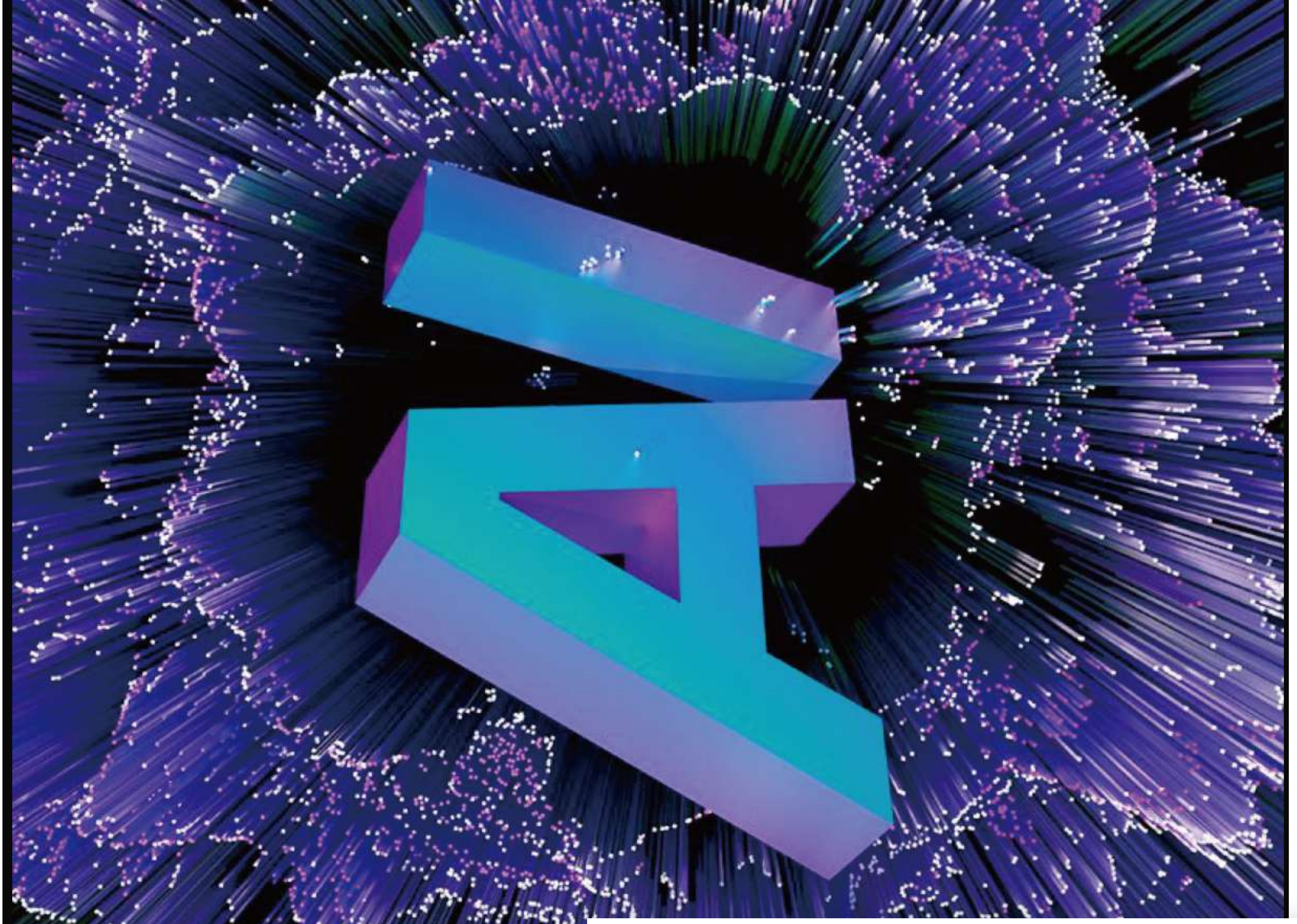
携程实时智能检测平台实践

潘国庆
携程

FLINK FORWARD # ASIA
实时即未来 # Real-time Is The Future

FLINK FORWARD

Contents
目录



背景介绍

Background

01

背景介绍

Background

规则告警配置复杂

Complex Configuration

规则告警效果差

Poor Effects

规则维护成本高

High Maintenance Cost

Prophet

Prophet

02

Prophet

What is Prophet

一站式异常检测解决方案

“One-Stop” Anomaly Detection Solution

- 基于时序类型数据

  Based on Time Series Data

- 以平台为接入对象
  以去规则化为目标

  Monitor System As Target
  Abandon Regular Configuration
  As Final Goal

- 基于深度学习算法
  实现异常智能检测

  Based on Deeping Learning
  Algorithm
  Achieve AI Monitoring

- 基于实时计算引擎
  实现异常实时检测

  Based on Real Time Processing
  Platform
  Achieve Real Time Monitoring

Prophet系统架构

Prophet System Architecture

Why Flink?

Why Flink?

