



Elastic Stack Overview

Search. Observe. Protect.



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"
}
```

The Elastic Search Platform

Out of the Box Solutions



Observability

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



Security

SIEM, Endpoint, Cloud



Search

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

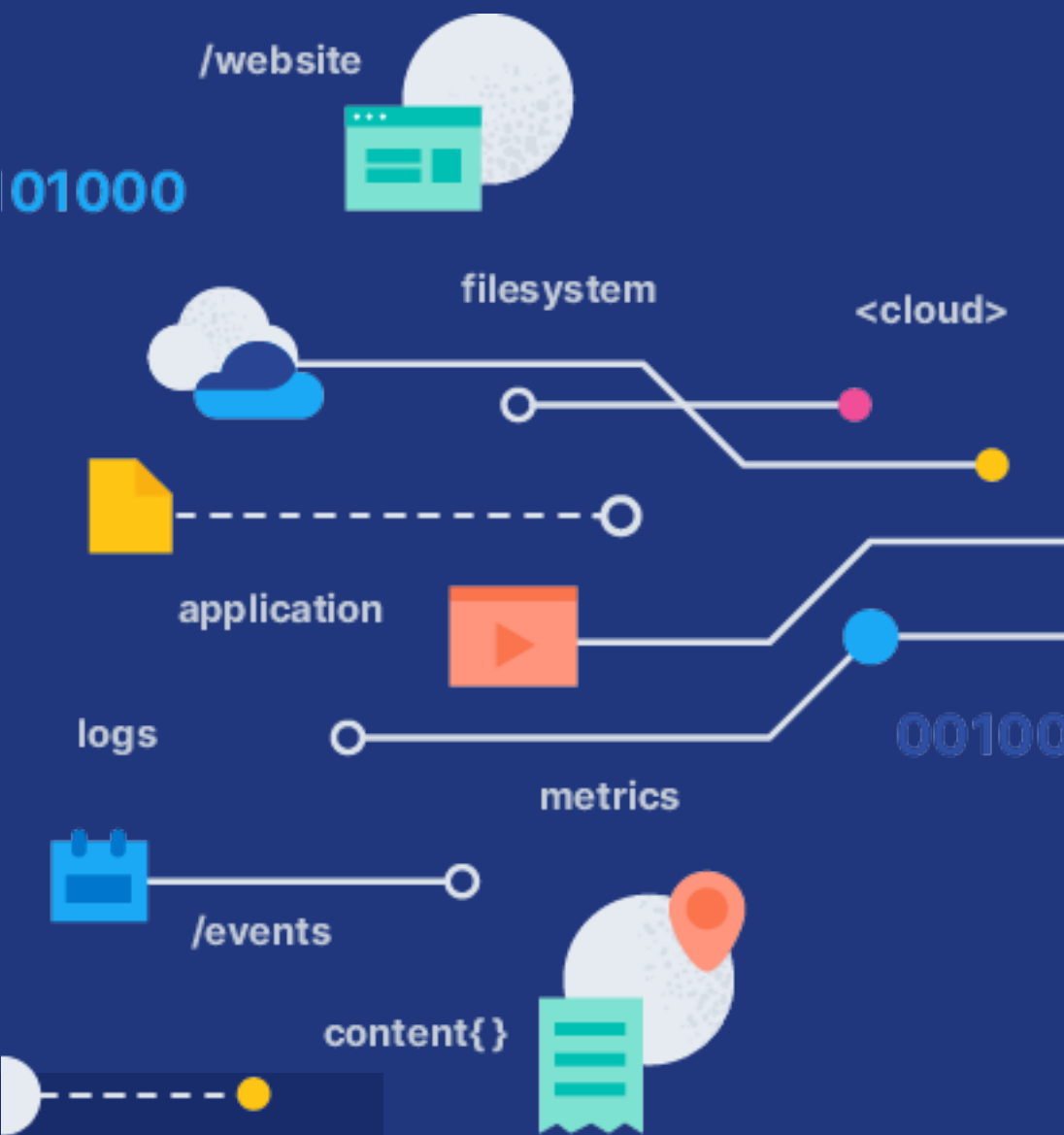
Build Your Own

Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

Integrations
Connect, Collect, Alert

ESRE™
Elasticsearch
Relevance Engine™



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

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



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)

Pilato David



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?

David





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)
```

