



Elastic Stack Overview

Search. Observe. Protect.

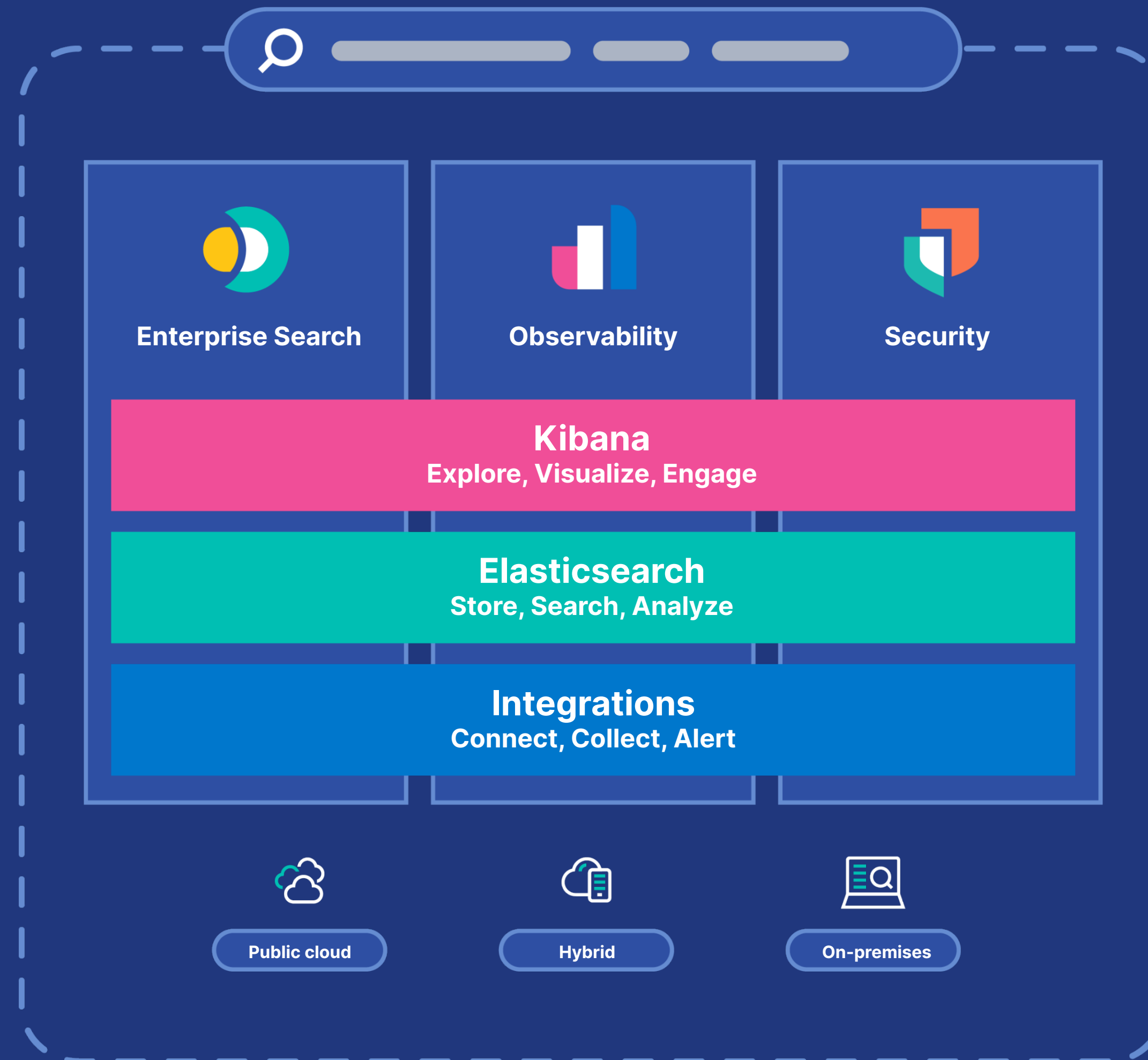


golumoi

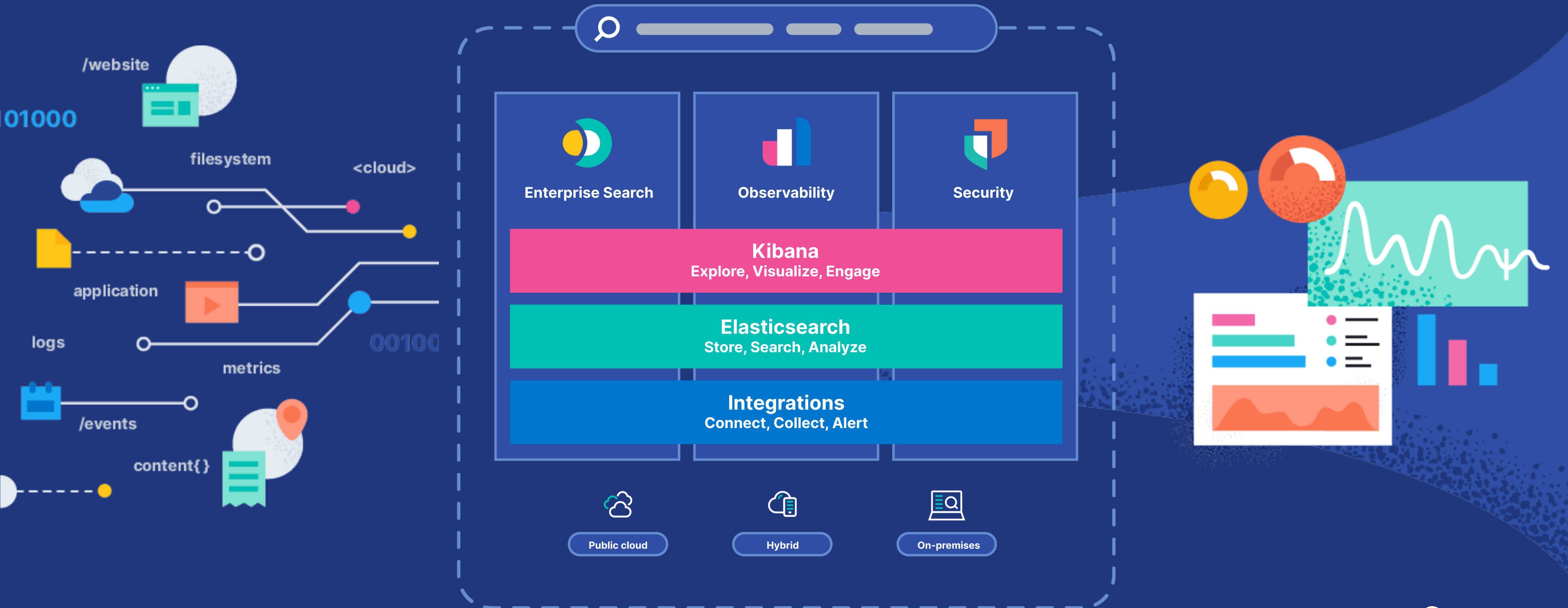
Who?

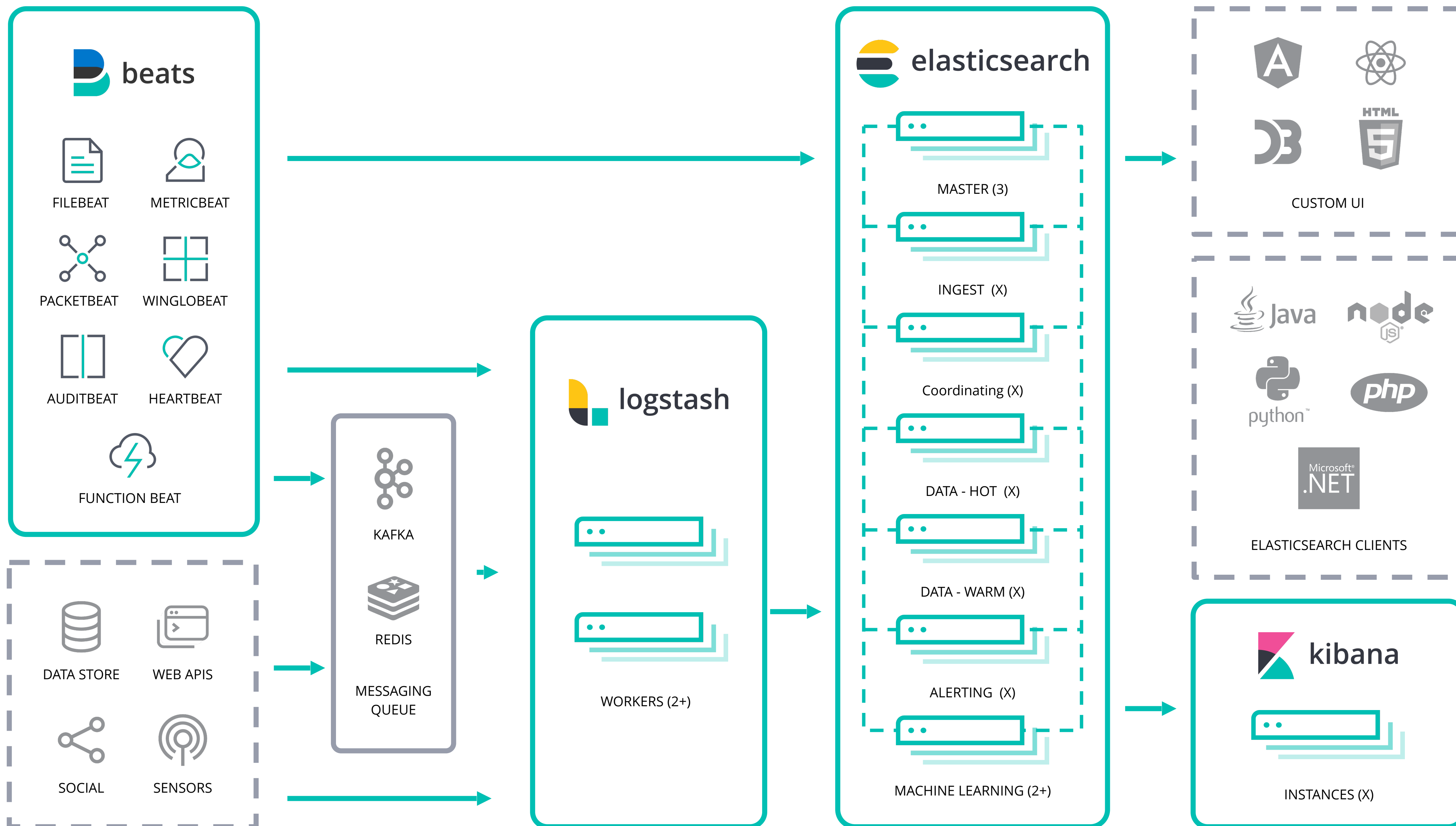
```
$ curl http://localhost:9200/speaker/_doc/dpilato
{
  "name" : "David Pilato",
  "jobs" : [
    { "name" : "SRA Europe (SSII)", "date" : "1995" },
    { "name" : "SFR", "date" : "1997" },
    { "name" : "e-Brands / Vivendi", "date" : "2000" },
    { "name" : "DGDDI (douane)", "date" : "2005" },
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

The Elastic Search Platform



The Elastic Search Platform





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
- ✔ Watcher²
- ✔ 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.

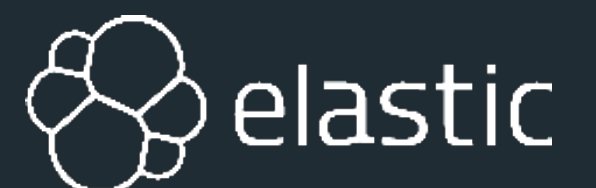
- [Observability Fundamentals](#)
- [Introduction to Observability: Logging](#)
- [Metrics Fundamentals](#)
- [APM Fundamentals](#)
- [Kibana Fundamentals](#)
- [Kibana for SPL Users](#)
- [Fundamentals of Securing Elasticsearch](#)
- [Elastic Security Fundamentals: SIEM](#)
- [Elastic Endgame Fundamentals](#)
- [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?');
```

