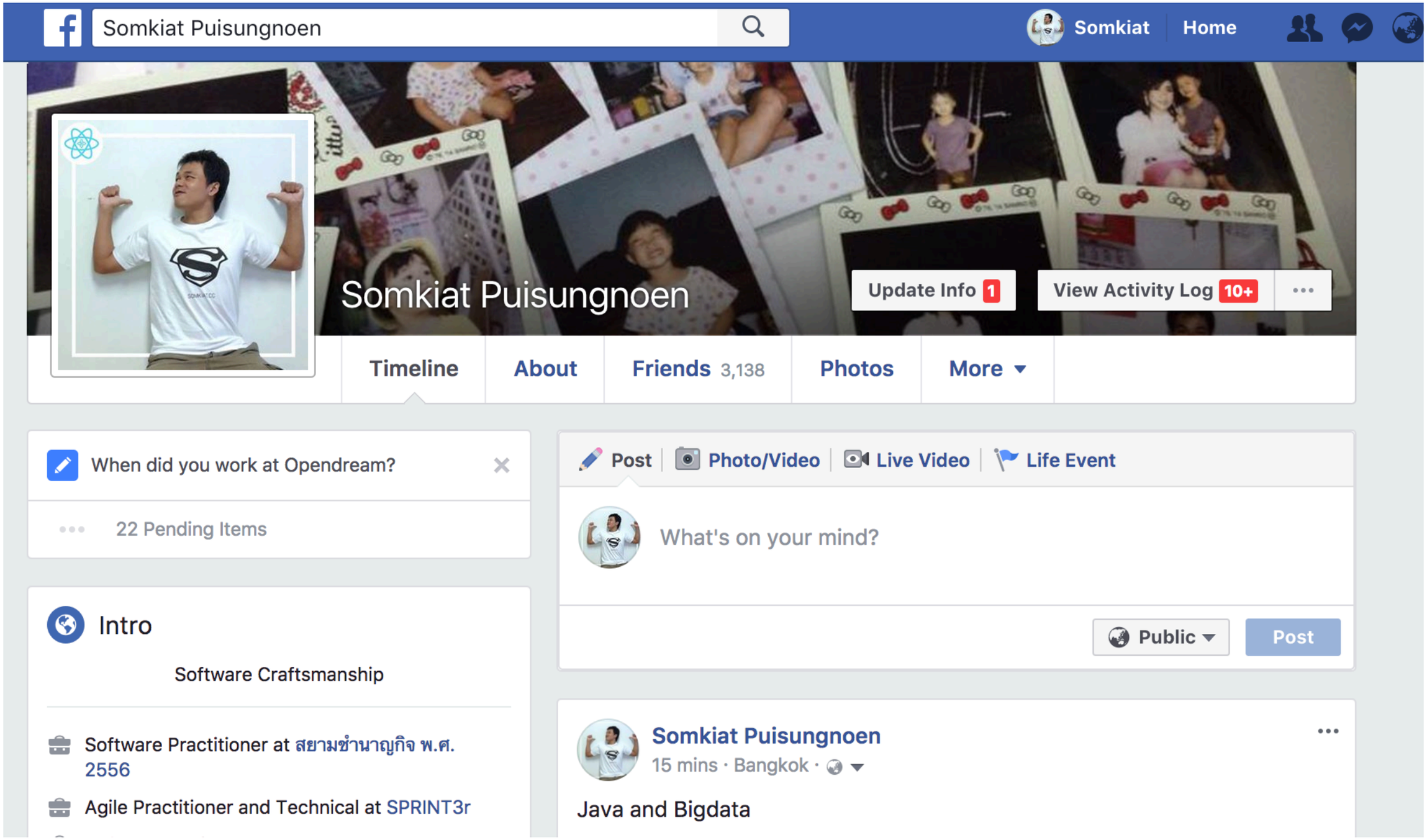
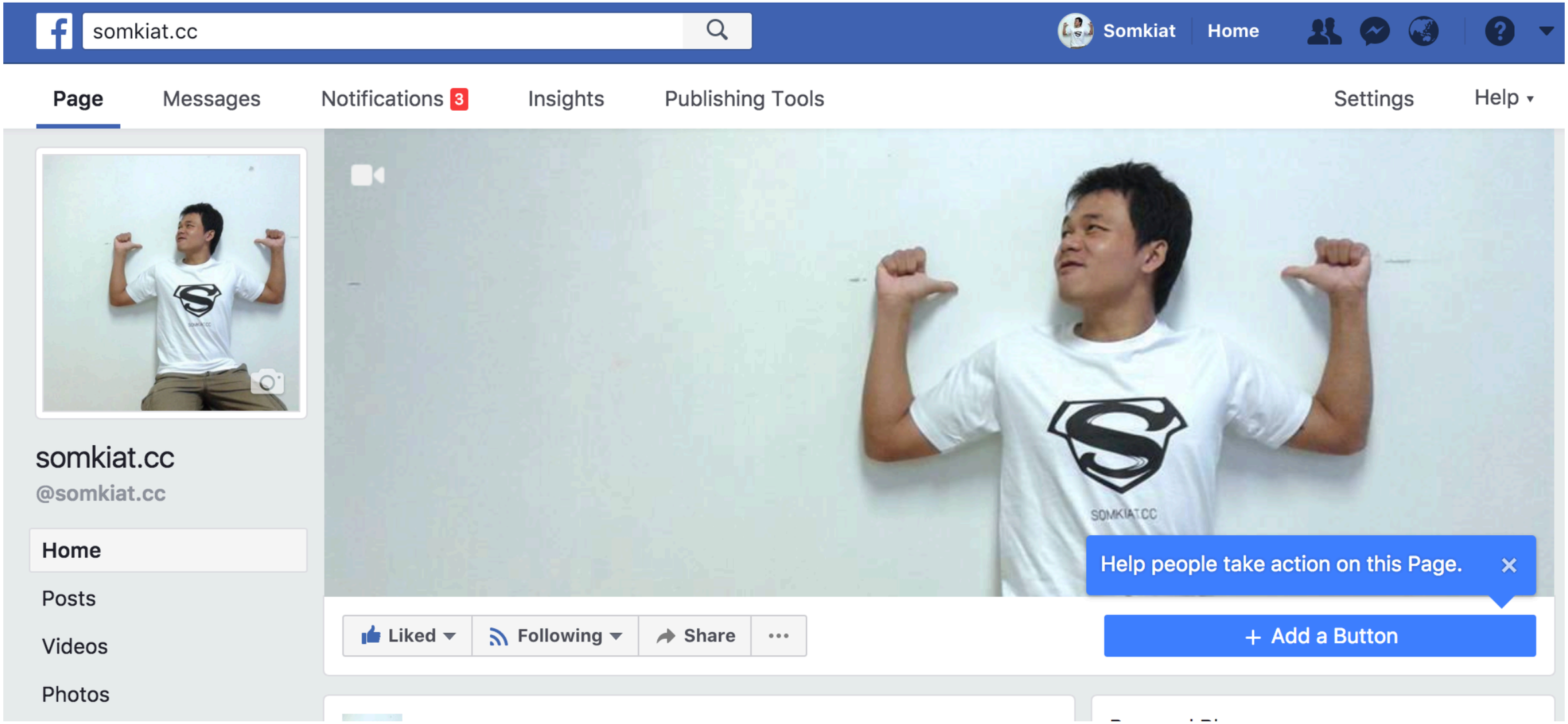
สยามชำนาญกิจ
SIAM CHAMNAN KIT

