# Intelligent Anomaly Detection in Heterogeneous Internet Services

Dong Wang

Principal Architect, wangdong13@baidu.com

Baidu Inc.

usenix LISA16

December 4–9, 2016 | Boston, MA

www.usenix.org/lisa16 #lisa16

# Agenda

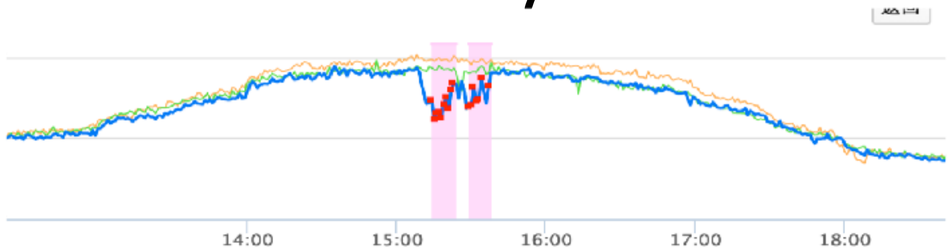
- Brief introduction to Baidu
- Heterogenous services and their challenges to our SREs
- Anomaly detection in typical services
- ARK : A generalized intelligent operation platform for Baidu services

# Introduction to Baidu

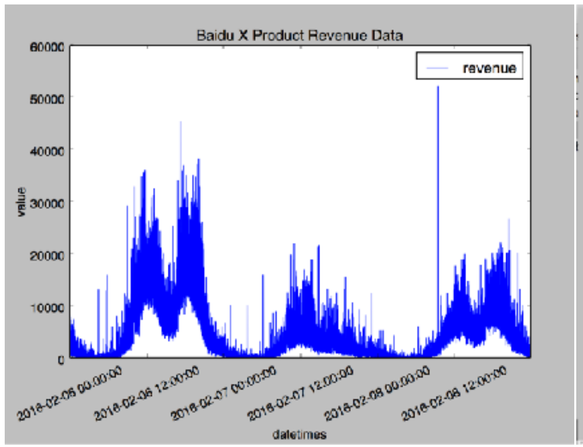
- One the largest search engines in the world
  - ✓ Web/Image/Video/News/…
- Besides search, we also have
  - ✓ Location Based Service - Maps
  - ✓ Social/Knowledge - Tieba/Zhidao
  - ✓ Online to Offline - Nuomi/Waimai
  - ✓ Finance/Payment - Wallet
  - ✓ Cloud computing - Cloud
- Covers more than 1 Billion users in total

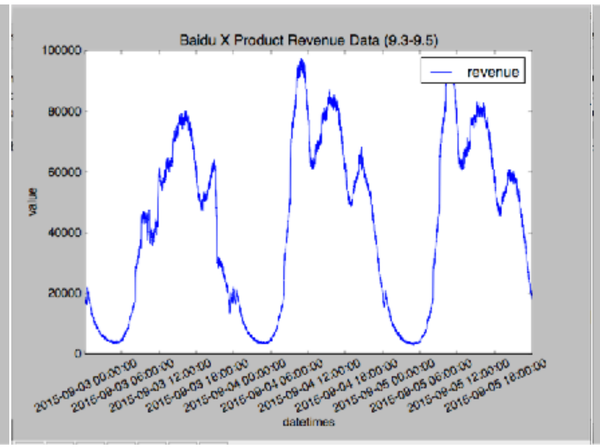
# Anomaly Detection in Heterogenous Services

