Become our local
Community Organizer!

We are looking for someone to help our local Elastic user group thrive.

Email us at meetups@elastic.co, if you’re interested.

Learn more:
https://ela.st/organize

Elastic Stack

Tomasz Gintowt
Warszawa 22.01.2019

Tomasz Gintowt

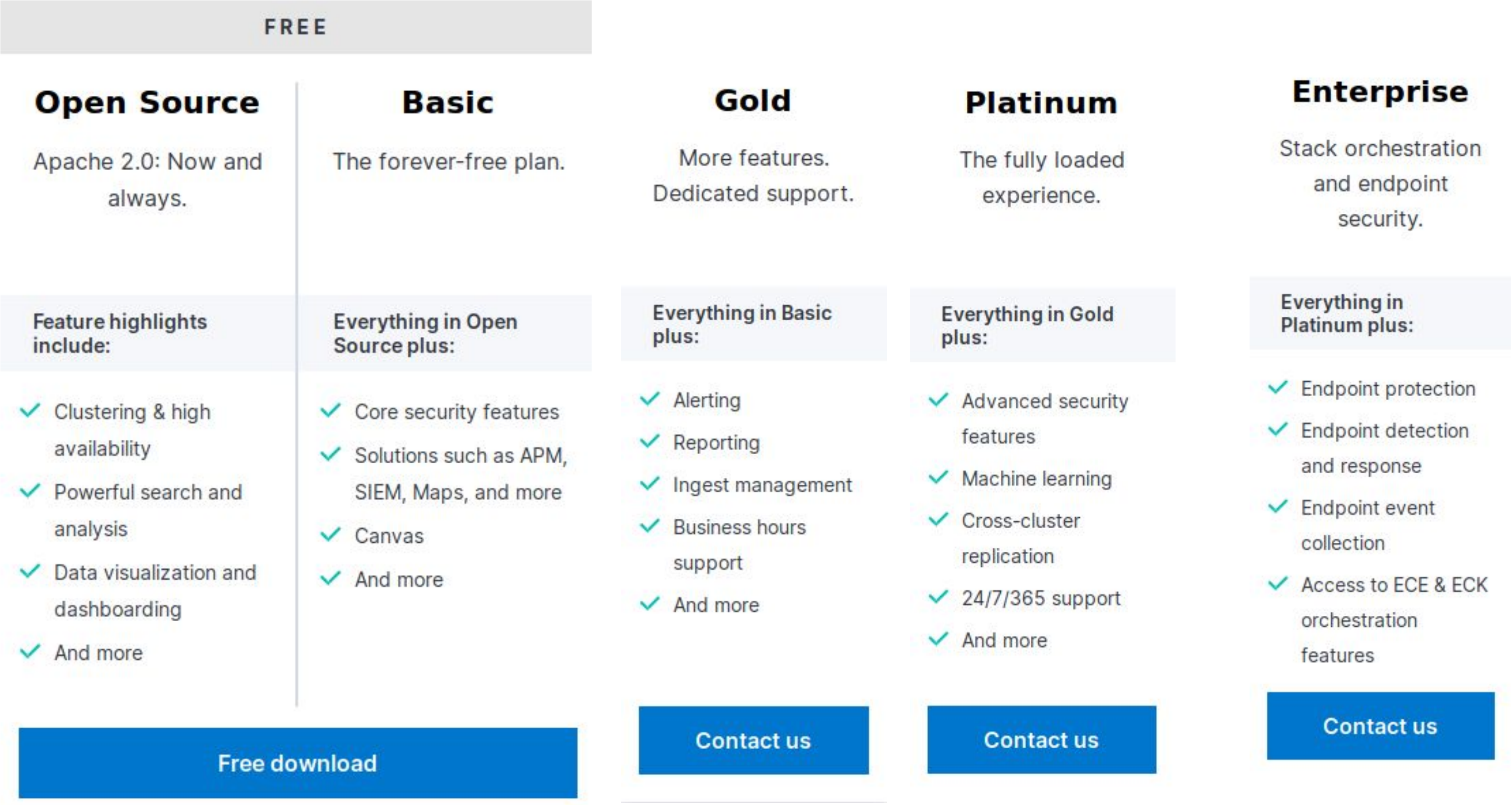
tomasz.gintowt@gmail.com

https://www.linkedin.com/in/tomasz-gintowt/

Agenda:

- Elastic Stack
- Beats
- Logstash
- ElasticSearch
- Demo
- AIops

Elastic Stack



FREE

Open Source

Apache 2.0: Now and always.

