elastic

Elastic Stack Overview

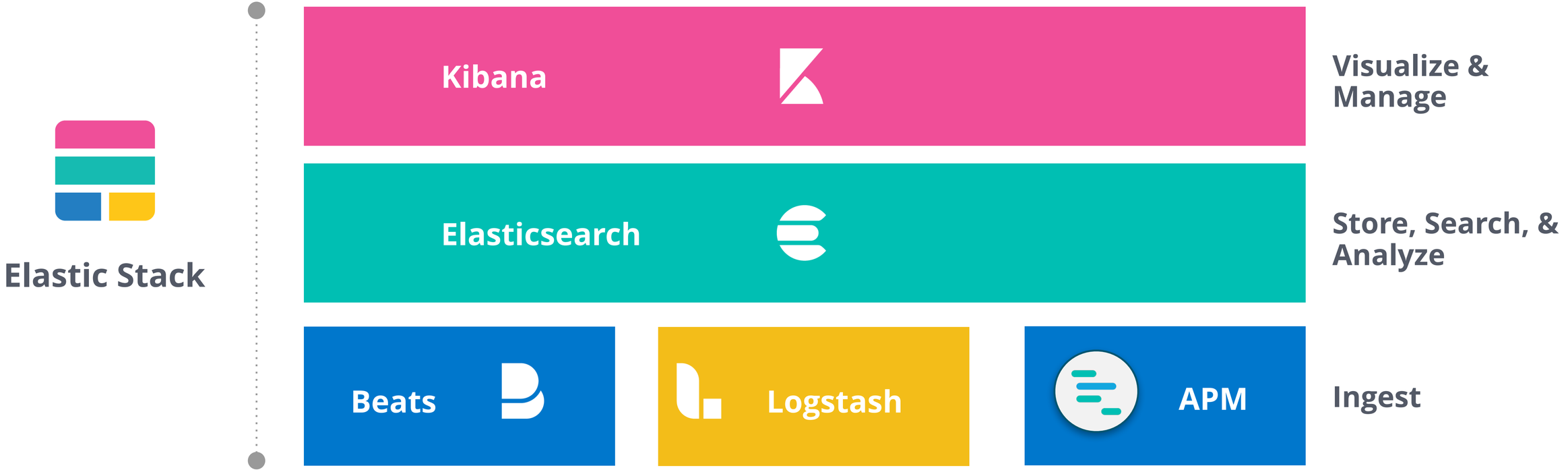
The world’s most popular enterprise products
for real-time search, logging, analytics, and more

