



# Kibana













Somkiat

Home






Somkiat Puisungnoen

Update Info
1

View Activity Log
10+

...


Timeline
About
Friends 3,138
Photos
More ▾



When did you work at Opendream?
×

...
22 Pending Items


Intro


Software Craftsmanship



Software Practitioner at สยามชำนาญกิจ พ.ศ. 2556



Agile Practitioner and Technical at SPRINT3r



Post


Photo/Video


Live Video


Life Event


What's on your mind?


Public ▾

Post



Somkiat Puisungnoen
15 mins · Bangkok · ▾

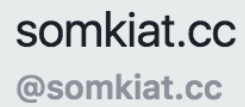
Java and Bigdata

...

© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

ELK Stack

3



## Photos



+ Add a Button

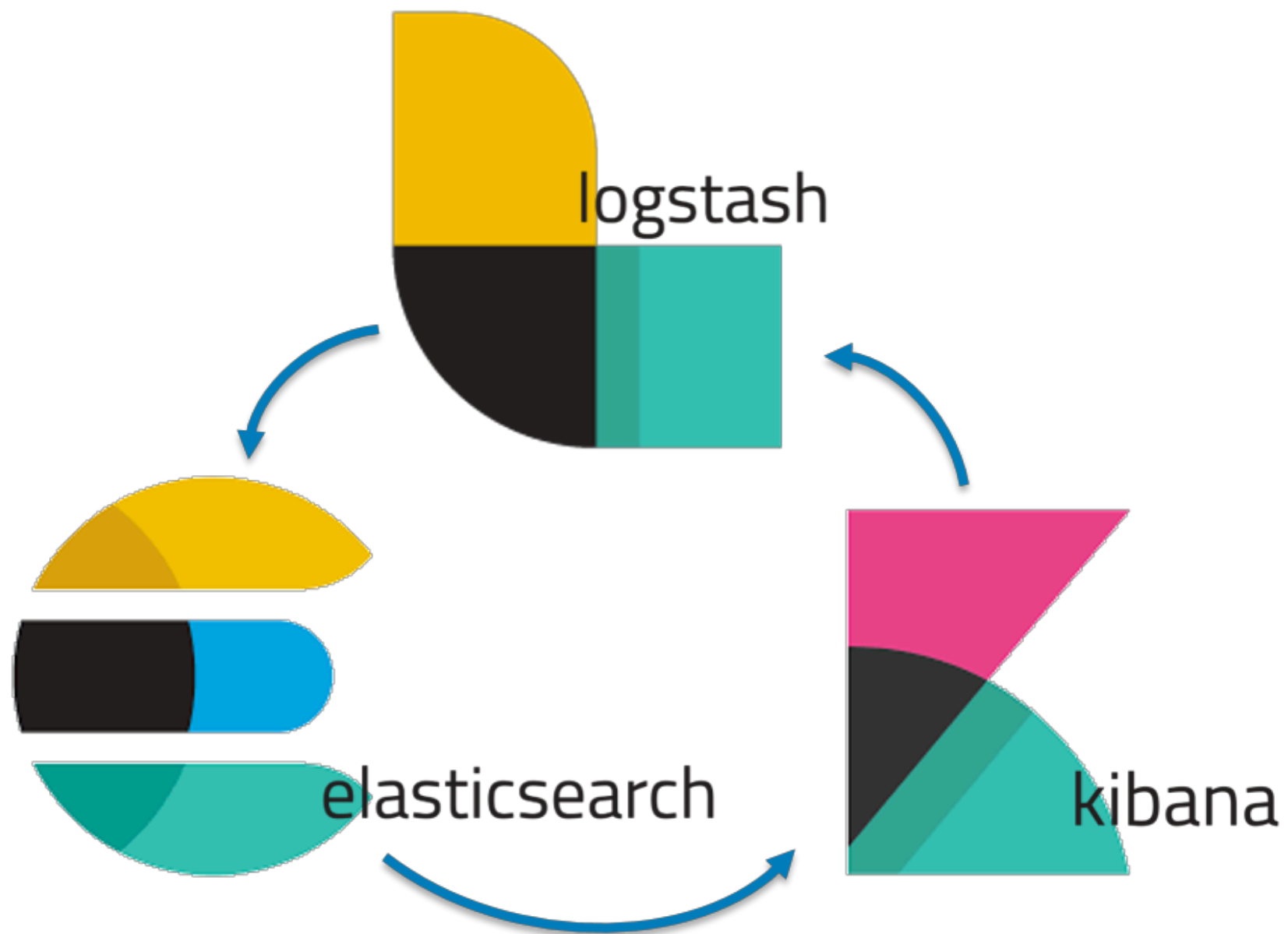
**[https://github.com/up1/course\\_elk](https://github.com/up1/course_elk)**



