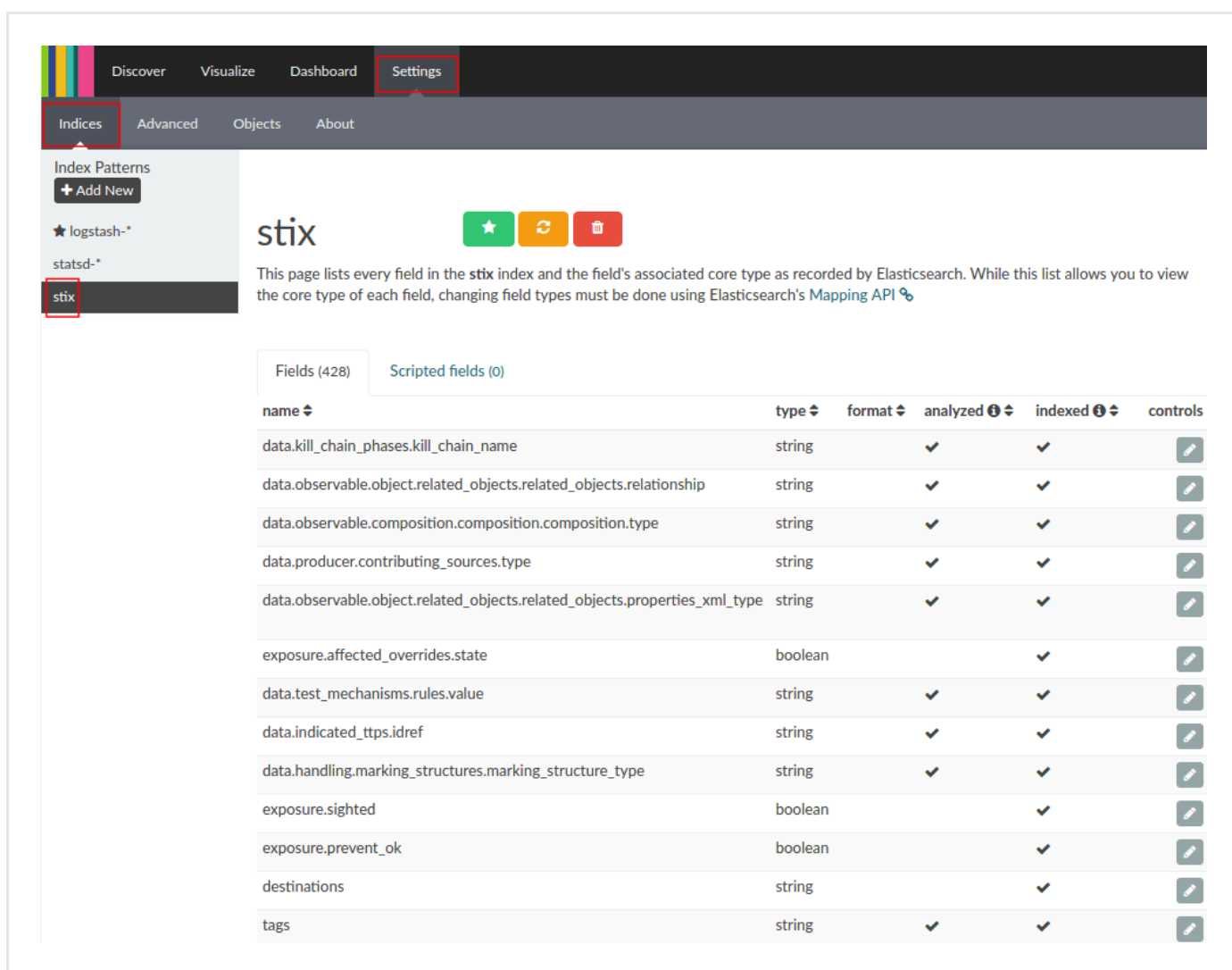
Enricher	Supported kinds (observable types)
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	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-sha512, 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**:



# 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](#).

<b>Flashpoint AggregINT</b>	<b>enricher</b>
<b>Enricher name</b>	Flashpoint AggregINT
<b>API endpoint</b>	<a href="https://endlesstunnel.info/v3">https://endlesstunnel.info/v3</a>
<b>Input</b>	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
<b>Output</b>	Enriches the supported observable types with information such as IP addresses, domains, host names, and hash files.
<b>Description</b>	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 <b>CBRN</b> ( <a href="https://en.wikipedia.org/wiki/cbrn_defense">https://en.wikipedia.org/wiki/cbrn_defense</a> ) 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 <b>ISO 8601</b> ( <a href="https://en.wikipedia.org/wiki/iso_8601">https://en.wikipedia.org/wiki/iso_8601</a> ) ( <b>RFC 3339</b> ) ( <a href="https://tools.ietf.org/html/rfc3339">https://tools.ietf.org/html/rfc3339</a> ) 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 supremacist 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](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.

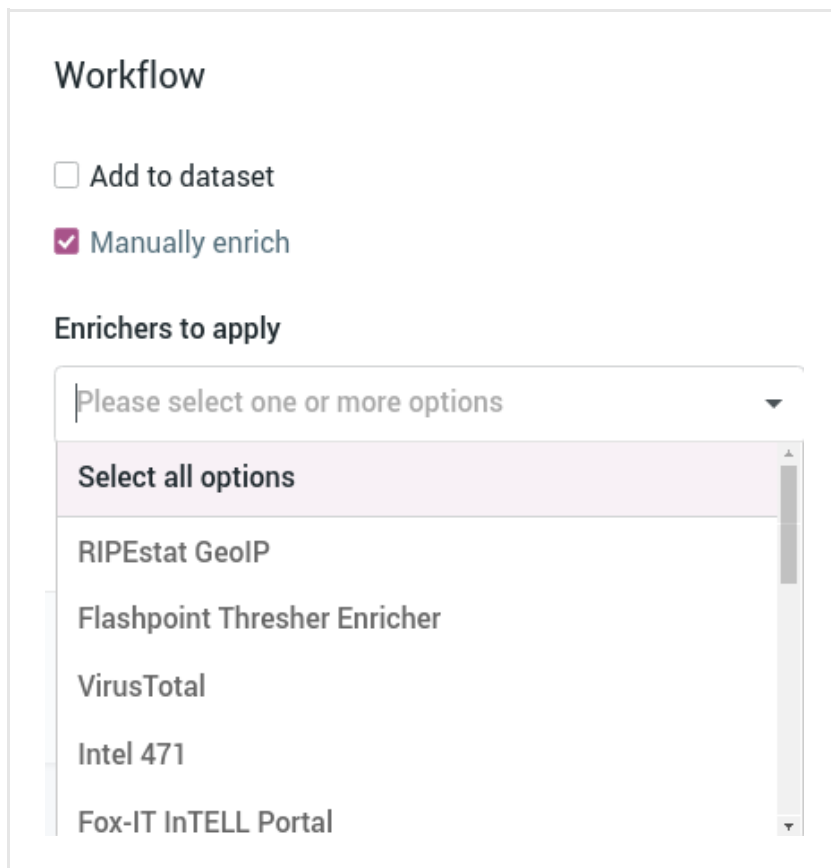
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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**

Please select one or more options

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▼

Enrich all observables

Enrich selected observables ▼

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin ▼ Maliciousness ▼ Date ▼

Lv Conn Origins Created ▼ ↻

Enrichment (1) 14 days ago ⋮

Enrichment (1) 14 days ago ⋮

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

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▼

Enrich all observables

Enrich selected observables ▼

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin ▼ Maliciousness ▼ Date ▼

Lv Conn Origins Created ▼ ↻

Enrichment (1) 14 days ago ⋮

Enrichment (1) 14 days ago ⋮

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 screenshot shows the Flashpoint AggregINT interface. At the top, a teal header bar displays the URL: `http://zebbugtennis.com/wp-conte...` with a close button. Below the header, a status bar shows 'Ingested: 09/15/2016 10:20 PM' and 'Incoming feed: guest.phishtank\_c...' with a 'TLP White' button. The main interface has tabs: OVERVIEW, OBSERVABLES (selected), NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The 'OBSERVABLES' tab shows a dropdown menu for 'Enrich' with options: 'Enrich all observables', 'Enrich selected observables (6)' (highlighted with a red box), 'Elastic Sightings Enricher', and 'OpenResolve'. Below the menu is a table of observables with columns: Origin, Maliciousness, Date, Lv, Conn, Origins, and Created. The table contains four rows of data, each with a checkbox in the first column (all checked and highlighted with a red box).

	Origin	Maliciousness	Date	Lv	Conn	Origins	Created
<input checked="" type="checkbox"/>	uri		5 months ago	2	2	Entity	7 days ago
<input checked="" type="checkbox"/>	uri		5 months ago	1	1	Direct	7 days ago
<input checked="" type="checkbox"/>	hash-md5		5 months ago	1	2	Entity (1)	7 days ago
<input checked="" type="checkbox"/>	domain		5 months ago	1	10	Entity (3)	7 days 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.

OVERVIEW

**OBSERVABLES**

NEIGHBORHOOD

JSON

VERSIONS

HISTORY

Enrich

Add observable

Actions 

Filters: Maliciousness

Origin


Kind

Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2 <div></div>	2 months ago	
<input type="checkbox"/>	country	us	2 <div></div>	2 months ago	
<input type="checkbox"/>	uri	http://t.esecurit...	2 <div></div>	2 months ago	
<input type="checkbox"/>	name	vcdb	2 <div></div>	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

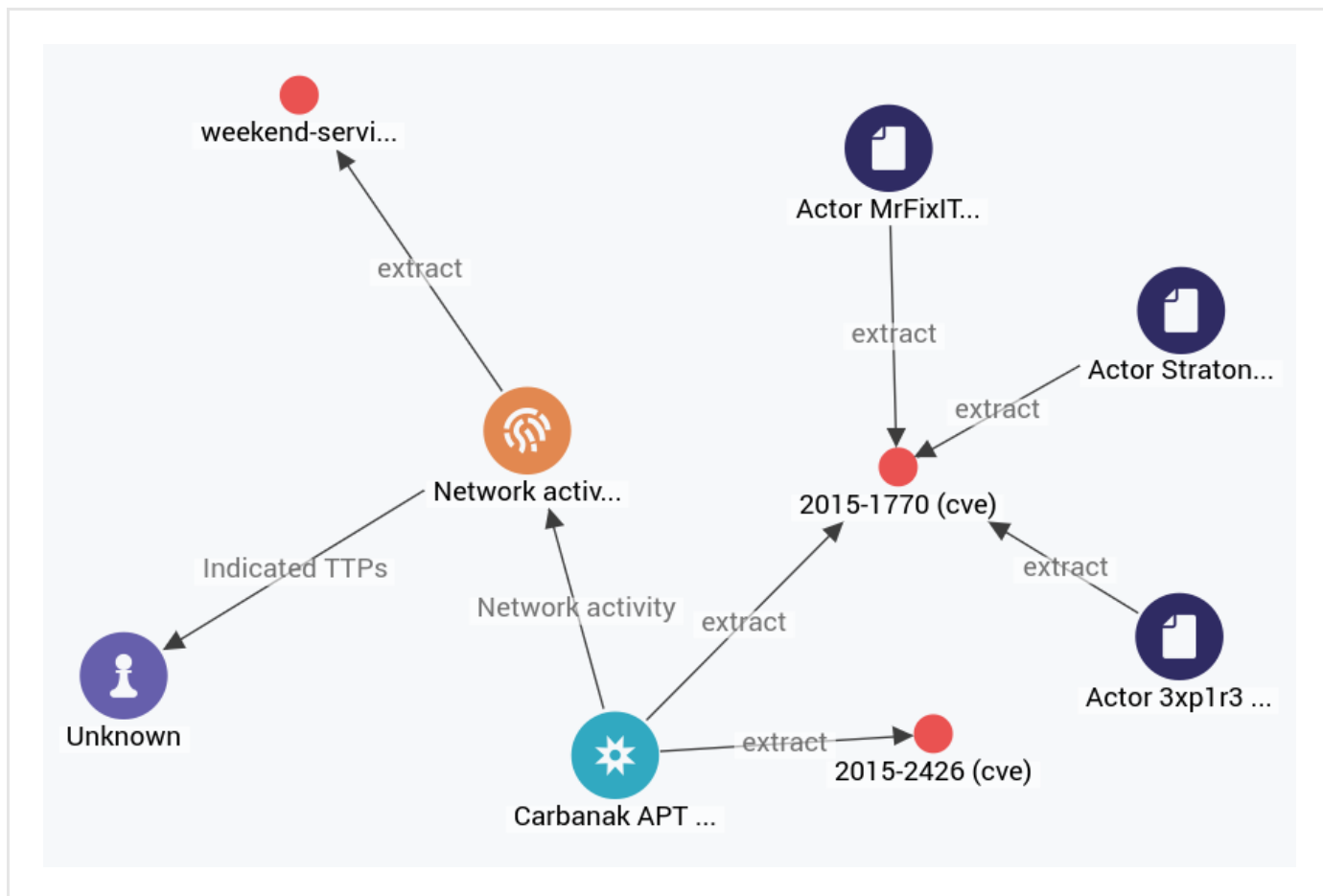
Ignore extract

Create sighting

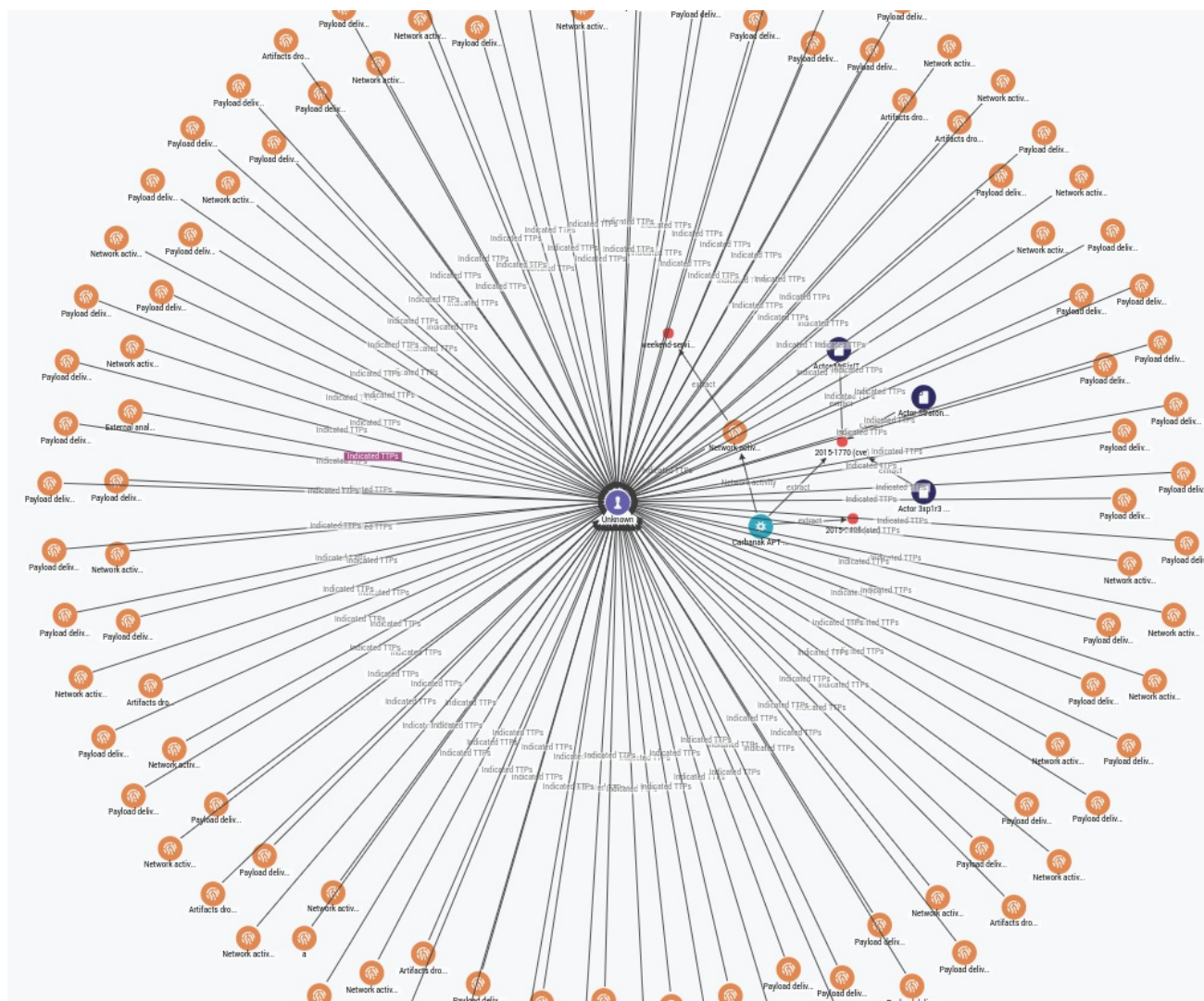
**Add to graph**

Set maliciousness >

- 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** .



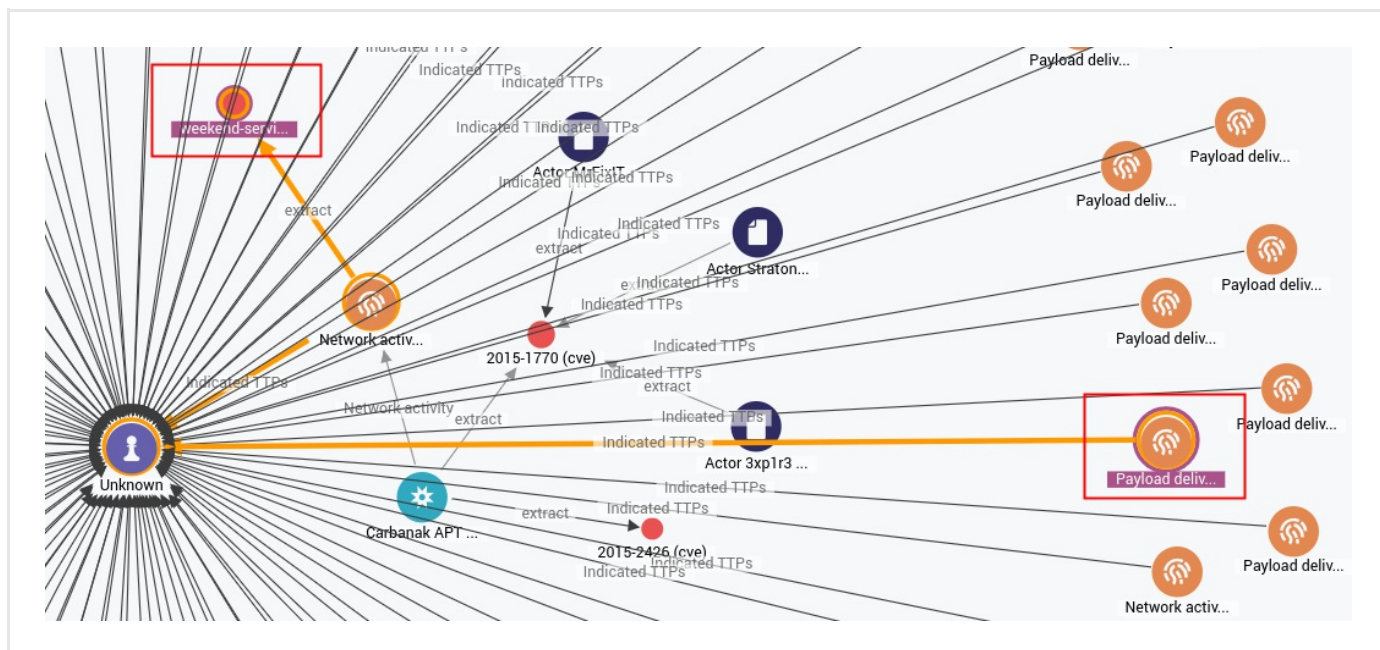
- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All** , **Load observables > All** or **Load entities by extract > All** .



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

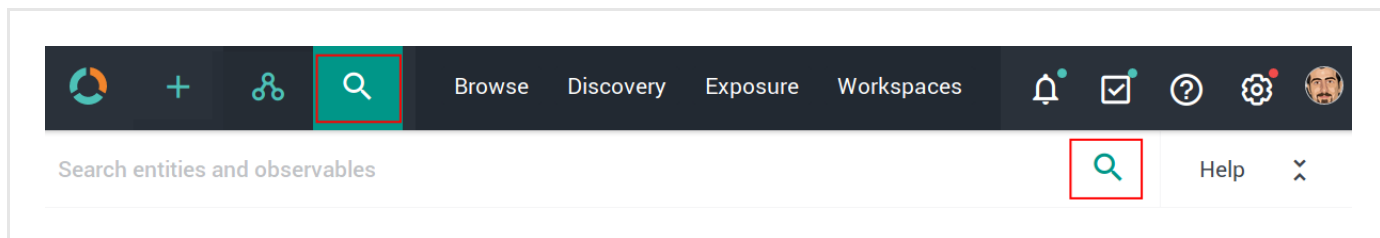
- **CTRL + click** two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist, 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.