Kibana

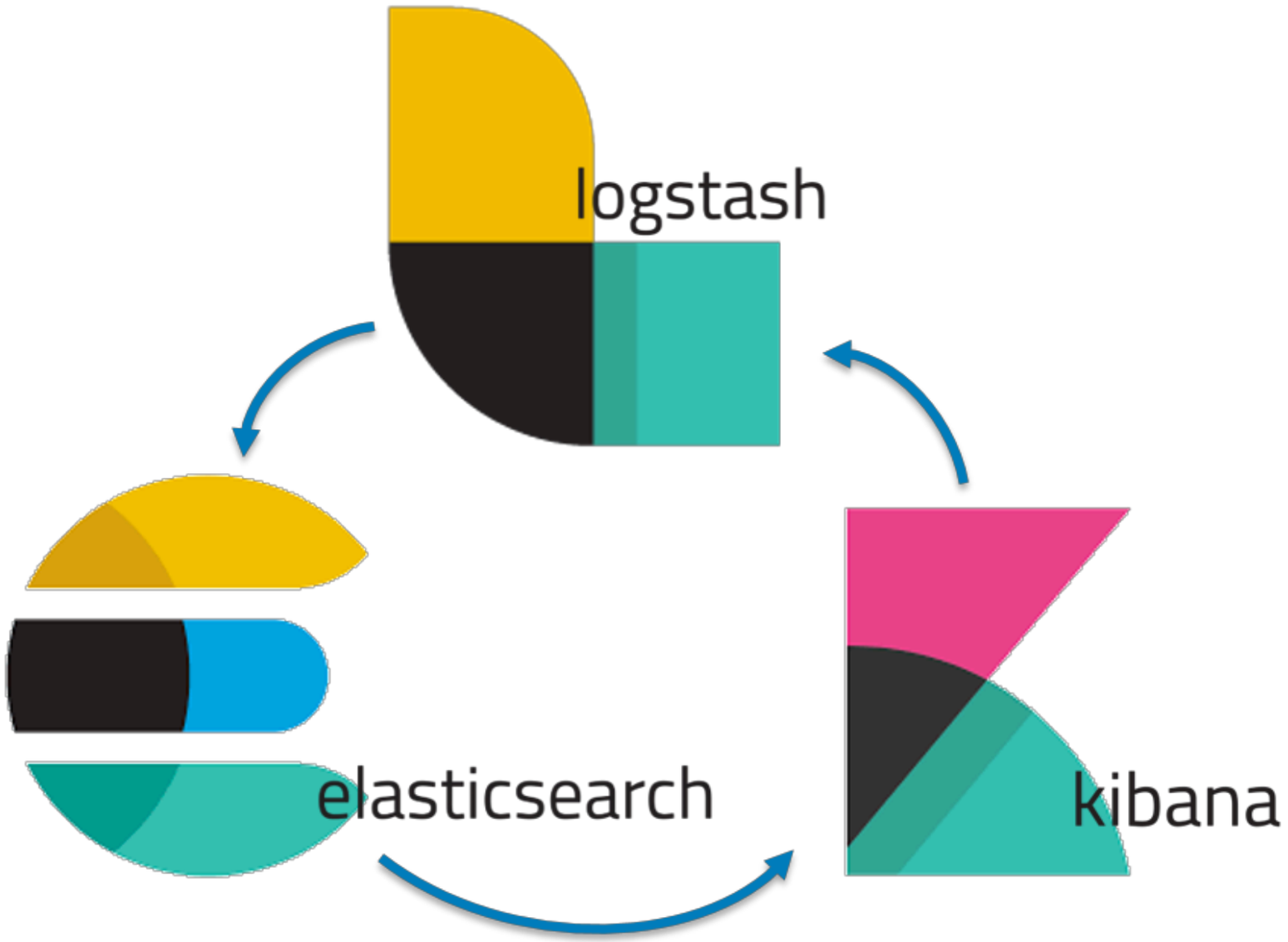




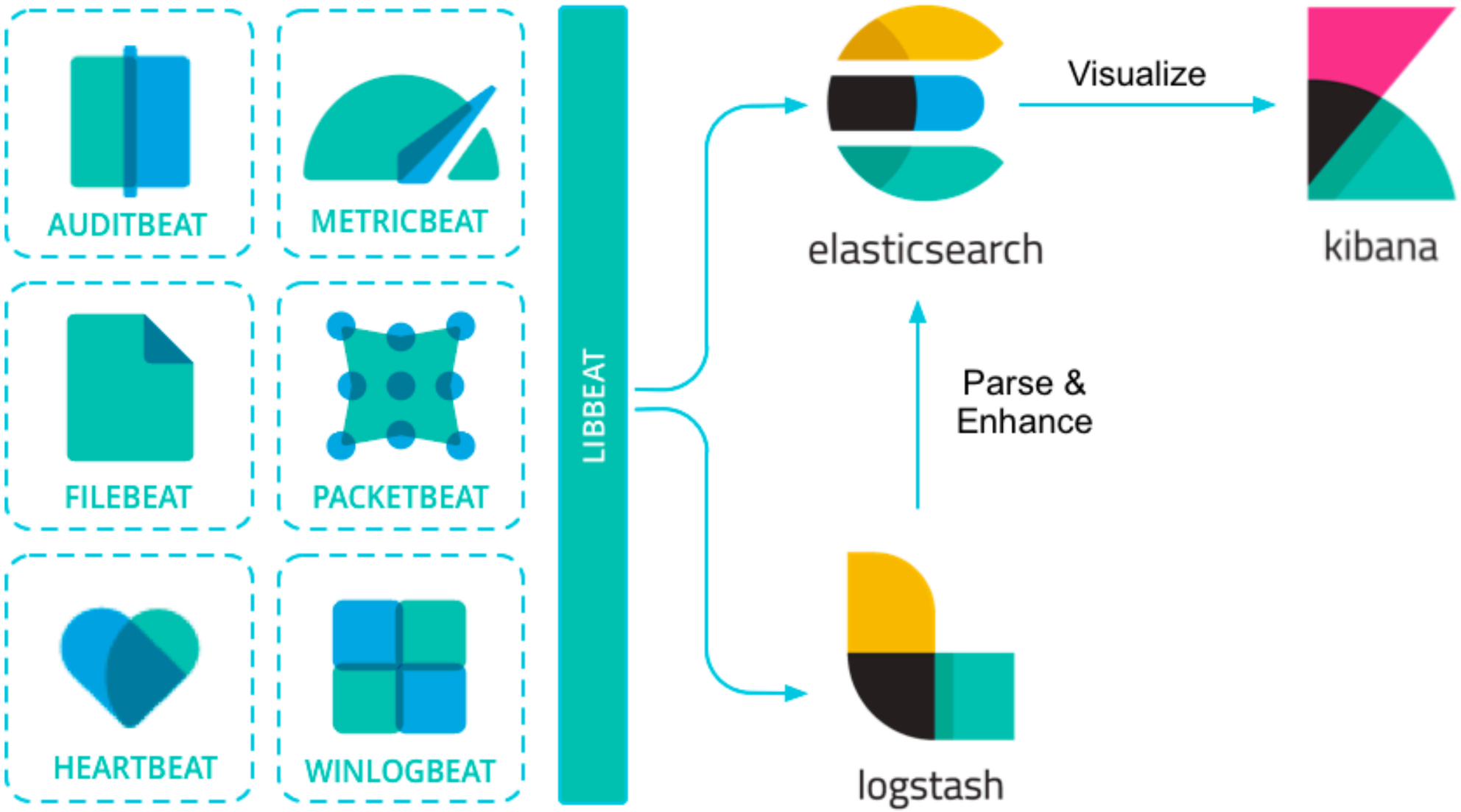
https://github.com/up1/course_elk

Agenda

- Working with Kibana
- Working with Logstash/Beat
- Monitoring with Kibana



Beat



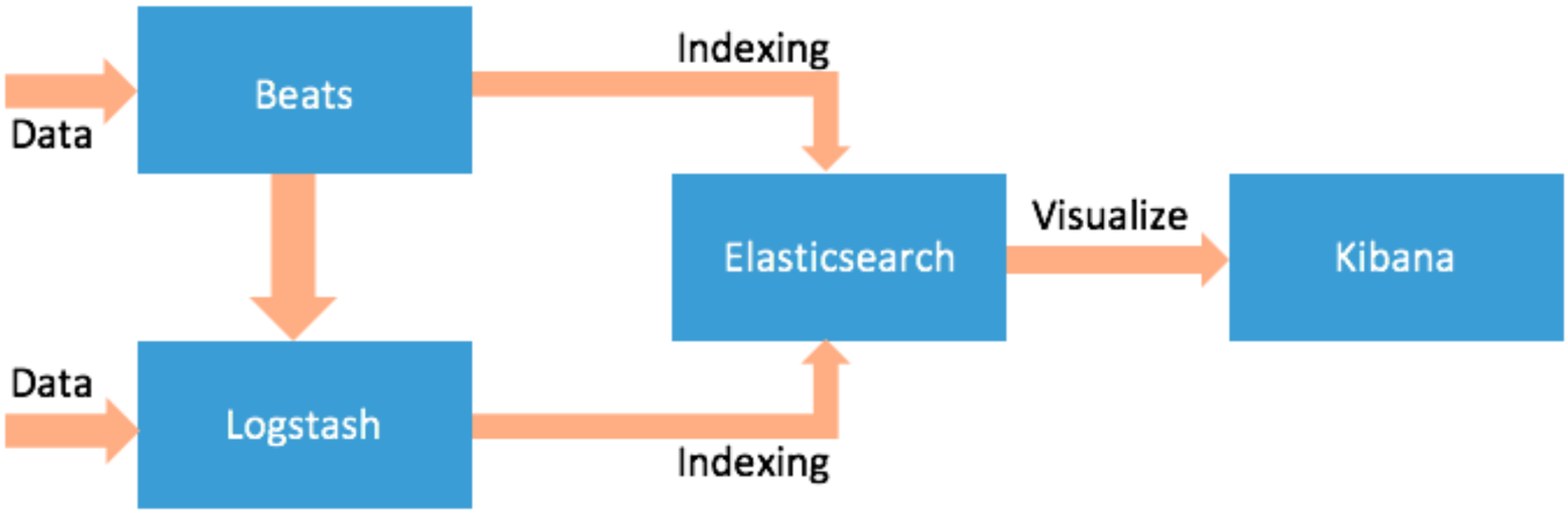
https://www.elastic.co/guide/en/beats/libbeat/current/index.html

Beat

Purpose	Library
Audit data	Auditbeat
Log files	Filebeat
Cloud data	Functionbeat
Availability	Heartbeat
Metrics	Metricbeat
Network traffic	Packetbeat
Windows event logs	Winlogbeat

