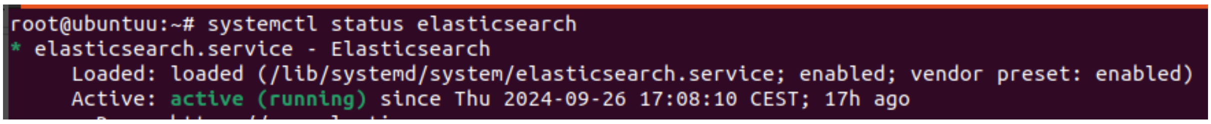
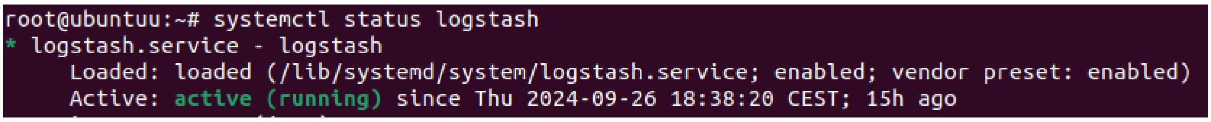
SIEM - Elk

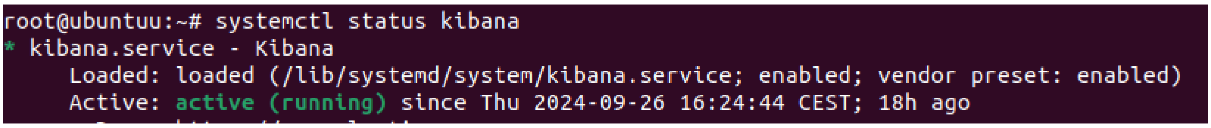
1. Install, start and enable Elasticsearch, Logstash and Kibana.



```
root@ubuntuu:~# systemctl status elasticsearch
* elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-09-26 17:08:10 CEST; 17h ago
```

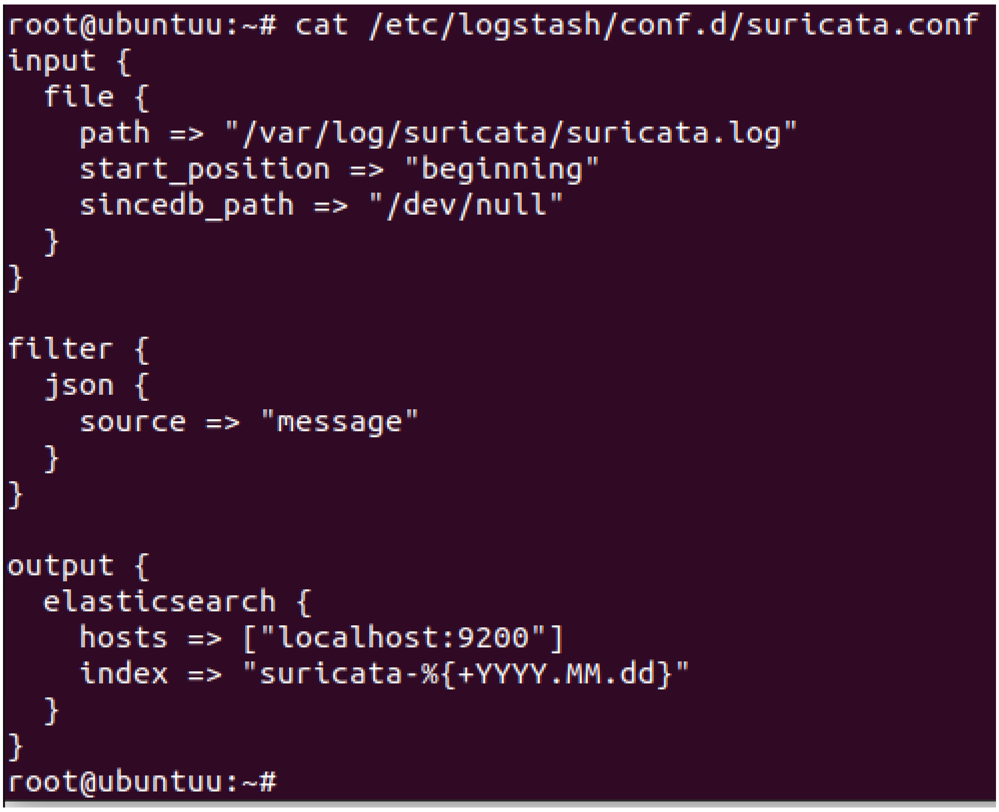


```
root@ubuntuu:~# systemctl status logstash
* logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-09-26 18:38:20 CEST; 15h ago
```

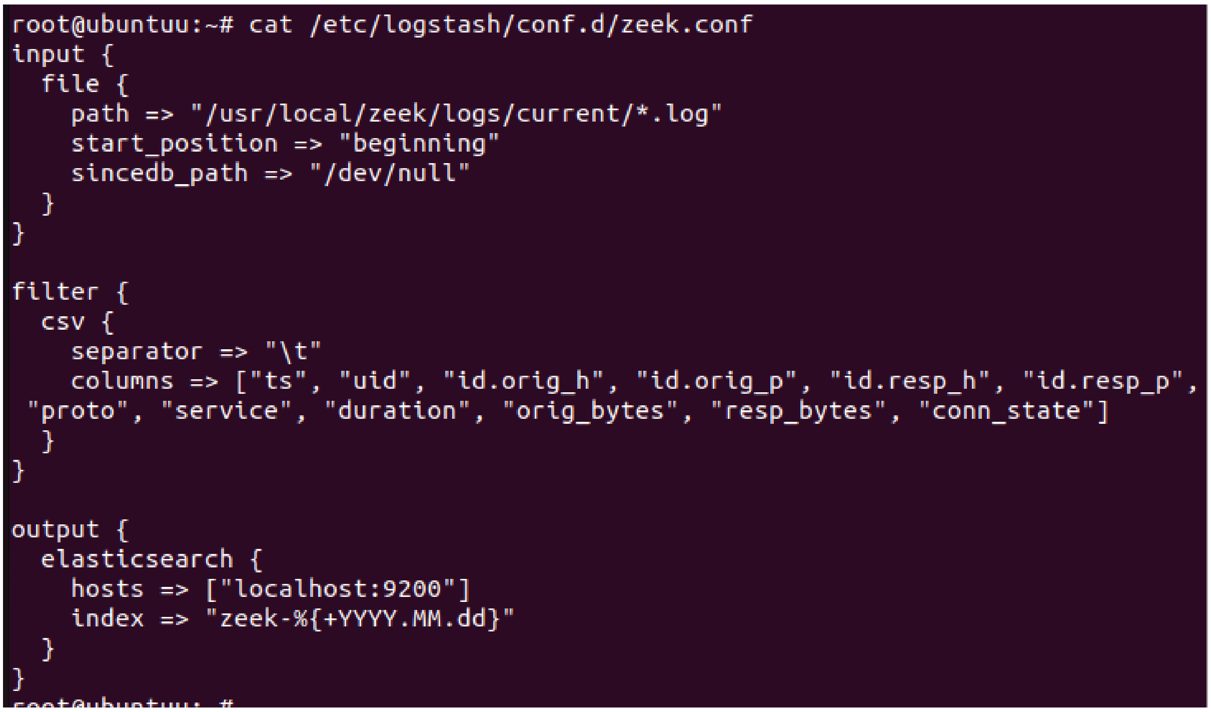


```
root@ubuntuu:~# systemctl status kibana
* kibana.service - Kibana
     Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-09-26 16:24:44 CEST; 18h ago
```

