

How-tos for EclecticIQ Platform

Hands-on articles on specific platform features

Last generated: May 26, 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 May 26, 2017

Table of contents

Table of contents	2
How-tos and tutorials — EclecticIQ Platform	6
Feedback	10
How to work with the Fox-IT InTELL Portal enricher	11
Work with the Fox-IT InTELL Portal enricher	11
Configure the Fox-IT InTELL Portal enricher	11
Configure enricher rules	12
Add enricher rules	12
Save options	13
Edit enricher rules	14
Delete enricher rules	15
Run the enricher	15
Automatically	15
Manually	16
Review enrichment observables	20
Review enrichment observables on the graph	21
Search for enrichment observables	24
How to work with the Intel 471 enricher	30
Work with the Intel 471 enricher	30
Configure the Intel 471 enricher	30
Configure enricher rules	31
Add enricher rules	31
Save options	32
Edit enricher rules	32
Delete enricher rules	33
Run the enricher	34
Automatically	34
Manually	34
Review enrichment observables	38
Review enrichment observables on the graph	39
Search for enrichment observables	42
How to work with the OpenResolve enricher	48
OpenDNS OpenResolve enricher	48
Configure the OpenDNS OpenResolve enricher	48
Configure enricher rules	49
Add enricher rules	49
Save options	50
Edit enricher rules	51
Delete enricher rules	52
Run the enricher	52
Automatically	52
Manually	53
Review enrichment observables	56
Review enrichment observables on the graph	57
Search for enrichment observables	60
How to work with the PassiveTotal enrichers	66
Work with the PassiveTotal enrichers	66
Configure the enrichers	66
Configure enricher rules	67
Add enricher rules	67
Save options	68
Edit enricher rules	69
Delete enricher rules	70
Run the enricher	70

Automatically	70
Manually	71
Review enrichment observables	75
Review enrichment observables on the graph	77
Search for enrichment observables	80
How to work with the PyDat enricher	86
Work with the PyDat enricher	86
Configure the enricher	86
Configure enricher rules	87
Add enricher rules	87
Save options	88
Edit enricher rules	89
Delete enricher rules	90
Run the enricher	90
Automatically	90
Manually	91
Review enrichment observables	94
Review enrichment observables on the graph	95
Search for enrichment observables	98
How to work with the Recorded Future enricher	104
Work with the Recorded Future enricher	104
Configure the Recorded Future enricher	104
Configure enricher rules	105
Add enricher rules	105
Save options	106
Edit enricher rules	107
Delete enricher rules	108
Run the enricher	108
Automatically	109
Manually	109
Review enrichment observables	113
Review enrichment observables on the graph	114
Search for enrichment observables	117
How to work with the RIPEstat GeolP enricher	123
Work with the RIPEstat GeolP enricher	123
Configure the RIPEstat GeolP enricher	123
Configure enricher rules	124
Add enricher rules	124
Save options	125
Edit enricher rules	125
Delete enricher rules	126
Run the enricher	127
Automatically	127
Manually	127
Review enrichment observables	131
Review enrichment observables on the graph	132
Search for enrichment observables	135
How to work with the RIPEstat Whois enricher	141
Work with the RIPEstat Whois enricher	141
Configure the RIPEstat Whois 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	149
Review enrichment observables on the graph	150
Search for enrichment observables	153
How to work with the ThreatGRID enricher	159
Work with the Cisco AMP Threat Grid enricher	159
Configure the Cisco AMP Threat Grid enricher	159
Configure enricher rules	160
Add enricher rules	160
Save options	161
Edit enricher rules	162
Delete enricher rules	163
Run the enricher	163
Automatically	163
Manually	164
Review enrichment observables	167
Review enrichment observables on the graph	168
Search for enrichment observables	171
How to work with the Unshorten-URL enricher	177
Work with the Unshorten-URL enricher	177
Configure the Unshorten-URL enricher	177
Configure enricher rules	178
Add enricher rules	178
Save options	179
Edit enricher rules	180
Delete enricher rules	181
Run the enricher	181
Automatically	181
Manually	182
Review enrichment observables	185
Review enrichment observables on the graph	186
Search for enrichment observables	189
How to work with the VirusTotal enricher	195
Work with the VirusTotal enricher	195
Configure the VirusTotal enricher	195
Configure enricher rules	196
Add enricher rules	196
Save options	197
Edit enricher rules	198
Delete enricher rules	199
Run the enricher	199
Automatically	200
Manually	200
Review enrichment observables	204
Review enrichment observables on the graph	205
Search for enrichment observables	208
How to work with the Elasticsearch sightings enricher	214
Work with the Elasticsearch sightings enricher	217
Configure the enricher	217
Configure enricher rules	218
Add enricher rules	218
Save options	219
Edit enricher rules	220
Delete enricher rules	221
Run the enricher	221

Automatically	221
Manually	222
Review enrichment observables	226
Review enrichment observables on the graph	227
Search for enrichment observables	230

How-tos and tutorials — EclecticIQ Platform

This section is dedicated to how-tos and tutorials about EclecticIQ Platform. Hands-on, example-driven documentation that addresses specific features and user scenarios in a pragmatic way.

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 check system health	System health gives you a clear basic overview of the overall platform health, as well as the operational status of its components.
How to configure a different database in OpenTAXII	By default, OpenTAXII uses SQLite as a database. You can change this setting to configure a different database, for example PostgreSQL.
How to configure incoming feeds	This summary page gives you an overview of the available how-to and tutorial articles about incoming feeds. They describe how to configure content types, transport types, and all the required optio...
How to configure Anubis Cyberfeed incoming feeds	Set up and configure AnubisNetworks Infections Detection Cyberfeed incoming feeds.
How to configure Group-IB accounts incoming feeds	Set up and configure Group-IB accounts incoming feeds.
How to configure Group-IB cards incoming feeds	Set up and configure Group-IB cards incoming feeds.
How to configure Group-IB IMEIs incoming feeds	Set up and configure Group-IB IMEIs incoming feeds.
How to configure Intel 471 incoming feeds	Set up and configure Intel 471 incoming feeds.
How to configure EclecticIQ JSON incoming feeds	Set up and configure EclecticIQ JSON incoming feeds.
How to configure PDF incoming feeds	Set up and configure PDF incoming feeds.

Title	Excerpt
How to configure STIX incoming feeds	Set up and configure STIX 1.0, 1.1, 1.1.1 and 1.2 incoming feeds.
How to configure text incoming feeds	Set up and configure plain text incoming feeds.
How to configure ThreatGRID incoming feeds	Set up and configure ThreatGRID incoming feeds.
How to configure Threat Recon incoming feeds	Set up and configure Threat Recon incoming feeds.
How to configure outgoing feeds	This summary page gives you an overview of the available how-to and tutorial articles about outgoing feeds. They describe how to configure content types, transport types, and all the required optio...
How to configure ArcSight CEF outgoing feeds	Set up and configure ArcSight CEF outgoing feeds.
How to configure EclecticIQ CSV outgoing feeds	Set up and configure EclecticIQ CSV outgoing feeds.
How to configure EclecticIQ JSON outgoing feeds	Set up and configure EclecticIQ JSON outgoing feeds.
How to configure STIX 1.2 outgoing feeds	Set up and configure STIX 1.2 outgoing feeds.
How to create a money mule TTP	Create a money mule TTP entity to investigate fraudulent activities and to identify the actors involved in them.
How to enable audit logging in Kibana	Enable audit logging to examine system events and user access to understand what happened and when, where in the platform, the results it produced, and who/what triggered it.
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 con...
How to install the platform via an RPM package	This step-by-step tutorial walks you through a fresh installation of the platform onto a virtual server via an RPM package.
How to make API calls with a script	Make calls to the EclecticIQ API using our simple 'papi' script.

Title	Excerpt
How to merge entities	Merge almost identical entities into a master entity and rewire relationships to reduce data noise.
How to monitor the platform	As a system administrator, you can use tools like Celery and Supervisor to monitor platform tasks to check day-to-day operations and to investigate, in case an issue occurs.
How to organize tags with taxonomies	The Taxonomy page displays an overview of the tags used to label entities in the platform. Besides using tags to organize entities, you can design taxonomies to structure the tags, and to create a ...
How to reindex Elasticsearch	You may need to reindex Elasticsearch for several reasons: from changes to data types or data analysis, to updating the Elasticsearch schema by adding or removing fields. Whenever a change in the d...
How to reindex the graph database	You may need to reindex the graph database for several reasons: from changes to data types or data analysis, to updating the data schema by adding or removing fields. Whenever a change in the data ...
How to report sightings through the API	Create and update sighting entities programmatically by making calls to the EclecticIQ API.
How to retrieve outgoing feeds through the API	Fetch outgoing feeds either manually through the platform GUI or programmatically via the API.
How to search logs for issues in Kibana	Search Kibana to retrieve log data about errors, warnings, or issues concerning specific platform components.
How to setup Nginx client certificate verification	Set up and configure SSL client certificate verification in Nginx.
How to shut down the platform	Graciously shut down the platform by first stopping its core services and processes.
How to split MISP STIX packages	Split MISP STIX packages into their corresponding embedded STIX packages by using the splitter command line utility.
How to address logging issues in Kibana	Inspect Kibana and Logstash configurations to identify and troubleshoot logging issues.
How to work with the DomainTools Hosted Domains enricher	The DomainTools Hosted Domains enricher returns all domain names related to the the specified input IP addresses.
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.

Title	Excerpt
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...
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, vie...
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...
How to work with exposure	Exposure shows you what your organization is doing with the ingested cyber threat intelligence, so that you can evaluate its usage to define courses of actions and other preventive or reactive proc...
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 e...
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 e...
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 en...
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 e...
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 o...
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...
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 d...

Title	Excerpt
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 obser...
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 ...
How to work with relationships	The Neighborhood tab in the entity detail pane includes a small graph canvas showing close relationships of the entity to other entities, as well as related observables, datasets, workspaces, and t...
How to work with the RIPEstat GeolIP 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 GeolIP enricher, view enrichm...
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 enrichm...
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 ...
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 ...

Feedback

No one reads manuals, ever. We know.

Yet, we strive to give you clear, concise, and complete documentation that helps you get stuff done neatly.

We are committed to crafting good documentation, because life is too short for bad doc.

We appreciate your comments, and we'd love to hear from you: if you have questions or suggestions, drop us a line and share your thoughts with us!

👉 The Product Team

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.

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 Fox-IT InTELL Portal enricher

This article describes how to configure the Fox-IT InTELL Portal enricher parameters.

To configure the general options for the Fox-IT InTELL Portal enricher, see [Configure enrichers](#).


Fox-IT InTELL Portal enricher	
Enricher name	Fox-IT InTELL Portal
API endpoint	<code>https://cybercrime-portal.fox-it.com/</code>
Input	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256
Output	Enriches observables with relevant contextual information from forums, chats, and IRC channels.
Description	Based on Fox-IT InTELL, the portal gathers cyber threat intelligence from a range of sources like forums and sites that have registered potentially suspicious activity.

Configure the Fox-IT InTELL Portal 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 Fox-IT InTELL Portal enricher:

- **Fox-IT InTELL portal URL**: the URL pointing to the API endpoint exposing the service that grants access to the enricher data. Contact the intel provider to subscribe to the service and to obtain this information.
- **SSL certificate file path**: enter the path to the locally stored *.pem* SSL certificate you obtain from Fox-IT after subscribing to InTELL.
- **SSL key file path**: enter the path to the locally stored *.pem* SSL private key related to the SSL certificate.
- **Username**: enter the user name associated to the Fox-IT InTELL Portal account to access and consume the InTELL service.
- **Password**: enter the password associated to the Fox-IT InTELL Portal account to access and consume the InTELL service.
- 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 table view by column. 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.

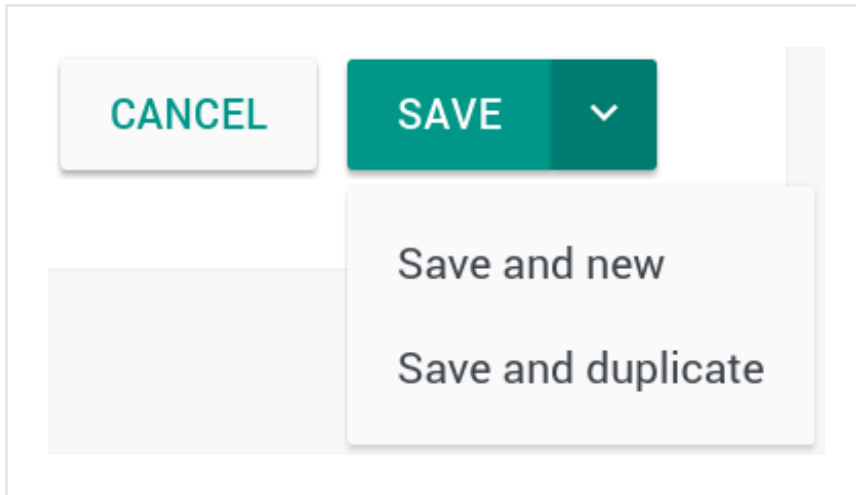
On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 GeolP 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 table view by column. 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 dotted menu 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 dotted menu 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://zebbugtennis.com/wp-conte...> ×

Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	←	Enrichment (1)	7 days ago
	←	Enrichment (2)	7 days ago
<input checked="" type="checkbox"/> 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 Fox-IT InTELL Portal enricher can take the following observable types as input:

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

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 Fox-IT InTELL Portal.

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

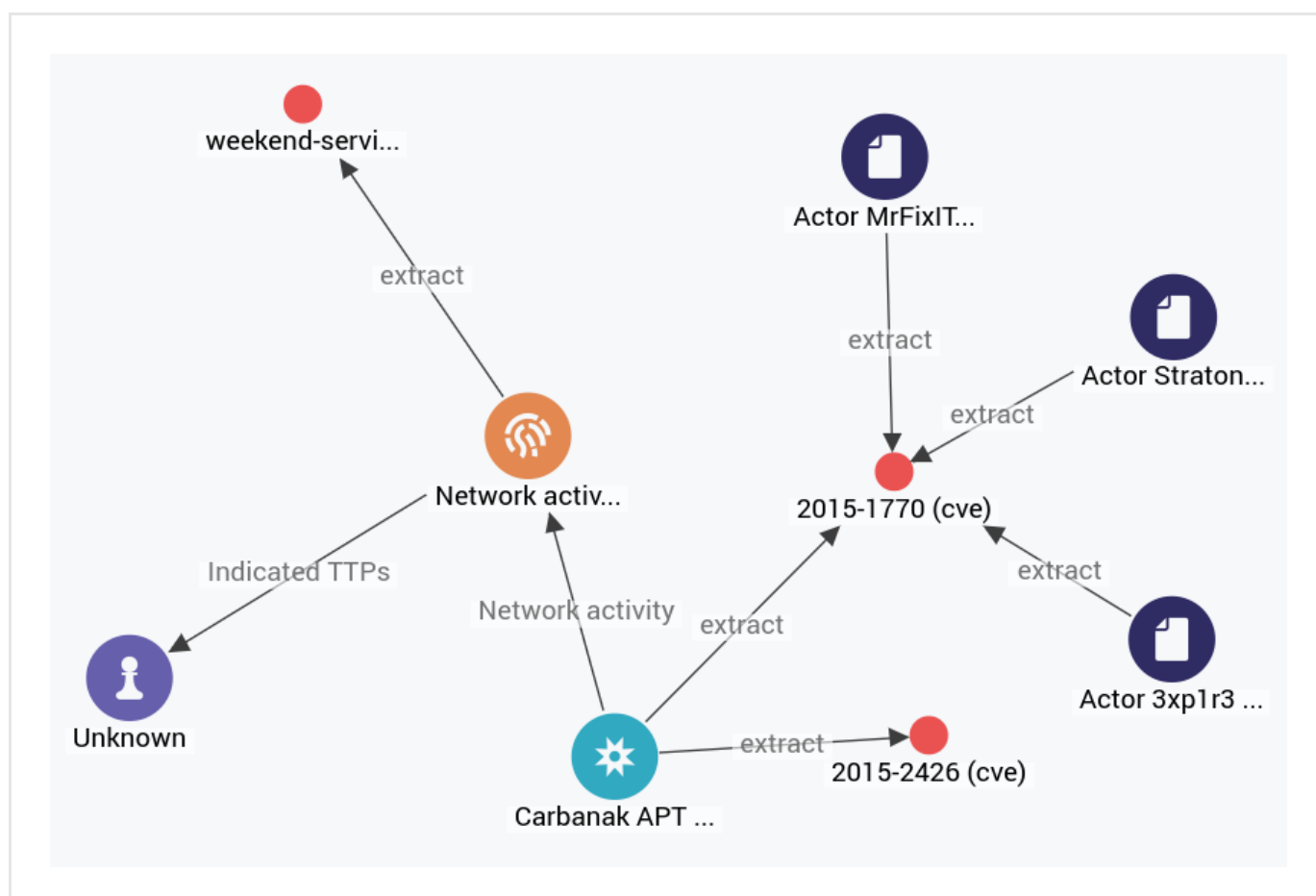
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

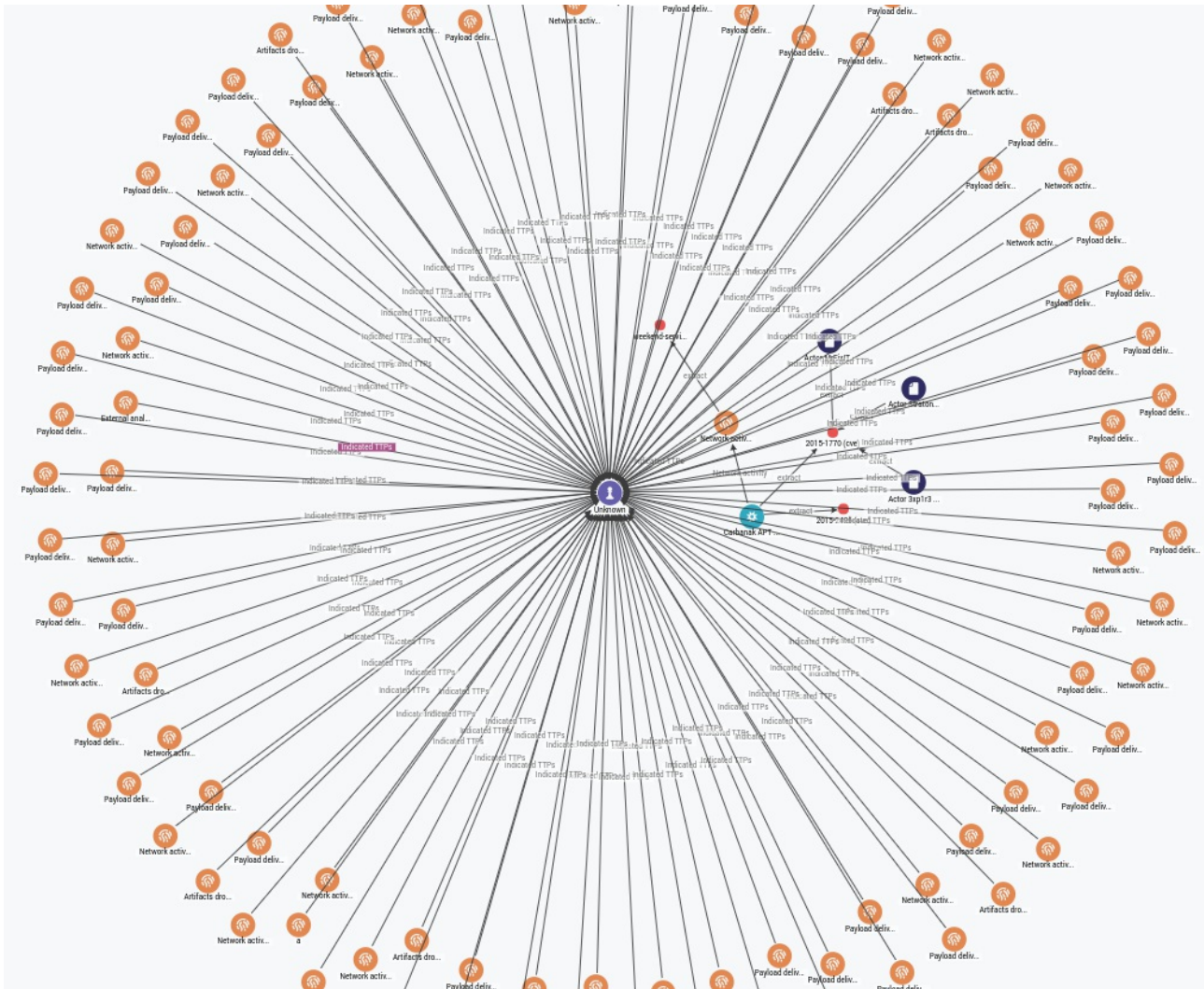
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

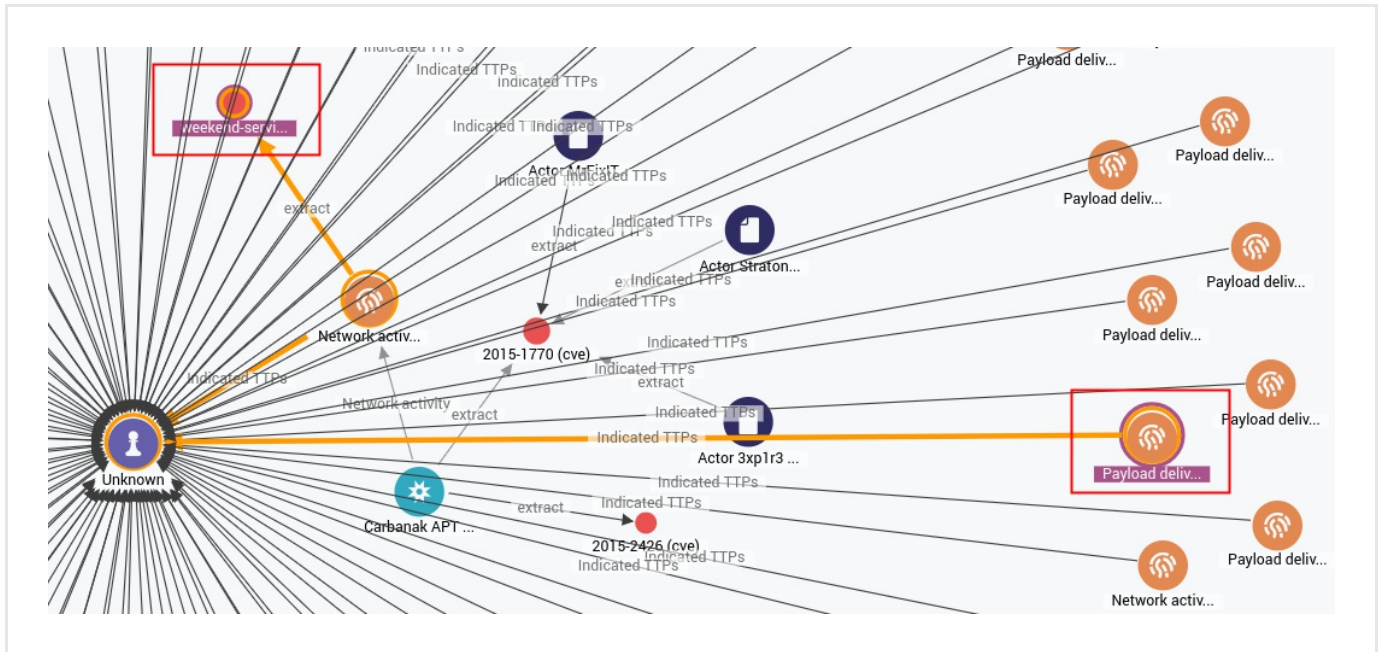


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



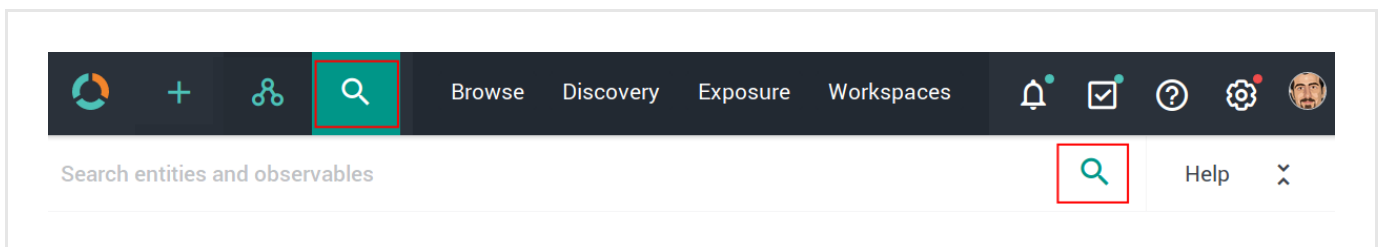
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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 home, add, share, and search, followed by tabs for Browse, Discovery, Exposure, and Workspaces. On the right are notification, checklist, help, settings, and user profile icons. Below the navigation bar is a search bar with the placeholder text "Search entities and observables". To the left of the search results is a sidebar with three buttons: "Filters", "Help", and "Entities". The "Entities" button is highlighted with a red box. The main search 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 same interface as the previous one, but with the "Help" button in the sidebar highlighted with a red box. The main search 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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

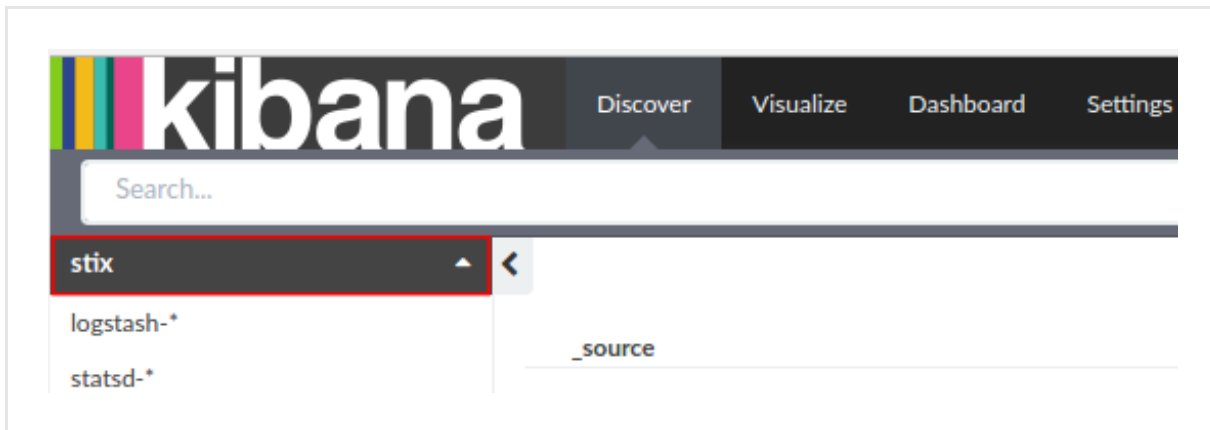
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

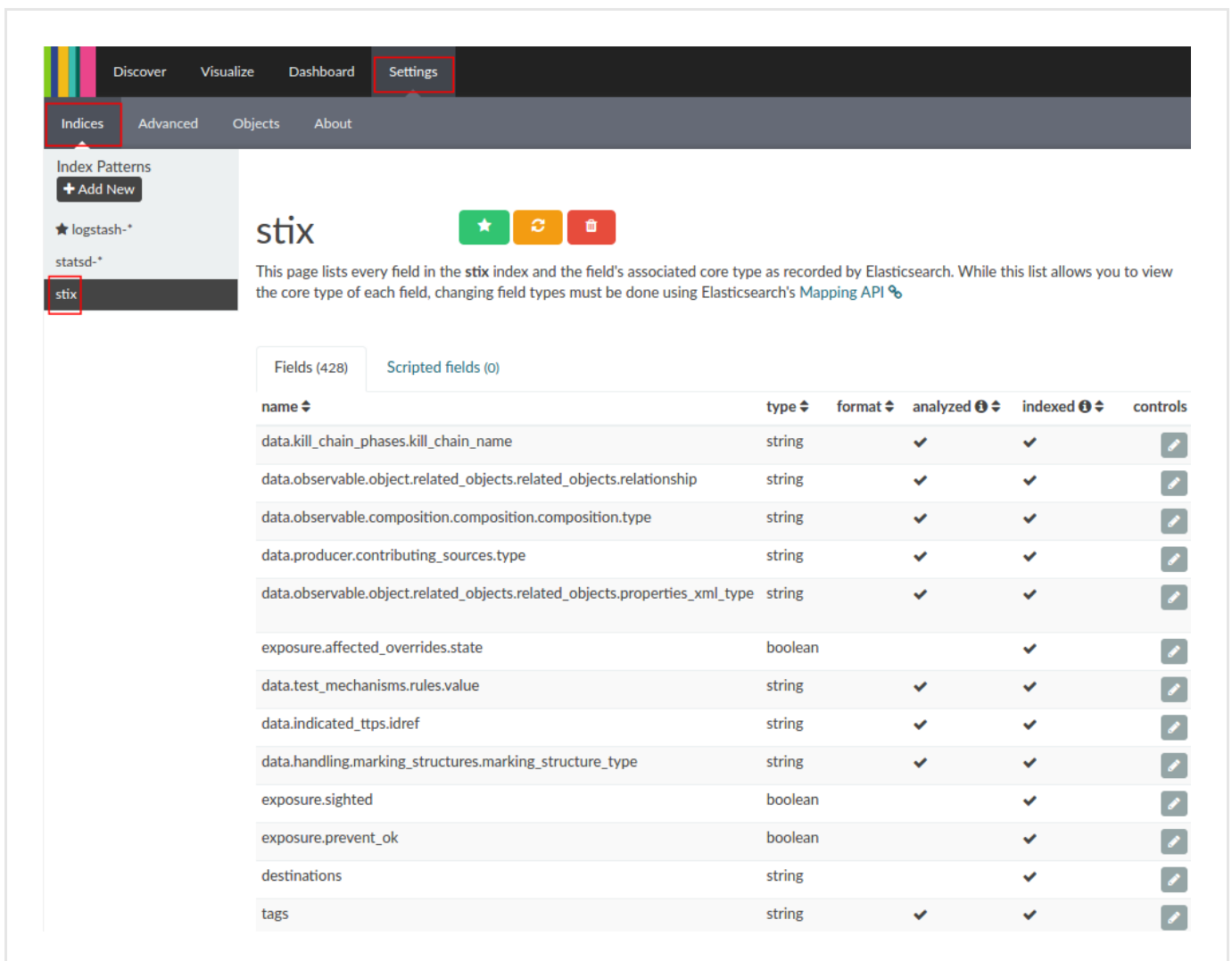
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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 Intel 471 enricher

This article describes how to configure the Intel 471 enricher parameters.

To configure the general options for the Intel 471 enricher, see [Configure enrichers](#).


Intel 471 enricher	
Enricher name	Intel 471
API endpoint	<code>https://api.intel471.com/v1/</code>
Input	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha256
Output	Enriches observables with data focusing on threat actor information.
Description	Besides data on compromised IP addresses, domains, URLs, and emails, Intel 471 focuses on providing first-hand information about threat actors and groups.

Configure the Intel 471 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 Intel 471 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.
- **API key**: contact Intel 471 to receive an API key, and then enter it in the corresponding input field.
- **Email**: enter the email address associated to the Intel 471 account to access and consume the Intel 471 API service.
- 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 table view by column. 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:

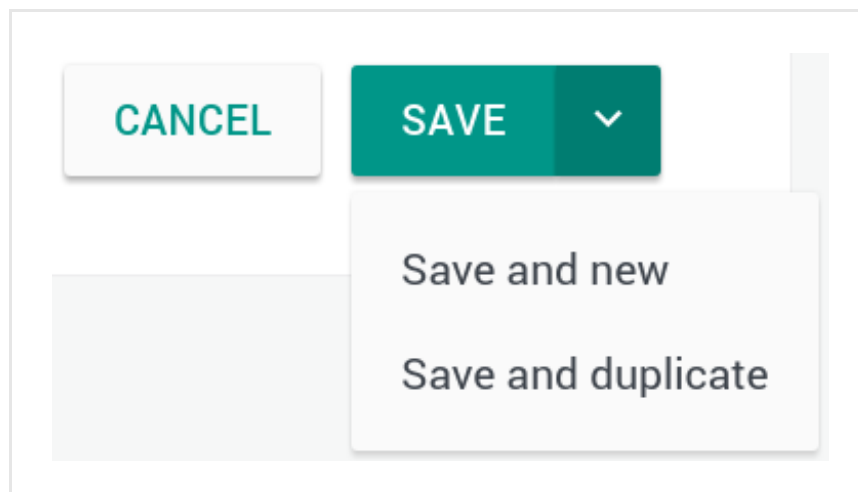
- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

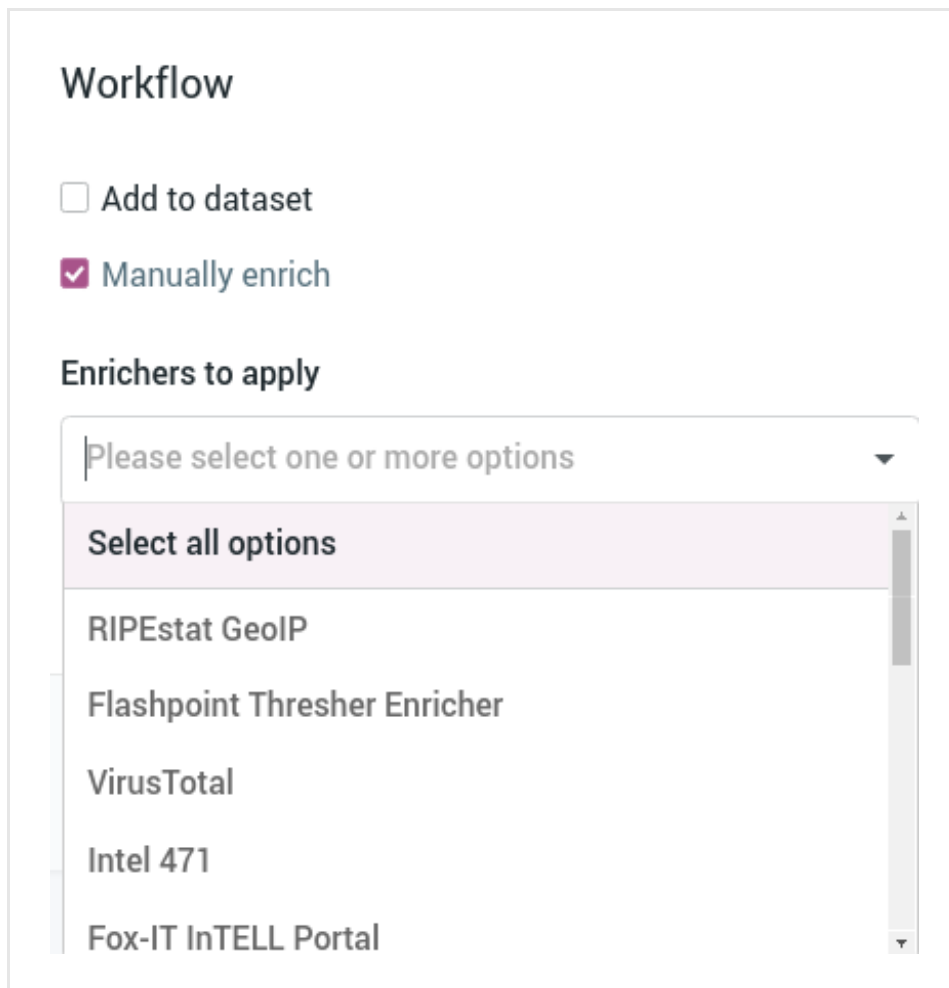
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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...' interface. At the top, there is a teal header bar with the title, a flag icon, and metadata: 'Ingested: 01/24/2017 12:14 AM', 'Group: Testing Group', 'Author: Tes...', and 'TLP None'. Below the header, there are tabs: OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The OBSERVABLES tab is selected. On the left, there is a red-bordered dropdown menu labeled 'Enrich' with the following options: 'Enrich all observables', 'Enrich selected observables', 'Elastic Sightings Enricher', and 'OpenResolve'. To the right of the dropdown is a button labeled 'ADD OBSERVABLE'. Below these, there is a table with columns: Origin, Maliciousness, Date, Lv, Conn, Origins, and Created. The 'Created' column has a refresh icon (a circular arrow) highlighted with a red box. The table shows two rows of data, both labeled 'Enrichment (1)' and '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://zebbugtennis.com/wp-conte...> ×

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

○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	←	Enrichment (1)	7 days ago ⋮
	←	Enrichment (2)	7 days ago ⋮
<input checked="" type="checkbox"/> 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 Intel 471 enricher can take the following observable types as input:

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

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 Intel 471.

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

Review enrichment observables on the graph

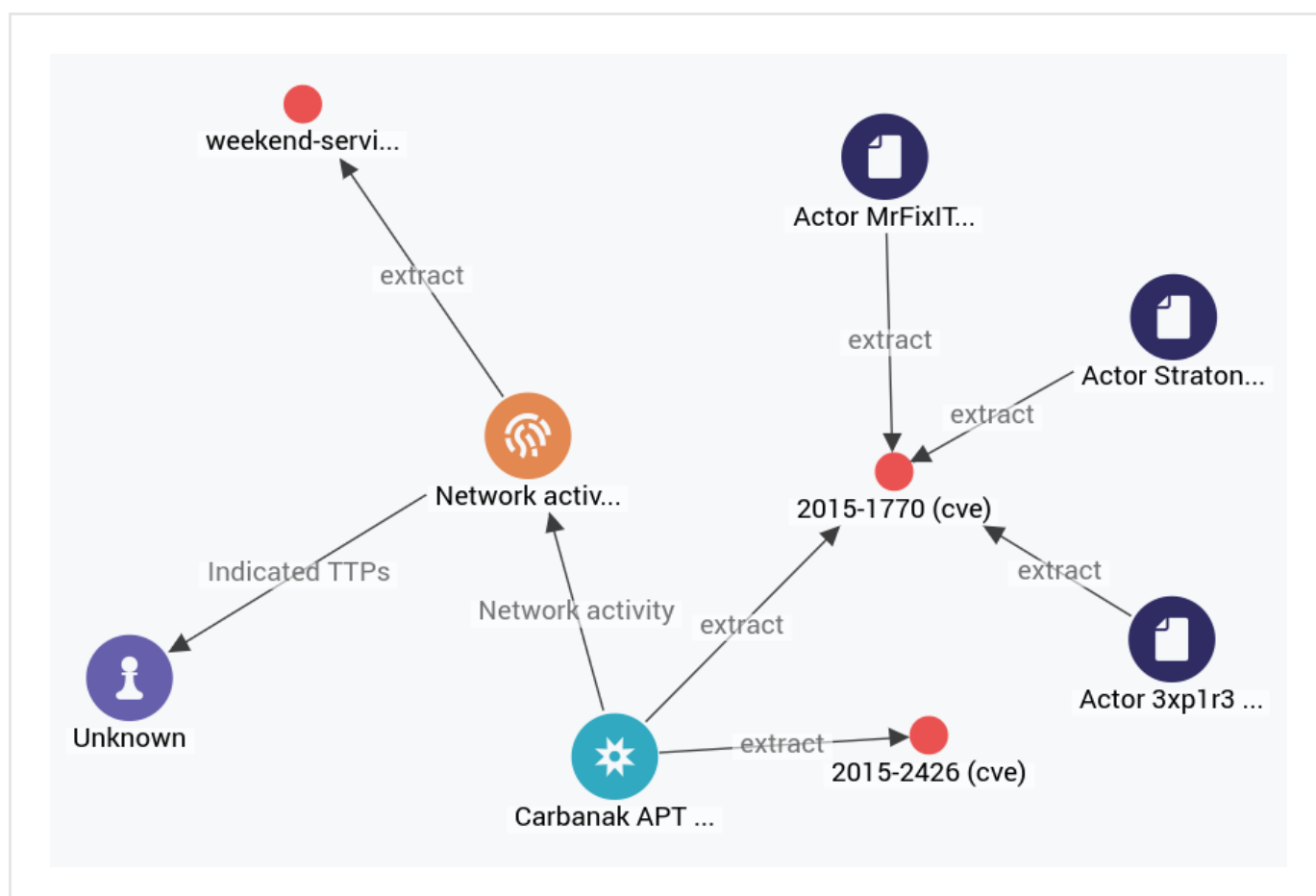
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

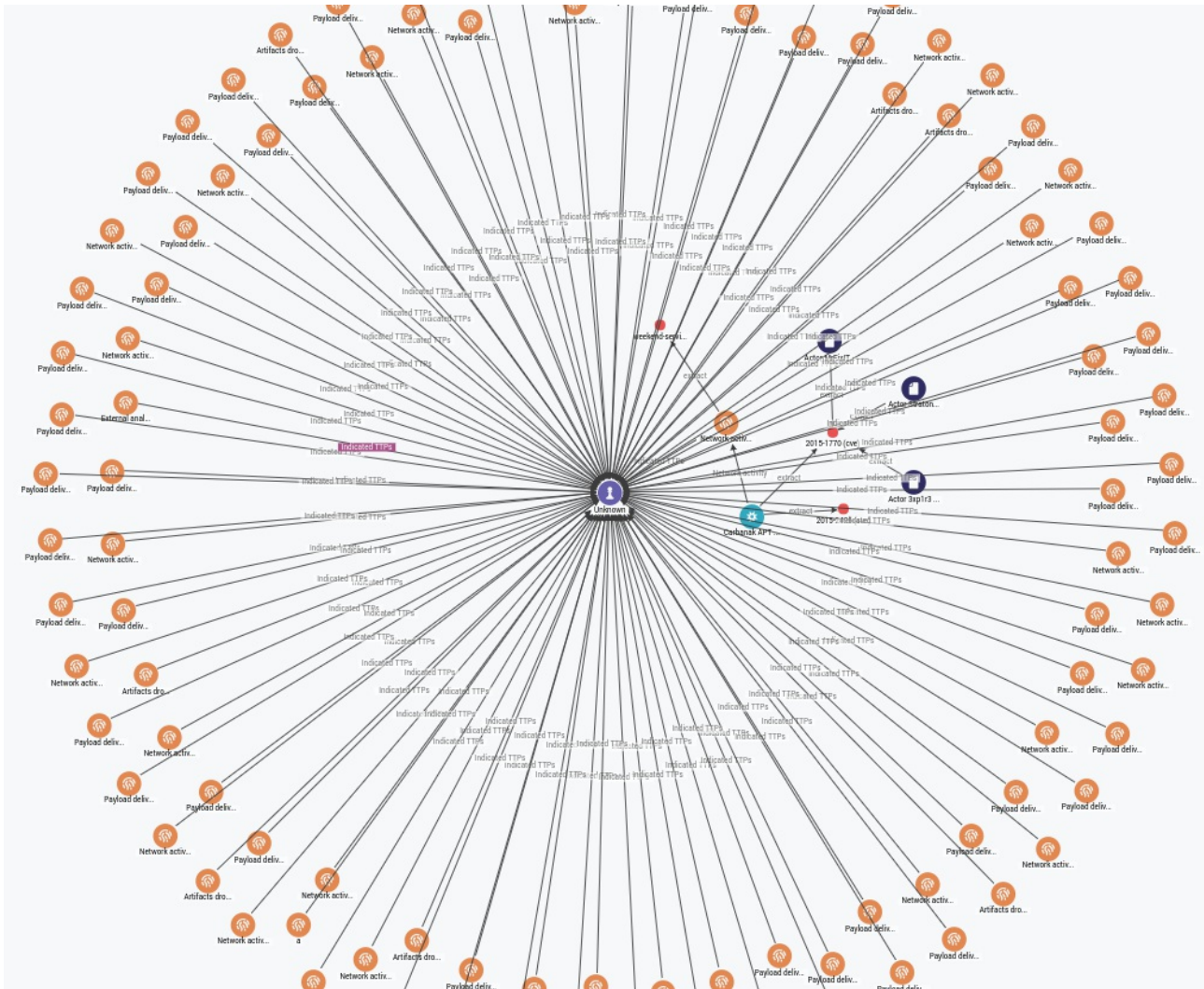
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	⋮
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdp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

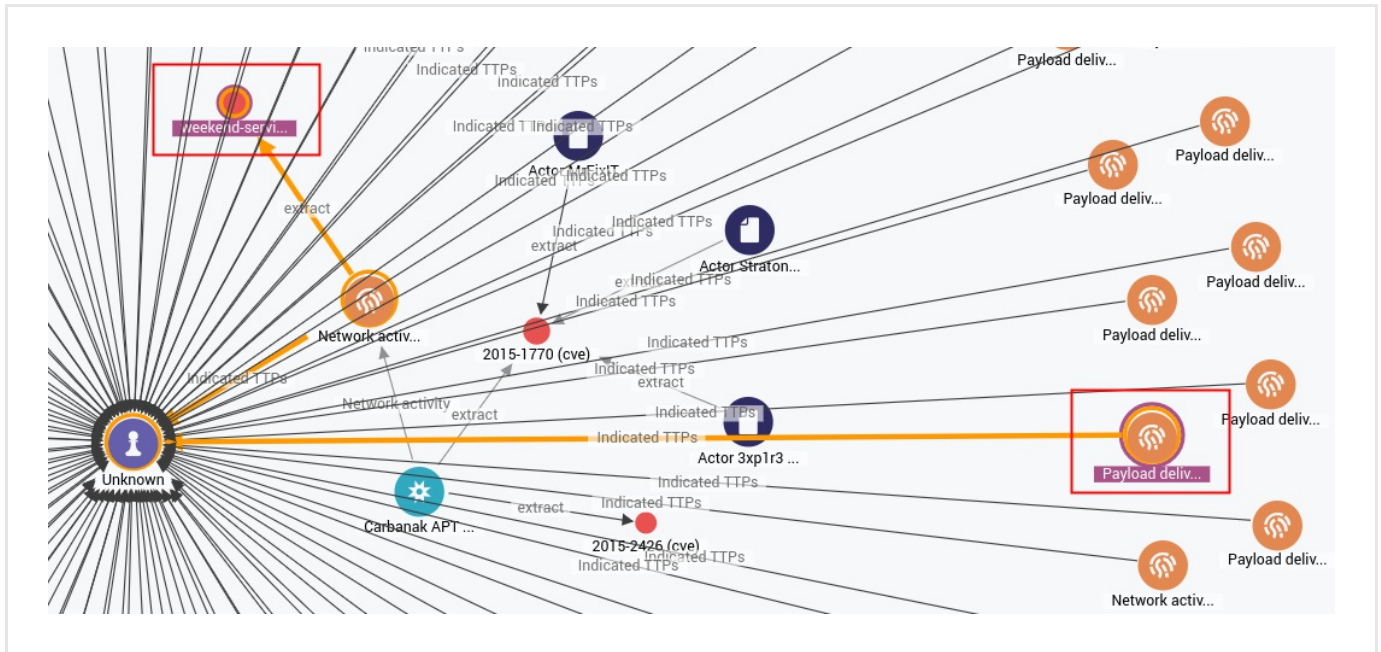


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



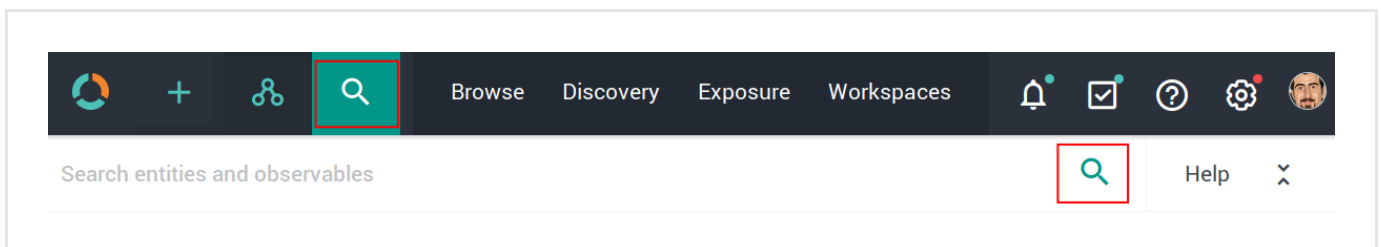
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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.