高效的状态管理

Memory、FileSystem、RocksDB State Backend

丰富的窗口支持

Tumbling、Sliding、Session Window

支持多种时间语义

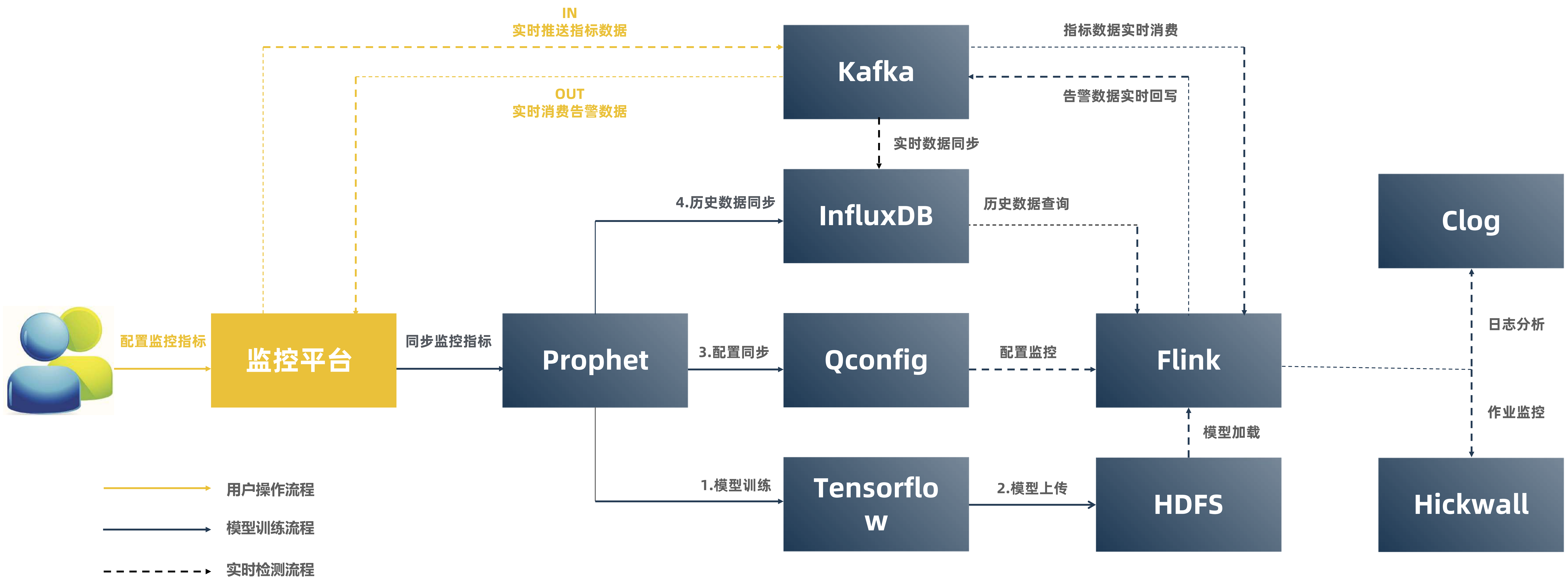
Processing、Ingestion、Event Time

支持不同级别的容错语义

At most、At least、Exactly Once Fault Tolerance

Prophet操作流程

Prophet Operating Procedures



智能化与实时化

AI and Real Time

03

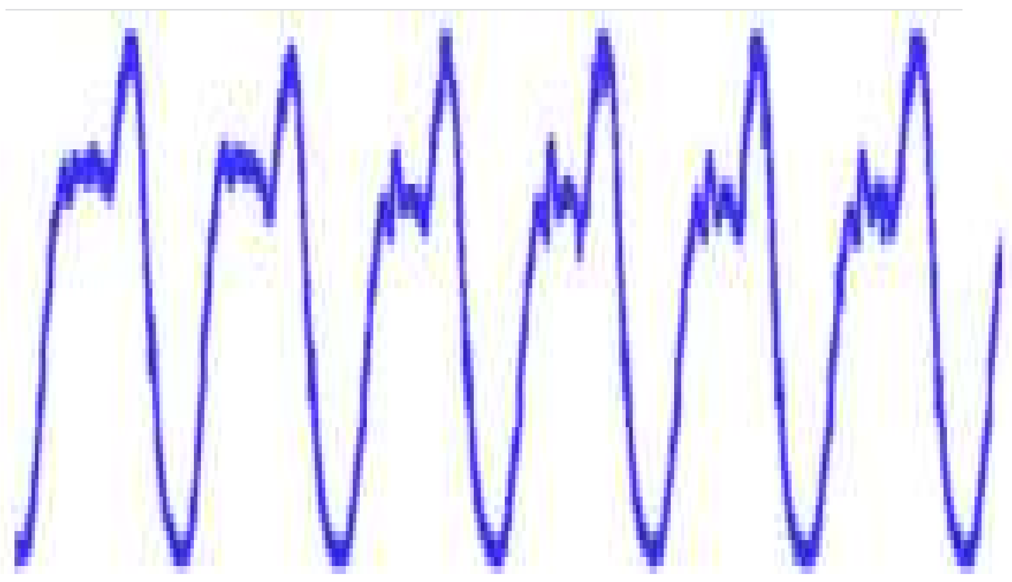
智能化挑战

Challenges in AI Alert

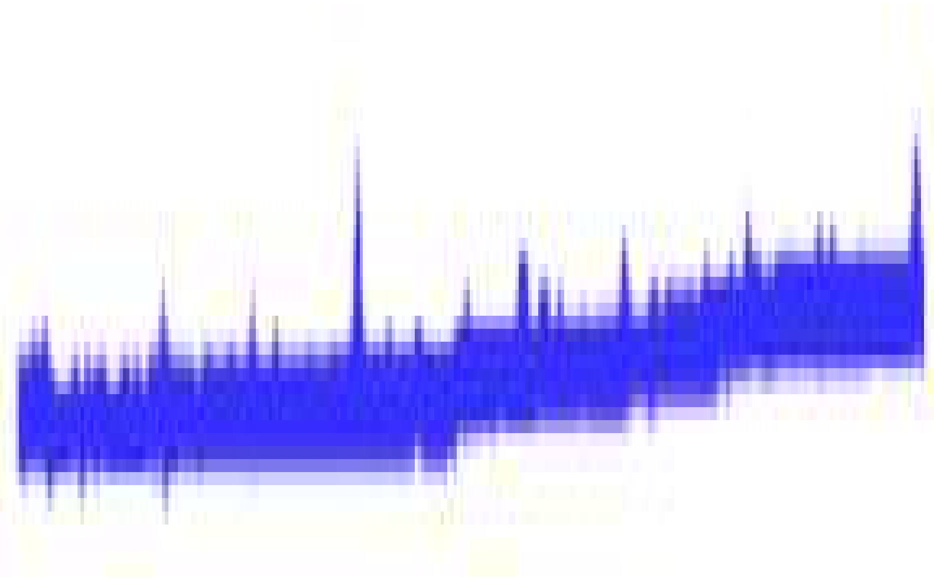
负样本少
Missing Negative Samples
异常发生频率低
Low frequency of abnormalities

业务指标类型多
Different types of Metrics
订单、支付等
Orders, Payments etc.

业务指标形态多
Different forms of Metrics
周期波动、稳定、非周期
Periodic, Stable, Aperiodic



周期波动
Periodic



稳定
Stable

非周期
Aperiodic

深度学习算法选择

Deep Learning

算法 Algorithm	优点 Advantage	缺点 Disadvantage
RNN	适合序列变化数据 Suitable for Time Series Data	存在梯度消失现象 Vanishing gradient
LSTM	解决RNN梯度消失问题 Solve Vanishing gradient	单指标单模型 One Model Per Metric
DNN	单模型覆盖所有场景 One Model Solves All Scenarios	特征工程复杂 需要大量标注数据 Feature Extraction is Complex Need more labels

