Why you need to monitor your model

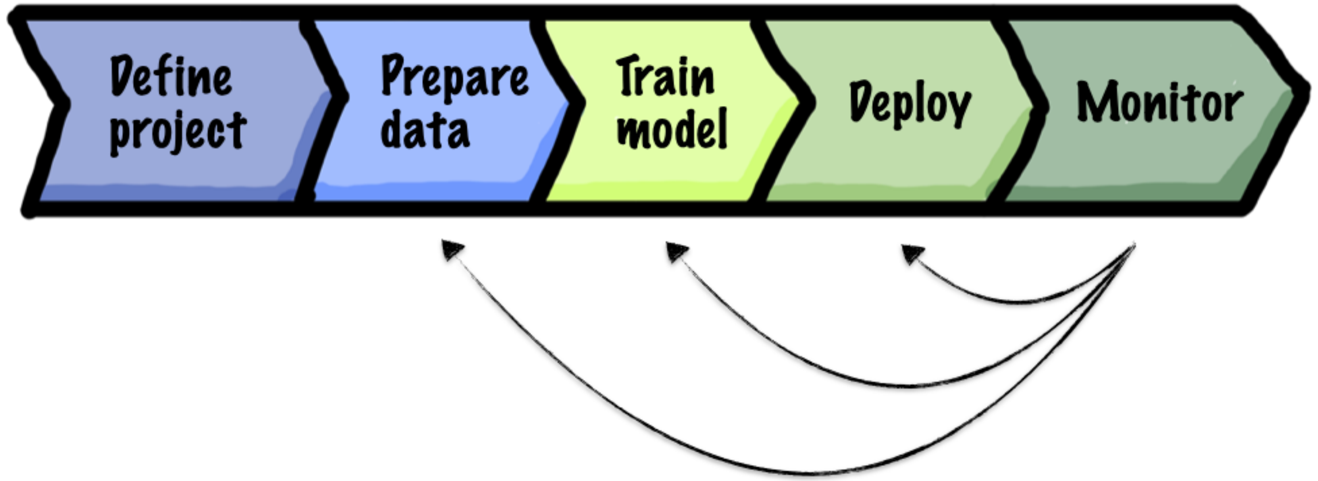
MACHINE LEARNING MONITORING CONCEPTS

Hakim Elakhrass
Co-founder and CEO of NannyML

Machine learning in production

Typical development process

After deployment



Reducing risk of failure

Zillow's case

Reasons for model to fail:

- Software issues
- Drifts in the input data
- Changes in relationship between features and targets

Maximizing business impact

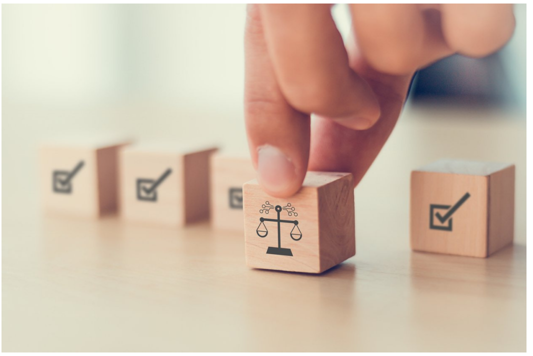
- Optimizing the model in relation to business goals

- Reducing cloud costs

Improving AI safety

Three safety problems:

- Bias - fair output for different groups of users



- Adversarial attacks - detect malicious manipulation of input data

- Lack of explainability - understanding of how the model makes decisions

Changing the world with data

The automatization process

Let's practice!

