



# Elastic Stack Overview

Search. Observe. Protect.



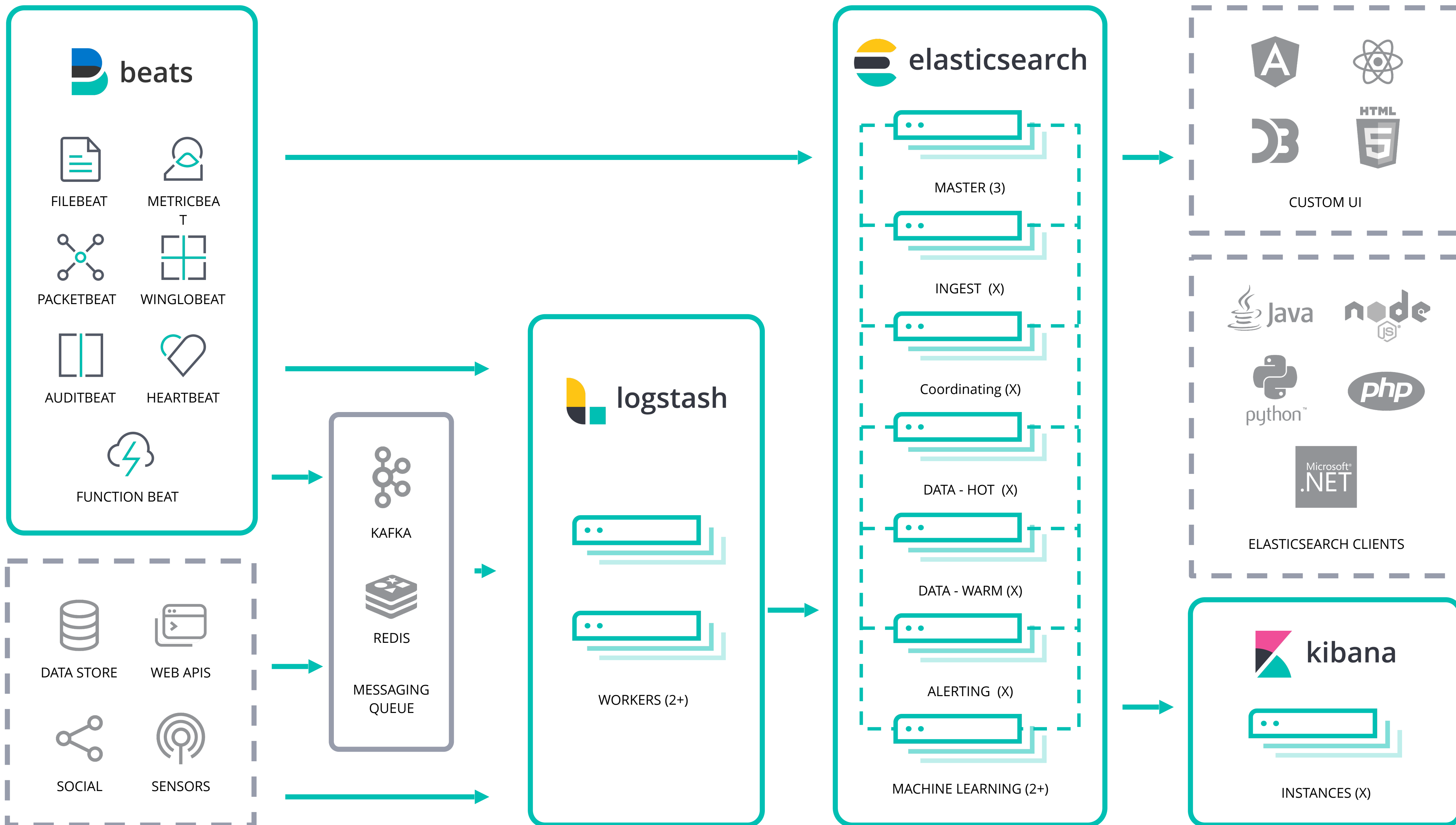
# Who?

```
$ 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

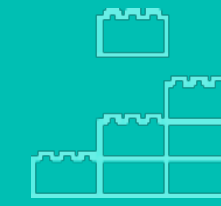
- Immersive learning experience
- Solution-based curriculum
- Flexible ways-to-train

**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**

# 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



### EXPERIENCED INSTRUCTORS

Expertly trained and deeply rooted in everything Elastic



### SOLUTION-BASED CURRICULUM

Real-world examples and common use cases



### 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)
```

