



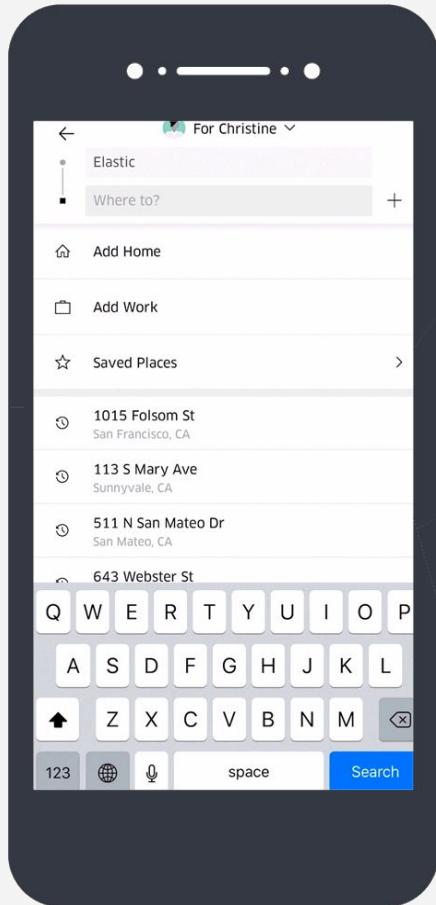
Elastic Workshop

The Elastic Stack

Welcome

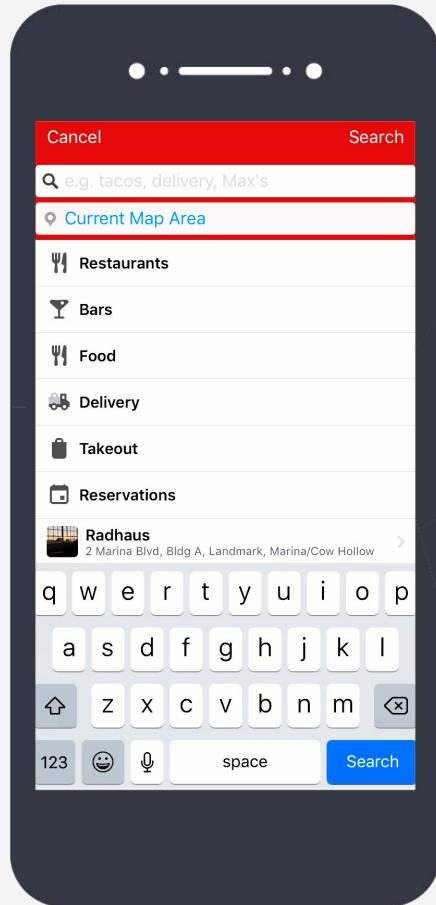
Lab	bit.ly/elastic-lab
Workshop	Instructor will provide a bit.ly link

