Elastic Stack Overview

Search. Observe. Protect.

ankor store

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" : "https://david.pilato.fr/",
  "twitter" : [ "@dadoonet", "@elasticfr" ],
  "email" : "david@pilato.fr"
}
```

elastic

The Elastic Search Platform

Out of the Box Solutions

Observability

Logs, APM, Tracing, Metrics, Synthetics, Profiling, RUM

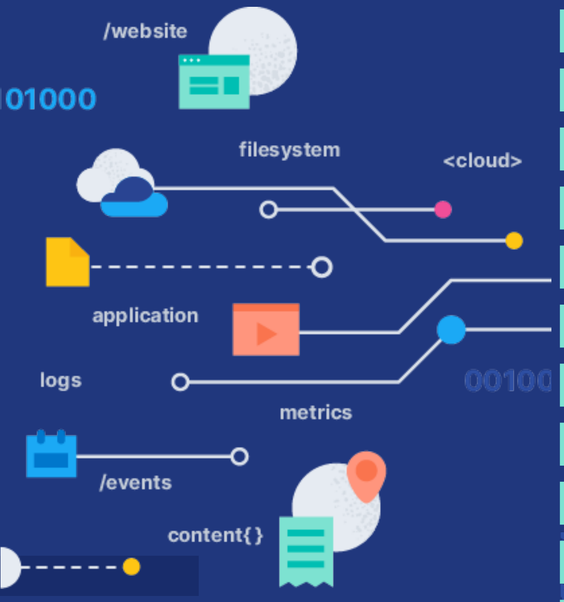
Security

SIEM, Endpoint, Cloud

Build Your Own

Search

Product Search, Workplace Search, Business Analytics, Custom Search Apps



Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

Integrations
Connect, Collect, Alert

ESRE™
Elasticsearch Relevance Engine™

elastic

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

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

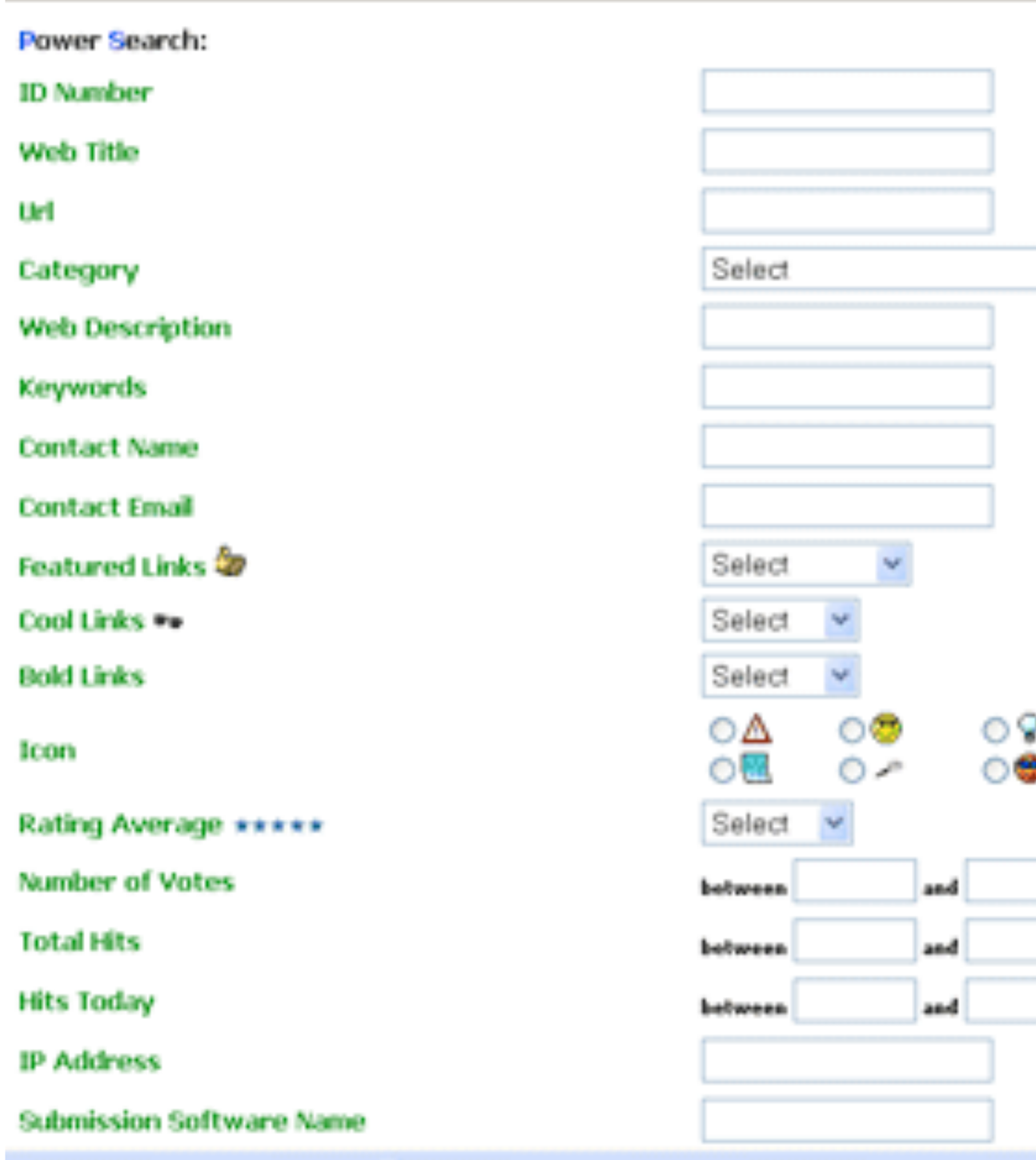
Search with typos

```
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_%";
```

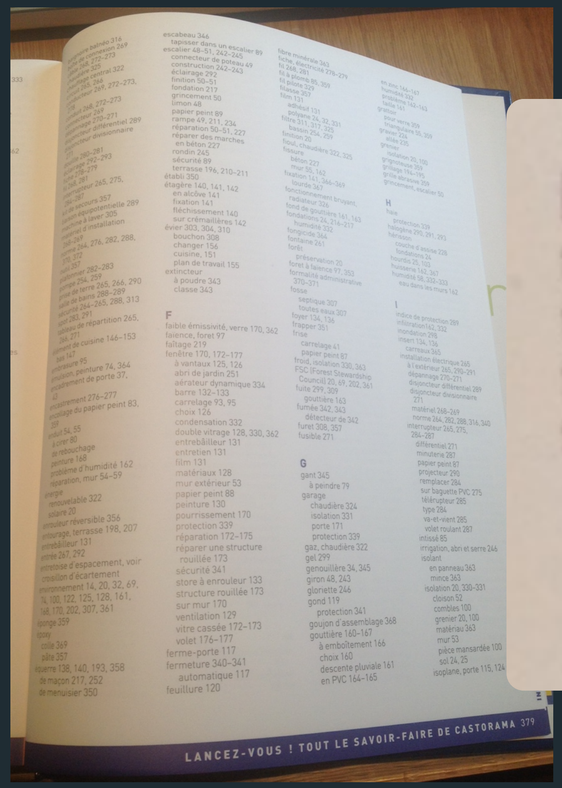
name	comments
David Pilato	Developer at elastic
David Gageot	Engineer at Doctolib
David David	Who is that guy?

