Elastic Stack

Tomasz Gintowt
Team Data Services
adform

Agenda

- LaaS
- AIOps
- Elastic Stack
- Beats
- Logstash
- Demo

Elastic Stack

Logging as a Service (LaaS) == Elastic Stack

Linas Daneliukas
IT Systems Engineer (Kaunas)

Giedrius Statkevičius
IT Systems Engineer (Kaunas)

Tomas Dabašinskas
Lead IT Systems Engineer (Kaunas)

Kęstutis Mizara
IT Systems Engineer (Vilnius)

Ruslanas Sobolevas
Senior IT systems engineer (Kaunas)

Robert Fabisiak
Senior IT systems engineer (Warsaw)

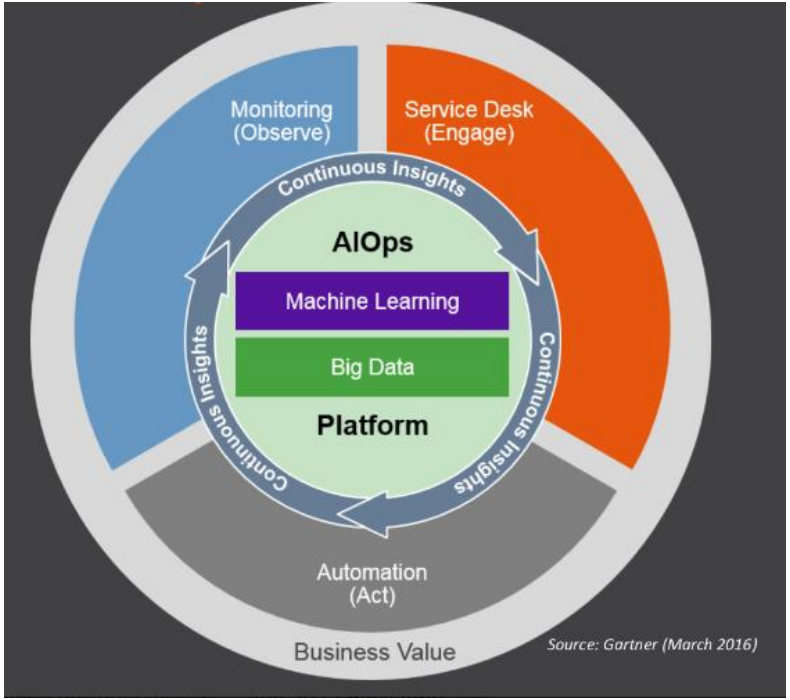
Tomasz Gintowt
IT systems engineer (Warsaw)