离线模型训练

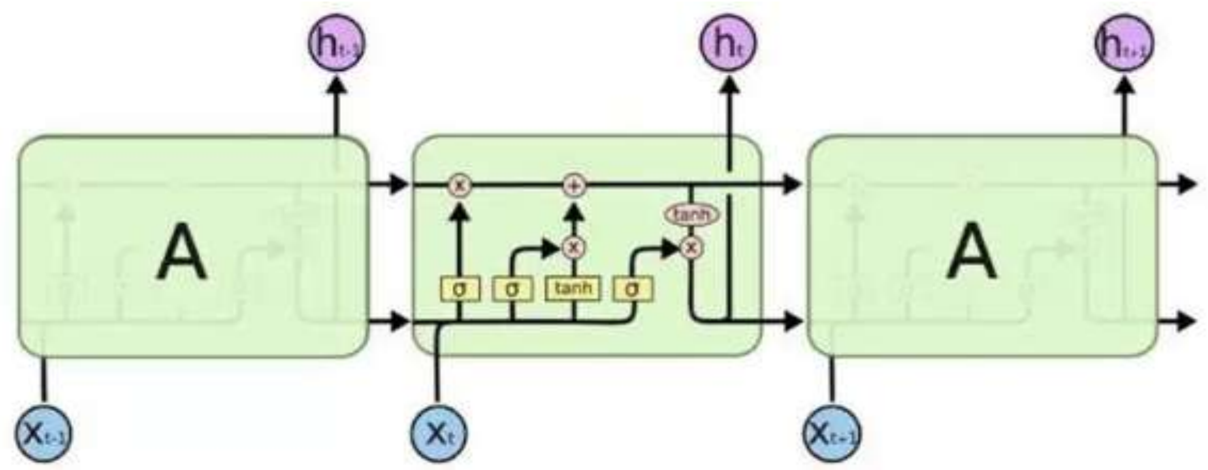
Offline Model Training

历史数据

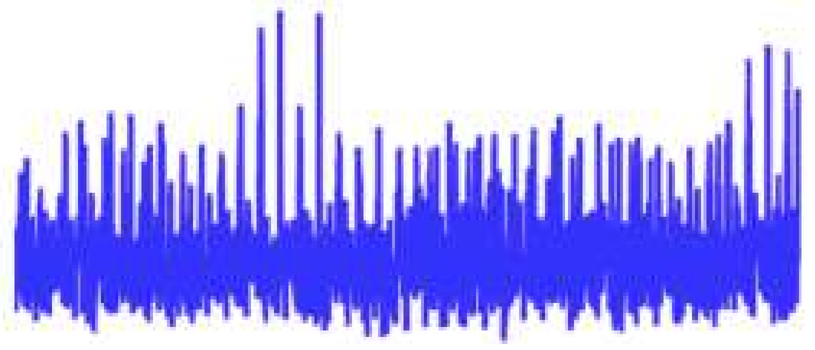
- 空值插补
- 异常区间数值替换
- 剔除节假日

- 多尺度滑动窗口时序特征
- 频域特征

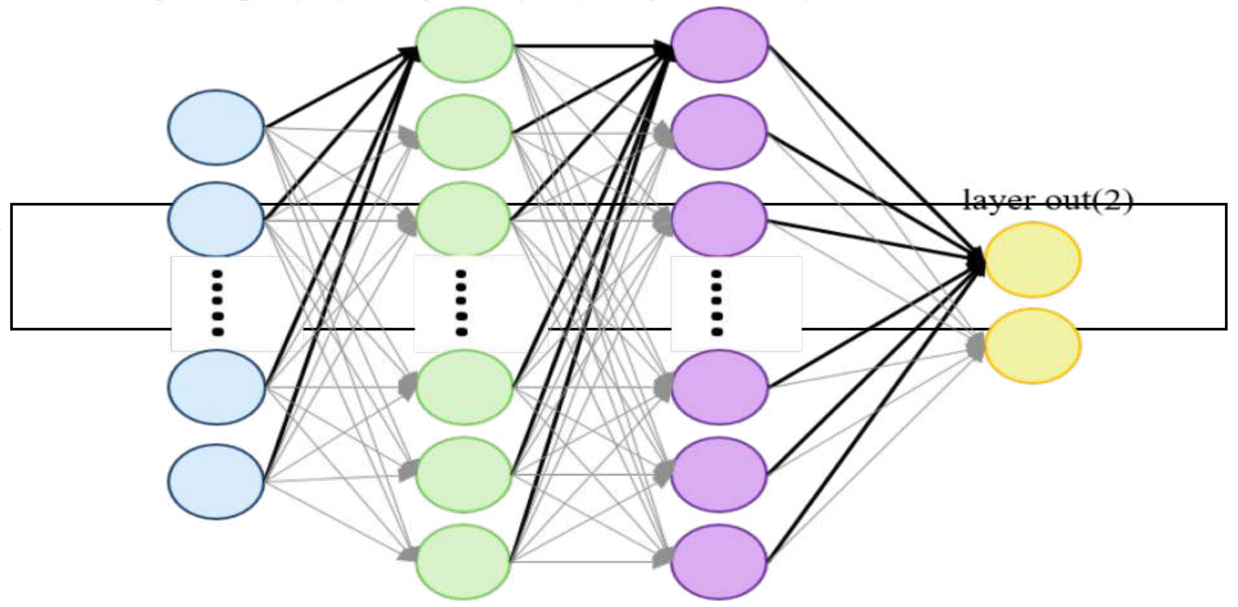
特征计算



非周期

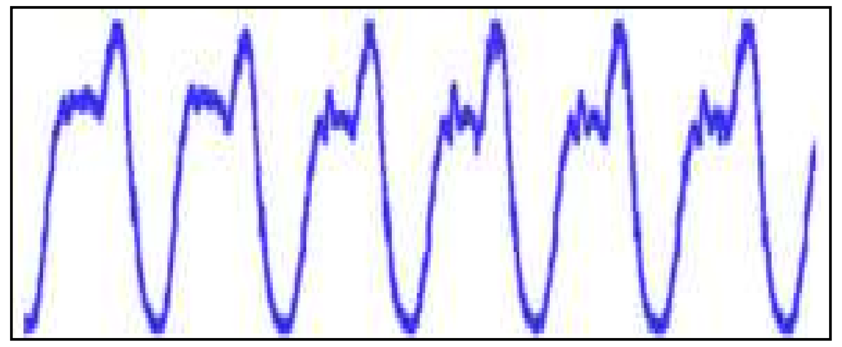


Model

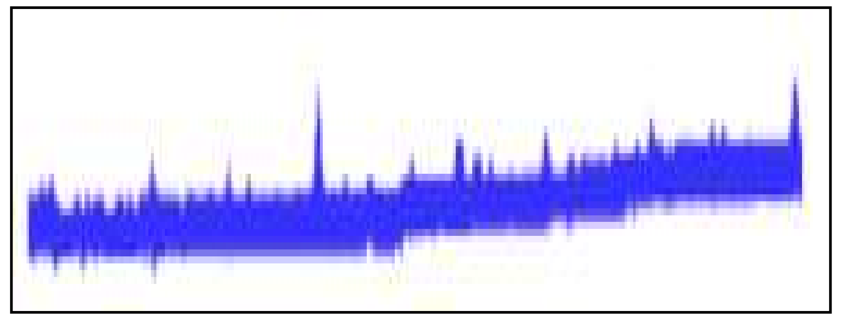


验证调参

周期



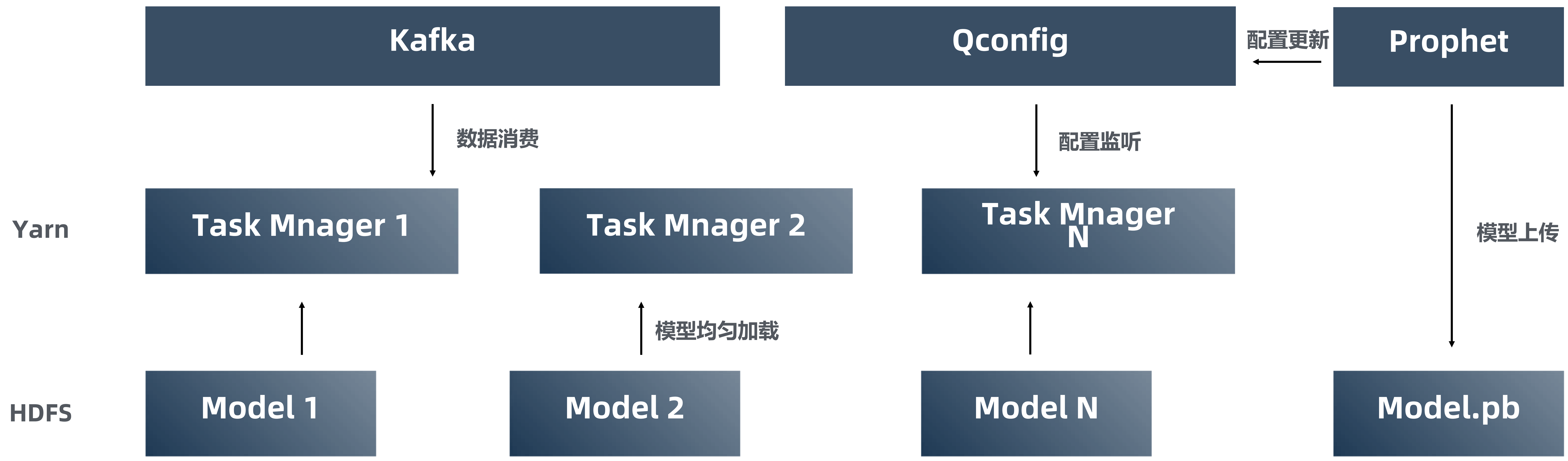
平稳



分类模型

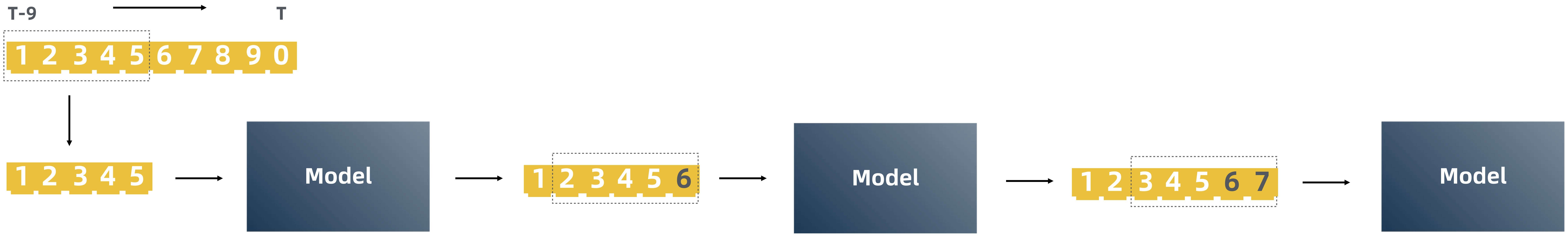
模型动态加载

Model Loading

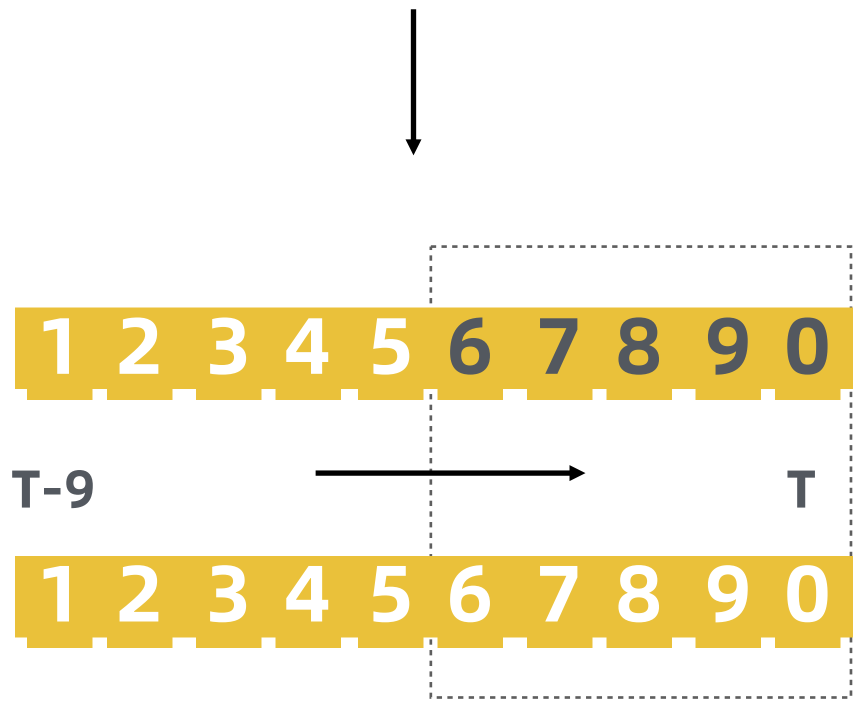


数据实时消费与预测

Data Real Time Consuming and Predicting

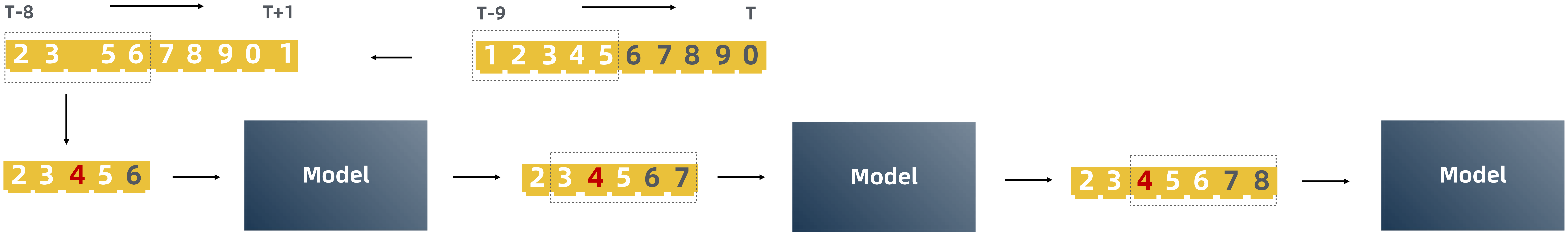


- 基于**Flink Event Time** + **滑动窗口**