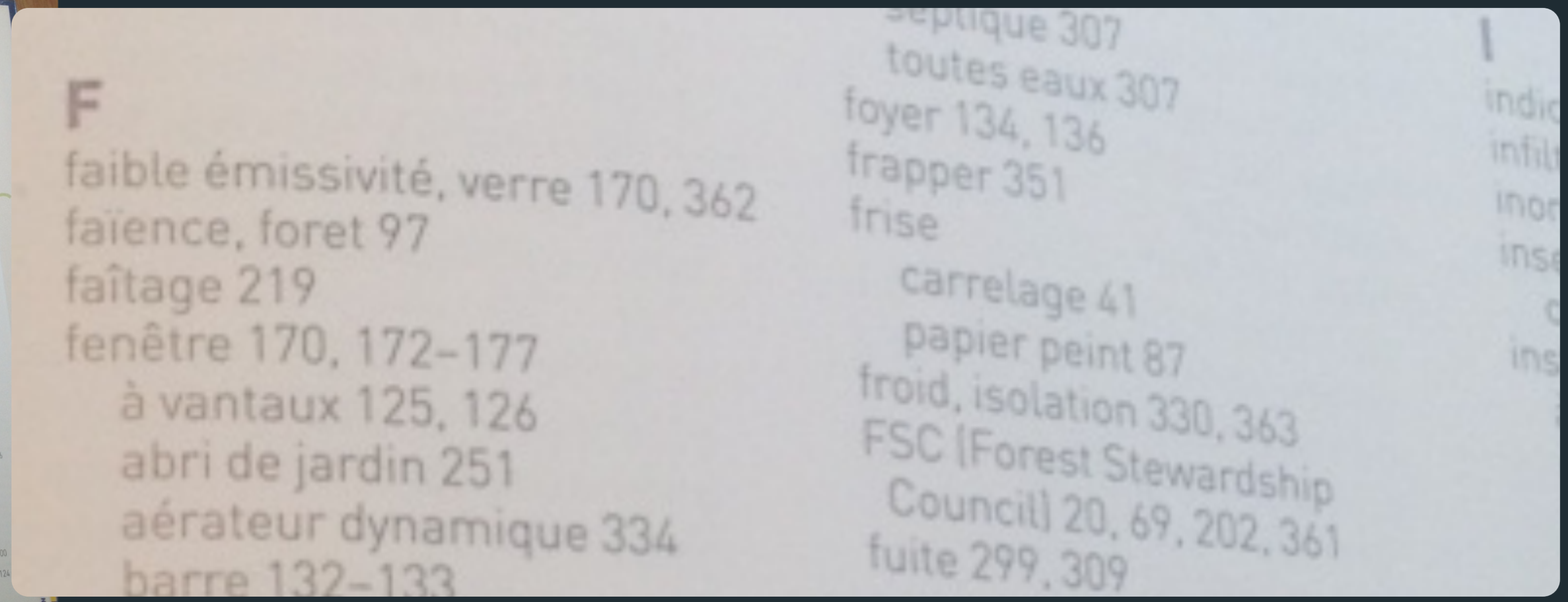
User Interface



What is a search engine?

Index engine (indexing documents)





Search engine (within the created indices)

elastic

Demo time!