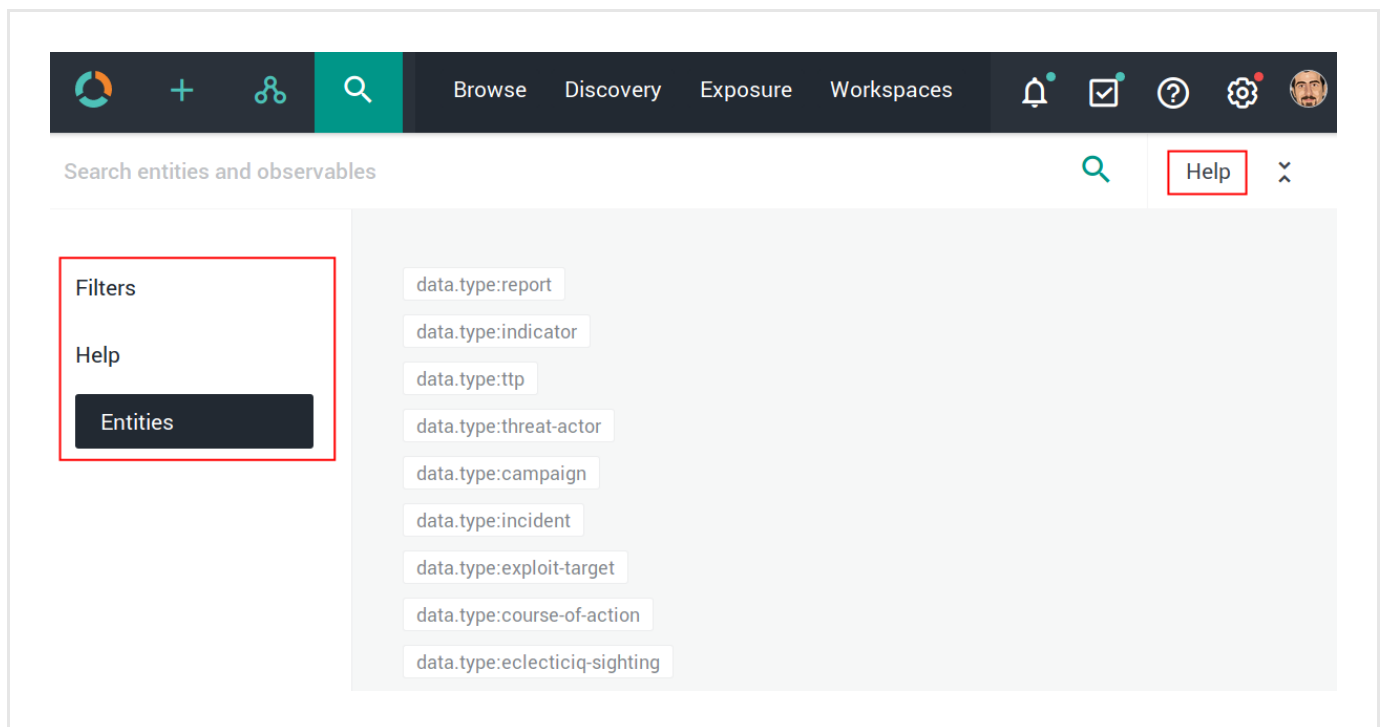


The search functionality uses **Elasticsearch query syntax**

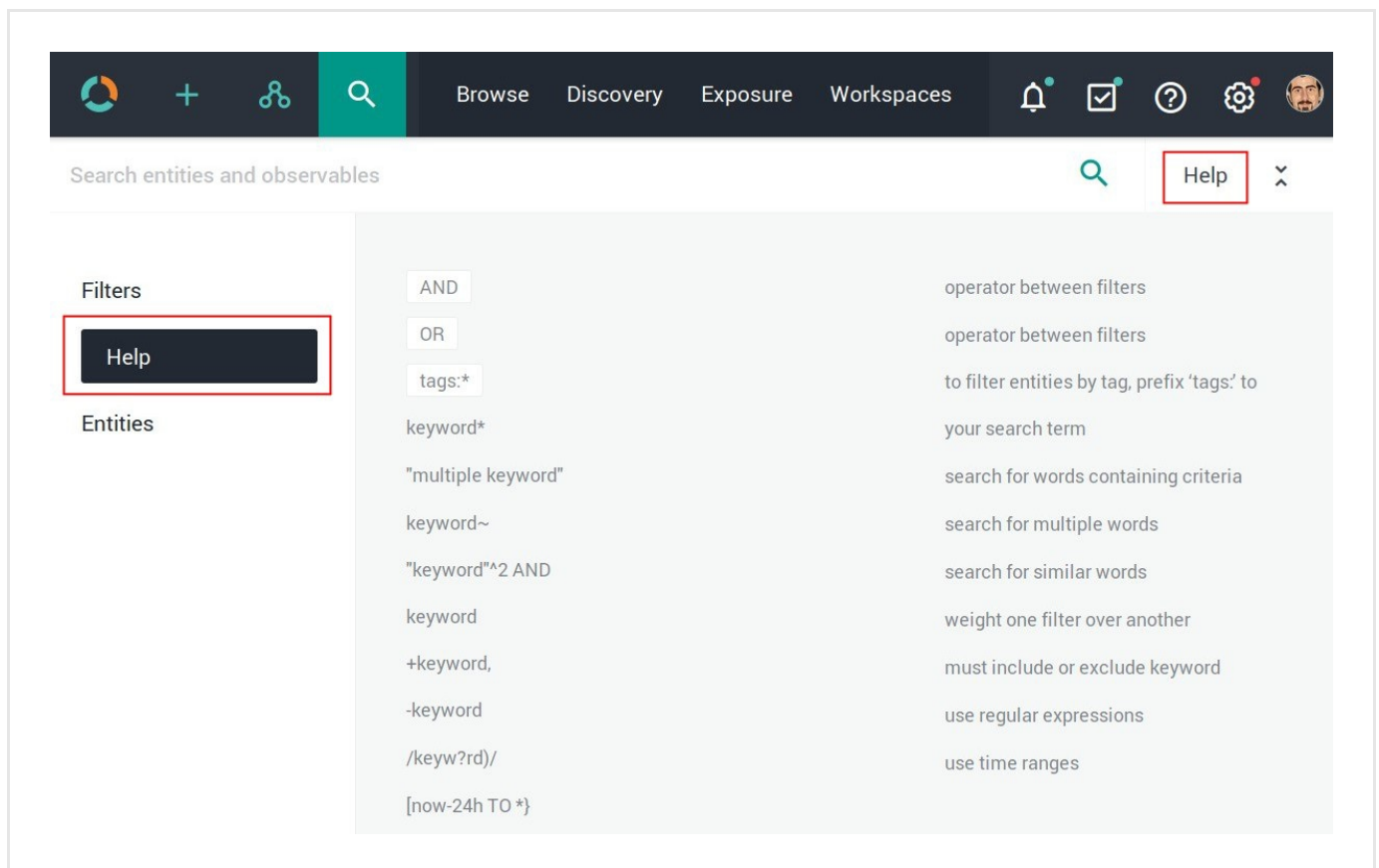
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

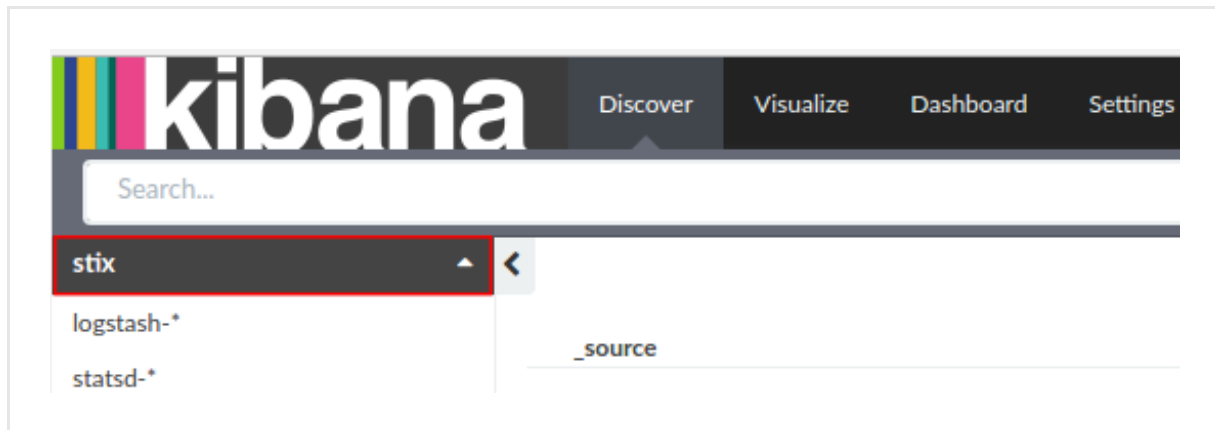
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

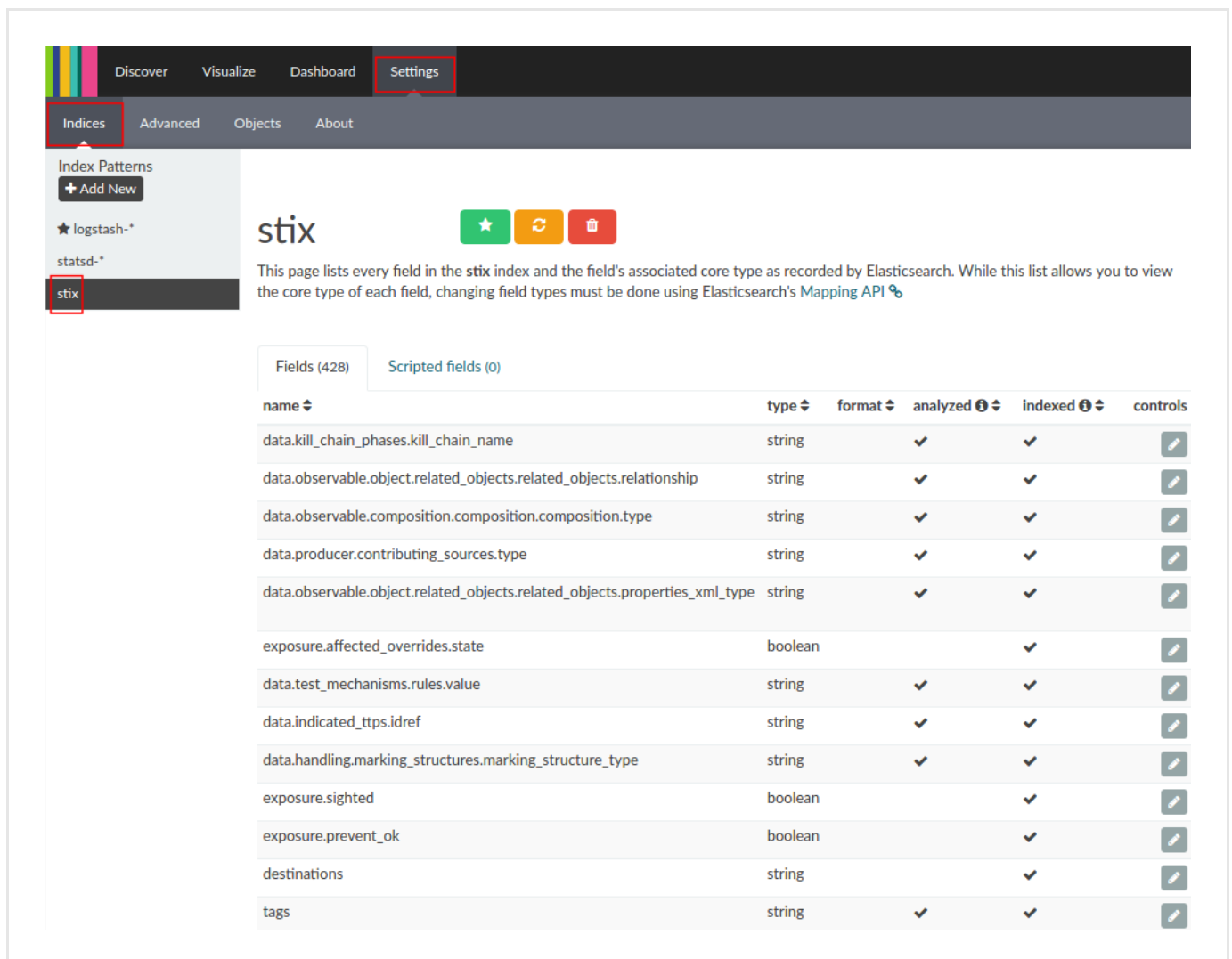
Keep the trailing /.

Example: [https://platform.host.com/api/kibana/app/kibana#/.](https://platform.host.com/api/kibana/app/kibana#/)

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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.


OpenDNS OpenResolve enricher

Configure the OpenDNS OpenResolve 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.

- **Name:** the name used to identify the enricher. It should be descriptive and easy to remember.
- **Description:** additional textual details. If you want, you can add a short description to provide more information and context.

- **Cache validity (sec)**: defines for how long enrichment data remains stored in the cache. The value is expressed in seconds.
- **Rate limit (per sec)**: sets the maximum allowed number of requests/executions per second.
- **Monthly execution cap (executions)**: sets a maximum allowed number of requests/executions per month.
Together with rate limiting, execution cap helps control data traffic for the enricher; for example, when the API or the service you are connecting to enforces usage limits.
- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).
Example: *B - Usually reliable*
- **Enabled**: checkbox. Select the **Enabled** checkbox to enable the enricher task immediately after editing and saving it.
If you select the checkbox, the rule is executed automatically. If you deselect it, you need to run the rule manually.
- Under **Parameters**, define the specific configuration options for the selected enricher, where applicable.
- Click **Save** to store your changes, or **Cancel** to discard them.


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 table view by column. 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.

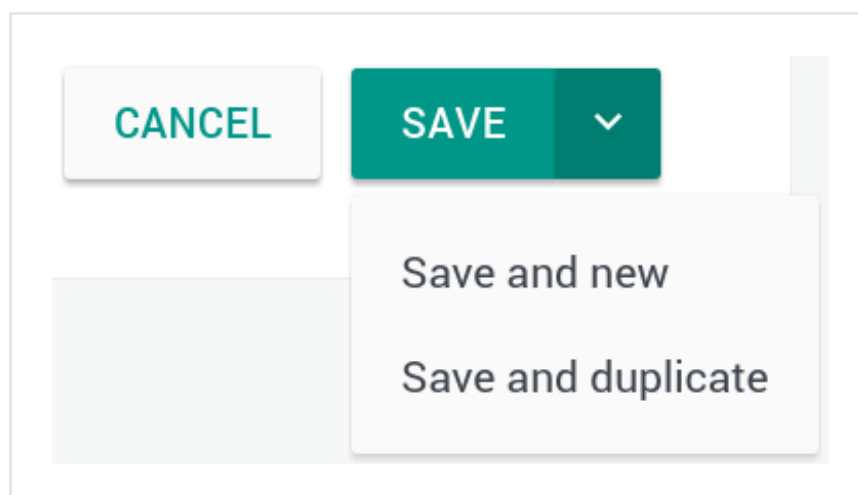
On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

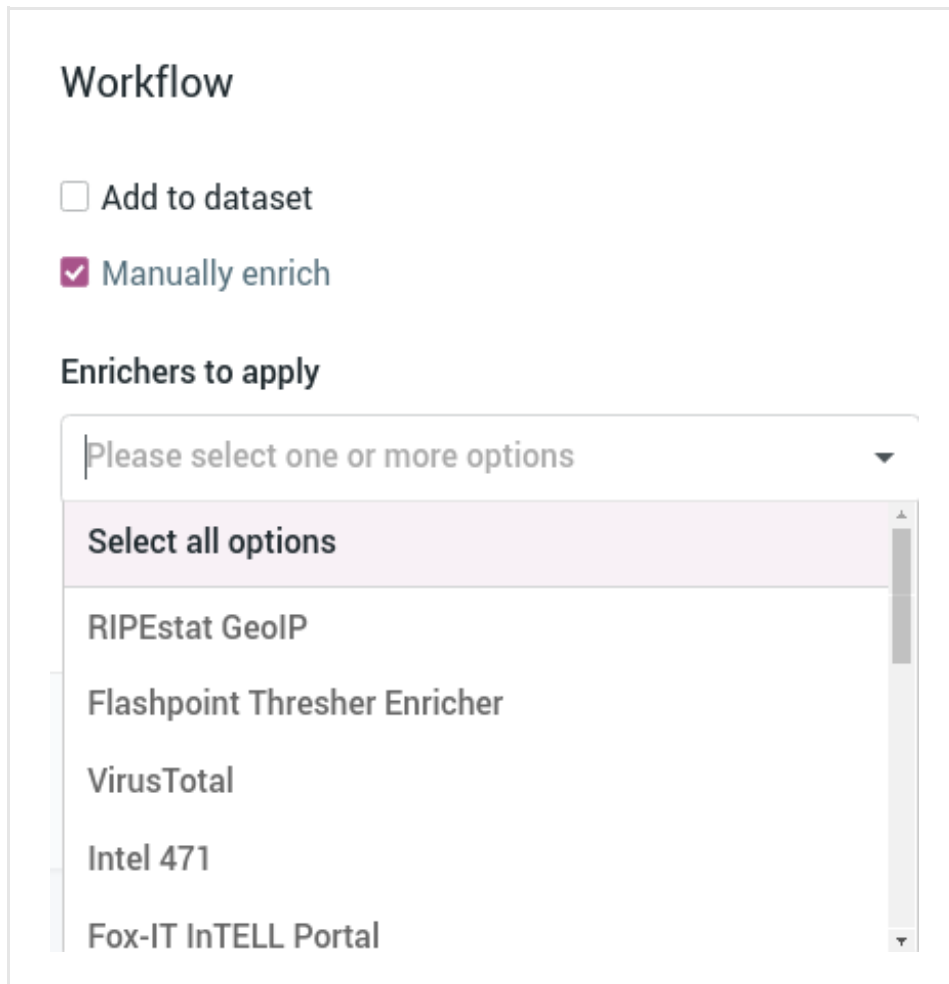
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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 GeolIP
- 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.

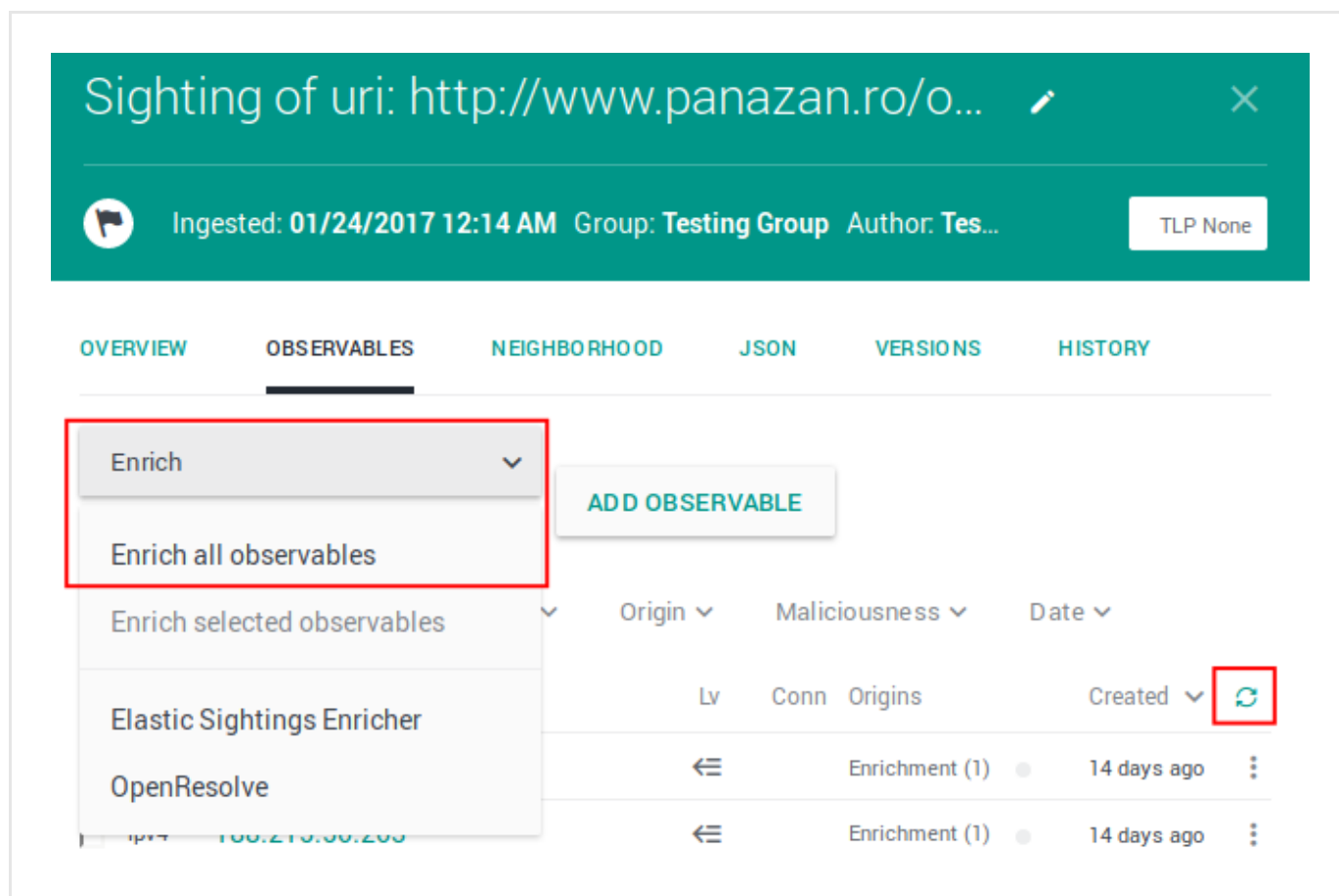
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.



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://zebbugtennis.com/wp-conte...> ×

Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

		Origin ▼	Maliciousness ▼	Date ▼
		Lv	Conn	Origins
				Created ▼ ↻
		⌄		Enrichment (1) ● 7 days ago ⋮
		⌄		Enrichment (2) ● 7 days ago ⋮
<input checked="" type="checkbox"/>	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

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

Review enrichment observables on the graph

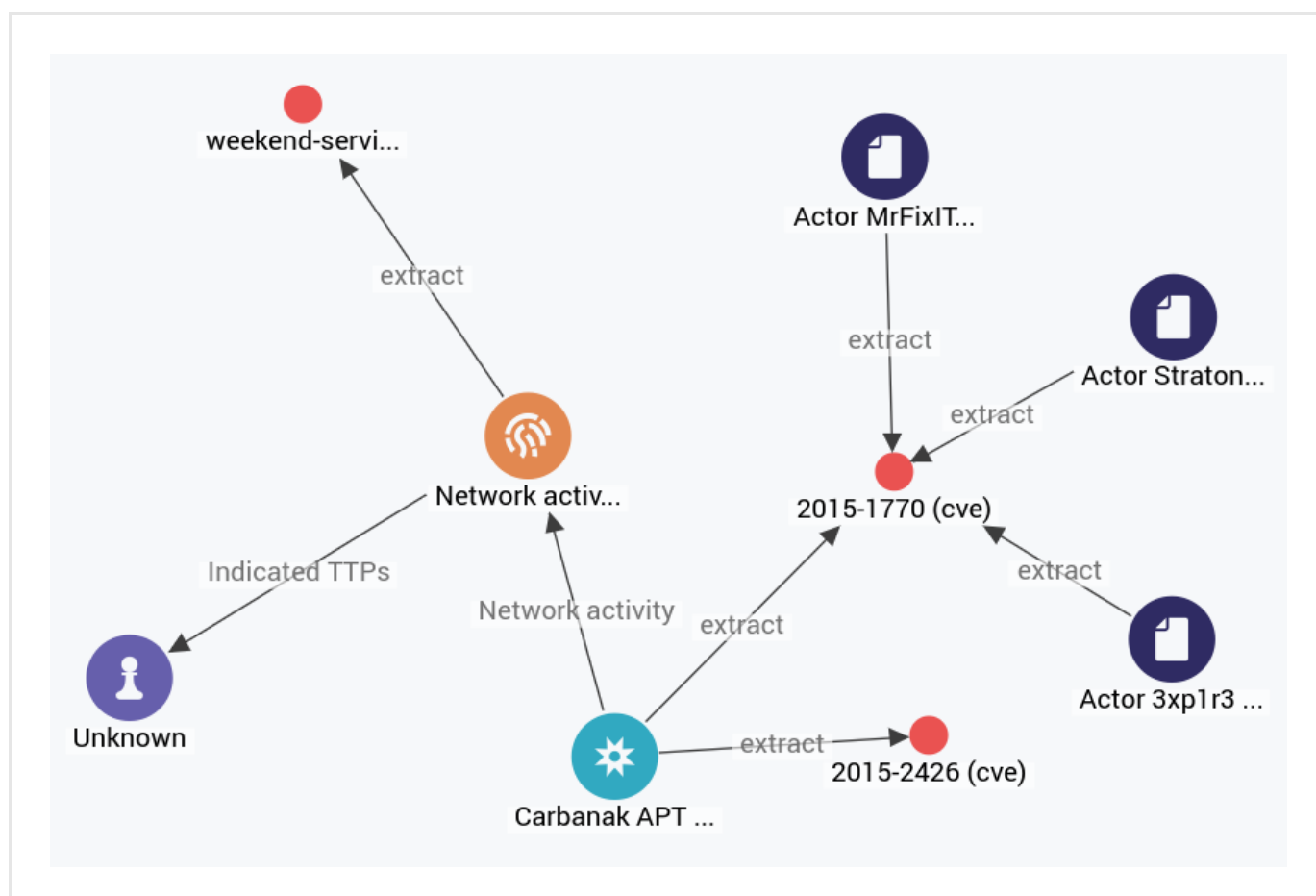
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

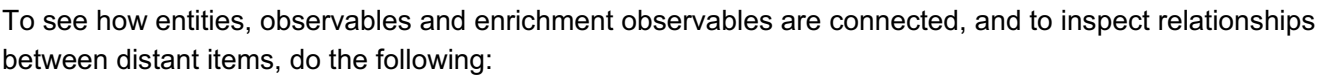
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

Ignore extract
 Create sighting
Add to graph
 Set maliciousness >

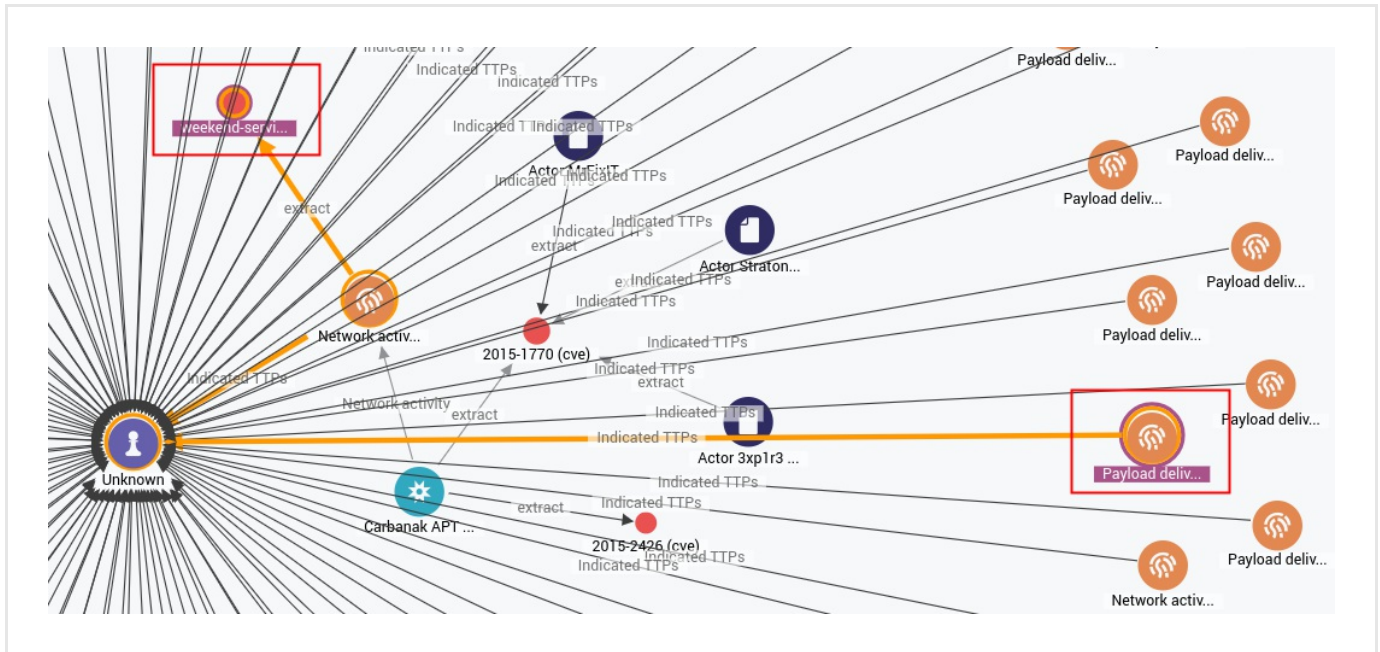
- To load the parent entity whose detail pane you are viewing, instead of its observables, from the pop-up **Actions** menu at the bottom of the pane select **Add to graph**.
- Click the graph thumbnail on the lower side of the screen to expand it.
- On the graph, right-click the entity you want to inspect,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

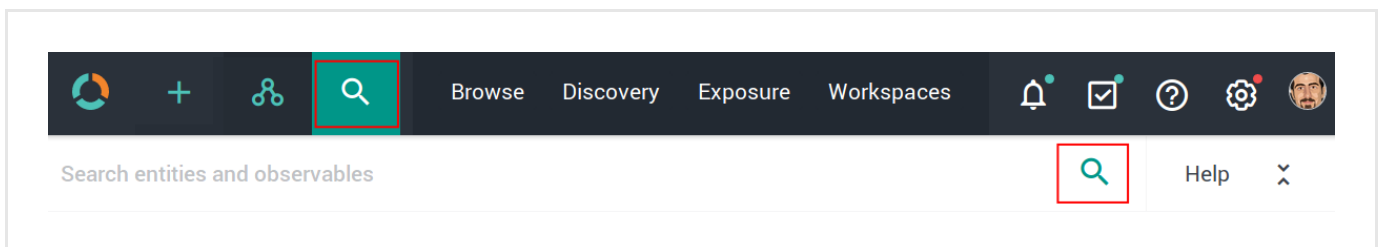


- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist,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

The screenshot shows the top navigation bar with icons for home, add, share, and search, followed by tabs for Browse, Discovery, Exposure, and Workspaces. On the right are notification, checklist, help, settings, and user profile icons. Below the navigation bar is a search bar with the placeholder text "Search entities and observables". To the left of the search results is a sidebar with three buttons: "Filters", "Help", and "Entities". The "Entities" button is highlighted with a red border. The main search 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 same interface as the previous one, but with the "Help" button in the sidebar highlighted with a red border. The main search 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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

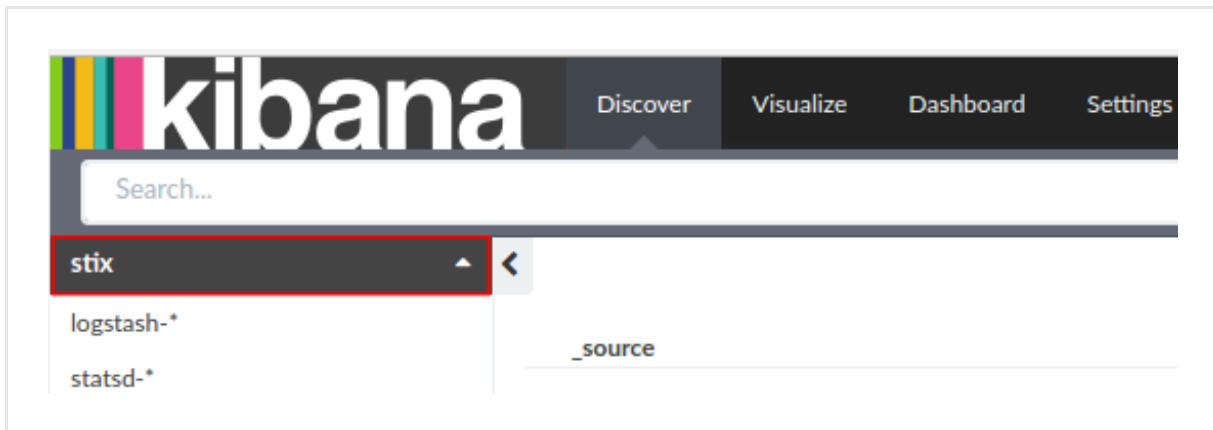
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

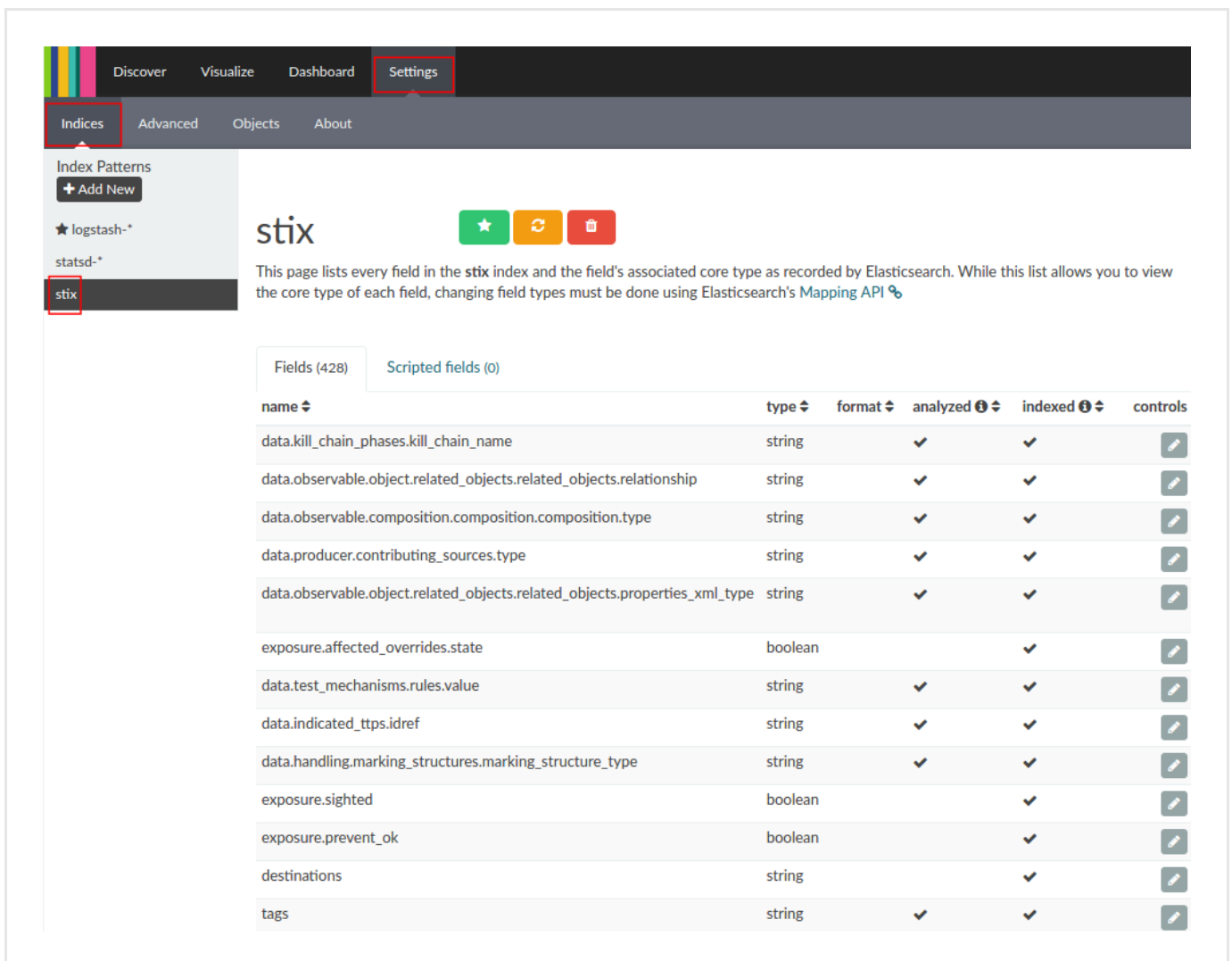
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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 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 PassiveTotal enrichers

EclecticIQ Platform includes the following PassiveTotal enrichers:

- PassiveTotal Whois
- PassiveTotal Passive DNS
- PassiveTotal IP/Domain
- PassiveTotal Malware

Configure the enrichers

The PassiveTotal enrichers included in the platform share the same configuration options.

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

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

Alternatively:

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



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

- **Name:** the name used to identify the enricher. It should be descriptive and easy to remember.
- **Description:** additional textual details. If you want, you can add a short description to provide more information and context.
- **Cache validity (sec):** defines for how long enrichment data remains stored in the cache. The value is expressed in seconds.
- **Rate limit (per sec):** sets the maximum allowed number of requests/executions per second.
- **Monthly execution cap (executions):** sets a maximum allowed number of requests/executions per month.
Together with rate limiting, execution cap helps control data traffic for the enricher; for example, when the API or the service you are connecting to enforces usage limits.
- **Source reliability:** from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).
Example: *B - Usually reliable*
- **Enabled:** checkbox. Select the **Enabled** checkbox to enable the enricher task immediately after editing and saving it.
If you select the checkbox, the rule is executed automatically. If you deselect it, you need to run the rule manually.
- Under **Parameters**, define the specific configuration options for the selected enricher, where applicable.
- Click **Save** to store your changes, or **Cancel** to discard them.


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 table view by column. 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.

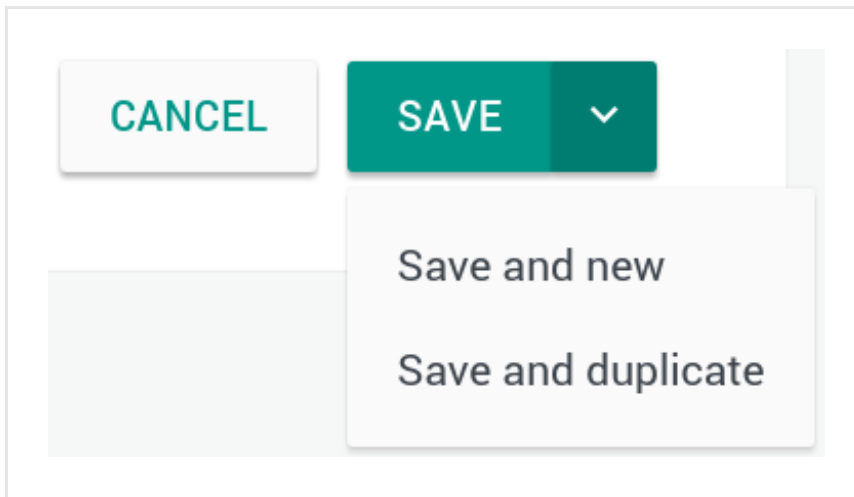
On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 GeolIP 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 table view by column. 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 dotted menu 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 dotted menu 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://zebbugtennis.com/wp-conte...> ×

Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
Origin ▼
Maliciousness ▼
Date ▼

Enrich selected observables (6)

Elastic Sightings Enricher
OpenResolve

		Origin ▼	Maliciousness ▼	Date ▼	
		Lv	Conn	Origins	Created ▼ ↻
<input checked="" type="checkbox"/>	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

PassiveTotal enrichers can take the following observable types as input:

- *ipv4, ipv6, domain, host*

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

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

- Select an entity; for example, from a dataset, from **Browse** or from **Discovery**.
An overlay slides in from the side of the screen to display the entity detail pane.

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

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

Kind	Value	Origin	Created
The data type of the retrieved enrichment that can be associated to the entity. For example, an IP address, a hash, an actor's name, and so on.	The value of the retrieved enrichment data. For example, <i>192.0.1.168</i> , <i>E61B746K5GB85OI7K99IPOIU89B...</i> , <i>Mr. Smith</i> (<i>images/mr-smith.png</i>).	The entity the retrieved enrichment data is related to. This piece of information connects the entity with the enrichment data in the observable.	The enrichment data ingestion date.

You can narrow down the displayed results by clicking one or more quick filters above the table view to select and filter by specific:

- **Maliciousness**: select the checkboxes to display only **Malicious**, **Safe**, or **Unknown** observables. You can select multiple choices to view combined results
- **Origin**: select the checkboxes to display only observables ingested through **Enrichment**, or only observables ingested as embedded objects in a containing **Entity**. You can select multiple choices to view combined results
- **Kind**: select the observable types to filter the observables you want to display. You can select multiple choices to view combined results

- **Date:** select a time interval to display only the observables ingested within the specified dates.

When available, a number next to the observable origin indicates a direct or an indirect relationship of the observable with the origin, and colored dots flag the observable maliciousness or safety level. You can adjust or set these values with observable rules.