https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html

ELK stack



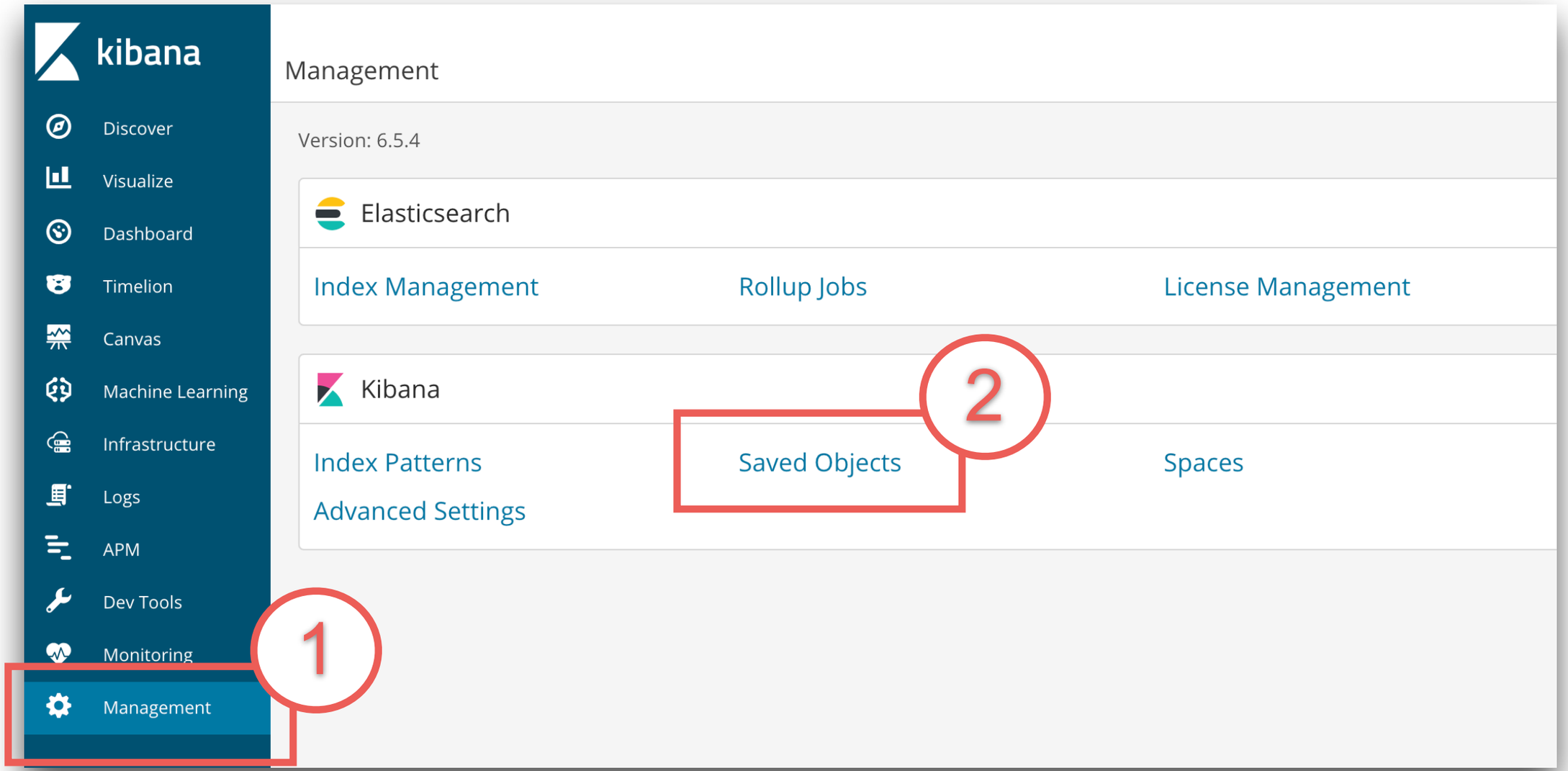
Kibana

Kibana

Create visualization
Create dashboard
Infrastructure
Monitoring

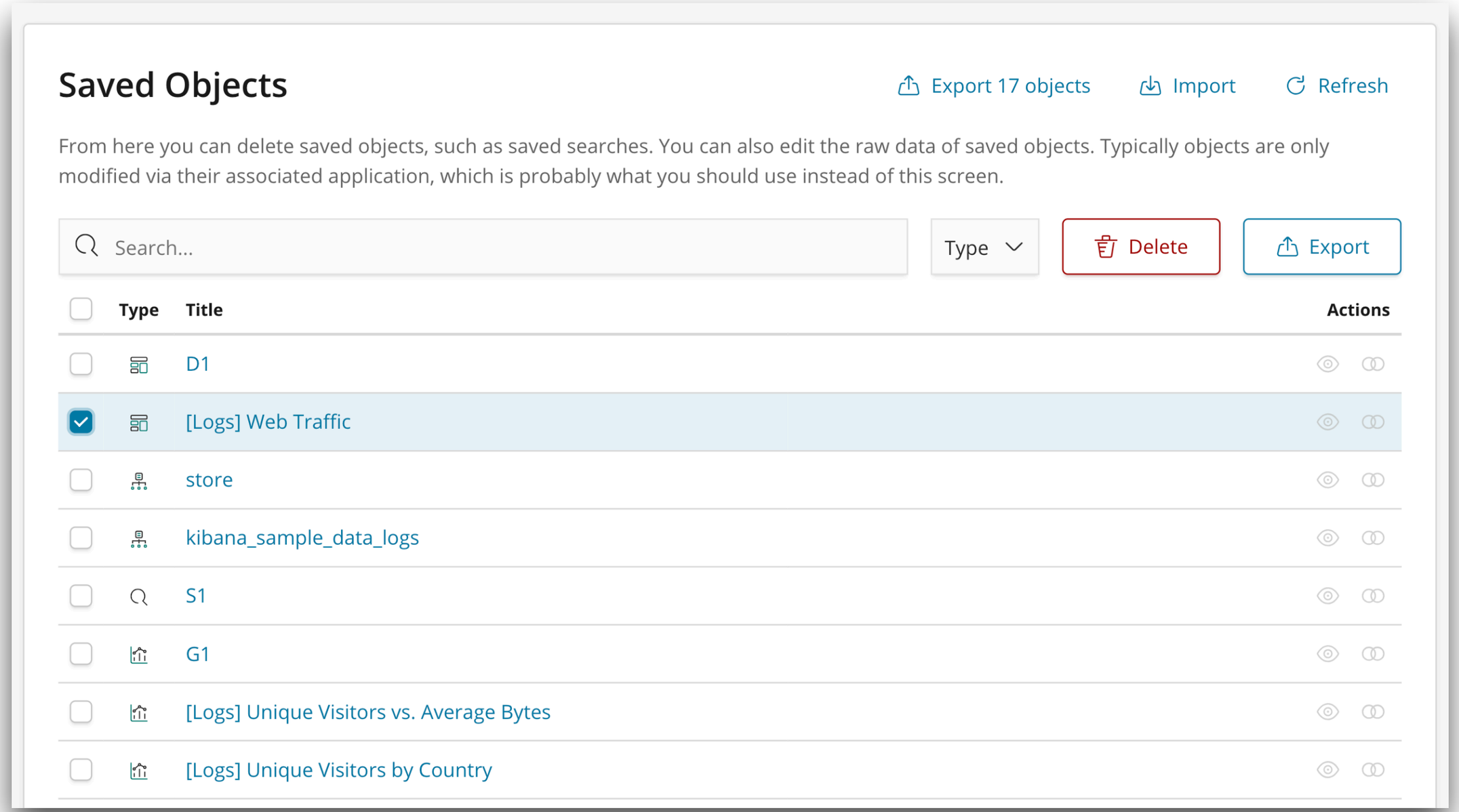
Import/Export

Go to **management** menu => **Saved Objects**



Import/Export

Working with JSON file

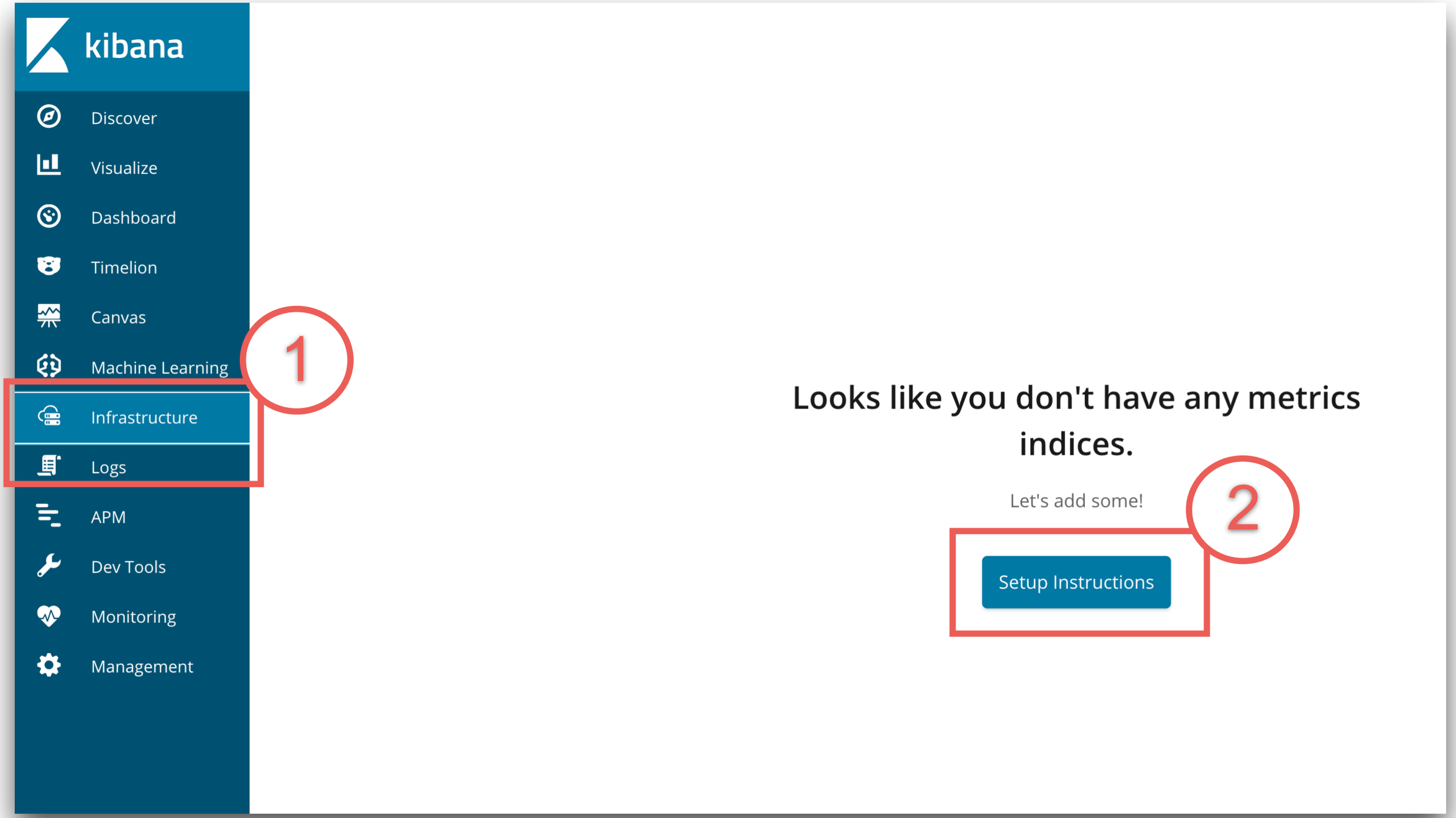


BETA

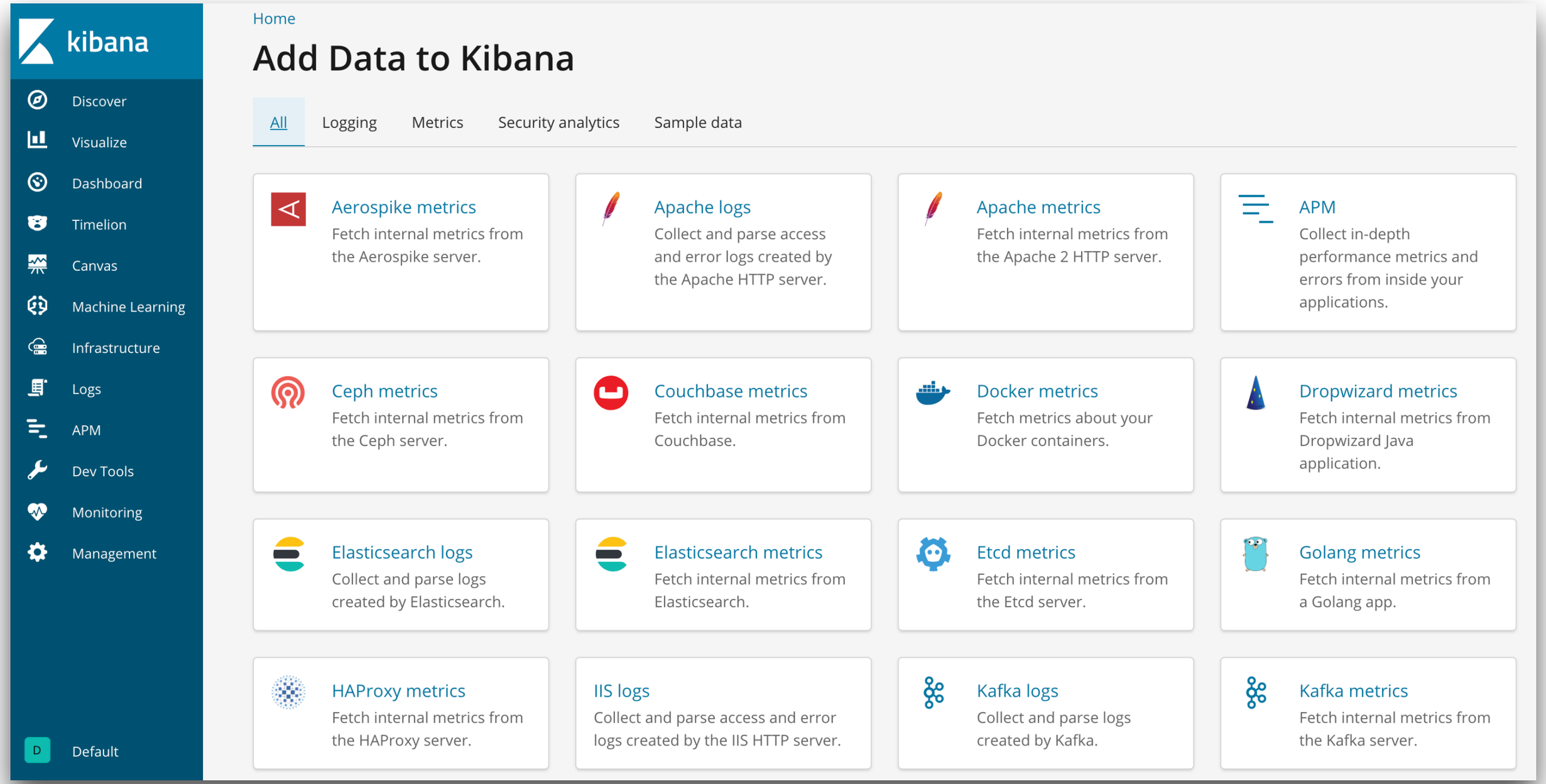
Infrastructure with Kibana

Elasticsearch and Kibana 6.5 +

Setup instruction



Add data to Kibana

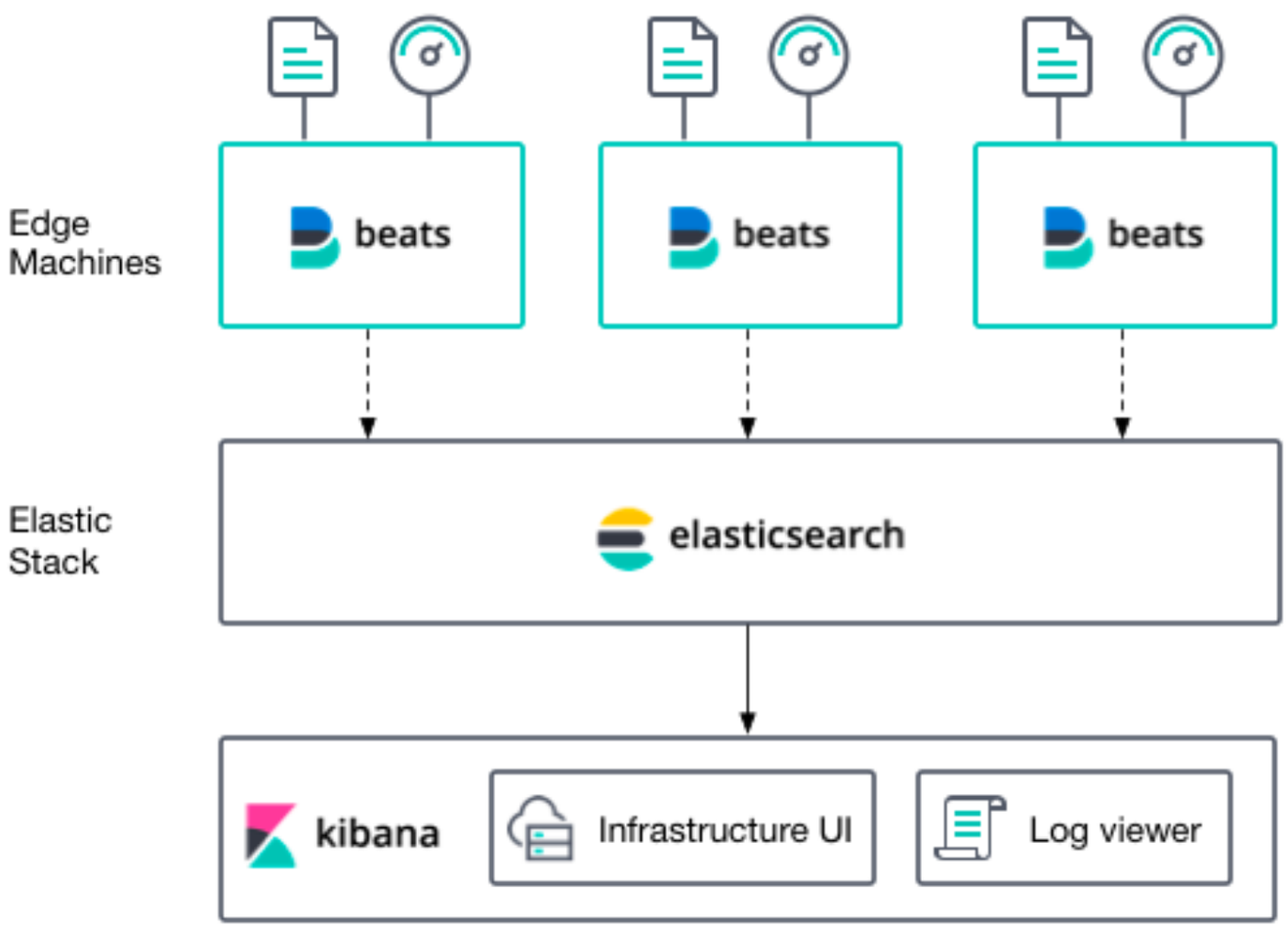


Monitor your infrastructure

Monitor hosts and containers
View metrics
View logs

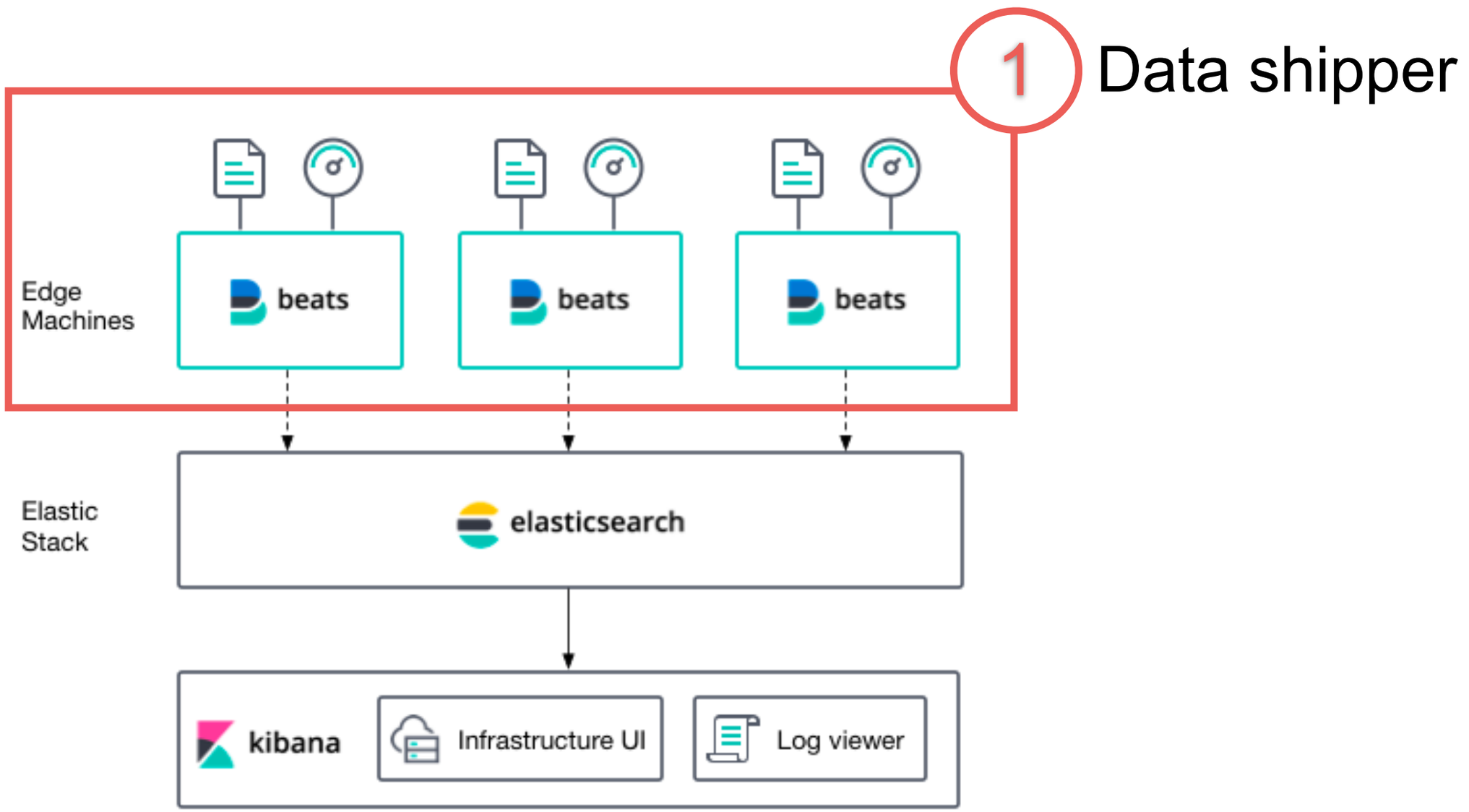
https://www.elastic.co/guide/en/kibana/current/monitor-infra.html

Infrastructure monitoring

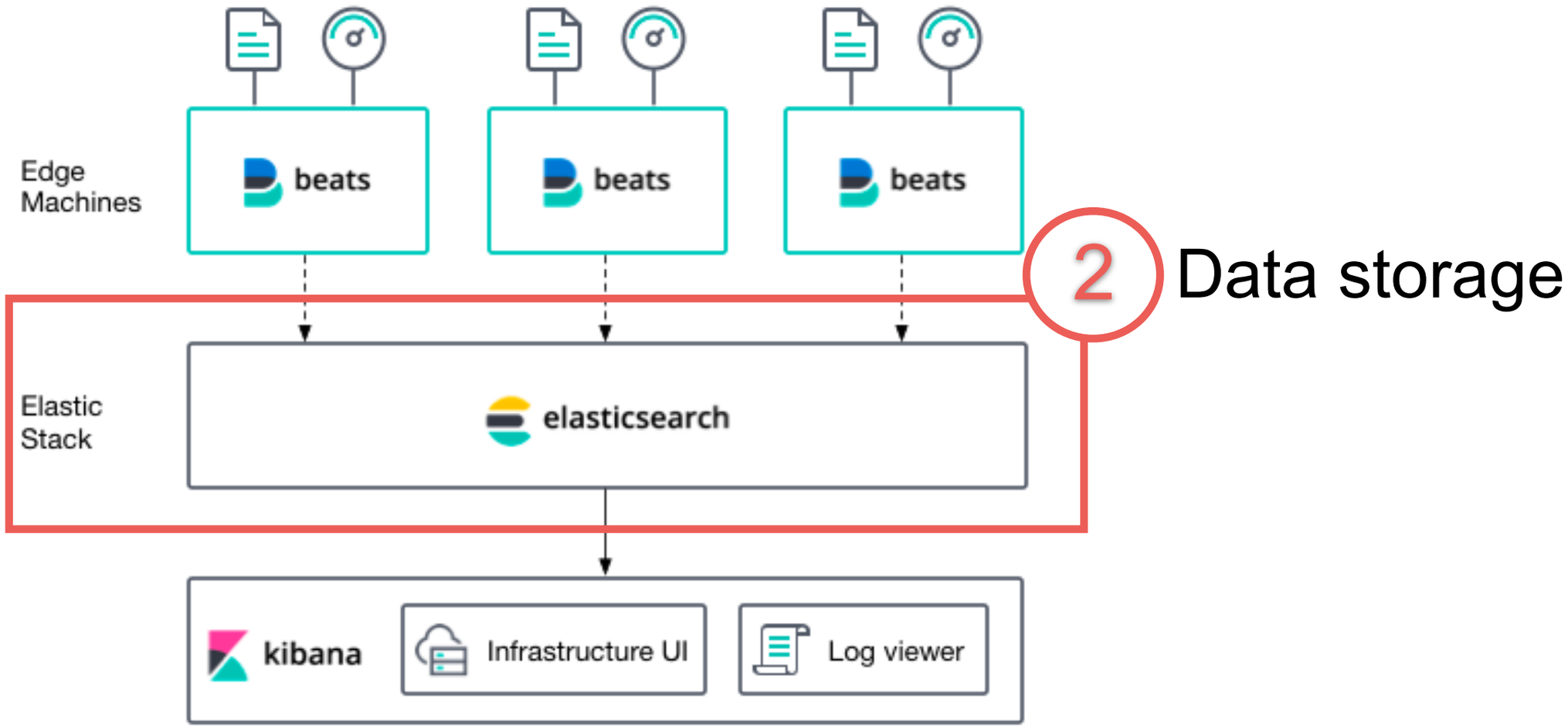


https://www.elastic.co/guide/en/infrastructure/guide/6.5/infrastructure-monitoring-overview.html

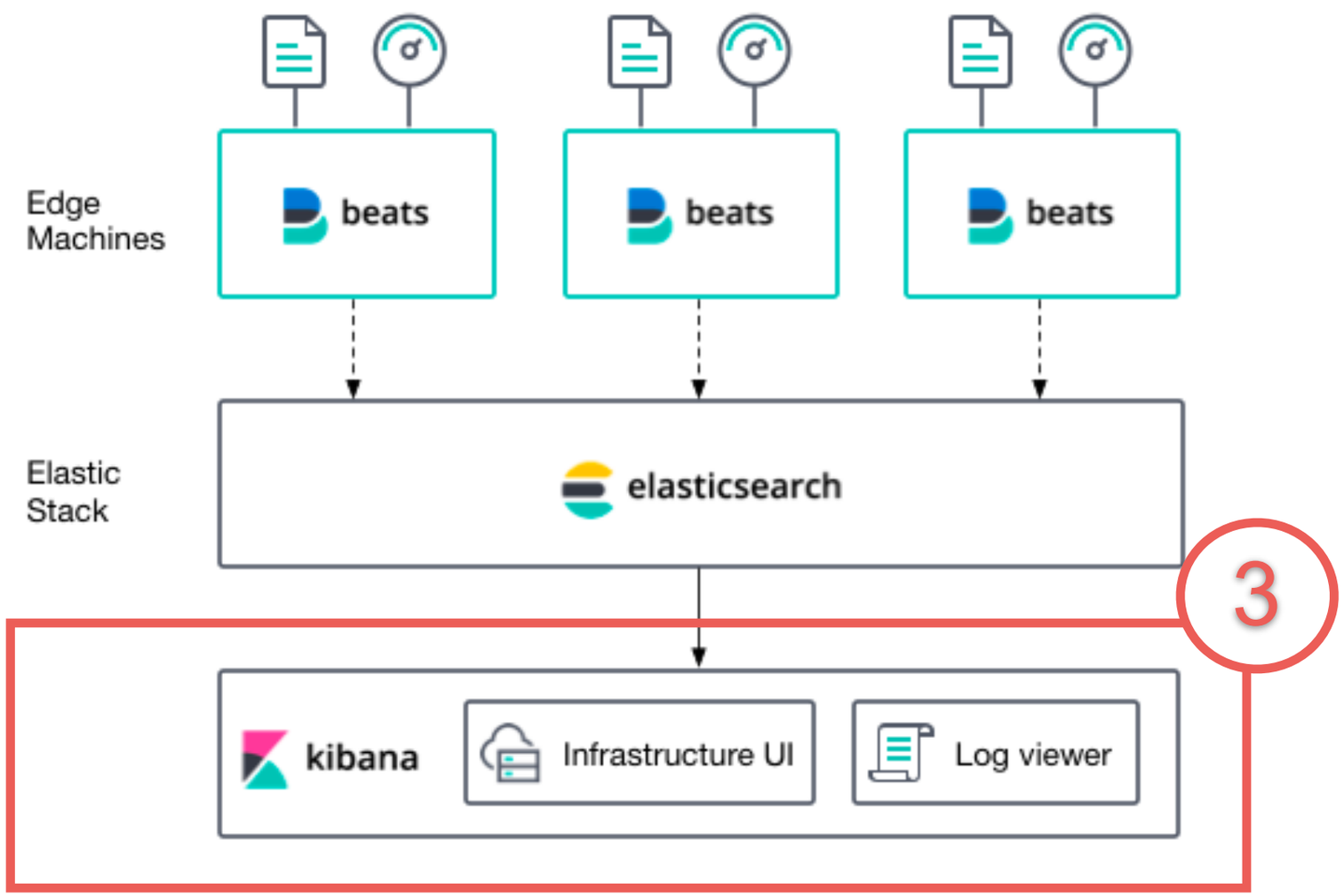
Infrastructure monitoring



Infrastructure monitoring



Infrastructure monitoring



Data visualization

Installation

Data Shippers

Metricbeat

Filebeat

Add metrics to Kibana

Add Data to Kibana

All | Logging | Metrics | Security analytics | Sample data

Aerospike metrics
Fetch internal metrics from the Aerospike server.

Apache metrics
Fetch internal metrics from the Apache 2 HTTP server.

Ceph metrics
Fetch internal metrics from the Ceph server.

Couchbase metrics
Fetch internal metrics from Couchbase.

