

**РОЗРОБКА КОМПЛЕКСНОГО ПІДХОДУ  
ДО ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ  
РЕЧЕЙ, ЩО БАЗУЄТЬСЯ НА РАННЬОМУ  
ВИЯВЛЕННІ ЗАГРОЗ І  
ГРАНУЛЬОВАНОМУ КОНТРОЛІ  
ДОСТУПУ**

**Науковий керівник: ст.викладач, к.т.н. Шабінська М. О.**

**Студент: Щербина С. С.**

# Актуальність

Широка  
розповсюдженість  
Інтернету Речей

Наслідки  
компрометації  
безпеки в IoT  
системах

Унікальні  
проблеми у сфері  
захисту Інтернету  
Речей

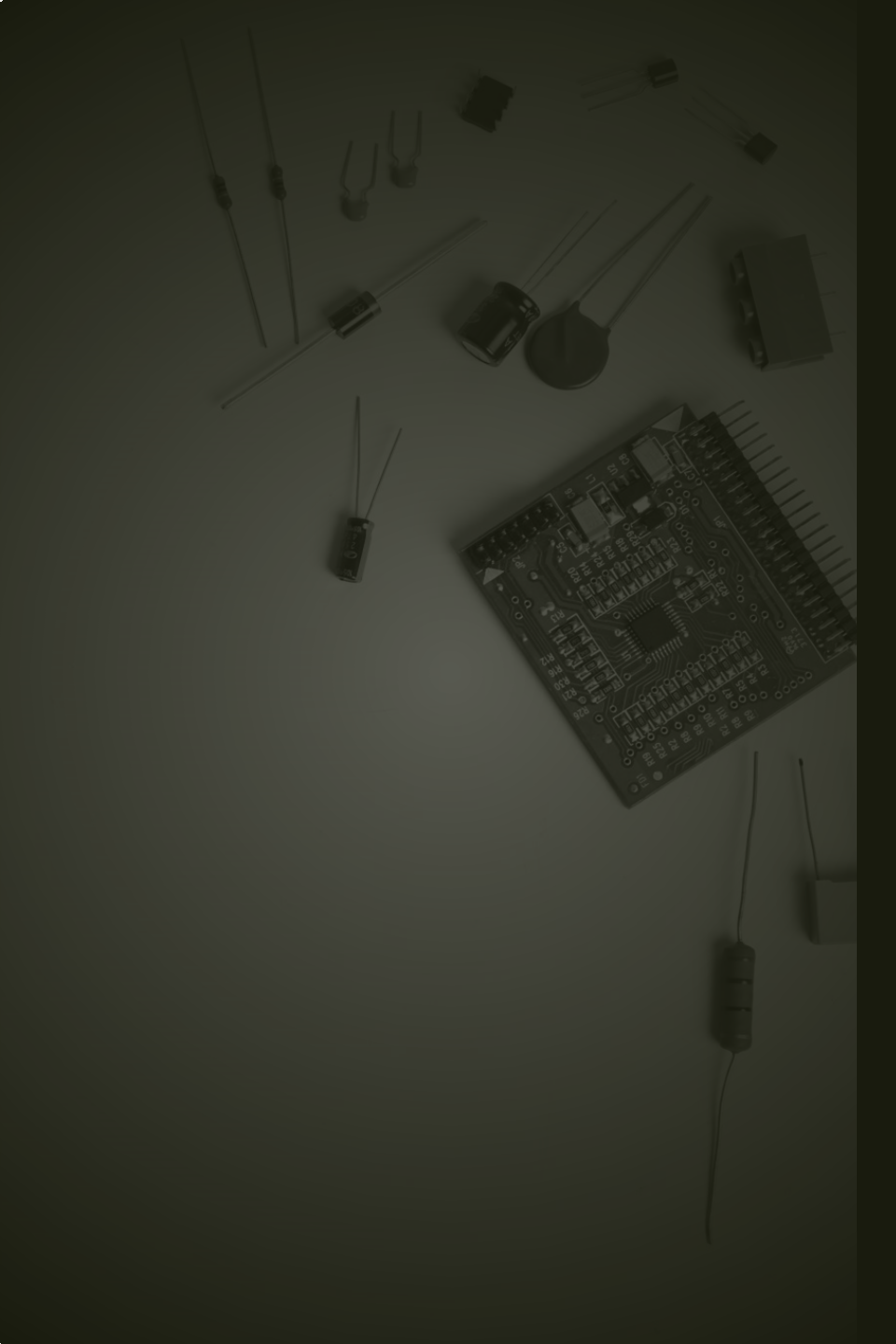
# Мета

1

Дослідження відомих та новітніх підходів до захисту IoT систем

2

Розробка комплексного рішення для захисту IoT систем



# Проблеми облікових даних та довіри

- Стандартні облікові дані
- Централізовані центри довіри
- Традиційні інтерфейси автентифікації та авторизації
- Використання IoT пристроїв в несприятливих умовах



# Шифрування

- TLS / DTLS
- Proxy Re-Encryption
- Novel Tiny Symmetric Encryption Algorithm
- Lightweight CA Cipher (LCC)
- Functional Encryption (FE)

