

# 学霸君安全建设之路

演讲者：atiger77



学 | 霸 | 君  
MASTER LEARNER

# 目录

1

情况介绍

2

运维安全

3

业务安全

4

应用安全

5

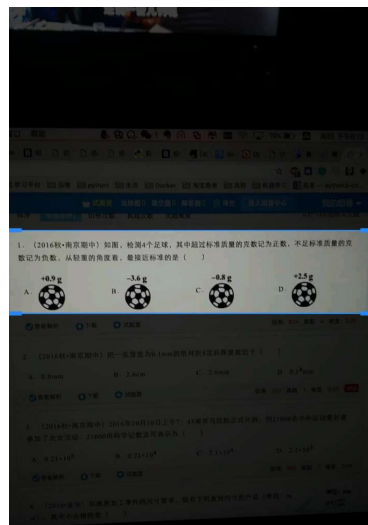
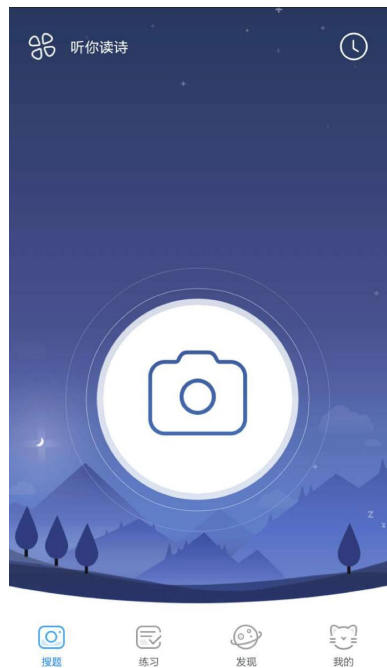
内部安全

6

总结

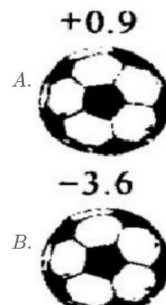
# 情况介绍

- 学霸君是一款拍照搜题、智能刷题、作业辅导考试通关的学习神器，金牌名师实在在线视频解答。



□ 题目

如图，检测4个足球，其中超过标准质量的克数记为正数，不足标准质量的克数记为负数，从轻重的角度看，最接近标准的是( )



再拍一题

老师答疑



◀ 解析

解决这道题目，求出每个数的绝对值，根据绝对值的大小找出绝对值最小的数即能得出答案。

◇ 答案

解：

$\because |+0.9|=0.9$ ,  $|-3.6|=3.6$ ,  $|-0.8|=0.8$ ,  $|+2.5|=2.5$ ,  $0.8 < 0.9 < 2.5 < 3.6$ ,  
 $\therefore$  从轻重的角度看，最接近标准的是-0.8.

故选C.

故答案为：c

再拍一题

老师答疑



学 霸 君

## 情况介绍

出现过的一些安全事件：

竞品攻击  
DDOS  
钓鱼邮件  
薅羊毛  
扫号  
安全漏洞  
webshell  
撞库  
垃圾注册

# 目录

1

情况介绍

2

运维安全

3

业务安全

4

应用安全

5

内部安全

6

总结

# 运维安全

## 安全基线

- SSH禁止ROOT登录
- 修改SSH默认端口
- 禁止密码登录系统
- 新建普通用户
- 设置别名把“rm -rf , mkfs”等危险命令进行替换
- 安全监控（敏感文件md5比对）
- 数据库权限控制
- ...



# 运维安全

## 漏洞处理流程

每一次爆出的高危漏洞都是对安全人员的一次考验，晚一步就可能被攻击者捷足先登。



# 运维安全

## 服务部署情况

显示 10 导出Excel 取消选择 搜索: nginx

选择	ID	主机名	IP	可用区	备注	维护人	部门	二级部门	项目	应用	服务	描述	更新日期
							平台开发				nginx/php		2016-12-29 09:52:21

风控平台

Welcome, 刘德华

风控数据

- 学籍数据
- 学籍辅导
- 安全相关
- ☒ 资源信息
- 外网IP统计
- 用户管理

Show 10 entries Search:

EIP标签	所属人	IP地址	创建时间	备注
ylw_001	ylw	192.168.1.1	2015-04-22 10:51:48	None
ylw_002	xlw	192.168.1.2	2016-03-19 10:20:26	None
ylw_003	xlw	192.168.1.3	2016-03-31 13:17:27	None
ylw_004	xlw	192.168.1.4	2015-11-16 11:26:54	None
ylw_005	xlw	192.168.1.5	2015-08-19 11:16:47	None
ylw_006	xlw	192.168.1.6	2015-03-11 10:05:53	None
ylw_007	zhw	192.168.1.7	2015-11-20 10:31:41	None
ylw_008	zhw	192.168.1.8	2015-07-20 09:53:24	None
ylw_009	hwy	192.168.1.9	2015-07-10 14:27:25	None
ylw_010	qinfeng	192.168.1.10	2015-11-22 14:44:48	None

Showing 1 to 10 of 95 entries

Previous 1 2 3 4 5 ... 10 Next



# 目录

1

情况介绍

2

运维安全

3

业务安全

4

应用安全

5

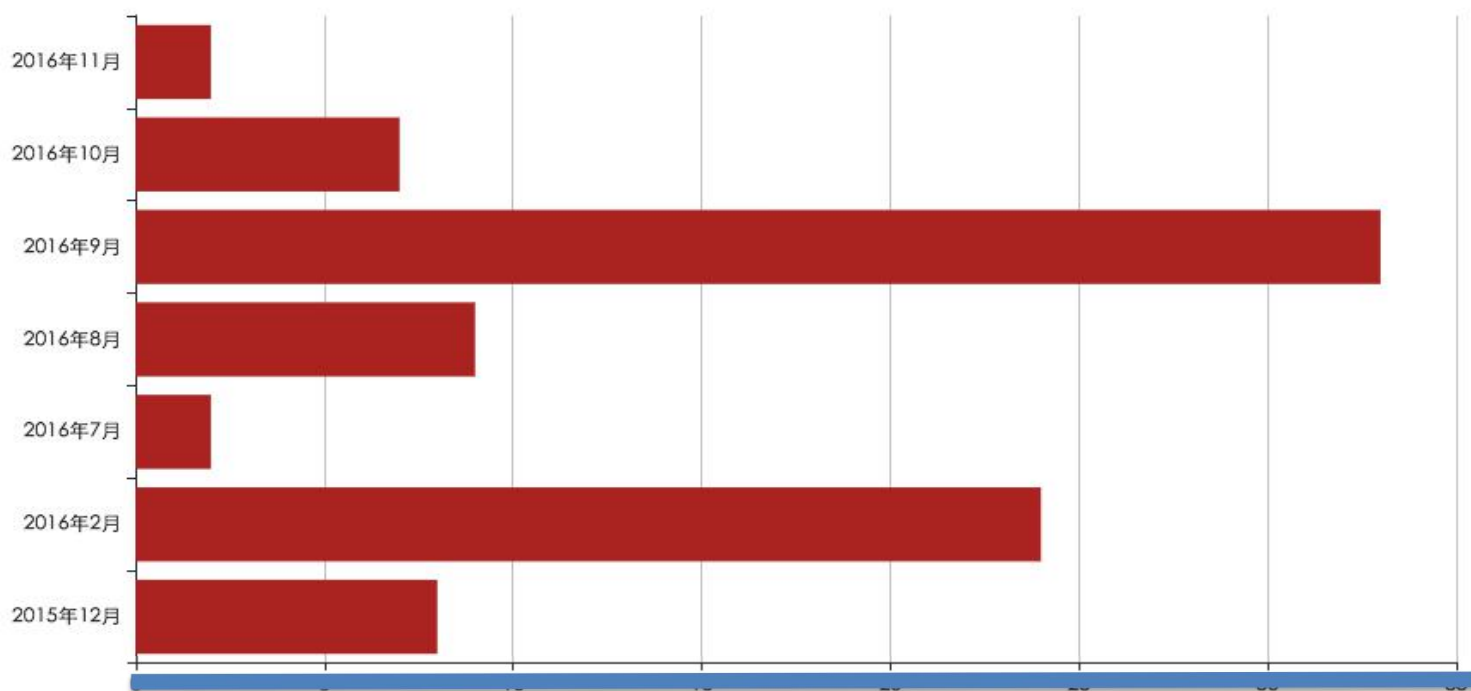
内部安全

6

总结

## 流量攻击

根据一年整体情况发现每到年前年后，熊孩子开学，运营活动都是高发期。



# APP安全

加固内容：

网络层：全站使用HTTPS协议，pinning强制校验证书；

移动端：代码混淆，公共接口人工混淆；

so加固，增加攻击成本；

第三方渗透测试，提高安全；



# APP安全

App安全加固的痛点：

1. 不能强制升级；如果某版本有安全问题，只能发布修复后的新版本，一点点迭代旧版本，同时要对问题版本做控制，降低功能使用频次等。

2. 端的防御永远是相对的；apk在大家都可以分析，能做的就是不断的加固恶心想要破解分析的人，增加一个破解时间。

#如果公司负责安全的同学比较少,可以看下这点

3. 关注发版动态；可以加到发版的讨论群中，特别关注下新上线的活动页面；

# 风控

发现的问题:

1. 刷单; 2. 恶意注册; 3. 竞品拍题; 4. ...