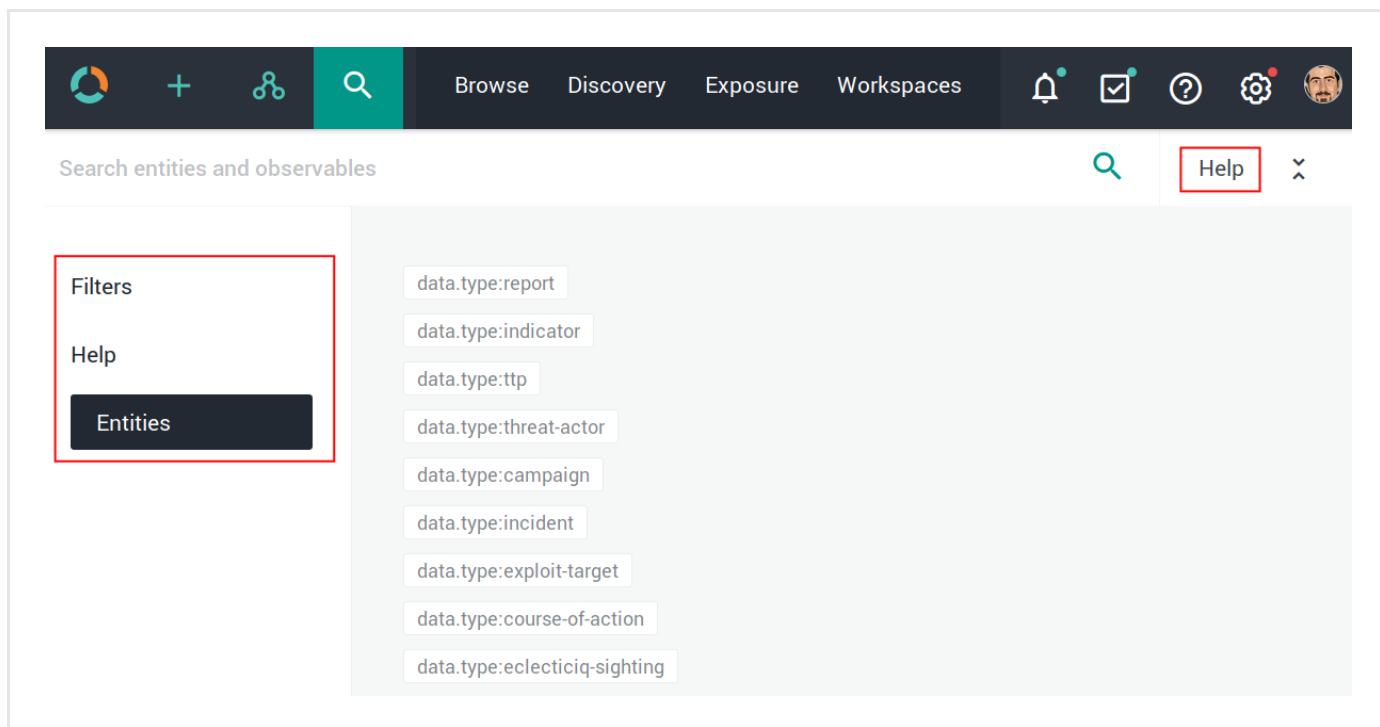


The search functionality uses **Elasticsearch query syntax**

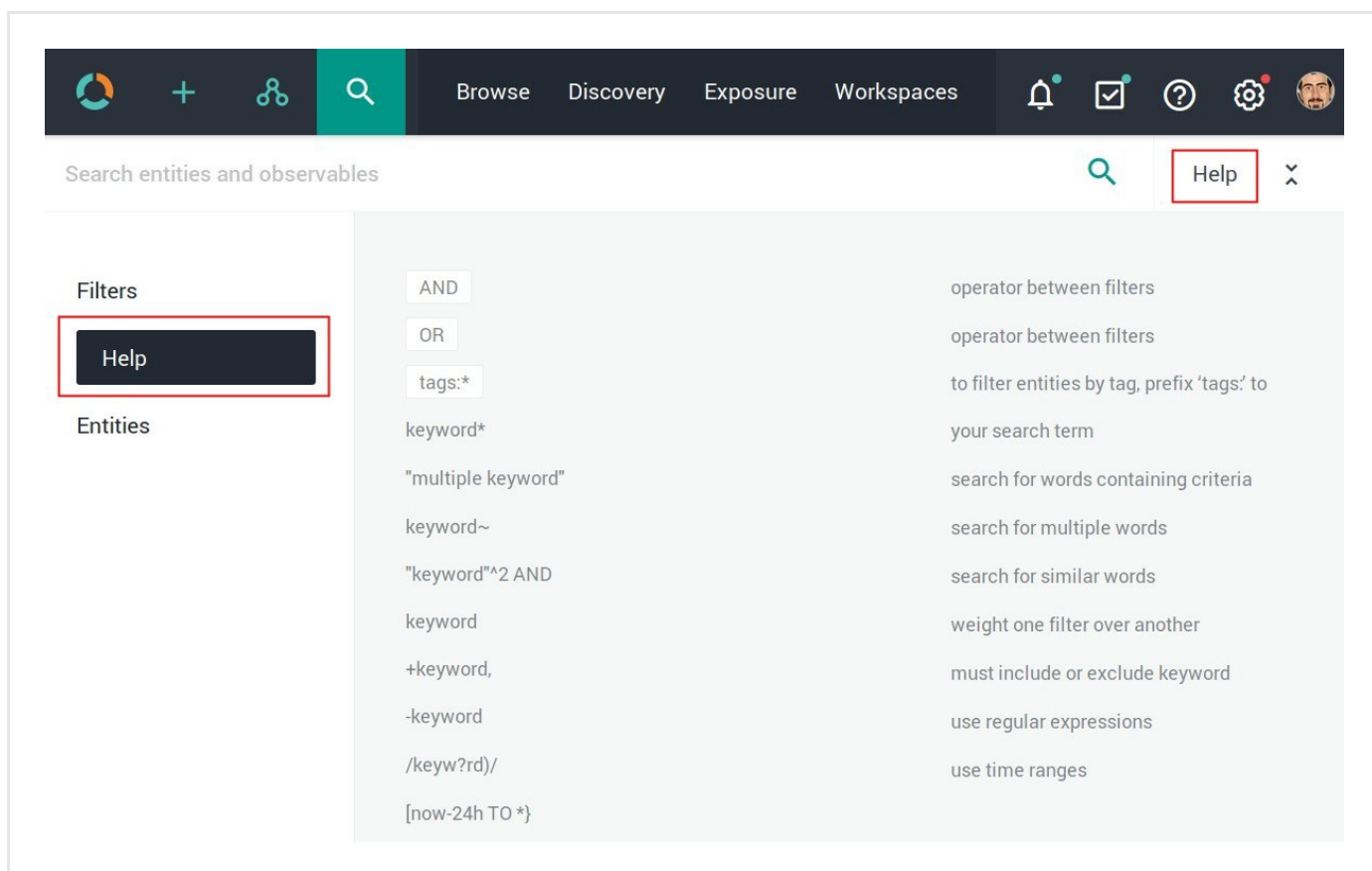
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
```

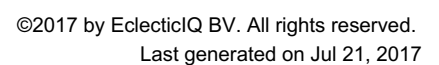
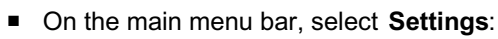
Field	Description	Example
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	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 GeolIP	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-sha512, 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:



# 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](#).

<b>Flashpoint Blueprint</b>	<b>enricher</b>
<b>Enricher name</b>	Flashpoint Blueprint
<b>API endpoint</b>	<a href="https://endlesstunnel.info/v3">https://endlesstunnel.info/v3</a>
<b>Input</b>	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
<b>Output</b>	Enriches the supported observable types with information such as IP addresses, domains, host names, and URLs.
<b>Description</b>	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 <b>CBRN</b> ( <a href="https://en.wikipedia.org/wiki/cbrn_defense">https://en.wikipedia.org/wiki/cbrn_defense</a> ) 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](#).

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

## Configure the Flashpoint Thresher enricher



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](#).


<b>DomainTools Hosted Domains</b>	<b>enricher</b>
<b>Enricher name</b>	DomainTools Hosted Domains
<b>API endpoint</b>	<code>http://api.domaintools.com/v1/{}/host-domains</code>
<b>Input</b>	ipv4
<b>Output</b>	Enriches the supported observable types with domain and host name information.
<b>Description</b>	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.

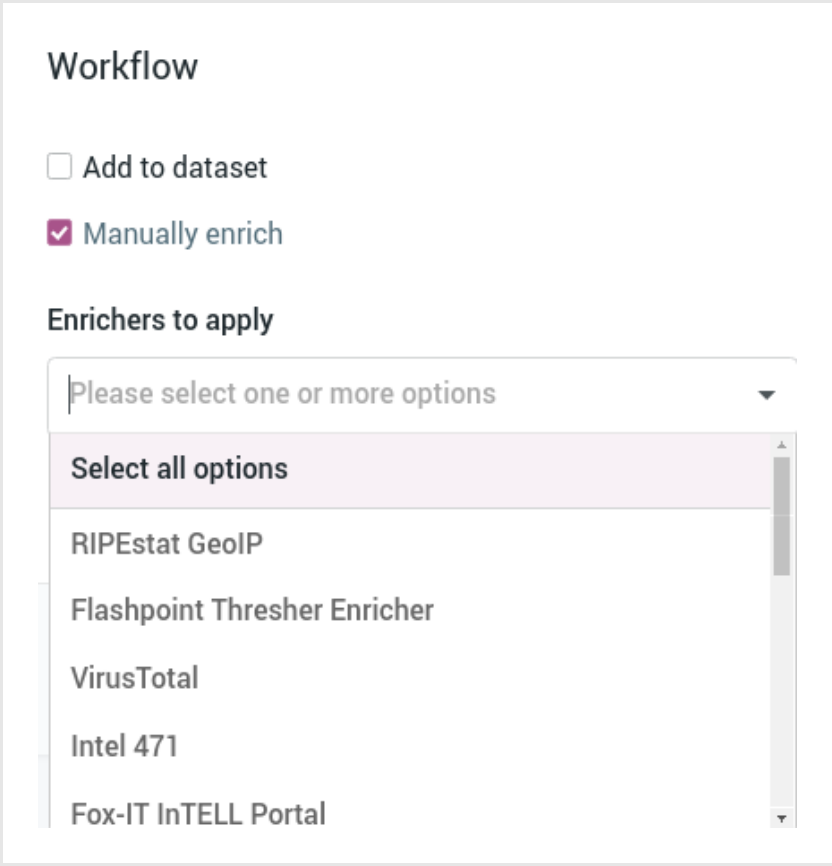
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 ▼

- Select all options
- RIPEstat GeolP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.


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

To manually enrich the entity observables:

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

Alternatively:

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



The screenshot shows the 'Sighting of uri: http://www.panazan.ro/o...' entity detail pane. The 'OBSERVABLES' tab is selected. The 'Enrich' dropdown menu is open, showing options: 'Enrich', 'Enrich all observables', 'Enrich selected observables', 'Elastic Sightings Enricher', and 'OpenResolve'. The 'Enrich all observables' option is highlighted. To the right of the dropdown is an 'ADD OBSERVABLE' button. Below the dropdown is a table of observables with columns: Origin, Maliciousness, Date, Lv, Conn, Origins, and Created. The 'Created' column has a refresh icon (circular arrow) next to it, which is highlighted with a red box. The table shows two rows of enrichment data, each with a status indicator (a circle) and a timestamp '14 days ago'.

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

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▾

ADD OBSERVABLE

Enrich all observables

Enrich selected observables ▾

Elastic Sightings Enricher

**OpenResolve**

Origin ▾	Maliciousness ▾	Date ▾	Lv	Conn	Origins	Created ▾	↻
←	Enrichment (1)	14 days ago					⋮
←	Enrichment (1)	14 days ago					⋮

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://zebugtennis.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	
<input checked="" type="checkbox"/> uri	<a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	2	2
<input checked="" type="checkbox"/> uri	<a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	1	1
<input checked="" type="checkbox"/> hash-md5	<a href="#">a47a1906802faf32be76732366...</a>	1	2
<input checked="" type="checkbox"/> domain	<a href="#">zebugtennis.com</a>	1	10

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.

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Add observable

Actions Filters: Maliciousness  Origin  Kind  Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2		2 months ago
<input type="checkbox"/>	country	us	2		2 months ago
<input type="checkbox"/>	uri	http://t.esecurit...	2		2 months ago
<input type="checkbox"/>	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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdb	2		

Ignore extract

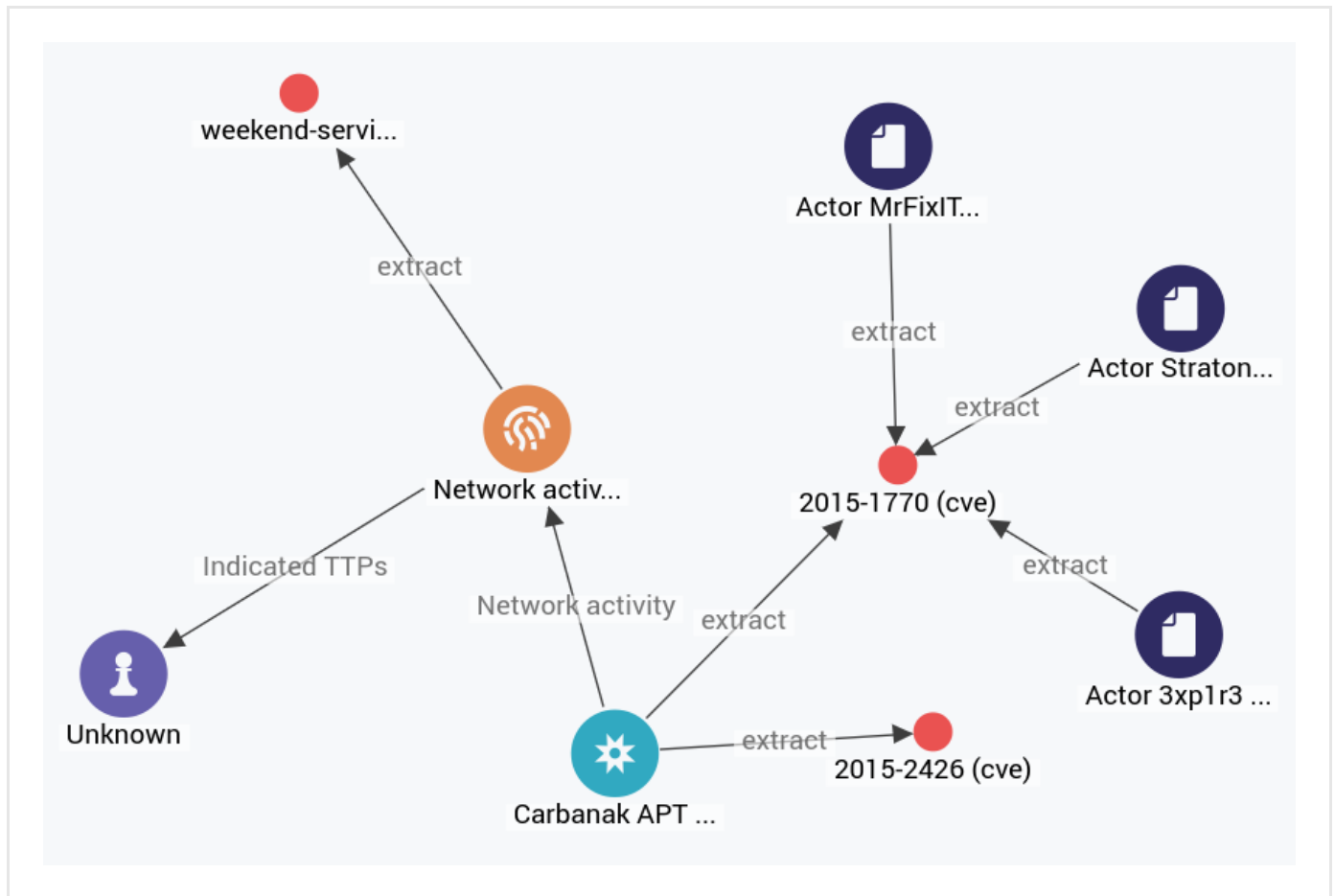
Create sighting

**Add to graph**

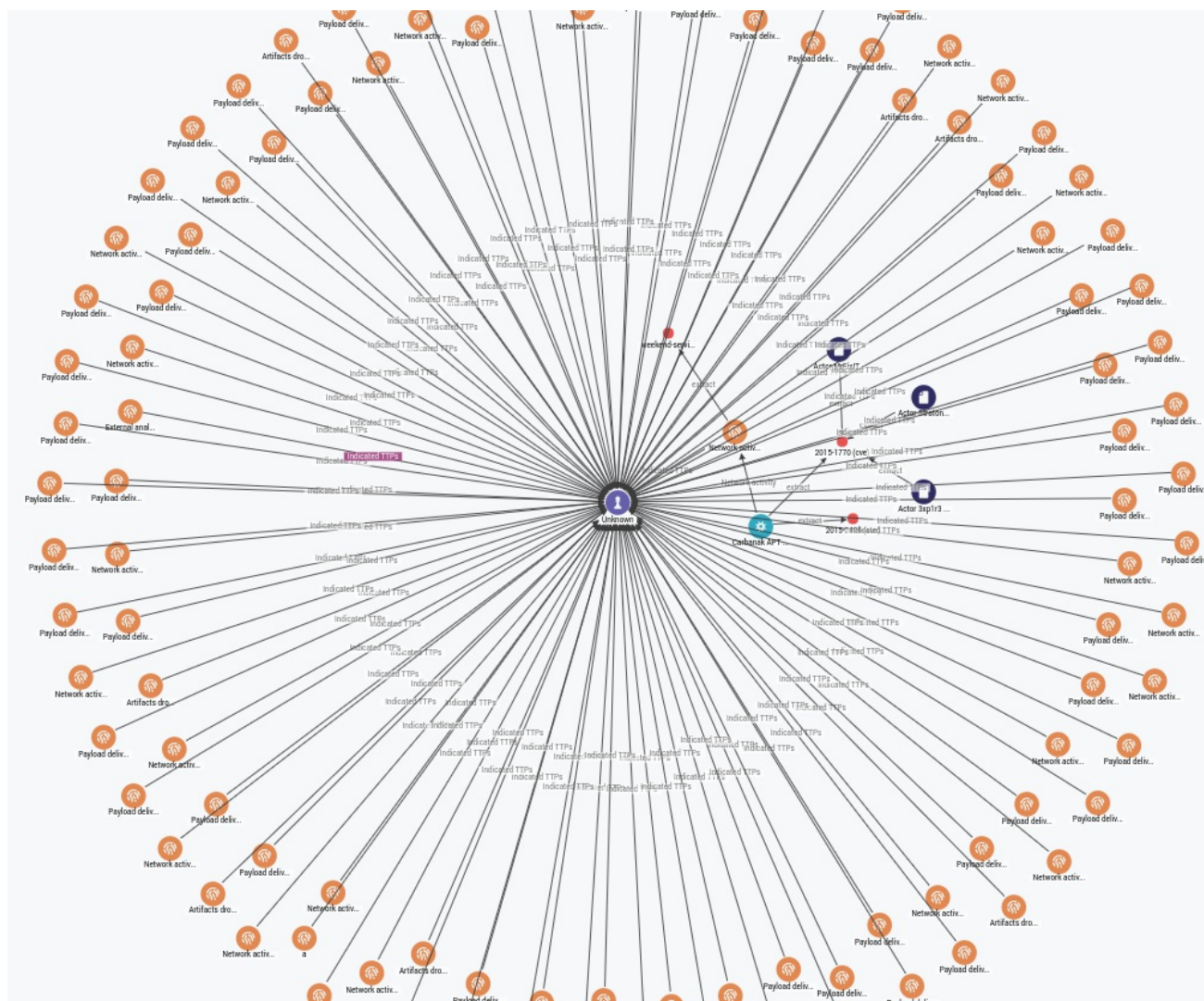
Set maliciousness >

- 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**.

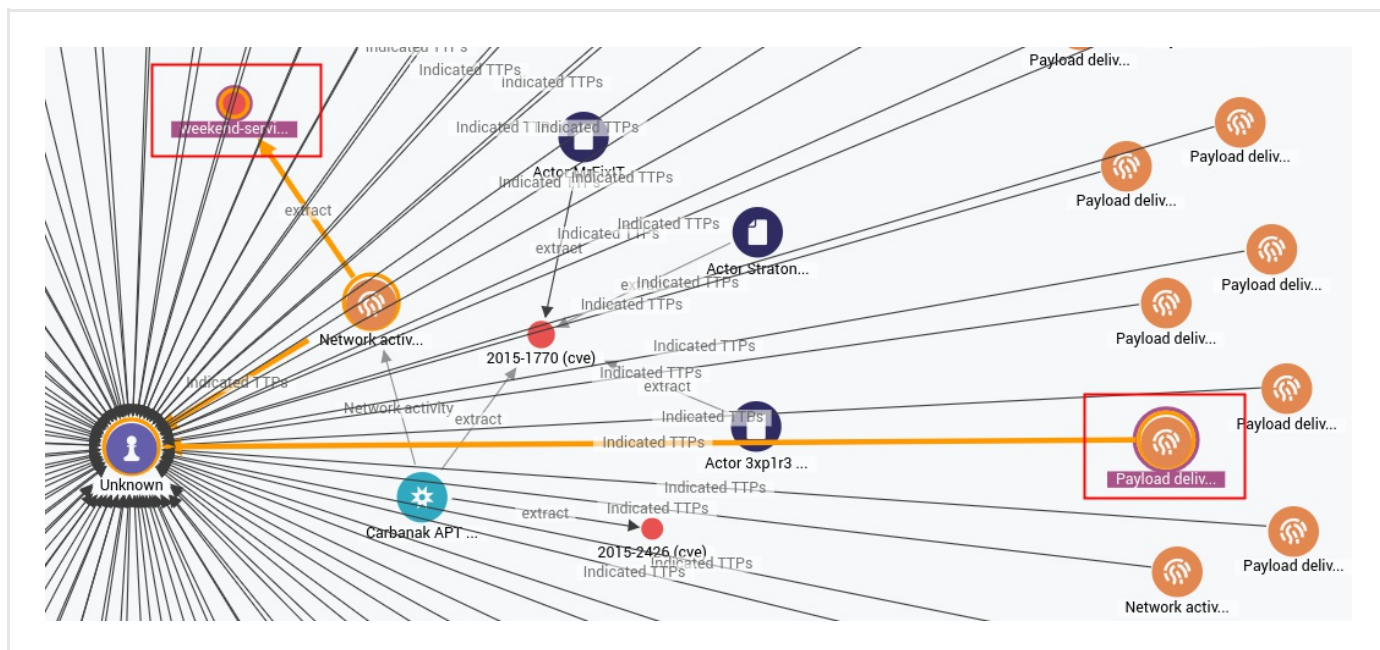


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



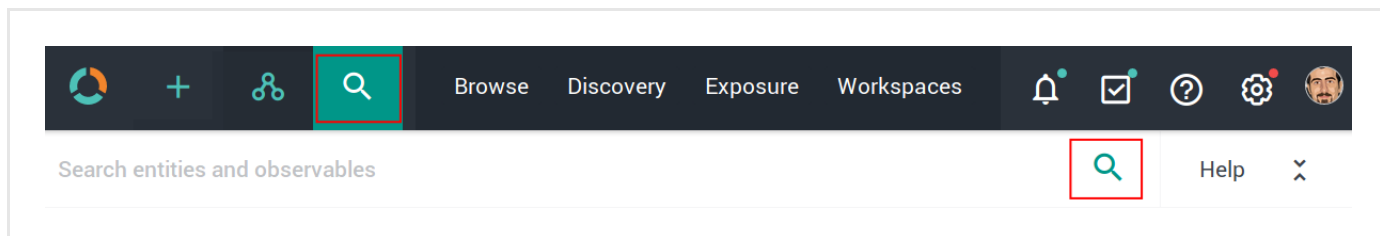
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 an 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.