AIOPS - Artificial Intelligence for IT Operations

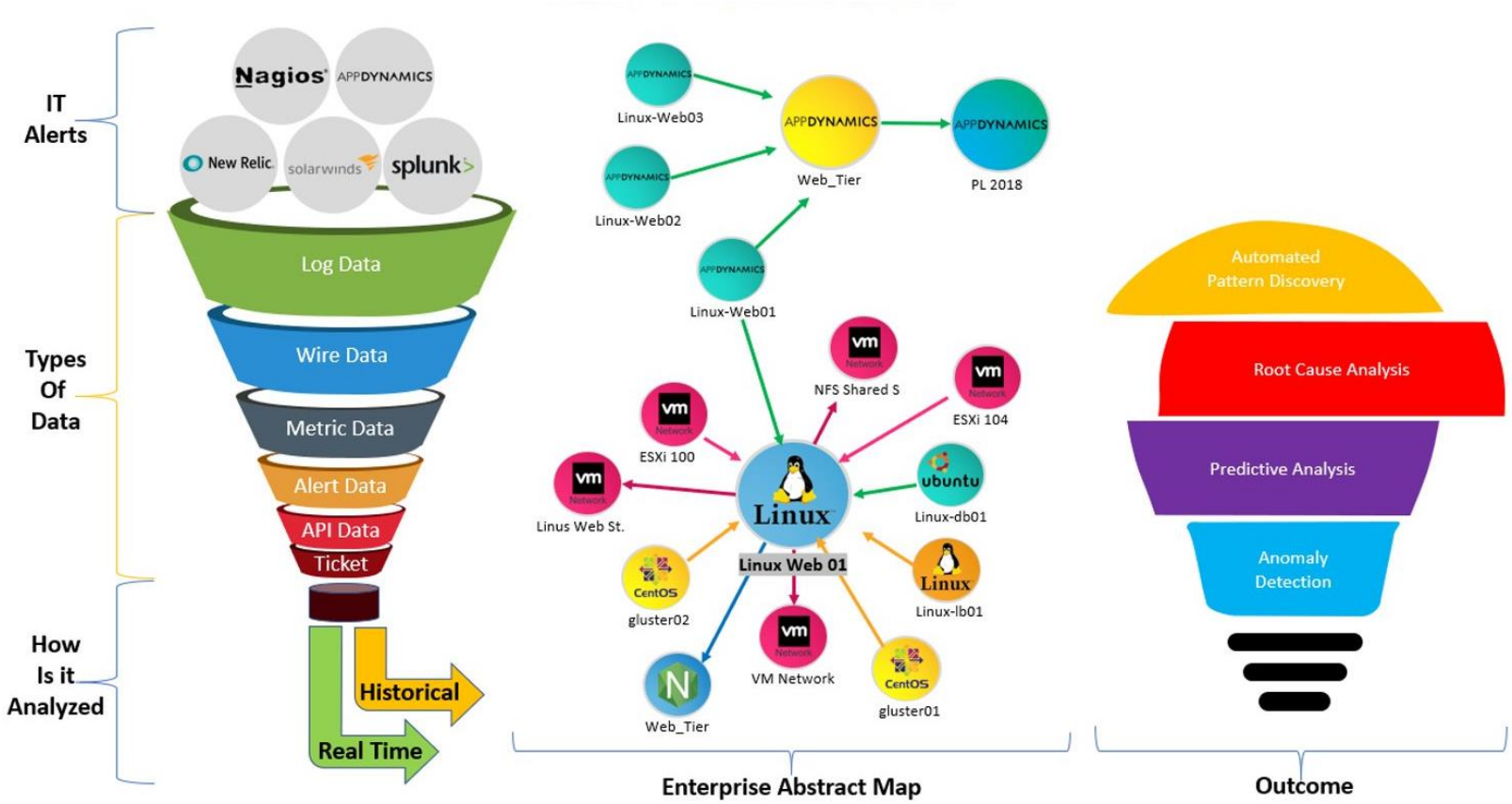
AIOps refers to multi-layered technology platforms that automate and enhance IT operations by

1. using analytics and machine learning to analyze big data collected from various IT operations tools and devices, in order to