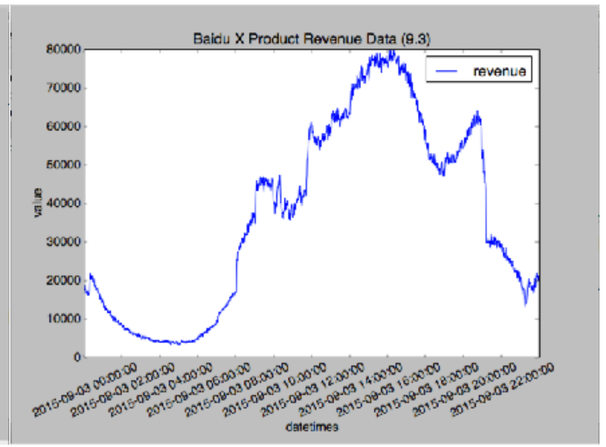
- Anomaly Detection in theory




- However, here are some realities



# Divide and Conquer

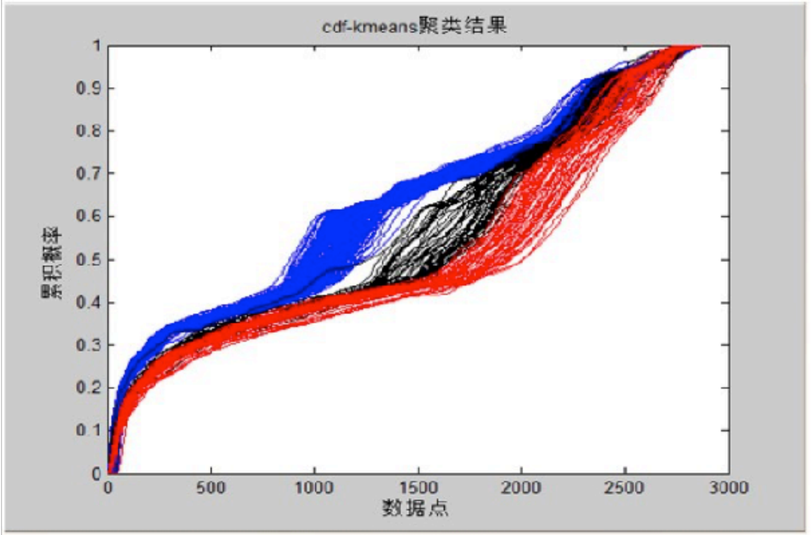
- Several typical categories we manually touch on
  - ✓ Holiday sensitive
  - ✓ Very unstable
  - ✓ Requiring fully automatic configuration

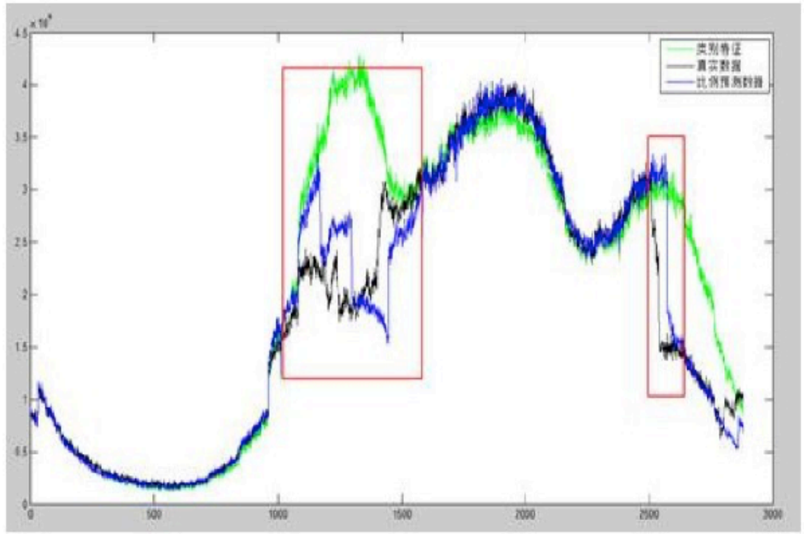
# Holiday Sensitive Curves

- Holidays in Chinese Calendar have no fixed dates
  - ✓ 2016 - Spring Festival (Feb., 8th) - Dragon Boat festival (Jun., 9th)
  - ✓ 2017 - Spring Festival (Jan., 28th) - Dragon Boat festival (May, 30th)
- There is no common pattern among different holidays
- It's hard to know the baselines!
  - ✓ The training data are pretty sparse

