ANTI-FRAUD FRAMEWORK

How to Identify and Prevent It with ML

MY BACKGROUND

Masters in Math

SBER CIB

Securities Analyst
2019-2020

Y

SWE-Analyst
2020-2021

playrix

Lead Data Analyst
2021-2022

exness

Senior Researcher
2023-

Consultant
2023-2024

CEO Glancing [AI, VC]
2024-

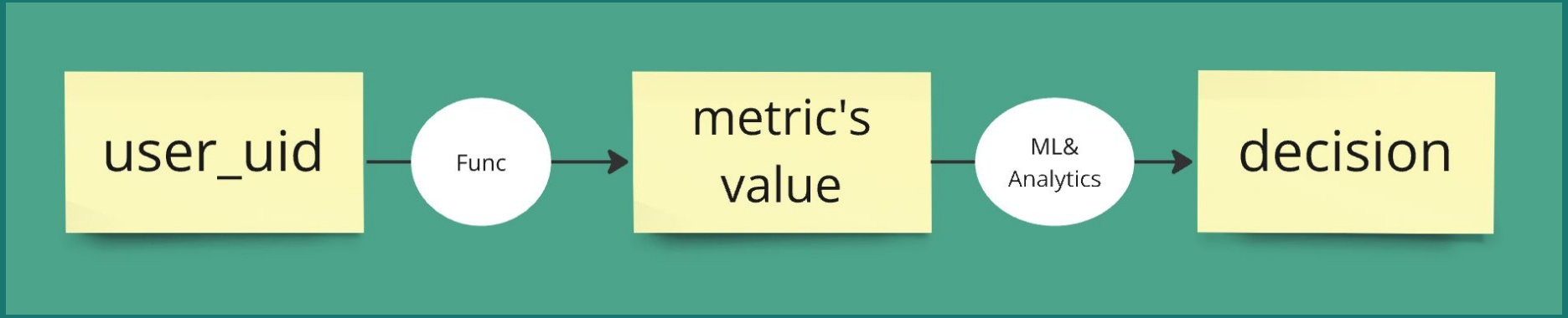
OUR AGENDA TODAY:

OVERVIEW OF AN ANTI-FRAUD SYSTEM: HOW IT WORKS AND WHY IT MATTERS

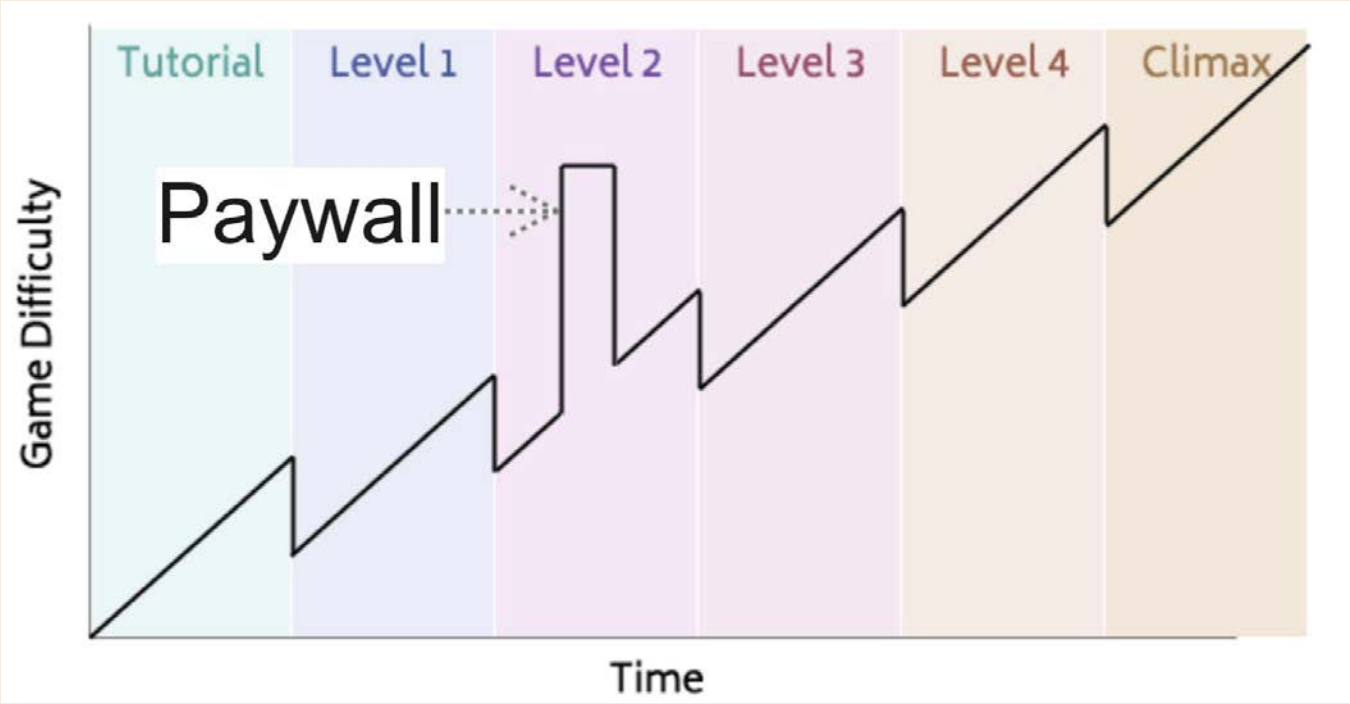
- **OVERVIEW OF AN ANTI-FRAUD SYSTEM: HOW IT WORKS AND WHY IT MATTERS**
  - *A case study from FinTech*
  - *A case study from GameDev*
- **KEY ASPECTS OF ML/ANALYTICAL DESIGN IN ANTI-FRAUD SYSTEMS**
  - *Integration of diverse data sources*
  - *Addressing multiple tracking objectives*
- **INFRASTRUCTURE SOLUTIONS AND IMPLEMENTATION STRATEGIES**
- **REAL-TIME MODELING VS. OFFLINE MODELING**
- **MONITORING MECHANISMS**
- **RESPONDING TO NEW THREATS. WHAT DO WE NEED EXCEPT ML**

