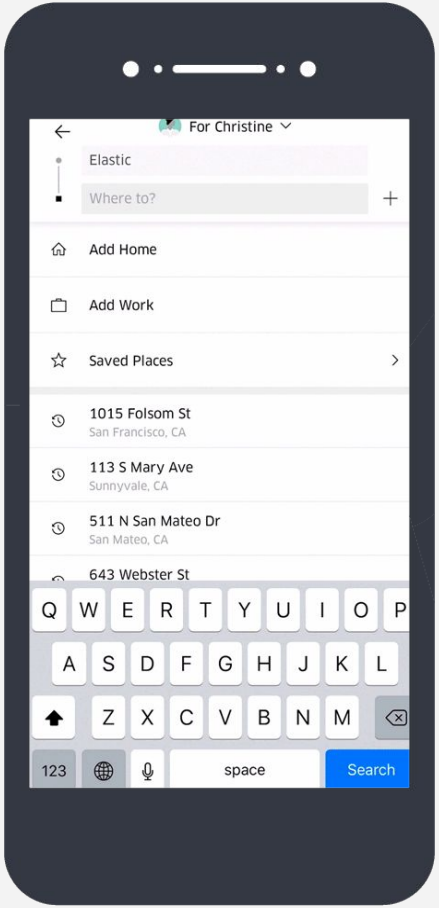
Elastic Workshop

The Elastic Stack

Welcome

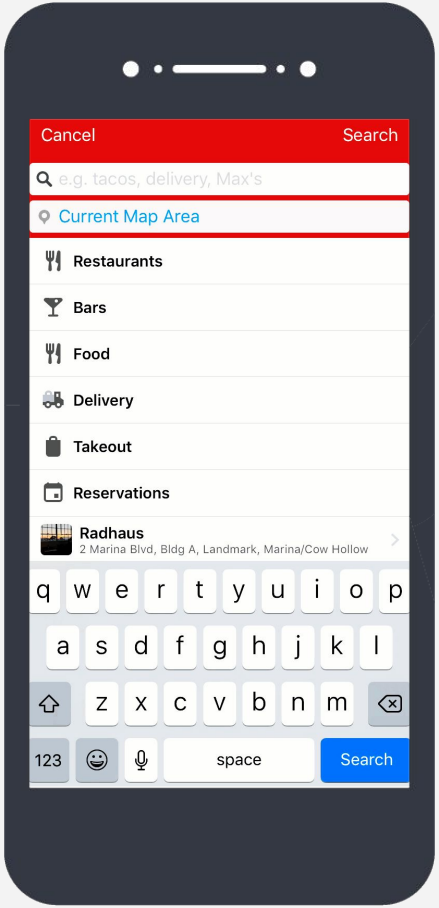
Lab	**bit.ly/elastic-lab**
Workshop	Instructor will provide a **bit.ly** link