Feature highlights include:

- ✓ Clustering & high availability
- ✓ Powerful search and analysis
- ✓ Data visualization and dashboarding
- ✓ And more

Basic

The forever-free plan.

Everything in Open Source plus:

- ✓ Core security features
- ✓ Solutions such as APM, SIEM, Maps, and more
- ✓ Canvas
- ✓ And more

Free download

Gold

More features. Dedicated support.

Everything in Basic plus:

- ✓ Alerting
- ✓ Reporting
- ✓ Ingest management
- ✓ Business hours support
- ✓ And more

Contact us

Platinum

The fully loaded experience.

Everything in Gold plus:

- ✓ Advanced security features
- ✓ Machine learning
- ✓ Cross-cluster replication
- ✓ 24/7/365 support
- ✓ And more

Contact us

Enterprise

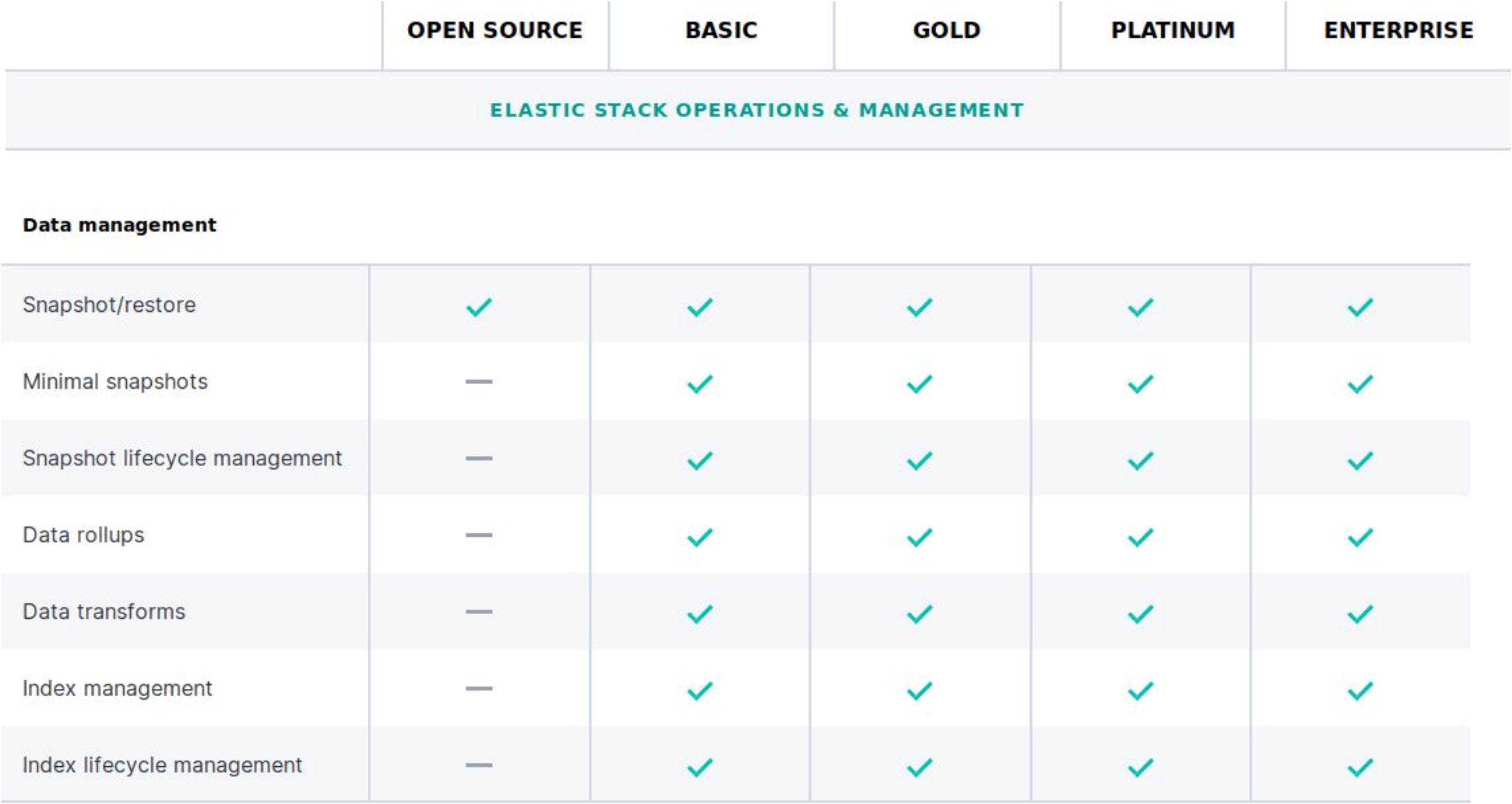
Stack orchestration and endpoint security.