# Basic idea and the result

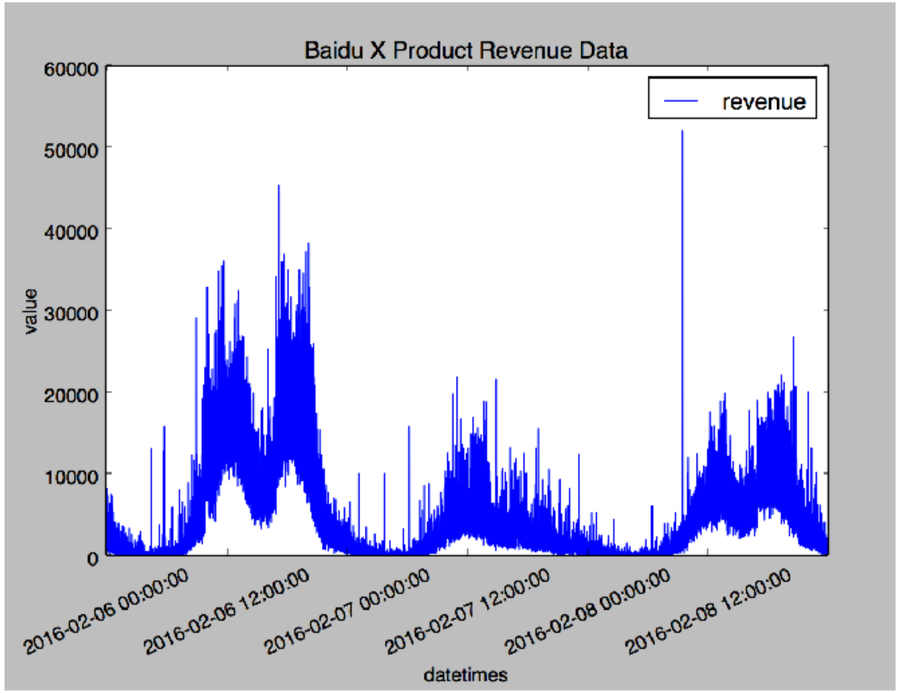
- Clustering on daily CDF of curves
- Classification on dates (features include weekend, holiday, etc.)
- LR based estimated algorithm



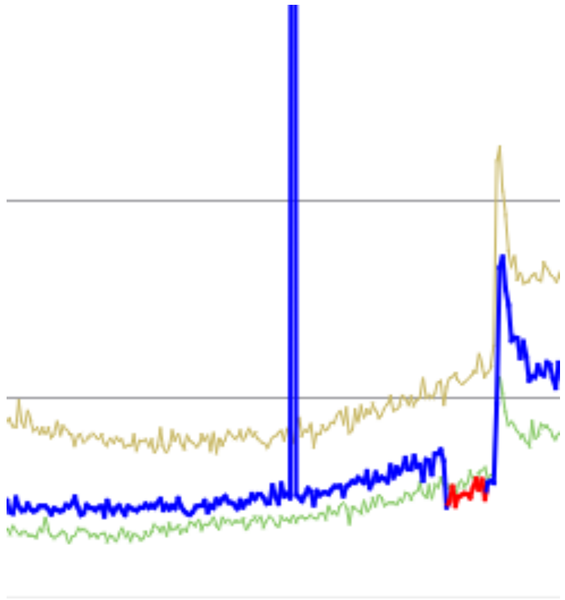
# Very Unstable Curves

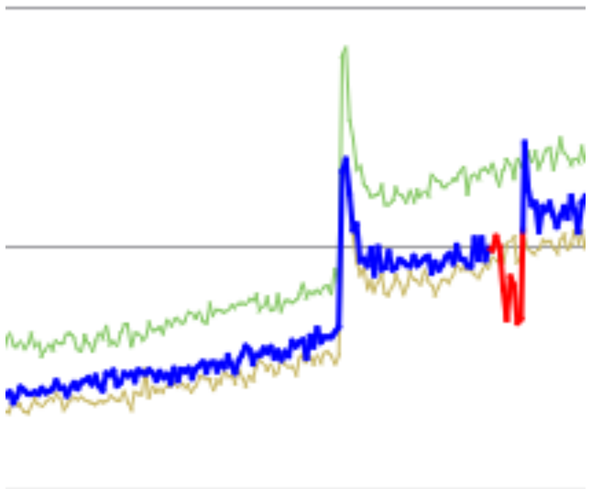
- Very unstable but not anomaly, caused by
  - ✓ Revenue with significantly different price goods
  - ✓ Revenue under some promotions
- The curve's variance is huge, traditional method cannot guarantee the precision/ recall



# Basic Idea and Result

- A compound solution, including
  - ✓ smoothing by sliding window
  - ✓ Reduce the impact from huge absolute values by using logarithm
  - ✓ Considering the increasing/decreasing rate
- The results





