学霸君安全建设之路

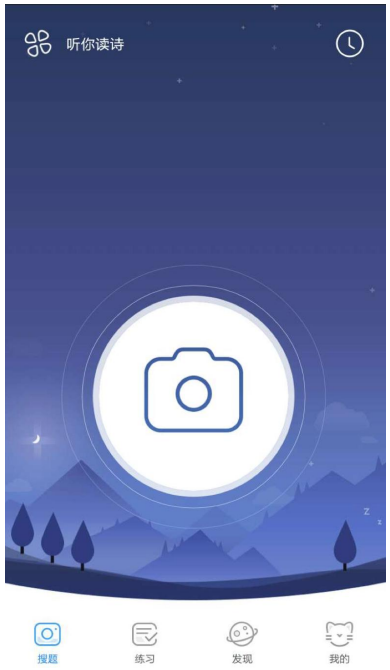
演讲者：atiger77

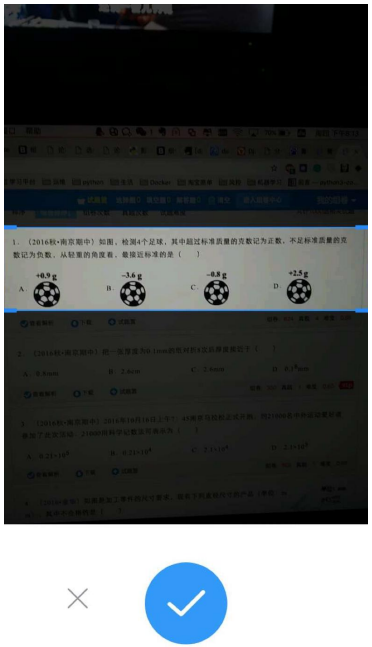
学霸君
MASTER LEARNER

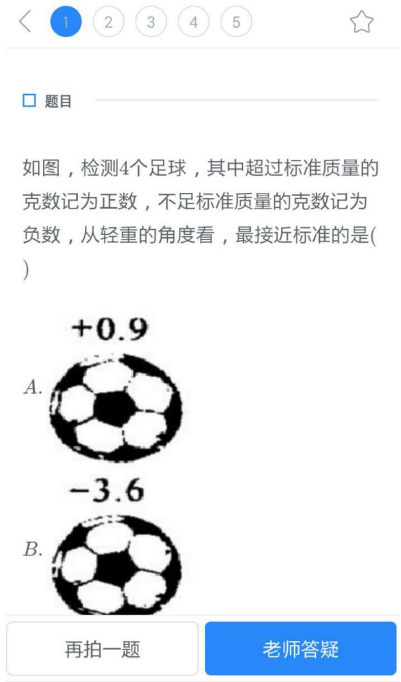
目录

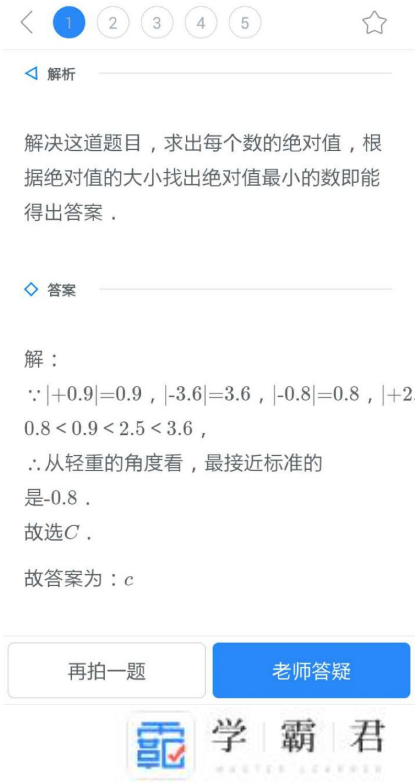
情况介绍

- 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。









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

垃圾注册

撞库

目录

运维安全

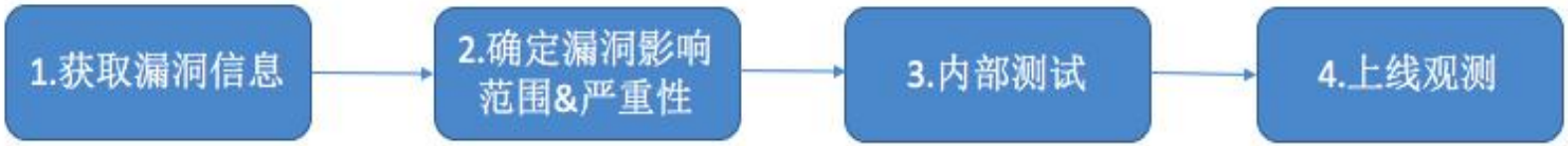
安全基线

