



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 Stack

SOLUTIONS

Kibana



Visualize & Manage

Elasticsearch



Store, Search, & Analyze

Beats



Logstash

APM

Ingest

SaaS



Elastic Cloud

SELF-MANAGED

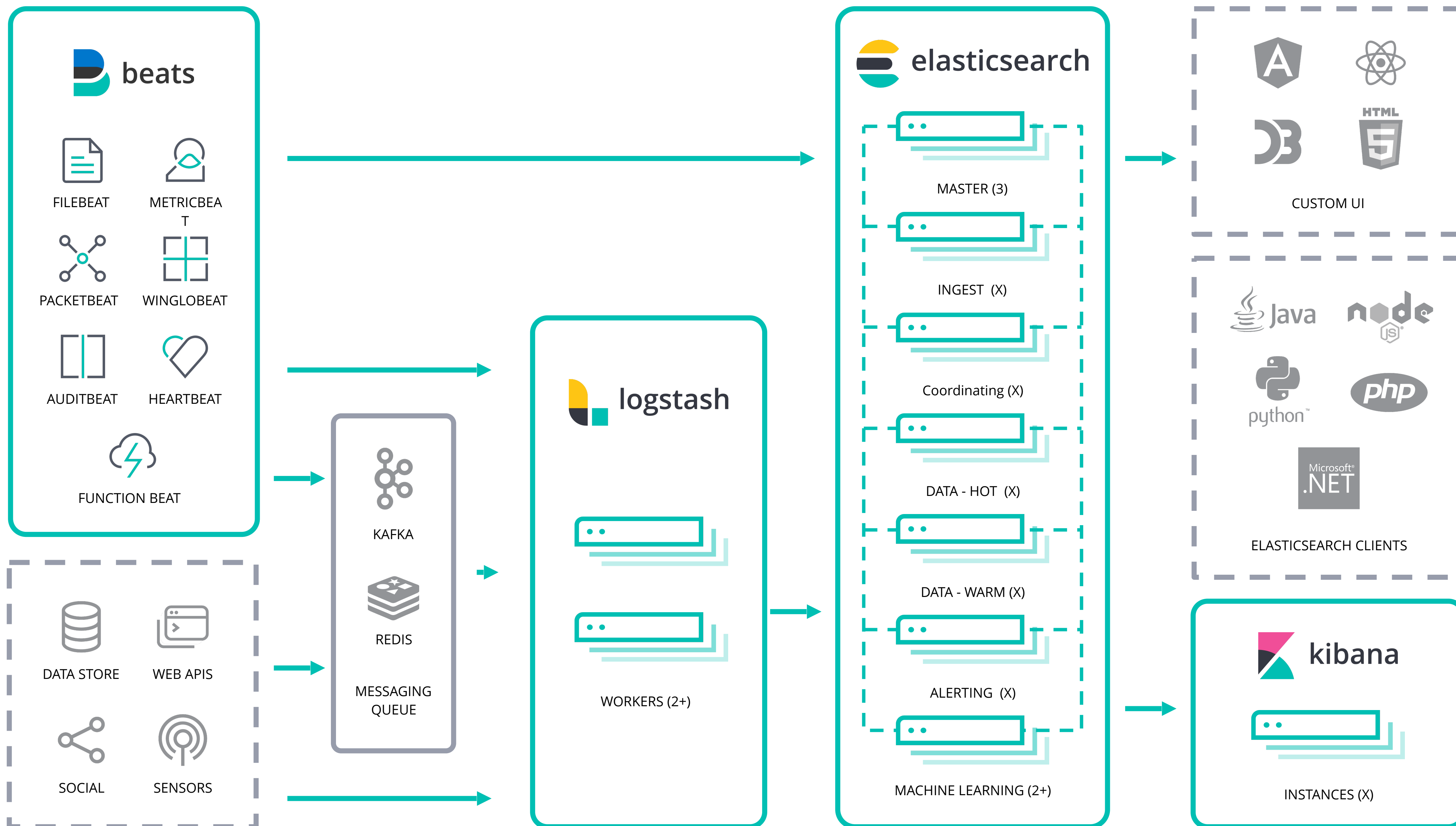


Elastic Cloud Enterprise



Standalone





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>

Services at a Glance



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

People Strategy



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



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

Project Strategy

