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

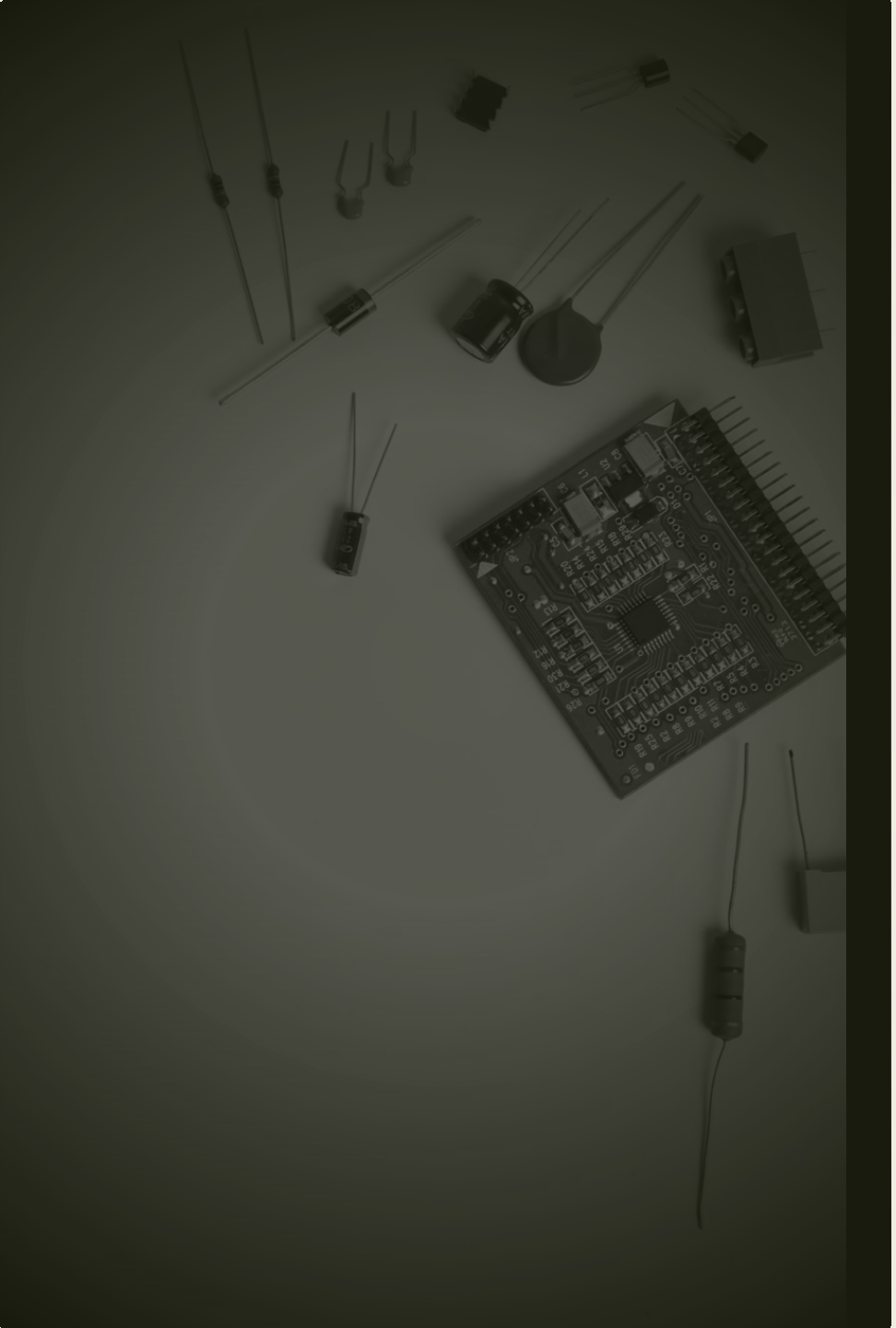
Мета

1

Дослідження відомих та новітніх підходів до захисту IoT систем