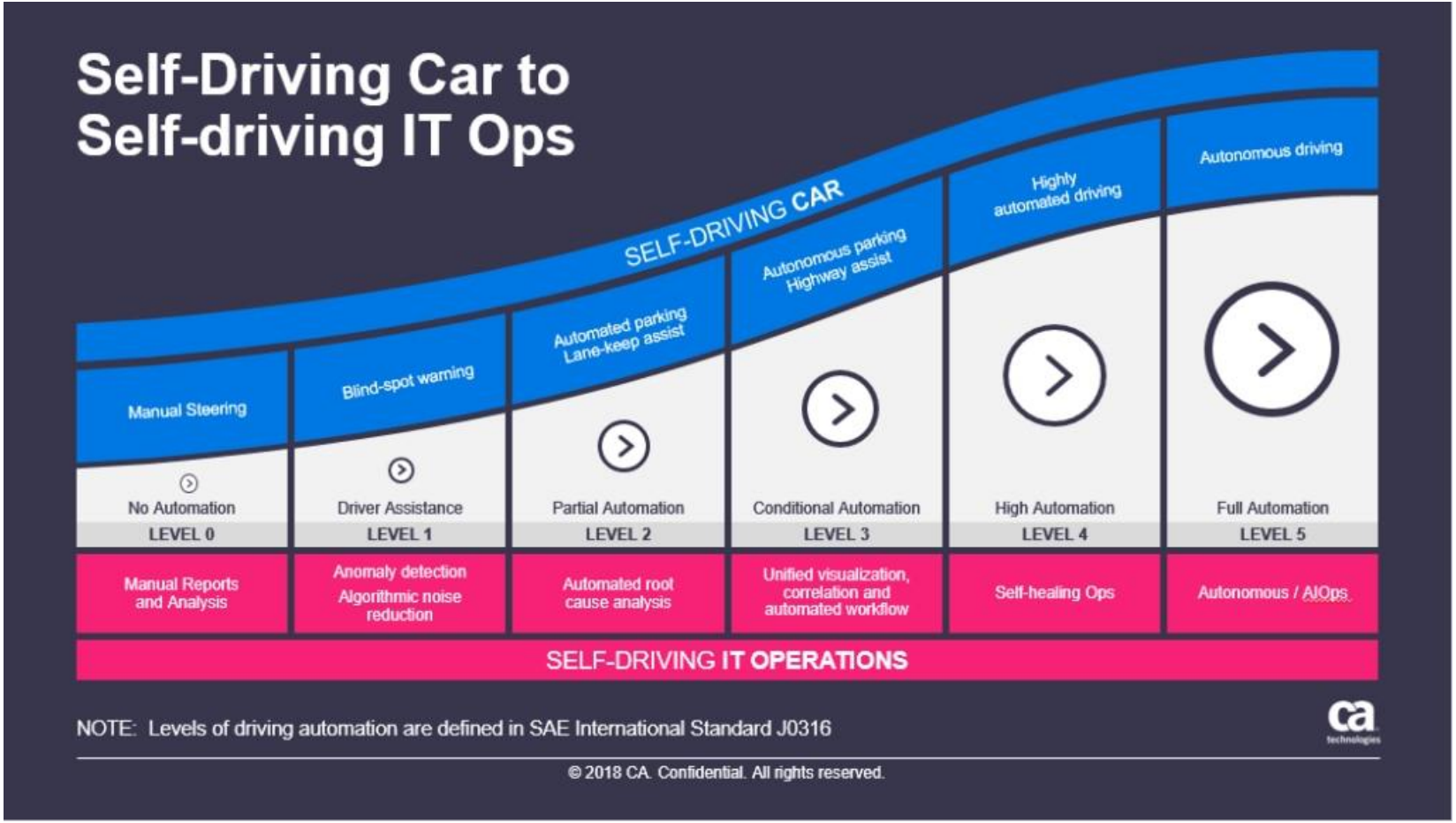
2. automatically spot and react to issues in real time