2. Create Logstash configuration files to parse logs from Suricata, Snort, and Zeek.

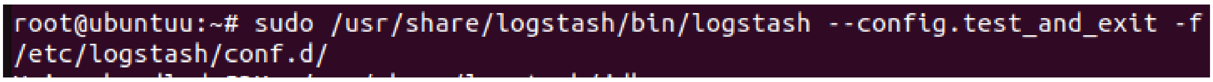


```
root@ubuntuu:~# cat /etc/logstash/conf.d/suricata.conf
input {
  file {
    path => "/var/log/suricata/suricata.log"
    start_position => "beginning"
    sincedb_path => "/dev/null"
  }
}

filter {
  json {
    source => "message"
  }
}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "suricata-%{+YYYY.MM.dd}"
  }
}
root@ubuntuu:~#
```

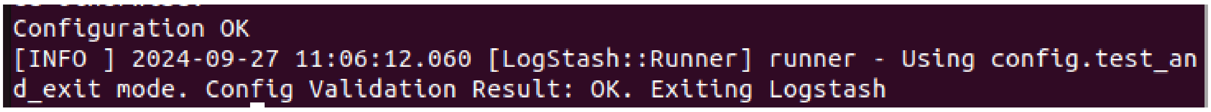


```
root@ubuntuu:~# cat /etc/logstash/conf.d/zeek.conf
input {
  file {
    path => "/usr/local/zeek/logs/current/*.log"
    start_position => "beginning"
    sincedb_path => "/dev/null"
  }
}

filter {
  csv {
    separator => "\t"
    columns => ["ts", "uid", "id.orig_h", "id.orig_p", "id.resp_h", "id.resp_p",
 "proto", "service", "duration", "orig_bytes", "resp_bytes", "conn_state"]
  }
}

output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "zeek-%{+YYYY.MM.dd}"
  }
}
root@ubuntuu:~#
```

3. Verify that Logstash is ingesting logs into Elasticsearch.

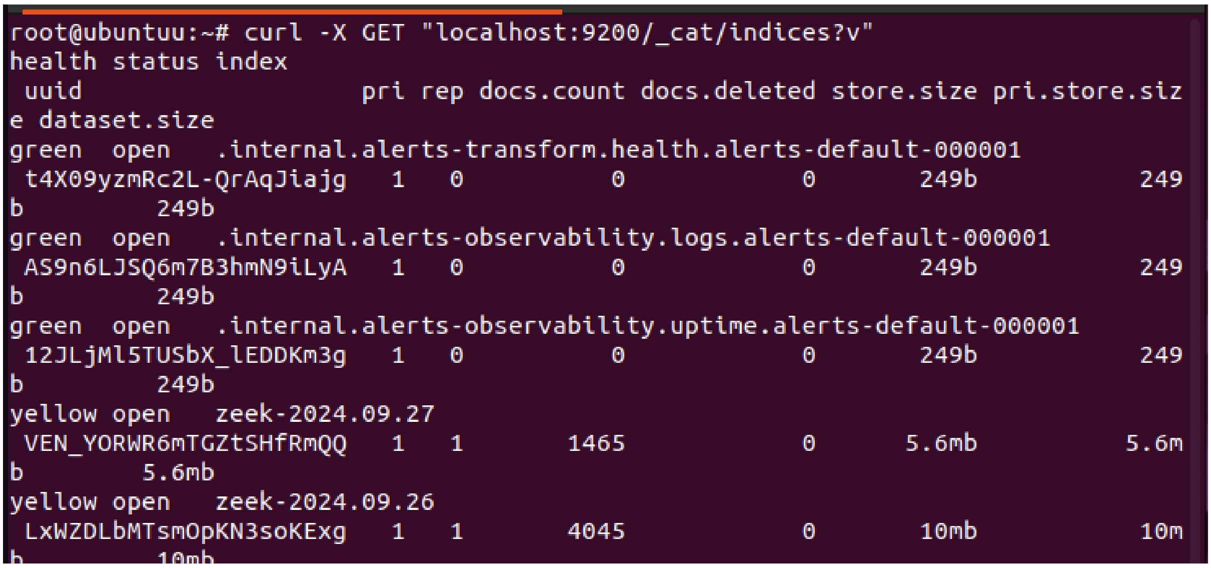
- 

```
root@ubuntuu:~# sudo /usr/share/logstash/bin/logstash --config.test_and_exit -f
/etc/logstash/conf.d/
```



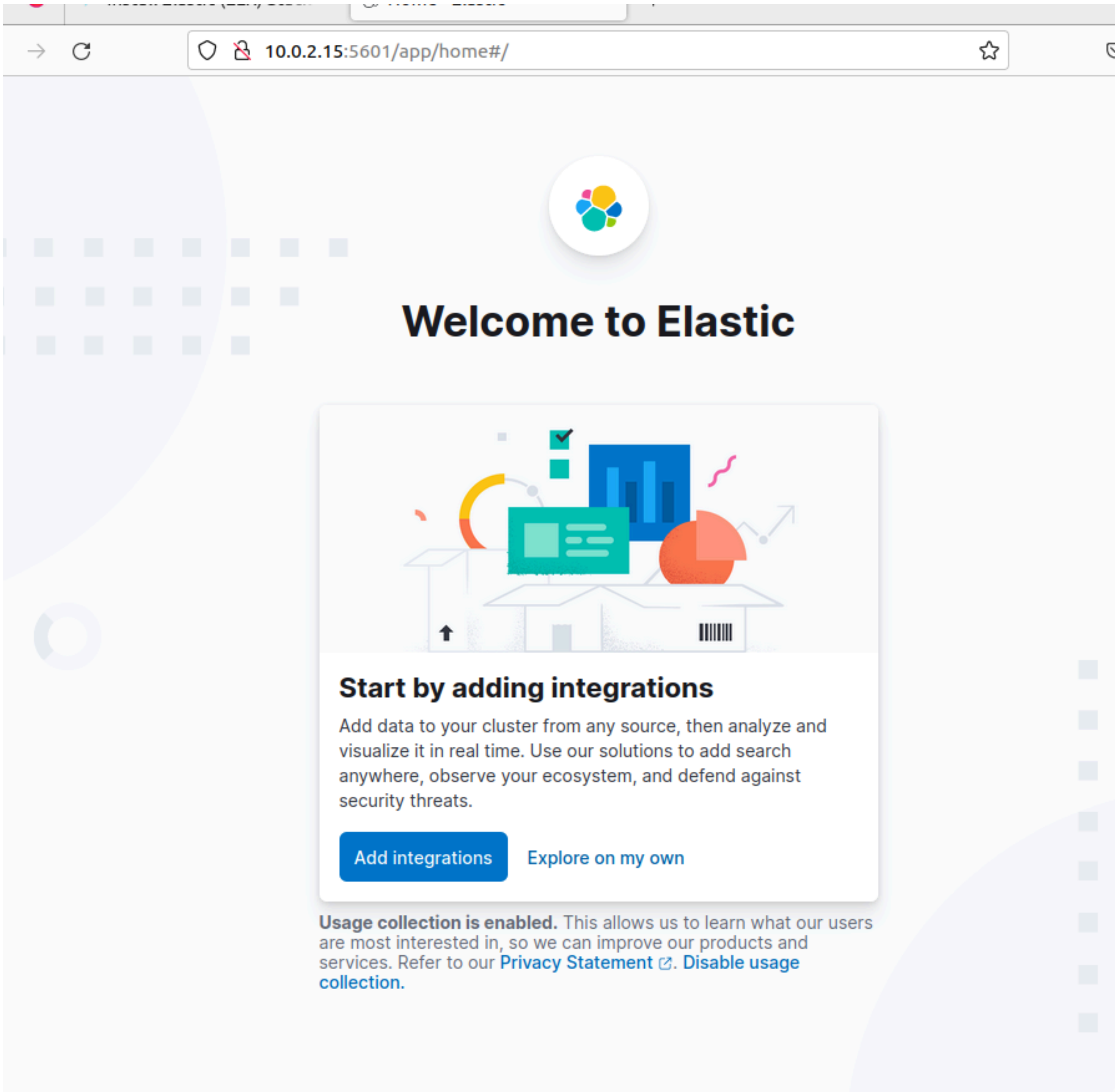
```
Configuration OK
[INFO ] 2024-09-27 11:06:12.060 [LogStash::Runner] runner - Using config.test_an
d_exit mode. Config Validation Result: OK. Exiting Logstash
```