# Curves requiring automatic configuration

- Two many curves to monitor, but
  - ✓ No enough bandwidth to do manual configuration from SRE side
  - ✓ Hard to select algorithms
  - ✓ Even harder to setup/adjust parameters
- The examples of such metrics
  - ✓ RPC numbers between two modules
  - ✓ Network transmission amount on some switch devices

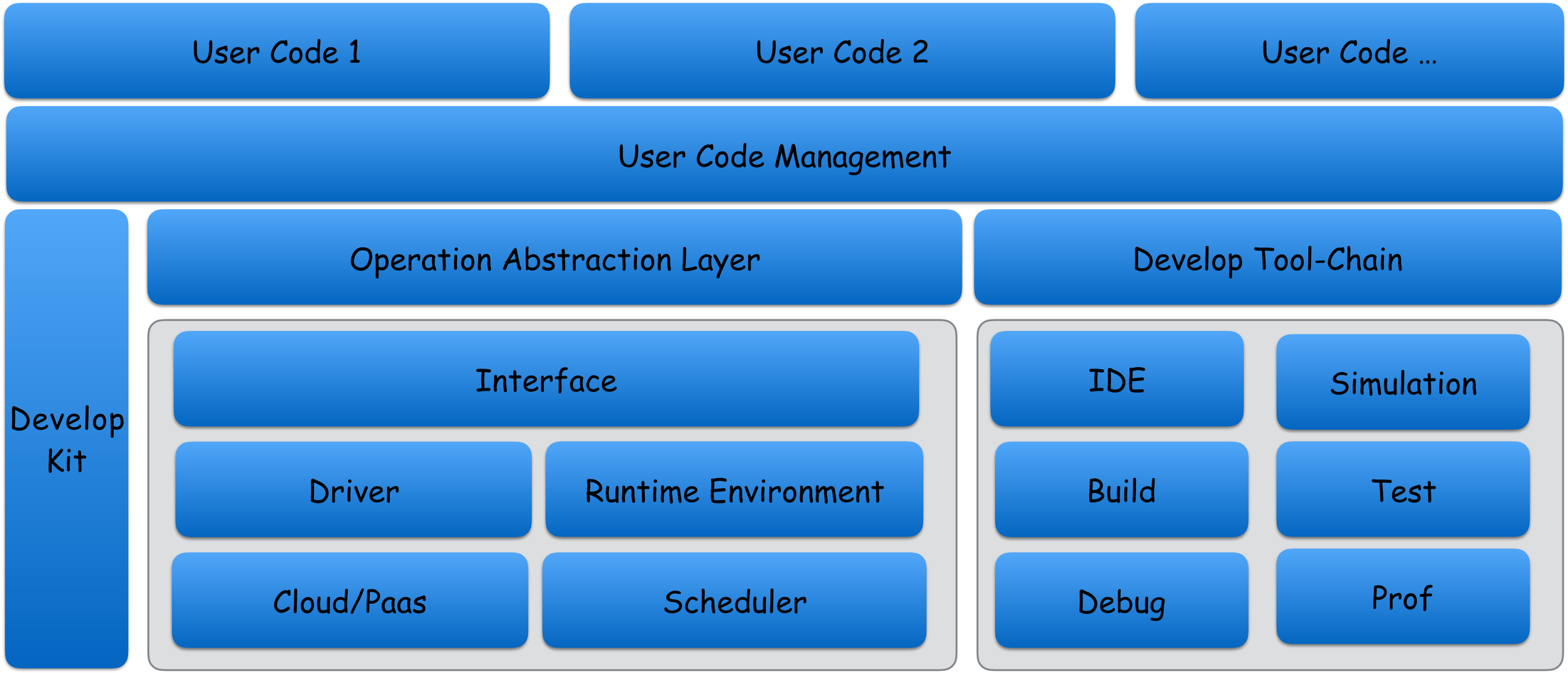
# Basic Idea and Results

- Using machine learning to select algorithm
  - ✓ Whether or not the curve is periodical
  - ✓ How the curve's stability look like
  - ✓ The difference between maximum and minimum
- The default parameters configuration, plus auto-adjustment based on user feedback (marked by on-call)
- The sampling results so far
  - ✓ Precision is about 84%