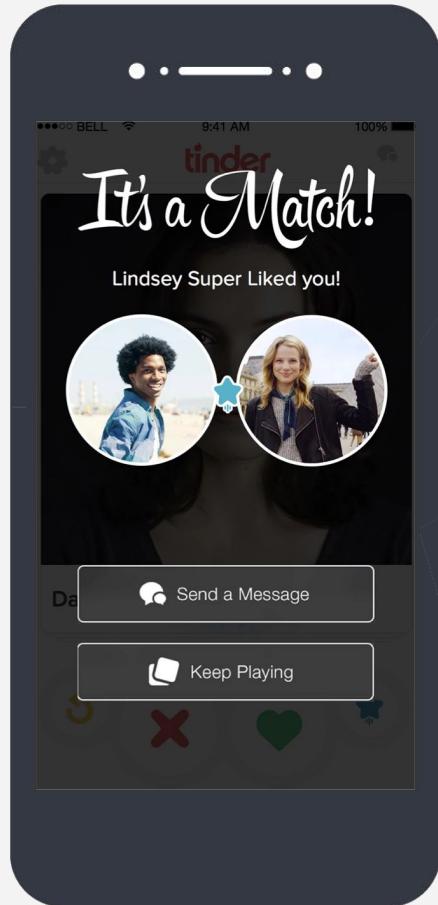
Elastic is a **search company**



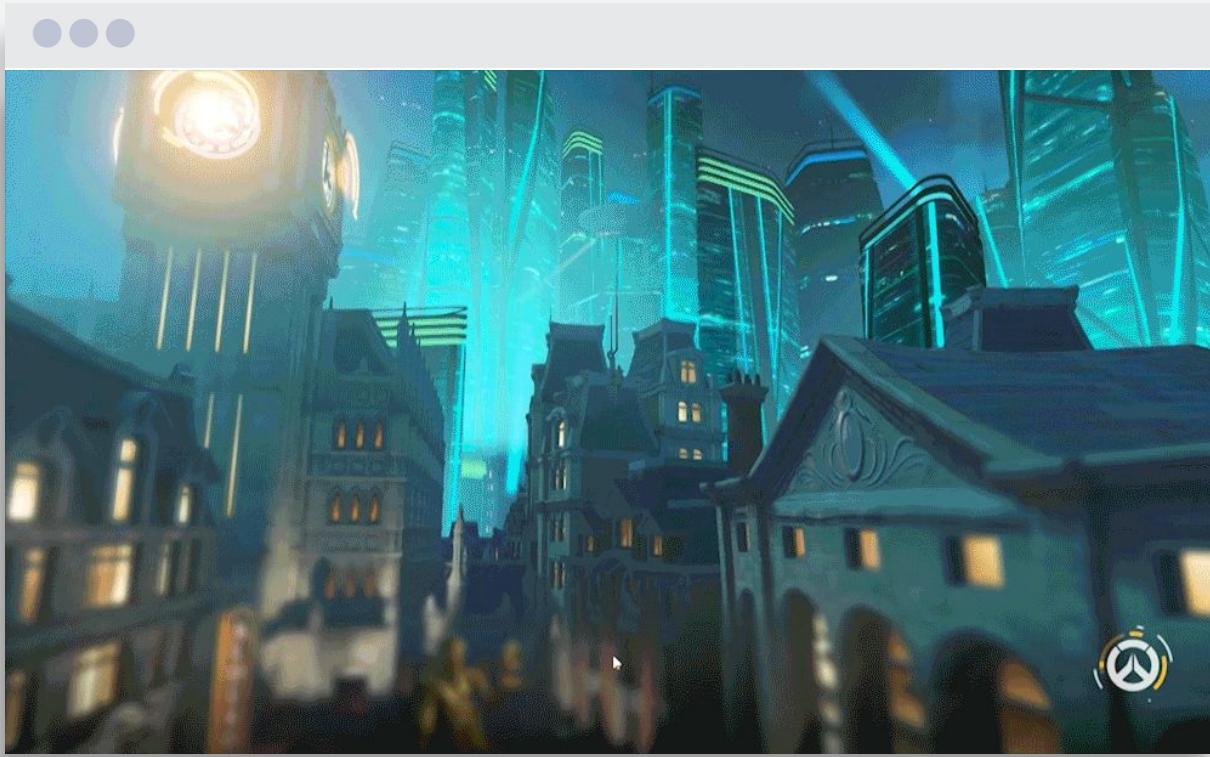
Uber







tinder™

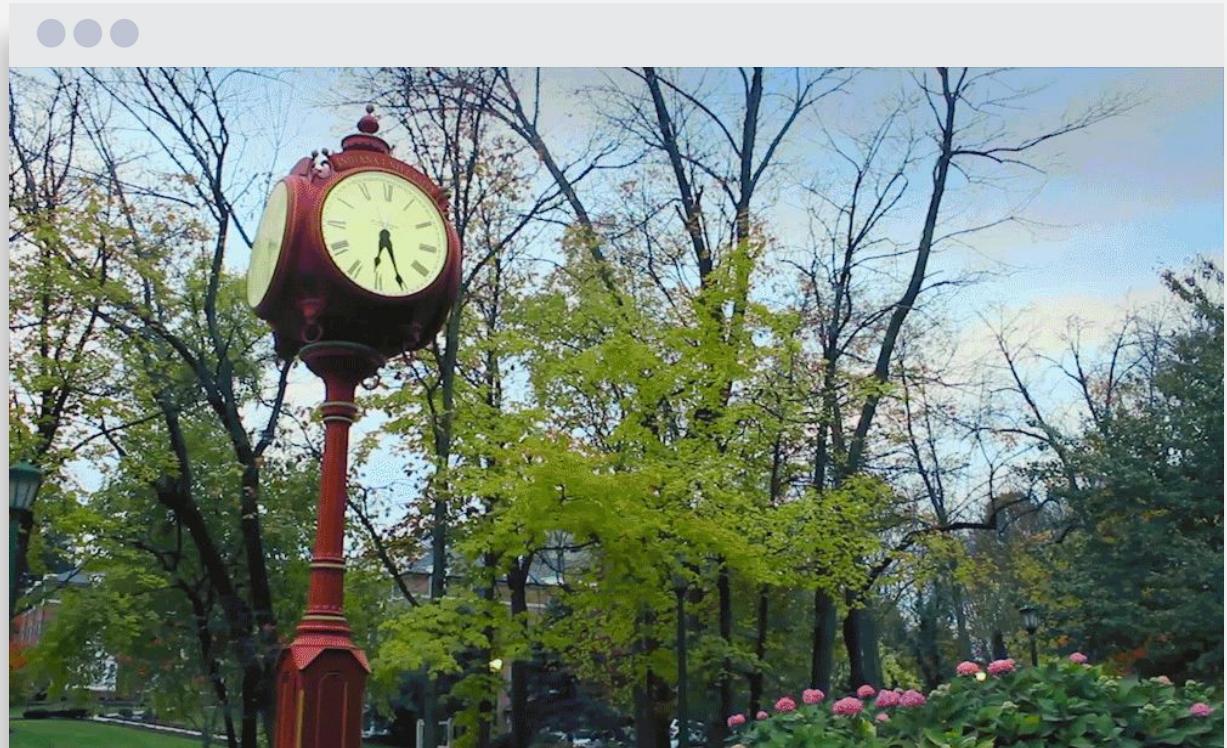


ACTIVISION
BLIZZARD





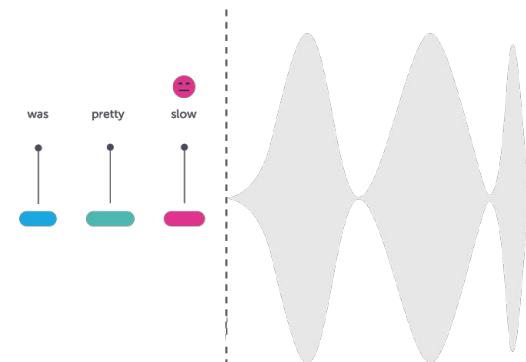
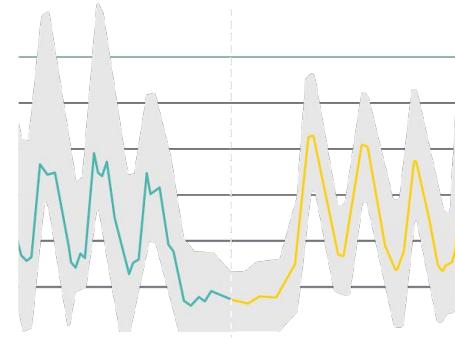
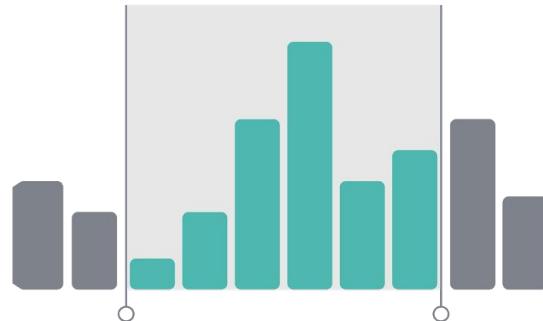
INDIANA UNIVERSITY