David



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)
```



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?

David

Q



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

David Pilato



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)



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

Pilato David



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?





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)
```



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

Power Search:

ID Number

Web Title

Url

Category

Web Description

Keywords

Contact Name

Contact Email

Featured Links 🏆

Cool Links 🌟

Bold Links

Icon

Rating Average ★★★★★

Number of Votes

Total Hits

Hits Today

IP Address

Submission Software Name

Select

Select

Select

Select

☐ ⚠ ☐ 😬 ☐ 💡
☐ 📄 ☐ 🔍 ☐ 🌐

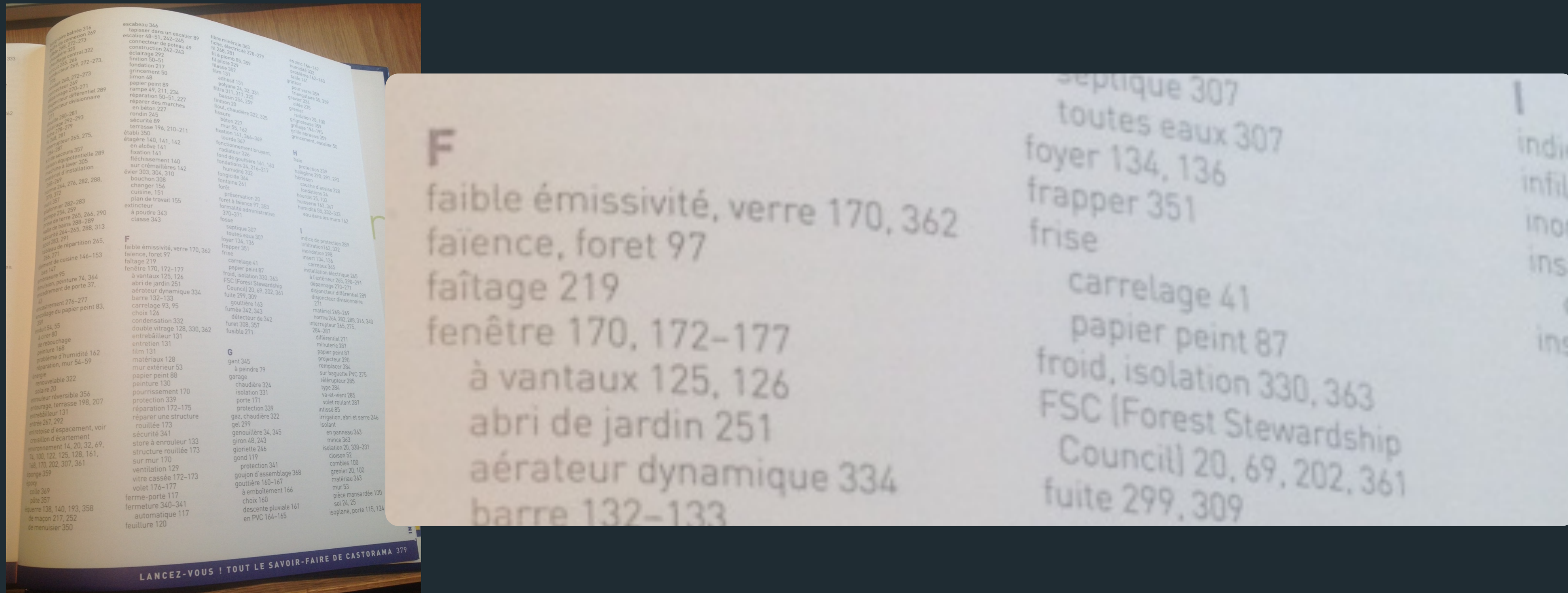
Select

between and

between and

between and

Index engine (indexing documents)



