

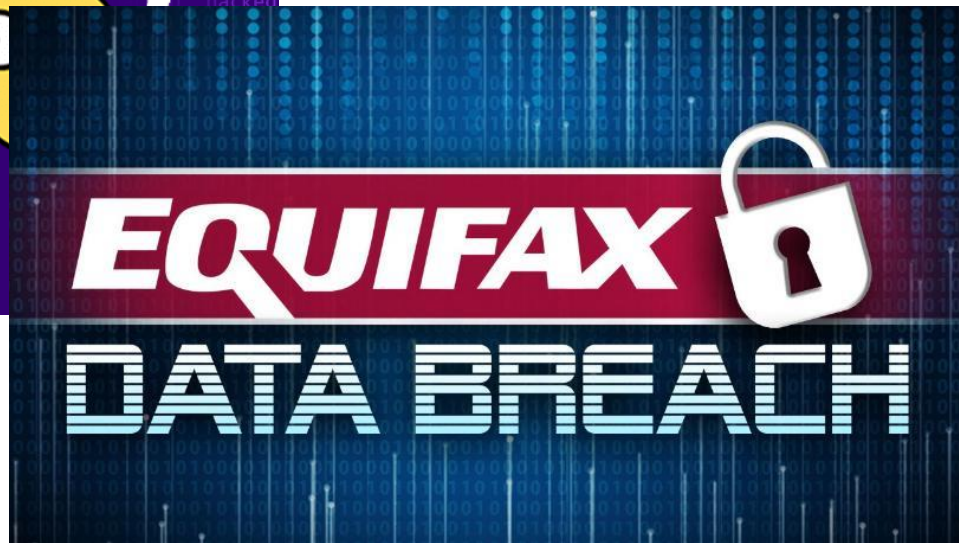
# 唯品会攻击检测实践

2018年11月17日

# 攻击检测



# 攻击检测



# 传统攻击检测



# 传统攻击检测

## 优点

- 简单直接
- 易于并行

## 缺点

- 已知攻击模式
- 正则匹配复杂度
- 资源消耗

更大的平台

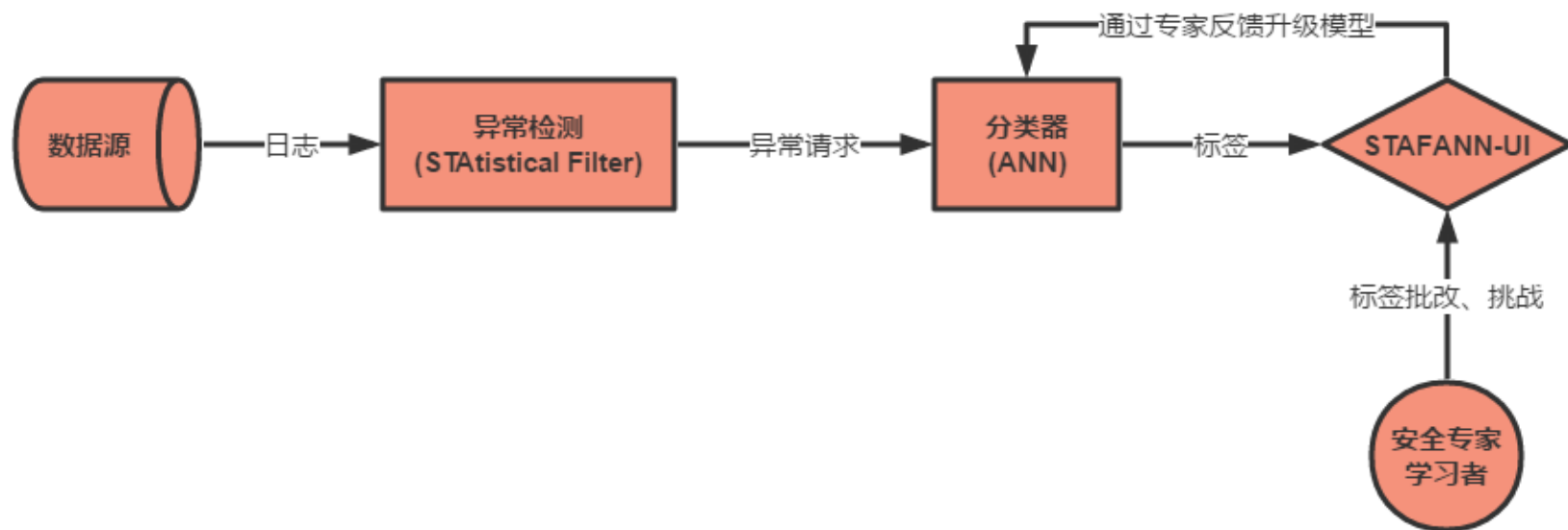
更大的流量

更多的资源

# 传统攻击检测



# 新场景 新方案



# 异常检测

正常流量 >> 攻击流量

