Alan Tech Talk #6

2020-07-15 — David Pilato

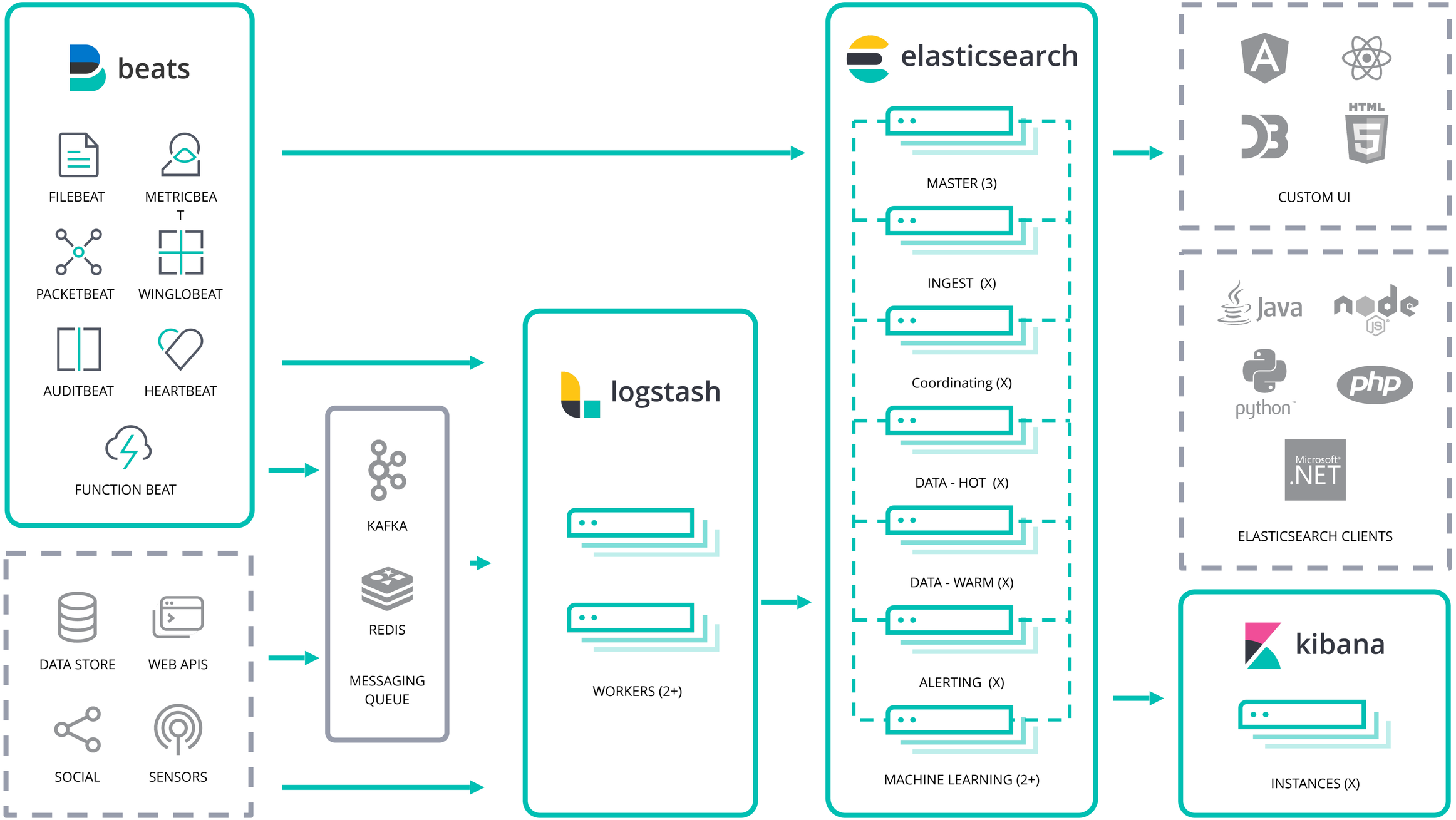
Introduction to Elasticsearch

elastic

Elastic Stack Overview

Search. Observe. Protect.

alan


beats
FILEBEAT
METRICBEAT
PACKETBEAT
WINGLOBEAT
AUDITBEAT
HEARTBEAT
FUNCTION BEAT
DATA STORE
WEB APIS
SOCIAL
SENSORS
KAFKA
REDIS
MESSAGING QUEUE
logstash
WORKERS (2+)
elasticsearch
MASTER (3)
INGEST (X)
Coordinating (X)
DATA - HOT (X)
DATA - WARM (X)
ALERTING (X)
MACHINE LEARNING (2+)
CUSTOM UI
Java
node
python
php
Microsoft .NET
ELASTICSEARCH CLIENTS
kibana
INSTANCES (X)

Deploy anywhere.

Elastic Cloud

Elastic Cloud Enterprise

Elastic Cloud on Kubernetes

SaaS

Orchestration

elastic

FREE

Open source

Apache 2.0 : aujourd'hui comme demain.

Entre autres fonctionnalités :

- Clustering et haute disponibilité
- Recherche et analyse ultra-performantes
- Visualisation des données et tableaux de bord
- Et plus encore

Basic

L'offre gratuite qui le restera toujours.

Tous les avantages de l'open source, plus :

- Les principales fonctionnalités de sécurité de la Suite Elastic
- Des fonctionnalités telles qu'Elastic APM, SIEM, ou encore Maps
- Canvas et Lens
- Et plus encore

Téléchargement gratuit

Gold

Plus de fonctionnalités. Un support technique dédié.

Tous les avantages de l'offre Basic, plus :

- Alerting
- Reporting
- Gestion de l'ingestion
- Support technique aux heures ouvrées
- Et plus encore

Nous contacter

Platinum

Des fonctionnalités avancées. Un support technique 24 h/24.

Tous les avantages de l'offre Gold, plus :

- Des fonctionnalités de sécurité avancées de la Suite Elastic
- Machine Learning
- Réplication inter-clusters
- Support technique 24 h/24, 7 j/7, 365 j par an
- Et plus encore

Nous contacter

Enterprise

L'orchestration de la Suite et Endpoint Security par défaut.

