EISS-2018企业信息安全峰会之上海站

"Face the challenge,Embrace the best practice"

November 30th,2018|SHANGHAI

2018年11月30日|上海

唯品会攻击检测实践

安全加

攻击检测


ALERT
Intrusion Detected
0101101010010110101001
1010010101111001010111

攻击检测

传统攻击检测

传统攻击检测

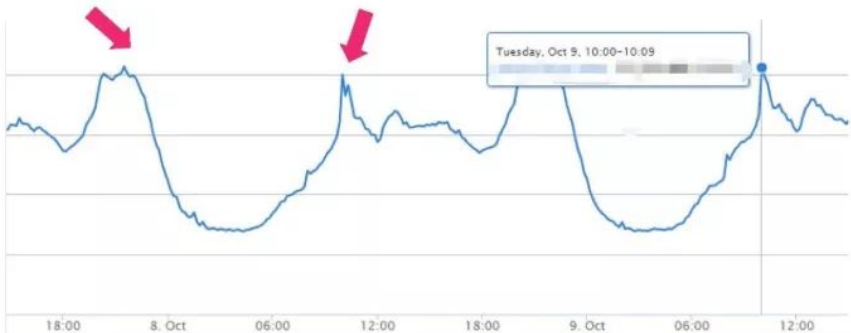
优点

- 简单直接
- 易于并行

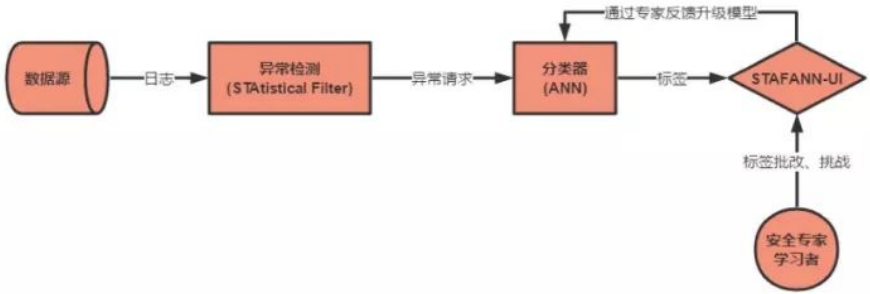
缺点

- 已知攻击模式
- 正则匹配复杂度
- 资源消耗!

传统攻击检测


Tuesday, Oct 9, 10:00–10:09
18:00
8. Oct
06:00
12:00
18:00
9. Oct
06:00
12:00

新场景 新方案


通过专家反馈升级模型
数据源
日志
异常检测
(STAtistical Filter)
异常请求
分类器
(ANN)
标签
STAFANN-UI
标签批改、挑战
安全专家
学习者

异常检测

正常流量 >> 攻击流量

攻击模式：只有你想不到

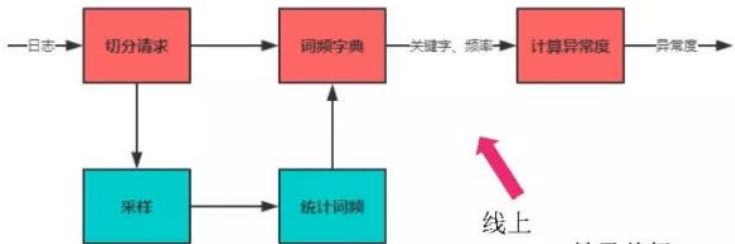
业务场景固定

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

线下

- 统计正常流量模式
- 模型更新周期长

异常检测

分类器：正则匹配

sele

sele

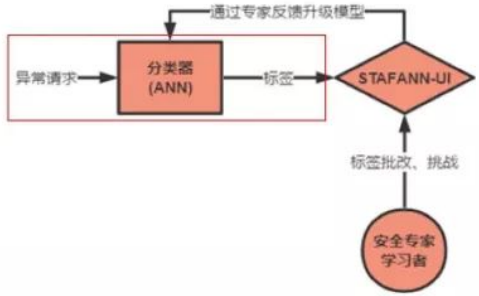
分类器：正则匹配

分类器：正则匹配

分类器：机器学习

RNN

影评情感 → 请求标签



FAQ

- 标签数据？
- 专家经验？

分类器：机器学习

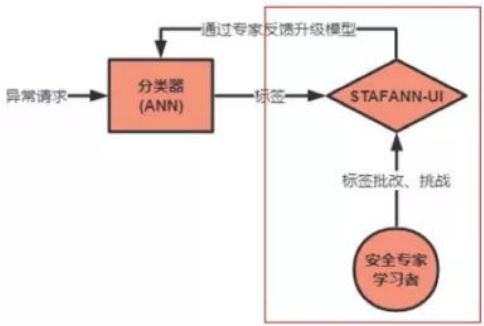
标签

- 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：机器学习

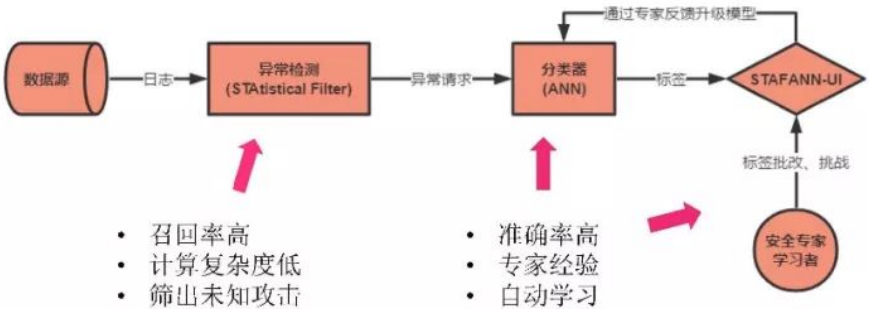
优点

- 准确率
- 专家经验
- 模式发掘

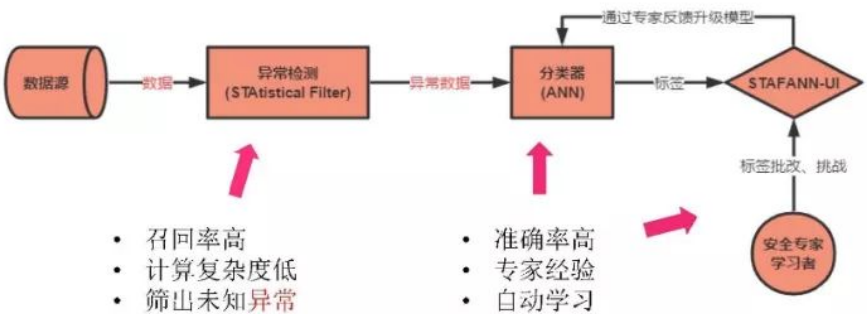
缺点

- 计算复杂度

STAFANN = STAF + ANN



STAFANN = STAF + ANN



业务安全

异常告警 ➡ 分析 ➡ 采取措施 ➡ 反馈

感谢聆听

THANKS!