# Agenda

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

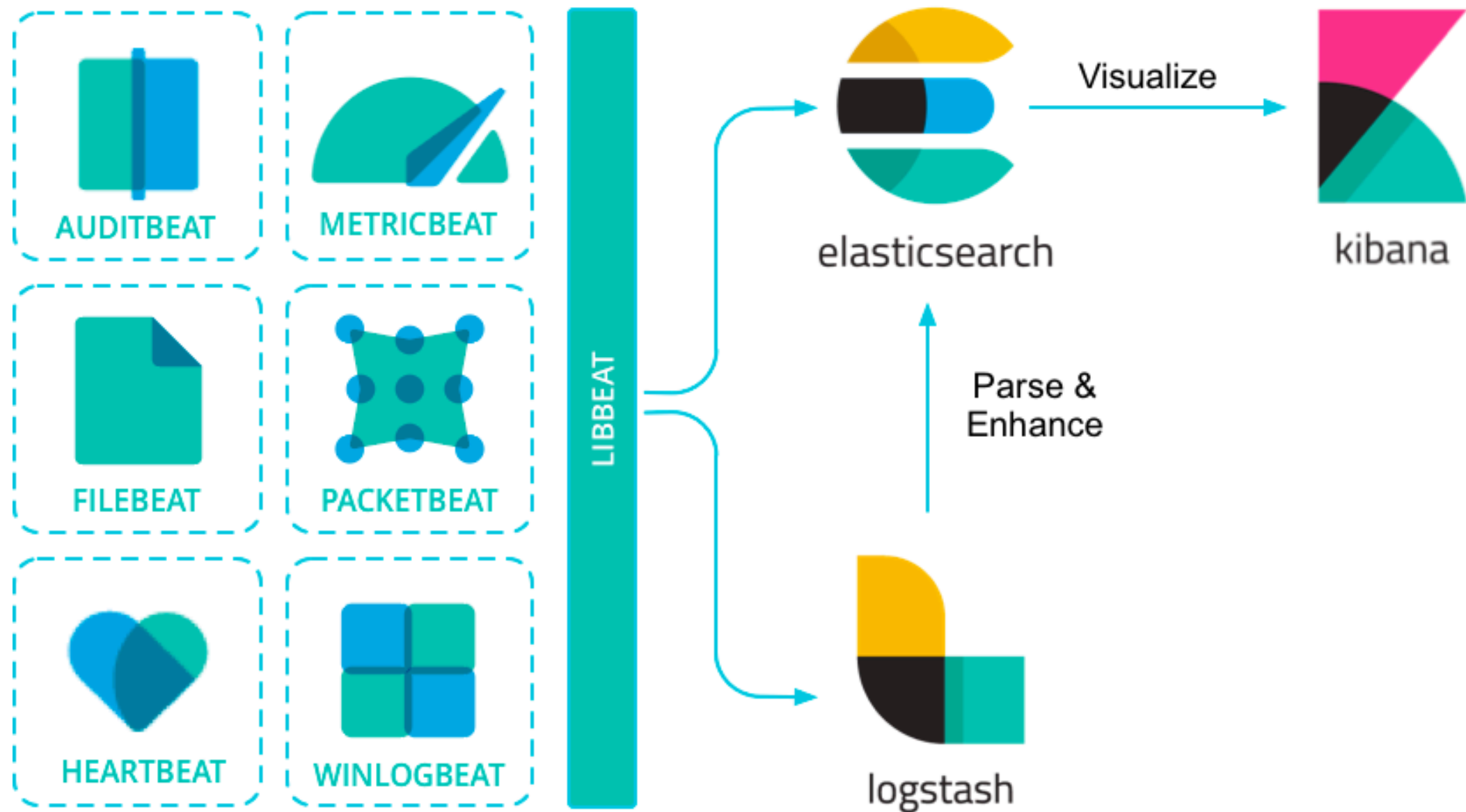








# Beat



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



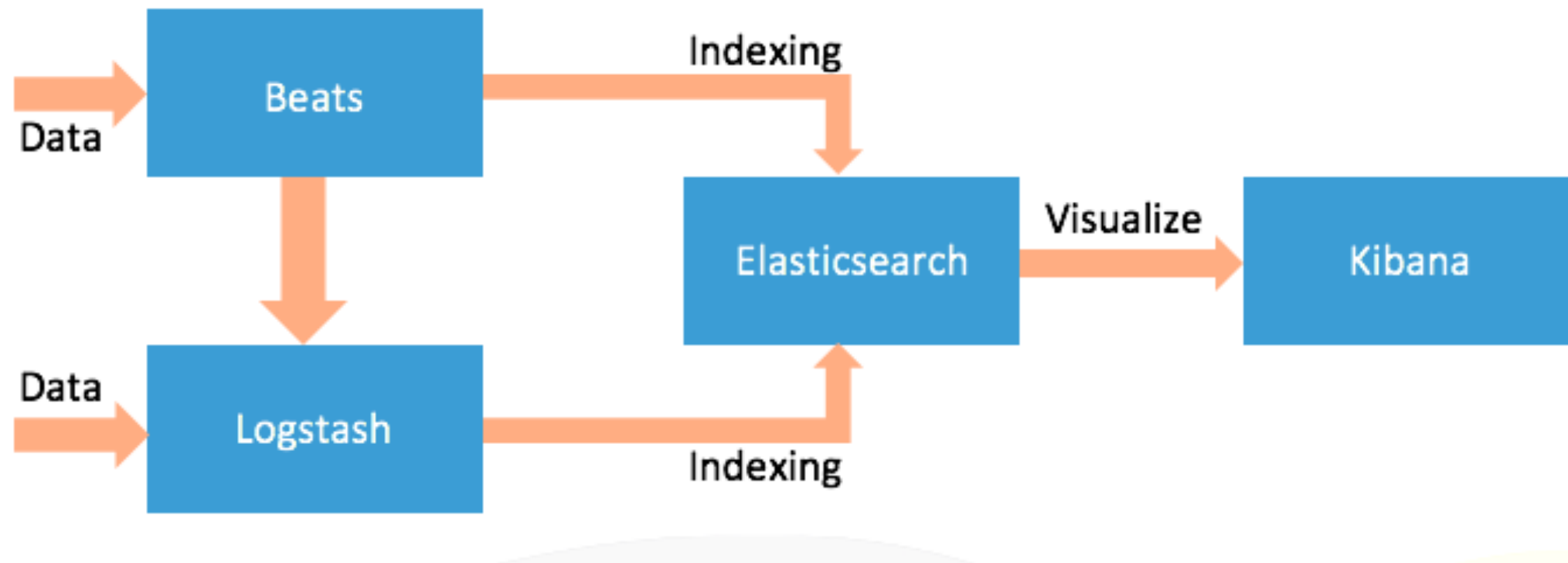
# Beat

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



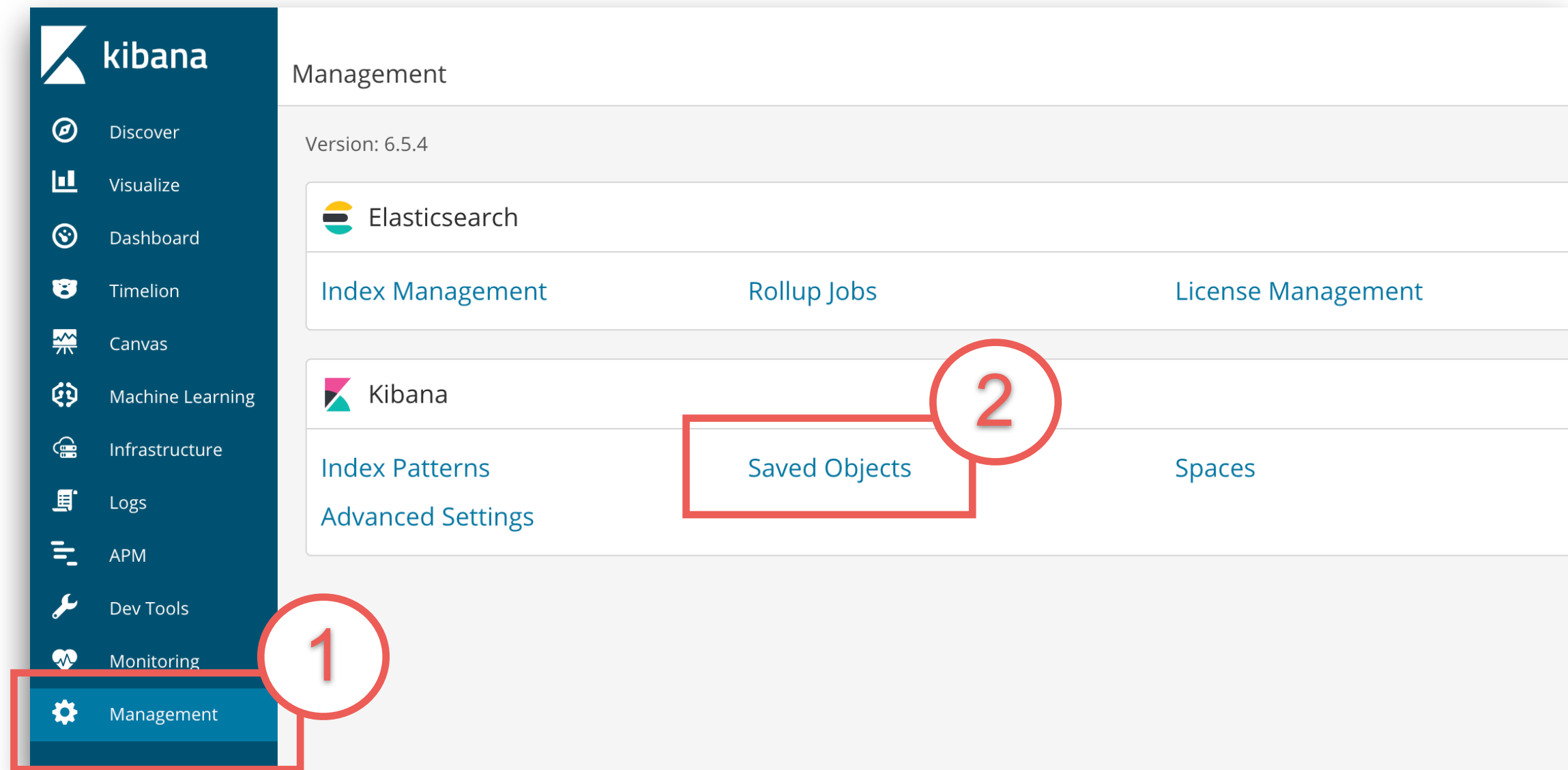
# Kibana

Create visualization  
Create dashboard  
Infrastructure  
Monitoring



# Import/Export

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



# Import/Export

## Working with JSON file

### Saved Objects

























[Export 17 objects](#) [Import](#) [Refresh](#)

From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen.

Type ▾

Delete

Export

<input type="checkbox"/>	Type	Title	Actions
<input type="checkbox"/>		D1	 
<input checked="" type="checkbox"/>		[Logs] Web Traffic	 
<input type="checkbox"/>		store	 
<input type="checkbox"/>		kibana_sample_data_logs	 
<input type="checkbox"/>		S1	 
<input type="checkbox"/>		G1	 
<input type="checkbox"/>		[Logs] Unique Visitors vs. Average Bytes	 
<input type="checkbox"/>		[Logs] Unique Visitors by Country	 



BETA

# Infrastructure with Kibana

*Elasticsearch and Kibana 6.5 +*





# Setup instruction

The screenshot shows the Kibana web interface. On the left is a dark blue sidebar with the 'kibana' logo at the top. Below the logo are several menu items, each with an icon: Discover (magnifying glass), Visualize (bar chart), Dashboard (circular arrows), Timelion (calendar), Canvas (wavy lines), Machine Learning (brain), Infrastructure (server rack), Logs (document), APM (three horizontal lines), Dev Tools (wrench), Monitoring (heart with pulse), and Management (gear). A red circle with the number '1' is drawn around the 'Infrastructure' and 'Logs' items, which are also enclosed in a red rectangular box. The main content area on the right is white and contains the text 'Looks like you don't have any metrics indices.' followed by 'Let's add some!'. Below this text is a blue button labeled 'Setup Instructions', which is highlighted by a red rectangular box and a red circle with the number '2'.

kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Canvas
- Machine Learning
- Infrastructure
- Logs
- APM
- Dev Tools
- Monitoring
- Management

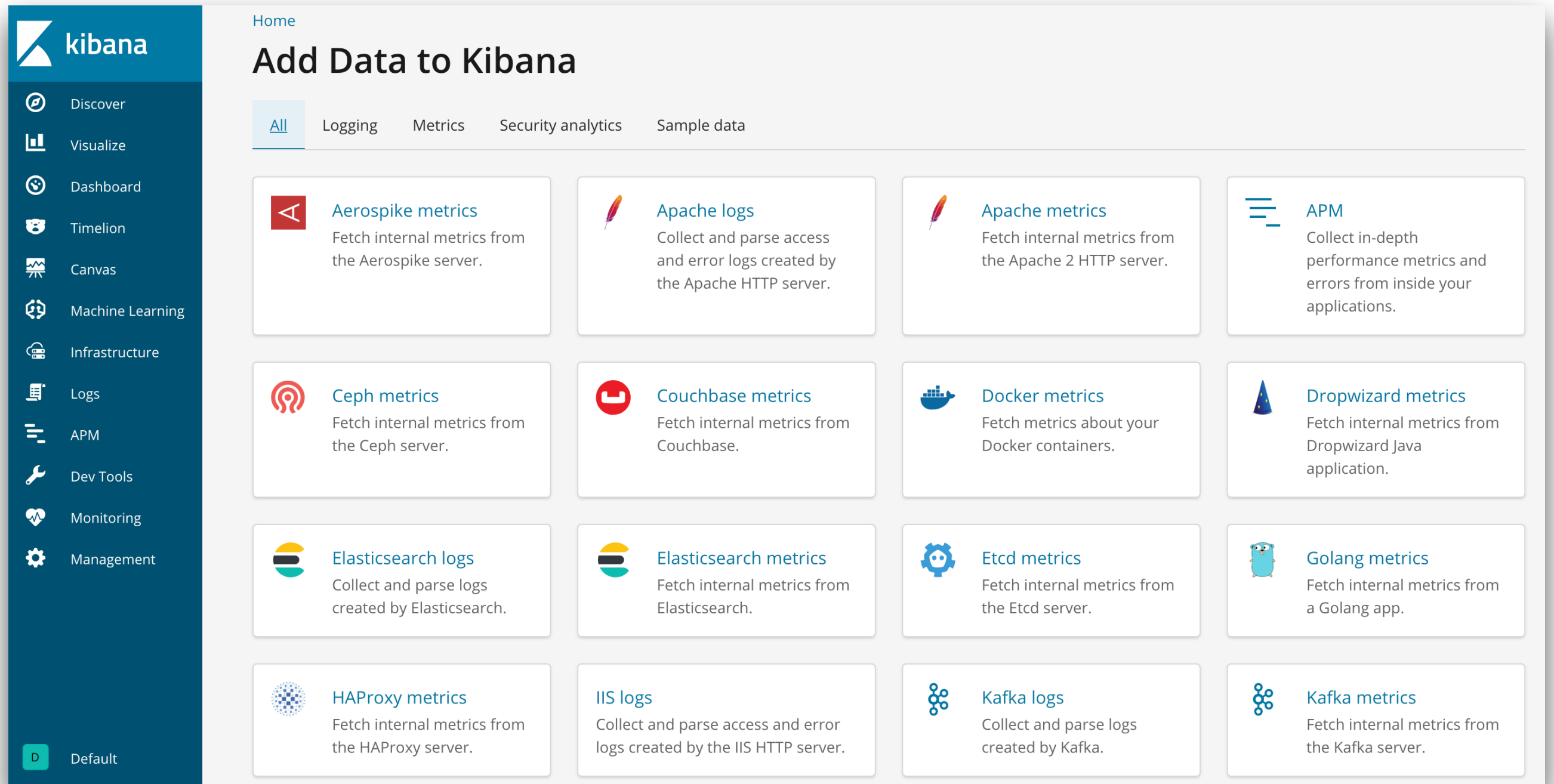
Looks like you don't have any metrics indices.