The Elastic Search Platform

Out of the Box Solutions

Observability

Logs, APM, Tracing, Metrics, Synthetics, Profiling, RUM

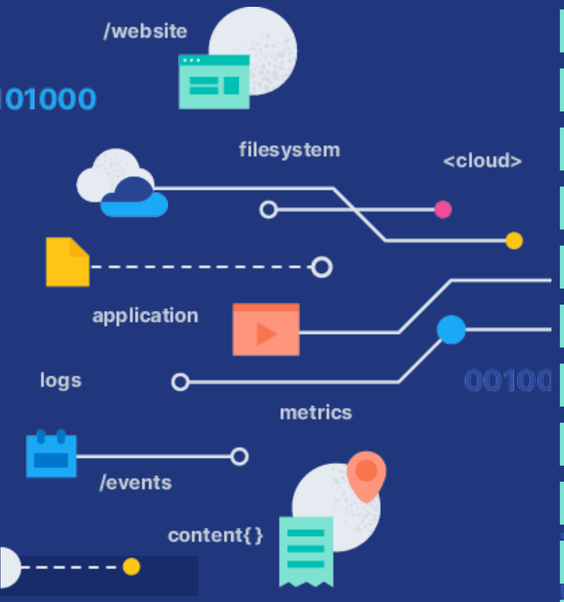
Security

SIEM, Endpoint, Cloud

Build Your Own

Search

Product Search, Workplace Search, Business Analytics, Custom Search Apps



Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

