

Elastic Stack Overview

Search. Observe. Protect.

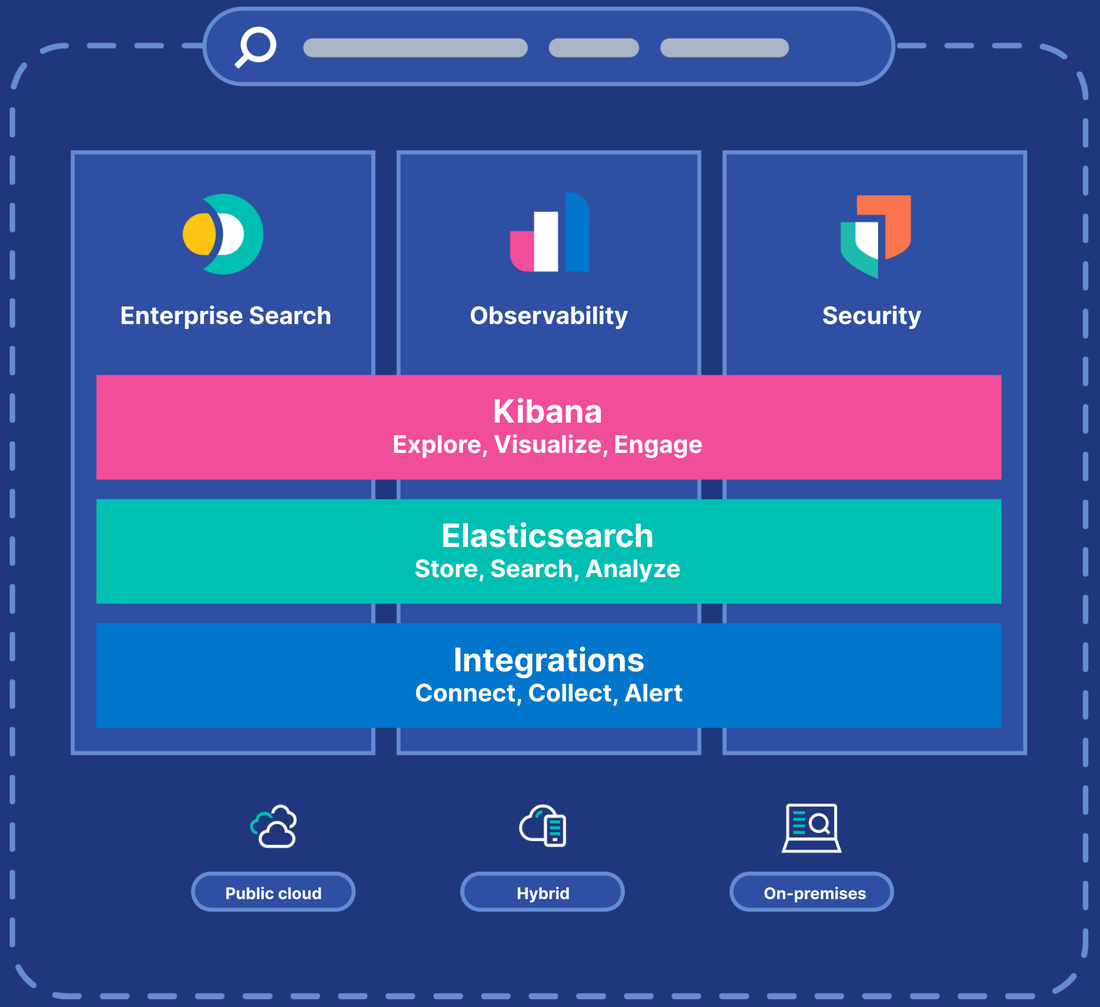
leboncoin

Who?

```
$ curl http://localhost:9200/speaker/_doc/dpilato
{
  "name" : "David Pilato",
  "jobs" : [
    { "name" : "SRA Europe (SSII)", "date" : "1995" },
    { "name" : "SFR", "date" : "1997"  },
    { "name" : "e-Brands / Vivendi", "date": "2000" },
    { "name" : "DGDDI (douane)", "date" : "2005" },
    { "name" : "elastic", "date" : "2013" }
  ],
  "motivations" : [ "family", "job", "deejay" ],
  "blog" : "http://david.pilato.fr/",
  "twitter" : [ "@dadoonet", "@elasticfr" ],
  "email" : "david@pilato.fr"
}
```