攻击模式：只有你想不到

业务场景固定



# 异常检测

关注攻击模式



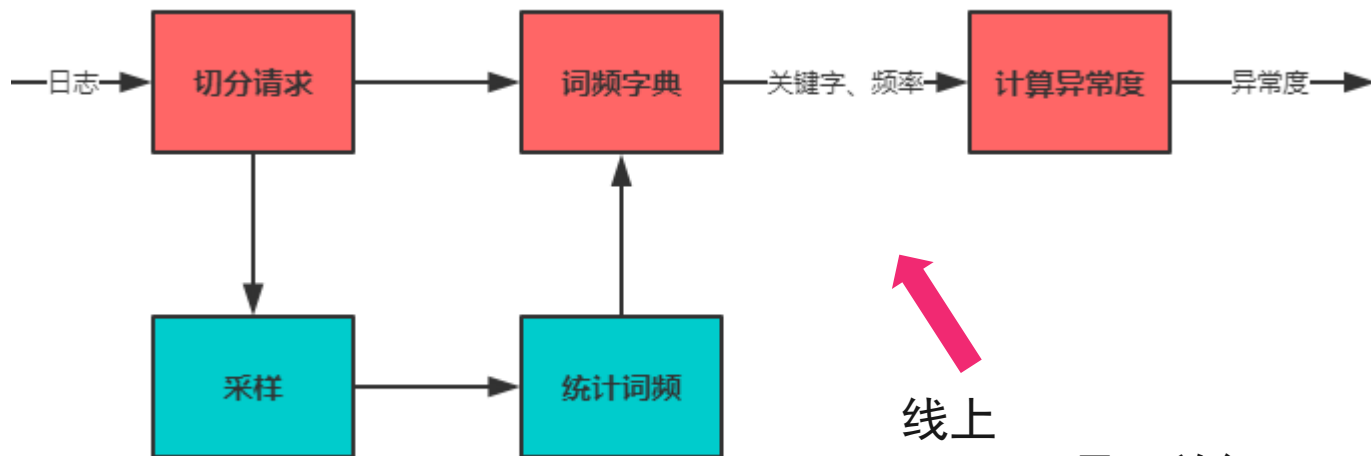
关注正常模式

攻击模式匹配



异常检测

# 异常检测



线下

- 统计正常流量模式
- 模型更新周期长

线上

- 易于并行
- 线性时间计算复杂度
- 流量：千分之一以下
- 定量化

# 异常检测



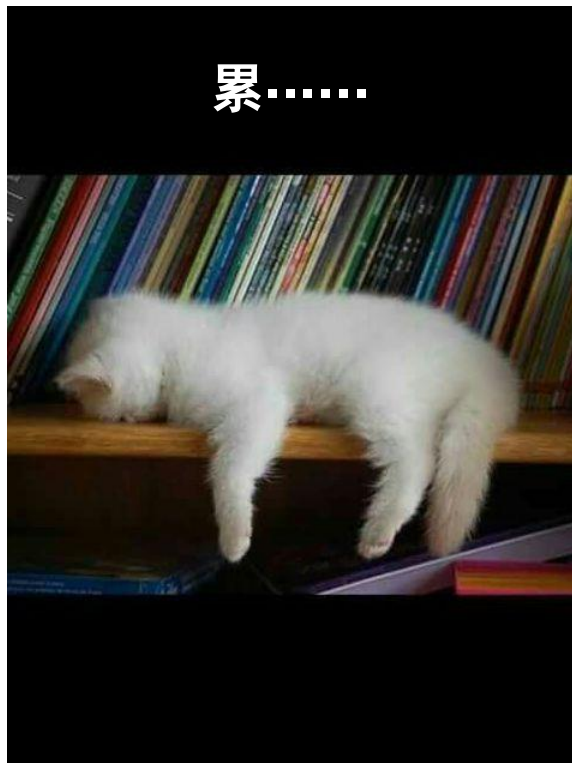
# 分类器：正则匹配



## 分类器：正则匹配



## 分类器：正则匹配



累.....