  Based On Flink Event Time and Sliding Windows
- 单个窗口累计**10个**时间粒度的数值
  Window of size 10 that slides by 1
- 使用前**5个**值预测下一个值
  Based on the previous 5 data to predict the next data
- 基于后**5位**预测值与实际值做对比
  Compare the predictive data sets with the actual data sets

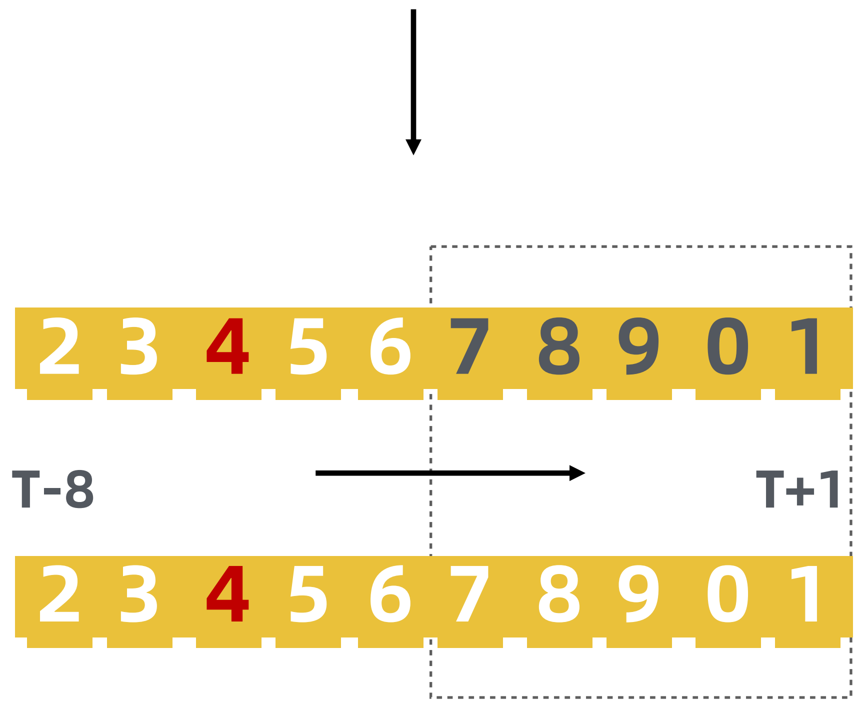


数据插补与替换

Data Completion and Correction



- 基于Flink StateBackEnd存储异常区间预测值
  Using Flink StateBackEnd to store the states
- 使用预测值替代异常区间的异常值
  Using the predicted value to replace the anomaly
- 使用均值与标准差补齐缺失数据
  Using the Standard deviation and Mean value to fix the missing value