Docker metrics
Fetch metrics about your Docker containers.

Dropwizard metrics
Fetch internal metrics from Dropwizard Java application.

Elasticsearch metrics
Fetch internal metrics from Elasticsearch.

Etcd metrics
Fetch internal metrics from the Etcd server.

Golang metrics
Fetch internal metrics from a Golang app.

HAProxy metrics
Fetch internal metrics from the HAProxy server.

Kafka metrics
Fetch internal metrics from the Kafka server.

Kibana metrics
Fetch internal metrics from Kibana.

Kubernetes metrics
Fetch metrics from your Kubernetes installation.

Logstash metrics
Fetch interal metrics from a Logstash server.

Memcached metrics
Fetch internal metrics from the Memcached server.

MongoDB metrics
Fetch internal metrics from MongoDB.

Setup Metricbeat

Home / Add Data

Elasticsearch metrics BETA

The `elasticsearch` Metricbeat module fetches internal metrics from Elasticsearch. Learn more.

View exported fields

Self managed | Elastic Cloud

Getting Started

macOS | DEB | RPM | Windows

1 Download and install Metricbeat

First time using Metricbeat? See the Getting Started Guide.

Copy snippet

```
curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.5.4-darwin-x86_64.tar.gz
tar xzvf metricbeat-6.5.4-darwin-x86_64.tar.gz
cd metricbeat-6.5.4-darwin-x86_64/
```

Setup Metricbeat

Install Metricbeat
Config Metricbeat
Enable Elasrticsearch module in Metricbeat
Start Metricbeat

Dashboard in Kibana

Create index pattern

Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.