WHAT IS ANTI-FRAUD?

Fraud - customer action that are not intended by the company, which result in a **deterioration of key metrics**. If the client uses **internal** inefficiencies of the company's mechanisms, fraud is called **endogenous**, otherwise **exogenous**.

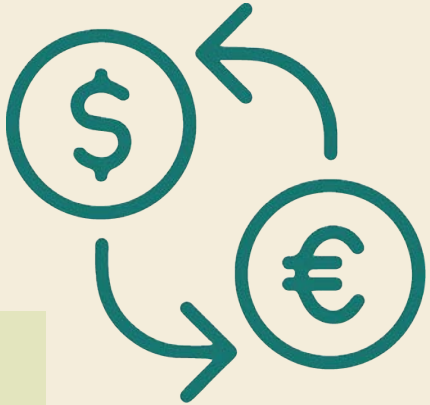


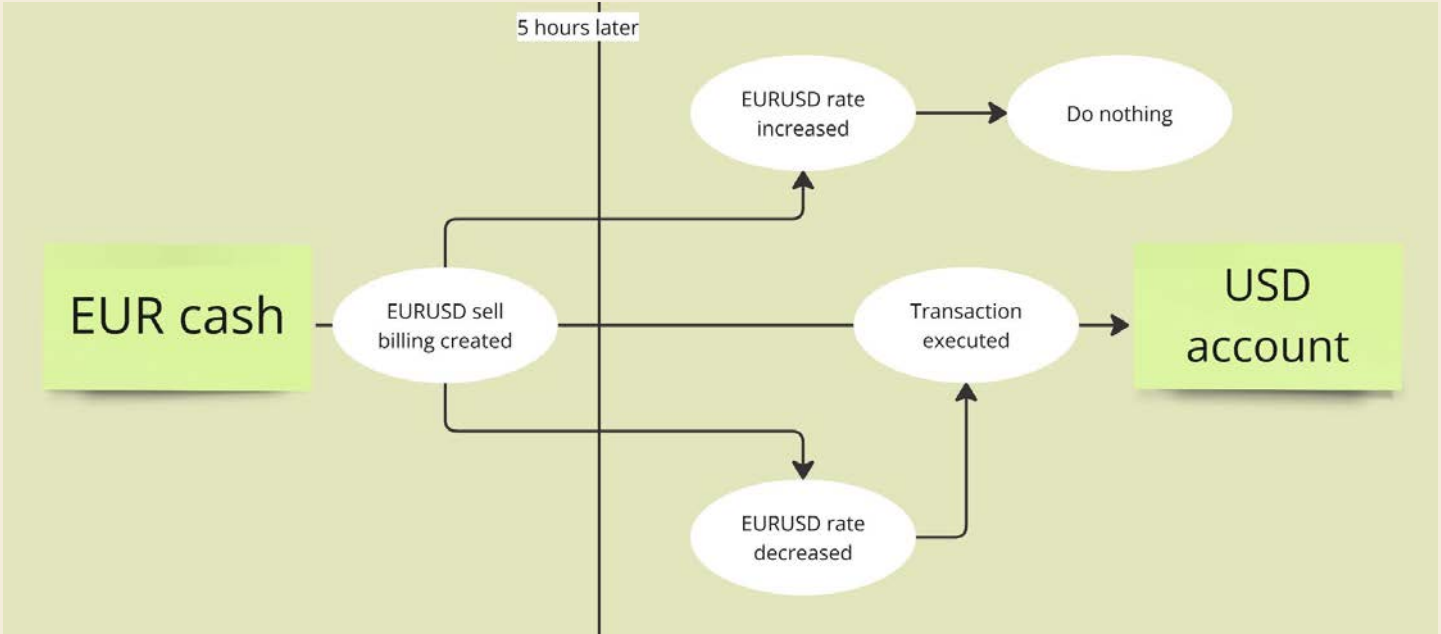
USERS ARE AVOIDING



1) User avoid paywall using dishonest algorithms