MACHINE LEARNING MONITORING CONCEPTS

The ideal monitoring workflow

MACHINE LEARNING MONITORING CONCEPTS

Hakim Elakhrass
Co-founder and CEO of NannyML

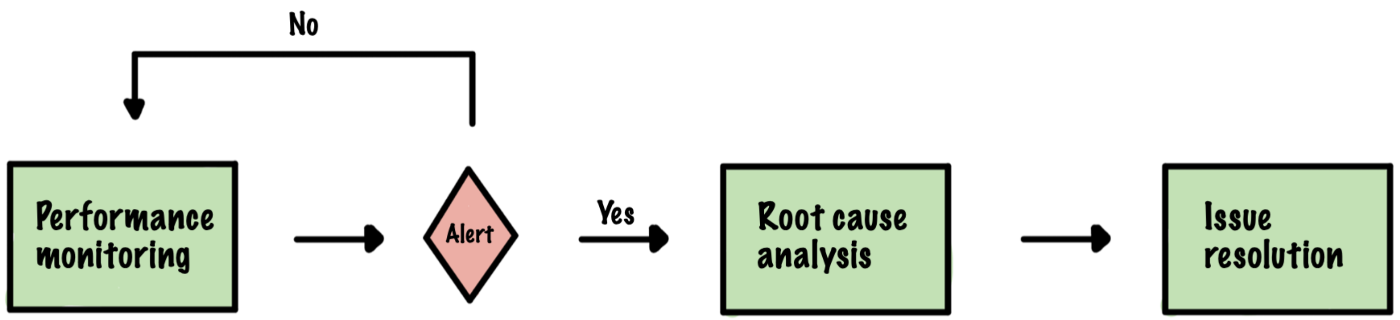
Monitoring workflows

Traditional monitoring workflow

- Calculate technical performance
- Alert based on drifts in the input data
- Results in many false alerts

Ideal monitoring workflow

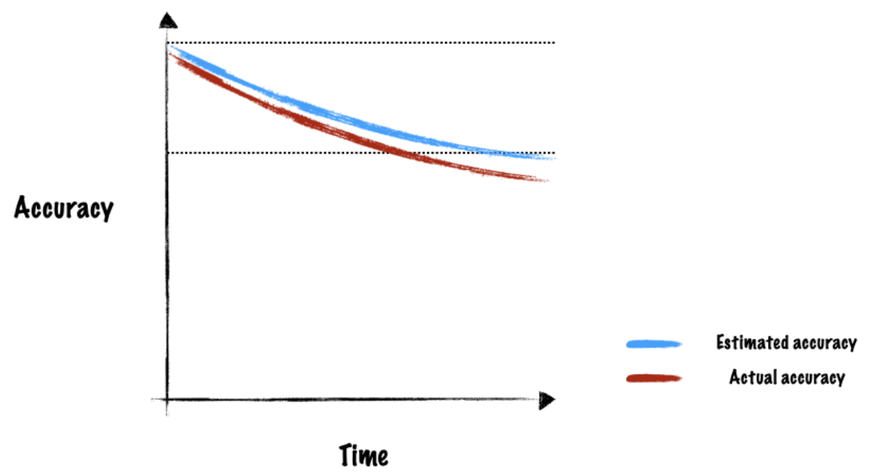
- Technical performance monitoring
  - Calculate and estimate performance
- Root cause analysis
  - Allows to link drifts with drops in performance

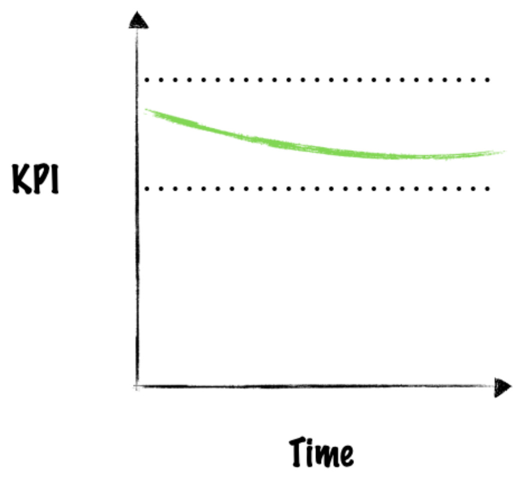


Monitoring performance

Involves:

- Calculating performance - for technical metrics like accuracy
- Estimating performance - if ground truth is not available
- Measuring business impact - monitor key performance indicators