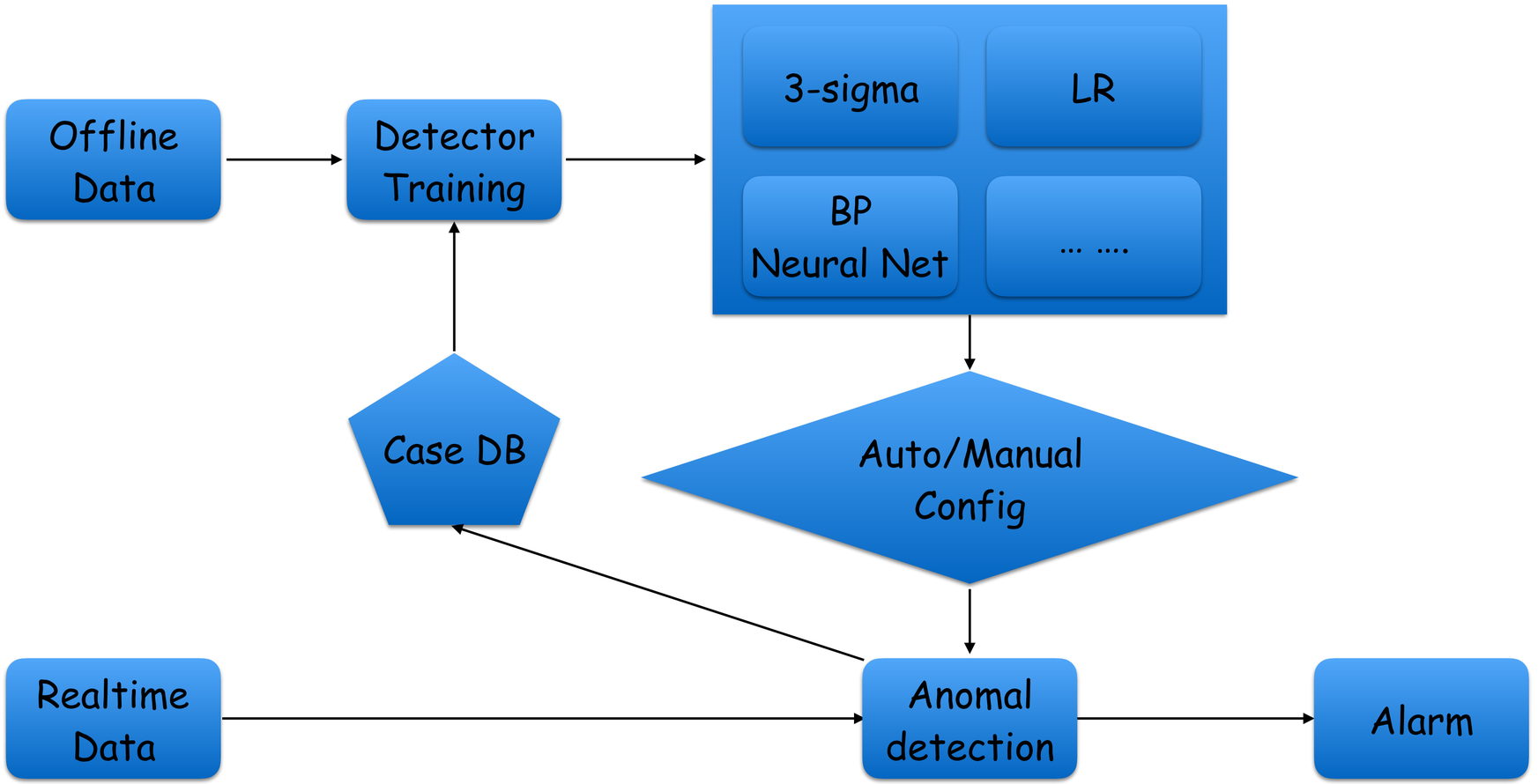
# More Pain Points

- Other SREs have needs to customize the existed algorithms
- Codes are hard to reuse
  - ✓ Different execution environments (programing languages)
  - ✓ Different data sources with different formats
  - ✓ Different teams/projects

