



**QCon** 全球软件开发大会  
INTERNATIONAL SOFTWARE  
DEVELOPMENT CONFERENCE

BEIJING 2017

# 甲方安全从0到1

SPEAKER / 吴文灏



促进软件开发领域知识与创新的传播



关注InfoQ官方信息  
及时获取QCon软件开发者  
大会演讲视频信息



扫码，获取限时优惠



全球架构师峰会 2017 [深圳站]

2017年7月7-8日 深圳·华侨城洲际酒店

咨询热线: 010-89880682



全球软件开发大会 [上海站]

2017年10月19-21日

咨询热线: 010-64738142

# About me

- 平名黑客
- 北冥鱼->知道创宇-> 
- Web安全工程师->安全研究员->安全产品研发->甲方安全
- bug@linux.com





# content

1. 攻防对抗

2. 安全体系建设

3. 业务安全与风控

4. 怎么汇报工作?

# 面临的挑战



大而老的系统

DedeCMS（漏洞之王）  
各个业务用着不同语言和框架



用户群体

技术宅，大学僧，小学生  
有着用不完的精力，熟悉接口。



高速增长

用户数每年翻一翻  
私有服务器、员工数翻一翻



从零起步

我入职时，运维2人加个CTO

# 攻防对抗



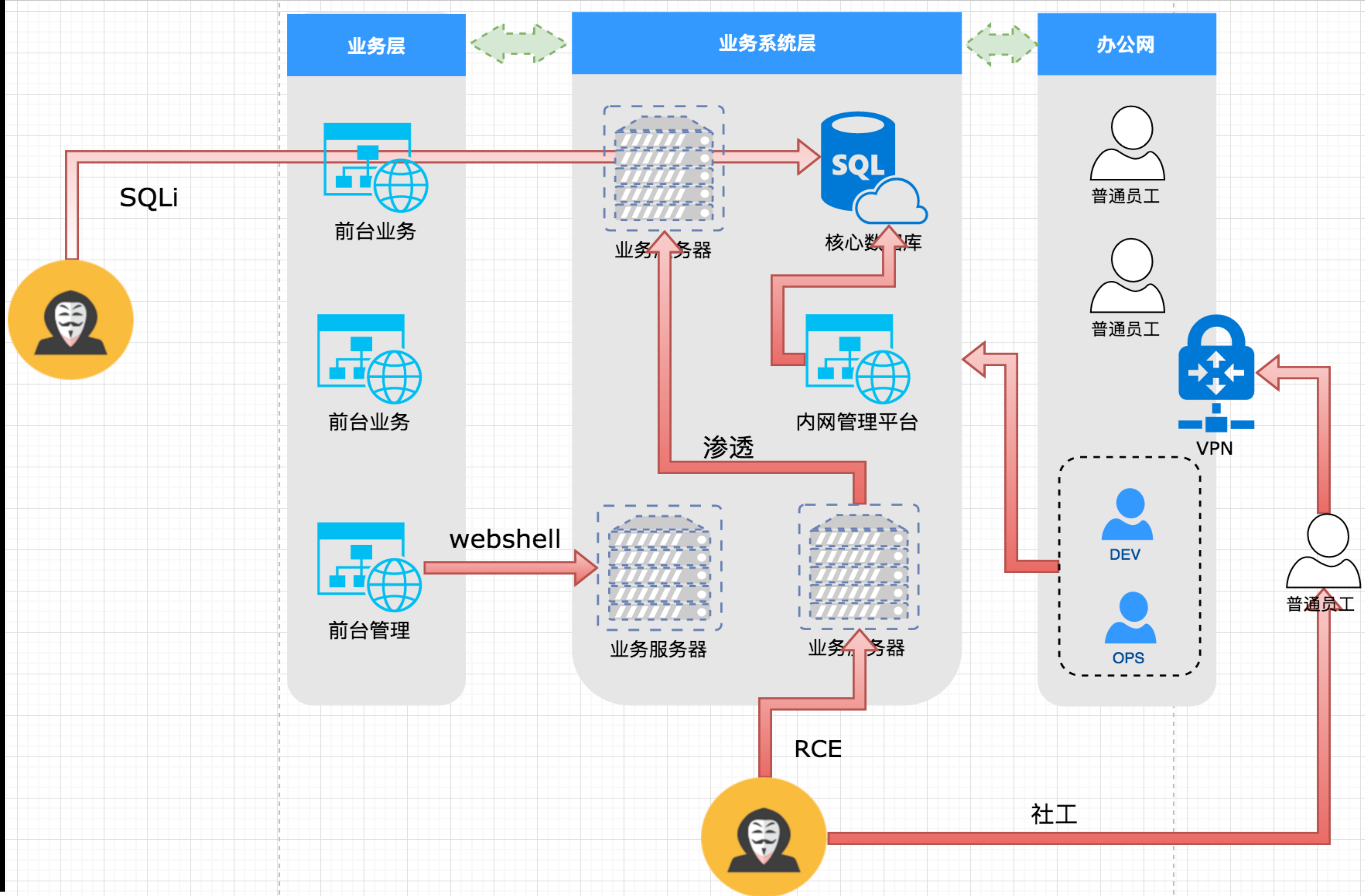
# 互联网安全残酷定律

1 / 以绝大多数开发对安全的认知还不轮不到拼技术

2 / 以绝大多数运维的惰性还轮不拼漏洞

3 / 以绝大多数公司对安全的重视程度还不至于拼努力

——长短短





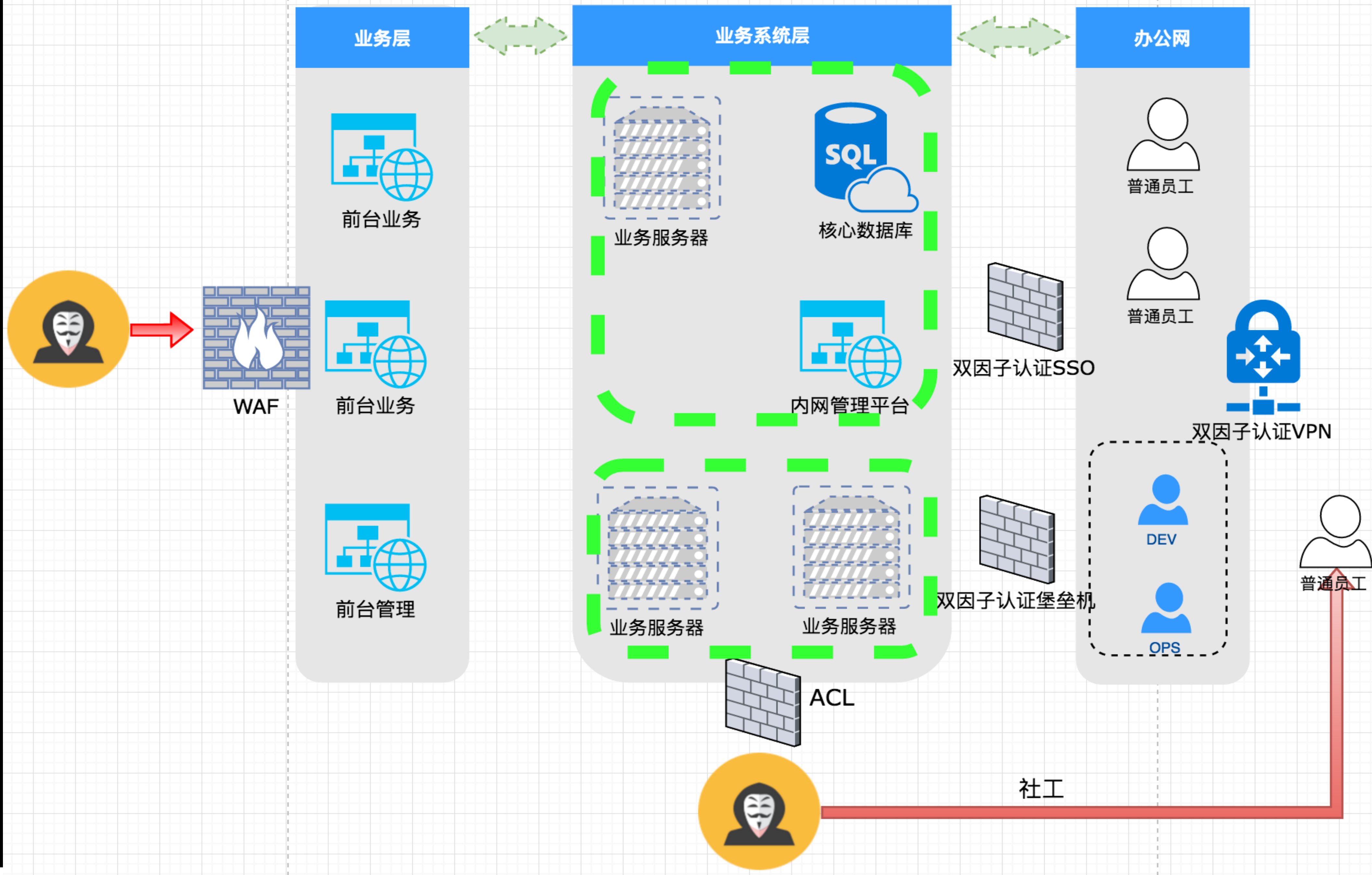


# 捻乱止于河防

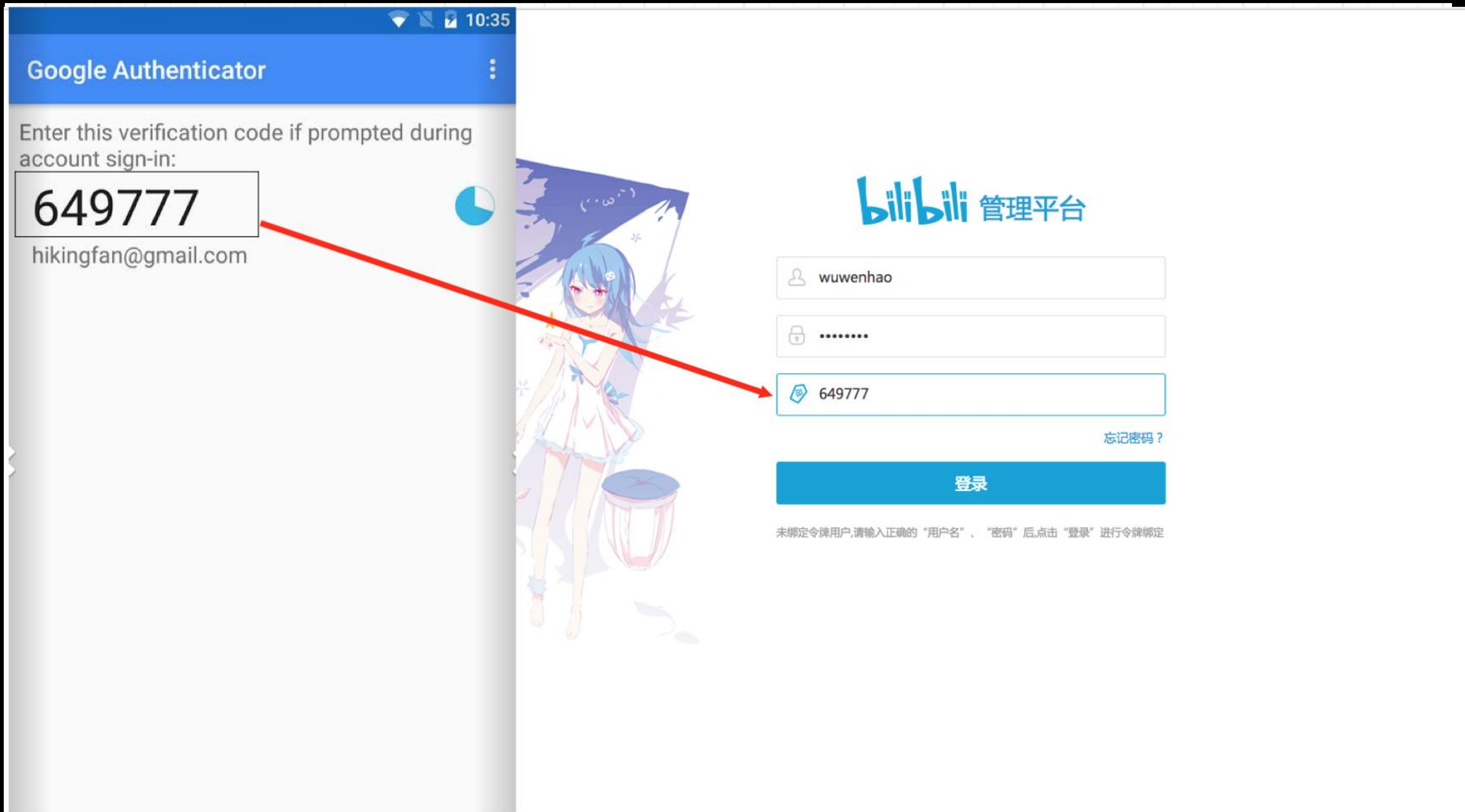
- 上WAF
- 端口管控, 后台管控
- 业务区域划分
- 堡垒机
- SSO+双因子认证