Everything in Platinum plus:

- ✓ Endpoint protection
- ✓ Endpoint detection and response
- ✓ Endpoint event collection
- ✓ Access to ECE & ECK orchestration features

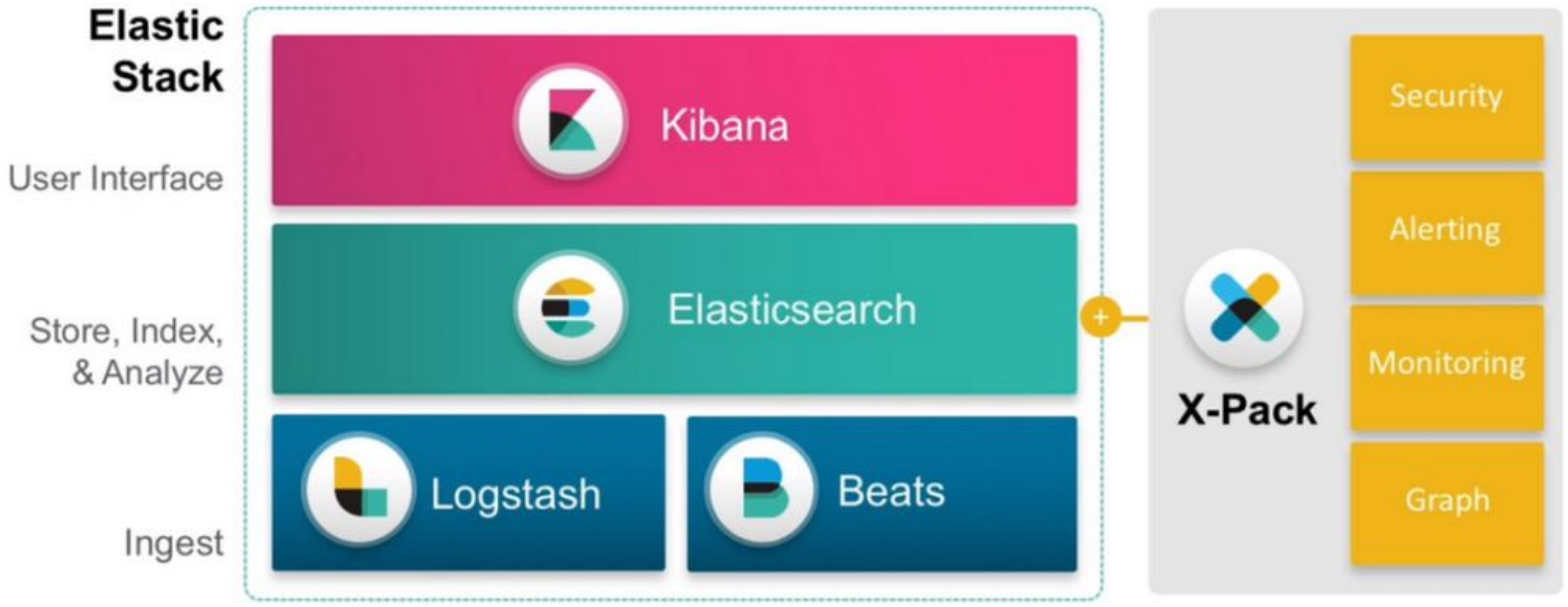
Contact us

Elastic Stack

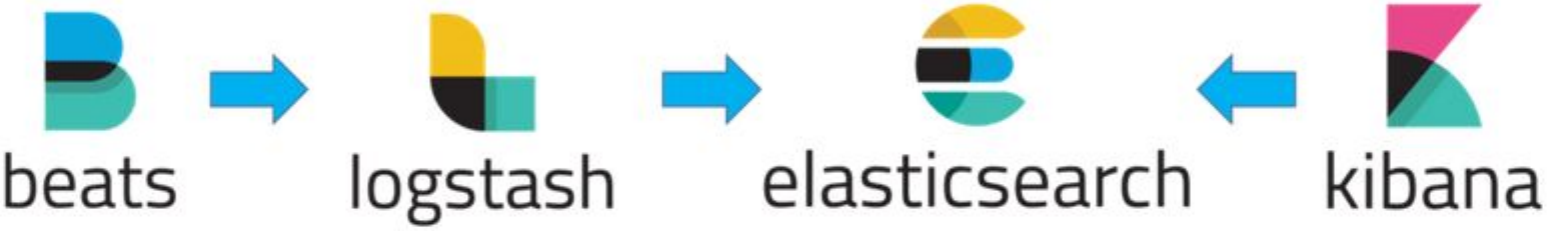


	OPEN SOURCE	BASIC	GOLD	PLATINUM	ENTERPRISE
ELASTIC STACK OPERATIONS & MANAGEMENT					
Data management					
Snapshot/restore	✓	✓	✓	✓	✓
Minimal snapshots	—	✓	✓	✓	✓
Snapshot lifecycle management	—	✓	✓	✓	✓
Data rollups	—	✓	✓	✓	✓
Data transforms	—	✓	✓	✓	✓
Index management	—	✓	✓	✓	✓
Index lifecycle management	—	✓	✓	✓	✓