Elastic is a **search company**



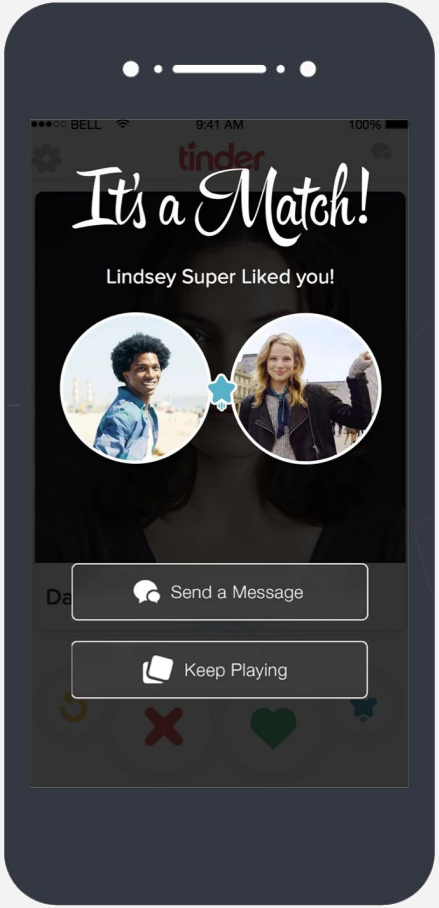
Uber

elastic



yelp®

elastic



tinder™

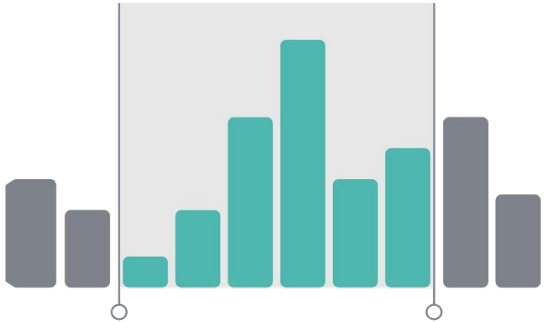
elastic

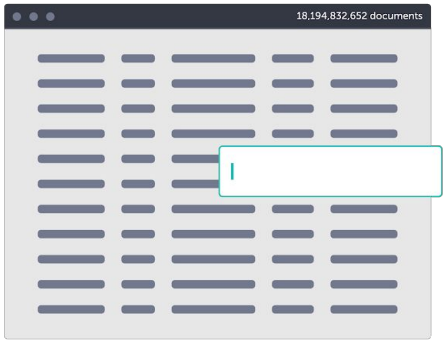
ACTIVISION BLIZZARD

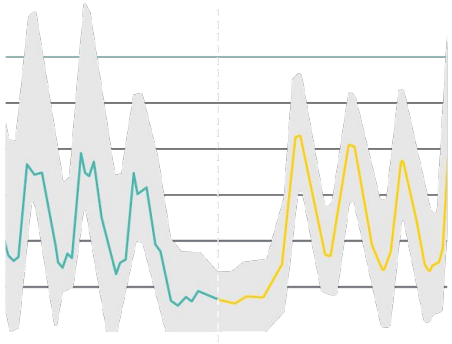
elastic

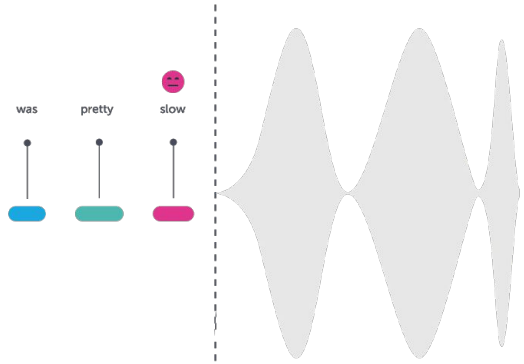
INDIANA UNIVERSITY

Search is a **constant/foundation**









Technology **differentiation**

SCALE

Distributed by design

SPEED

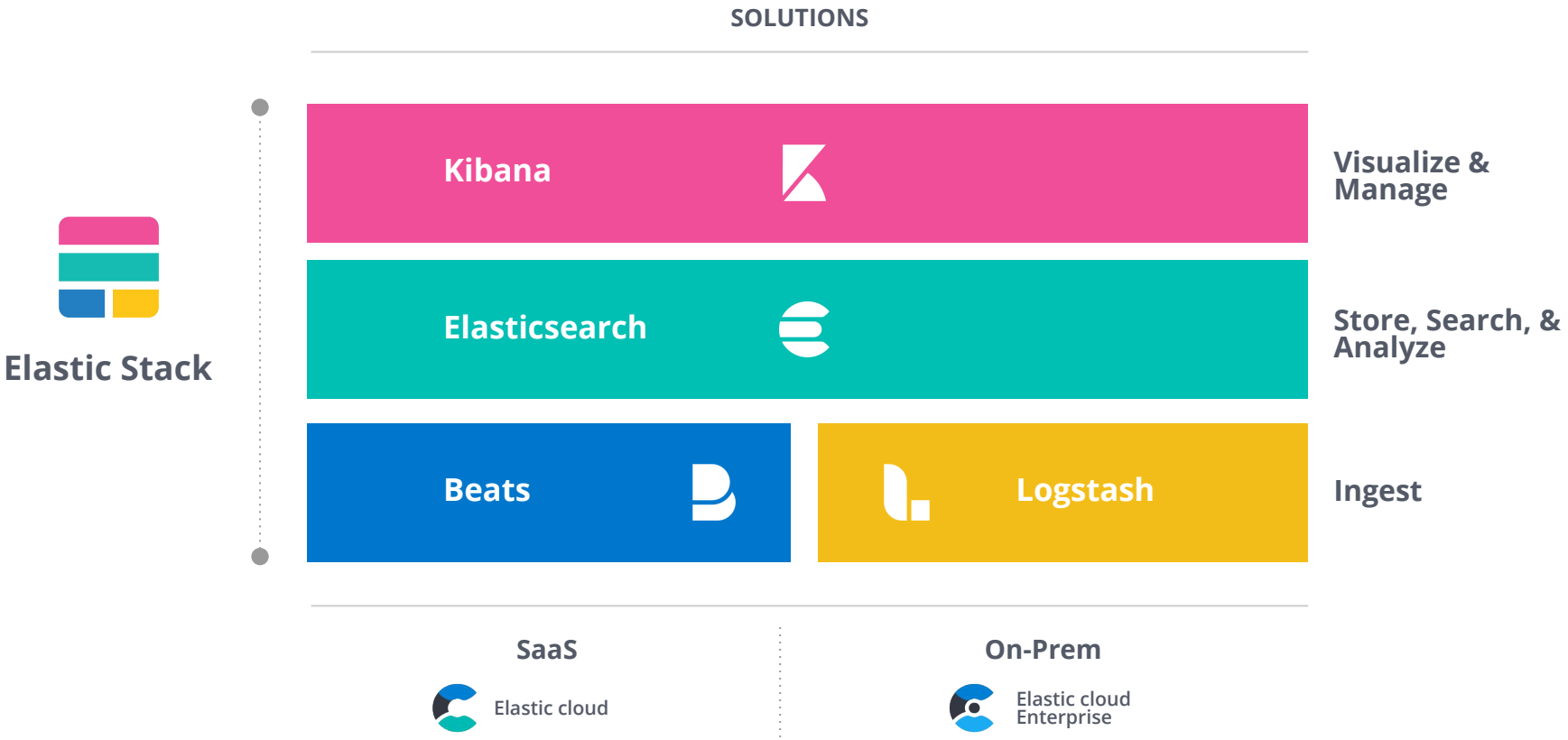
Find matches in milliseconds