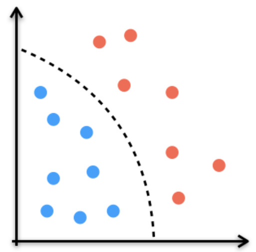




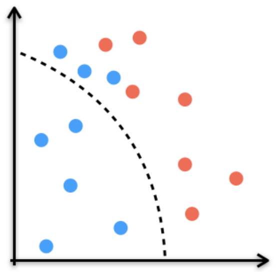
Root Cause Analysis

The goal is to investigate:

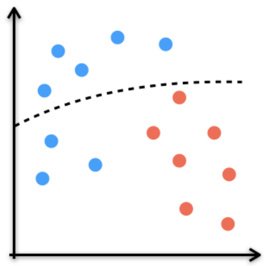
- Covariate shift - shifts in the input data distribution
- Concept drift - changes in relationship between features and targets



The original model



Covariate shift

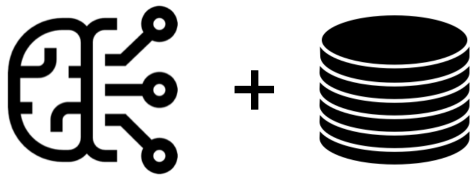


Concept drift

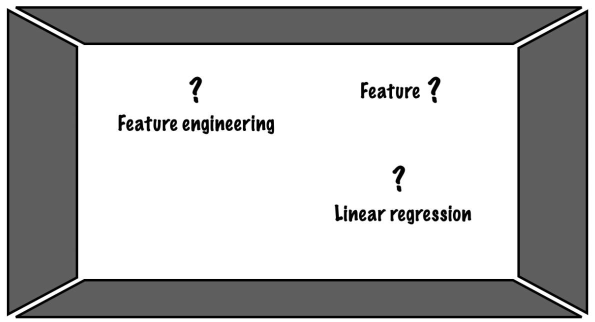
Issue resolution

Possible solutions:

- Retraining - requires additional data and compute



- Refactoring the use case - take a step back and rethink used methods



- Changing the downstream processes - modify processes around the prediction

Let's practice!