Elastic Stack



Elastic Stack



beats

Data
Collection

logstash

Data
Aggregation
& Processing

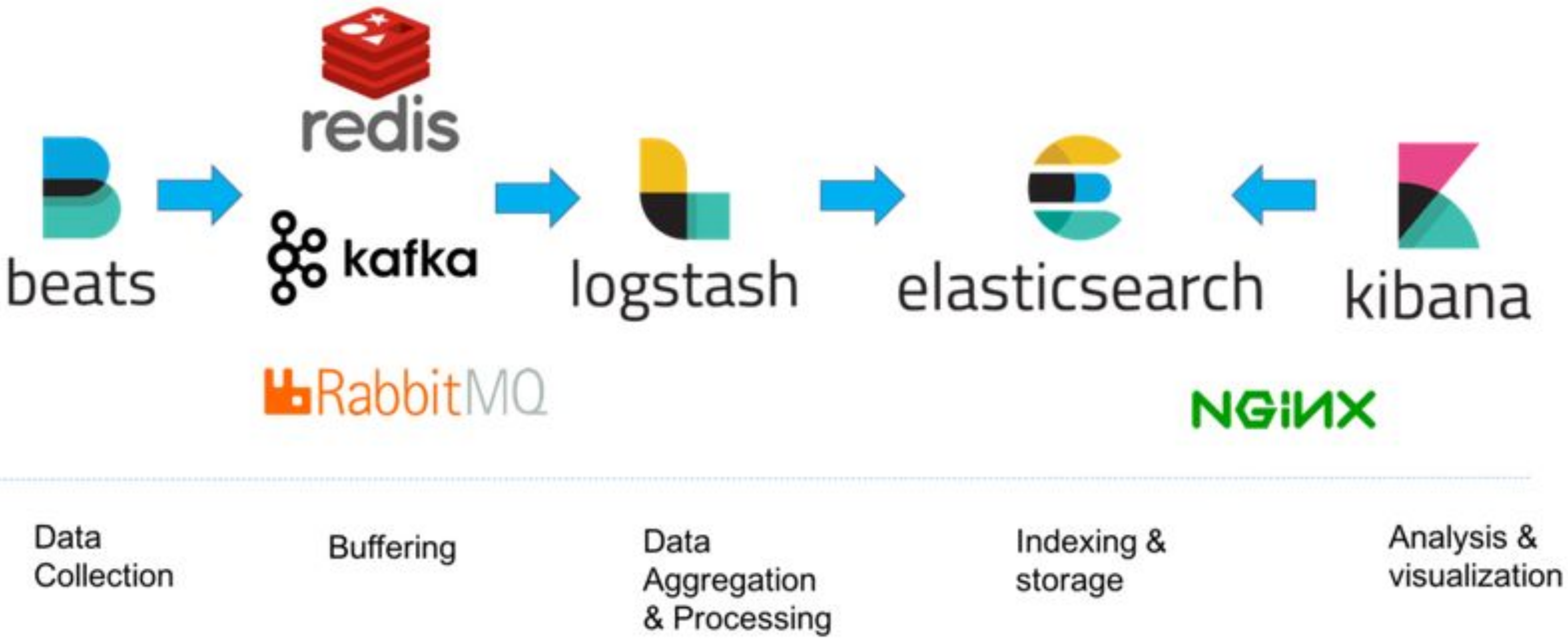
elasticsearch

Indexing &
storage

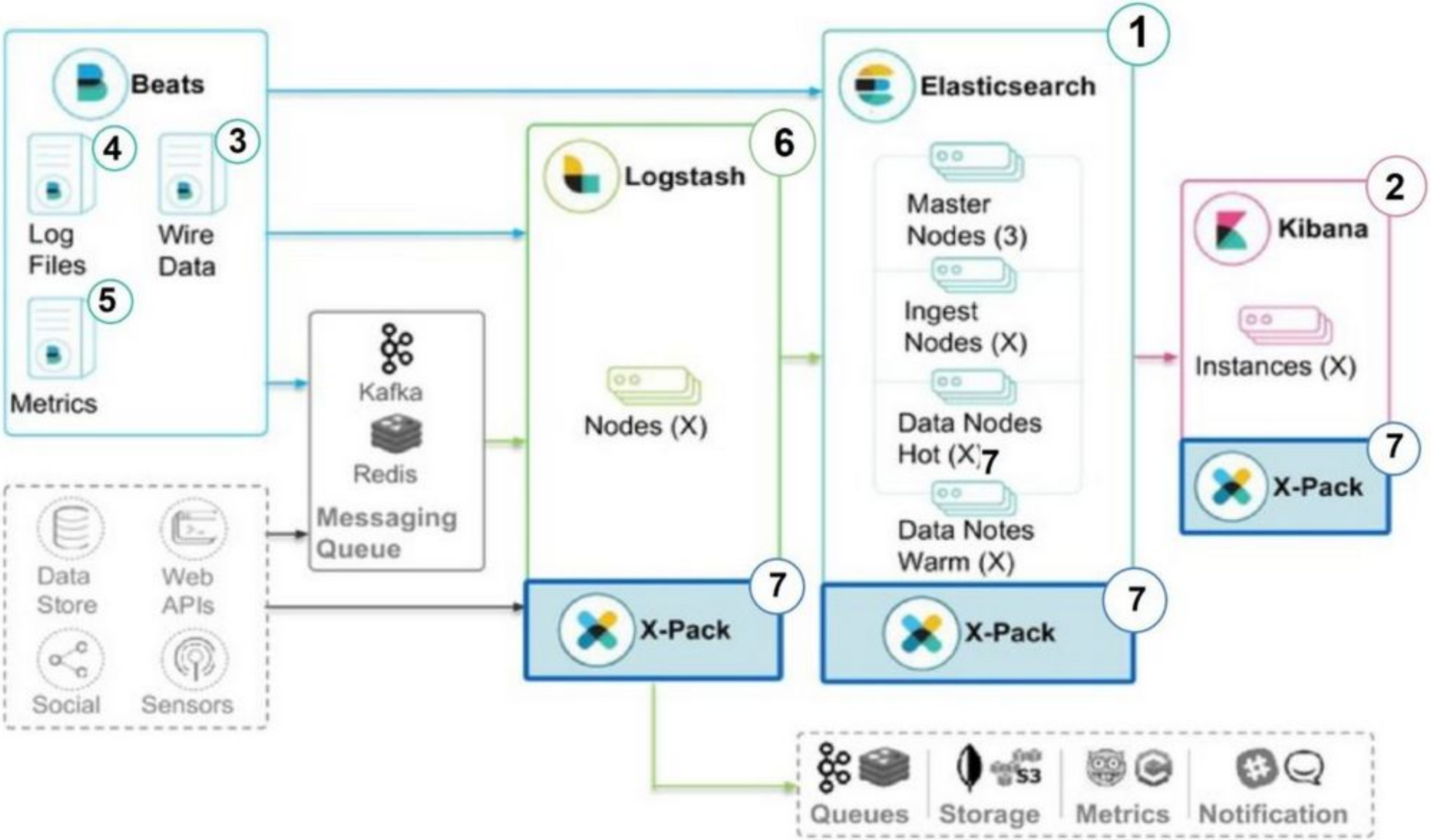
kibana

Analysis &