Let's add some!

Setup Instructions



# Add data to Kibana



Home

## Add Data to Kibana

[All](#) Logging Metrics Security analytics Sample data

- Aerospike metrics**  
Fetch internal metrics from the Aerospike server.
- Apache logs**  
Collect and parse access and error logs created by the Apache HTTP server.
- Apache metrics**  
Fetch internal metrics from the Apache 2 HTTP server.
- APM**  
Collect in-depth performance metrics and errors from inside your applications.
- 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 logs**  
Collect and parse logs created by Elasticsearch.
- 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.
- IIS logs**  
Collect and parse access and error logs created by the IIS HTTP server.
- Kafka logs**  
Collect and parse logs created by Kafka.
- Kafka metrics**  
Fetch internal metrics from the Kafka server.



# Monitor your infrastructure

Monitor hosts and containers

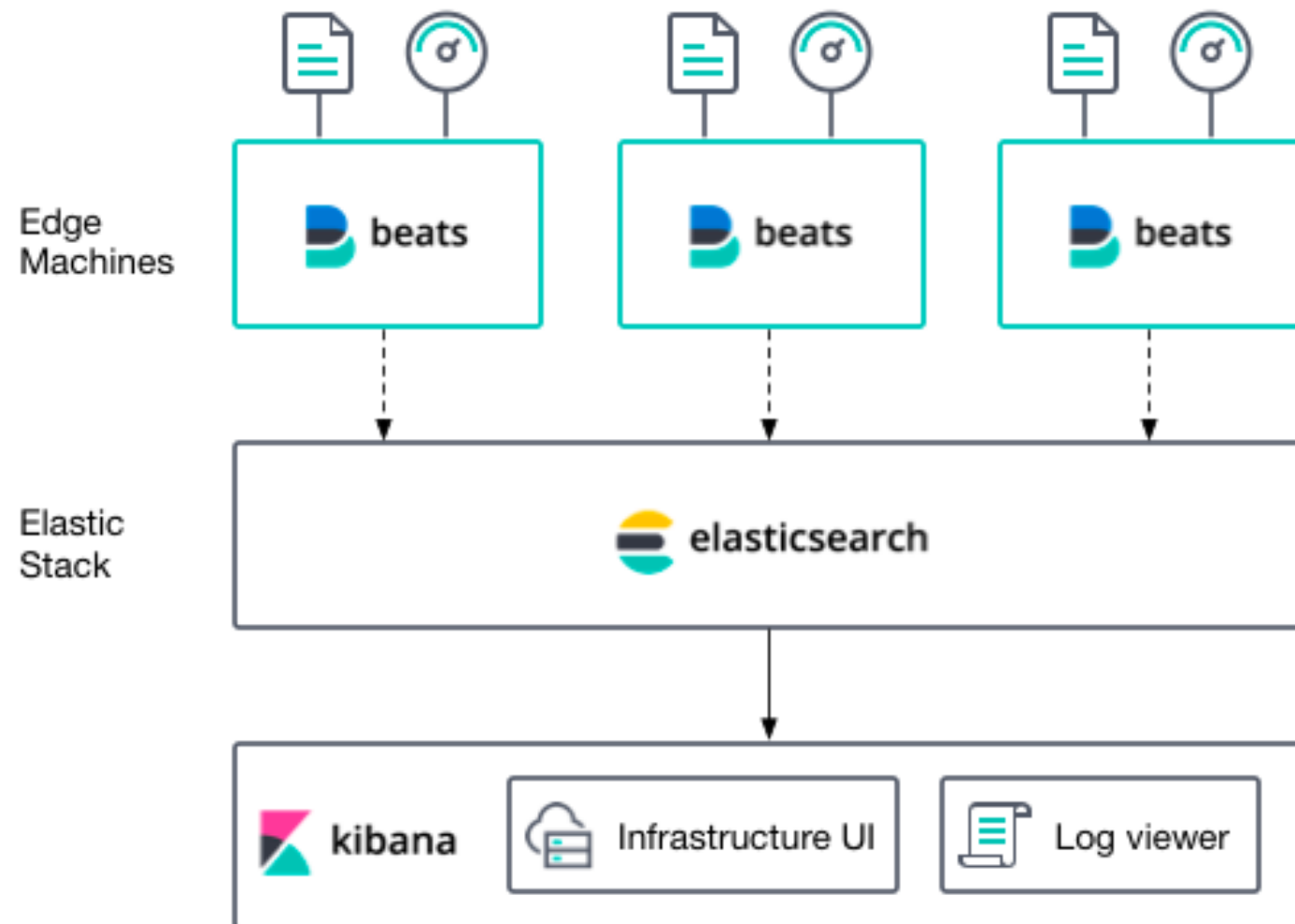
View metrics

View logs

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



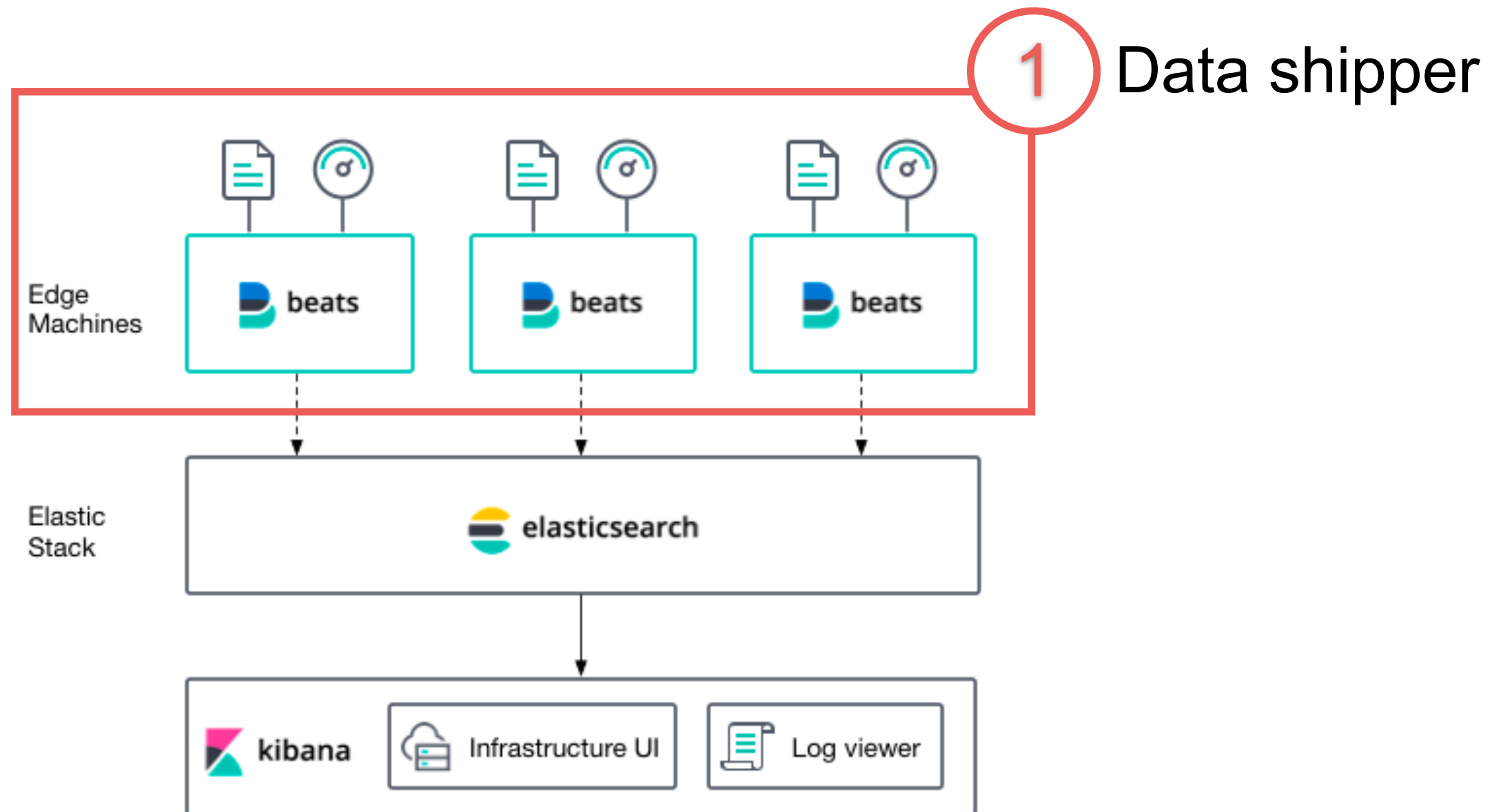
# Infrastructure monitoring



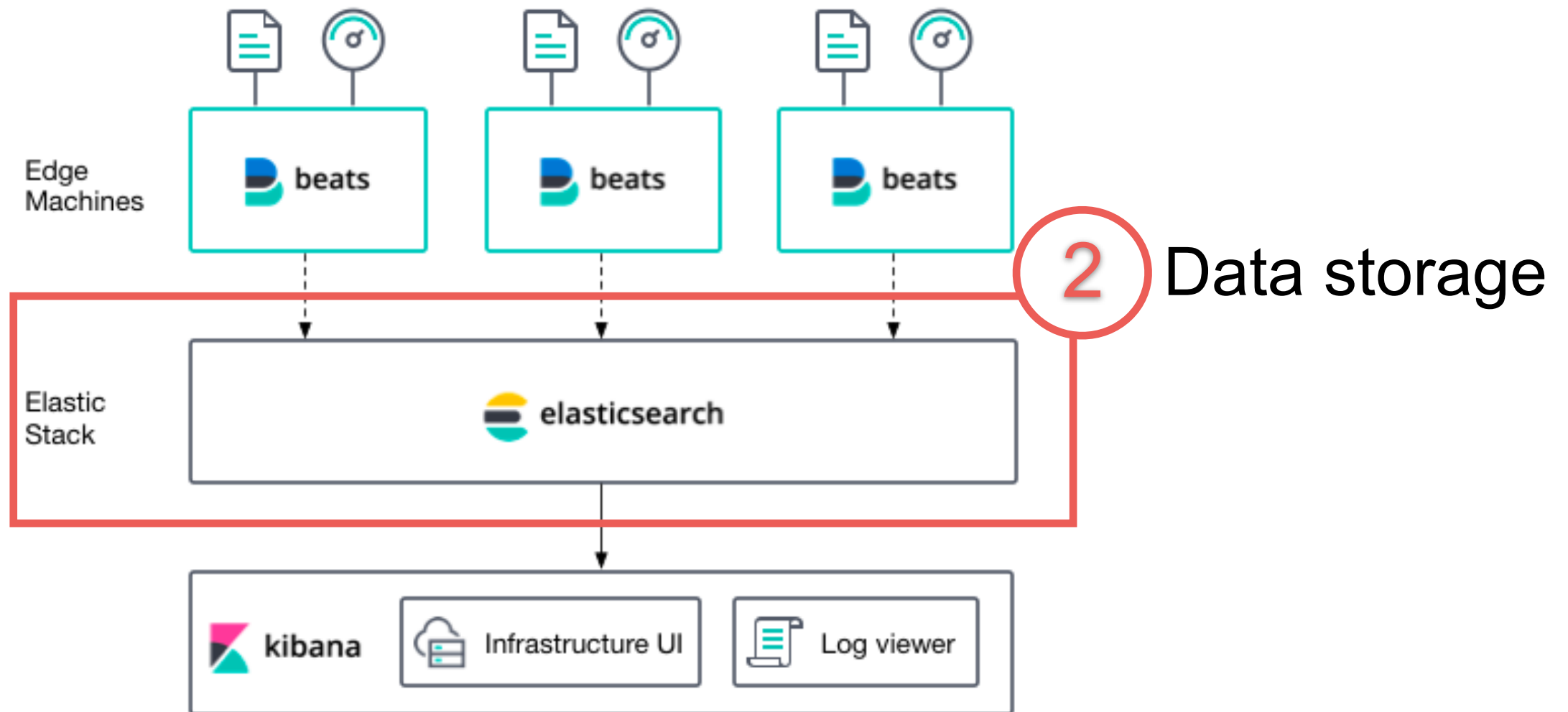
<https://www.elastic.co/guide/en/infrastructure/guide/6.5/infrastructure-monitoring-overview.html>



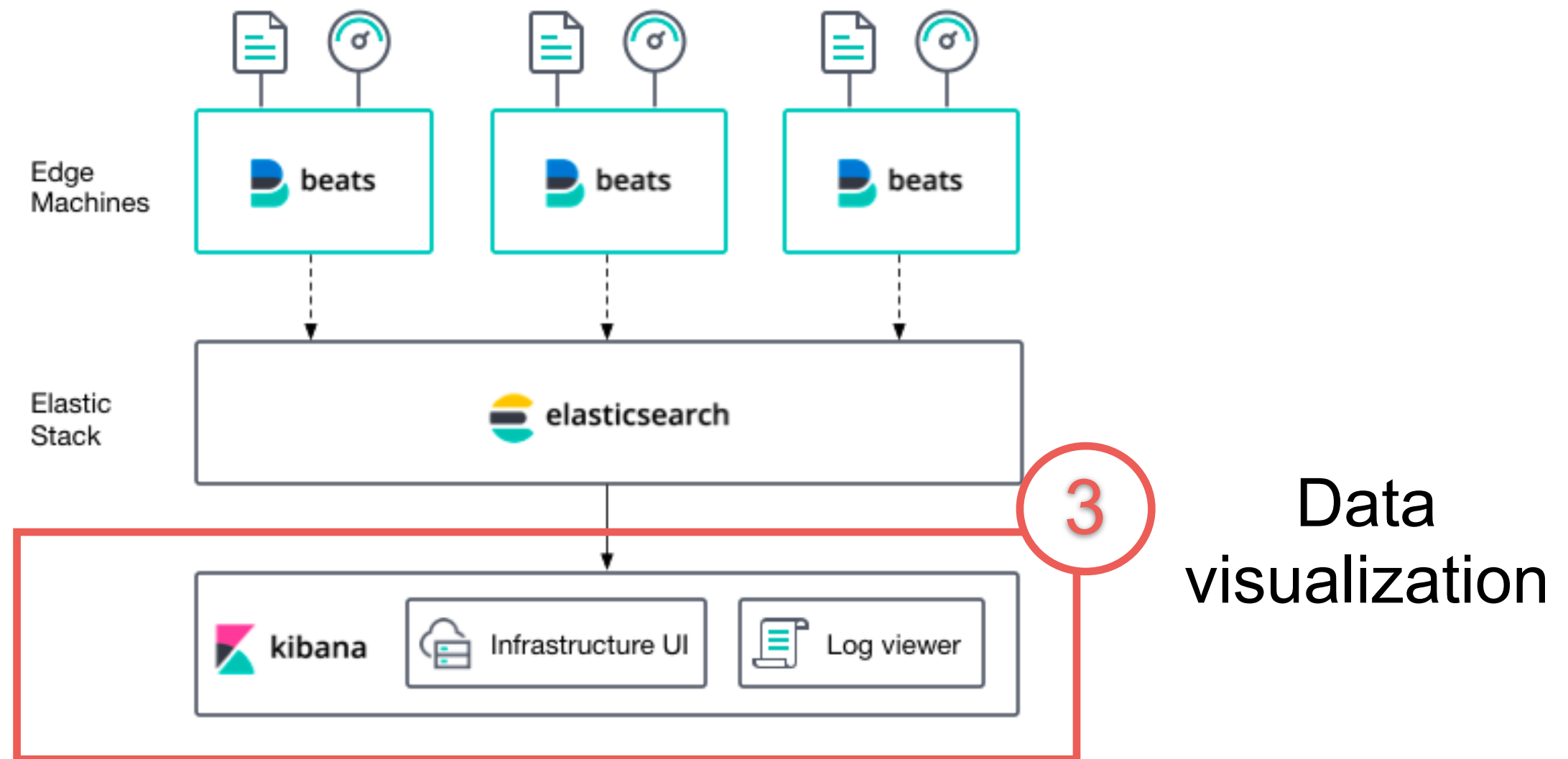
# Infrastructure monitoring



# Infrastructure monitoring



# Infrastructure monitoring



# 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 internal 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 Elasticsearch 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

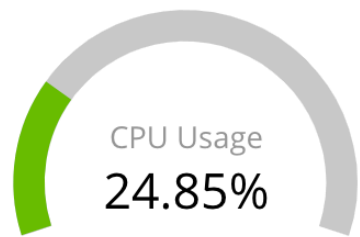