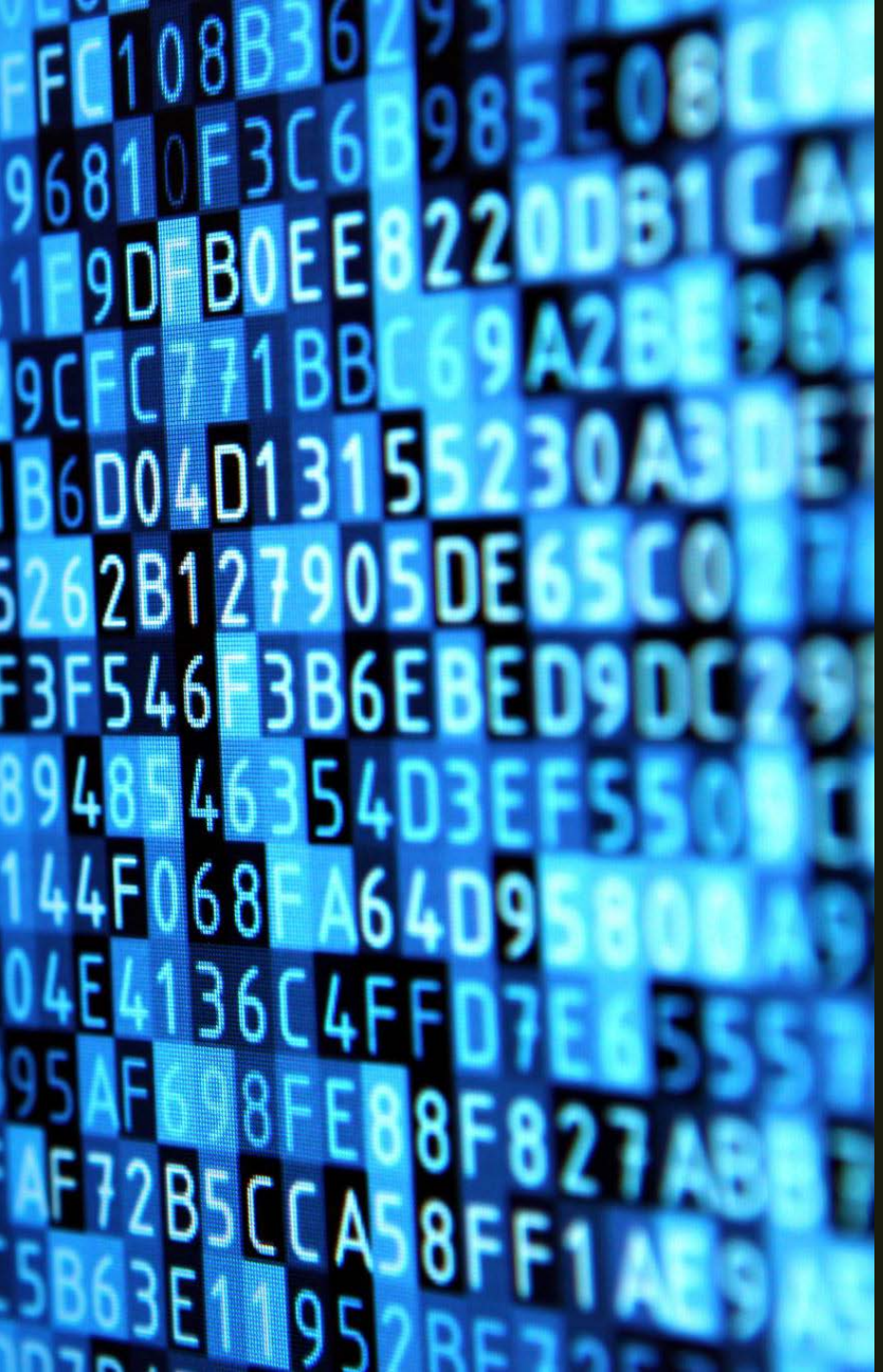
2

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

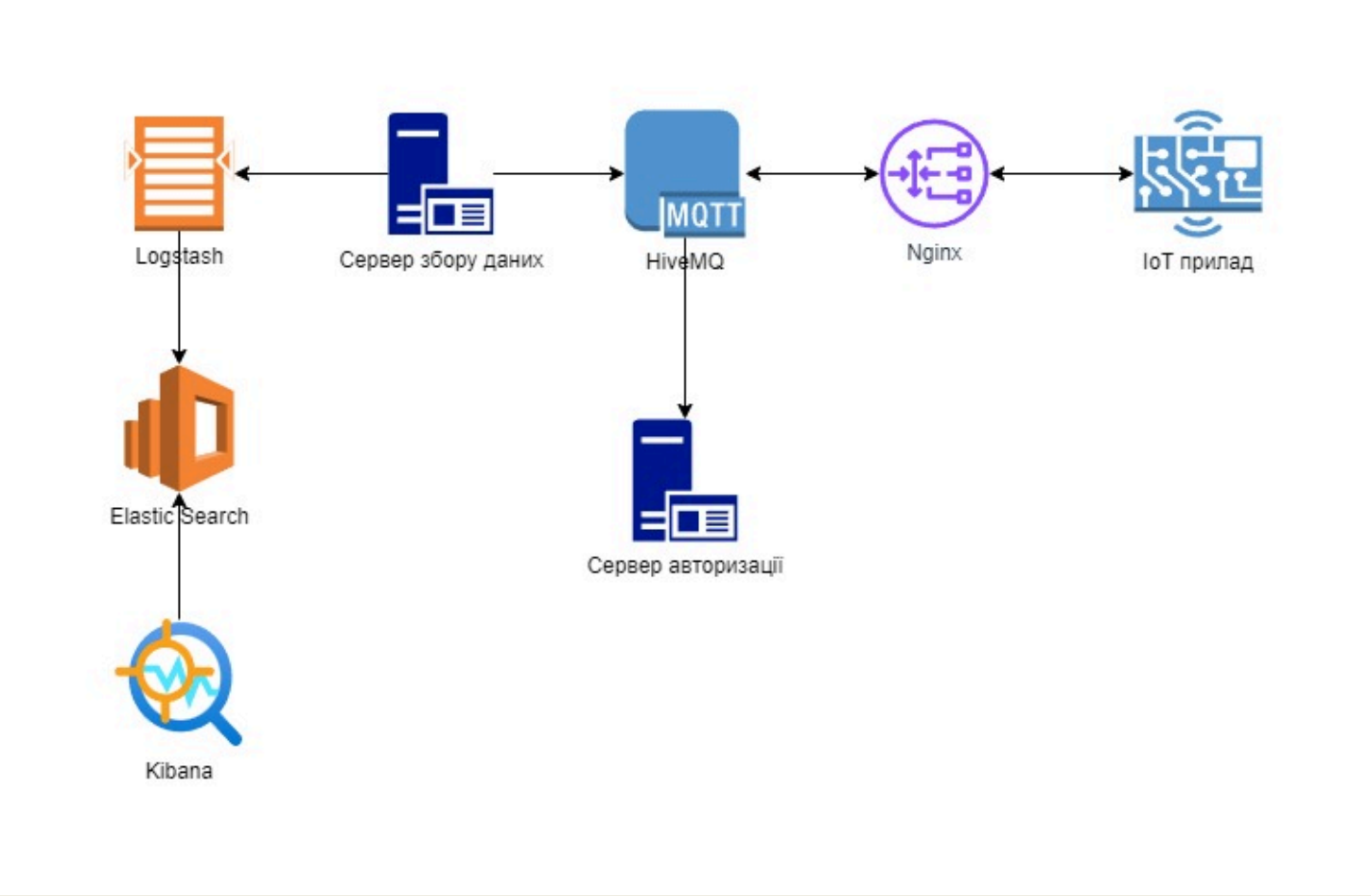


Шифрування

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