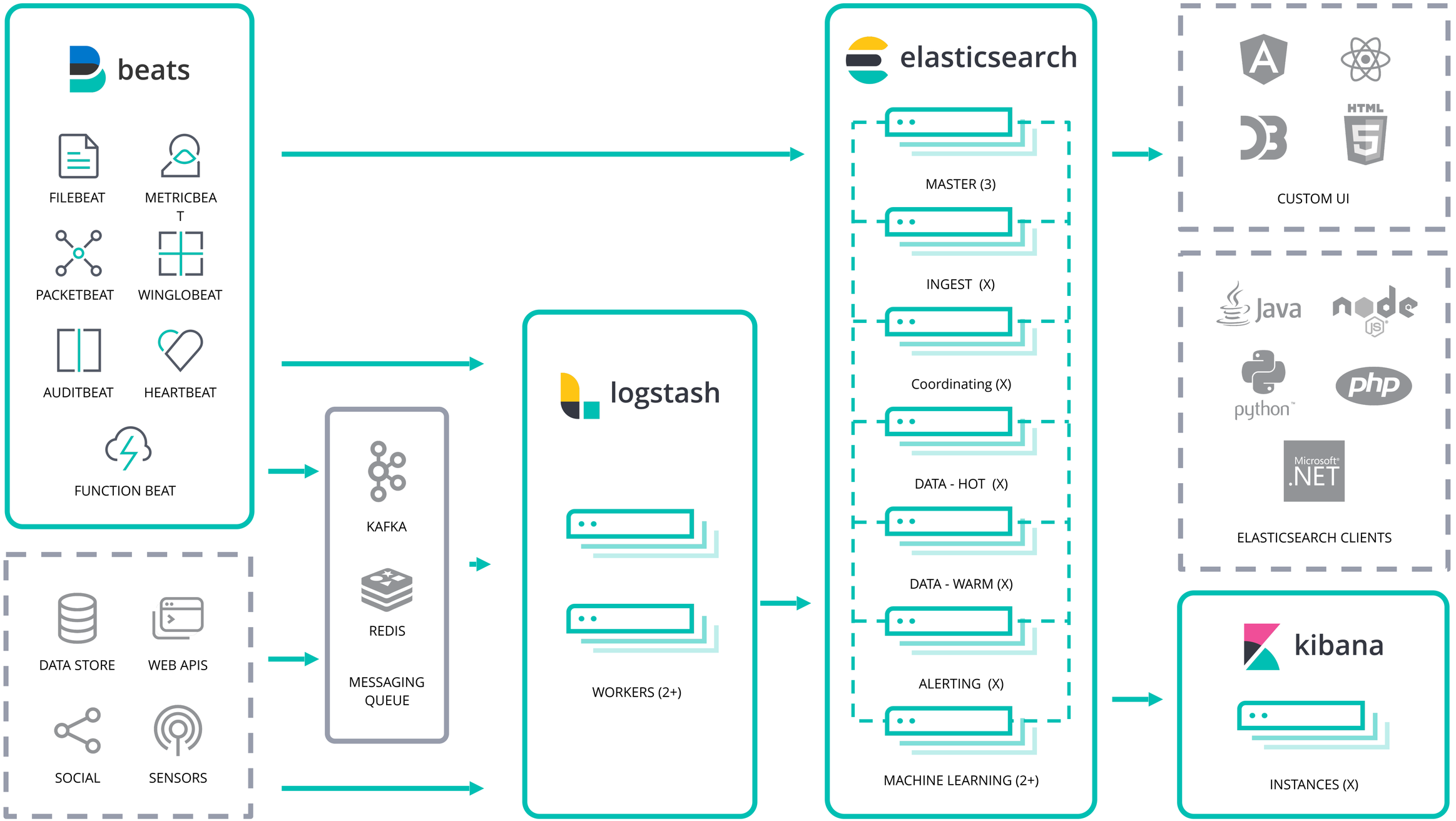
Who?

```
$ curl http://localhost:9200/speaker/_doc/dpilato
{
  "nom" : "David Pilato",
  "jobs" : [
    { "boite" : "SRA Europe (SSII)", "mission" : "bon à tout faire", "date" : "1995" },
    { "boite" : "SFR", "mission" : "touche à tout", "date" : "1997"  },
    { "boite" : "e-Brands / Vivendi", "mission" : "chef de projets", "date": "2000" },
    { "boite" : "DGDDI (douane)", "mission" : "mouton à 5 pattes", "date" : "2005" },
    { "boite" : "IDEO Technologies", "mission" : "CTO", "date" : "2012" },
    { "boite" : "elastic", "mission" : "développeur", "date" : "2013" } ],
  "passions" : [ "famille", "job", "deejay" ],
  "blog" : "http://david.pilato.fr/",
  "twitter" : [ "@dadoonet", "@elasticfr" ],
  "email" : "david@pilato.fr"
}
```

elastic

Elastic **Stack**




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)

Open source

Apache 2.0 : aujourd'hui comme demain.

Téléchargement gratuit

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.

Téléchargement gratuit

Tous les avantages de l'open source, plus :

- Principales fonctionnalités de sécurité
- Solutions telles qu'APM, SIEM, Maps et d'autres encore
- Canvas
- Et plus encore

Gold

Plus de fonctionnalités. Support technique dédié.

Nous contacter

Tous les avantages de l'offre Basic, plus :

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

Platinum

L'expérience ultra-complète.

Nous contacter

Tous les avantages de l'offre Gold, plus :

- Fonctionnalités de sécurité avancées
- Machine Learning
- Réplication inter-clusters
- Support technique 24 h/24, 7 j/7, 365 j par an
- Et plus encore

https://www.elastic.co/fr/subscriptions

elastic

Services at a Glance

Elastic Training

- Immersive learning experience
- Solution-based curriculum
- Flexible ways-to-train

Certification

- Performance-based exam
- Solve real-world tasks, in real-time
- Remote, secure testing

People Strategy

Elastic Consulting

- Expert services focused on your business goals
- Phased-based packages
- Product expertise

Project Strategy

Elastic Training

Montréal / Canada

Course offerings

Elasticsearch Engineer I: Apr 6-7

Elasticsearch Engineer II: Apr 8-9

Who should attend?

Software Developers, Engineers, Data Architects, System Administrators, DevOps

What will I learn?

- How to manage deployments and develop solutions.
- Advanced cluster management techniques, best practices for capacity planning and scaling, and more.