Tous les avantages de l'offre Platinum, plus :

- Prévention aux points de terminaison
- Protection et réponse aux points de terminaison mappées vers MITRE ATT&CK
- Collecte d'événements aux points de terminaison
- L'accès aux fonctionnalités d'orchestration d'Elastic Cloud Enterprise (ECE) et d'Elastic Cloud sur Kubernetes (ECK)

Nous contacter

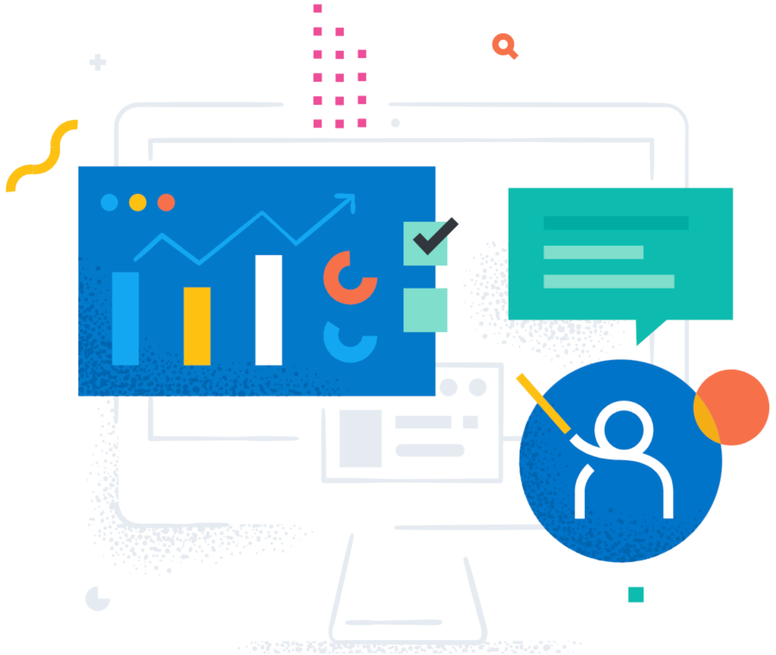
Free Elastic training

Start your Elastic journey and become an expert faster than ever — for free. Build your enterprise search, observability, security, and Elastic Stack skills with our on-demand training.

Fundamentals training

Our self-paced courses include expertly designed materials, engaging demos, hands-on lab exercises, and access to Elastic experts to help you build and retain new skills. And they're all available anywhere you have an internet connection.

- Observability Fundamentals
- Introduction to Observability: Logging
- Metrics Fundamentals
- APM Fundamentals
- Kibana Fundamentals
- Kibana for Splunk Users
- Fundamentals of Securing Elasticsearch
- Elastic SIEM Fundamentals



https://www.elastic.co/training/free

A typical search implementation…

```
CREATE TABLE user
(
   name VARCHAR(100),
   comments VARCHAR(1000)
);
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

elastic

Search on term

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name="David";
Empty set (0,00 sec)
```

David

elastic

Search like

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%";
+---------------+-----------------------+
| name          | comments              |
+---------------+-----------------------+
| David Pilato  | Developer at elastic  |
| David Gageot  | Engineer at Google    |
| David David   | Who is that guy?      |
+---------------+-----------------------+
```

David

elastic

Search for terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David Pilato%";
+---------------+-----------------------+
| name          | comments              |
+---------------+-----------------------+
| David Pilato | Developer at elastic |
+---------------+-----------------------+
```

David Pilato

elastic

Search with inverted terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%Pilato David%";
Empty set (0,00 sec)
SELECT * FROM user WHERE name LIKE "%Pilato%David%";
Empty set (0,00 sec)
```

Pilato David

elastic

Search for terms

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%" AND
                         name LIKE "%Pilato%";
+---------------+-----------------------+
| name          | comments              |
+---------------+-----------------------+
| David Pilato  | Developer at elastic  |
+---------------+-----------------------+
```

Pilato David

elastic

Search in two fields

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%David%" OR
                         comments LIKE "%David%";
+---------------+-----------------------------------------+
| name          | comments                                |
+---------------+-----------------------------------------+
| David Pilato  | Developer at elastic                    |
| Malloum Laya  | Worked with David at french customs service |
| David Gageot  | Engineer at Google                      |
| David David   | Who is that guy?                        |
+---------------+-----------------------------------------+
```

David

Search with typos

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%Dadid%";
Empty set (0,00 sec)
```

Dadid

elastic

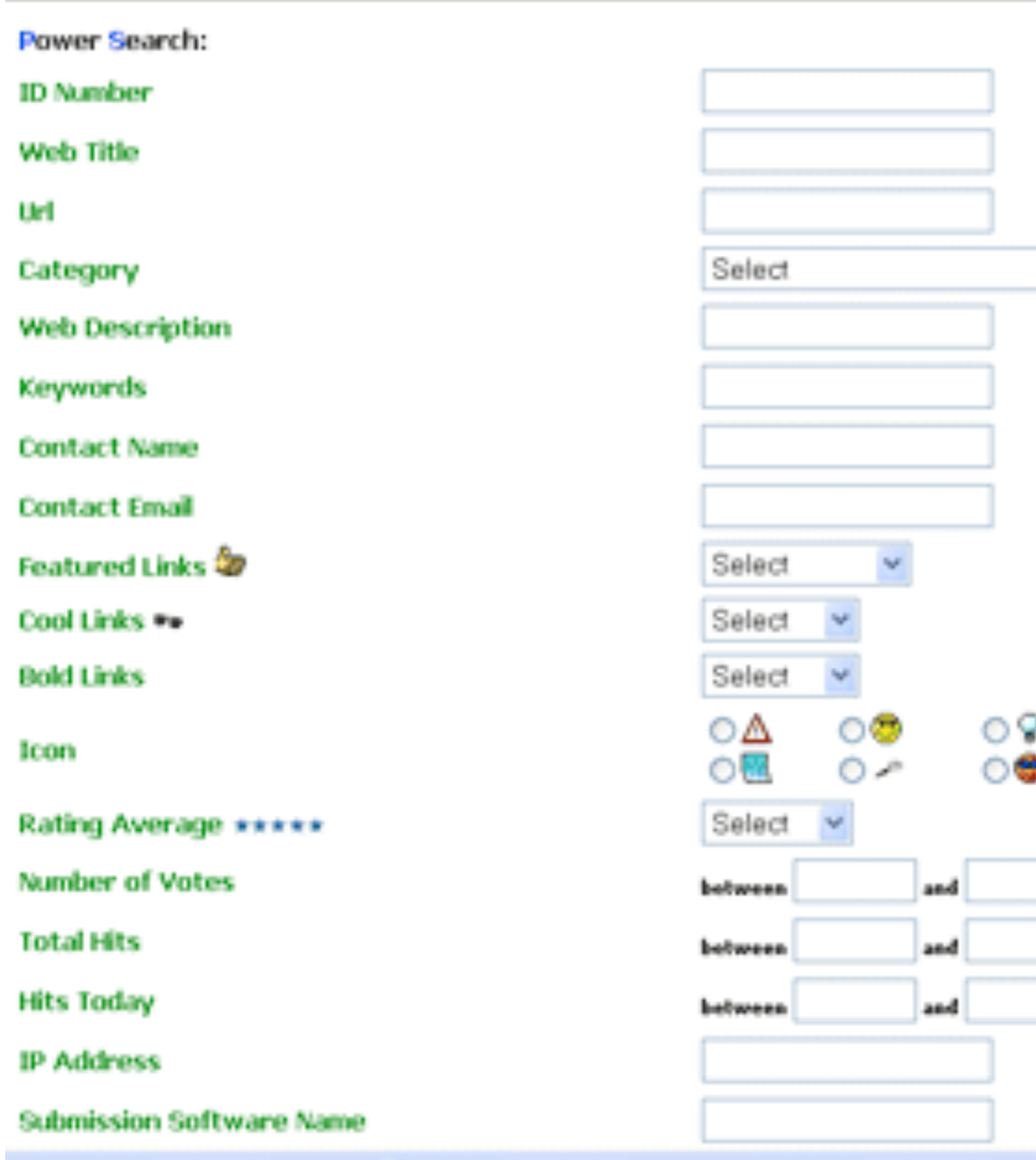
Search with typos

```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Google');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
SELECT * FROM user WHERE name LIKE "%_adid%" OR
                         name LIKE "%D_did%" OR
                         name LIKE "%Da_id%" OR
                         name LIKE "%Dad_d%" OR
                         name LIKE "%Dadi_%";
+---------------+-----------------------+
| name          | comments              |
+---------------+-----------------------+
| David Pilato  | Developer at elastic  |
| David Gageot  | Engineer at Google    |
| David David   | Who is that guy?      |
+---------------+-----------------------+
```