Dadid



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 ▼

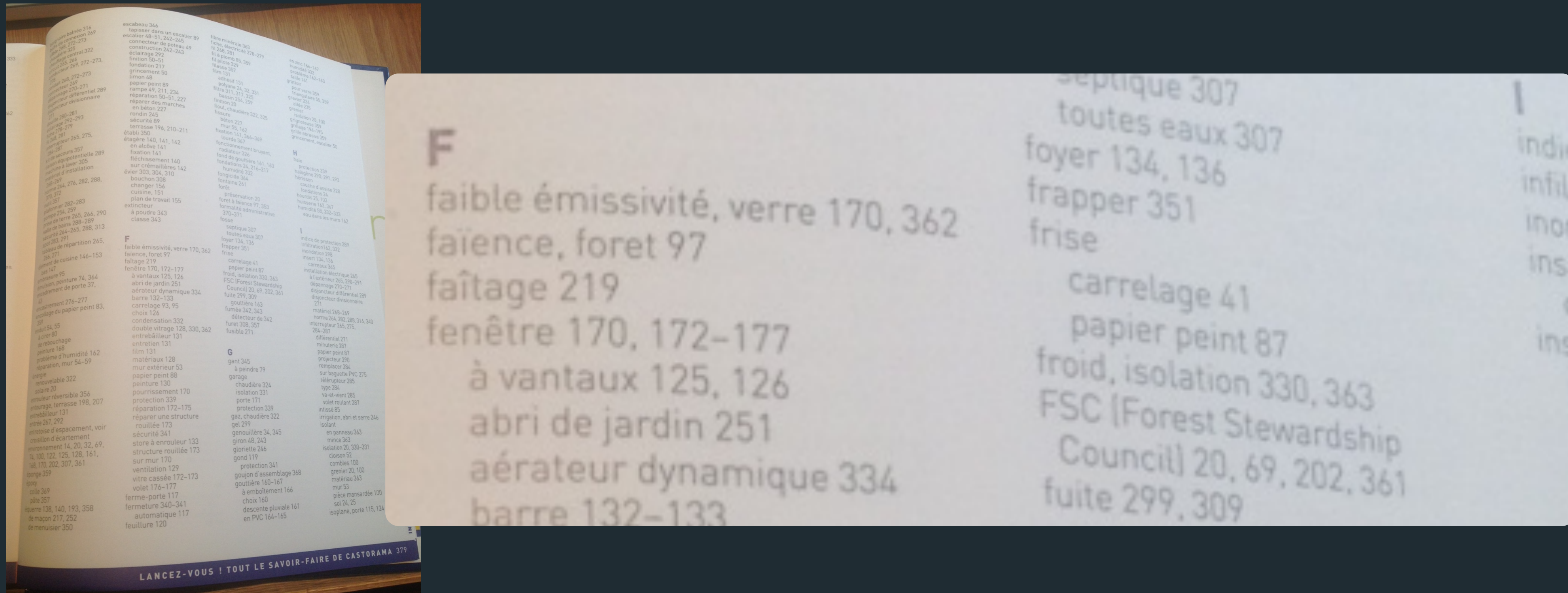
between and

between and

between and

What is a search engine?

Index engine (indexing documents)



Search engine (within the created indices)

Demo time!