David



# 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

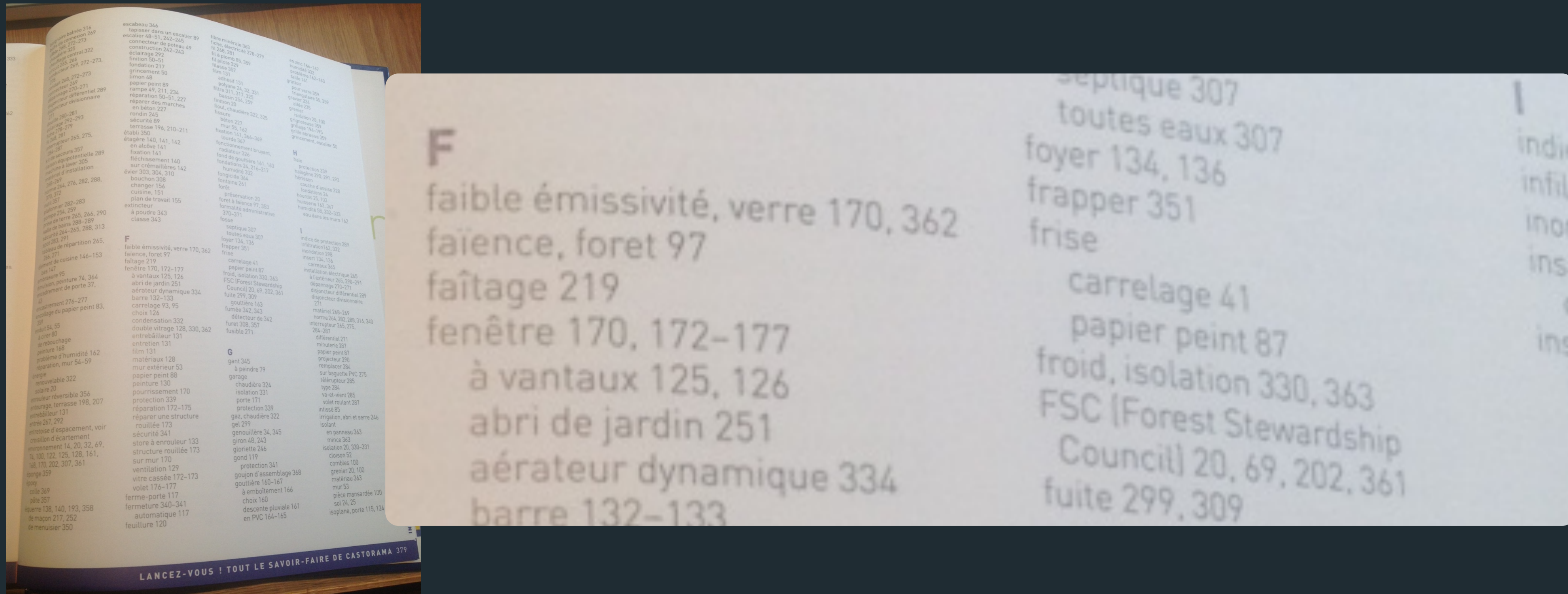
between  and

between  and

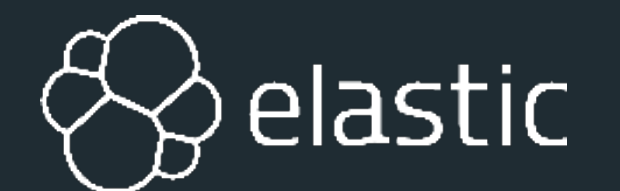
between  and

# 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

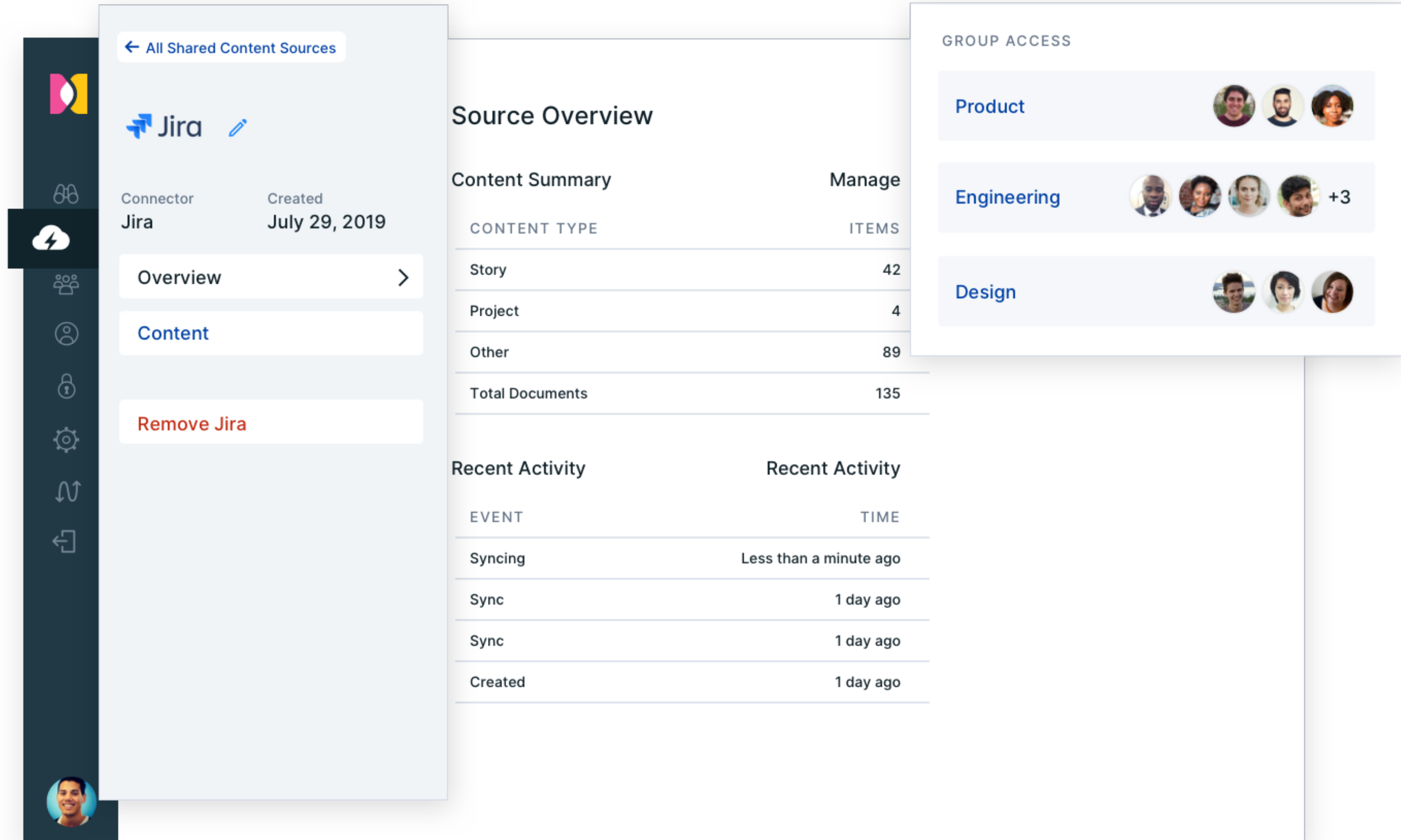
App Search

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 and recent activity.