<input type="checkbox"/>	KIND	VALUE		ORIGIN	CREATED ▾
<input type="checkbox"/>	ipv4	65.19.141.203	2		a month ago
<input type="checkbox"/>	domain	ict.org.il	2		a month ago
<input type="checkbox"/>	hash-md5	4e1e2b9cd6b5bca2b1b935ddc97...	2		a month ago
<input type="checkbox"/>	cve	2012-4792	2		a month 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 dotted menu 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

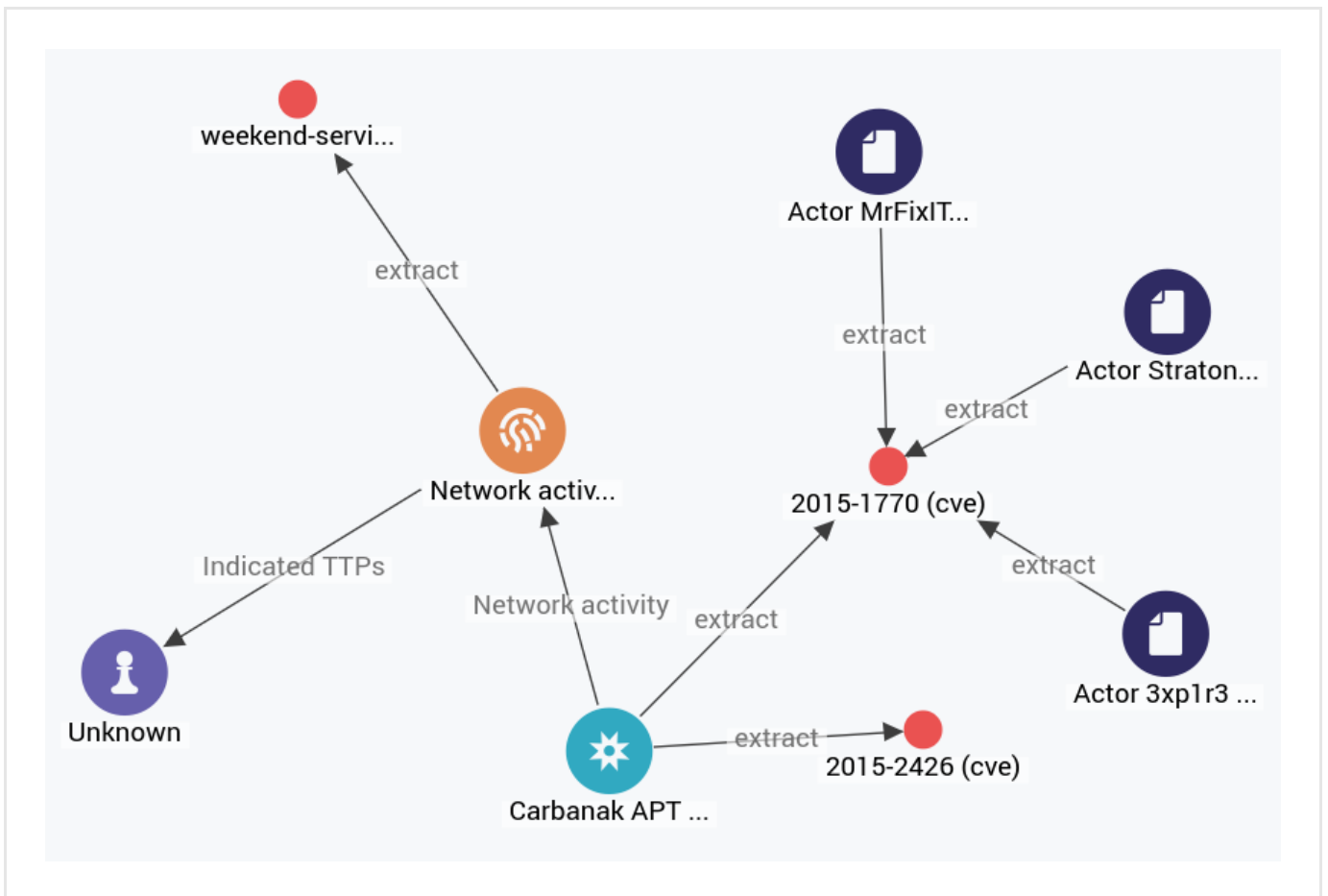
Create sighting

Add to graph

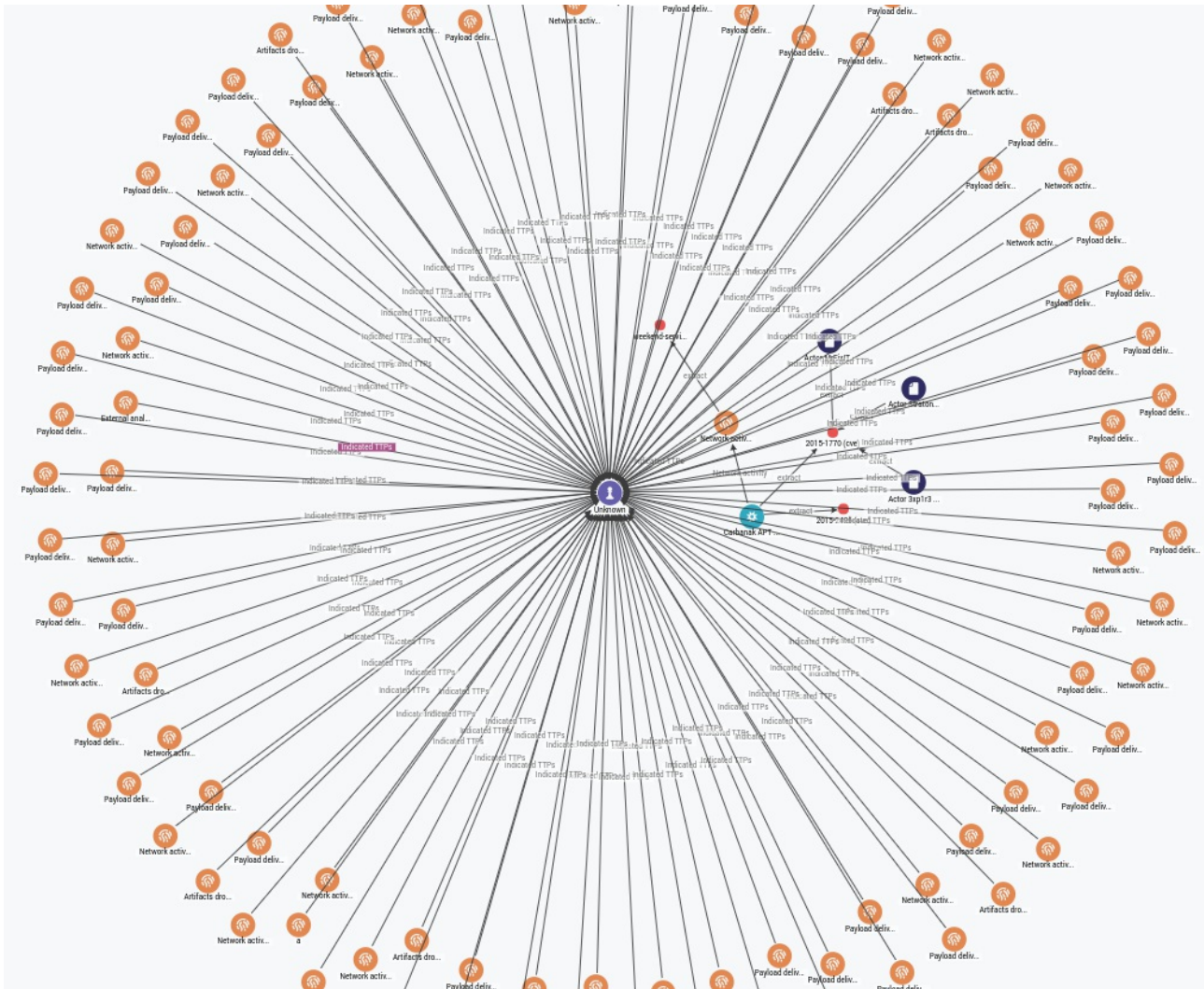
Set maliciousness >

- 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**.

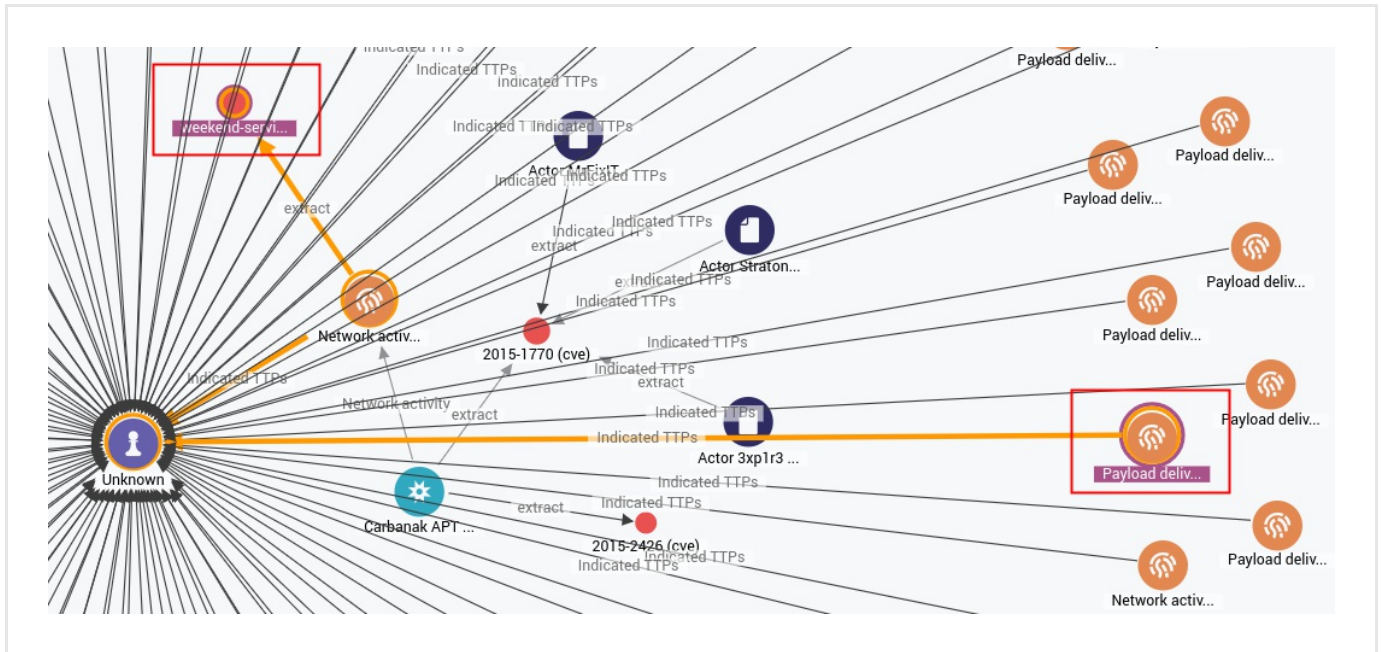


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All, Load observables > All** or **Load entities by extract > All**.



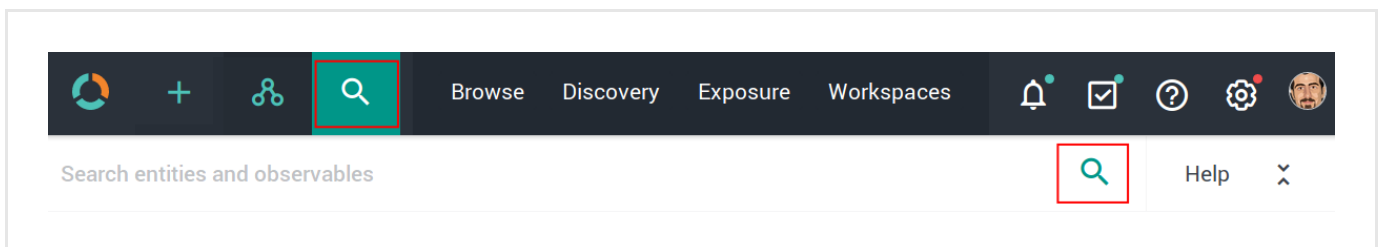
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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.