IMMERSIVE LEARNING ENVIRONMENT

Lab-based exercises 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 skills to real-world use cases, in real-time

50% discount on the 2nd seat

Vouchers for free trainings

https://training.elastic.co/elearning/

Training	Voucher
Logging Fundamentals	**Logging**
Metrics Fundamentals	**Metrics**
APM Fundamentals	**APM**
Elastic Machine Learning for Cybersecurity	**MLCyber**
ECE Fundamentals	**ECEF**
Fundamentals of Securing Elasticsearch	**FSE**

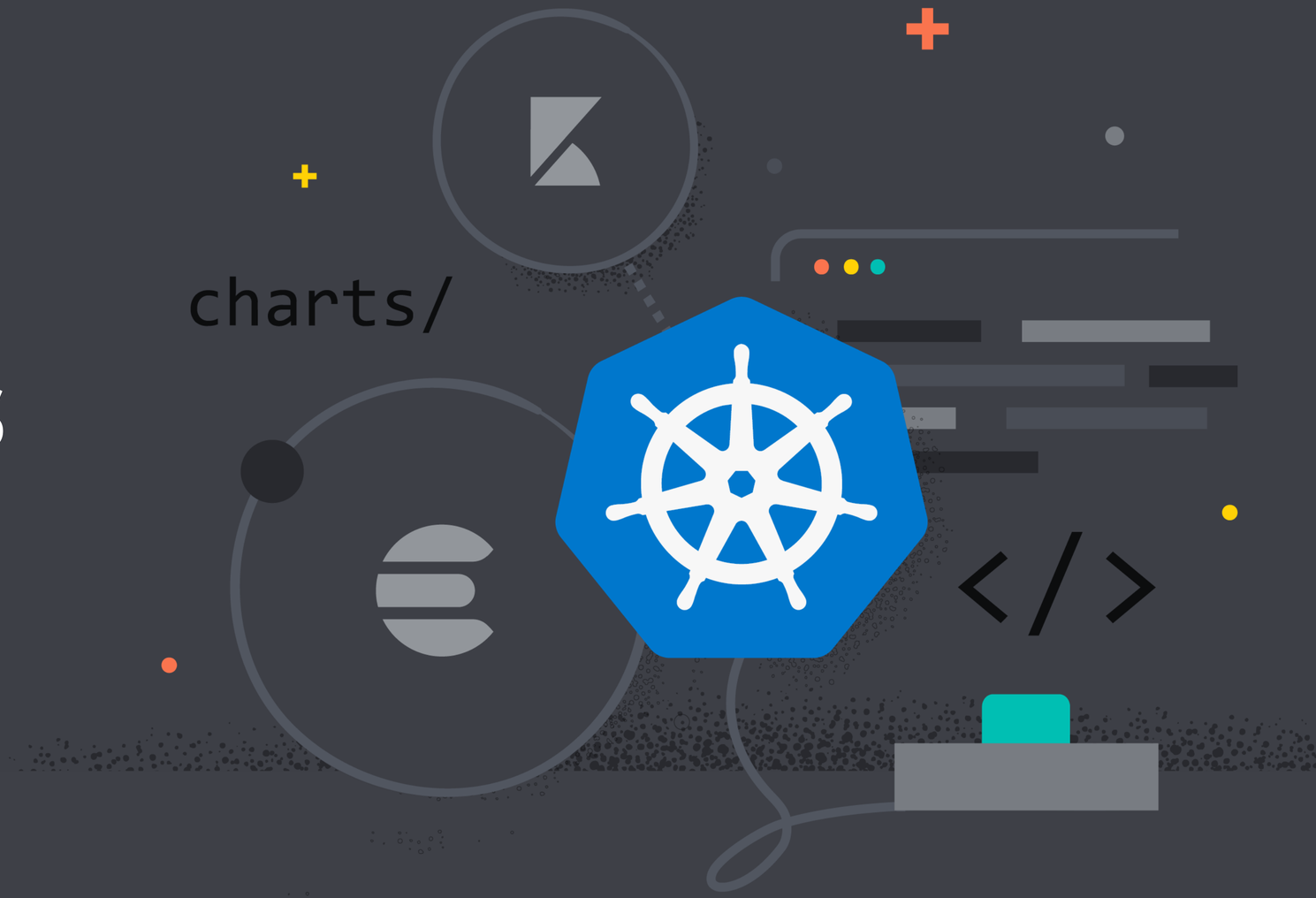
Please do not share those codes

elastic

Demo time!