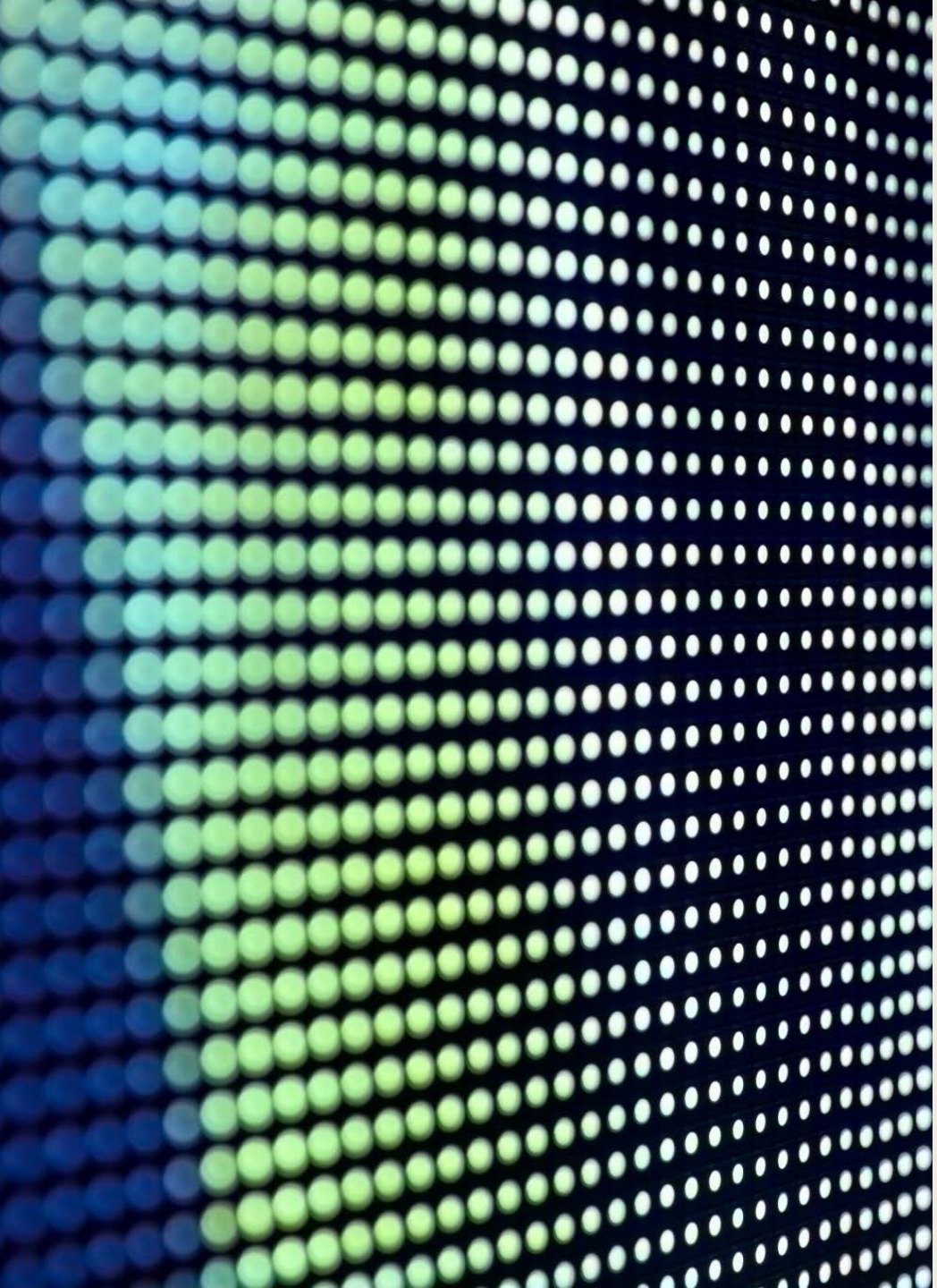
Проблематика безпеки в IoT системах

- Доменна область
- Обмеженість в ресурсах
- Способи комунікації
- Шифрування
- Контроль доступу