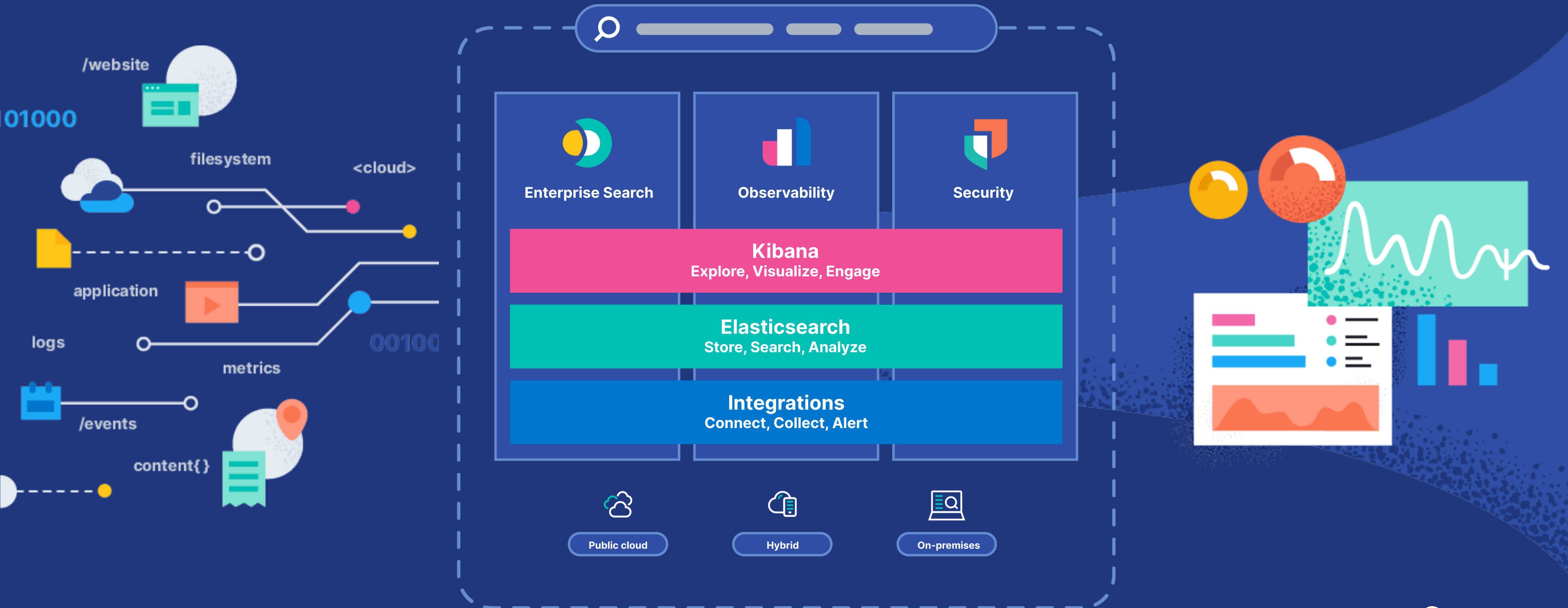
Search engine (within the created indices)

Demo time!



4GIFs.com

The Elastic Search Platform





Search everything, anywhere

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

← All Shared Content Sources

Jira

Connector Jira Created July 29, 2019

Overview >

Content

Remove Jira

Source Overview

Content Summary

Manage

CONTENT TYPE	ITEMS
Story	42
Project	4
Other	89
Total Documents	135

Recent Activity

Recent Activity

EVENT	TIME
Syncing	Less than a minute ago
Sync	1 day ago
Sync	1 day ago
Created	1 day ago