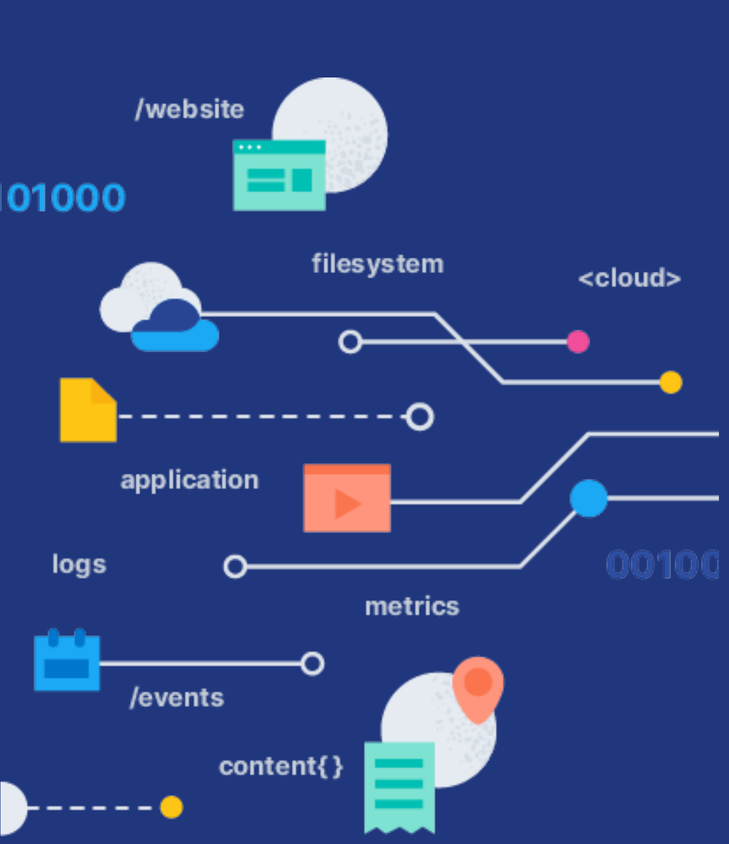
elastic

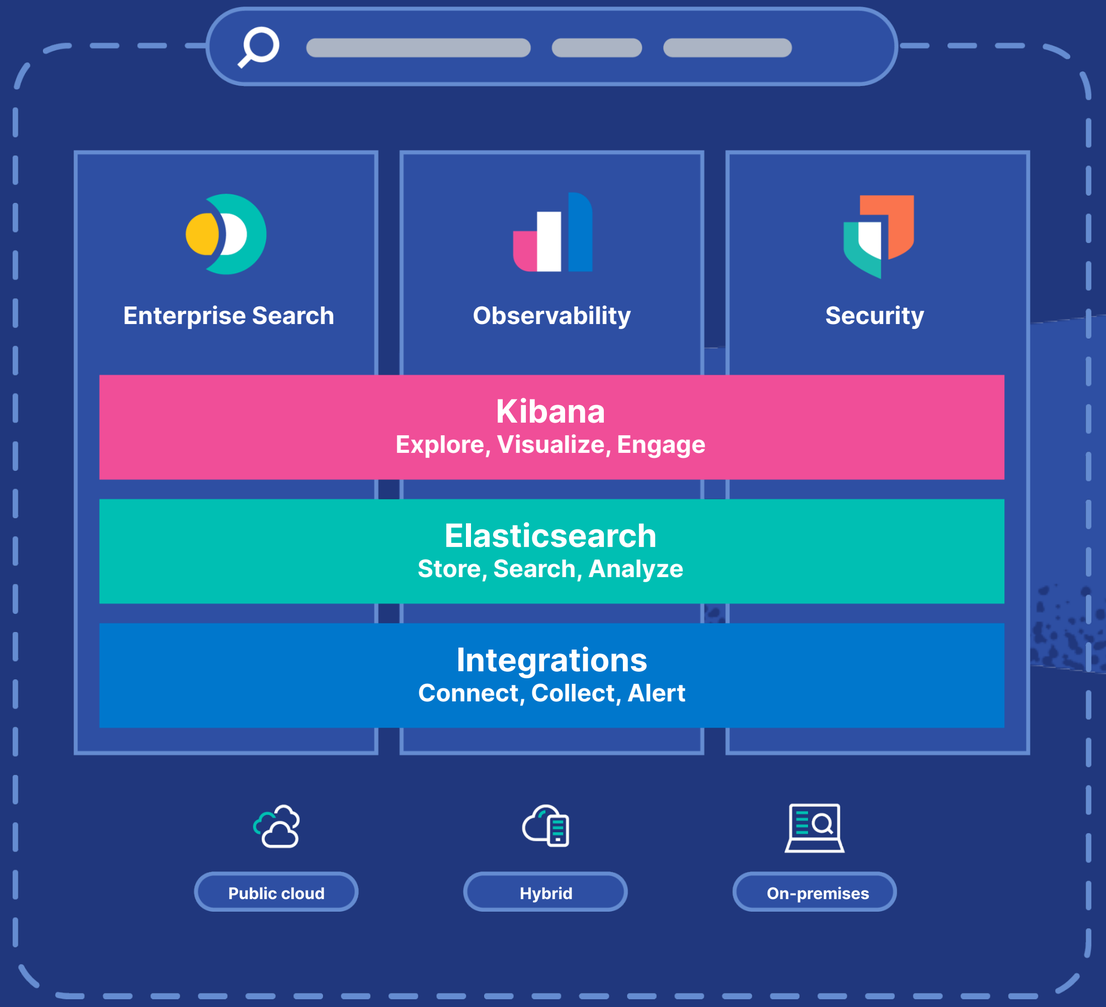
The Elastic Search Platform



elastic

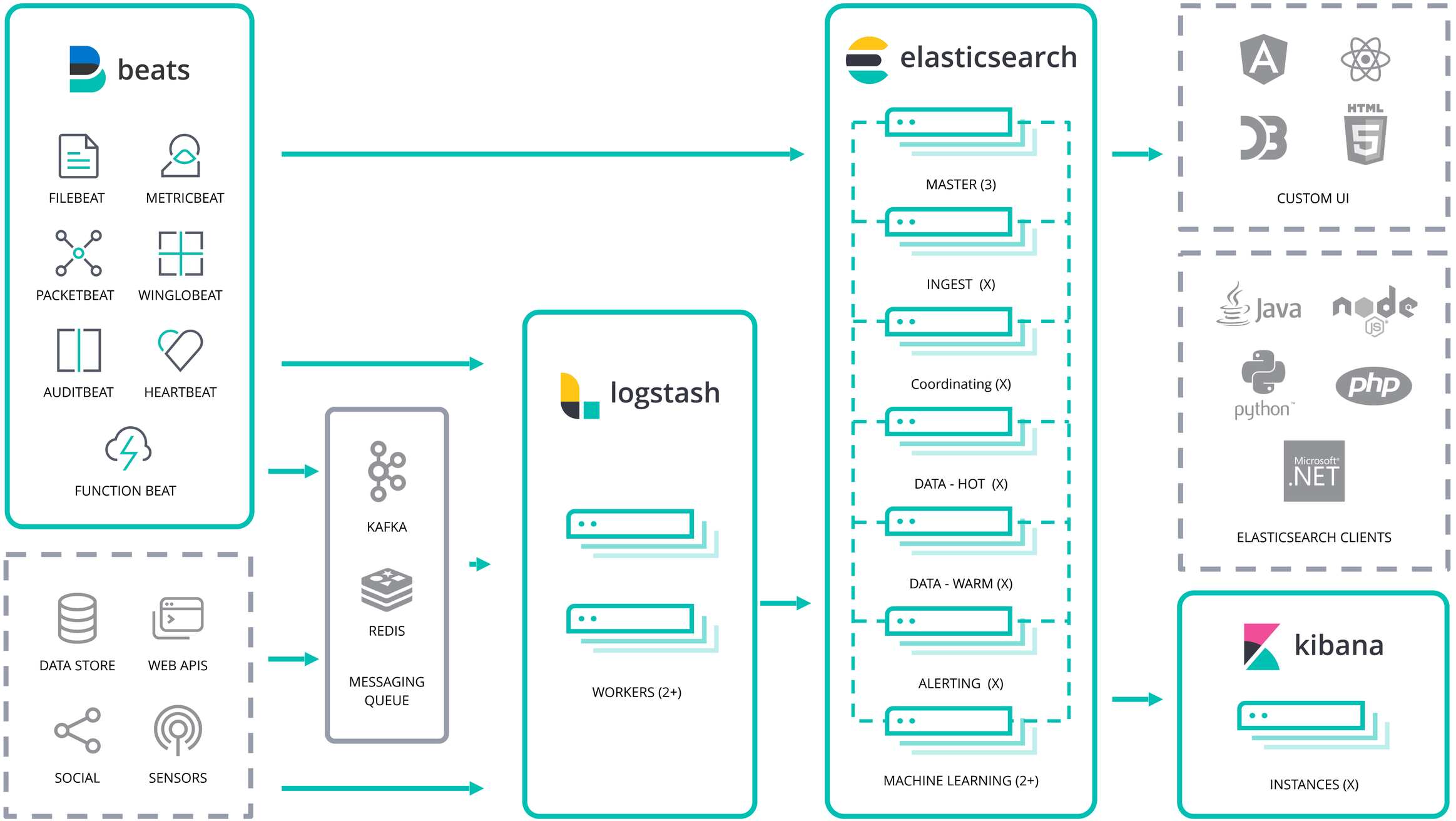
The Elastic Search Platform







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)

Elastic pricing

The best way to consume Elastic is Elastic Cloud, a public cloud managed service available on major cloud providers. Customers who want to manage the software themselves, whether on public, private, or hybrid cloud, can download the Elastic Stack.