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:** A list of groups with associated user avatars: Product (3 users), Engineering (+3 users), and Design (3 users).



# Elastic Observability

---

Logs

Metrics

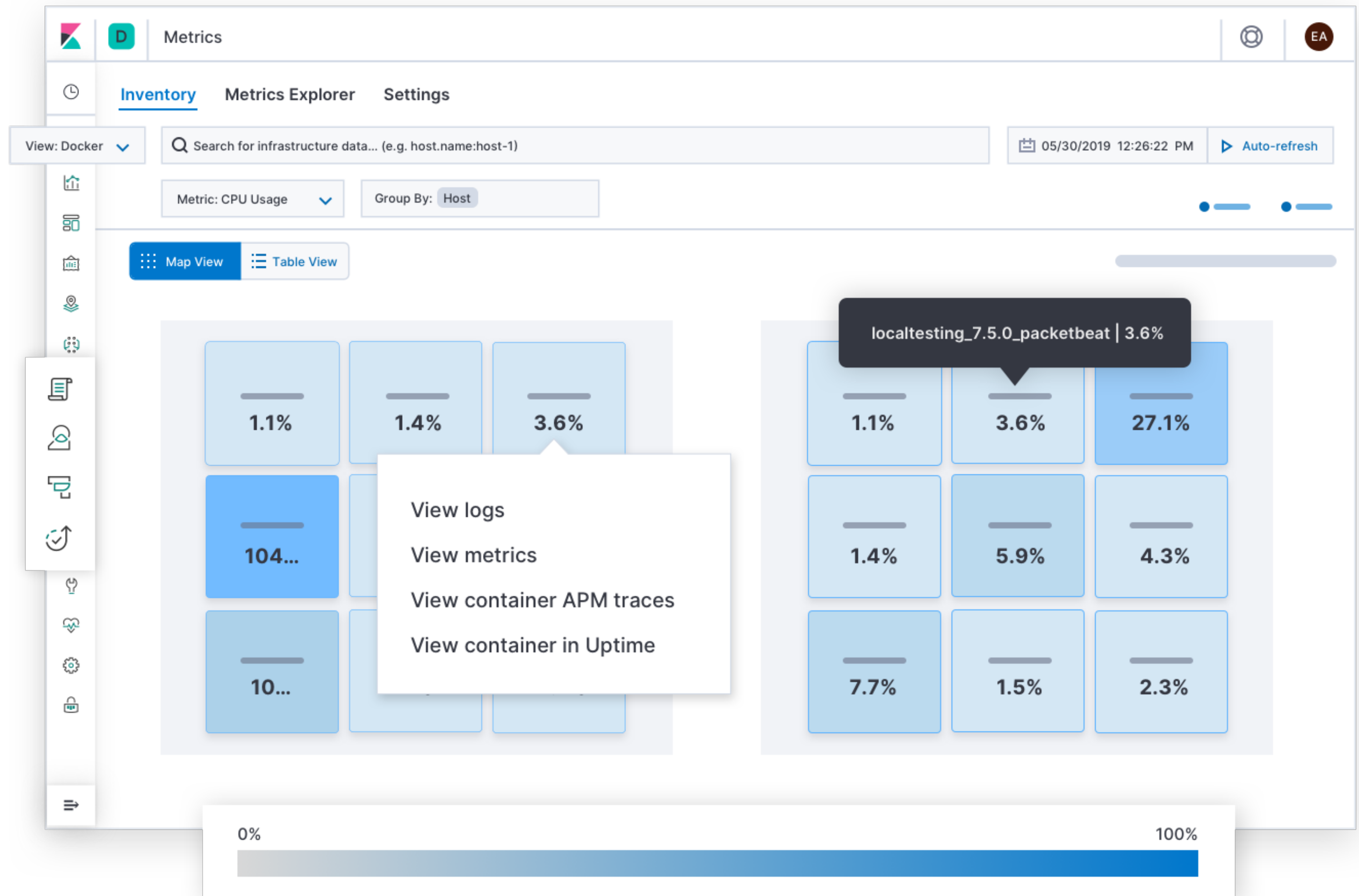
APM

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

---

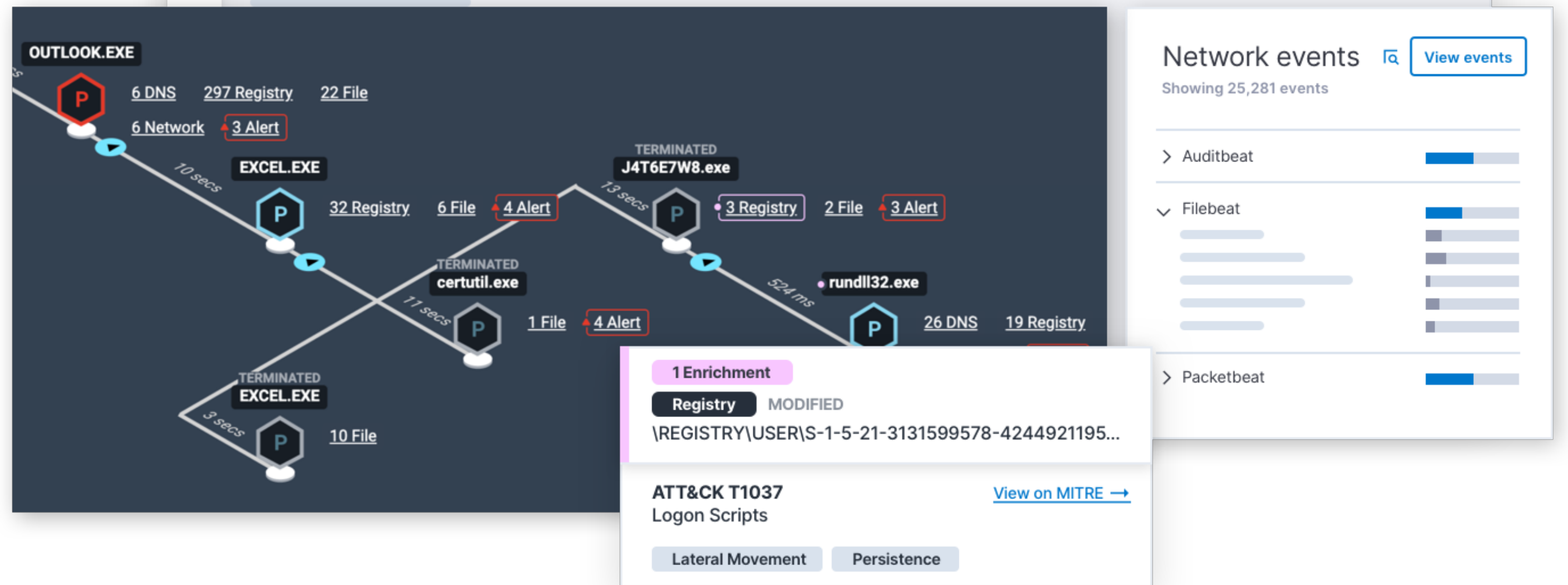
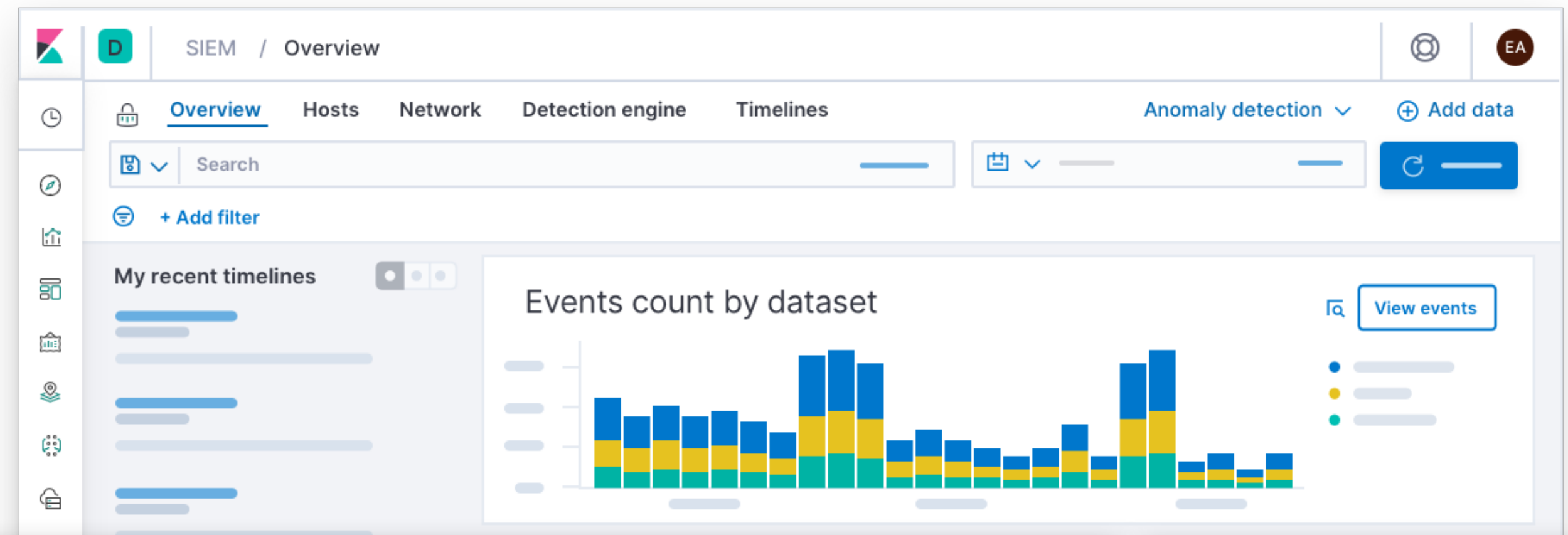
Endpoint