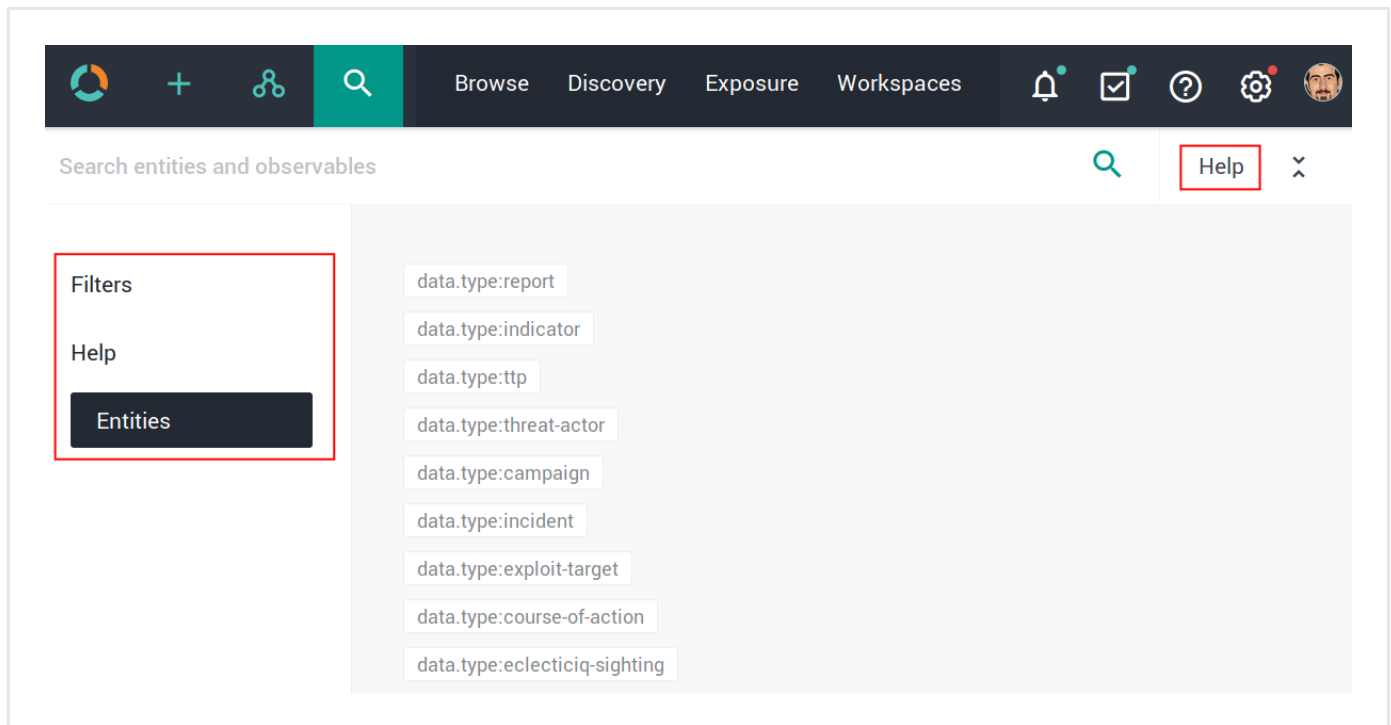


The search functionality uses **Elasticsearch query syntax**

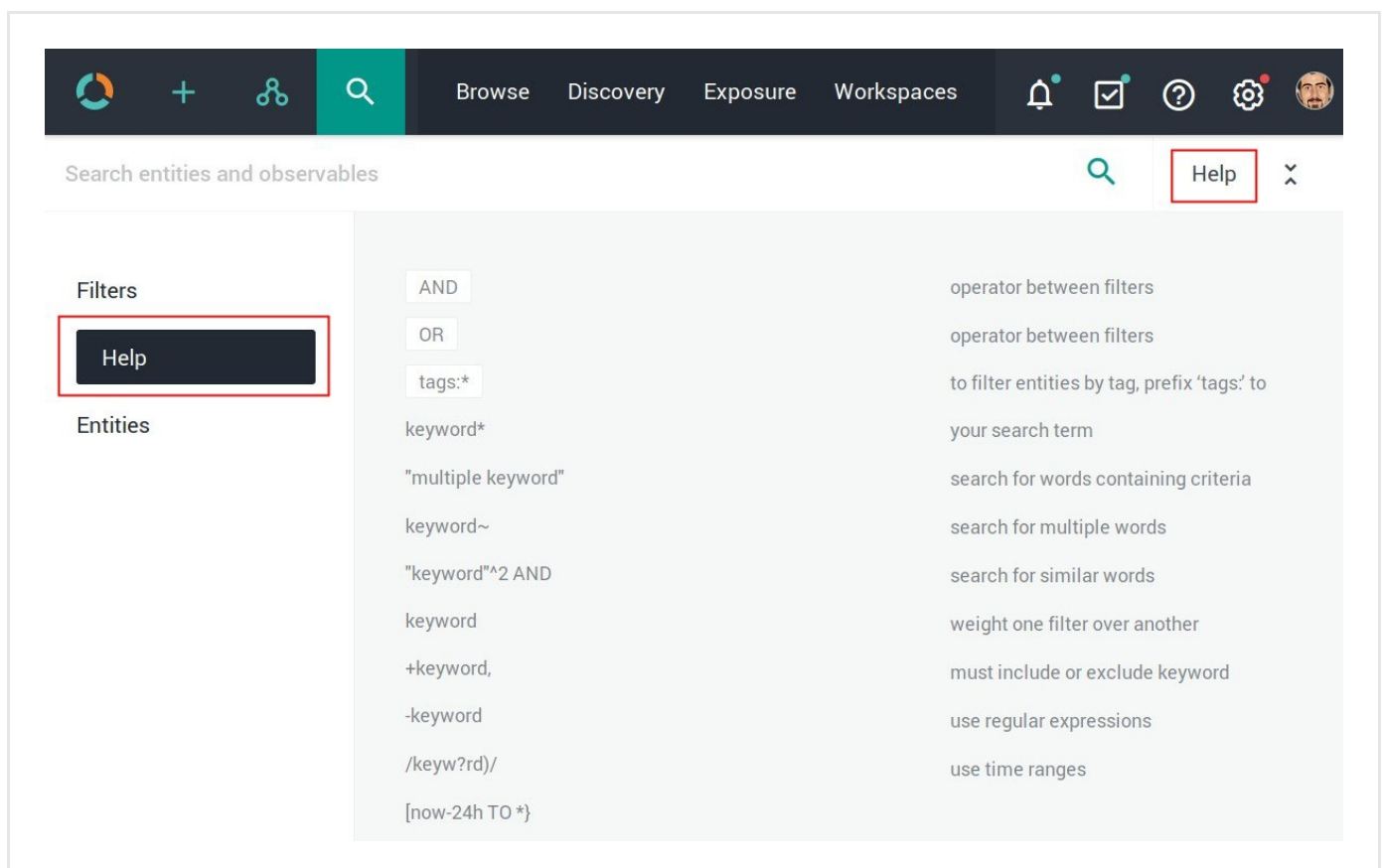
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	string — The actual value of the enrichment observable, based on the enrichment observable data type.	doom.dismay.biz

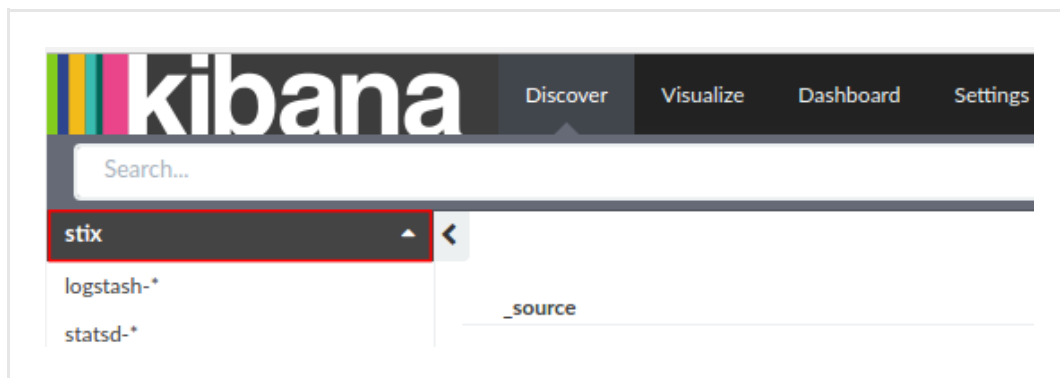
Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeolIP	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-sha512, 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**:

A screenshot of the Kibana Settings page for the 'stix' index pattern. The page has a dark header with navigation tabs: Discover, Visualize, Dashboard, and Settings. The 'Settings' tab is selected. Below the header is a sub-menu with tabs: Indices, Advanced, Objects, and About. The 'Indices' tab is selected. The left sidebar shows the index pattern 'stix' selected. The main content area displays the 'stix' index pattern with a star icon, a refresh icon, and a delete icon. Below this is a description: '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'. Below the description is a table with 6 columns: name, type, format, analyzed, indexed, and controls. The table lists 14 fields with their respective types and settings. The 'Fields (428)' tab is selected, and the 'Scripted fields (0)' tab is also visible.

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](#).


<b>DomainTools Malicious Server Domains</b>	<b>enricher</b>
<b>Enricher name</b>	DomainTools Malicious Server Domains
<b>API endpoint</b>	<code>http://api.domaintools.com/v1/{}/name-server-domains/</code>
<b>Input</b>	domain, host
<b>Output</b>	Enriches the supported observable types with malicious domain names that are served from the same name server.
<b>Description</b>	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

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv	Conn	Origins	Created	
←		Enrichment (1)	14 days ago	⋮
←		Enrichment (1)	14 days ago	⋮

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

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv	Conn	Origins	Created	
←		Enrichment (1)	14 days ago	⋮
←		Enrichment (1)	14 days ago	⋮

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 screenshot shows the EclecticIQ interface for an entity. At the top, a teal banner displays the URL: `http://zebbugtennis.com/wp-conte...`. Below the banner, a status bar indicates 'Ingested: 09/15/2016 10:20 PM' and 'Incoming feed: guest.phishtank\_c...'. A 'TLP White' button is visible on the right.

The main interface has tabs: OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The 'OBSERVABLES' tab is active.

An 'Enrich' dropdown menu is open, showing options: 'Enrich all observables', 'Enrich selected observables (6)' (highlighted with a red box), 'Elastic Sightings Enricher', and 'OpenResolve'.

Below the menu, a table lists observables. The first four rows have checkboxes in the left margin, all of which are checked and highlighted with a red box. The table columns include type, value, origin, maliciousness, and date.

	Origin	Maliciousness	Date
uri <a href="http://zebbugtennis.com/wp-co...">http://zebbugtennis.com/wp-co...</a>	Lv	Conn	Origins
uri <a href="http://zebbugtennis.com/wp-co...">http://zebbugtennis.com/wp-co...</a>	1	1	Direct
hash-md5 <a href="#">a47a1906802faf32be76732366...</a>	1	2	Entity (1)
domain <a href="#">zebbugtennis.com</a>	1	10	Entity (3)

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.

OVERVIEW	OBSERVABLES	NEIGHBORHOOD	JSON	VERSIONS	HISTORY
<div>Enrich <span>▼</span> <span>Add observable</span></div>					
Actions <span>▼</span> Filters: Maliciousness <span>▼</span> Origin <span>▼</span> Kind <span>▼</span> Date <span>▼</span>					
<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED <span>▼</span>	<span>↻</span>
<input type="checkbox"/>	domain	t.esecurityplanet...	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	country	us	2 <span>+</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	uri	http://t.esecurit...	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	name	vcdb	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>

## 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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED <span>▼</span>	<span>↻</span>
<input type="checkbox"/>	domain	www.thestar.com.my	2 <span>+</span>	a month ago	<span>⋮</span>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2 <span>+</span>		
<input type="checkbox"/>	country	my	2 <span>+</span>		
<input type="checkbox"/>	uri	notes:the	2 <span>+</span>		
<input type="checkbox"/>	name	vcdb	2 <span>+</span>		

Ignore extract

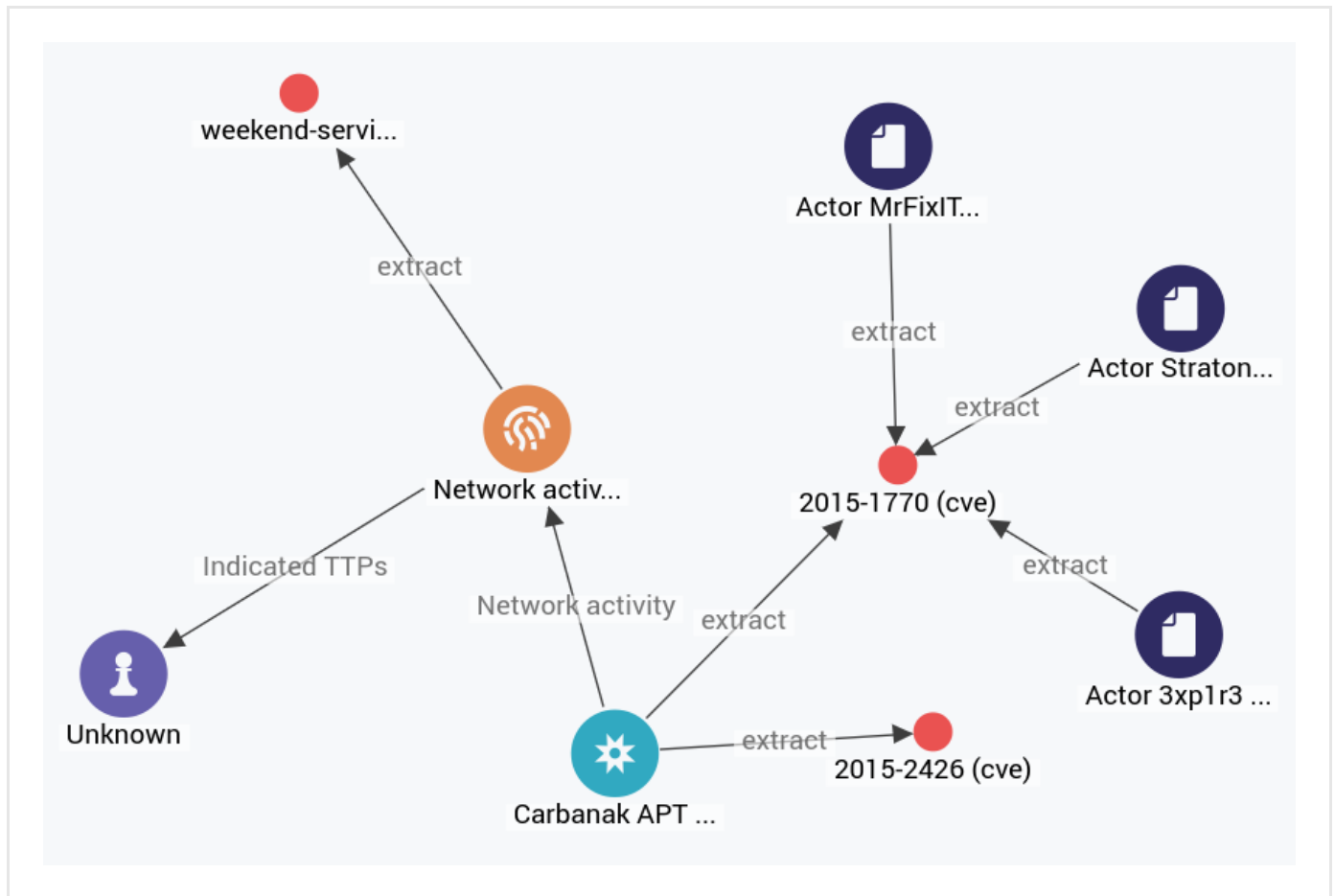
