

Monitor Your Containers

with the  elastic **Stack**

Philipp Krenn

@xeraa



elastic

Infrastructure | Developer Advocate

ALL THE THINGS!





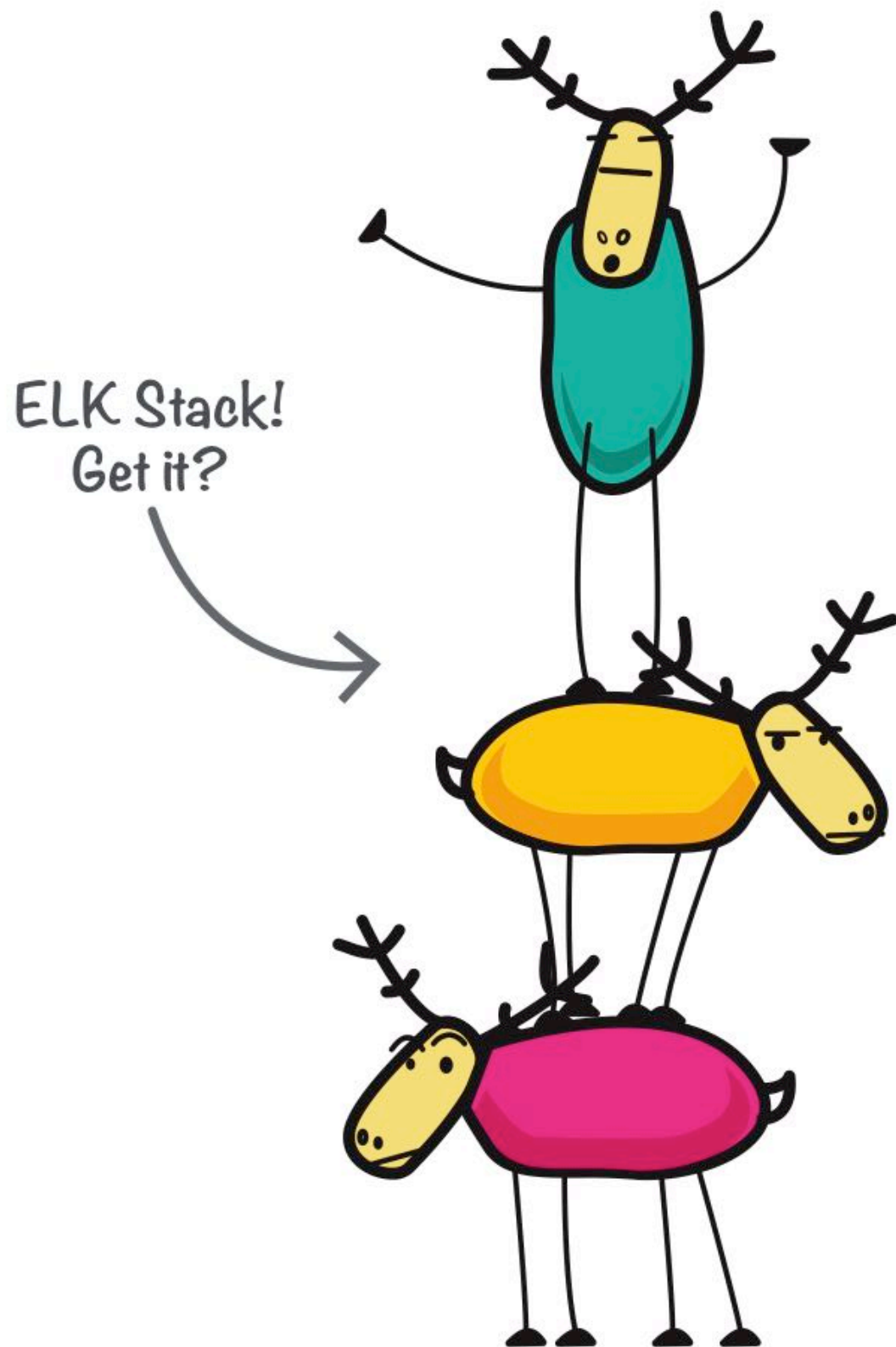
elasticsearch.

```
$ curl http://localhost:9200
{
  "name": "zDODSc4",
  "cluster_name": "docker-cluster",
  "cluster_uuid": "qbx3DVATRfW0gHB6uiLtNw",
  "version": {
    "number": "6.3.0",
    "build_flavor": "default",
    "build_type": "tar",
    "build_hash": "424e937",
    "build_date": "2018-06-11T23:38:03.357887Z",
    "build_snapshot": false,
    "lucene_version": "7.3.1",
    "minimum_wire_compatibility_version": "5.6.0",
    "minimum_index_compatibility_version": "5.0.0"
  },
  "tagline": "You Know, for Search"
}
```