2) Such users go through game much faster
3) Such users pay much less

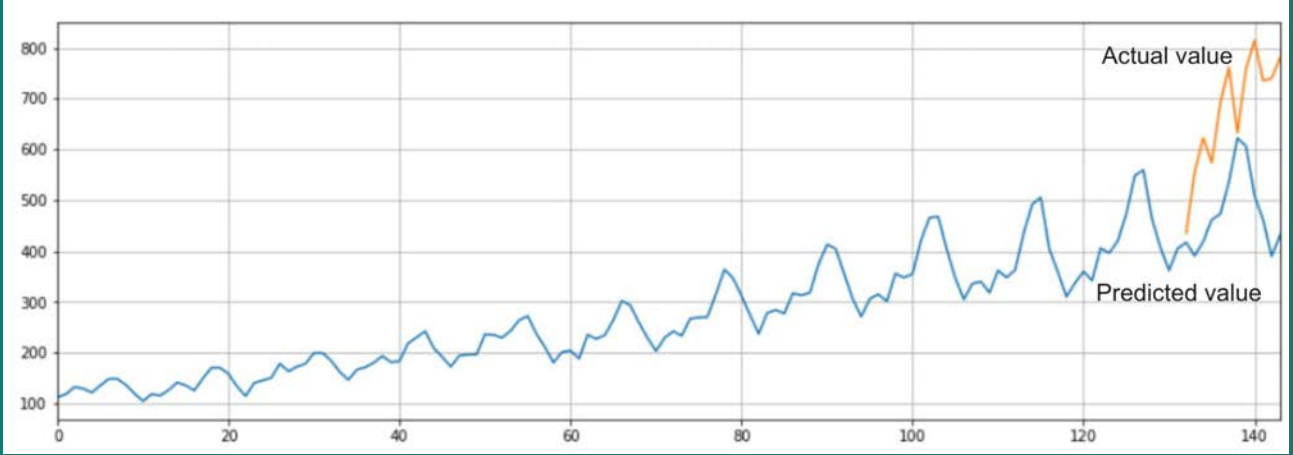
HOW TO TAKE ADVANTAGE OF FINTECH COMPANIES





1 BUILDING AN ANTI-FRAUD PLATFORM

The idea is to customise a pipeline of the model starting from a simple concept so we get a complex framework in the last slide.



Key concepts

- Gradient boosting
- Autoregression
- CI prediction
- Is Actual value in CI predicted or not?