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**

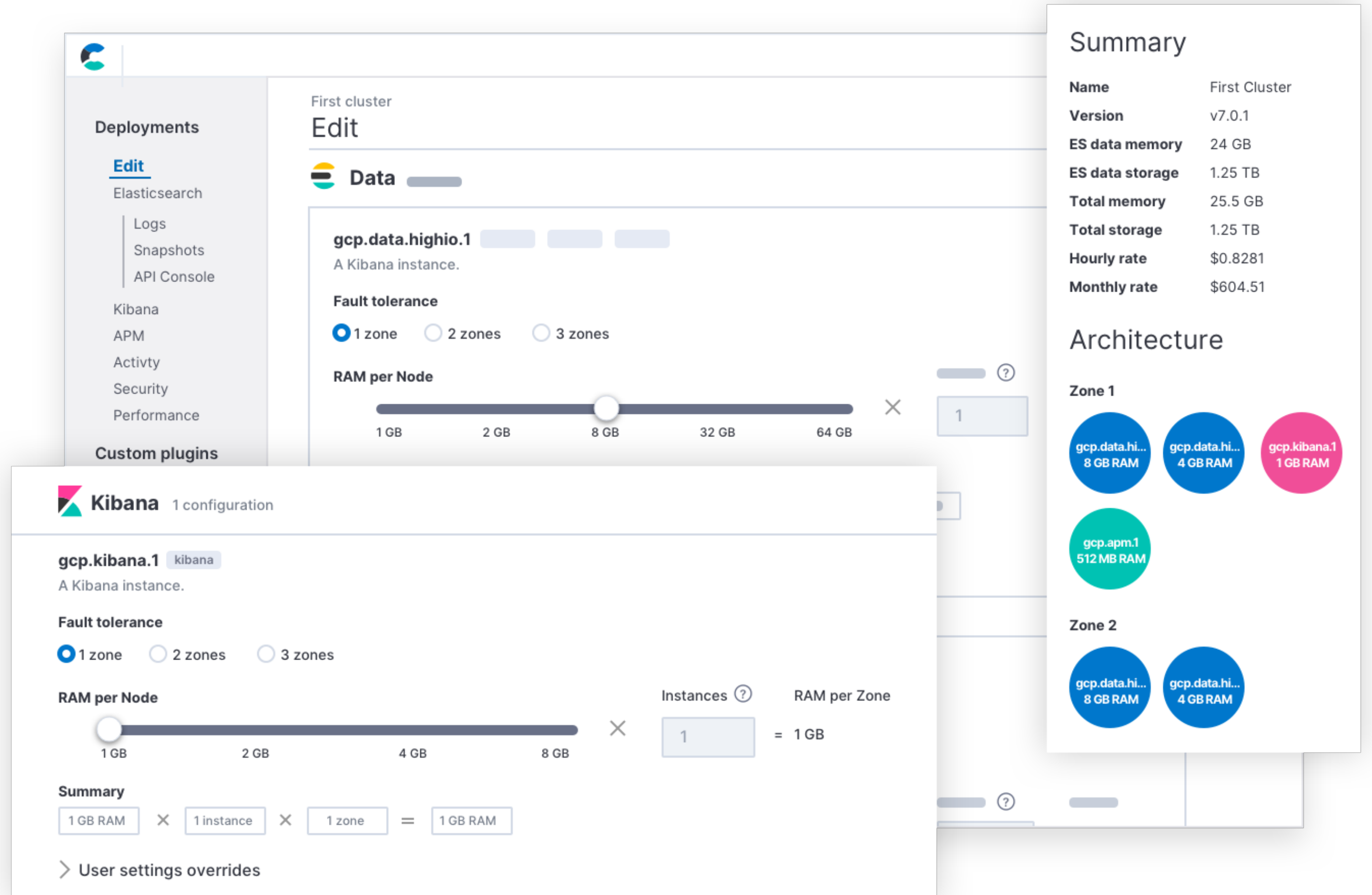


**Elastic Cloud on  
Kubernetes**

Orchestration

 ELASTIC CLOUD  
**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. On the left, a sidebar lists various services under 'Deployments', including Elasticsearch, Logs, Snapshots, API Console, Kibana, APM, Activity, Security, Performance, and Custom plugins. The main area shows the configuration for a 'First cluster' Kibana instance named 'gcp.kibana.1'. It includes options for 'Fault tolerance' (1, 2, or 3 zones) and a 'RAM per Node' slider (1 GB to 8 GB). A summary box at the bottom shows the configuration: 1 GB RAM x 1 instance x 1 zone = 1 GB RAM. On the right, a 'Summary' panel lists cluster 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), and Monthly rate (\$604.51). Below the summary is an 'Architecture' diagram showing nodes in Zone 1 (gcp.data.hi... 8 GB RAM, gcp.data.hi... 4 GB RAM, gcp.kibana.1 1 GB RAM) and Zone 2 (gcp.data.hi... 8 GB RAM, gcp.data.hi... 4 GB RAM), along with a gcp.apm.1 node (512 MB RAM).