## Dashboards

[Create new dashboard](#)

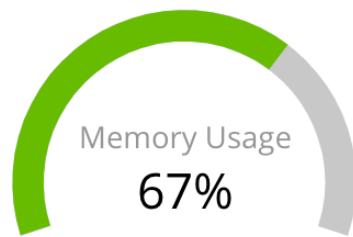
<input type="checkbox"/> Title	Description	Actions
<input type="checkbox"/> <a href="#">[Metricbeat Docker] Overview</a>	Overview of docker containers	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat Apache] Overview</a>	Overview of Apache server status	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat System] Containers overview</a>	Overview of container metrics	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat Golang] Overview</a>	Overview of Go profiling information	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat HAProxy] HTTP backend</a>	HAProxy HTTP backend metrics	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat HAProxy] Backend</a>	HAProxy backend metrics	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat HAProxy] Frontend</a>	HAProxy frontend metrics	<a href="#">Edit</a>
<input type="checkbox"/> <a href="#">[Metricbeat System] Host overview</a>	Overview of host metrics	<a href="#">Edit</a>



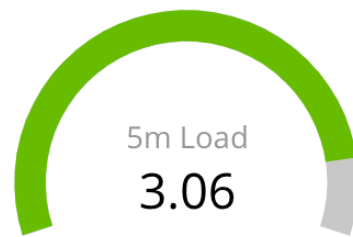
# Host overview dashboard



Swap usage [Metricbeat...



Memory usage vs total



Number of processes [...

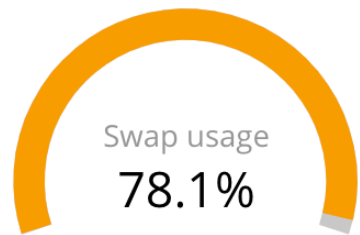
Inbound Traffic  
**132.531KB/s**  
Total Transferred 45.333MB

Disk used [Metricbeat S...