RELEVANCE

Get highly relevant results

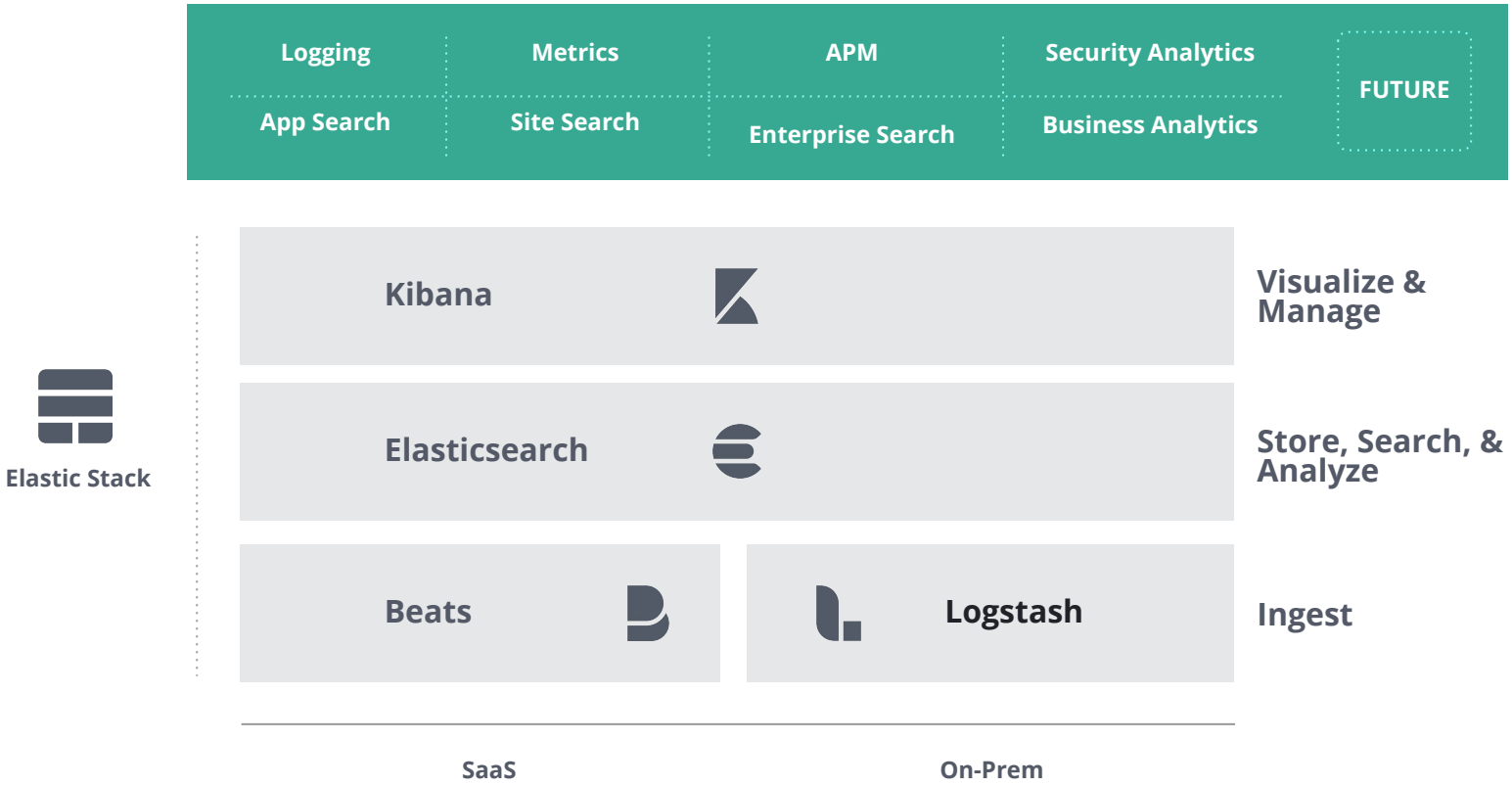
Elastic Products

Elastic **Stack**



elastic

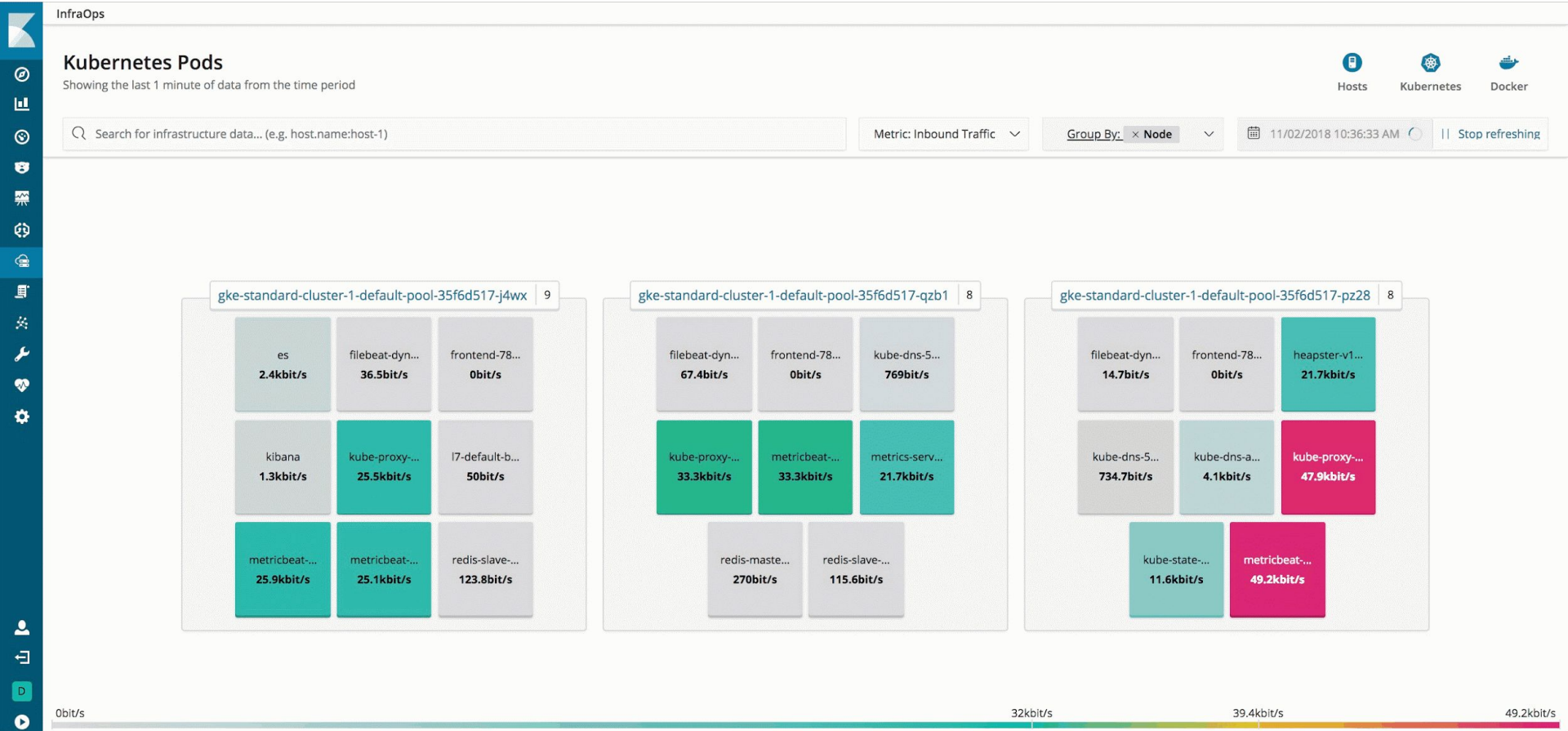
Solutions



elastic

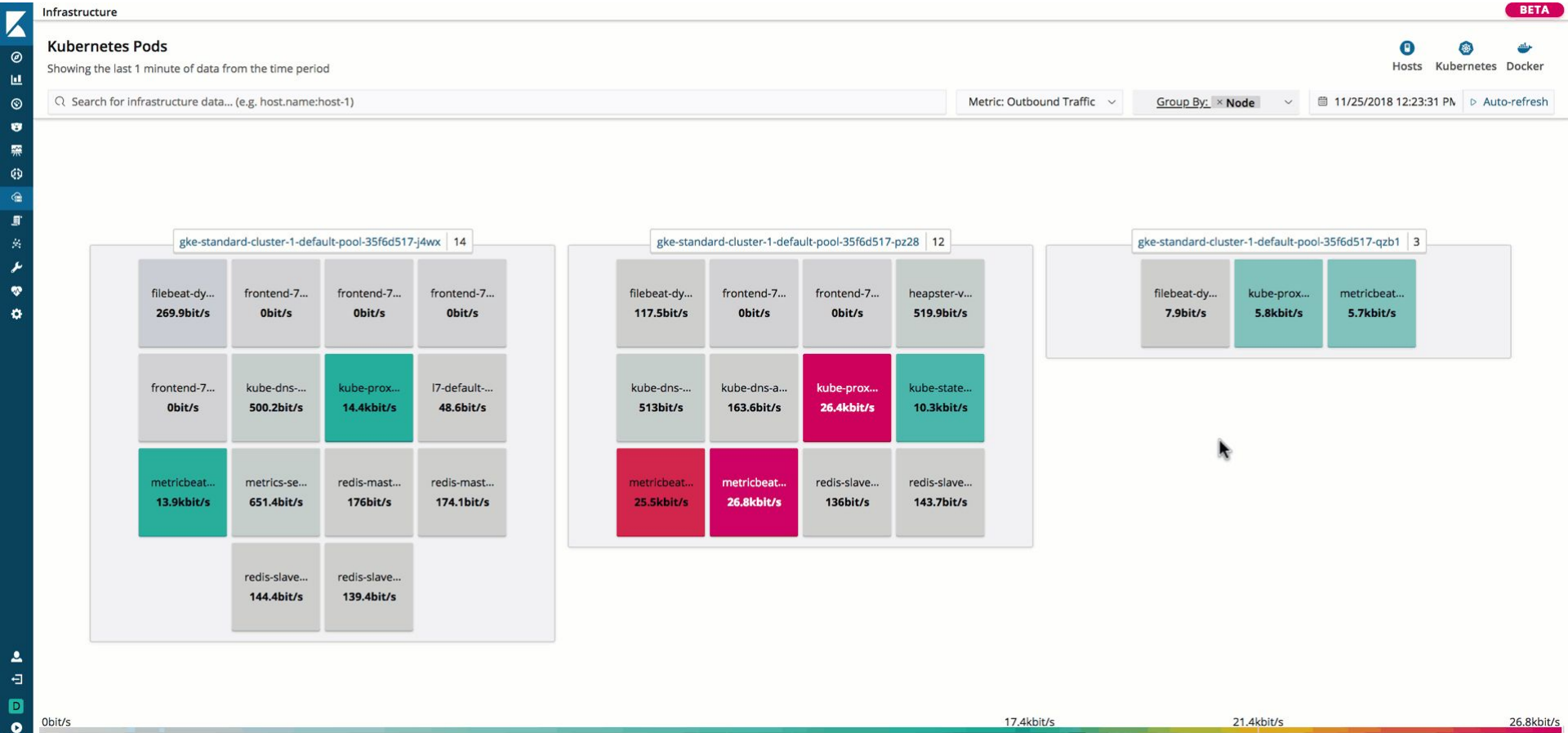
Logging

Your logs, your way. At any scale, with speed.



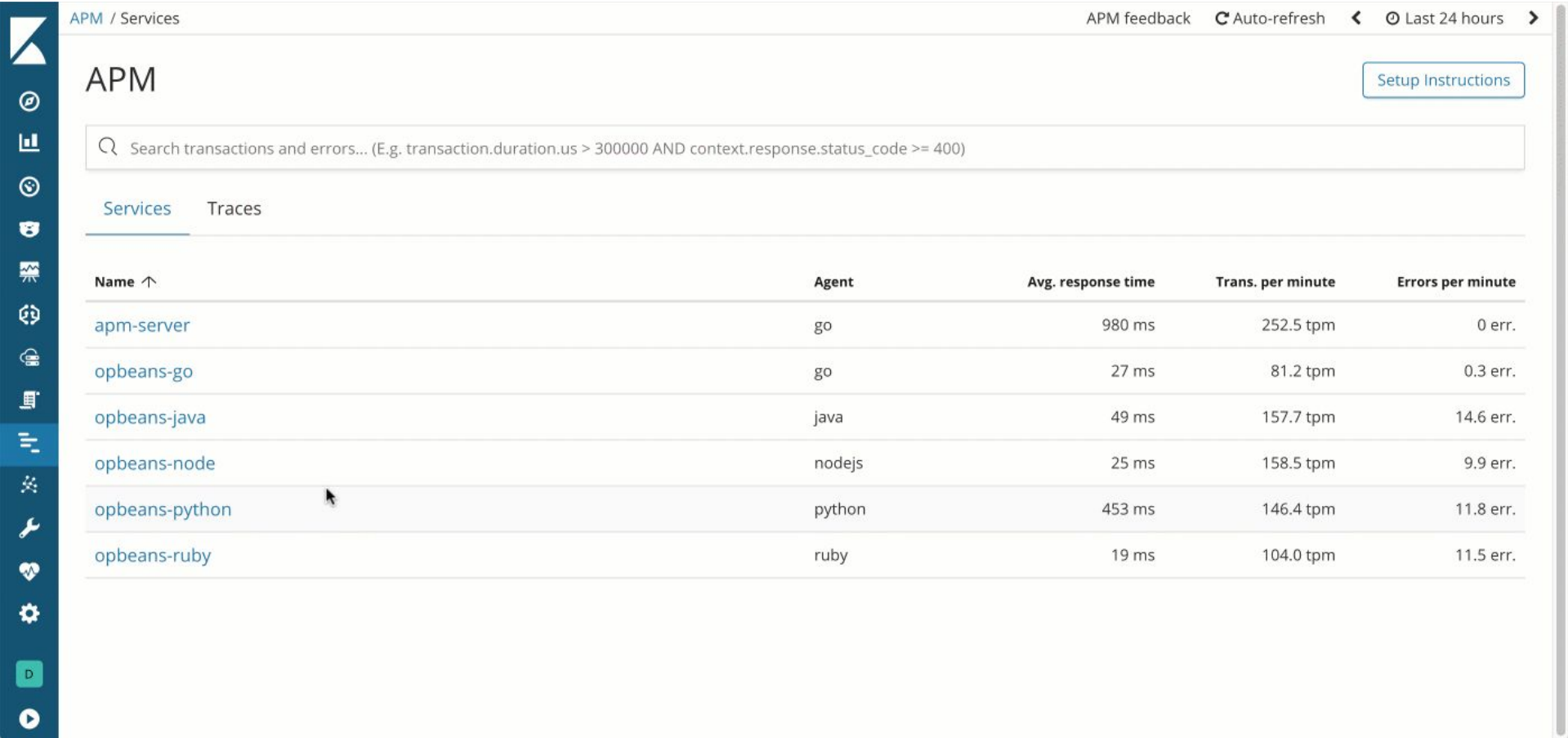
Infrastructure Metrics

Unify your infrastructure monitoring (logs, metrics, and traces) in one place



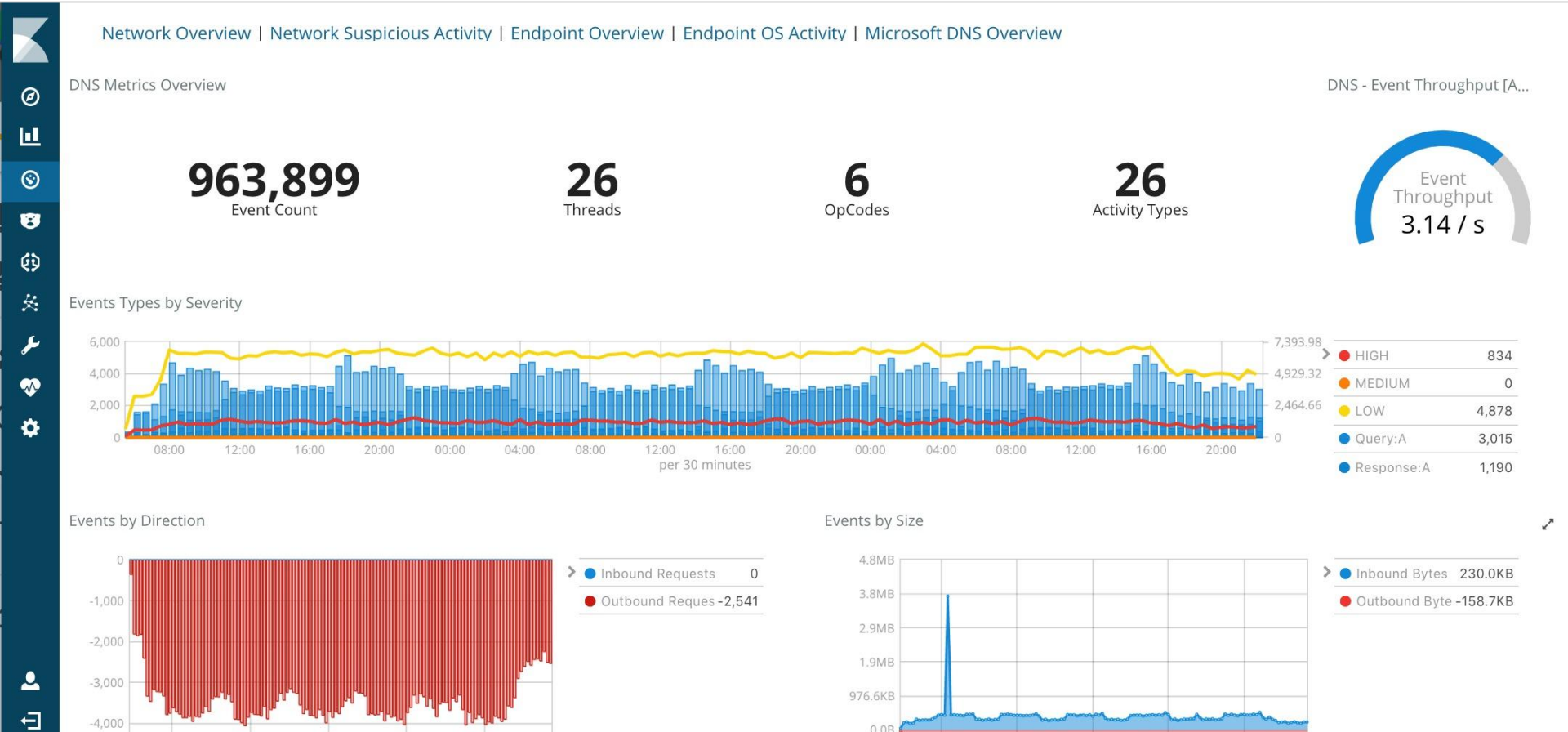
Application Performance Monitoring (APM)