Elastic Training

Paris / France



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

En français

50% discount on the 2nd seat - discount until Feb 24th

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?');
```

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 Google');  
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 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?

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 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

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 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)



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

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 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?





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)



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

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

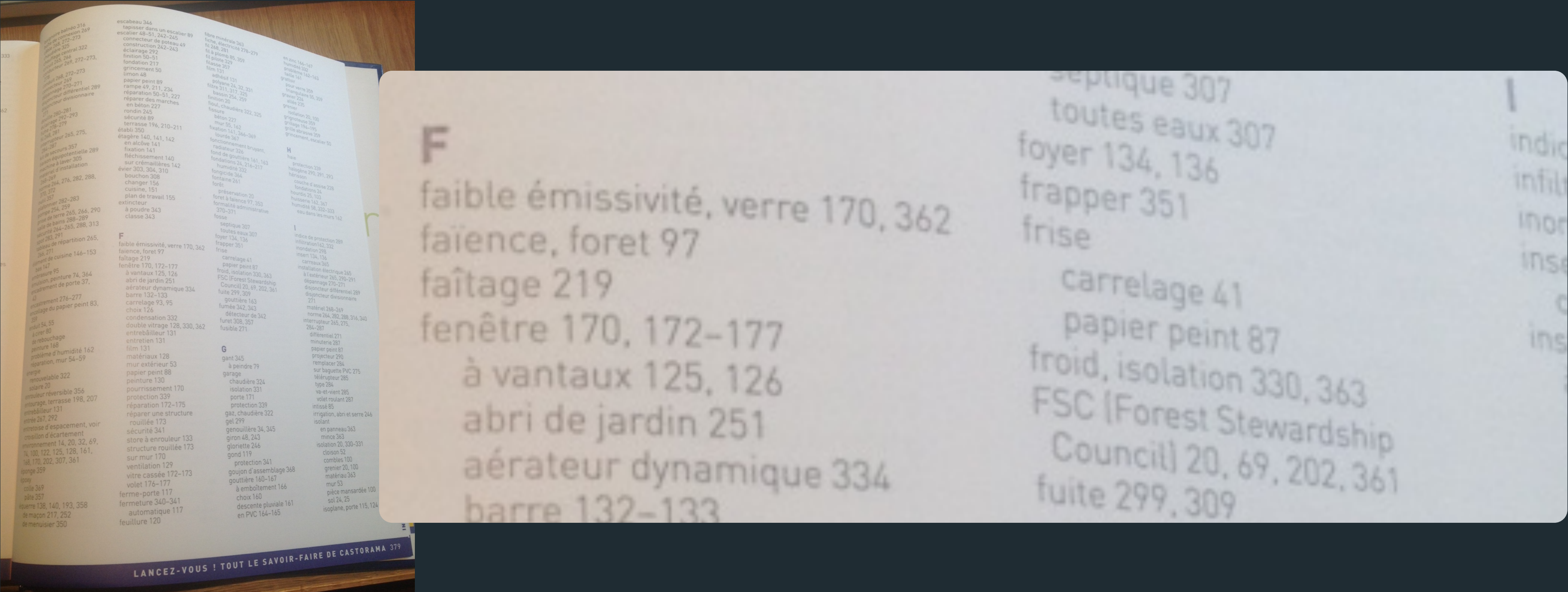
between and

between and

between and

Search engine?

Moteur d'indexation de documents



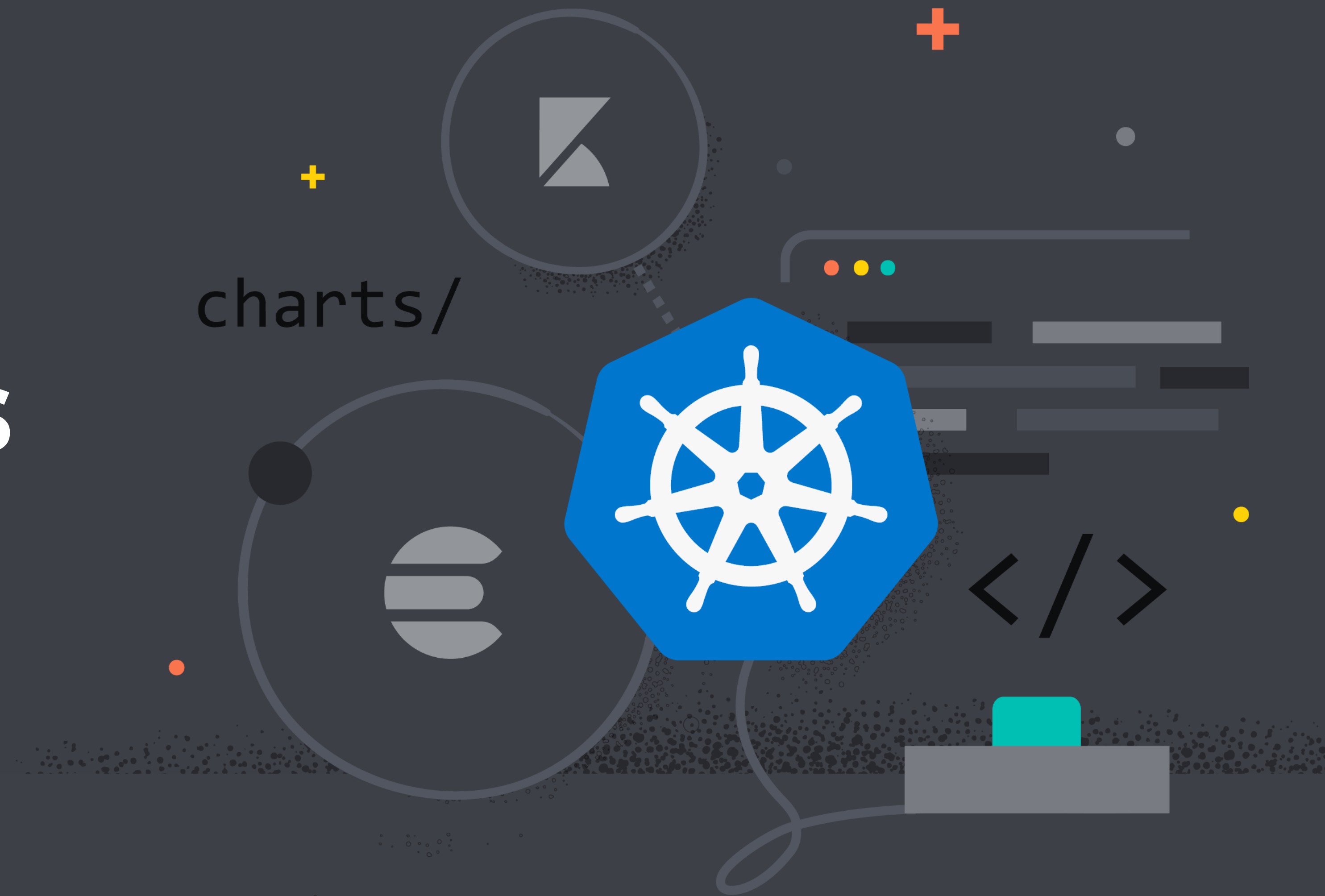
Moteur de **recherche** dans les **index**

