Elastic Stack Overview

Search. Observe. Protect.

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"
}
```

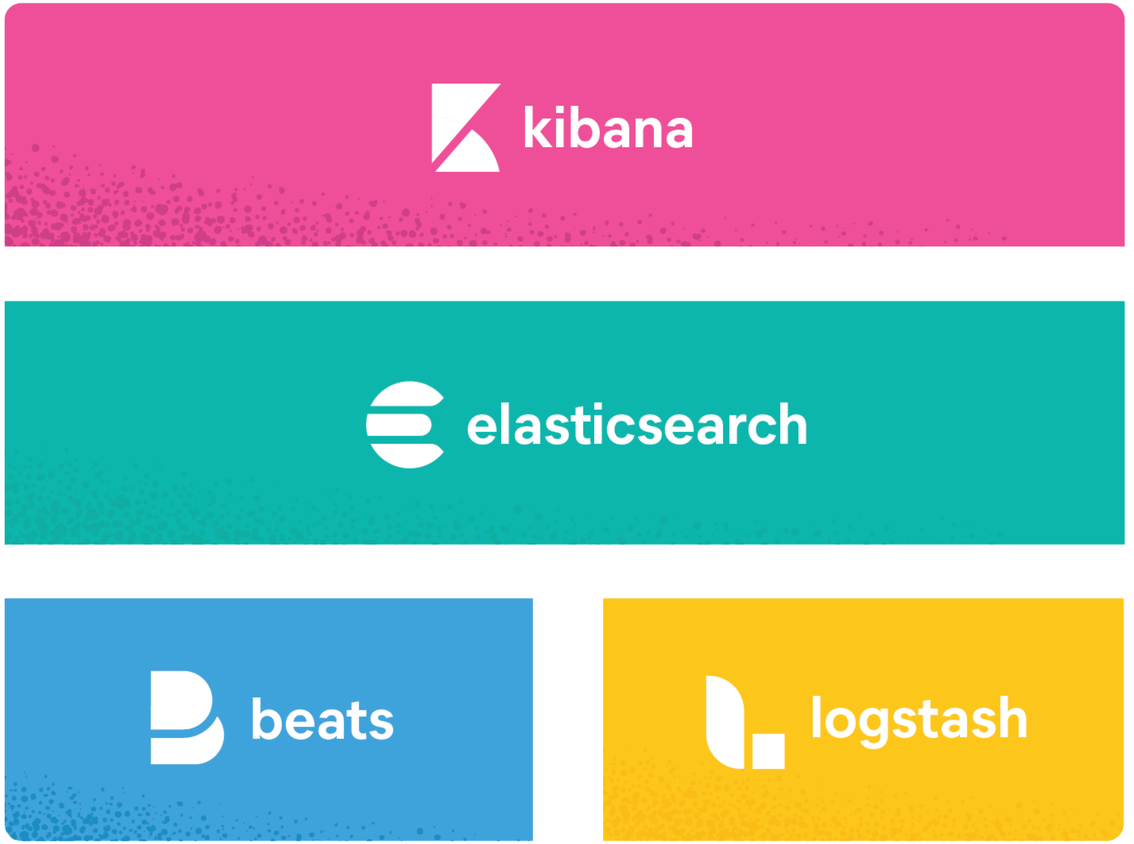
elastic

Employees in 40+ countries

Public company on NYSE

The Elastic Stack

Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.



elastic

Deploy anywhere.

Elastic Cloud

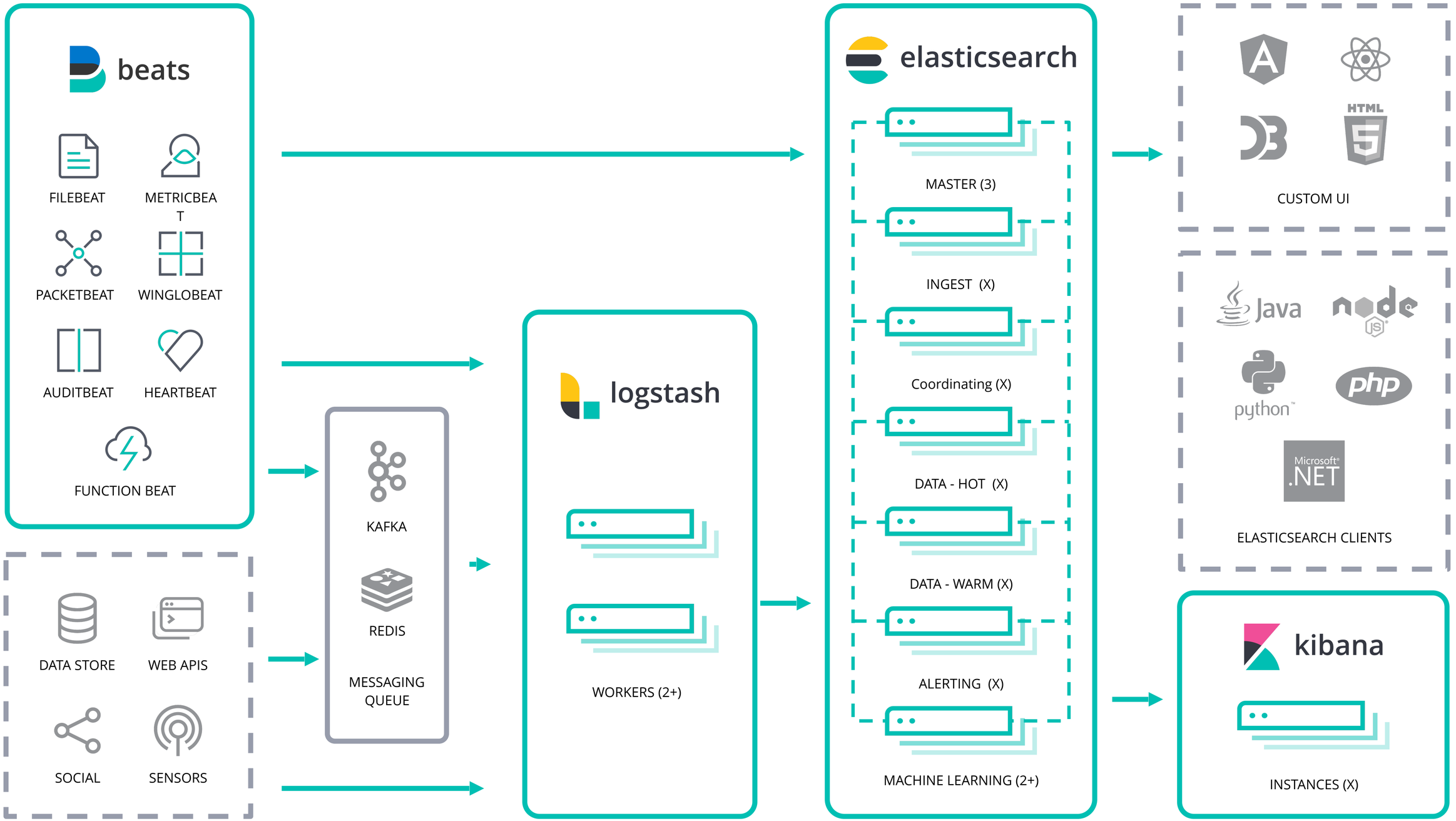
Elastic Cloud Enterprise

Elastic Cloud on Kubernetes

SaaS

Orchestration

elastic


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)

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

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

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

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)