# Проблематика безпеки в IoT системах

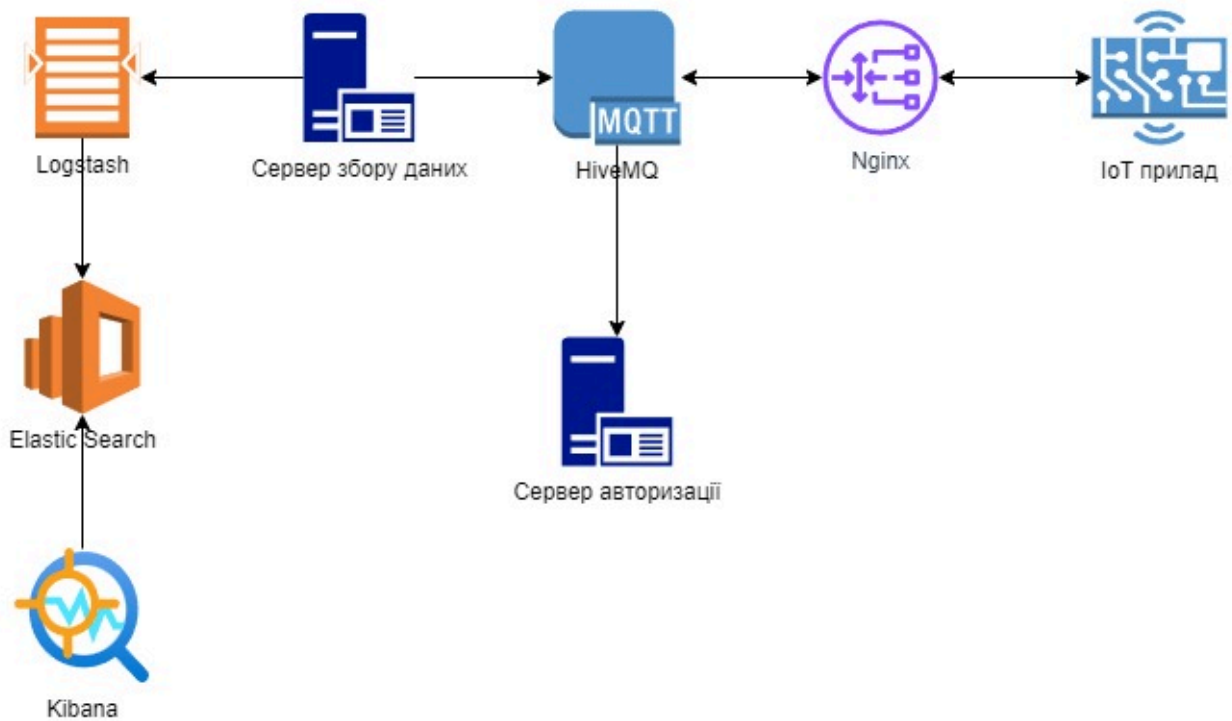
Доменна область

Обмеженість в ресурсах

Способи комунікації

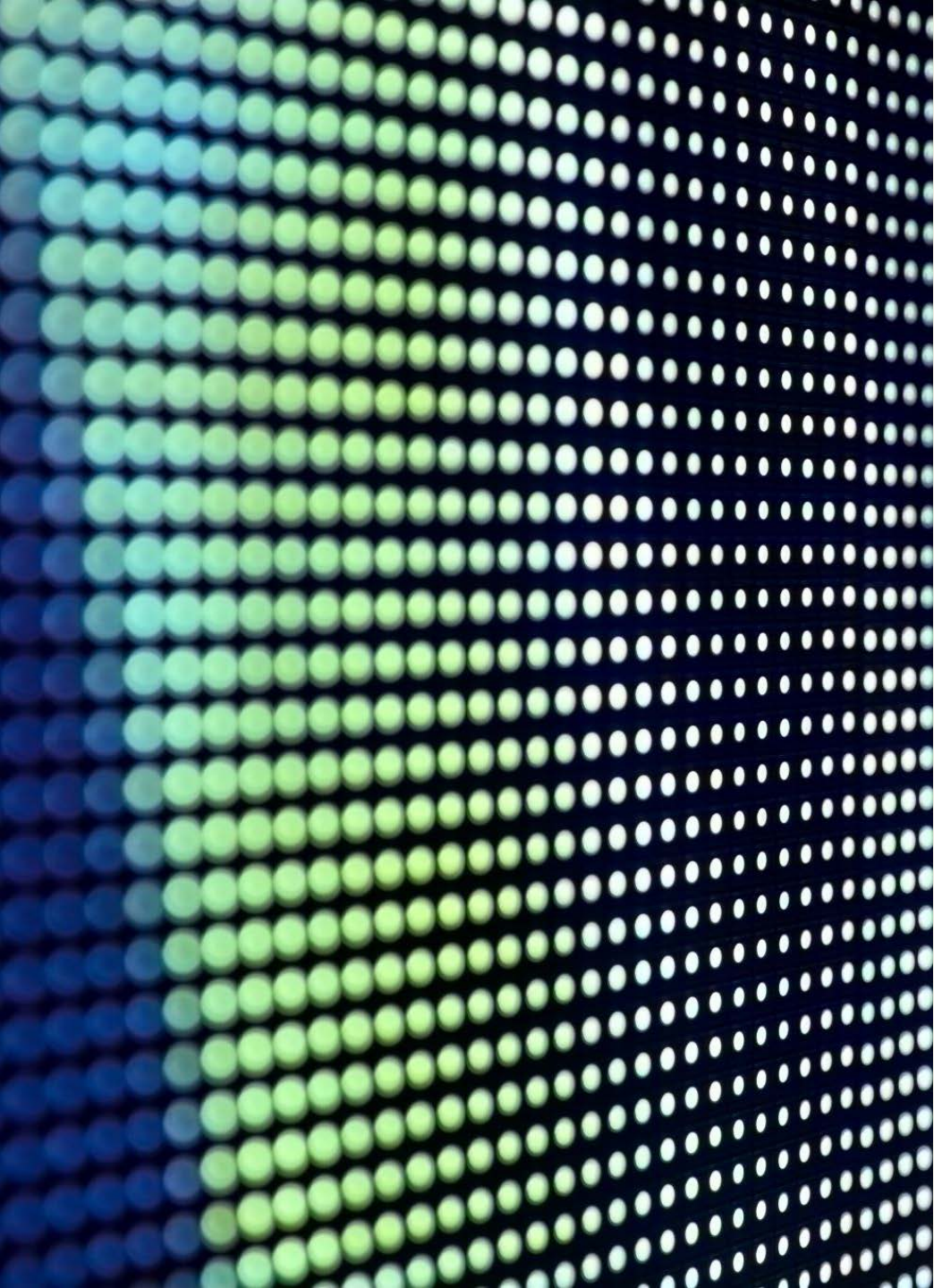
Шифрування

Контроль доступу



## АРХИТЕКТУРА РОЗРОБЛЕНОЇ СИСТЕМИ

- Nginx
- HiveMQ
- Сервер авторизації
- Сервер збору даних
- Logstash
- ElasticSearch
- Kibana