实时异常检测

Real Time Anomaly Dection

基于异常类型与敏感度判断

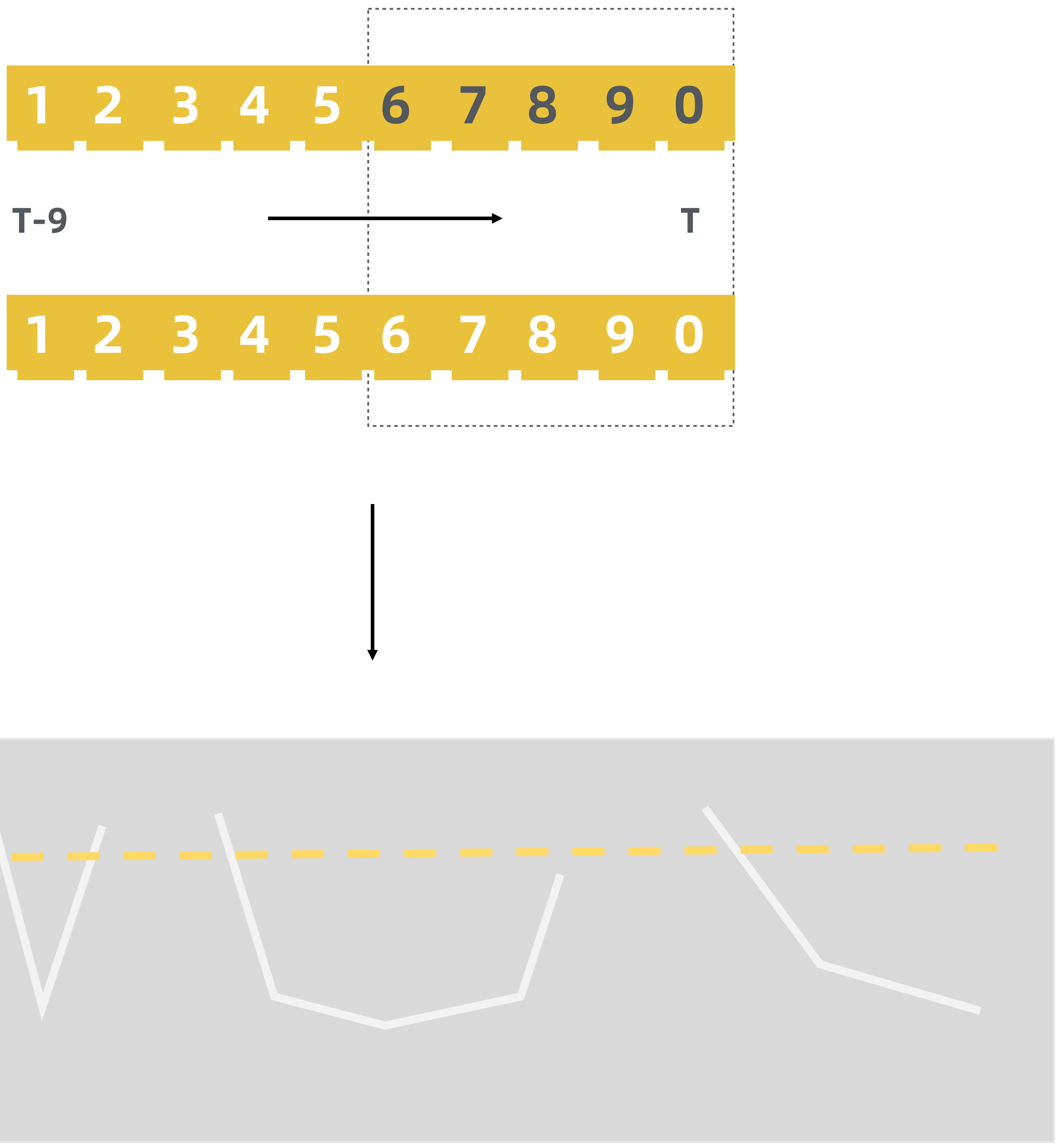
Based on anomaly type and Sensitivity to detect
异常类型包含上升、下降或两者，敏感度分高中低
Anomaly type: increase and decrease, Sensitivity: High, Medium and Low

基于预测集与实际集的偏差判断

Based on the deviation between the predicted data set and the actual data set to detect
当偏差过大时，将当前窗口数据作为潜在异常指标
When the deviation is large, considering the current data set as the potential anomaly

基于历史同期数据均值与标准差判断

Comparing with the history data by Calculating the Standard deviation and Mean value
潜在异常还需与历史同期数据比较来最终确认是否存在异常
Two step confirmations are needed which compare with the current actual data sets and the history data sets