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

Elastic Consulting

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

People Strategy

Project Strategy

elastic

Elastic Training

Paris / France

En français

Course offerings

Elasticsearch Engineer I: Apr 20-21

Elasticsearch Engineer II: Apr 22-23

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 - discount until Feb 24th

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

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

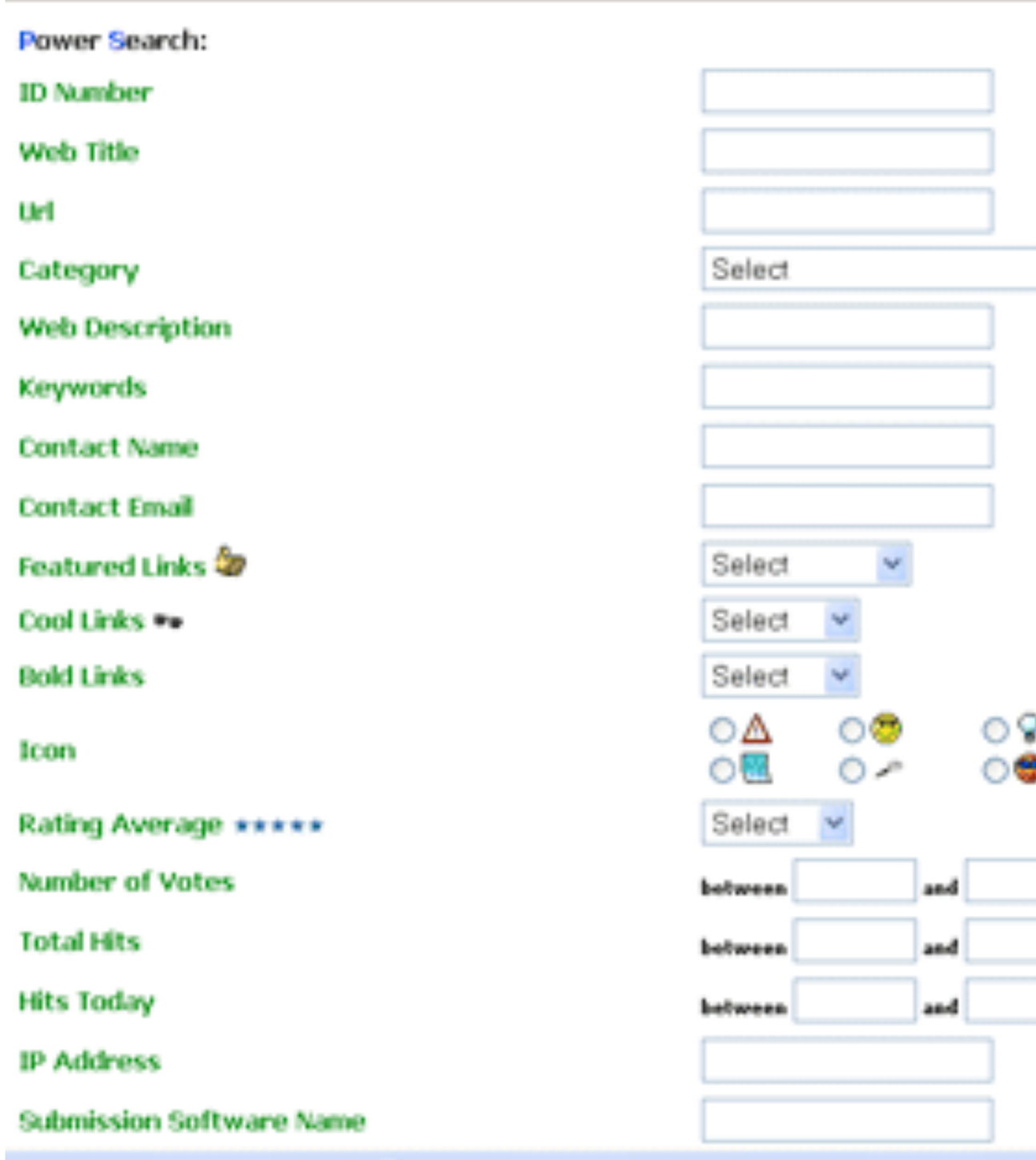
Search with typos

```
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_%";
```

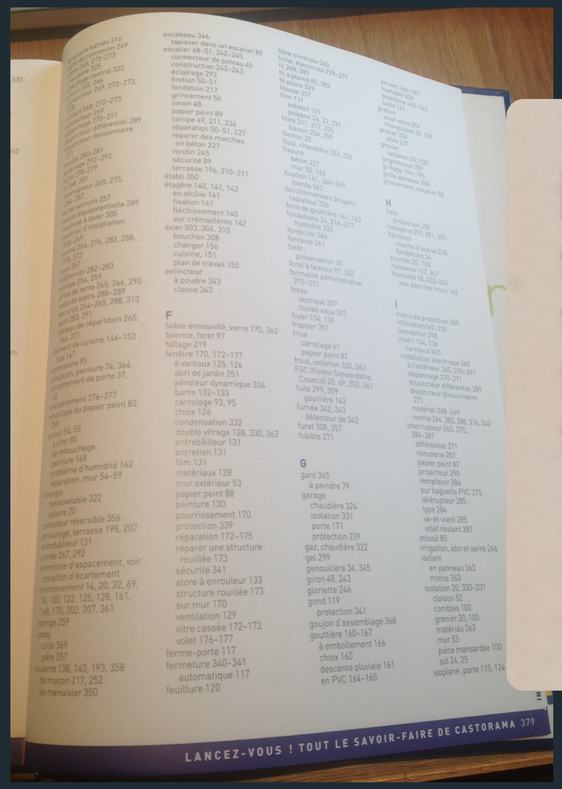
name	comments
David Pilato	Developer at elastic
David Gageot	Engineer at Google
David David	Who is that guy?