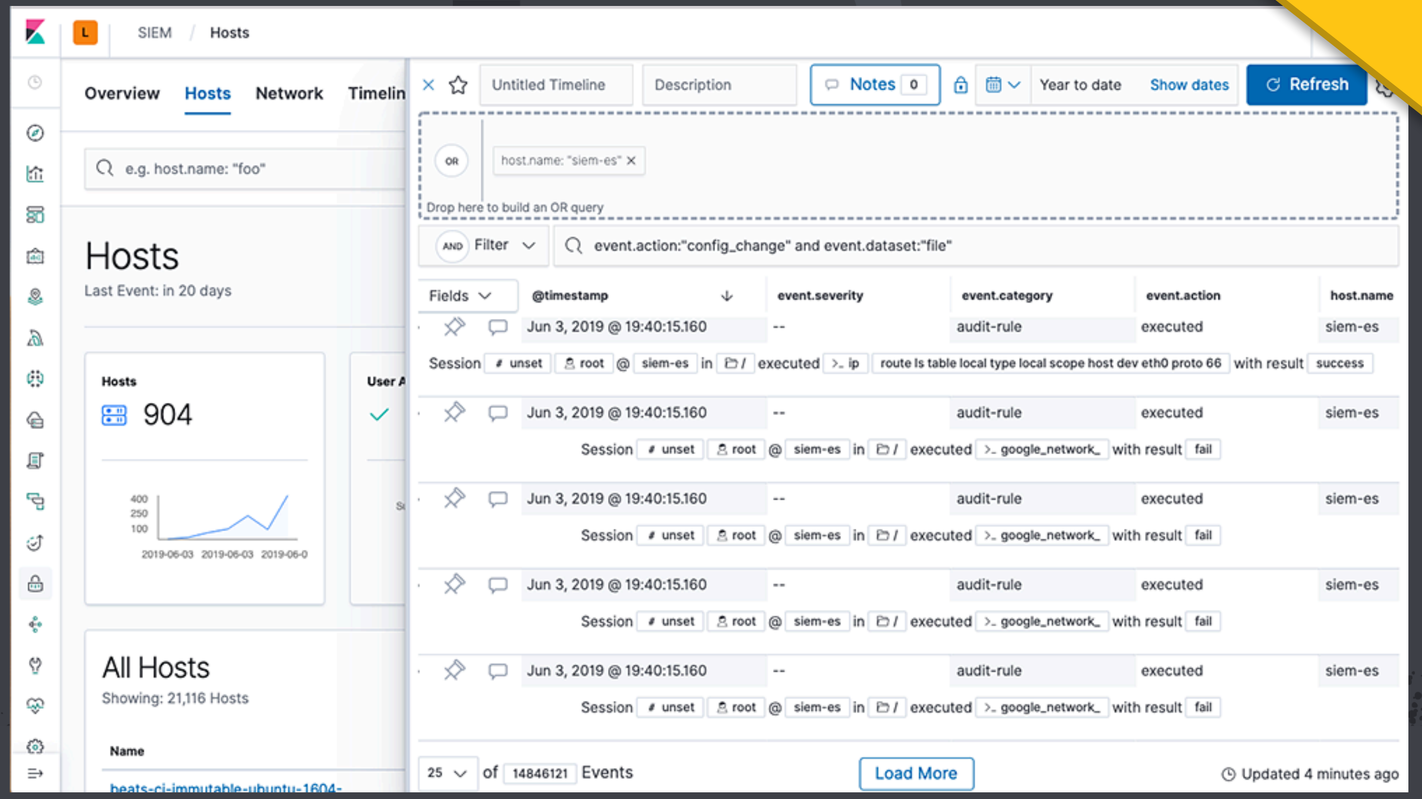
Elastic Cloud on Kubernetes

The official Operator (and more)
for Elasticsearch and Kibana



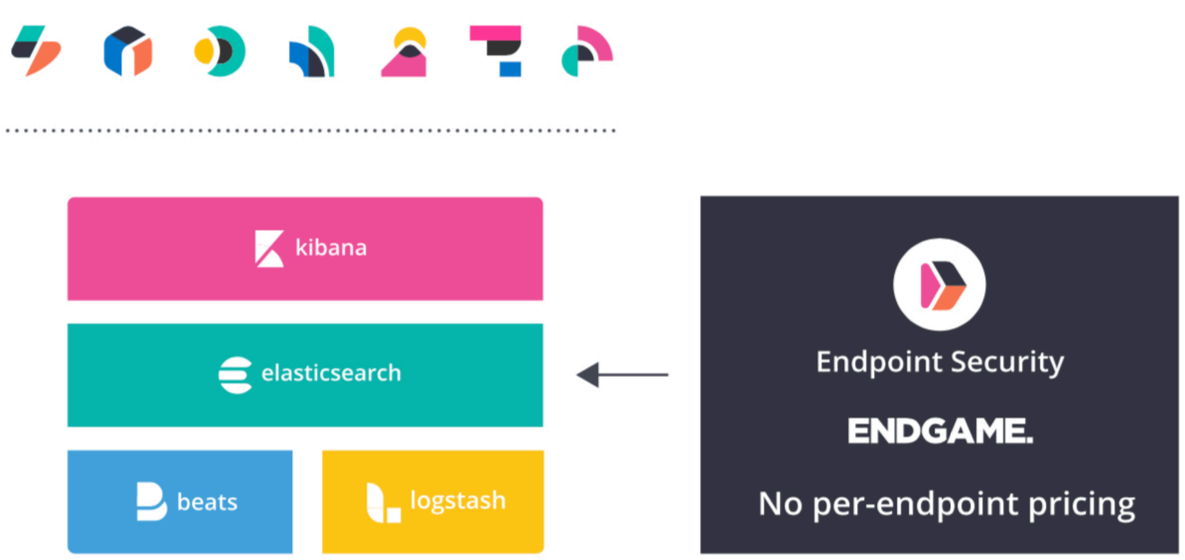
Elasticsearch SIEM solution available for free