Outbound Traffic  
**1.331MB/s**  
Total Transferred 638.012MB

Disk Usage [Metricbeat System]

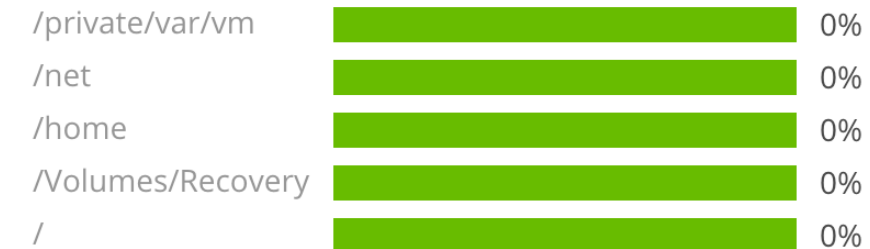
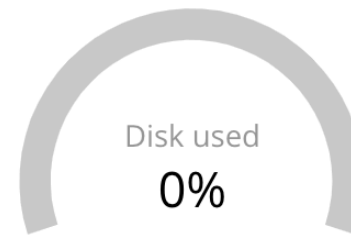
In Packetloss  
**0**  
Out Packetloss 205



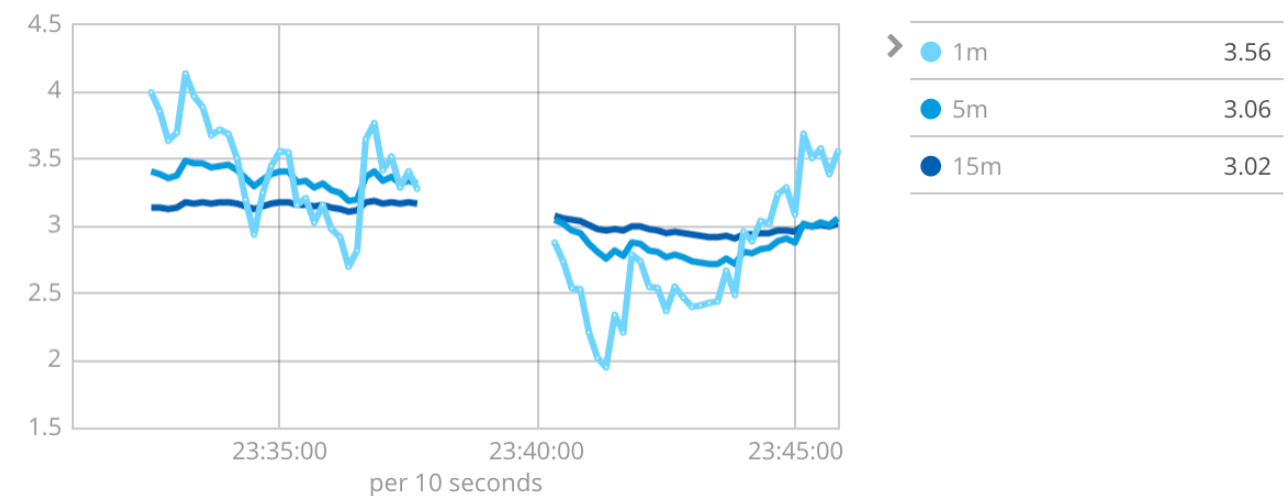
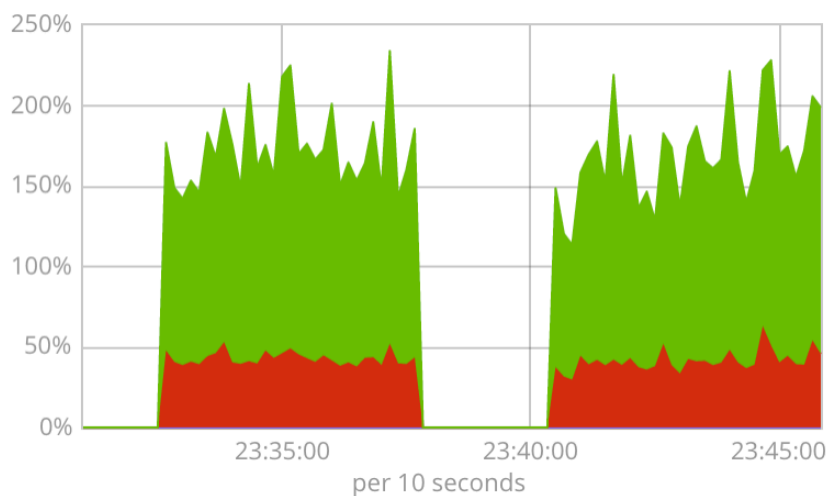
CPU Usage [Metricbeat System]

Memory usage  
**10.72GB**  
Total Memory 16GB

**27**  
Processes



System Load [Metricbeat System]



# 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

The screenshot shows the Kibana web interface. On the left is a dark blue sidebar with the 'kibana' logo at the top. Below the logo are several menu items: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The 'Monitoring' item is highlighted with a red box and a red circle containing the number '1'. The main content area has a light gray background with the title 'Clusters' at the top. In the center of this area is a white card with a heart icon and a pulse line. The card contains the text 'Monitoring is currently off' and 'Monitoring provides insight to your hardware performance and load.' Below this, it says 'We checked the cluster defaults settings and found that `xpack.monitoring.collection.enabled` is set to `false`.' At the bottom of the card, it asks 'Would you like to turn it on?' and features a blue button labeled 'Turn on monitoring'. This button is highlighted with a red box and a red circle containing the number '2'.



# Monitoring in Kibana

The screenshot displays the Kibana Monitoring dashboard. On the left is a dark blue sidebar with the Kibana logo and navigation links: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring (selected), and Management. At the bottom of the sidebar are buttons for 'Default' and 'Collapse'.

The main content area is titled 'Clusters' and shows the 'elasticsearch' cluster. At the top right of this section are controls for a live view: a pause icon, '10 seconds', and a time range selector set to 'Last 1 hour'.

The Elasticsearch section features a header with the Elasticsearch logo, 'Health is yellow', and a link to 'Basic license'. It contains three overview cards:

- Overview:** Version 6.5.4, Uptime 10 hours.
- Nodes: 1:** Disk Available 61.76% (287.6 GB / 465.6 GB), JVM Heap 35.85% (354.9 MB / 989.9 MB).
- Indices: 9:** Documents 14,139, Disk Usage 11.4 MB, Primary Shards 21, Replica Shards 0.

The Kibana section features a header with the Kibana logo, 'Health is green', and an 'Overview' card:

- Overview:** Requests 4, Max. Response Time 27 ms.

To the right of the Kibana Overview card is an 'Instances: 1' card:

- Connections:** 0
- Memory Usage:** 16.17% (231.5 MB / 1.4 GB)



# Subscription of Kibana

	FREE		GOLD	PLATINUM
	OPEN SOURCE	BASIC		
	Download		Request Info	Request Info
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