visualization

Elastic Stack



Elastic Stack



Beats

Filebeat

Metricbeat

Packetbeat

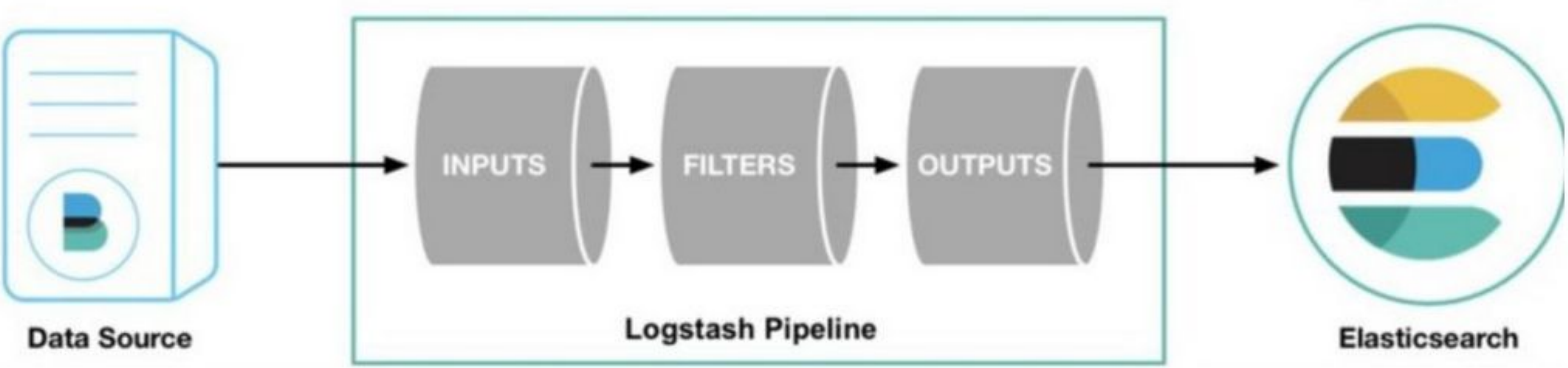
Winlogbeat

Auditbeat

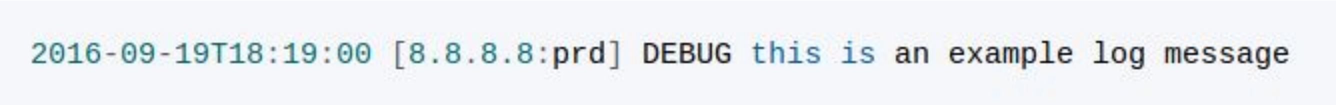
Heartbeat

Functionbeat

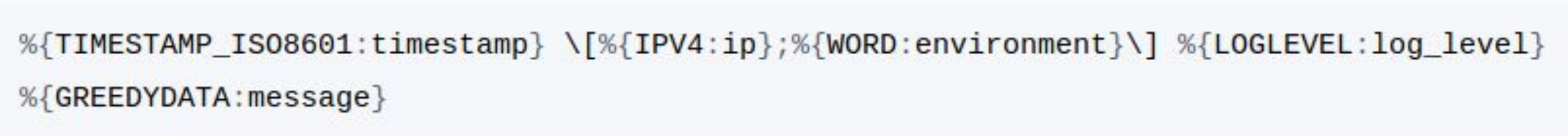