Search is a **constant/foundation**



.54 seconds | 1,000,000,000 records



Technology **differentiation**



SCALE

Distributed by design

SPEED

Find matches in milliseconds

RELEVANCE

Get highly relevant results

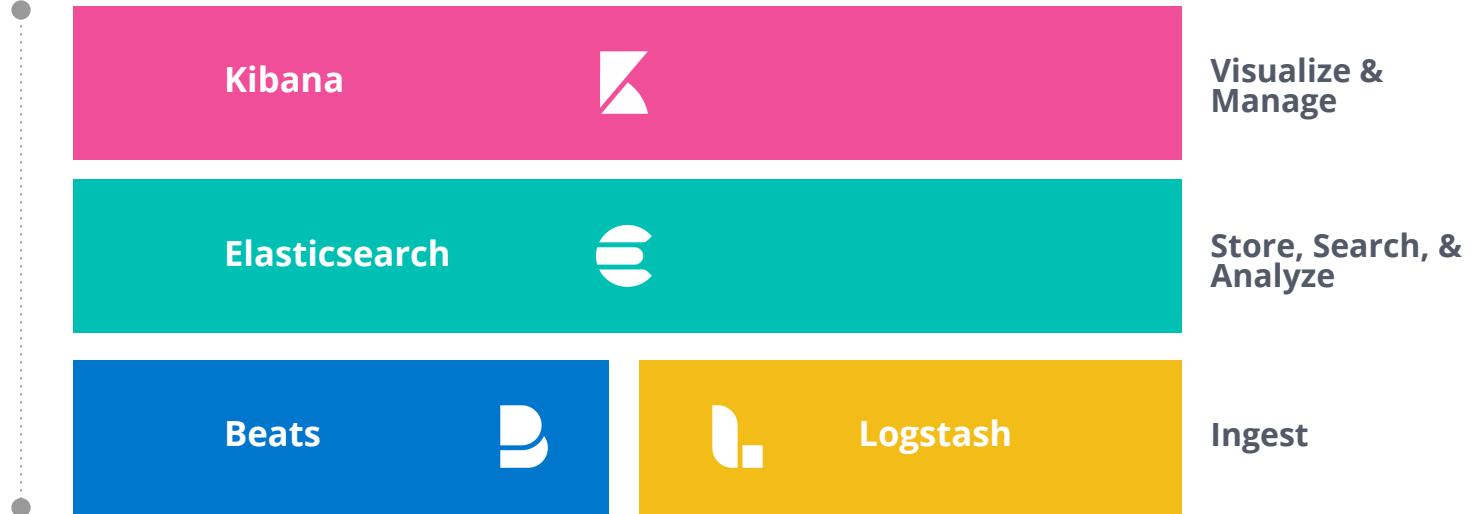
Elastic Products

Elastic Stack

SOLUTIONS



Elastic Stack



SaaS



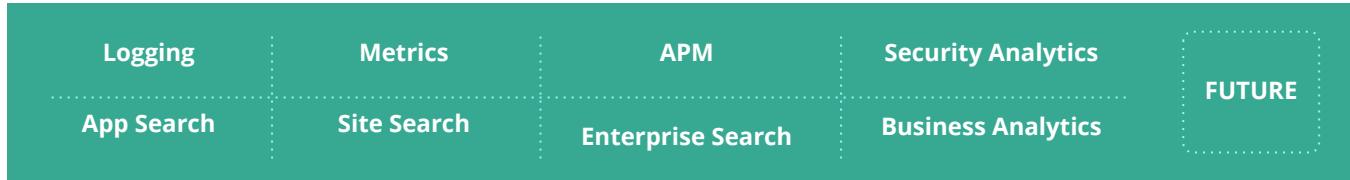
Elastic cloud

On-Prem



Elastic cloud
Enterprise

Solutions



Elastic Stack

Kibana



Visualize & Manage

Elasticsearch



Store, Search, & Analyze

Beats



Logstash



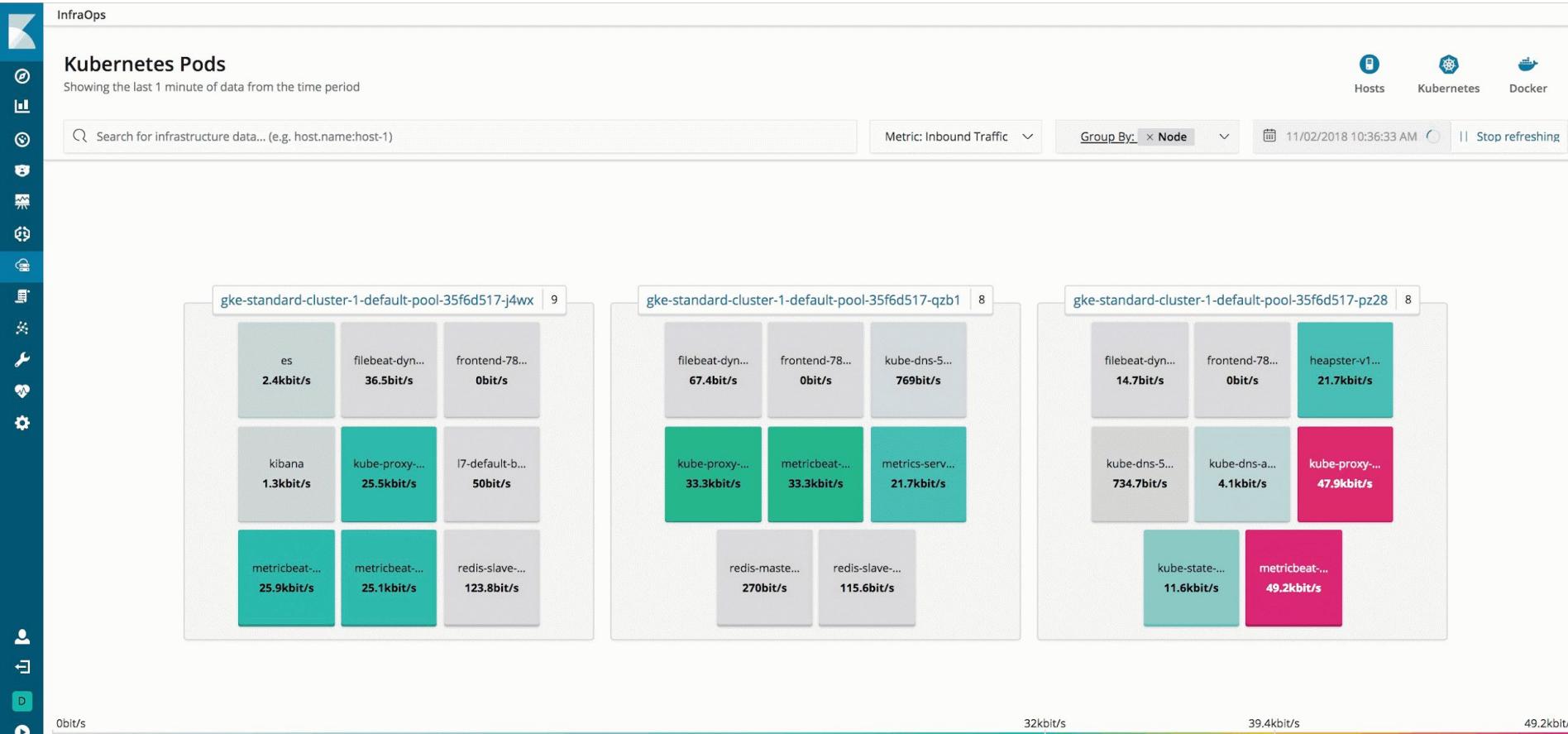
Ingest

SaaS

On-Prem

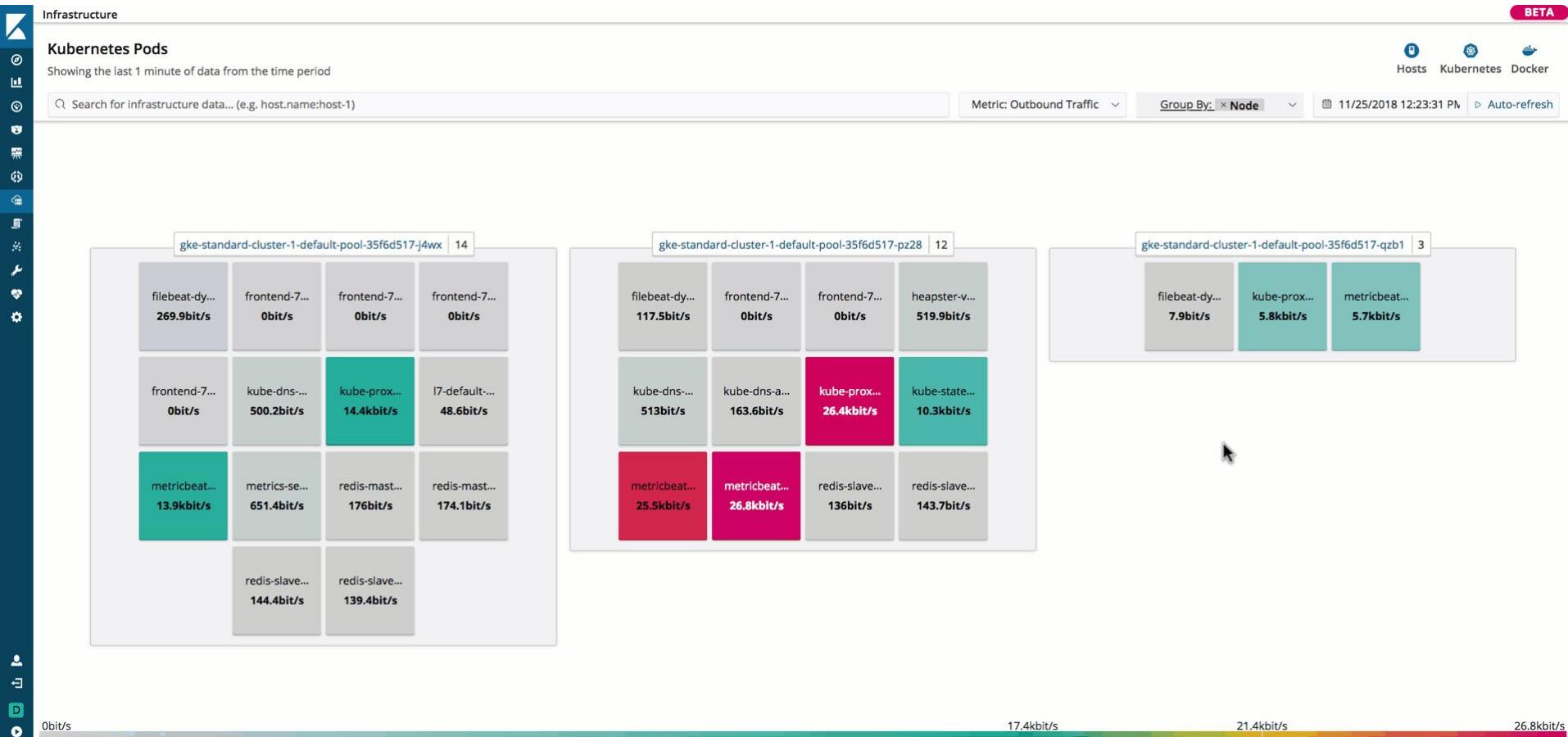
Logging

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

APM / Services

APM feedback Auto-refresh Last 24 hours

Setup Instructions

APM

Search transactions and errors... (E.g. transaction.duration.us > 300000 AND context.response.status_code >= 400)

Services Traces

Name ↑	Agent	Avg. response time	Trans. per minute	Errors per minute
apm-server	go	980 ms	252.5 tpm	0 err.
opbeans-go	go	27 ms	81.2 tpm	0.3 err.
opbeans-java	java	49 ms	157.7 tpm	14.6 err.
opbeans-node	nodejs	25 ms	158.5 tpm	9.9 err.
opbeans-python	python	453 ms	146.4 tpm	11.8 err.
opbeans-ruby	ruby	19 ms	104.0 tpm	11.5 err.

Security Analytics

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

[Network Overview](#) | [Network Suspicious Activity](#) | [Endpoint Overview](#) | [Endpoint OS Activity](#) | [Microsoft DNS Overview](#)

DNS Metrics Overview

DNS - Event Throughput [A...]

