



# Elastic Stack Overview

Search. Observe. Protect.

---

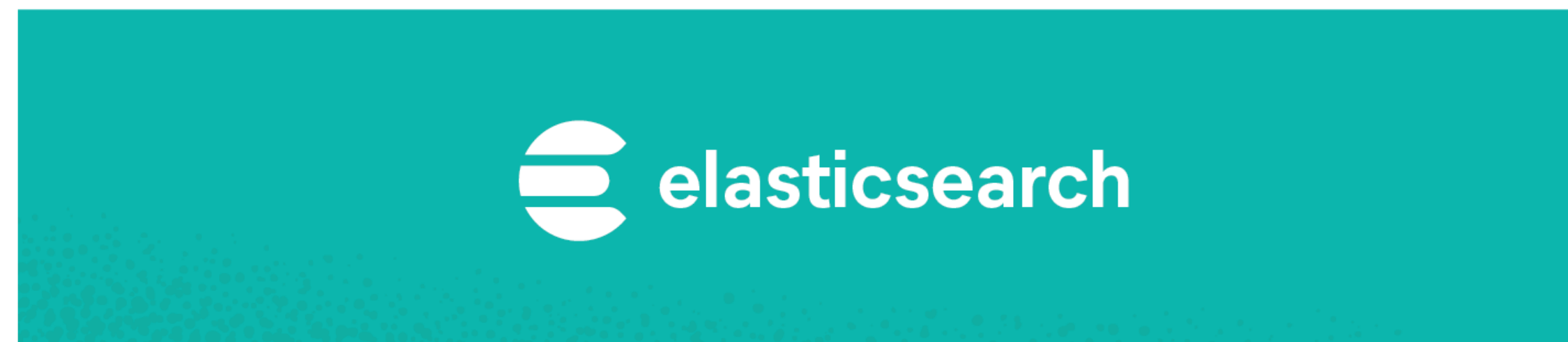


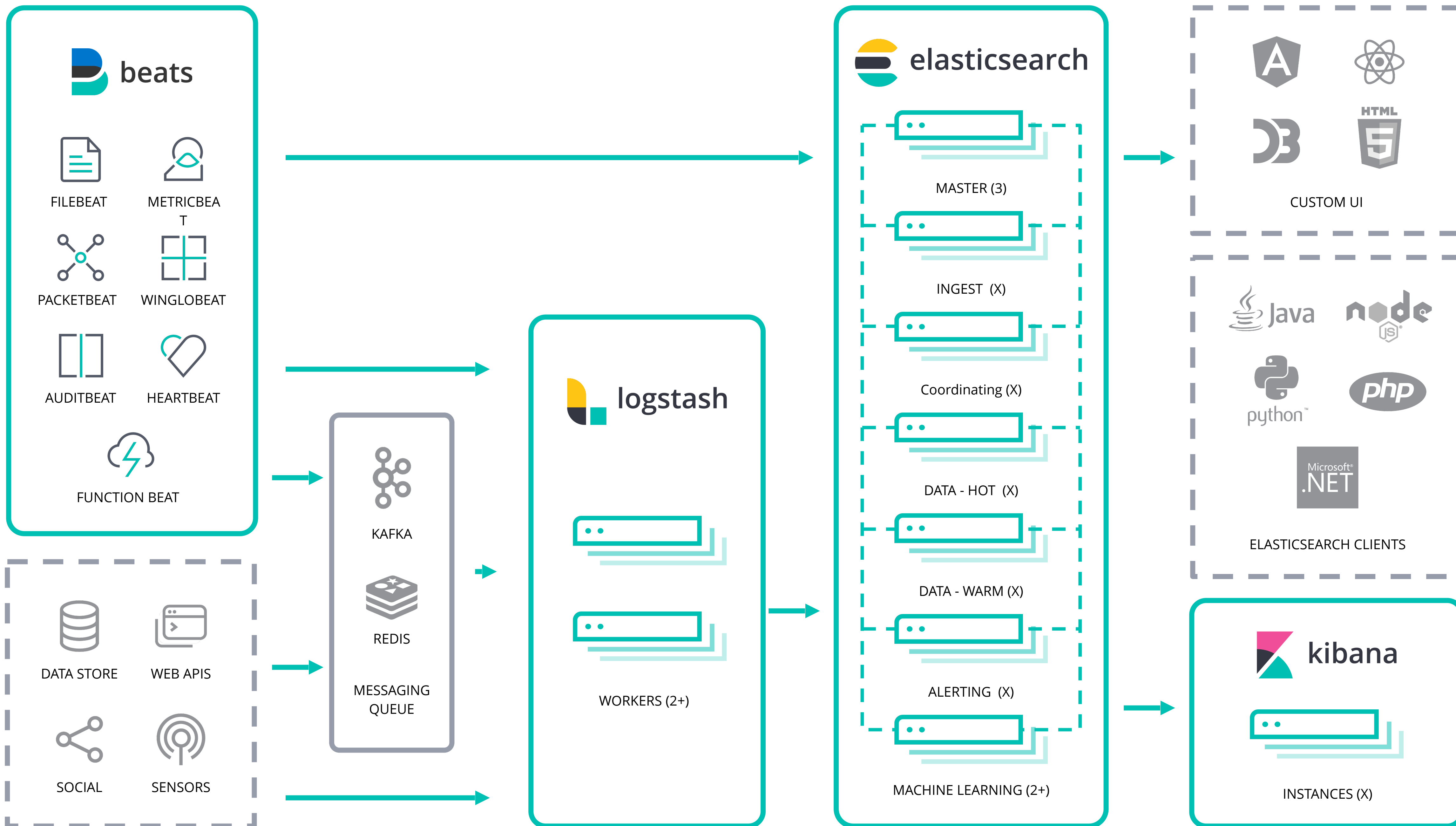
# Who?

```
$ 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"
}
```

# The Elastic Stack

Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.