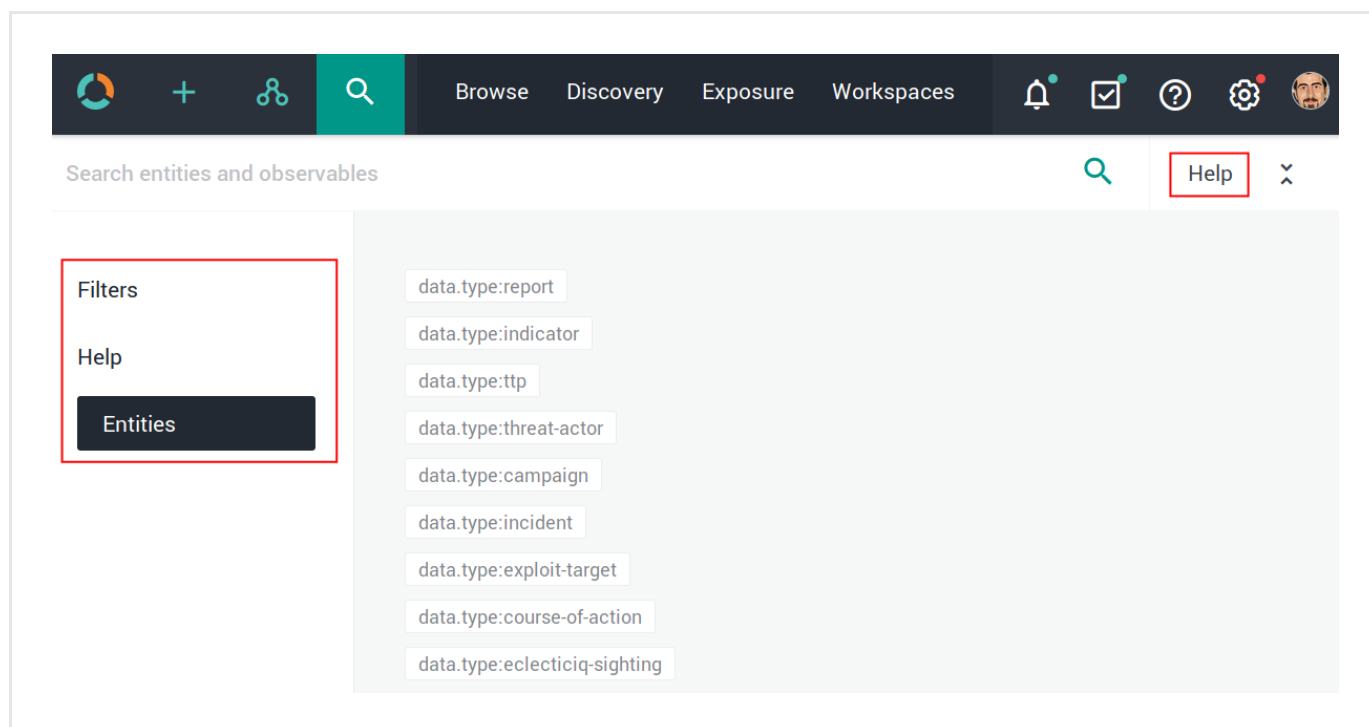


The search functionality uses **Elasticsearch query syntax**

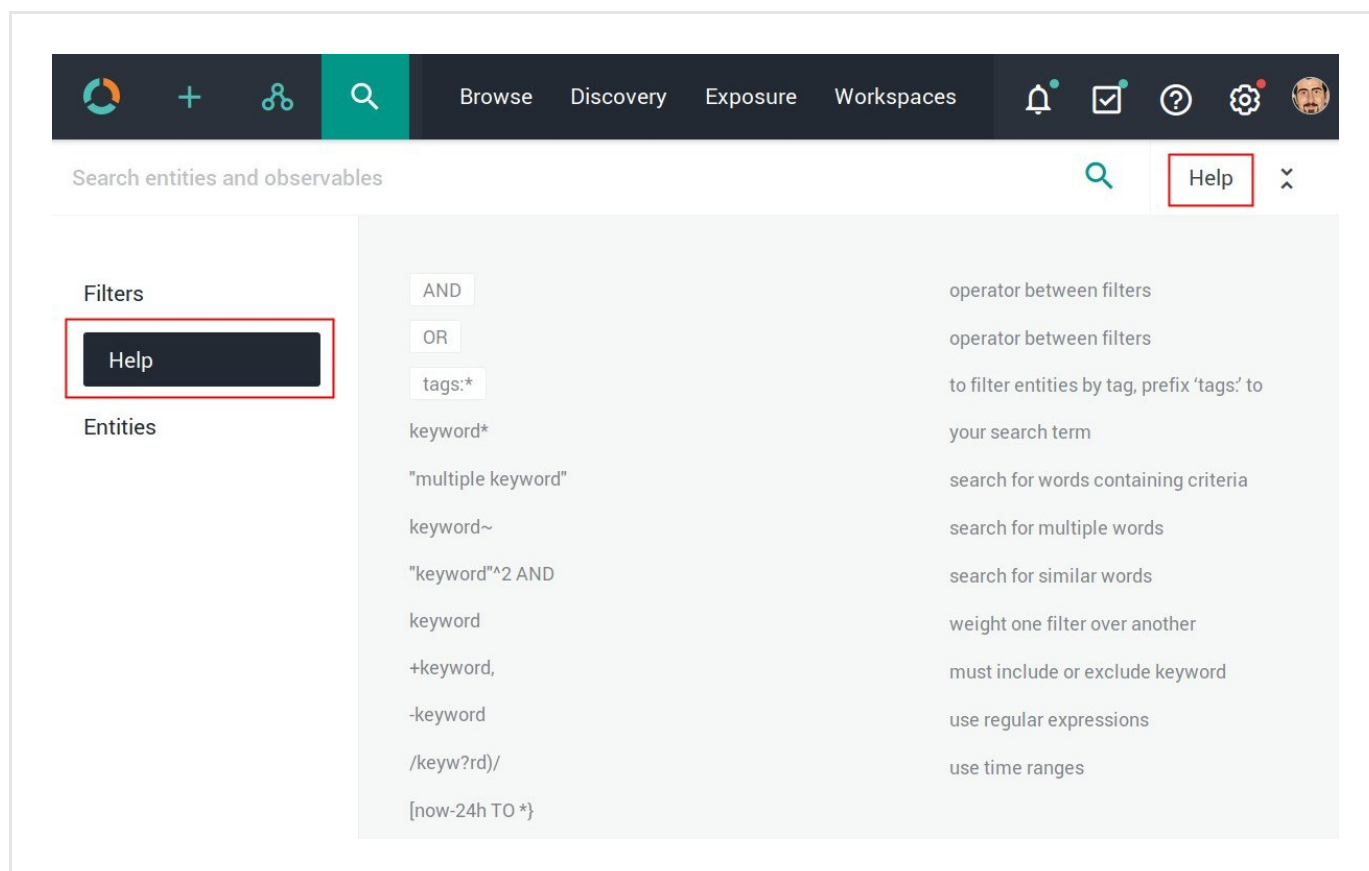
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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
```

The enricher observable-specific query fields are summed up below:

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

Enricher	Supported kinds (observable types)
RIPEstat GeolIP	ipv4, ipv6
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

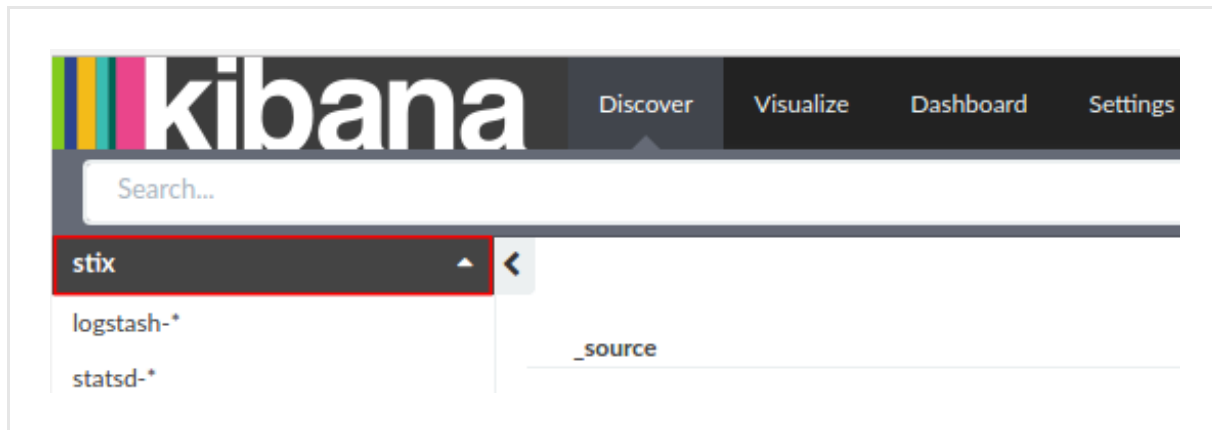
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

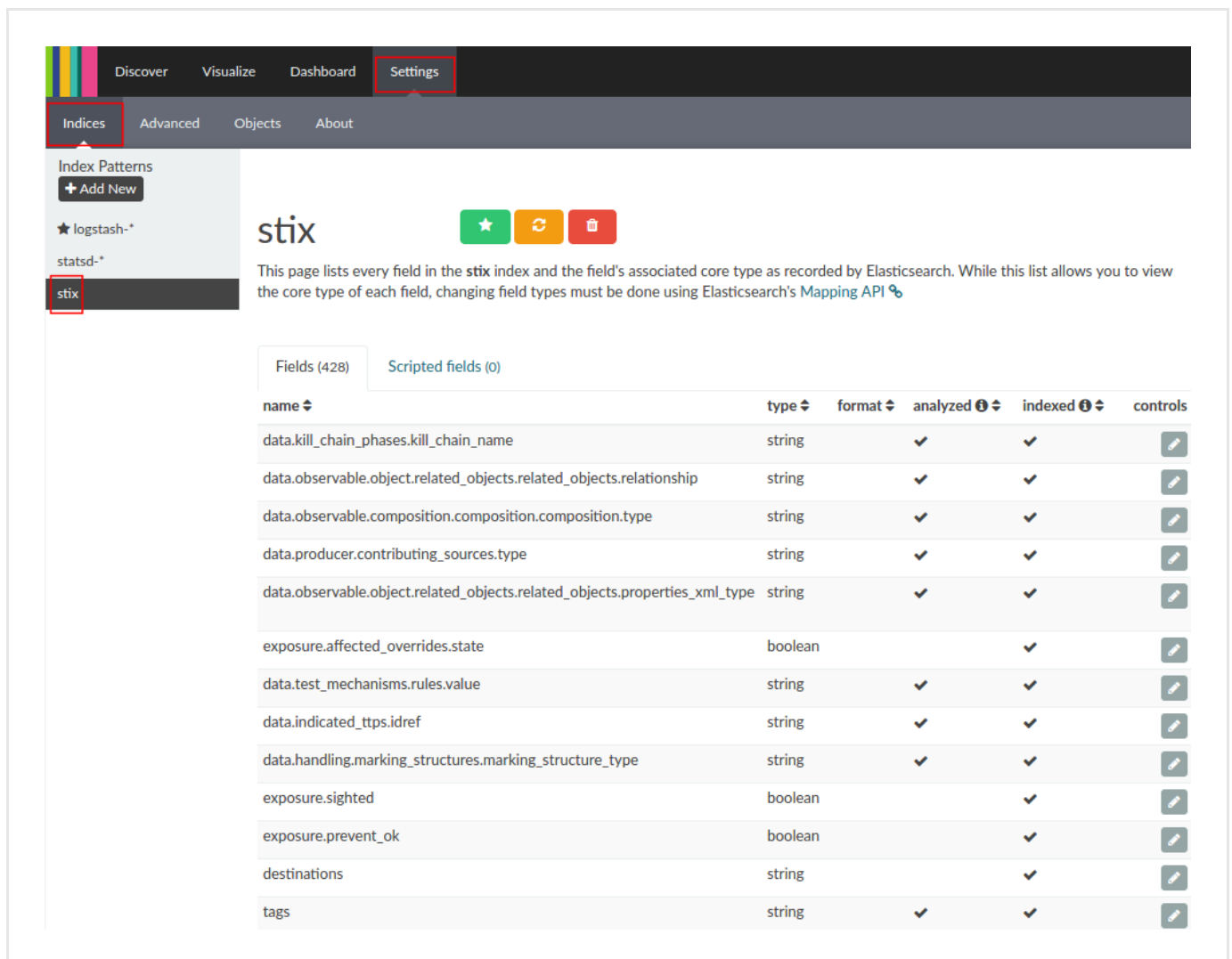
Keep the trailing /.

Example: [https://platform.host.com/api/kibana/app/kibana#/.](https://platform.host.com/api/kibana/app/kibana#/)

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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 PyDat enricher

This article describes how to configure the PyDat enricher parameters.

To configure the general options for the PyDat enricher, see [Configure enrichers](#).


PyDat enricher	
Enricher name	PyDat
API endpoint	<code>http://10.0.1.60:8000/</code> (example)
Input	ipv4, ipv6, domain
Output	Enriches observables with whois data, current IP resolution and passive DNS information.
Description	PyDat (https://github.com/mitrecnd/whodat#pydat) is installed locally, and it can work together with an Elasticsearch instance (https://github.com/mitrecnd/whodat/tree/master/pydat#pydat-with-elasticsearch) to provide whois, including historical whois, and passive DNS lookup information. Analysts can retrieve name, organization, country, city, street, ZIP code, telephone, and email details.

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 PyDat enricher:

- **API URL**: the URL allowing access to the local **PyDat** (<https://github.com/mitrecnd/whodat#pydat-api>) instance.
Example: *http://10.0.1.60:8000/ (example)*
- 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 table view by column. 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.

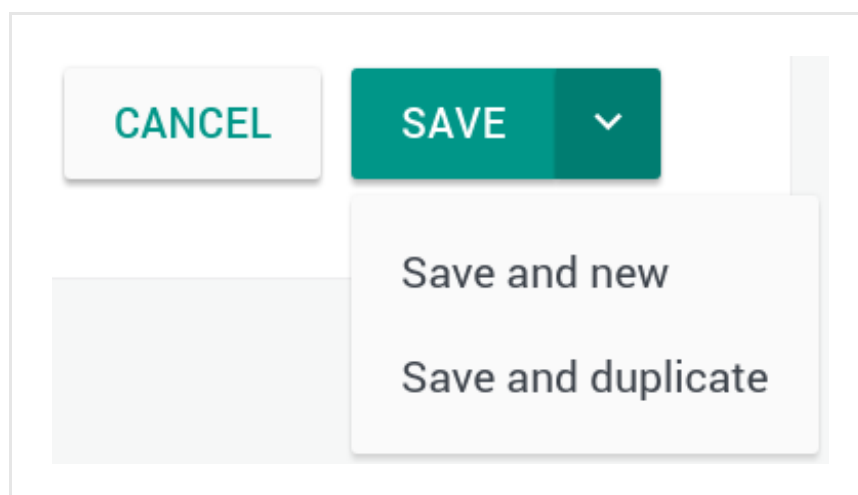
On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

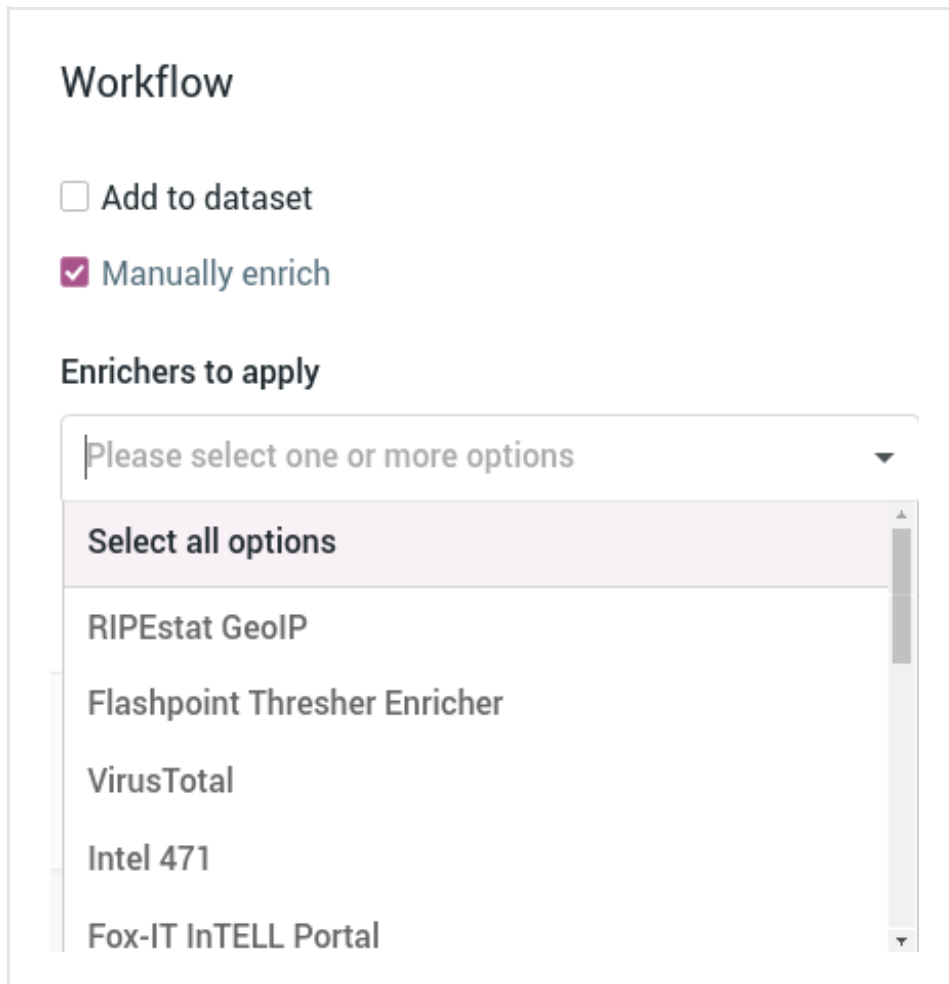
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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.

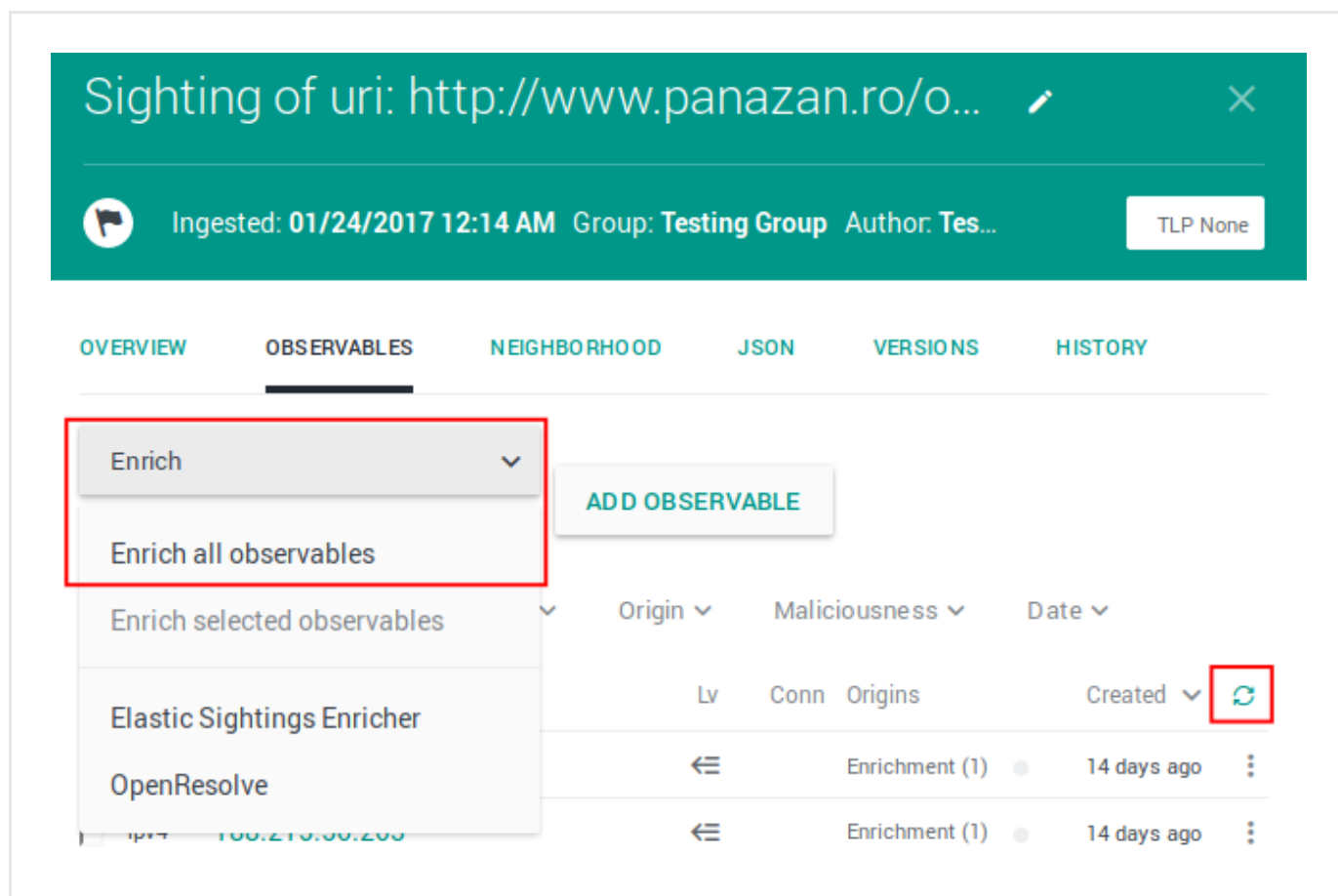
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.



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://zebbugtennis.com/wp-conte...> ×

Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	←	Enrichment (1)	7 days ago
	←	Enrichment (2)	7 days ago
<input checked="" type="checkbox"/> 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 PyDat enricher can take the following observable types as input:

- *ipv4, ipv6, domain*

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 PyDat.

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

Review enrichment observables on the graph

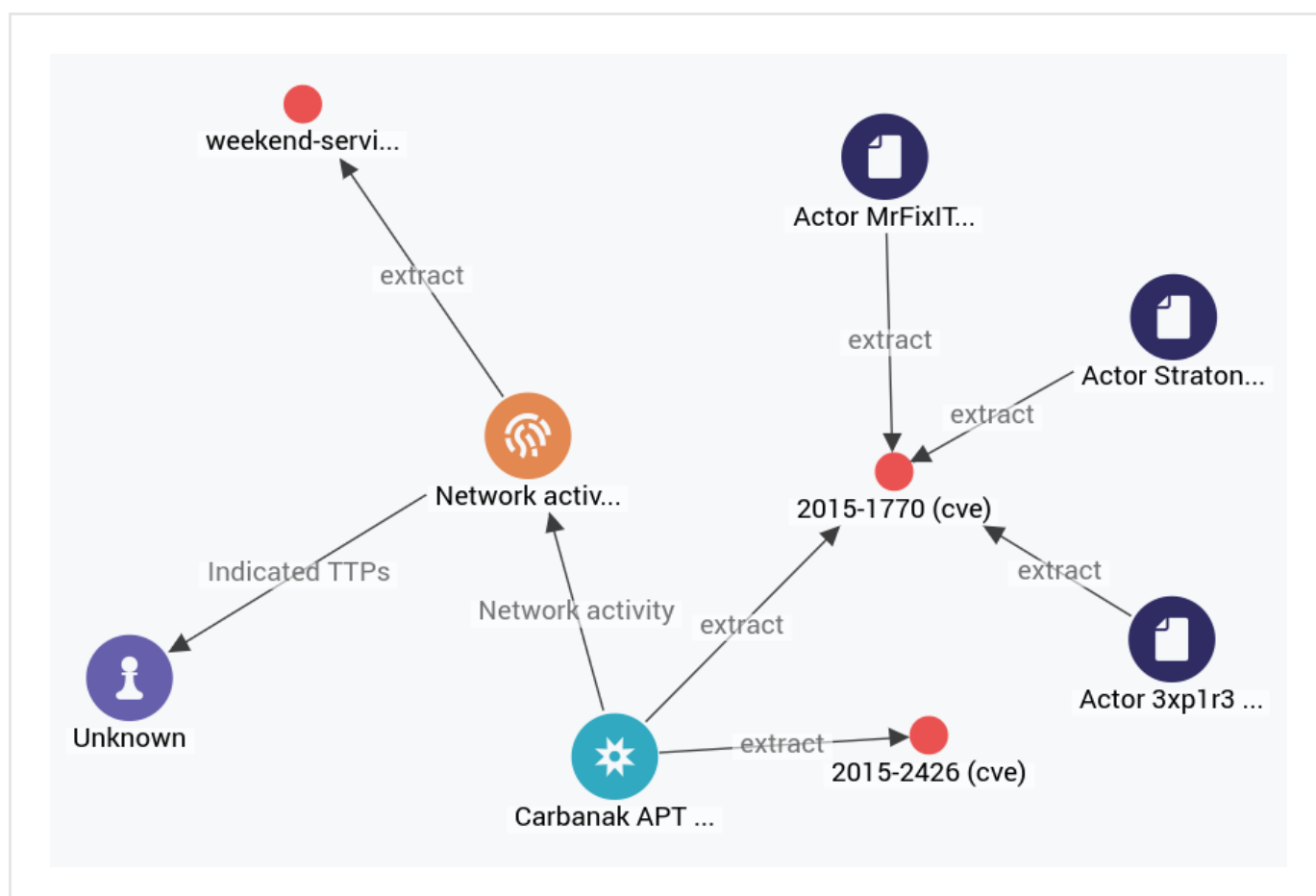
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

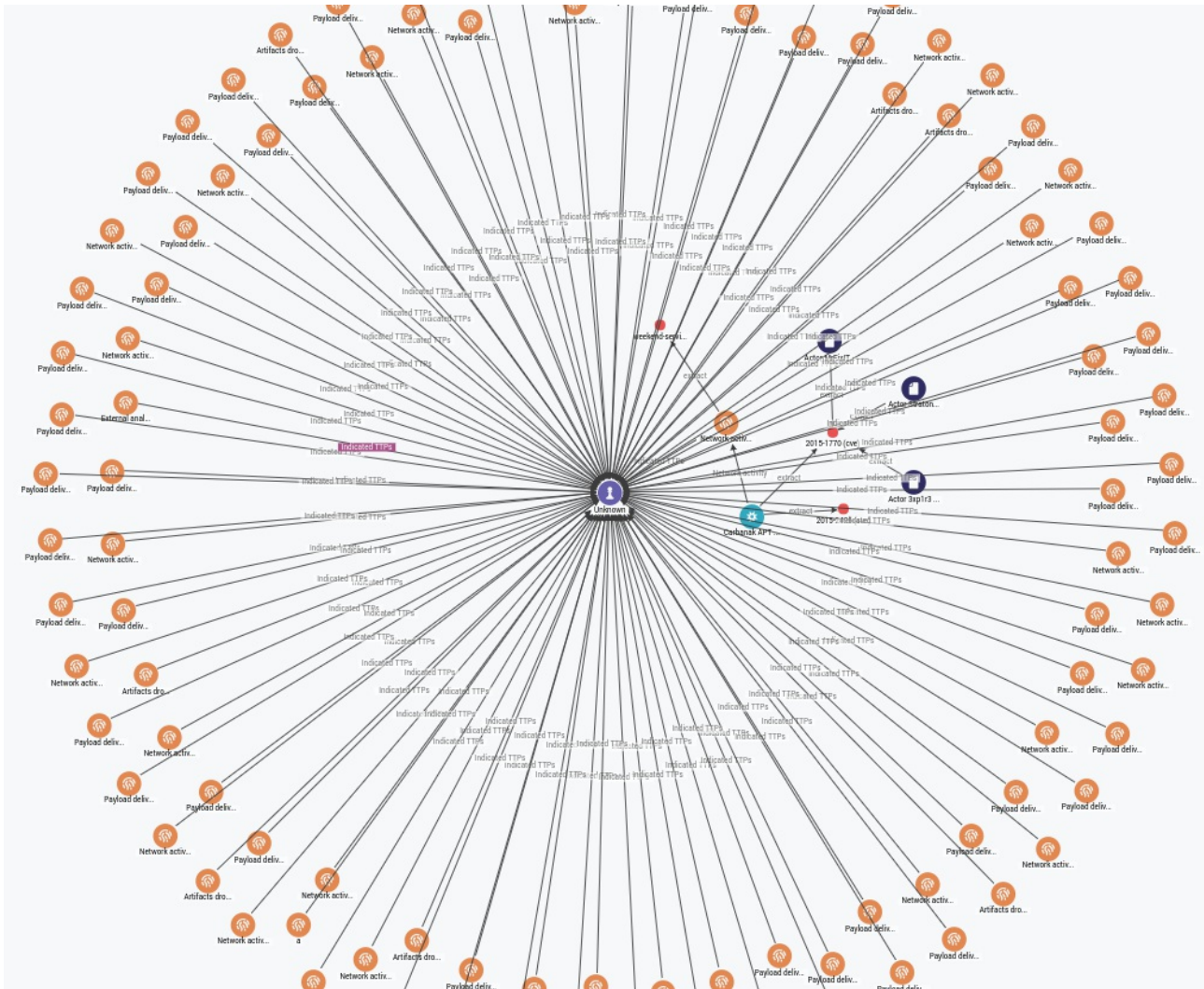
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

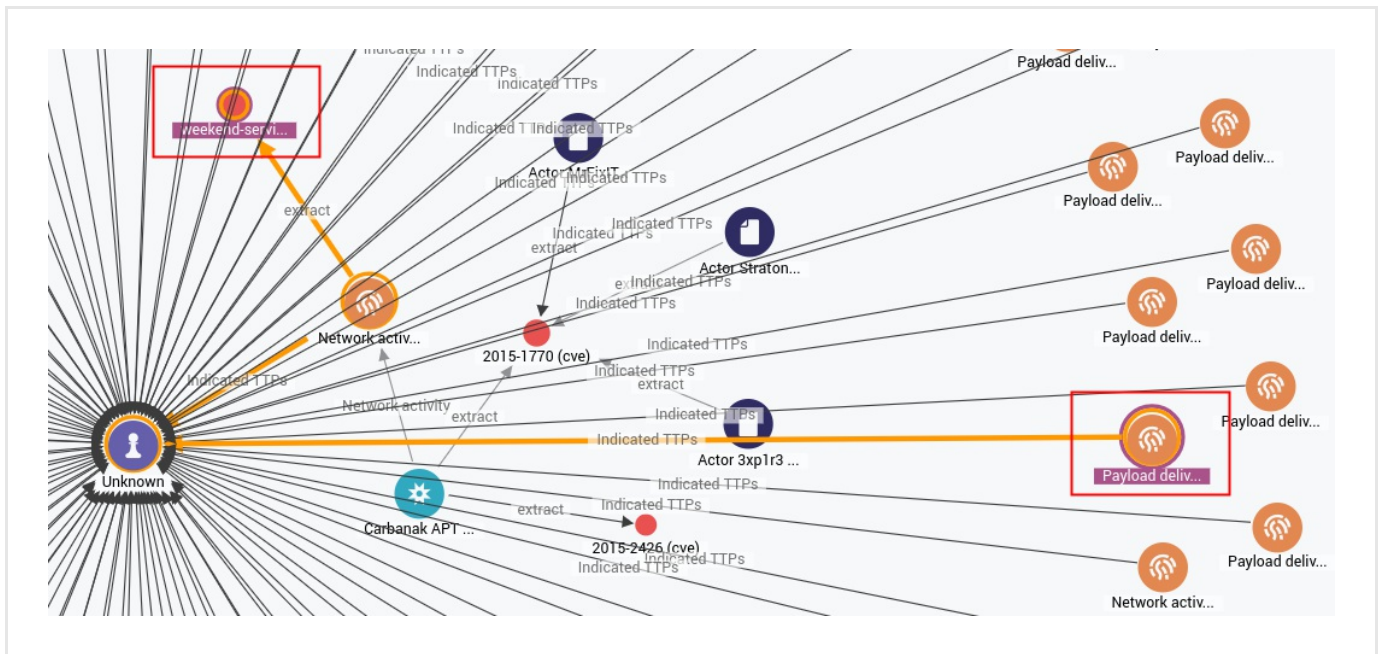


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



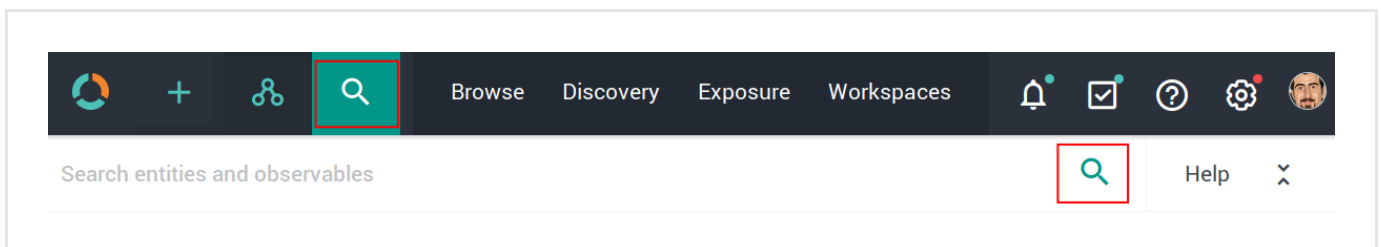
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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.

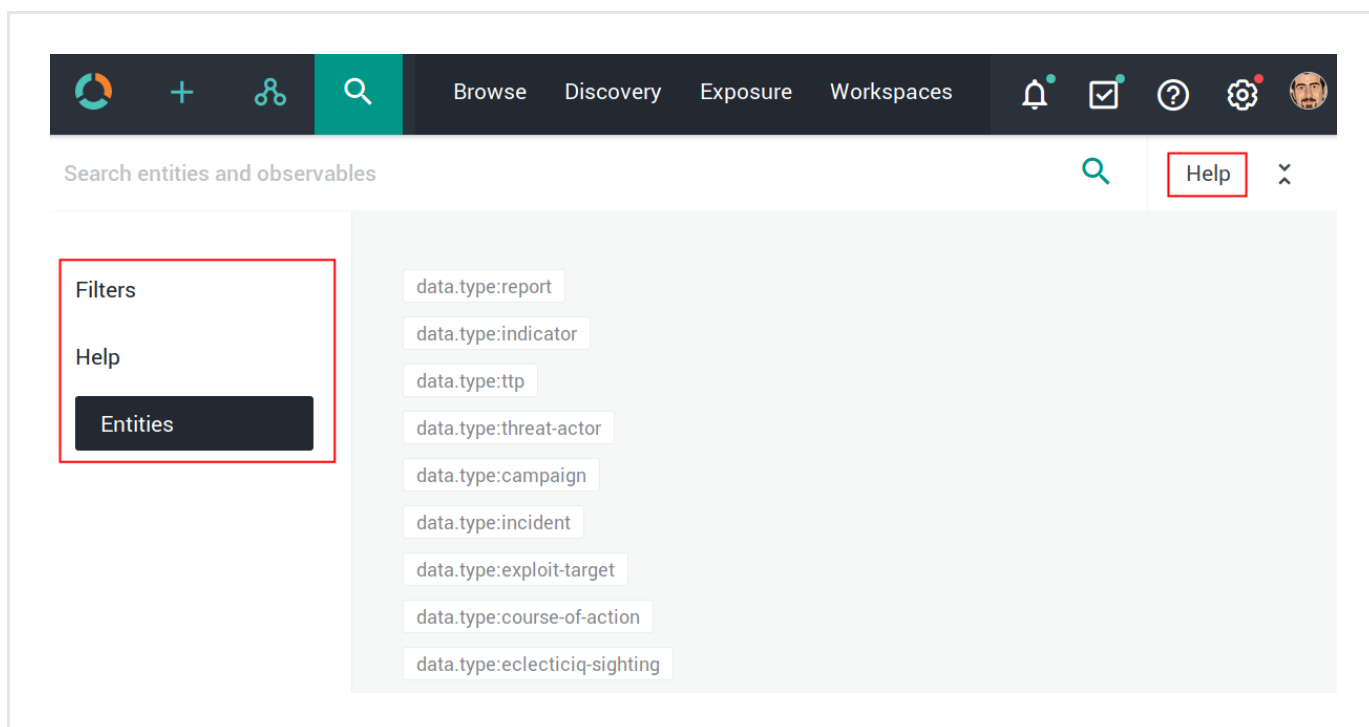


The search functionality uses **Elasticsearch query syntax**

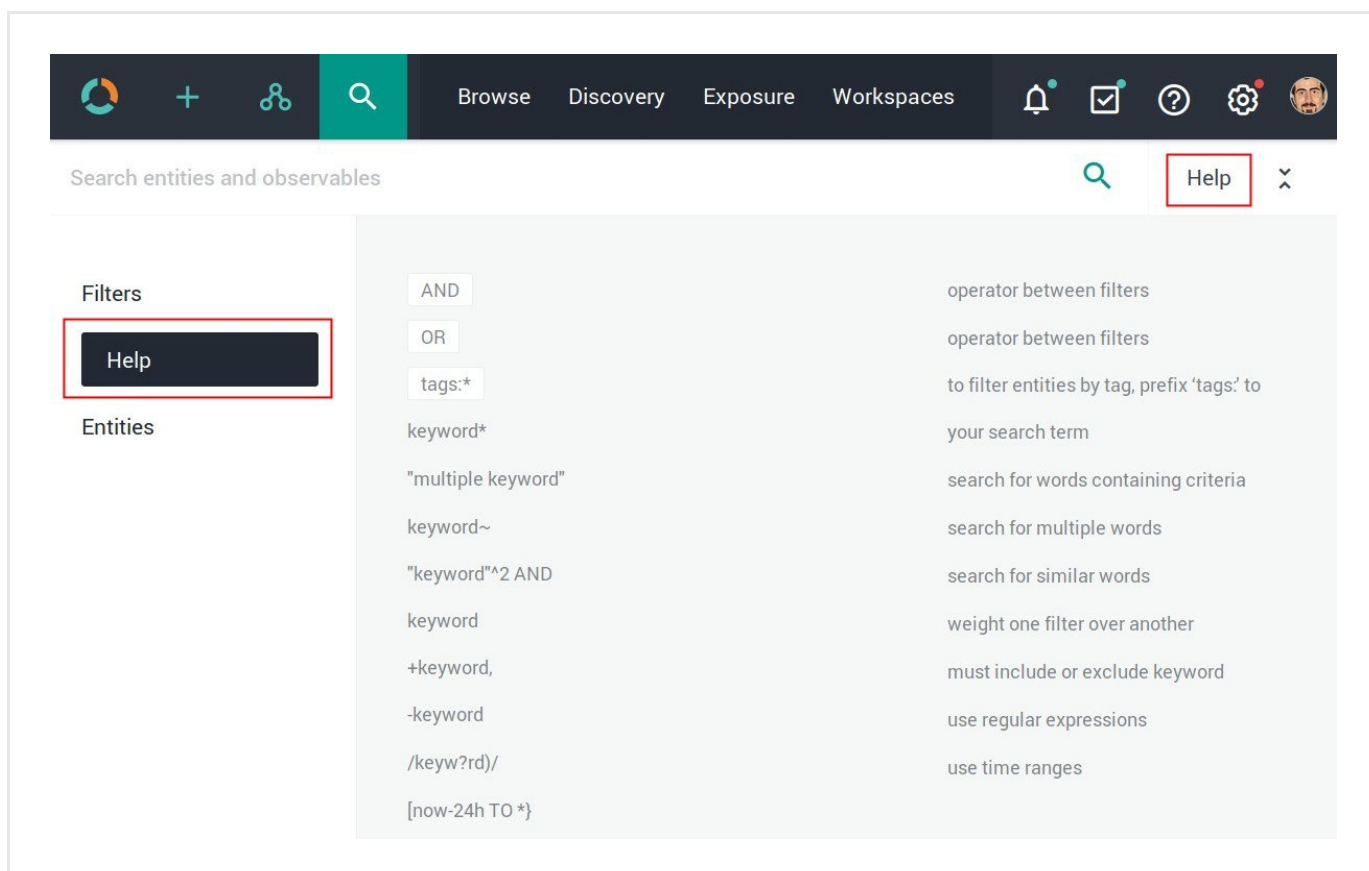
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

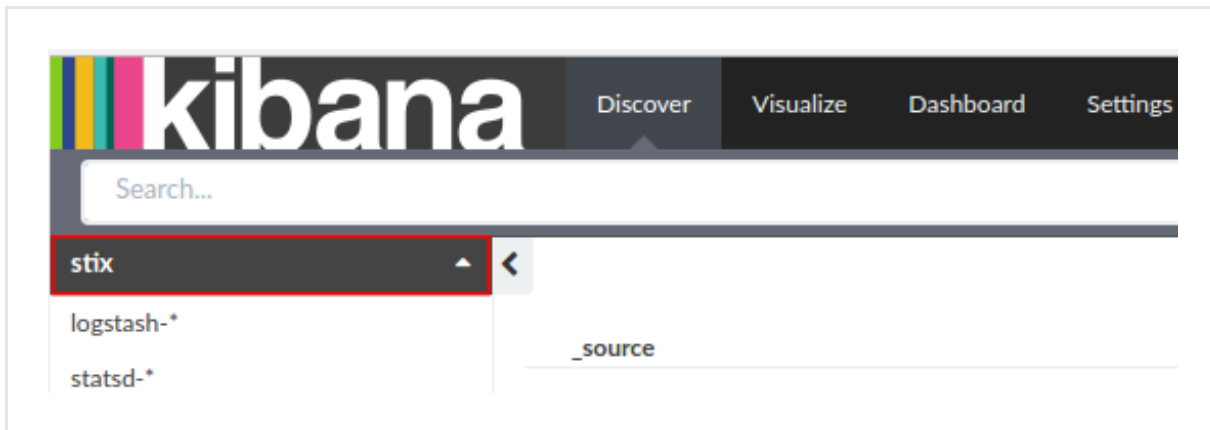
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

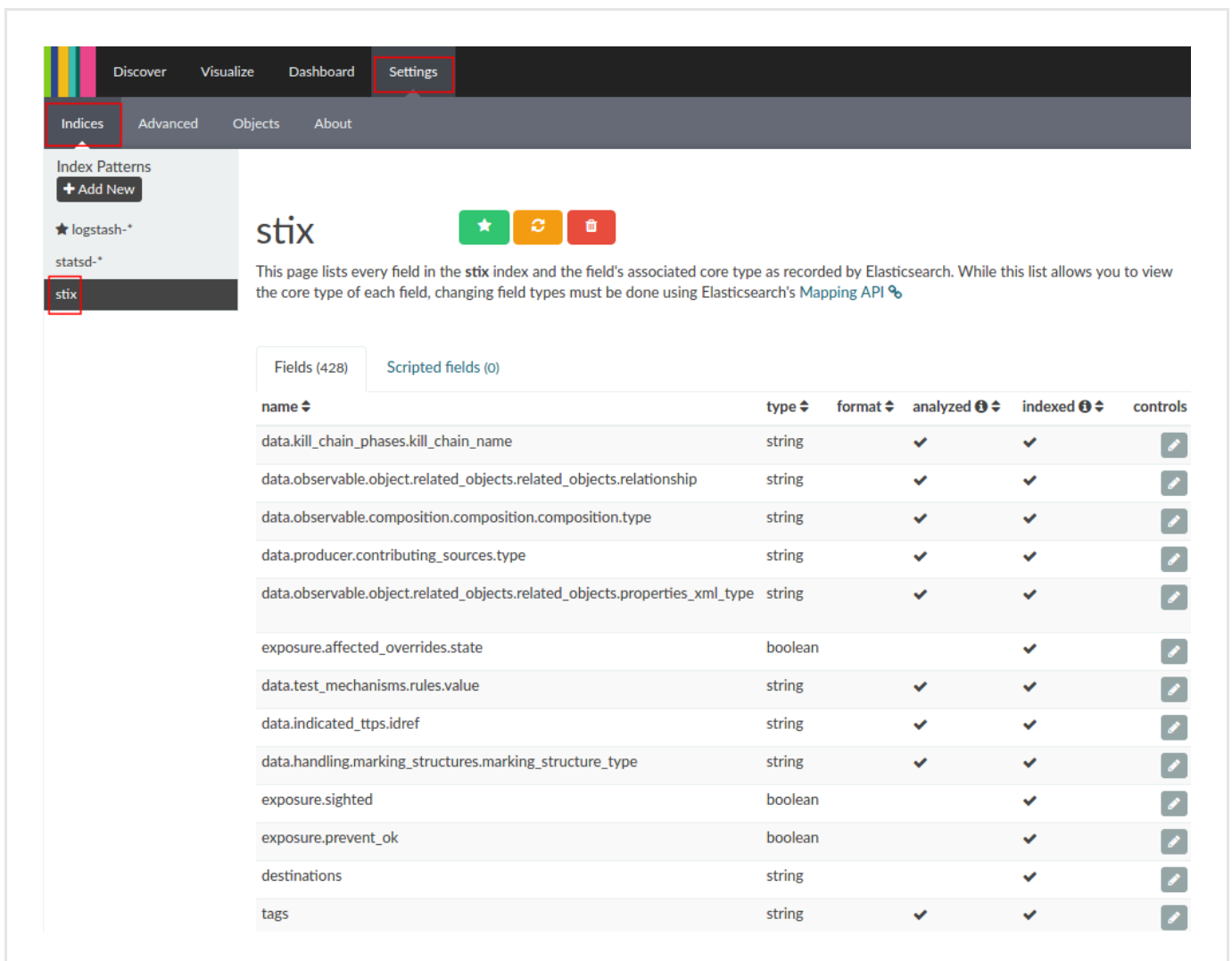
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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 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 Recorded Future enricher

This article describes how to configure the Recorded Future enricher parameters. To configure the general options for the Recorded Future enricher, see [Configure enrichers](#).


Recorded Future enricher	
Enricher name	Recorded Future
API endpoint	<code>https://app.recordedfuture.com/live/sc/entity/{}</code>
Input	domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, ipv4, ipv6
Output	Enriches observables with pattern matching search results produced by the Recorded Future Temporal Analytics Engine.
Description	The enricher returns additional data, such as IPs, domains, email addresses, and hashes related to the submitted observables in the specified types, as well as maliciousness confidence levels based on the retrieved risk scores.

Configure the Recorded Future 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*
- *hash-md5*
- *hash-sha1*
- *hash-sha256*
- *hash-sha256*
- *ipv4*
- *ipv6*

Under **Parameters**, define the specific configuration options for the Recorded Future 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.
- Click **Save** to store your changes, or **Cancel** to discard them.

Maliciousness confidence rating is based on the Recorded Future risk scoring, where *0* means *no current evidence of risk*, whereas *99* means *very malicious*:

- If the returned Recorded Future risk score is equal to or higher than 65, enriched observables are flagged with **Malicious - High confidence**.
- If the returned Recorded Future risk score is lower than 65, enriched observables are flagged with **Malicious - Medium confidence**.


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 table view by column. 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.

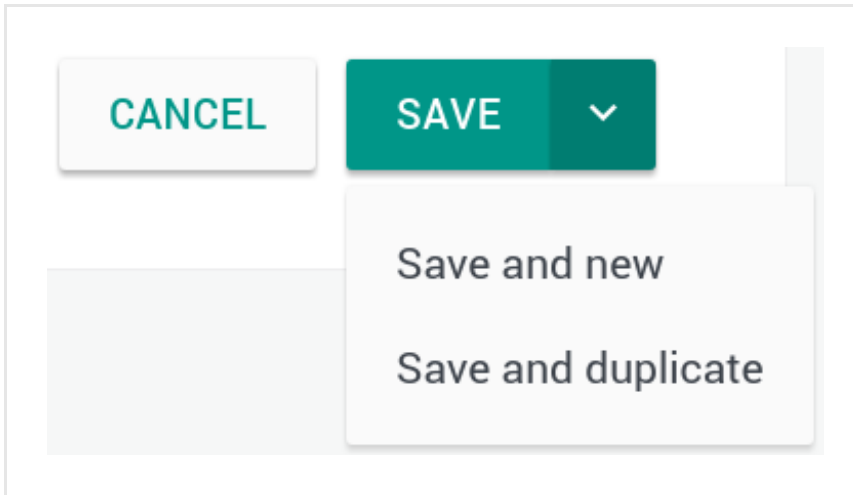
On the **Rules** > **Enrichment** > **Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 GeolP 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 table view by column. 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 dotted menu 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 dotted menu 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

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 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

OVERVIEWOBSERVABLESNEIGHBORHOODJSONVERSIONSHISTORY

Enrich




ADD OBSERVABLE



Enrich all observables




Enrich selected observables




Elastic Sightings Enricher

OpenResolve

OriginMaliciousnessDate

LvConnOriginsCreated

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://zebbugtennis.com/wp-conte...> ×

Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	←	Enrichment (1)	7 days ago
	←	Enrichment (2)	7 days ago
<input checked="" type="checkbox"/> 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 Recorded Future enricher can take the following observable types as input:

- *domain, hash-md5, hash-sha1, hash-sha256, hash-sha256, 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 Recorded Future.

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

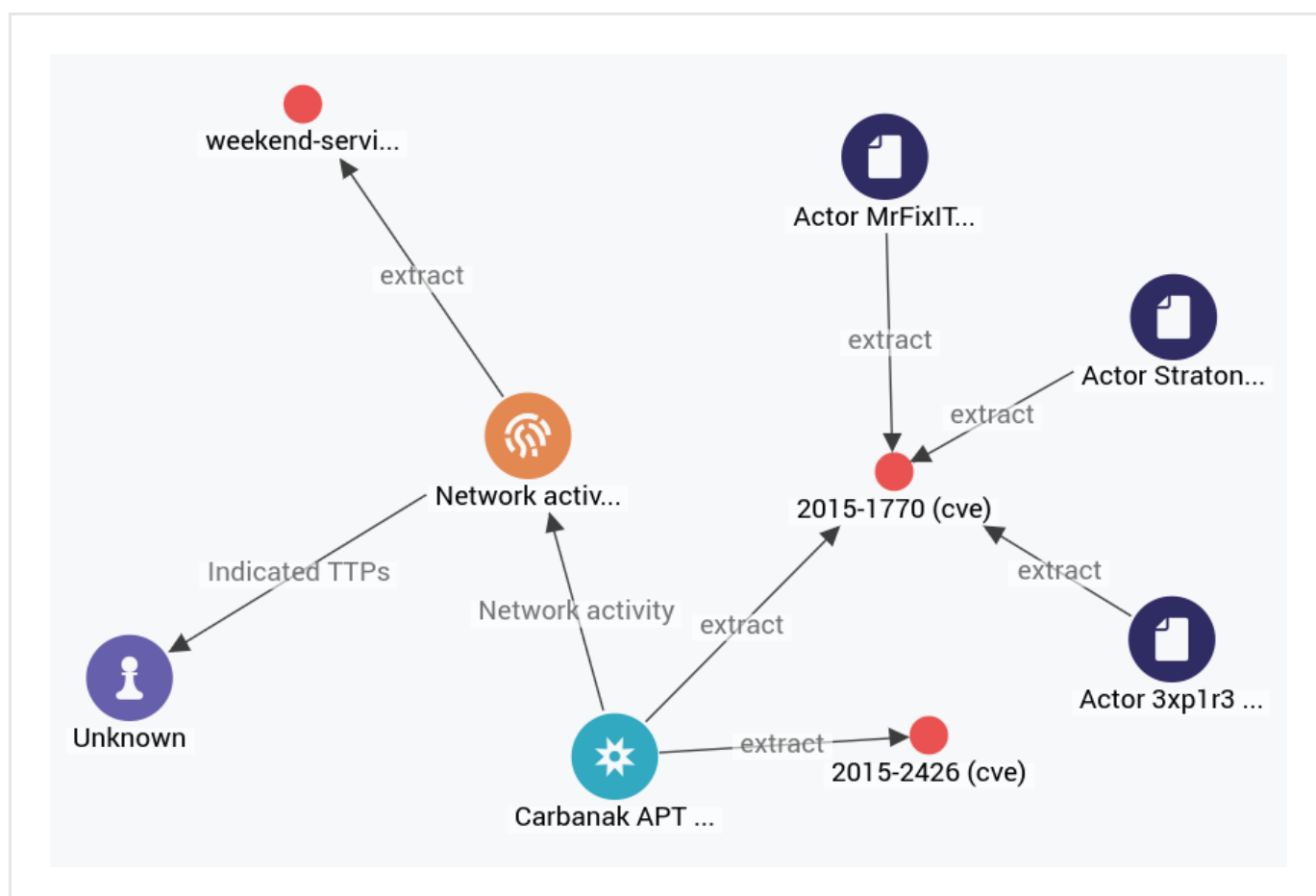
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

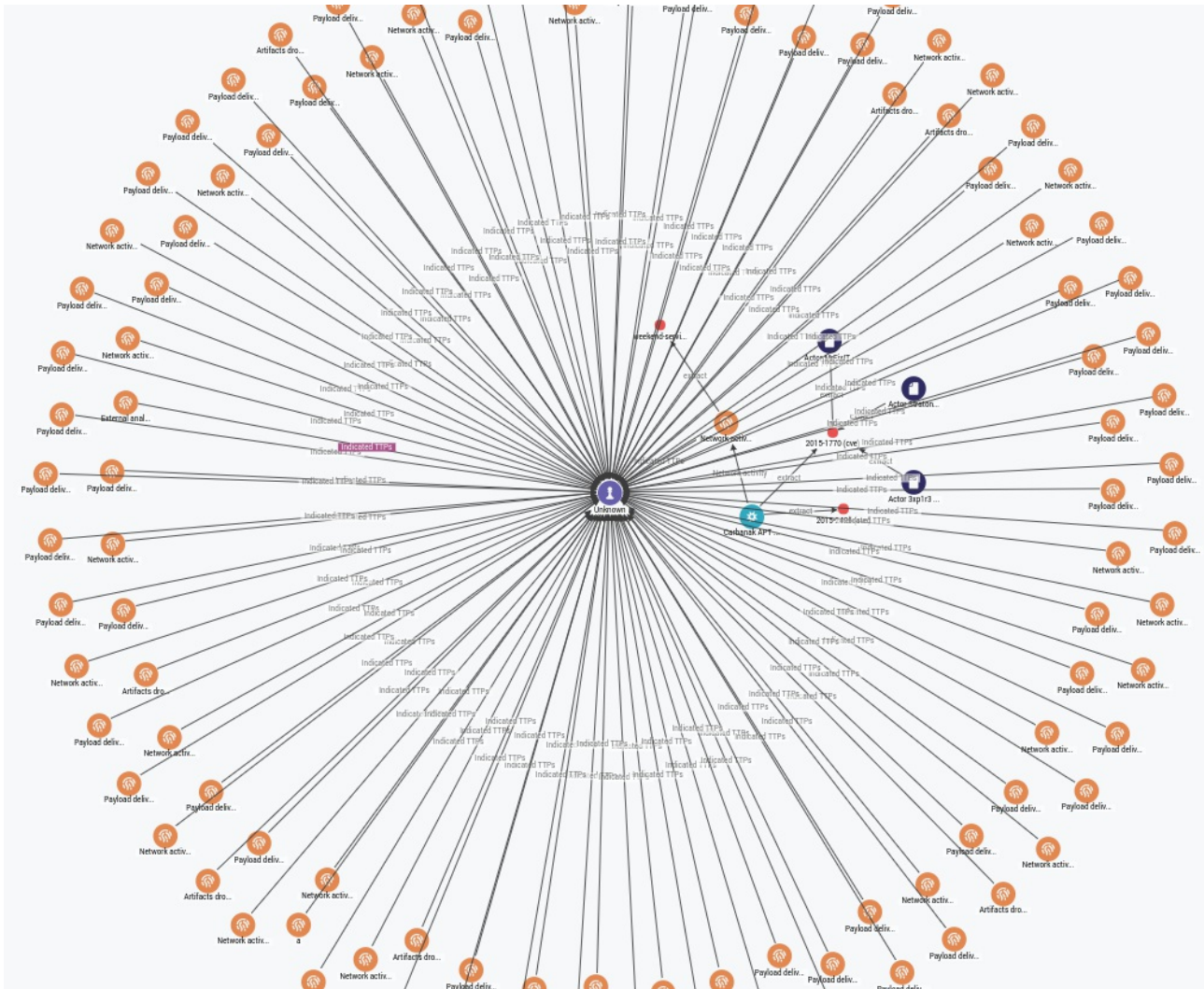
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

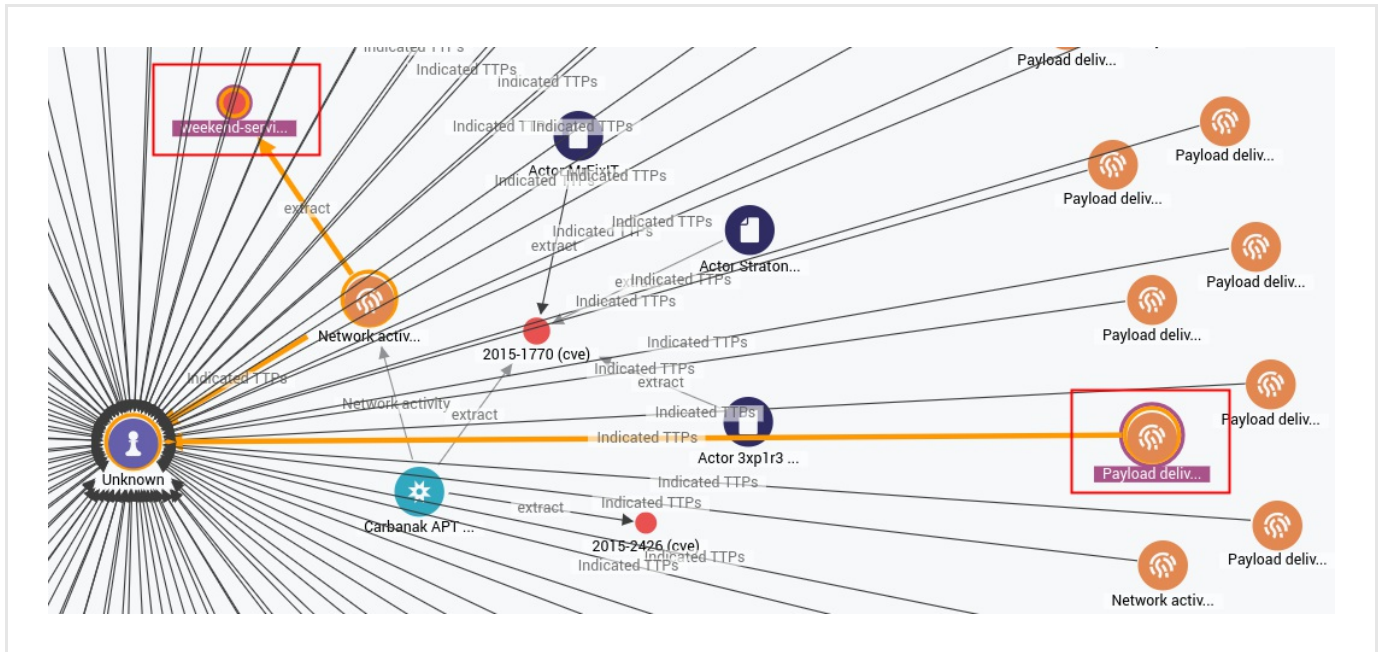


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



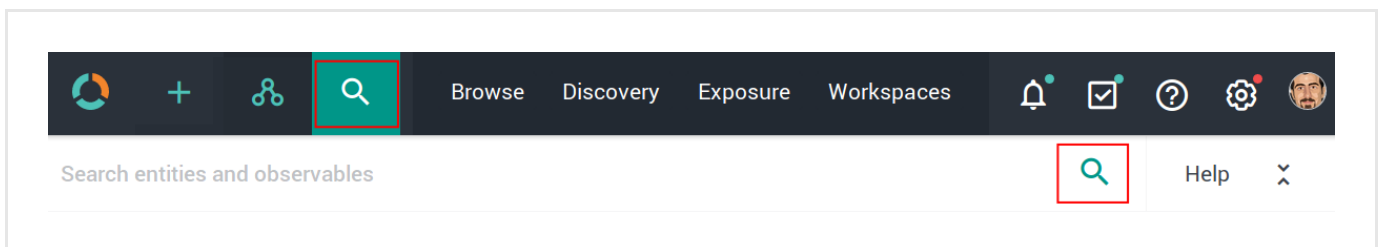
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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.

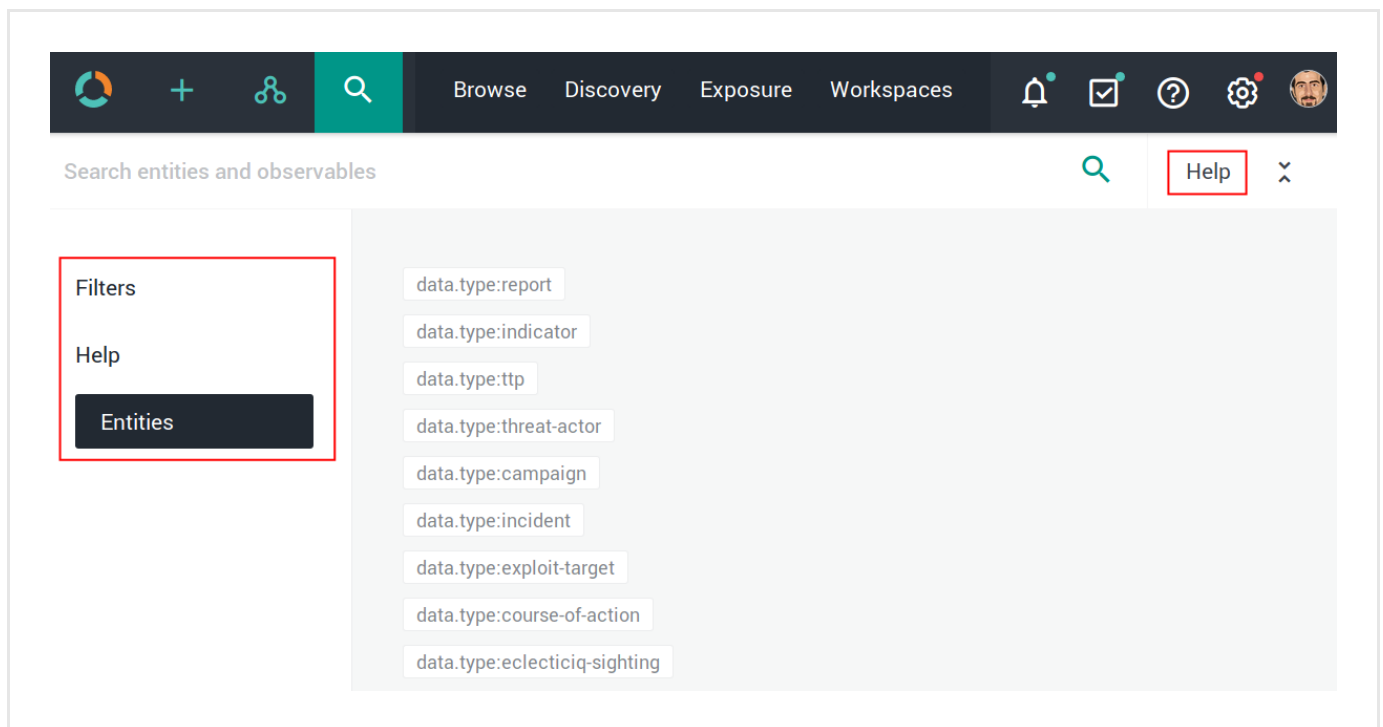


The search functionality uses **Elasticsearch query syntax**

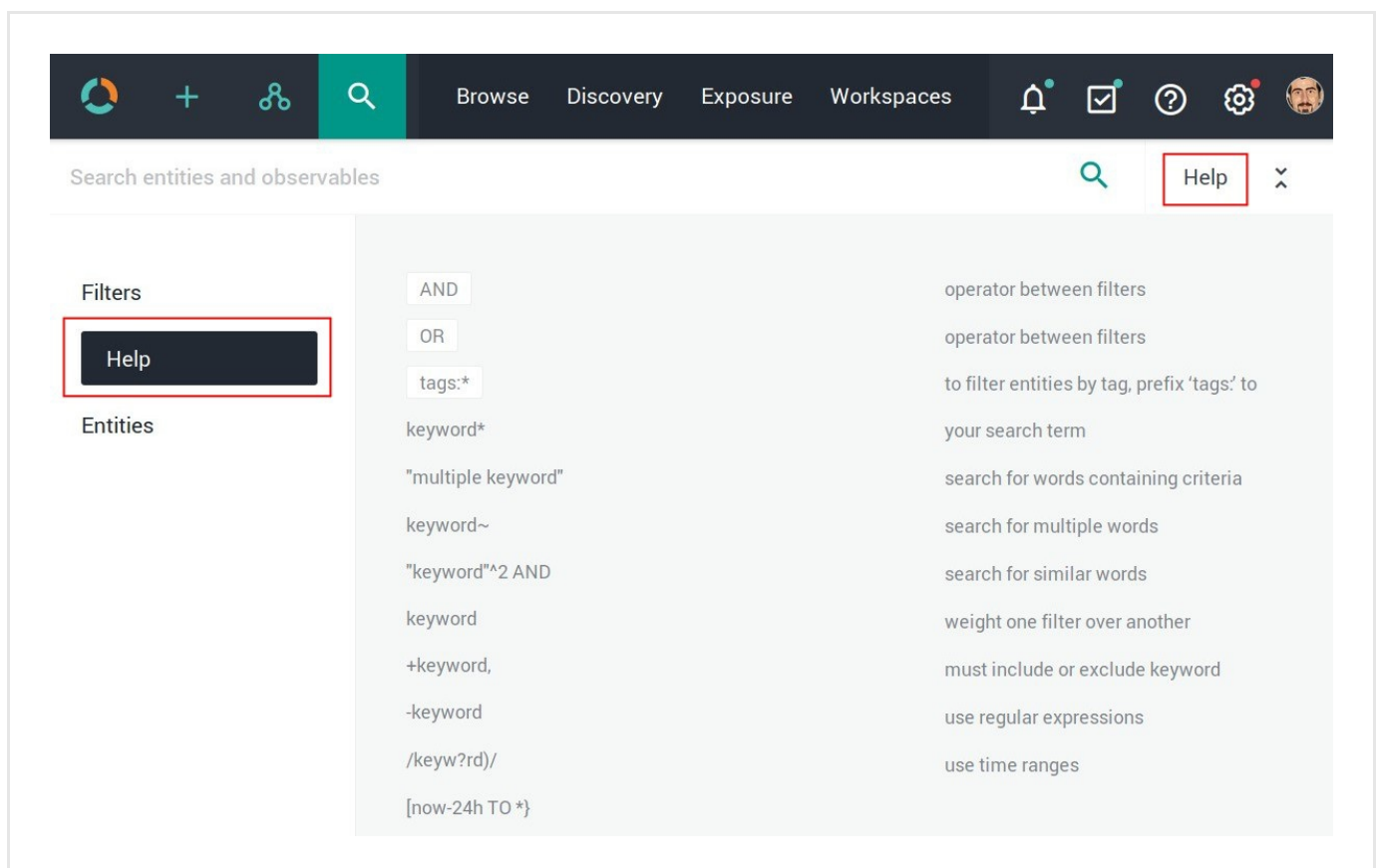
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

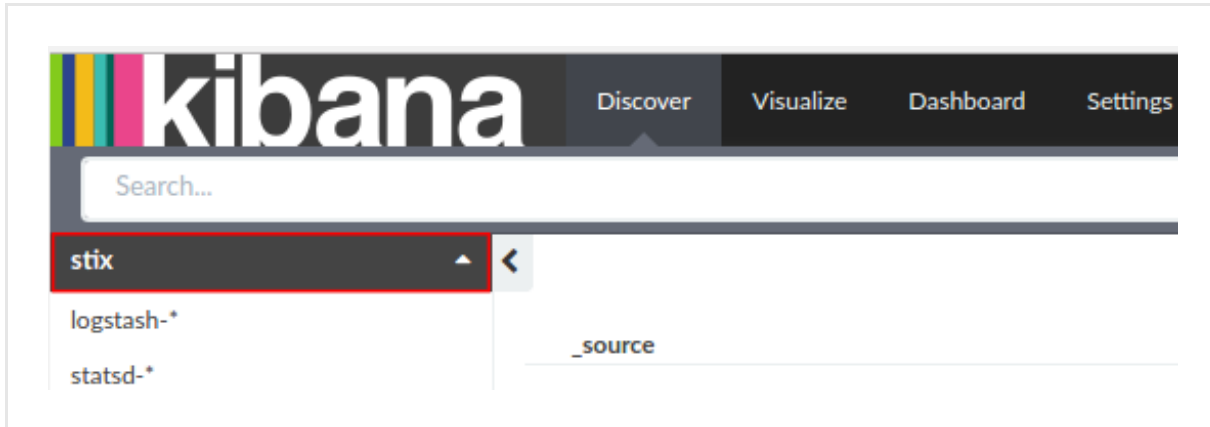
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

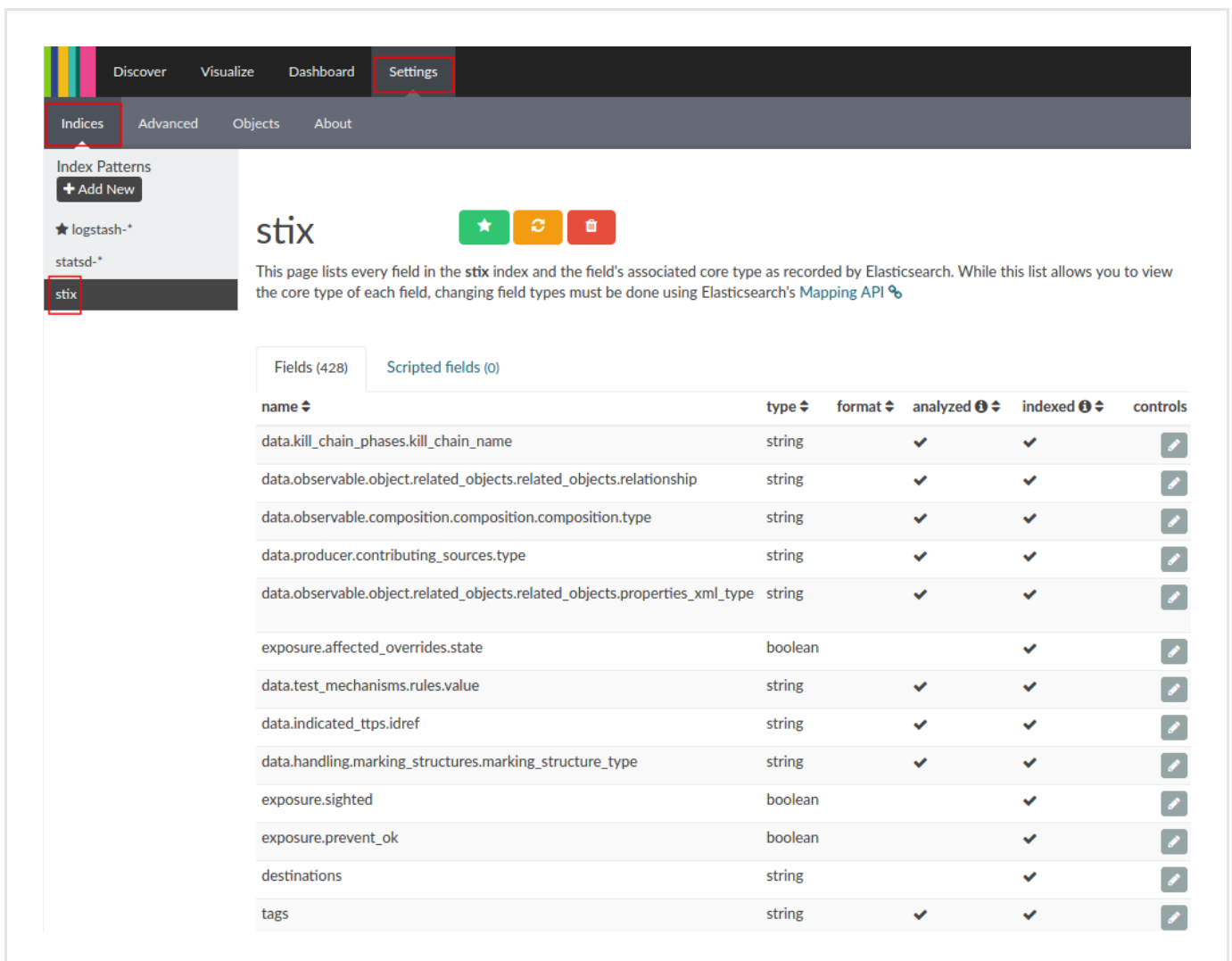
Keep the trailing /.

Example: [https://platform.host.com/api/kibana/app/kibana#/.](https://platform.host.com/api/kibana/app/kibana#/)

- Select the **stix** index field:



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



Last generated on May 26, 2017

How to work with the RIPEstat GeolIP 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 GeolIP 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 RIPEstat GeolIP enricher

This article describes how to configure the RIPEstat GeolIP enricher parameters. To configure the general options for the RIPEstat GeolIP enricher, see [Configure enrichers](#).


RIPEstat GeolIP enricher	
Enricher name	RIPEstat GeolIP
API endpoint	<code>https://stat.ripe.net/data/geoloc/data.json?resource={IP_address}</code> (Geoloc (<code>https://stat.ripe.net/docs/data_api#geoloc</code>))
Input	ipv4, ipv6