963,899
Event Count

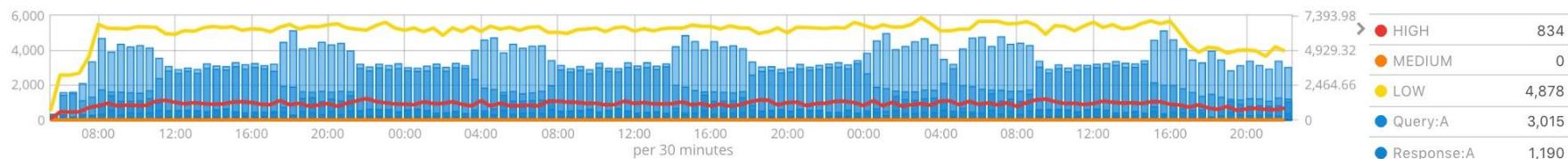
26
Threads

6
OpCodes

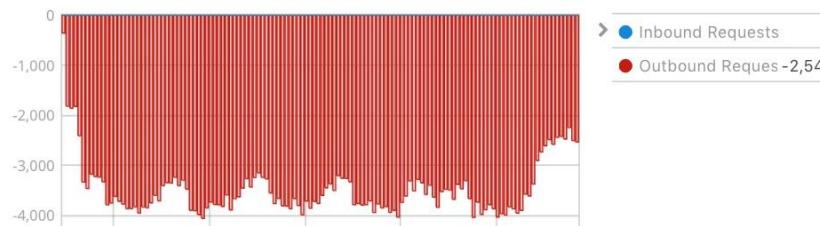
26
Activity Types



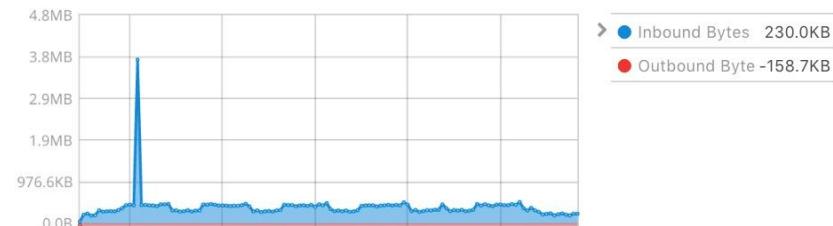
Events Types by Severity



Events by Direction



Events by Size



Deployment **options**

SOLUTIONS



Elastic Stack



Kibana



Visualize & Manage

Elasticsearch



Store, Search, & Analyze

Beats



Logstash



Ingest

SaaS



Elastic Cloud

On-Prem



Elastic Cloud Enterprise

Elasticsearch Service

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



Deployments

Custom plugins

Account

Help

Create deployment

1 Name your deployment

Give your deployment a name

2 Select a cloud platform

Pick your cloud and let us handle the rest. No additional accounts required.



Amazon Web Services



[Google Cloud Platform](#)

3 Select a region

US Central 1 (Iowa)

US West 1 (Oregon)

[Europe West 1 \(Belgium\)](#)

Europe West 3 (Frankfurt)

Elastic Cloud Enterprise

Packaging years of SaaS experience into a product

[Deployments](#)

Platform

Activity Feed

Deployments

Filter by deployment name or id . [More filters](#) [Create deployment](#)

Showing all 8 matching deployments

admin-console-elasticsearch

e68992 v5.6.11

data.default
4 GB RAM, 1 node,
1 zone



app-prod-logging

2dc22b v6.4.0

data.default 4 GB RAM, 1 node, 1 zone	data.highstorage 4 GB RAM, 1 node, 1 zone
Kibana Included	



logging-and-metrics

7b14db v5.6.11

data.default 1 GB RAM, 1 node, 1 zone	Kibana Included
--	---------------------------



rad-app-logging

999d16 v6.4.0



security-threat-hunting

f4fb8b v6.4.0



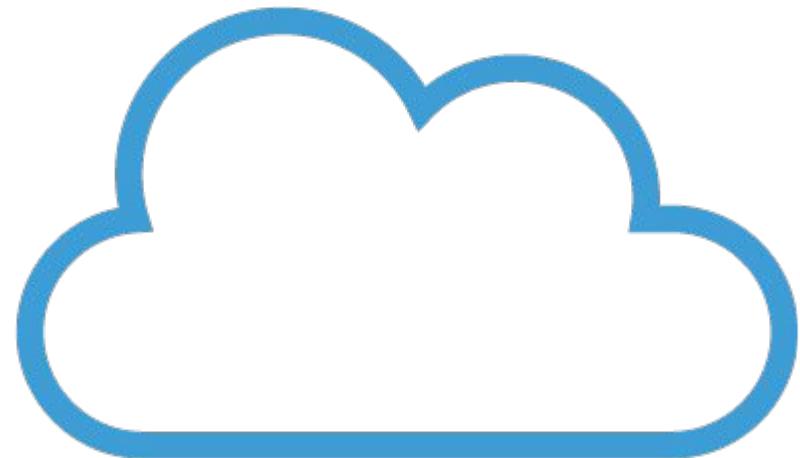
server-telemetry

1d3972 v6.4.0



Lab: Section 1

Build an Elastic Cluster





Create deployment



cloud.elastic.co

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:dXMtZWFzdC0xLmF3cy5mb3VuZC5pbvRhNjY2NGFhNDJiODU0NW
Y2YjE4ZDE40DNlZGEwNzE30SQ2M2Y5YzI1YTljMWQ0YTNkYmZmN2M2YTBh0
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

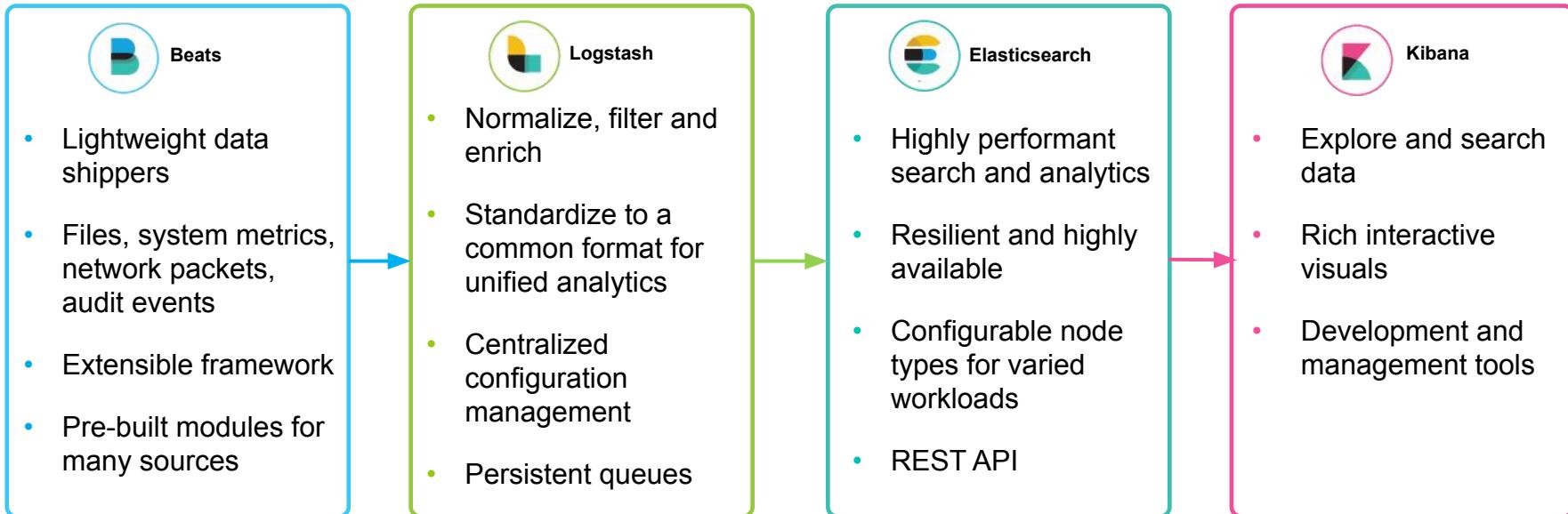
What use-case was Elasticsearch originally created for?