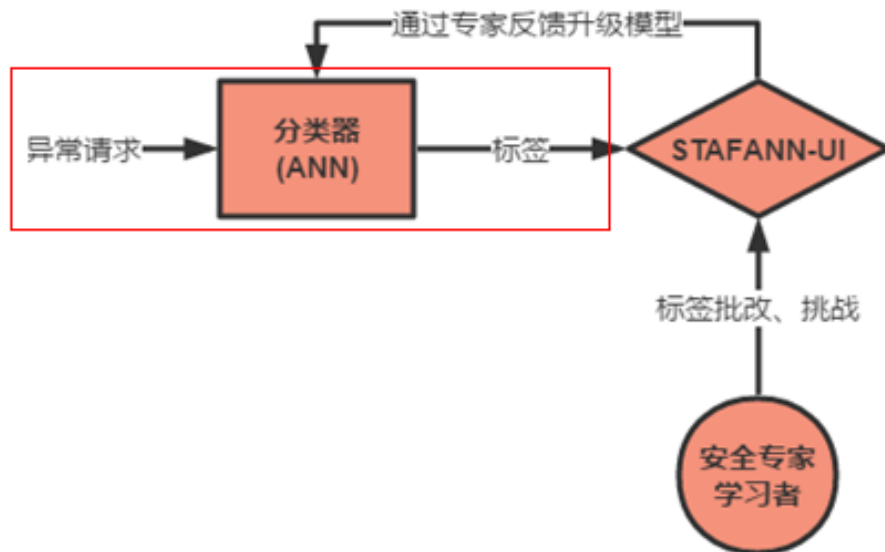
# 分类器：机器学习

RNN

影评情感 → 请求标签

标签数据？

专家经验？



# 分类器：机器学习

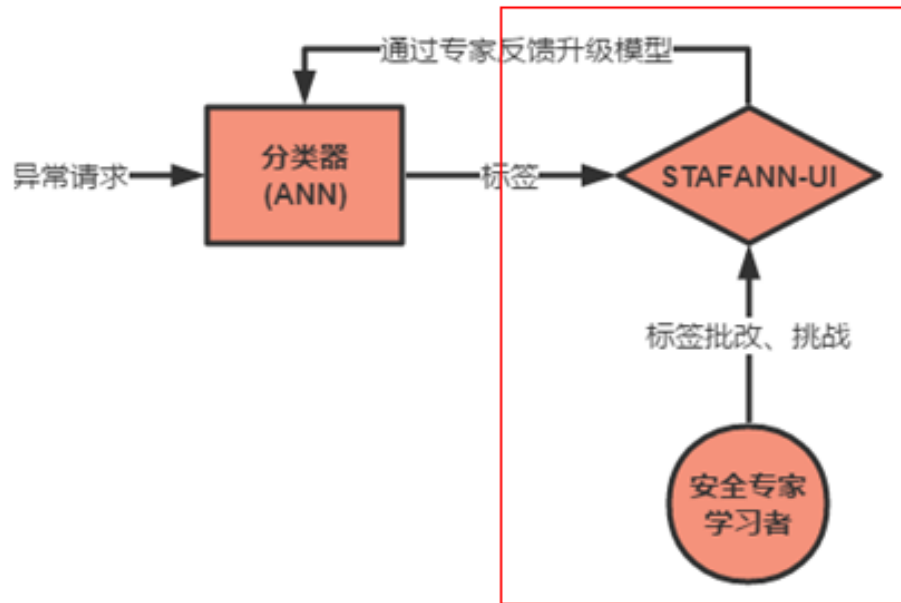
标签

- 貌似正常
- SQL 注入
- XSS
- .....

专家标签 > 1000:

覆盖率提升显著

准确率 > 99%





# 分类器

## 优点

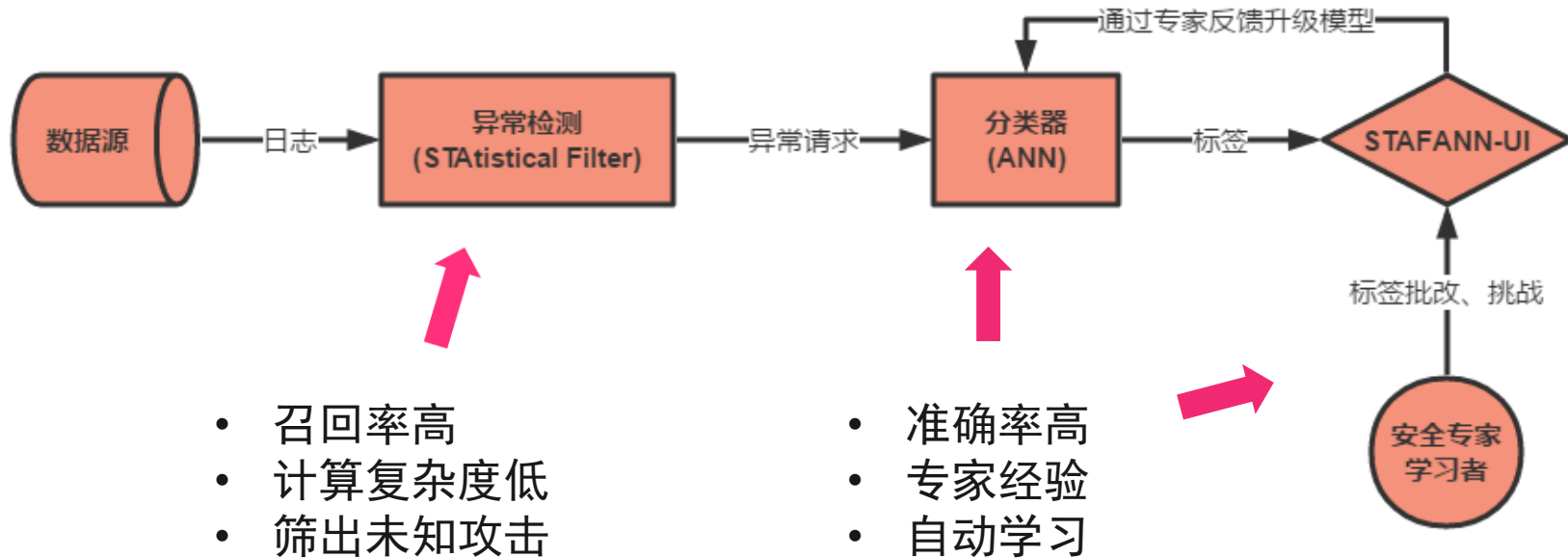
- 准确率
- 专家经验
- 模式发掘

## 缺点

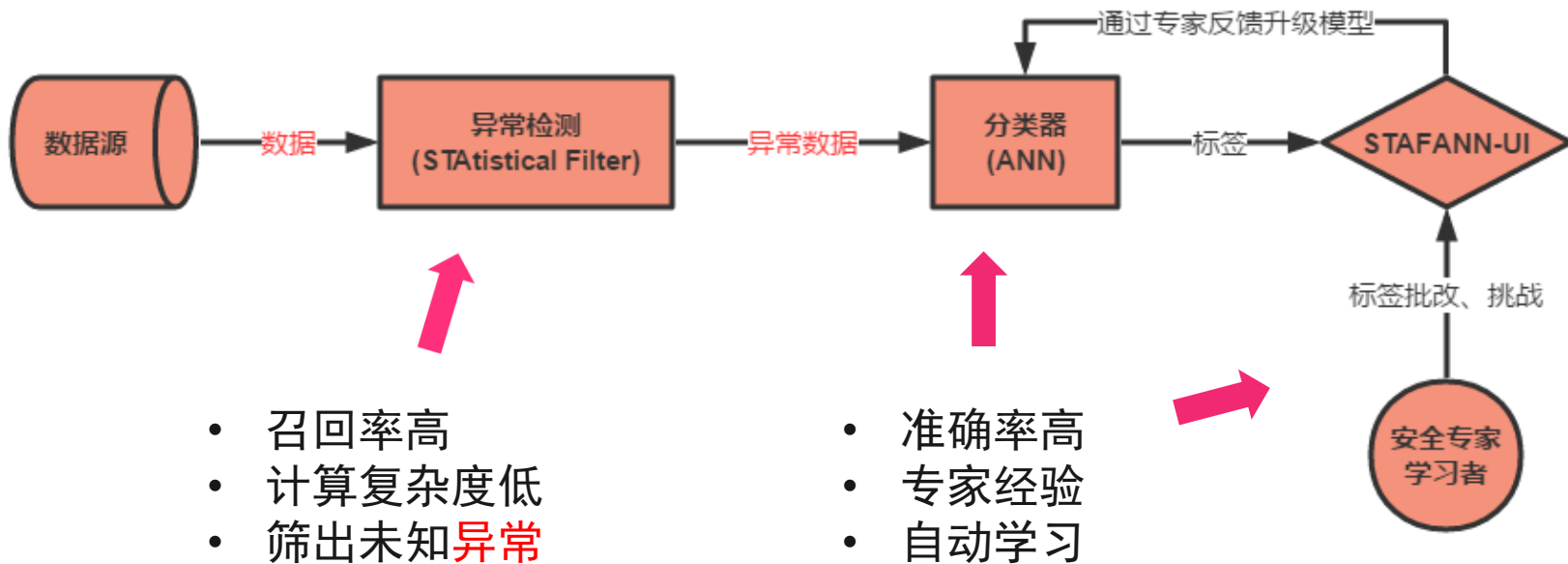
- 计算复杂度



# STAFANN = STAF + ANN



# 不仅仅是攻击检测



# 业务安全



异常告警



分析



采取措施



反馈

感谢聆听

—

THANKS!