GROUP ACCESS

Product

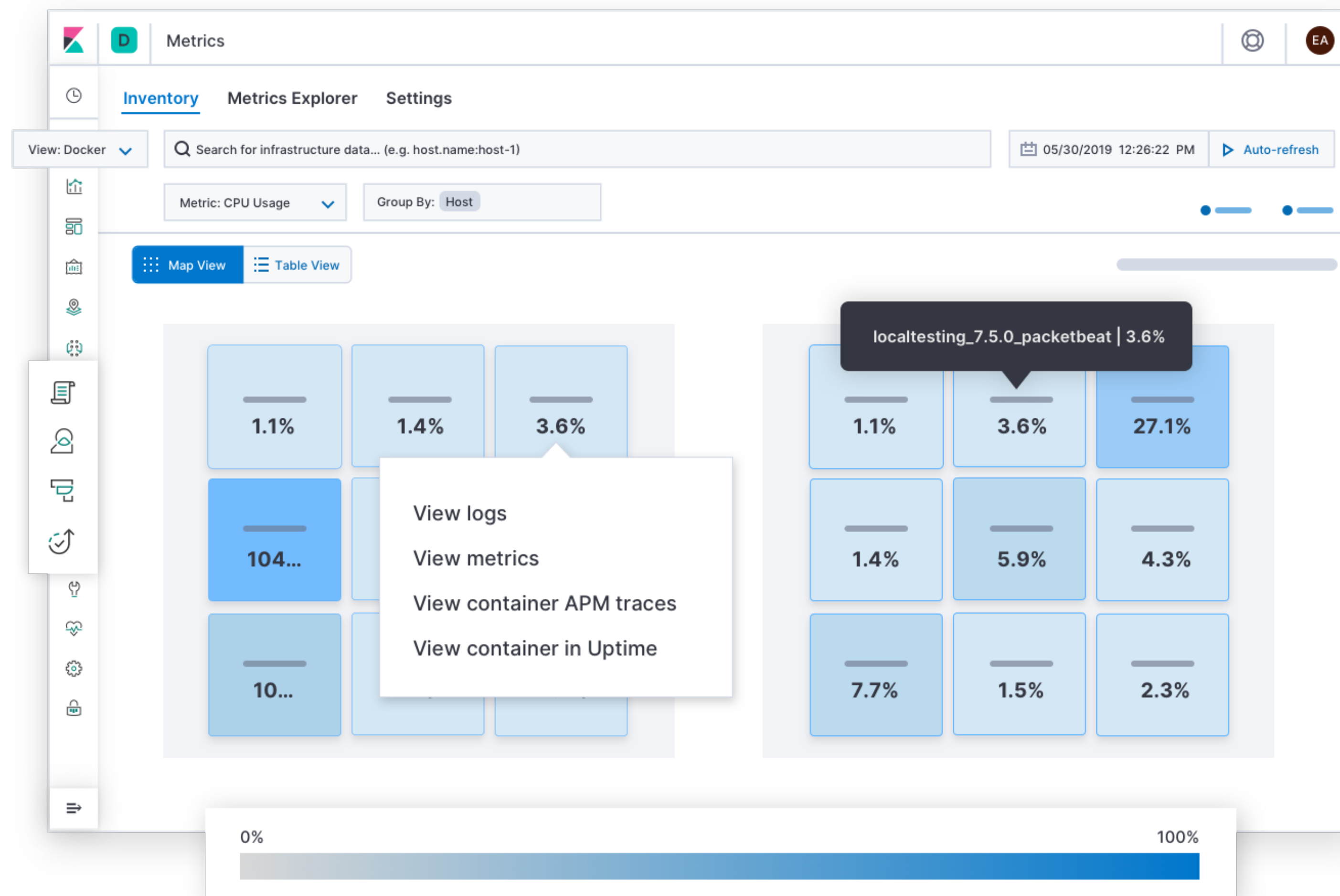
Engineering +3

Design



Unified visibility across your entire ecosystem

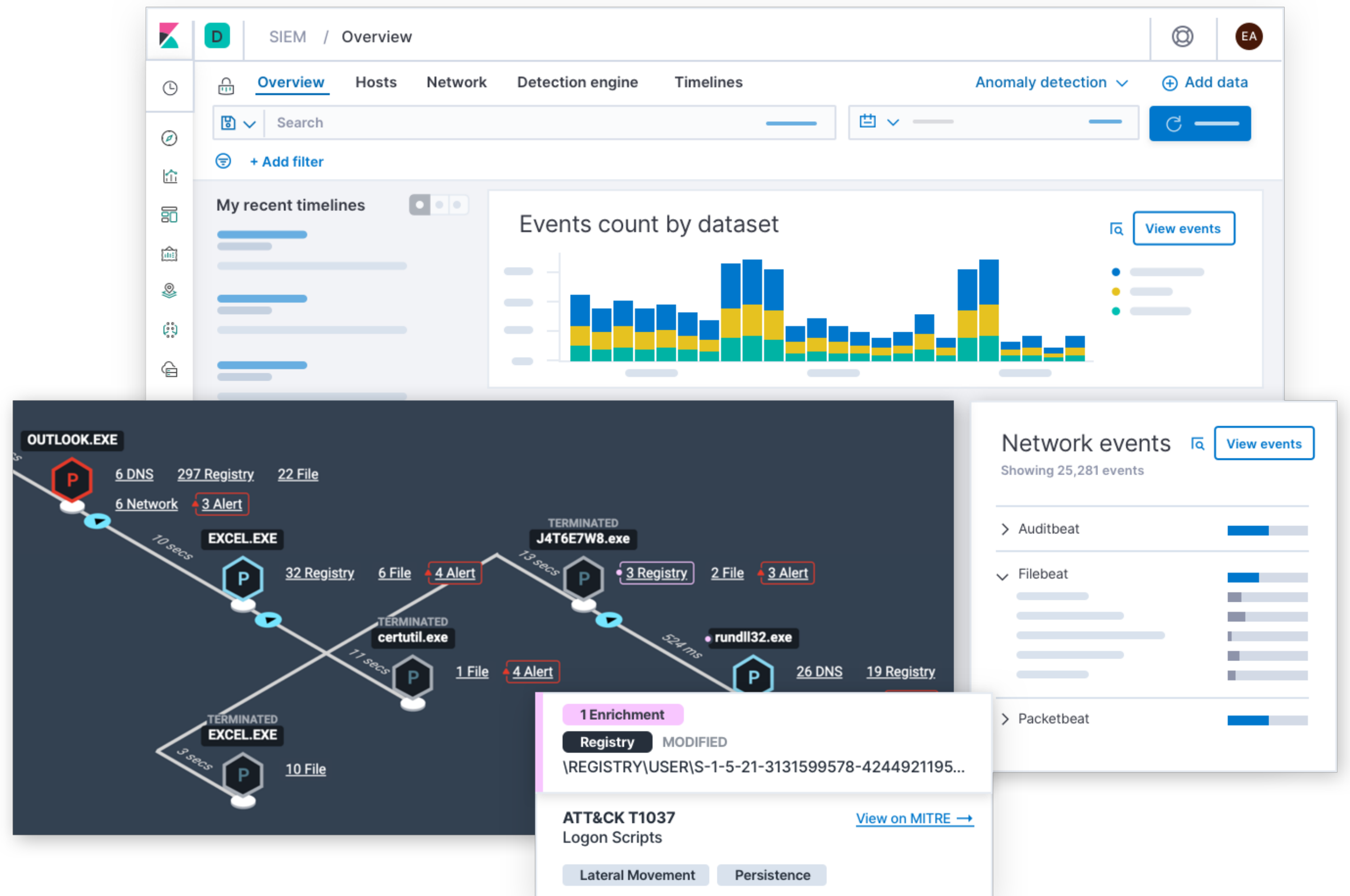
Bring your logs, metrics, and traces together into a single stack so you can monitor, detect, and react to events with speed.