Create sighting

Add to graph

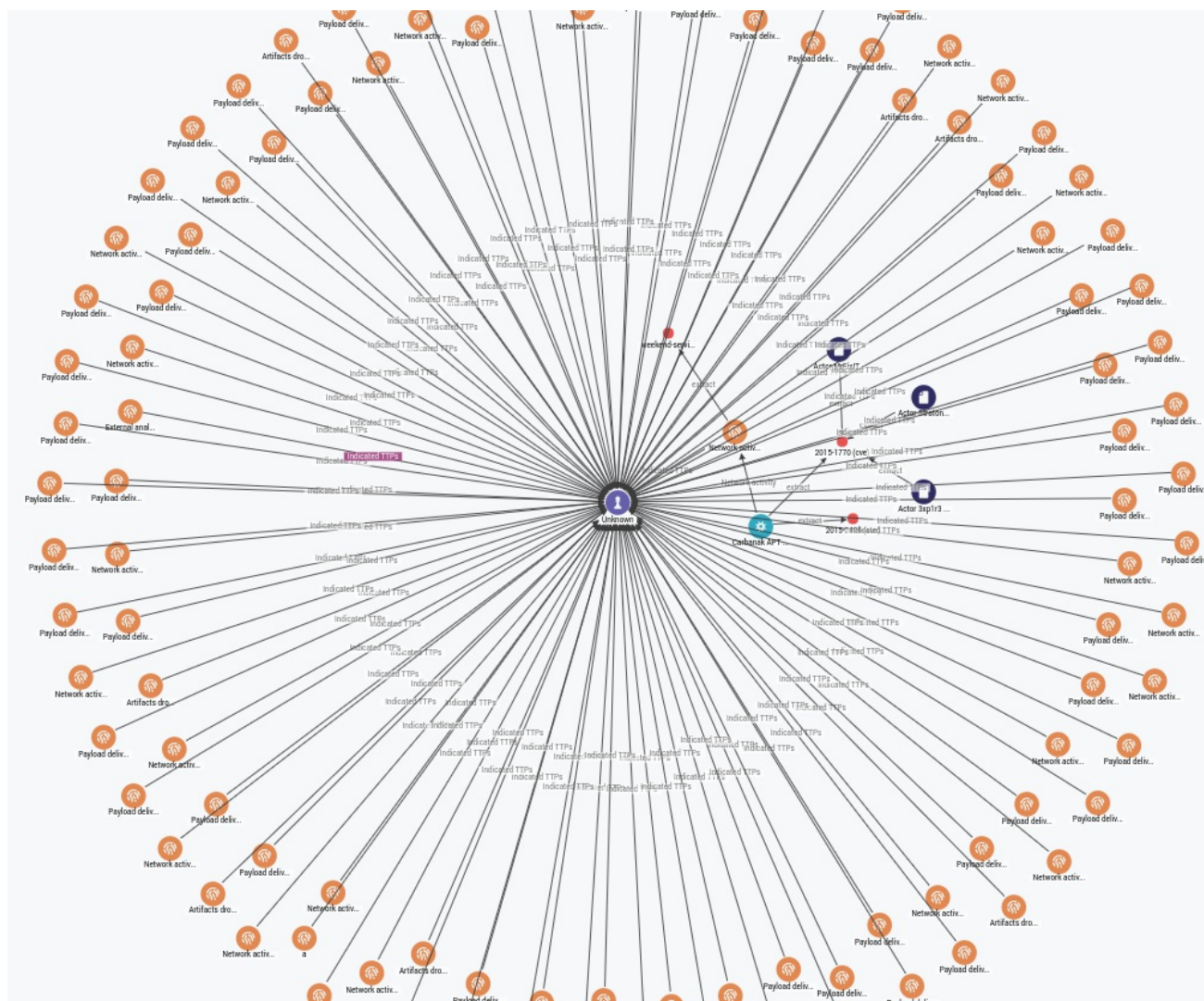
Set maliciousness >

- 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**.

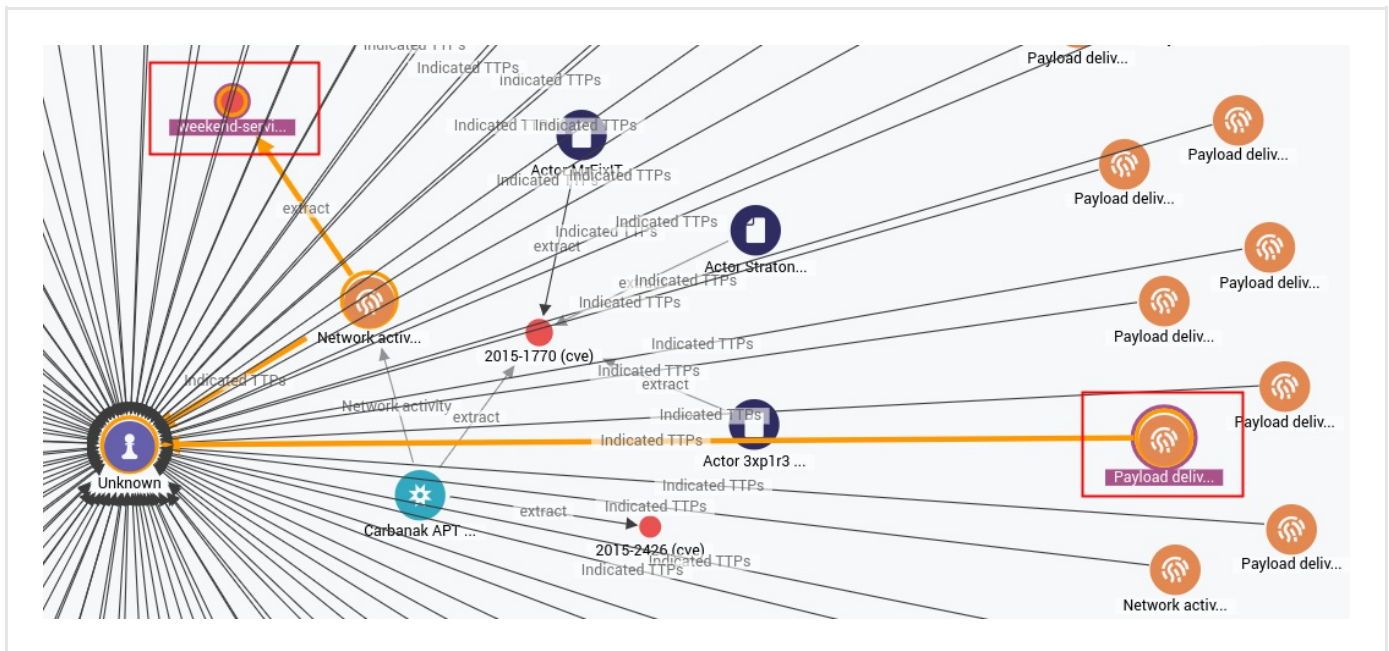


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



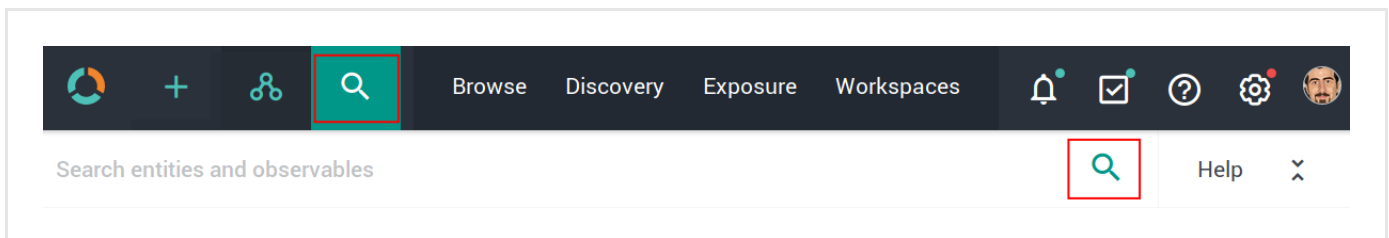
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 an 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.

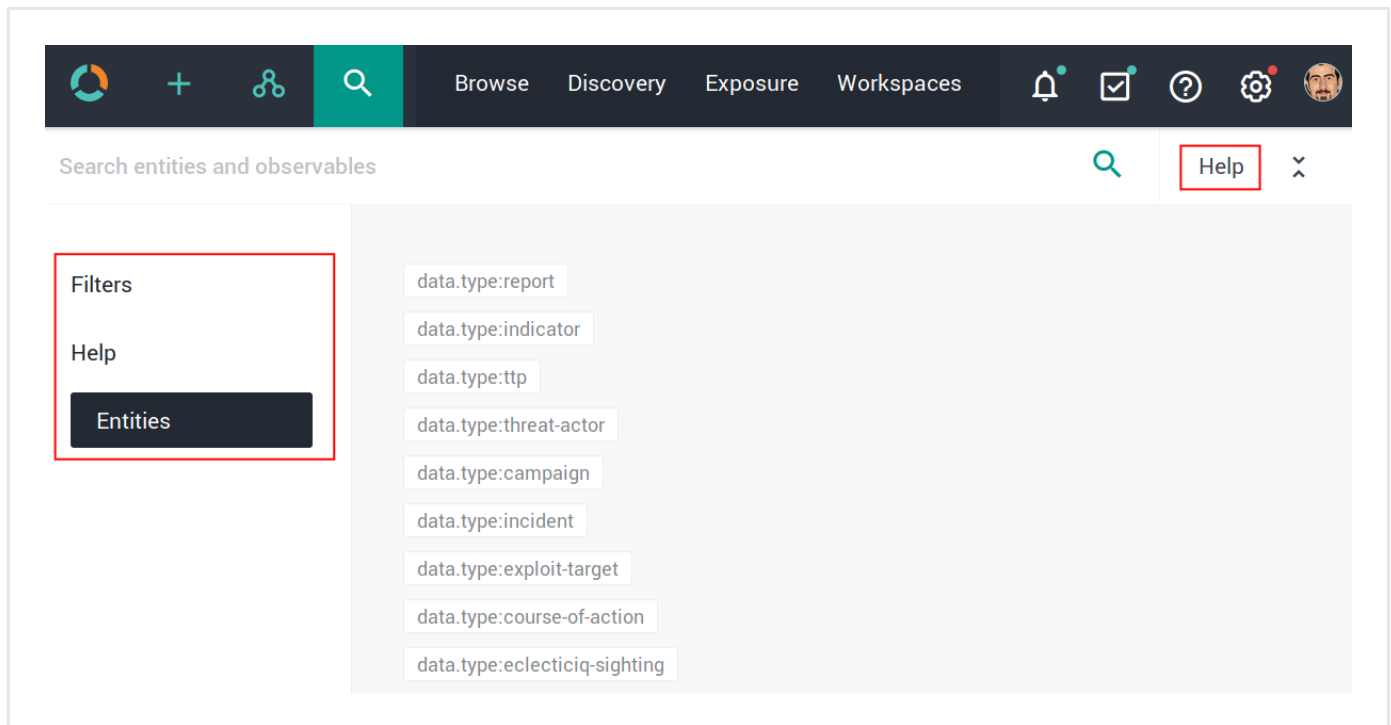


The search functionality uses **Elasticsearch query syntax**

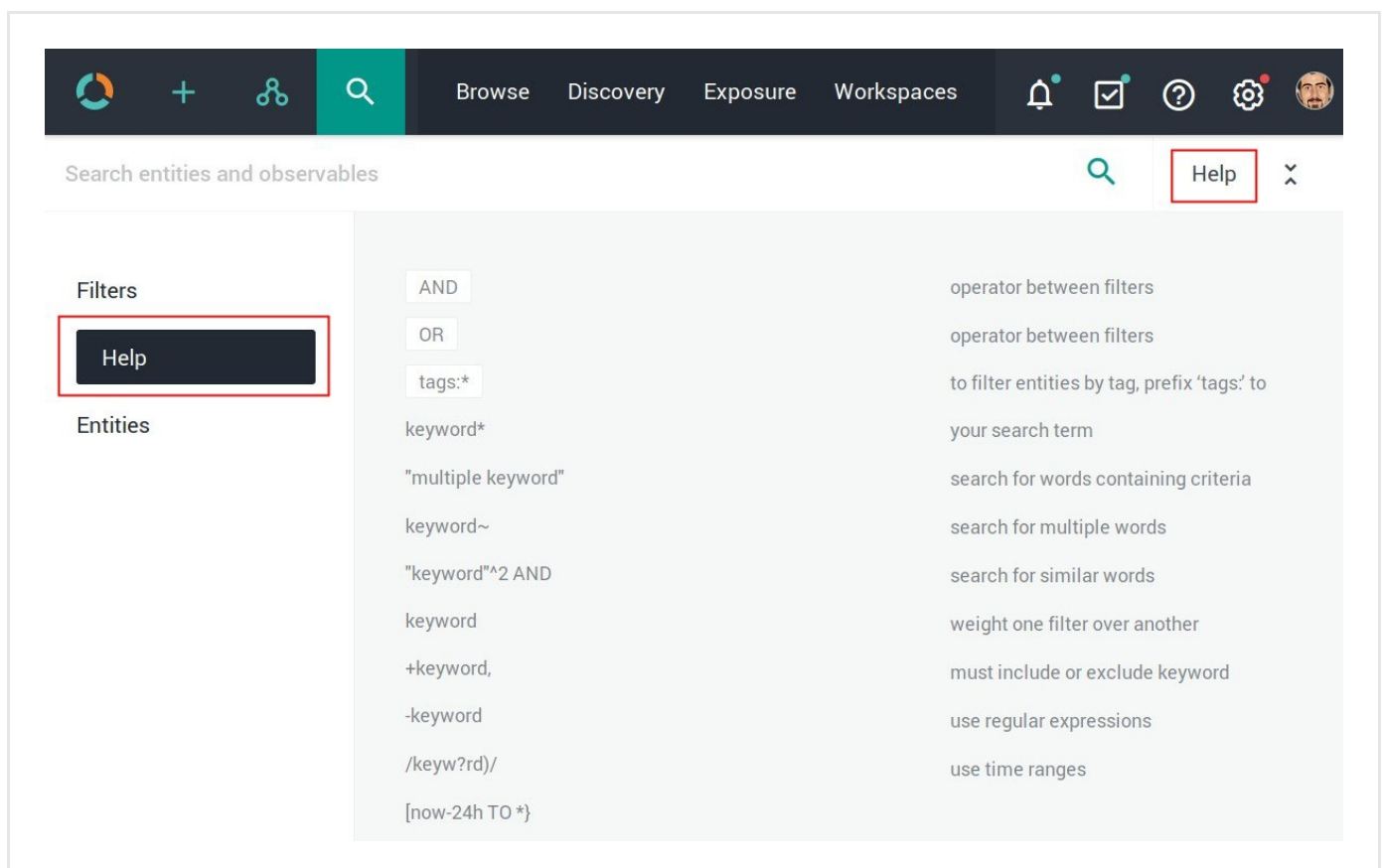
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	string — The actual value of the enrichment observable, based on the enrichment observable data type.	doom.dismay.biz

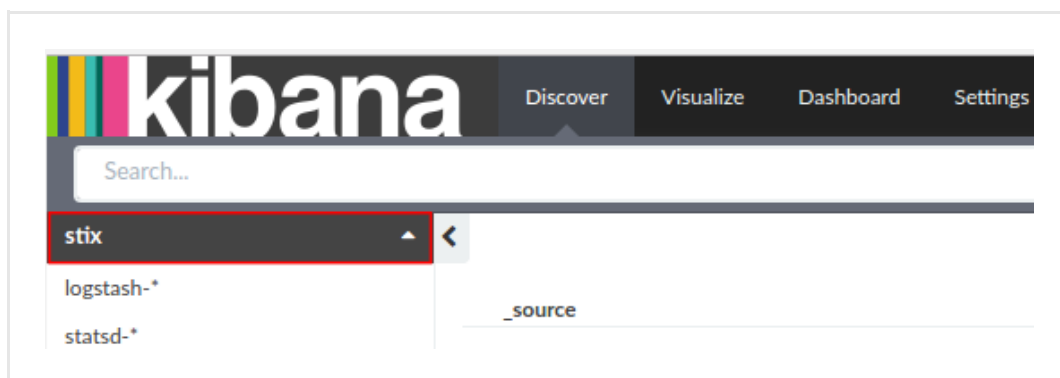
Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeolIP	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-sha512, 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**:

 A screenshot of the Kibana Settings page for the 'stix' index pattern. The 'Settings' tab is selected in the top navigation bar. On the left sidebar, 'Indices' is selected, and 'stix' is chosen from the list of index patterns. The main content area shows the 'stix' index pattern with a star icon, a refresh icon, and a delete icon. Below this, a text block explains that the page lists every field in the index and its associated core type as recorded by Elasticsearch. A table titled 'Fields (428)' and 'Scripted fields (0)' displays the following data:
 

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	<code>http://api.domaintools.com/v1/reputation</code>
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.

**Workflow**

☐ Add to dataset

☒ Manually enrich

**Enrichers to apply**

Please select one or more options

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▼

Enrich all observables

Enrich selected observables ▼

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin ▼ Maliciousness ▼ Date ▼

Lv Conn Origins Created ▼ ↻

Enrichment (1) 14 days ago ⋮

Enrichment (1) 14 days ago ⋮

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

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▼

Enrich all observables

Enrich selected observables ▼

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin ▼ Maliciousness ▼ Date ▼

Lv Conn Origins Created ▼ ↻

Enrichment (1) 14 days ago ⋮

Enrichment (1) 14 days ago ⋮

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 screenshot shows the EclecticIQ interface for a specific URL entity. At the top, a teal header bar displays the URL: `http://zebbugtennis.com/wp-conte...`. Below the header, a status bar indicates the entity was ingested on 09/15/2016 at 10:20 PM from the 'guest.phishtank\_c...' feed, with a 'TLP White' label.

The main interface has tabs for OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The 'OBSERVABLES' tab is active. On the left, an 'Enrich' dropdown menu is open, showing options: 'Enrich all observables', 'Enrich selected observables (6)' (highlighted with a red box), 'Elastic Sightings Enricher', and 'OpenResolve'.

Below the dropdown, a table lists the selected observables. The first column contains checkboxes, all of which are checked and highlighted with a red box. The table columns are: type, value, left arrow, count, conn, origins, status, and created time.

	uri	http://zebbugtennis.com/wp-co...	←	2	2	Entity	●	5 months ago
<input checked="" type="checkbox"/>	uri	http://zebbugtennis.com/wp-co...	←	1	1	Direct	●	5 months ago
<input checked="" type="checkbox"/>	hash-md5	a47a1906802faf32be76732366...	←	1	2	Entity (1)	●	5 months ago
<input checked="" type="checkbox"/>	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.

OVERVIEW

**OBSERVABLES**

NEIGHBORHOOD

JSON

VERSIONS

HISTORY

Enrich

Add observable

Actions 

Filters: Maliciousness

Origin

Kind

Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2		2 months ago
<input type="checkbox"/>	country	us	2		2 months ago
<input type="checkbox"/>	uri	http://t.esecurit...	2		2 months ago
<input type="checkbox"/>	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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdb	2		

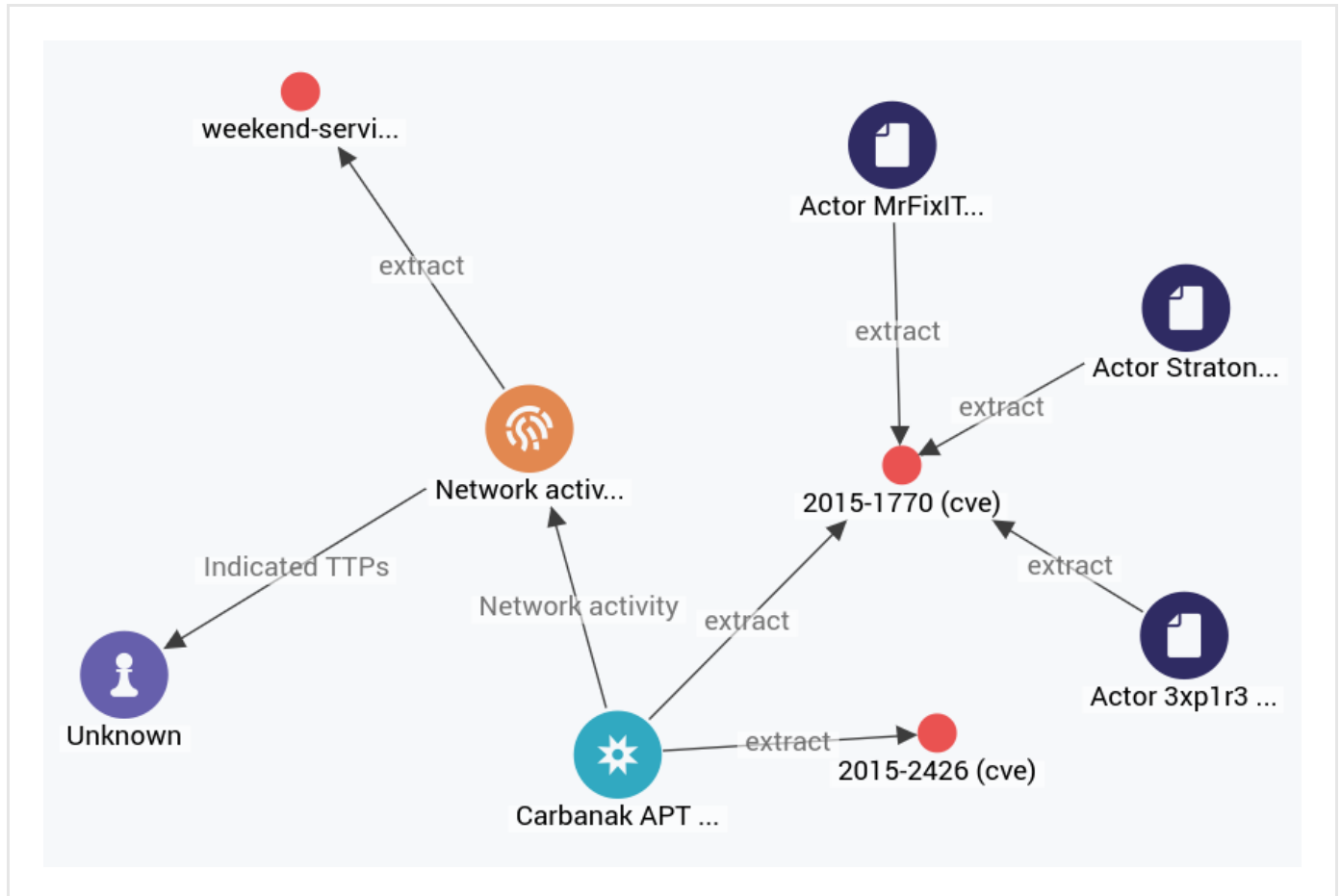
Ignore extract

Create sighting

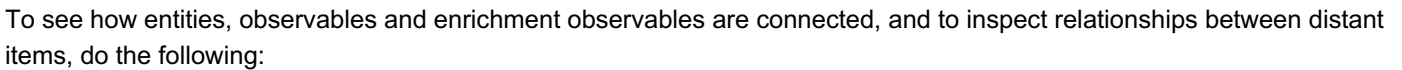
**Add to graph**

Set maliciousness >

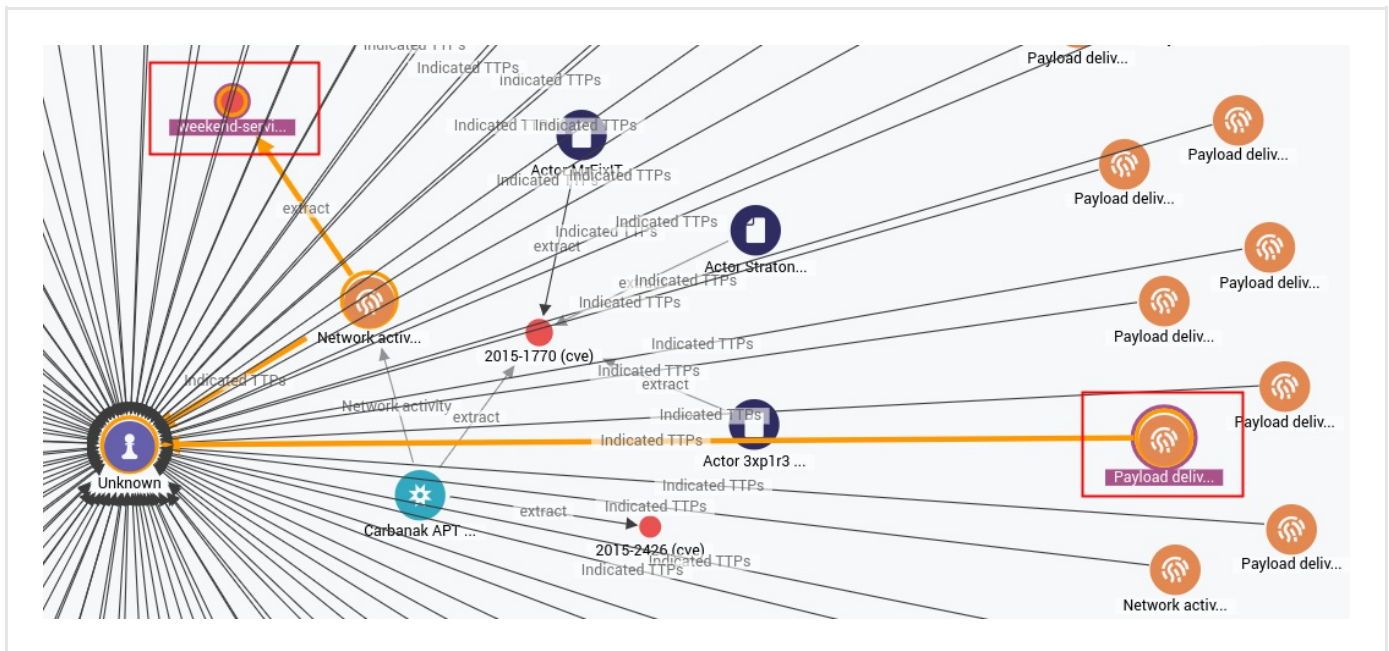
- To load the parent entity whose detail pane you are viewing, instead of its observables, from the pop-up **Actions** menu at the bottom of the pane select **Add to graph**.
- Click the graph thumbnail on the lower side of the screen to expand it.
- On the graph, right-click the entity you want to inspect,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