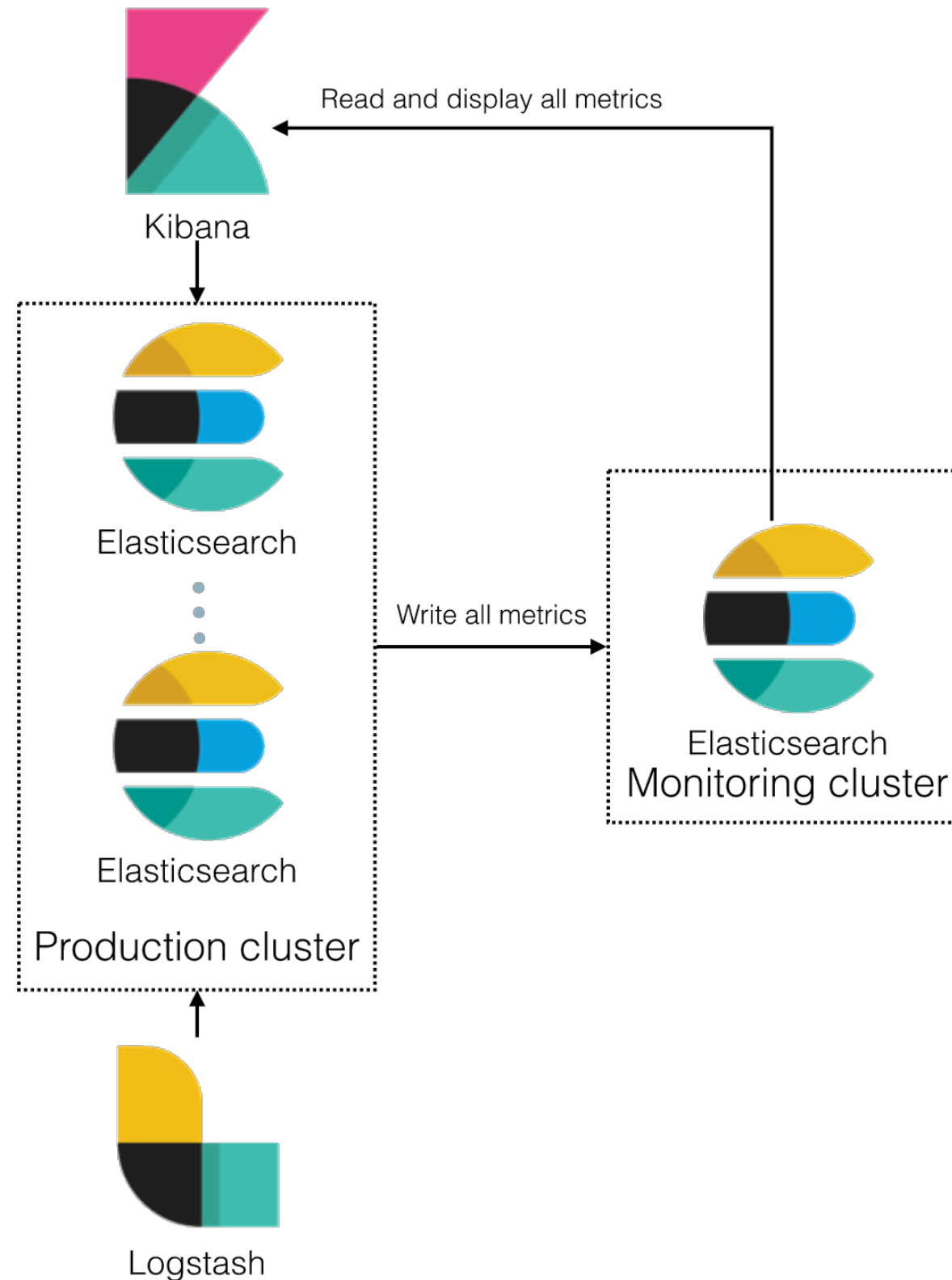
Logstash nodes

Kibana instances

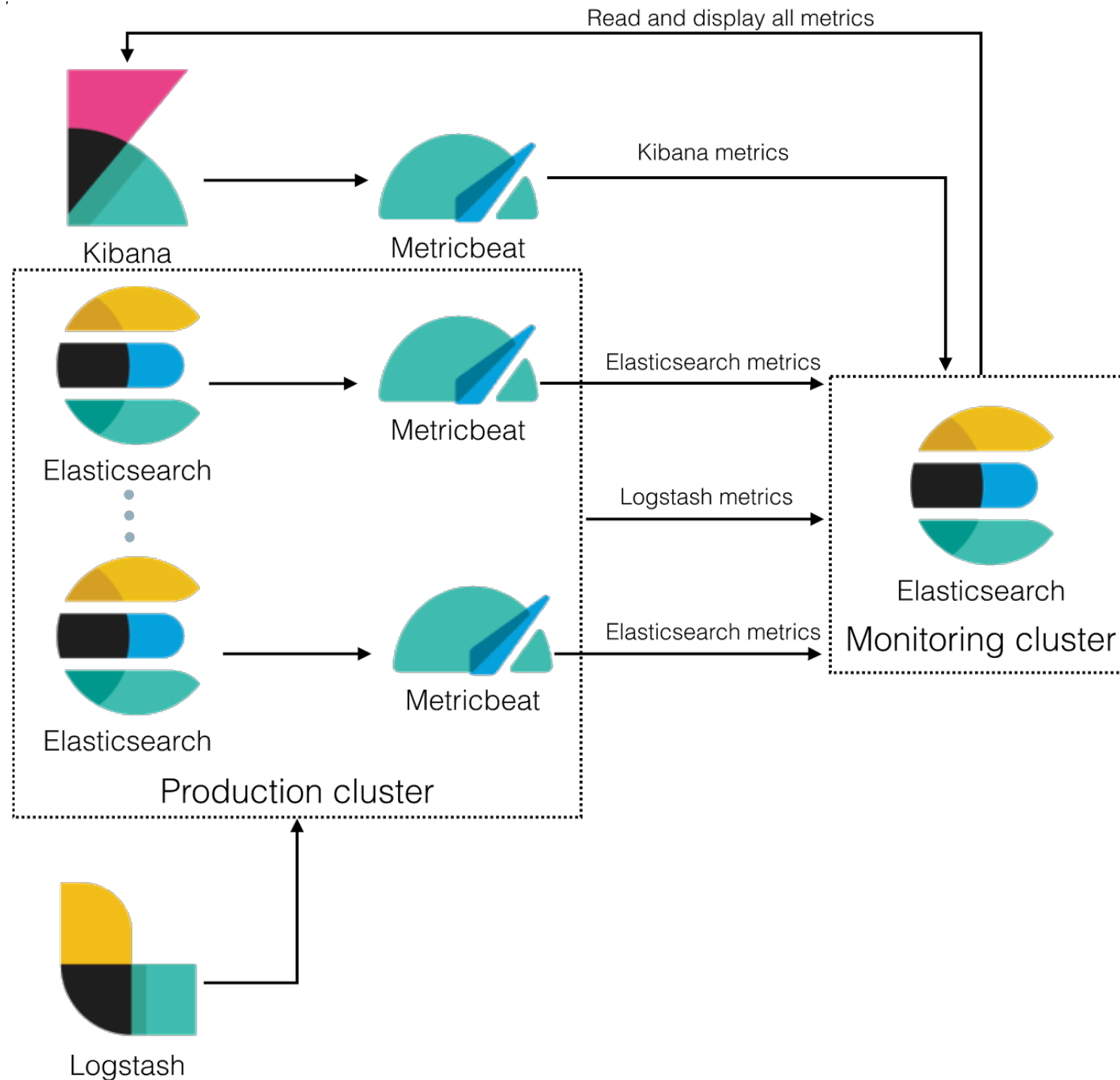
<https://www.elastic.co/guide/en/elastic-stack-overview/6.5/xpack-monitoring.html>



# Recommend architecture

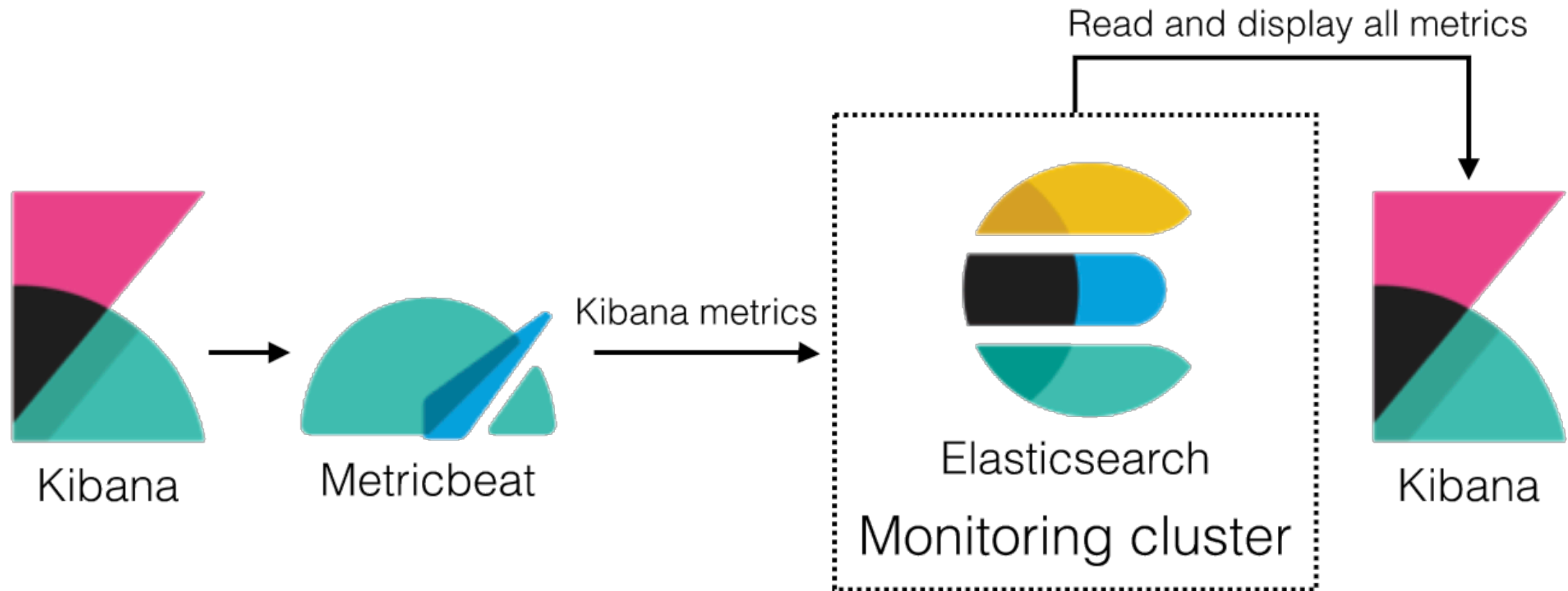


# Elasticsearch 6.4 + (beta)





# Try to separate kibana



# Working with Logstash

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



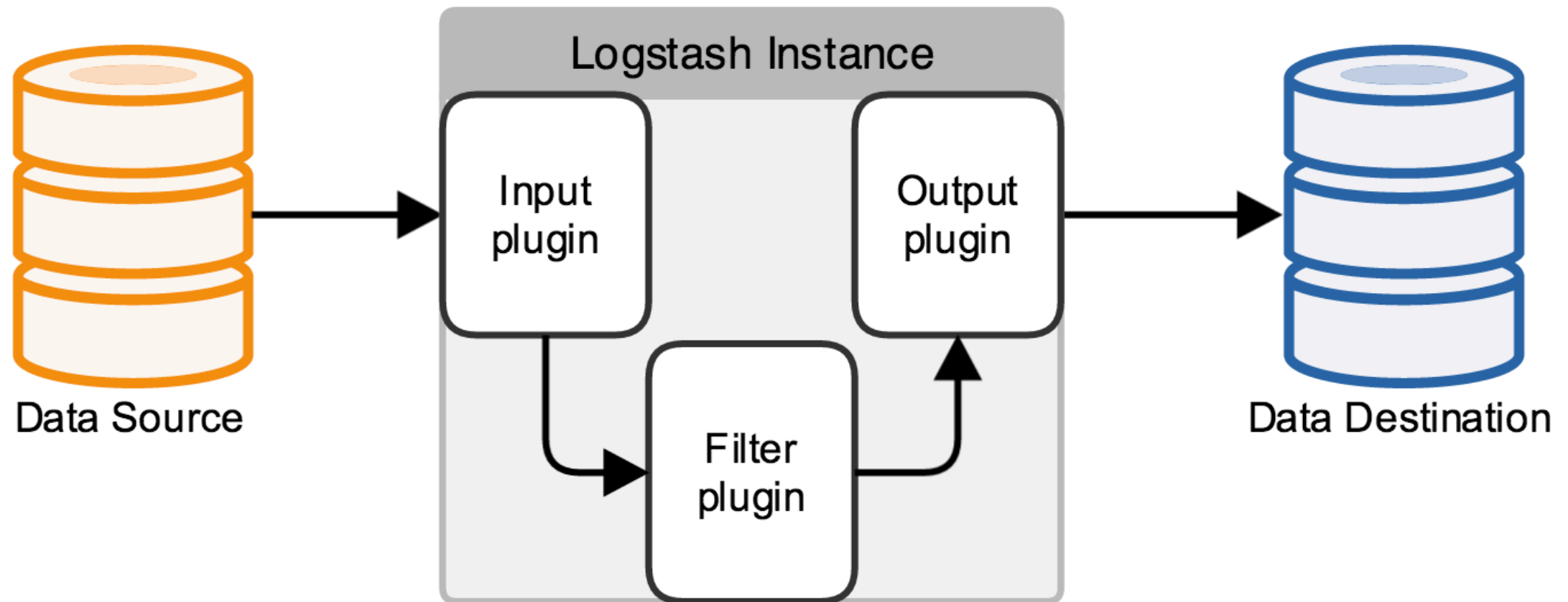
# Logstash



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

Elasticsearch

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 !!