## 可控!

自己搞不定就买买买



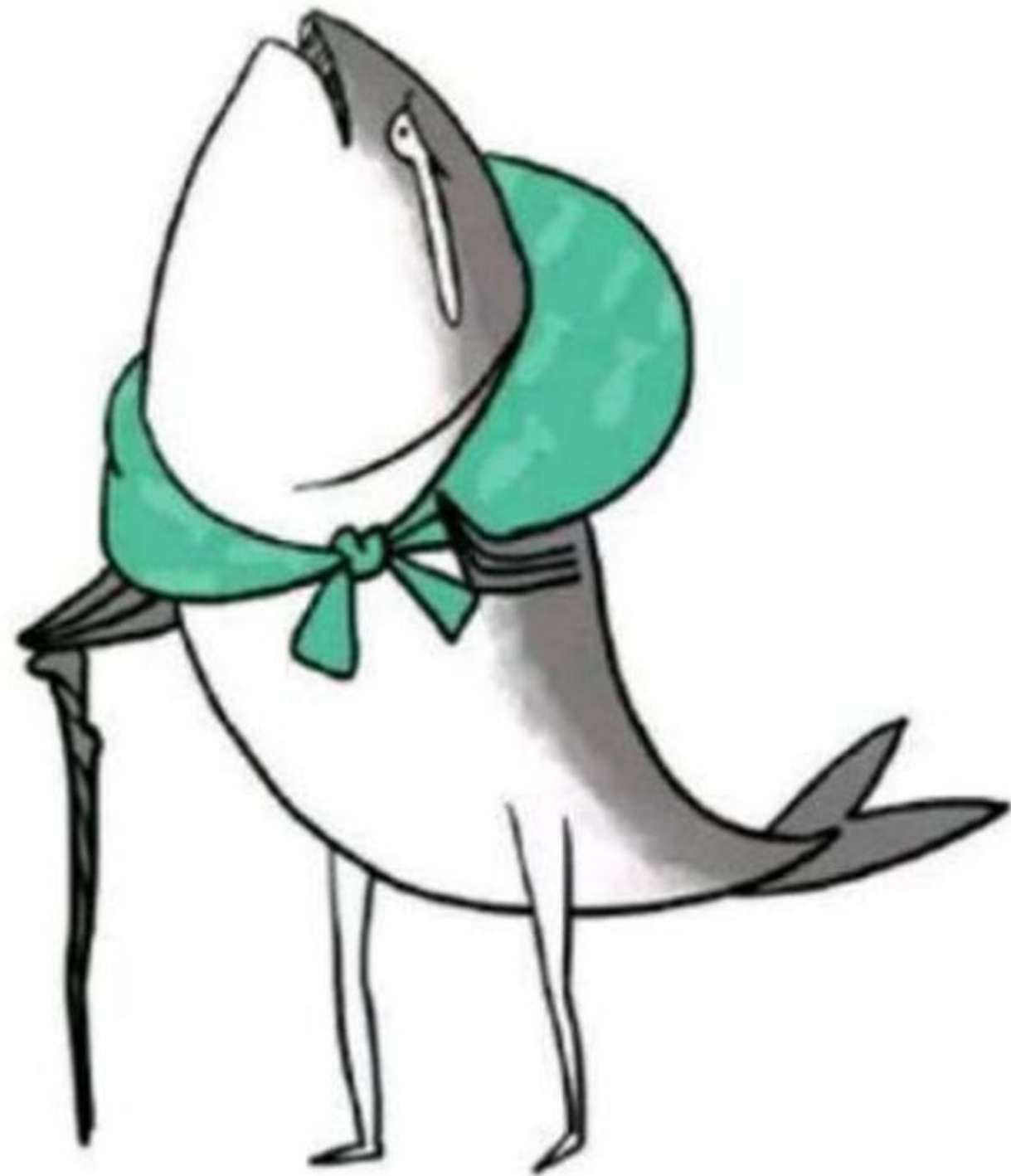
# 双因子认证实现方案





# 领导

- 不太了解和重视安全
- 帝王级需求
- 怎么实现我不管, 明天功能上线



这里没有我这条咸鱼的容身之处

# 安全

- 修业务漏洞代码的不是安全工程师
- 登服务器打补丁的执行者不是安全工程师
- 基础的东西没做好, 查问题麻烦

形成一个完整的闭环



# 安全体系建设



# 从零开始的大方向

1 / 不可能永远救火