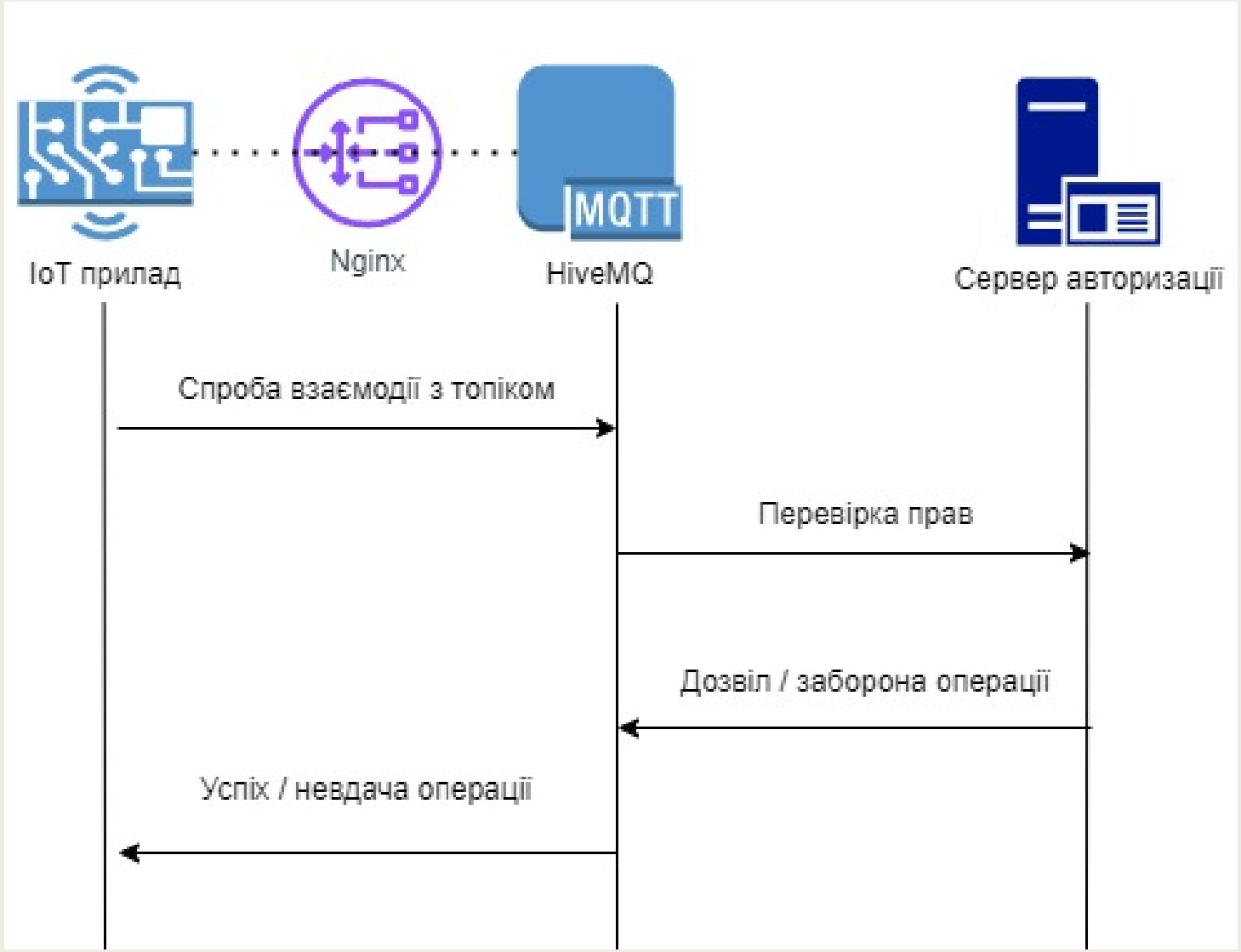
АРХІТЕКТУРА РОЗРОБЛЕНОЇ СИСТЕМИ

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



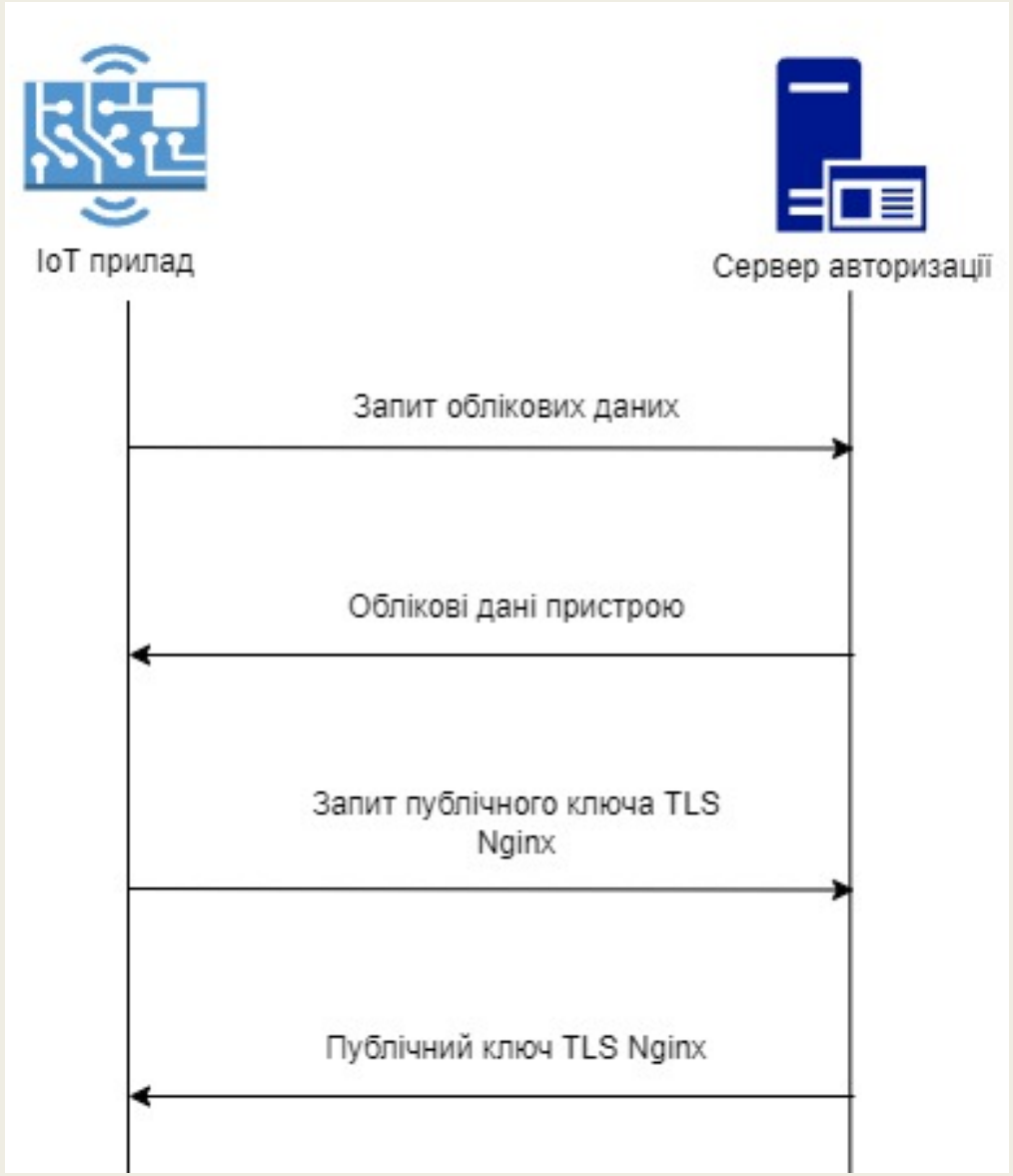
NGINX