4GIFs.com

The Elastic Search Platform

Out of the Box Solutions



Observability

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



Security

SIEM, Endpoint, Cloud



Search

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

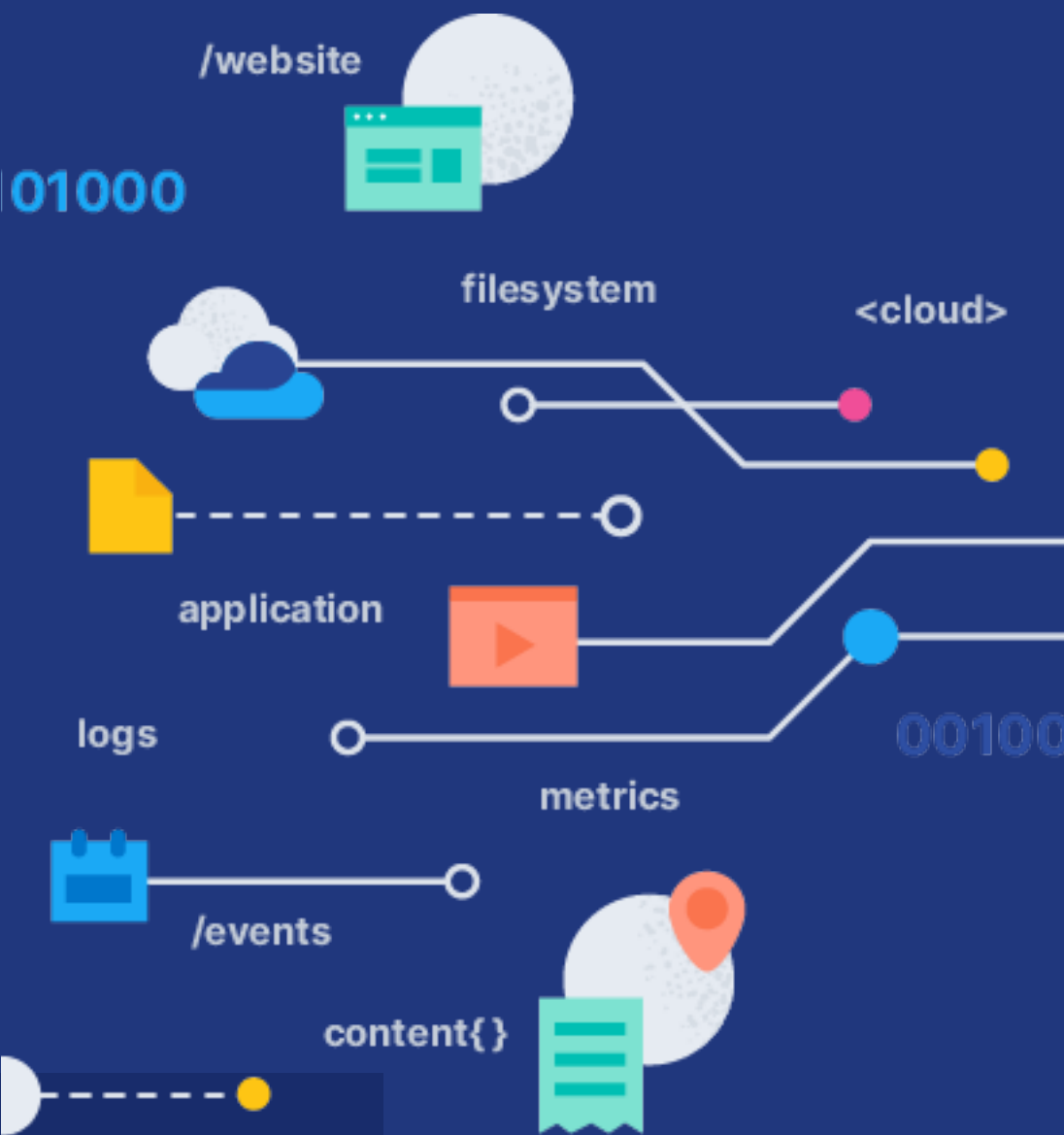
Build Your Own

Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

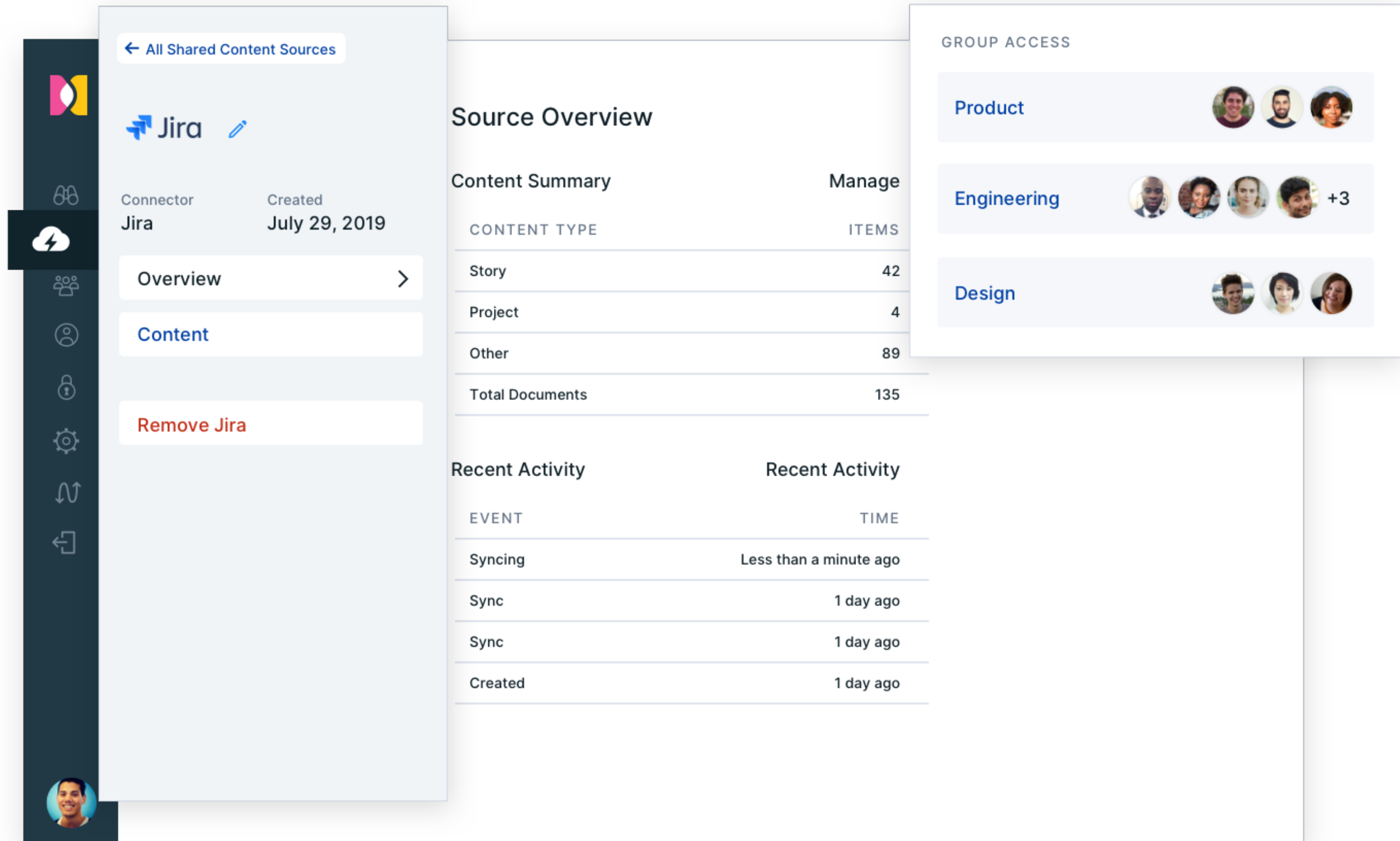
Integrations
Connect, Collect, Alert

ESRE™
Elasticsearch
Relevance Engine™



Search everything, anywhere

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



The screenshot displays the Elastic Enterprise Search interface. On the left is a dark sidebar with navigation icons. The main content area is divided into three panels:

- Connector Overview:** Shows a Jira connector created on July 29, 2019. It includes tabs for Overview and Content, and a 'Remove Jira' button.
- Source Overview:** A table showing content summary for the Jira source.