Try free | Estimate your costs

Standard

A great place to start

- Core Elastic Stack features, including security
- Kibana Lens, Elastic Maps, and Canvas
- Alerting and in-stack Actions

SECURITY

- Alerting including detection engine and prebuilt rules for SIEM and endpoint

Gold

Everything in Standard plus:

- Reporting
- Third-party Alerting Actions
- Watcher[2]
- Multi-stack monitoring

SECURITY

- Optimized workflows including third-party incident response workflows

Platinum

Everything in Gold plus:

- Advanced Elastic Stack security features
- Machine learning - anomaly detection, supervised learning, 3rd-party model management
- Cross-cluster replication

SECURITY

- Machine learning anomaly detection and prebuilt jobs for SIEM

Enterprise

Everything in Platinum plus:

- Searchable snapshots
- Support for searchable cold and frozen tiers
- Elastic Maps Server

SECURITY

- Searchable snapshots for longer retention of security-related data

Free Elastic training

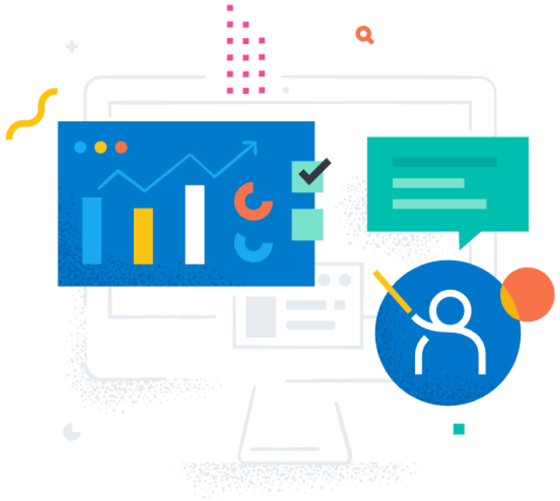
Start your Elastic journey and become an expert faster than ever — for free. Build your enterprise search, observability, security, and Elastic Stack skills with our on-demand training.

Quick Starts

Not sure where to start with Elastic? Start here. Our Quick Start guides will have you in your own Elastic Cloud cluster exploring data sets in less than 15 minutes.

- Logging Quick Start
- Metrics Quick Start
- APM Quick Start
- Workplace Search Quick Start
- App Search Quick Start
- App Search web crawler Quick Start
- Elastic Security Quick Start
- User Experience Monitoring Quick Start





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 SPL Users
- Fundamentals of Securing Elasticsearch
- Elastic Security Fundamentals: SIEM
- Elastic Endgame Fundamentals
- Anomaly Detection for Cybersecurity
- ECE Fundamentals

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 Doctolib');
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 Doctolib');
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 Doctolib');
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 Doctolib  |
| 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 Doctolib');
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 Doctolib');
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 Doctolib');
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 Doctolib');
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 Doctolib
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 Doctolib');
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