常见场景

Common Scenarios

常见问题
Common Issues

监控指标多、纬度广、QA人力不足

Too Many metrics and too many Dimensions, not enough resources

异常原因
Abnormal Causes

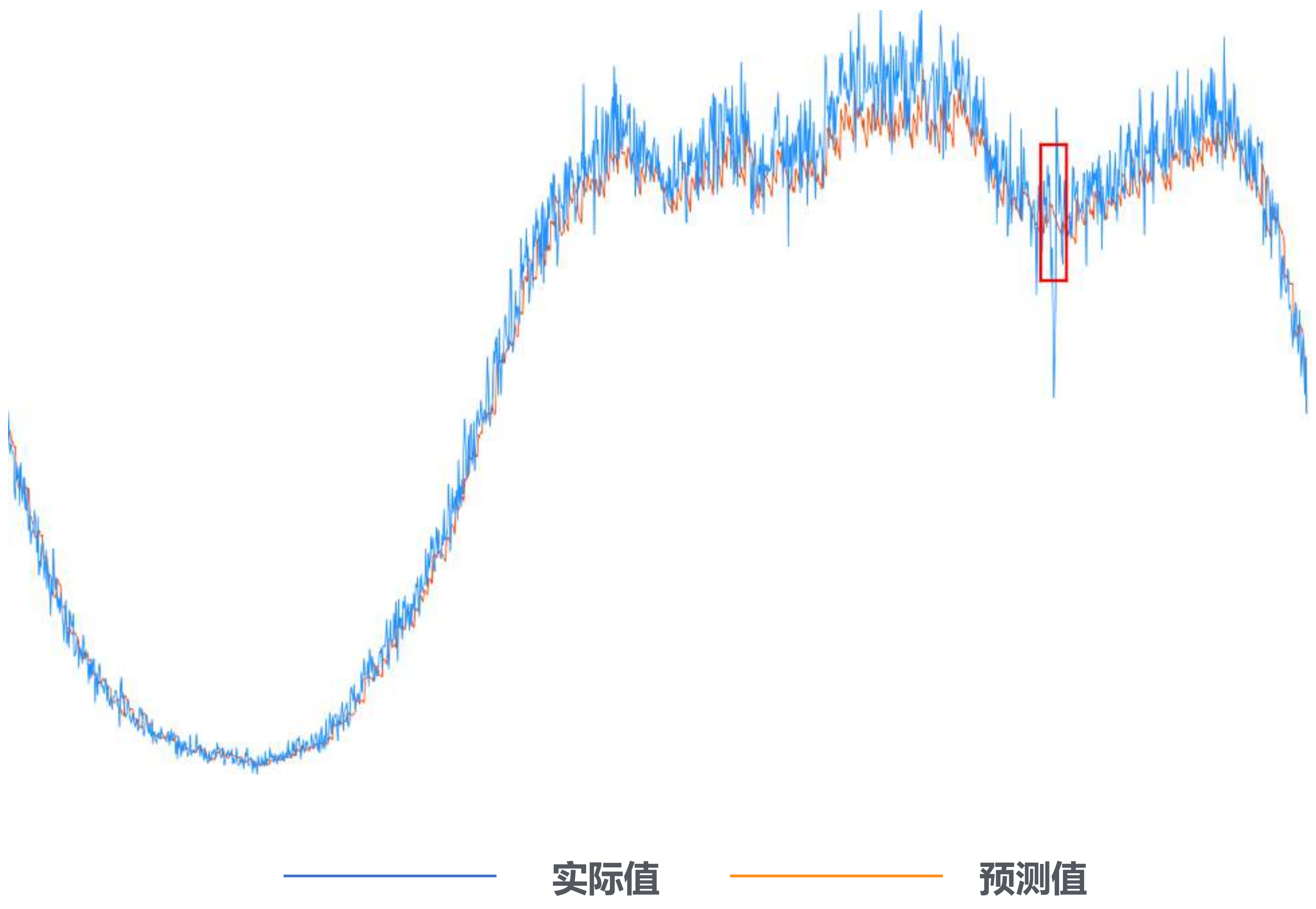
多由技术性问题引起, 少量外部因素

Mostly caused by technical issues, Few external factors

解决方案
Solutions

用户协助打标记，基于标记数据持续优化模型

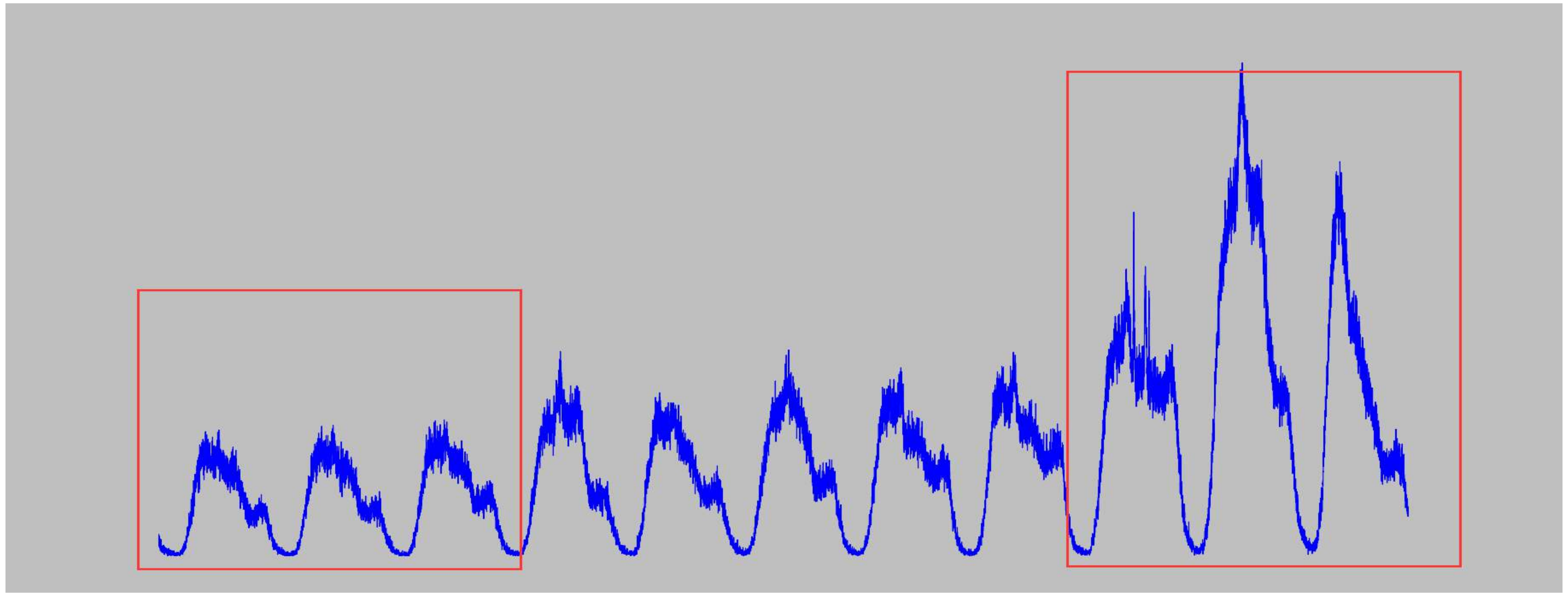
Based on users' labels to optimize the model



节假日场景

Holidays Scenario

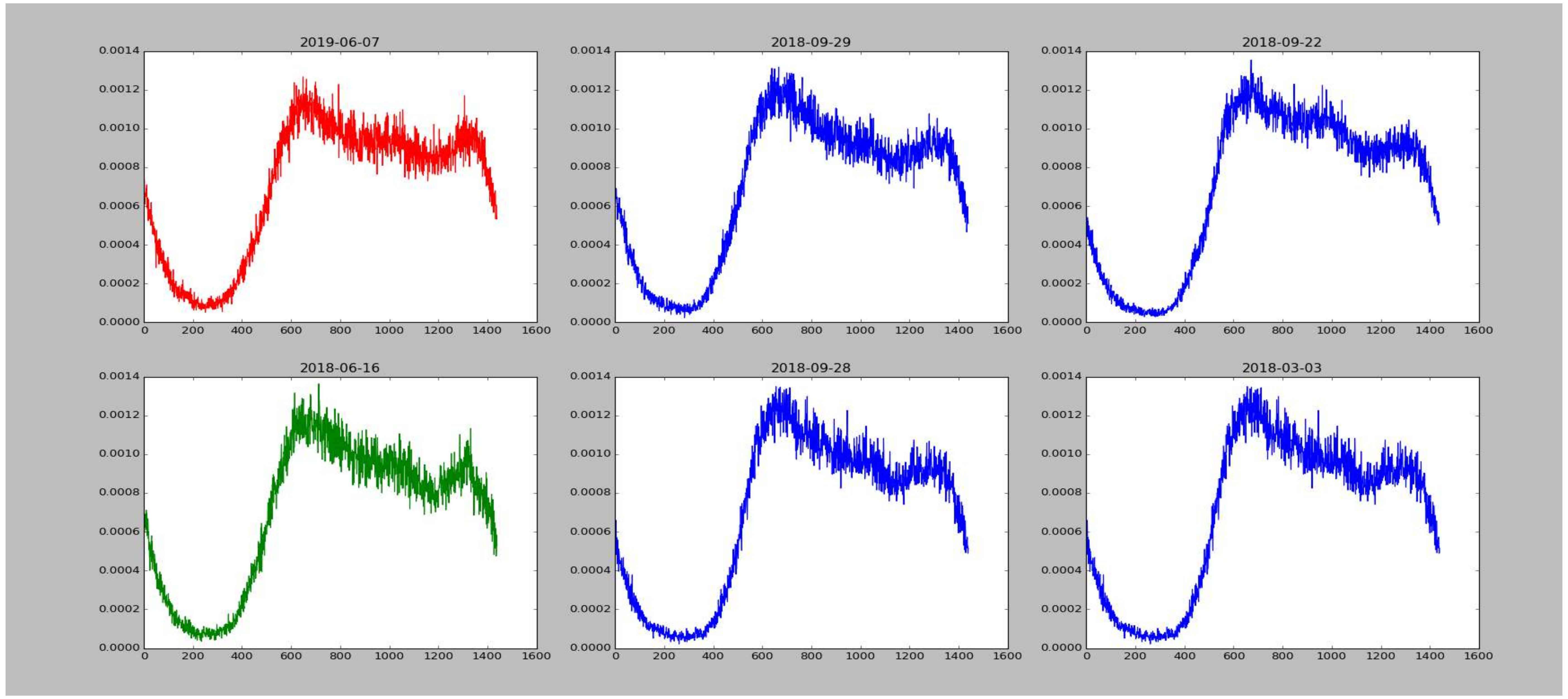
- 不同业务间上涨与下跌的趋势不同
  Different Metrics have different trends
- 上涨幅度大，容易产生漏报
  Large increase makes more missing alarms
- 下跌幅度大，容易产生误报
  Large decrease makes more false alarms
- 小业务活动多，波动剧烈
  Some metrics are volatile due to Promotional Activities