Amplify your observability with application transaction and tracing

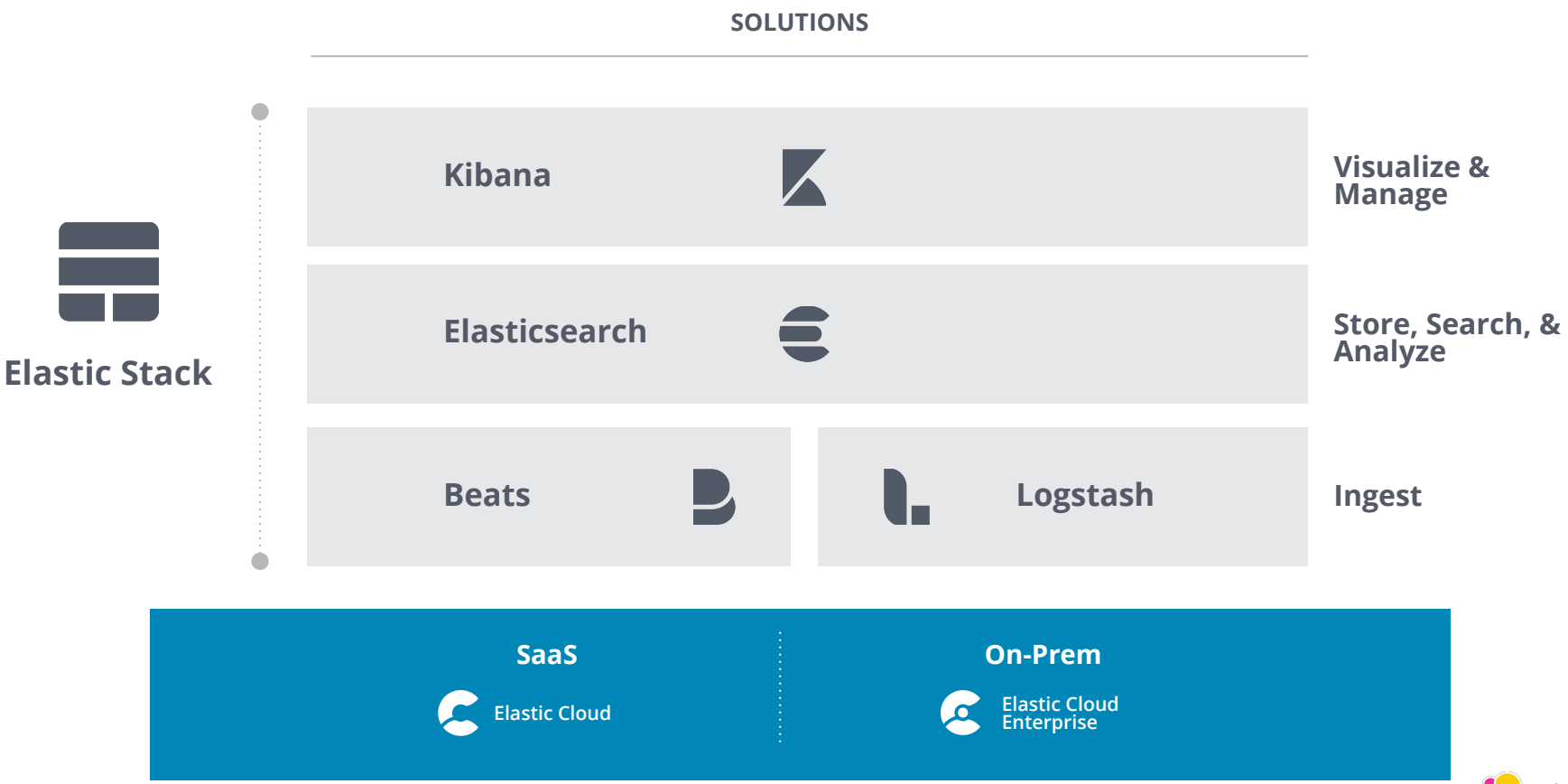


Security Analytics

A solution designed for fast, ad hoc exploration of security data at petabyte scale.