New in 7.2



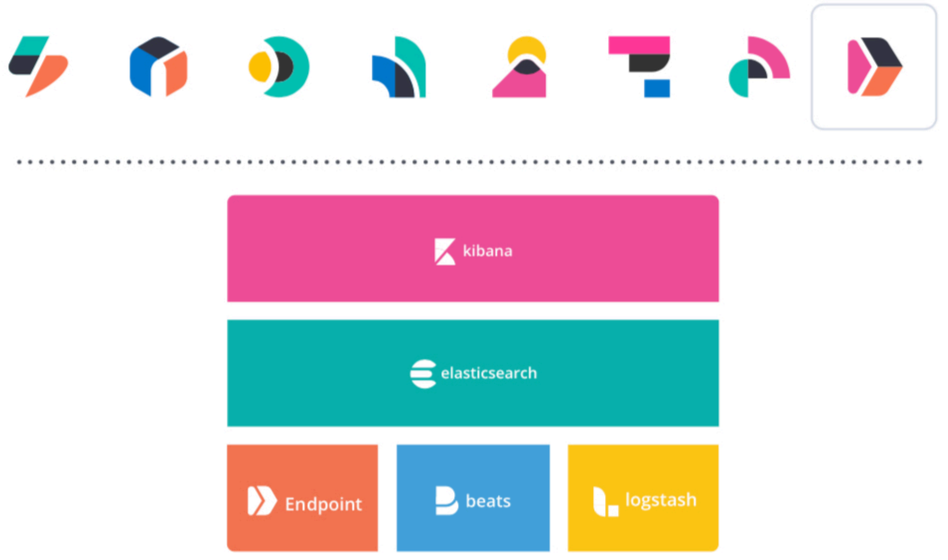
Today

Comprehensive endpoint protection, detection, and response (EPP+EDR) and no per-endpoint pricing. Just pay for what you use.



Future

EPP, EDR, and SIEM delivered in a single, simplified architecture: Elasticsearch, Kibana, Elastic Endpoint.



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)
```

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?      |
+--------------+-----------------------+
```

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  |
+--------------+-----------------------+
```

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)
```

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  |
+--------------+-----------------------+
```

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?                        |
+--------------+-----------------------------------------+
```

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 "%Dadid%";
Empty set (0,00 sec)
```

elastic

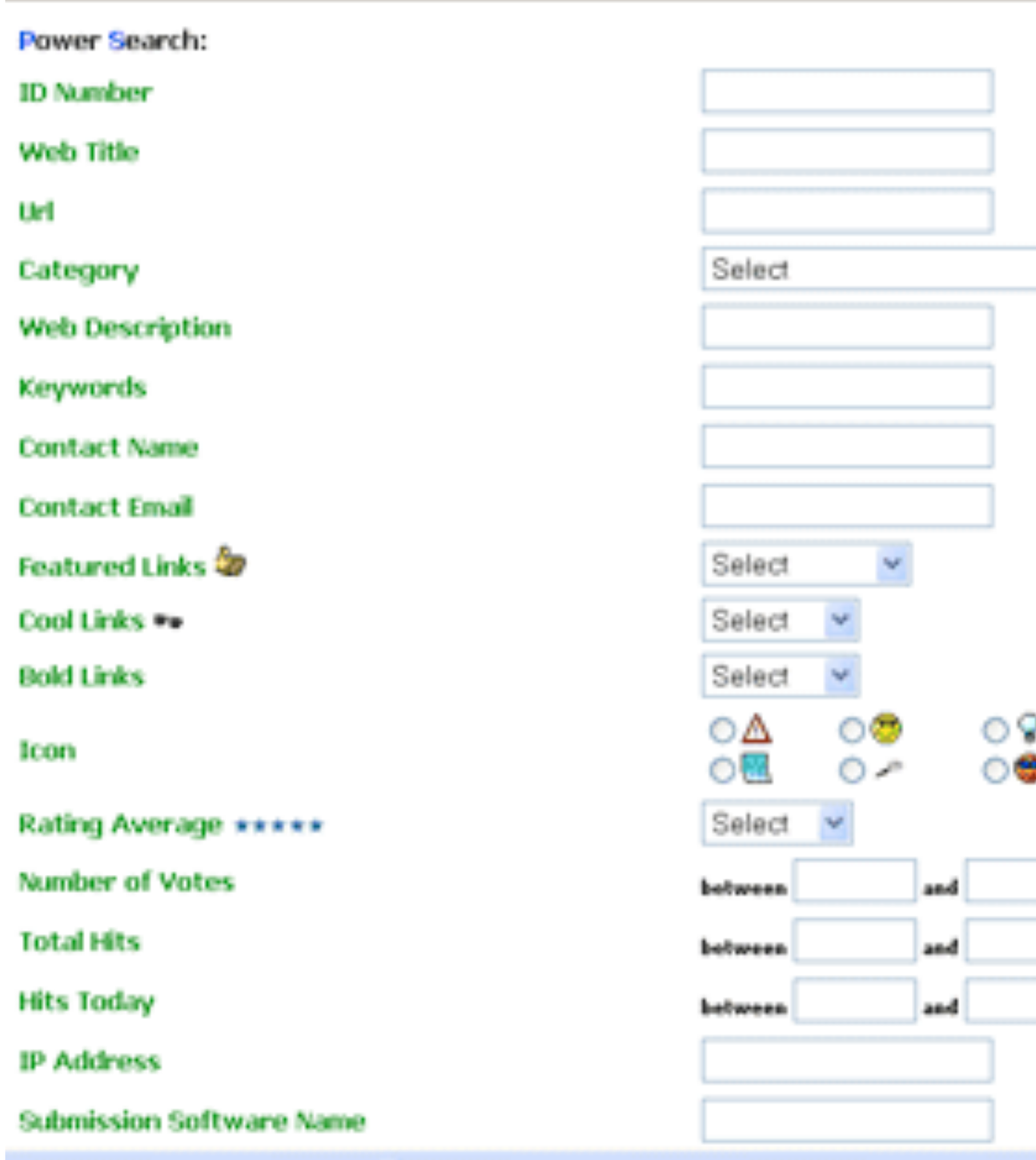
Search with typos