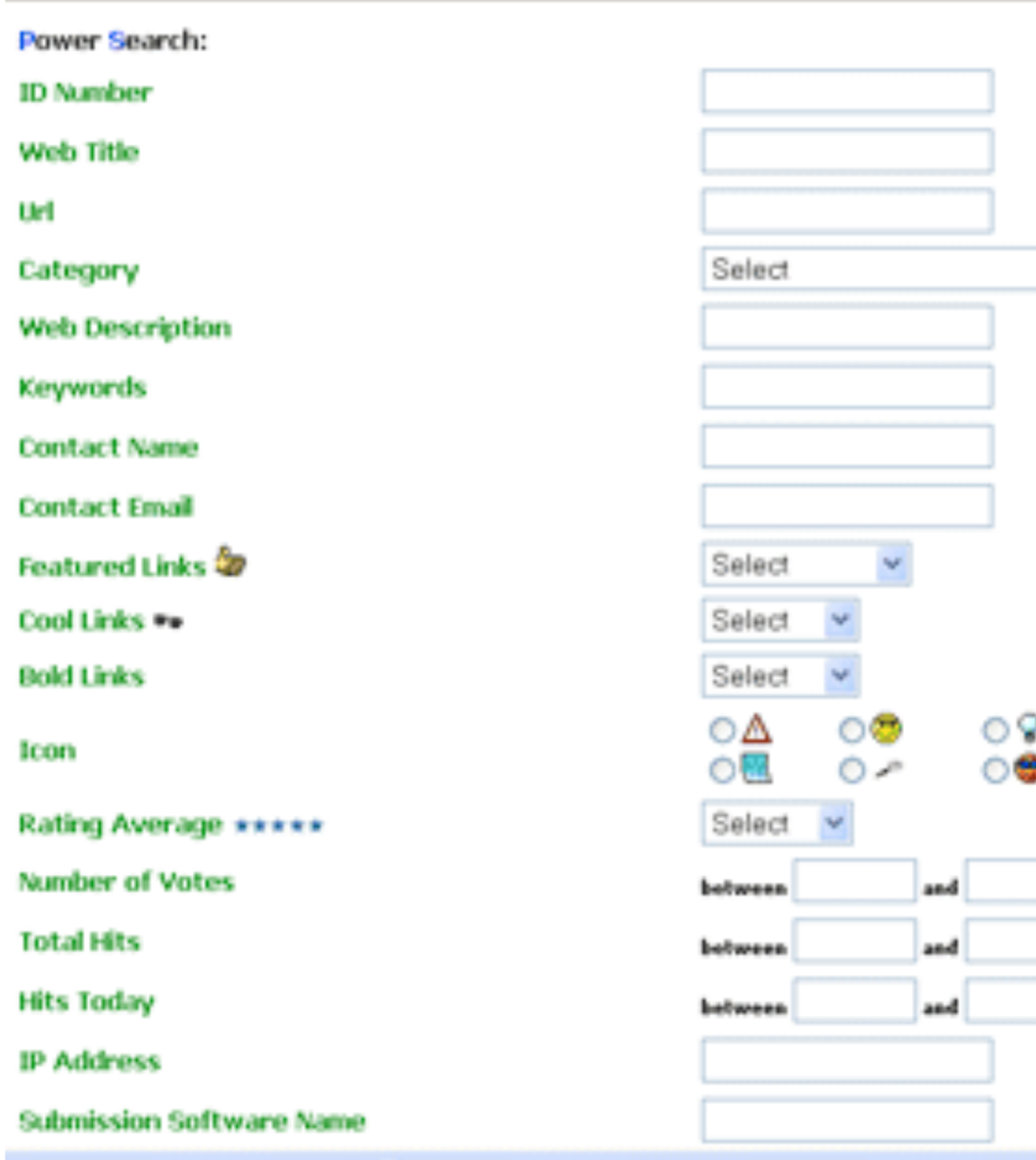
```
INSERT INTO user VALUES ('David Pilato', 'Developer at elastic');
INSERT INTO user VALUES ('Malloum Laya', 'Worked with David at
french customs service');
INSERT INTO user VALUES ('David Gageot', 'Engineer at Doctolib');
INSERT INTO user VALUES ('David David', 'Who is that guy?');
```

```
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 Doctolib
David David	Who is that guy?

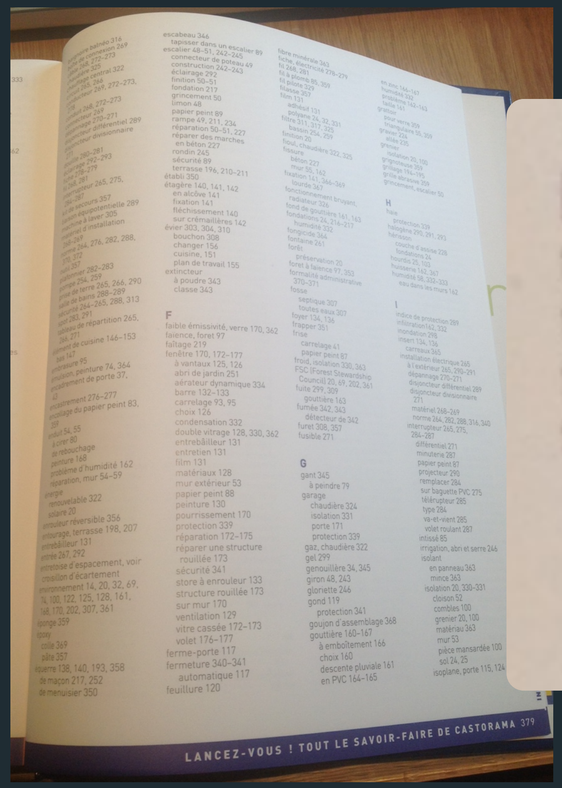


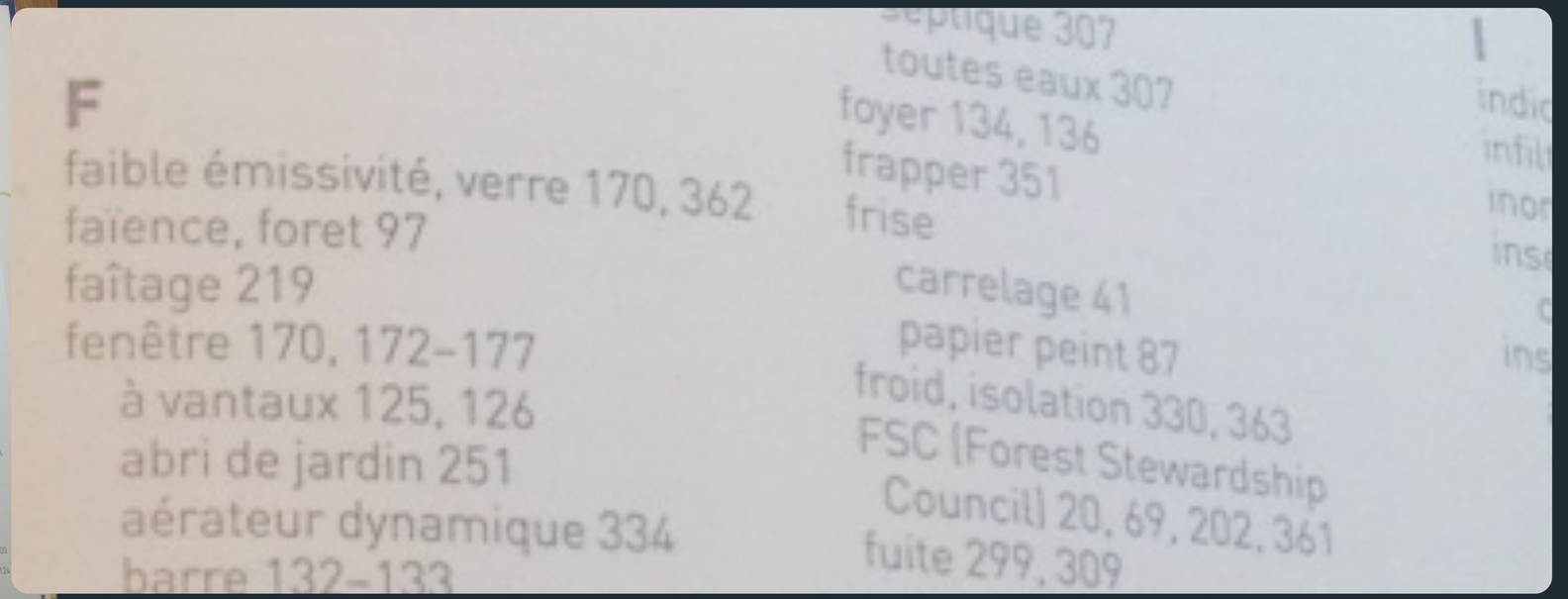
User Interface



What is a search engine?

Index engine (indexing documents)