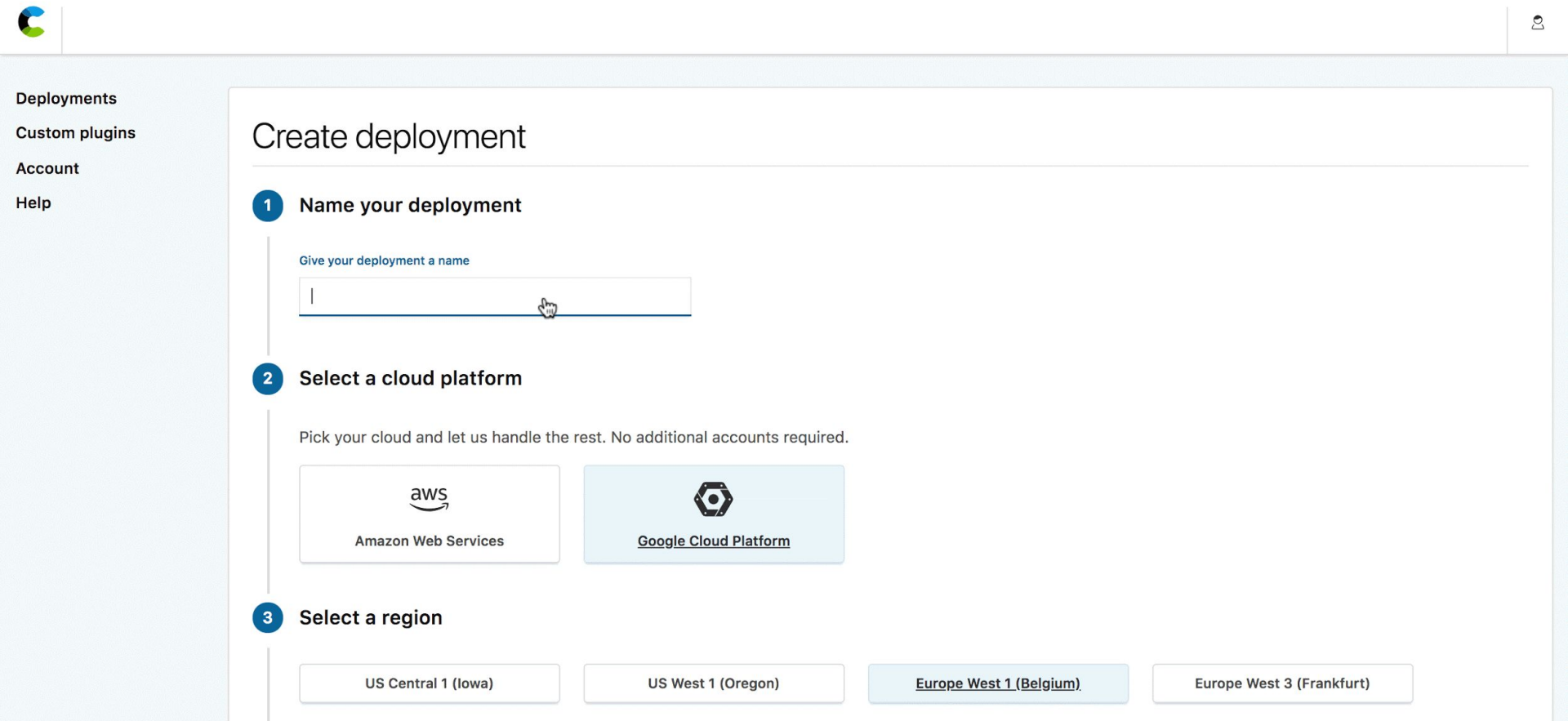
Deployment **options**



elastic

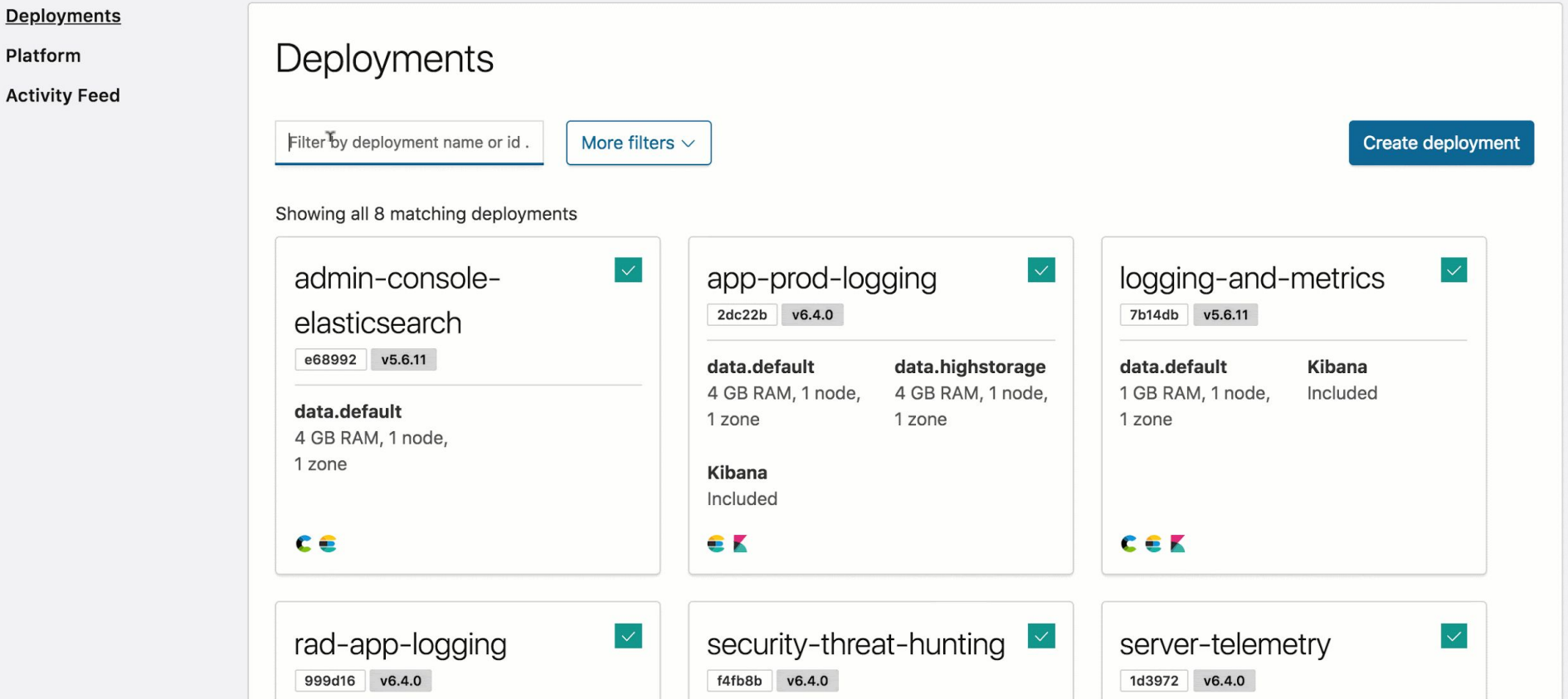
Elasticsearch Service

Hosted Elasticsearch, from the creators. No one hosts it better.



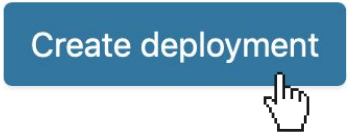
Elastic Cloud Enterprise

Packaging years of SaaS experience into a product



Lab: Section 1

Build an Elastic Cluster



cloud

cloud.elastic.co

elastic

Generated user

You can use the credentials below to login to Elasticsearch or Kibana. Make sure to save the password somewhere as this is the only time we can

Username `elastic`

Password `xdw5MILYNyaWI2eIVbCCaJYA`

Cloud ID

```
Workshop:dXMtZWFzdC0xLmF3cy5mb3VuZC5pbyRhNjY2NGFhNDJiODU0NW
Y2YjE4ZDE4ODNlZGEwNzE3OSQ2M2Y5YzI1YTljMWQ0YTNkYmZmN2M2YTBhO
WFmNWEzNg==
```

Get started with Beats and Logstash quickly. The Cloud ID simplifies sending data to your cluster on Elastic Cloud. Learn more ...

Lab: Section 2

Setup Linux

Trivia

What use-case was Elasticsearch originally created for?

recipe search

Ingest

Acquiring, enriching & transforming data

Logical Processing Pipeline

Beats

- Lightweight data shippers
- Files, system metrics, network packets, audit events
- Extensible framework
- Pre-built modules for many sources

Logstash

- Normalize, filter and enrich
- Standardize to a common format for unified analytics
- Centralized configuration management
- Persistent queues

Elasticsearch

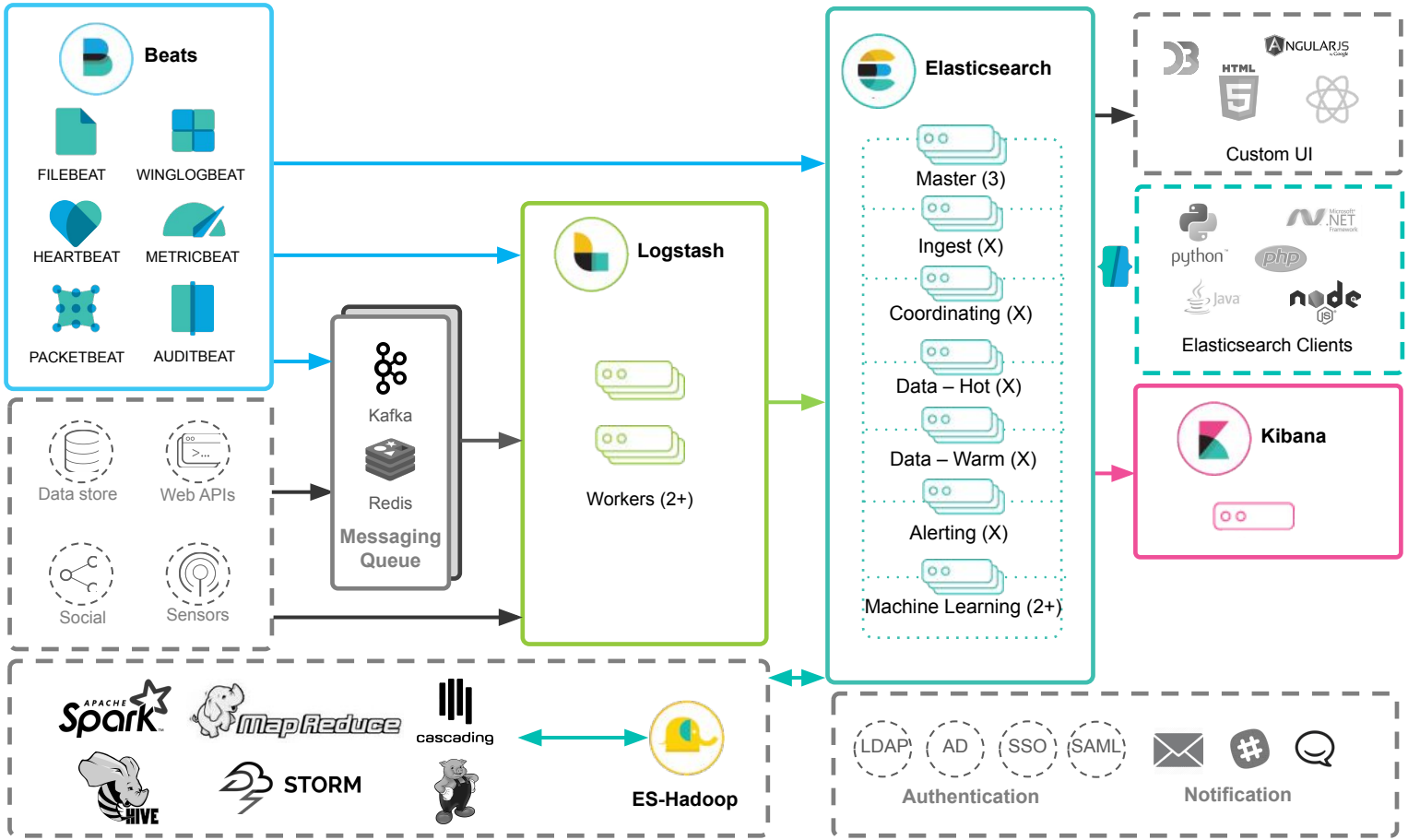
- Highly performant search and analytics
- Resilient and highly available
- Configurable node types for varied workloads
- REST API

Kibana

- Explore and search data
- Rich interactive visuals
- Development and management tools

elastic

Deployment in the Enterprise



elastic

Applications Web apps, servers, APIs log4j, JMX Twitter, Salesforce, Github	**Platform Infrastructure** Windows, Linux/Unix, MacOS Load balancers, proxies, caches S3, HDFS
Containers & Cloud Docker, Kubernetes AWS, Azure, GCP Openshift	**Data Stores & Streams** DBs, Data Warehouses NoSQL Kafka, Spark, Storm, Hive
Networking Netflow, PCAP HTTP, TCP, UDP, DNS, TLS syslog, auditd	**Security Devices** NSM, IDS/IPS, firewalls Web proxies, endpoints ArcSight
Messaging & Alerting Slack, HipChat Pagerduty, Email Nagios, Zabbix	**Raw Documents** PDF, XLS, PPT Technical, legal, healthcare documents
IoT Sensors, robots Connected cars Smart homes	**Build Your Own**