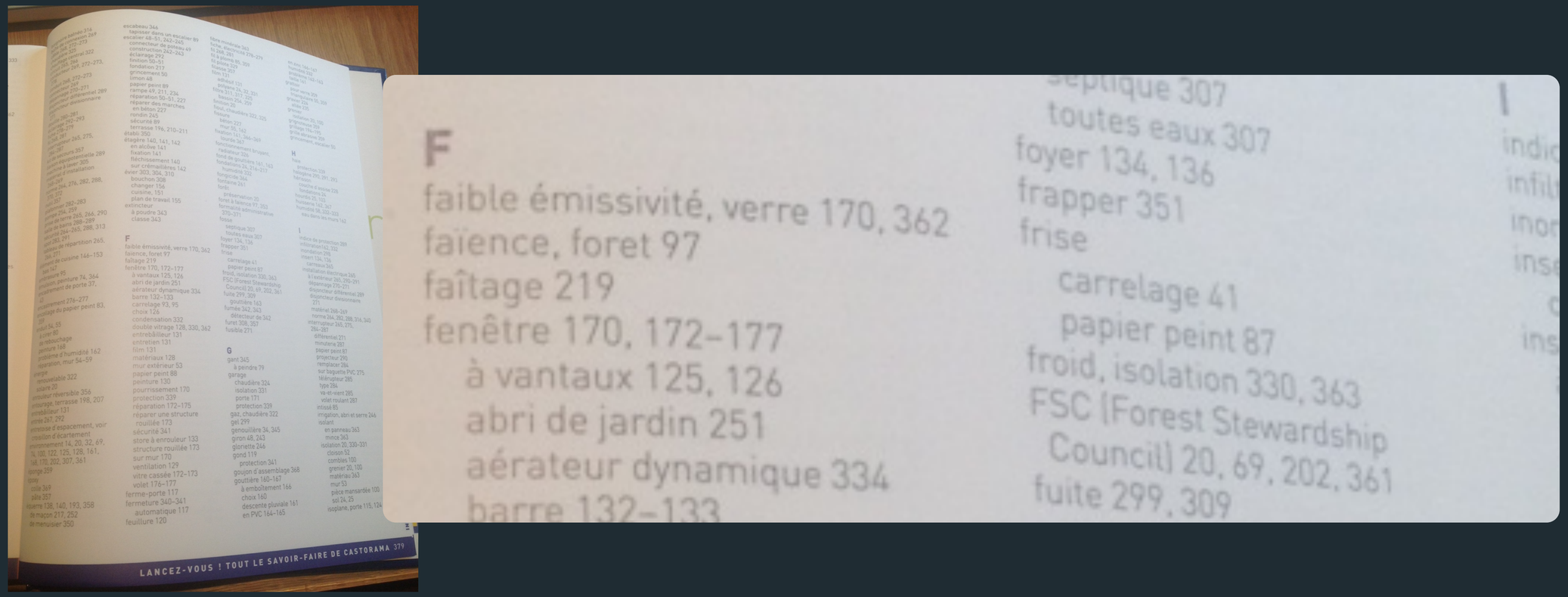
elastic

User Interface



Search engine?

Moteur d'**indexation de documents**



Moteur de **recherche dans les index**

elastic

Demo time!