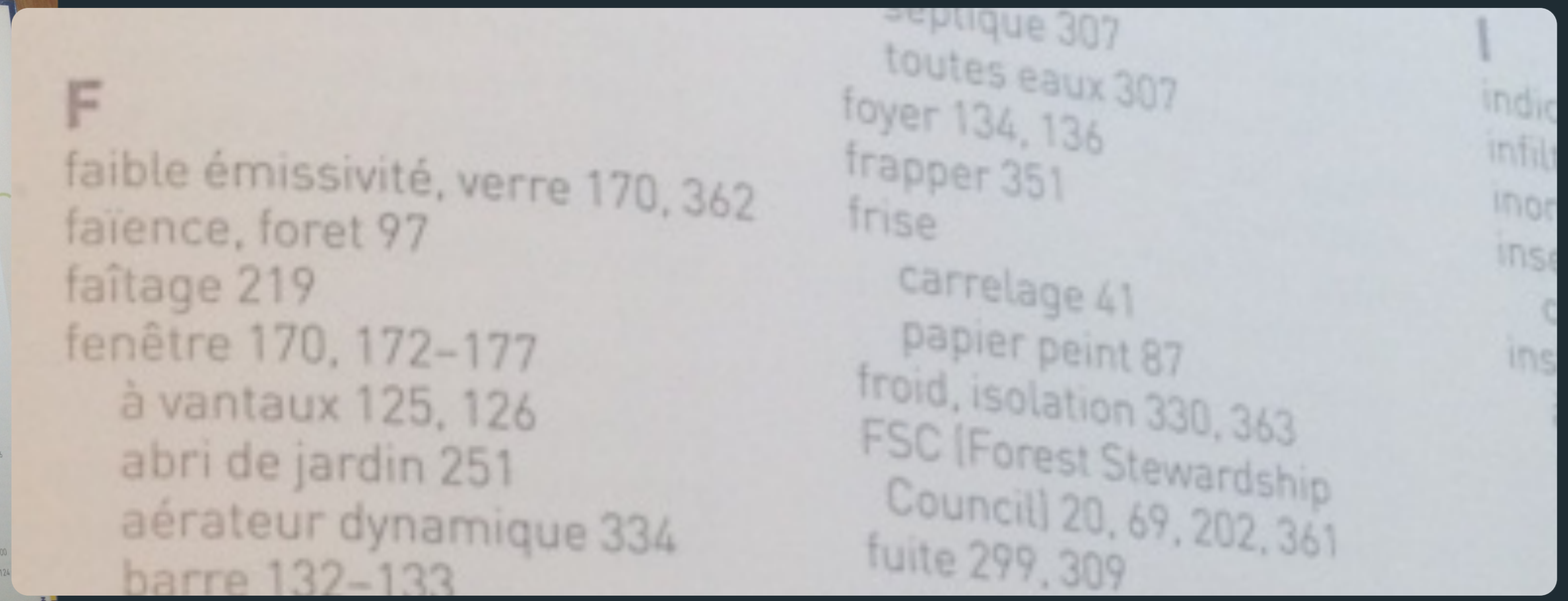
User Interface



Search engine?