# NGINX

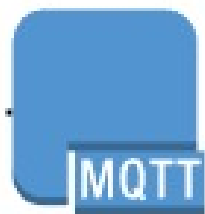
Reverse proxy



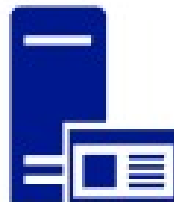
IoT прилад



Nginx



HiveMQ



Сервер авторизації

Спроба взаємодії з топіком

Перевірка прав

Дозвіл / заборона операції

Успіх / невдача операції

## HiveMQ

- MQTT брокер
- Extension SDK



IoT прилад

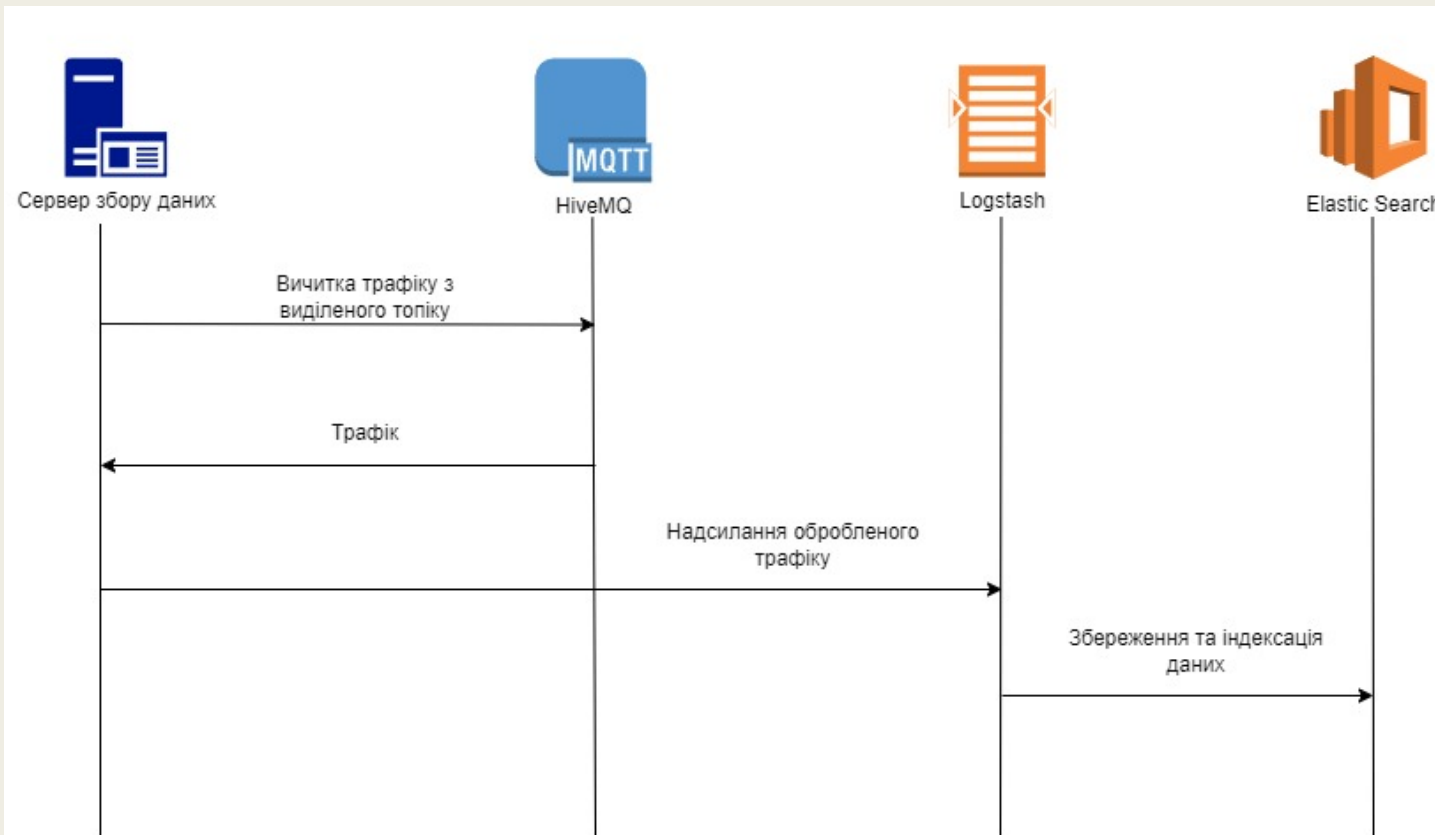


Сервер авторизації



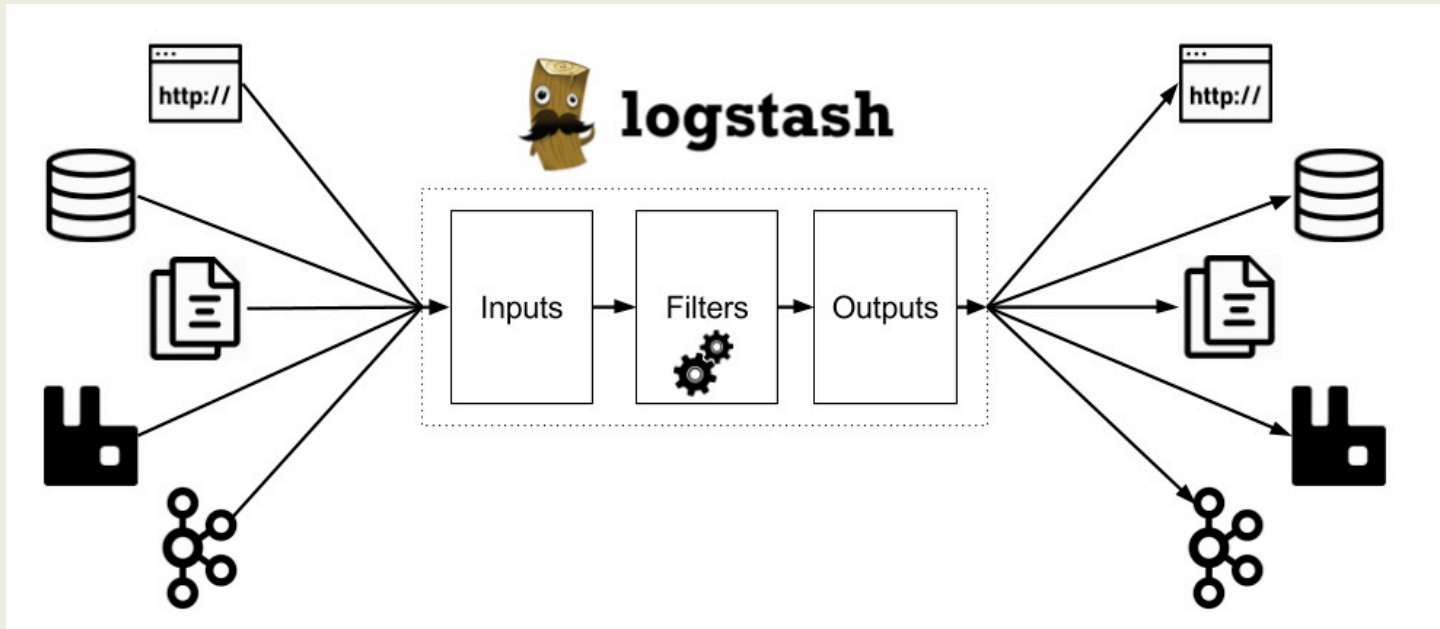
## Сервер авторизації

- Spring Framework
- Дані про облікові дані пристадів
- Дані про доступи



## Сервер збору даних

- Spring Framework
- Вичитка, обробка та надсилання даних