3 solutions powered by 1 stack

Elastic Enterprise Search

Elastic Observability

Elastic Security

Elastic Stack

elastic

Elastic Enterprise Search

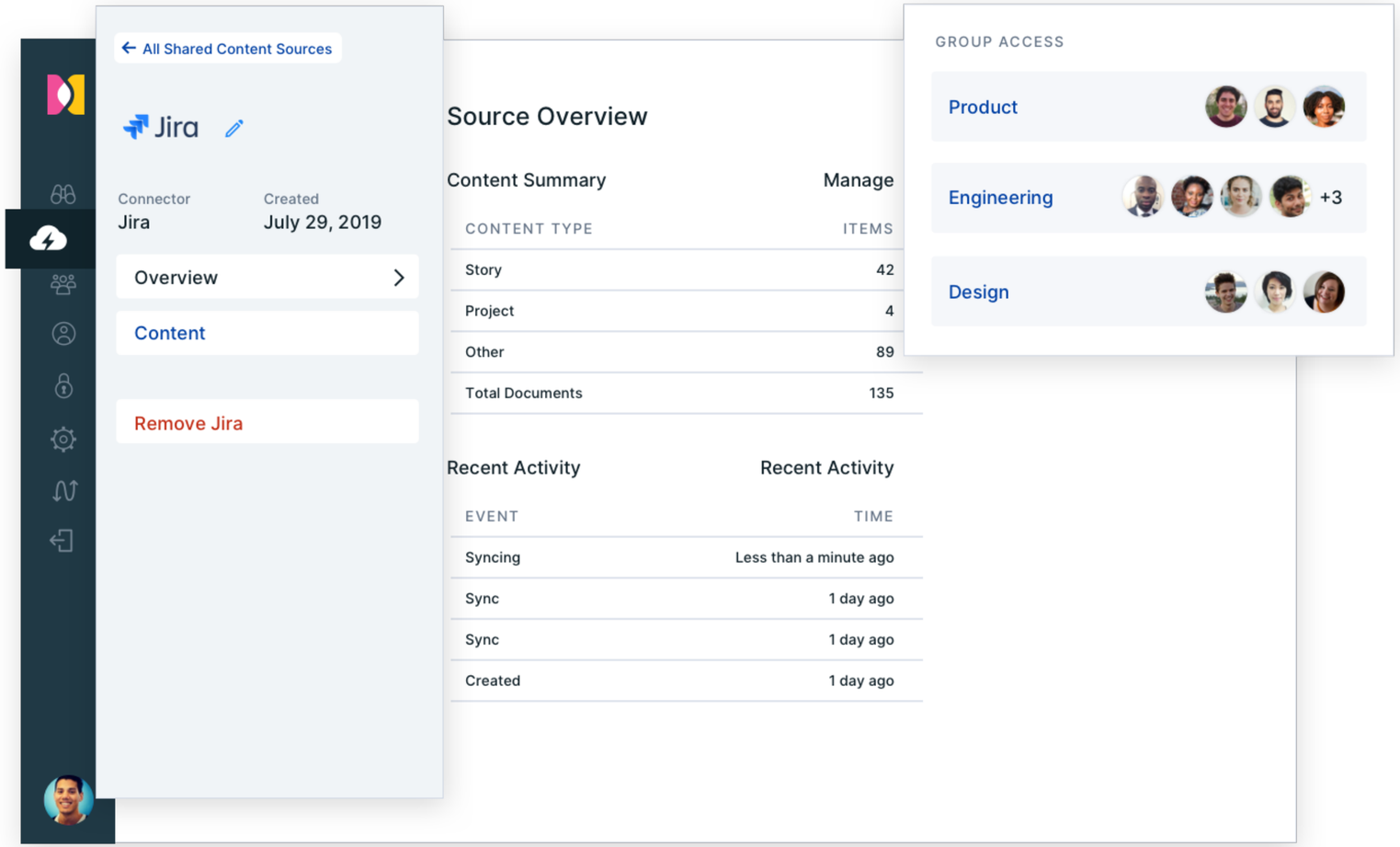
Workplace Search App Search Site Search

elastic

ELASTIC ENTERPRISE SEARCH

Search everything, anywhere

Easily implement powerful, modern search experiences across your website, app, or digital workplace. Search it all, simply.



elastic

Elastic Observability

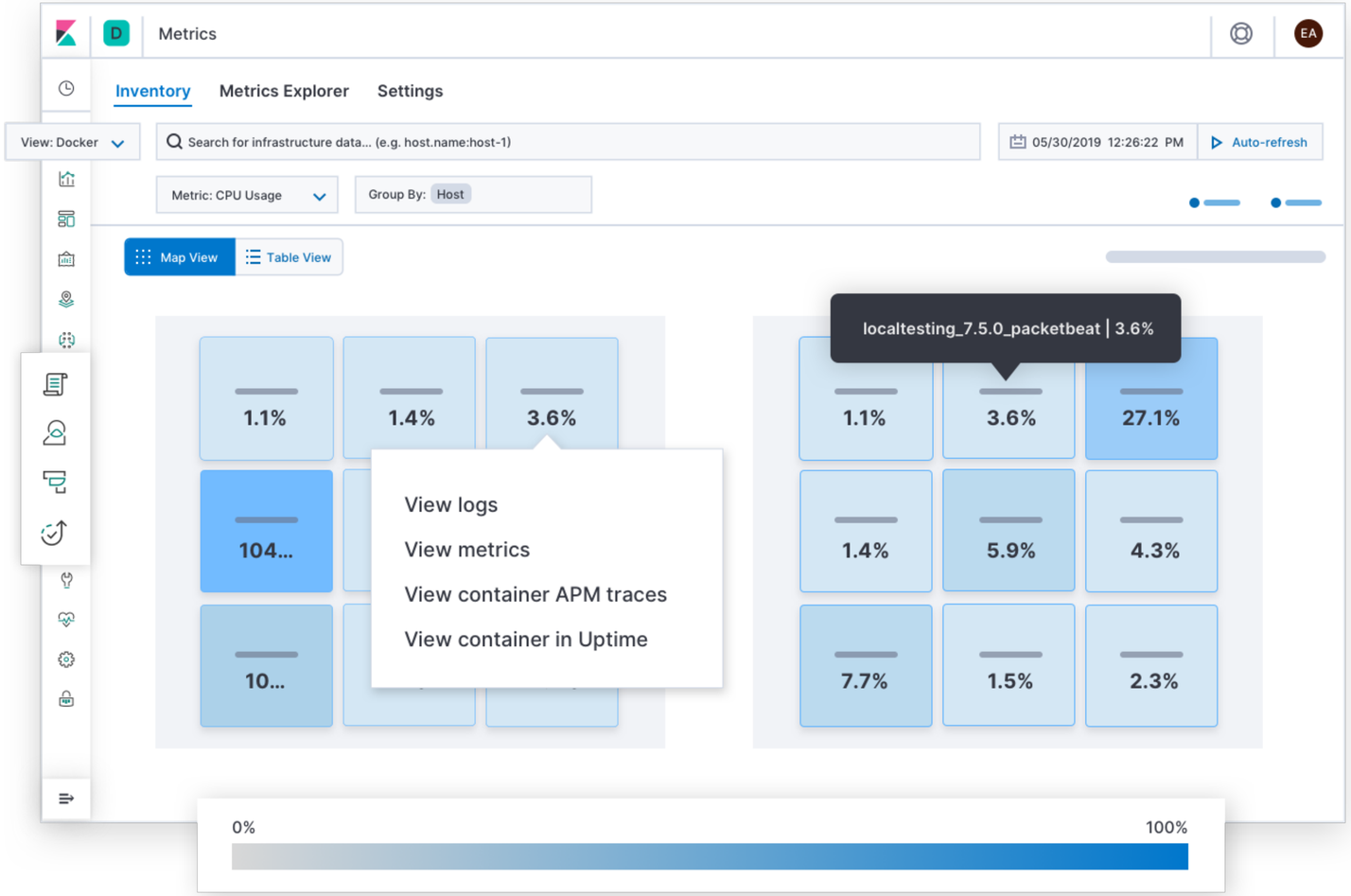
Logs Metrics APM Uptime

elastic

ELASTIC OBSERVABILITY

Unified visibility across your entire ecosystem

Bring your logs, metrics, and traces together into a single stack so you can monitor, detect, and react to events with speed.