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

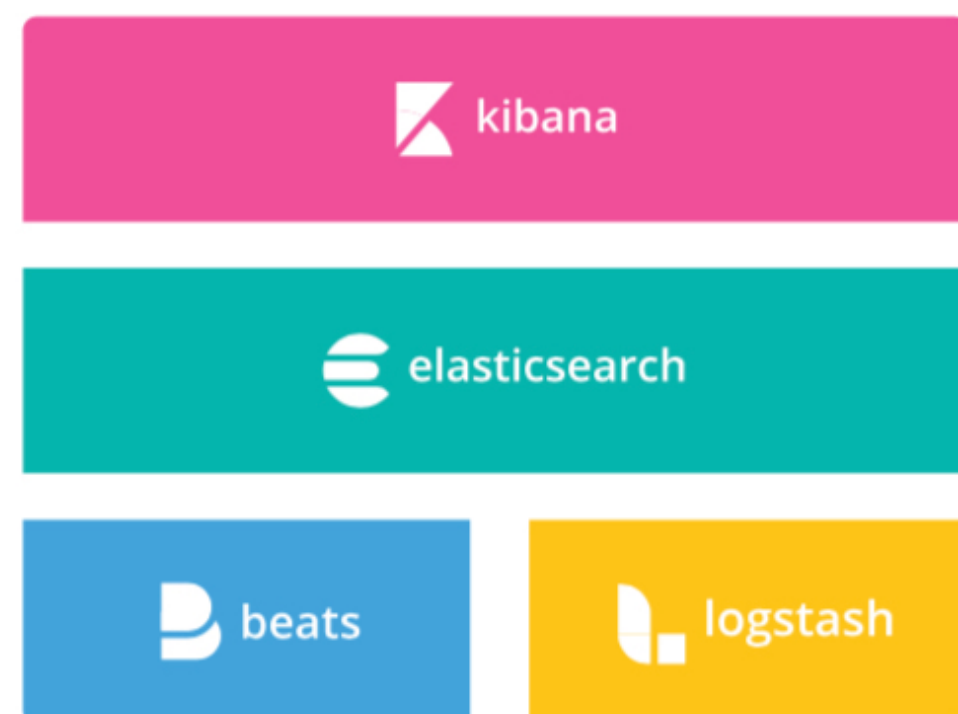
The screenshot displays the Elasticsearch SIEM interface. The left sidebar contains navigation icons. The main panel is titled 'SIEM / Hosts' and has tabs for 'Overview', 'Hosts' (selected), 'Network', and 'Timeline'. A search bar shows 'e.g. host.name: "foo"'. Below the search bar, the 'Hosts' section shows 'Last Event: in 20 days' and a card with '904' hosts and a line graph. The 'All Hosts' section shows 'Showing: 21,116 Hosts'. On the right, a 'Timeline' panel is open, showing a list of events. The events are filtered