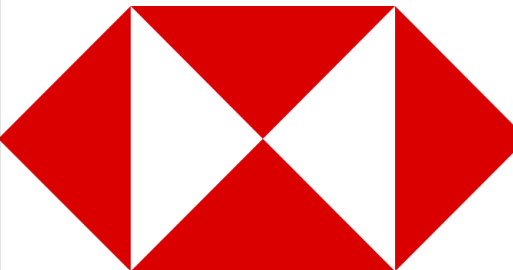
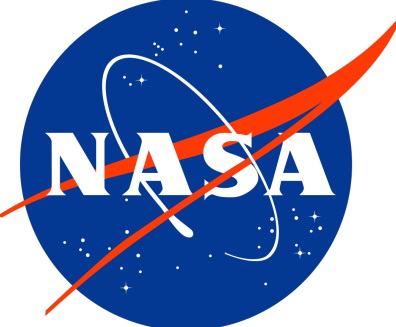
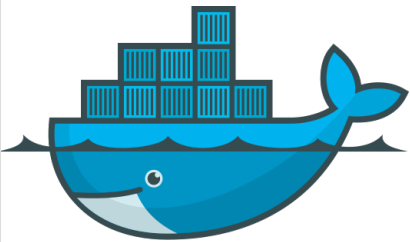