- Sudo systemctl start logstash

- 

```
root@ubuntuu:~# curl -X GET "localhost:9200/_cat/indices?v"
health status index
 uuid                   pri rep docs.count docs.deleted store.size pri.store.siz
e dataset.size
green  open   .internal.alerts-transform.health.alerts-default-000001
 t4X09yzmRc2L-QrAqJiajg   1   0          0            0       249b           249
b         249b
green  open   .internal.alerts-observability.logs.alerts-default-000001
 AS9n6LJSQ6m7B3hmN9iLyA   1   0          0            0       249b           249
b         249b
green  open   .internal.alerts-observability.uptime.alerts-default-000001
 12JLjMl5TUSbX_lEDDKm3g   1   0          0            0       249b           249
b         249b
yellow open   zeek-2024.09.27
 VEN_YORWR6mTGZtSHfRmQQ   1   1       1465            0      5.6mb          5.6m
b        5.6mb
yellow open   zeek-2024.09.26
 LxWZDLbMTsmOpKN3soKExg   1   1       4045            0       10mb           10m
b         10mb
```

4. Access Kibana by navigating in a web browser.



Welcome to Elastic

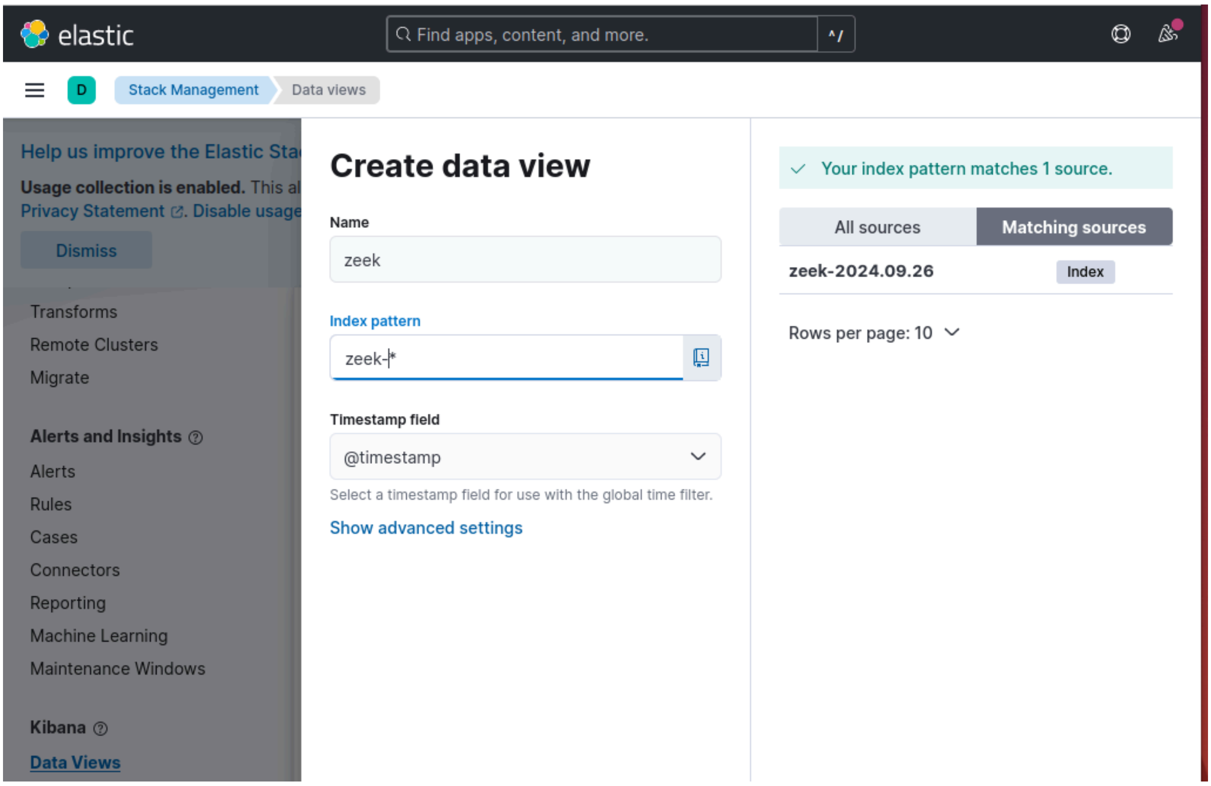
Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

Add integrations   Explore on my own

Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement. Disable usage collection.

5. Configure index patterns for Suricata, Snort, and Zeek logs.



Create data view

Name: zeek

Index pattern: zeek-*

Timestamp field: @timestamp

Select a timestamp field for use with the global time filter.

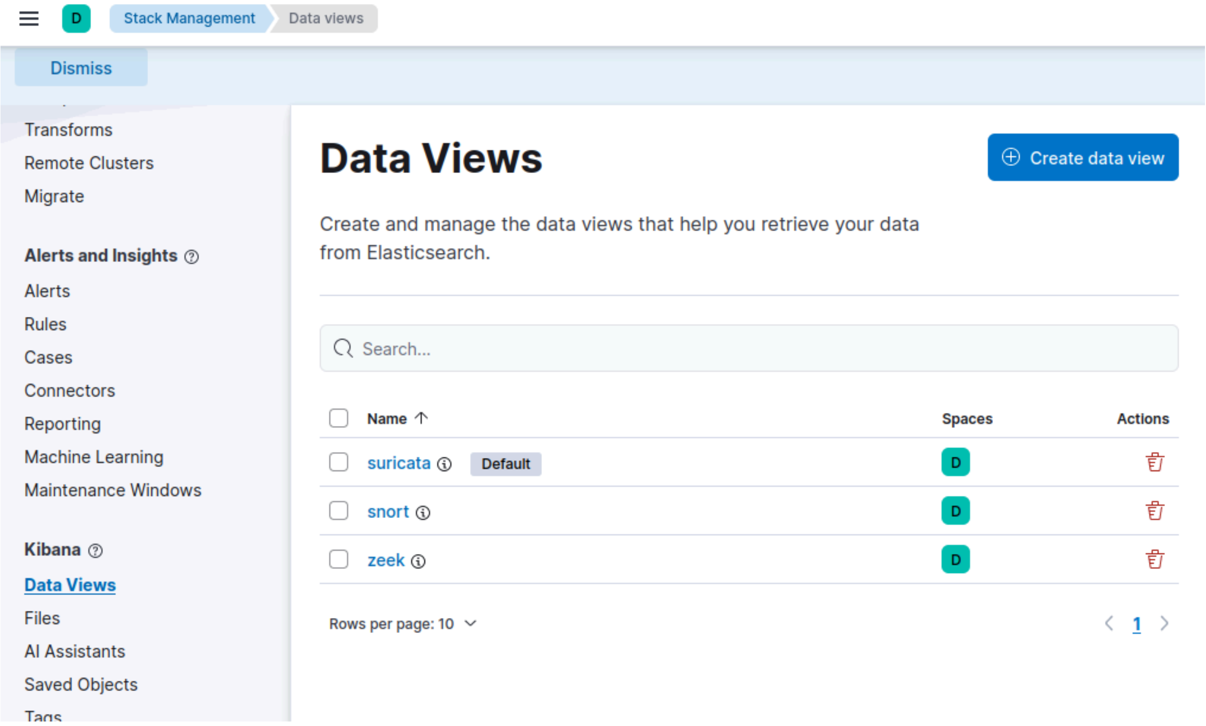
Show advanced settings

✓ Your index pattern matches 1 source.

All sources | Matching sources

zeek-2024.09.26 Index

Rows per page: 10



Data Views

Create data view

Create and manage the data views that help you retrieve your data from Elasticsearch.