Logstash


Data Source
INPUTS
FILTERS
OUTPUTS
Logstash Pipeline
Elasticsearch

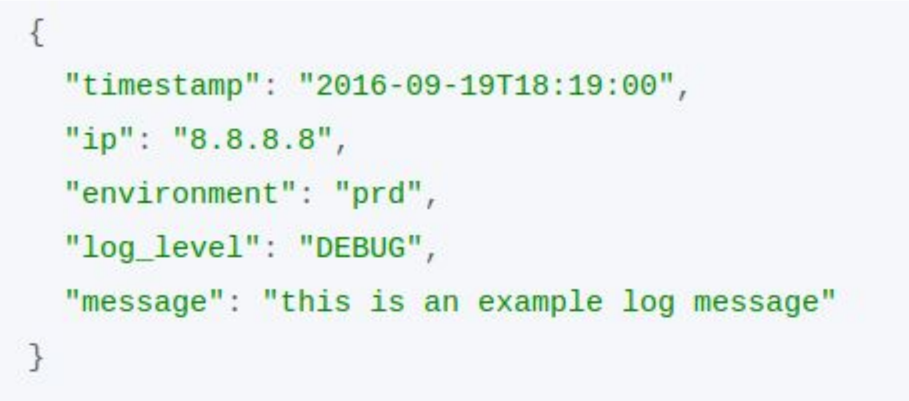
Logstash, grok filters



```
2016-09-19T18:19:00 [8.8.8.8:prd] DEBUG this is an example log message
```