Moteur d'**indexation de documents**



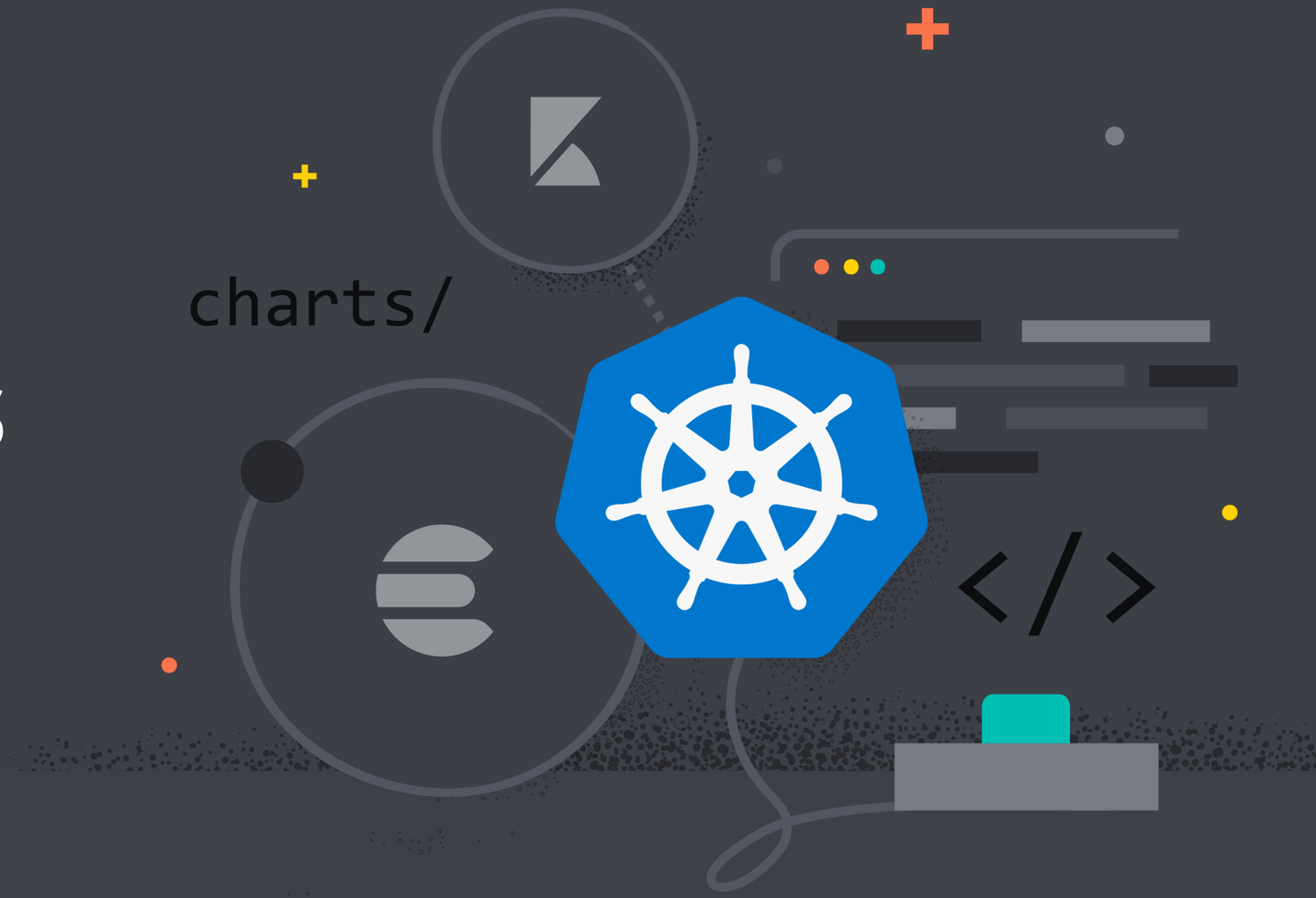


Moteur de **recherche dans les index**

Demo time!

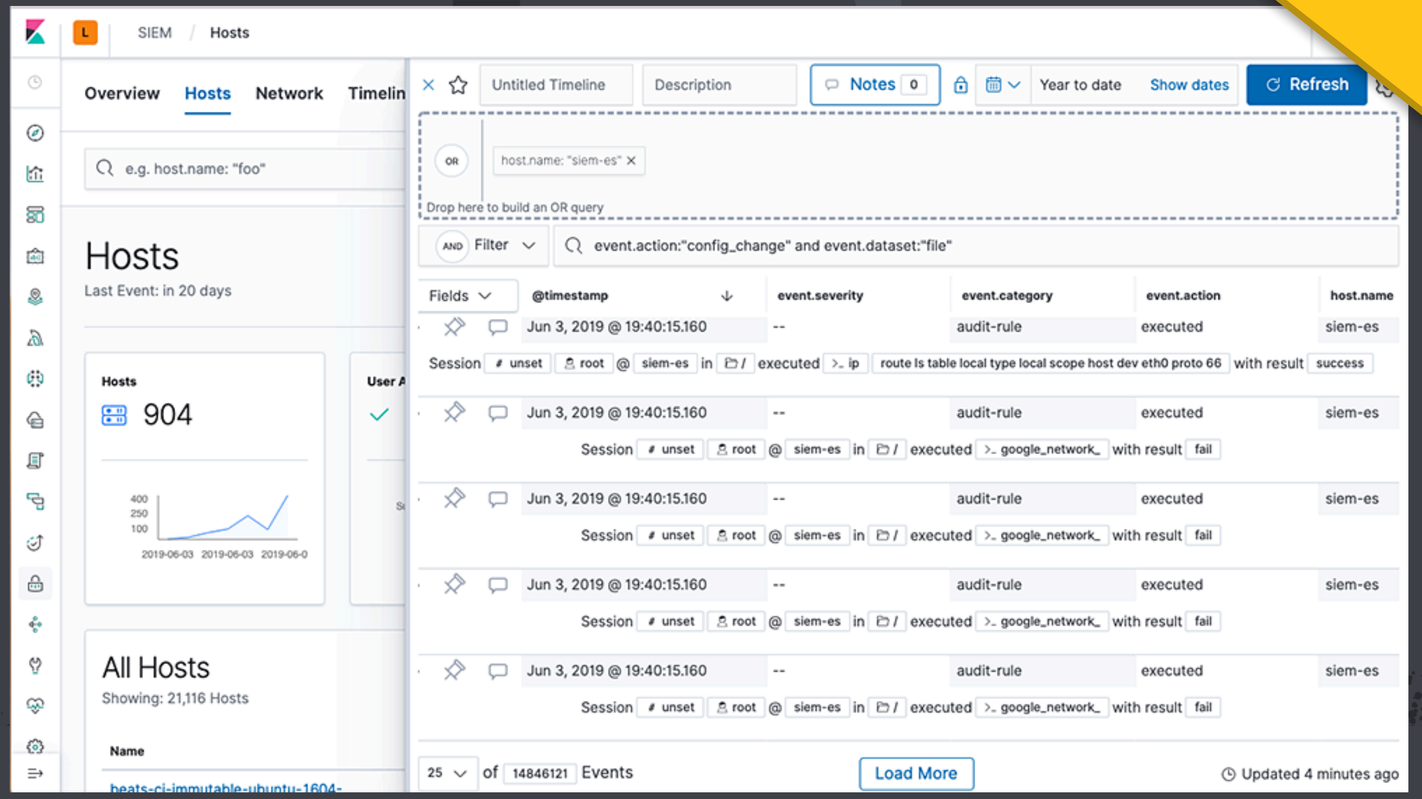
Elastic Cloud on Kubernetes

The official Operator (and more)
for Elasticsearch and Kibana