elastic

Elastic Security

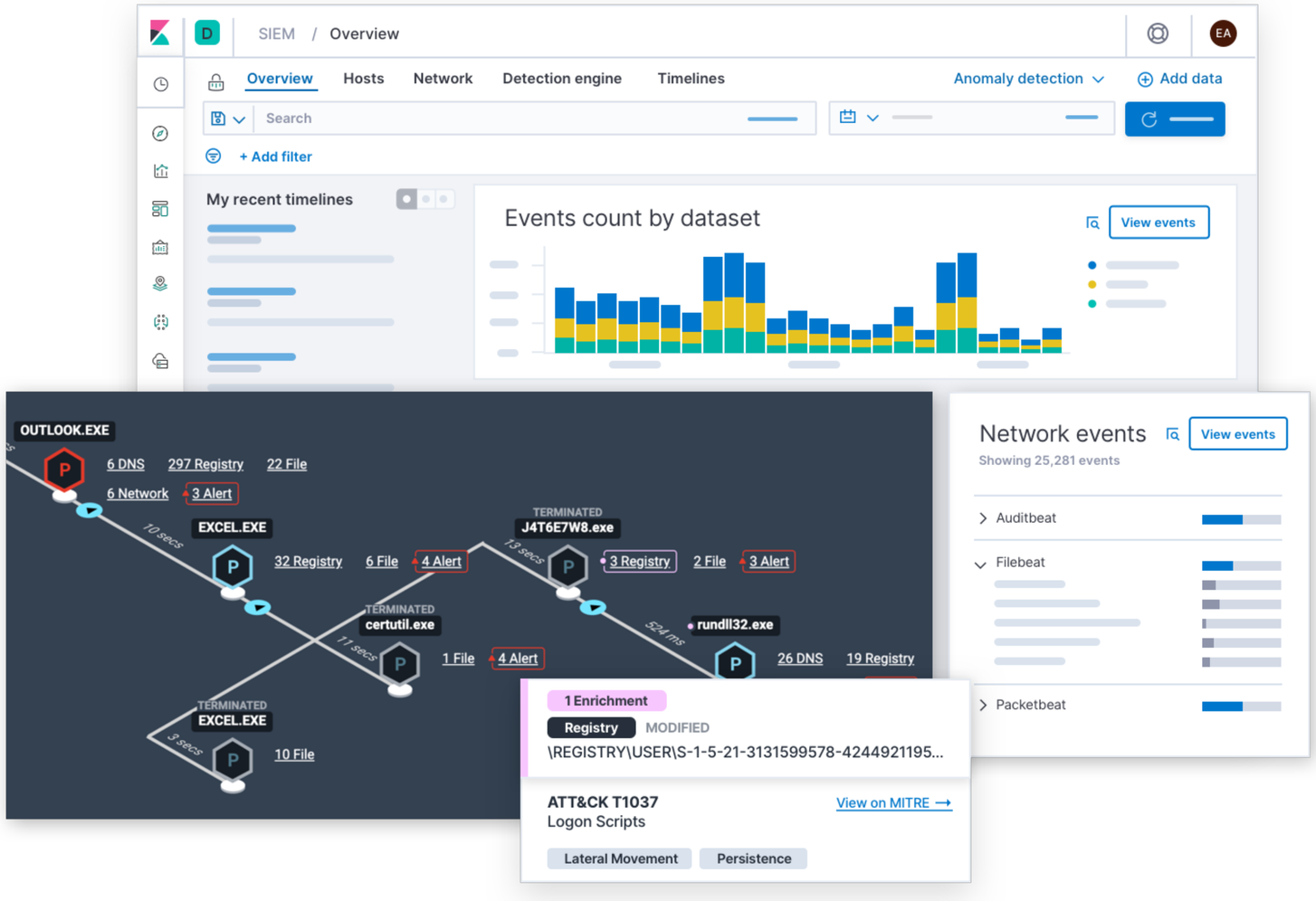
Endpoint SIEM

elastic

ELASTIC SECURITY

Security how it should be: open

Elastic Security integrates endpoint security and SIEM to give you prevention, collection, detection, and response capabilities for unified protection across your infrastructure.



elastic

Deploy anywhere.