Include system indices

Step 1 of 2: Define index pattern

Index pattern

index-name-*

You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.

Next step

Your index pattern can match any of your **5 indices**, below.

kibana_sample_data_logs

metricbeat-6.5.4-2019.01.10

mobile

store

xxx

Rows per page: 10

Dashboard in Kibana

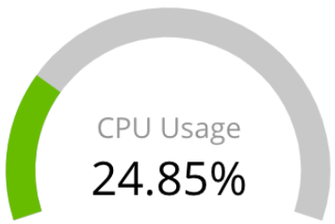
Dashboards

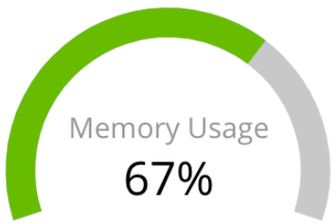
Create new dashboard

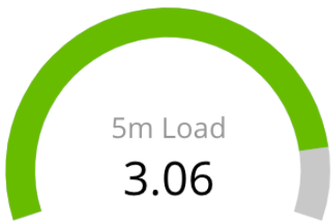
Search...

	Title	Description	Actions
☐	[Metricbeat Docker] Overview	Overview of docker containers	Edit
☐	[Metricbeat Apache] Overview	Overview of Apache server status	Edit
☐	[Metricbeat System] Containers overview	Overview of container metrics	Edit
☐	[Metricbeat Golang] Overview	Overview of Go profiling information	Edit
☐	[Metricbeat HAProxy] HTTP backend	HAProxy HTTP backend metrics	Edit
☐	[Metricbeat HAProxy] Backend	HAProxy backend metrics	Edit
☐	[Metricbeat HAProxy] Frontend	HAProxy frontend metrics	Edit
☐	[Metricbeat System] Host overview	Overviw of host metrics	Edit

Host overview dashboard







Inbound Traffic
132.531KB/s
Total Transferred 45.333MB

Outbound Traffic
1.331MB/s
Total Transferred 638.012MB

In Packetloss
0
Out Packetloss 205

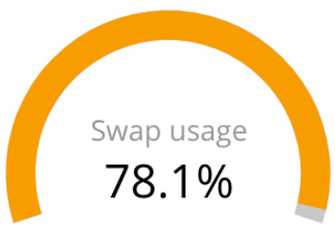
Swap usage [Metricbeat...

Memory usage vs total

Number of processes [...

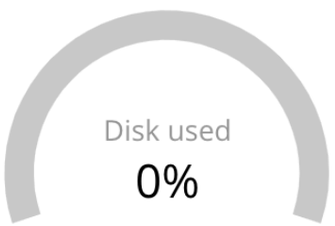
Disk used [Metricbeat S...

Disk Usage [Metricbeat System]

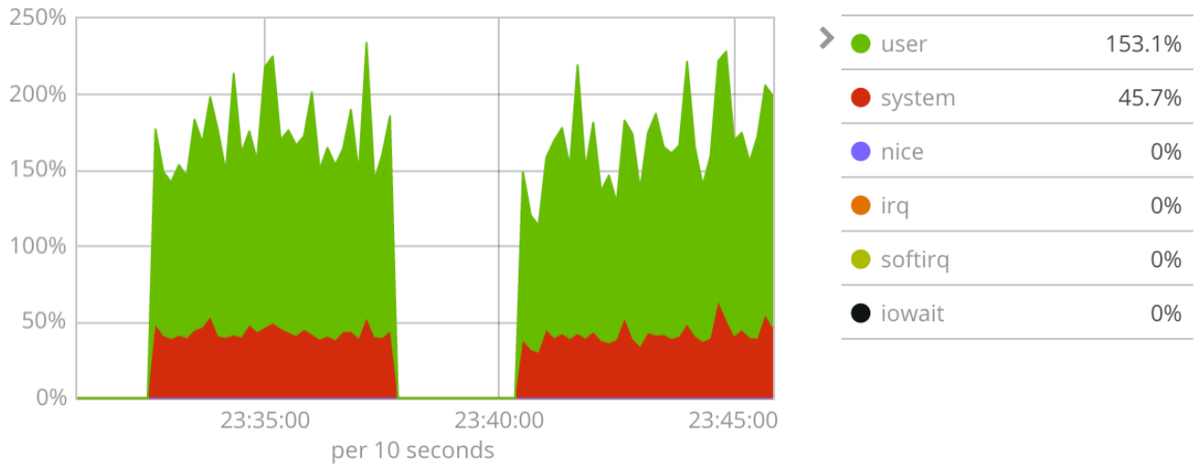


Memory usage
10.72GB
Total Memory 16GB

27
Processes

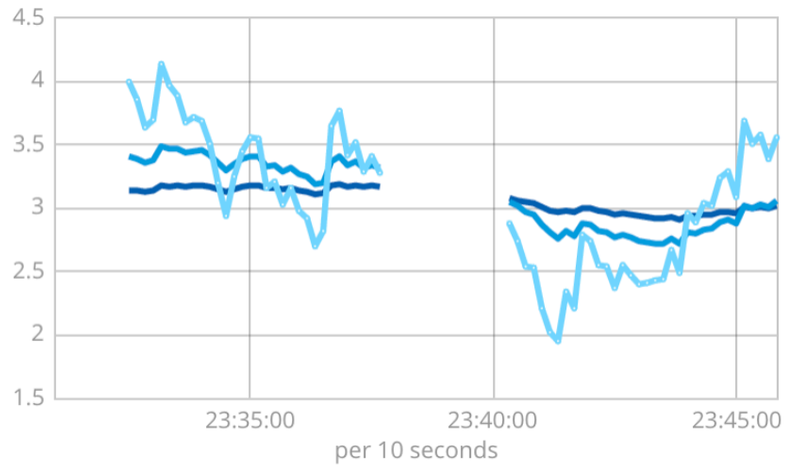


CPU Usage [Metricbeat System]



user	153.1%
system	45.7%
nice	0%
irq	0%
softirq	0%
iowait	0%

System Load [Metricbeat System]



1m	3.56
5m	3.06
15m	3.02

Try to setup Logging !!

Add logging to Kibana

Home

Add Data to Kibana

All | Logging | Metrics | Security analytics | Sample data

Apache logs
Collect and parse access and error logs created by the Apache HTTP server.

Elasticsearch logs
Collect and parse logs created by Elasticsearch.

IIS logs
Collect and parse access and error logs created by the IIS HTTP server.

Kafka logs
Collect and parse logs created by Kafka.

Logstash logs
Collect and parse debug and slow logs created by Logstash itself.

MySQL logs
Collect and parse error and slow logs created by MySQL.

Nginx logs
Collect and parse access and error logs created by the Nginx HTTP server.

PostgreSQL logs
Collect and parse error and slow logs created by PostgreSQL.

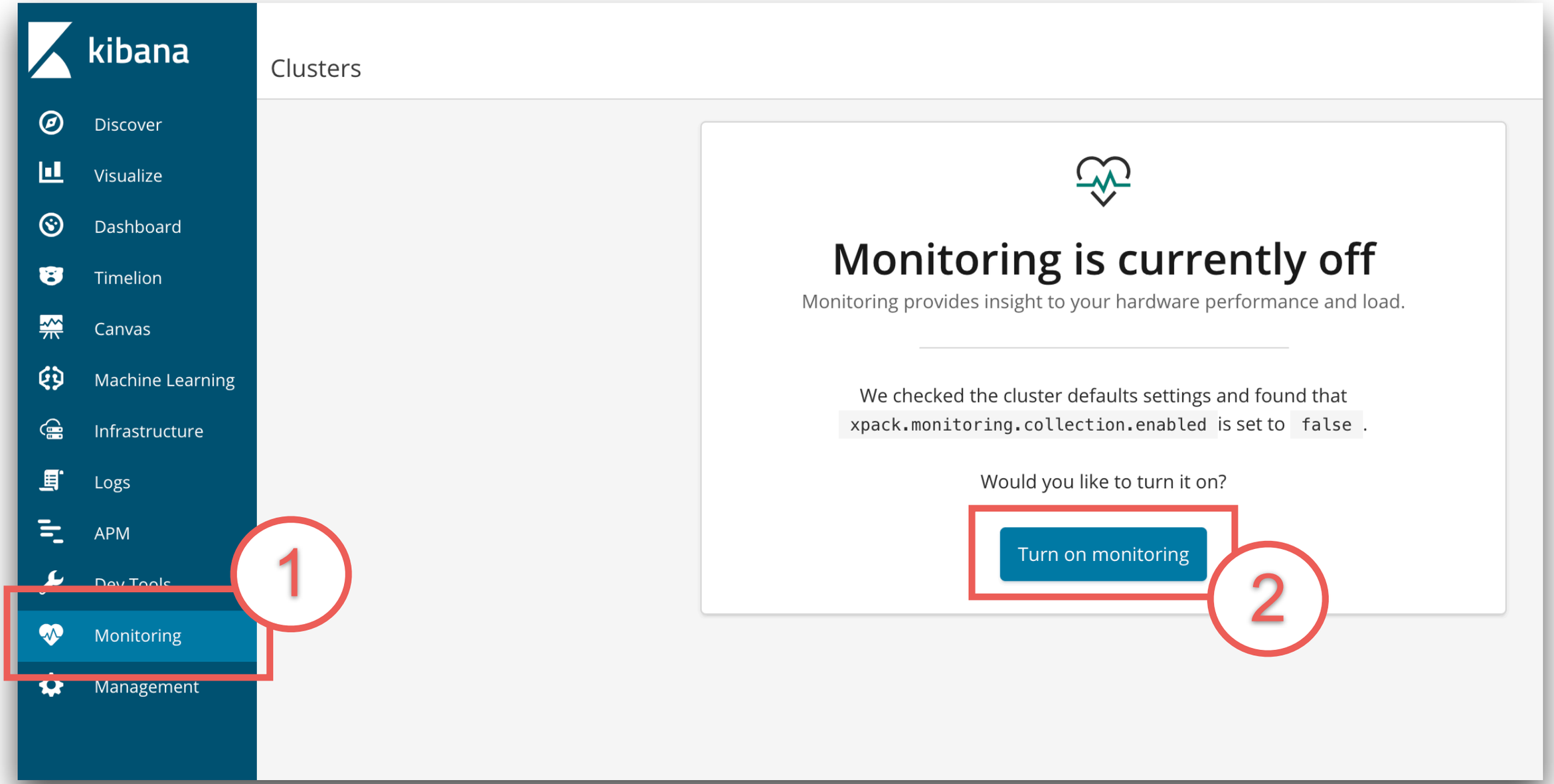
Redis logs
Collect and parse error and slow logs created by Redis.

System logs
Collect and parse logs written by the local Syslog server.