by 'host.name: "siem-es"'. The timeline shows events from 'Jun 3, 2019 @ 19:40:15.160'. The events are categorized by 'event.severity' (audit-rule), 'event.action' (executed), and 'host.name' (siem-es). The events show a session of 'root' user executing 'google_network_' commands, resulting in 'fail'.

Fields	@timestamp	event.severity	event.category	event.action	host.name
Session	# unset	root	@ siem-es	in / executed > ip route is table local type local scope host dev eth0 proto 66 with result success	siem-es
Session	# unset	root	@ siem-es	in / executed > google_network_ with result fail	siem-es
Session	# unset	root	@ siem-es	in / executed > google_network_ with result fail	siem-es
Session	# unset	root	@ siem-es	in / executed > google_network_ with result fail	siem-es
Session	# unset	root	@ siem-es	in / executed > google_network_ with result fail	siem-es
Session	# unset	root	@ siem-es	in / executed > google_network_ with result fail	siem-es

25 of 14846121 Events [Load More](#) Updated 4 minutes ago

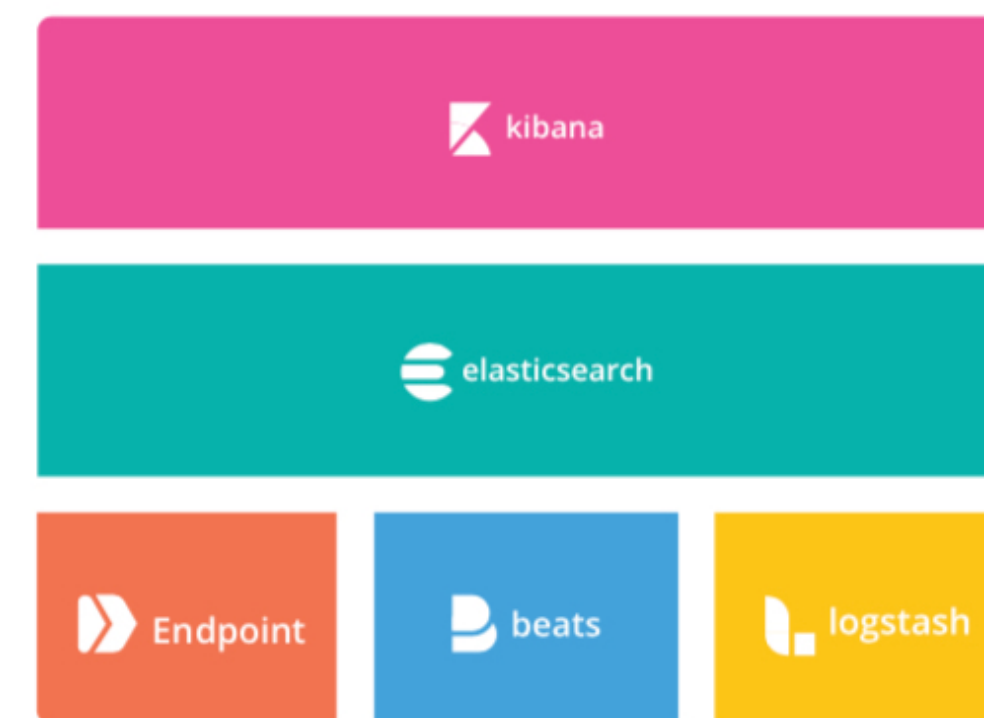
Today

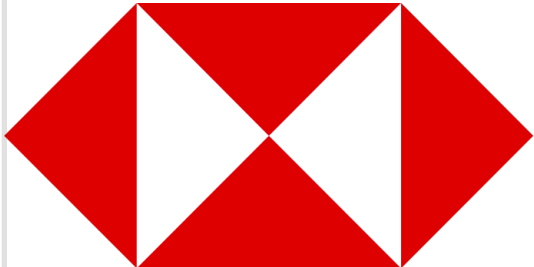
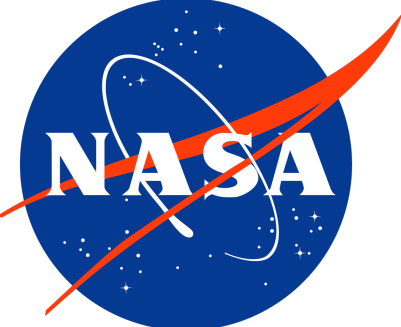
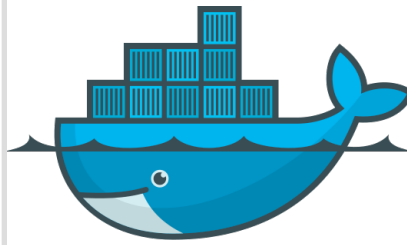