recipe search

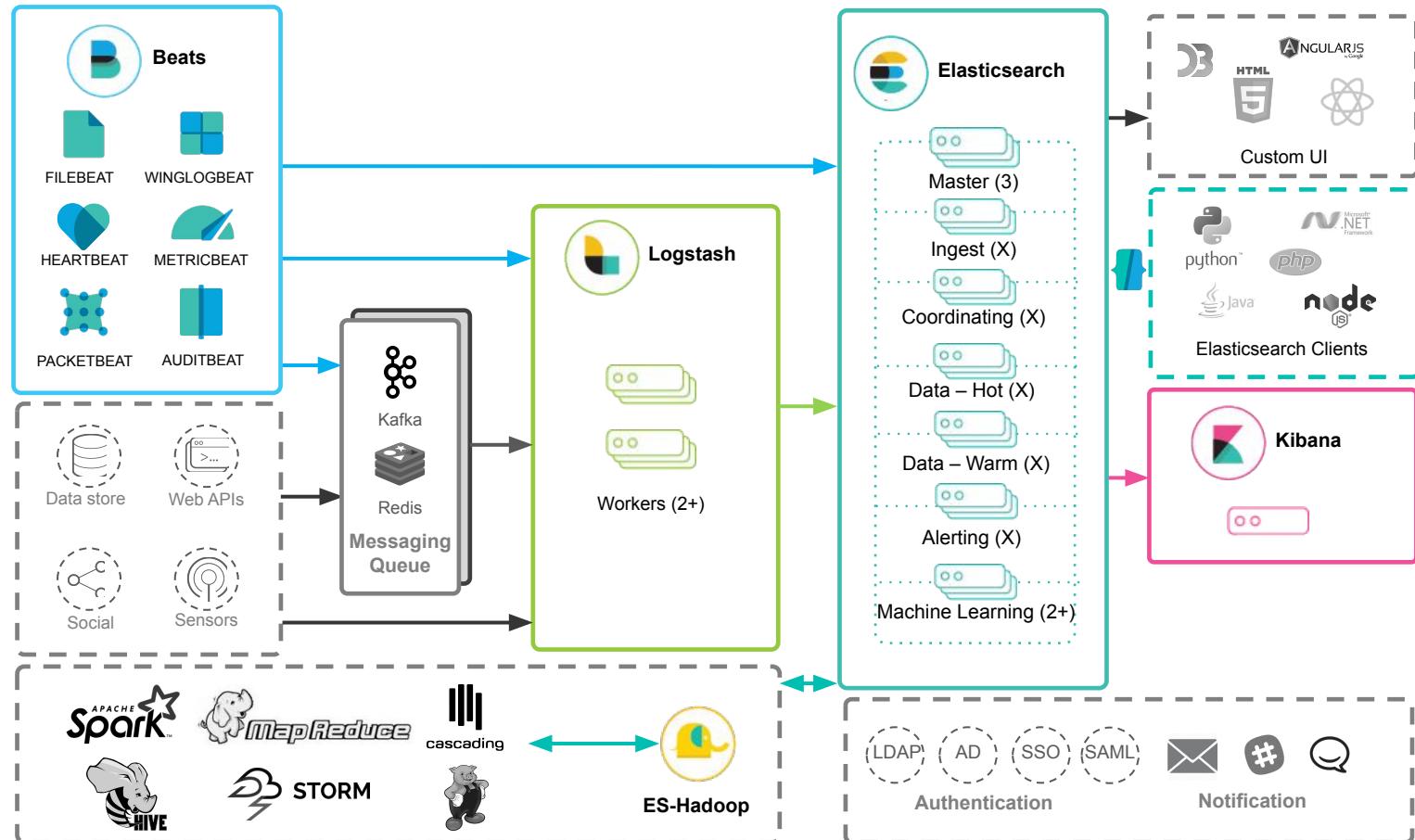
Ingest

Acquiring, enriching & transforming data

Logical Processing Pipeline



Deployment in the Enterprise



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



Ingest Integrations



The Elastic Stack



Beats

Lightweight data shippers

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



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

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

Device Metrics Overview [ArcSight]

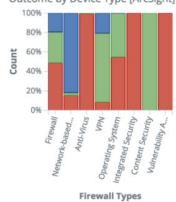
Event Count **330,453**, Devices **57**, Sources **254**, Destinations **425**, Ports **88**



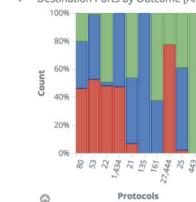
Events by Source [ArcSight]



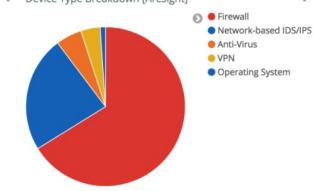
Outcome by Device Type [ArcSight]



Destination Ports by Outcome [ArcSight]



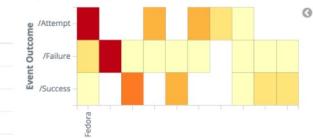
Device Type Breakdown [ArcSight]



Top 10 Devices by Bandwidth [ArcSight]

Device	Source(s)	Destination(s)	Destination Ports	Bandwidth (Incoming)	Bandwidth (Outgoing)
Fedora	54	50	17	48,543,771	775,106,603
	1	96	1	1,827,840	1,763,328
	3	5	3	275,800	264,950
	1	0	1	775	456
	1	1	1	128	128

Top 10 Devices by Outcome [ArcSight]



Beats Modules

Simplify collecting, parsing, and visualizing common log formats

System

Apache

Kafka

Couchbase

Redis

HAProxy

Elasticsearch

Windows

NGINX

Zoo
keeper

CEPH

Docker

Golang

Postgres

Dropwizard

Aerospike

Prometheus

MySQL

Memcache

Jolokia

PHP-FPM

Kibana

HTTP

Auditd



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



apm-high-load-opbeans

Send an alert when a specific condition is met. This will run every 10 seconds.