# 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.

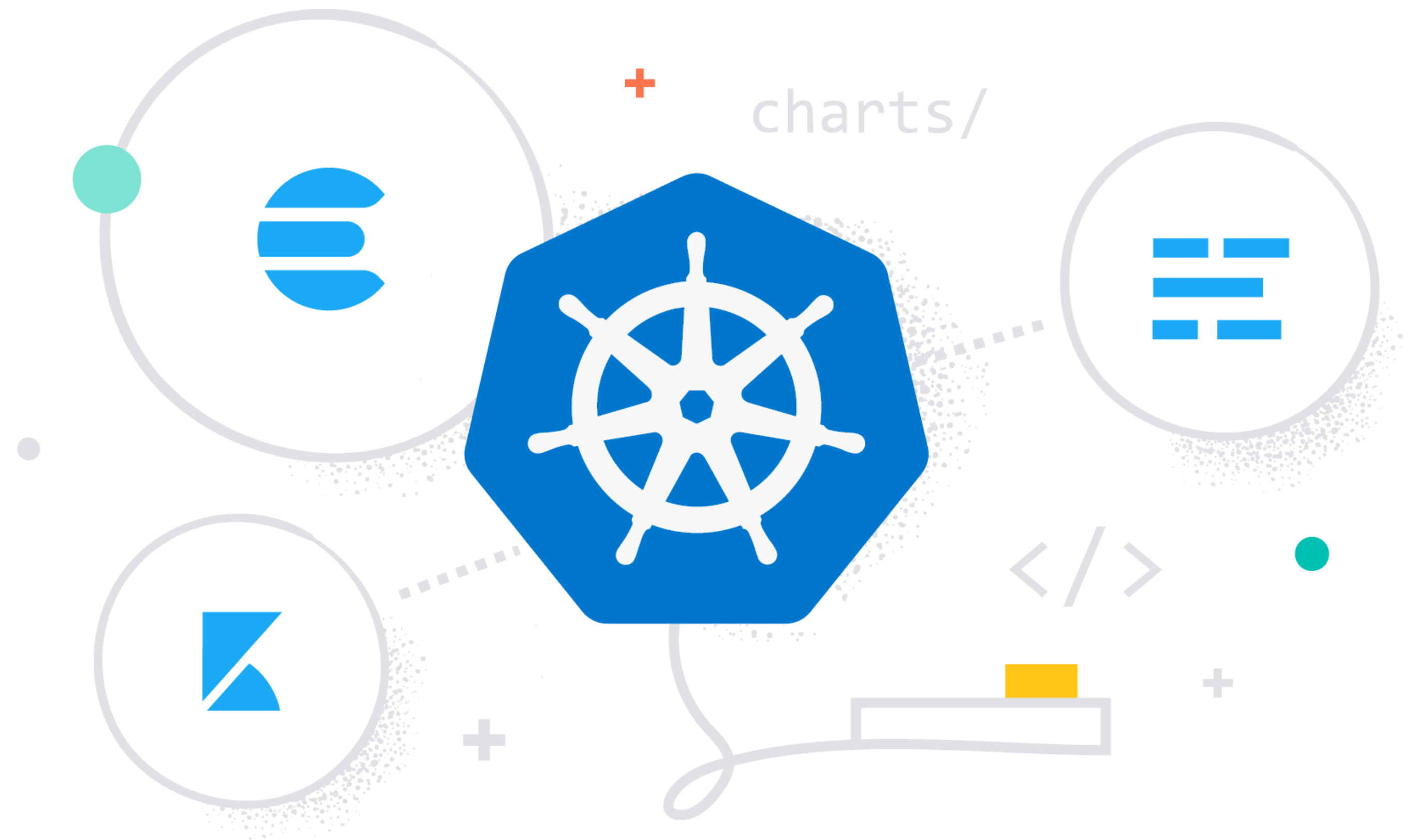
The screenshot displays the Elastic Cloud Enterprise console interface. On the left, a navigation menu includes 'Deployments', 'Platform' (with sub-items: Summary, Allocators, Runners, Proxies, Elastic Stack, Templates, Repositories, Settings), and 'Activity Feed'. The main content area shows a summary 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-zone-2'. Two detailed panels are overlaid on the right side, showing details for 'ece-zone-0'. The top panel shows two runners: '192.168.44.10' and '192.168.44.13', both with status checkmarks. The bottom panel shows an 'Allocator' for 'ece-zone-0' with an available capacity of 27.57 GB. It lists instance distribution with a bar chart showing 4 GB of Kibana and 1 GB of Elasticsearch. The instance list includes IP addresses, status checkmarks, and tags like 'env: prod', 'team: devops', and 'zone:00'.