```
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_%";
```

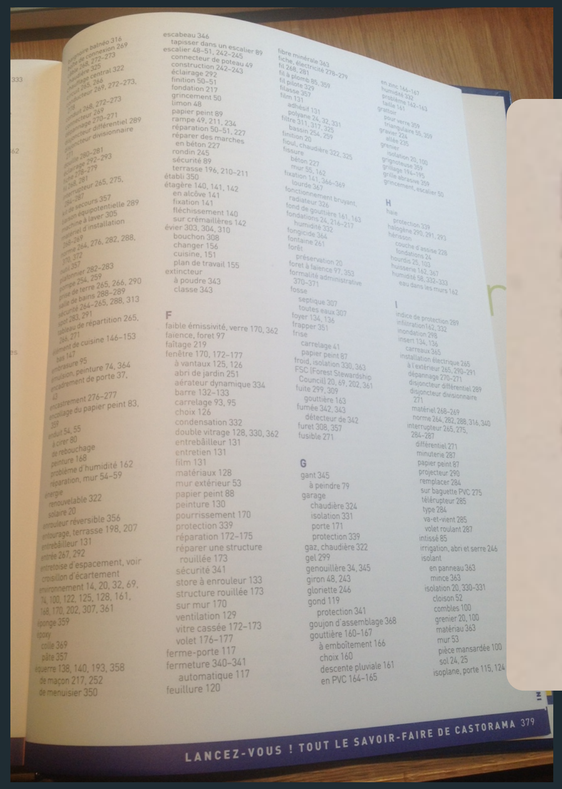
name	comments
David Pilato	Developer at elastic
David Gageot	Engineer at Google
David David	Who is that guy?

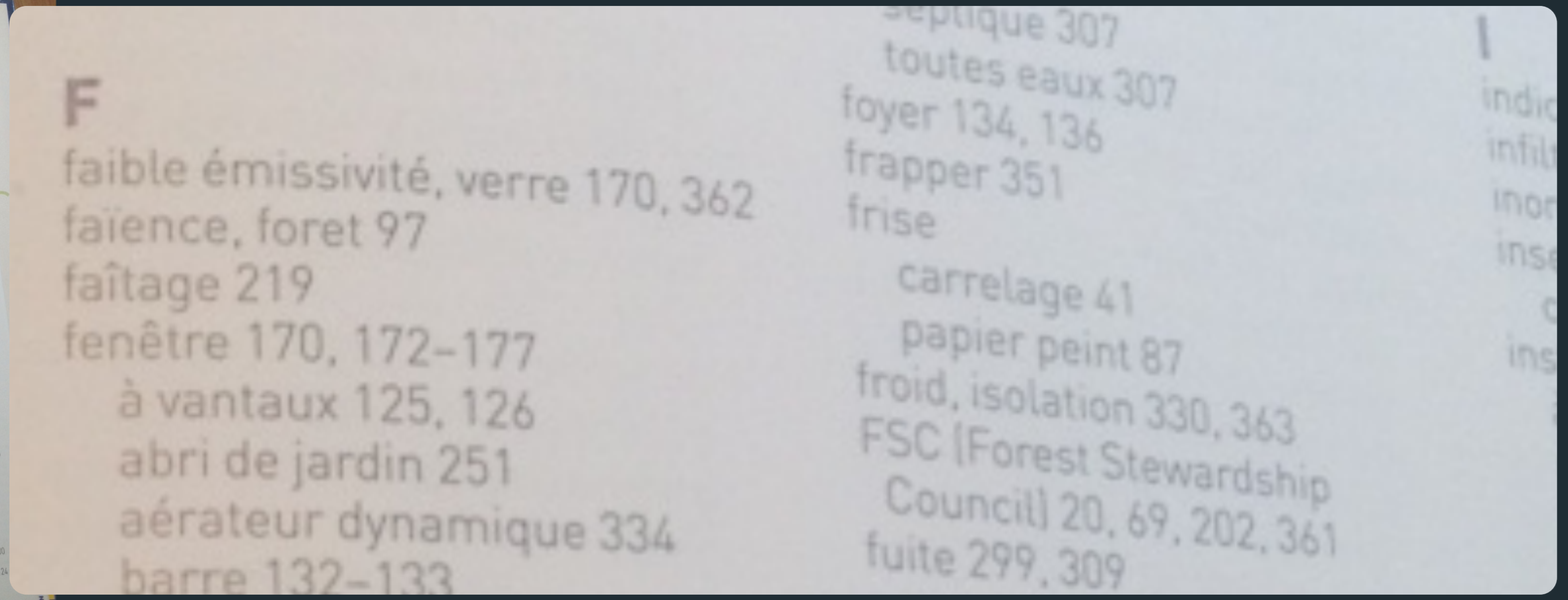
User Interface



Search engine?

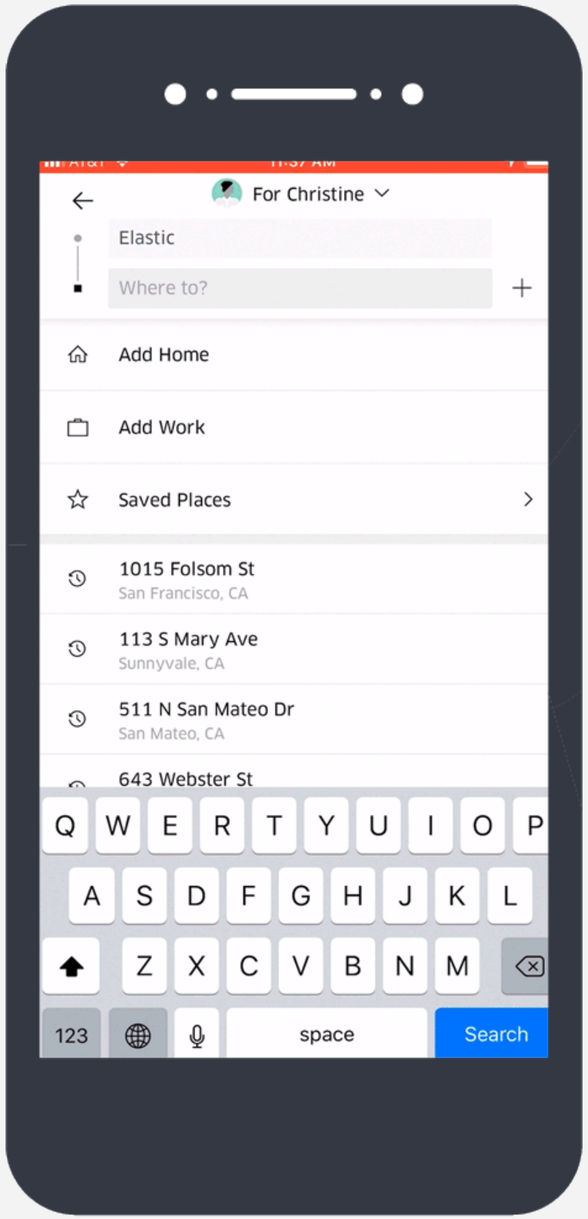
Moteur d'**indexation de documents**





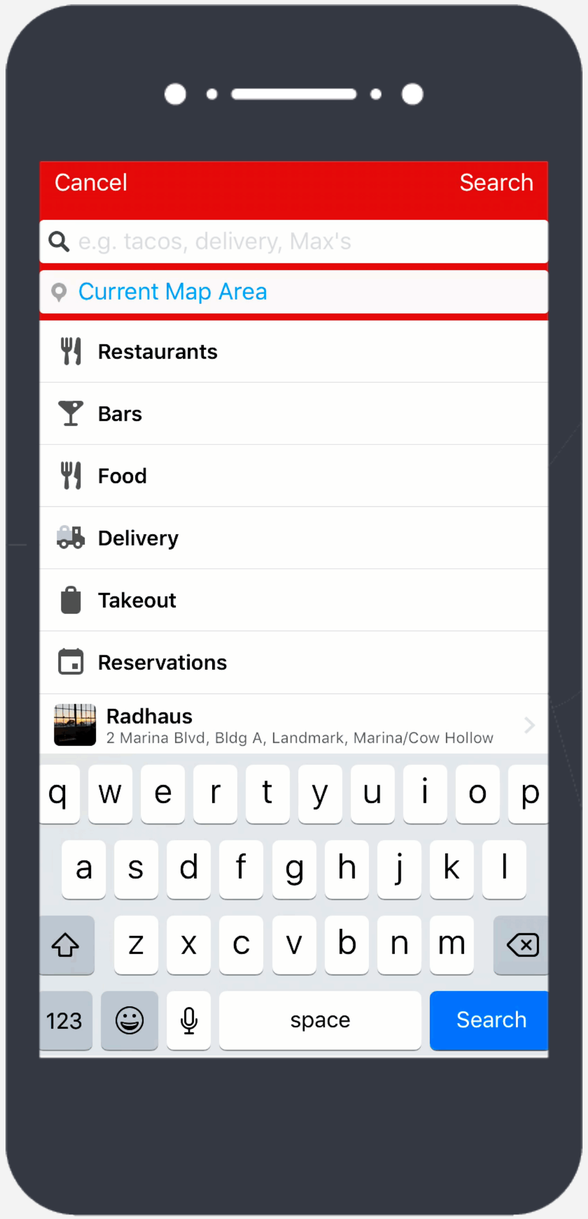
Moteur de **recherche dans les index**


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



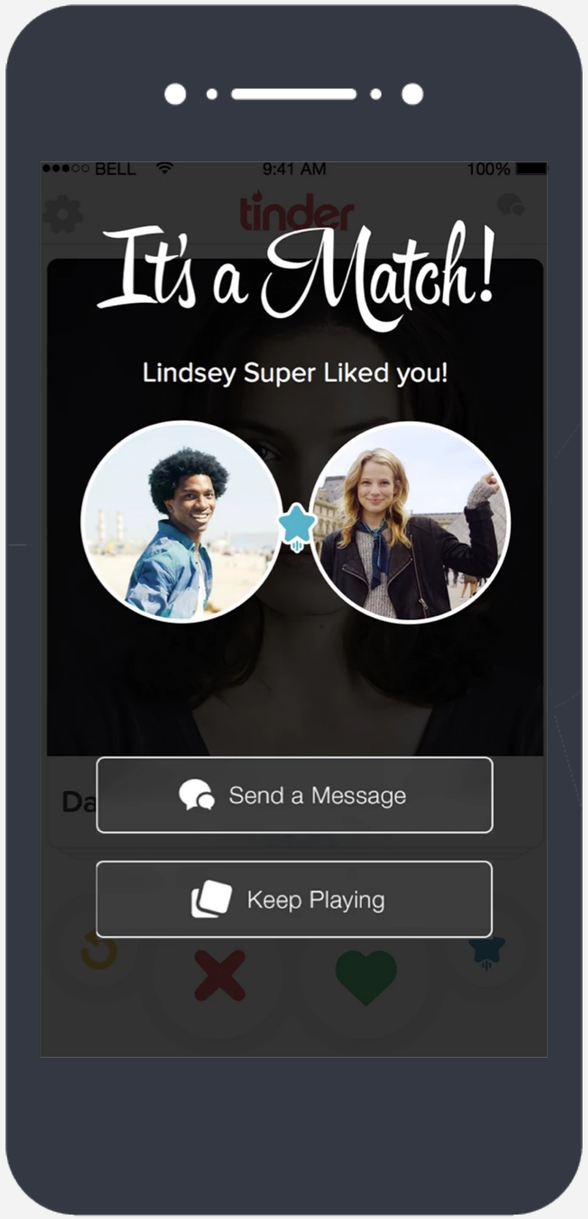
Uber

elastic



yelp®

elastic



tinder™

elastic


keljob

BlaBlaCar

SwissLife

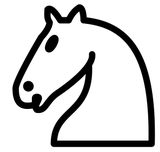
PSA PEUGEOT CITROËN

LesFurets.com
Comparez et achetez futé

francetvinfo

radio
france

LEROY MERLIN
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Crédit Mutuel
ARKEA


DHL

LES ANGES DE LA TELEREALITE

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


#ElasticStories

Elastic Training

Montréal / Canada

Course offerings

Elasticsearch Engineer I: Apr 6-7

Elasticsearch Engineer II: Apr 8-9

Who should attend?

Software Developers, Engineers, Data Architects, System Administrators, DevOps

What will I learn?

- How to manage deployments and develop solutions.
- Advanced cluster management techniques, best practices for capacity planning and scaling, and more.

IMMERSIVE LEARNING ENVIRONMENT

Lab-based exercises 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 skills to real-world use cases, in real-time

50% discount on the 2nd seat

elasticfr

@elasticfr

elastic
User Group

discuss.elastic.co