Comprehensive endpoint protection, detection, and response (EPP+EDR) and no per-endpoint pricing. Just pay for what you use.

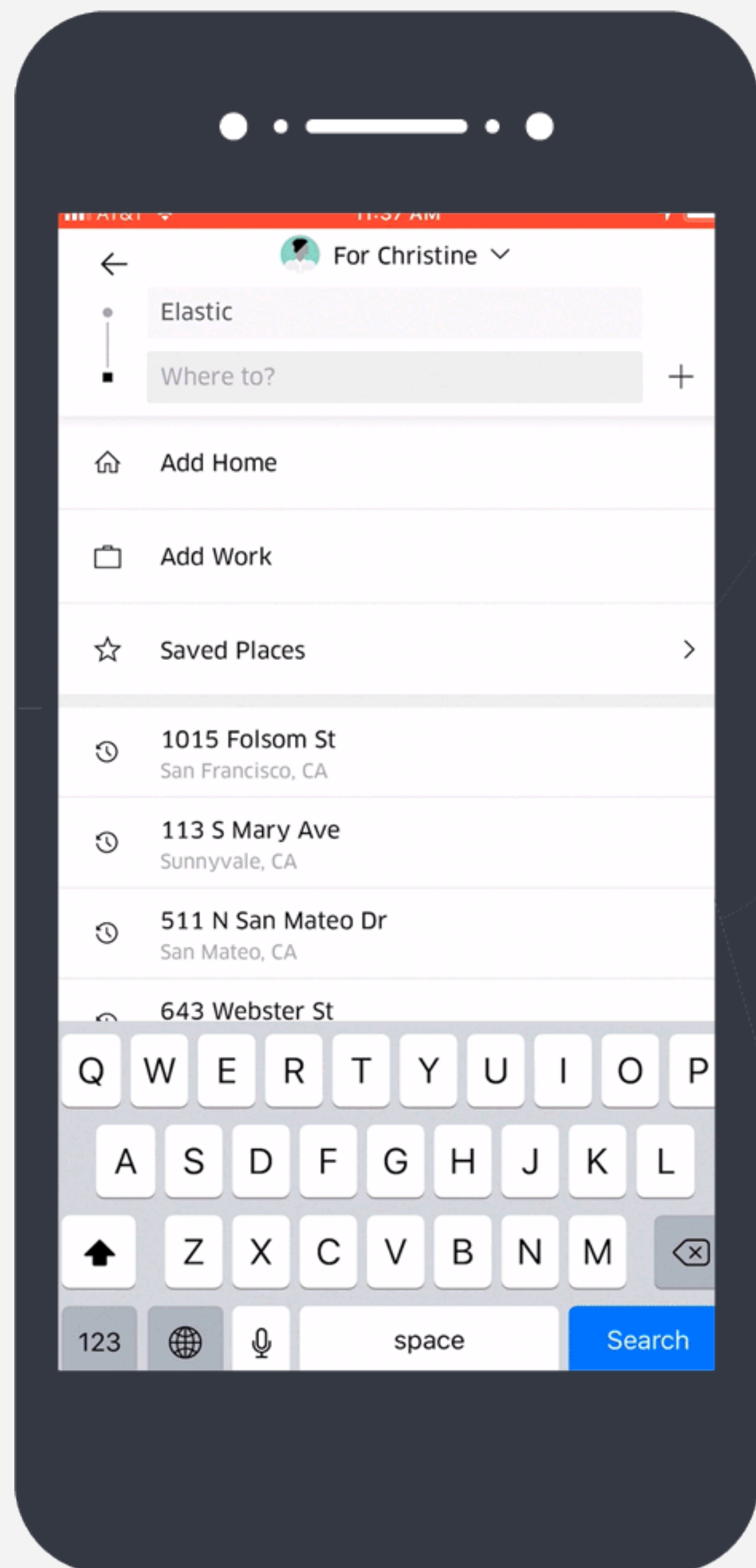


Future

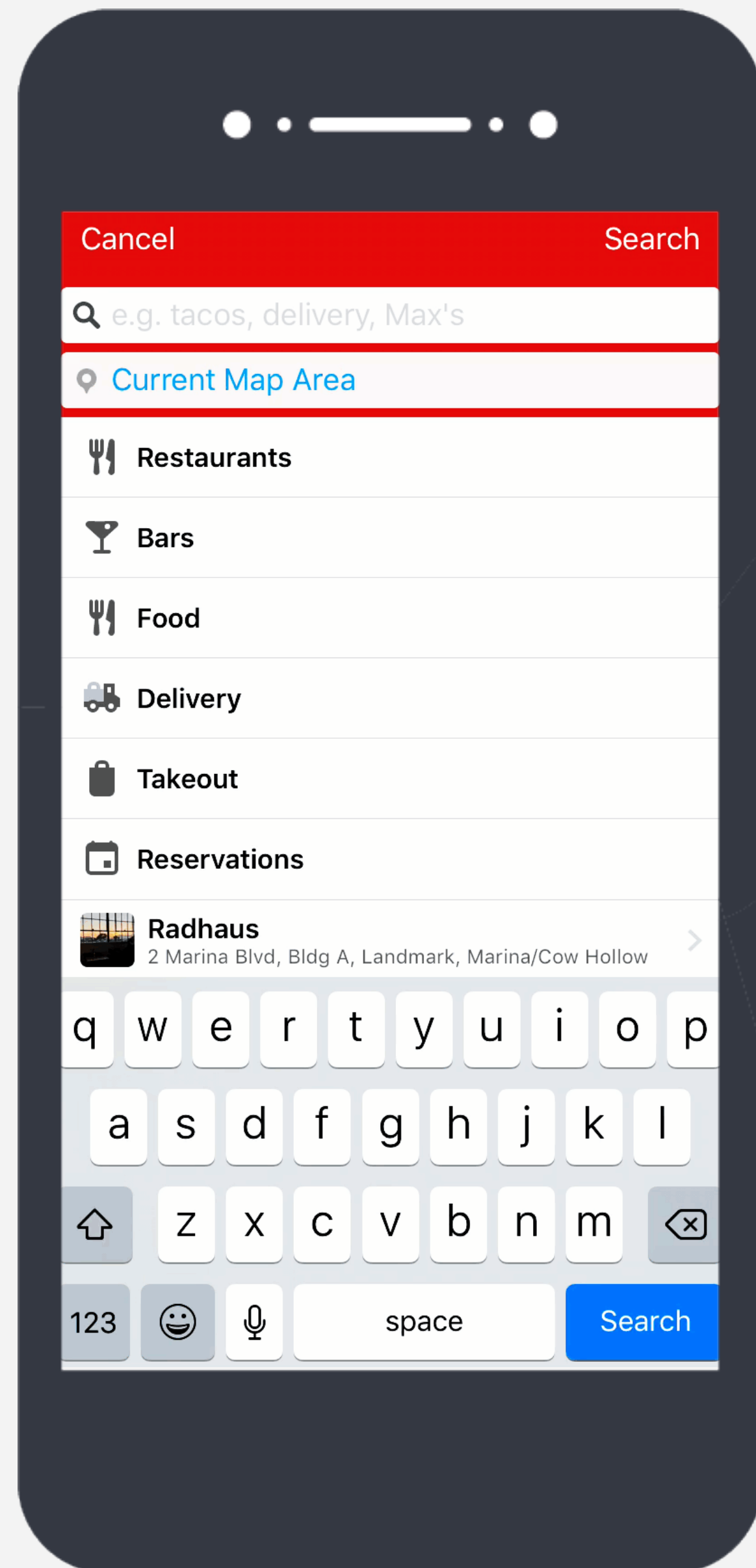
EPP, EDR, and SIEM delivered in a single, simplified architecture: Elasticsearch, Kibana, Elastic Endpoint.

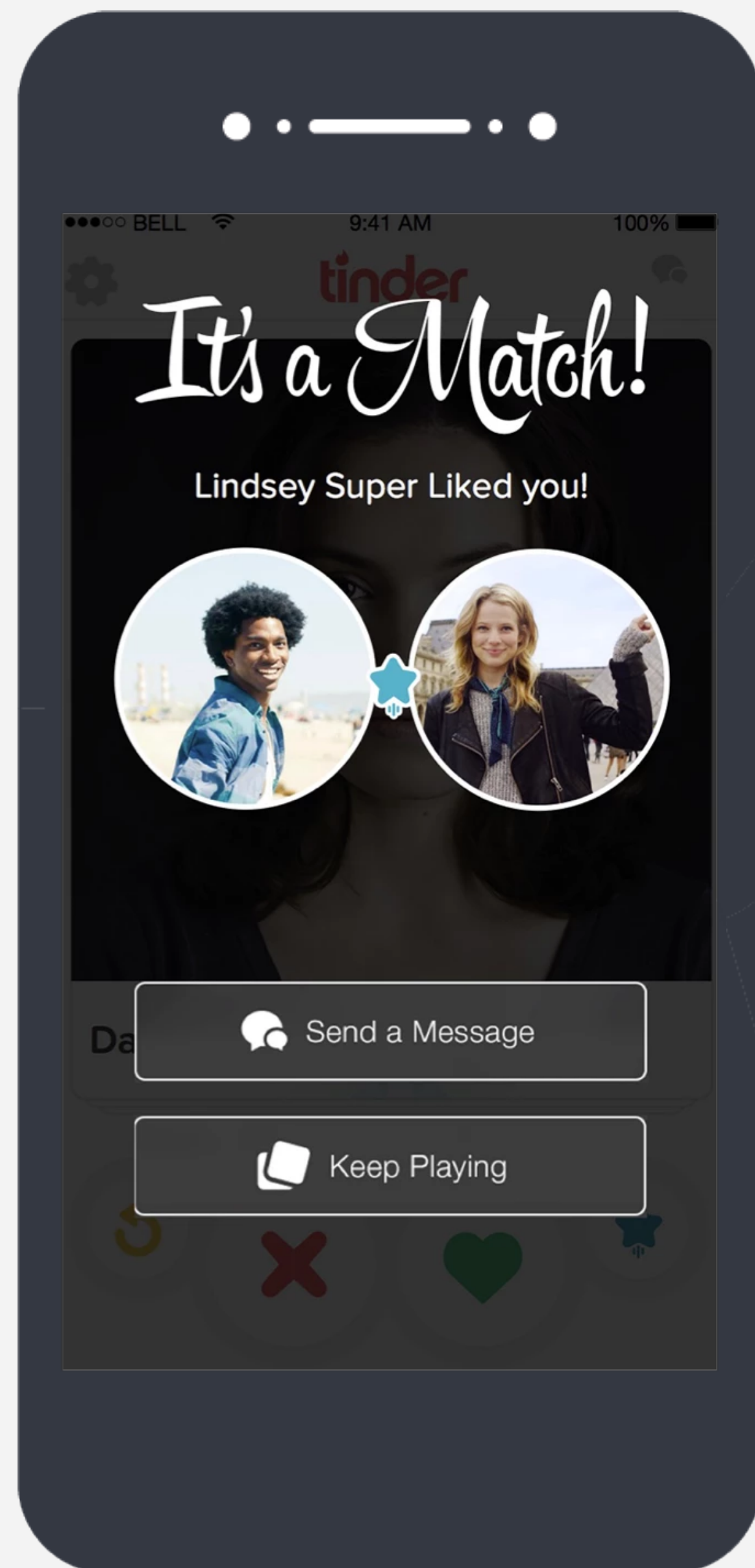


 HSBC		 SOUNDCLOUD	 mozilla FOUNDATION	 Microsoft
GROUPON	facebook	 Expedia	vimeo	 salesforce
 FOURSQUARE		ACTIVISION BLIZZARD	 stack overflow	
	 Symantec		The New York Times	 Unilever
ebay	Eventbrite	 Alcatel-Lucent	 CONCUR	verizon