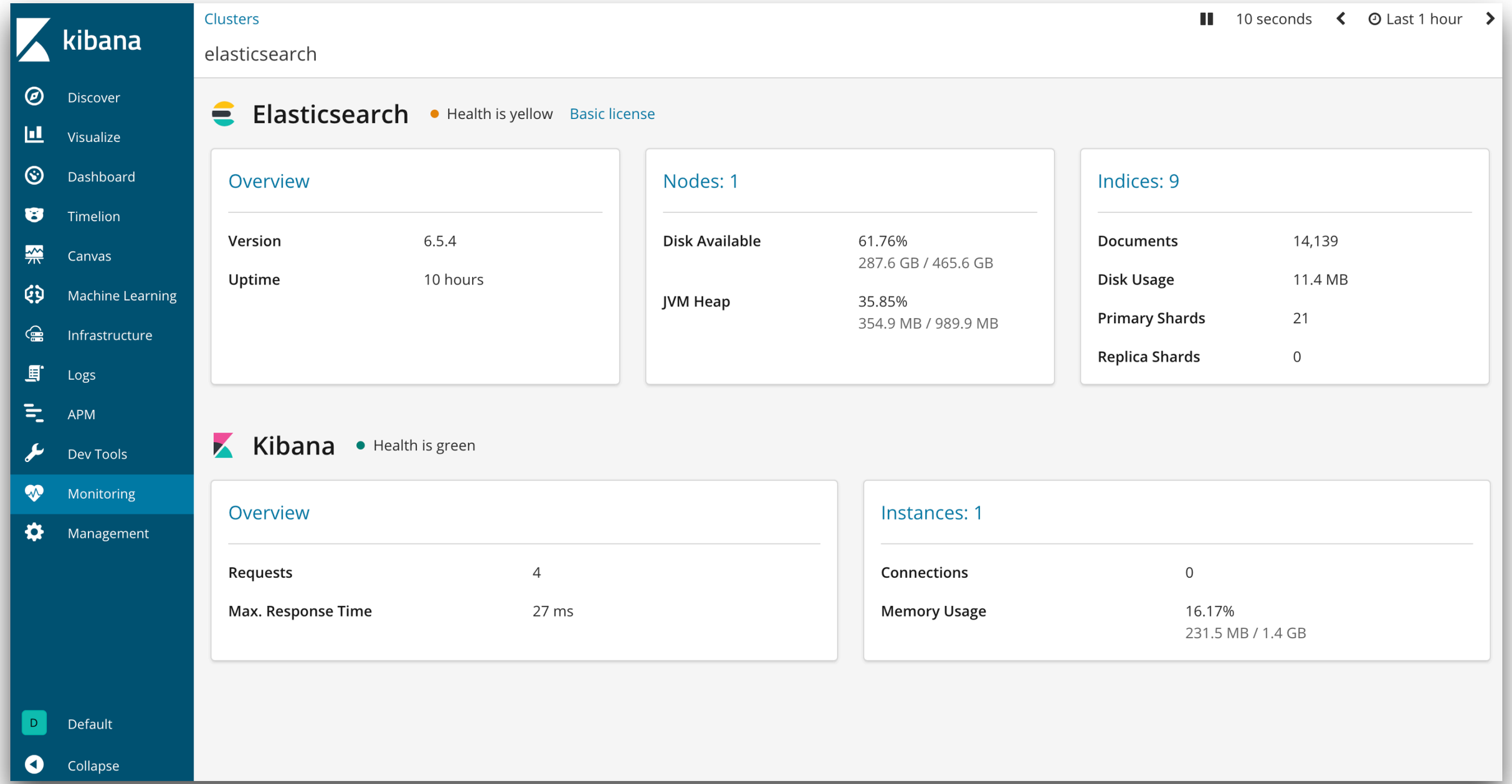
Traefik logs
Collect and parse access logs created by the Traefik Proxy.

Monitoring with Kibana

Enable monitoring in Kibana



Monitoring in Kibana



Subscription of Kibana

	FREE		GOLD	PLATINUM
	OPEN SOURCE	BASIC	Request Info	Request Info
	Download			
Kibana				
Explore & Visualize	✓	✓	✓	✓
Stack Management & Tooling	✓	✓	✓	✓
Stack Monitoring		✓	✓	✓
Full stack monitoring		✓	✓	✓
Multi-stack monitoring support			✓	✓
Configurable retention policy			✓	✓
Automatic alerts on stack issues			✓	✓
Share & Collaborate	✓	✓	✓	✓
Security			✓	✓
Alerting			✓	✓
Machine Learning		✓	✓	✓

https://www.elastic.co/subscriptions

Subscription of Beat

	FREE		GOLD	PLATINUM
	OPEN SOURCE	BASIC		
	Download		Request Info	Request Info
Beats				
Data Collection	✓	✓	✓	✓
Data Shipping	✓	✓	✓	✓
Modules	✓	✓	✓	✓
Monitoring and Management		✓	✓	✓
Beats monitoring		✓	✓	✓
Centralized Beats management			✓	✓

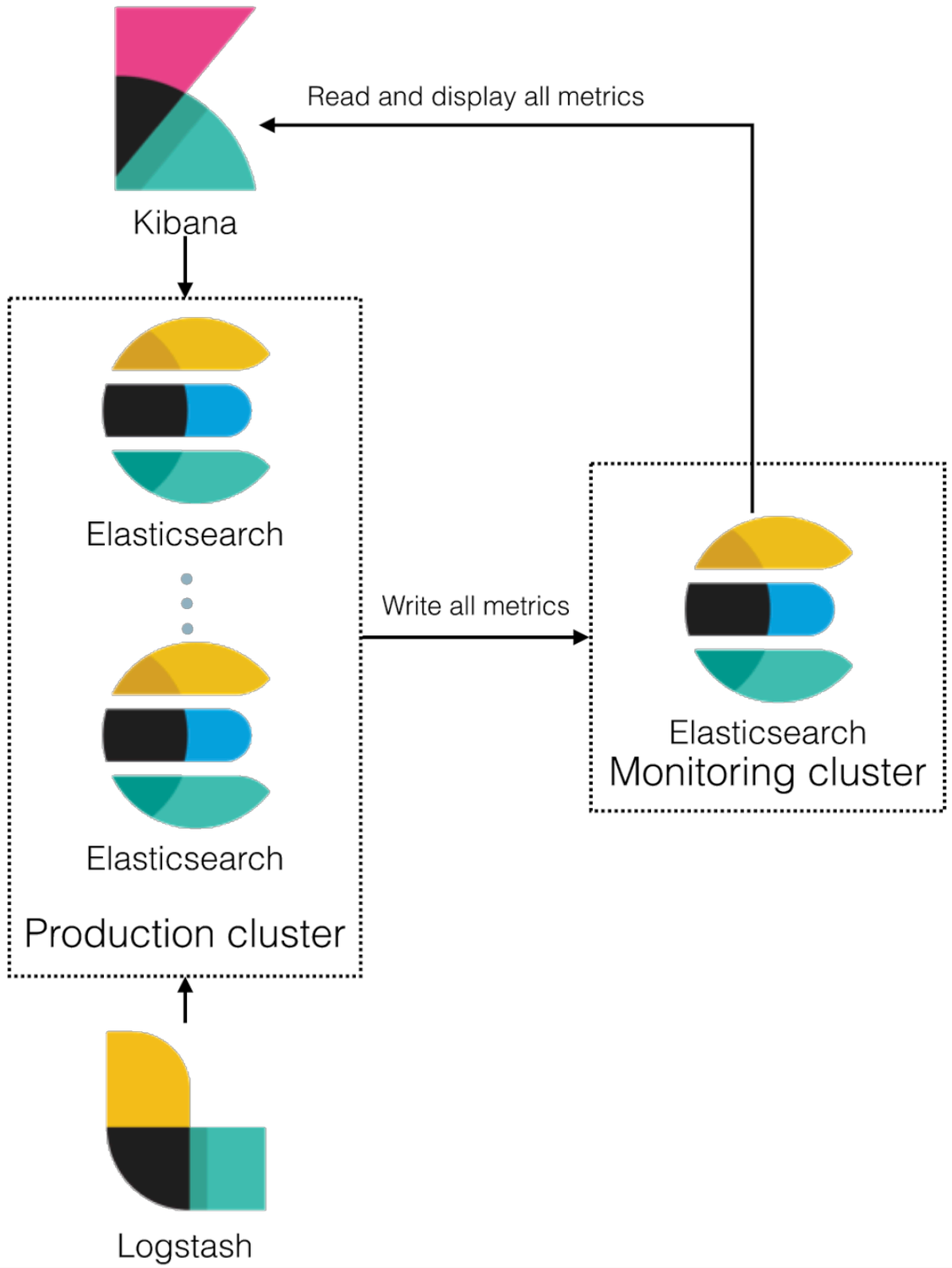
https://www.elastic.co/subscriptions

Collect data from ?

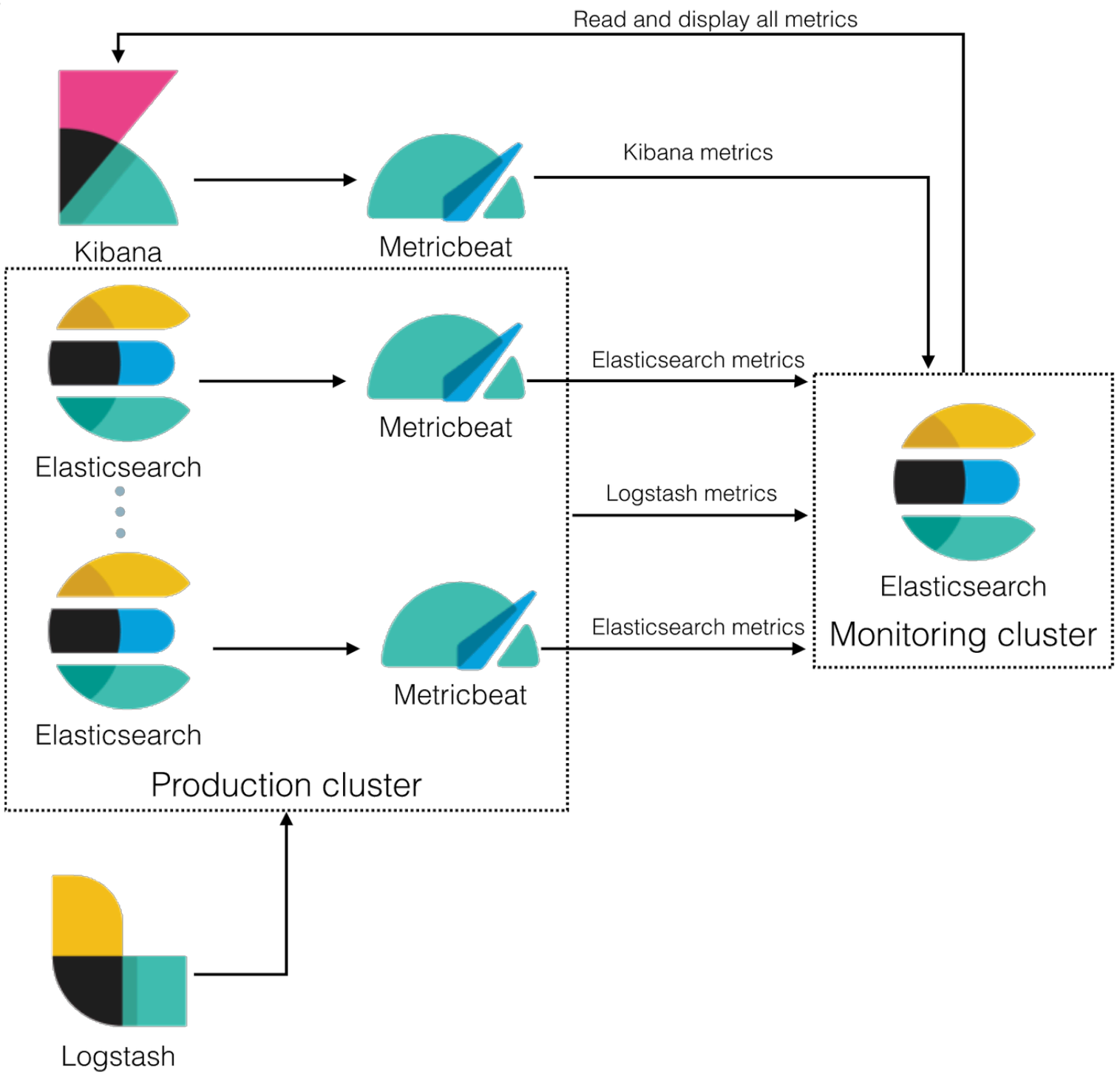
Elasticsearch nodes
Logstash nodes
Kibana instances

https://www.elastic.co/guide/en/elastic-stack-overview/6.5/xpack-monitoring.html

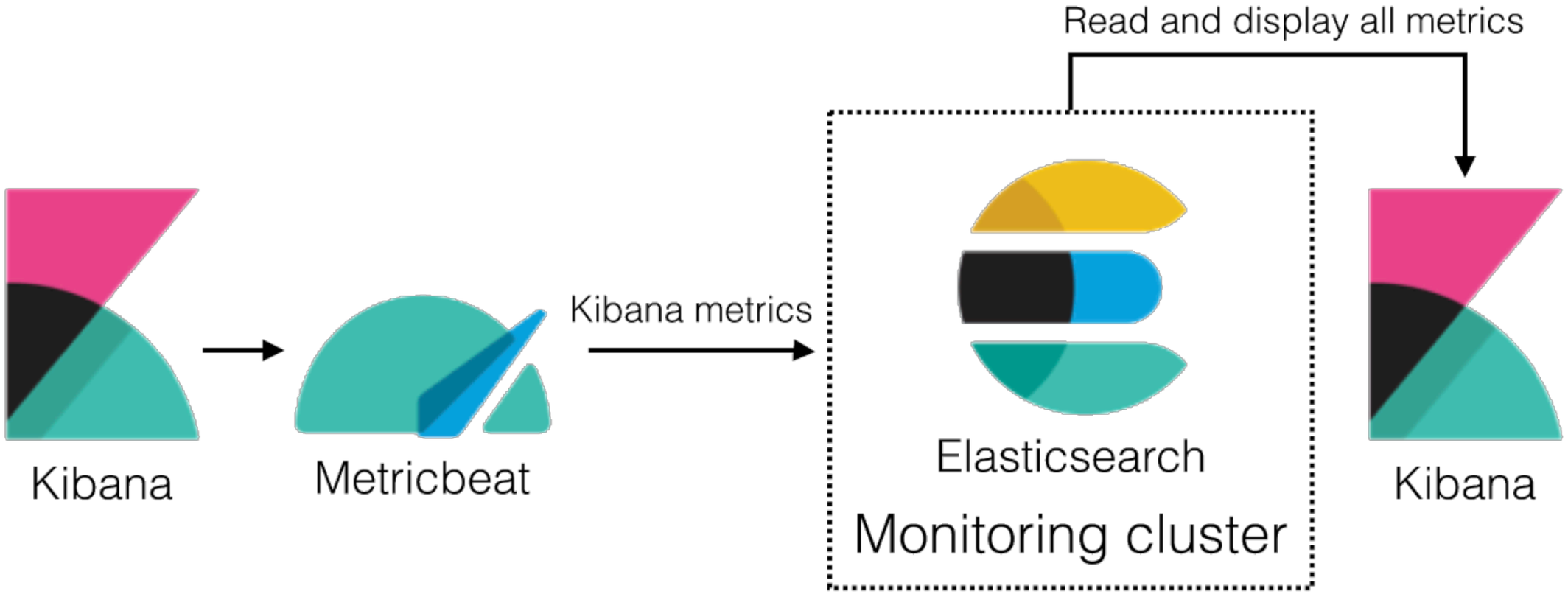
Recommend architecture



Elasticsearch 6.4 + (beta)