学霸君

优惠多多哦

¥2.26 包邮 347人付款

学霸君, 学霸君账号总课时30分钟2张15分钟的答疑卡券, 自动发货

上百无一用是深情

广东 广州



霸

¥1.70 包邮 347人付款

学霸君, 学霸君账号含2张15分钟答疑卡券总课时30分钟, 自动发货

zhajie2005

江苏 泰州



¥55.00 包邮 175人付款

学霸君答疑师专用数码本、笔芯优惠组合包邮套餐【内含5本+5芯】

学霸君app

天津



学霸君

优惠多多哦

¥2.00 包邮 78人付款

自动秒发学霸君账号答疑30分钟总课时30分钟2张15分钟的答疑卡券

诚信商家店铺0

北京

# 风控

做风控必须有数据的支持，没有数据就没有风控。

收集后端行为日志，进行日志分析。

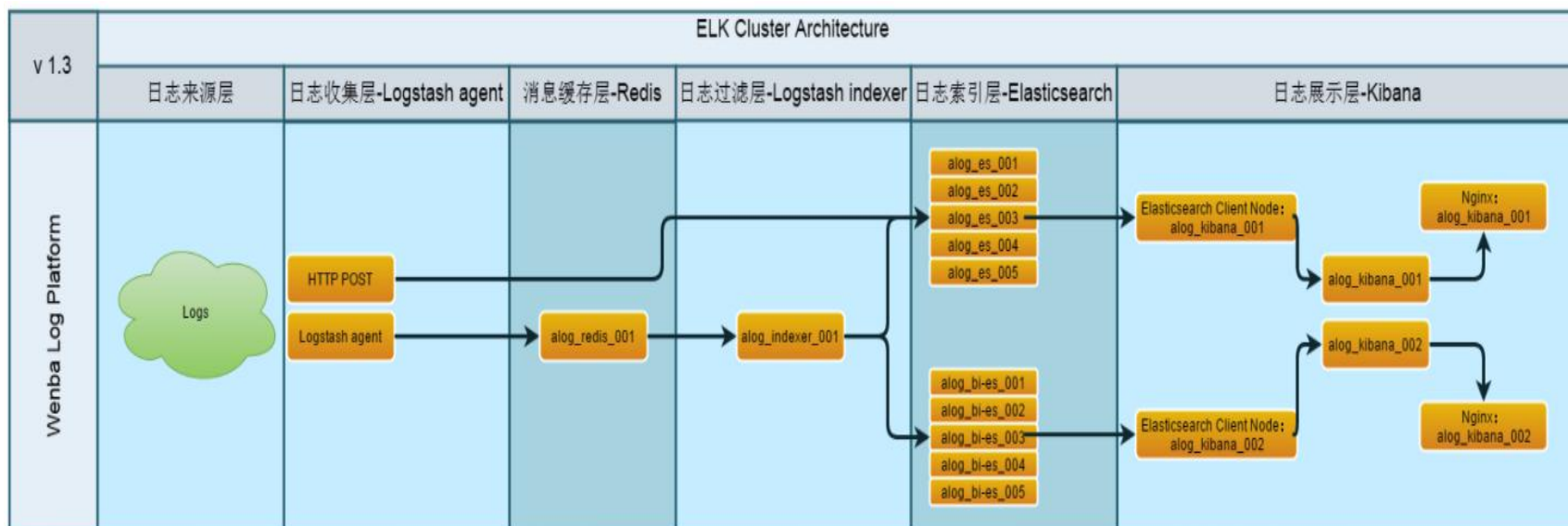
参数：

时间,UID,手机号,deviceid,useragent,version,用户行为,手机号所属地,ip所在地等等信息



# 风控

## 整体架构。



# 风控

有了数据就要制定规则，我们拿用户模块举例

根据不同行为进行调整

注册行为\_单IP下注册数，注册行为\_单IP下UID数量，找回密码行为\_  
uid对应多IP，找回密码行为\_ uid对应多devicedid,等等。





# 风控

对触发规则的用户打上用户标签，根据触发行为级别进行处理

## 用户基本资料

uid	[REDACTED]	birthdate	946656000	channel	AppStore
city	南京	classid	0	grade	0
logdate	2016-12-29	nickname		phone_channel	中国联通
phoneno	[REDACTED]	platform	1	province	江苏
qq		schoolid	0	sex	10