# Deploy anywhere.

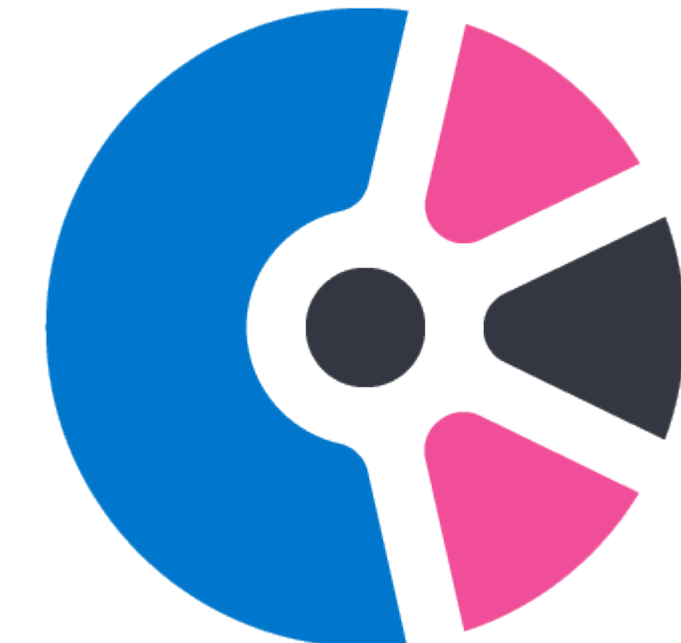


**Elastic Cloud**

SaaS



**Elastic Cloud  
Enterprise**



**Elastic Cloud on  
Kubernetes**

Orchestration

FREE

## Open source

Apache 2.0 :  
aujourd'hui comme  
demain.

Entre autres  
fonctionnalités :

- ✓ Clustering et haute disponibilité
- ✓ Recherche et analyse ultra-performantes
- ✓ Visualisation des données et tableaux de bord
- ✓ Et plus encore

Téléchargement gratuit

## Basic

L'offre gratuite qui le  
restera toujours.

Tous les avantages de  
l'open source, plus :

- ✓ Les principales fonctionnalités de sécurité de la Suite Elastic
- ✓ Des fonctionnalités telles qu'Elastic APM, SIEM, ou encore Maps
- ✓ Canvas et Lens
- ✓ Et plus encore

## Gold

Plus de  
fonctionnalités. Un  
support technique  
dédié.

Tous les avantages de  
l'offre Basic, plus :

- ✓ Alerting
- ✓ Reporting
- ✓ Gestion de l'ingestion
- ✓ Support technique aux heures ouvrées
- ✓ Et plus encore

Nous contacter

## Platinum

Des fonctionnalités  
avancées. Un  
support technique  
24 h/24.

Tous les avantages de  
l'offre Gold, plus :

- ✓ Des fonctionnalités de sécurité avancées de la Suite Elastic
- ✓ Machine Learning
- ✓ Réplication inter-clusters
- ✓ Support technique 24 h/24, 7 j/7, 365 j par an
- ✓ Et plus encore

Nous contacter

## Enterprise

L'orchestration de la  
Suite et  
Endpoint Security  
par défaut.

Tous les avantages de  
l'offre Platinum, plus :

- ✓ Prévention aux points de terminaison
- ✓ Protection et réponse aux points de terminaison mappées vers MITRE ATT&CK
- ✓ Collecte d'événements aux points de terminaison
- ✓ L'accès aux fonctionnalités d'orchestration d'Elastic Cloud Enterprise (ECE) et d'Elastic Cloud sur Kubernetes (ECK)

Nous contacter

# Services at a Glance



## Elastic Training

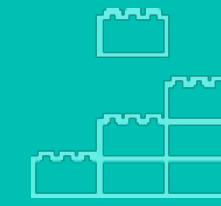
- Immersive learning experience
- Solution-based curriculum
- Flexible ways-to-train

**People Strategy**



## Certification

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



## Elastic Consulting

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

**Project Strategy**

# Free on-demand training

We're releasing **free** on-demand courses over the next few weeks. We know social distancing isn't fun, but it can be a great opportunity to learn new things. So while other people are making a second pass through their Netflix queue, you can build your [Elastic Stack](#), [observability](#), and [security](#) skills and come out the other side an expert.

## Observability

---

<a href="#">Observability Fundamentals</a>	Fundamental skills for achieving observable systems with the Elastic Stack.	<a href="#">Register</a>
<a href="#">Kibana for Splunk SPL Users</a>	For users of Splunk's Search Processing Language (SPL) that would like to translate their analysis skills to Kibana and Elasticsearch.	<a href="#">Register</a>
<a href="#">Introduction to Observability: Logging</a>	Fundamentals of shipping, analyzing, and visualizing log data for system observability.	<a href="#">Register</a>
<a href="#">Metrics Fundamentals</a>	Fundamental skills for building high-capacity metric systems. You will learn about common metrics problems and their solutions.	Coming April 20
<a href="#">APM Fundamentals</a>	Fundamental skills for monitoring software services and applications in real time.	Coming April 20

## Security

---

<a href="#">Elastic Endpoint Security Fundamentals</a>	Fundamental skills for utilizing Elastic Endpoint Security to protect those endpoints.	<a href="#">Register</a>
<a href="#">Anomaly Detection for Cybersecurity</a>	Learn how anomaly detection with Elastic machine learning can help you quickly and efficiently detect security threats, regardless of data size.	<a href="#">Register</a>

<https://training.elastic.co/learn-from-home>



# 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



# 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)

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 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?

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 Google');  
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 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