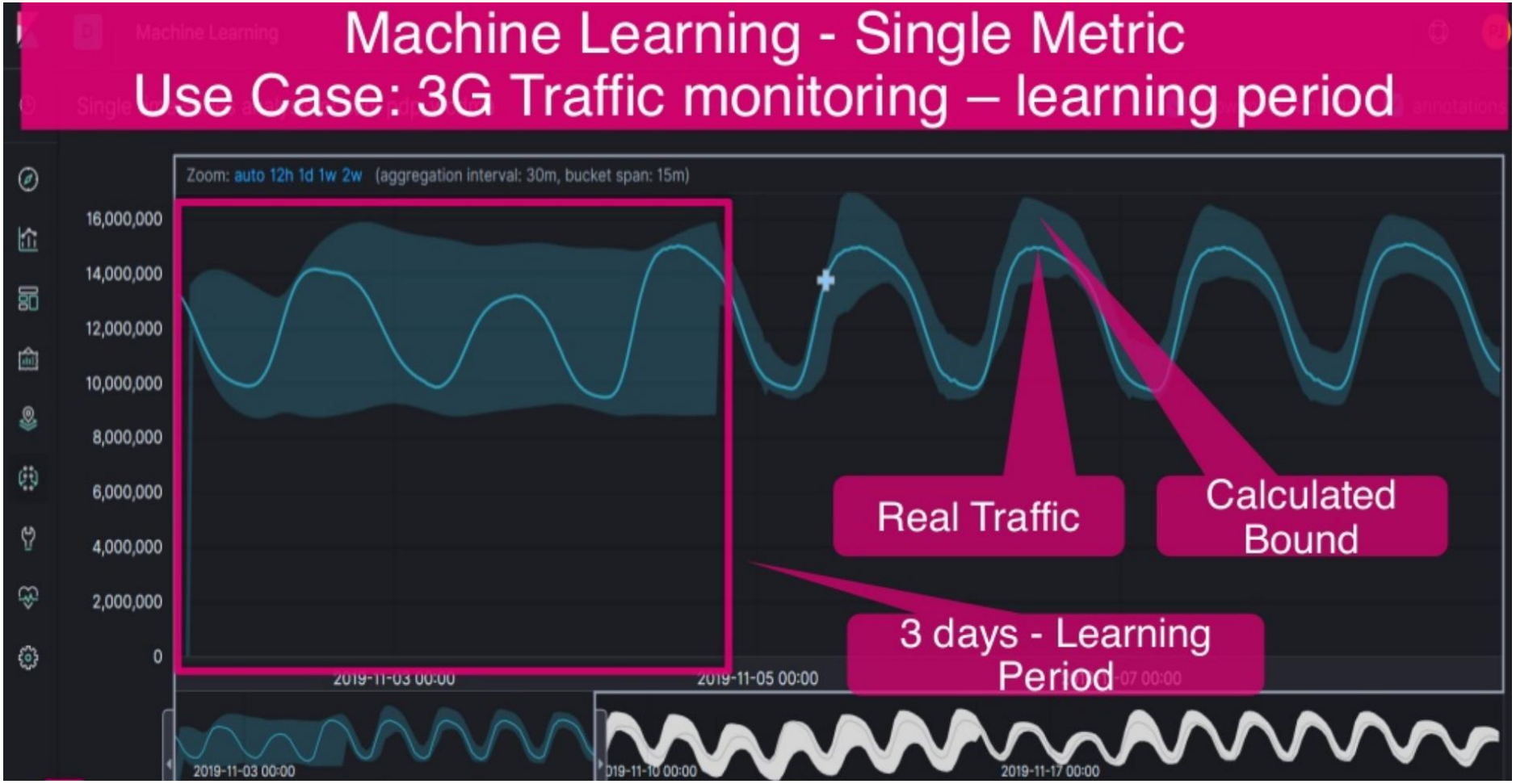
AIOPS - Artificial Intelligence for IT Operations



AIOPS - Artificial Intelligence for IT Operations



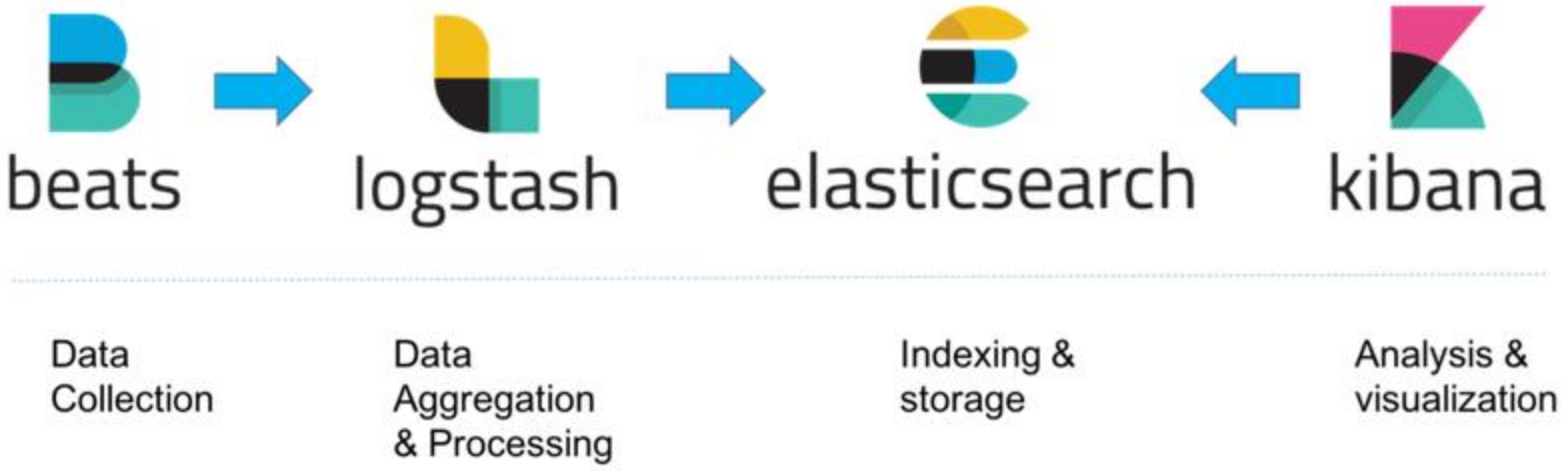
AIOPS - Artificial Intelligence for IT Operations