- 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。

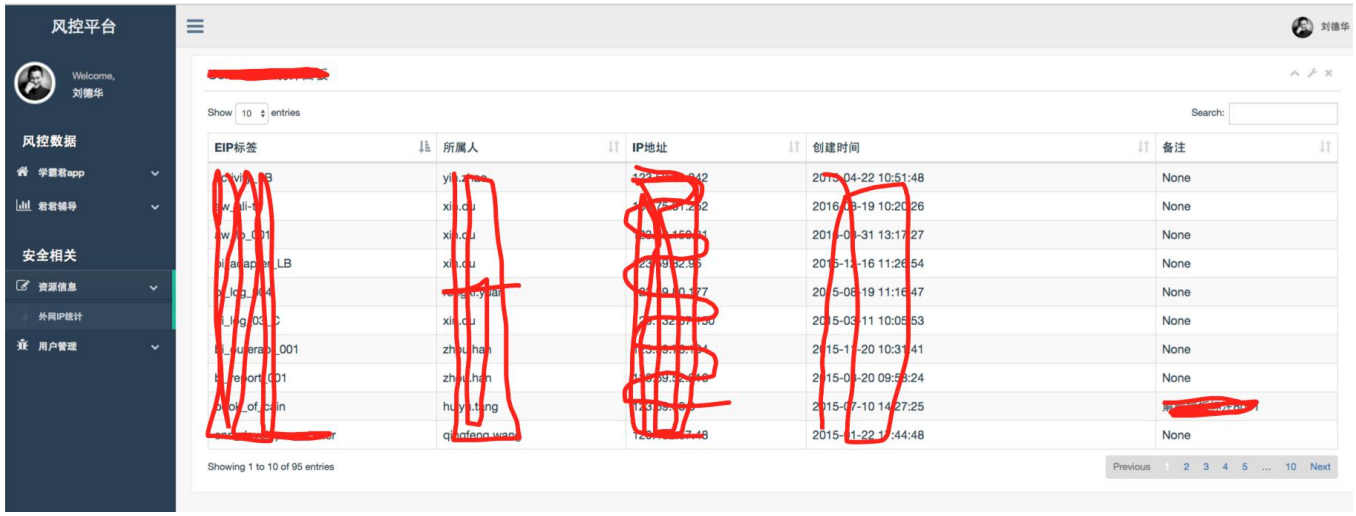


运维安全

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



学霸君

目录

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

风控

做风控必须有数据的支持，没有数据就没有风控。

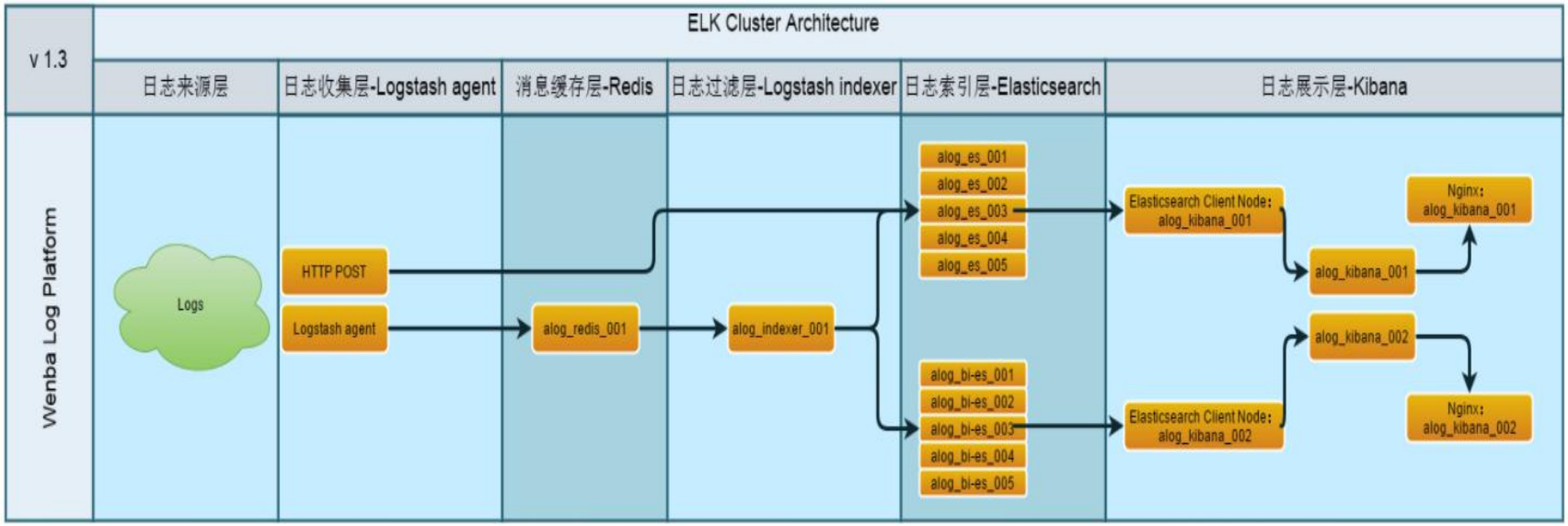
收集后端行为日志，进行日志分析。

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。


v 1.3
ELK Cluster Architecture
日志来源层
日志收集层-Logstash agent
消息缓存层-Redis
日志过滤层-Logstash indexer
日志索引层-Elasticsearch
日志展示层-Kibana
Wenba Log Platform
Logs
HTTP POST
Logstash agent
alog_redis_001
alog_indexer_001
alog_es_001
alog_es_002
alog_es_003
alog_es_004
alog_es_005
alog_bi-es_001
alog_bi-es_002
alog_bi-es_003
alog_bi-es_004
alog_bi-es_005
Elasticsearch Client Node:
alog_kibana_001
Elasticsearch Client Node:
alog_kibana_002
alog_kibana_001
alog_kibana_002
Nginx:
alog_kibana_001
Nginx:
alog_kibana_002