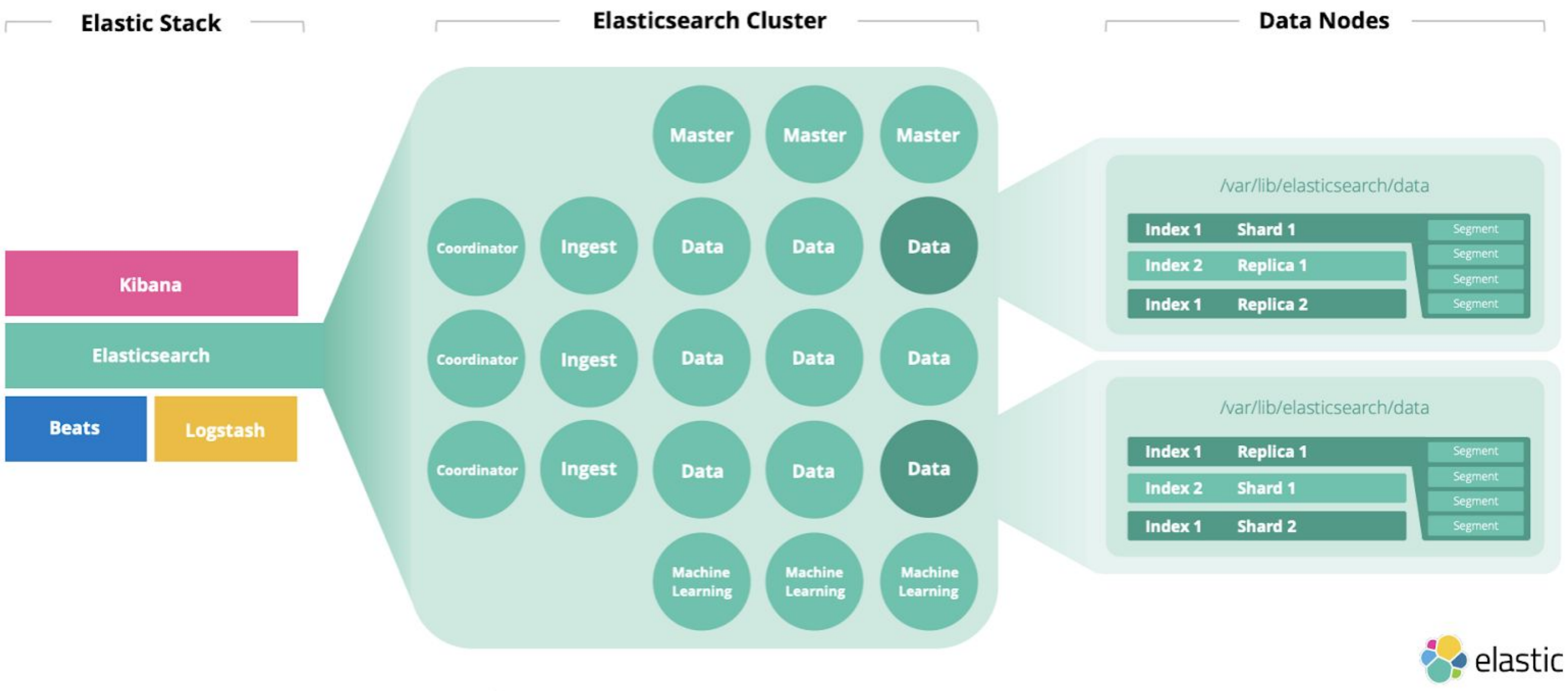


```
%{TIMESTAMP_ISO8601:timestamp} \[%{IPV4:ip};%{WORD:environment}\] %{LOGLEVEL:log_level}
%{GREEDYDATA:message}
```