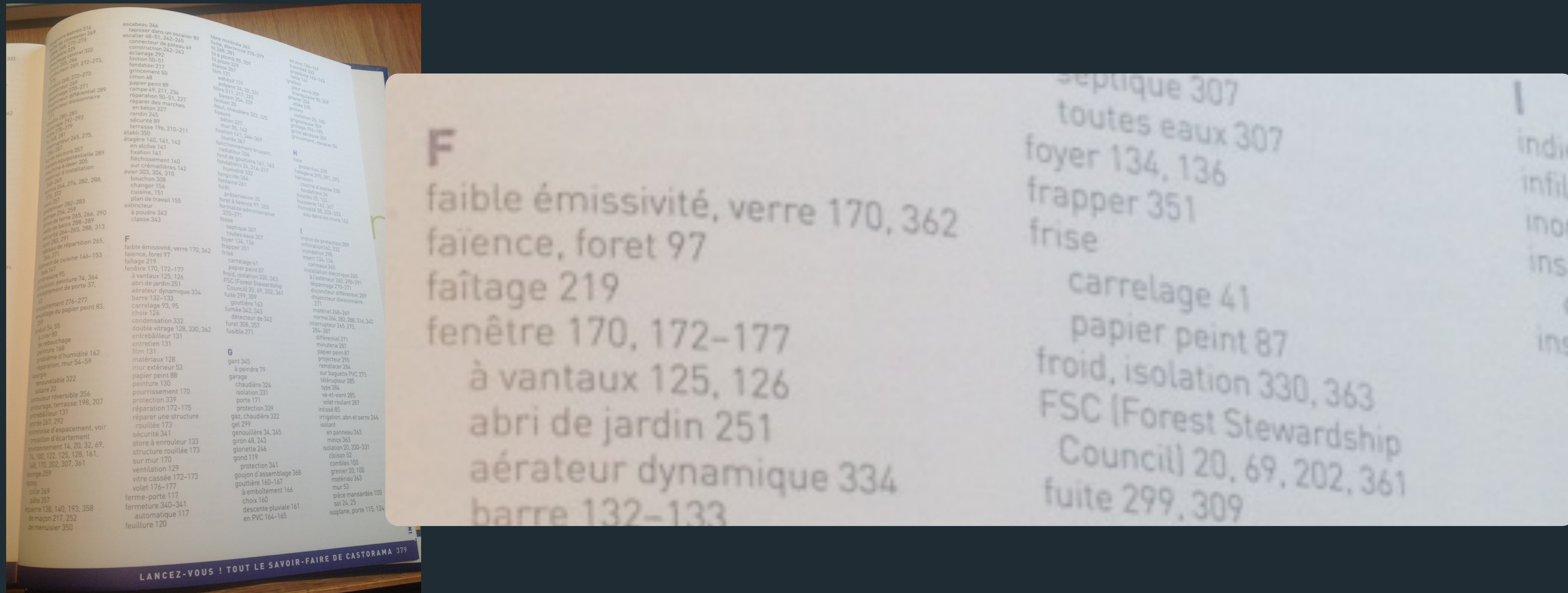
between  and

between  and



# Search engine?

## Moteur d'indexation de documents



## Moteur de recherche dans les index



Demo time!



# 3 solutions powered by 1 stack



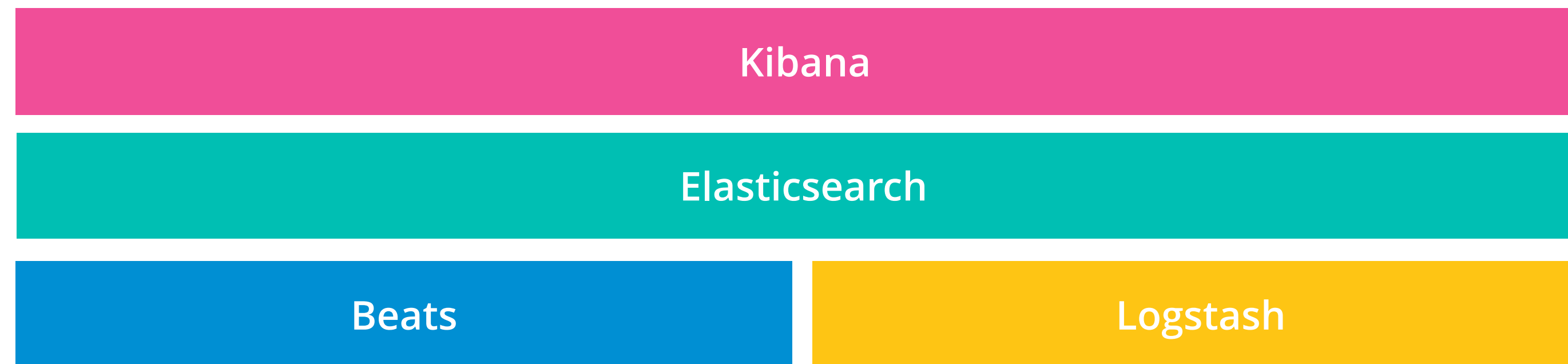
Elastic Enterprise Search



Elastic Observability



Elastic Security



Elastic Stack



# Elastic Enterprise Search

---

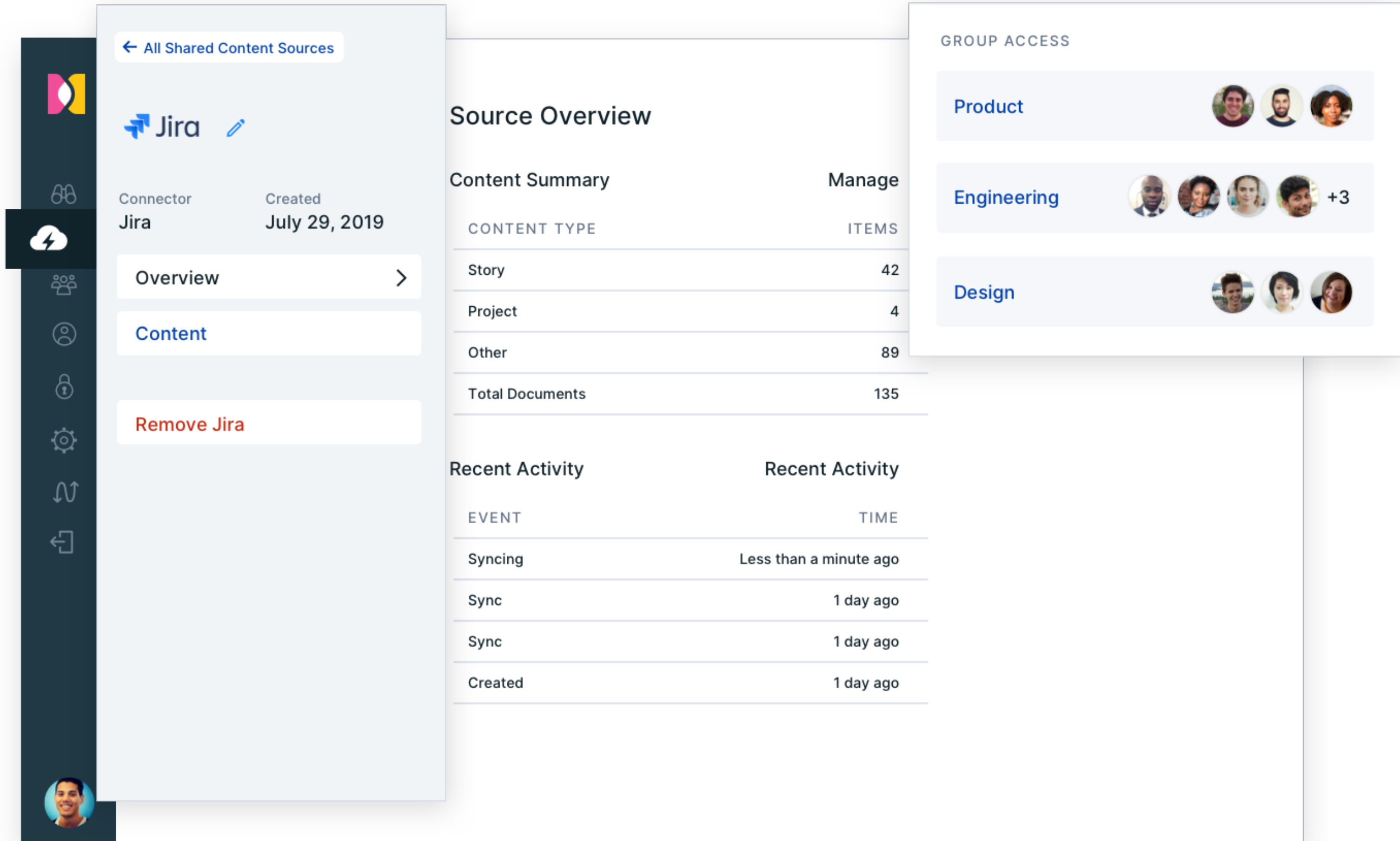
Workplace Search

App Search

Site Search

# 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
<b>Total Documents</b>	<b>135</b>

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 list of groups with their members:
  - Product: 3 members
  - Engineering: 4 members (+3 more)
  - Design: 3 members