SOME COMMENT REGARDING THE MODEL

That's good

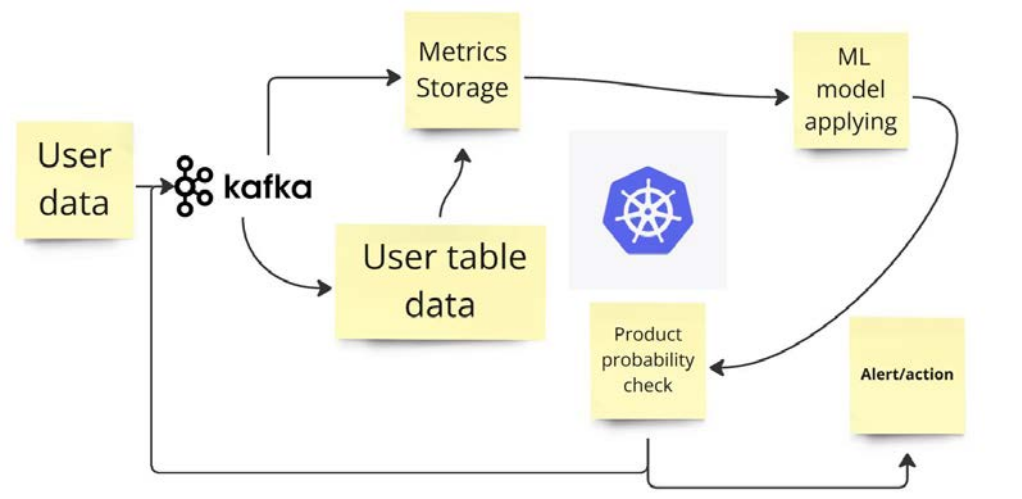
- Quantile regressions with data with enrichments
- Monte carlo probability estimates
- Tree-based XGB, LightGBM, and CatBoost Models
- Automatic ARIMA-GARCH
- Identifying trend and variance

That's bad

- Naive Tree/regression models
- Deep learning
- RNN
- Temporal fusion Transformers
- Lag-Llama

2 BUILDING AN ANTI-FRAUD PLATFORM

AFTER TRAINING THE MODEL ON USER DATA OFFLINE, WE DEPLOY IT:



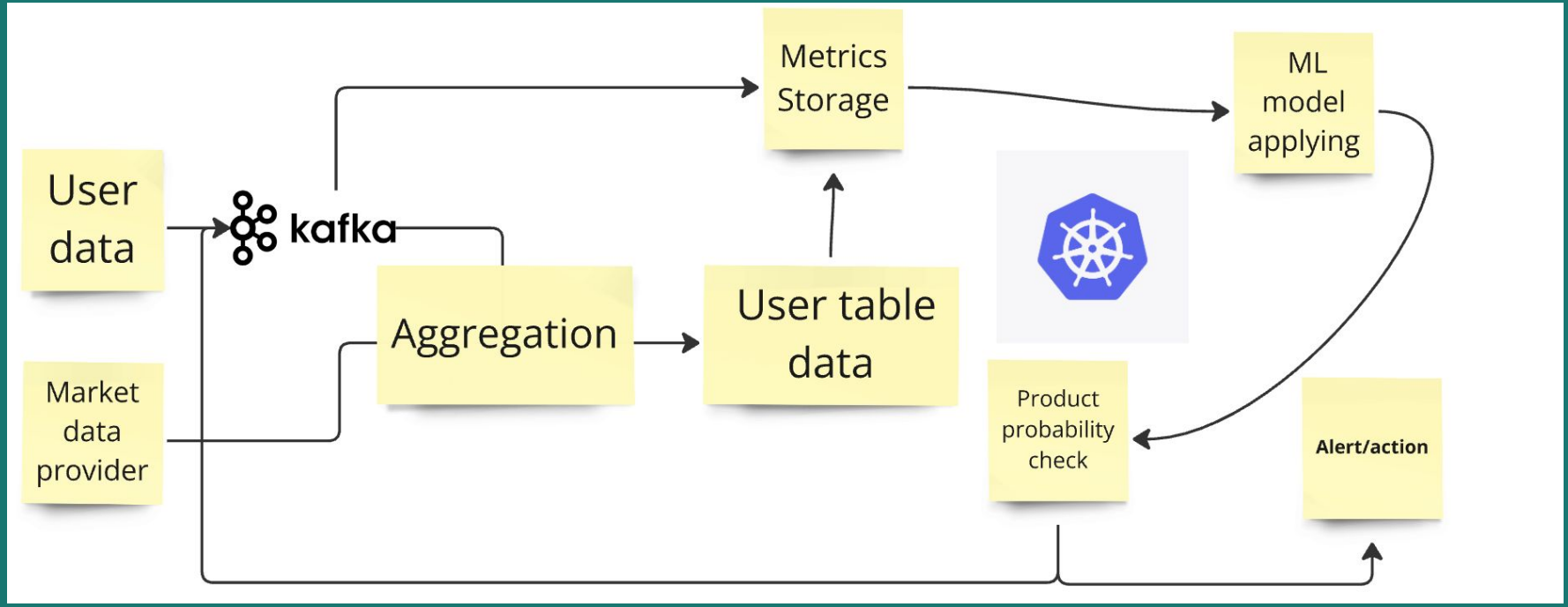
Kubernetes operates the model within a persistent pod that monitors data from Kafka.