Reverse proxy



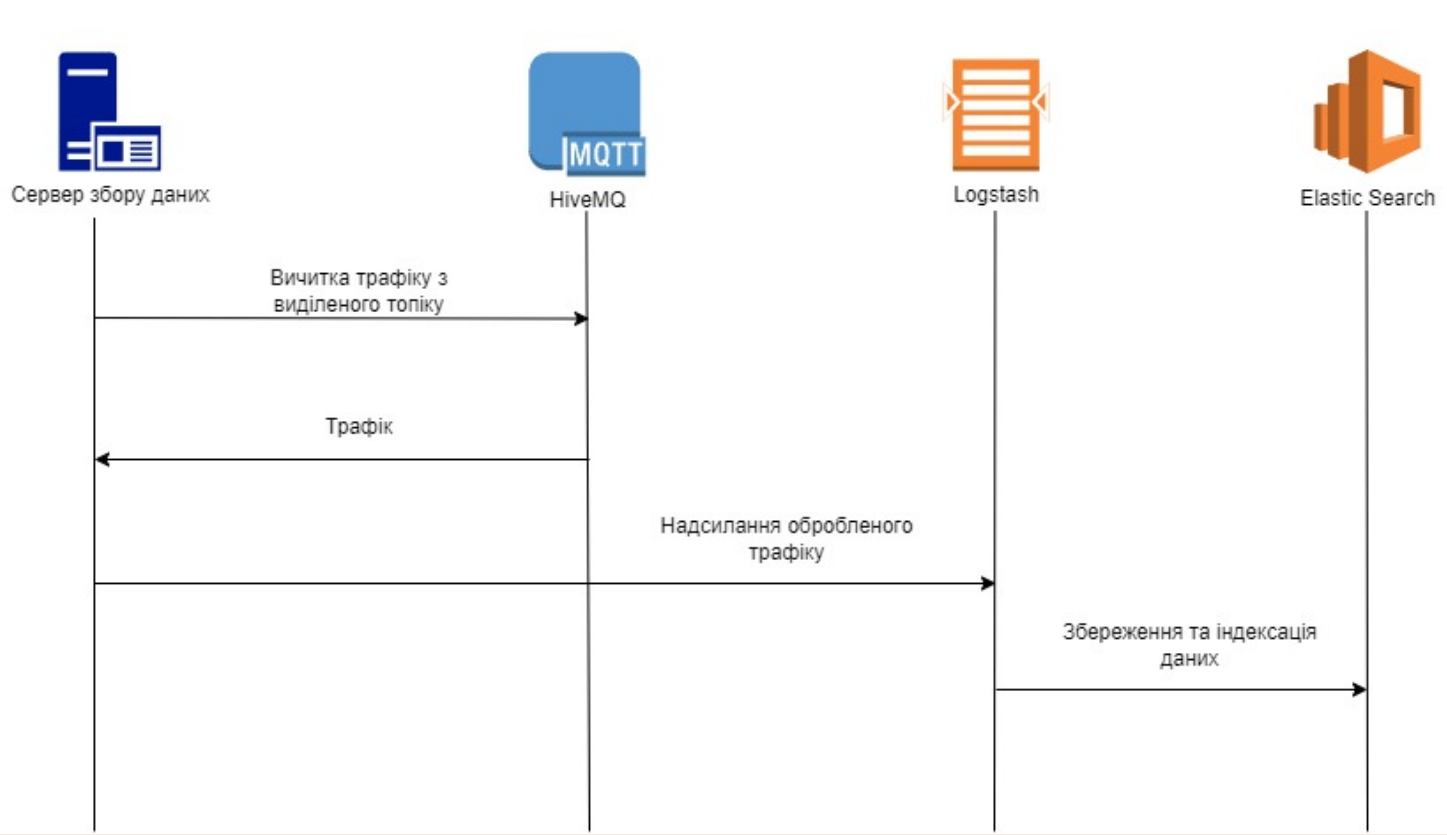
HiveMQ

- MQTT брокер
- Extension SDK



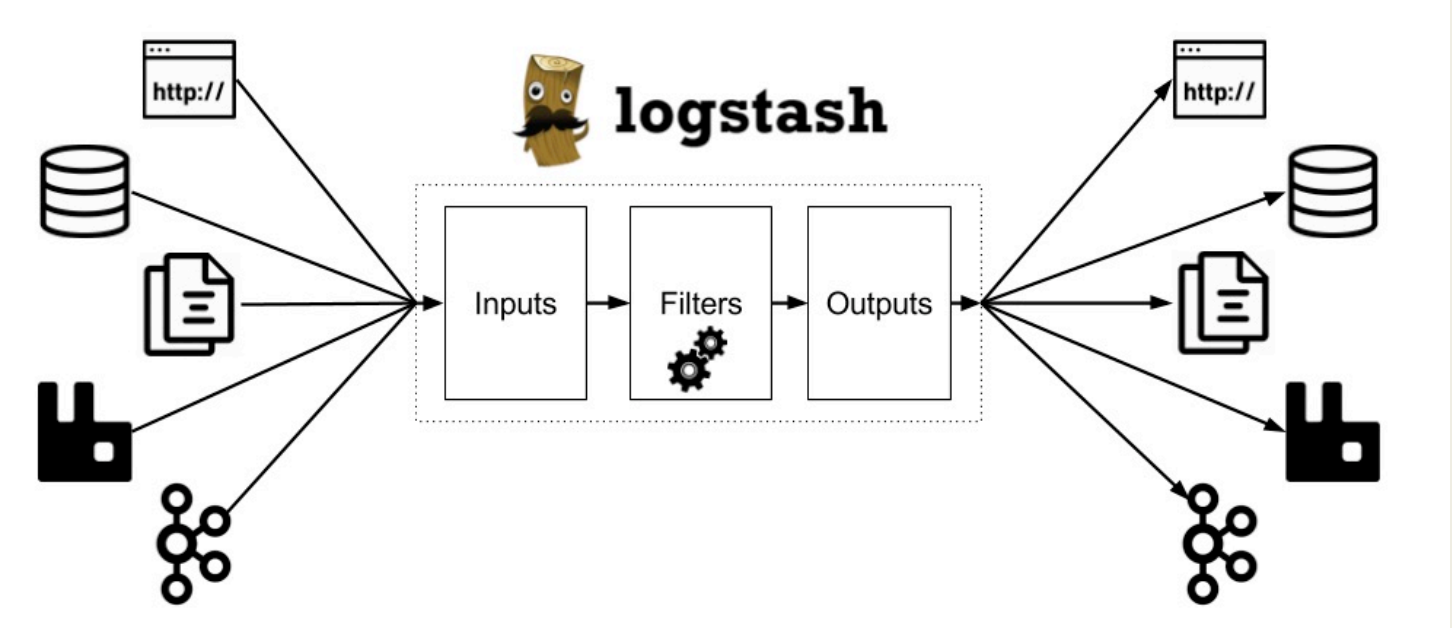
Сервер авторизації