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

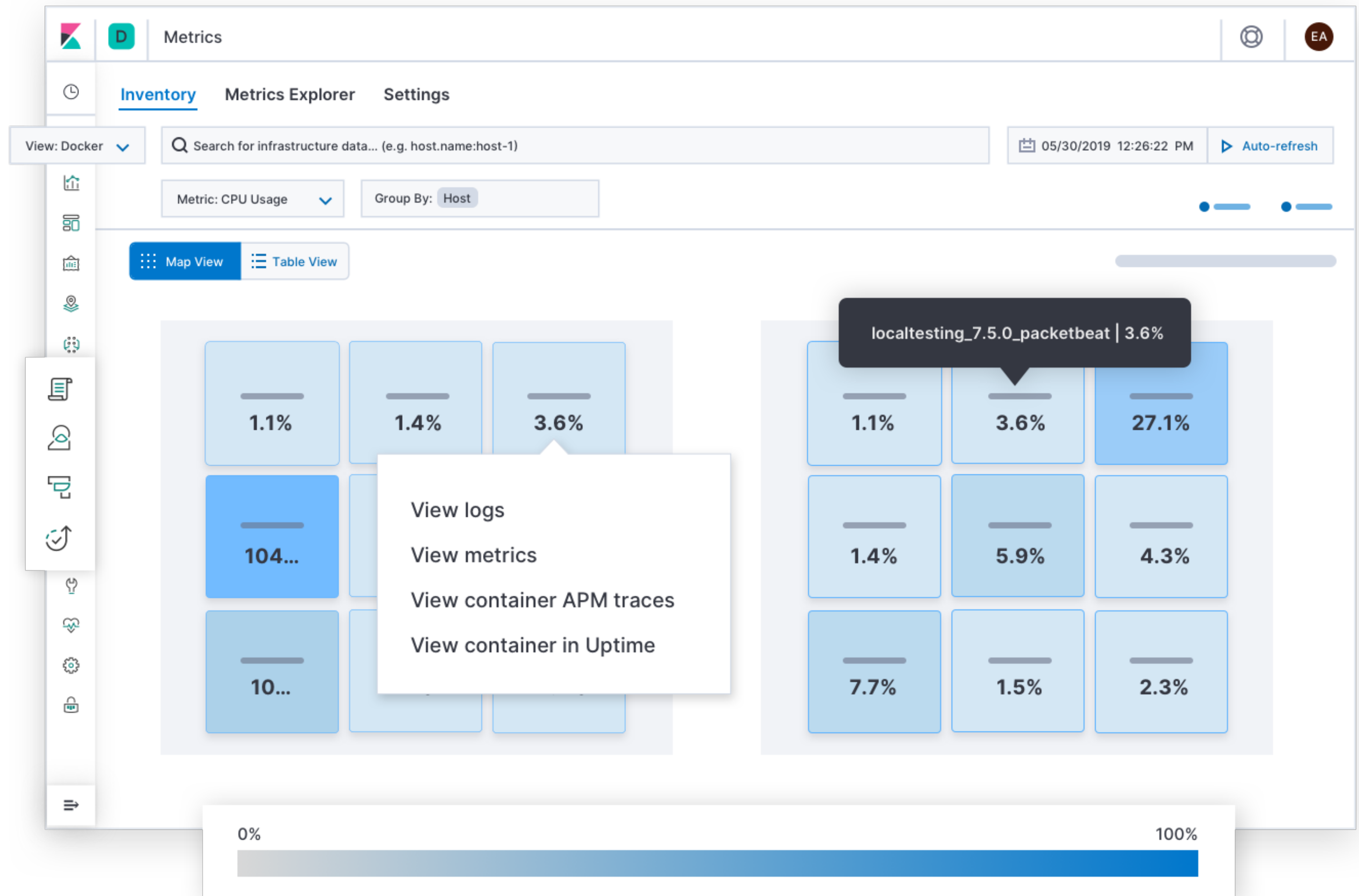
Below the table is a 'Recent Activity' section with a table:

EVENT	TIME
Syncing	Less than a minute ago
Sync	1 day ago
Sync	1 day ago
Created	1 day ago
- GROUP ACCESS:** A panel showing access for three groups: Product (3 users), Engineering (+3 users), and Design (3 users).



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.

SIEM / Overview

Overview Hosts Network Detection engine Timelines Anomaly detection Add data

Search Add filter

My recent timelines

Events count by dataset View events

Network events View events Showing 25,281 events

Auditbeat

Filebeat

1 Enrichment Registry \REGISTRY\U ATT&CK T103 Logon Scripts Lateral Move

Find bash started by ubuntu > kevin Shell startup

```
/home/kevin $ ls | head -3 | tail -1
I/O (bash) $ echo hello Alerts (4)
/home/kevin $ ps
/home/kevin $ cat /etc/shadow Alerts (17)
```