logstash

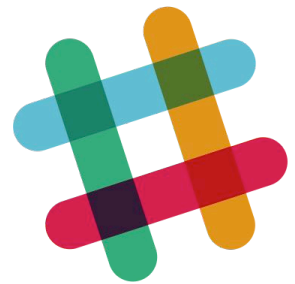


E Elasticsearch

L Logstash

K Kibana

mozilla

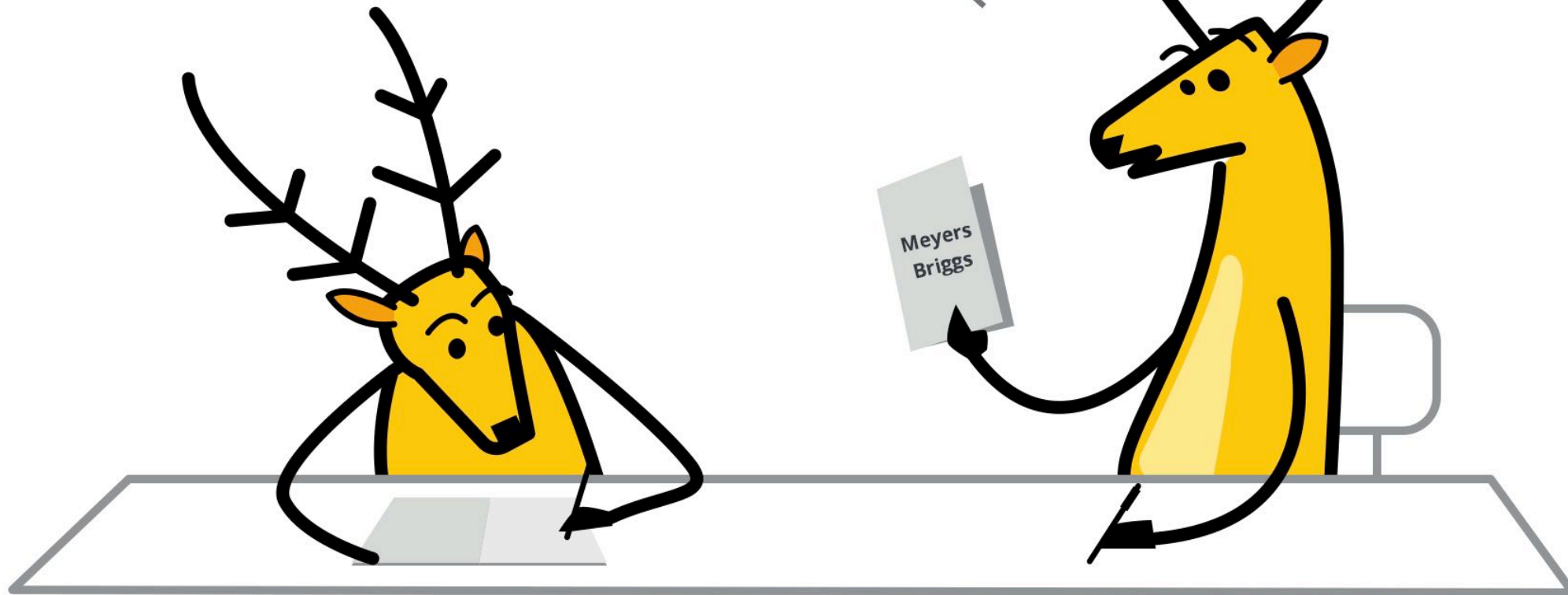


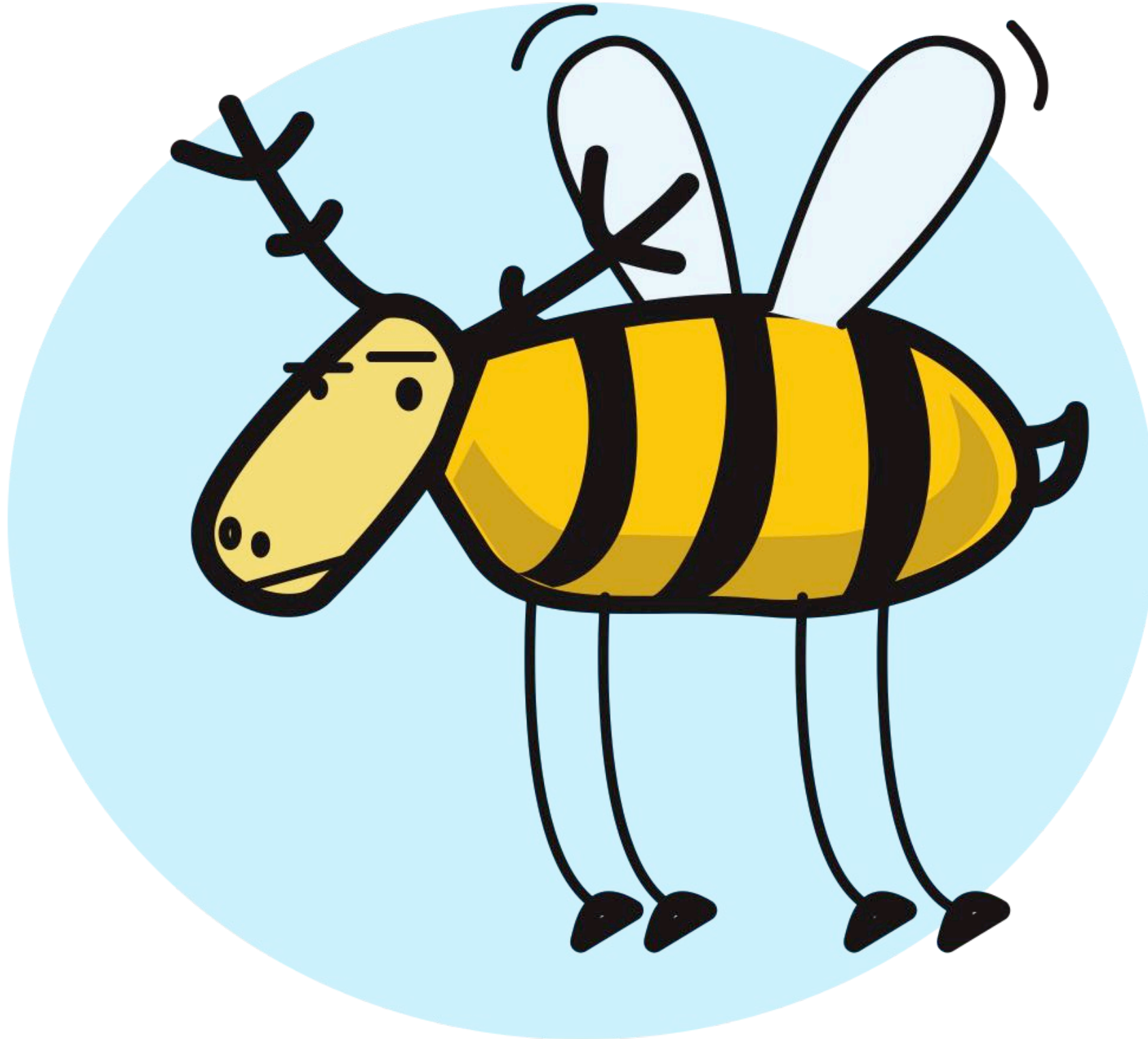
slack

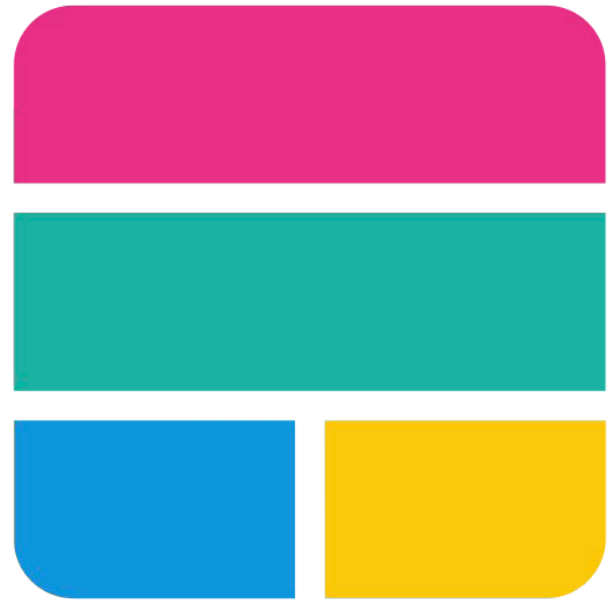




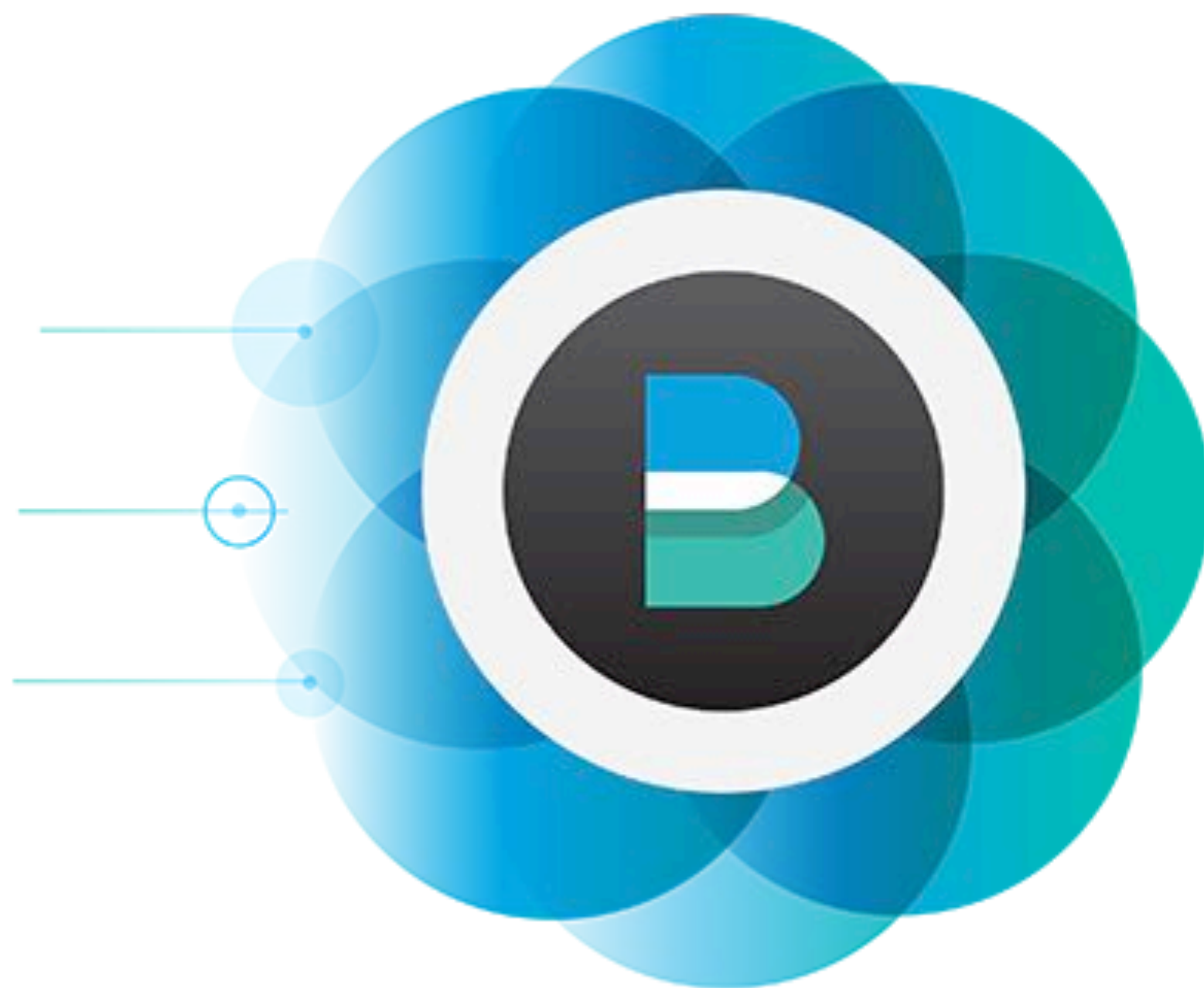
*Apparently, I'm an
ELKB personality.*