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



Сервер збору даних

- Spring Framework
- Вичитка, обробка та надсилання даних

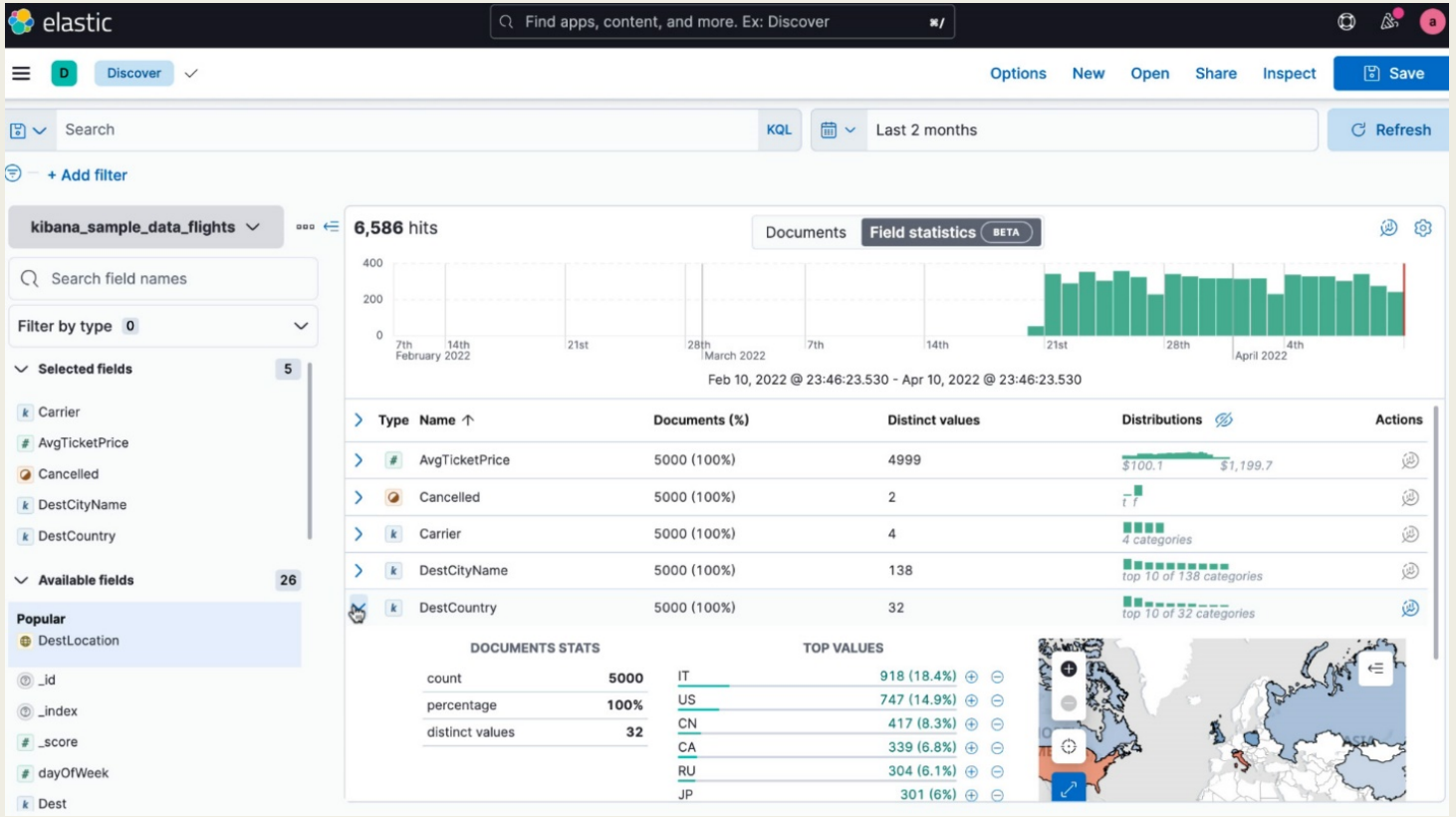


LOGSTASH

Пайплайн даних до ElasticSearch