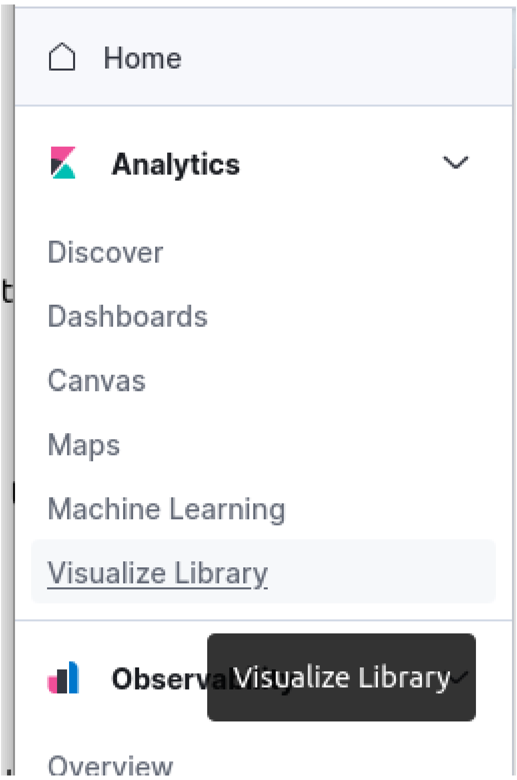
Search...

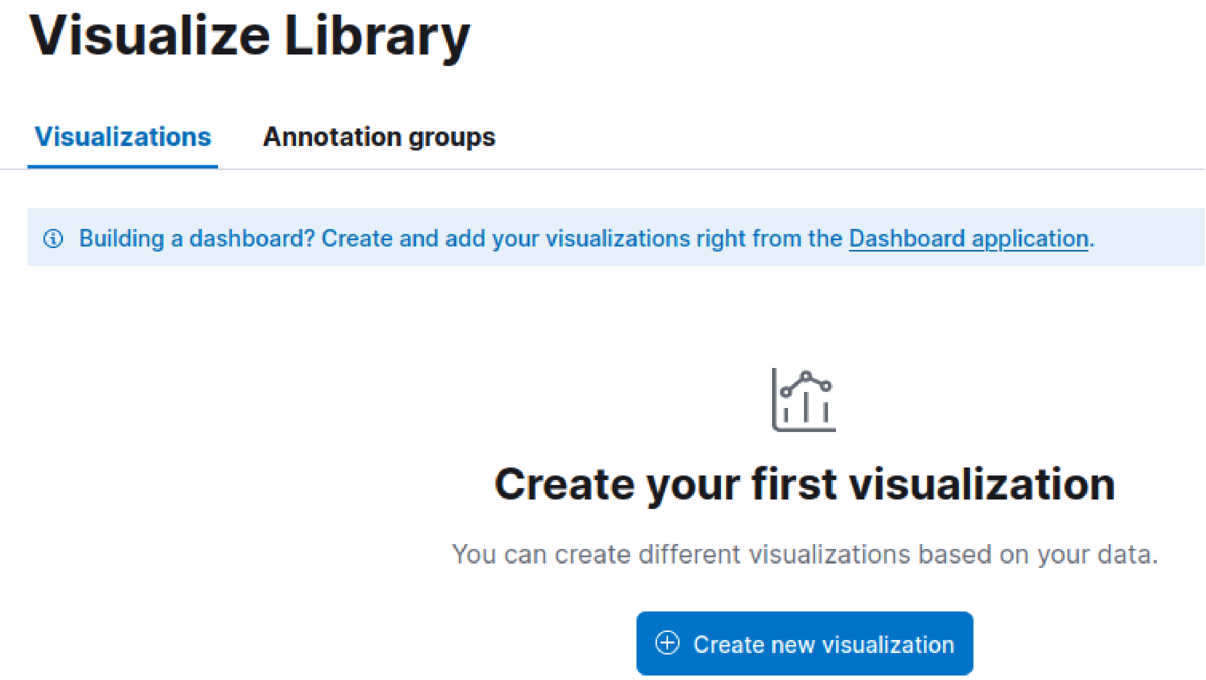
Name	Spaces	Actions
suricata Default	D	🗑
snort	D	🗑
zeek	D	🗑

Rows per page: 10

1

6. Create visualizations and dashboards to monitor network traffic data.



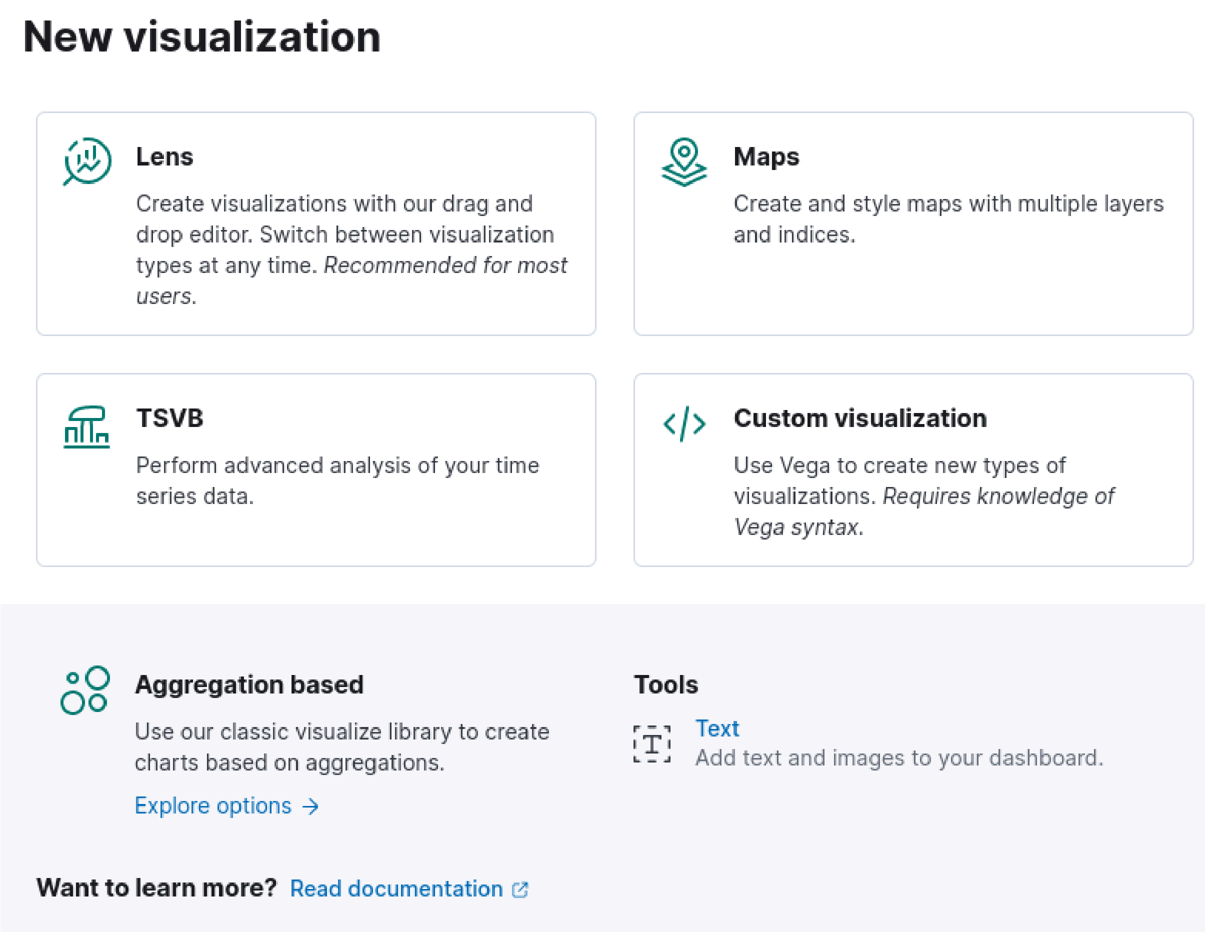


Visualize Library

Building a dashboard? Create and add your visualizations right from the Dashboard application.

Create your first visualization

You can create different visualizations based on your data.