Output	Enriches observables with geolocation information related to IP addresses: coordinates, country, and city.
Description	Geolocation IP information from the RIPEstat web-based interface (Data API (<code>https://stat.ripe.net/docs/data_api</code>)), including latitude, longitude, country, and city.

Configure the RIPEstat GeolIP 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 RIPEstat GeoIP enricher:

- **API URL**: the basic URL allowing access to the **RIPEstat Data API**
(https://stat.ripe.net/docs/data_api).
The value is: *<https://stat.ripe.net/data>*.
- 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 table view by column. 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:

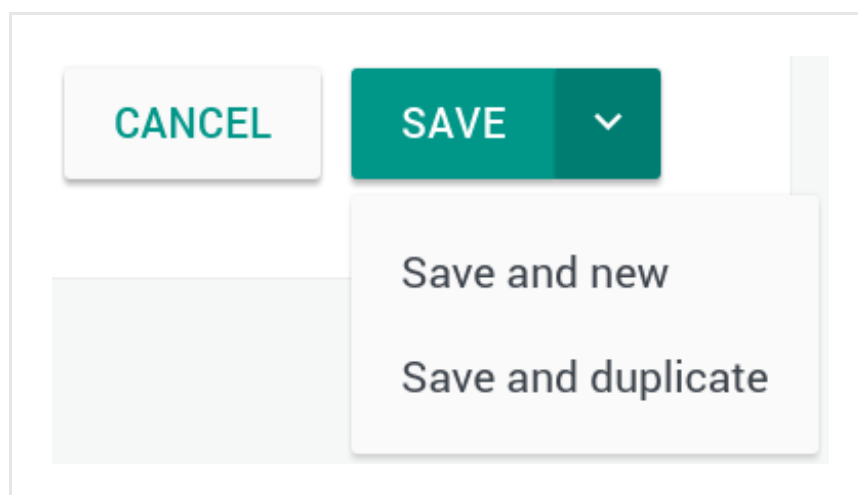
- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

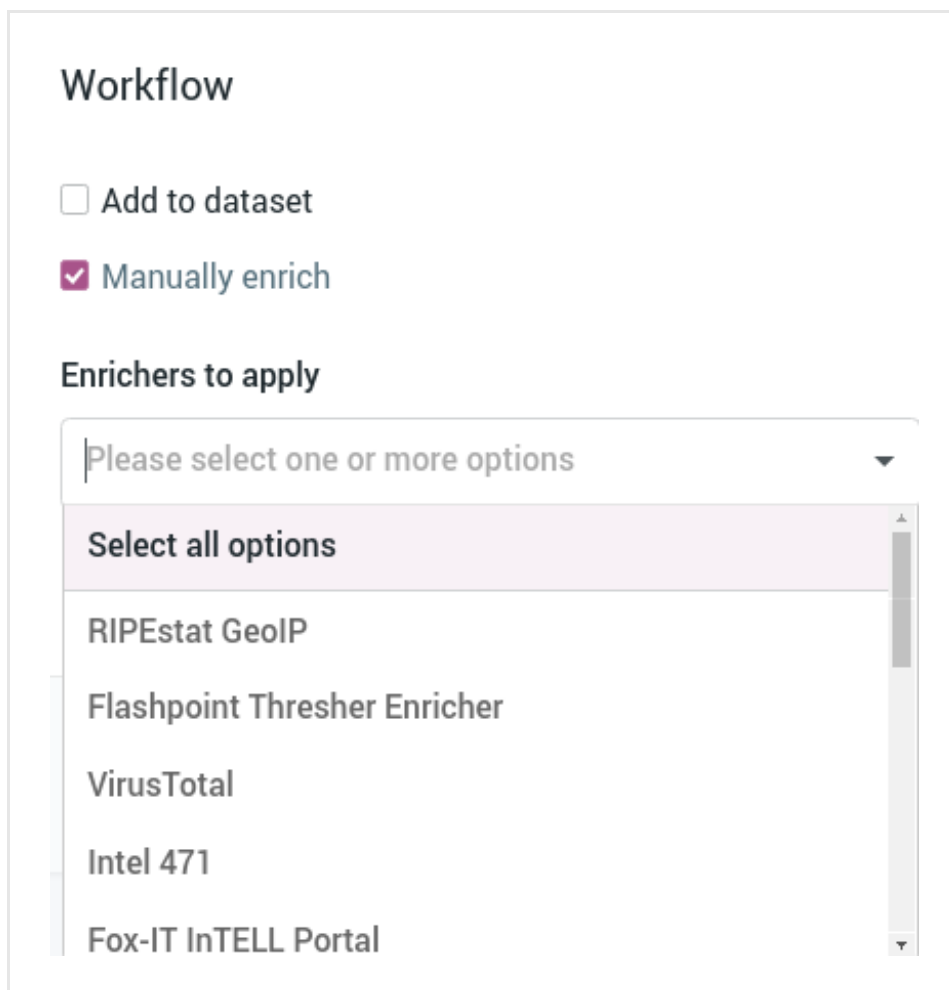
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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...' interface. At the top, there is a teal header bar with the title, a flag icon, and metadata: 'Ingested: 01/24/2017 12:14 AM', 'Group: Testing Group', 'Author: Tes...', and 'TLP None'. Below the header, there are tabs: OVERVIEW, OBSERVABLES, NEIGHBORHOOD, JSON, VERSIONS, and HISTORY. The OBSERVABLES tab is selected. On the left, there is a dropdown menu labeled 'Enrich' with a red box around it. The dropdown menu is open, showing options: 'Enrich all observables' (highlighted with a red box), 'Enrich selected observables', 'Elastic Sightings Enricher', and 'OpenResolve'. 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, both showing 'Enrichment (1)' and '14 days ago'. A red box highlights a refresh icon (a circular arrow) next to the 'Created' column header.

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://zebbugtennis.com/wp-conte...> ×

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

○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	⌵	Enrichment (1)	7 days ago ⋮
	⌵	Enrichment (2)	7 days ago ⋮
<input checked="" type="checkbox"/> 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 RIPEstat GeoIP enricher can take the following observable types as input:

- *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 RIPEstat GeoIP.

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

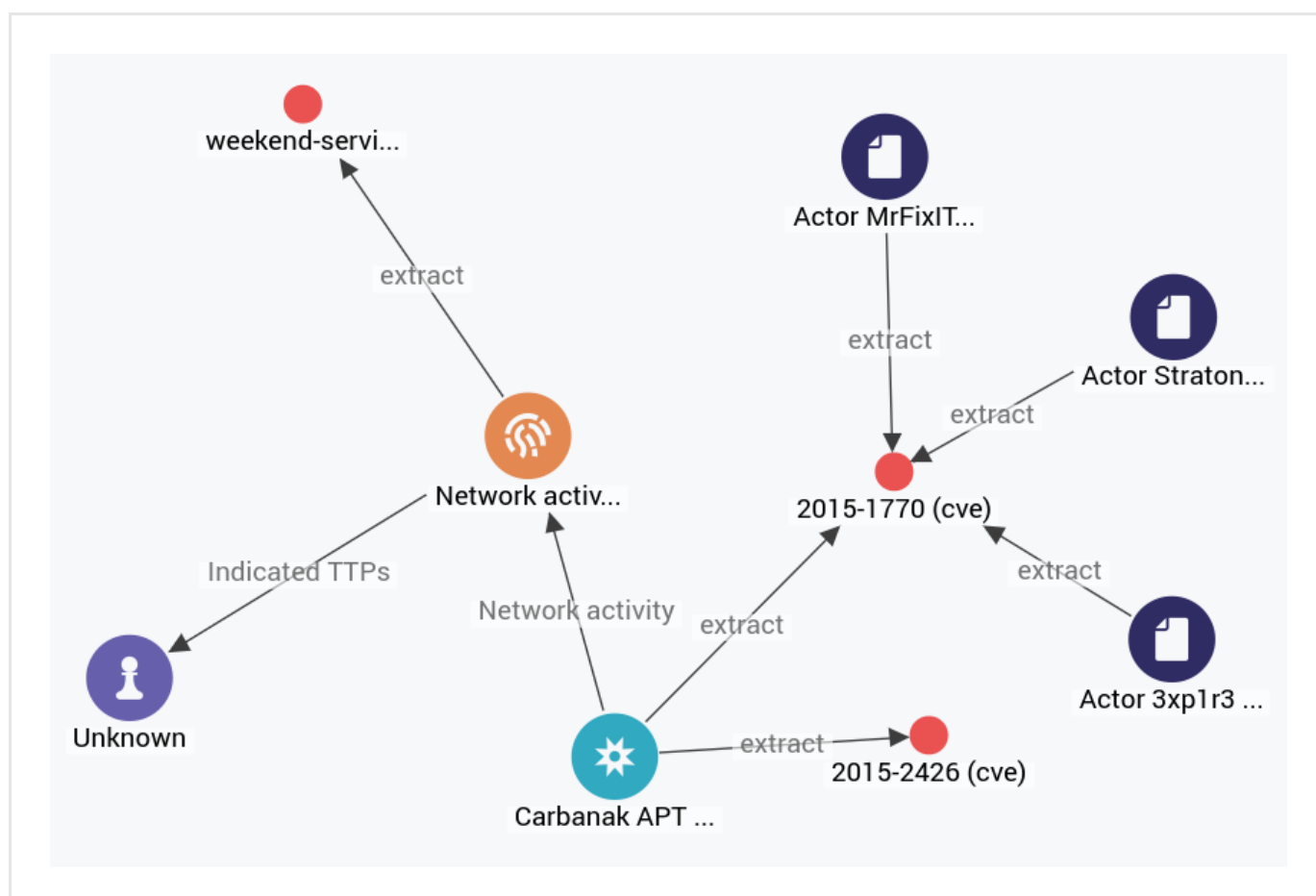
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

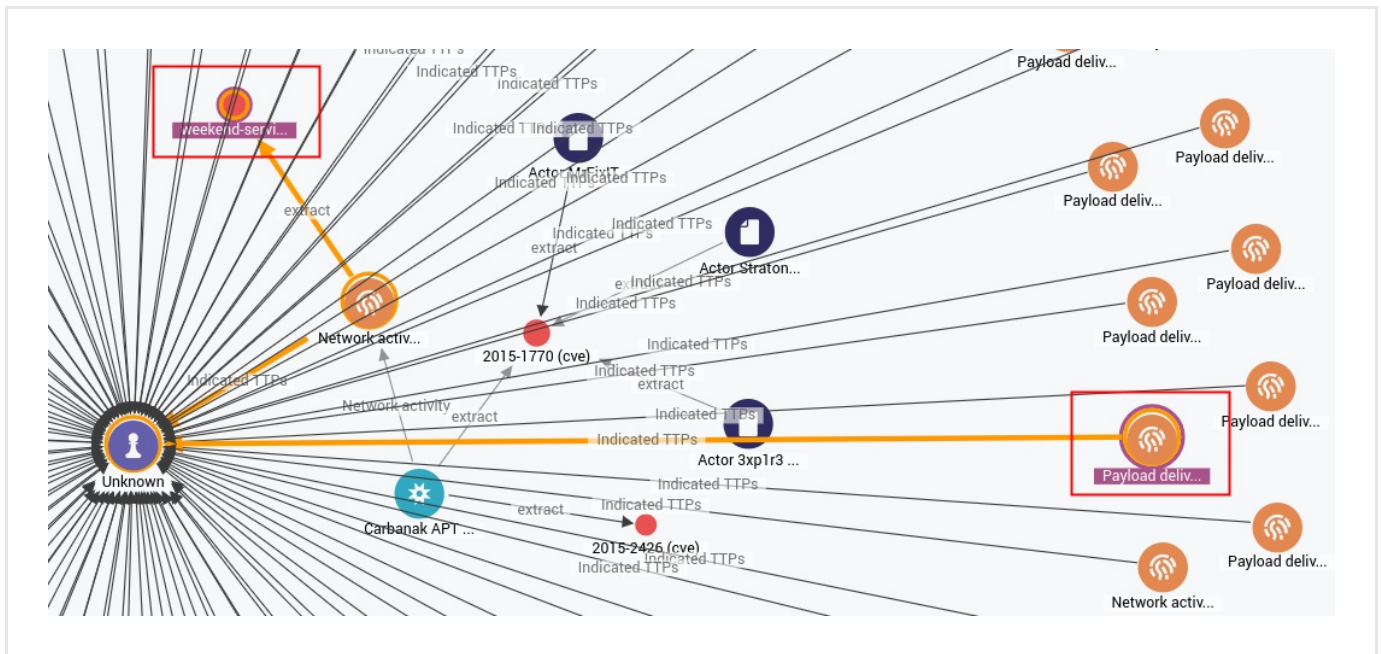
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	⋮
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdp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

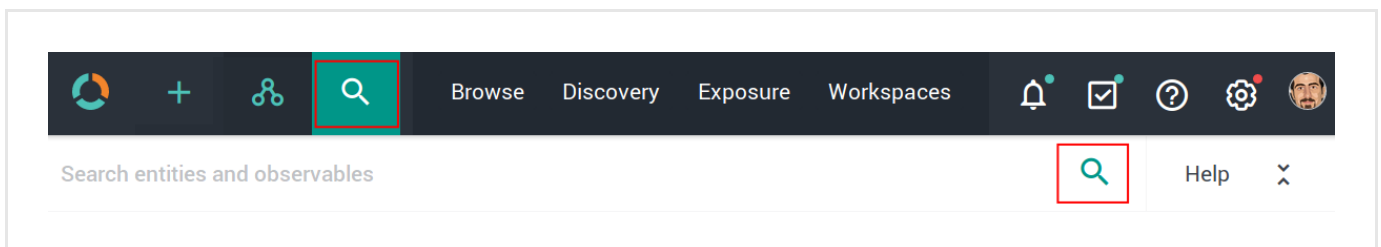


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



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.

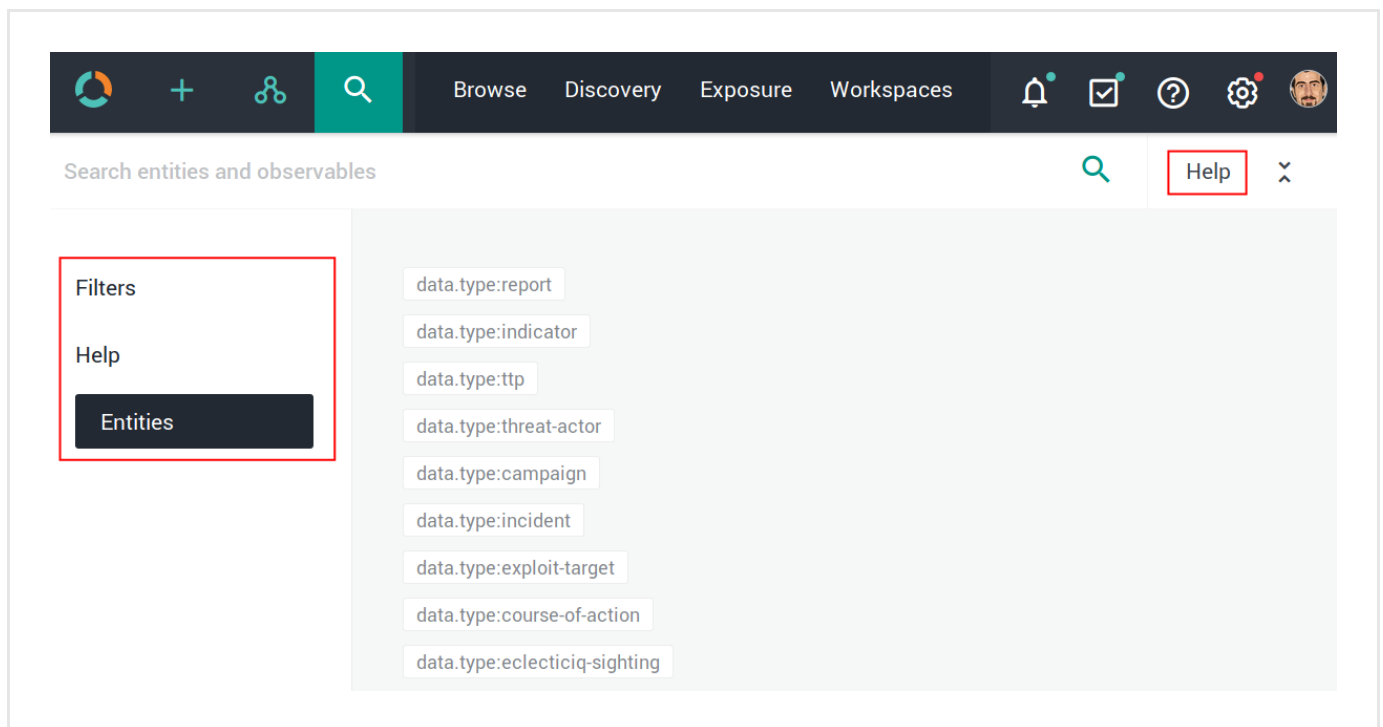


The search functionality uses **Elasticsearch query syntax**

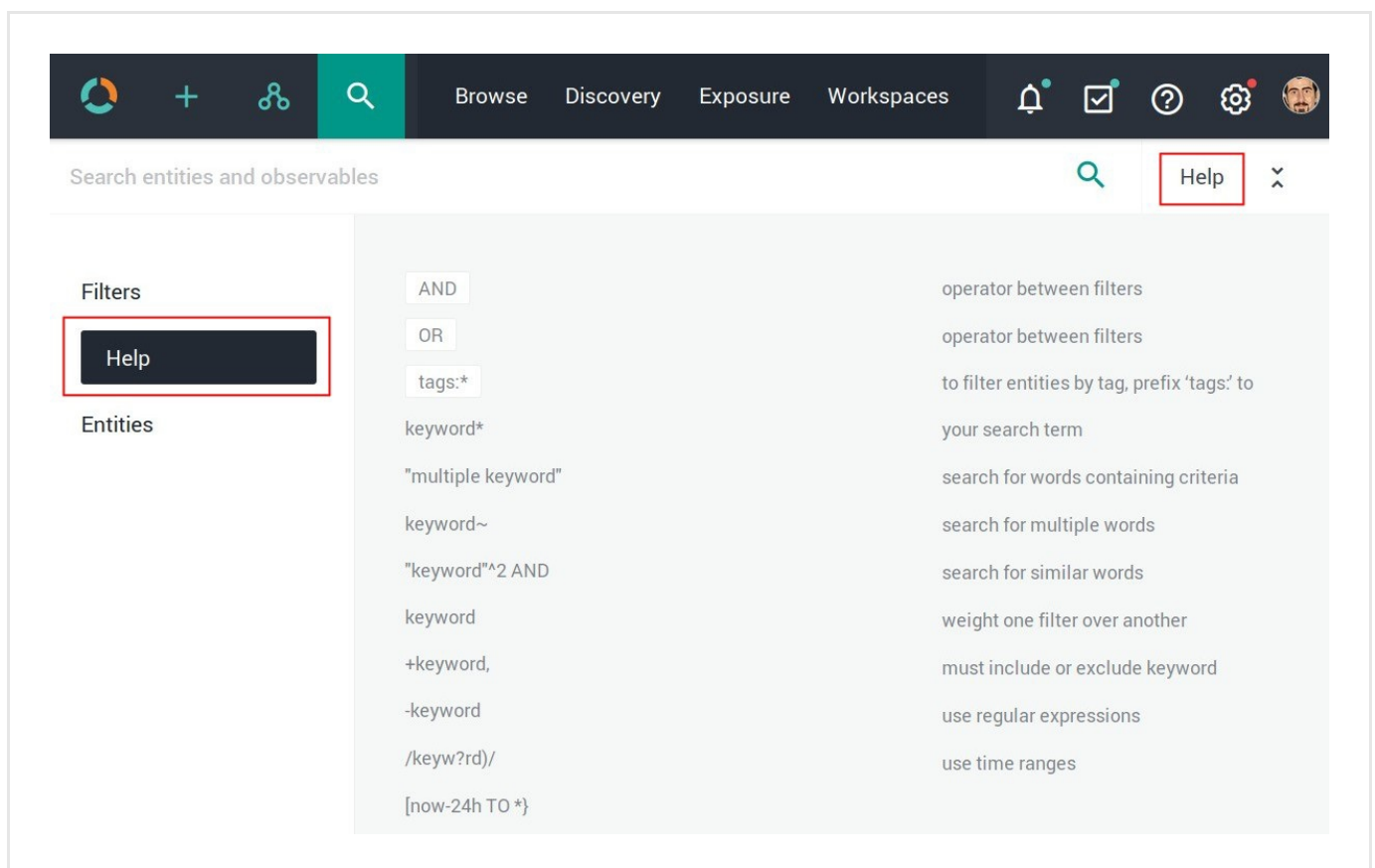
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

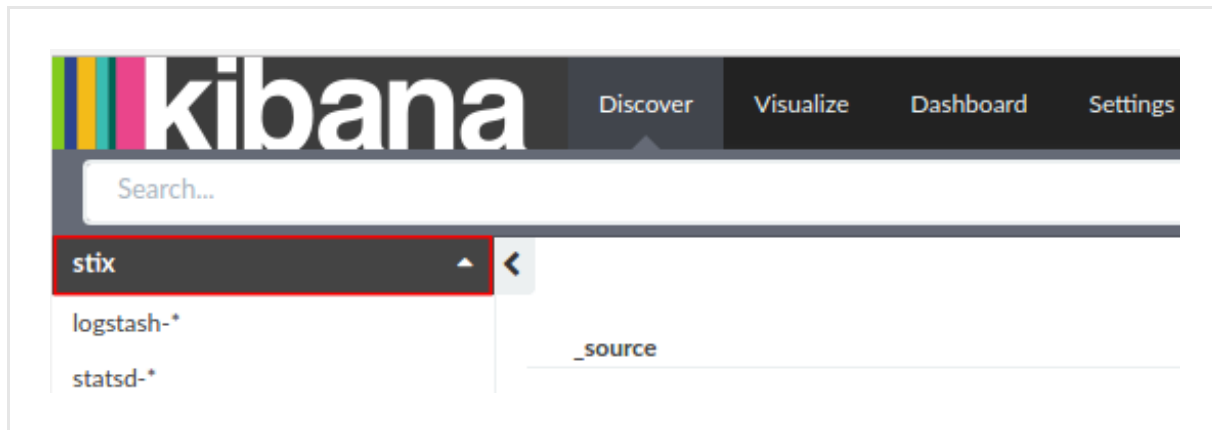
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

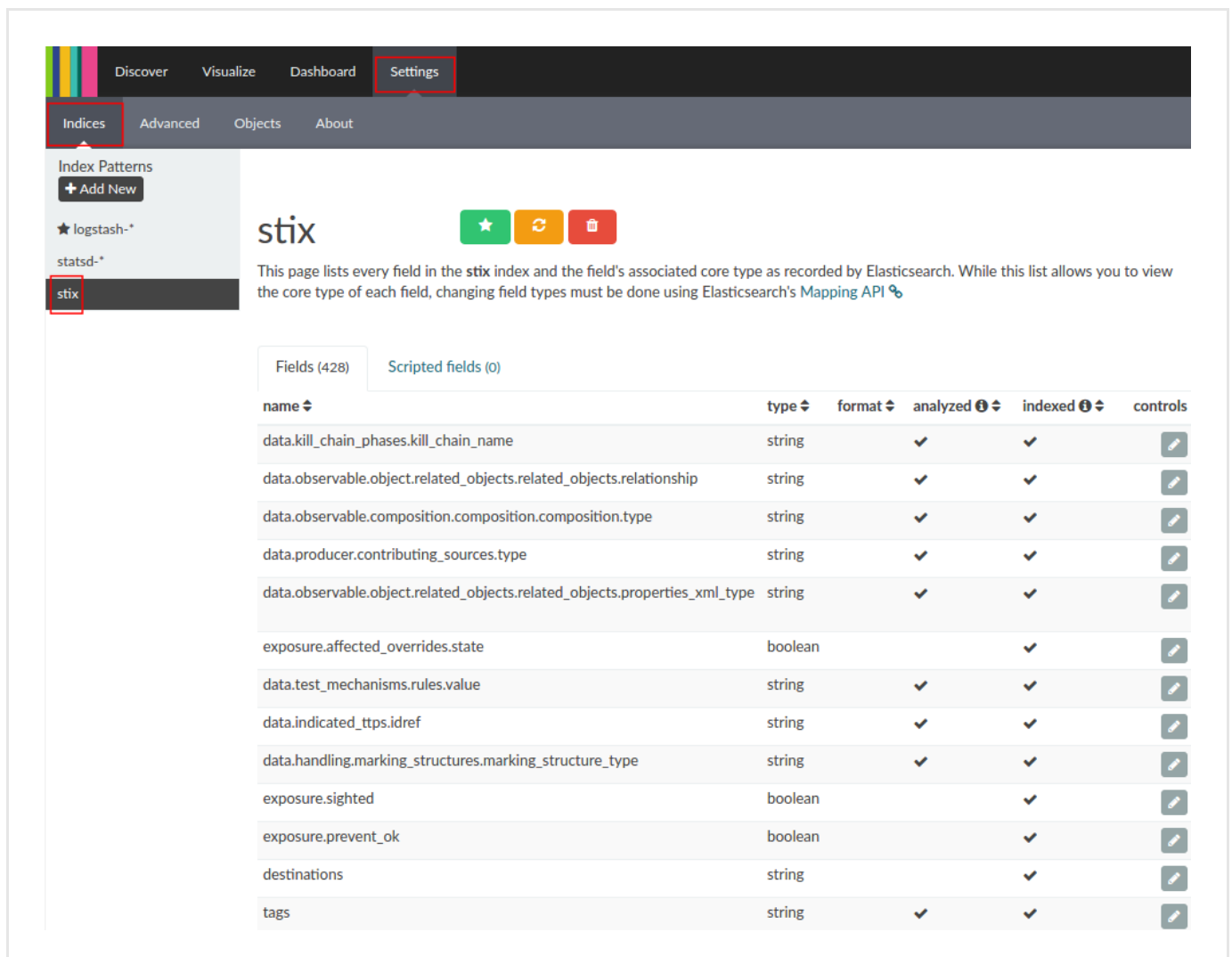
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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 RIPEstat Whois enricher

This article describes how to configure the RIPEstat Whois enricher parameters.

To configure the general options for the RIPEstat Whois enricher, see [Configure enrichers](#).


RIPEstat Whois enricher	
Enricher name	RIPEstat Whois
API endpoint	<code>https://stat.ripe.net/data/whois/data.json?resource={IP_address}</code> (Whois (<code>https://stat.ripe.net/docs/data_api#whois</code>))
Input	ipv4, ipv6
Output	Enriches observables with whois information related to IP addresses.
Description	Whois information from the RIPEstat web-based interface (Whois REST API (<code>https://github.com/ripe-ncc/whois/wiki/whois-rest-api</code>)), including inet number, name, organization, country, city, street, and telephone.

Configure the RIPEstat Whois 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 RIPEstat Whois enricher:

- **API URL**: the basic URL allowing access to the **RIPEstat Data API**
(https://stat.ripe.net/docs/data_api).
The value is: *<https://stat.ripe.net/data>*.
- 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 table view by column. 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:

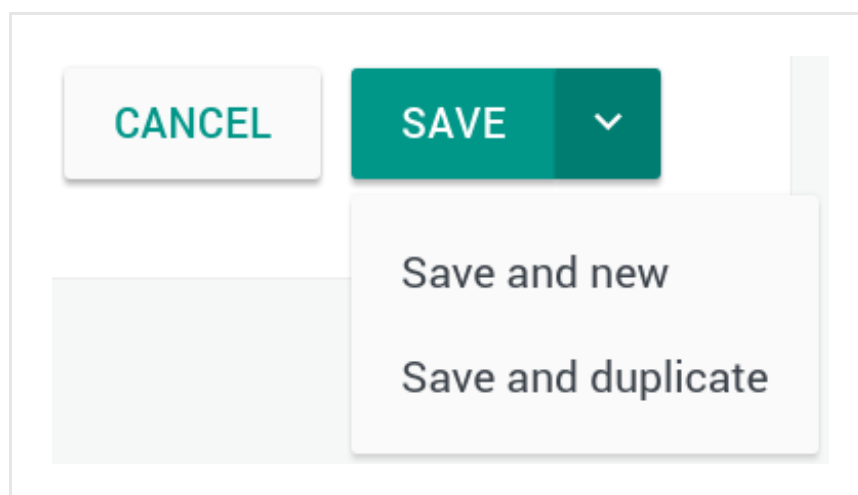
- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

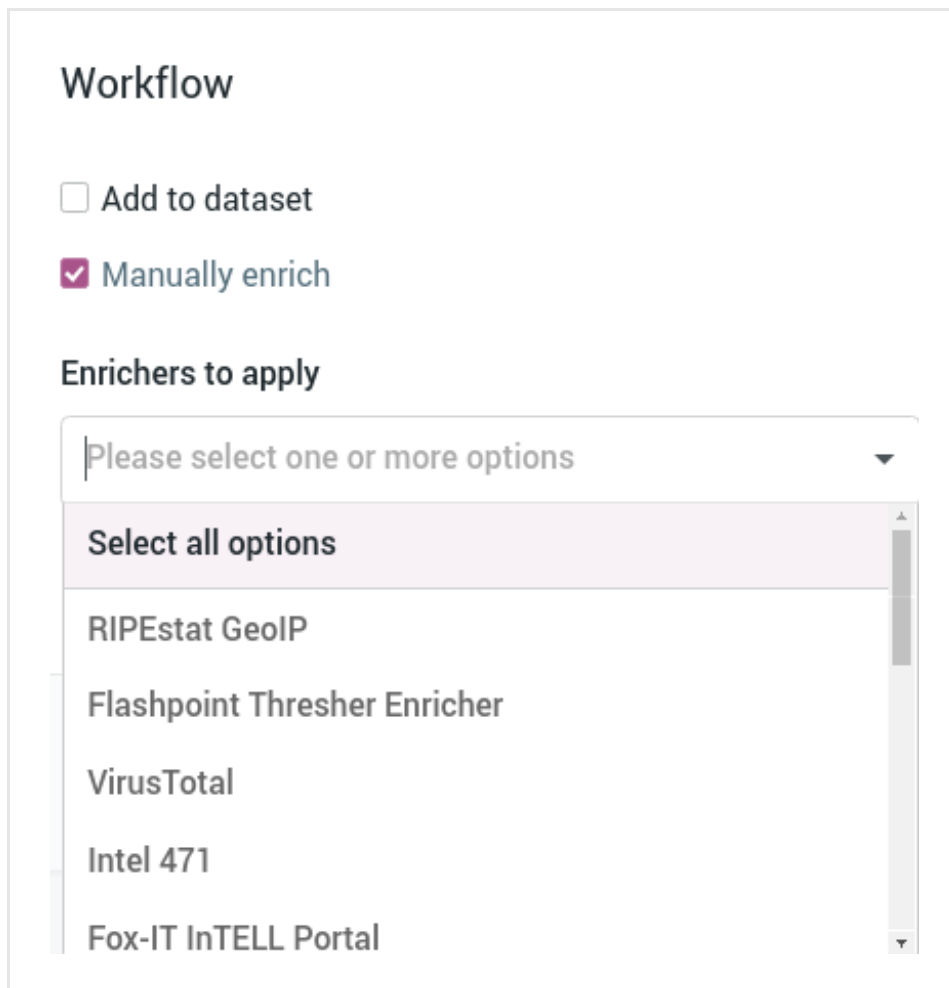
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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...' interface. At the top, there is a teal header bar with the title, a pencil icon, and a close icon. Below the header, there is a status bar showing 'Ingested: 01/24/2017 12:14 AM', 'Group: Testing Group', 'Author: Tes...', and a 'TLP None' button. The main content area has tabs for 'OVERVIEW', 'OBSERVABLES', 'NEIGHBORHOOD', 'JSON', 'VERSIONS', and 'HISTORY'. The 'OBSERVABLES' tab is selected. On the left, there is a dropdown menu labeled 'Enrich' with a red box around it. The dropdown menu is open, showing options: 'Enrich all observables' (highlighted with a red box), 'Enrich selected observables', 'Elastic Sightings Enricher', and 'OpenResolve'. 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 'Created' column has a refresh icon (a circular arrow) next to it, which is also highlighted with a red box. The table contains two rows of data, both labeled 'Enrichment (1)' and '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://zebbugtennis.com/wp-conte...> ×

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

○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	⌄		Enrichment (1) ● 7 days ago ⋮
	⌄		Enrichment (2) ● 7 days ago ⋮
<input checked="" type="checkbox"/> 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 RIPEstat Whois enricher can take the following observable types as input:

- *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 RIPEstat Whois.

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

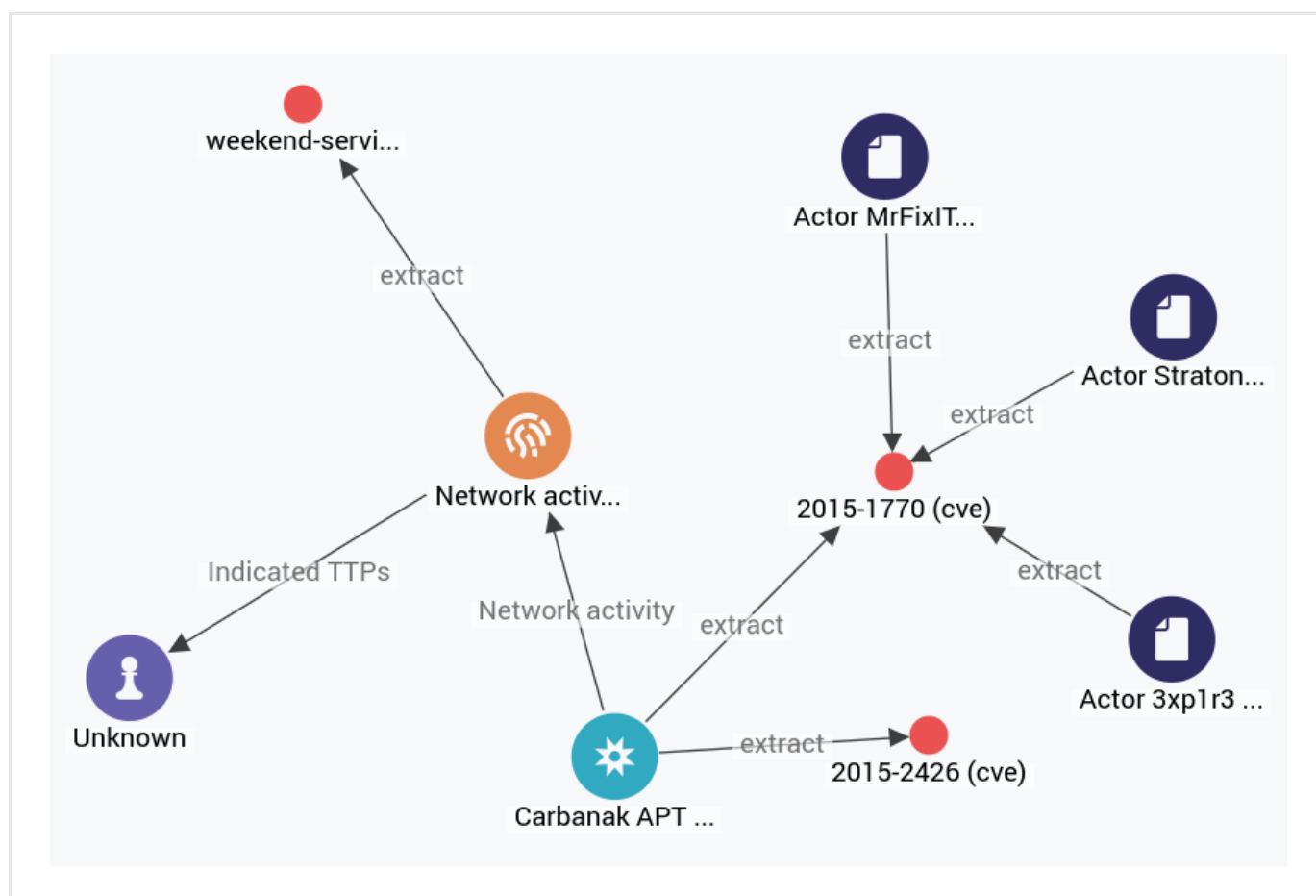
Date

<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	

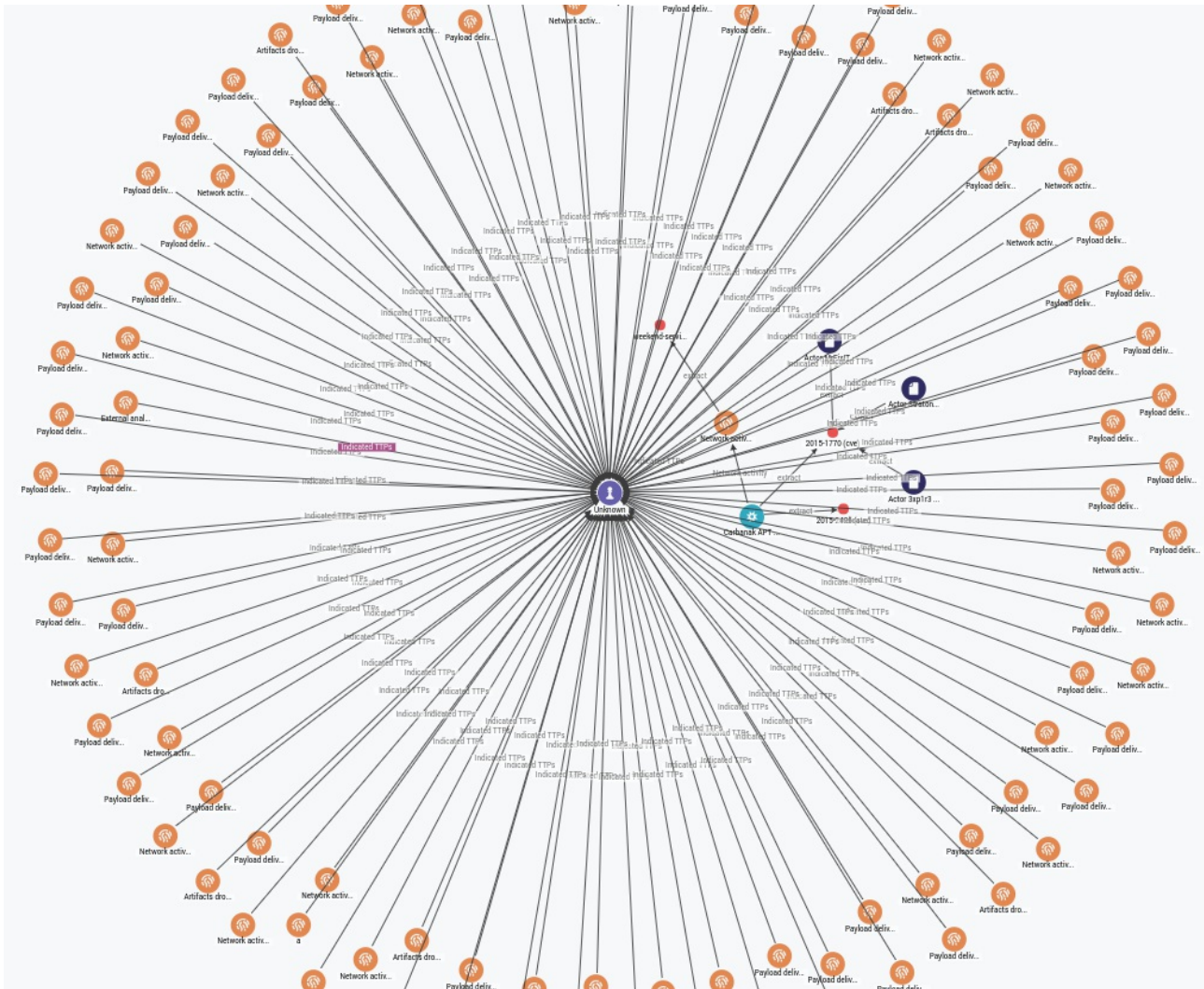
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

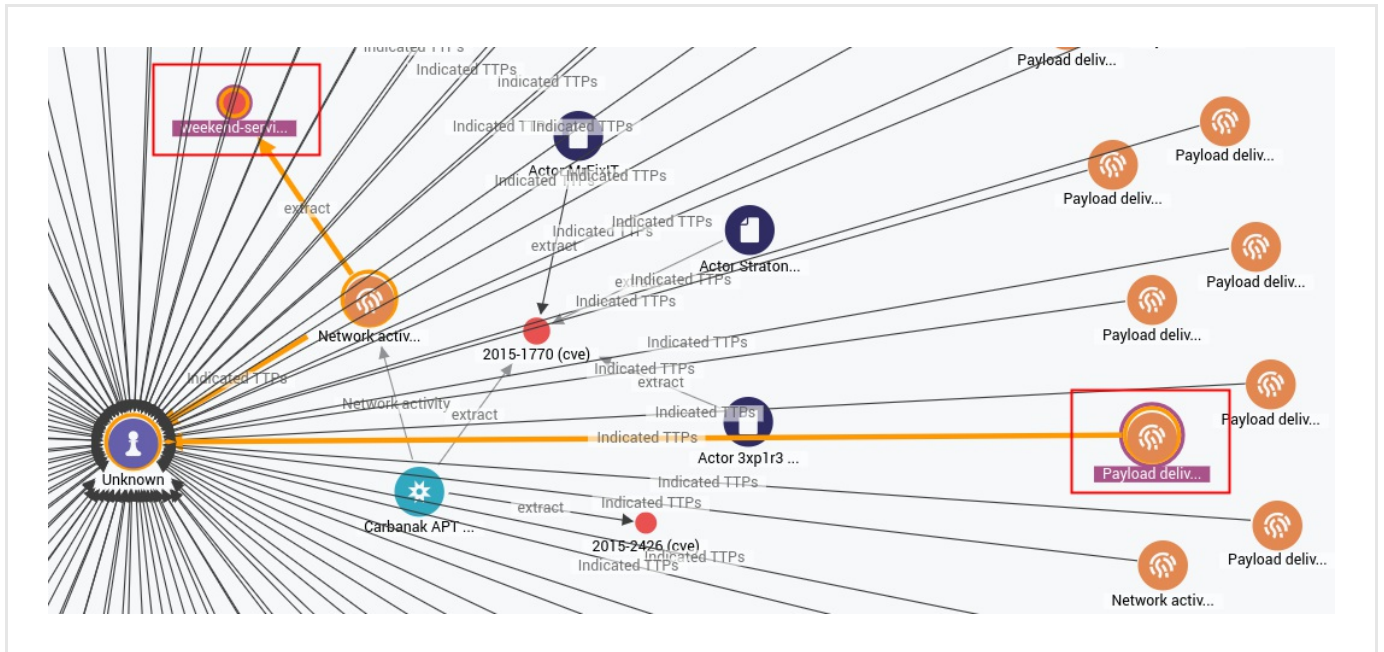


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



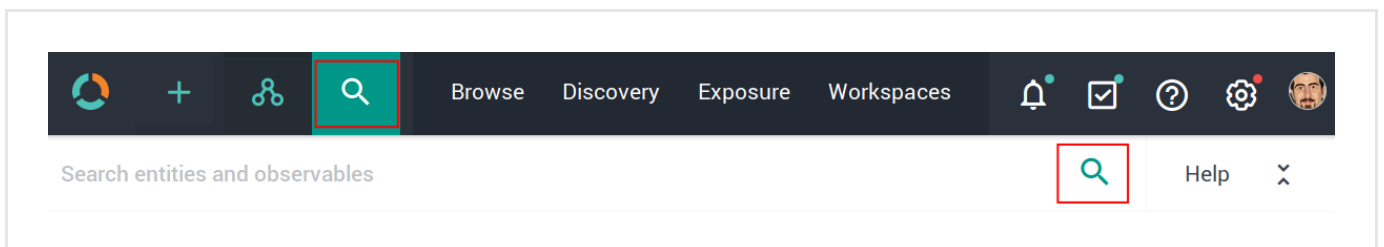
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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.

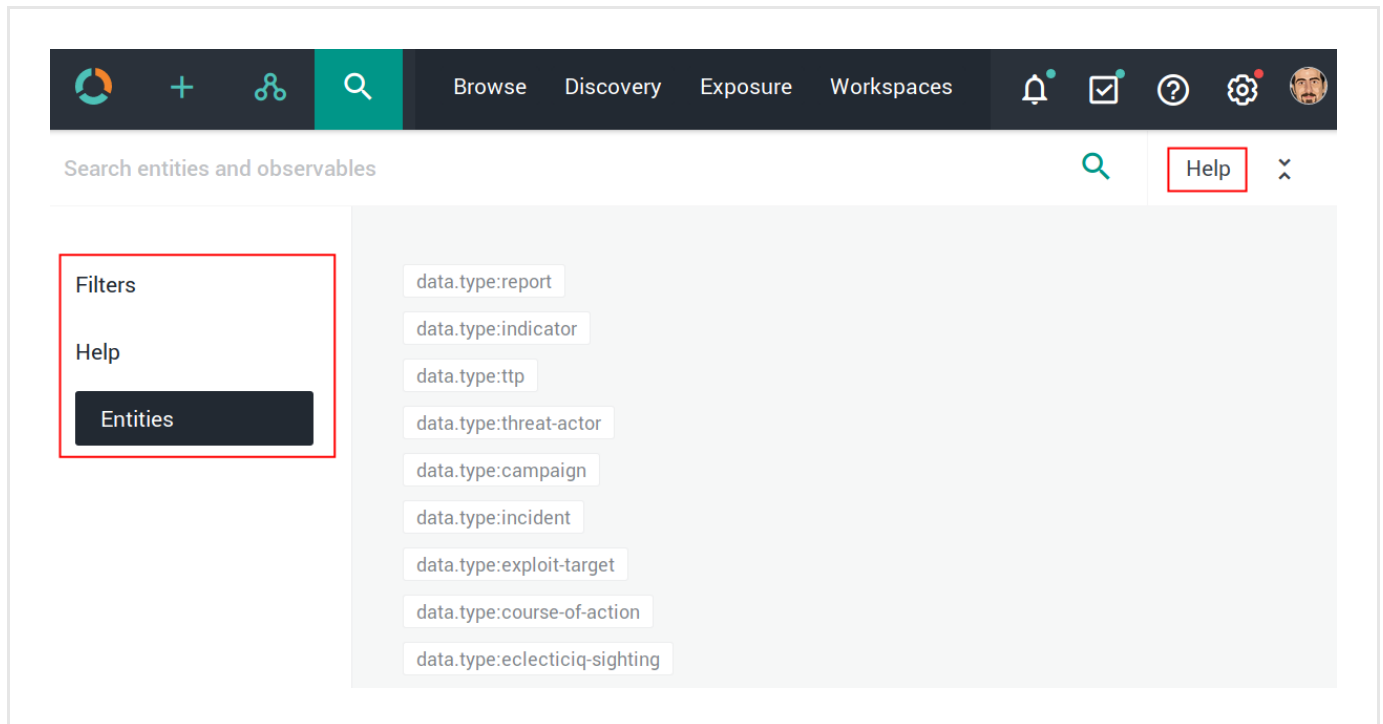


The search functionality uses **Elasticsearch query syntax**

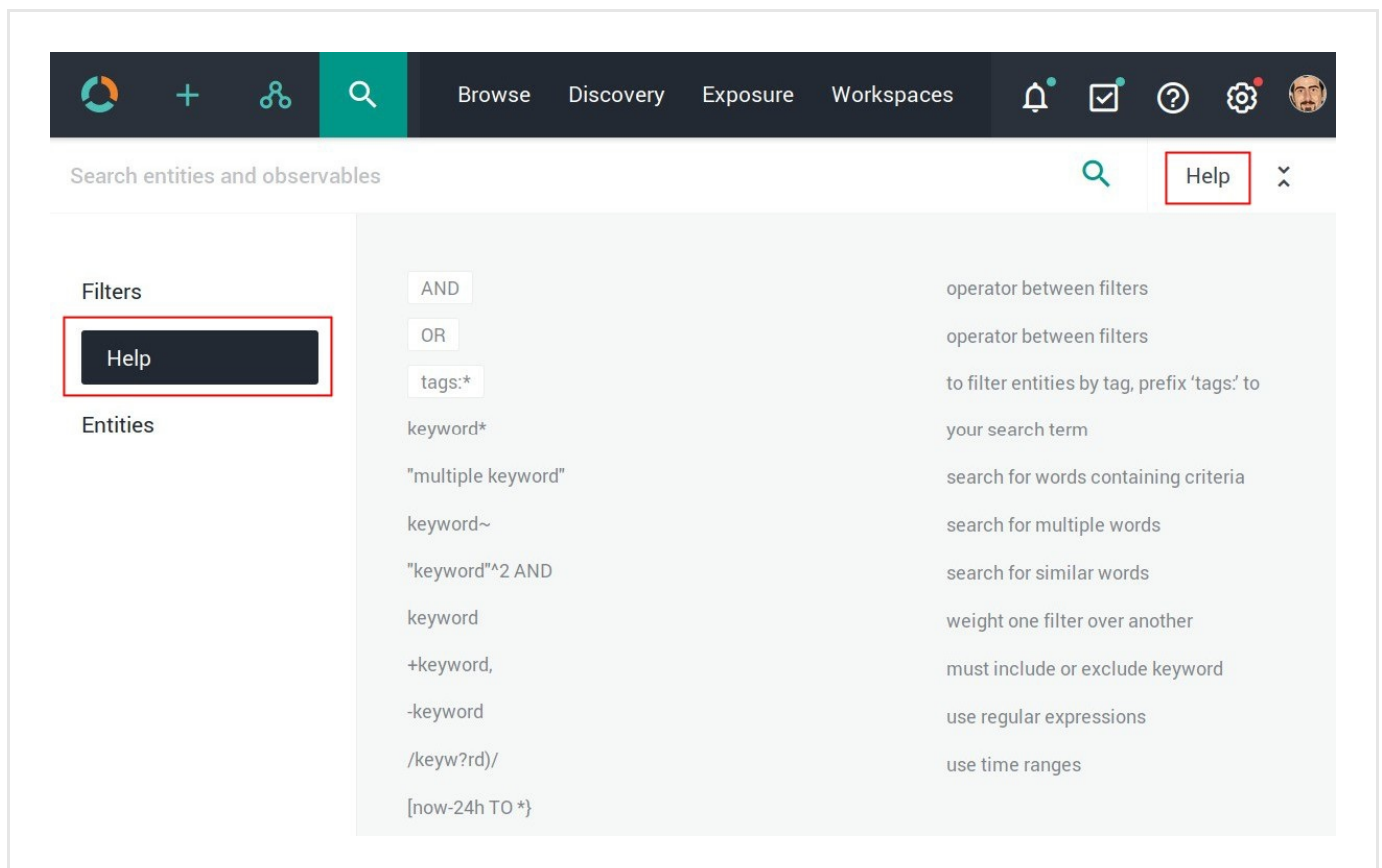
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

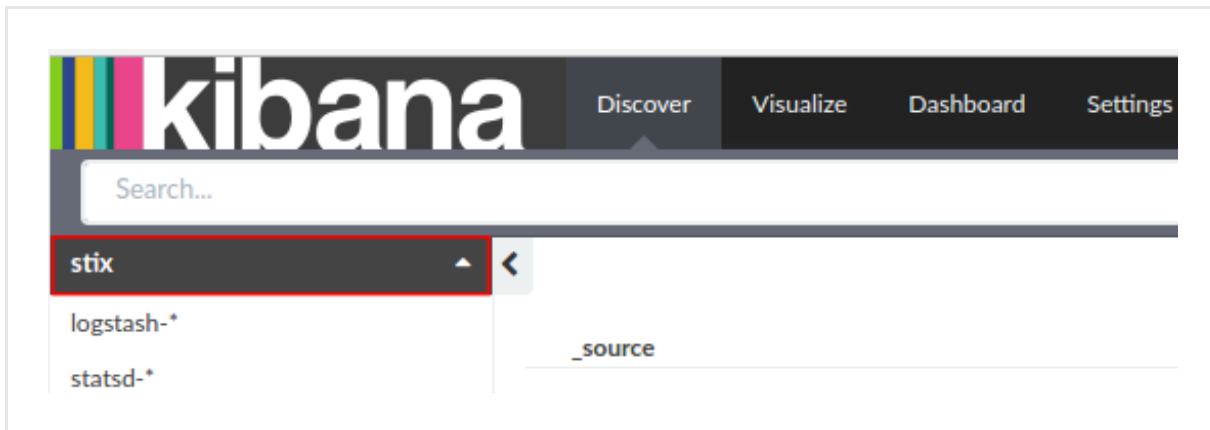
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

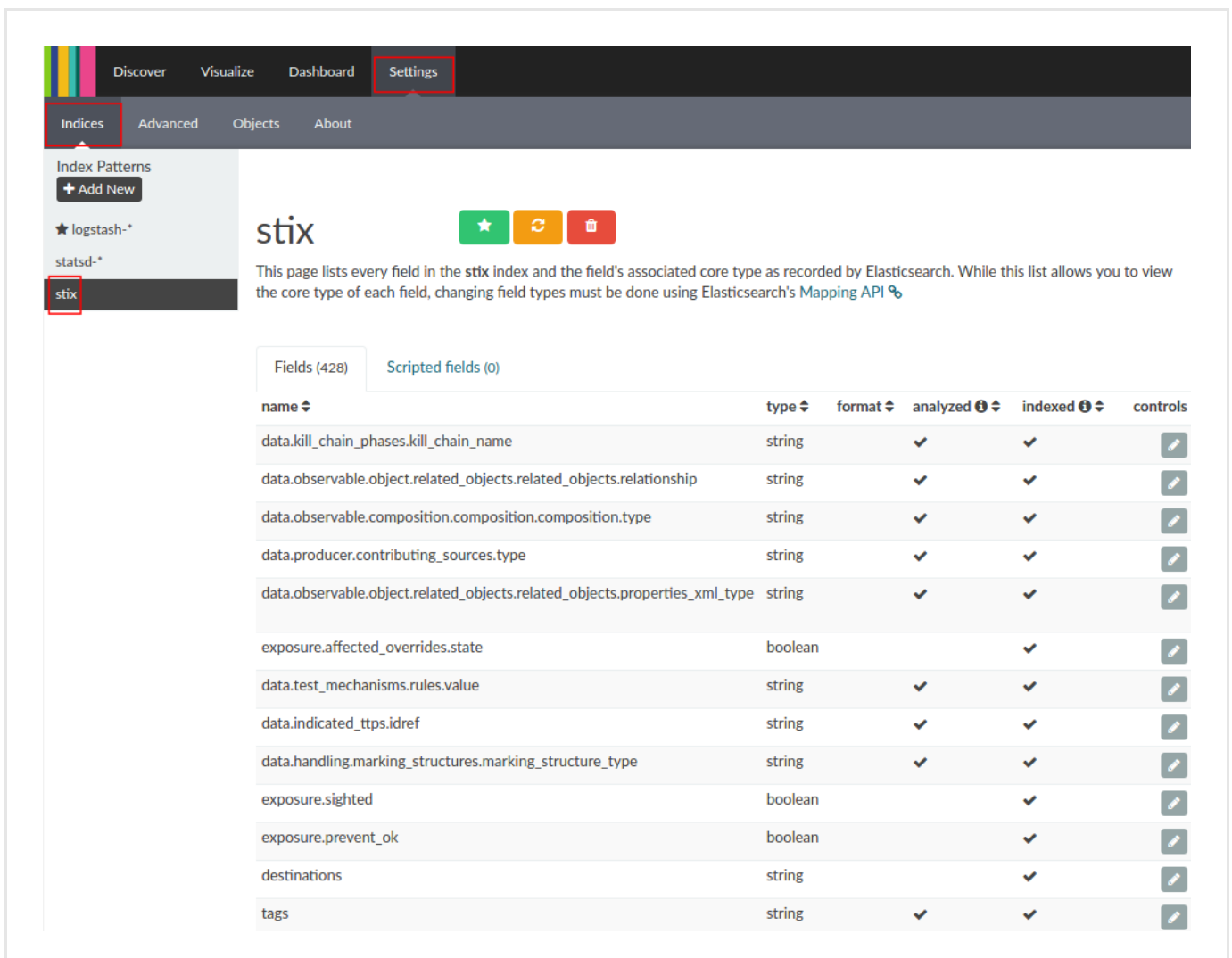
Keep the trailing /.

Example: [https://platform.host.com/api/kibana/app/kibana#/.](https://platform.host.com/api/kibana/app/kibana#/)

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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 Cisco AMP Threat Grid enricher

Configure the Cisco AMP Threat Grid 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.

- **Name:** the name used to identify the enricher. It should be descriptive and easy to remember.
- **Description:** additional textual details. If you want, you can add a short description to provide more information and context.

- **Cache validity (sec)**: defines for how long enrichment data remains stored in the cache. The value is expressed in seconds.
- **Rate limit (per sec)**: sets the maximum allowed number of requests/executions per second.
- **Monthly execution cap (executions)**: sets a maximum allowed number of requests/executions per month.
Together with rate limiting, execution cap helps control data traffic for the enricher; for example, when the API or the service you are connecting to enforces usage limits.
- **Source reliability**: from the drop-down menu select an option to flag the content of the outgoing feed with a predefined reliability value to help other users assess how trustworthy the feed source is.
Values in this menu have the same meaning as the first character in the **two-character Admiralty System code** (https://en.wikipedia.org/wiki/admiralty_code).
Example: *B - Usually reliable*
- **Enabled**: checkbox. Select the **Enabled** checkbox to enable the enricher task immediately after editing and saving it.
If you select the checkbox, the rule is executed automatically. If you deselect it, you need to run the rule manually.