# LOGSTASH

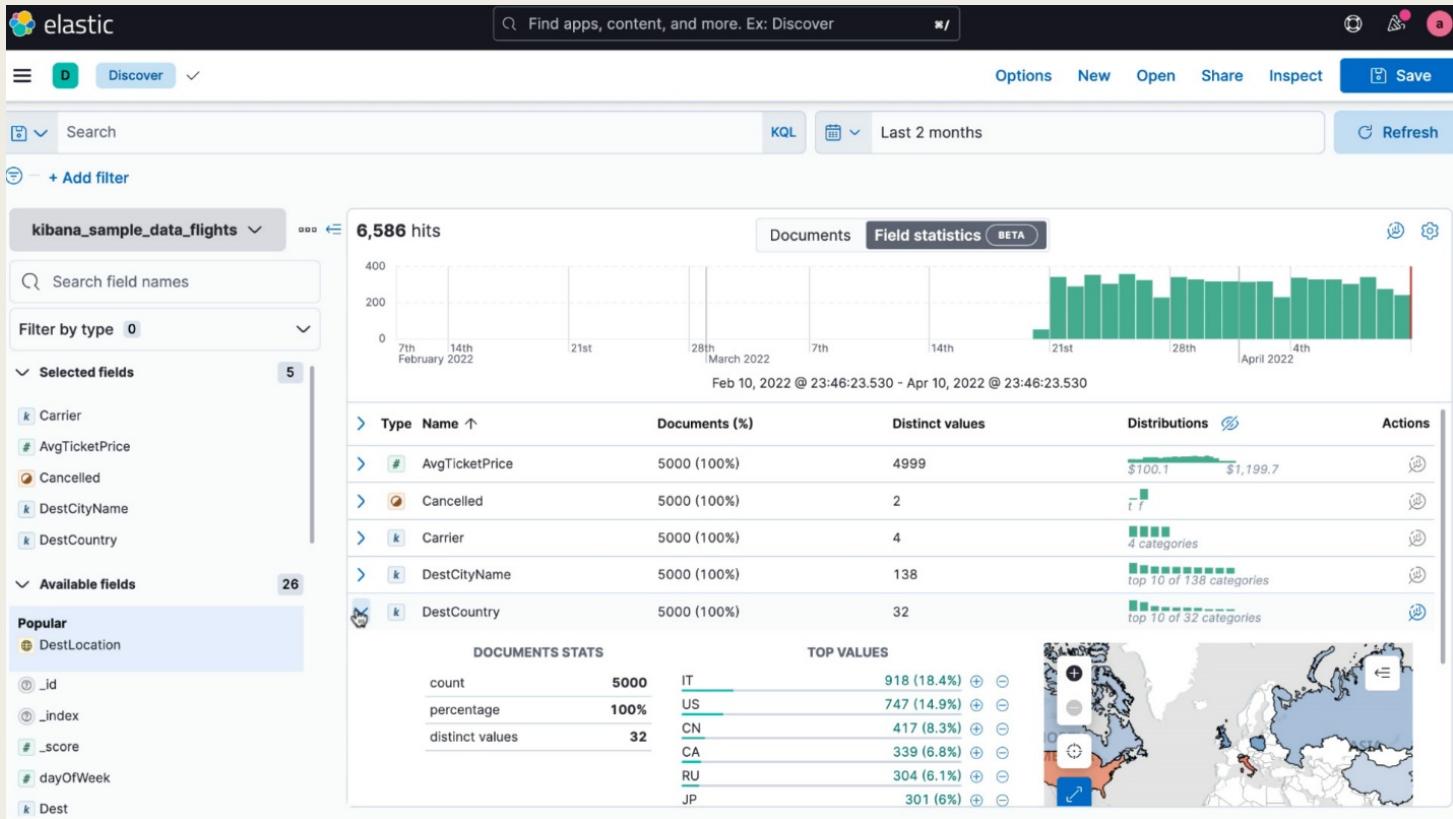
Пайплайн даних до  
ElasticSearch



# elastic

## ElasticSearch

- Пошукова система
- Машинне навчання
- Навчання моделей в реальному часі
- Виявлення аномалій в реальному часі



# Kibana

- Інтерфейс для ЕКЛ стеку
- Візуалізація даних

## Machine Learning

Overview  
Notifications  
Memory Usage

## Anomaly Detection

Jobs  
Anomaly Explorer  
Single Metric Viewer  
Settings

## Data Frame Analytics

Jobs  
Results Explorer  
Analytics Map

## Model Management

Trained Models

## Anomaly Detection Jobs

Auto refresh 30 seconds

Refresh

Active ML nodes: 1 Total jobs: 2 Open jobs: 2 Closed jobs: 0 Active datafeeds: 1

Create job

Search...

Opened Closed Failed Started Stopped Group

<input type="checkbox"/>	ID ↑	Description	Processed records	Memory ...	Job state	Datafeed state	Latest timestamp	Actions
<input type="checkbox"/>	>	first-anomaly-job	16,632	ok	opened	stopped	2024-05-01 03:41:09	<a href="#">📈</a> <a href="#">📄</a> <a href="#">⋮</a>
<input type="checkbox"/>	∨	second-job	15,327	ok	opened	started	2024-05-01 17:18:27	<a href="#">📈</a> <a href="#">📄</a> <a href="#">⋮</a>

Job settings Job config Datafeed Counts JSON Job messages Datafeed preview Forecasts Annotations Model snapshots