New visualization

Lens

Create visualizations with our drag and drop editor. Switch between visualization types at any time. *Recommended for most users.*

Maps

Create and style maps with multiple layers and indices.

TSVB

Perform advanced analysis of your time series data.

Custom visualization

Use Vega to create new types of visualizations. *Requires knowledge of Vega syntax.*

Aggregation based

Use our classic visualize library to create charts based on aggregations.

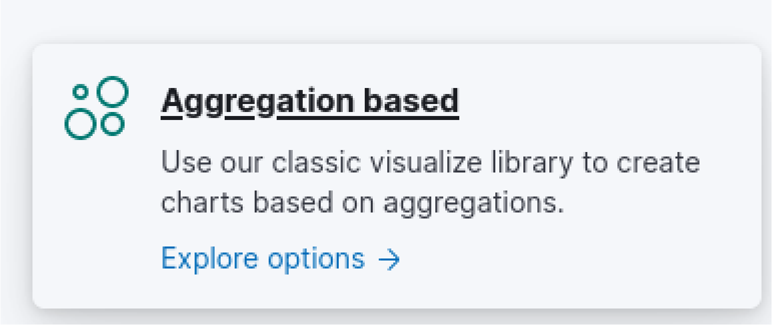
Explore options →

Tools

Text

Add text and images to your dashboard.

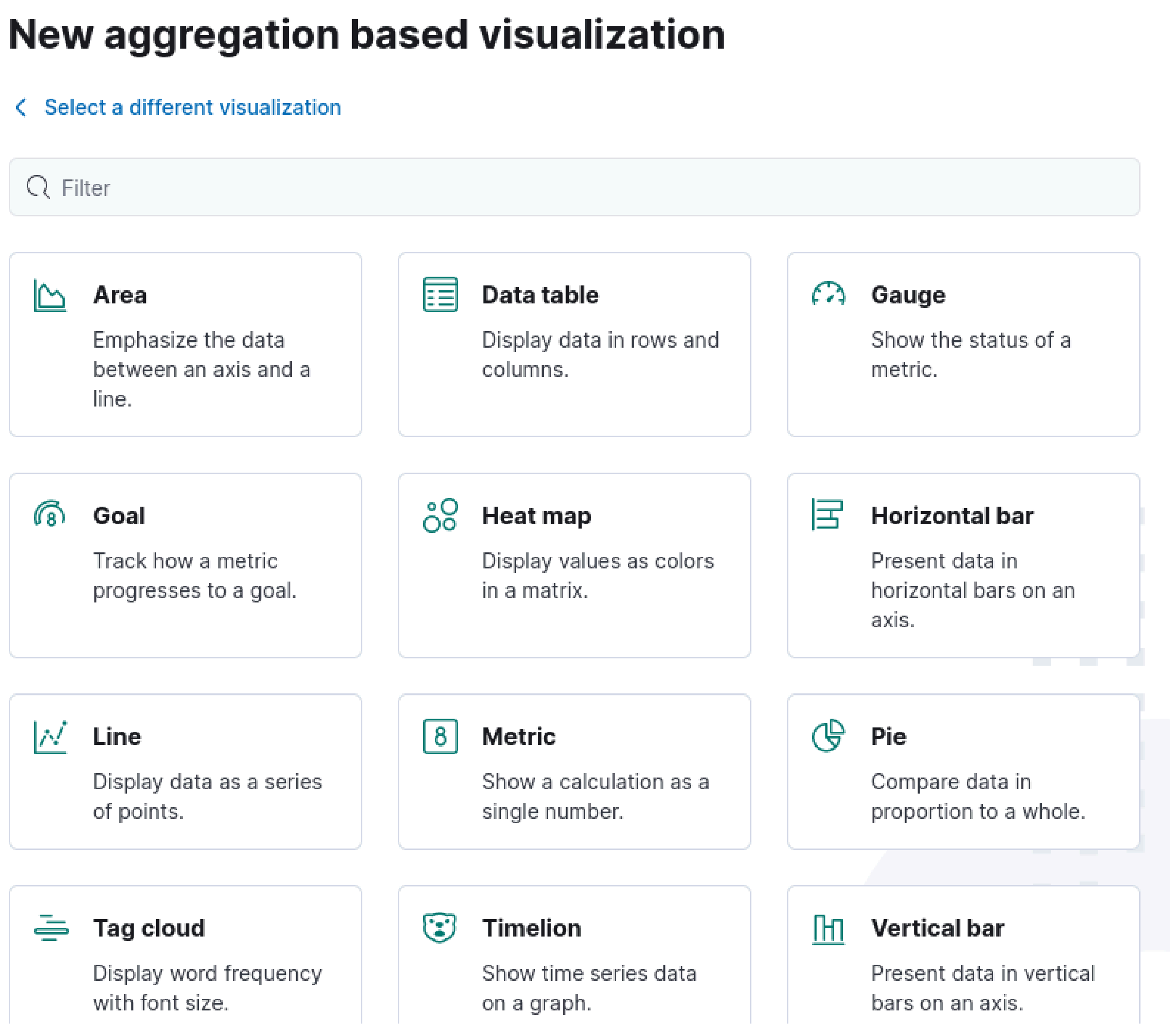
Want to learn more? Read documentation



Aggregation based

Use our classic visualize library to create charts based on aggregations.

Explore options →



New aggregation based visualization

< Select a different visualization

Filter

Area
Emphasize the data between an axis and a line.

Data table
Display data in rows and columns.

Gauge
Show the status of a metric.

Goal
Track how a metric progresses to a goal.

Heat map
Display values as colors in a matrix.

Horizontal bar
Present data in horizontal bars on an axis.

Line
Display data as a series of points.

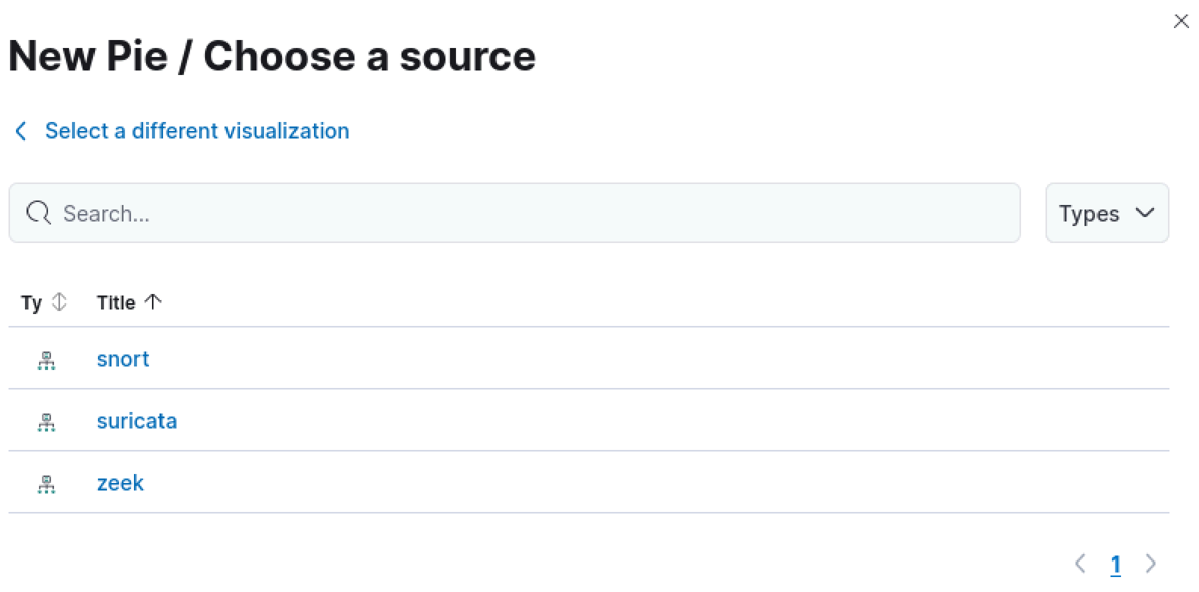
Metric
Show a calculation as a single number.