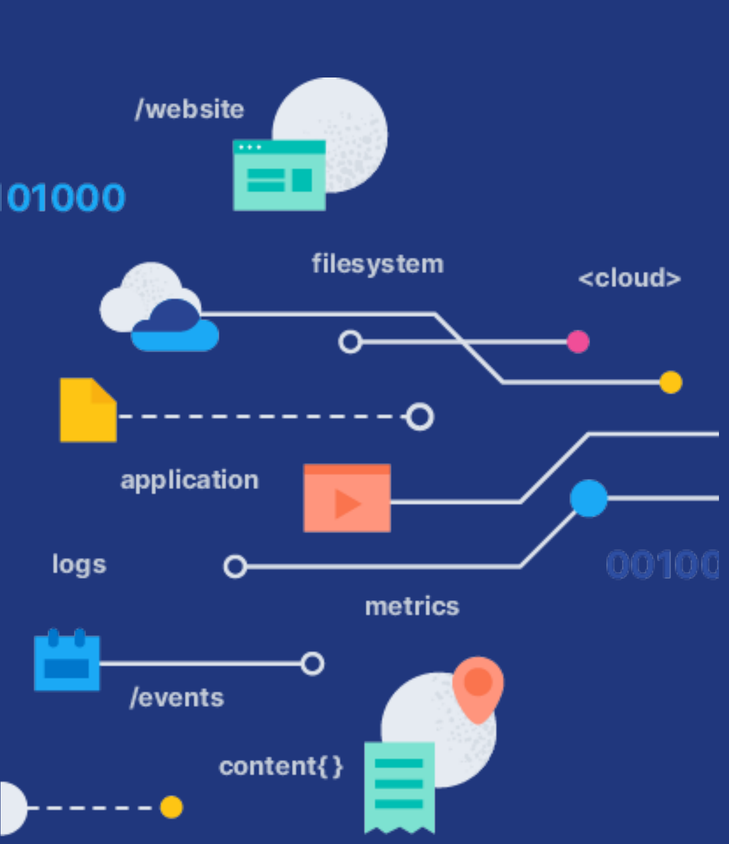
Search engine (within the created indices)

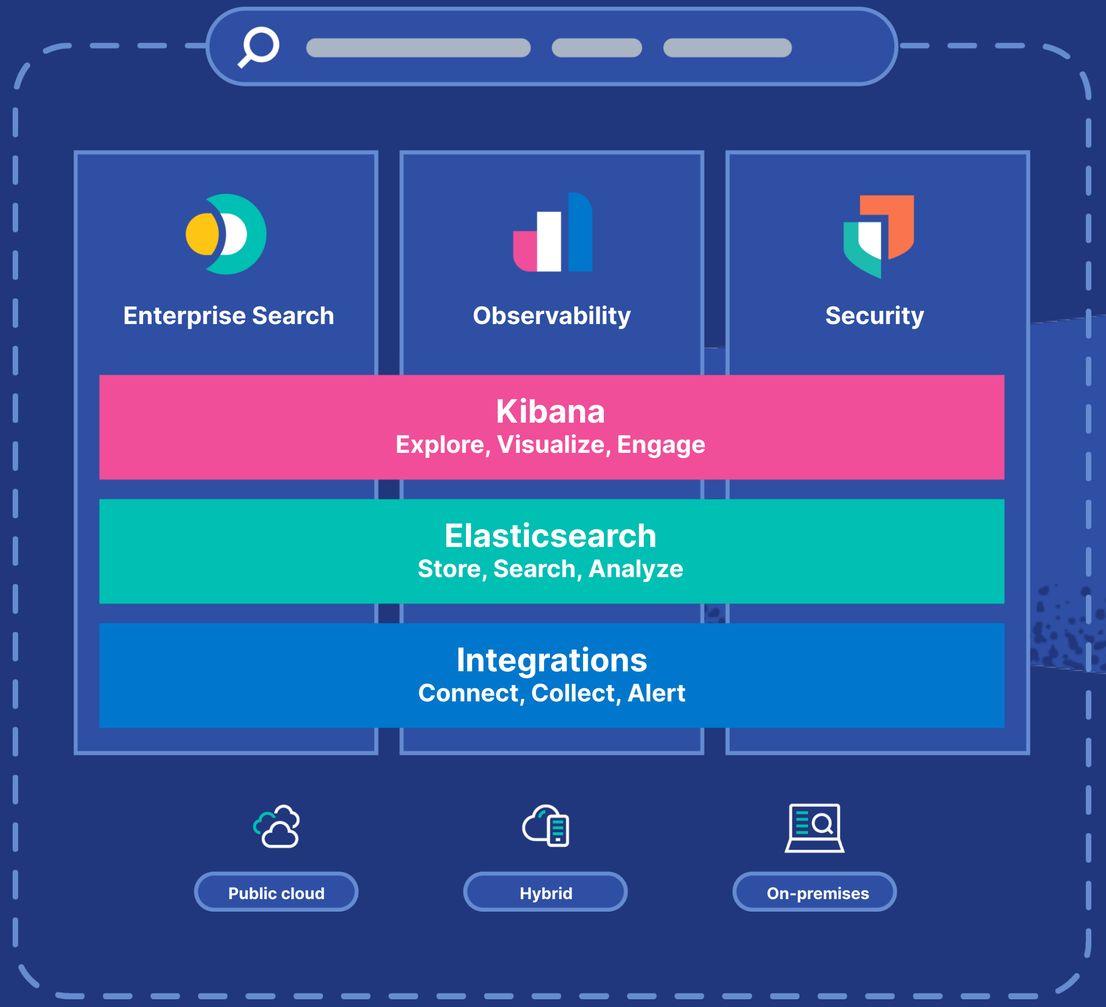
elastic

Demo time!



The Elastic Search Platform





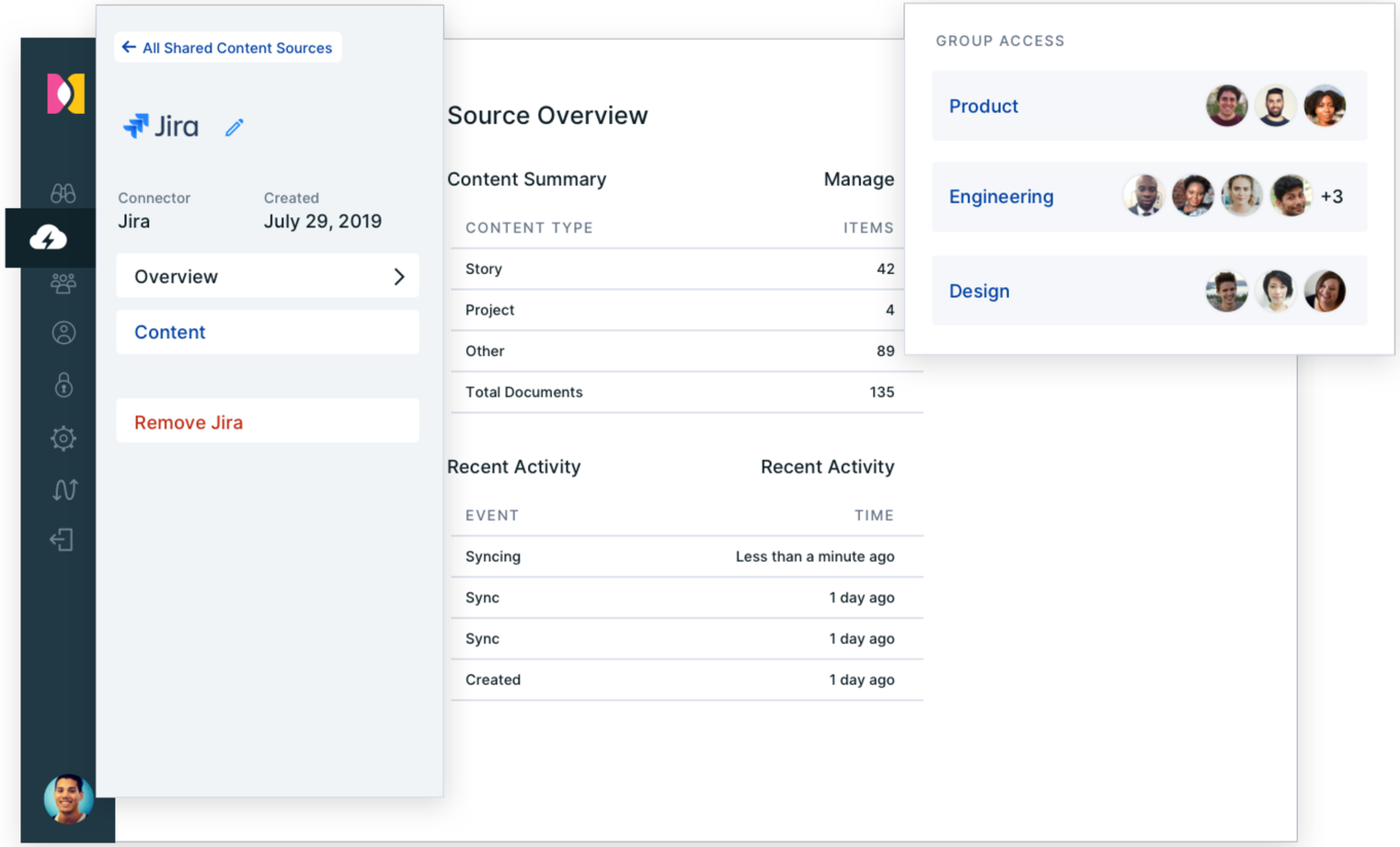


elastic

ELASTIC ENTERPRISE SEARCH

Search everything, anywhere

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

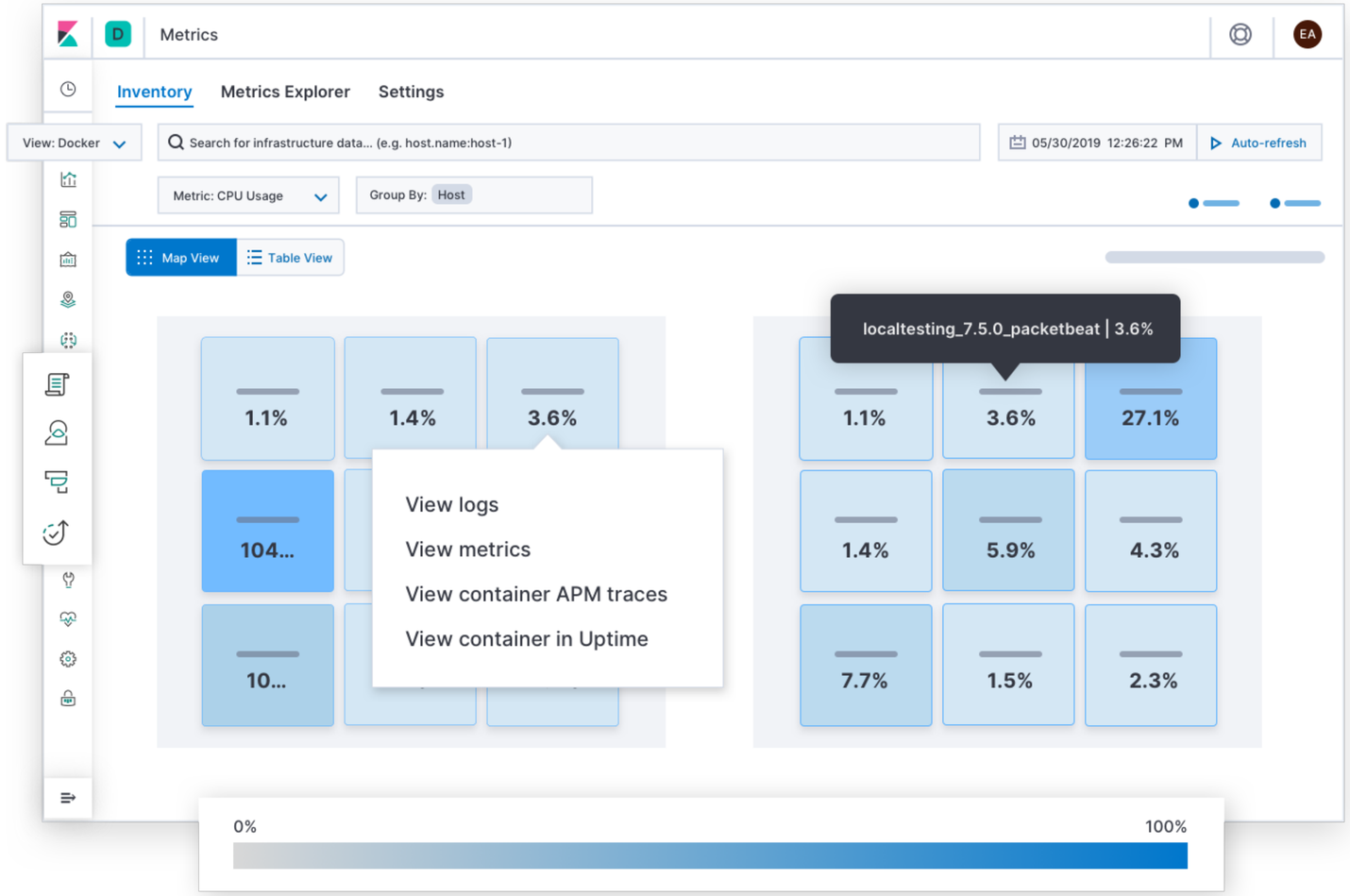


elastic

ELASTIC OBSERVABILITY

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.

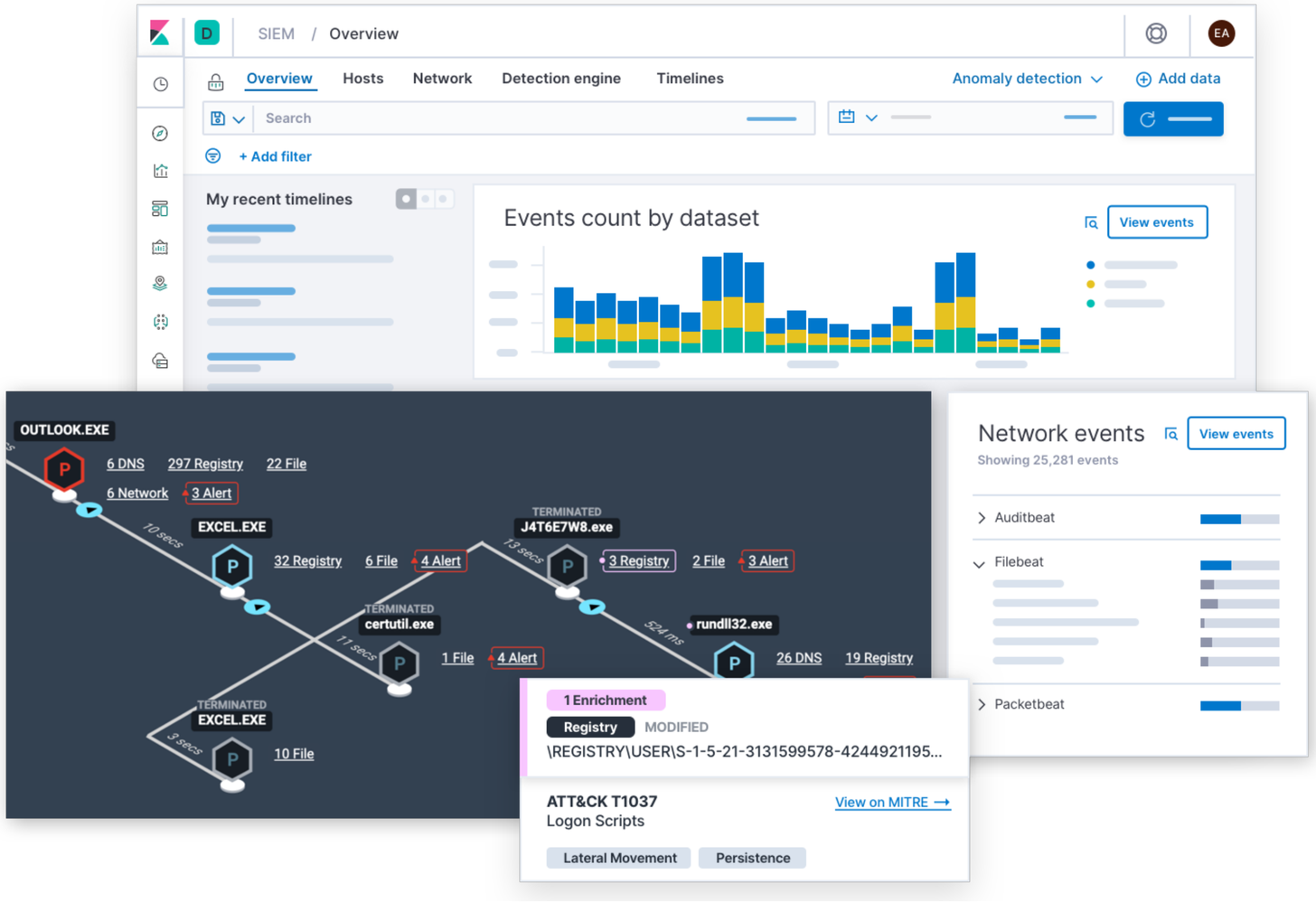


elastic

ELASTIC SECURITY

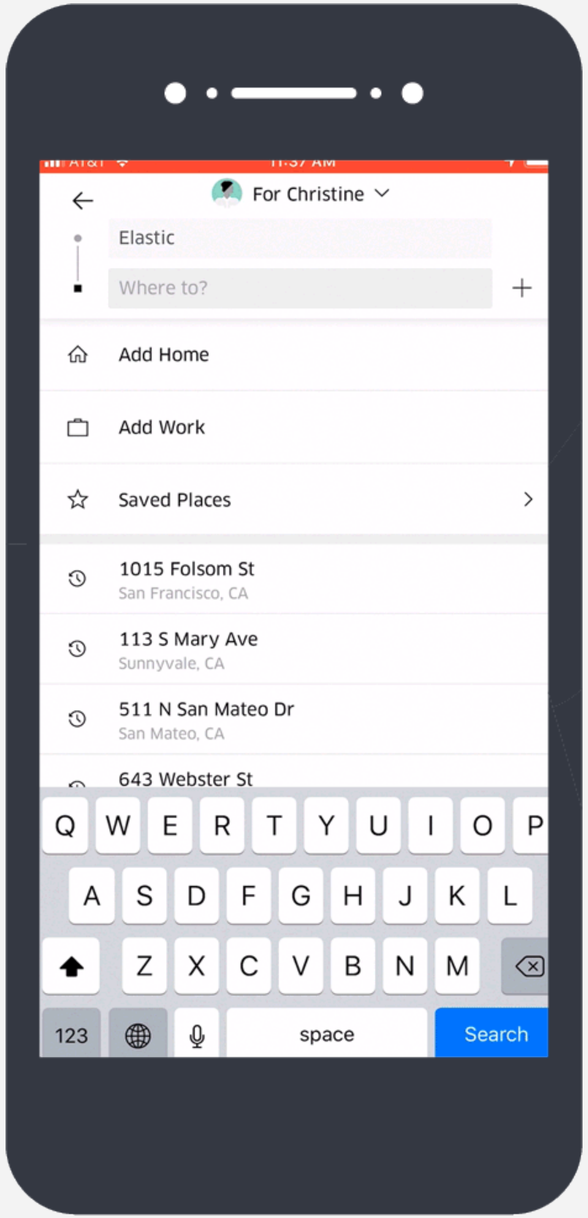