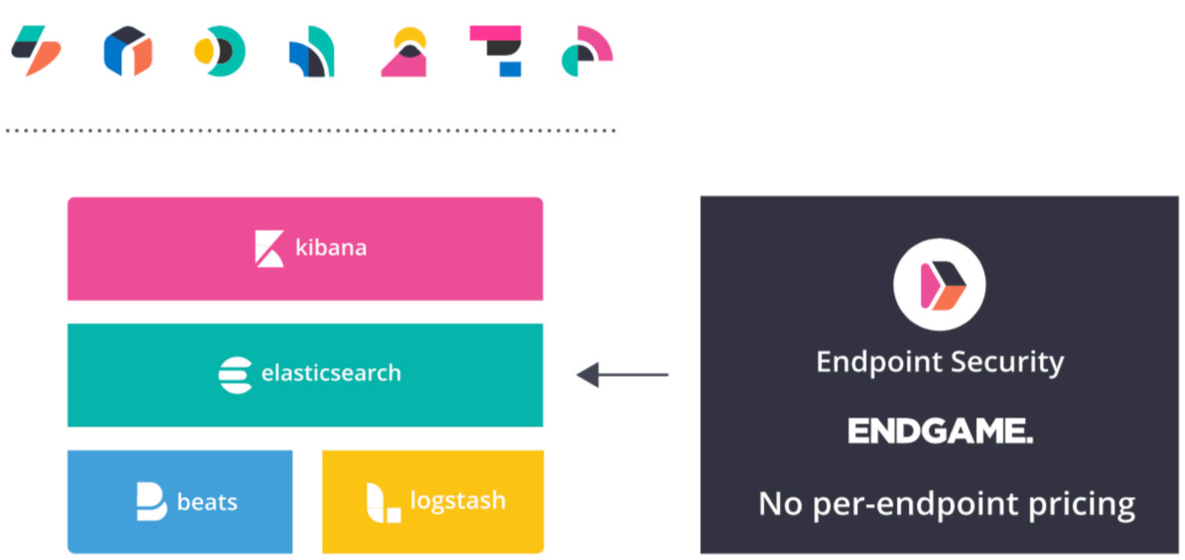
Elasticsearch SIEM solution available for free

New in 7.2



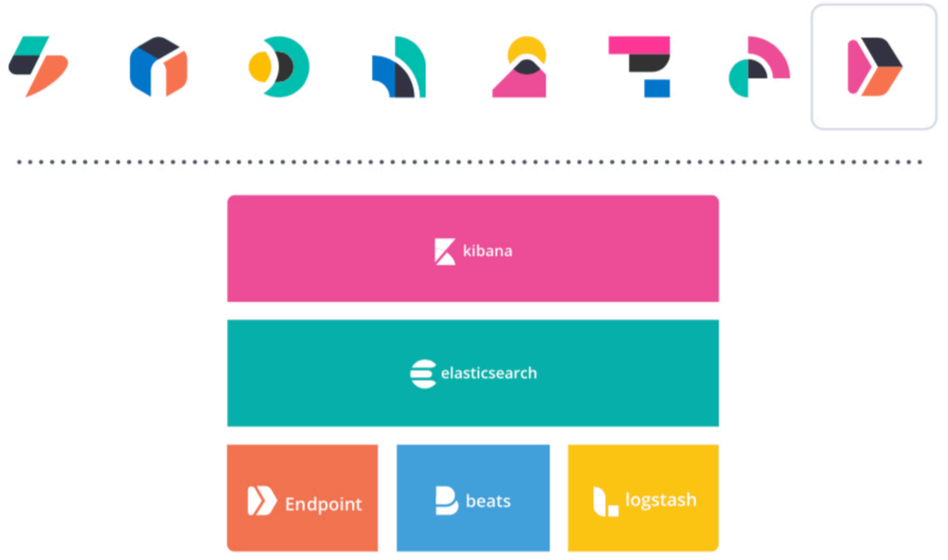
Today

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.



3 solutions

Elastic Enterprise Search