# Elastic Observability

---

Logs

Metrics

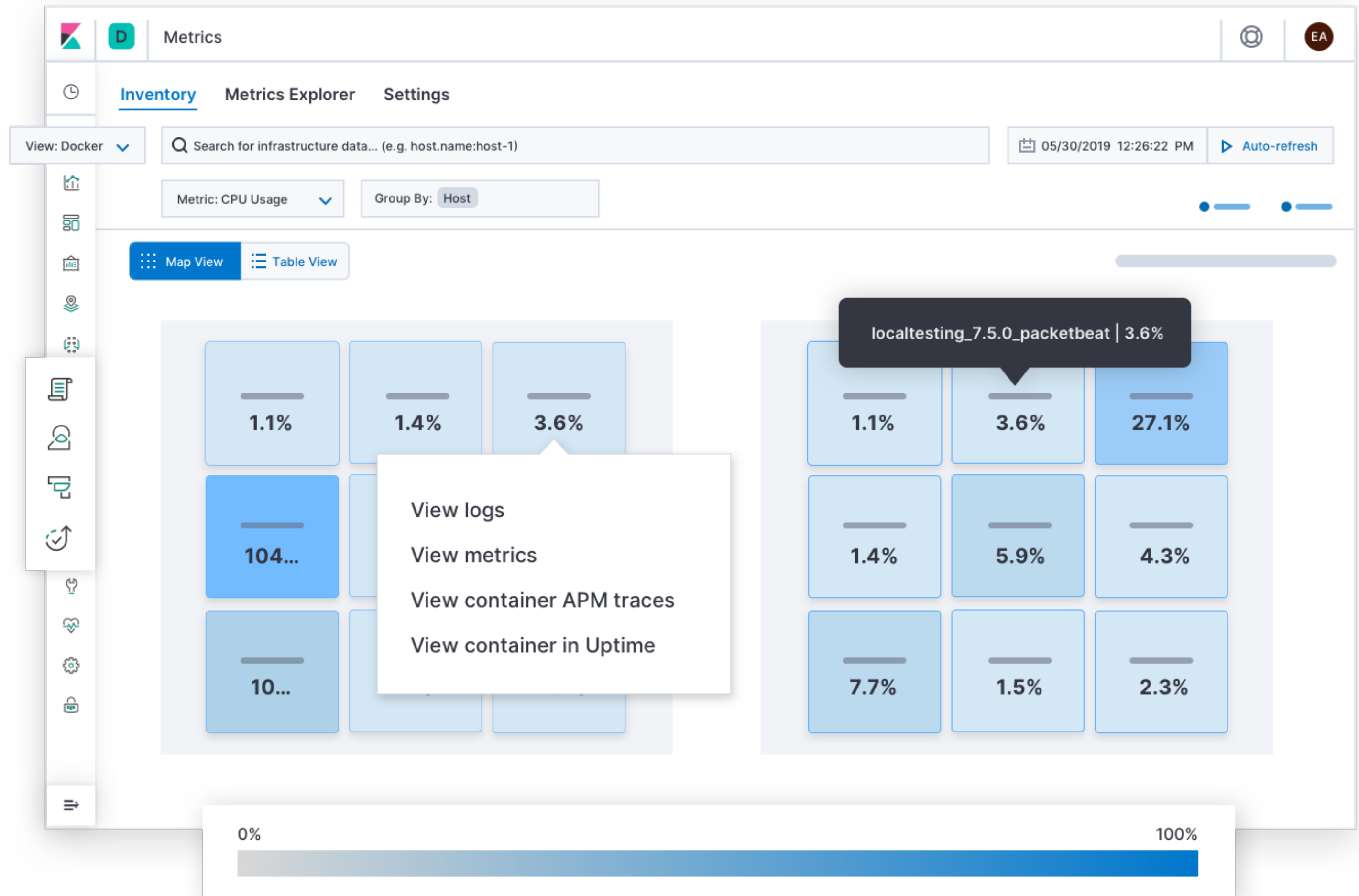
APM

Uptime



# 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 Security

---

Endpoint

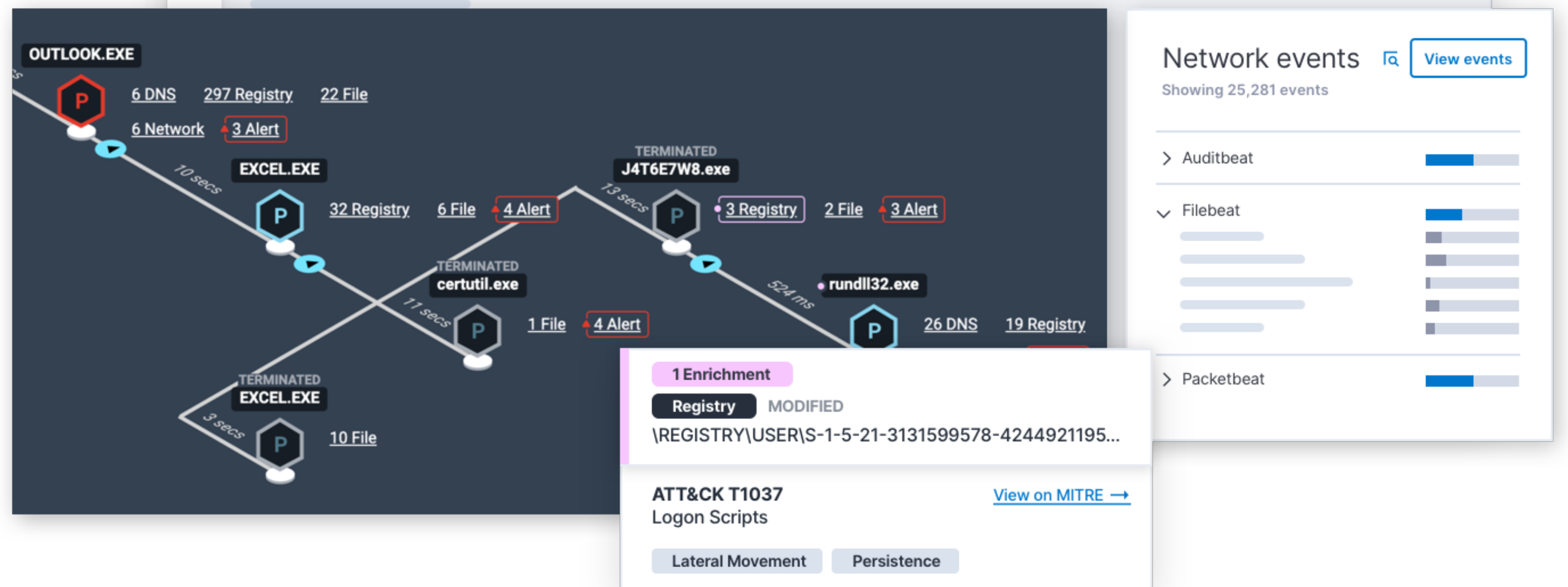
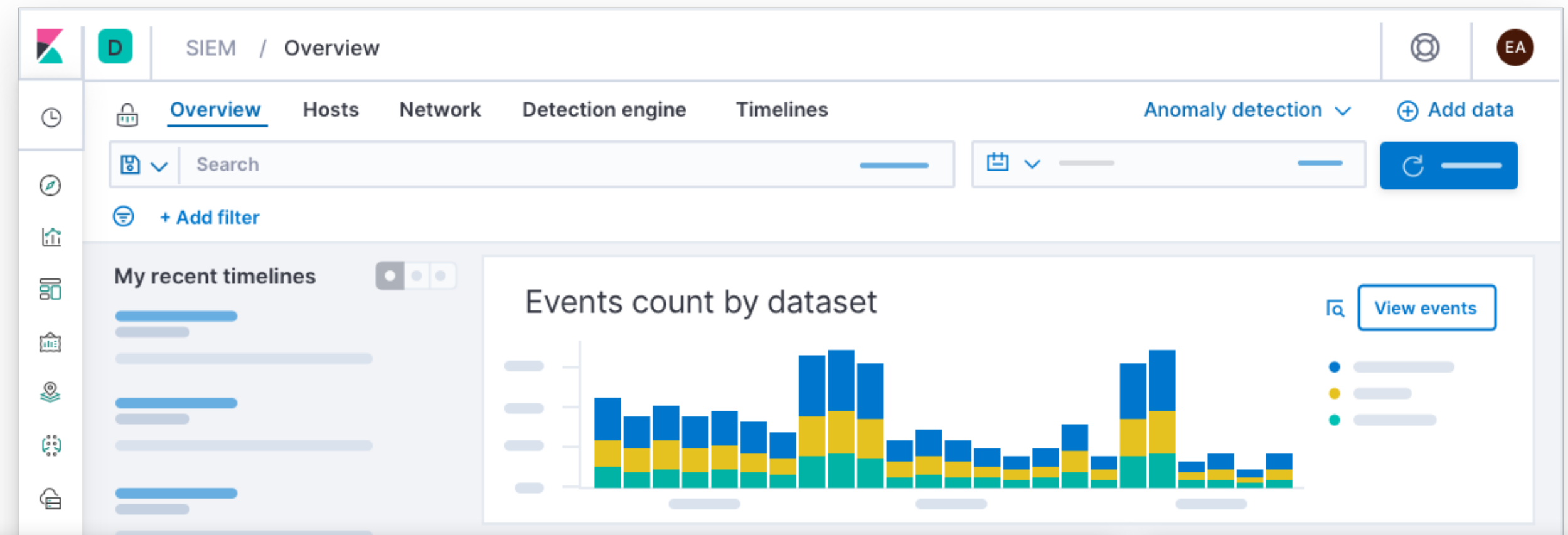
SIEM





# 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.



# Deploy anywhere.

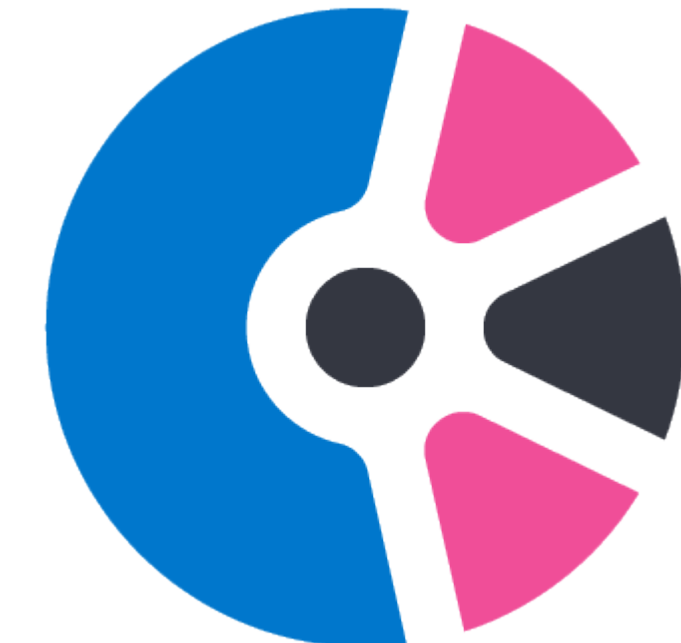


**Elastic Cloud**

SaaS



**Elastic Cloud  
Enterprise**



**Elastic Cloud on  
Kubernetes**

Orchestration



# Family of SaaS Offerings

Easily launch, operate, and scale deployments on AWS, GCP, or Azure with a SaaS experience tailor-made for Elastic products and solutions.

The screenshot displays the Elastic Cloud console interface for configuring a deployment. The main view is titled "First cluster Edit" and shows a "Data" section with a slider for "RAM per Node" set to 8 GB. Below this, there are radio buttons for "Fault tolerance" (1 zone, 2 zones, 3 zones) and a "Summary" section with a calculation: 1 GB RAM x 1 instance x 1 zone = 1 GB RAM.

A modal window titled "Kibana 1 configuration" is open, showing a "RAM per Node" slider set to 1 GB and an "Instances" input field set to 1. The "Summary" section in the modal shows: 1 GB RAM x 1 instance x 1 zone = 1 GB RAM. Below the modal, there is a "User settings overrides" link.

On the right side of the console, there is a "Summary" table and an "Architecture" diagram. The "Summary" table lists the following details:

Name	First Cluster
Version	v7.0.1
ES data memory	24 GB
ES data storage	1.25 TB
Total memory	25.5 GB
Total storage	1.25 TB
Hourly rate	\$0.8281
Monthly rate	\$604.51

The "Architecture" diagram shows two zones. Zone 1 contains three nodes: two "gcp.data.hi..." nodes with 8 GB RAM and one "gcp.kibana.1" node with 1 GB RAM. Zone 2 contains two "gcp.data.hi..." nodes with 8 GB RAM. A "gcp.apm.1" node with 512 MB RAM is also shown between the zones.