- Under **Parameters**, define the specific configuration options for the selected enricher, where applicable.
- Click **Save** to store your changes, or **Cancel** to discard them.


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 table view by column. 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.

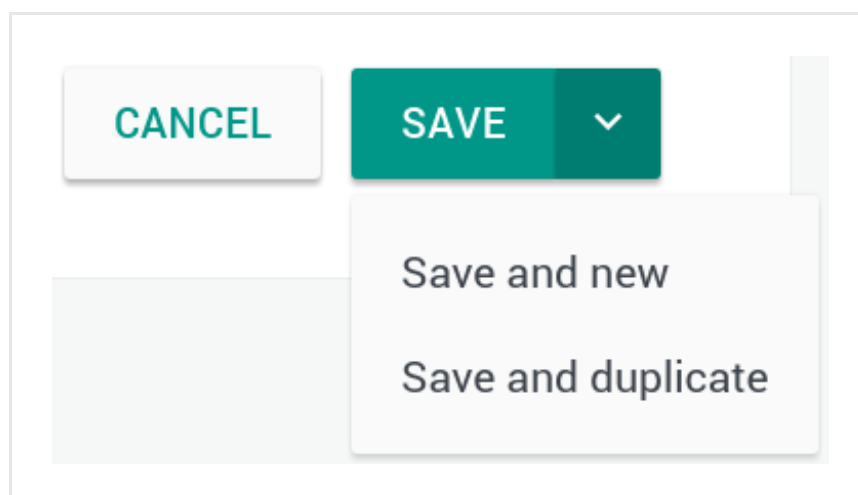
On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

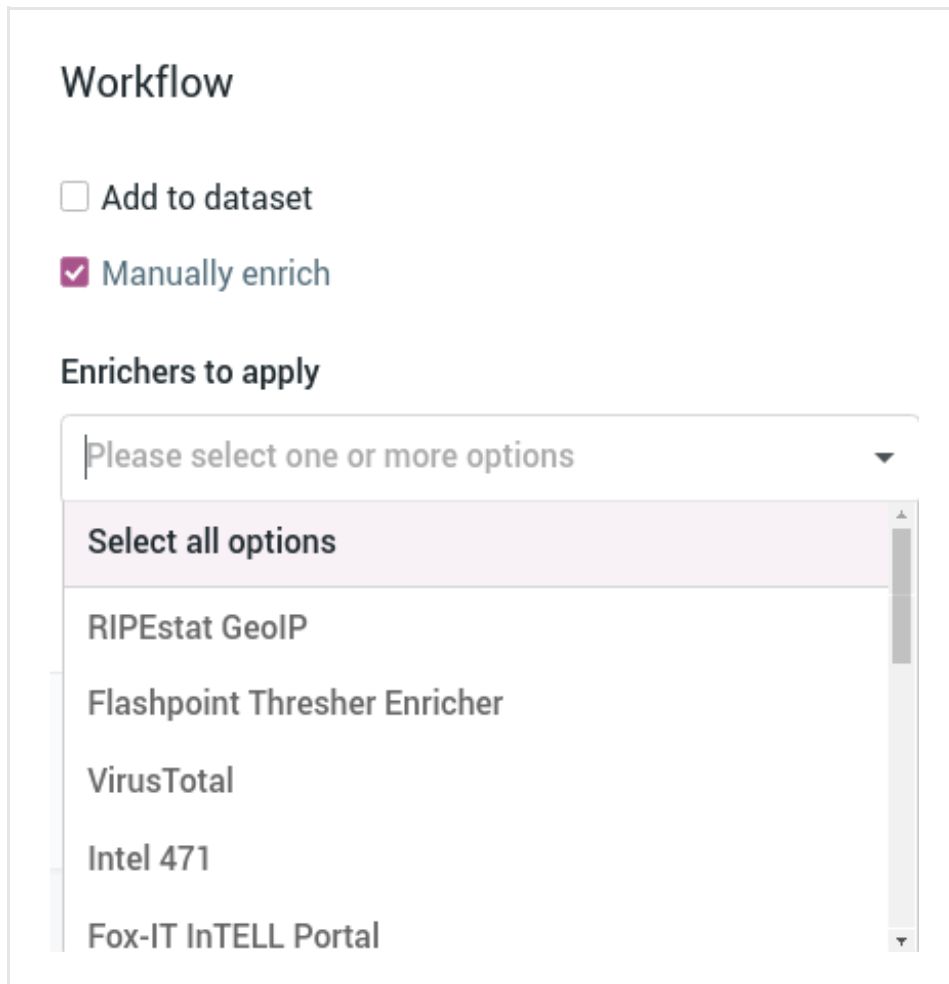
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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.

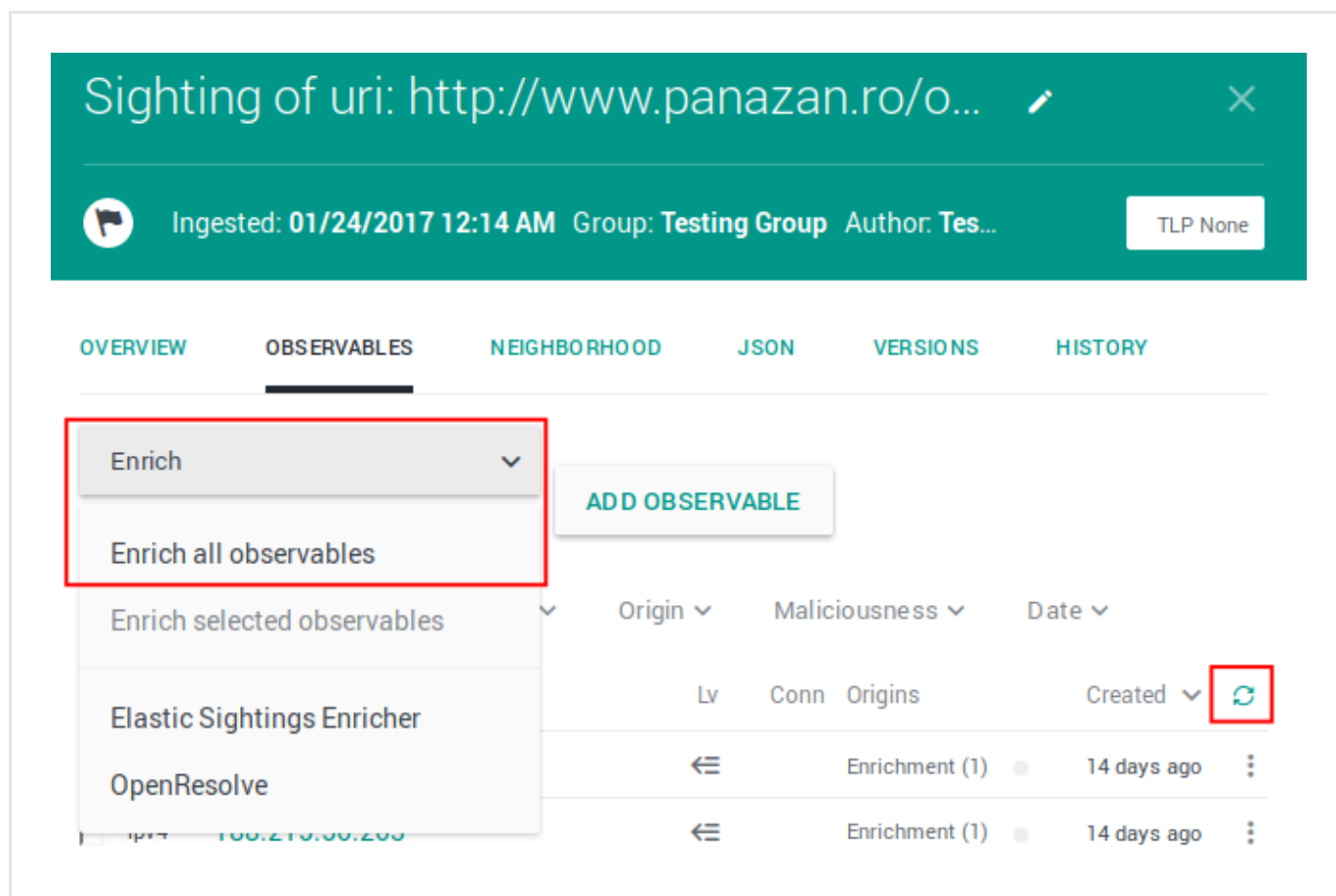
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.



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.




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

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://zebbugtennis.com/wp-conte...> ×

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

○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

		Origin ▼	Maliciousness ▼	Date ▼
		Lv	Conn	Origins
				Created ▼ ↻
<input checked="" type="checkbox"/>	uri	http://zebbugtennis.com/wp-co...	2	2
<input checked="" type="checkbox"/>	uri	http://zebbugtennis.com/wp-co...	1	1
<input checked="" type="checkbox"/>	hash-md5	a47a1906802faf32be76732366...	1	2
<input checked="" type="checkbox"/>	domain	zebbugtennis.com	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






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

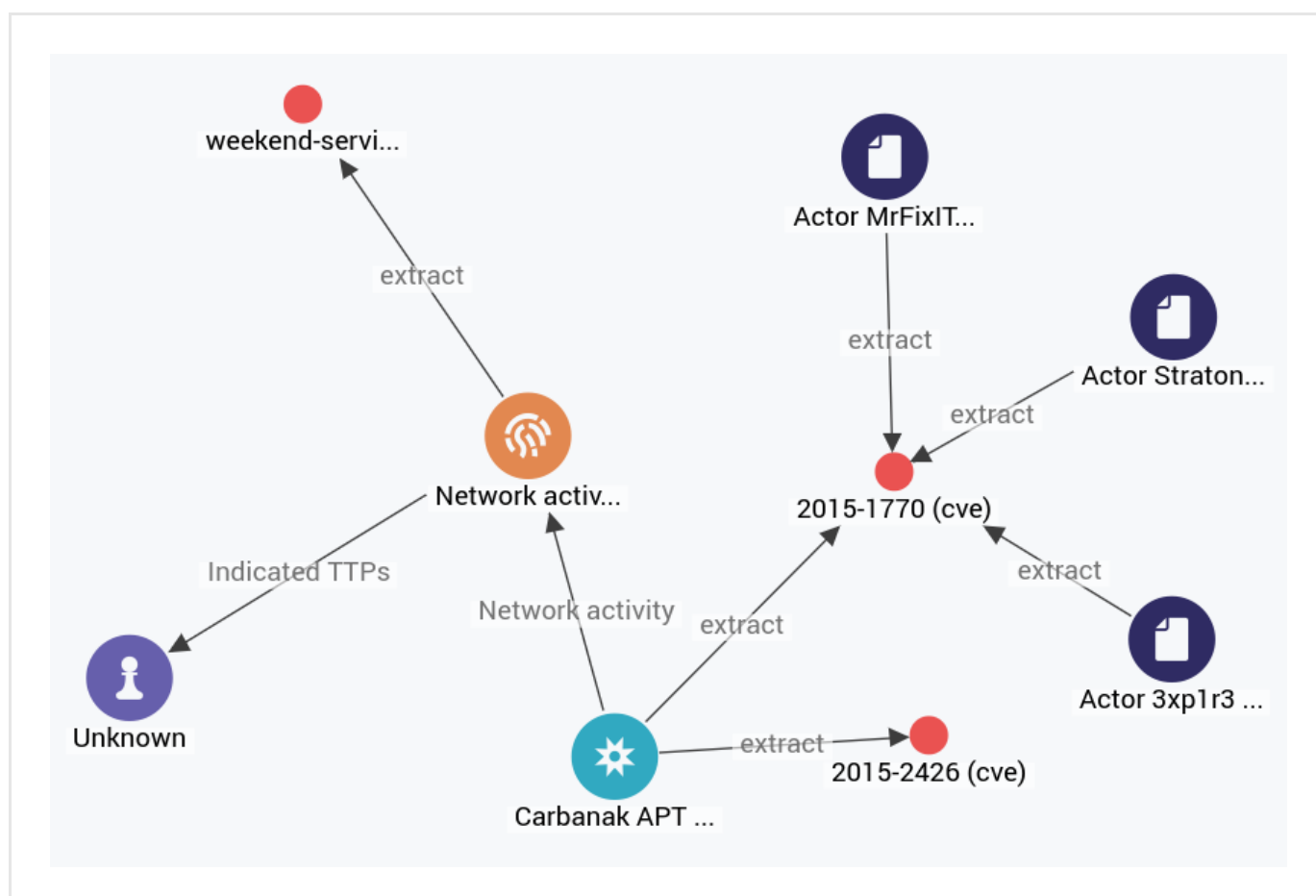
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

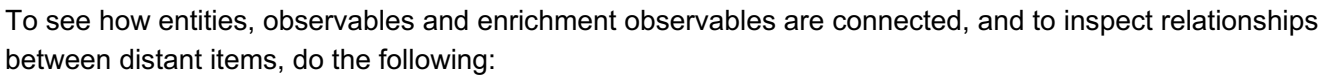
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

Ignore extract
 Create sighting
Add to graph
 Set maliciousness >

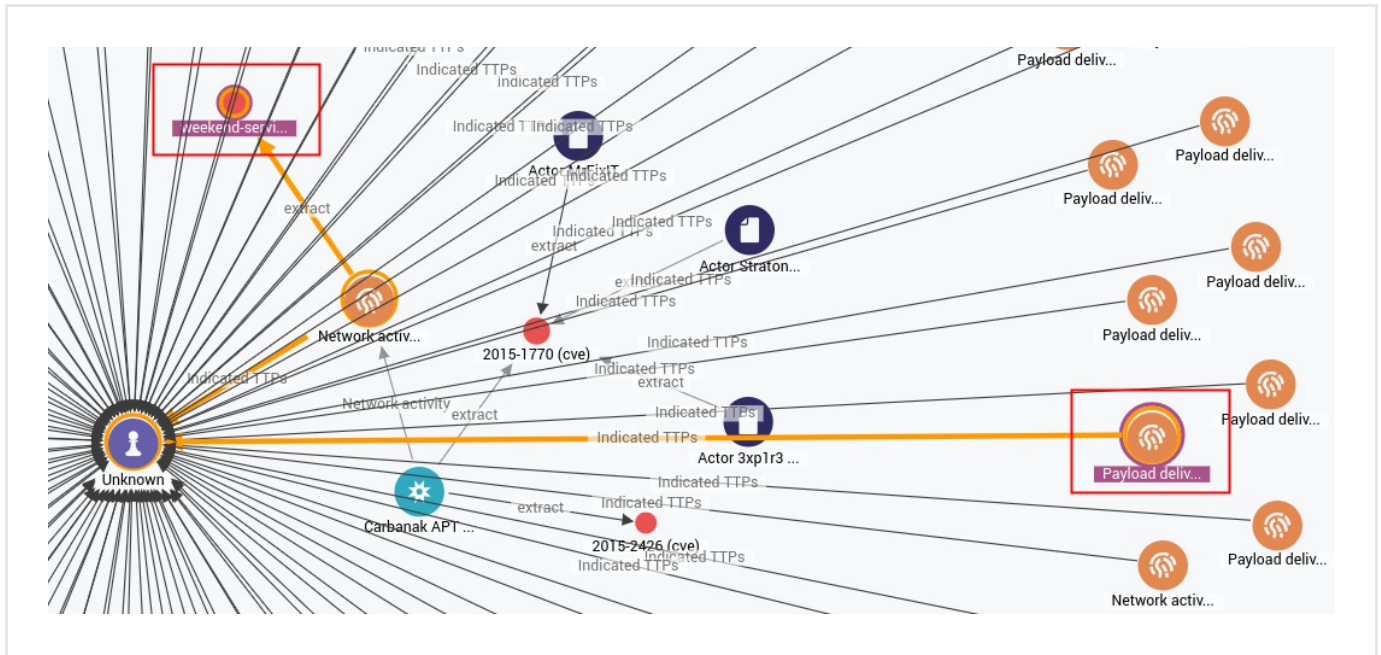
- To load the parent entity whose detail pane you are viewing, instead of its observables, from the pop-up **Actions** menu at the bottom of the pane select **Add to graph**.
- Click the graph thumbnail on the lower side of the screen to expand it.
- On the graph, right-click the entity you want to inspect,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

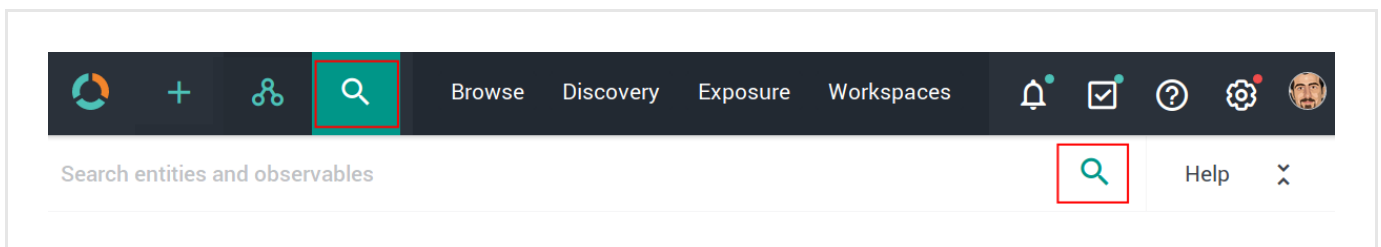


- **CTRL** + click two nodes on the graph to select them.
- Right-click either selected node, and from the context menu select **Find path** to query the graph database about the existence of a path between the nodes, or **Show path** to highlight an existing path on the graph.
- If a path does exist,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

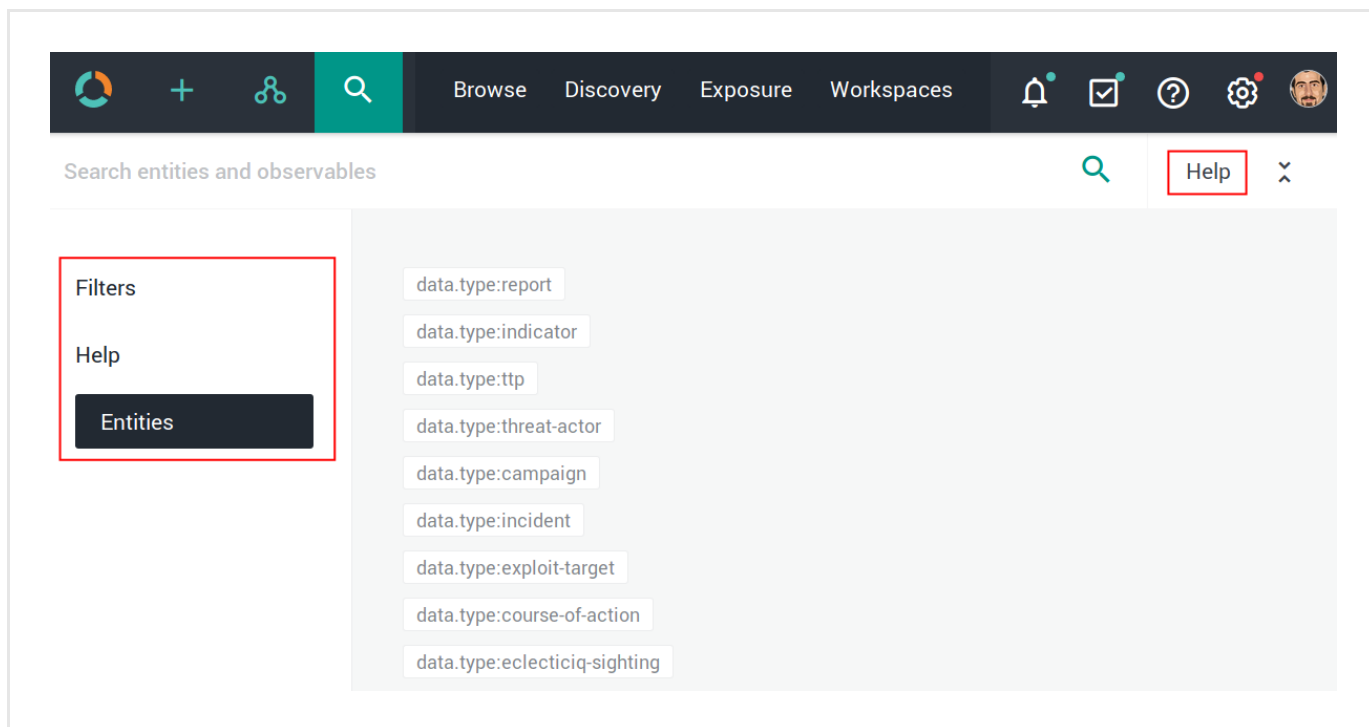


The search functionality uses **Elasticsearch query syntax**

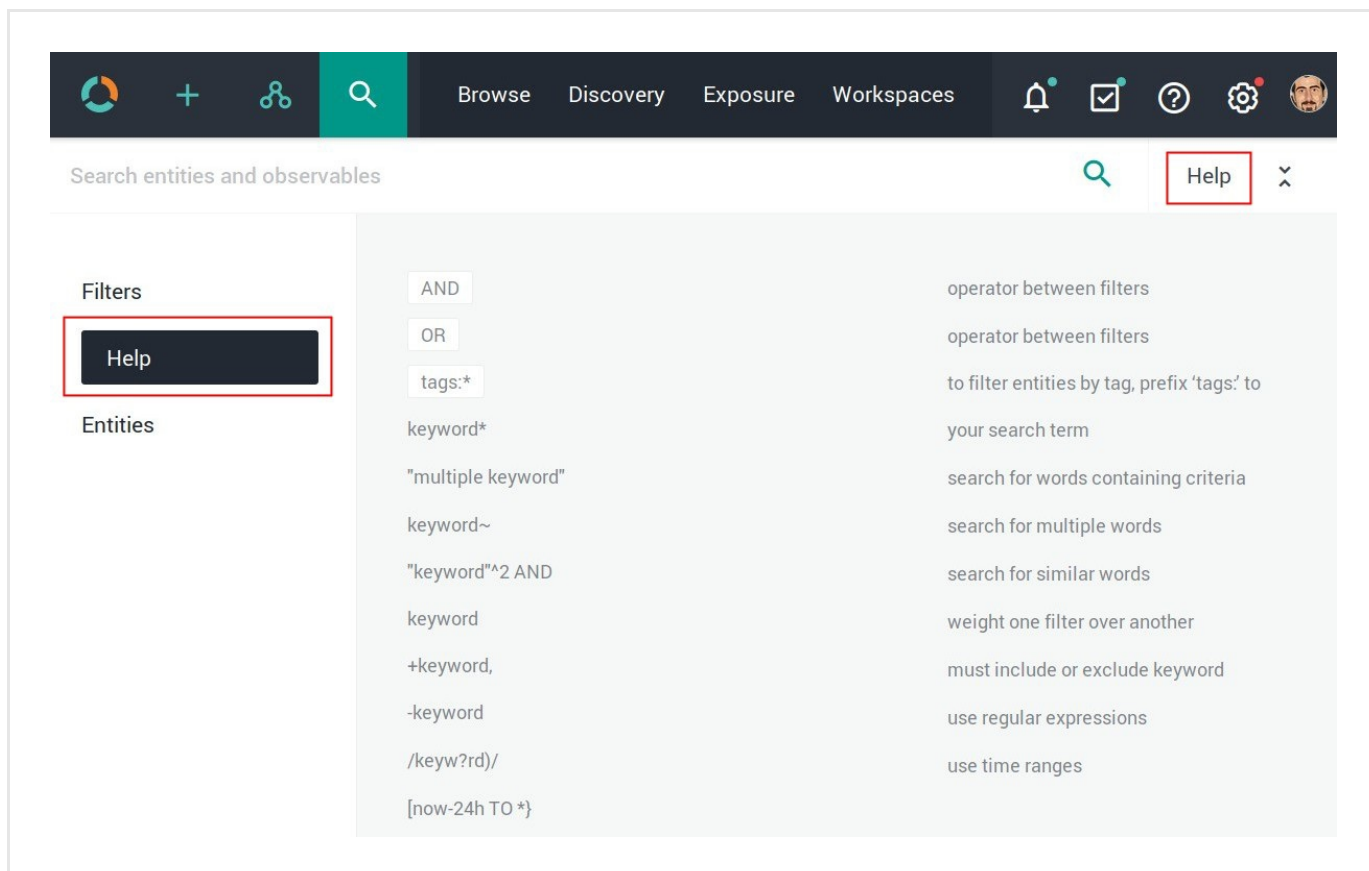
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

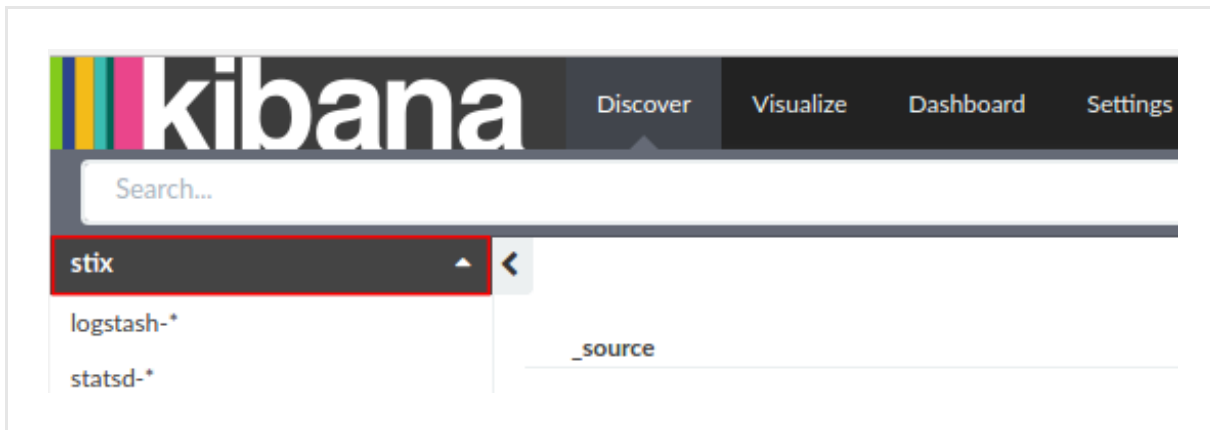
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

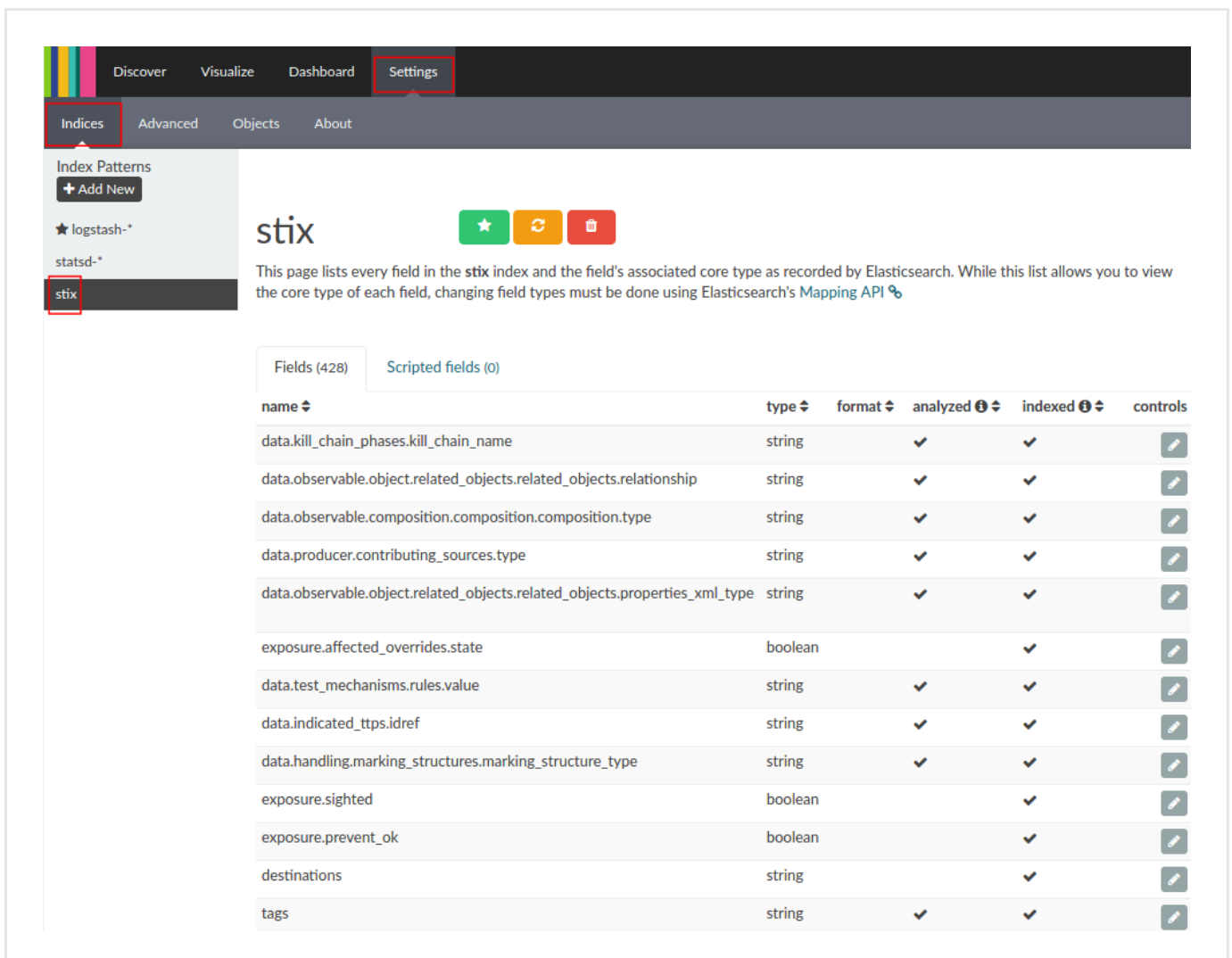
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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 Unshorten-URL enricher

This article describes how to configure the Unshorten-URL enricher parameters.

To configure the general options for the Unshorten-URL enricher, see [Configure enrichers](#).

RIPEstat GeolIP enricher	
Enricher name	Unshorten-URL
API endpoint	<code>https://unshorten.me/s/{}</code>
Input	uri
Output	Original URL the submitted shortened one.
Description	It takes shortened URL as an input, and it returns the corresponding resolved original URLs, which can then be analyzed in the platform to discover relationships with other entities.

Configure the Unshorten-URL 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 the observable type representing the shortened URLs that the enricher submits to the specified services.
The supported observable type is *uri*.

Under **Parameters**, define the specific configuration options for the Unshorten-URL enricher:

- **Providers:** enter one or more URL shortener services to use with the enricher.

Separate multiple URL shortener services with either a comma or a white space.

Example: *bit.ly, goo.gl, tinyurl.com*, or *bit.ly goo.gl tinyurl.com*

You do not need to prefix the domains with the transmission protocol. If included, *http://* or *https://* is stripped at runtime.

- 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 table view by column. 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.

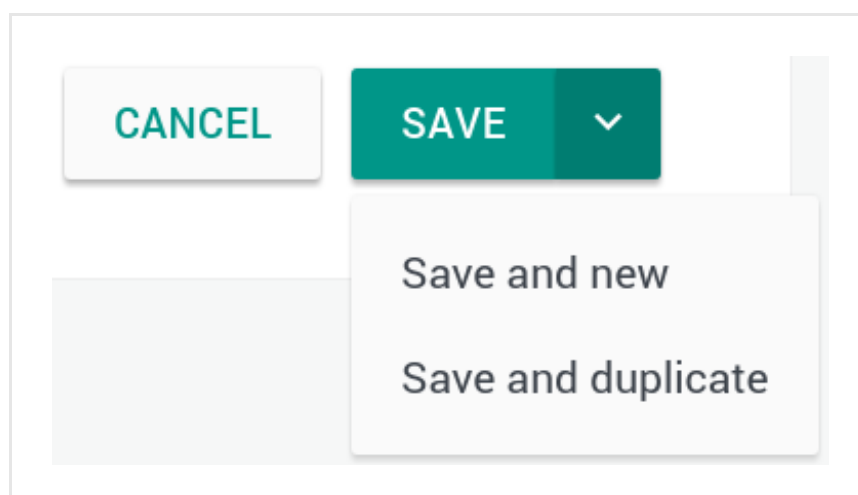
On the **Rules > Enrichment > Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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.

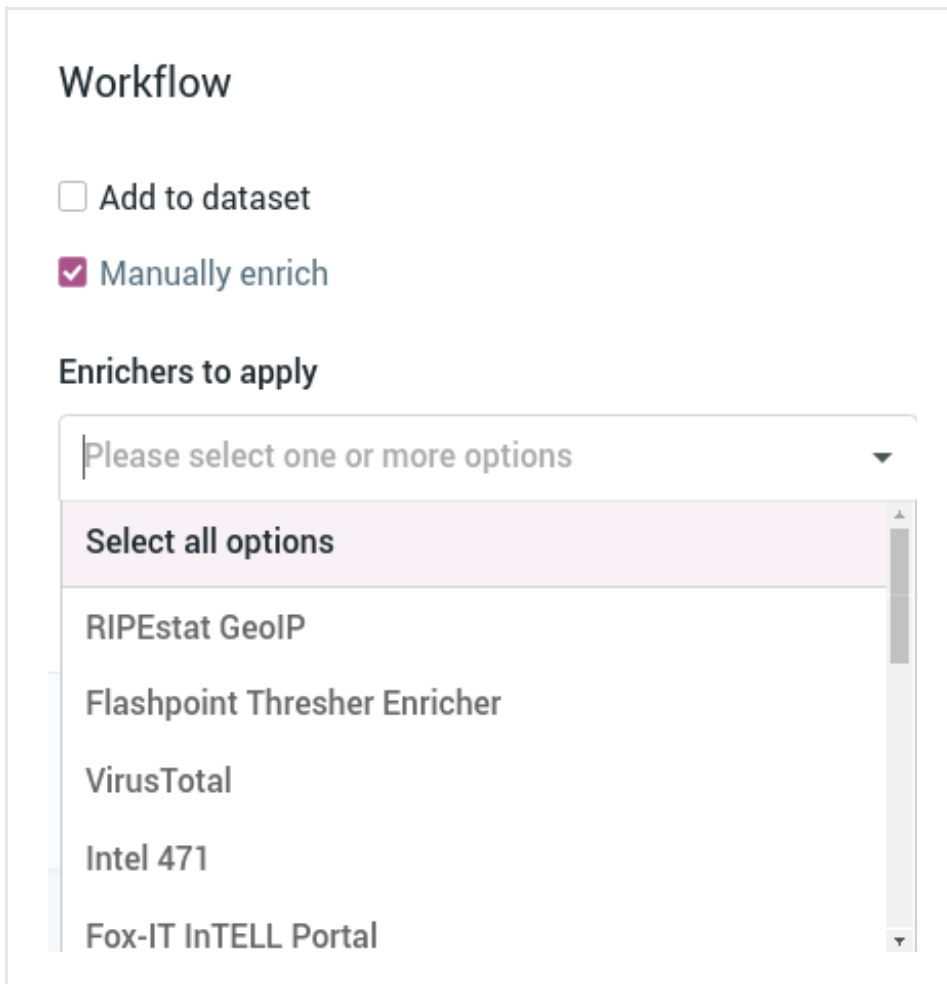
To run the enricher automatically, go to the enricher edit mode, and make sure the **Enabled** checkbox on the edit form is selected.

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 dotted menu 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 GeolIP
- 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.

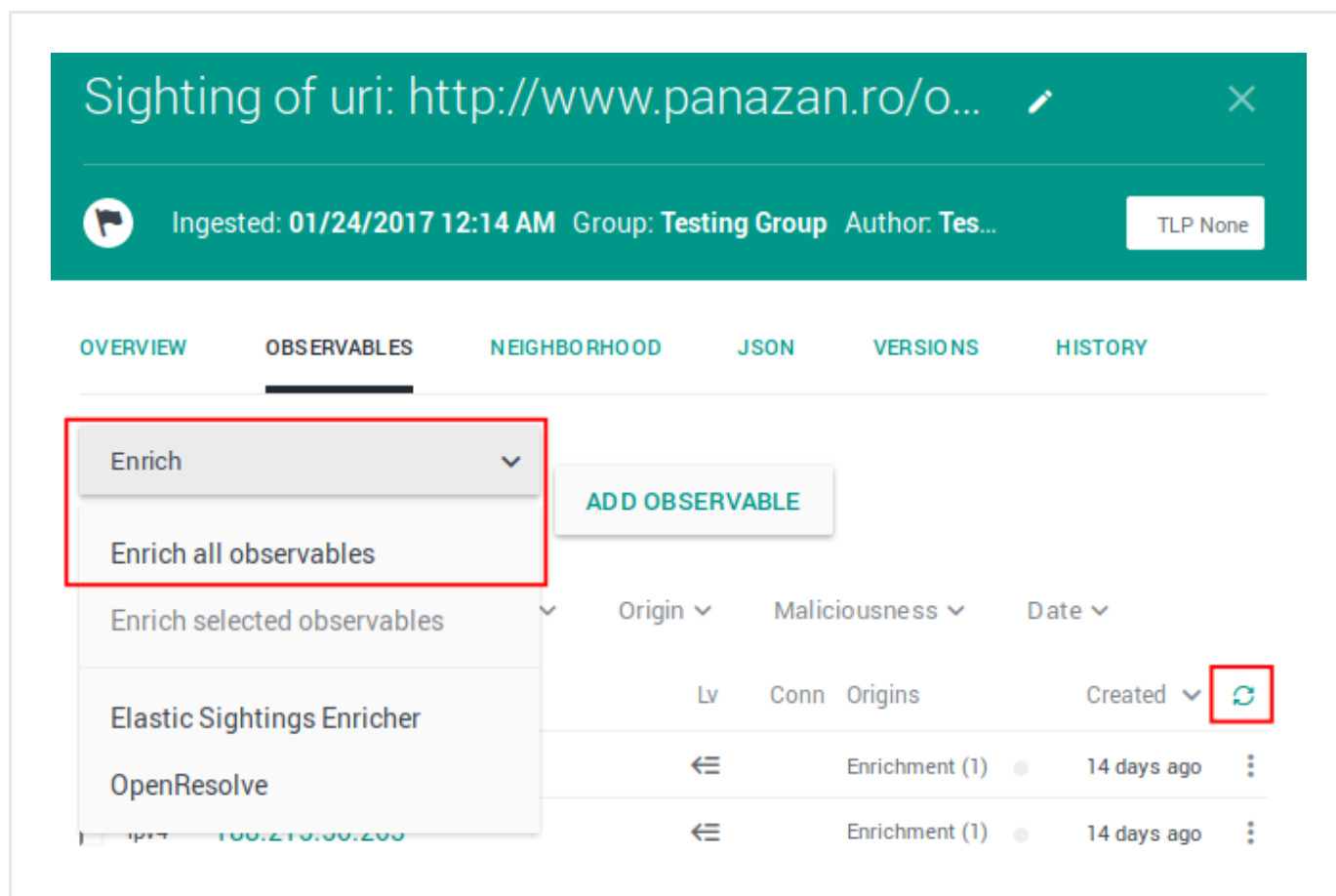
- On the entity detail pane, click **Observables**.
- The **Observables** tab shows an overview of the enrichment observables the entity has been augmented with.



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://zebbugtennis.com/wp-conte...> ×

Ingested: 09/15/2016 10:20 PM Incoming feed: guest.phishtank_c...
○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	⌄		Enrichment (1) ● 7 days ago ⋮
	⌄		Enrichment (2) ● 7 days ago ⋮
<input checked="" type="checkbox"/> 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 Unshorten-URL enricher can take the following observable types as input:

- *uri*

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 Unshorten-URL.

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

Review enrichment observables on the graph

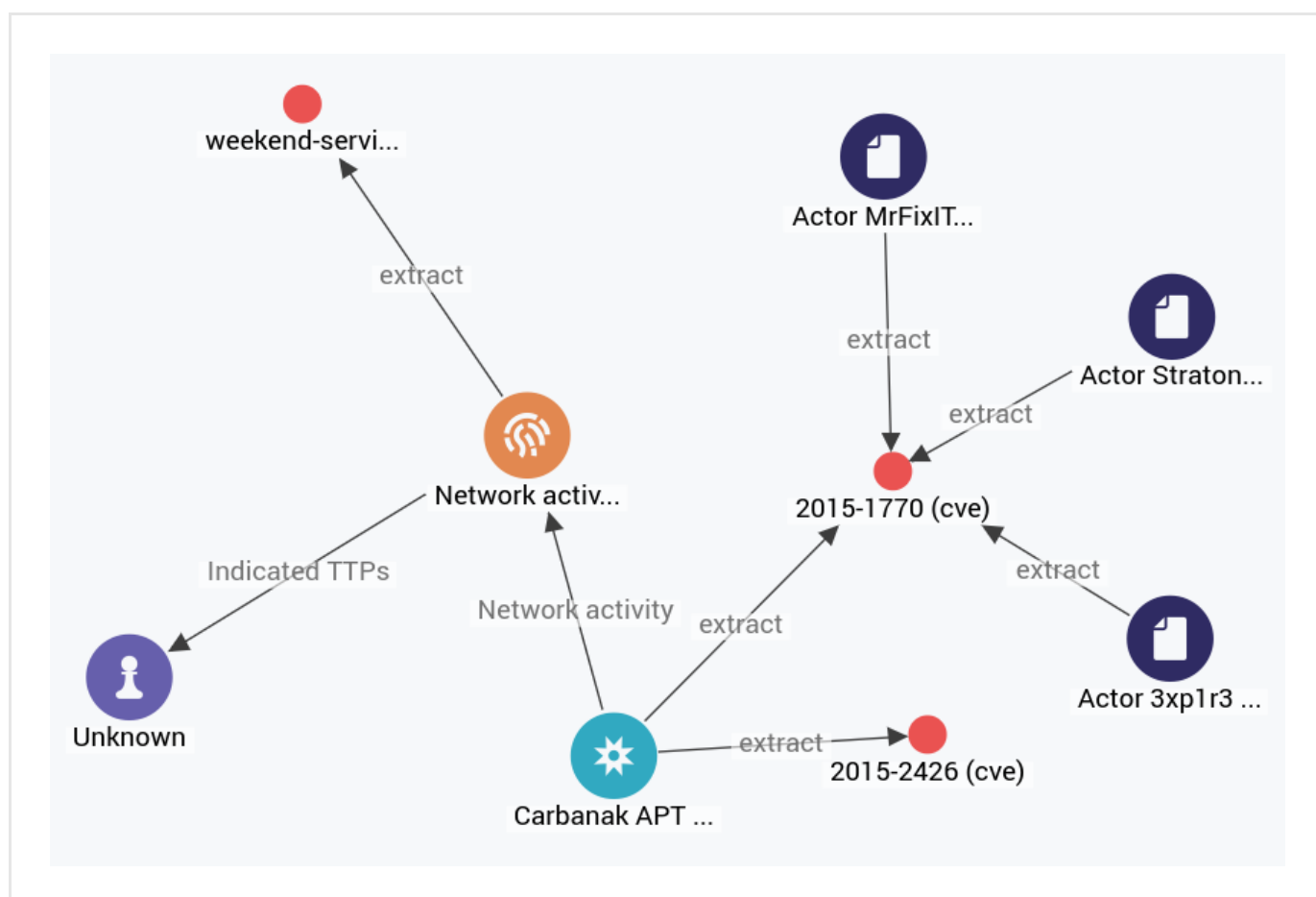
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

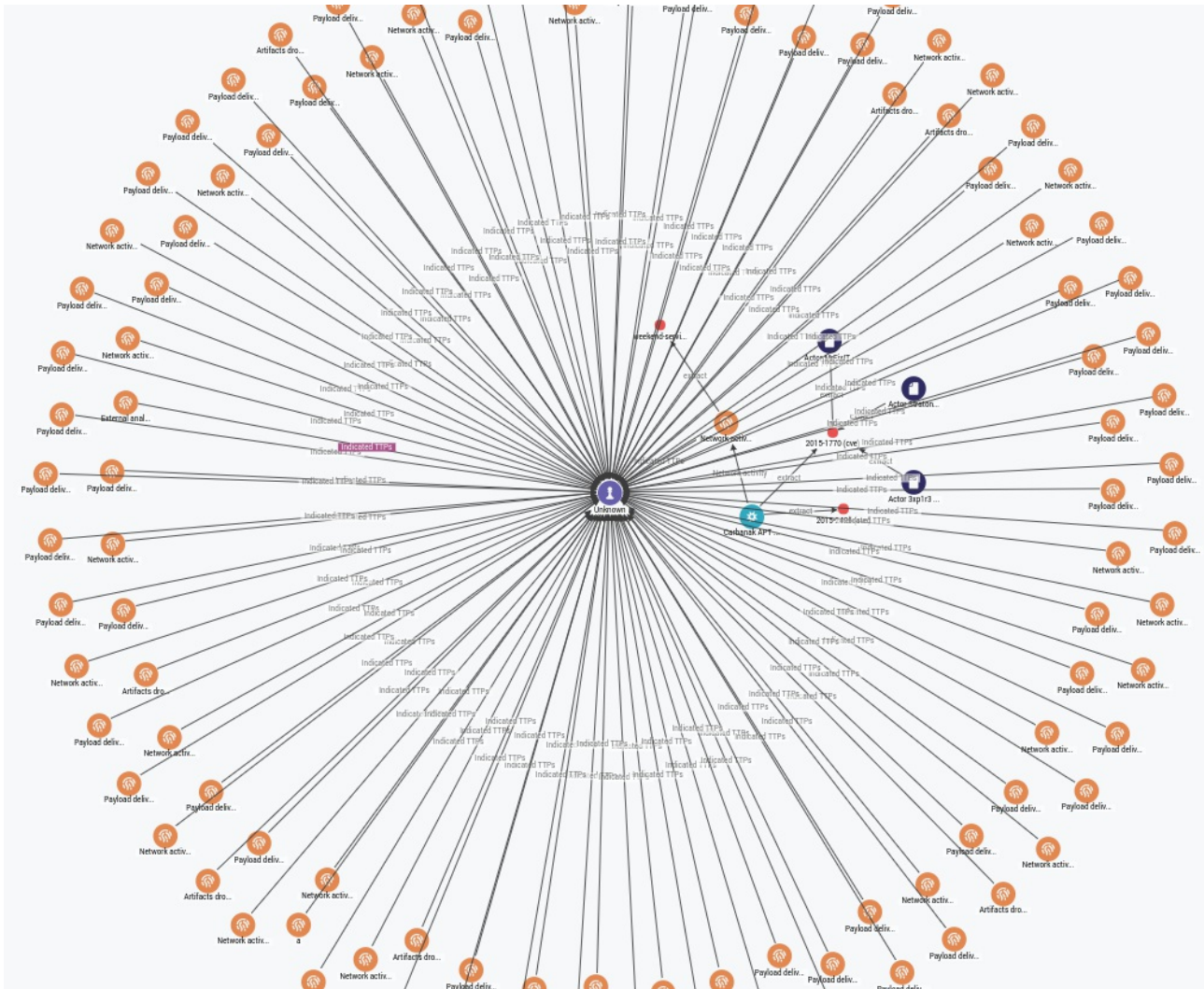
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	⋮
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>	name	vcdp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

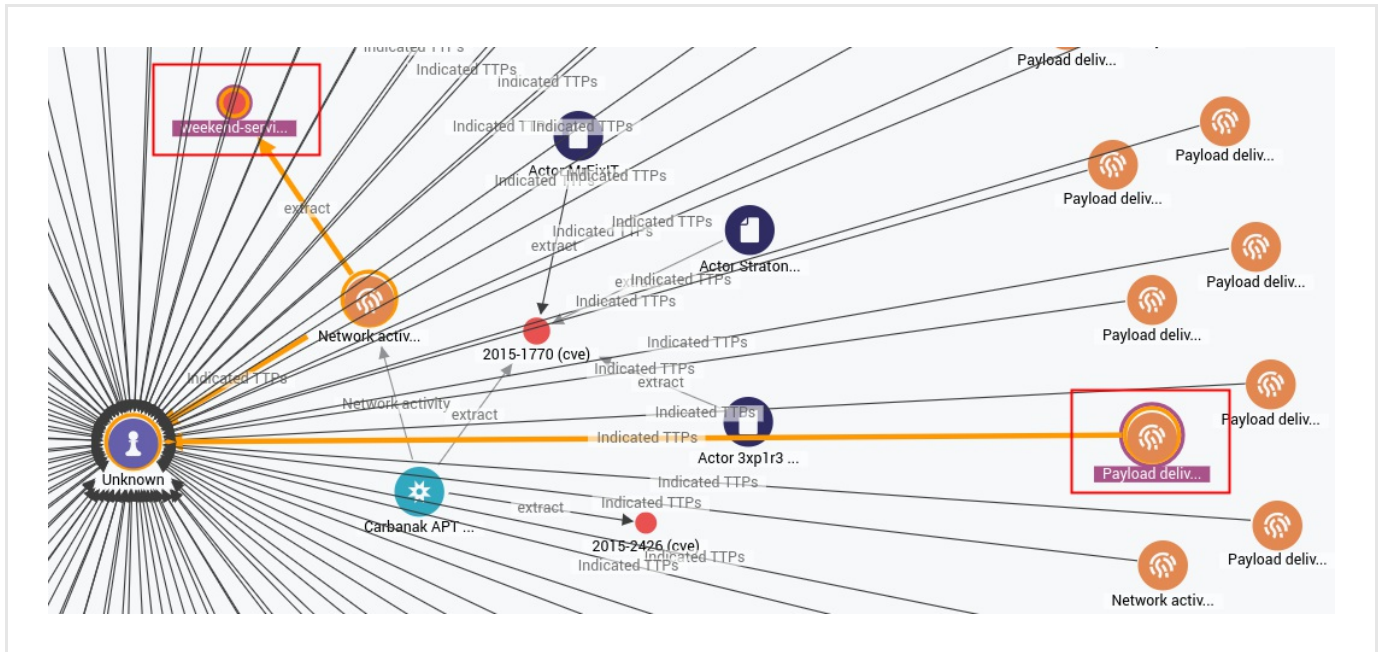


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



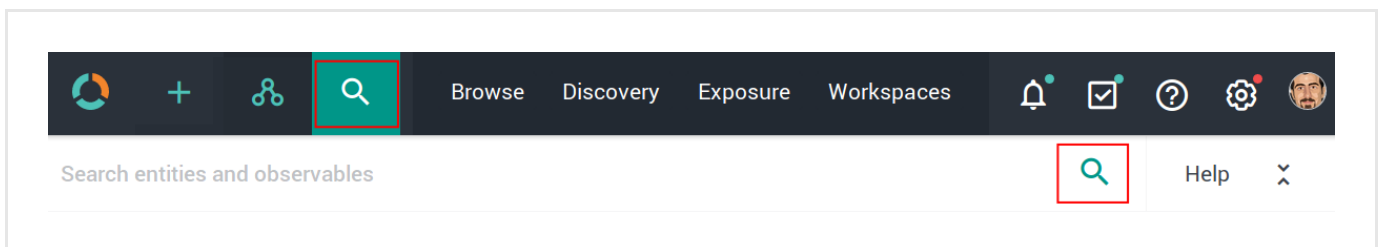
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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.

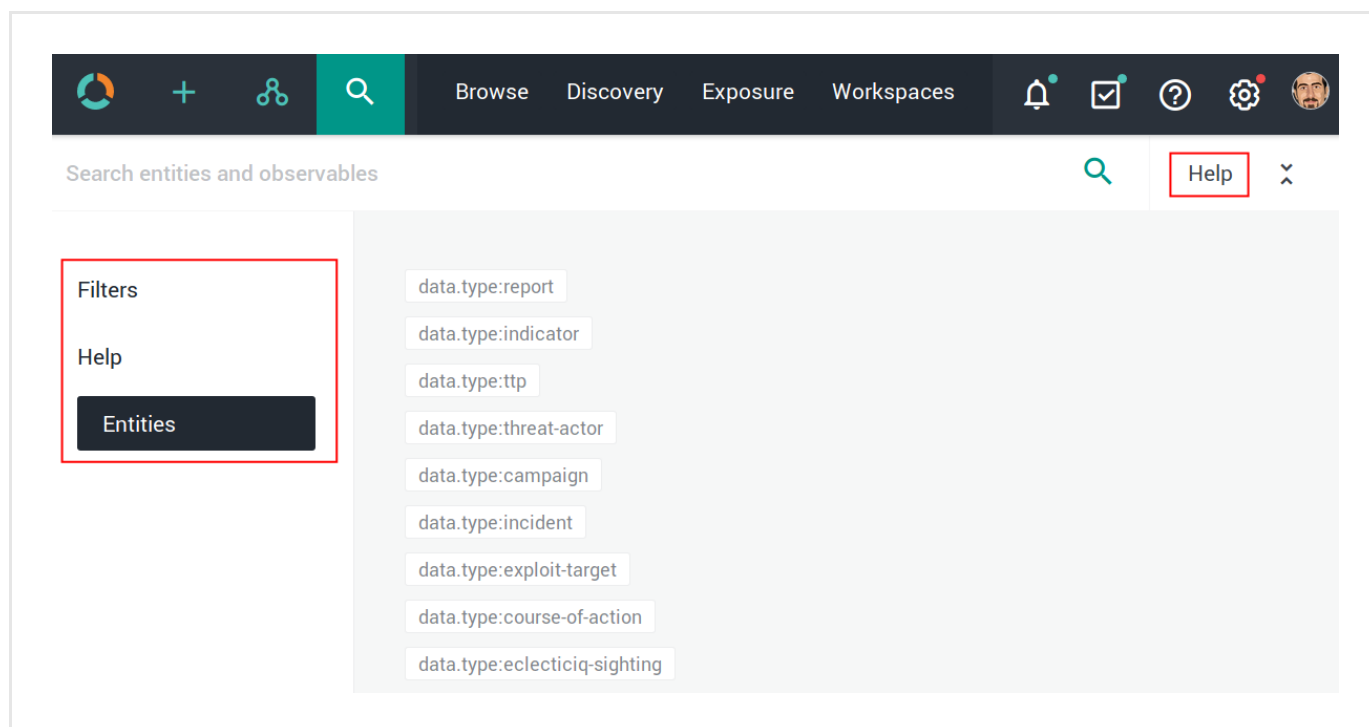


The search functionality uses **Elasticsearch query syntax**

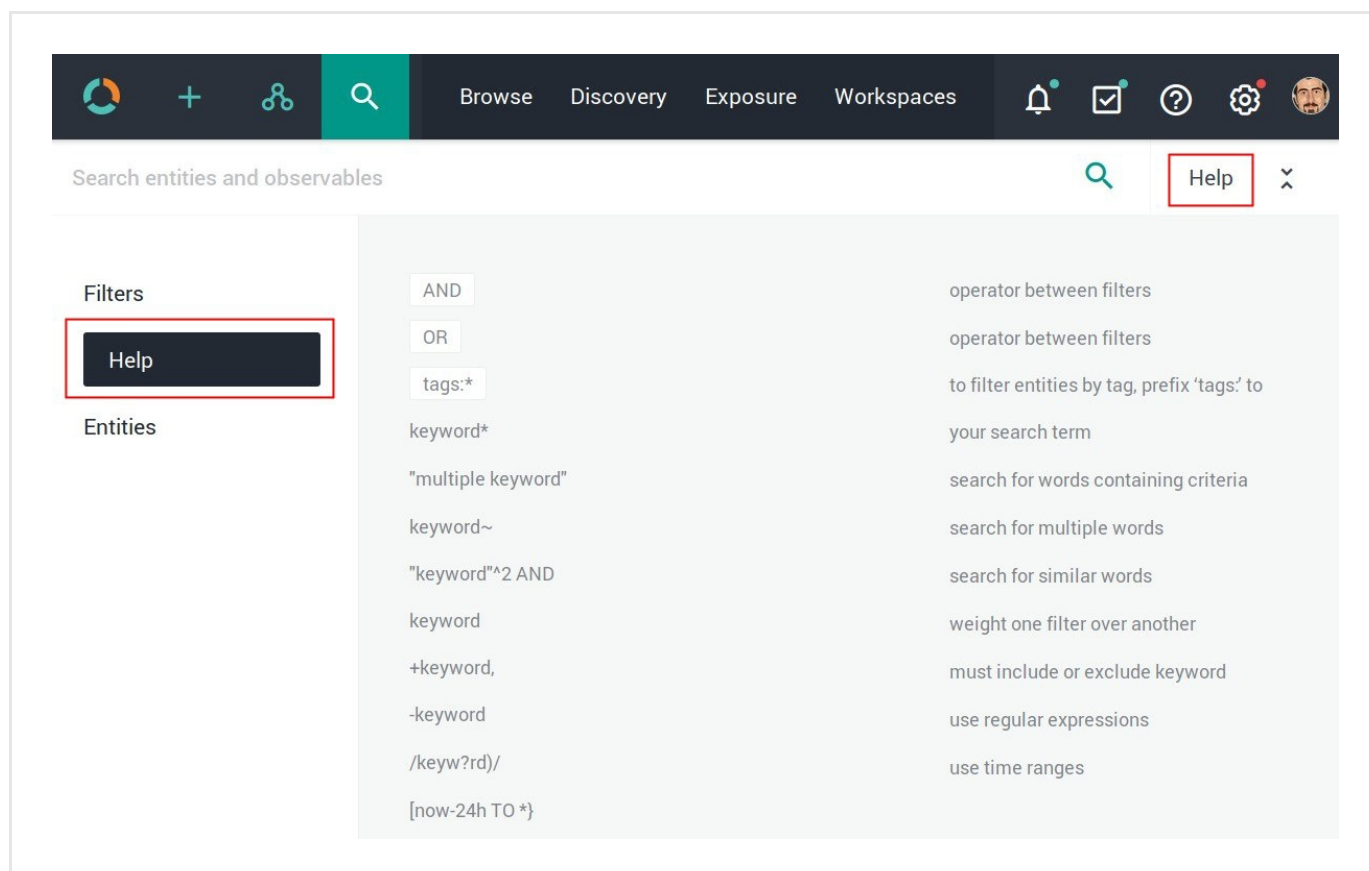
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

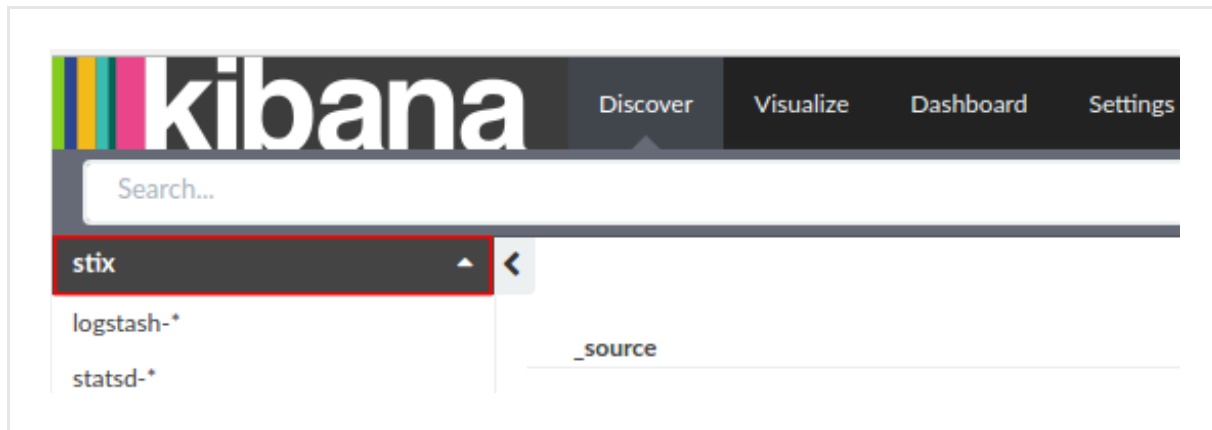
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

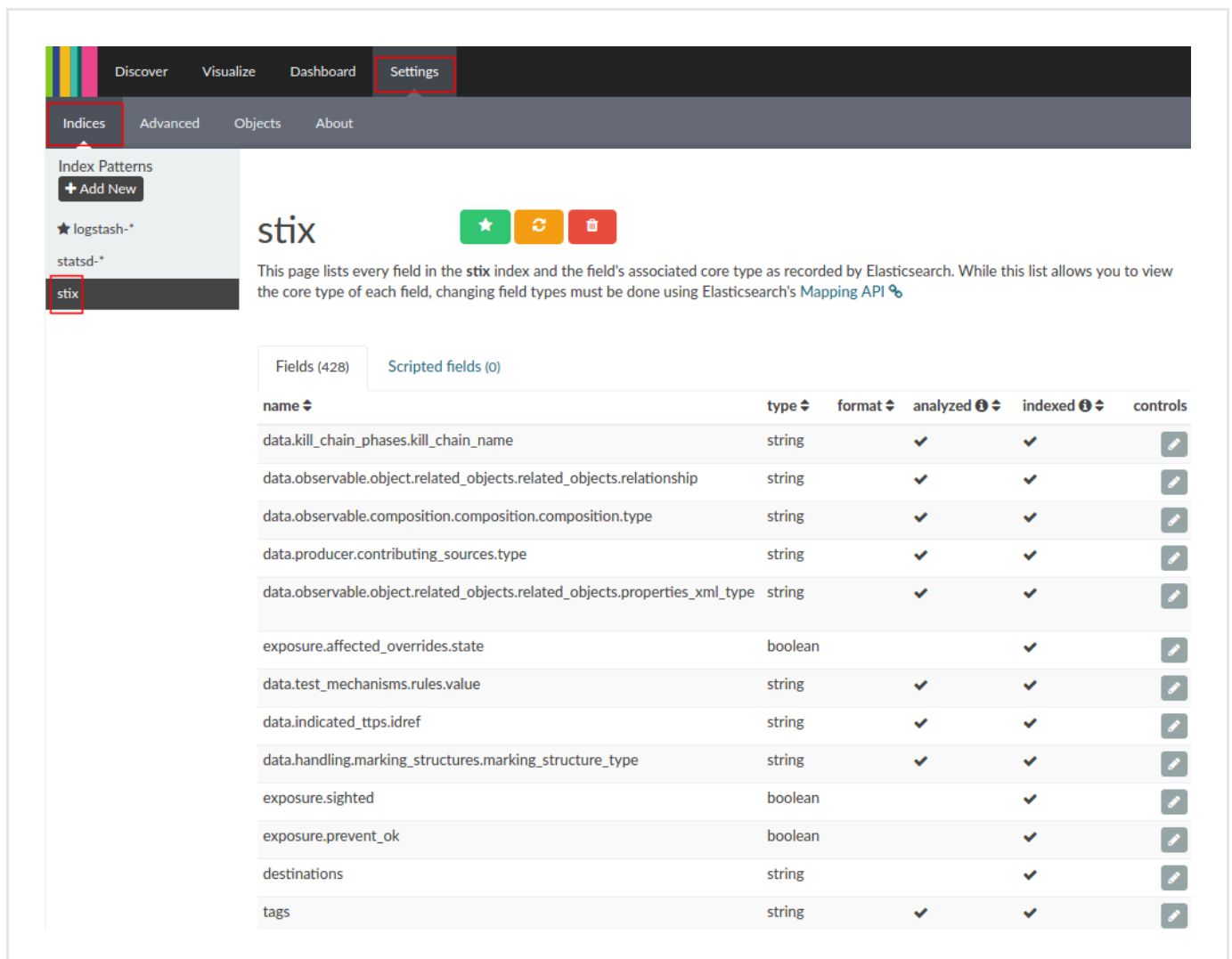
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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.

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 VirusTotal enricher

This article describes how to configure the VirusTotal enricher parameters.

To configure the general options for the VirusTotal enricher, see [Configure enrichers](#).

VirusTotal enricher	
Enricher name	VirusTotal
API endpoint	<code>https://www.virustotal.com/vtapi/v2/{}</code>
Input	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Output	Enriches the submitted entity observables with maliciousness confidence level information.
Description	Polls data from the VirusTotal API. It provides information on malware, domains (passive DNS) and IP addresses. Submitted data is checked against 60+ antimalware products, resulting in a detection ratio output and additional metadata information, when available.

Configure the VirusTotal 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 VirusTotal enricher:

- **API key: sign up** (<https://www.virustotal.com/en/documentation/public-api/#getting-started>) to the VirusTotal community to automatically be assigned a personal API key to access the VirusTotal public API, and then enter it in this field.
- **Scan URLs:** select this checkbox to to **submit URLs** (<https://www.virustotal.com/en/documentation/public-api/#scanning-urls>) to VirusTotal.
- **Scan files:** select this checkbox to to **submit files/file hashes** (<https://www.virustotal.com/en/documentation/public-api/#scanning-files>) to VirusTotal. File hashes are embedded inside entities as raw artifacts.
- **Max low confidence infection rate:** you can set an *upper threshold* to automatically flag enriched observables with a *low confidence* value.
After completing the sample analysis, enriched observables with a *lower* detection ratio than the specified value are flagged with **Malicious - Low confidence**.