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

风控

碰到的一些问题&&处理方法

1.Kibana面板图像超时

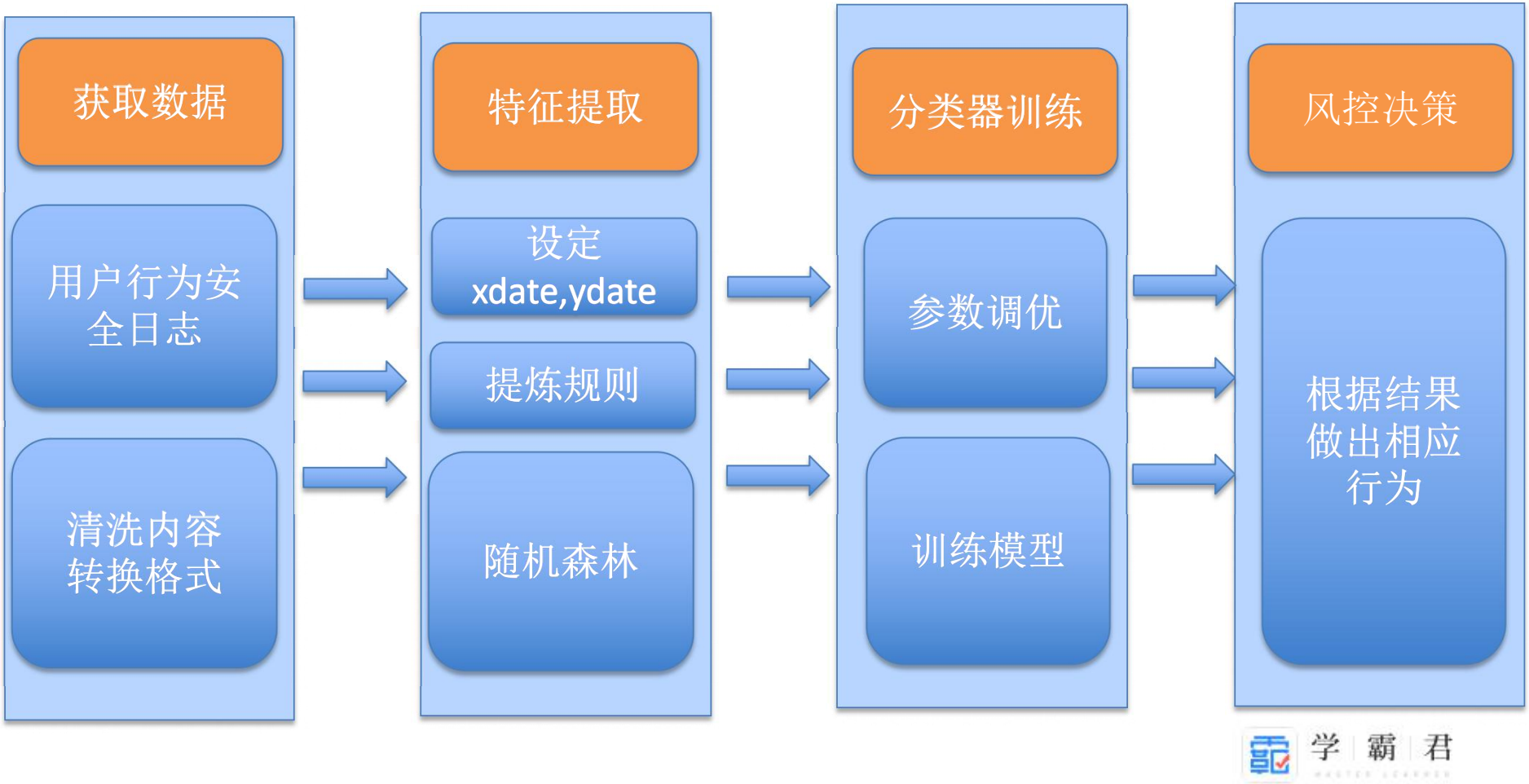
大量的聚合操作会占用比较大的内存资源，有几种解决方法可以参考下，a.减少单一面板图像数量,拆分成多个面板 b.直接调ES接口获取数据 c.增加服务器内存或者增加服务器...

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

安全风控使用到的机器学习

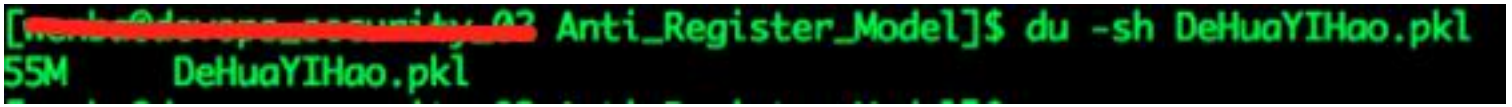


风控

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”

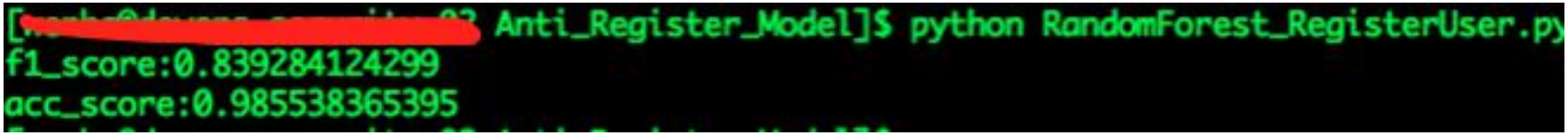
```
rf = RandomForestClassifier(n_estimators=500)
rf.fit(xdata,ydata)
joblib.dump(rf,'DeHuaYIHao.pkl')
```