# Centrally manage your Elastic deployments

Provision, manage, and monitor Elastic products and solutions, at any scale, on any infrastructure, while managing everything from a single console.

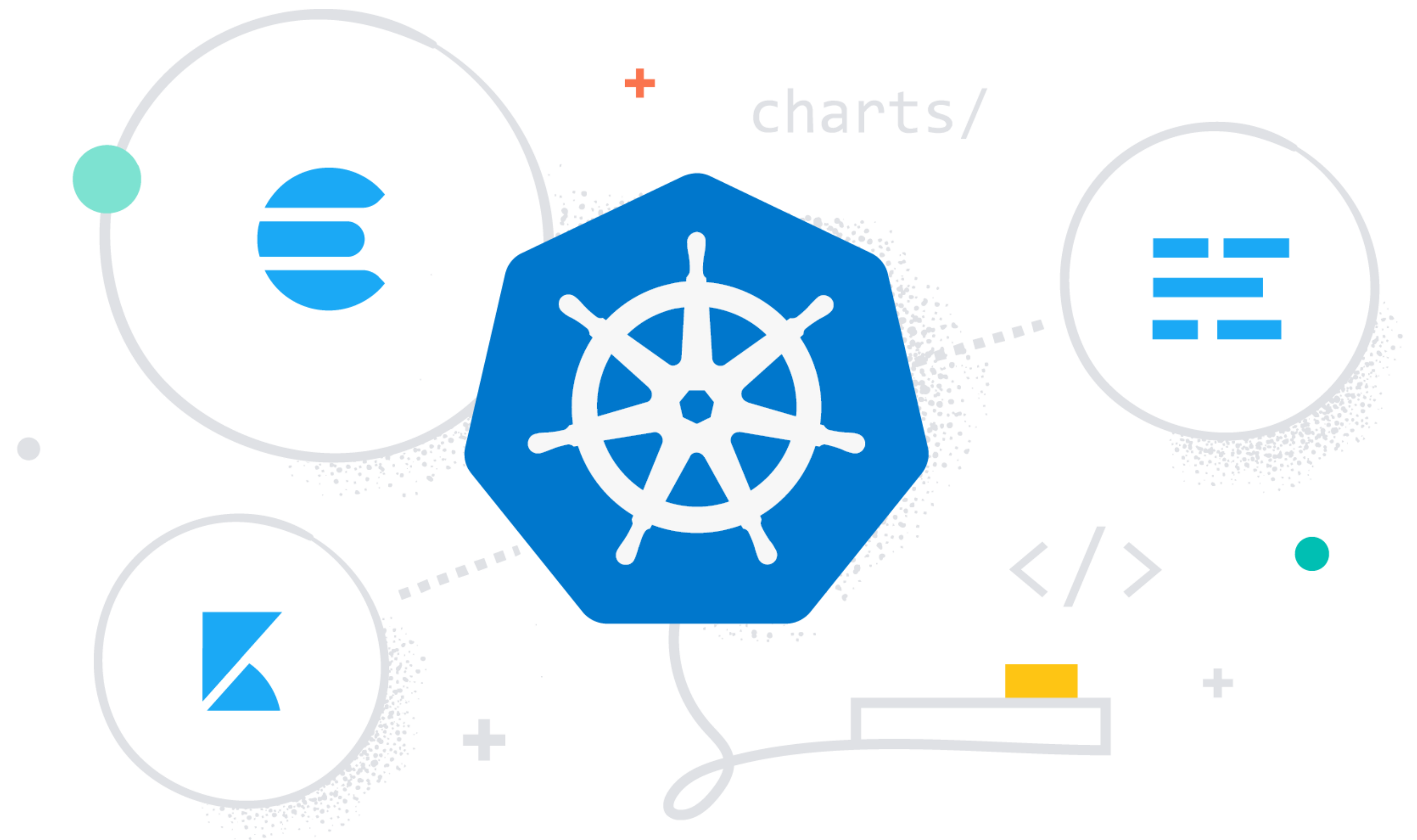
The screenshot displays the Elastic Cloud Enterprise console interface. On the left is a navigation menu with sections for 'Deployments' and 'Platform', including options like 'Summary', 'Allocators', 'Runners', 'Proxies', 'Elastic Stack', 'Templates', 'Repositories', 'Settings', and 'Activity Feed'. The main area shows a summary for 'ece-region' with metrics: 3 Zones, 9 Allocators, 88.72 GB Available capacity, 1 Proxies, 7 Elasticsearch clusters, and 6 Kibana instances. Below this, a 'Your installation' section shows three zones: 'ece-zone-0', 'ece-zone-1', and 'ece-'. A detailed view for 'ece-zone-0' is overlaid, showing two runners: '192.168.44.10' and '192.168.44.13'. Each runner has a list of roles and containers. The runner at 192.168.44.10 has roles: allocator, coordinator, director, proxy and containers: admin-console, allocator, beats-runner, blueprint, client-forwarder, cloud-ui, constructor, curator, director, proxy, runner, services-forwarder, zookeeper. The runner at 192.168.44.13 has roles: allocator and containers: allocator, beats-runner, client-forwarder, runner, services-forwarder. A table at the bottom provides a detailed view of the 'ece-zone-0' allocators, showing their IP addresses, instance distribution (4 GB and 1 GB), and tags (env: prod, team: devops, zone:00).

Allocator	Instance distribution	Tags
192.168.44.16	4 GB, 1 GB	env: prod, team: devops, zone:00
192.168.44.10	4 GB, 1 GB	env: prod, team: devops, zone:00