Elastic Cloud

Elastic Cloud Enterprise

Elastic Cloud on Kubernetes

SaaS

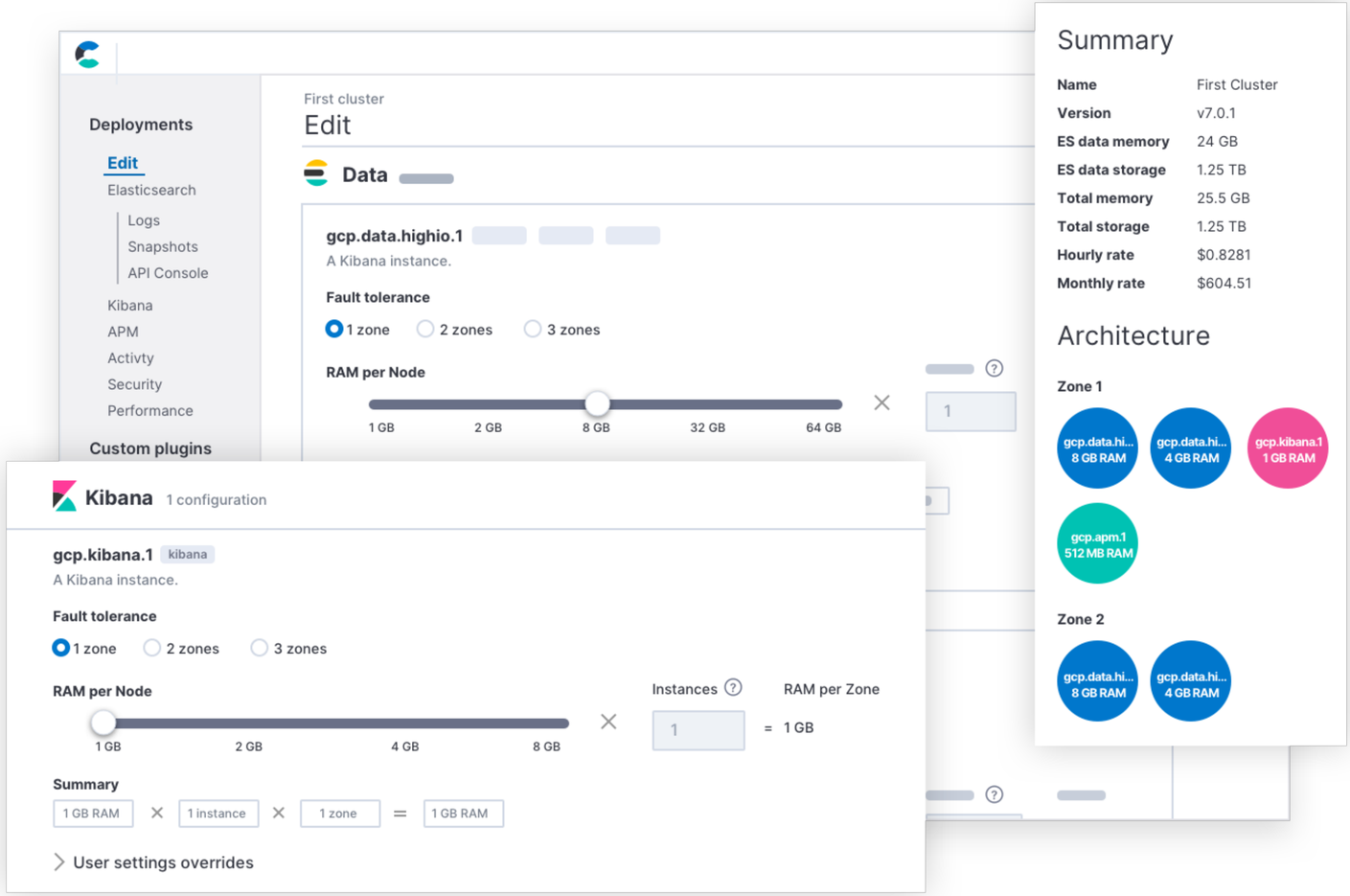
Orchestration

elastic

ELASTIC CLOUD

Family of SaaS Offerings

Easily launch, operate, and scale deployments on AWS, GCP, or Azure with a SaaS experience tailor-made for Elastic products and solutions.

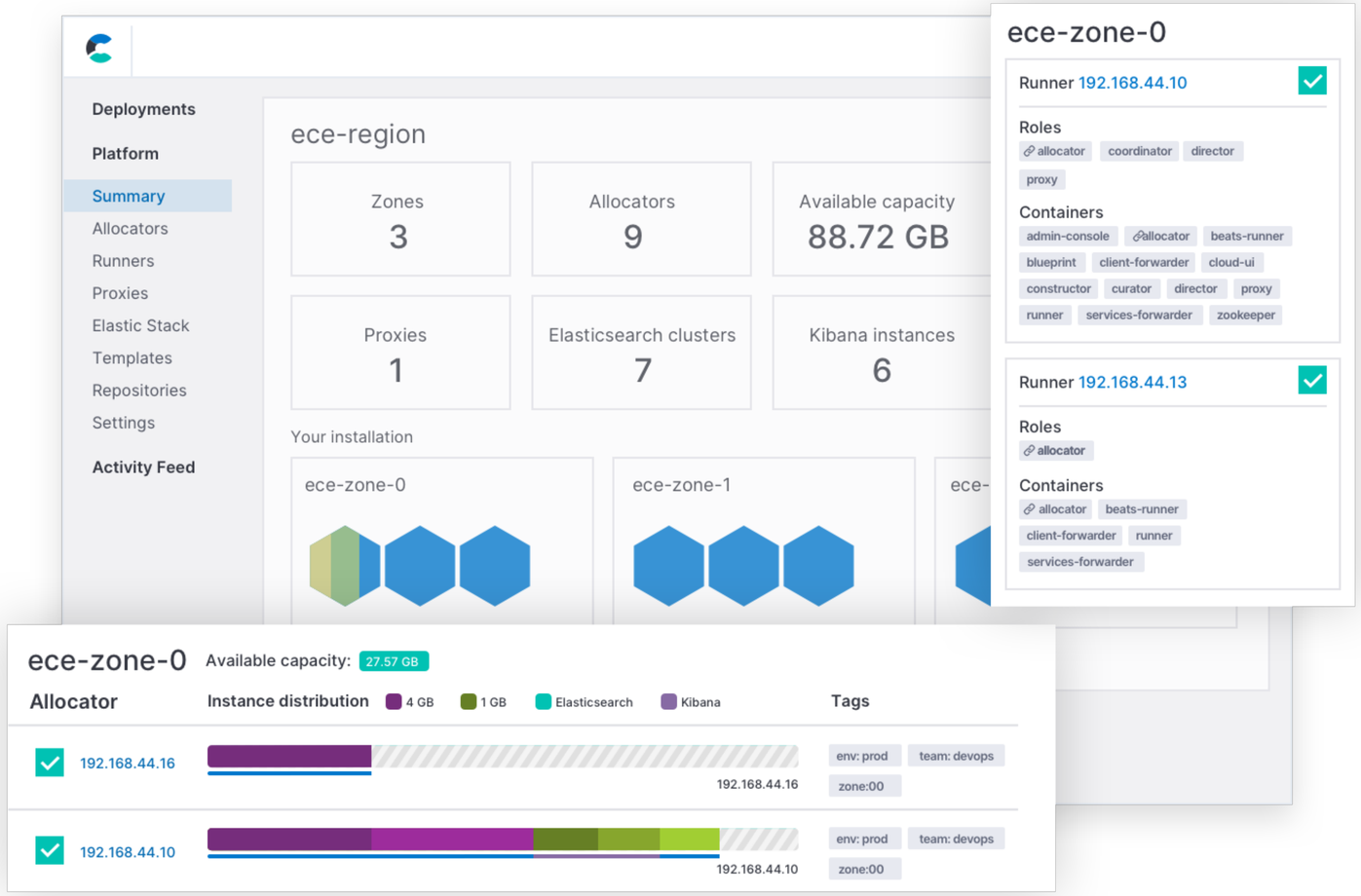


elastic

ELASTIC CLOUD ENTERPRISE

Centrally manage your Elastic deployments

Provision, manage, and monitor Elastic products and solutions, at any scale, on any infrastructure, while managing everything from a single console.