Pie
Compare data in proportion to a whole.

Tag cloud
Display word frequency with font size.

Timelion
Show time series data on a graph.

Vertical bar
Present data in vertical bars on an axis.

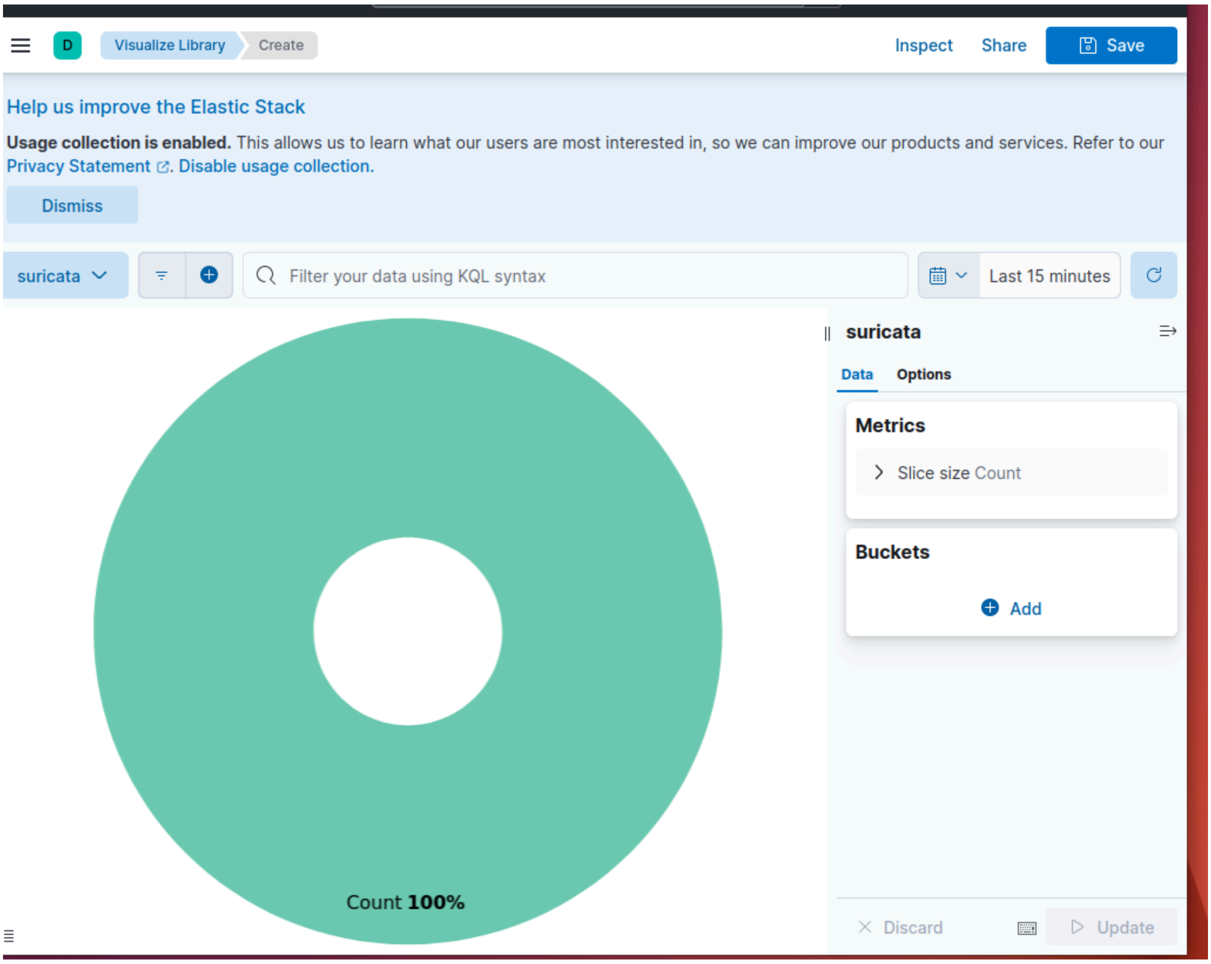


New Pie / Choose a source

< Select a different visualization

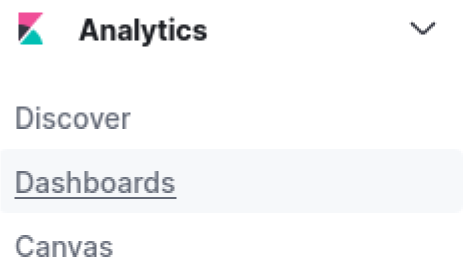
Search...

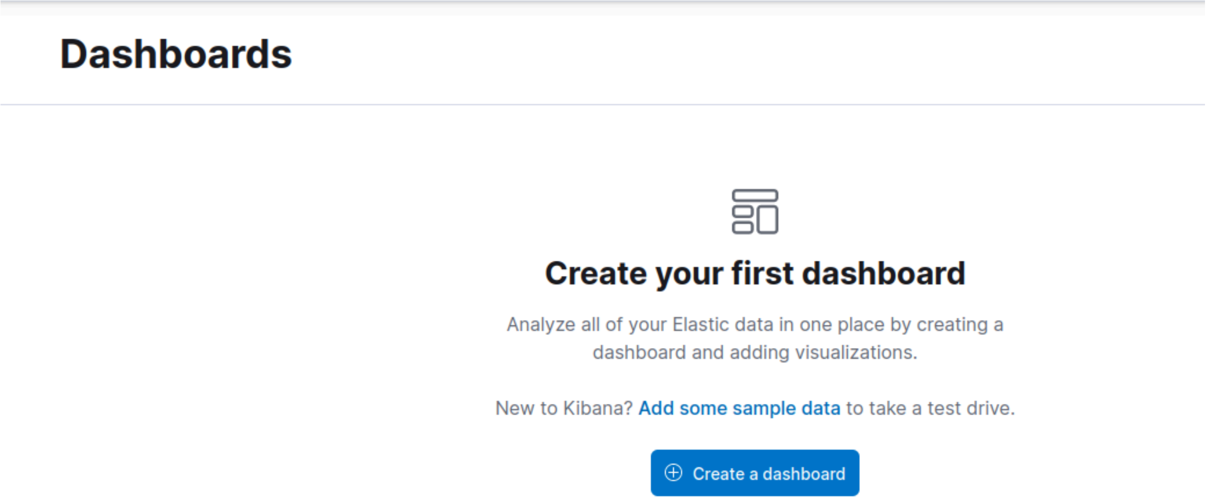
Ty	Title ↑
	snort
	suricata
	zeek



Help us improve the Elastic Stack

Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement. Disable usage collection.