 - Enter a numeric value between 0.1 and 0.9 — that is, $0 < value < 1$.
 - Default value: 0.2.
- **Min high confidence infection rate:** you can set a *bottom threshold* to automatically flag enriched observables with *high confidence* value.
After completing the sample analysis, enriched observables with a *higher* detection ratio than the specified value are flagged with **Malicious - High confidence**.
 - Enter a numeric value between 0.1 and 0.9 — that is, $0 < value < 1$.
 - Default value: 0.5.
- Enriched observables with a detection ratio falling in the range defined by **Max low confidence infection rate** (range lower limit) and **Min high confidence infection rate** (range upper limit) are flagged with **Malicious - Medium confidence**.
- 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 table view by column. 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.

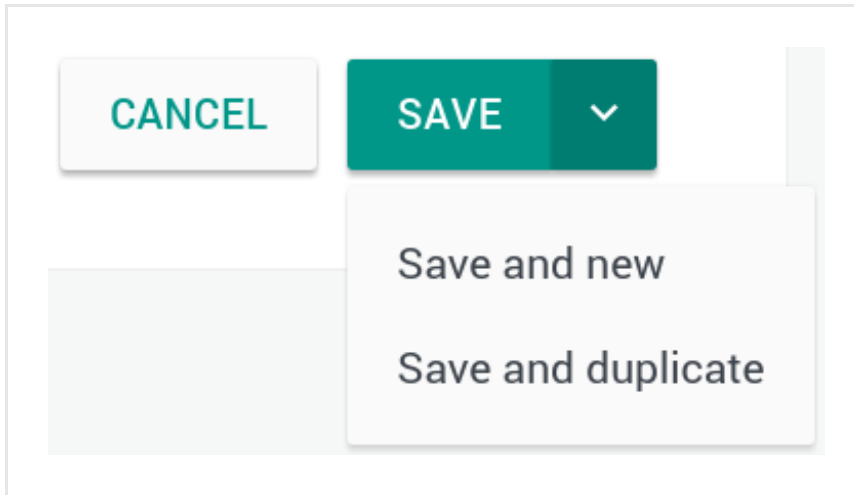
On the **Rules** > **Enrichment** > **Create** page, fill out the fields to create the new enricher rule:

- **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 table view by column. 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 dotted menu 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 GeolP 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 table view by column. 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 dotted menu 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 dotted menu 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...' interface. At the top, there is a teal header bar with the title and a close button. Below the header, a status bar shows 'Ingested: 01/24/2017 12:14 AM', 'Group: Testing Group', 'Author: Tes...', and a 'TLP None' button. The main content area has tabs for 'OVERVIEW', 'OBSERVABLES', 'NEIGHBORHOOD', 'JSON', 'VERSIONS', and 'HISTORY'. The 'OBSERVABLES' tab is selected. On the left, a red box highlights the 'Enrich' dropdown menu, which is open, showing options: 'Enrich', 'Enrich all observables', 'Enrich selected observables', 'Elastic Sightings Enricher', and 'OpenResolve'. To the right of the dropdown is a button labeled 'ADD OBSERVABLE'. Below the dropdown, there is a table with columns: 'Origin', 'Maliciousness', 'Date', 'Lv', 'Conn', 'Origins', and 'Created'. The 'Created' column has a refresh icon (a circular arrow) highlighted with a red box. The table shows two rows of data, both labeled 'Enrichment (1)' and '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

OVERVIEWOBSERVABLESNEIGHBORHOODJSONVERSIONSHISTORY

Enrich




ADD OBSERVABLE



Enrich all observables




Enrich selected observables




Elastic Sightings Enricher

OpenResolve

OriginMaliciousnessDate

LvConnOriginsCreated

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://zebbugtennis.com/wp-conte...> ×

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

○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
Origin ▼
Maliciousness ▼
Date ▼

Enrich selected observables (6)

Elastic Sightings Enricher
⏪
Enrichment (1)
●
7 days ago
⋮

OpenResolve
⏪
Enrichment (2)
●
7 days ago
⋮

			Lv	Conn	Origins	Created	⌂	
<input checked="" type="checkbox"/>	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 VirusTotal enricher can take the following observable types as input:

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

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 VirusTotal.

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

Review enrichment observables on the graph

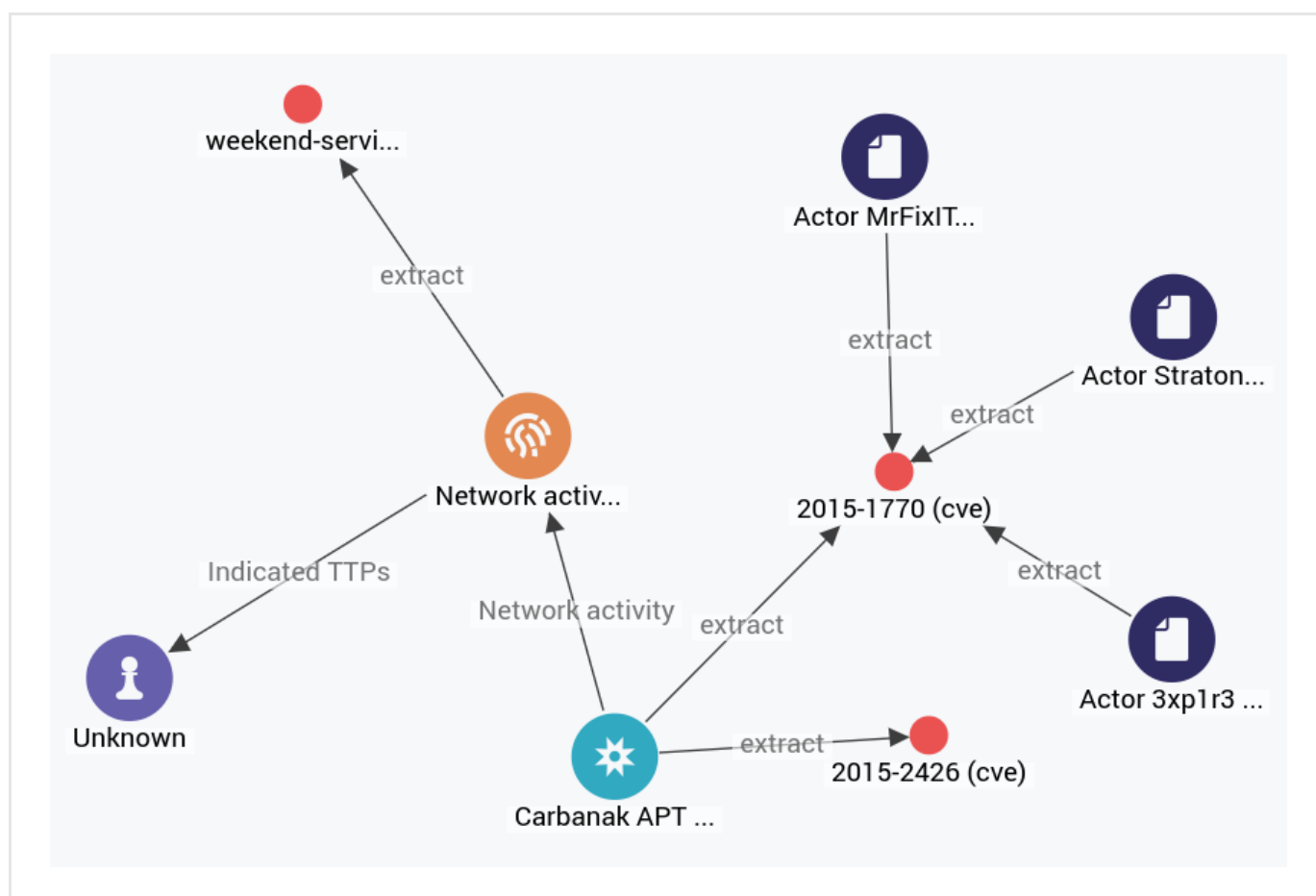
To view enrichment data and their connections with other entities and observables on the graph, do the following:

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

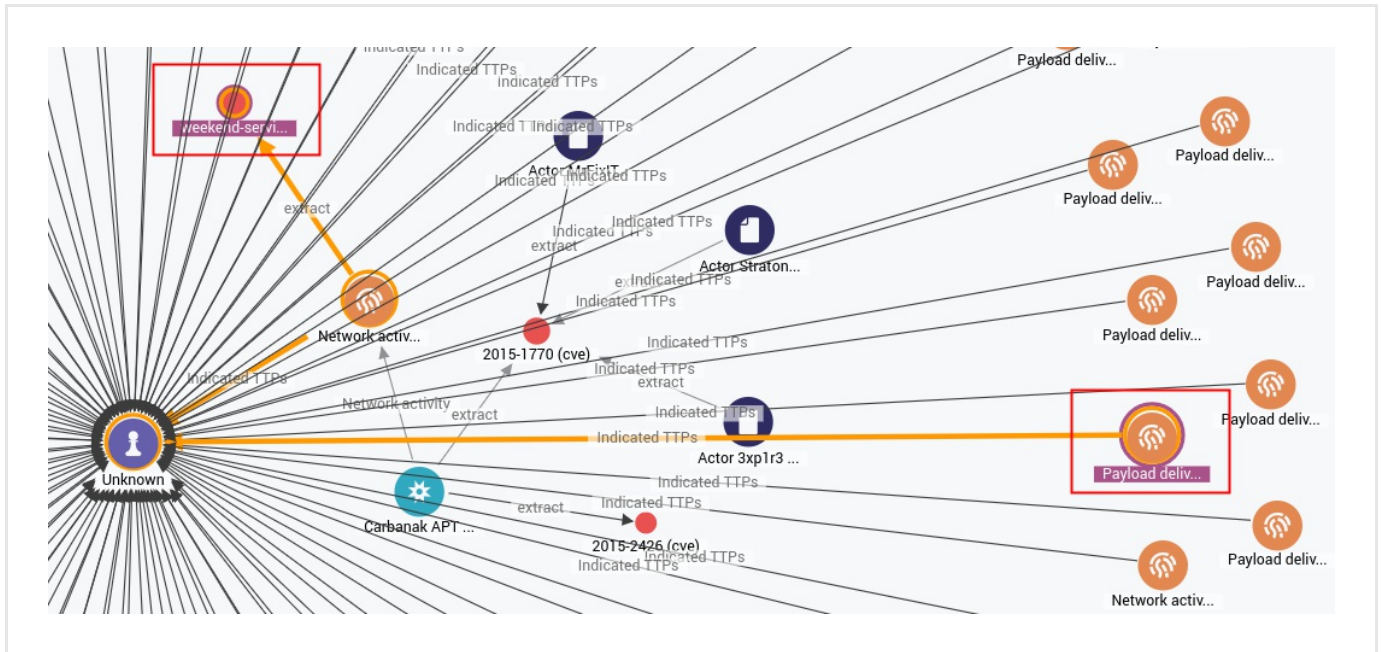
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

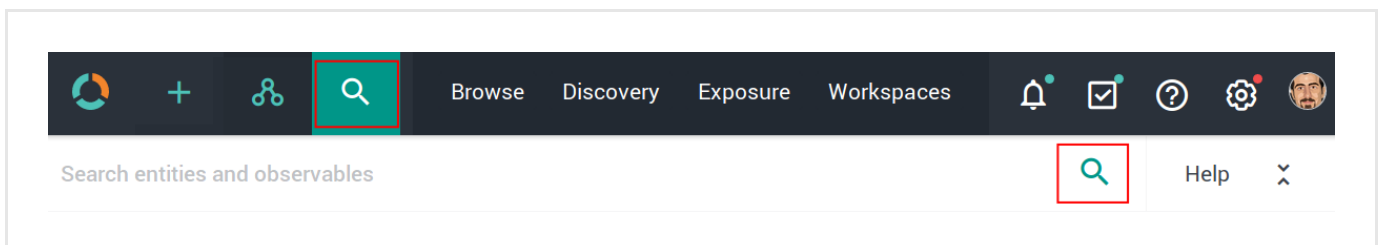


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



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.

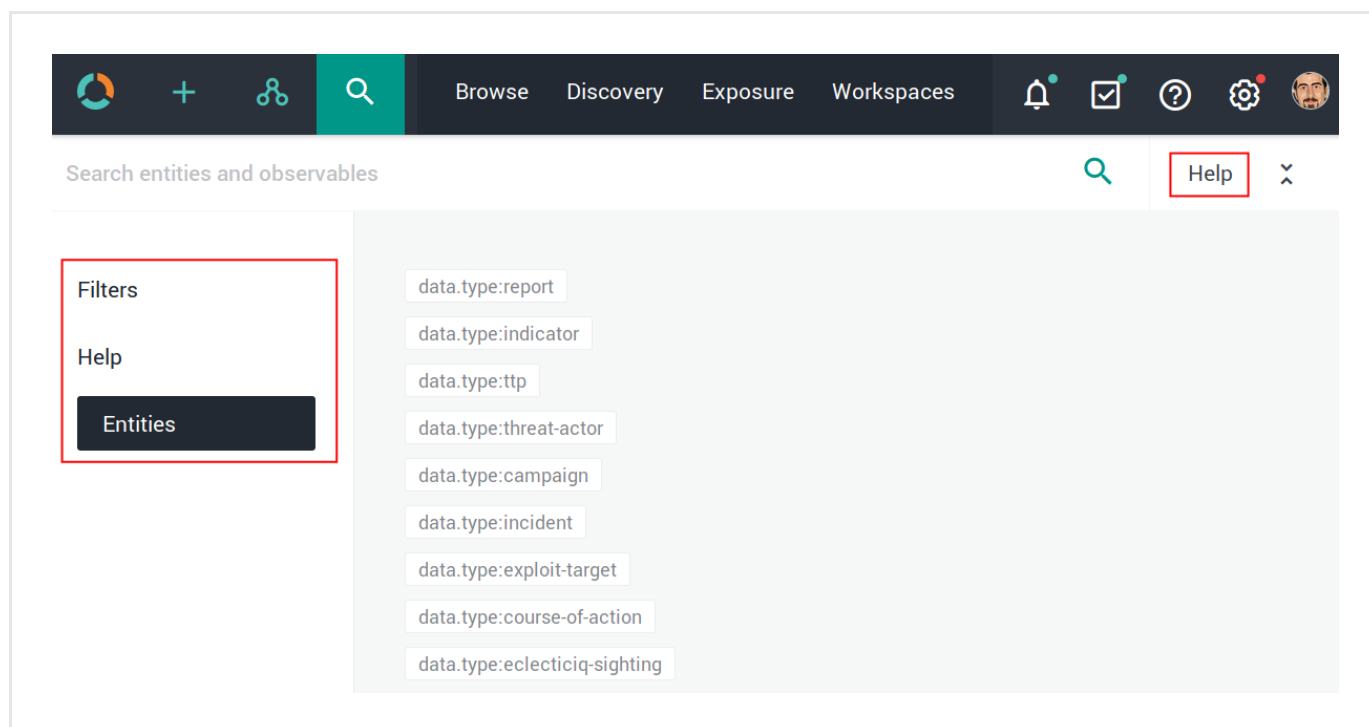


The search functionality uses **Elasticsearch query syntax**

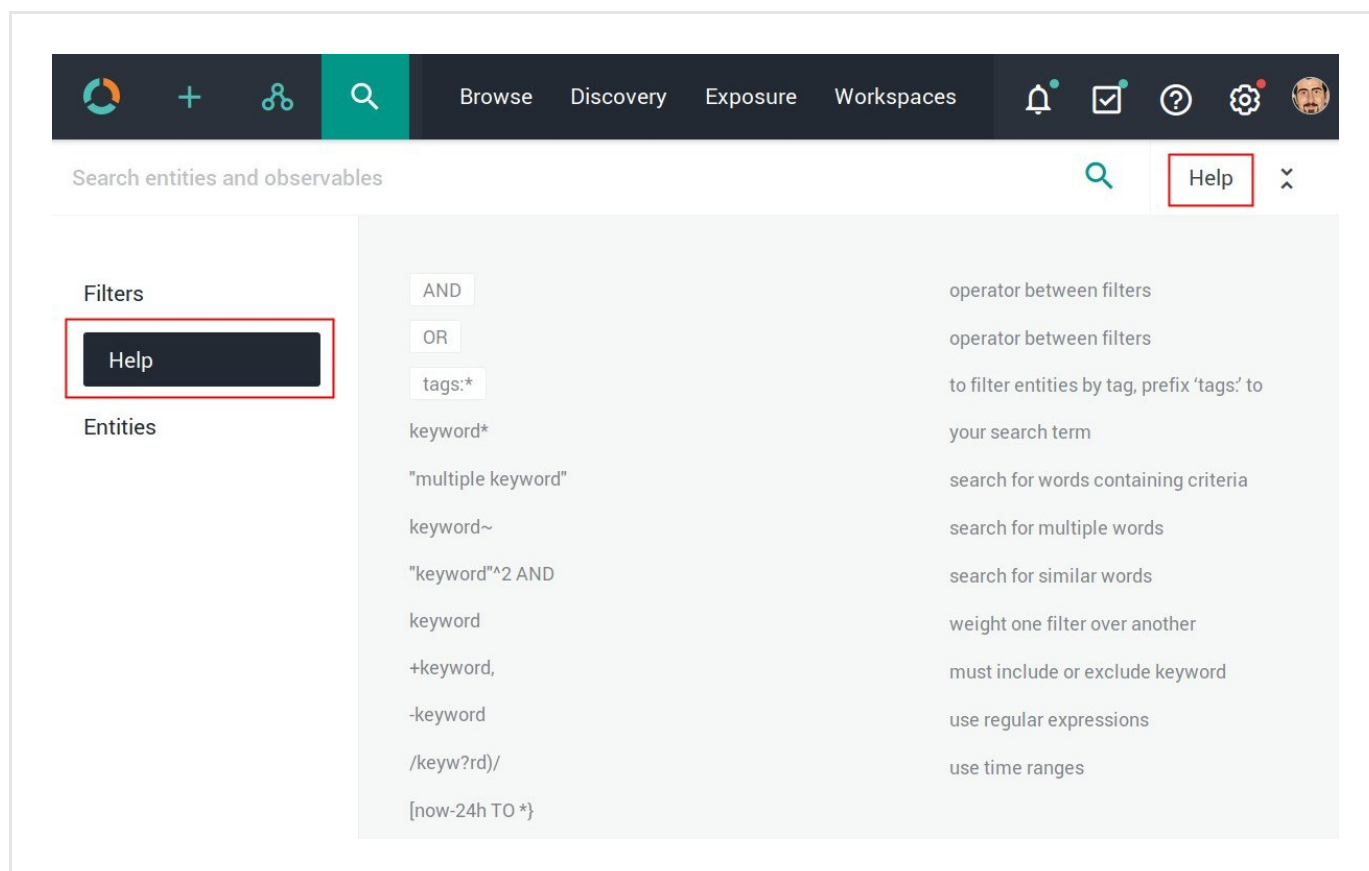
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

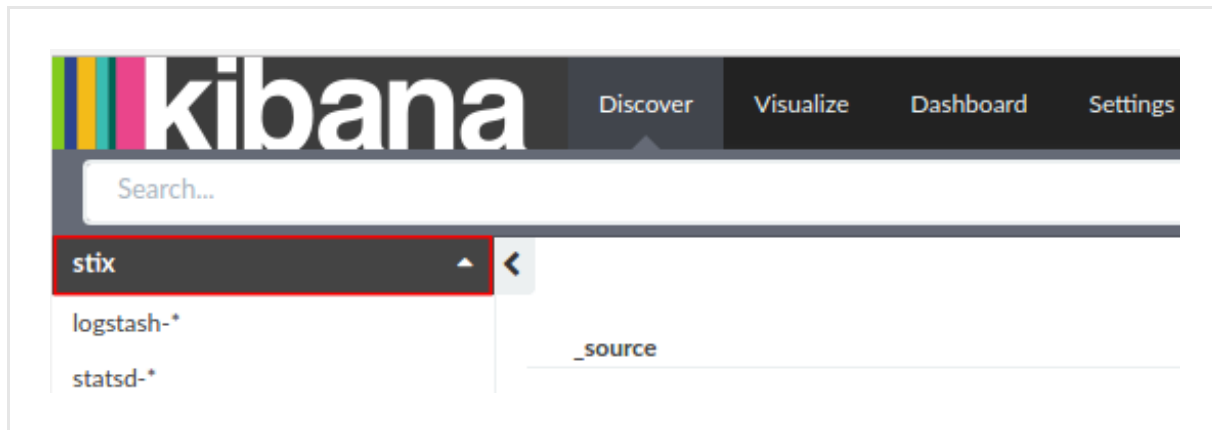
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

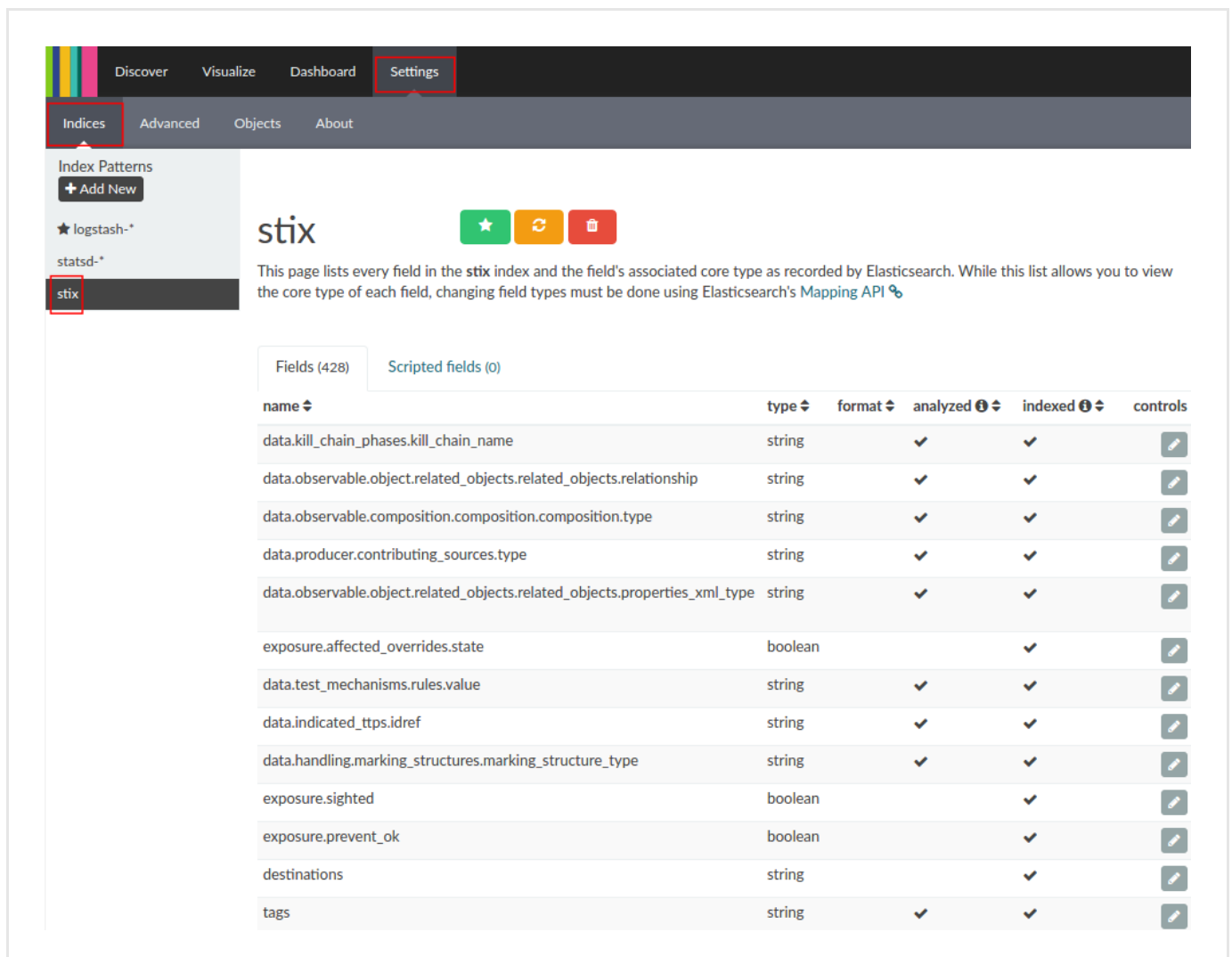
Keep the trailing /.

Example: <https://platform.host.com/api/kibana/app/kibana#/>

- Select the **stix** index field:



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



Last generated on May 26, 2017

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	Information
Elasticsearch sightings	<code>http://<elasticsearch_url>:9200/<schema_resource></code>	Searches an external Elasticsearch index. Criteria are processed to automatically generate sightings.
Fox-IT InTELL Portal	<code>https://cybercrime-portal.fox-it.com/</code>	Based on Fox-IT InTELL, the platform provides a range of sources like forums and social media to identify suspicious activity.
Intel 471	<code>https://api.intel471.com/v1/</code>	Besides data on compromised IP addresses, Intel 471 focuses on providing information about individuals and groups.
OpenDNS OpenResolve	<code>http://api.openresolve.com/{}/{}></code>	OpenResolve by OpenDNS offers a service to retrieve reverse-DNS lookup information.
PyDat	<code>http://10.0.1.60:8000/ (example)</code>	PyDat (https://github.com/mitre-internal/pydat) is a Python library that can work together with Elasticsearch to provide passive DNS lookup information, including organization, country, city, street, and more.
RIPEstat GeoIP	<code>https://stat.ripe.net/data/geoloc/data.json?resource={IP_address}</code>	Geolocation IP information from RIPEstat API (https://stat.ripe.net) including longitude, country, and city.
RIPEstat Whois	<code>https://stat.ripe.net/data/whois/data.json?resource={IP_address}</code>	Whois information from the RIPEstat API (https://github.com/ripe/ripestat-api) including inet number, name, or telephone.

Enricher	API endpoint	Information
Cisco AMP Threat Grid	https://panacea.threatgrid.com/api/v2/	Polls data from the Cisco AMP Threat Grid a range of cyber threat data like network streams, and hash files
VirusTotal	https://www.virustotal.com/vtapi/v2/{ }	Polls data from the VirusTotal API domains (passive DNS) and IP addresses against 60+ antimalware products and additional metadata information.
Flashpoint AggregINT	https://endlesstunnel.info/v3	Polls data from the Flashpoint AggregINT hosts, domains, IP addresses, and thematic datasets focusing on hacker groups, communities in conflict, CBRN (https://en.wikipedia.org/) produces enrichment observable user name of the author of a post, UTC date and time of a post in ISO (https://en.wikipedia.org/) (https://tools.ietf.org/html)
Flashpoint Blueprint	https://endlesstunnel.info/v3	Polls data from the Flashpoint Blueprint geolocation and IP ranges, as well as search thematic datasets focusing on supremacist groups, state actors (https://en.wikipedia.org/) enrichment observables like city latitude/longitude or IP address a hit, user name uniquely match
Flashpoint Thresher	https://endlesstunnel.info/v3	Polls data from the Flashpoint Thresher datasets focusing on hackers, threat CBRN (https://en.wikipedia.org/) produces enrichment observable
PassiveTotal Whois	https://api.passivetotal.org/v2	Polls data from the PassiveTotal (https://api.passivetotal.org/v2) (https://api.passivetotal.org/v2/getv2whoisquery). It provides associated with an IP address or details. Analysts can retrieve request telephone, and email details. They queries to obtain, for example, request same individual or the same corporation
PassiveTotal Passive DNS	https://api.passivetotal.org/v2	Polls data from the PassiveTotal (https://api.passivetotal.org/v2) (https://api.passivetotal.org/v2/getv2dnspassivequery). It provides cross-referencing IP addresses over time. Analysts can examine IP addresses over time. They can more domain names that may be

Enricher	API endpoint	Description
PassiveTotal IP/Domain	https://api.passivetotal.org/v2	<p>Polls data from the PassiveTotal (https://api.passivetotal.org/v2/enrichmentquery). It provides queried IP address or domain name, any sub-domains, inet details, and (ASN) (https://en.wikipedia.org/wiki/AS_(internet_routing)) as well as geolocation information. It also looks for further connections that</p>