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。



目录

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

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；

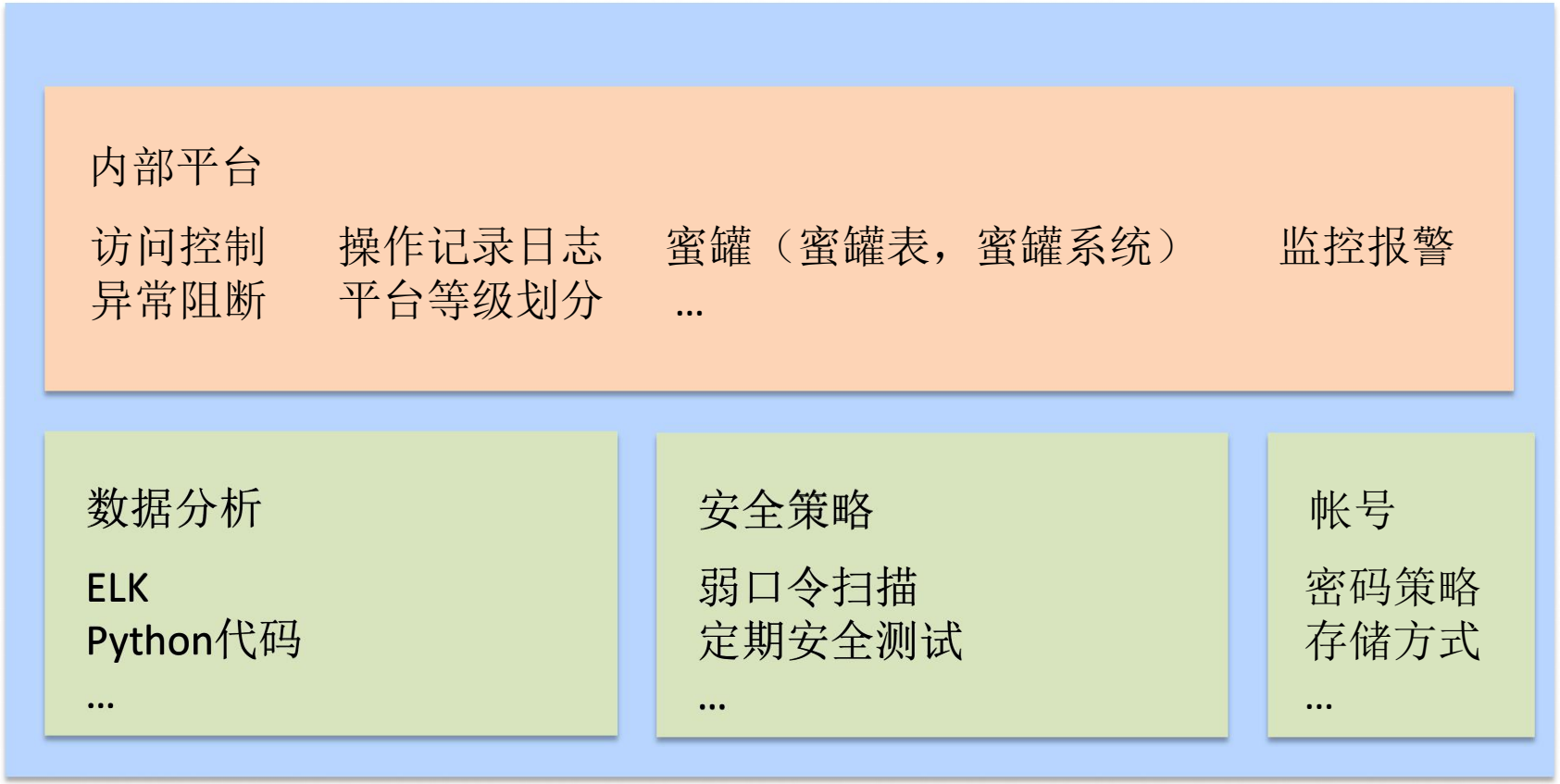
内部安全

- 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**



目录

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。

THANKS & QA