elastic stack



Filebeat

tail -f

tail -f
over the network

tail -f
over the network
on 

Parse & Enrich

Logstash or Ingest-Node

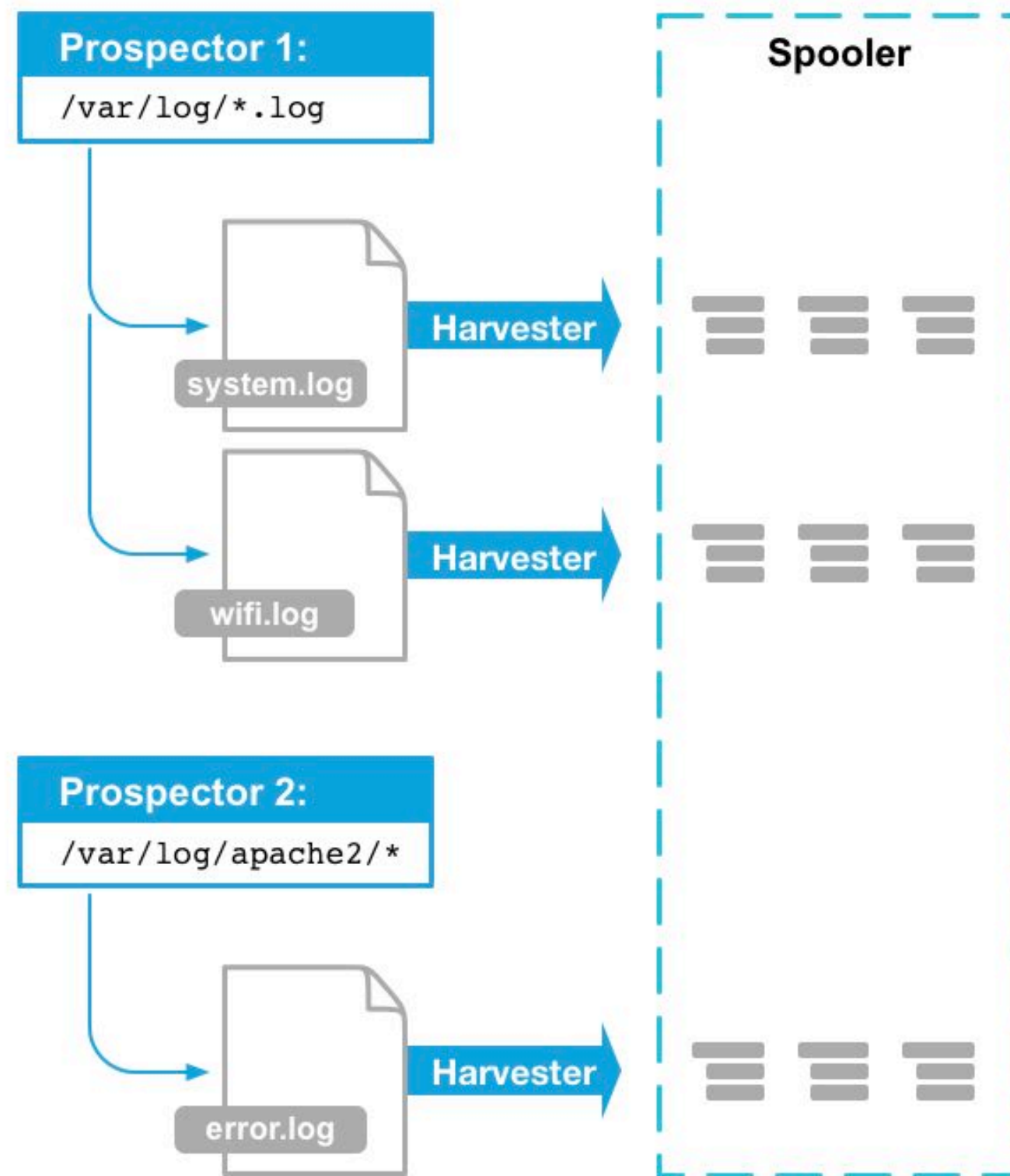
```
34.253.145.46 - - [06/Sep/2017:22:33:30 +0000]  
"GET /server-status HTTP/1.1" 200 97  
"- "Go-http-client/1.1" "-"
```