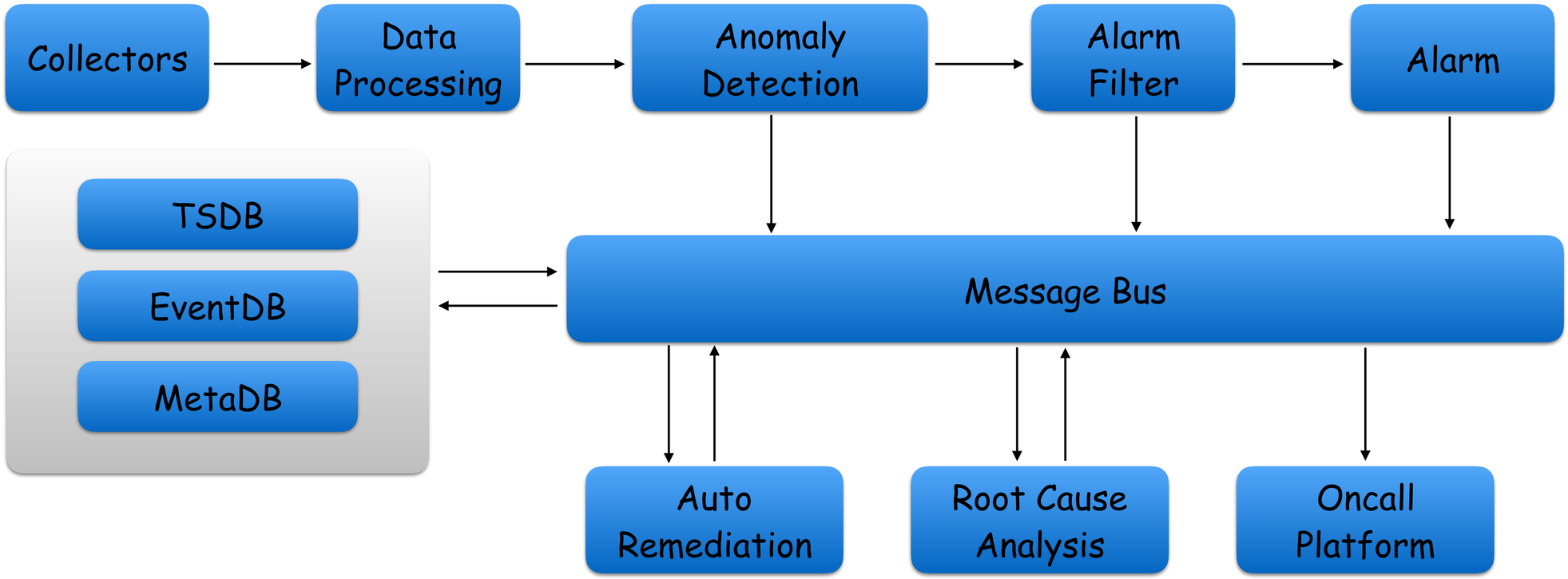
# ARK - A Generalized OP Platform



# Unified Algorithms and deployment



# Unified Monitoring DB and Platform




智能OnCall
百度地图十一出行高峰保障直播间
地图活动直播间10.1
活动状态
12点开抢猴子
最高QPS:
累计PV
12点抢猴子
最高QPS:
累计PV
十一狂欢节-AR活动
最高QPS
累计PV
玩游戏，赢汽车！
最高QPS
止损历史
异常指标已恢复正常，止损...
异常指标已恢复正常，止损...
决策多个特征异常，无法自...
核心 决策多个特征异常，无...
直播内容
输入命令
发送
止损信息
常指标已恢复正常，止损成功
止损信息 18:42:26
预案执行成功，等待止损效果检测
止损信息 18:42:15
成预案决策，开始执行[ma
预案详情
止损信息 18:42:13
发现指标异常，[c
可用性报警异常，开始进行预案决策
状态通知 8:00:00
各位值班同学辛苦了，当前地图出行服务正常，各服务指标如下：
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
流量 当前 日级增长 周级增长 服务正常
状态通知 :00:00
各位值班同学辛苦了，当前地图出行服务正常，各服务指标如下：
流量 当前 日级增长 周级增长 服务正常
相关操作以及信息
VI机器人
止损通知 开启 关闭
定位通知 开启 关闭
状态通知 开启 关闭
活动通知 开启 关闭
作战部
智能机器人（@vi）
快捷链接
能监控
预案平台
服务可用性
外网监控

Thanks Very Much

&

Welcome Questions!