节假日应对

Holidays Scenario

- 需维护每年节假日信息
  Need to maintain every year's holiday info
- 每个节假日对时间序列的影响程度不同
  Every holiday has its own impact factor
- 提取指标2年内节假日期间的数据
  Prepare 2 years' holidays data
- 计算出相似度最高的4个日期
  Calculate Similarity
- 组合数据重新训练模型
  Training model by using the combined data



FLINK FORWARD

平台现状

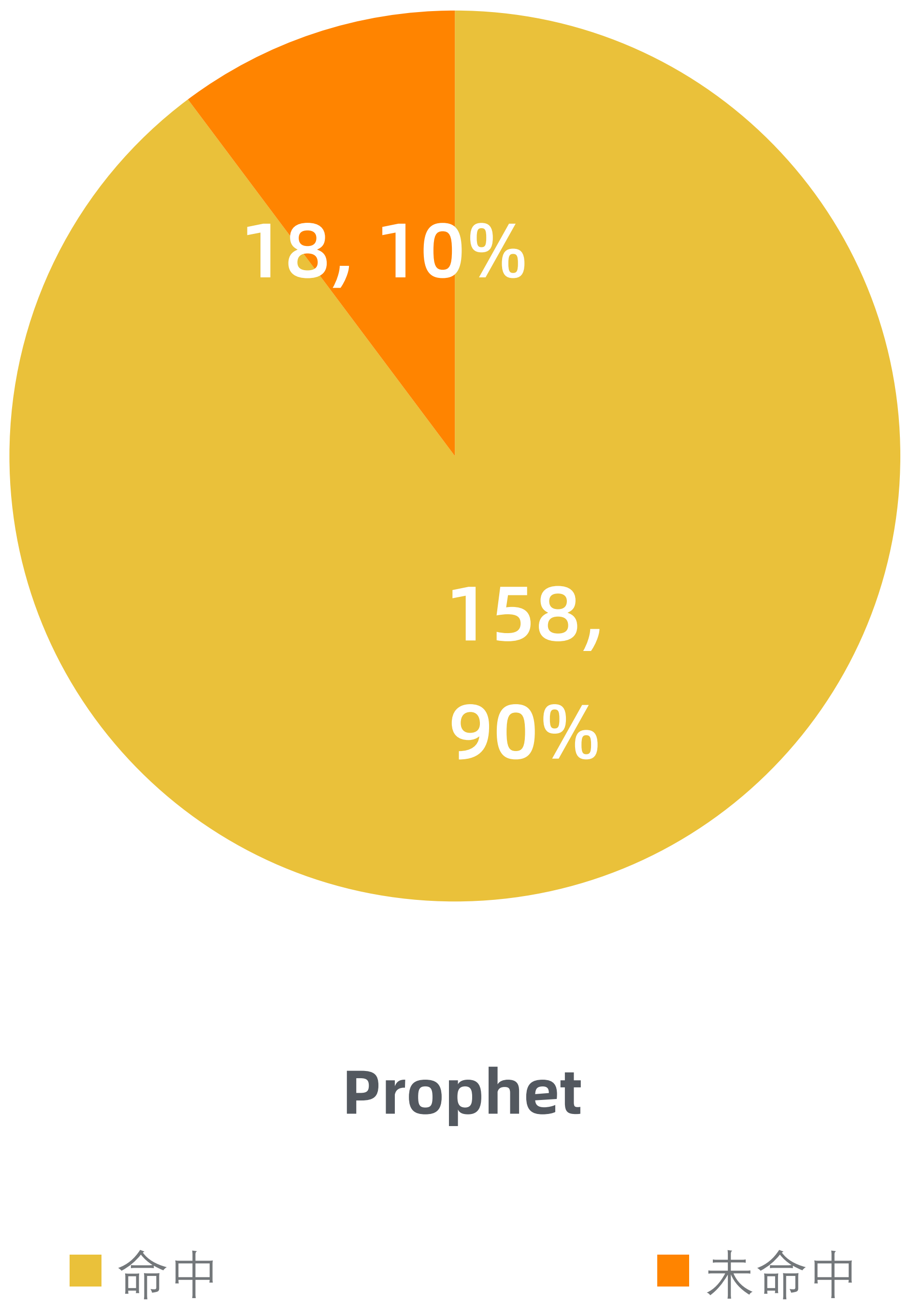
Prophet Current Status

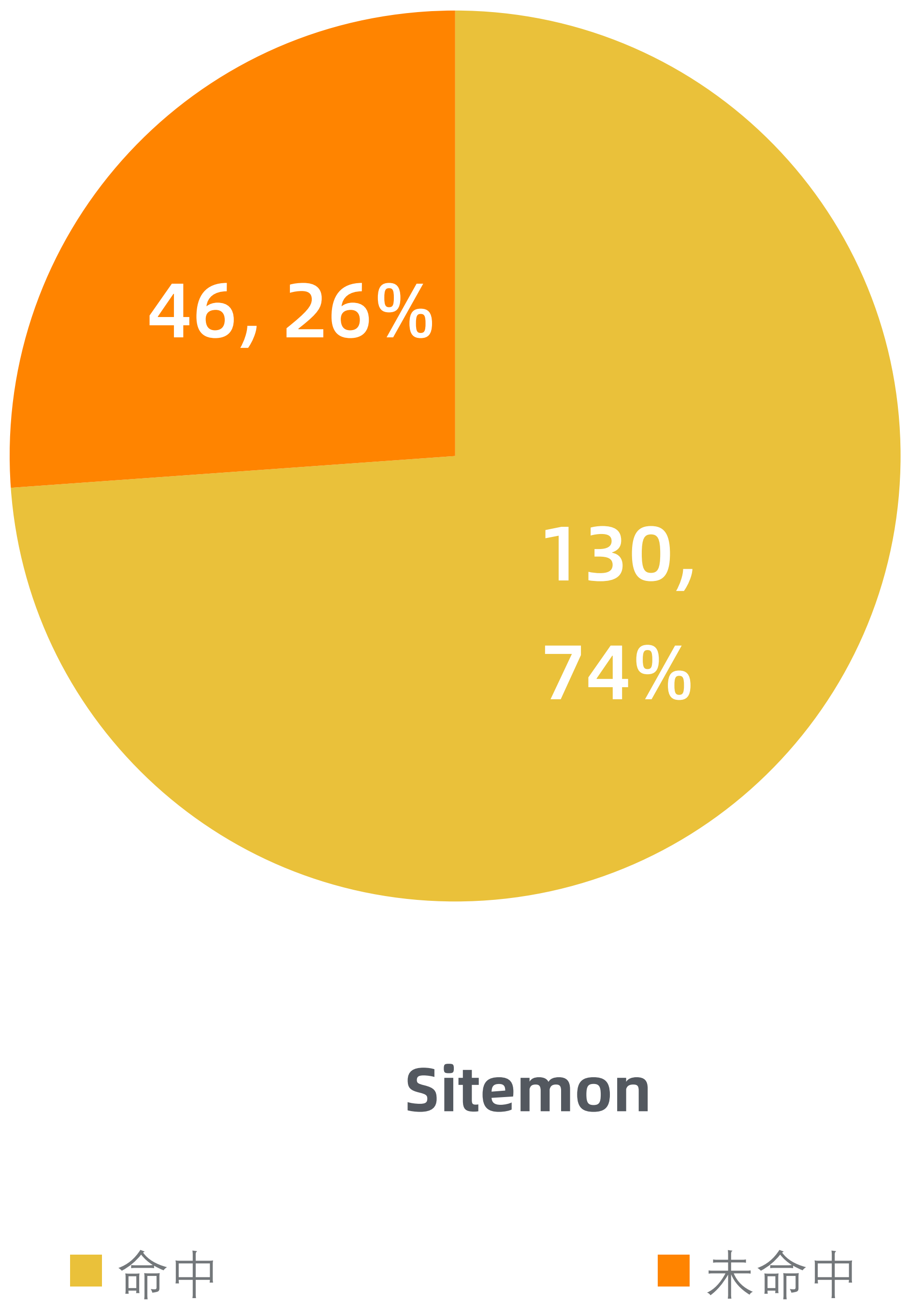
业务线覆盖 Business Coverage	业务类型 Metric Types	监控指标数 Metric Counts	接入平台数 Accessed Platforms
16条	7种	10K+	10+