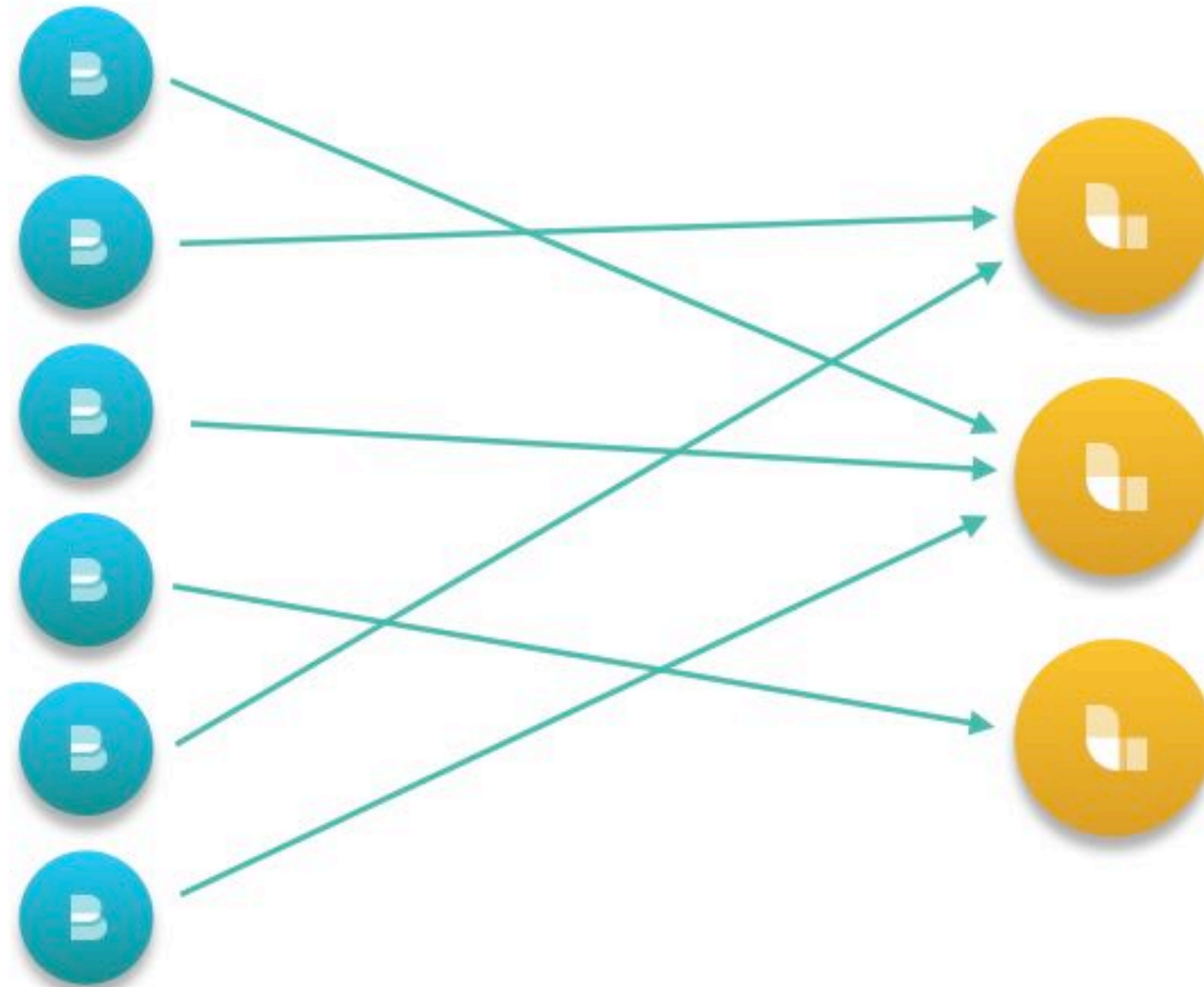
```
"remote_ip": "34.253.145.46",  
"method": "GET",  
"url": "/server-status",  
"http_version": "1.1",  
"response_code": 200,
```

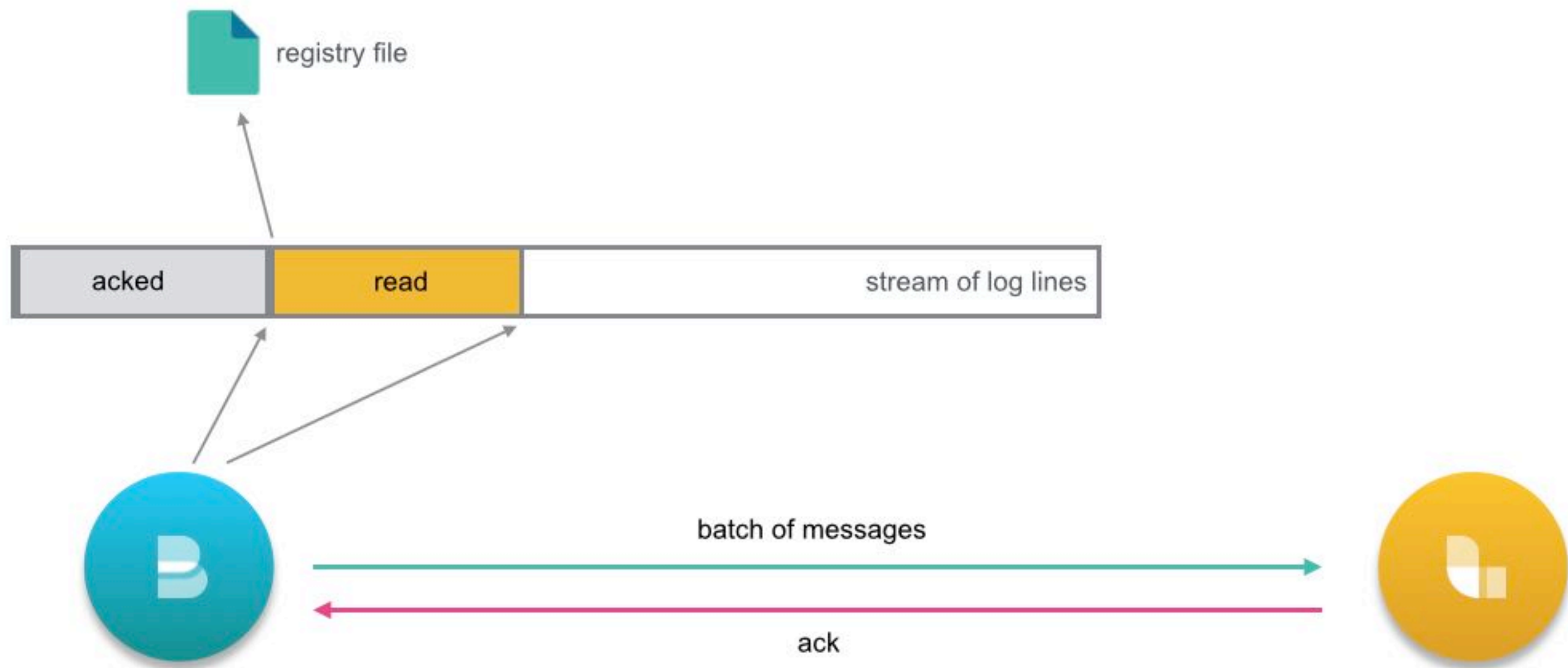
```
"remote_ip": "34.253.145.46"

"geoip": {
  "continent_name": "North America",
  "city_name": "Houston",
  "country_iso_code": "US",
  "region_name": "Texas",
  "location": {
    "lon": -95.5858,
    "lat": 29.6997
  }
}
```

At-Least-Once Backpressure Graceful Downtime







Filtering

include_lines

exclude_lines

exclude_files

```
filebeat.prospectors:
```

```
- input_type: log  
  paths:
```

```
    - /var/log/myapp/*.log
```

```
  include_lines: ["^ERR", "^WARN"]
```

Multiline

```
Exception in thread "main" java.lang.IllegalStateException: A book has a null property
    at com.example.myproject.Author.getBookIds(Author.java:38)
    at com.example.myproject.Bootstrap.main(Bootstrap.java:14)
Caused by: java.lang.NullPointerException
    at com.example.myproject.Book.getId(Book.java:22)
    at com.example.myproject.Author.getBookIds(Author.java:35)
    ... 1 more
```