Name

apm-high-load-opbeans

Indices to query

apm-*-transaction-* X

Use * to broaden your search query

Matching the following condition

WHEN count() GROUPED OVER top 10 'context.service.name' IS ABOVE 20 FOR THE LAST 70

context.service.name (1 of 4): opbeans-node



Alert Users to Conditions

Host Behavior

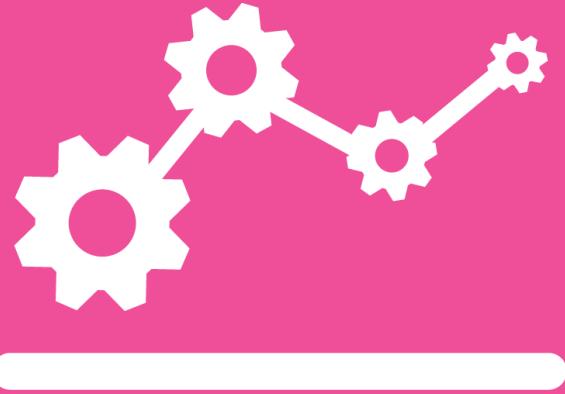
- Free disk space goes below 5%
- Process X starts on any server

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

The screenshot shows the Kibana interface for creating a new threshold alert. On the left, there is a vertical sidebar with various icons: a square, a person, a gear, a chart, a clock, a gear, a wrench, a heart, and a gear.

Create a new threshold alert
Send out an alert when specific conditions are met. This will run once every 1 minute.

Name: CPU Utilization

Select an Index: metricbeat-*
Broad searches can be done by adding * to your query

Select a time field: @timestamp

Run this watch every: 1 minutes

Matching the following condition:

```
WHEN average() OF system.cpu.user.pct OVER all documents IS ABOVE 100 FOR THE LAST 5 minutes
```

Your index and condition combo did not return any data.

Action Options:

- E-mail: Disabled. Configure elasticsearch.yml.
- Logging: Add a new item to the logs.
- Slack: Send a message to a slack user or channel.

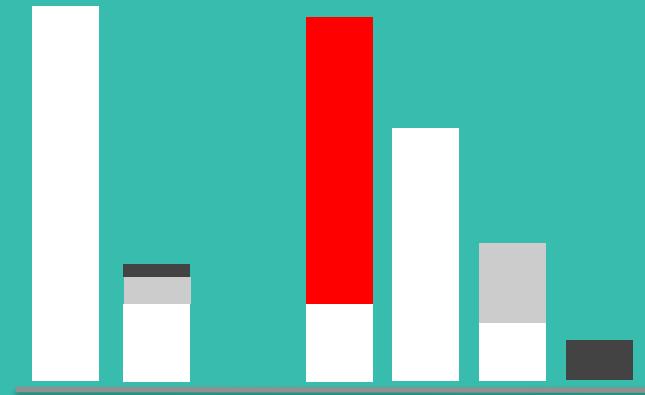
Will perform 0 actions once met

Add new action

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?



Lab: Section 5

Alerting

Trivia

What is the default Kibana port?

5601

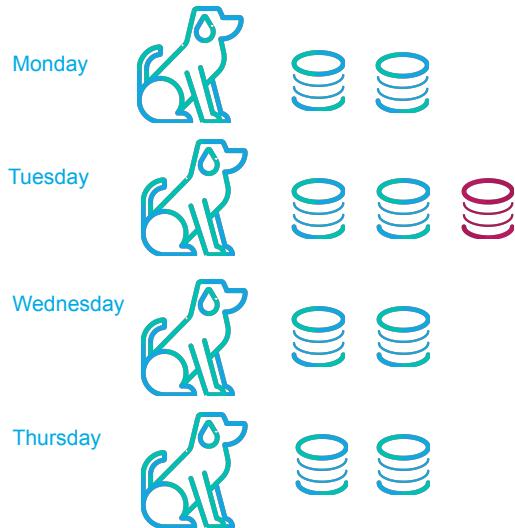
Logs

Machine Learning

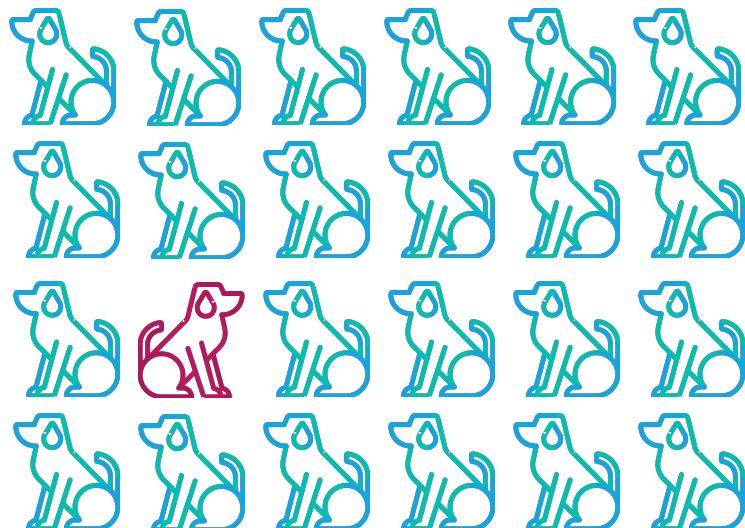
Finding potential problems automatically

What is Normal?