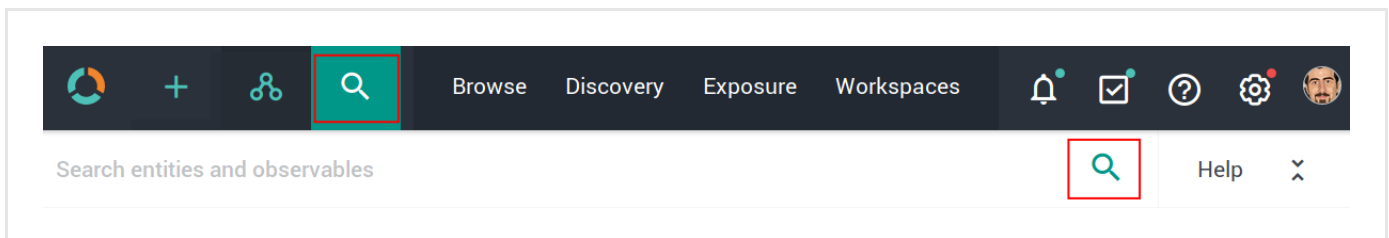


- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist, 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.

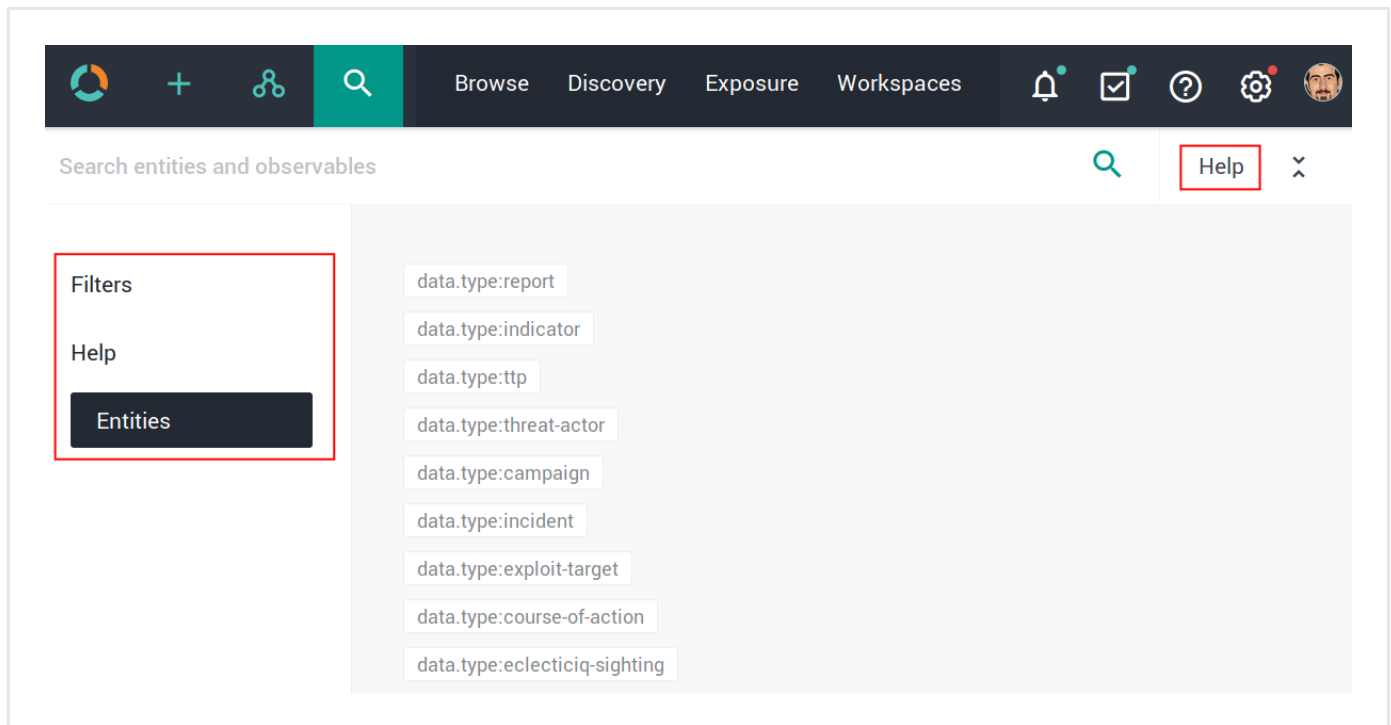


The search functionality uses **Elasticsearch query syntax**

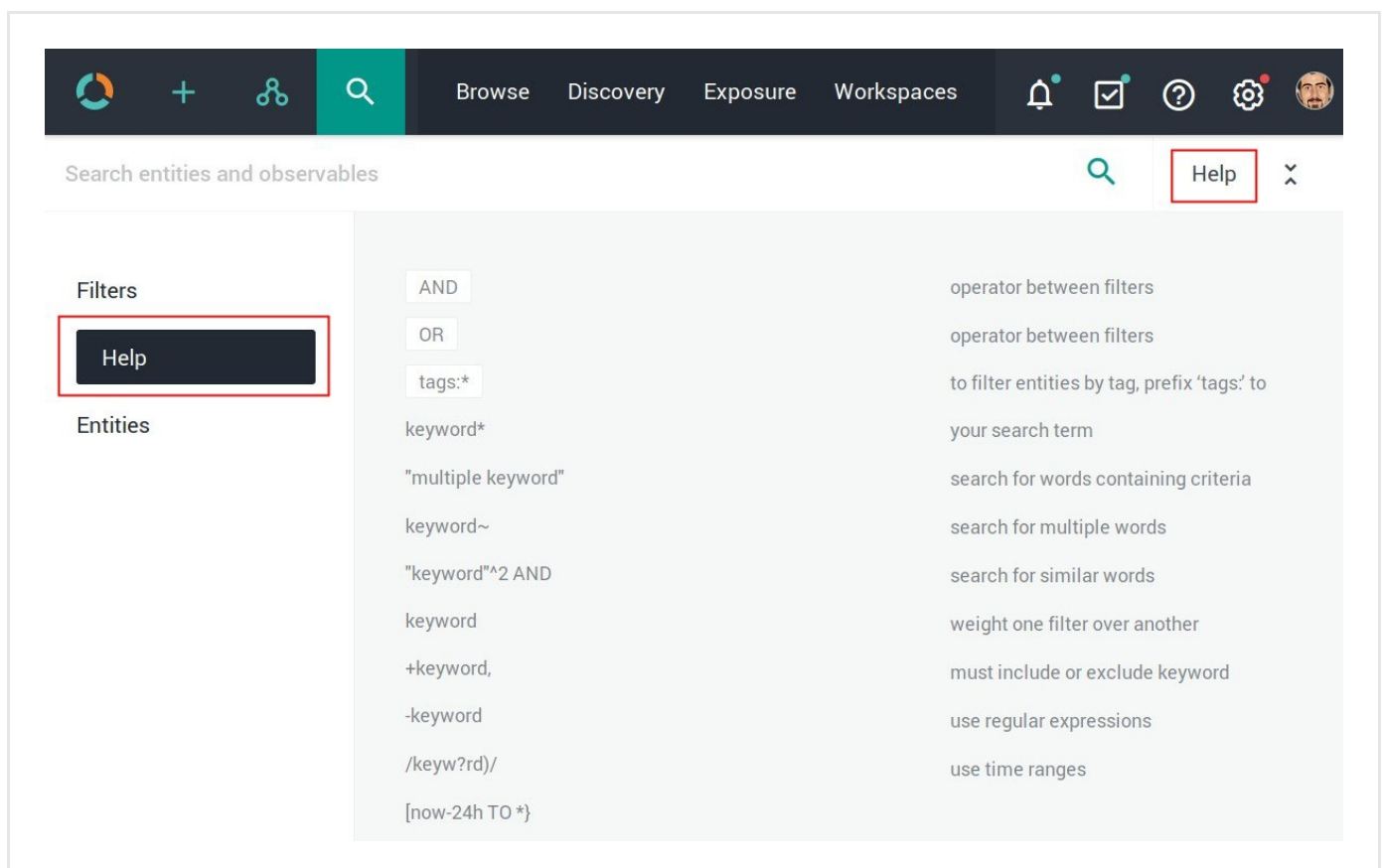
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	string — The actual value of the enrichment observable, based on the enrichment observable data type.	doom.dismay.biz

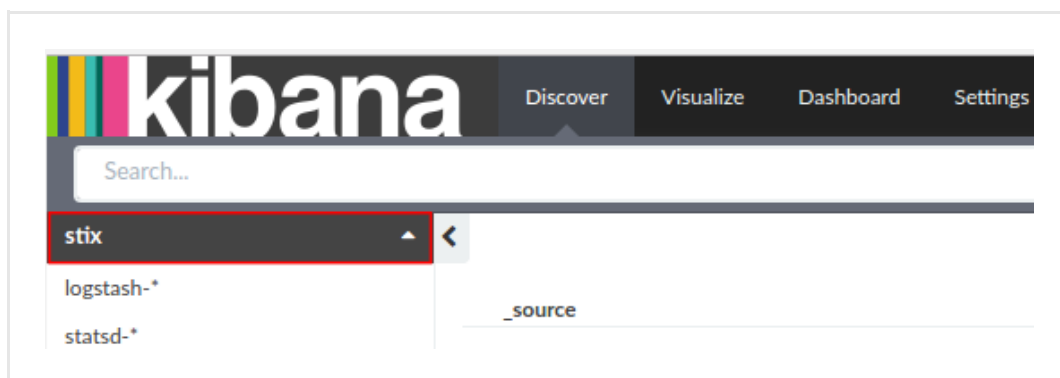
Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeolIP	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-sha512, 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**:

 A screenshot of the Kibana Settings page for the 'stix' index pattern. The 'Settings' tab is selected in the top navigation bar. On the left sidebar, 'Indices' is selected, and 'stix' is chosen from the index patterns list. The main content area shows the 'stix' index pattern with a star icon, a refresh icon, and a delete icon. Below this, a text description states: '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](#).' Below the text, there are two tabs: 'Fields (428)' and 'Scripted fields (0)'. The 'Fields (428)' tab is active, displaying a table of fields.
 

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](#).


<b>DomainTools Retrieve Parsed Whois Observables</b>	<b>enricher</b>
<b>Enricher name</b>	DomainTools Retrieve Parsed Whois Observables
<b>API endpoint</b>	<code>http://api.domaintools.com/v1/{}/whois/parsed</code>
<b>Input</b>	domain, host, ipv4
<b>Output</b>	Enriches the supported observable types with structured Whois information.
<b>Description</b>	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.

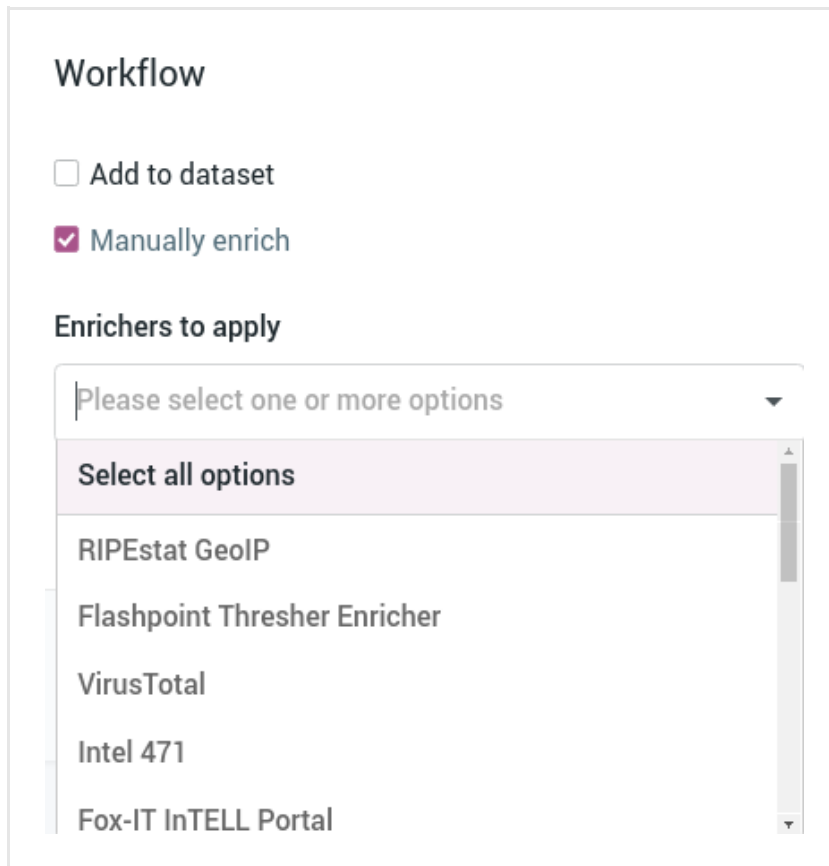
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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**

Please select one or more options

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv Conn Origins Created

Enrichment (1) 14 days ago

Enrichment (1) 14 days ago

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

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv Conn Origins Created

Enrichment (1) 14 days ago

Enrichment (1) 14 days ago

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 screenshot shows the EclecticIQ interface for a specific URL entity. At the top, a teal header bar displays the URL: `http://zebbugtennis.com/wp-conte...`. Below this, a status bar indicates the entity was ingested on 09/15/2016 at 10:20 PM from the 'guest.phishtank\_c...' feed, with a 'TLP White' label.

The main interface has tabs for OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The 'OBSERVABLES' tab is active. On the left, an 'Enrich' dropdown menu is open, showing options: 'Enrich all observables', 'Enrich selected observables (6)' (highlighted with a red box), 'Elastic Sightings Enricher', and 'OpenResolve'.

To the right of the menu is a table of observables. The first column contains checkboxes, with the first four rows (uri, uri, hash-md5, domain) having their checkboxes checked and highlighted with a red box. The table columns include type, value, a menu icon, a count, a category, a status indicator, and a timestamp.

	Origin	Maliciousness	Date
	Lv	Conn	Origins
	Created		
	Enrichment (1)		7 days ago
	Enrichment (2)		7 days ago
uri	2	2	Entity
uri	1	1	Direct
hash-md5	1	2	Entity (1)
domain	1	10	Entity (3)

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.

OVERVIEW	OBSERVABLES	NEIGHBORHOOD	JSON	VERSIONS	HISTORY
<div>Enrich <span>▼</span> <span>Add observable</span></div>					
Actions <span>▼</span> Filters: Maliciousness <span>▼</span> Origin <span>▼</span> Kind <span>▼</span> Date <span>▼</span>					
<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED <span>▼</span>	<span>↻</span>
<input type="checkbox"/>	domain	t.esecurityplanet...	2 <span>+</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	country	us	2 <span>+</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	uri	http://t.esecurit...	2 <span>+</span> <span>●</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>
<input type="checkbox"/>	name	vcdb	2 <span>+</span> <span>●</span> <span>●</span>	2 months ago	<span>⋮</span>

## 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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED <span>▼</span>	<span>↻</span>
<input type="checkbox"/>	domain	www.thestar.com.my	2 <span>+</span>	a month ago	<span>⋮</span>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2 <span>+</span>		
<input type="checkbox"/>	country	my	2 <span>+</span>		
<input type="checkbox"/>	uri	notes:the	2 <span>+</span>		