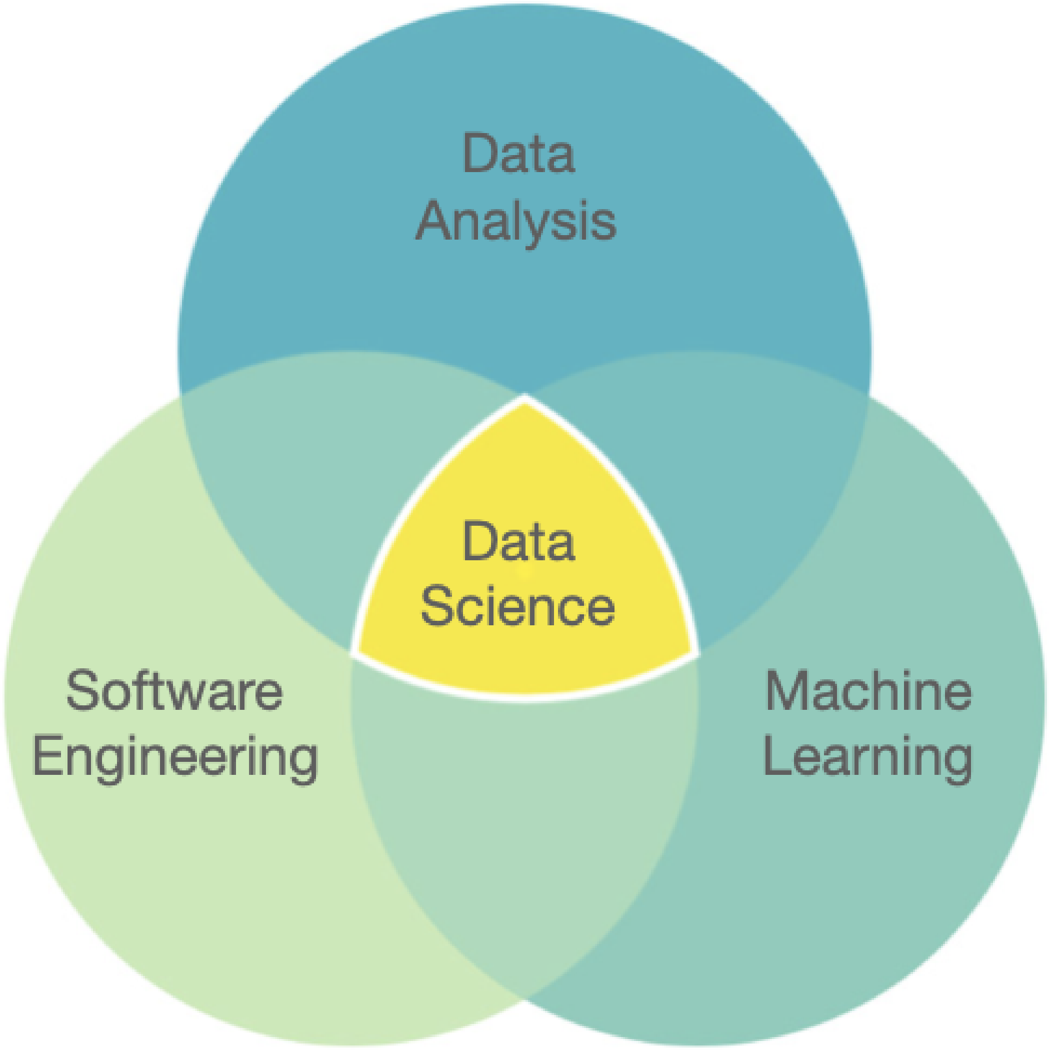
MACHINE LEARNING MONITORING CONCEPTS

Challenges of monitoring ML models

MACHINE LEARNING MONITORING CONCEPTS

Hakim Elakhrass
Co-founder and CEO of NannyML

Machine learning project components



The model fails to make predictions

Possible problems :

- Language barriers - combining different programming languages using the "glue" code

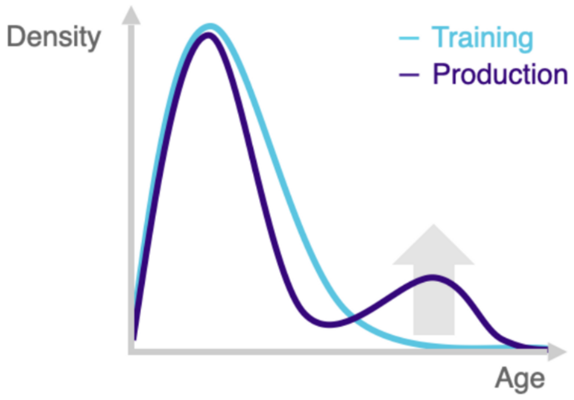
- Code maintenance - compatibility problem of updated dependencies

- Scaling issues - not robust infrastructure to handle more users

The model predictions fail

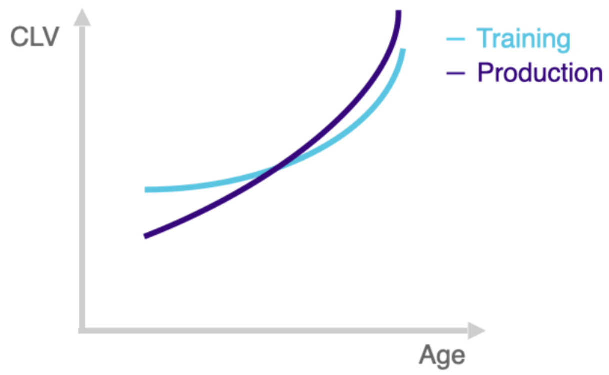
Covariate shift

- Change in the input's distribution
- Possible to detect using statistical methods
- Not every drift impact performance



Concept drift

- Change in the relationship between the input data and targets
- Difficult to detect
- Almost always affects the business impact of the model



Availability of ground truth

Let's practice!

MACHINE LEARNING MONITORING CONCEPTS