When something behaves like itself

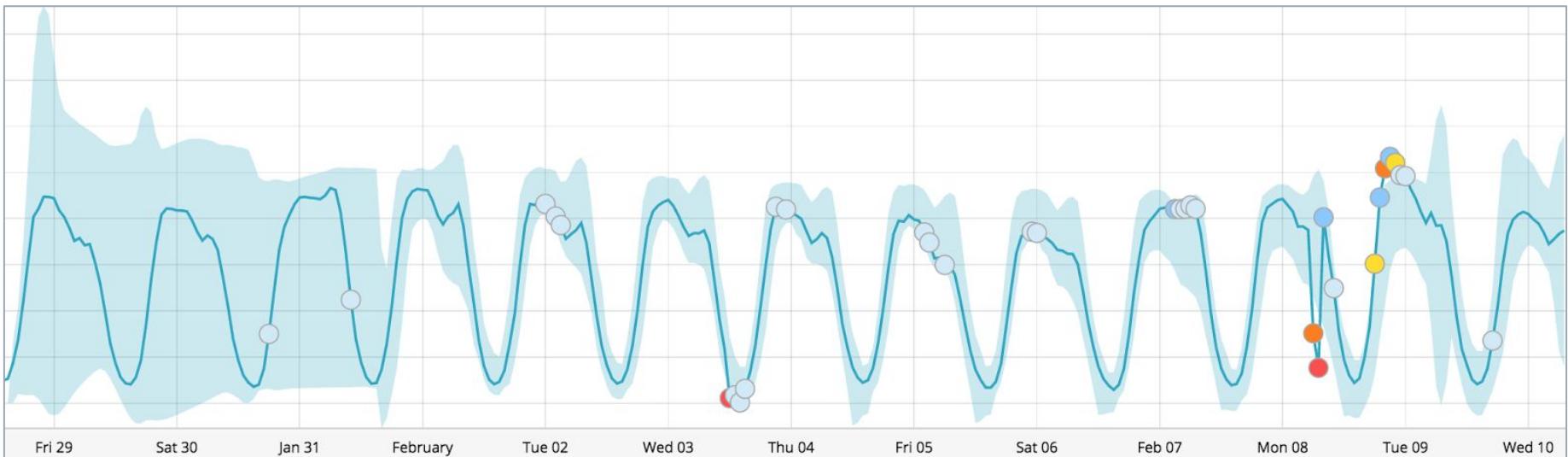


When something behaves like its peers



Learning what is normal for your environment

A model always evolving



When *abnormal* matters

Host Behavior

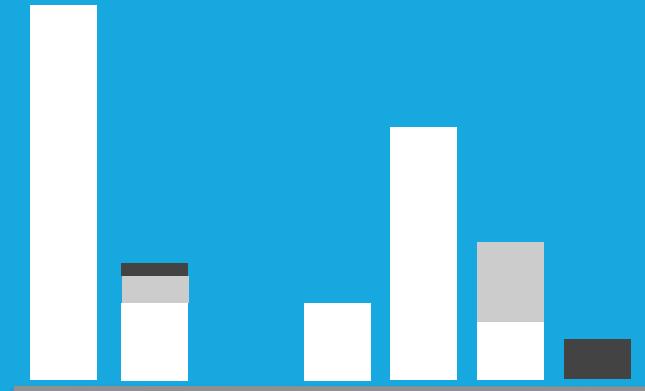
- Free disk space lower than average
- Unusual log entries

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



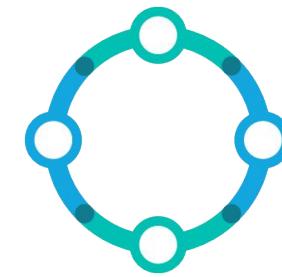
**Understand
Seasonality**



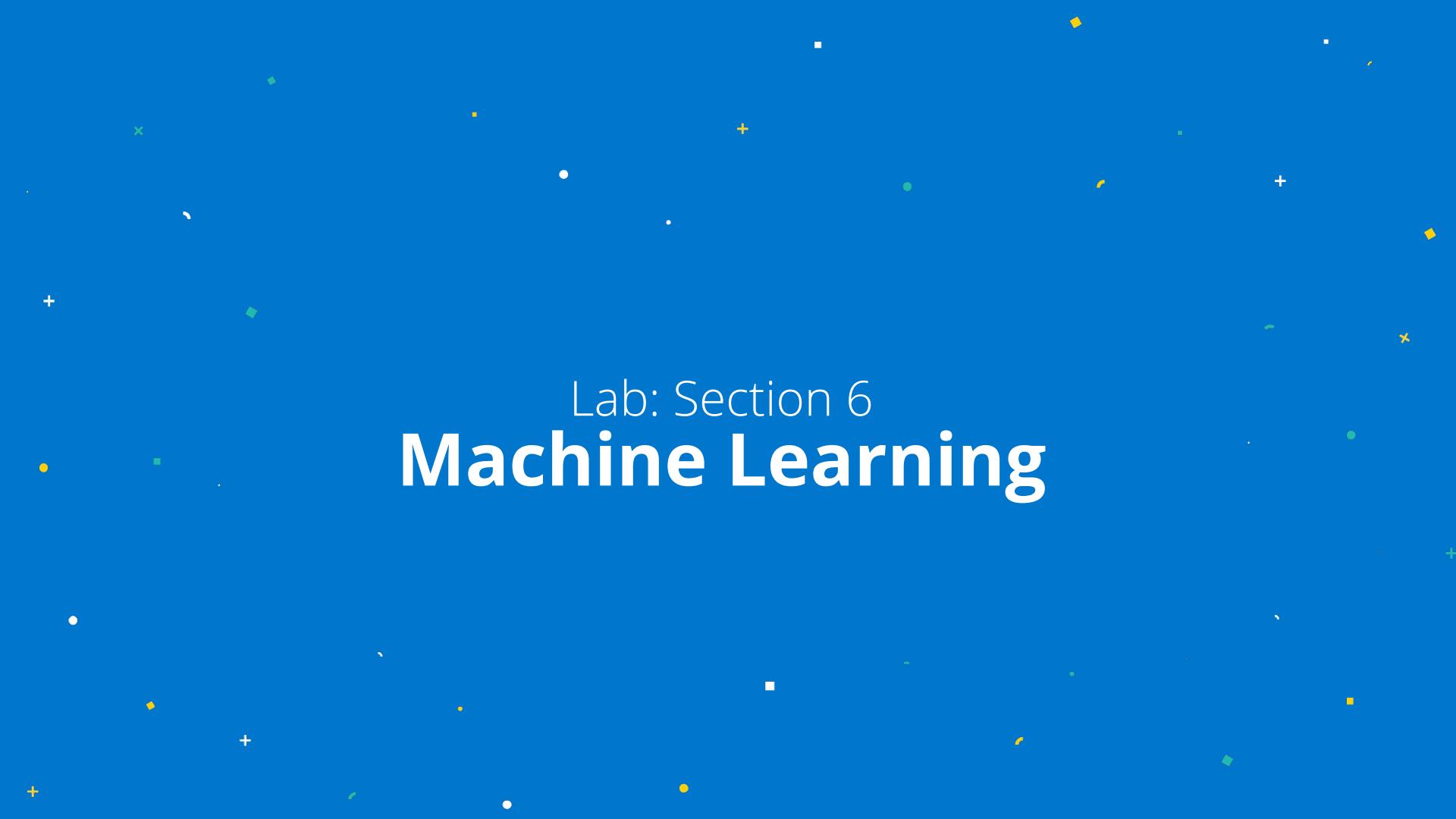
**Reduce False
Positives**



**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

FOUNDATION



SPECIALIZATIONS





THANK YOU