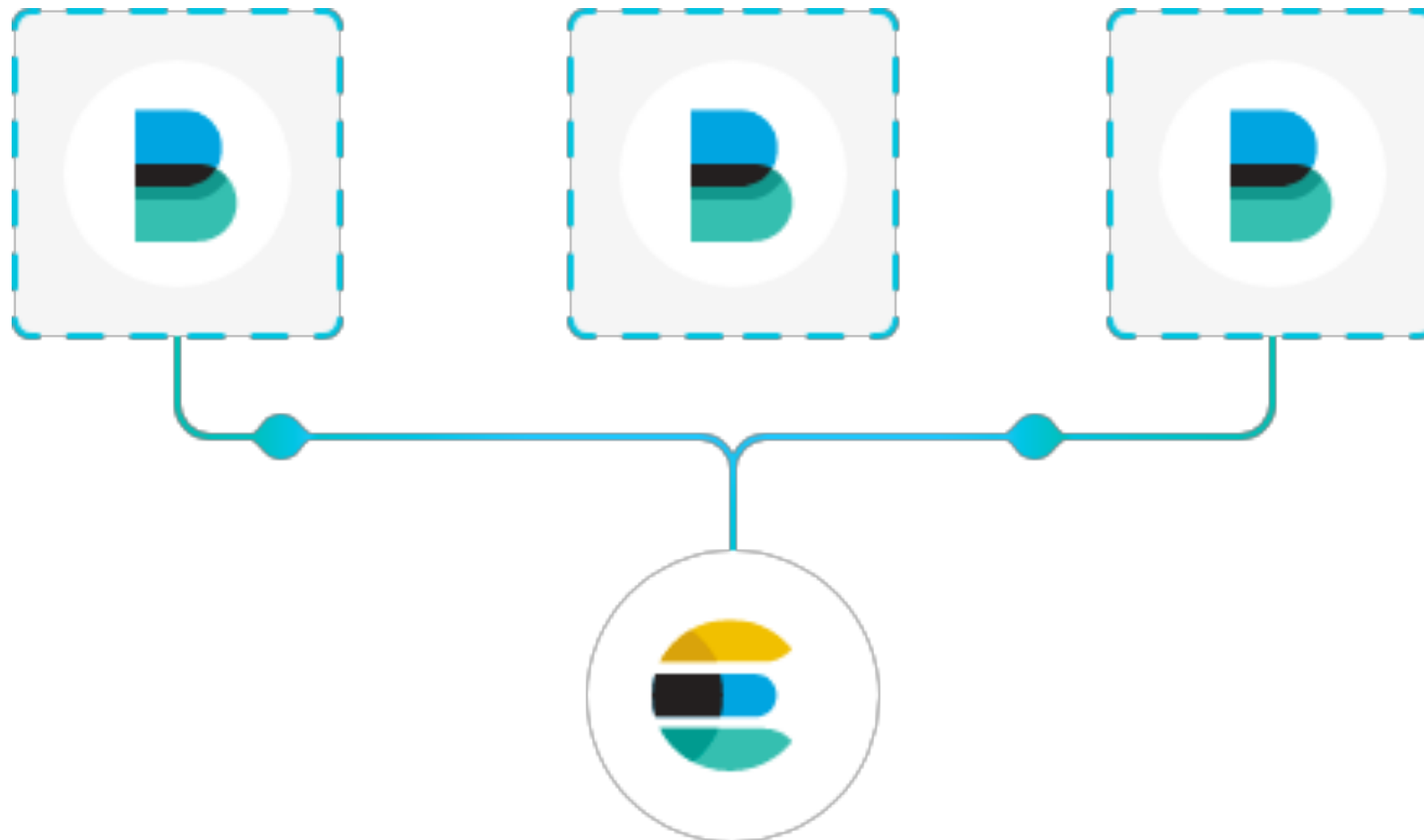


# Use beats is better

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



# Beat



# Beat



**Filebeat**

Log Files



**Metricbeat**

Metrics



**Packetbeat**

Network Data



**Winlogbeat**

Windows Event Logs



**Auditbeat**

Audit Data



**Heartbeat**

Uptime Monitoring



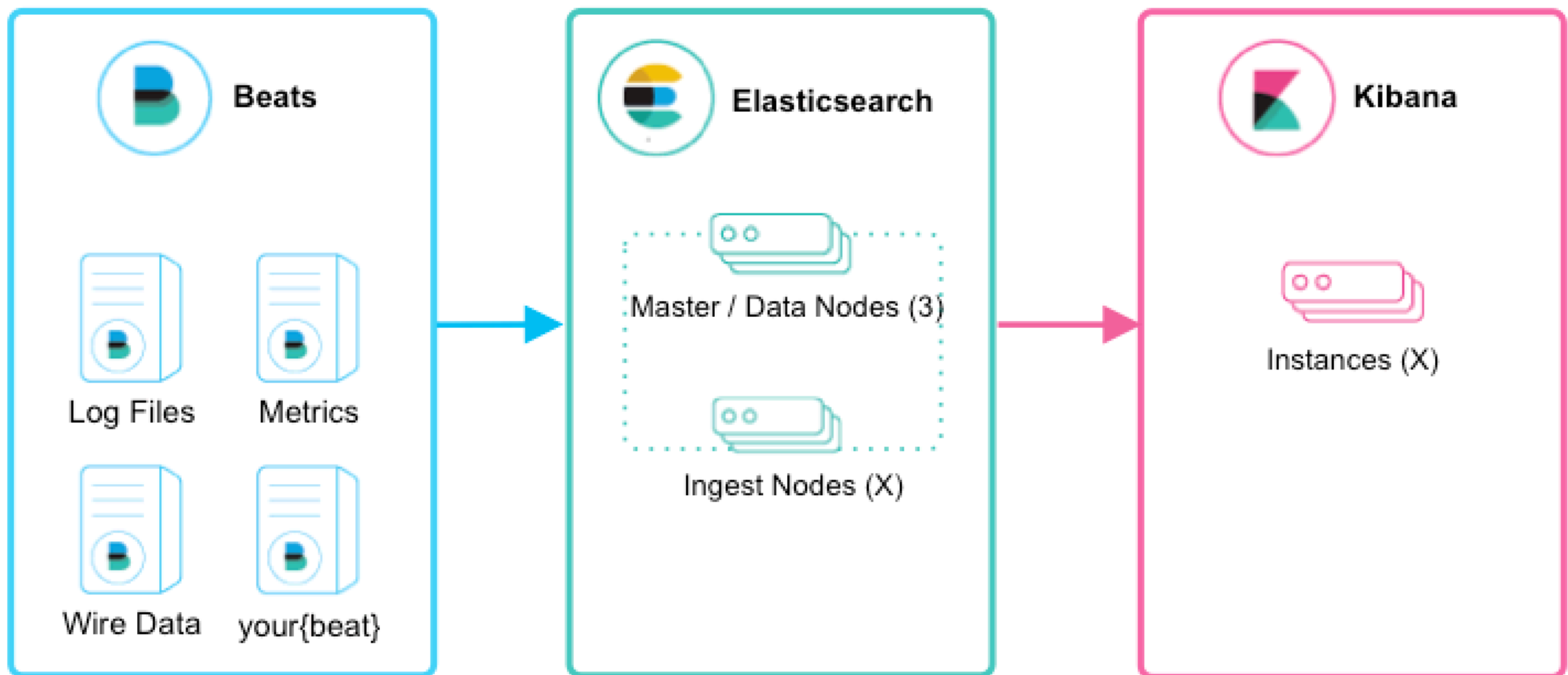
# Example

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