<input type="checkbox"/>	Time ↓	Node	Message
<input type="checkbox"/>	2024-05-07 22:51:48	elasticsearch	Datafeed continued in real-time
<input type="checkbox"/>	2024-05-07 22:51:48	elasticsearch	Datafeed lookback completed
<input type="checkbox"/>	2024-05-07 22:51:48	elasticsearch	Datafeed started (from: 2024-05-01T14:18:27.001Z to: real-time) with frequency [450000ms]
<input type="checkbox"/>	2024-05-07 22:51:48	elasticsearch	Starting datafeed [datafeed-second-job] on node [elasticsearch]
<input type="checkbox"/>	2024-05-07 22:51:47	elasticsearch	Loading model snapshot [1715111451] with latest_record_timestamp [2024-05-01T14:18:27.000Z], job latest_record_timestamp [2024-05-01T14:18:27.000Z]

ТРЕНУВАННЯ МОДЕЛЕЙ

## Machine Learning

Overview  
Notifications ●  
Memory Usage

## Anomaly Detection

Jobs  
[Anomaly Explorer](#)  
Single Metric Viewer  
Settings

## Data Frame Analytics

Jobs  
Results Explorer  
Analytics Map

## Model Management


Trained Models

## Data Visualizer

File  
Data View  
ES|QL  
Data Drift

## AIOps Labs

Log Rate Analysis  
Log Pattern Analysis

Top influencers 

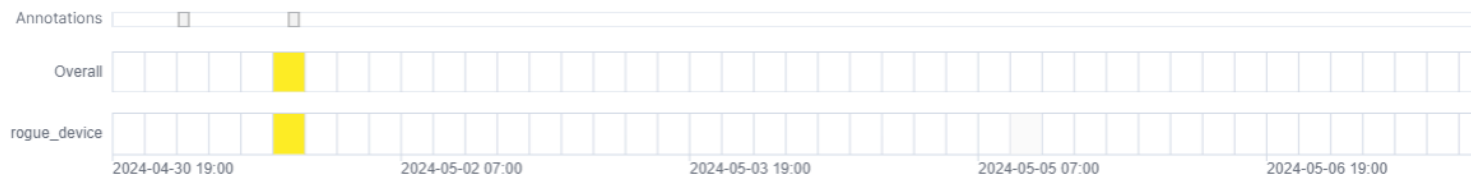
## timestamp



## name.keyword

Anomaly timeline 




(Sorted by max anomaly score)



&gt; Annotations Total: 2

## Anomalies

Severity warning Interval Auto

Time	Severity	Detector	Influenced by	Actual	Typical	Description	Actions
> May 1st 2024, 17:00	49	max(humidity)	name.keyword: rogue_device timestamp: 1714572875033 timestamp: 1714572851832 timestamp: 1714572896201 timestamp: 1714572888139 and 21 more	72.451	51.55	↑ 1.4x higher	
> May 1st 2024, 17:00	49	max(temperature)	name.keyword: rogue_device timestamp: 1714572839710 timestamp: 1714572895196 timestamp: 1714572888139 timestamp: 1714572885112 and 24 more	73.452	21.515	↑ 3x higher	
> May 1st 2024, 17:00	49	min(humidity)	name.keyword: rogue_device timestamp: 1714572846780 timestamp: 1714572857868 timestamp: 1714572870981	27.375	48.468	↓ 2x lower	

# ВІЯВЛЕННЯ АНОМАЛІЙ

### Create rule ×

---

#### Anomaly detection

Alert when anomaly detection jobs results match the condition. [Learn more](#)

---

Select job

second-job × ▼

Result type

<b>Bucket</b> How unusual was the job within the bucket of time? <span>✓ Selected</span>	<b>Record</b> What individual anomalies are present in a time range? Select	<b>Influencer</b> What are the most unusual entities in a time range? Select
--	---	--

Severity 75 0 25 50 75 100

Include interim results

> Advanced settings

Check the rule condition with an interval

15d, 6m Test

Check every 1 minute ▼

> Advanced options

# РЕАКЦІЯ НА АНОМАЛІЇ

# Результати

Аналіз актуальних вразливостей в IoT системах

Проблеми контролю доступу

Підходи до шифрування даних

Розроблений комплексний підхід до захисту IoT системи, на основі гранульованого контролю доступу та виявленню аномалій даних в реальному часі.



ДЯКУЮ ЗА УВАГУ