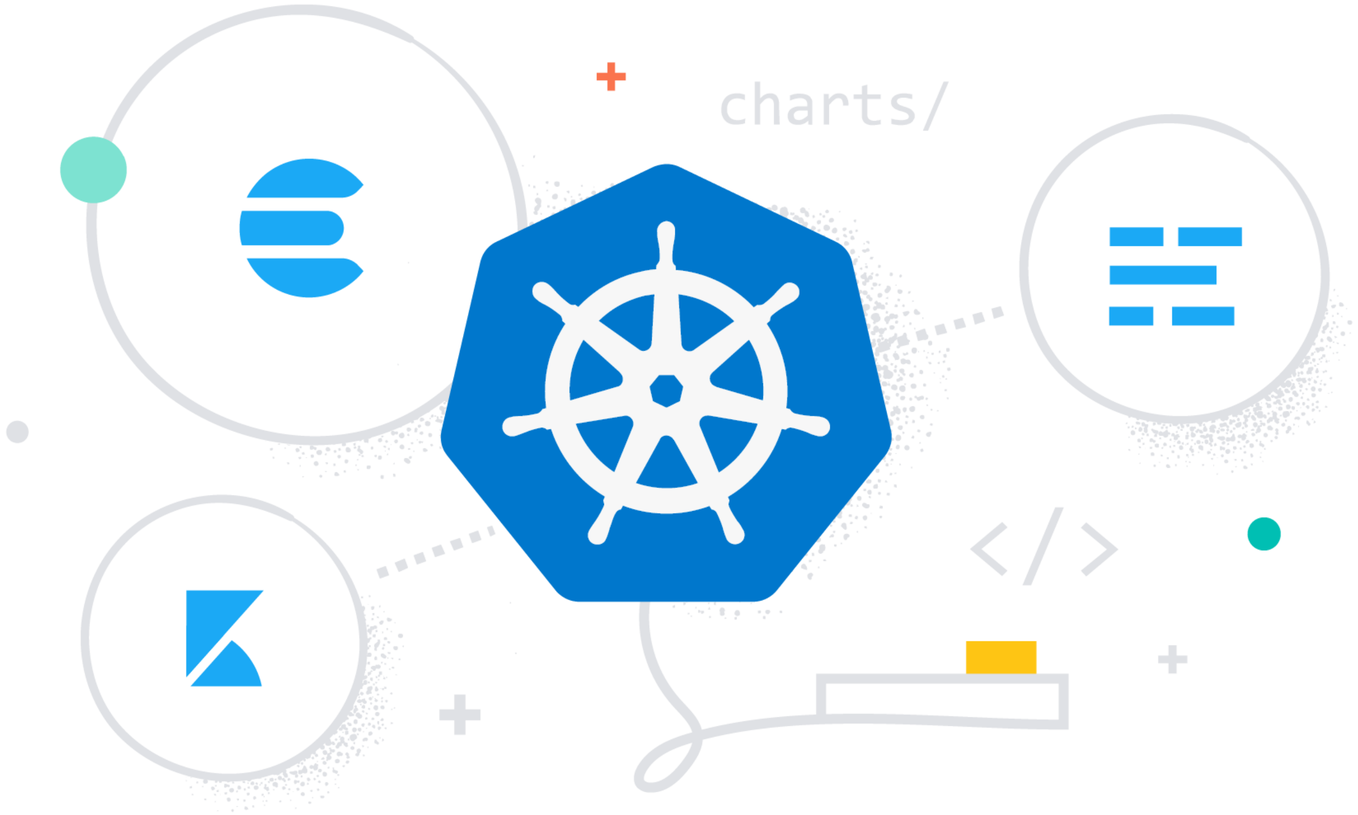


elastic

ELASTIC CLOUD ON KUBERNETES

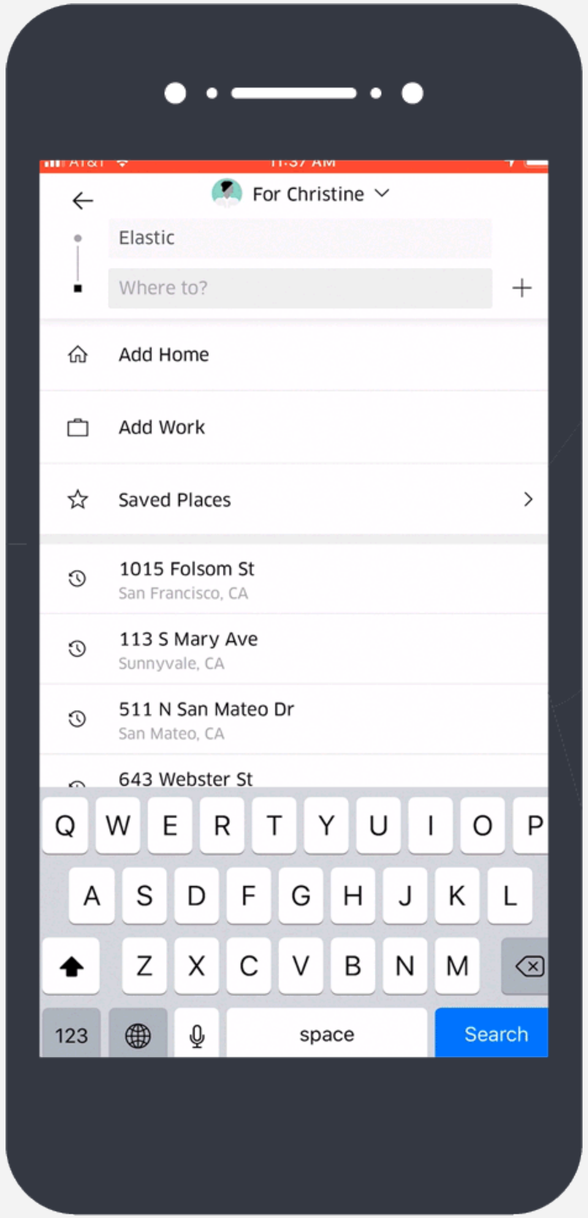
Official Operator, and much more

Simplify setup, upgrades, snapshots, scaling, high availability, security, and more when running Elastic products and solutions on Kubernetes.