Logs

Metrics

Configs

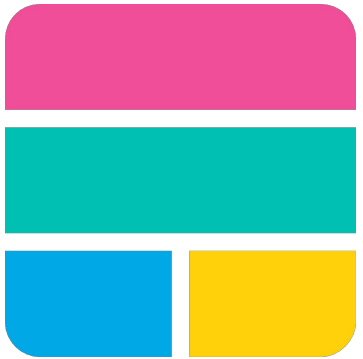
Messages

Scripts

Tickets

Alerts

Ingest Integrations



The Elastic Stack

elastic

Beats

Lightweight data shippers

- Ship from any source
- Transform at the edge
- Docker and k8s ready
- Cloud metadata enrichment
- 70+ community Beats
- 50+ modules

elastic

FILEBEAT
Log Files

METRICBEAT
Metrics

PACKETBEAT
Network Data

FUNCTIONBEAT
Serverless Monitoring

WINLOGBEAT
Window Events

HEARTBEAT
Uptime Monitoring

AUDITBEAT
Audit Data

Plus a growing set of community Beats

elastic

Immediate Insights with Modules

Turnkey experience for specific data types

Data to dashboard in just one step

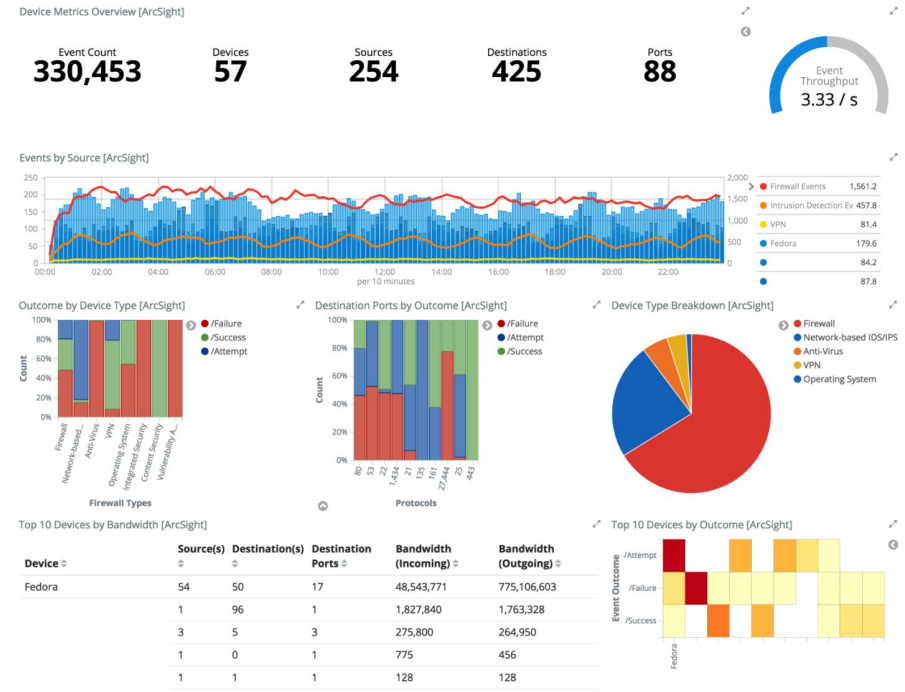
Automated parsing and enrichment

Default dashboards, alerts, ML jobs

Common schema (ECS) (Roadmap)

Available with

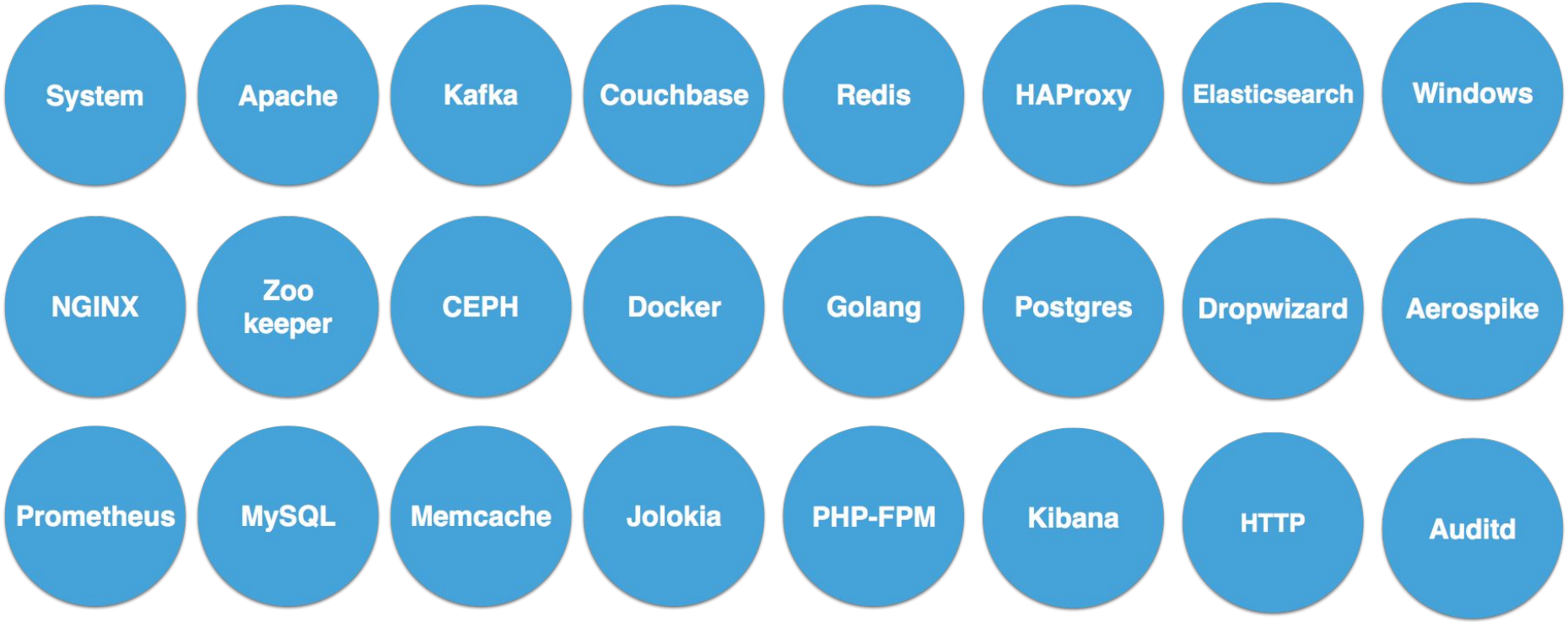
Logging | **Metrics** | **Security**



elastic

Beats Modules

Simplify collecting, parsing, and visualizing common log formats



elastic

Lab: Section 3

Metricbeat

Lab: Section 4

Filebeat

Trivia

How many people does Elastic employ?

1597

Alerting

Be notified about your data and take action

Alerting

Alert on anything you can query

Powered by Elasticsearch

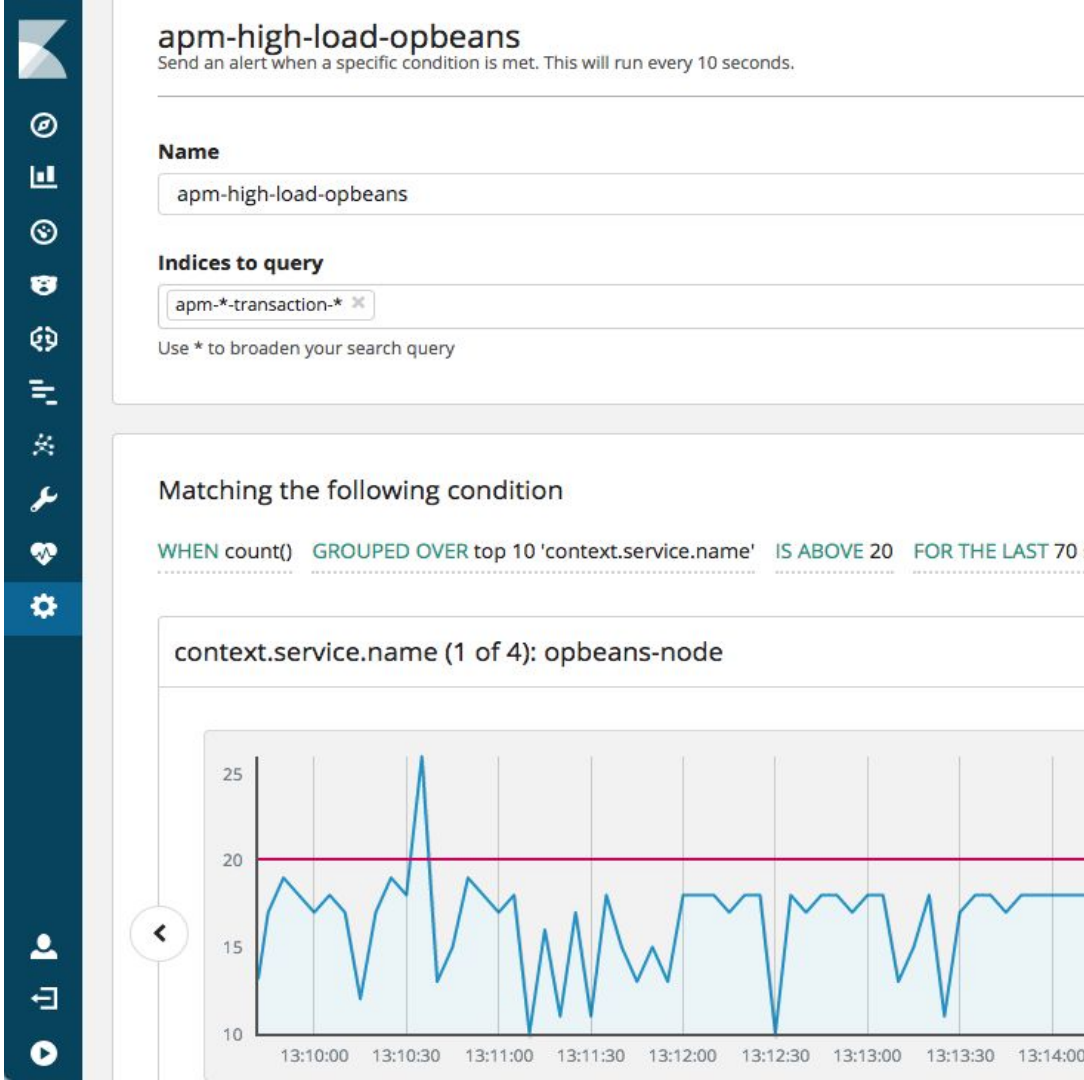
Alert on any Elasticsearch query
Distributed execution
Highly available