## 用户标签



恶意DeviceID\_拍题行为 (Sys)

恶意IP\_拍题行为 (Sys)

恶意UID\_注册行为 (Sys)



学 霸 君

MASTER LEARNER

# 风控

碰到的一些问题&&处理方法

## 1.Kibana面板图像超时

大量的聚合操作会占用比较大的内存资源，有几种解决方法可以参考下，a.减少单一面板图像数量,拆分成多个面板 b.直接调ES接口获取数据 c.增加服务器内存或者增加服务器...

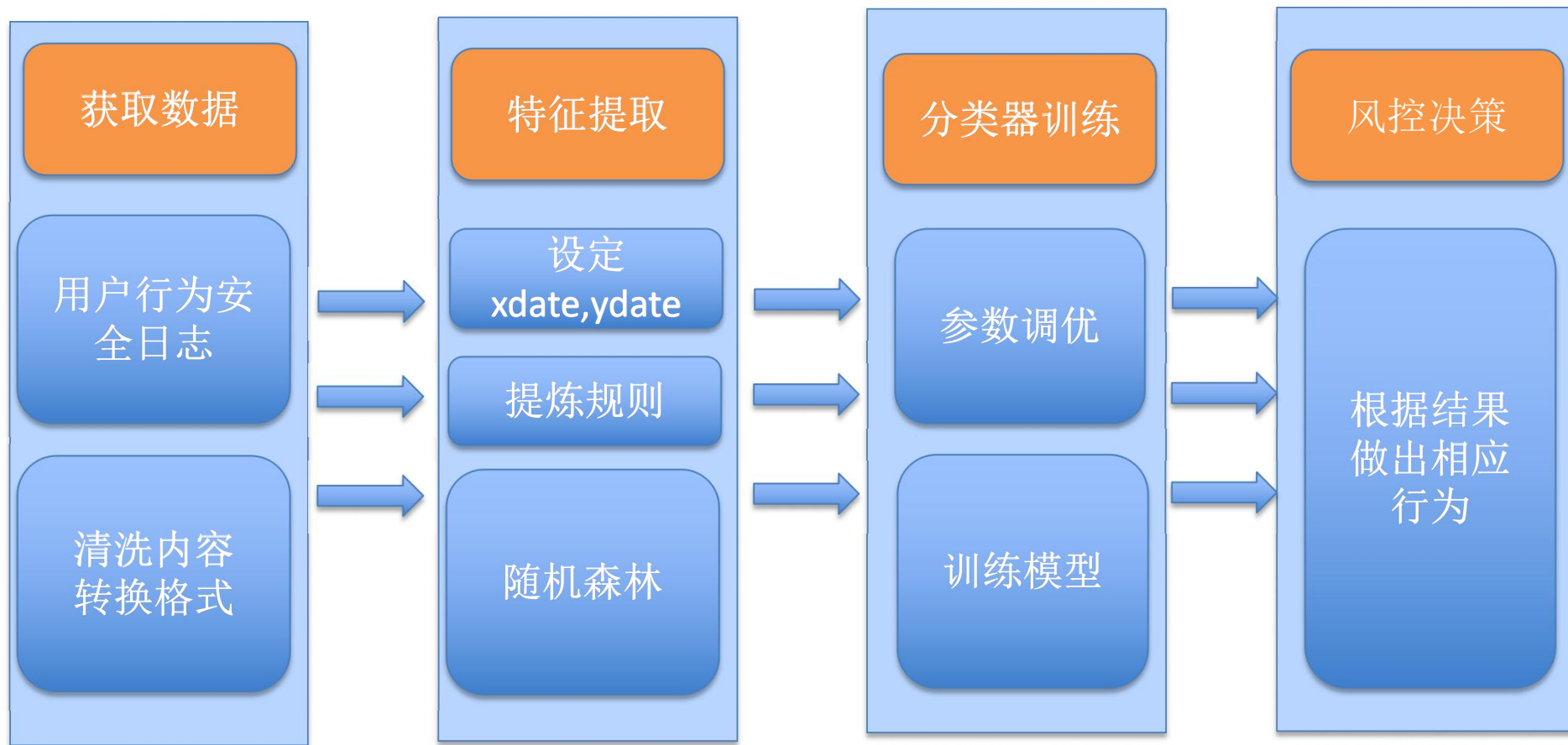
## 2. 异常点不明显

刚接入的安全日志后第一眼很难发现明显的异常，之后细化规则内容，反溯异常行为,用户并分析，找到异常原因解决异常。



# 风控

## 安全风险使用到的机器学习



# 风控

应用场景：使用随机森林判断用户行为是否异常

第一个模型 “德华一号”

```
rf = RandomForestClassifier(n_estimators=500)
```

```
rf.fit(xdata,ydata)
```

```
joblib.dump(rf,'DeHuaYIHao.pkl')
```

```
[nono@develop-security 02 Anti_Register_Model]$ du -sh DeHuaYIHao.pkl  
55M    DeHuaYIHao.pkl
```



# 风控

## 机器学习

可以看到模型跑出的分数很高，我的样本是根据规则判断的，所以最好的情况结果就是逼近规则，需要一直对模型进行迭代去提炼更多的规则，继续调优参数，让模型判断不单单限于几个限定的样本规则。

```
[root@devops ~]# python Anti_Register_Model.py  
f1_score:0.839284124299  
acc_score:0.985538365395
```



# 目录

1

情况介绍

2

运维安全

3

业务安全

4

应用安全

5

内部安全

6

总结

# 应用安全

## • 内部：

### 安全扫描

每周定期扫描(avws,nessus)关键业务，特别关注快速迭代的一些业务线，往往都是这些项目会出安全隐患；

### 安全培训

- a. 新同学入职培训；（每月一次）
- b. 全体技术人员安全分享；（半年一次）
- c. 全体人员安全分享；（半年一次）

# 应用安全

## • 外部：

### 渗透测试

定期和第三方合作做渗透测试项目，对检测出的漏洞进行修复；

### 抗D

和第三方合作购买流量清洗来抵御流量攻击；

#反欺诈应该算在业务安全中，这里我归类到了一起

### 反欺诈

某安测试下来结果挺理想，是一个很好的判断纬度；





# 目录

1

情况介绍

2

运维安全

3