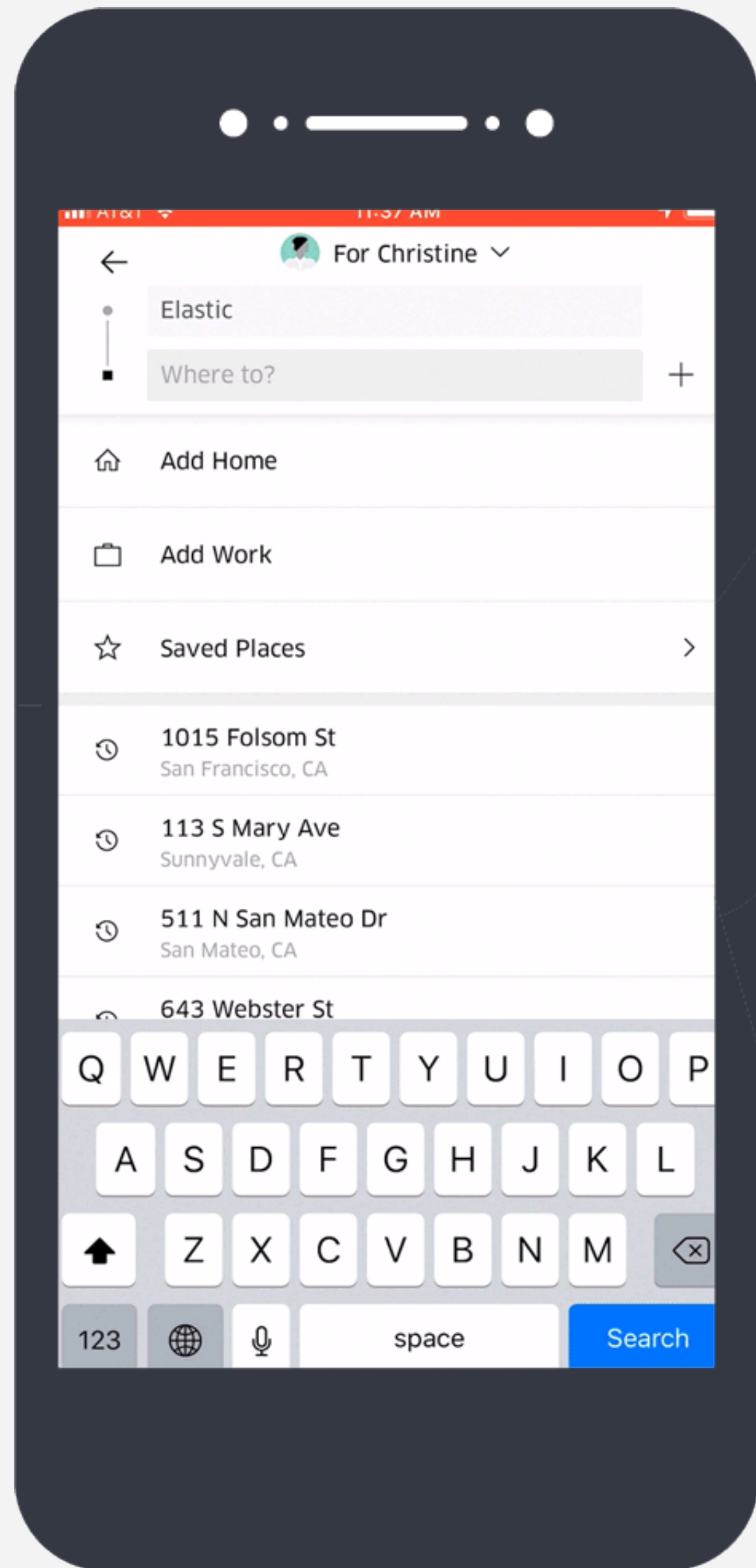


# Official Operator, and much more

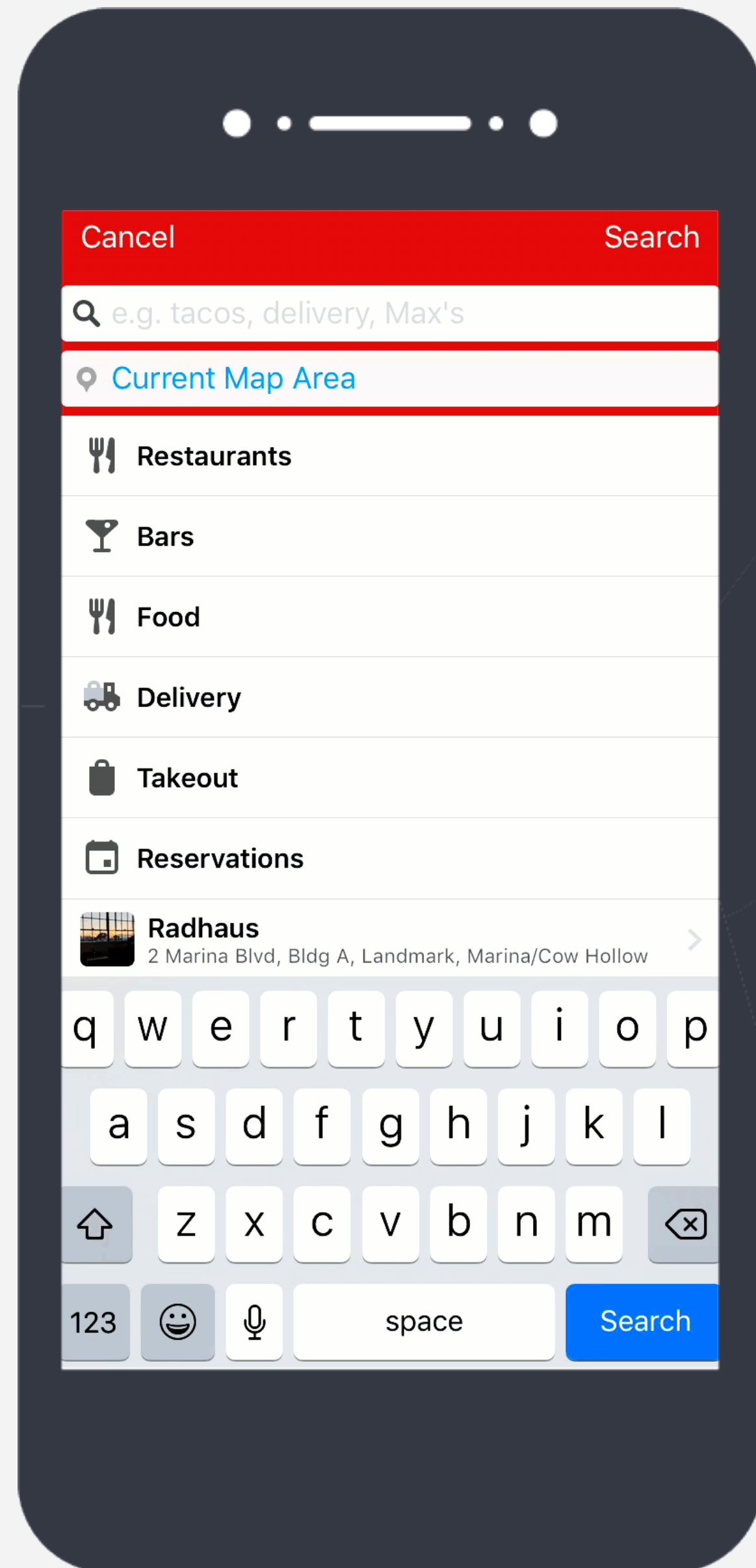
Simplify setup, upgrades, snapshots, scaling, high availability, security, and more when running Elastic products and solutions on Kubernetes.