Notifications

Email, Slack, PagerDuty.
Custom (webhook)

Stack Integrations

Machine learning, Monitoring, and Reporting



Alert Users to Conditions

Host Behavior

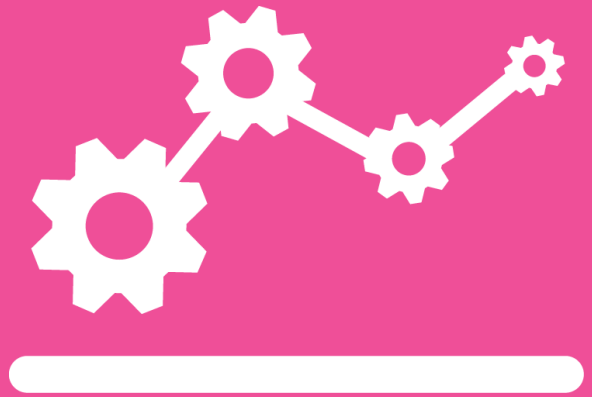
- Free disk space goes below 5%
- Process X starts on any server

Network or User Behavior

- > 5 failed logins on a machine in 5 min
- Excessive data transfer

Application Monitoring

- App response time exceeds SLA
- Active connections exceed threshold



Alert using all of the power of Elasticsearch

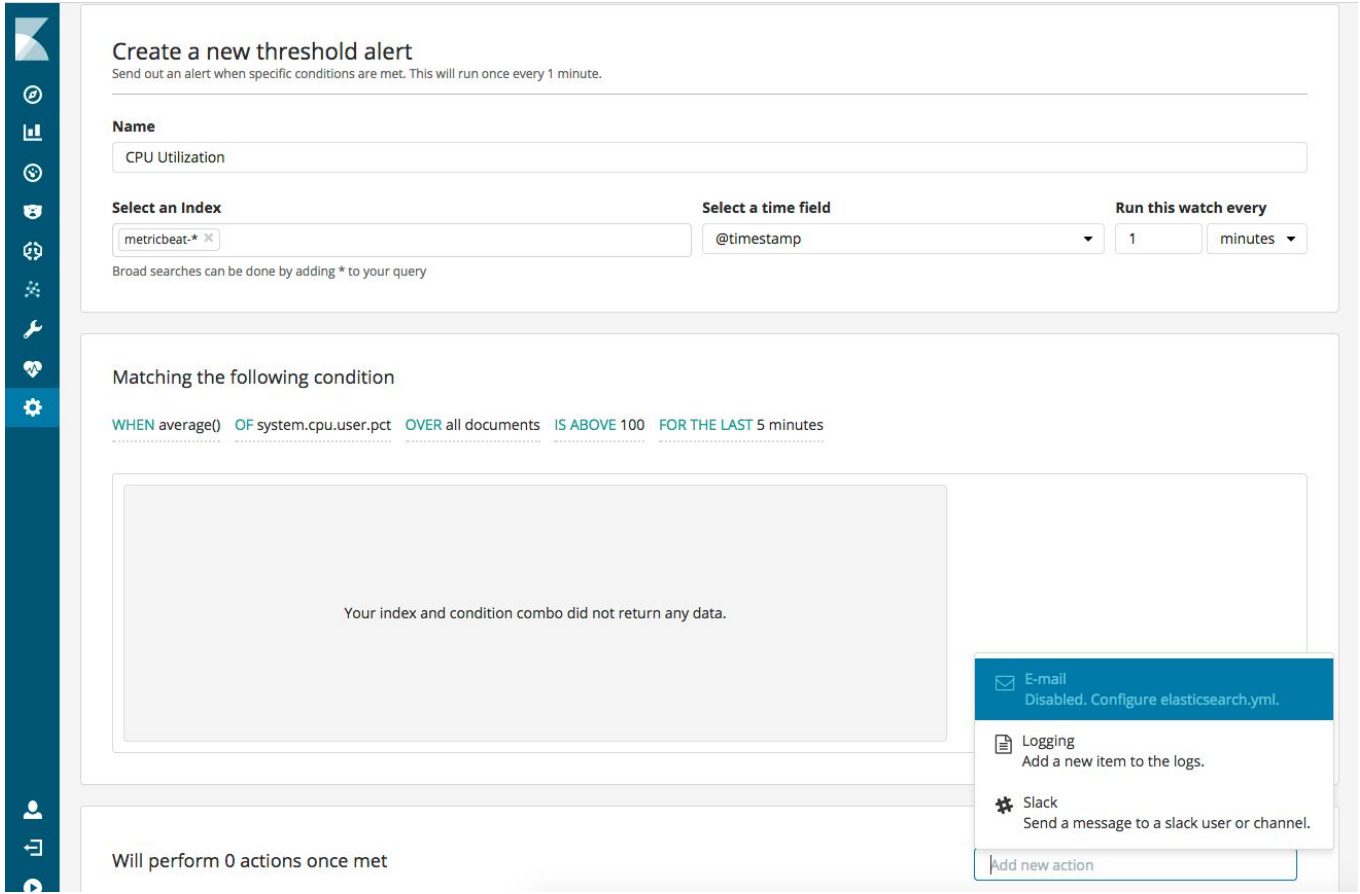
If you can query it, you can alert on it

- any Elasticsearch queries (full-text, geo, date math, pipeline aggs)
- anomalies detected by **machine learning**

Combine data from multiple sources

- Combine multiple Elasticsearch indices
- Include external http feeds (weather, threats feeds, etc.)

Creating Threshold Based Alerts is Easy

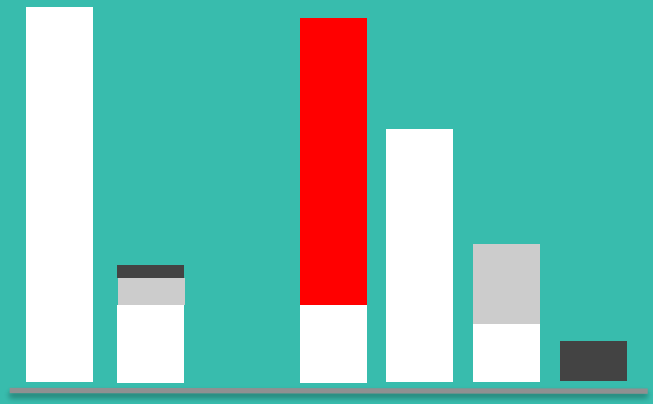


elastic

Leverage Your Alert History

Full alert history is available:

- How often are SLAs violated?
- What security incidents are trending?
- Which servers fail the most?
- What events are correlated with other events in the infrastructure?



high memory alerts

-- server 1 -- server 2 -- server 3

Lab: Section 5

Alerting

Trivia

What is the default Kibana port?

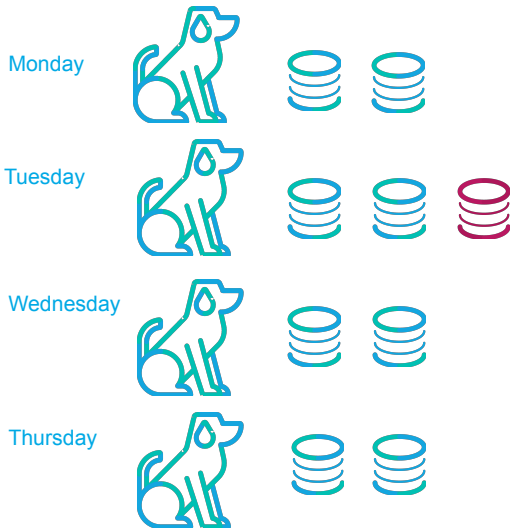
5601

Machine Learning

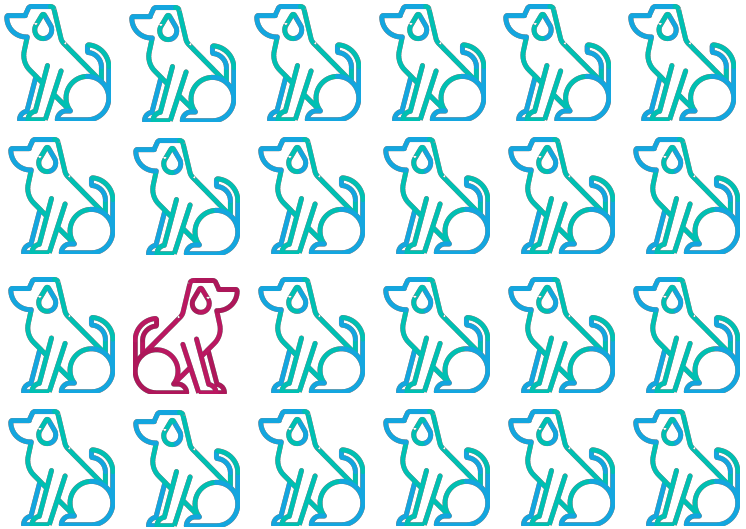
Finding potential problems automatically

What is Normal?