Elastic Observability

Elastic Security

elastic

Elastic Enterprise Search

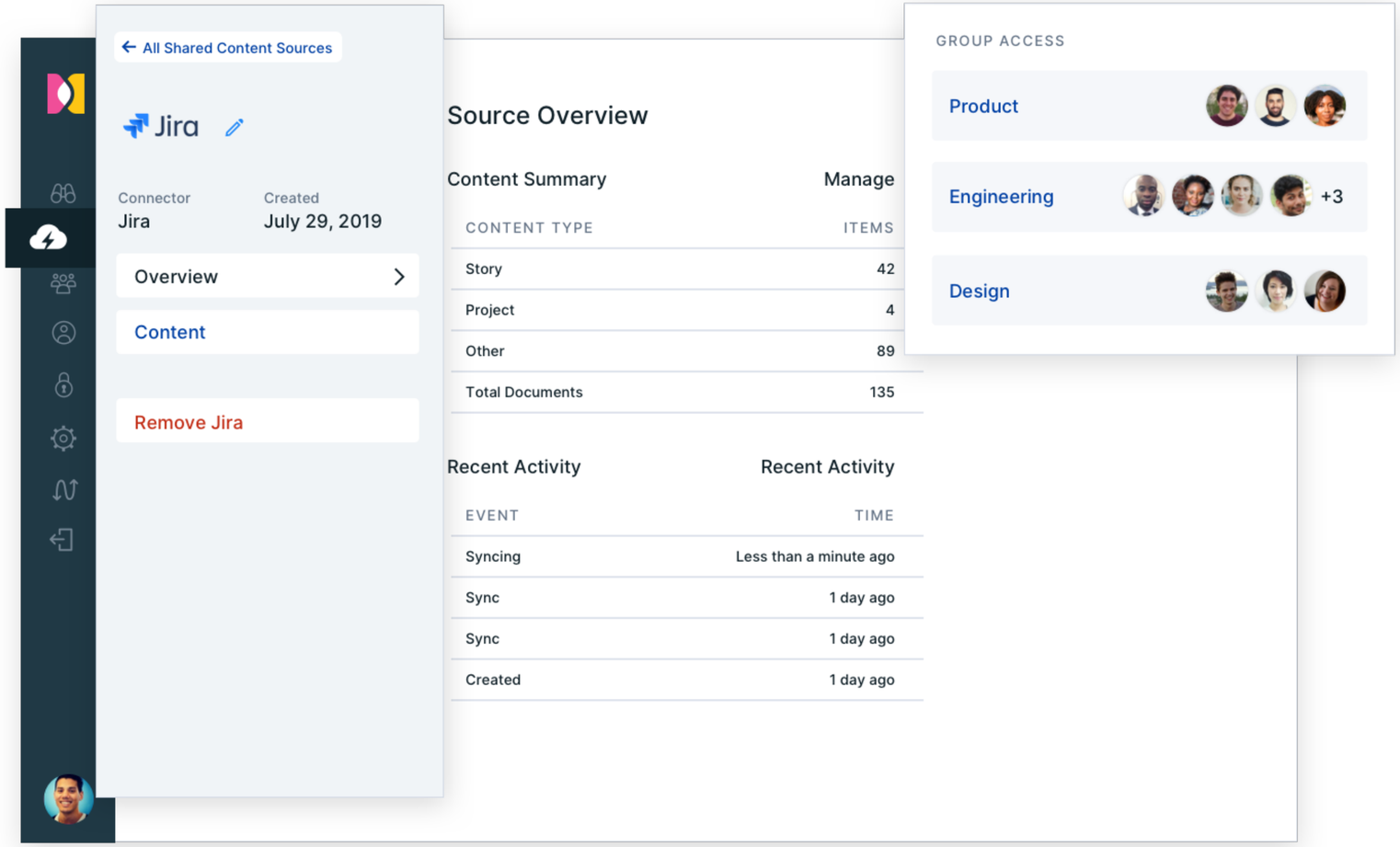
Workplace Search App Search Site Search

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

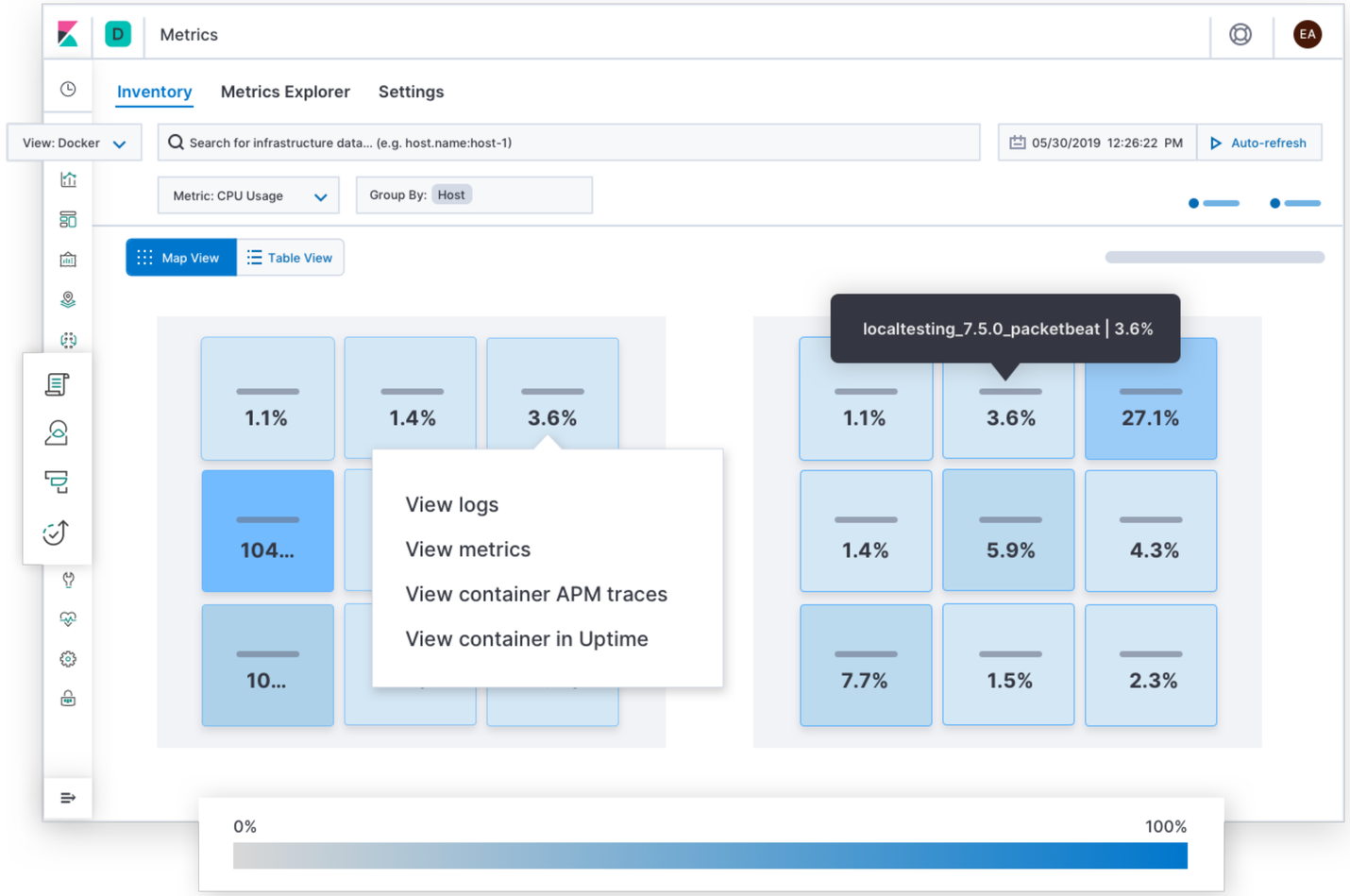