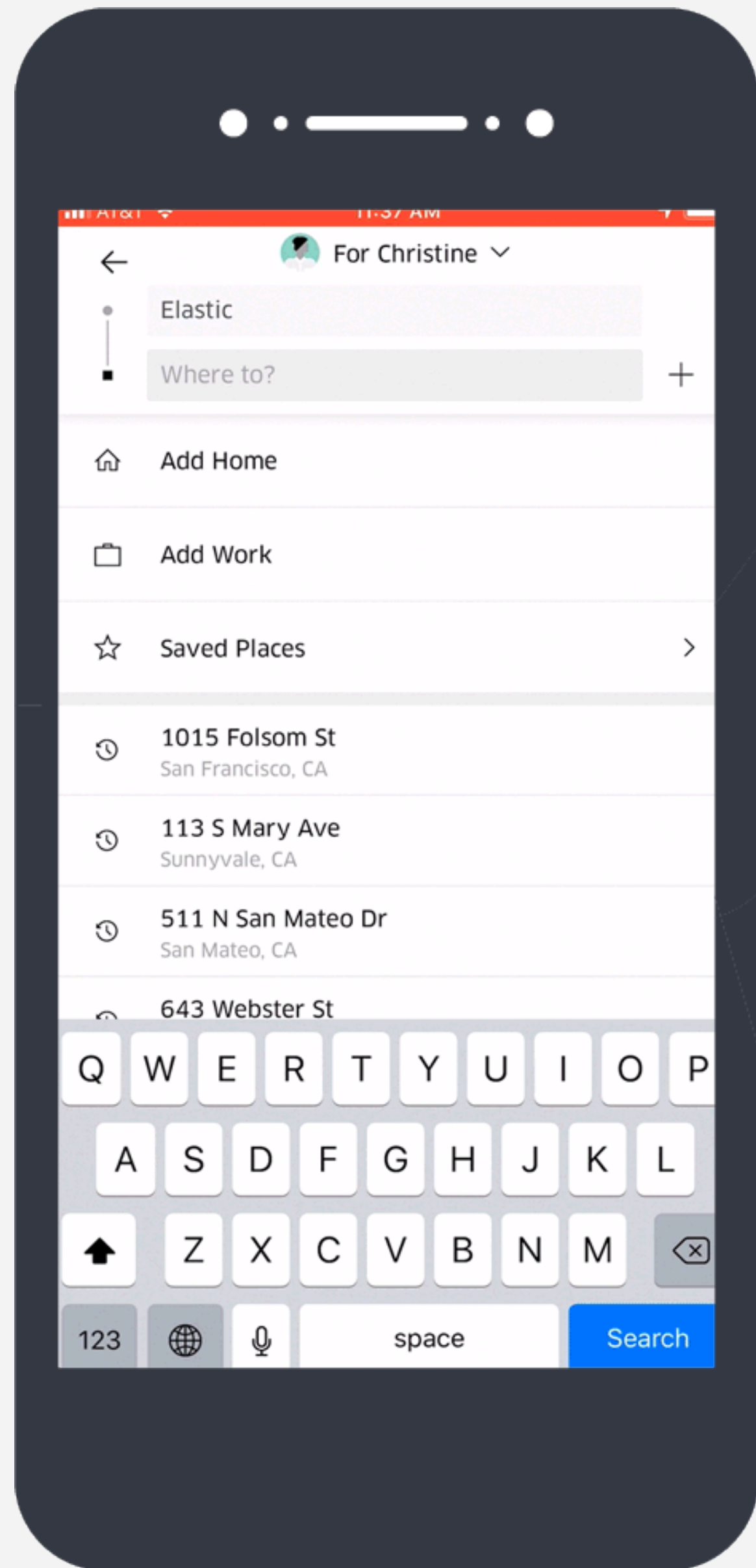
# Official Operator, and much more

Simplify setup, upgrades, snapshots, scaling, high availability, security, and more when running Elastic products and solutions on Kubernetes.

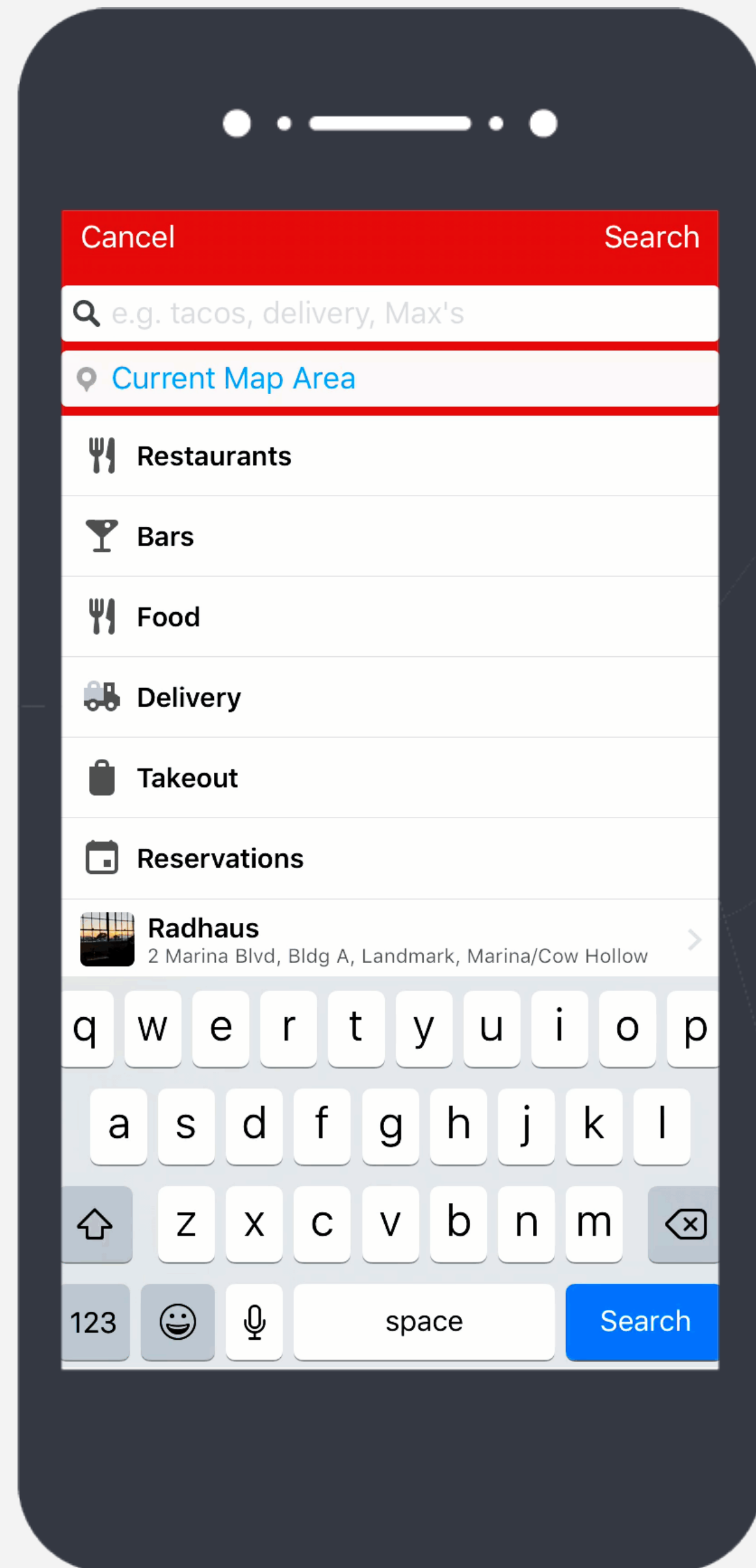




 <b>HSBC</b>		 <b>SOUNDCLOUD</b>	 <b>mozilla</b> FOUNDATION	 <b>Microsoft</b>
<b>GROUPON</b>	<b>facebook</b>	 <b>Expedia</b>	<b>vimeo</b>	 <b>salesforce</b>
 <b>FOURSQUARE</b>		<b>ACTIVISION</b> <b>BLIZZARD</b>	 <b>stack overflow</b>	
	 <b>Symantec</b>		<b>The New York Times</b>	 <b>Unilever</b>
<b>ebay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