When something behaves like itself



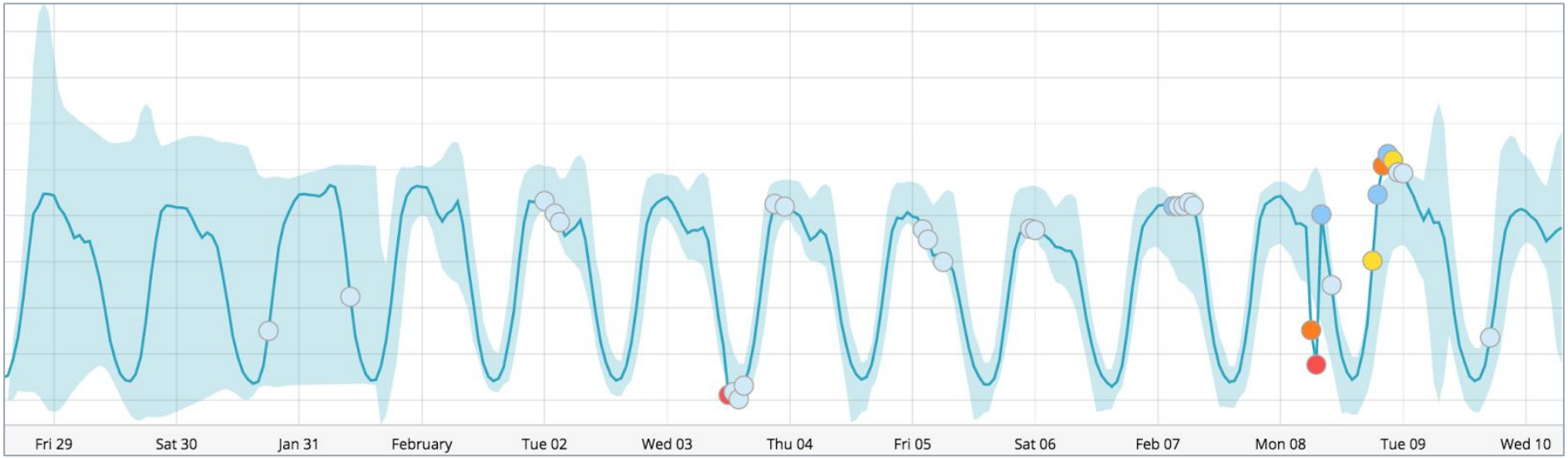
When something behaves like its peers



elastic

Learning what is normal for your environment

A model always evolving



elastic

When *ab*normal matters

Host Behavior

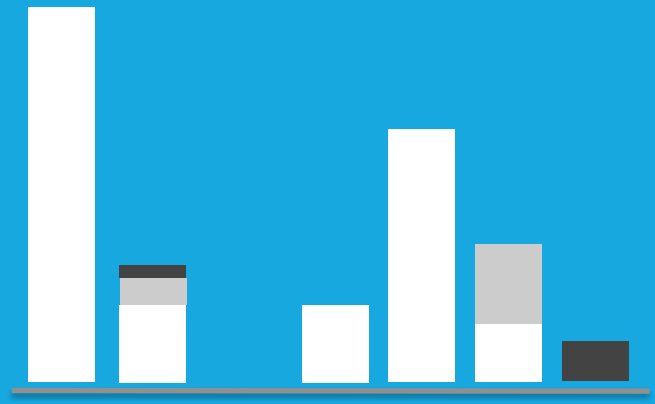
- Free disk space lower than average
- Unusual log entries

Network Behavior

- Unusual connections between hosts
- Higher than average data transfer

Application Behavior

- App response time abnormally high
- Active connections exceed normal



high memory alerts

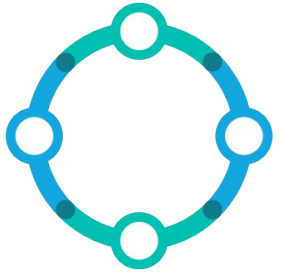
-- server 1 -- server 2 -- server 3

The advantages of anomaly-driven alerting

Understand Seasonality

Reduce False Positives

Identify Areas of Focus



Avoid Manual Review and Revision

Lab: Section 6

Machine Learning

Conclusion

Thank You

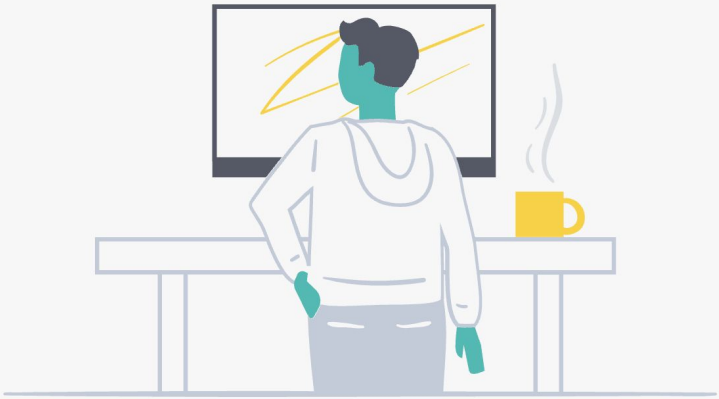
- Your **lab Linux host** will be **deleted** after the Lab ends
- Take the Lab to try at Home or Work (**use any Linux box**)
- Your **cloud.elastic.co** cluster you built is good for **2 weeks**
- Please submit anonymous feedback to help us improve

Want More?

https://www.elastic.co/training

X-Pack: Machine Learning

Register



Course Details

Audience

Anybody who would want to use X-Pack Machine Learning to discover anomalies in their data and create automation of Machine learning jobs.

Duration

With nearly 2.5 hours of instructional video, 4 labs and 30 quizzes we expect participants to allocate between 6-8 hours to complete this course.

Language

English

Elastic Training

https://www.elastic.co/training

Immersive Learning

Lab-based exercises and knowledge checks to help master new skills

Solution-based Curriculum

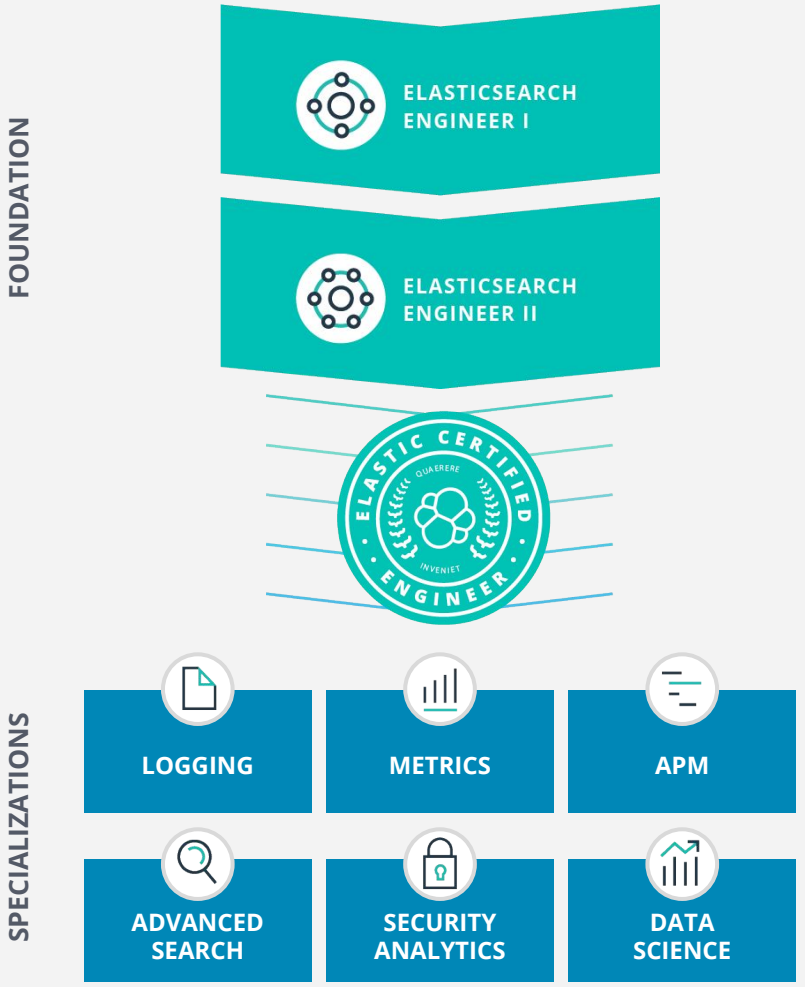
Real-world examples and common use cases

Experienced Instructors

Expertly trained and deeply rooted in everything Elastic

Performance-based Certification

Apply practical knowledge to real-world use cases, in real-time



THANK YOU