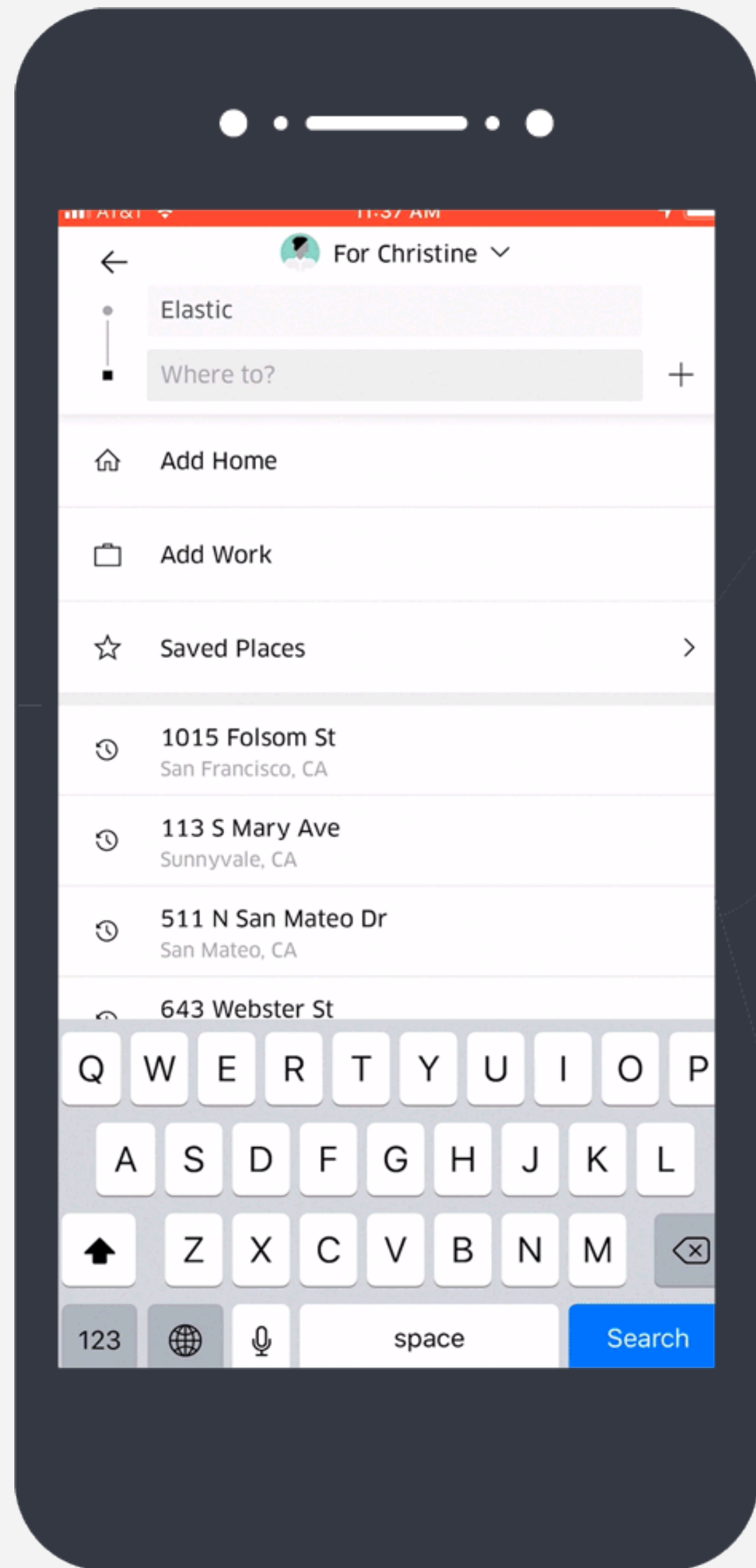
Showing 5 of 17 alerts

- Suspicious MS Office Child Process Open
- Potentially Malicious Hostname has been Queried Open
- Malware Detection Alert Acknowledged
- Encoding or Decoding Files via CertUtil Open
- LS catch Open