`multiline.pattern: '^[[[:space:]]+|^Caused by: '`

`multiline.negate: false`

`multiline.match: after`

JSON Decode

Filebeat Modules

**Apache2, Auditd, Icinga, IIS, Kafka,
Logstash, MongoDB, MySQL, Nginx,
Osquery, PostgreSQL, Redis, System,
Traefik**

Logging with Docker

101 options

Driver	Description
<code>none</code>	Disables any logging for the container. <code>docker logs</code> won't be available with this driver.
<code>json-file</code>	Default logging driver for Docker. Writes JSON messages to file.
<code>syslog</code>	Syslog logging driver for Docker. Writes log messages to syslog.
<code>journald</code>	Journald logging driver for Docker. Writes log messages to journald.
<code>gelf</code>	Graylog Extended Log Format (GELF) logging driver for Docker. Writes log messages to a GELF endpoint like Graylog or Logstash.
<code>fluentd</code>	Fluentd logging driver for Docker. Writes log messages to <code>fluentd</code> [forward input].
<code>awslogs</code>	Amazon CloudWatch Logs logging driver for Docker. Writes log messages to Amazon CloudWatch Logs.
<code>splunk</code>	Splunk logging driver for Docker. Writes log messages to <code>splunk</code> using HTTP Event Collector.
<code>etwlogs</code>	ETW logging driver for Docker on Windows. Writes log messages as ETW events.
<code>gcplogs</code>	Google Cloud Logging driver for Docker. Writes log messages to Google Cloud Logging.

<https://docs.docker.com/engine/admin/logging/overview/>

001 JSON-File

Filebeat for JSON

+

**Simple, default, well integrated
Metadata (name, labels,...)**

`docker logs`

—

**Potentially slow
By default unlimited file size**

010 Syslog

Local Syslog server and Filebeat

+

Configurable path, rotation,...

—

Custom Syslog server
Metadaten serialized and deserialized
Multiline

011 Journald

Filebeat

+

Widely available

Metadata

`docker logs`

—

Not yet supported by Filebeat (Community Beat: Journalbeat)

100 GELF

Logstash-GELF-Input

+

Direct Logstash connection

—

UDP — no ACK, no backpressure

101 Volume

Filebeat

+

Simple installation (if app rotates logs)

Scalable

—

Metadata



Today: JSON, Syslog, Volume

Future: Journald

Docker Metadata

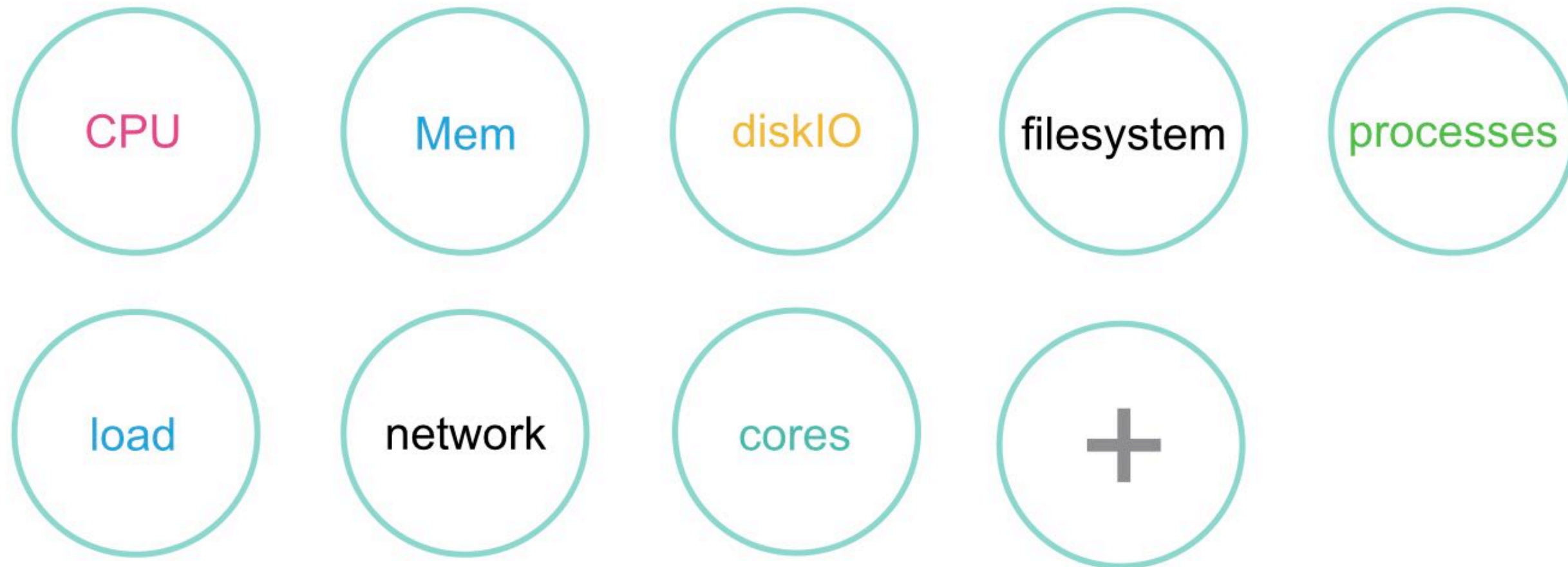
```
- input_type: log
  paths:
    - /var/lib/docker/containers/*/*-json.log
  document_type: docker
  json.message_key: log
  processors:
    - add_docker_metadata: ~
```

Kubernetes Metadata

```
processors:  
  - add_kubernetes_metadata:  
    in_cluster: true
```

Metrickbeat

Metricbeat System



Add your own

Metricbeat Service

Many: <https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-modules.html>

Read cgroup data from /proc/

Part of the system module

No Docker API access required

Security

All containers

Docker, rkt, runC, LXD,...

**Enriches process information
automatically with cgroup data**

No container names or labels

But Docker...