Reloading the model based on a cooldown period or a timeframe suitable for an anti-fraud platform.

WHAT IS THE CHALLENGE?
THE LACK OF DATA

- It’s not possible to implement the model by using user data only.
- The complicated data sources such as currency conversion rates should be added.
- In production, the model is "waiting" for all the data, as we see our data from Kafka before the external source needs us to do time-based joins.

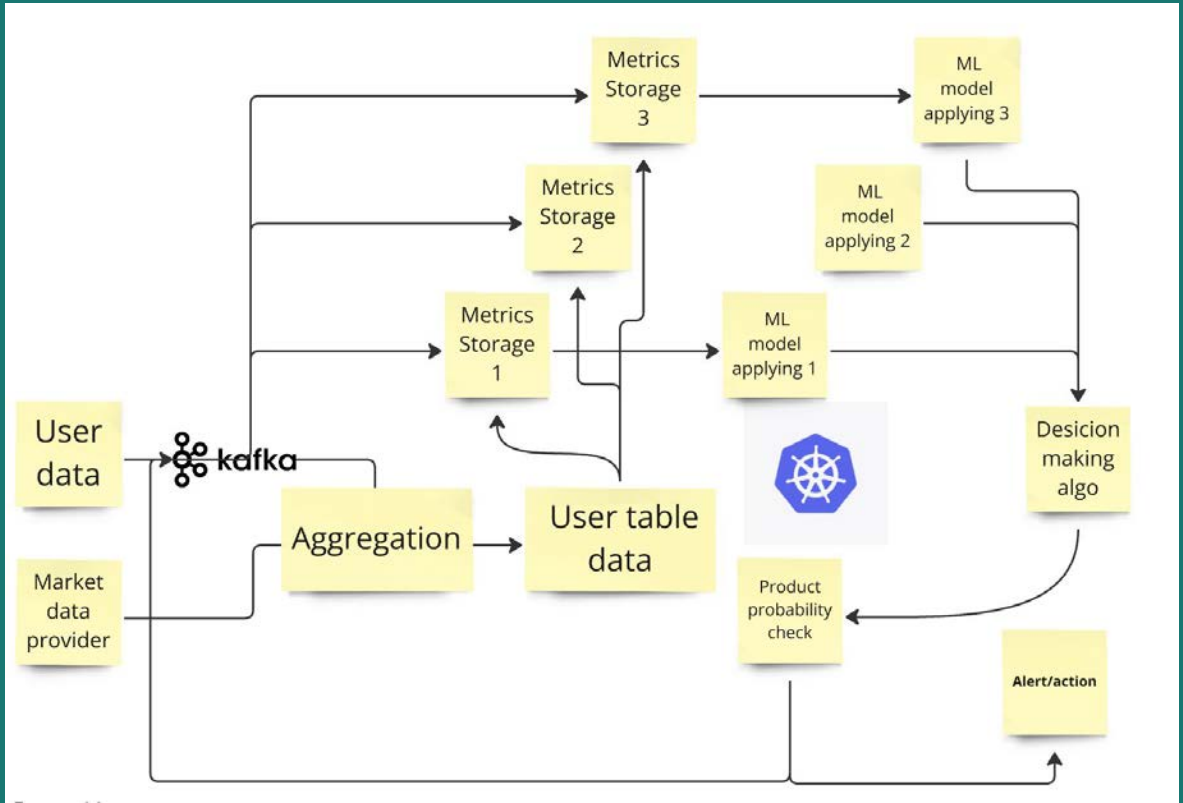
DATA SOURCES



WHAT IS THE CHALLENGE?
THE TARGETS ARE TOO DIFFERENT

- For one quality metric, let’s say, Payments_cost, many related costs/details can be attributed to it that deal with one type of fraud.
- In case there are multiple targets, stacking different models could be worth considering.
- When it comes to supervised gradient boosting, it is right to see it as some sort of smart ifs. Don't forget: the smartest if can be determined only by you.