Try to separate kibana



Working with Logstash

https://www.elastic.co/guide/en/logstash/current/index.html

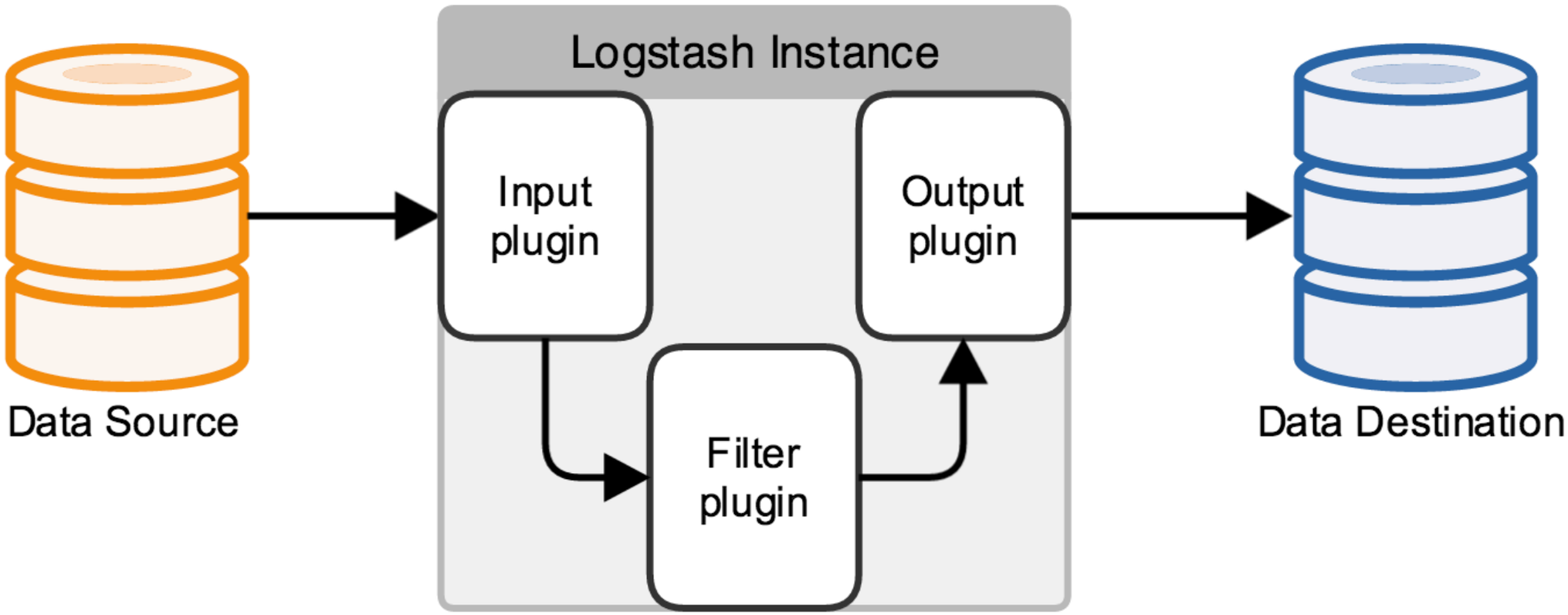
Logstash

Input

Filter

Output

Logstash



Inputs

File system
Syslog
Redis
Elasticsearch
Beats
More …

https://www.elastic.co/guide/en/logstash/current/input-plugins.html

Filters

Grok
Mutate
Drop
Clone
GeoIP
More …

https://www.elastic.co/guide/en/logstash/current/filter-plugins.html

Outputs

Elasticsersch
File system
StatsD
Graphite
More …

https://www.elastic.co/guide/en/logstash/current/output-plugins.html

Codecs

JSON
Multiple
Plain
RubyDebug

More …

https://www.elastic.co/guide/en/logstash/current/codec-plugins.html

Running Logstash

$./bin/logstash -f your-config.yml

Demo of configuration file /workshop/grok

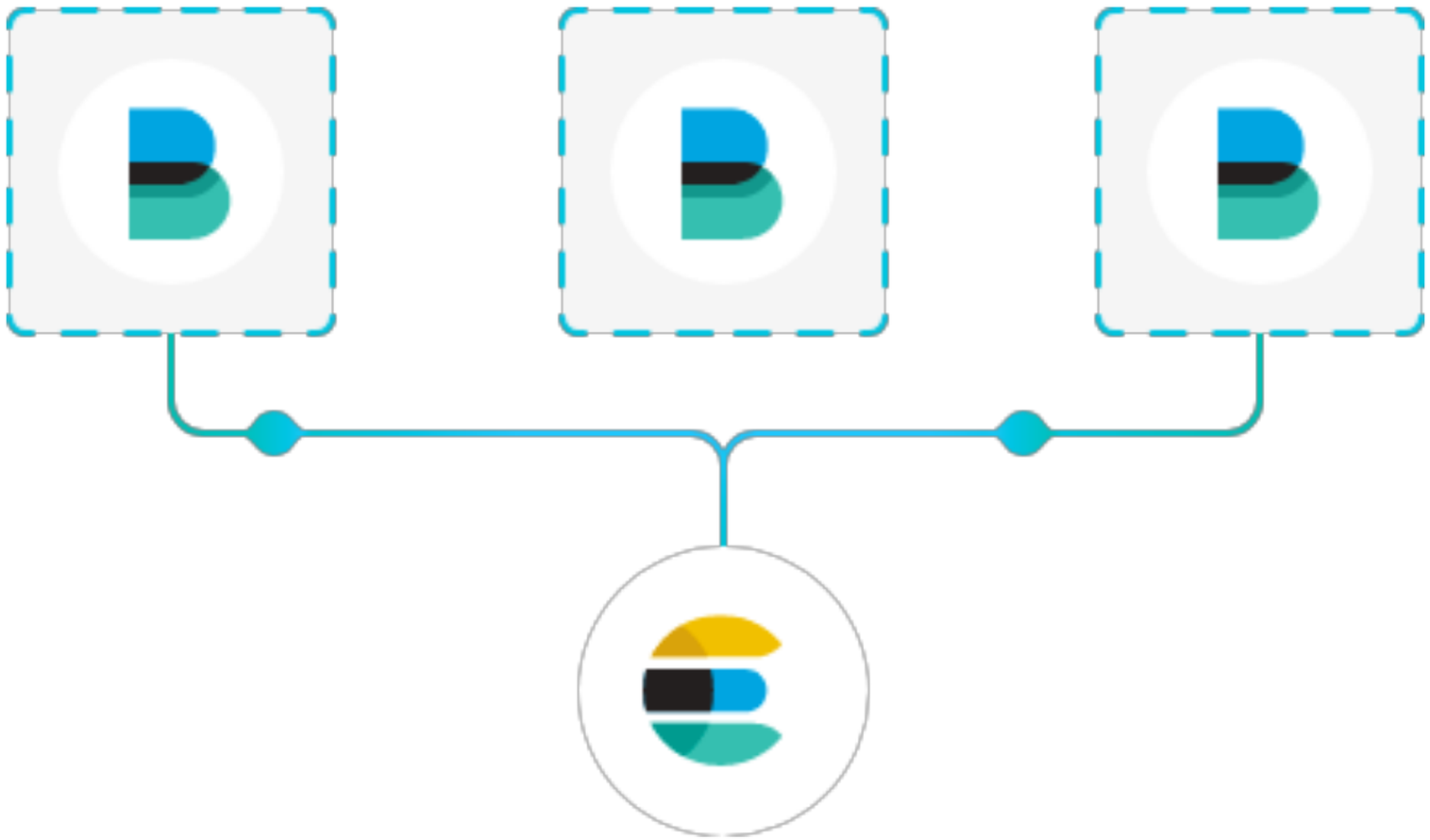
https://www.elastic.co/guide/en/logstash/current/running-logstash-command-line.html

Design your input first !!

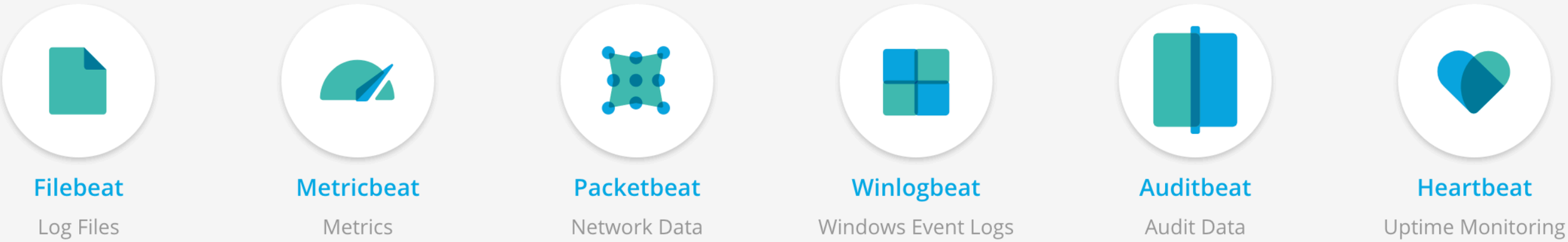
Use beats is better

https://www.elastic.co/products/beats

Beat



Beat

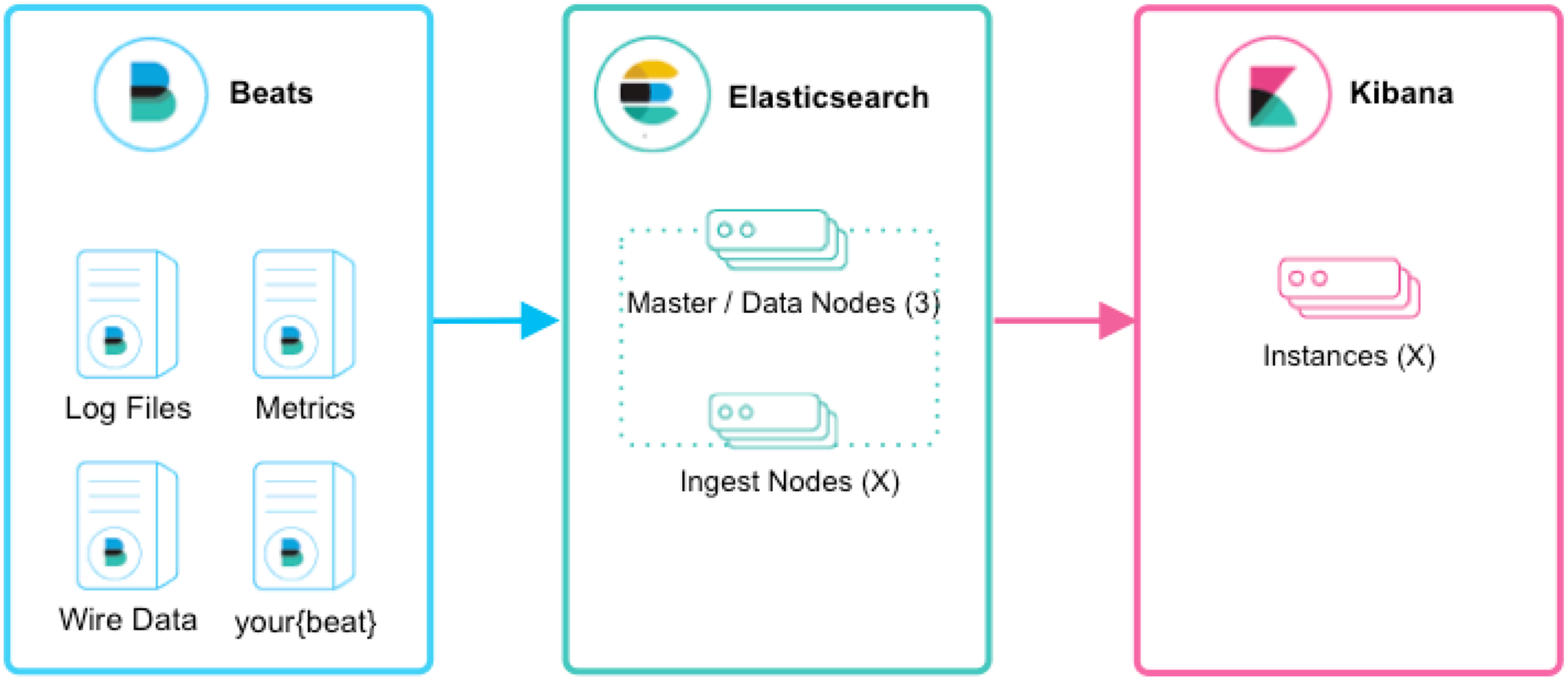


Example

$filebeat -e -c **beat.yml** -d "publish"