Dockerbeat

<https://github.com/Ingensi/dockerbeat>

~~Dockerbeat~~

~~<https://github.com/Ingenisi/dockerbeat>~~

Dockbeat

<https://github.com/Ingensi/dockbeat>

Metricbeat 5.1+

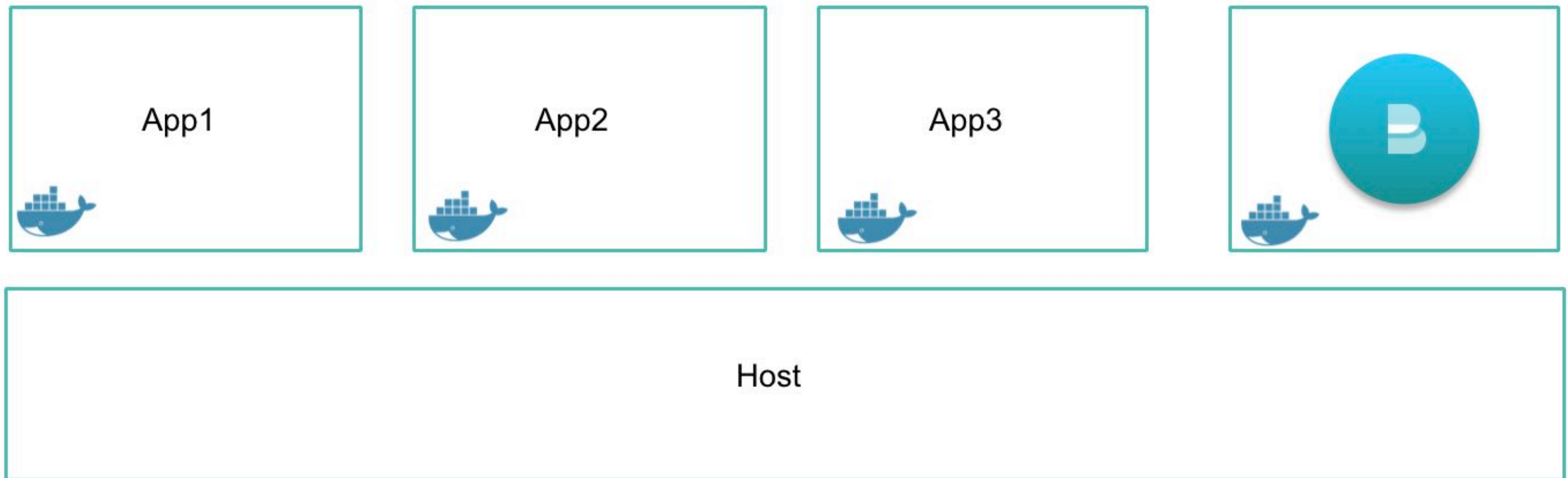
System Permissions

```
$ docker run \  
  --volume=/proc:/hostfs/proc:ro \  
  --volume=/sys/fs/cgroup:/hostfs/sys/fs/cgroup:ro \  
  --volume=/:/hostfs:ro \  
  --net=host  
docker.elastic.co/beats/metricbeat:6.3.0 -system.hostfs=/hostfs
```

Service Permissions

```
$ docker run \  
  --link some-mysql:mysql \  
  -e MYSQL_PASSWORD=secret \  
  docker.elastic.co/beats/metricbeat:6.3.0
```

Metricbeat and Docker



Docker Metadata

processors:

- add_docker_metadata: ~

Kubernetes Metadata

```
processors:  
  - add_kubernetes_metadata:  
    in_cluster: true
```

Kubernetes Metrics

```
- module: kubelet  
  metricsets: ["node", "container", "volume", "pod", "system"]  
  hosts: ["localhost:10255"]
```



*

Uses lucene query syntax



Kubernetes - Nodes

Kubernetes - Deployments

Available pods per deployment [Metricbeat Kubernetes]

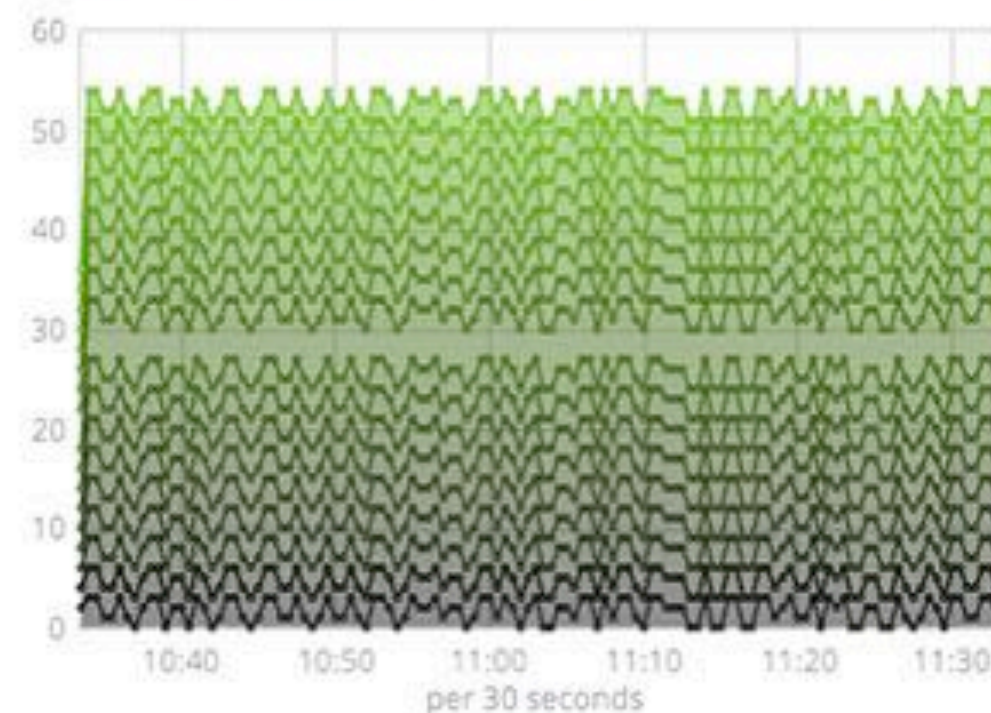


Nodes

1

Deployments

18



● carts	3
● carts-db	3
● catalogue	3
● catalogue-db	3
● front-end	3
● kube-dns	3
● kube-state-metrics	3
● load-test	6

Kubernetes - Desired p...

Kubernetes - Available ...

Kubernetes - Unavailab...

Unavailable pods per deployment [Metricbeat Kubernetes]



Desired Pods

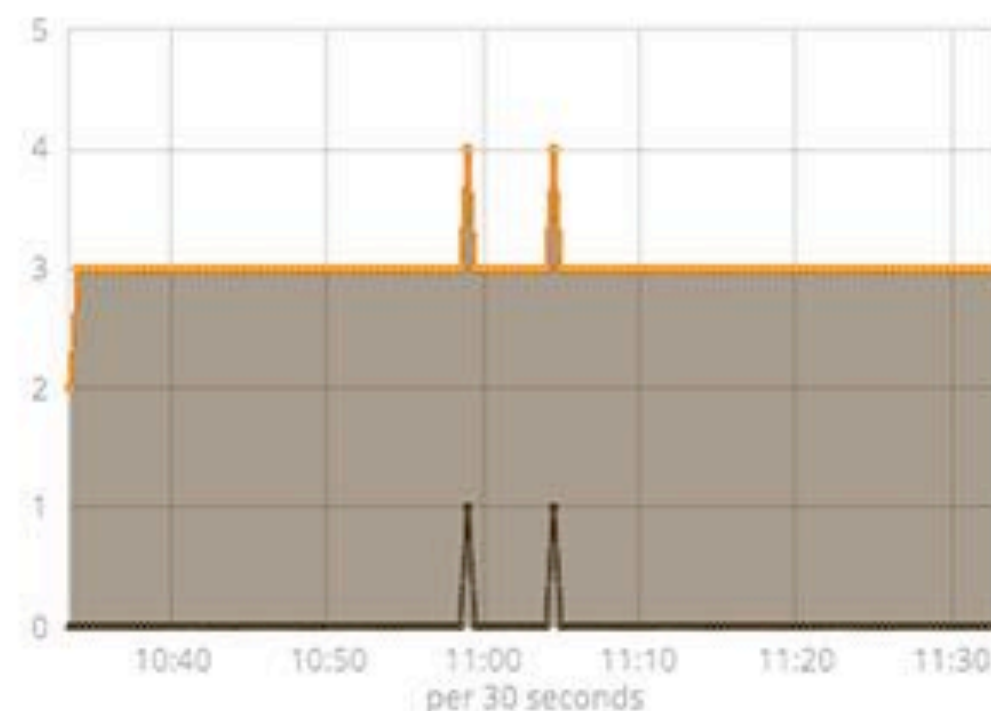
18

Available Pods

17

Unavailable Pods

1



● carts	0
● carts-db	0
● catalogue	0
● catalogue-db	0
● front-end	0
● kube-dns	0
● kube-state-metrics	0
● load-test	0