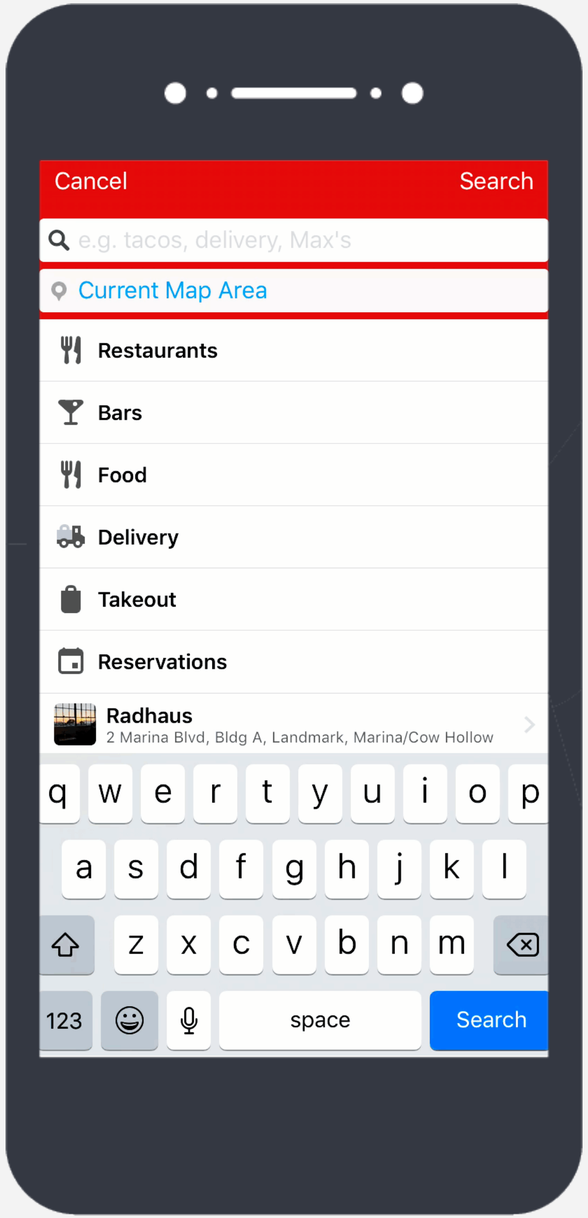
elastic

HSBC
SOUNDCLOUD
mozilla FOUNDATION
Microsoft
GROUPON
facebook
Expedia
vimeo
salesforce
FOURSQUARE
ACTIVISION BLIZZARD
stackoverflow
NASA
Symantec
DELL
The New York Times
Unilever
ebay
Eventbrite
Alcatel·Lucent
CONCUR
verizon
NETFLIX
IBM
PayPal
Adobe
CISCO
docker
The Guardian
THOMSON REUTERS
Quora
TOMTOM



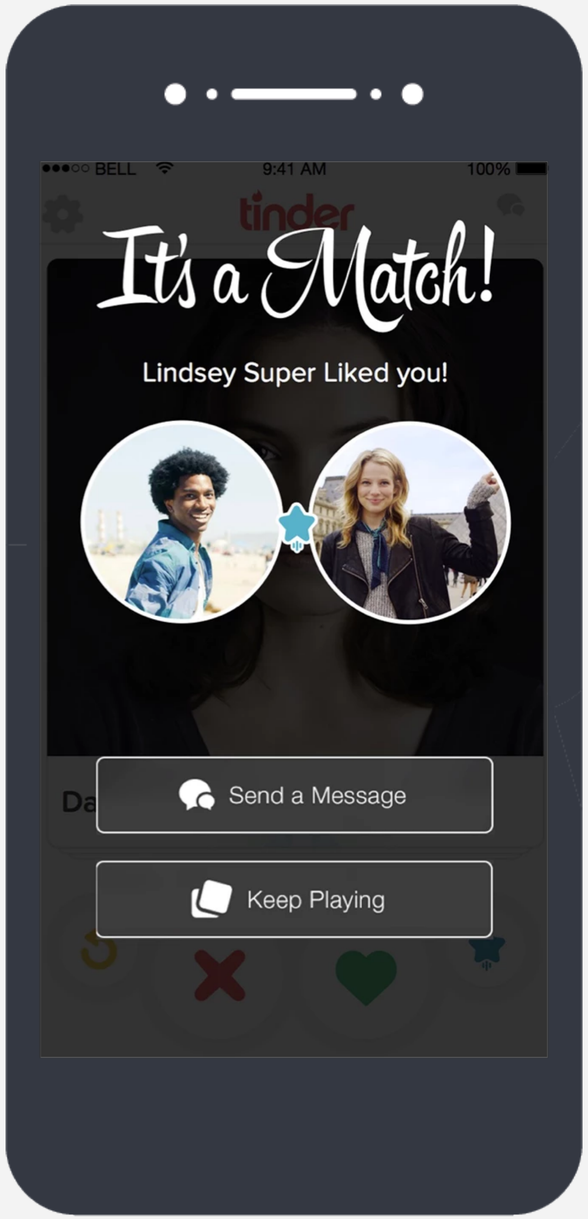
Searching for **Rides**

elastic



Searching for **Restaurants**

elastic



Searching for **Love**

elastic

keljob
BlaBlaCar
SwissLife
PSA PEUGEOT CITROËN
LesFurets.com
Comparez et achetez futé
francetvinfo
radio france
LEROY MERLIN
Crédit Mutuel ARKEA
DHL
Les Anges de la Télé Réalité
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
1805 PICTET
REGIONSJOB
saur
MACSF
fotolia by Adobe
orange™
meetic
SOCIETE GENERALE
FIGARO immo
OVH.com
SeLoger.com
BANQUE DE FRANCE
EUROSYSTÈME
Carrefour
CADREMPLOI
Alcatel·Lucent
118 218
DEEZER
CANAL+
arjel
viadeo
AXA

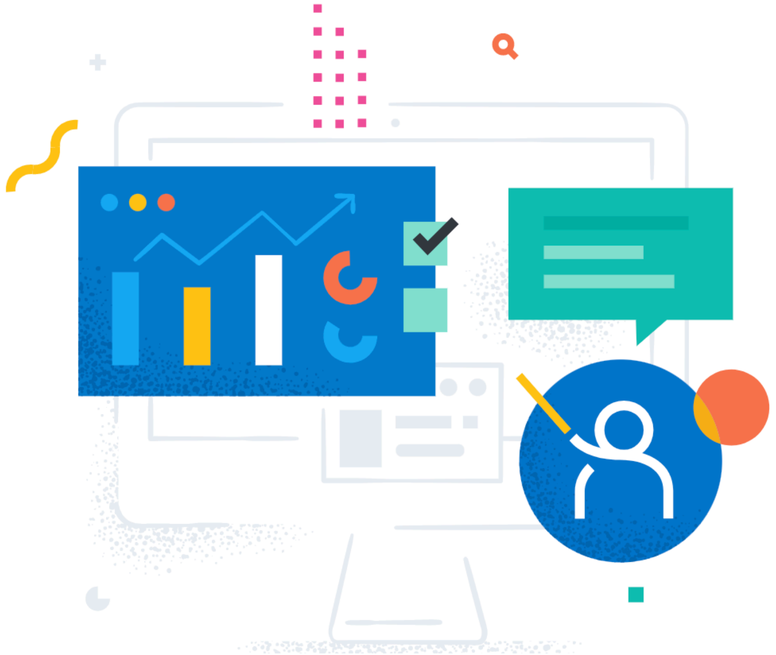
Free Elastic training

Start your Elastic journey and become an expert faster than ever — for free. Build your enterprise search, observability, security, and Elastic Stack skills with our on-demand training.

Fundamentals training

Our self-paced courses include expertly designed materials, engaging demos, hands-on lab exercises, and access to Elastic experts to help you build and retain new skills. And they're all available anywhere you have an internet connection.

- Observability Fundamentals
- Introduction to Observability: Logging
- Metrics Fundamentals
- APM Fundamentals
- Kibana Fundamentals
- Kibana for Splunk Users
- Fundamentals of Securing Elasticsearch
- Elastic SIEM Fundamentals



https://www.elastic.co/training/free

ElasticFR
https://community.elastic.co/

@elasticfr

elastic
User Group

discuss.elastic.co

Next Alan Tech Talks

Tuesday, July 28th

Front-end debugging
by Maxence Bouret

Vote for the next talk
and **submit** your talk proposals
on the Trello board