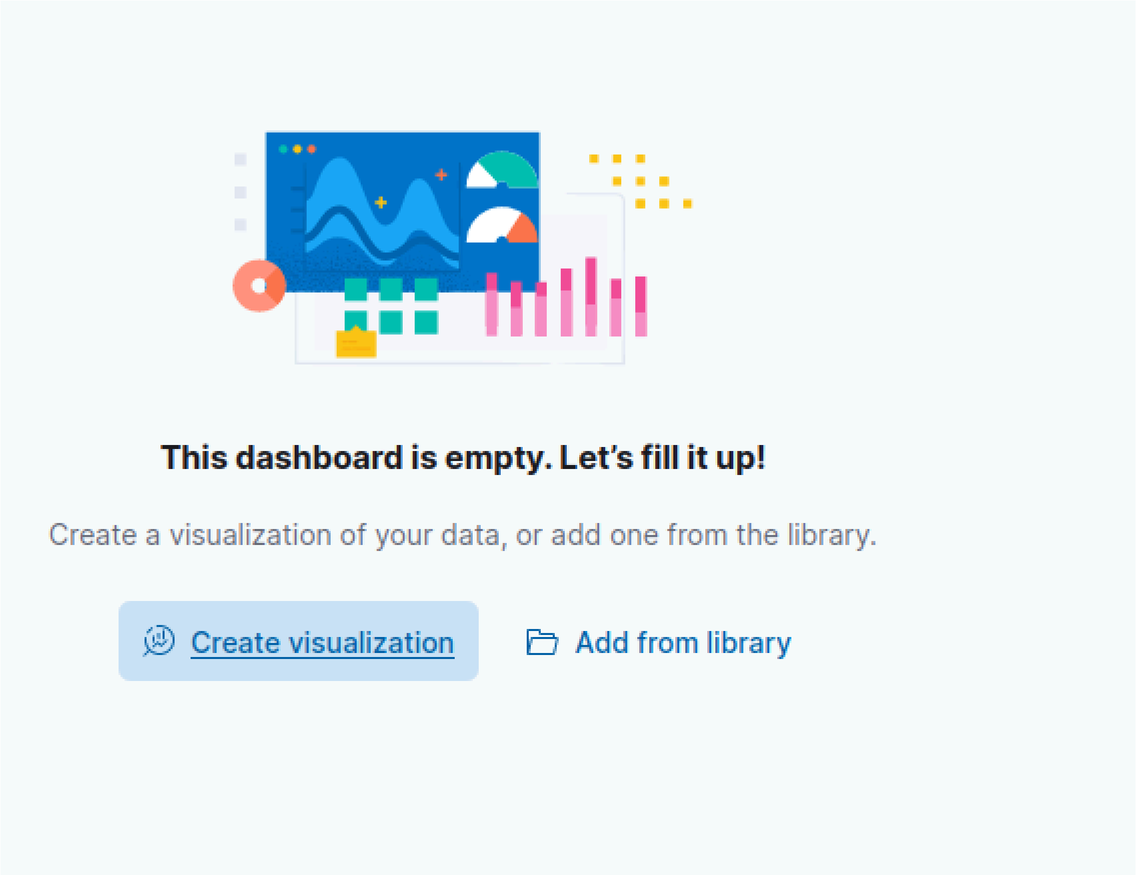




Create your first dashboard

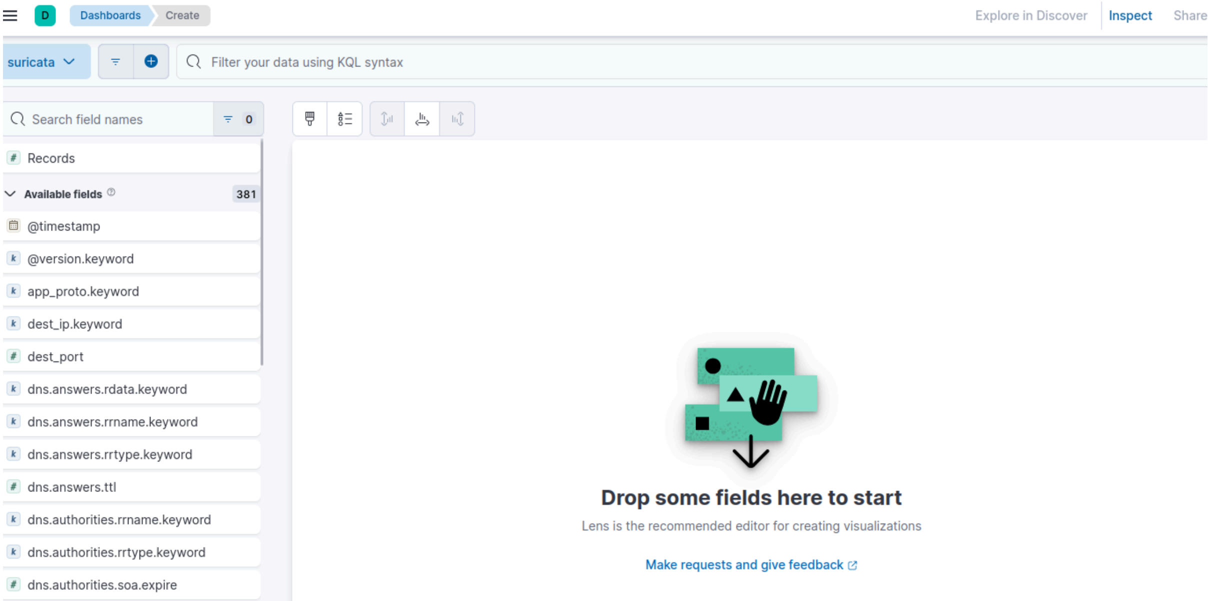
Analyze all of your Elastic data in one place by creating a dashboard and adding visualizations.

New to Kibana? Add some sample data to take a test drive.



This dashboard is empty. Let's fill it up!

Create a visualization of your data, or add one from the library.