CPU usage by node [Metricbeat Kubernetes]

Memory usage by node [Metricbeat Kubernetes]

Packetbeat

Protocols



HTTP



Thrift-RPC



DNS



MySQL



PostgreSQL



Redis



Memcached



MongoDB



ICMP



AMQP



Cassandra



Add your own

Flows

Application layer: Unsupported or encrypted protocols

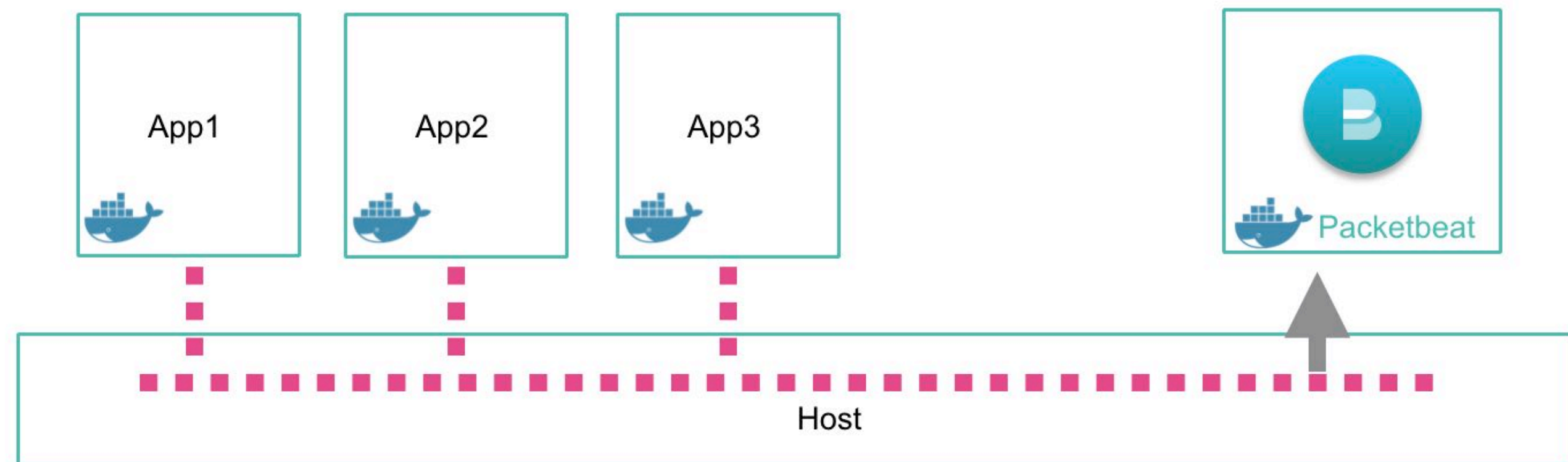
IP / TCP / UDP

Number of packets & bytes

Retransmissions

Temporal flow

Packetbeat and Docker



■ ■ ■ traffic exchanged between your containers

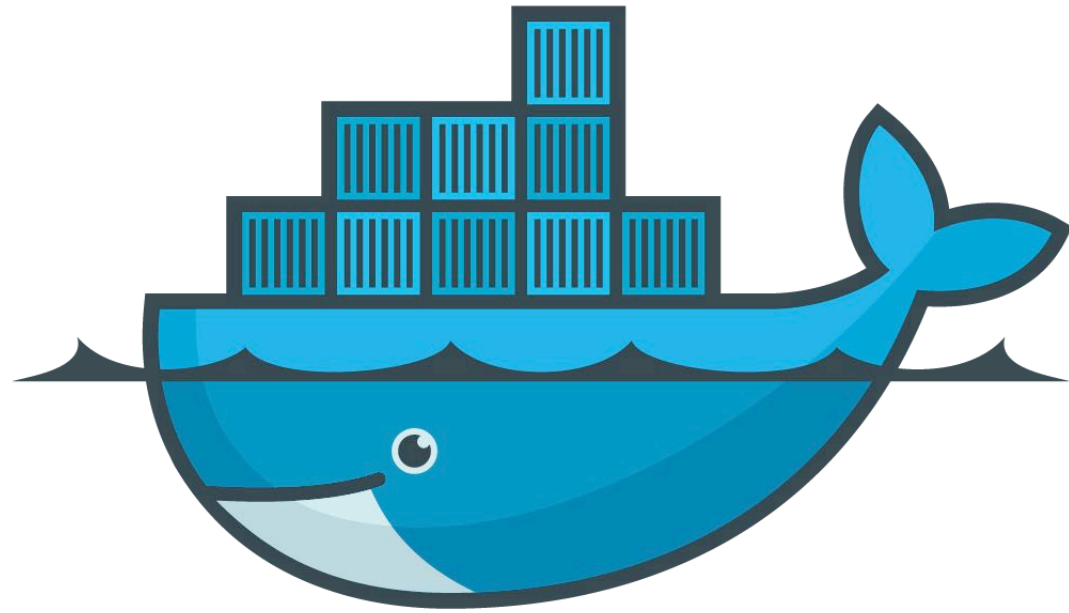
Auditbeat

Linux Kernel

File Integrity

Heartbeat

Winlogbeat



docker

<https://github.com/elastic/elasticsearch-docker>

<https://github.com/elastic/kibana-docker>

<https://github.com/elastic/logstash-docker>

<https://github.com/elastic/beats-docker>

```
---
version: '2'
services:
  kibana:
    image: docker.elastic.co/kibana/kibana:6.3.0
    links:
      - elasticsearch
    ports:
      - 5601:5601

  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:6.3.0
    volumes:
      - esdata:/usr/share/elasticsearch/data
    ports:
      - 9200:9200

volumes:
  esdata:
    driver: local
```

Docker @ Elastic

At Elastic, we care about Docker. We provide Docker images for all the products in our stack, and we consider them a first-class distribution format. We also host a dedicated Docker Registry to provide the best possible experience and the most reliable service for you.

On this page, you'll find all the resources — **docker** commands, links to product release notes, documentation and source code — for installing and using the Docker images.

Watch a [presentation](#) from our developers at the Elastic{ON} conference to get details about the background behind our Docker efforts and to see a live demo for the entire stack.



Elasticsearch

6.2  `docker pull docker.elastic.co/elasticsearch/elasticsearch:6.2.3`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-basic:6.2.3`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-basic:6.2.2`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-basic:6.2.1`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-basic:6.2.0`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-oss:6.2.3`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-oss:6.2.2`   