Integrations
Connect, Collect, Alert

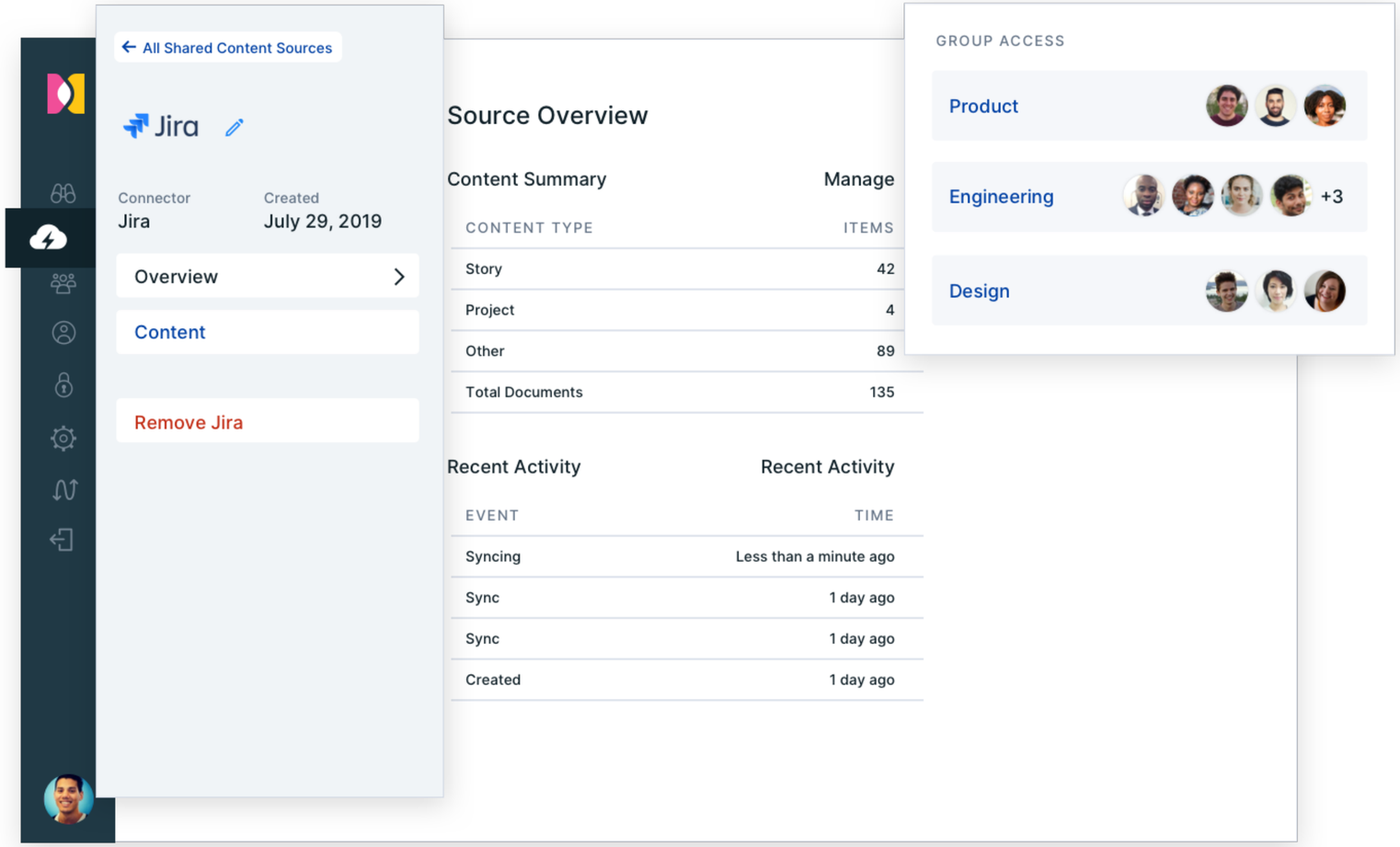
ESRE™
Elasticsearch Relevance Engine™

elastic

ELASTIC ENTERPRISE SEARCH

Search everything, anywhere

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

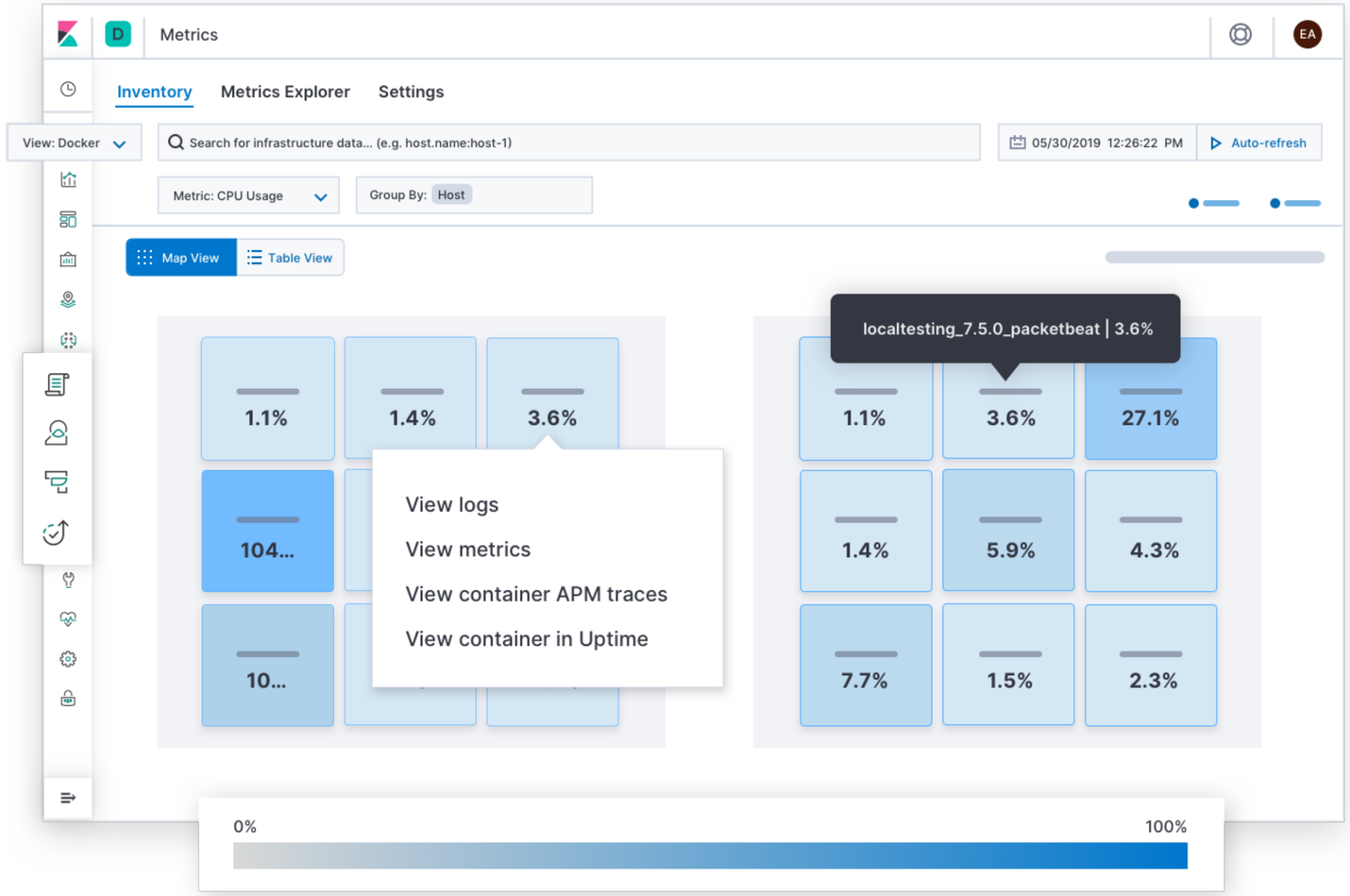


elastic

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.