STACKING DIFFERENT MODELS AND FILTERS



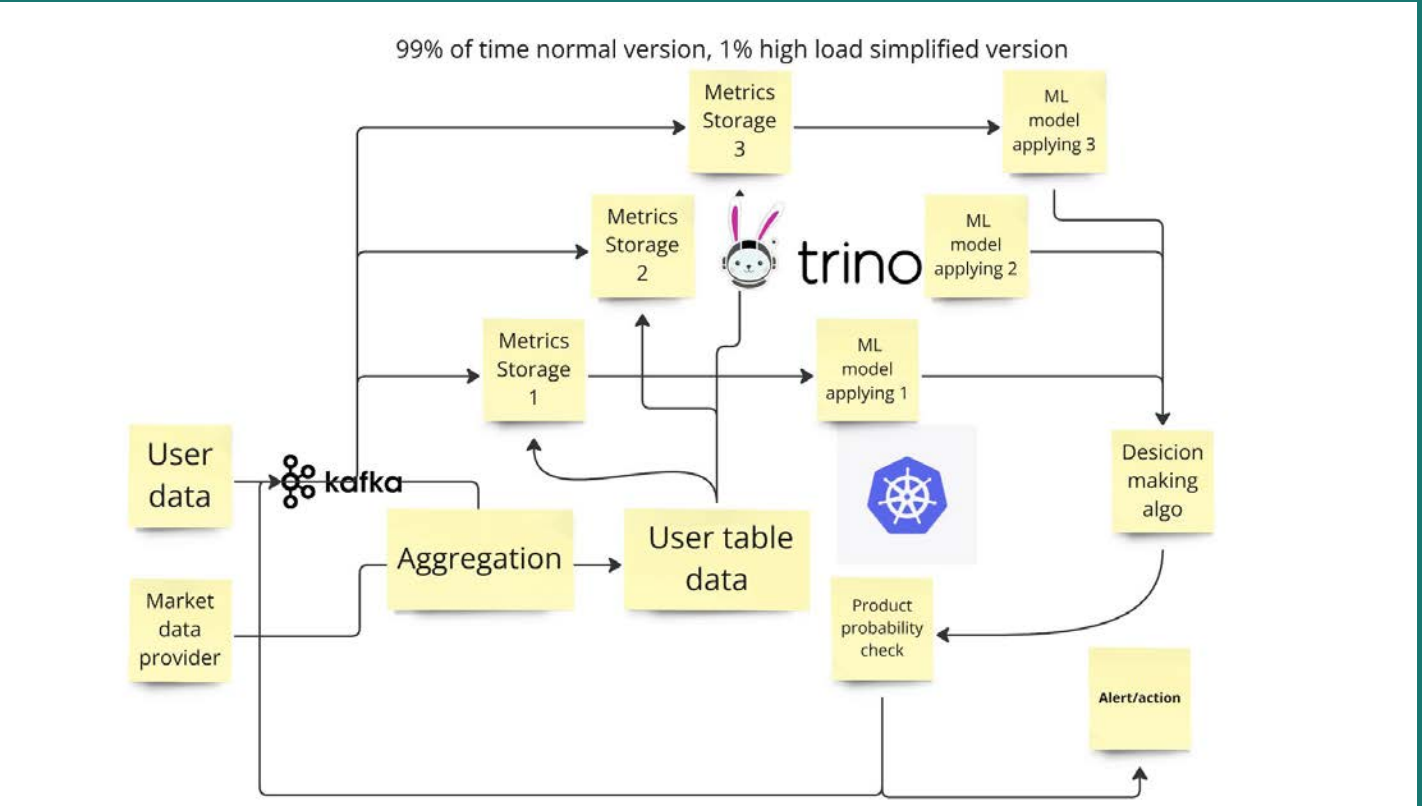
INFRASTRUCTURE FEATURES

- In production, it’s crucial to perform fast joins of large datasets or create complex data samples.
- Equally important to access historical data by user_uid.

STACK: SPARK CPU ⟶ TRINO (MEMORY MANAGEMENT)

The best practices working with real-time modeling include preserving the previous state of user data and filtering the data stream that feeds into the model.