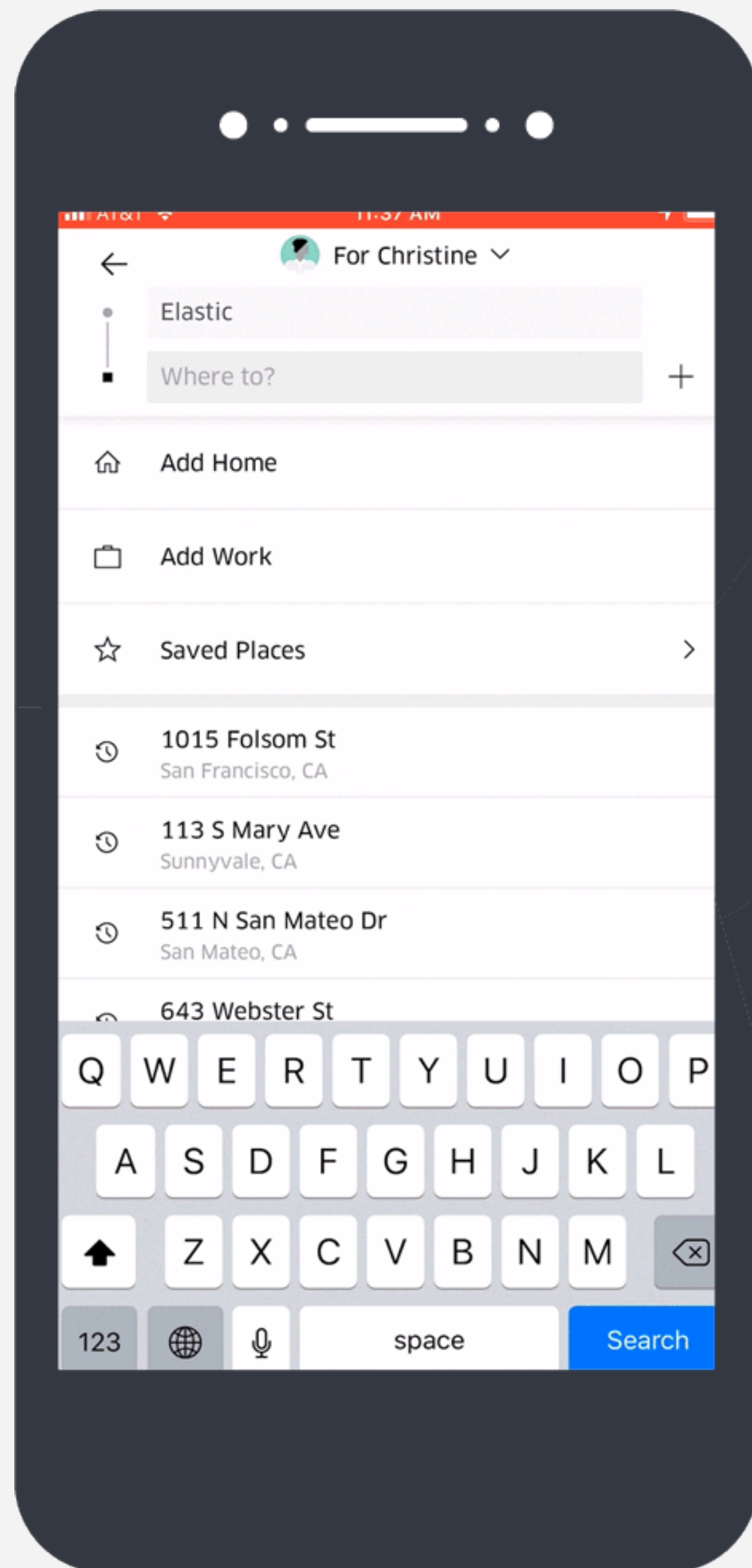


Security how it should be: open

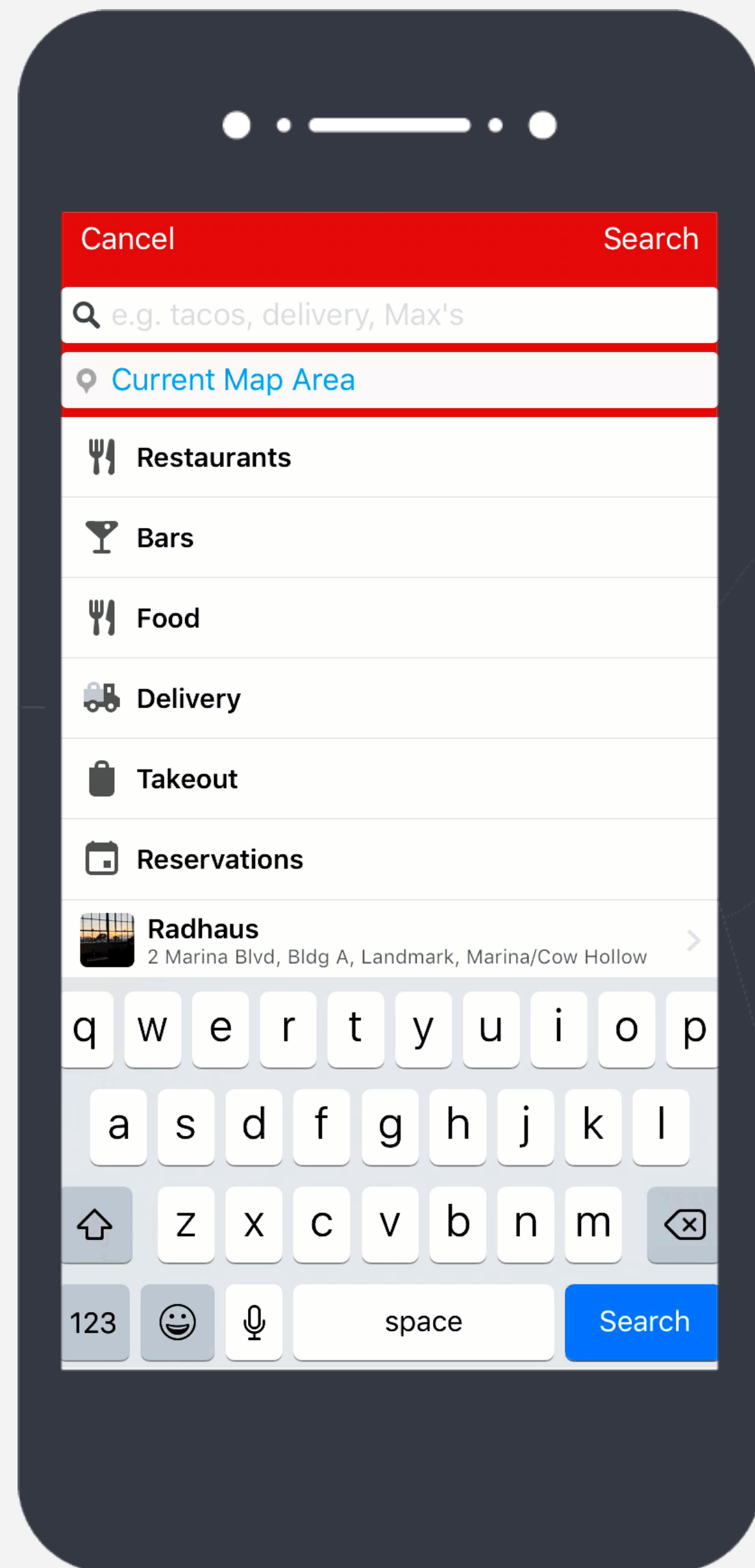
Elastic Security integrates endpoint security and SIEM to give you prevention, collection, detection, and response capabilities for unified protection across your infrastructure.