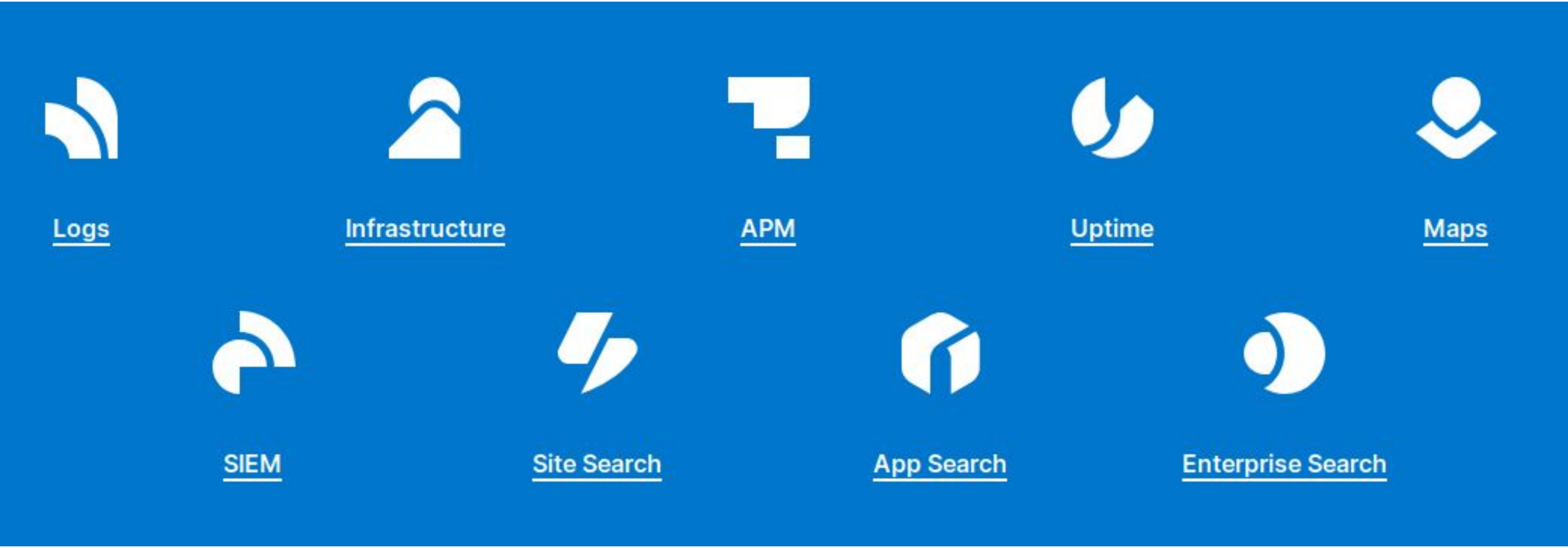


```
{
  "timestamp": "2016-09-19T18:19:00",
  "ip": "8.8.8.8",
  "environment": "prd",
  "log_level": "DEBUG",
  "message": "this is an example log message"
}
```

ElasticSearch



Demo


Logs
Infrastructure
APM
Uptime
Maps
SIEM
Site Search
App Search
Enterprise Search

Kafka

- Zookeeper 3 nodes
- Kafka 3 nodes
- Disk size!
- Cluster close to producers, per DC/Location
- First line defence (log flood)

Logstash Indexer

- perfect for K8S: stateless, scaling
- More CPU, less RAM
- Close to ElasticSearch, in the same DC

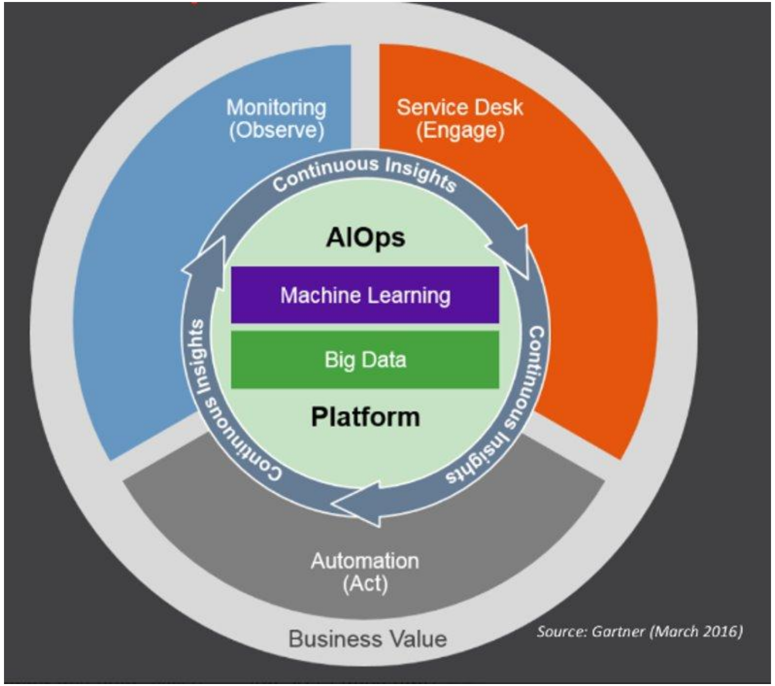
ElasticSearch

- max 32G heap memory
- between 800 to 1000 shards per data node
- shard size 20-100G
- Roles: master, data hot/warm/cold, ingest, coordinator

AIOPS - Artificial Intelligence for IT Operations

AIOps refers to multi-layered technology platforms that automate and enhance IT operations by

1. using analytics and machine learning to analyze big data collected from various IT operations tools and devices, in order to
2. automatically spot and react to issues in real time



Source: Gartner (March 2016)

Links:

- https://demo.elastic.co
- https://www.elastic.co/subscriptions

Questions ?

tomasz.gintowt@gmail.com