INFRASTRUCTURE FEATURES



OFFLINE SUPPORT TEAM

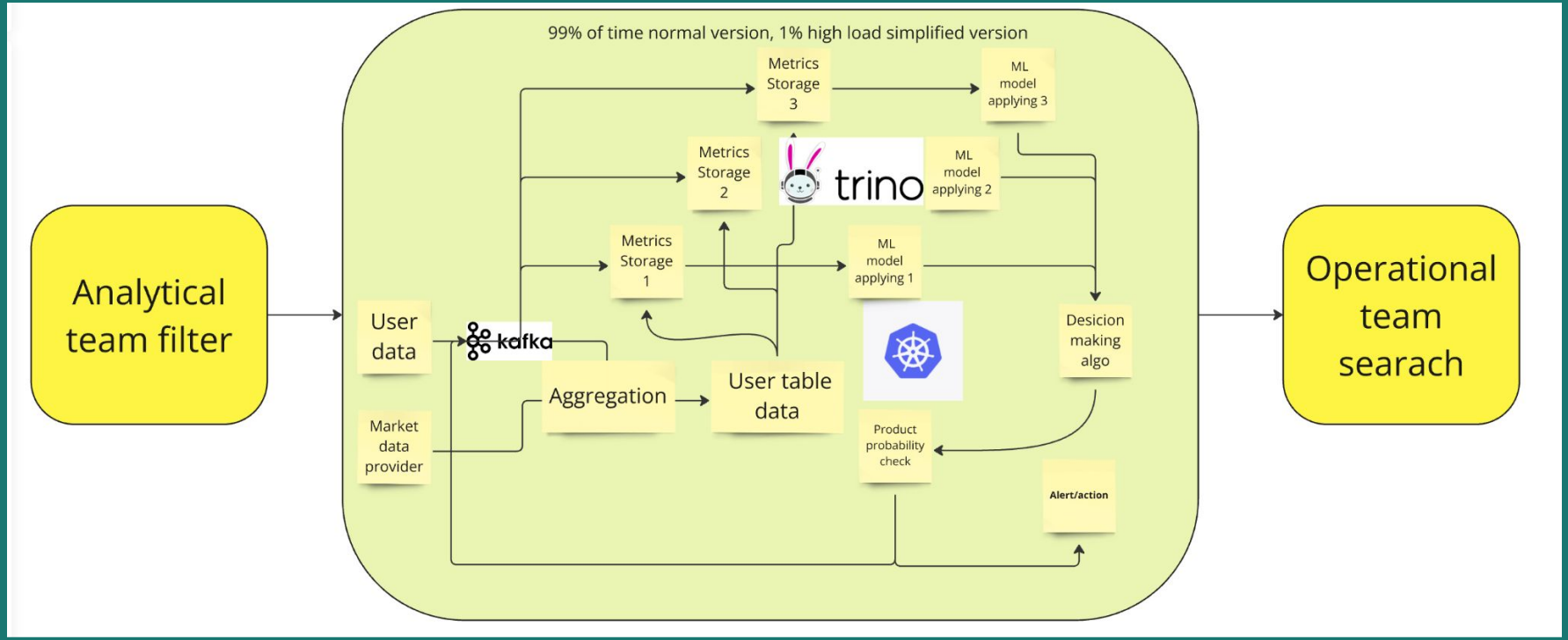
We need guys who are looking at the screen:

- P1 - prob that the catch one with ML
- P2 - prob that analytical filter catch one
- P3 - prob that operational team catch one

Overall P = 1 - (1-P1)(1-P2)(1-P3)
Good precision!

The contribution of the operational and analytical team to improving the quality of detection cannot be underestimated.