NETFLIX		 PayPal	 Adobe	 CISCO
 docker	The Guardian	 THOMSON REUTERS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

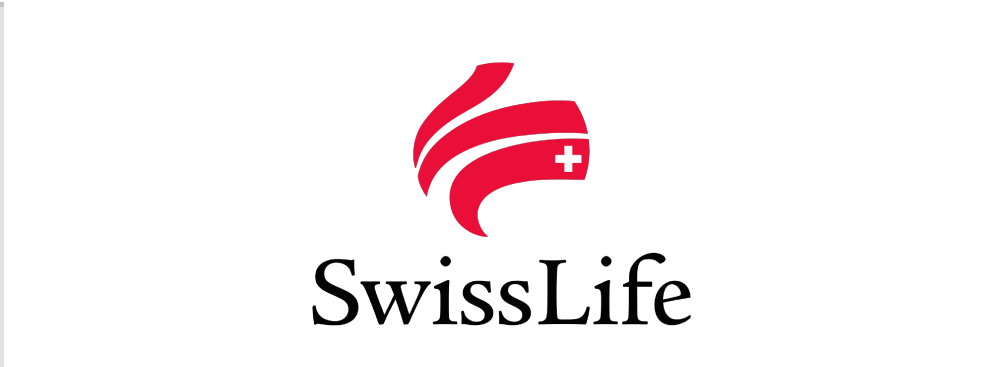
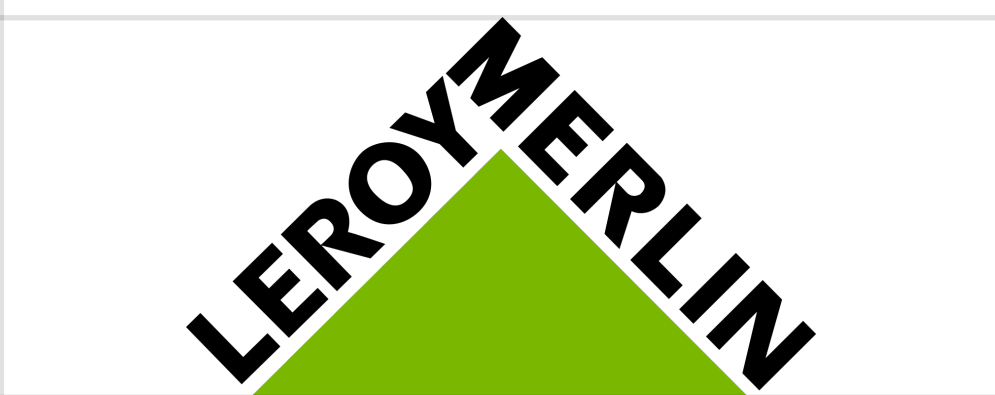
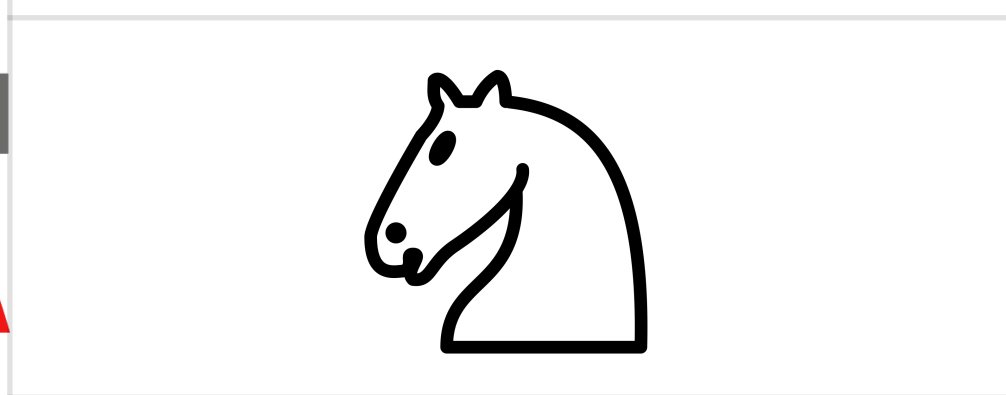
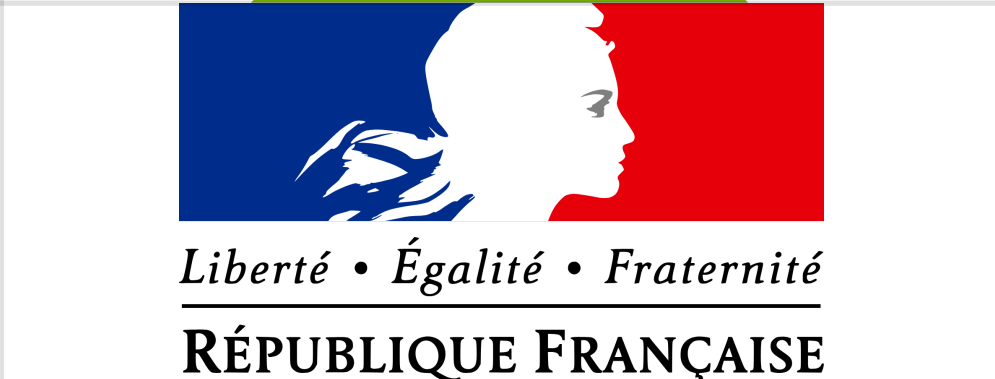
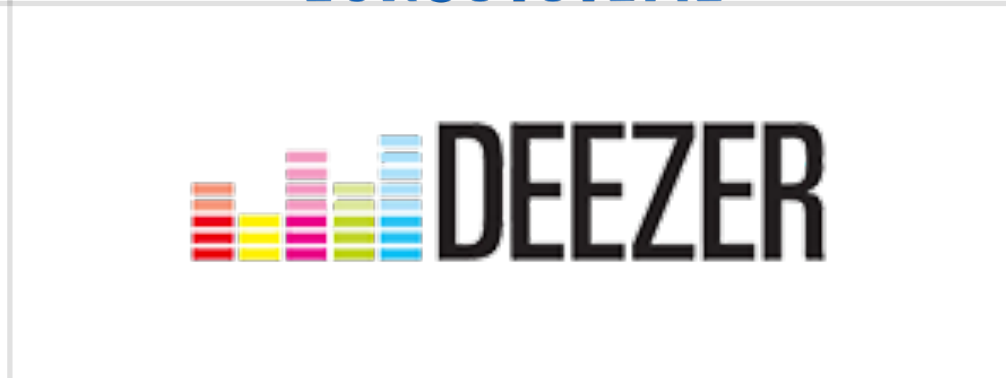


Uber





tinder™



#ElasticStories

Elastic Training

Paris / France



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

En français

50% discount on the 2nd seat - discount until Feb 24th



elasticfr



@elasticfr



elastic

User Group

discuss.elastic.co