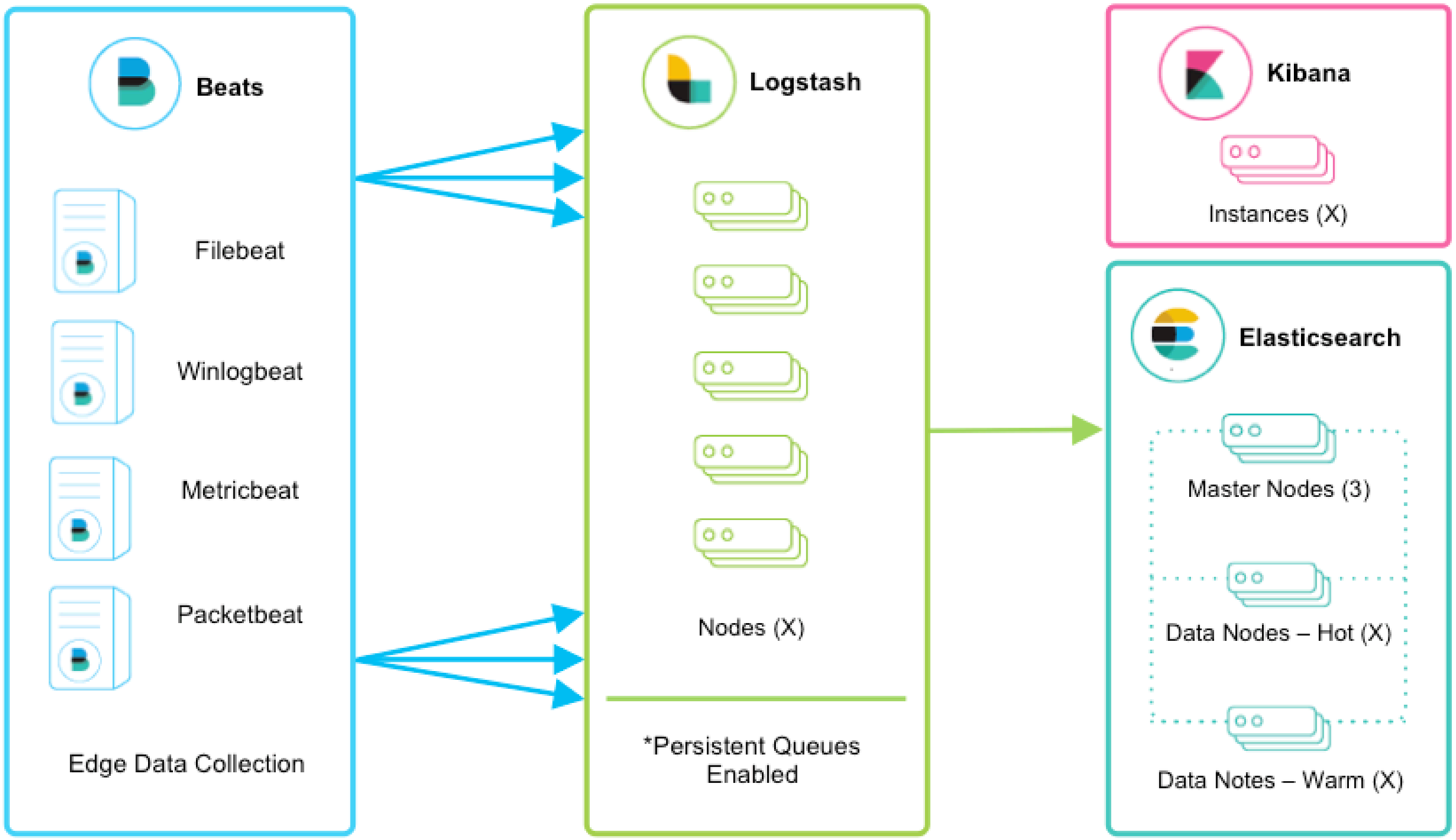
https://www.elastic.co/guide/en/beats/filebeat/current/index.html

Beat and Logstash



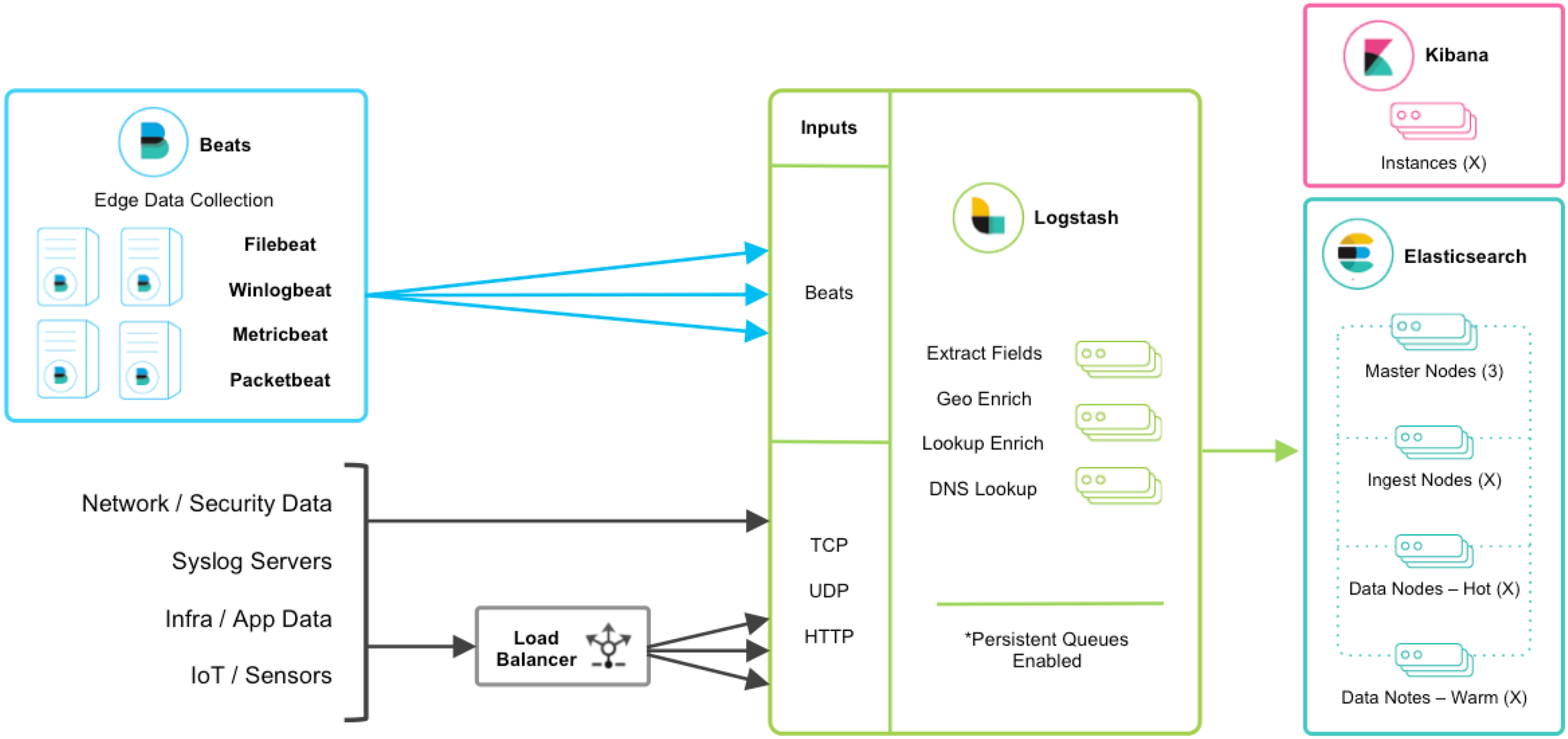
https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html

Scaling



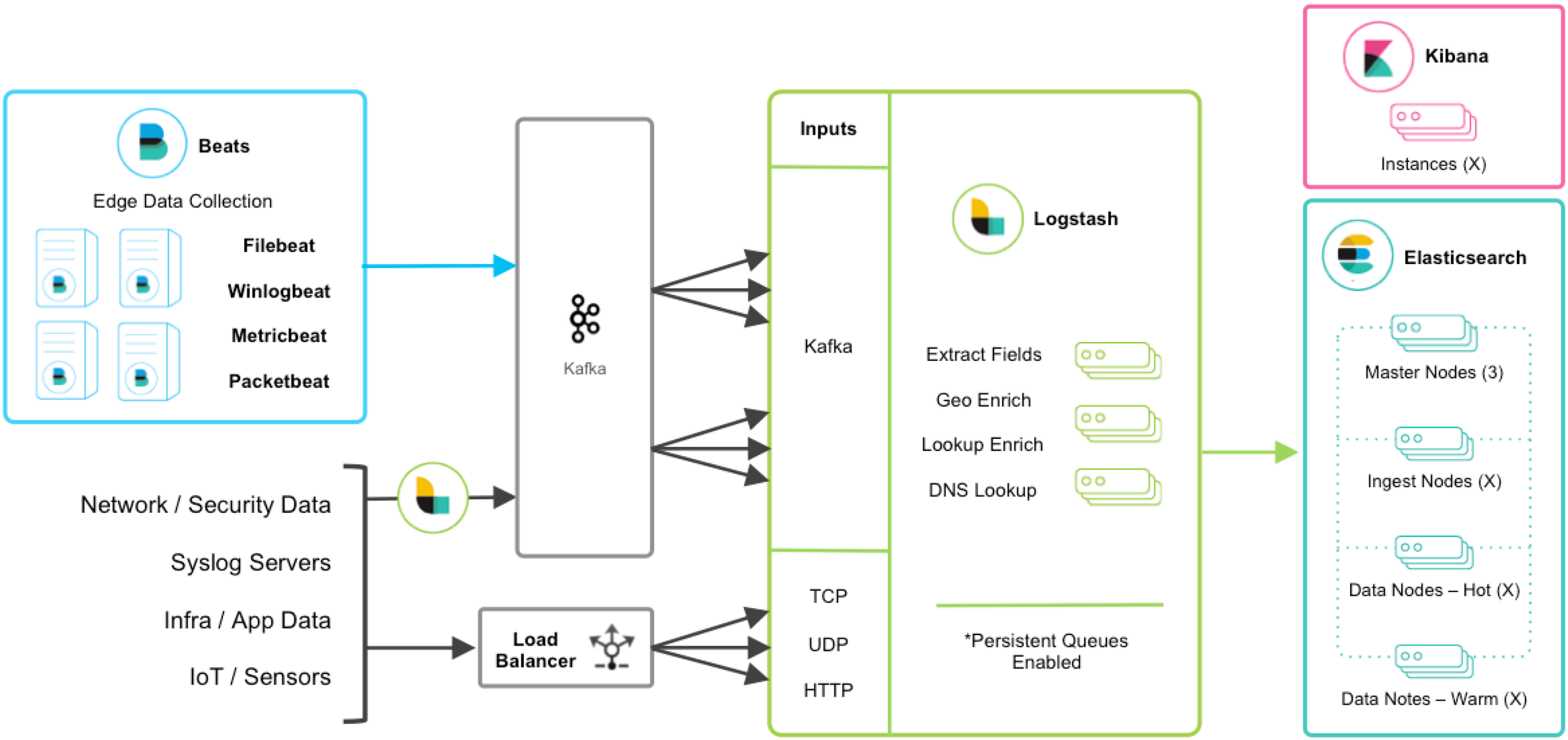
https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html

More data sources



https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html

Use messaging Queue



https://www.elastic.co/blog/logstash-persistent-queue