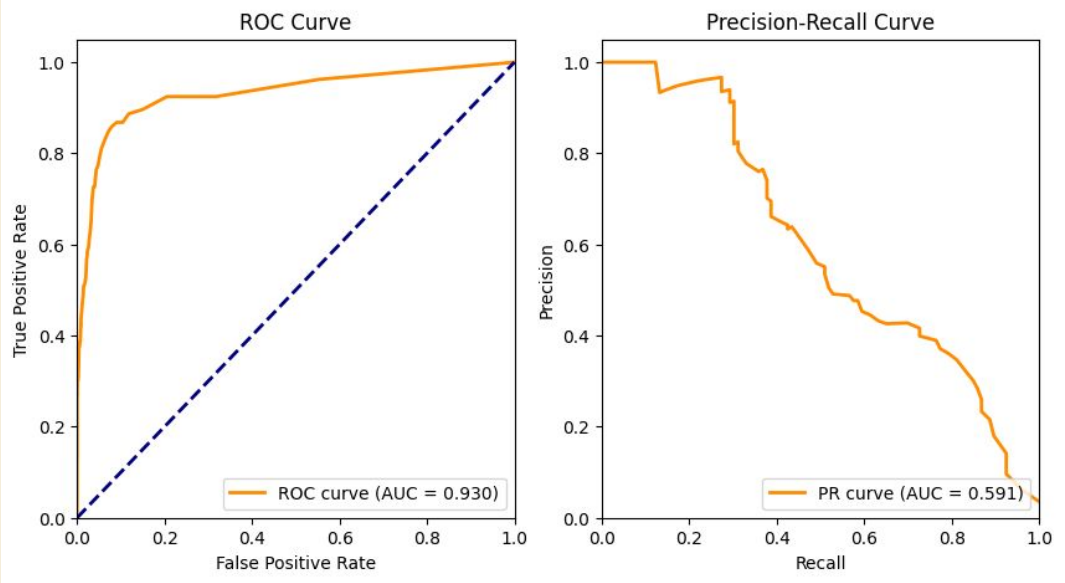
OFFLINE PART OF THE PLATFORM



MONITORING MECHANISMS

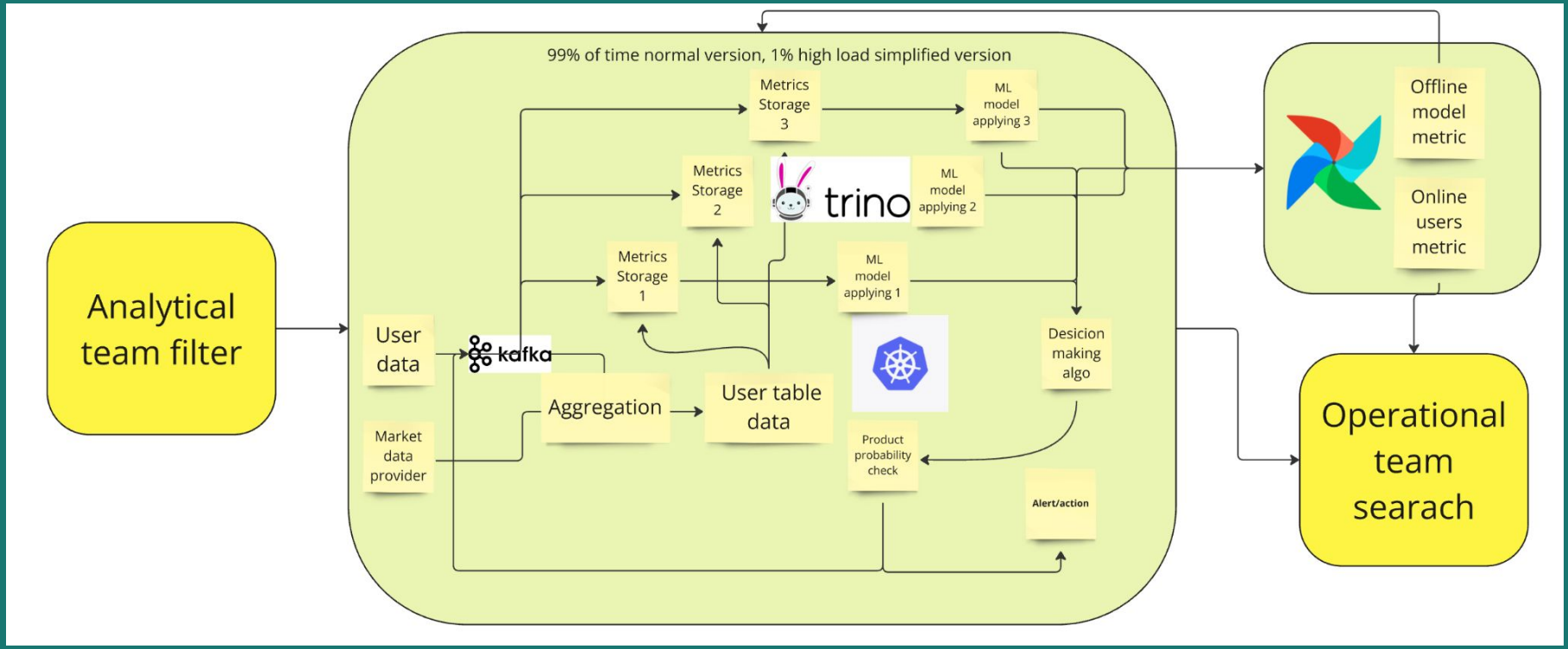
Online and Offline Model Metrics:

- Payment Cost
- Technical metrics
- PR AUC
- FPR



Visualisation and the importance of case review to understand what *exactly* is going on

FINAL FRAMEWORK



THANK YOU FOR YOUR ATTENTION!

@raymor @pavel-zapolskii pavel@zapolskii.com