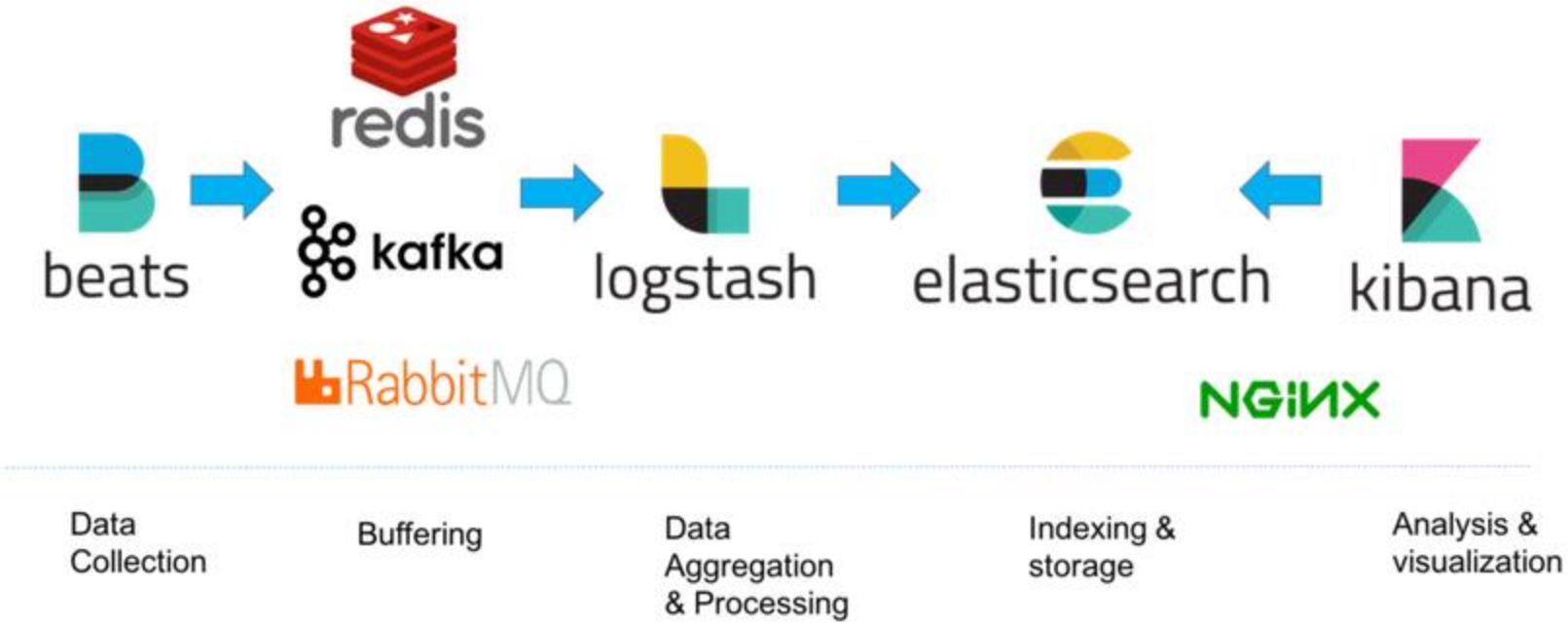
Elastic Stack

Elastic Stack

Elastic Stack



Elastic Stack



Beats

Filebeat

Metricbeat

Packetbeat

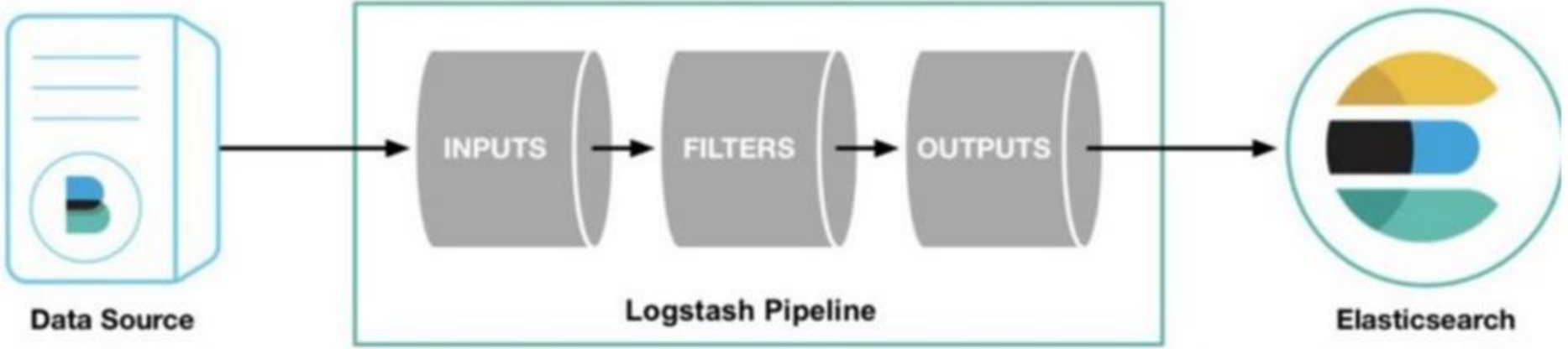
Winlogbeat

Auditbeat

Heartbeat

Functionbeat

Logstash