故障覆盖率 Anomaly Coverage	报警准确率 Accuracy	告警延迟 Delay	告警数量 Alert Count
95%	75%	ms	10倍↓

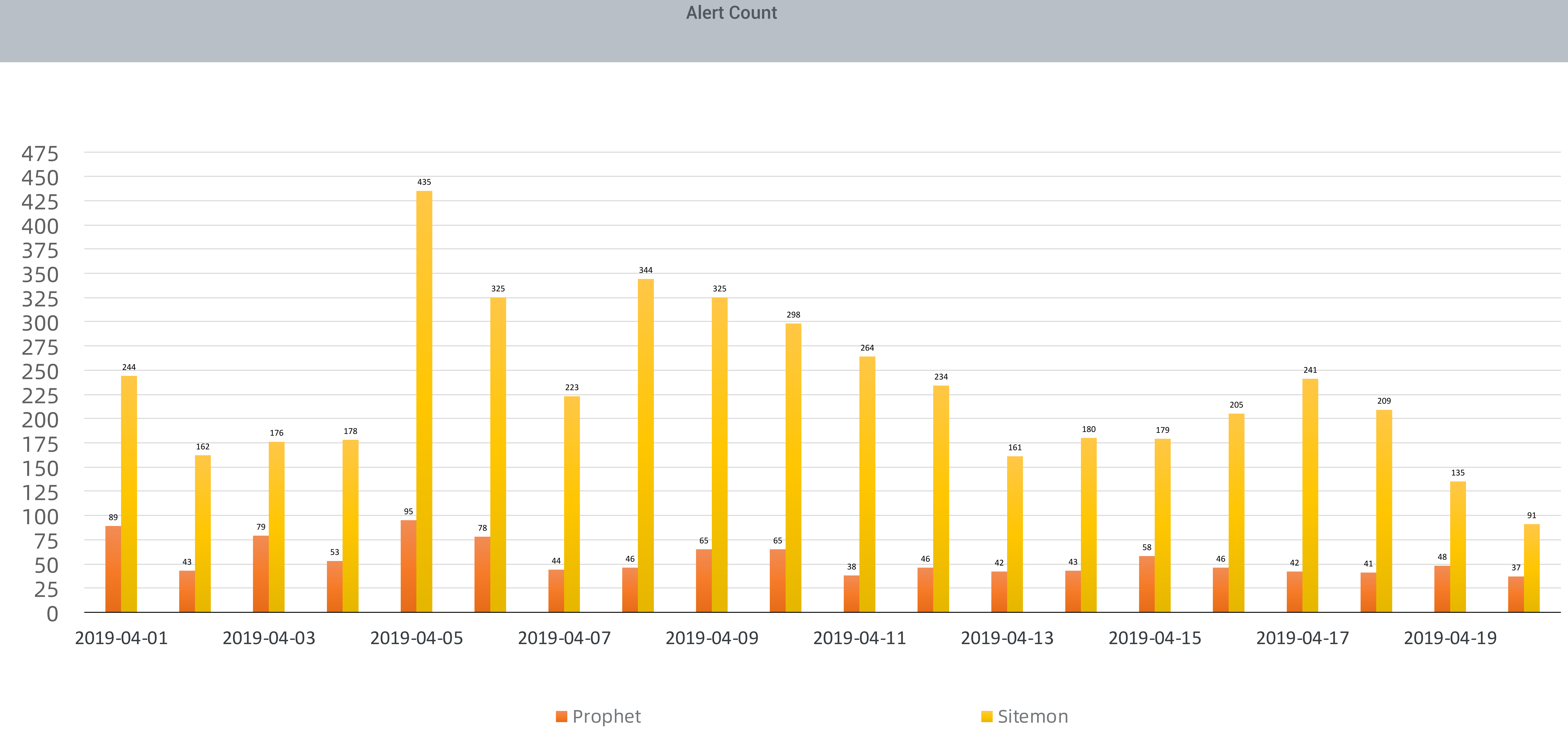
效果对比：召回率

Recall





效果对比：报警数量


Alert Count
475
450
425
400
375
350
325
300
275
250
225
200
175
150
125
100
75
50
25
0
89
244
43
162
79
176
53
178
95
435
78
325
44
223
46
344
65
325
65
298
38
264
46
234
42
161
43
180
58
179
46
205
42
241
41
209
48
135
37
91
2019-04-01
2019-04-03
2019-04-05
2019-04-07
2019-04-09
2019-04-11
2019-04-13
2019-04-15
2019-04-17
2019-04-19
Prophet
Sitemon

挑战与展望

Challenges and Future

04

遭遇挑战

Challenges

资源消耗大

Huge Resources Cost

单指标单模型
模型数量等同于指标数量
One Model Per Metric

节假日影响大

Holidays have more impact

业务指标节假日趋势不同
告警准确性受影响
Different Metrics have different trends

无法适用于全部场景

Not Suitable for All Scenarios

波动剧烈的非周期性指标hold不住
比如遇到大促、活动等
It's hard to hold Aperiodic Metrics

未来展望

Future

通用模型迫在眉睫

Using DNN Model to deal with all the Scenarios
重要业务指标采用单指标单模型
VIP Metrics use LSTM model
非重要业务指标采用通用模型
Other Metrics use DNN model

节假日算法上线

Release holidays Scenario Solution to Production Env
采用节假日对齐方式依据上个节假日的数据加权作为训练数据
Using previous several holidays combined data to train a new model

覆盖全部监控平台

Covering all the platforms in Trip.com
接入更多的监控平台与指标
Monitoring more metrics


THANKS
AI