Security how it should be: open

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



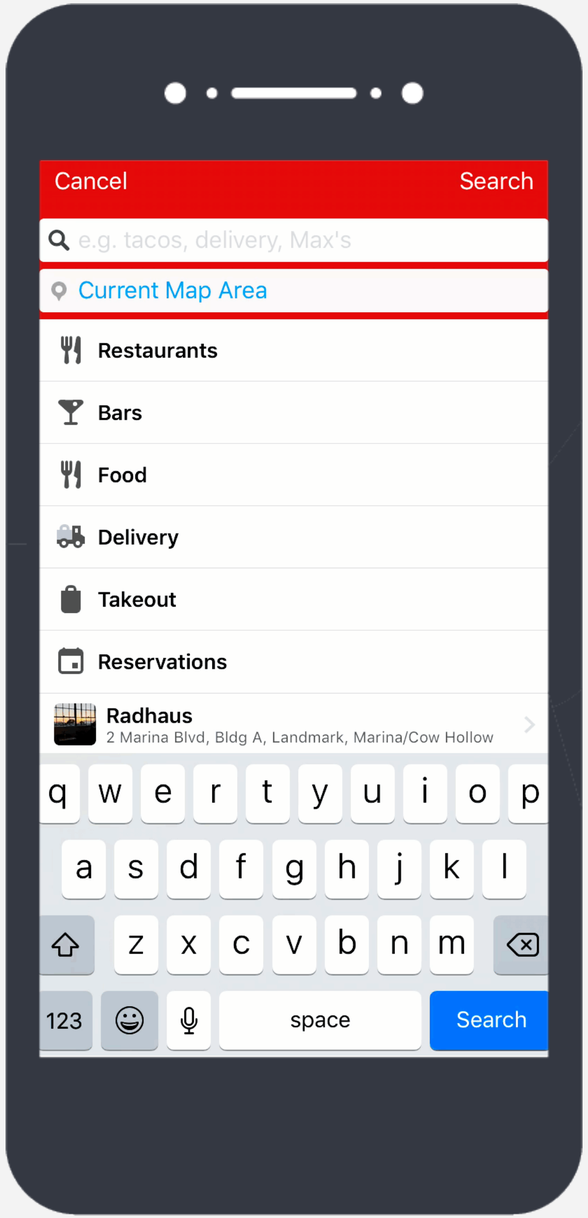
elastic


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
ROBLOX
PayPal
Adobe
CISCO
docker
The Guardian
THOMSON REUTERS
Quora
TOMTOM



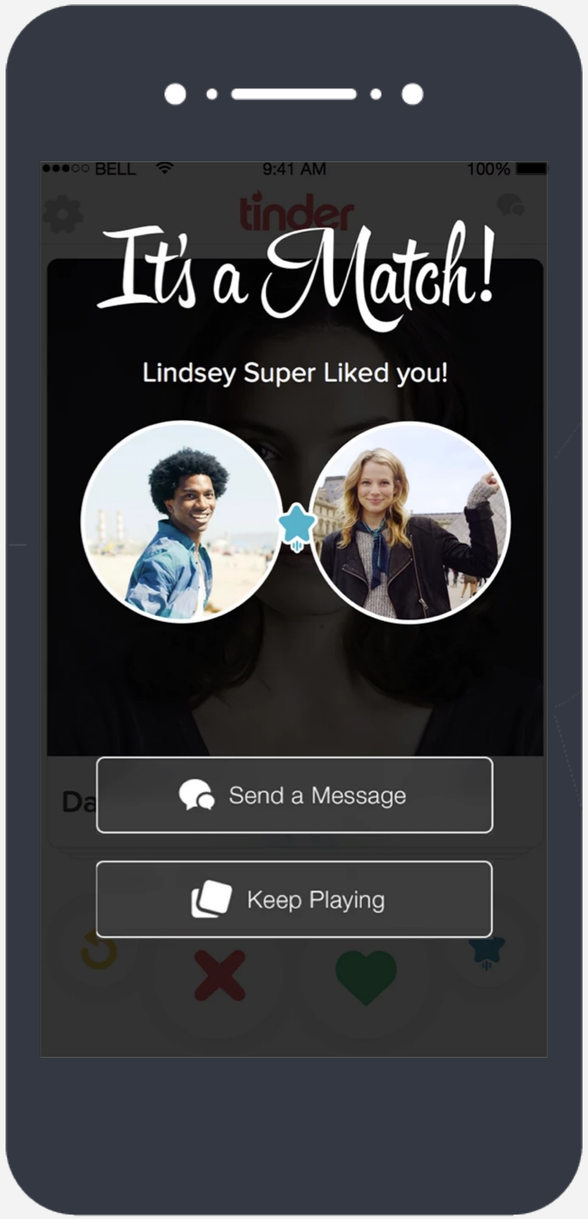
Searching for **Rides**

elastic



Searching for **Restaurants**

elastic

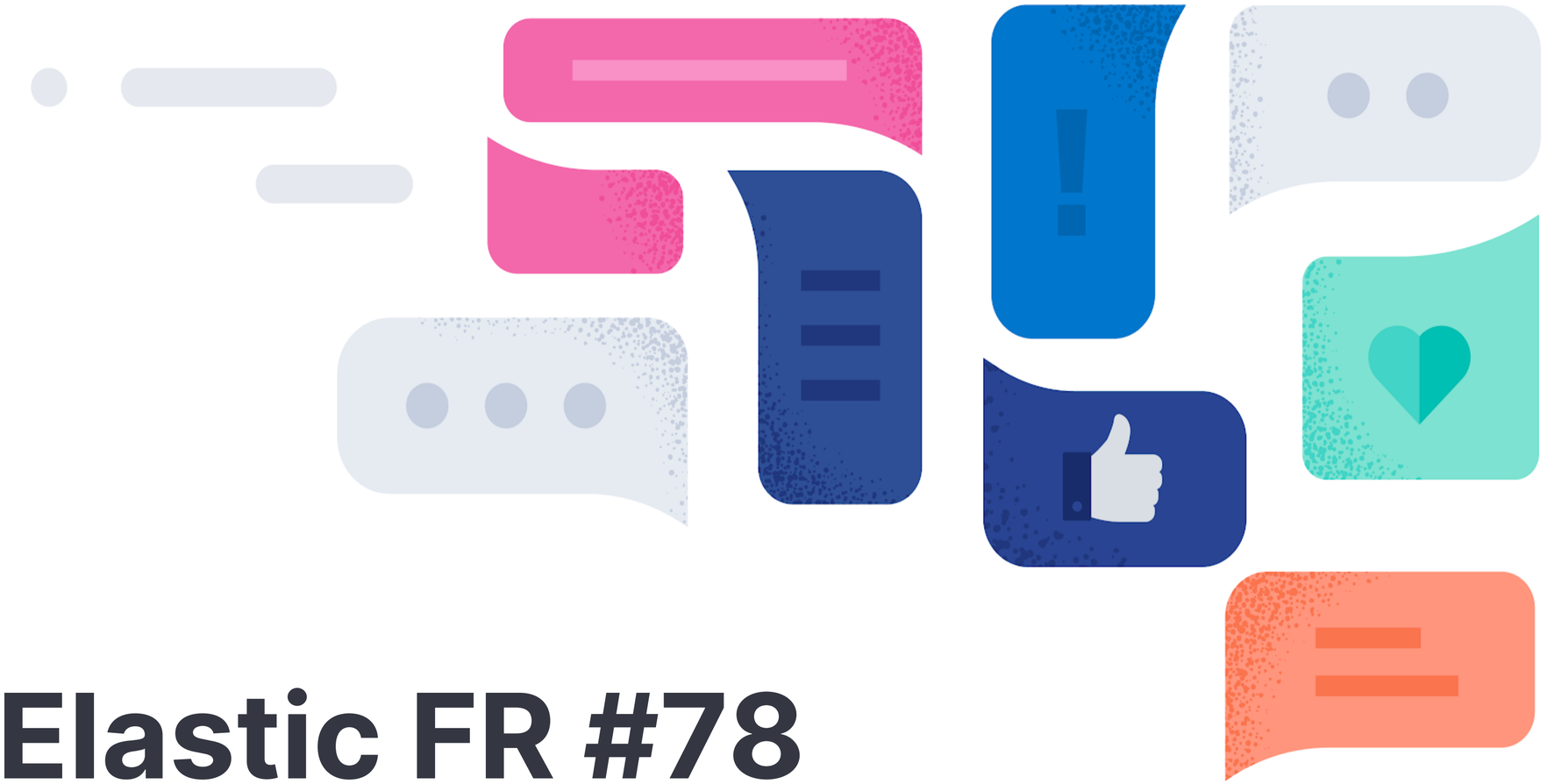


Searching for **Love**

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 TELEREALITE
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