Records

Available fields 381

@timestamp

@version.keyword

app_proto.keyword

dest_ip.keyword

dest_port

dns.answers.rdata.keyword

dns.answers.rrname.keyword

dns.answers.rrtype.keyword

dns.answers.ttl

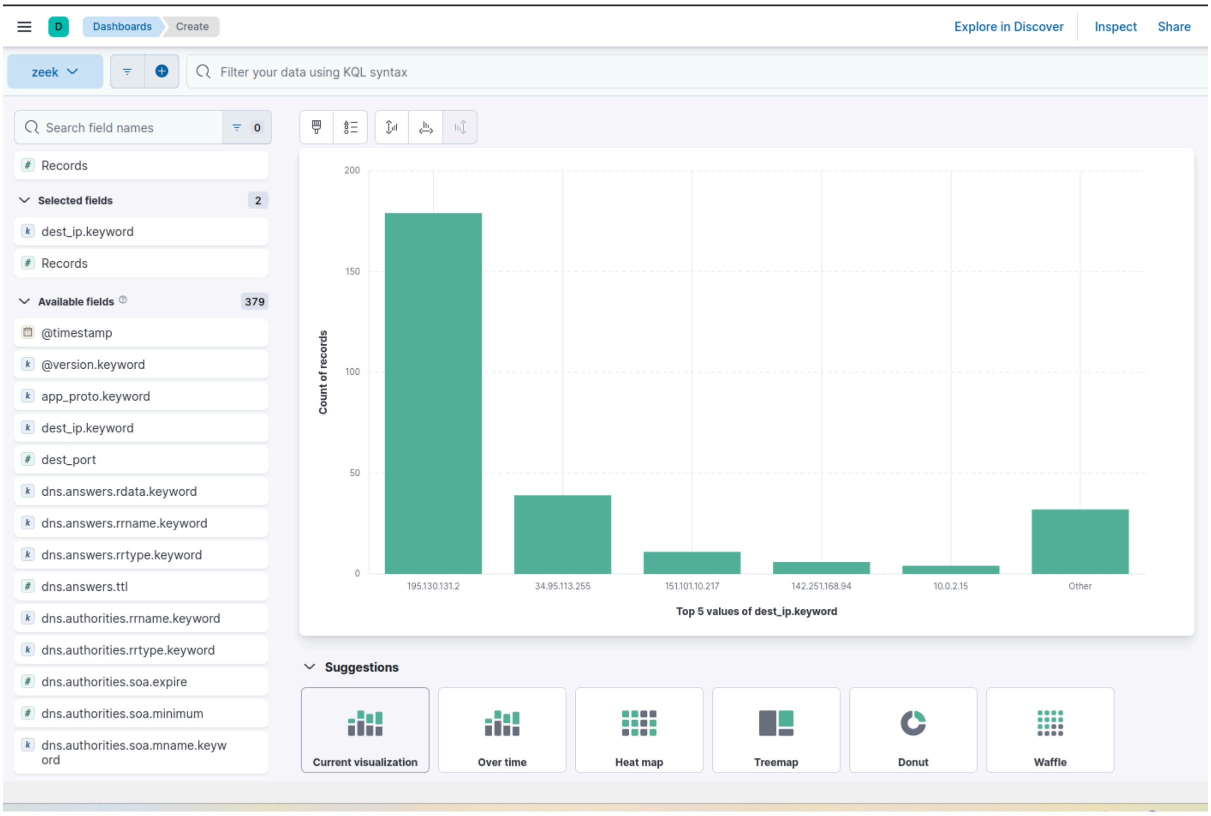
dns.authorities.rrname.keyword

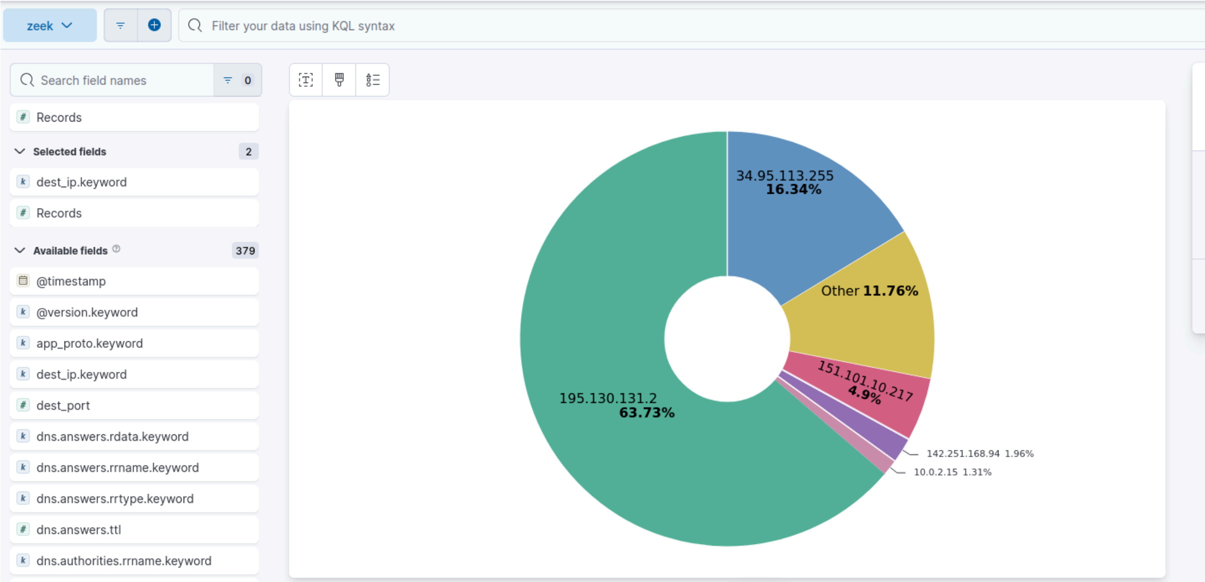
dns.authorities.rrtype.keyword

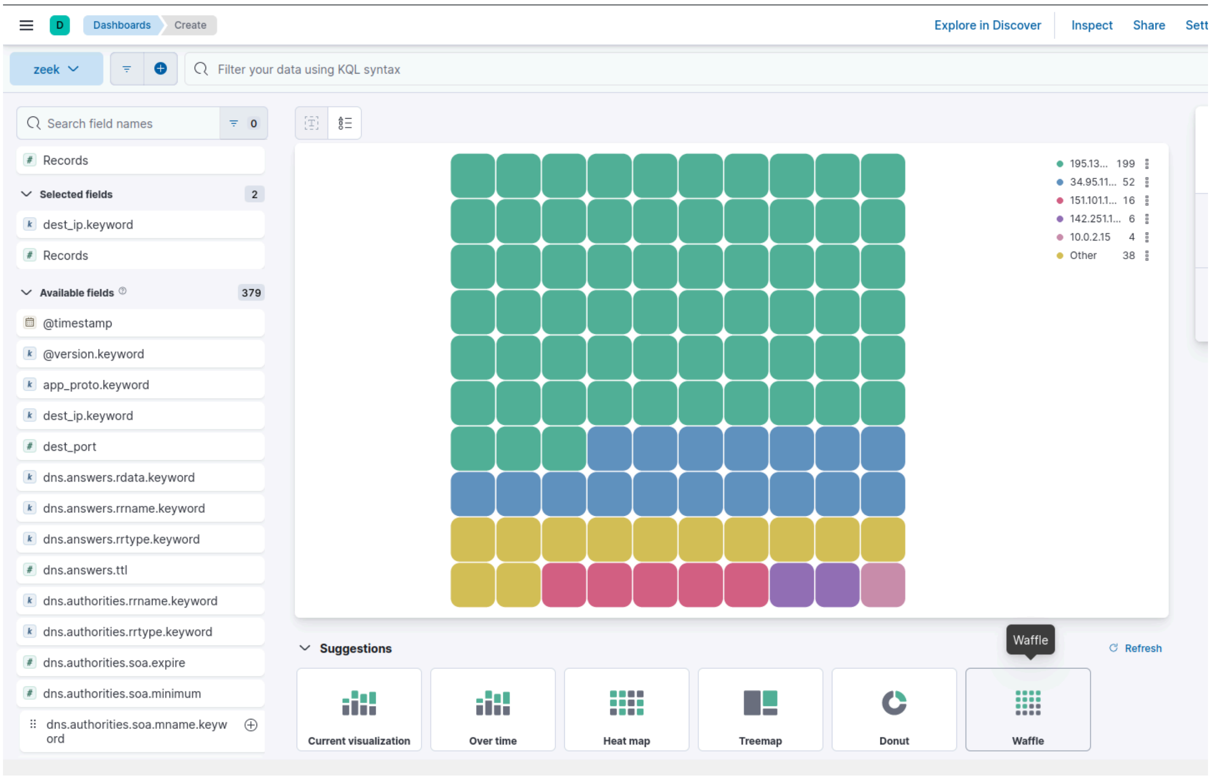
dns.authorities.soa.expire

Drop some fields here to start

Lens is the recommended editor for creating visualizations


D
Dashboards
Create
Explore in Discover
Inspect
Share
zeek
Filter your data using KQL syntax
Search field names
0
Records
Selected fields
2
dest_ip.keyword
Records
Available fields
379
@timestamp
@version.keyword
app_proto.keyword
dest_ip.keyword
dest_port
dns.answers.rdata.keyword
dns.answers.rrname.keyword
dns.answers.rrtype.keyword
dns.answers.ttl
dns.authorities.rrname.keyword
dns.authorities.rrtype.keyword
dns.authorities.soa.expire
dns.authorities.soa.minimum
dns.authorities.soa.mname.keyword
200
150
100
50
0
Count of records
195.130.131.2
34.95.113.255
151.101.10.217
142.251.168.94
10.0.2.15
Other
Top 5 values of dest_ip.keyword
Suggestions
Current visualization
Over time
Heat map
Treemap
Donut
Waffle


zeek
Filter your data using KQL syntax
Search field names
0
Records
Selected fields
2
dest_ip.keyword
Records
Available fields
379
@timestamp
@version.keyword
app_proto.keyword
dest_ip.keyword
dest_port
dns.answers.rdata.keyword
dns.answers.rrname.keyword
dns.answers.rrtype.keyword
dns.answers.ttl
dns.authorities.rrname.keyword
34.95.113.255
16.34%
Other 11.76%
151.101.10.217
4.9%
142.251.168.94 1.96%
10.0.2.15 1.31%
195.130.131.2
63.73%


D
Dashboards
Create
Explore in Discover
Inspect
Share
Sett
zeek
Filter your data using KQL syntax
Search field names
0
Records
Selected fields
2
dest_ip.keyword
Records
Available fields
379
@timestamp
@version.keyword
app_proto.keyword
dest_ip.keyword
dest_port
dns.answers.rdata.keyword
dns.answers.rrname.keyword
dns.answers.rrtype.keyword
dns.answers.ttl
dns.authorities.rrname.keyword
dns.authorities.rrtype.keyword
dns.authorities.soa.expire
dns.authorities.soa.minimum
dns.authorities.soa.mname.keyword
195.13... 199
34.95.11... 52
151.101.1... 16
142.251.1... 6
10.0.2.15 4
Other 38
Suggestions
Refresh
Waffle
Current visualization
Over time
Heat map
Treemap
Donut
Waffle