<input type="checkbox"/>	name	vcdb	2 <span>+</span>		

Ignore extract

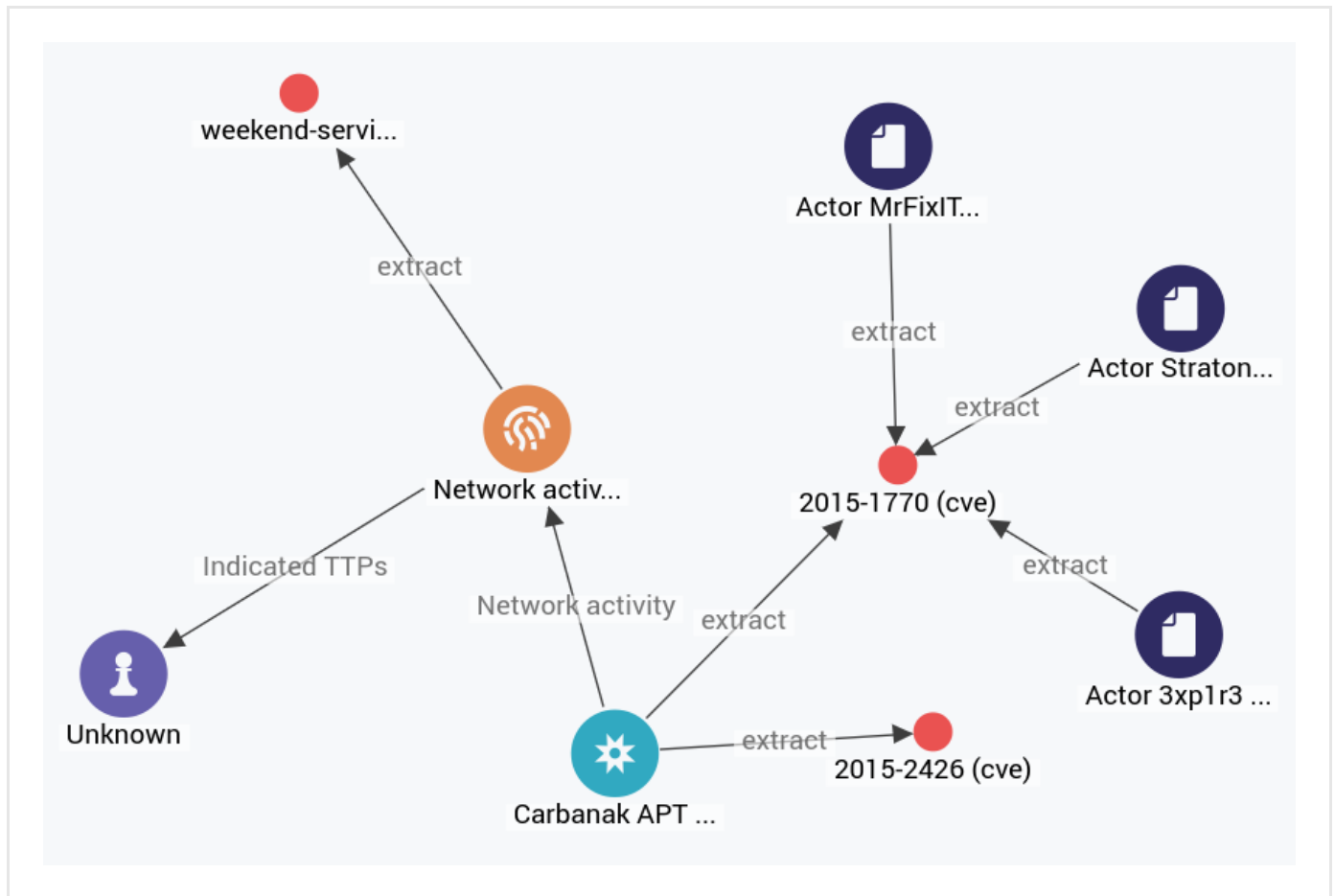
Create sighting

Add to graph

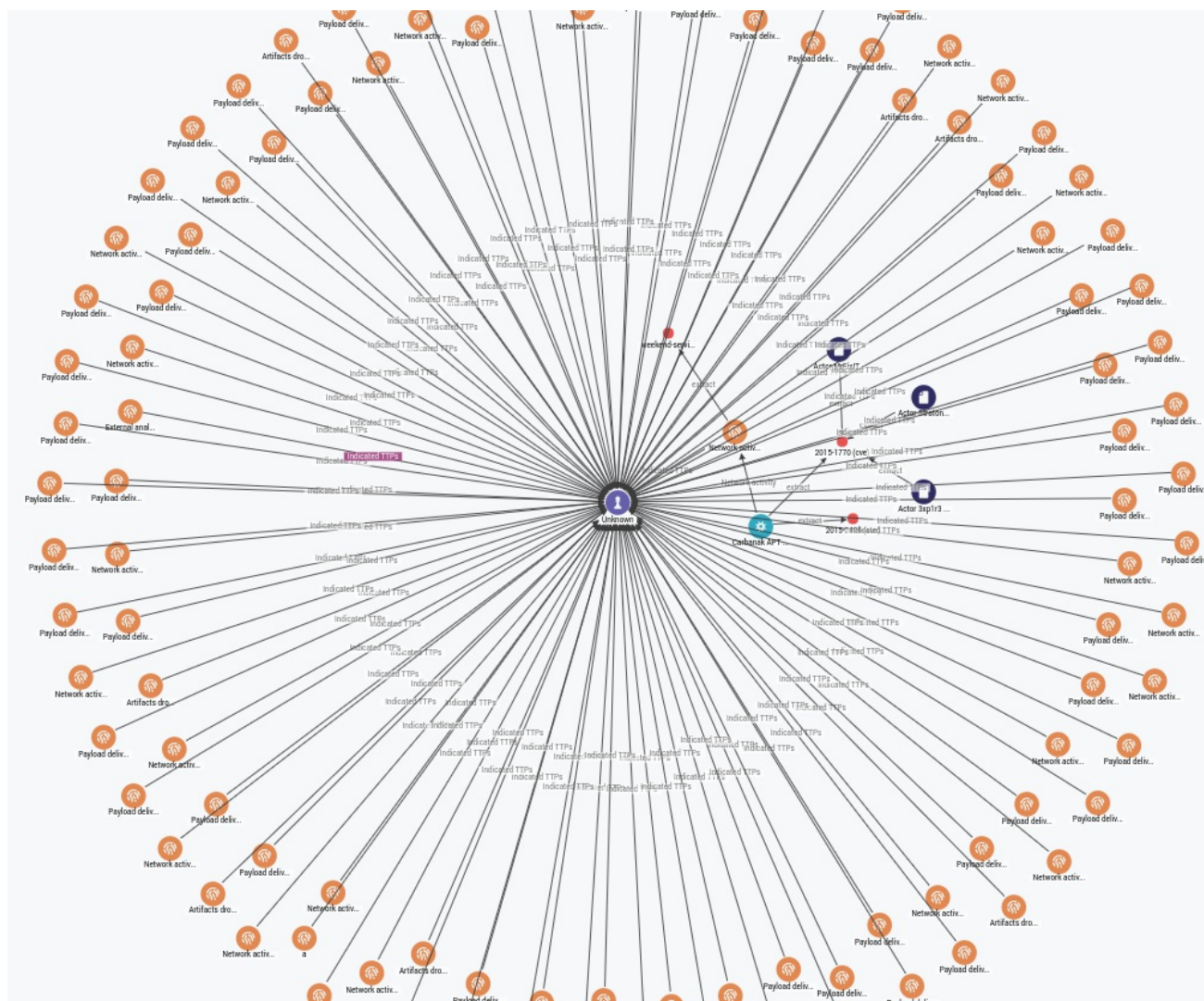
Set maliciousness >

- 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**.

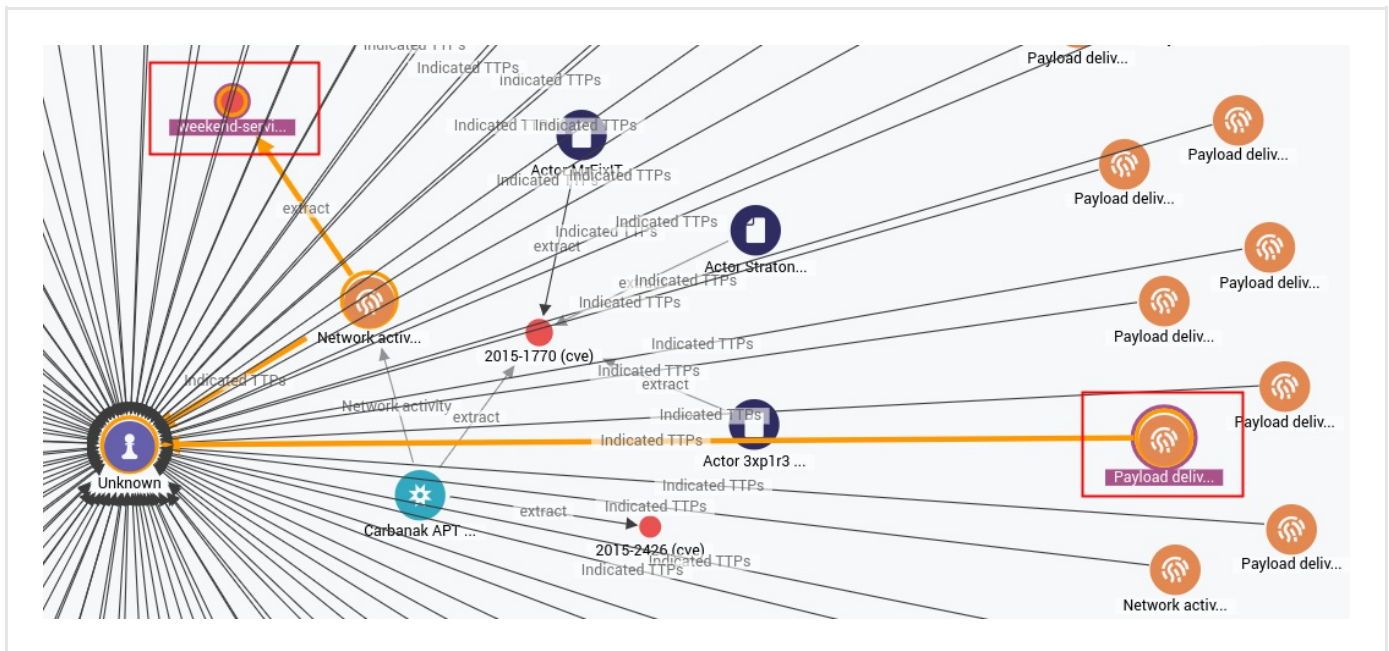


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



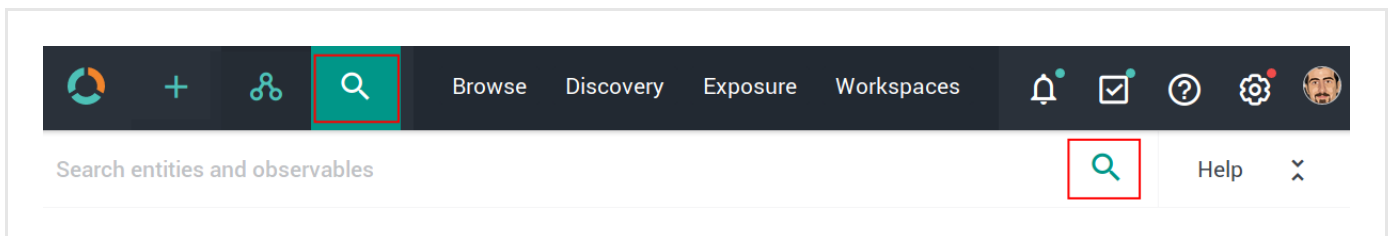
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 an 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.

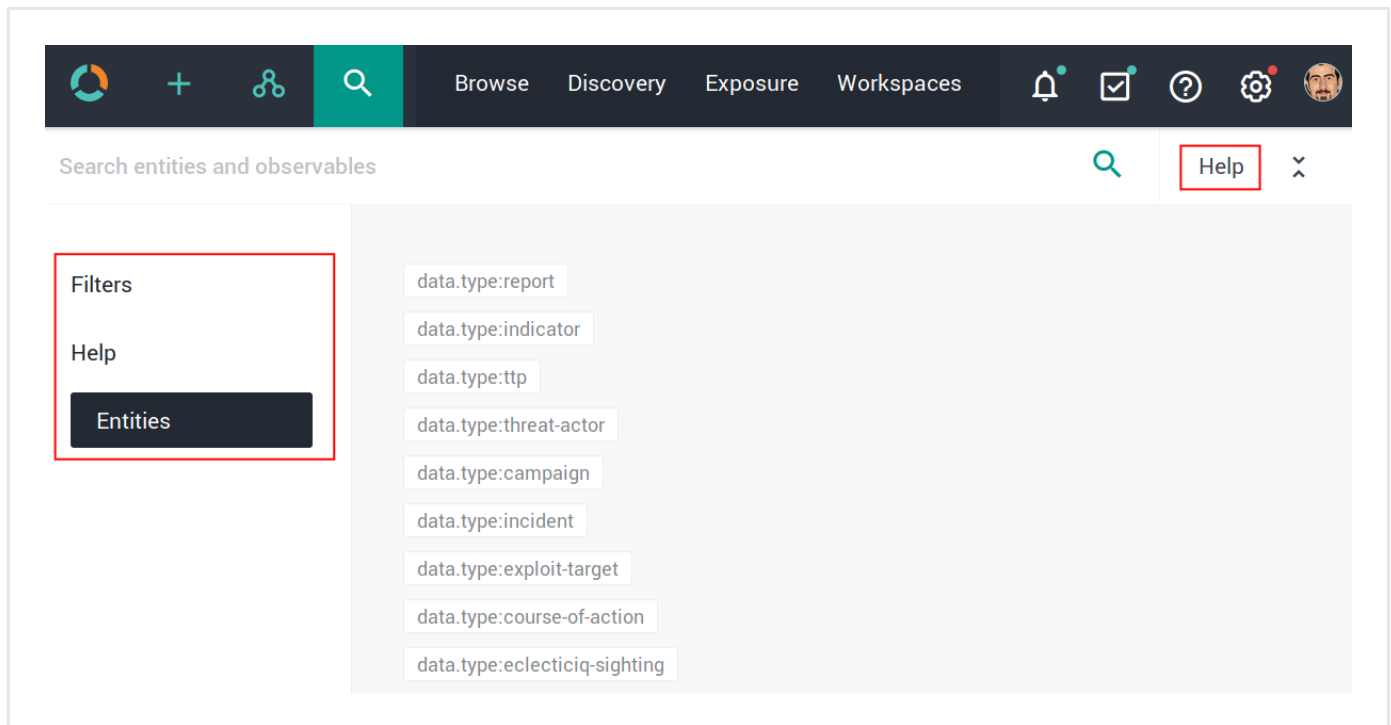


The search functionality uses **Elasticsearch query syntax**

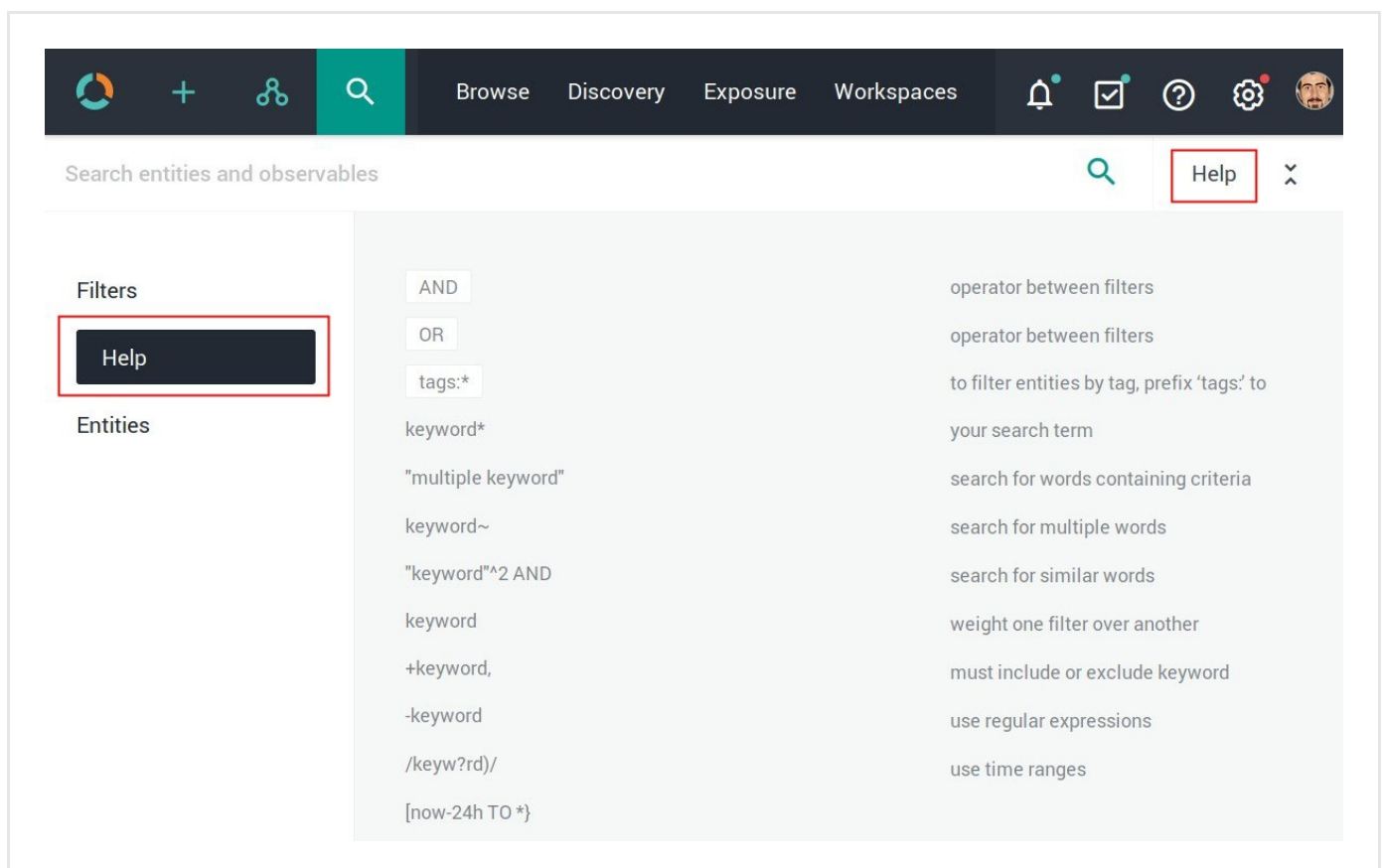
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	string — The actual value of the enrichment observable, based on the enrichment observable data type.	doom.dismay.biz

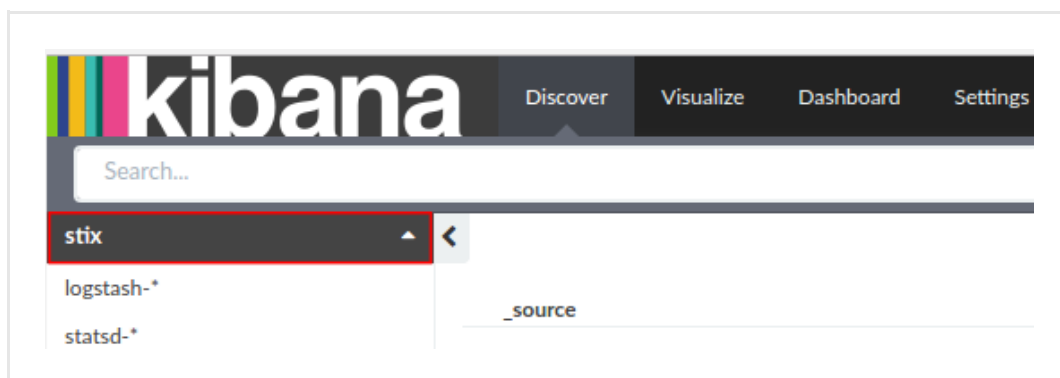
Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeolP	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-sha512, 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**:

 A screenshot of the Kibana Settings page for the 'stix' index pattern. The 'Settings' tab is selected in the top navigation bar. On the left sidebar, 'Indices' is selected, and 'stix' is chosen from the index patterns list. The main content area shows the 'stix' index pattern with a star, refresh, and delete icon. Below this, a text description states: '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](#).' Below the text are two tabs: 'Fields (428)' and 'Scripted fields (0)'. The 'Fields (428)' tab is active, displaying a table of fields.
 

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 addresses, 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](#).


<b>DomainTools Suspicious Domains</b>	<b>enricher</b>
<b>Enricher name</b>	DomainTools Suspicious Domains
<b>API endpoint</b>	<code>https://api.domaintools.com/v1/{}/host-domains</code>
<b>Input</b>	ipv4
<b>Output</b>	Enriches the supported observable types with suspicious domain and host name information.
<b>Description</b>	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**

Please select one or more options

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv Conn Origins Created

Enrichment (1) 14 days ago

Enrichment (1) 14 days ago

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

OVERVIEW OBSERVABLES NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich

Enrich all observables

Enrich selected observables

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin Maliciousness Date

Lv Conn Origins Created

Enrichment (1) 14 days ago

Enrichment (1) 14 days ago

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://zebugtennis.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
uri	<a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	2	2
uri	<a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	1	1
hash-md5	<a href="#">a47a1906802faf32be76732366...</a>	1	2
domain	<a href="#">zebugtennis.com</a>	1	10

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.

OVERVIEW

**OBSERVABLES**

NEIGHBORHOOD

JSON

VERSIONS

HISTORY

Enrich

Add observable

Actions 

Filters: Maliciousness

Origin

Kind

Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2		2 months ago
<input type="checkbox"/>	country	us	2		2 months ago
<input type="checkbox"/>	uri	http://t.esecurit...	2		2 months ago
<input type="checkbox"/>	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**.

<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdb	2		

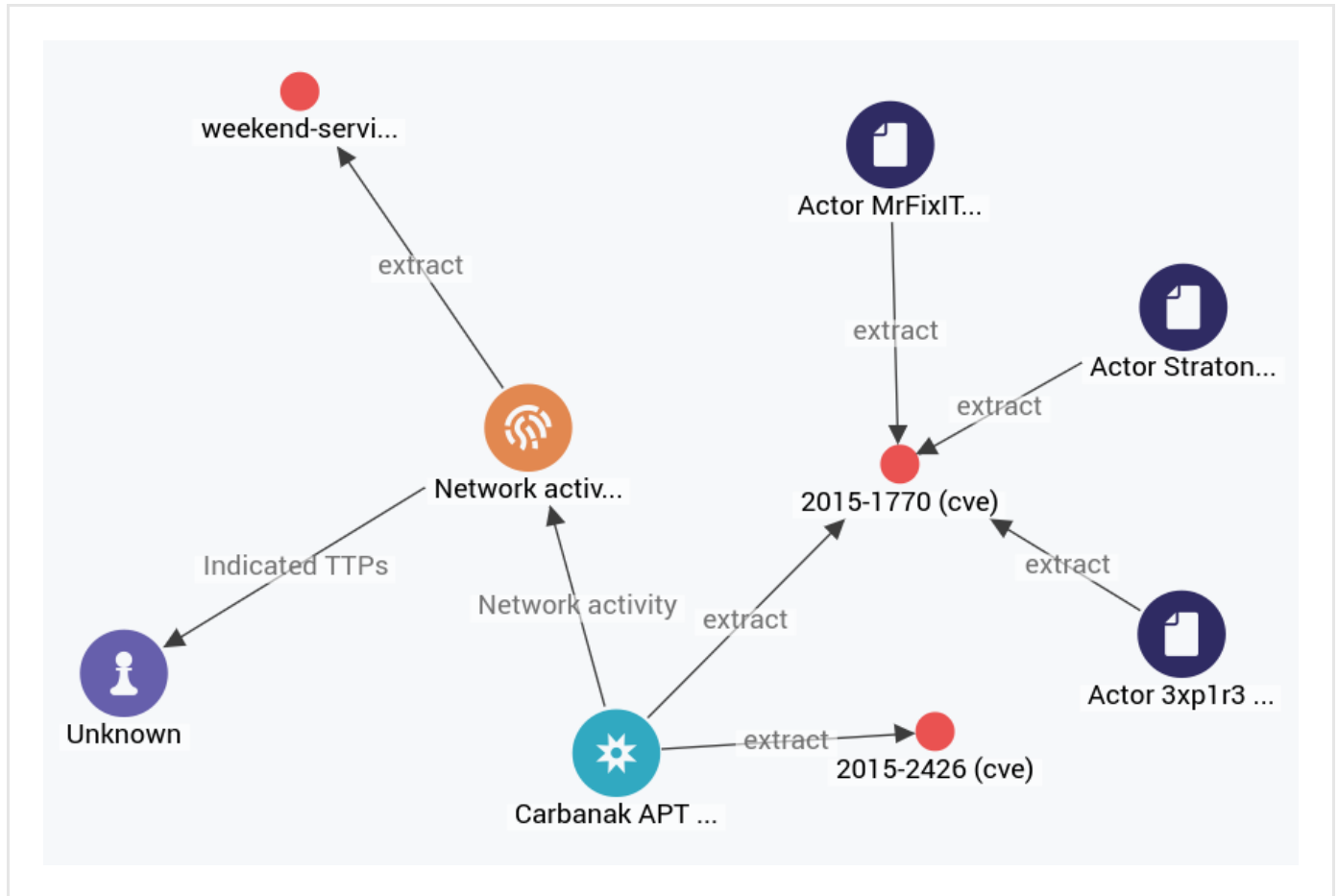
Ignore extract

Create sighting

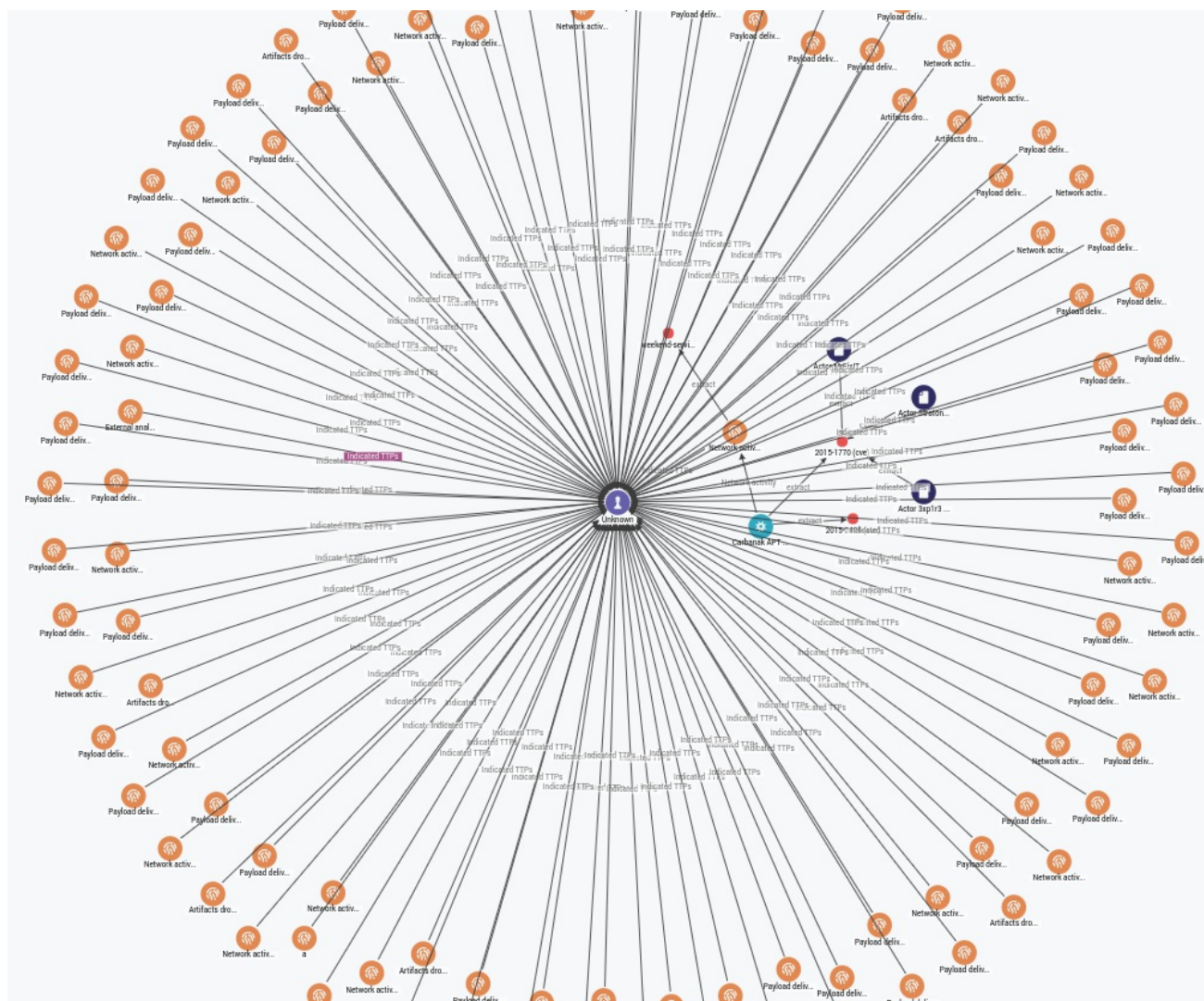
**Add to graph**

Set maliciousness >

- 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** .

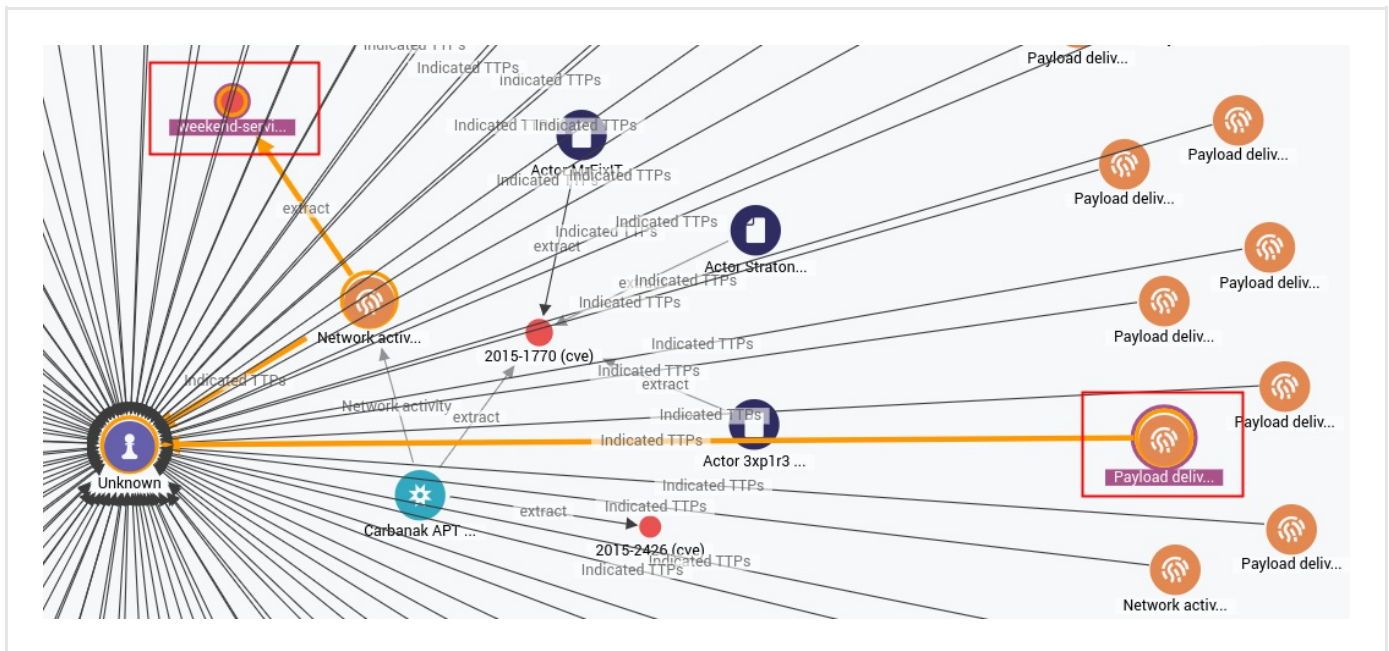


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All** , **Load observables > All** or **Load entities by extract > All** .



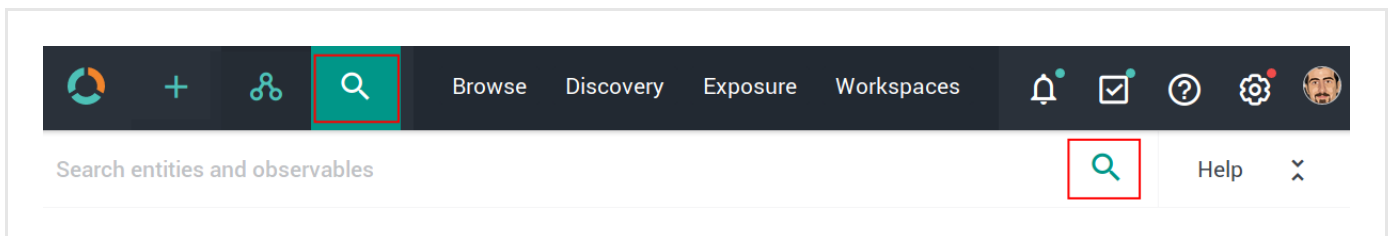
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 an 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.

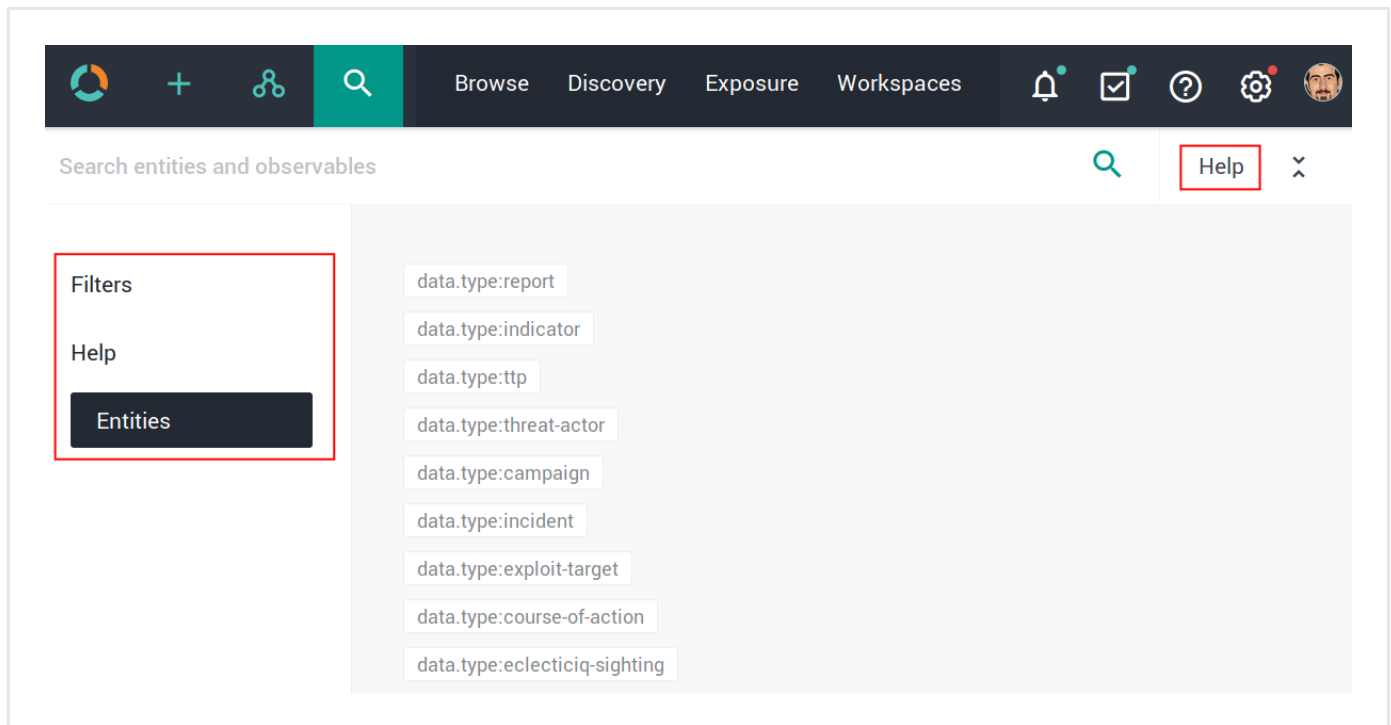


The search functionality uses **Elasticsearch query syntax**

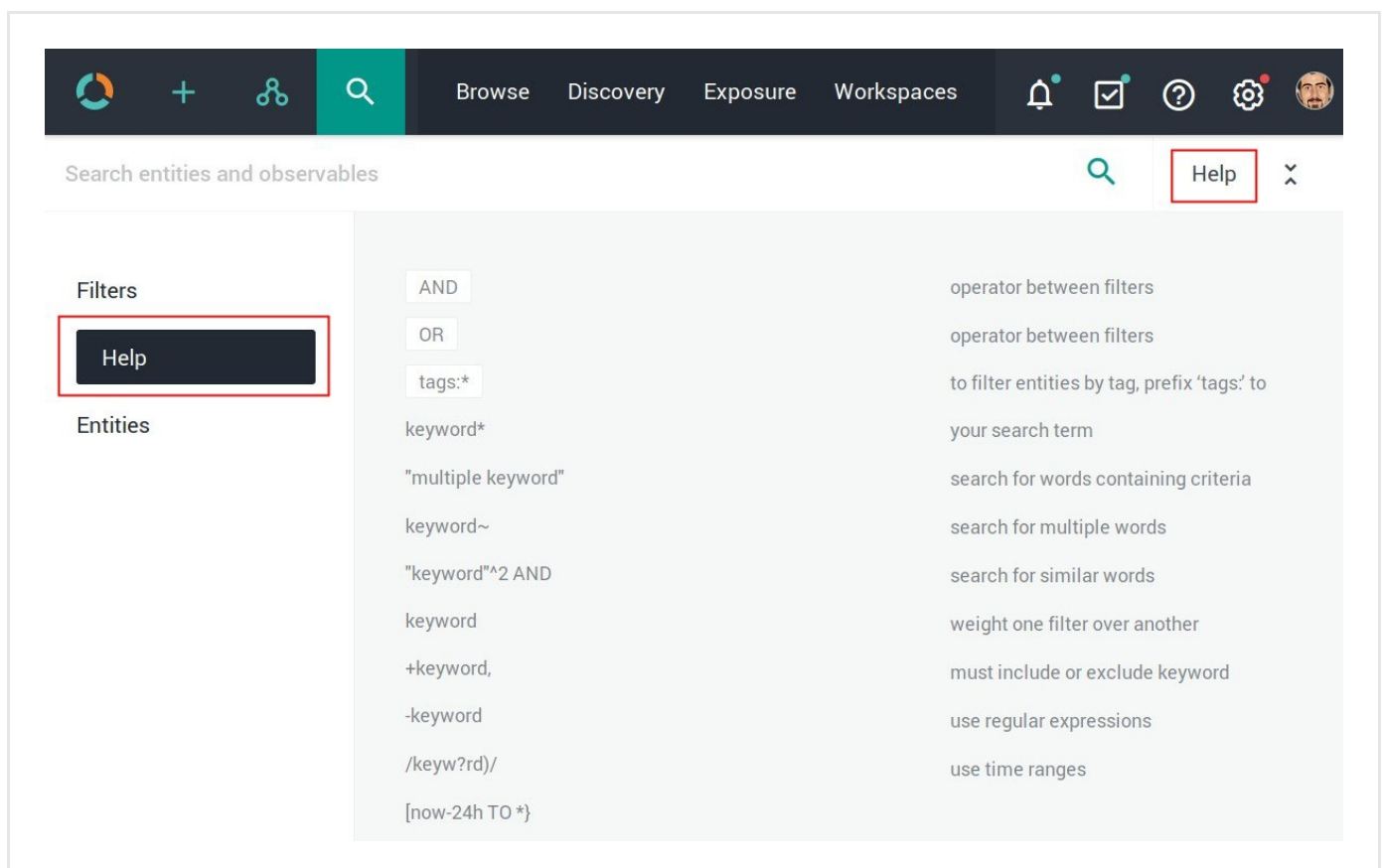
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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.



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
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	string — The actual value of the enrichment observable, based on the enrichment observable data type.	doom.dismay.biz

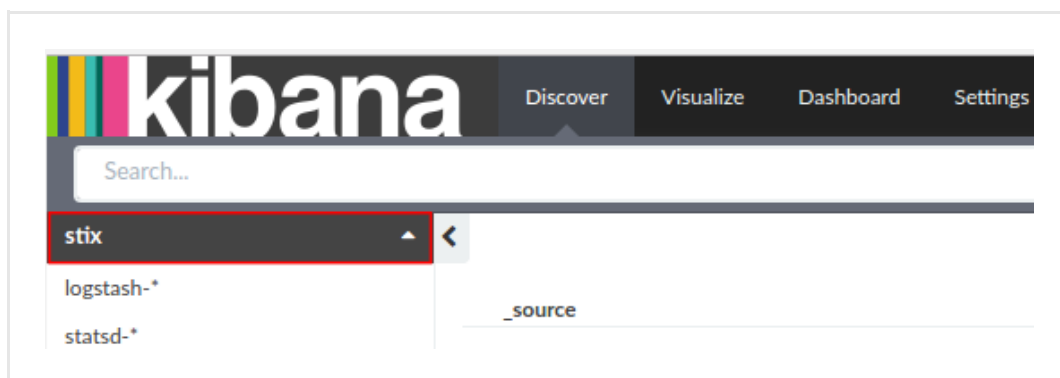
Enricher	Supported kinds (observable types)
Elasticsearch sightings	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