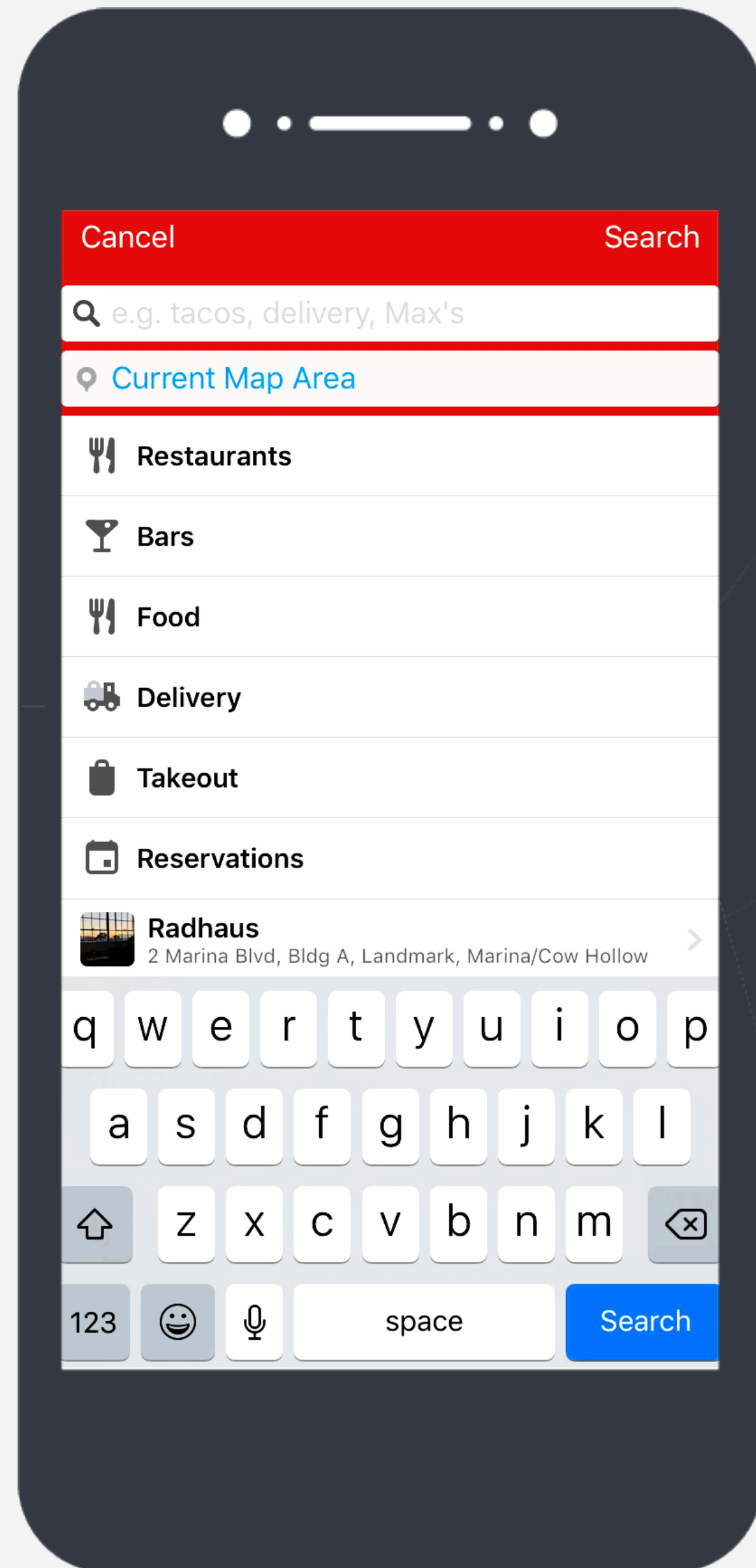
I/O (bash) \$ echo hello



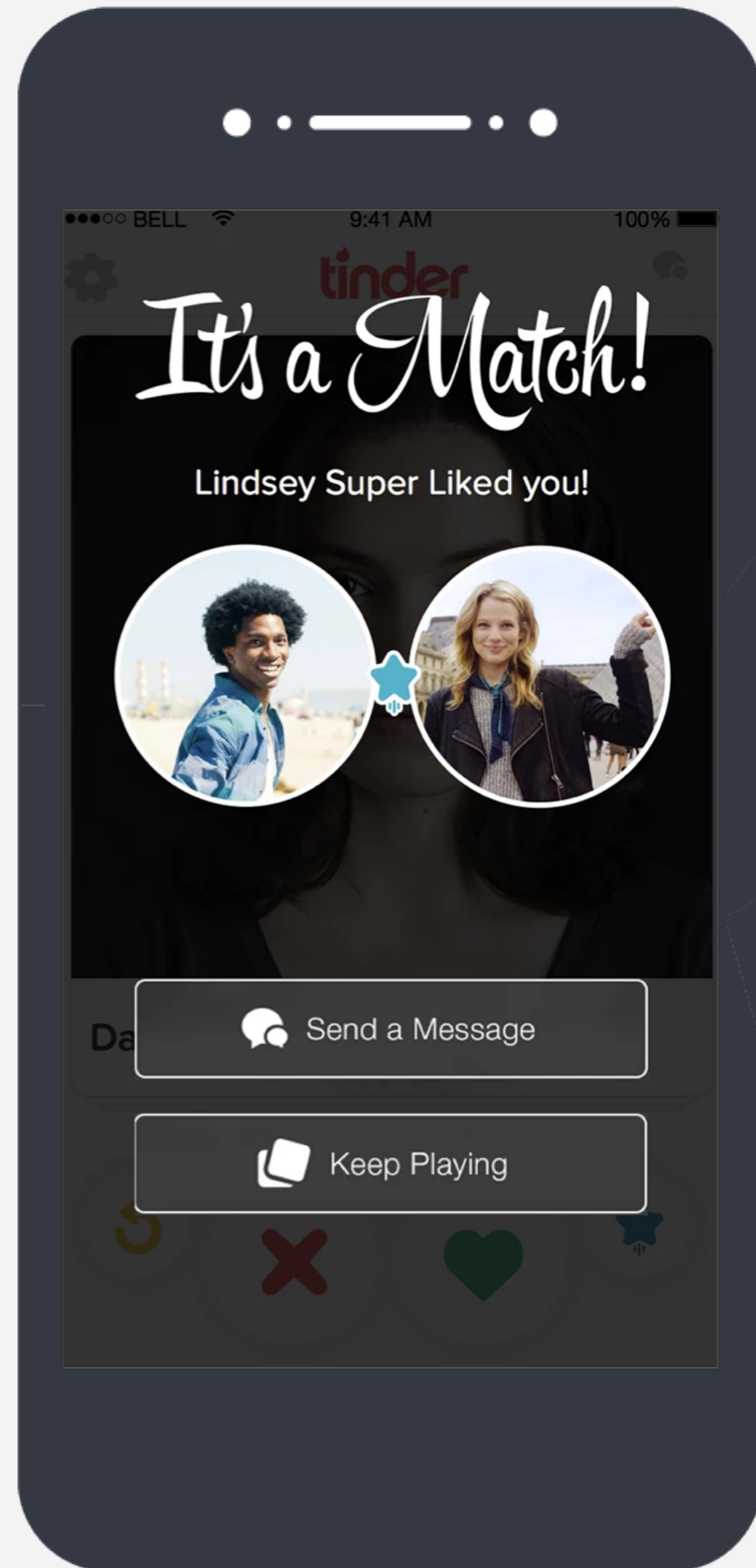
 HSBC		 SOUNDCLOUD	 mozilla FOUNDATION	 Microsoft
GROUPON	facebook	 Expedia	vimeo	 salesforce
 FOURSQUARE		ACTIVISION BLIZZARD	 stack overflow	
	 Symantec		The New York Times	 Unilever
ebay	Eventbrite	 Alcatel-Lucent	 CONCUR	verizon
NETFLIX	ROBLOX	 PayPal	 Adobe	 CISCO
 docker	The Guardian	 THOMSON REUTERS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



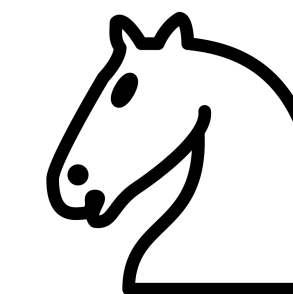
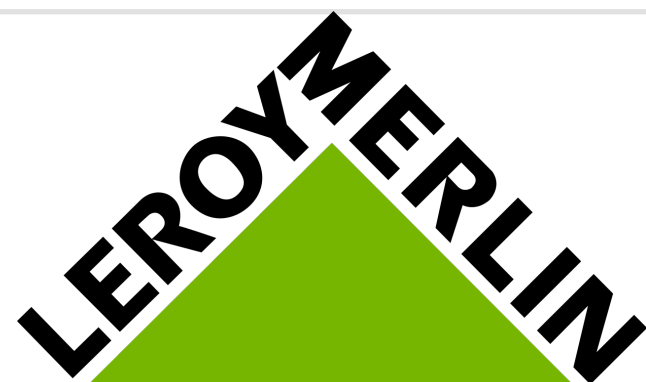
Searching for **Rides**



Searching for **Restaurants**



Searching for **Love**





Elastic France

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



@elasticfr



discuss.elastic.co



Elastic for Students and Educators

- Access to Elastic Cloud
- Free Training/Support (on demand courses)
- Student focused presentations and workshops
- Connect and network with the community

*Learn more: Visit the “Students” tab on the Community page or reach out directly to students_highered@elastic.co



Get started today!
Scan here to activate your free extended trial of Elastic Cloud!