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



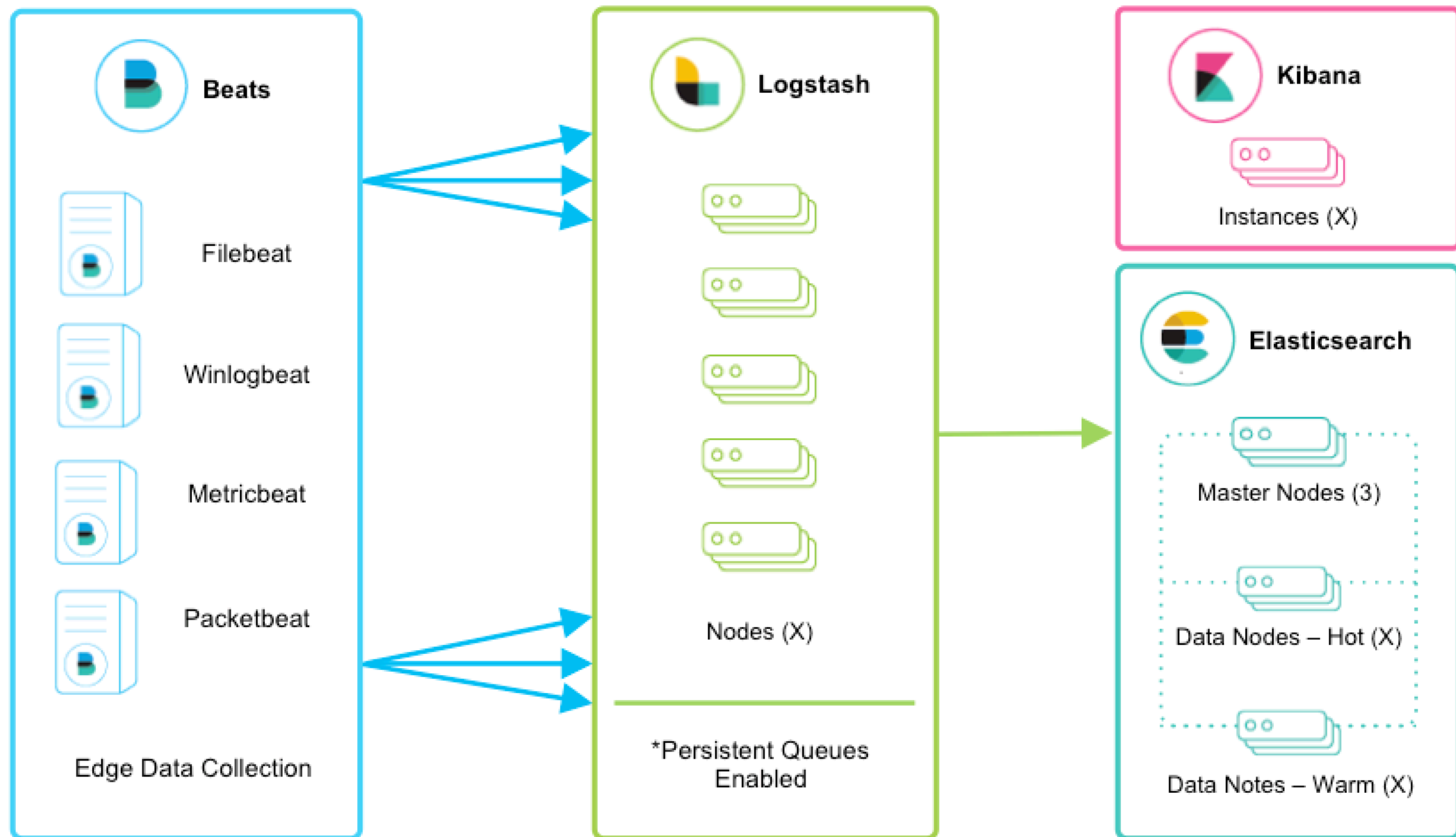
# Beat and Logstash



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



# Scaling

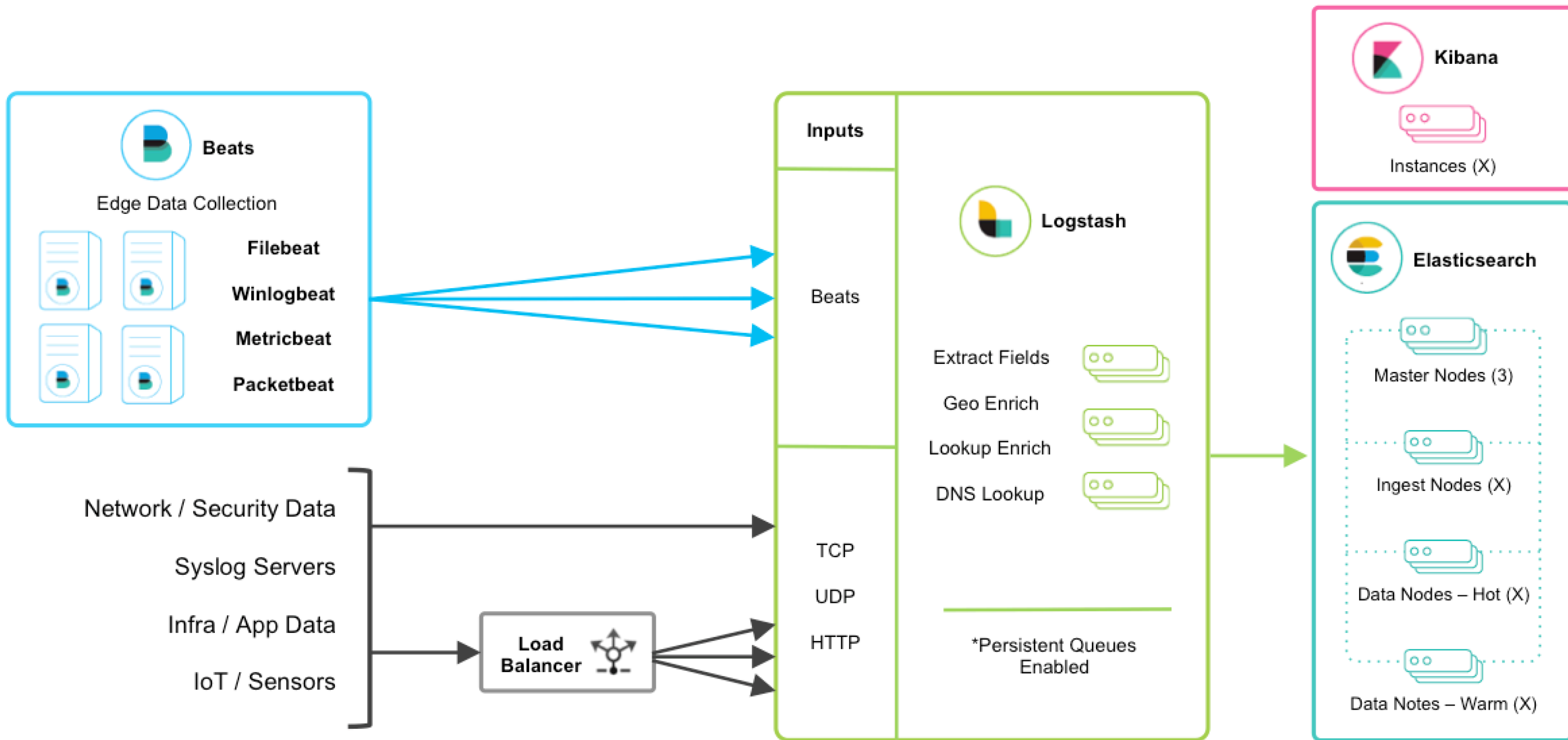


<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>





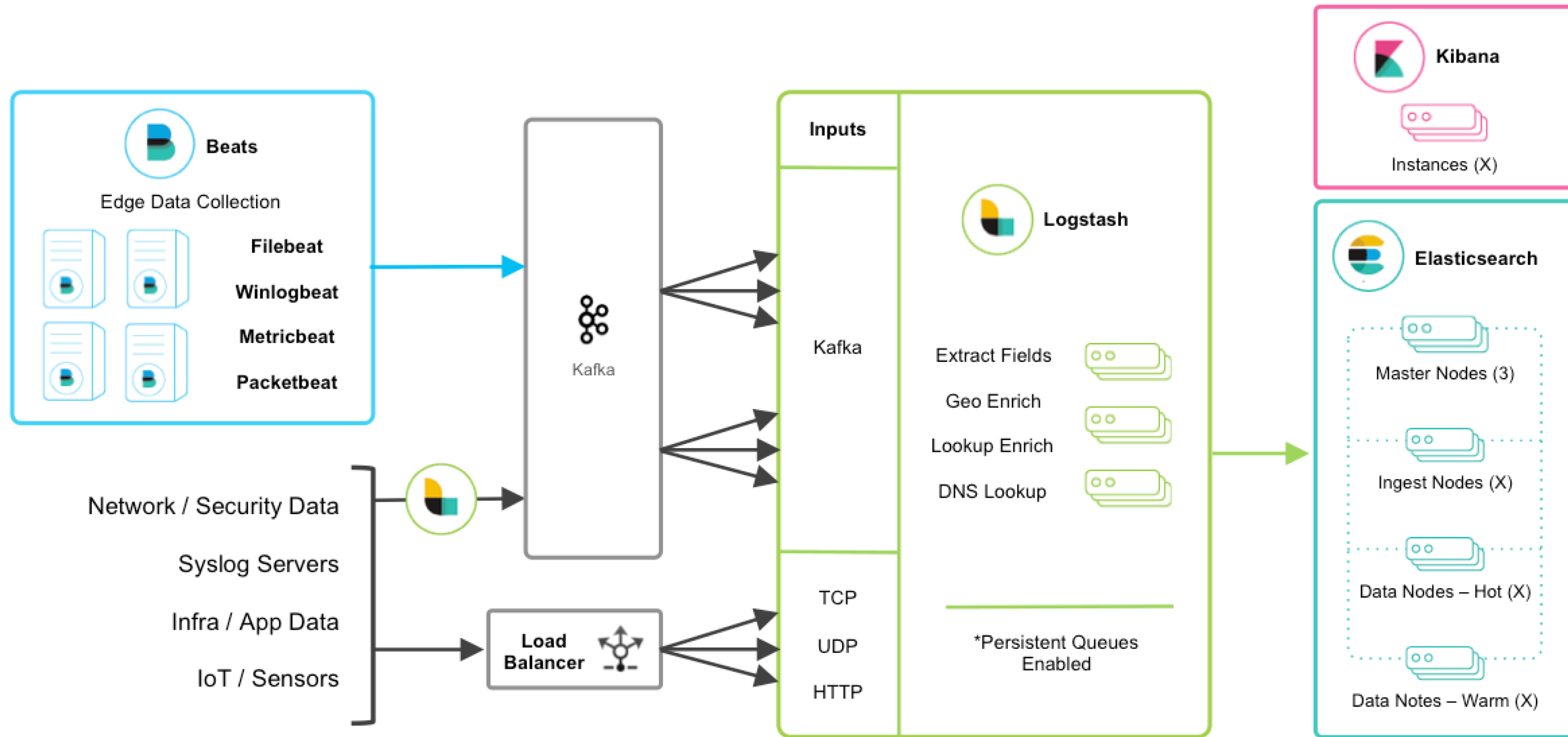
# More data sources



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



# Use messaging Queue



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