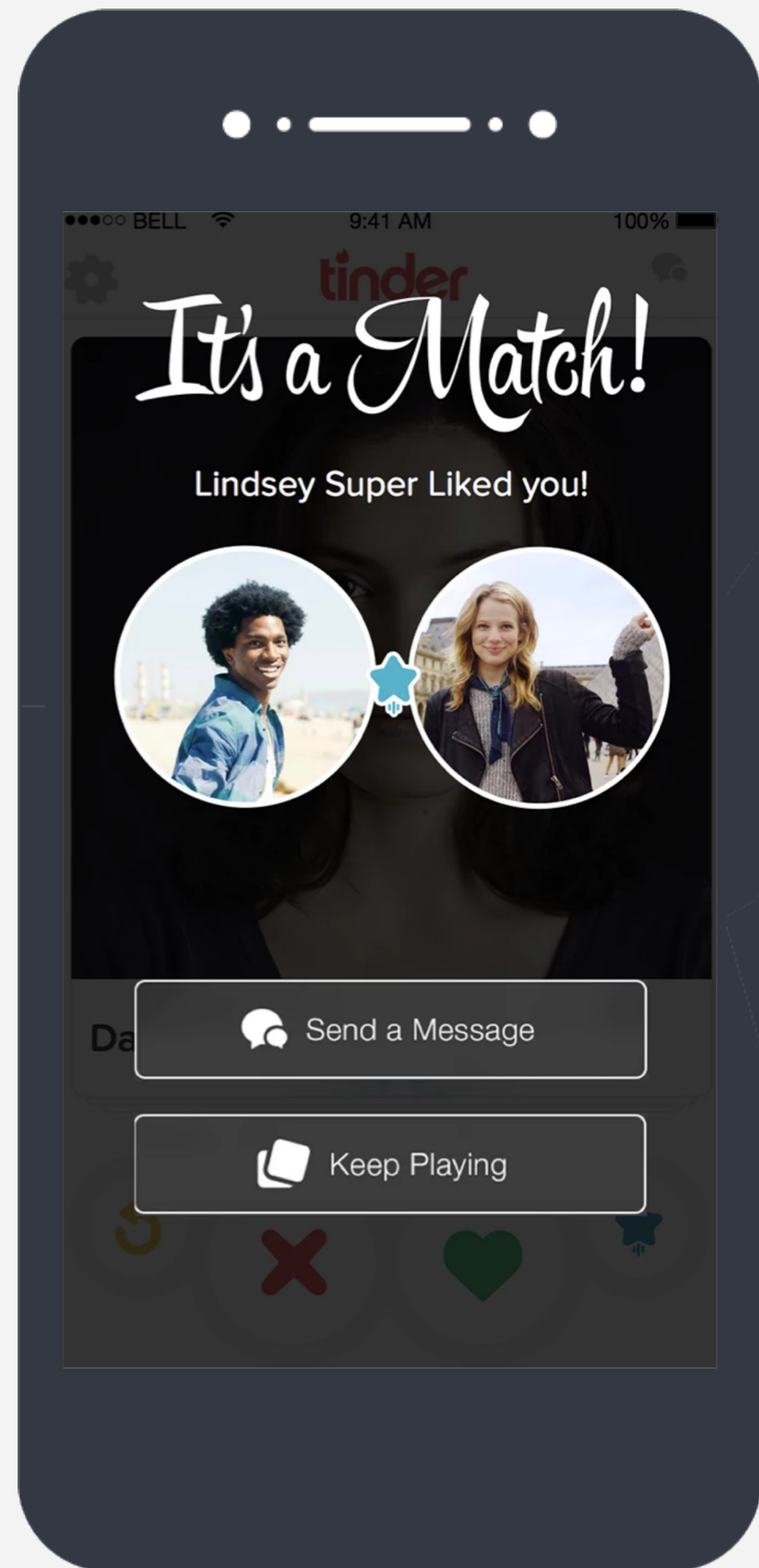


# Searching for **Rides**

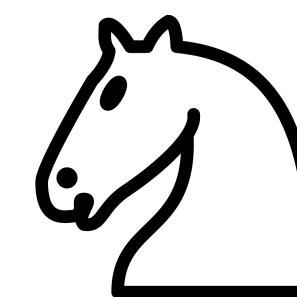


# Searching for **Restaurants**





# Searching for **Love**





#ElasticStories



# Free on-demand training

We're releasing **free** on-demand courses over the next few weeks. We know social distancing isn't fun, but it can be a great opportunity to learn new things. So while other people are making a second pass through their Netflix queue, you can build your [Elastic Stack](#), [observability](#), and [security](#) skills and come out the other side an expert.

## Observability

---

<a href="#">Observability Fundamentals</a>	Fundamental skills for achieving observable systems with the Elastic Stack.	<a href="#">Register</a>
<a href="#">Kibana for Splunk SPL Users</a>	For users of Splunk's Search Processing Language (SPL) that would like to translate their analysis skills to Kibana and Elasticsearch.	<a href="#">Register</a>
<a href="#">Introduction to Observability: Logging</a>	Fundamentals of shipping, analyzing, and visualizing log data for system observability.	<a href="#">Register</a>
<a href="#">Metrics Fundamentals</a>	Fundamental skills for building high-capacity metric systems. You will learn about common metrics problems and their solutions.	Coming April 20
<a href="#">APM Fundamentals</a>	Fundamental skills for monitoring software services and applications in real time.	Coming April 20

## Security

---

<a href="#">Elastic Endpoint Security Fundamentals</a>	Fundamental skills for utilizing Elastic Endpoint Security to protect those endpoints.	<a href="#">Register</a>
<a href="#">Anomaly Detection for Cybersecurity</a>	Learn how anomaly detection with Elastic machine learning can help you quickly and efficiently detect security threats, regardless of data size.	<a href="#">Register</a>

<https://training.elastic.co/learn-from-home>





ElasticFR

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



@elasticfr



elastic

User Group

[discuss.elastic.co](https://discuss.elastic.co)