Logs Metrics APM Uptime

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

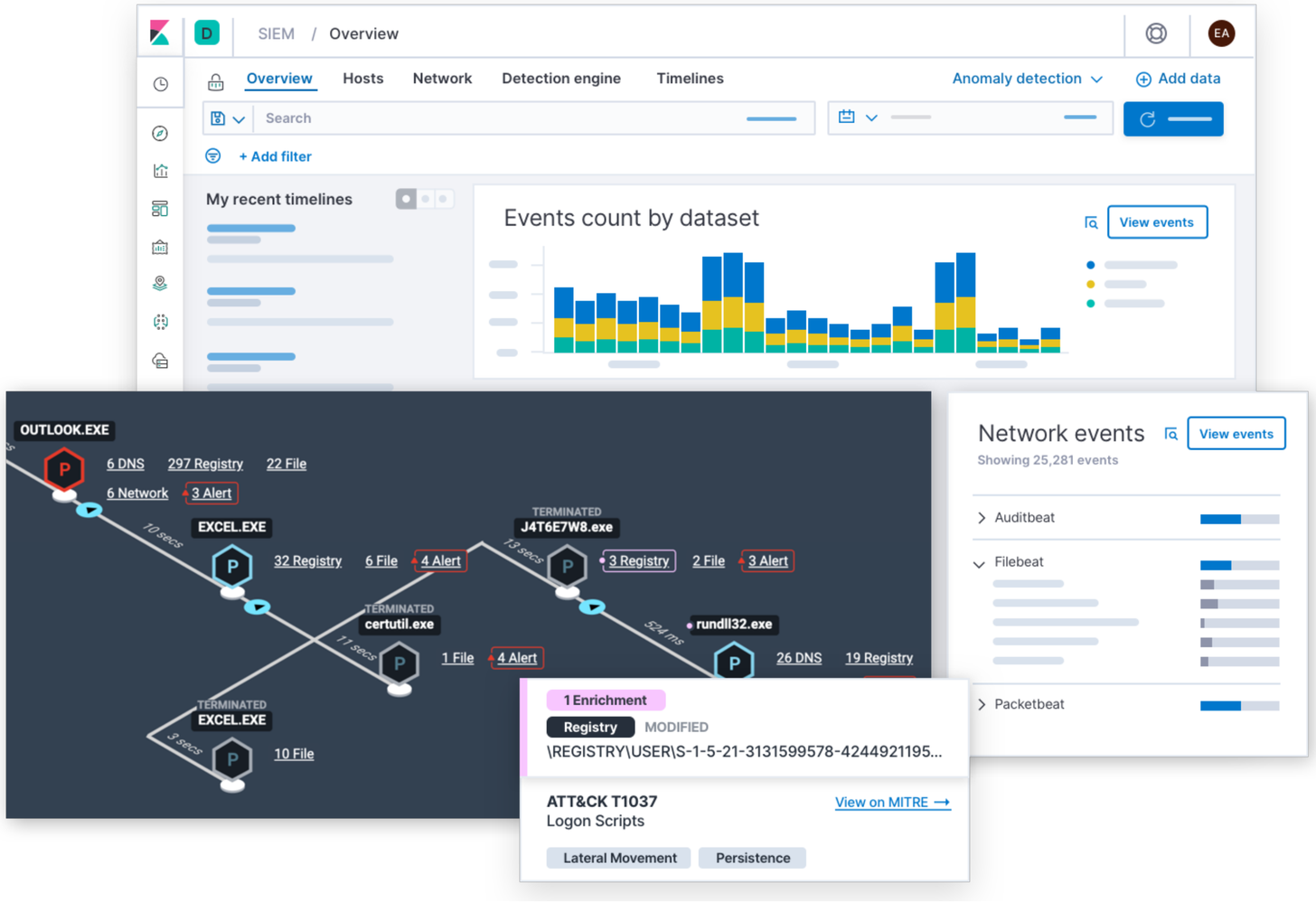
Endpoint SIEM

elastic

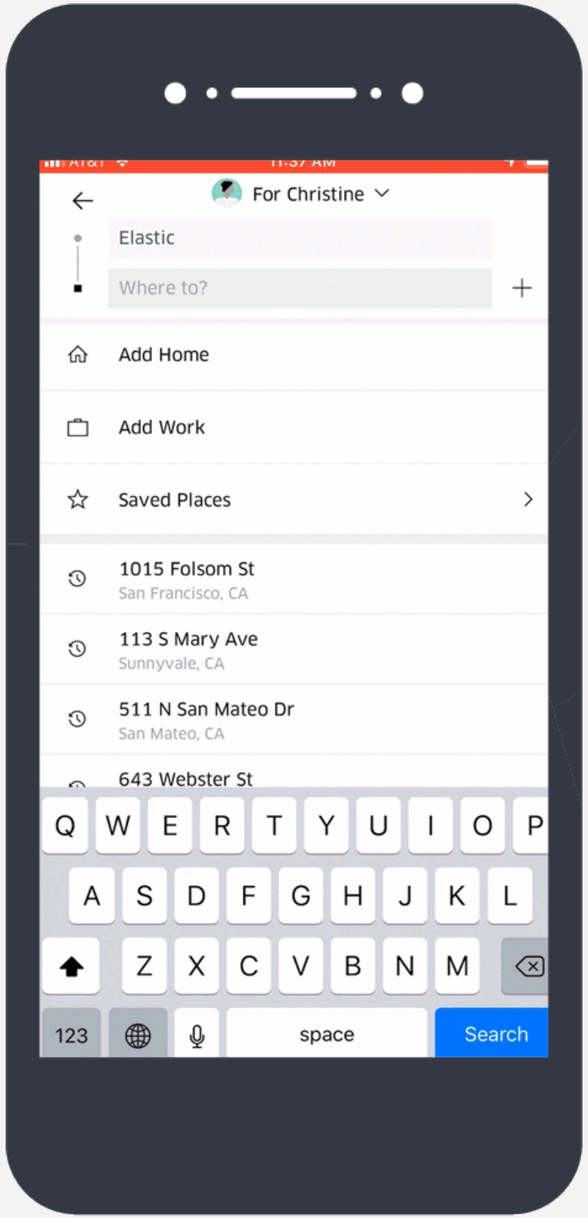
ELASTIC SECURITY

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.