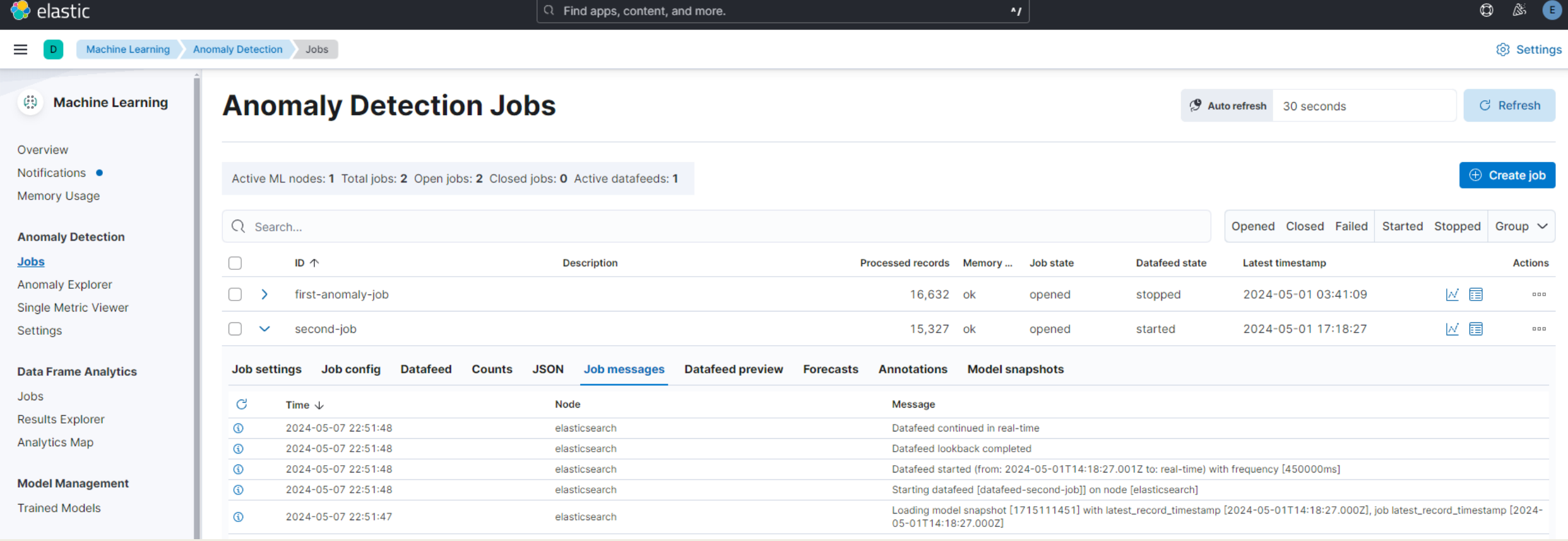
ElasticSearch

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

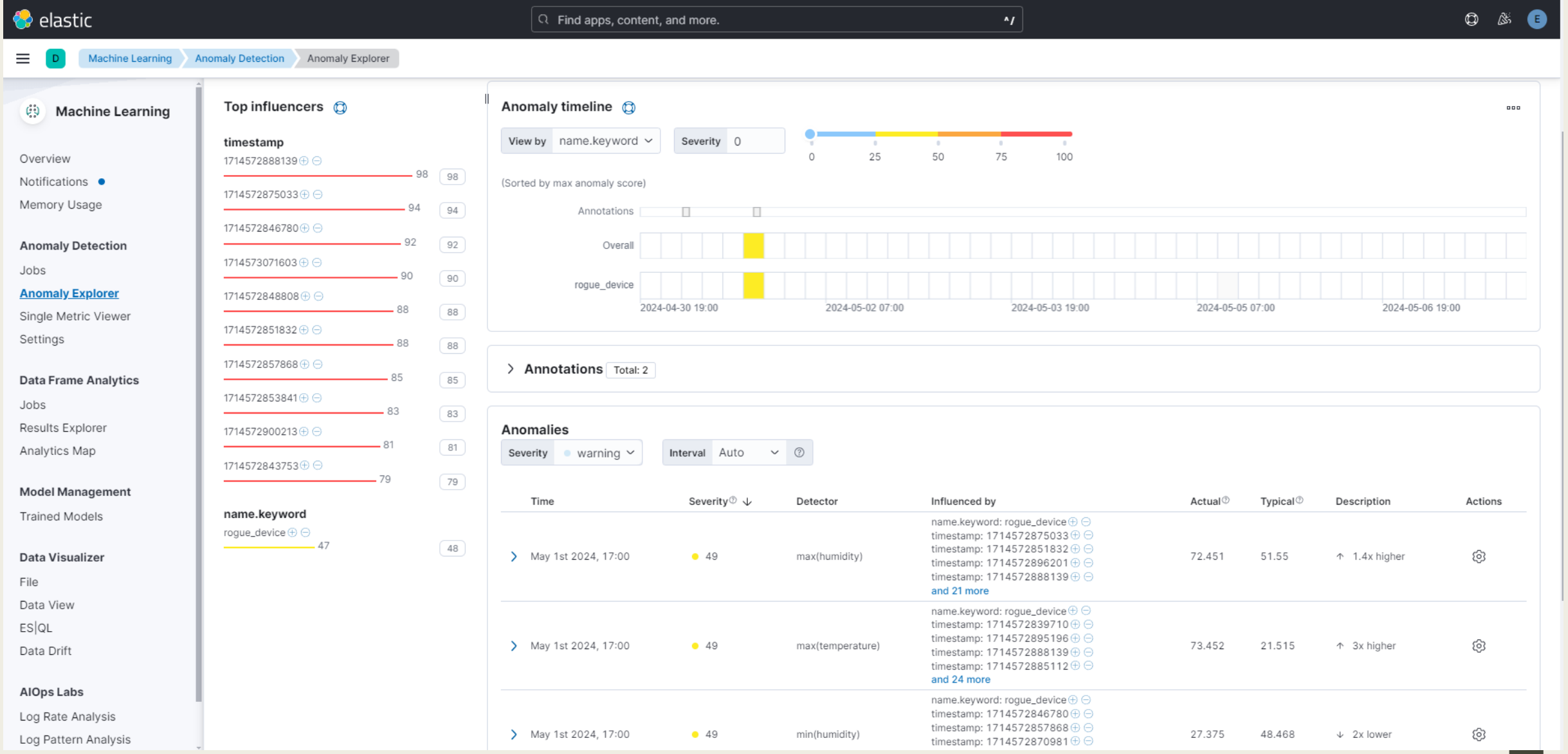


Kibana