PassiveTotal Malware	https://api.passivetotal.org/v2	<p>Polls data from the PassiveTotal (https://api.passivetotal.org/v2/enrichmentmalwarequery) to the queried host or domain, sha1, hash-sha256, hash-sha512. Malware entries are also tagged with enrichment_extracts.meta.category. Set the value you set under Rules > as malicious; enrichment_extracts.confidence corresponds to the value you set under Confidence > Malicious - Low</p>
Splunk sightings	http://10.0.1.22:8089/ (example)	Based on the search queries defined in the platform, it matches data in the specified Splunk index and saved to the platform as sightings.
DomainTools Hosted Domains	http://api.domaintools.com/v1/{}/host-domains	Enriches IPv4 observables by related domains and therefore related to, the input IP address.
DomainTools Reputation	http://api.domaintools.com/v1/reputation	Enriches domain and host name information to assess maliciousness based on defined threshold values.
DomainTools Suspicious Domains	https://api.domaintools.com/v1/{}/host-domains	Enriches IPv4 observables with related domains and addresses. It includes configuration and confidence levels to the process of identifying malicious IPs.
FireEye		Enriches platform observables with related fields such as critical infrastructure, hacktivism, frauds, and vulnerabilities.
Recorded Future	https://app.recordedfuture.com/live/sc/entity/{}	The enricher returns additional context, related addresses, and hashes related to the specified types, as well as maliciousness and retrieved risk scores.

Enricher	API endpoint	
Unshorten-URL	<code>https://unshorten.me/s/{}</code>	It takes shortened URL as an input and returns resolved original URLs, which can be used to discover relationships with other entities.
Farsight DNSDB	<code>https://api.dnsdb.info/{}</code>	Historical passive DNS lookup endpoint pointing to a specified IP address. Returns nameserver, domain names pointing to the IP address, and domains existing below a parent domain.

Work with the Elasticsearch sightings enricher

This article describes how to configure the Elasticsearch sightings enricher parameters.

To configure the general options for the Elasticsearch sightings enricher, see [Configure enrichers](#).

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

Configure the enricher

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

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

Alternatively:

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

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

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

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

- **ElasticSearch URL:** enter the URL pointing to the external Elasticsearch instance you want to use as a source for the enricher, including the sub-resource pointing to the **data mapping schema** (<https://www.elastic.co/guide/en/elasticsearch/guide/current/mapping-intro.html>).
Example: *http://localhost:9200/default*
In a usage scenario, you may want to obtain data from an external Elasticsearch instance that acts as a centralized log aggregator to check for correlations with the platform observables, indicators, and other entities. If it is possible to establish a relationship between Elasticsearch data and a platform entity, a sighting is automatically created.
- **Username:** valid user name credentials to authenticate and receive authorization to access the resource(s). For example, *nigeltufnel*.
- **Password:** valid password credentials to authenticate and receive authorization to access the resource(s). For example, *s3cr3tp@SSw0rd_*.
- **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. The supported extract types are:
ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512
 - In the second input field, specify the *observable value* associated to the observable type. You can use free text, wildcards, as well as **Elasticsearch query syntax** (<https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html>).
- 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 table view by column. 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:

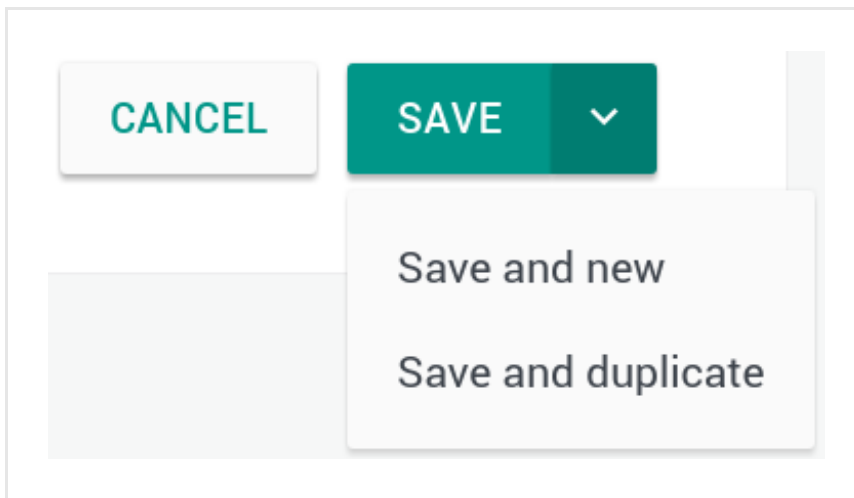
- **Name**: define a name to identify the rule. It should be descriptive and easy to remember.
- **Description**: additional textual details. If you want, you can add a short description to provide more information and context.
- Click **+ Add** or **+ More** to add a filtering option.
- **Source**: 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 table view by column. 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 dotted menu 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 table view by column. 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 dotted menu 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 dotted menu 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

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 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://zebbugtennis.com/wp-conte...> ×

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

○ TLP White

OVERVIEW
OBSERVABLES
NEIGHBORHOOD
JSON
VERSIONS
HISTORY

Enrich
▼

Enrich all observables
▼

Enrich selected observables (6)

Elastic Sightings Enricher
▼

OpenResolve
▼

	Origin ▼	Maliciousness ▼	Date ▼
	Lv	Conn	Origins
			Created ▼ ↻
	←	Enrichment (1)	7 days ago
	←	Enrichment (2)	7 days ago
<input checked="" type="checkbox"/> 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 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

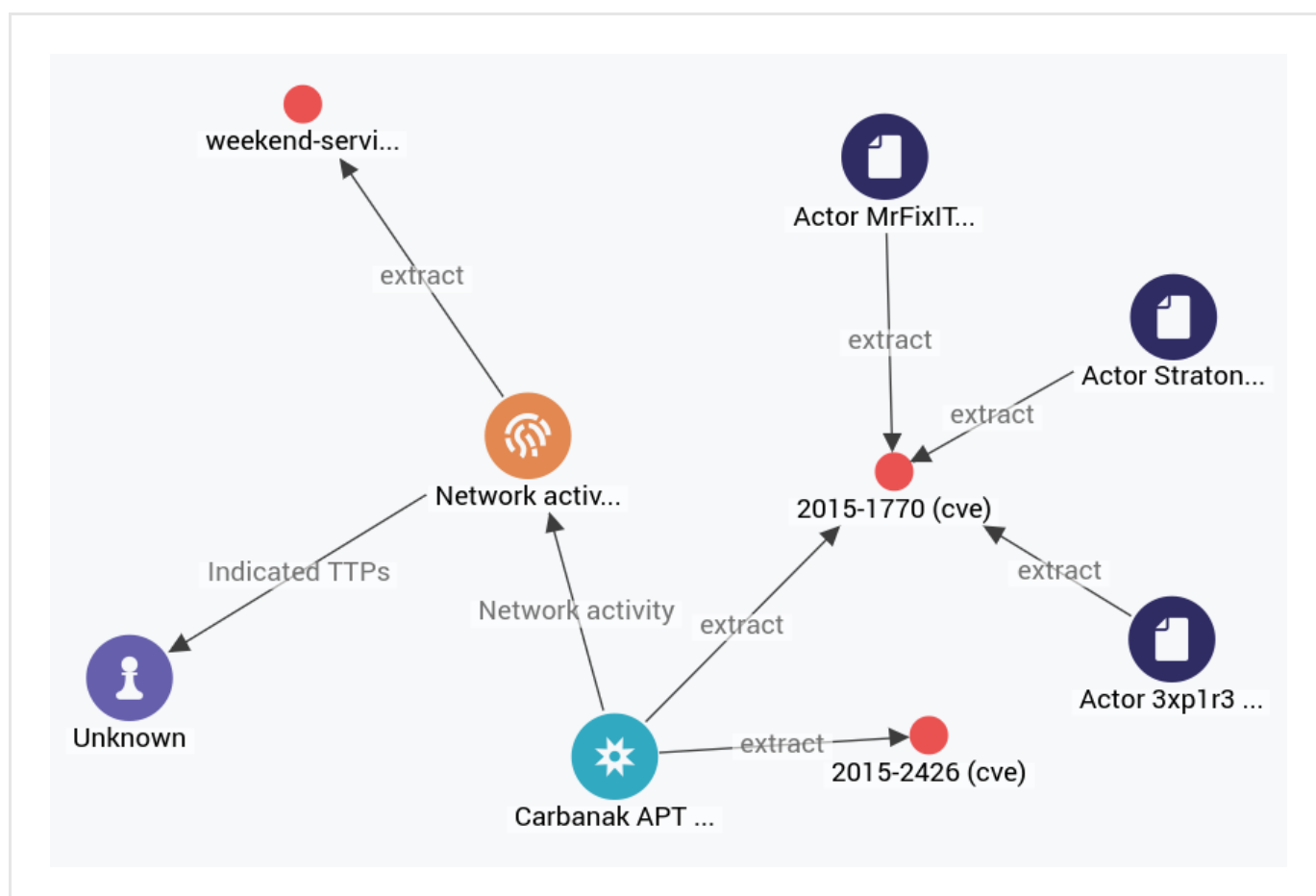
Date

<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	

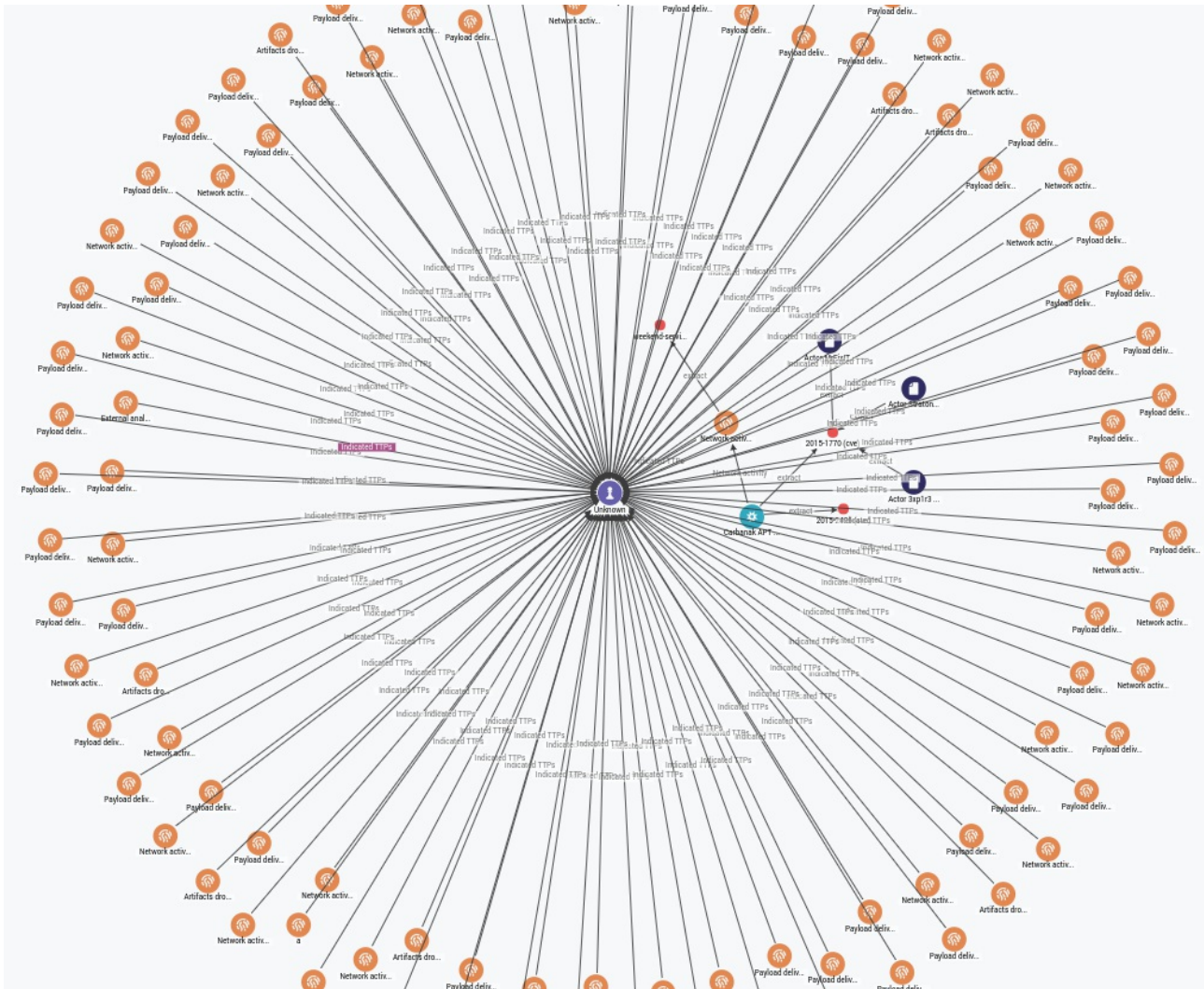
<input type="checkbox"/>	KIND	VALUE	ORIGIN	CREATED	
<input type="checkbox"/>	domain	www.thestar.com.my	2	a month ago	<div>⋮</div>
<input type="checkbox"/>	uri	http://www.thestar.com.my/New...	2		
<input type="checkbox"/>	country	my	2		
<input type="checkbox"/>	uri	notes:the	2		
<input type="checkbox"/>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

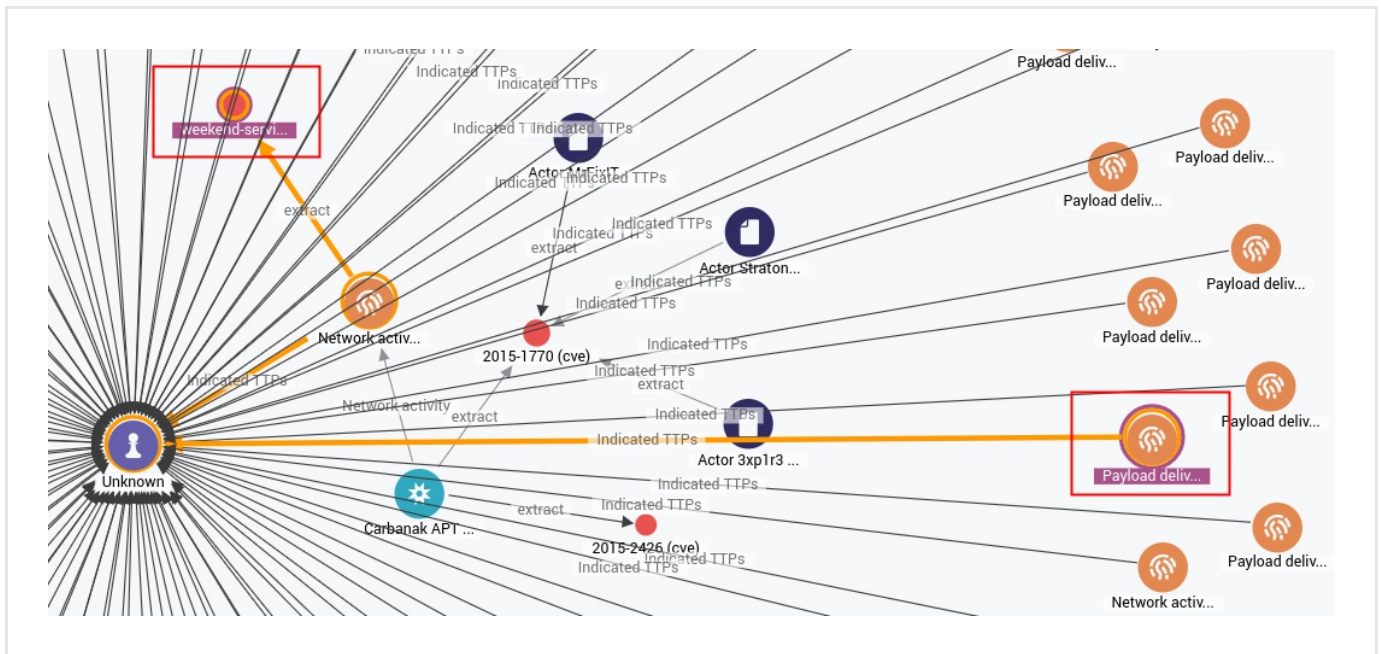


- Right-click an extract or an entity for further inspection and from the context menu select **Load entities > All**, **Load observables > All** or **Load entities by extract > All**.



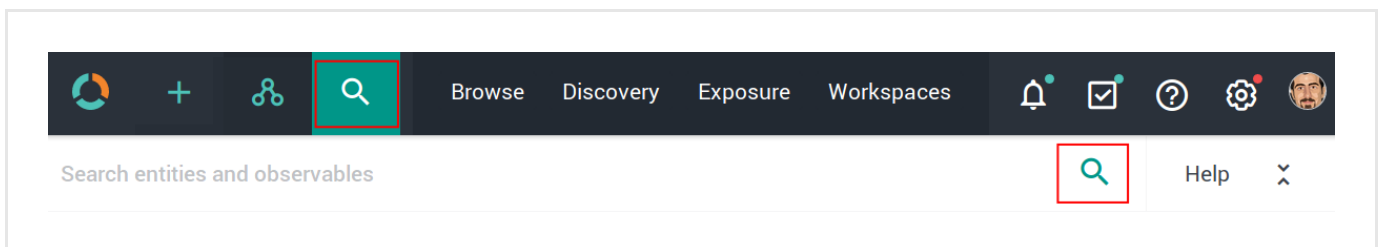
To see how entities, observables and enrichment observables are connected, and to inspect relationships between distant items, do the following:

- **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 any 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.

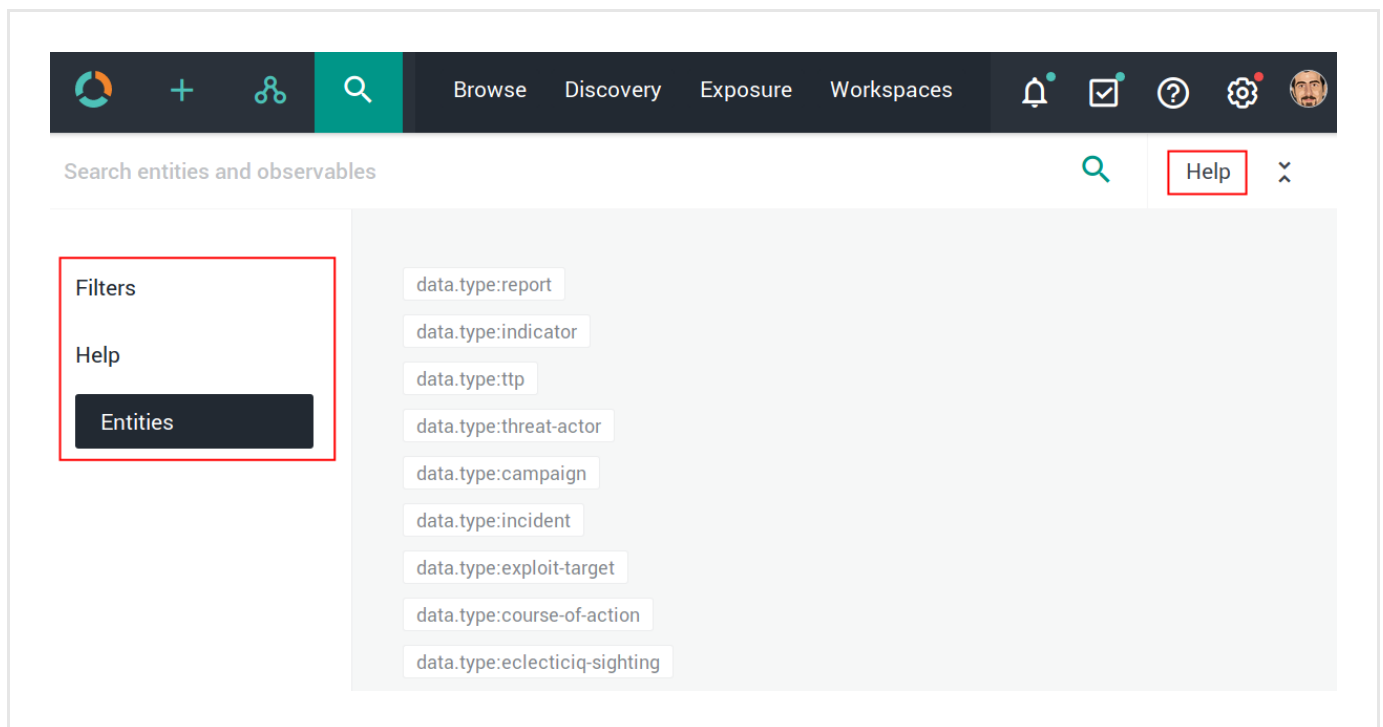


The search functionality uses **Elasticsearch query syntax**

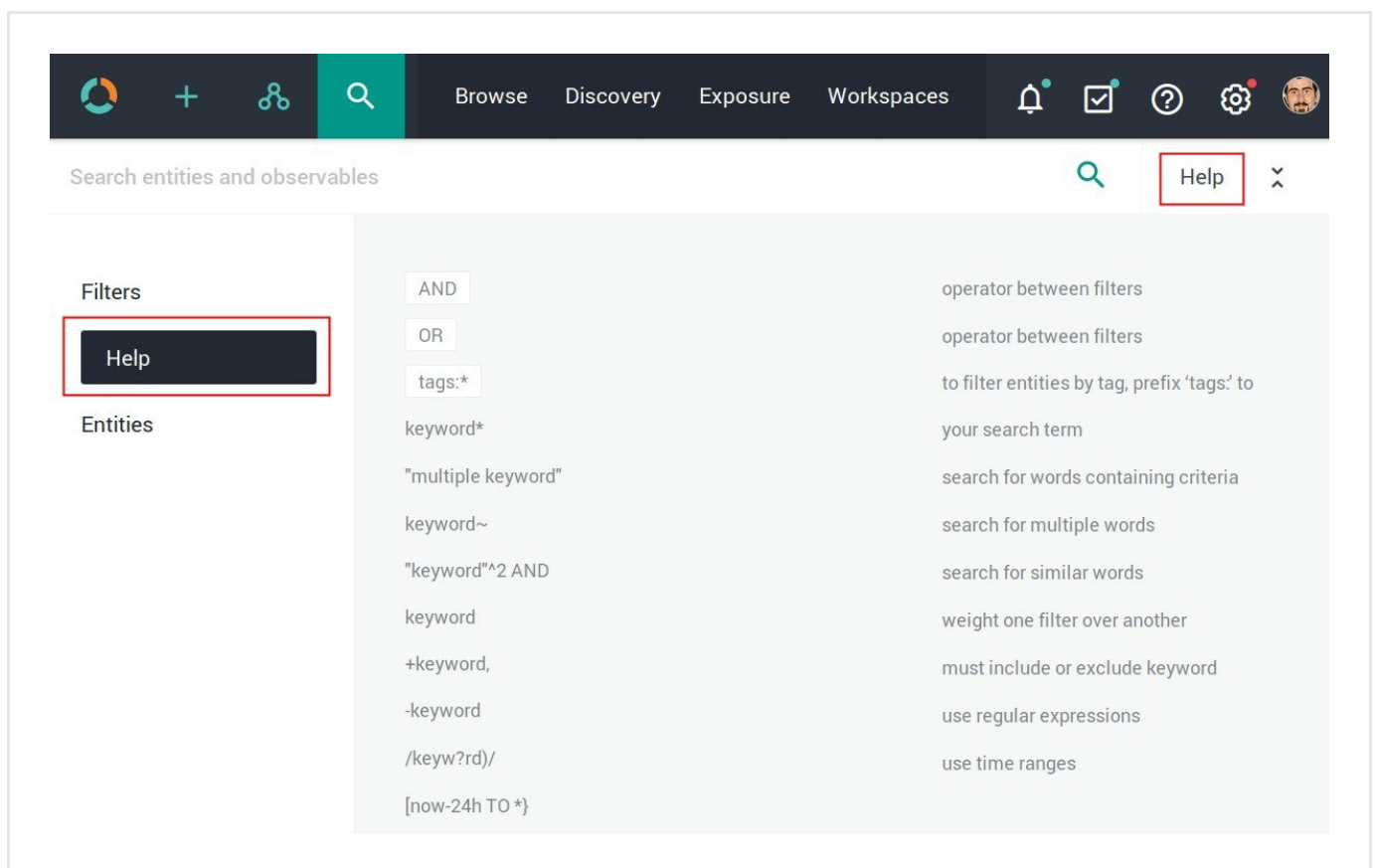
(<https://www.elastic.co/guide/en/elasticsearch/reference/current/full-text-queries.html>).

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 Rules by selecting appropriate options under Action and Confidence . 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 Rules by selecting the appropriate option under Action and Confidence . The selected action must be Mark as malicious for the Confidence drop-down list to become available. Allowed confidence metadata values are <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

Enricher	Supported kinds (observable types)
RIPEstat Whois	ipv4, ipv6
Cisco AMP Threat Grid	ipv4, ipv6, domain, host, uri, hash-md5, hash-sha1, hash-sha256, hash-sha512, winregistry
VirusTotal	ipv4, ipv6, domain, uri, hash-md5, hash-sha1, hash-sha256
Flashpoint AggregINT	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Blueprint	ipv4, ipv6, domain, host, uri, email, actor-id, hash-md5, hash-sha1, hash-sha256, hash-sha512
Flashpoint Thresher	ipv4, domain, host, uri, hash-sha1, file
PassiveTotal Whois	ipv4, ipv6, domain, host
PassiveTotal Passive DNS	ipv4, ipv6, domain, host
PassiveTotal IP/Domain	ipv4, ipv6, domain, host
PassiveTotal Malware	domain, host
Splunk sightings	domain, email, hash-md5, hash-sha1, hash-sha256, hash-sha512, host, ipv4, ipv6, uri
DomainTools Hosted Domains	ipv4
DomainTools Reputation	domain, host
DomainTools Suspicious Domains	ipv4
FireEye	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

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.

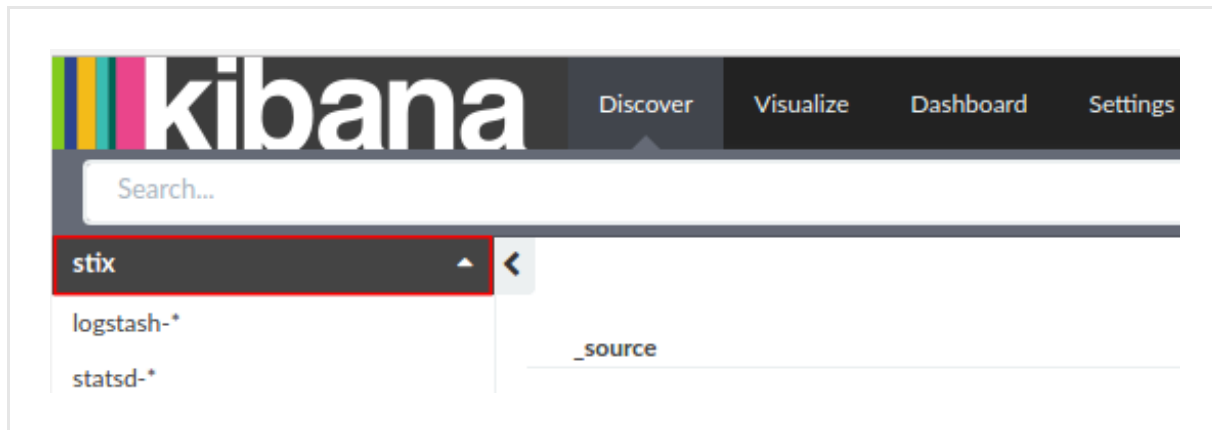
- To access Kibana, enter in the web browser address bar a URL with the following format:

<platform_host_name>/api/kibana/app/kibana#/.

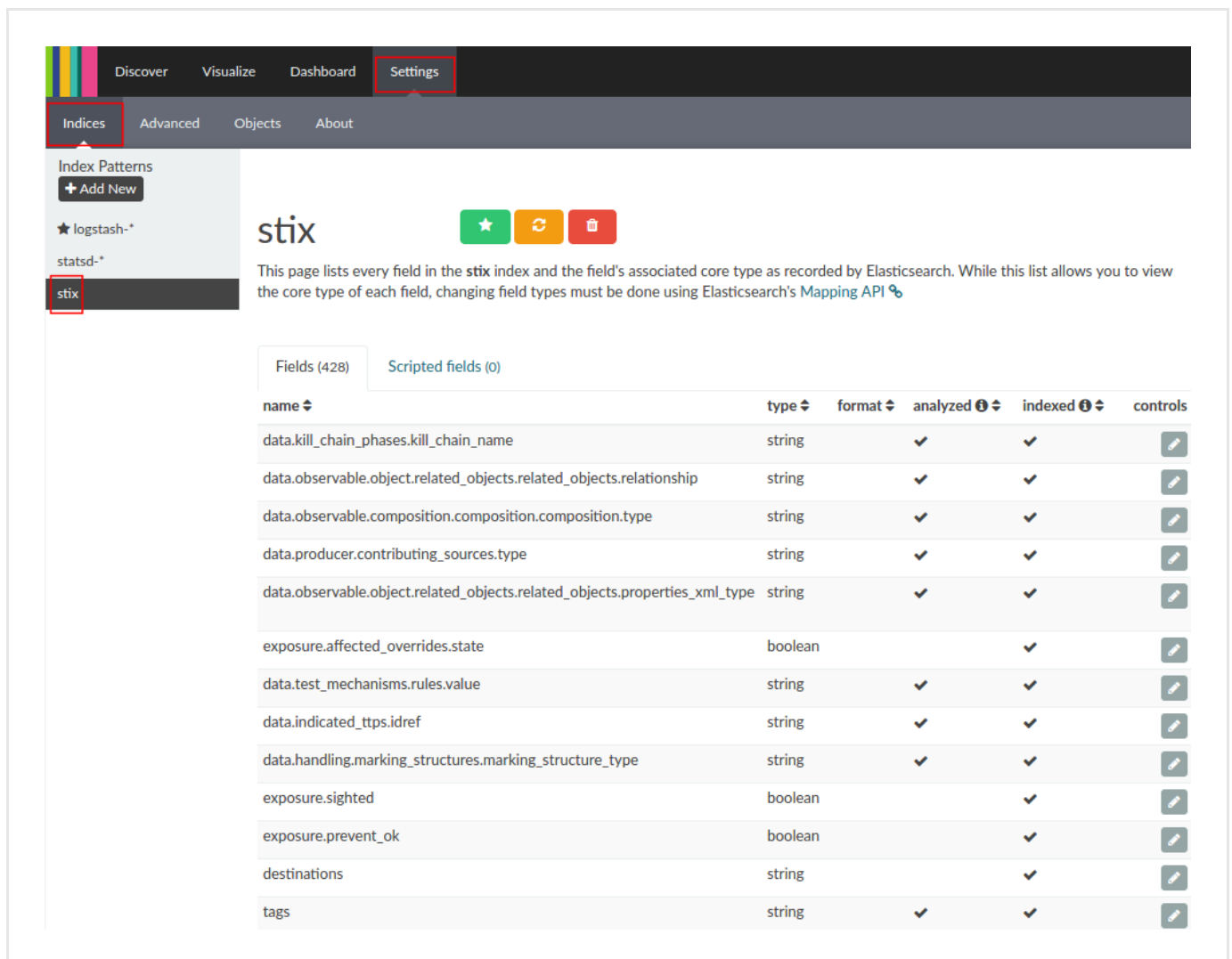
Keep the trailing /.

Example: [https://platform.host.com/api/kibana/app/kibana#/.](https://platform.host.com/api/kibana/app/kibana#/)

- Select the **stix** index field:



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



Last generated on May 26, 2017