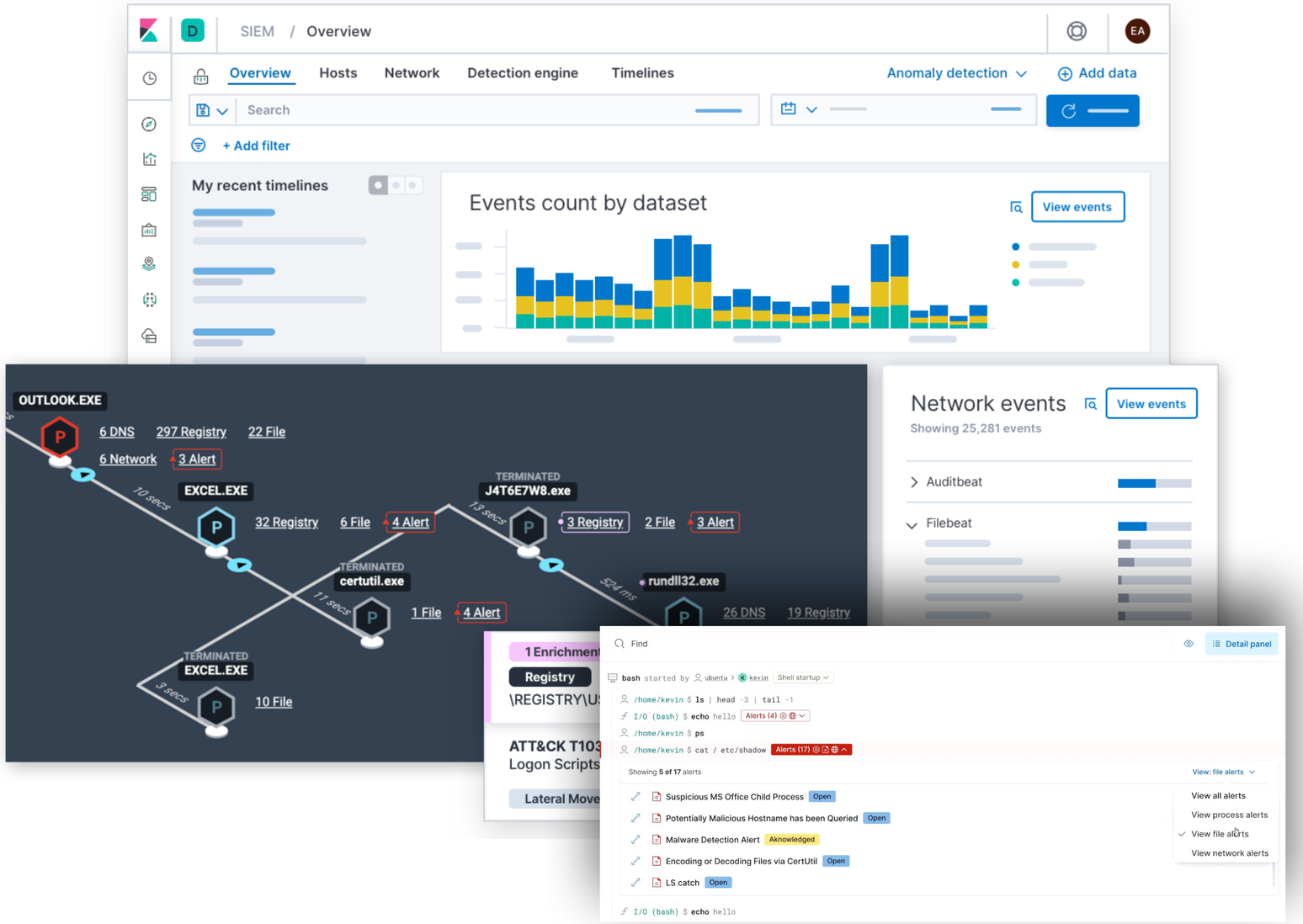


elastic

ELASTIC SECURITY

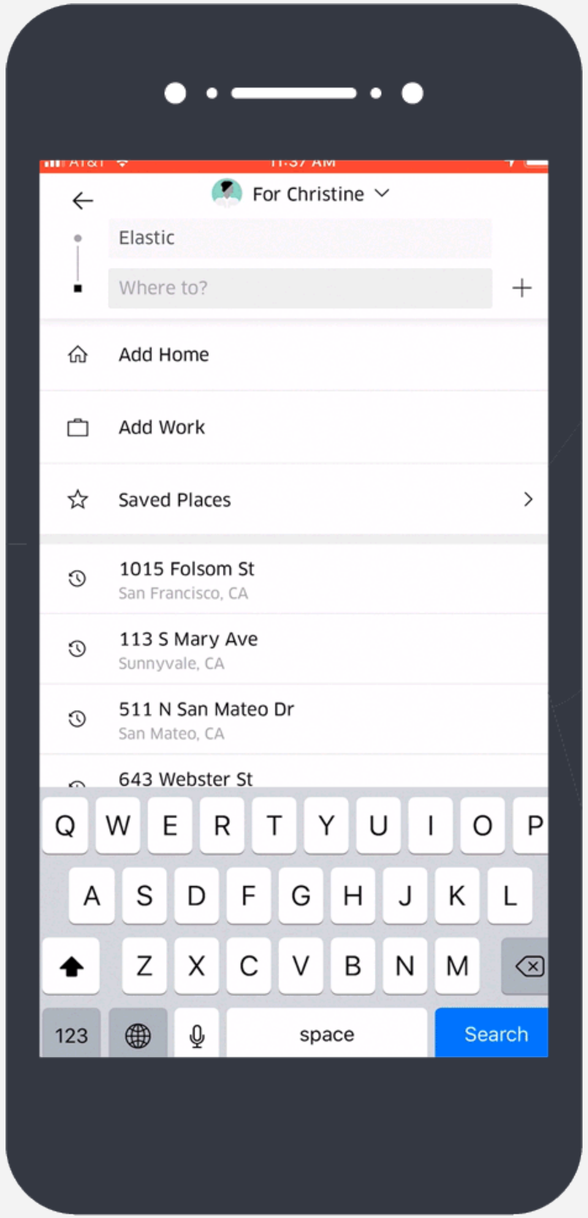
Security how it should be: open