INPUTS
FILTERS
OUTPUTS
Data Source
Logstash Pipeline
Elasticsearch

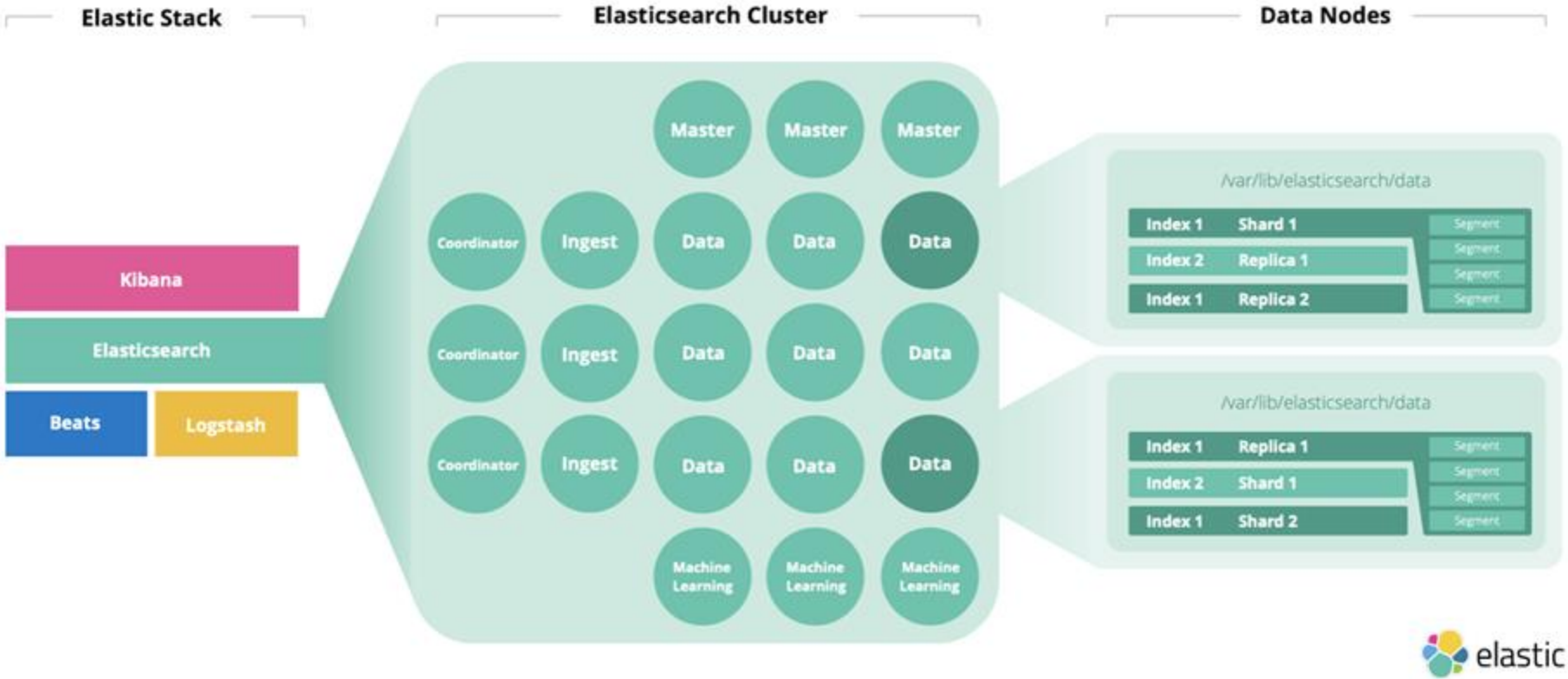
Logstash, grok filters

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

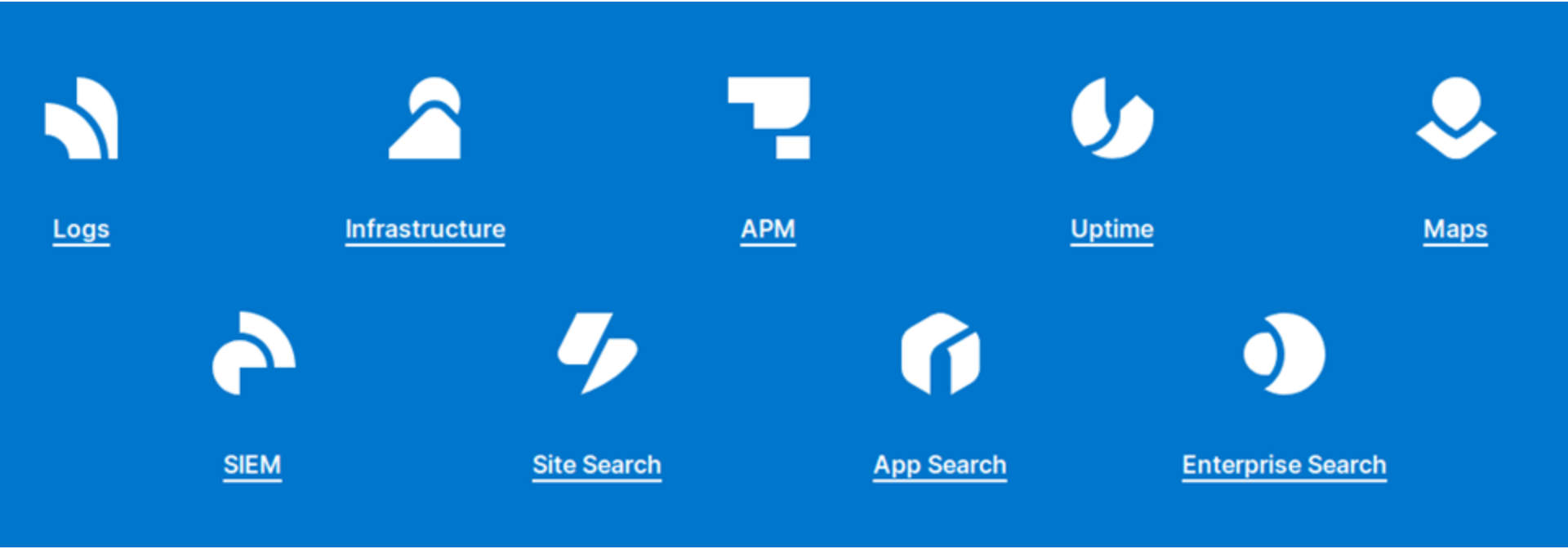
```
%{TIMESTAMP_ISO8601:timestamp} \[%{IPV4:ip};%{WORD:environment}\] %{LOGLEVEL:log_level}
%{GREEDYDATA:message}
```

```
{
  "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

Links:

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

Questions ?