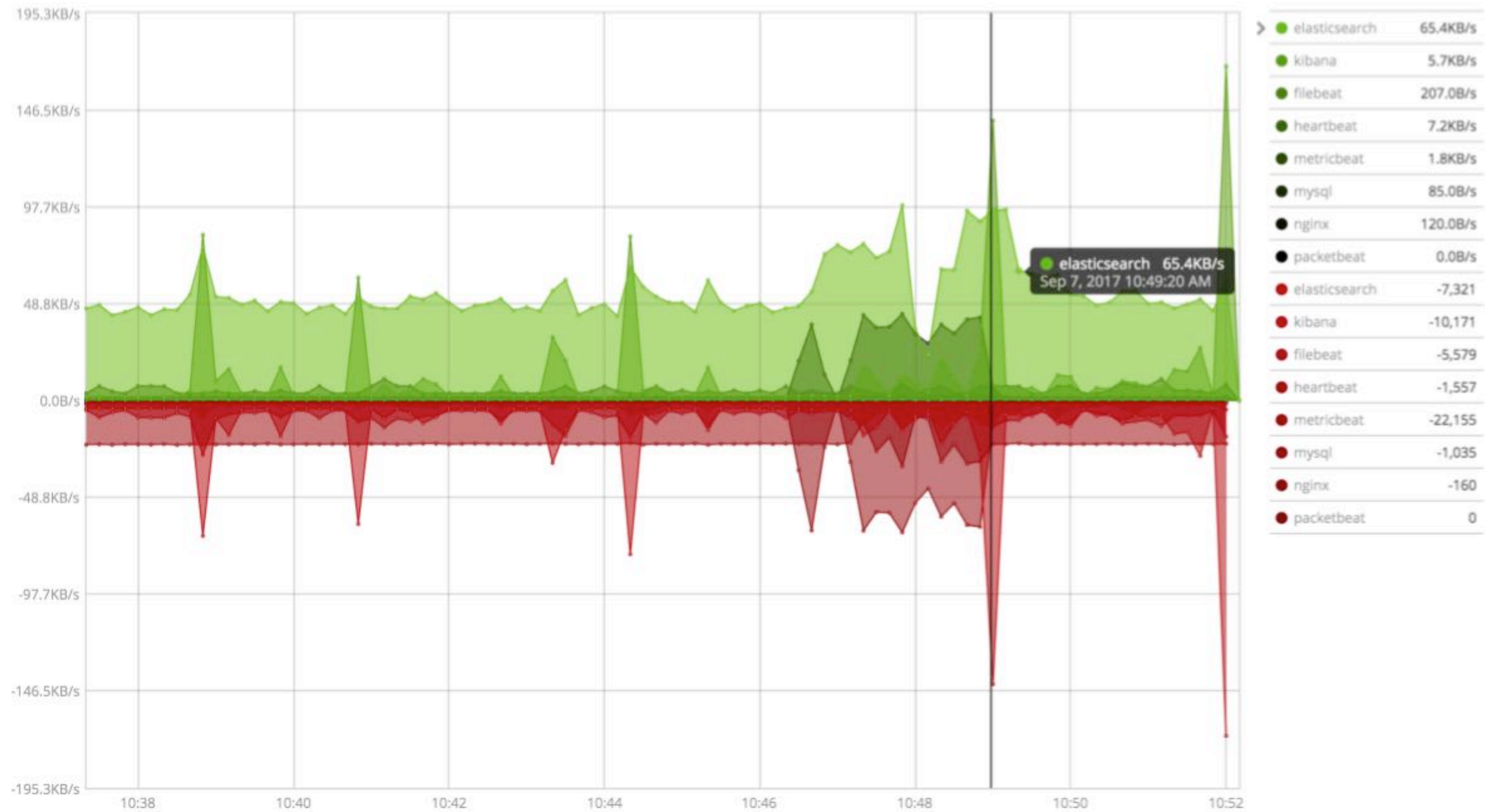
`docker pull docker.elastic.co/elasticsearch/elasticsearch-oss:6.2.1`   

`docker pull docker.elastic.co/elasticsearch/elasticsearch-oss:6.2.0`   

Demo

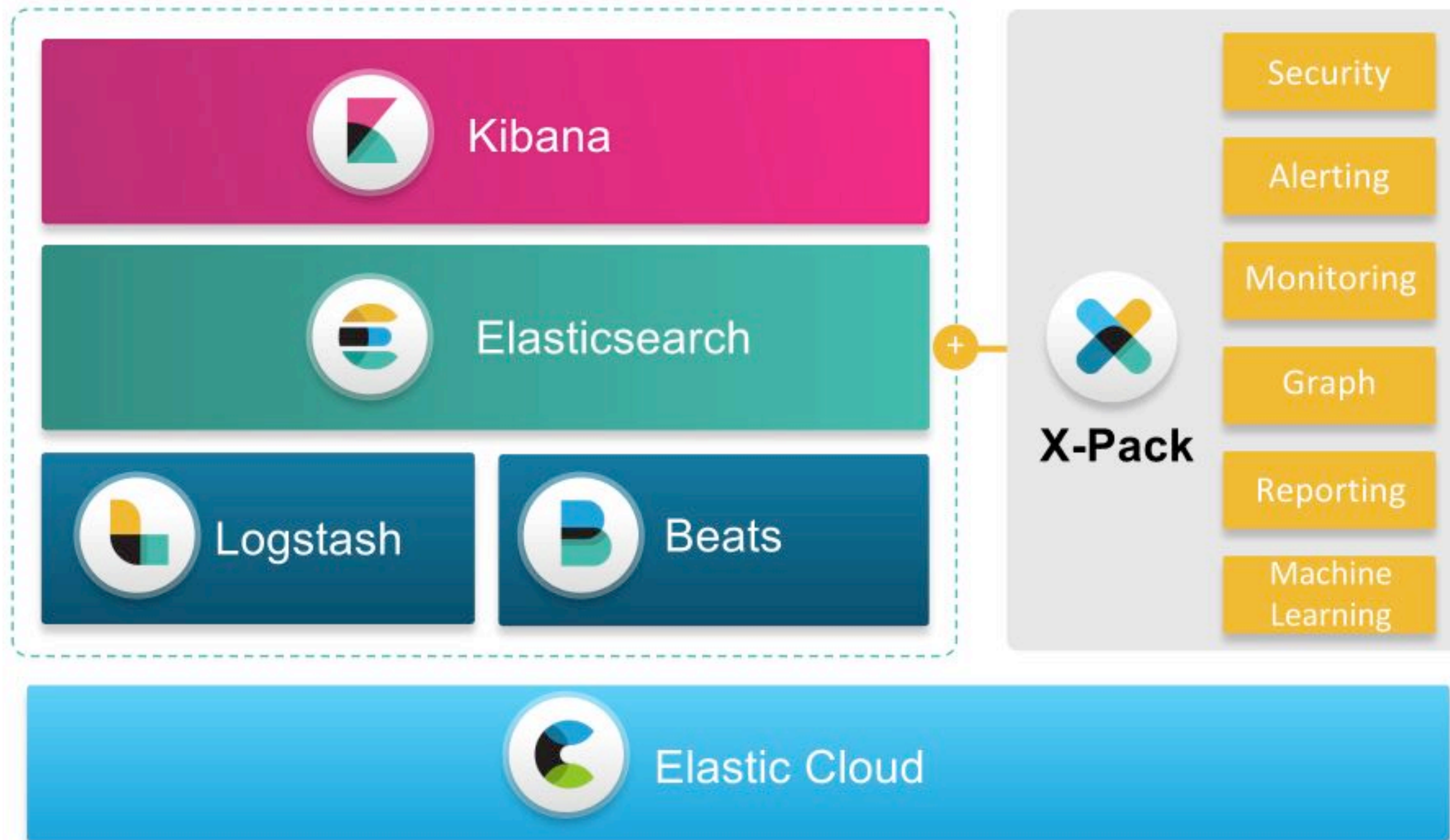
**[https://github.com/xeraa/elastic-docker/
tree/master/full_stack](https://github.com/xeraa/elastic-docker/tree/master/full_stack)**

**Elasticsearch, Kibana, Filebeat, Heartbeat, Metricbeat,
Packetbeat, nginx, MySQL**



Conclusion





Questions?

Philipp Krenn

@xeraa

PS: Sticker