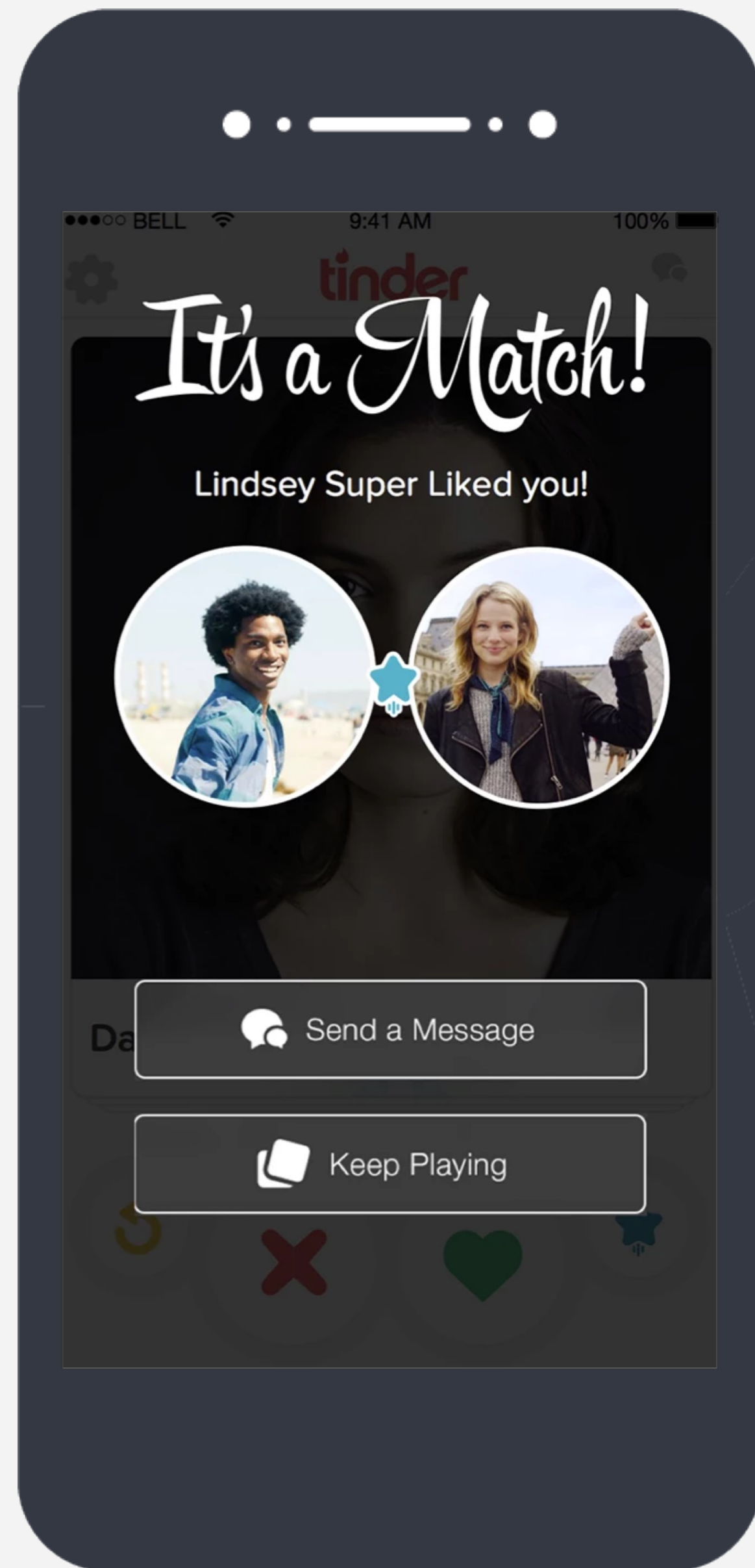
 HSBC		 SOUNDCLOUD	 mozilla FOUNDATION	 Microsoft
GROUPON	facebook	 Expedia	vimeo	 salesforce
 FOURSQUARE		ACTIVISION BLIZZARD	 stack overflow	
	 Symantec		The New York Times	 Unilever
ebay	Eventbrite	 Alcatel-Lucent	 CONCUR	verizon
NETFLIX	ROBLOX	 PayPal	 Adobe	 CISCO
 docker	The Guardian	 THOMSON REUTERS	Quora	TomTom



Searching for
Rides



Searching for Restaurants



Searching for
Love



Elastic France

<https://community.elastic.co/france/>



@elasticfr



discuss.elastic.co