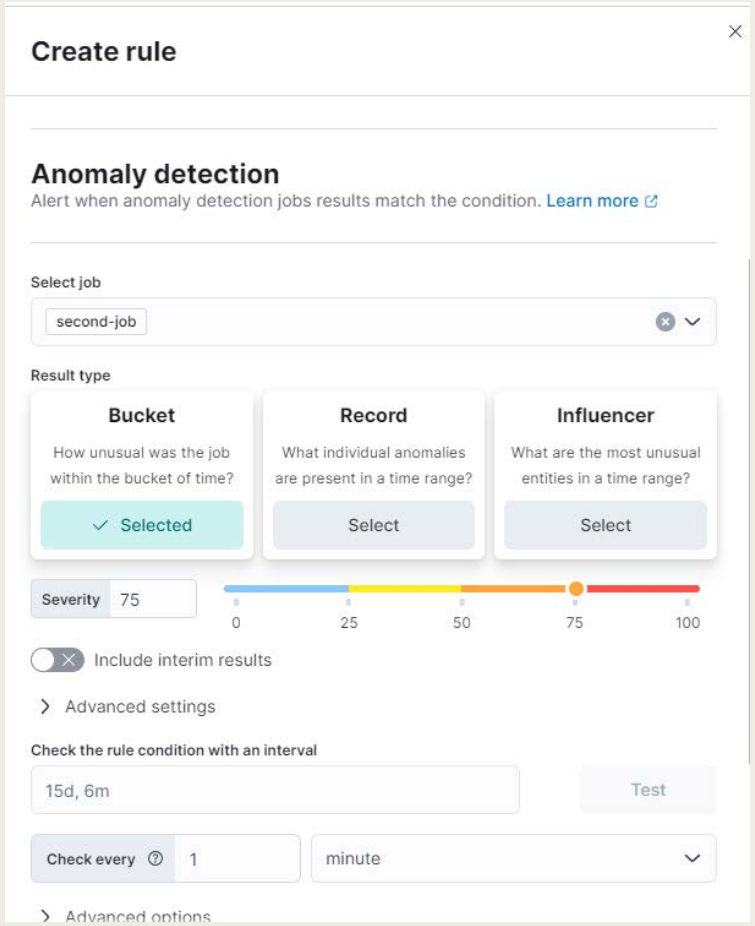
- Інтерфейс для EKL стеку
- Візуалізація даних



ТРЕНУВАННЯ МОДЕЛЕЙ



ВИЯВЛЕННЯ АНОМАЛІЙ



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