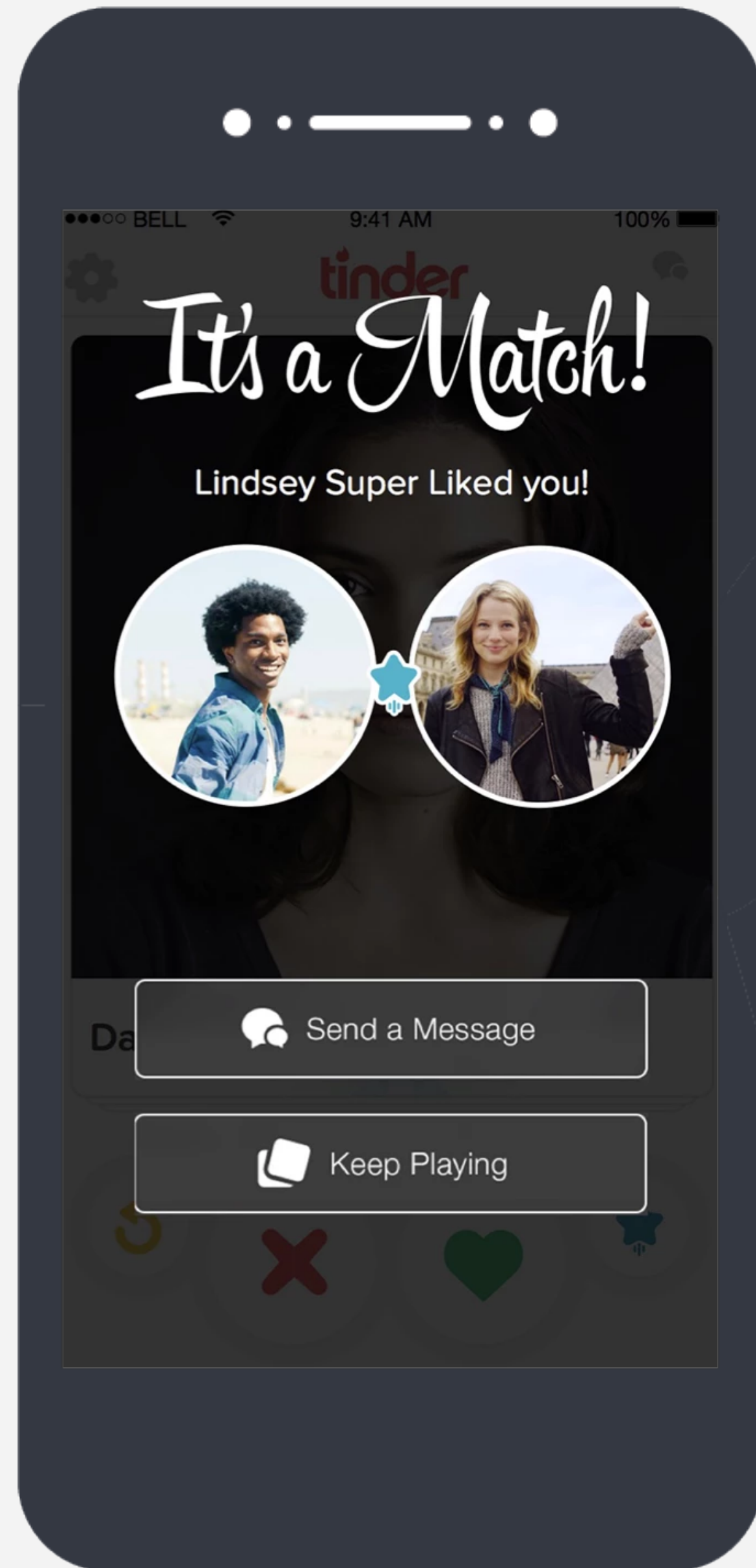
 <b>HSBC</b>		 <b>SOUNDCLOUD</b>	 <b>mozilla</b> FOUNDATION	 <b>Microsoft</b>
<b>GROUPON</b>	<b>facebook</b>	 <b>Expedia</b>	<b>vimeo</b>	 <b>salesforce</b>
 <b>FOURSQUARE</b>		<b>ACTIVISION</b> <b>BLIZZARD</b>	 <b>stack overflow</b>	
	 <b>Symantec</b>		<b>The New York Times</b>	 <b>Unilever</b>
<b>ebay</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>



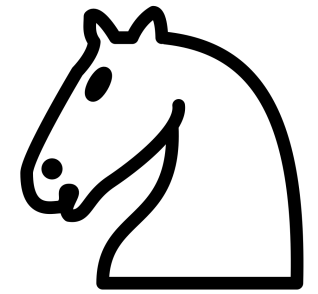
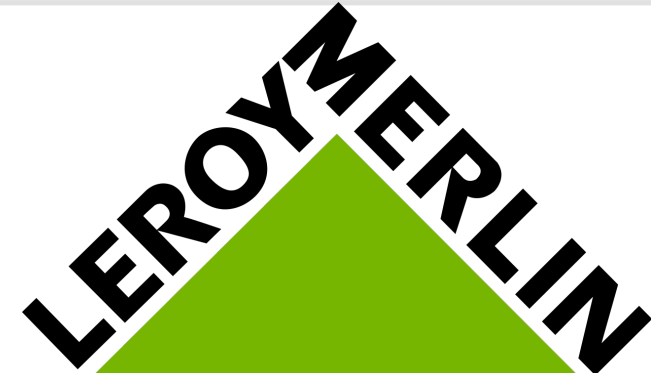
# Searching for **Rides**



# Searching for Restaurants



# Searching for **Love**





#ElasticStories

# 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



### EXPERIENCED INSTRUCTORS

Expertly trained and deeply rooted in everything Elastic



### SOLUTION-BASED CURRICULUM

Real-world examples and common use cases



### 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

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



@elasticfr



elastic

User Group

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