Fox-IT InTELL Portal	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Intel 471	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
OpenDNS OpenResolve	ipv4, ipv6, domain, host
PyDat	ipv4, ipv6, domain
RIPEstat GeolP	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-sha512, 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**:

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

Enricher	API endpoint	Descri
Flashpoint AggregINT	<a href="https://endlesstunnel.info/v3">https://endlesstunnel.info/v3</a>	<p>Polls data from the Flashpoint API. It i hosts, domains, IP addresses, and ha thematic datasets focusing on hacker groups, communities in conflict, state <b>CBRN</b> (<a href="https://en.wikipedia.org">https://en.wikipedia.org</a>) produces enrichment observables like user name of the author of a post (as UTC date and time of a post in <b>ISO 86</b> (<a href="https://en.wikipedia.org/wiki/">https://en.wikipedia.org/wiki/</a>) (<a href="https://tools.ietf.org/html/rfc">https://tools.ietf.org/html/rfc</a></p>
Flashpoint Blueprint	<a href="https://endlesstunnel.info/v3">https://endlesstunnel.info/v3</a>	<p>Polls data from the Flashpoint API. It i geolocation and IP ranges, as well as search thematic datasets focusing on supremacist groups, state actors invol (<a href="https://en.wikipedia.org/wiki/">https://en.wikipedia.org/wiki/</a>) enrichment observables like city/coun latitude/longitude or IP address hit, for a hit, user name uniquely matched to</p>
Flashpoint Thresher	<a href="https://endlesstunnel.info/v3">https://endlesstunnel.info/v3</a>	<p>Polls data from the Flashpoint API. Th datasets focusing on hackers, terrorists and <b>CBRN</b> (<a href="https://en.wikipedia">https://en.wikipedia</a>) threats. It produces enrichment obser thresher data.</p>
PassiveTotal Whois	<a href="https://api.passivetotal.org/v2">https://api.passivetotal.org/v2</a>	<p>Polls data from the <b>PassiveTotal API</b> (<a href="https://api.passivetotal.org/a">https://api.passivetotal.org/a</a> getv2whoisquery). It provides inform associated with an IP address or a do details. Analysts can retrieve registrar telephone, and email details. They can further queries to obtain, for example, the same individual or the same comp</p>
PassiveTotal Passive DNS	<a href="https://api.passivetotal.org/v2">https://api.passivetotal.org/v2</a>	<p>Polls data from the <b>PassiveTotal API</b> (<a href="https://api.passivetotal.org/a">https://api.passivetotal.org/a</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</p>
PassiveTotal IP/Domain	<a href="https://api.passivetotal.org/v2">https://api.passivetotal.org/v2</a>	<p>Polls data from the <b>PassiveTotal API</b> (<a href="https://api.passivetotal.org/a">https://api.passivetotal.org/a</a> getv2enrichmentquery). It provides queried IP address or domain name. I name, any sub-domains, inet details, i (<b>ASN</b>) (<a href="https://en.wikipedia.org/wiki/">https://en.wikipedia.org/wiki/</a>) as well as geolocation information. An to look for further connections that ma investigation.</p>

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

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

## 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](#).


<b>Elasticsearch sightings</b>	<b>enricher</b>
<b>Enricher name</b>	Elasticsearch sightings
<b>API endpoint</b>	<a href="http://&lt;elasticsearch_url&gt;:9200/&lt;schema_resource&gt;">http://&lt;elasticsearch_url&gt;:9200/&lt;schema_resource&gt;</a>
<b>Input</b>	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
<b>Output</b>	Creates sightings from matching results returned from a search in an external Elasticsearch instance.
<b>Description</b>	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.

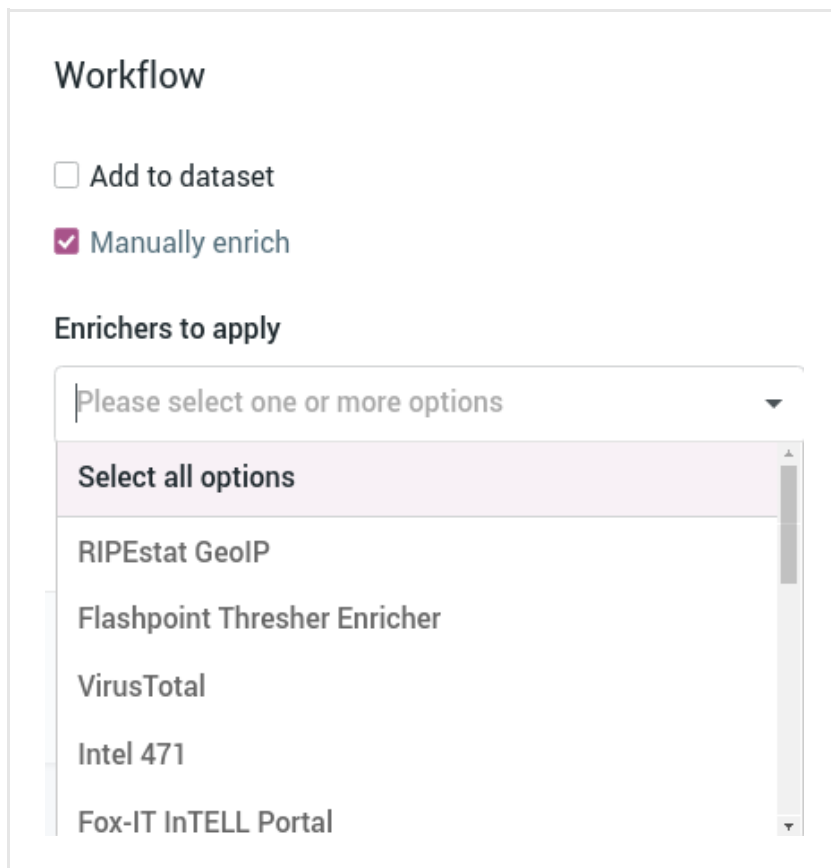
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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

- Select all options
- RIPEstat GeoIP
- Flashpoint Thresher Enricher
- VirusTotal
- Intel 471
- Fox-IT InTELL Portal


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

Alternatively, you can manually enrich an entity by selecting it; for example, from a dataset, from **Browse** or from **Discovery**.

An overlay slides in from the side of the screen to display the entity detail pane.

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

To manually enrich the entity observables:

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

Alternatively:

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

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

Ingested: 01/24/2017 12:14 AM Group: Testing Group Author: Tes... TLP None

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▾

Enrich all observables

Enrich selected observables ▾