业务安全

4

应用安全

5

内部安全

6

总结

# ■ 内部安全

- 边界安全

1.所有公网访问的内容都要做二次认证；比如企业邮箱等。

定期查看哪些熊孩子没有绑定企业邮箱提醒其绑定；

2.办公网WIFI单独划出GUEST区域，对重要部门可采取绑定分配地址；



# 内部安全

- 人员安全

涉及人员	安全隐患	解决方法
全体同学	钓鱼邮件	安全讲座，内部安全测试；
开发同学	代码上传 Github	内部安全技术分享，安全检测， Github定向搜索；
开发同学	代码问题导致漏洞	
开发,运维同学	命令误操作	安全基线，设置别名；

# 内部安全

- 内部系统安全

内部平台

访问控制  
异常阻断

操作记录日志  
平台等级划分

蜜罐（蜜罐表，蜜罐系统）  
...

监控报警

数据分析

ELK  
Python代码  
...

安全策略

弱口令扫描  
定期安全测试  
...

帐号

密码策略  
存储方式  
...

# 目录

1

情况介绍

2

运维安全

3

业务安全

4

应用安全

5

内部安全

6

总结



学 霸 君

MASTER LEARNER

# 总结

- 如果你也像我一样公司只有一个人做安全，希望我的总结的经验能帮到你。
  1. **没有老板支持一切都是吹牛逼**；从上往下推和从下往上推是两个概念；
  2. 先做最紧急的需求，全部解决以后再考虑可视化；东西丑不重要 关键是管用，东西再好看解决不了问题也是白搭；
  3. 必要时可考虑商业化产品/合作，如堡垒机，渗透测试等；



## 总结

4. 统计公司相关资源如外网IP,机器部署服务，别到了漏洞爆发在去问开发你的机器有没有部署XX服务；
5. 做好外部控制别忘记做内控，有时候内部安全事件比外面攻击更可怕；
6. 多和公司老司机聊聊天，你碰到的一些坑他们可能也遇到过，一些架构上的设计、冗余、优化方案都可以多找他们讨论下；



## 总结

这次分享的内容我写了很多的干货，把自己安全建设的过程从零到一的都简单说了下，对ppt内容有问题的同学可以加我微信一起交流，请备注来源，感谢。





The background is a solid blue color with various white geometric shapes scattered across it. These shapes include circles, squares, triangles, diamonds, and lines. Some shapes are solid, while others are outlines. The shapes are distributed throughout the slide, creating a modern and abstract design.

# THANKS & QA