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



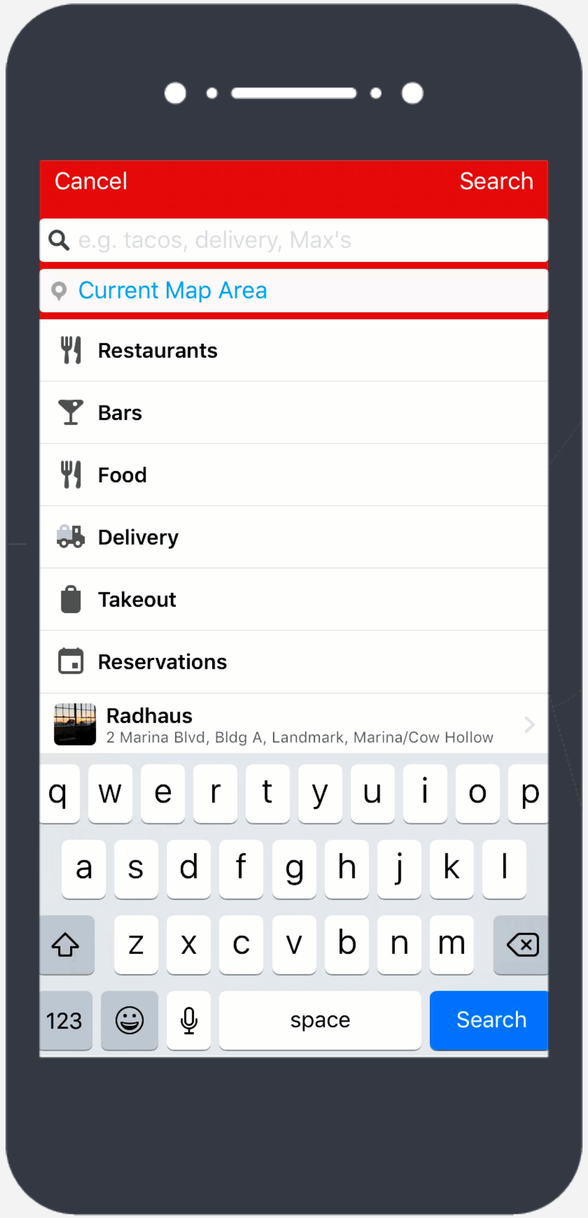
elastic


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



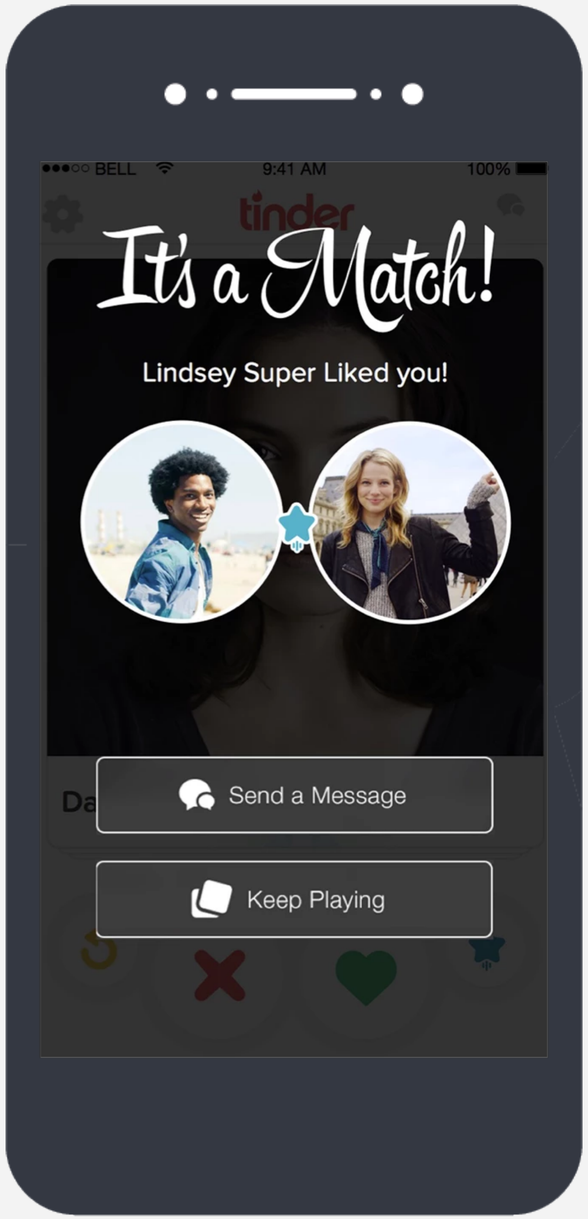
Searching for **Rides**

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

www.meetup.com/ElasticFR

@elastic

elastic
User Group

discuss.elastic.co