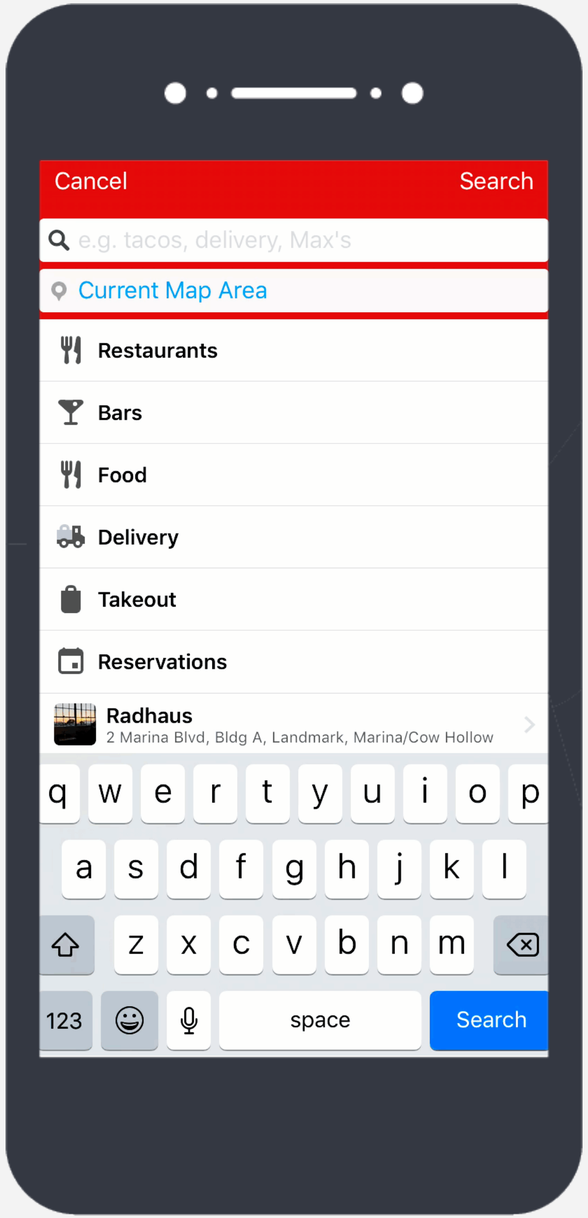



HSBC
SOUNDCLOUD
mozilla FOUNDATION
Microsoft
GROUPON
facebook
Expedia
vimeo
salesforce
FOURSQUARE
ACTIVISION BLIZZARD
stackoverflow
NASA
Symantec
DELL
The New York Times
Unilever
ebay
Eventbrite
Alcatel·Lucent
CONCUR
verizon
NETFLIX
IBM
PayPal
Adobe
CISCO
docker
The Guardian
THOMSON REUTERS
Quora
TOMTOM



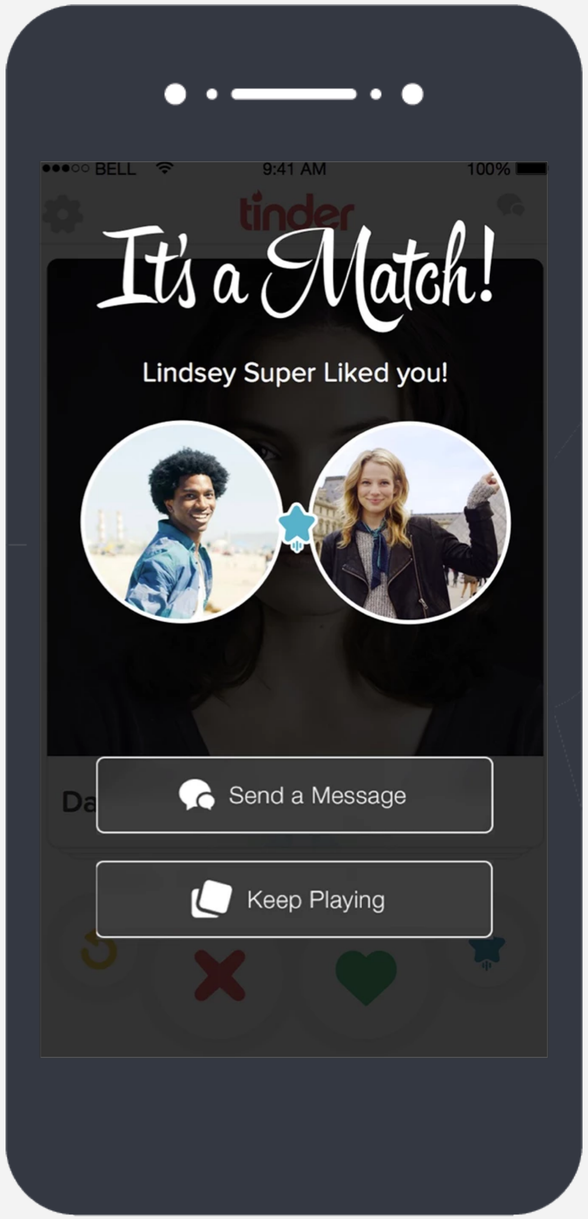
Searching for **Rides**

elastic



Searching for **Restaurants**

elastic



tinder™

elastic

Searching for

Rides

elastic


keljob

BlaBlaCar

SwissLife

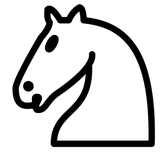
PSA PEUGEOT CITROËN

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

Paris / France

En français

Course offerings

Elasticsearch Engineer I: Apr 20-21

Elasticsearch Engineer II: Apr 22-23

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 - discount until Feb 24th

elasticfr

@elasticfr

elastic
User Group

discuss.elastic.co