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin ▾ Maliciousness ▾ Date ▾

Lv Conn Origins Created ▾ ↻

Enrichment (1) 14 days ago ⋮

Enrichment (1) 14 days ago ⋮

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

OVERVIEW **OBSERVABLES** NEIGHBORHOOD JSON VERSIONS HISTORY

Enrich ▾

Enrich all observables

Enrich selected observables ▾

Elastic Sightings Enricher

OpenResolve

ADD OBSERVABLE

Origin ▾ Maliciousness ▾ Date ▾

Lv Conn Origins Created ▾ ↻

Enrichment (1) 14 days ago ⋮

Enrichment (1) 14 days ago ⋮

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://zebugtennis.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
uri <a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	2	2	Entity
uri <a href="http://zebugtennis.com/wp-co...">http://zebugtennis.com/wp-co...</a>	1	1	Direct
hash-md5 <a href="#">a47a1906802faf32be76732366...</a>	1	2	Entity (1)
domain <a href="#">zebugtennis.com</a>	1	10	Entity (3)

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.

OVERVIEW

**OBSERVABLES**

NEIGHBORHOOD

JSON

VERSIONS

HISTORY

Enrich

Add observable

Actions 

Filters: Maliciousness

Origin


Kind

Date

<input type="checkbox"/>	KIND	VALUE	ORIGINS	CREATED	
<input type="checkbox"/>	domain	t.esecurityplanet...	2	2 months ago	
<input type="checkbox"/>	country	us	2	2 months ago	
<input type="checkbox"/>	uri	http://t.esecurit...	2	2 months ago	
<input type="checkbox"/>	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

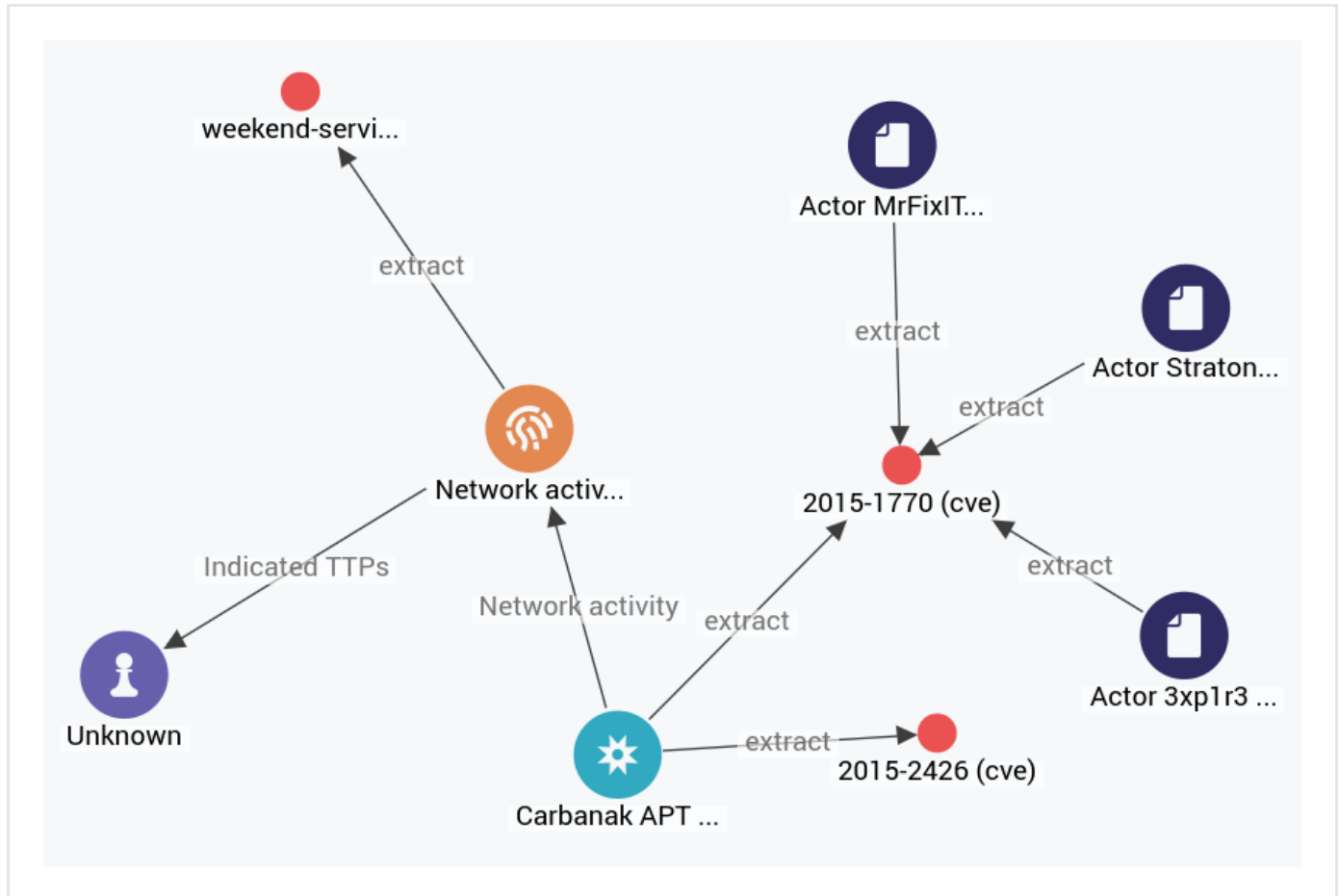
Ignore extract

Create sighting

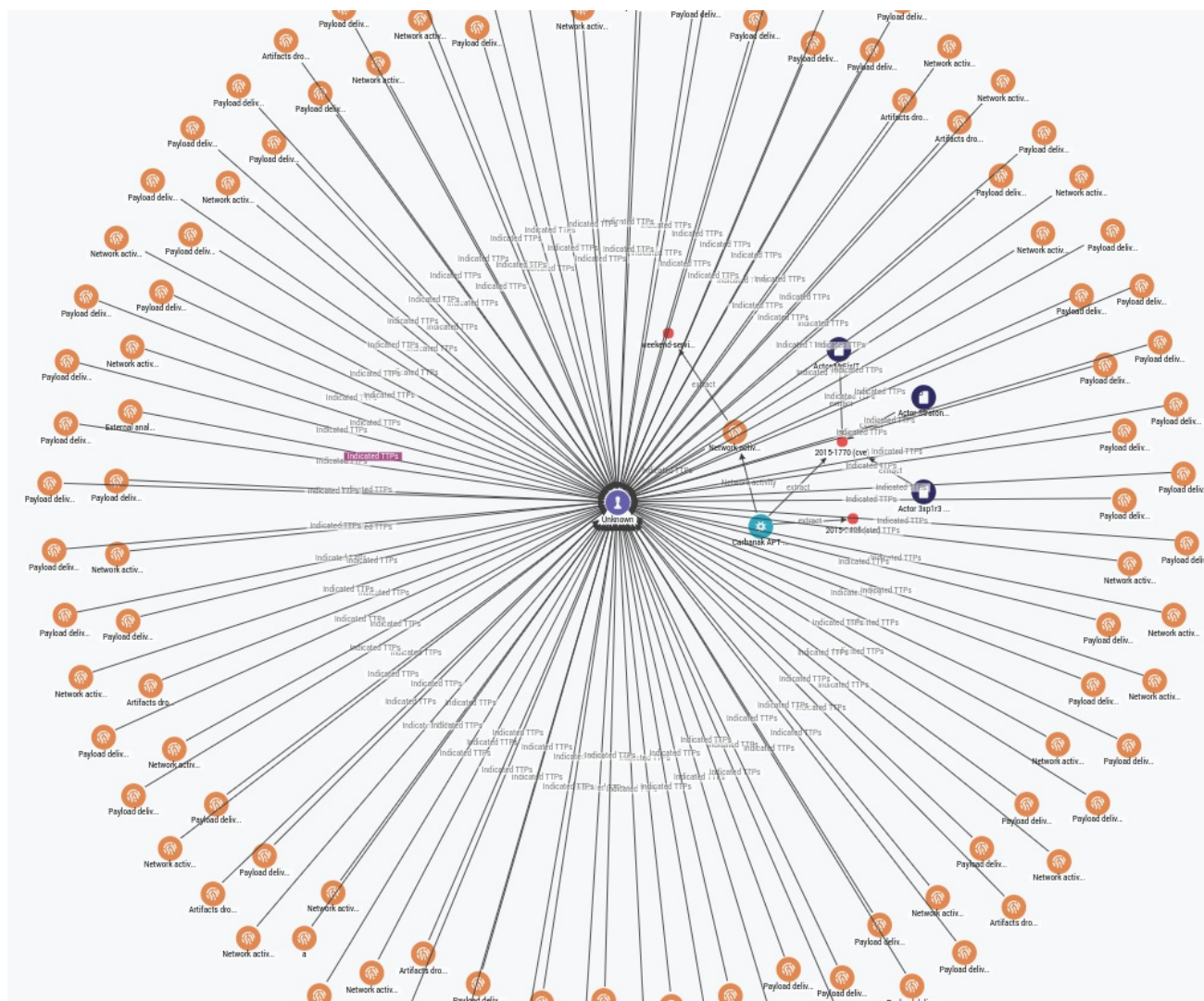
**Add to graph**

Set maliciousness >

- 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** .



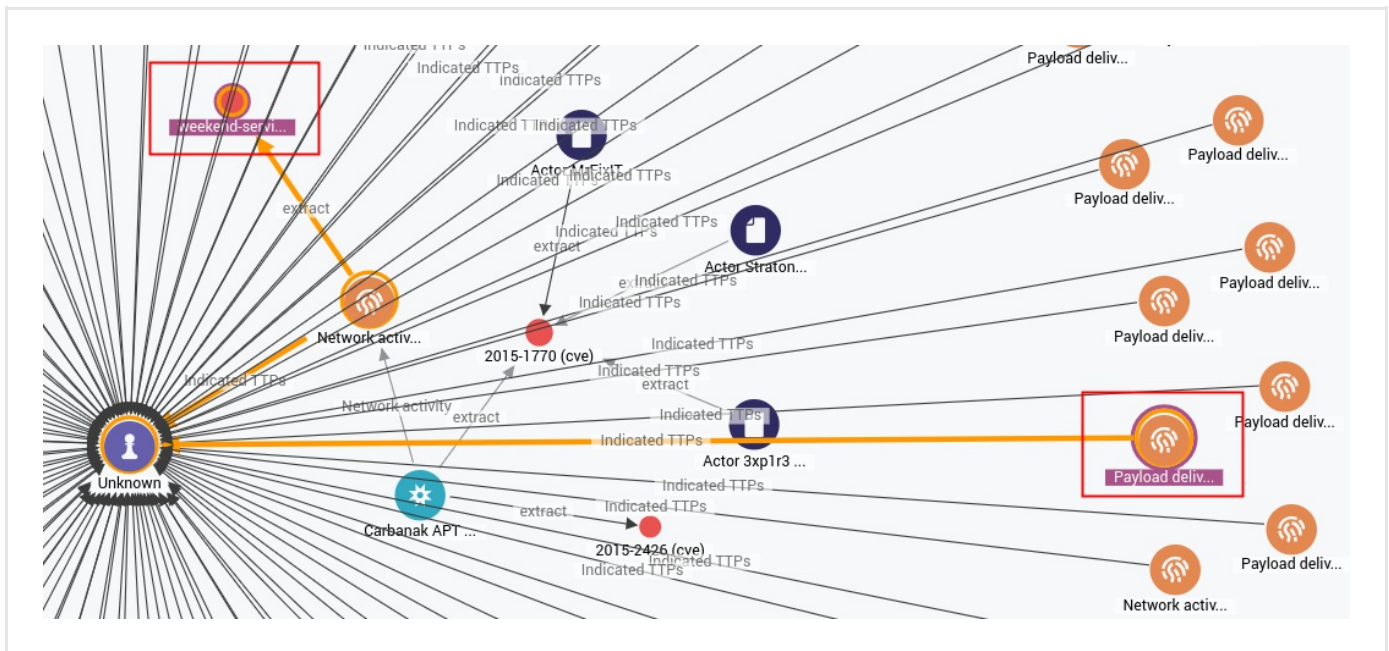
- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All** , **Load observables > All** or **Load entities by extract > All** .



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

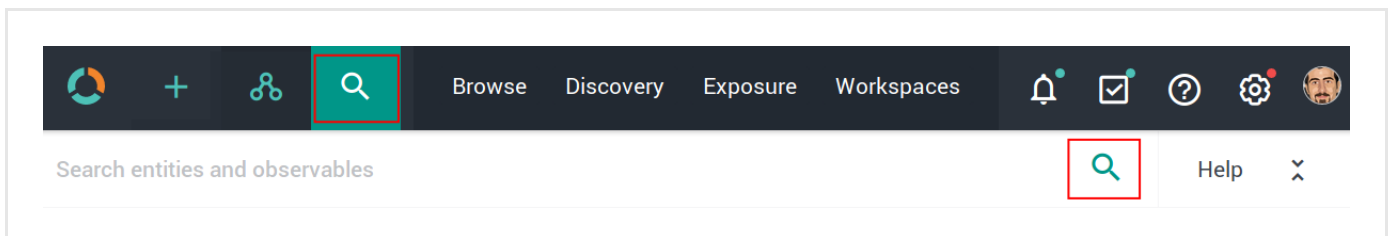
- **CTRL + click** two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist, 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.

The screenshot shows the top navigation bar with icons for search, add, share, and a magnifying glass. Below the navigation bar is a search bar with the text "Search entities and observables". To the right of the search bar are icons for help, settings, and a user profile. A red box highlights the "Help" icon. Below the search bar is a sidebar with three options: "Filters", "Help", and "Entities". The "Entities" option is highlighted with a red box. The main content area displays a list of 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, and 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.

The screenshot shows the top navigation bar with icons for search, add, share, and a magnifying glass. Below the navigation bar is a search bar with the text "Search entities and observables". To the right of the search bar are icons for help, settings, and a user profile. A red box highlights the "Help" icon. Below the search bar is a sidebar with three options: "Filters", "Help", and "Entities". The "Help" option is highlighted with a red box. The main content area displays a list of search operators and their descriptions:

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

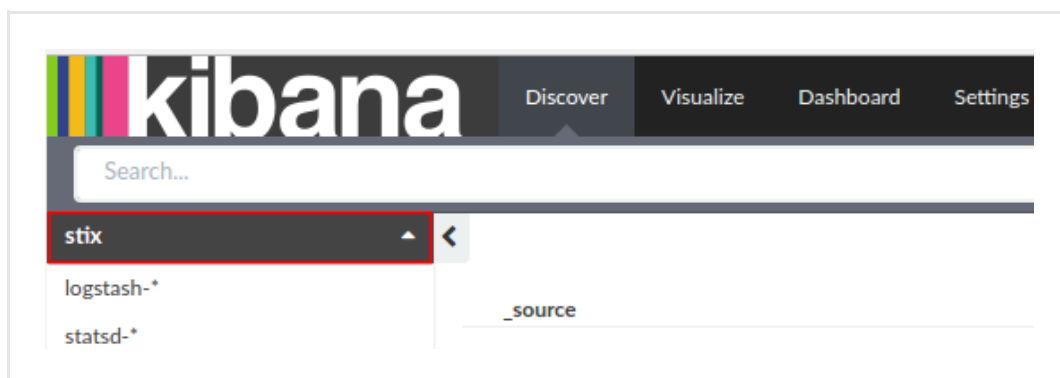
Field	Description	Example
<i>enrichment_extracts.id</i>	string — The alphanumeric ID string that uniquely identifies the enrichment observable.	01h12x45-01q2-1234-od01-123456h78h90
<i>enrichment_extracts.kind</i>	string — The enrichment observable data type.	domain
<i>enrichment_extracts.meta.blacklisted</i>	Boolean — An observable is blacklisted when it is included in the results returned by an <i>ignore</i> extraction rule. Allowed values: <code>true</code> , <code>false</code> .	true
<i>enrichment_extracts.meta.classification</i>	string — This value is defined in <b>Rules</b> by selecting appropriate options under <b>Action</b> and <b>Confidence</b> . Allowed classification metadata values are <code>good</code> , <code>bad</code> , and <code>unknown</code> .	good
<i>enrichment_extracts.meta.confidence</i>	string — This value is defined in <b>Rules</b> by selecting the appropriate option under <b>Action</b> and <b>Confidence</b> . The selected action must be <b>Mark as malicious</b> for the <b>Confidence</b> drop-down list to become available. Allowed confidence metadata values are <code>low</code> , <code>medium</code> , and <code>high</code> .	high
<i>enrichment_extracts.value</i>	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 GeolIP	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-sha512, 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		✓	✓	