1805
PICTET
REGIONSJOB
saur
MACSF
fotolia
by Adobe
orange
meetic
SOCIETE GENERALE
FIGARO immo
OVH.com
SeLoger
BANQUE DE FRANCE
EUROSYSTÈME
Carrefour
CADREMPLOI
Alcatel·Lucent
118 218
DEEZER
CANAL+
arjel
Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE
viadeo
AXA
GBIF
Global Biodiversity Information Facility

elastic



Meetup Elastic FR #78

leboncoin à partir de 19h
85 Rue du Faubourg Saint-Martin
75010 Paris

leboncoin

elastic

leboncoin

Mehdi Boissat-Bron, Développeur

Utilisation des datastreams chez leboncoin



- 13/09/2022 à partir de 19:00
- leboncoin

85 Rue du Faubourg Saint-Martin
75010 Paris

elastic

adyen

Sanchit Bhatnagar, Java Backend Developer

Improving User Search Experience using Elasticsearch at Adyen



- 13/09/2022 à partir de 19:00
- leboncoin

85 Rue du Faubourg Saint-Martin
75010 Paris

elastic

VESTIAIRE COLLECTIVE

Bader Ben Dhifallah, Senior Backend Developer

Elasticsearch percolator : dans la direction opposée

- 13/09/2022 à partir de 19:00
- leboncoin

85 Rue du Faubourg Saint-Martin
75010 Paris



Elastic France
https://community.elastic.co/france/

@elasticfr

elastic
User Group

discuss.elastic.co