2 / 建立监控能力

3 / 事后的应急处理

4 / 参（模）考（仿）大厂



# 从零开始的大方向



## 要做什么？

- 运维安全
- 应用安全
- 信息安全
- 业务安全



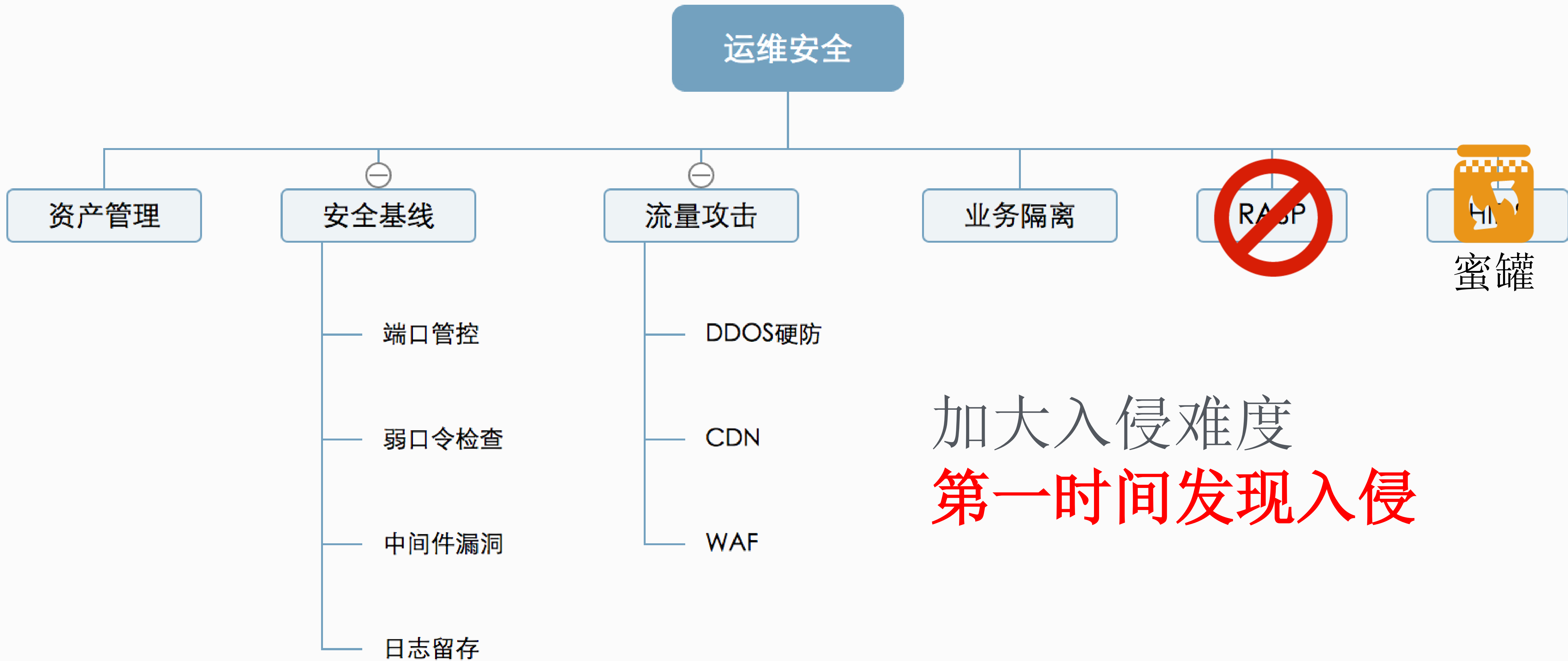
## 定目标

- 现在我们能做什么？
- 要做到什么程度？
- 怎么做？



## 定规矩

- 代码安全规范
- 运维安全规范
- 员工信息安全规范







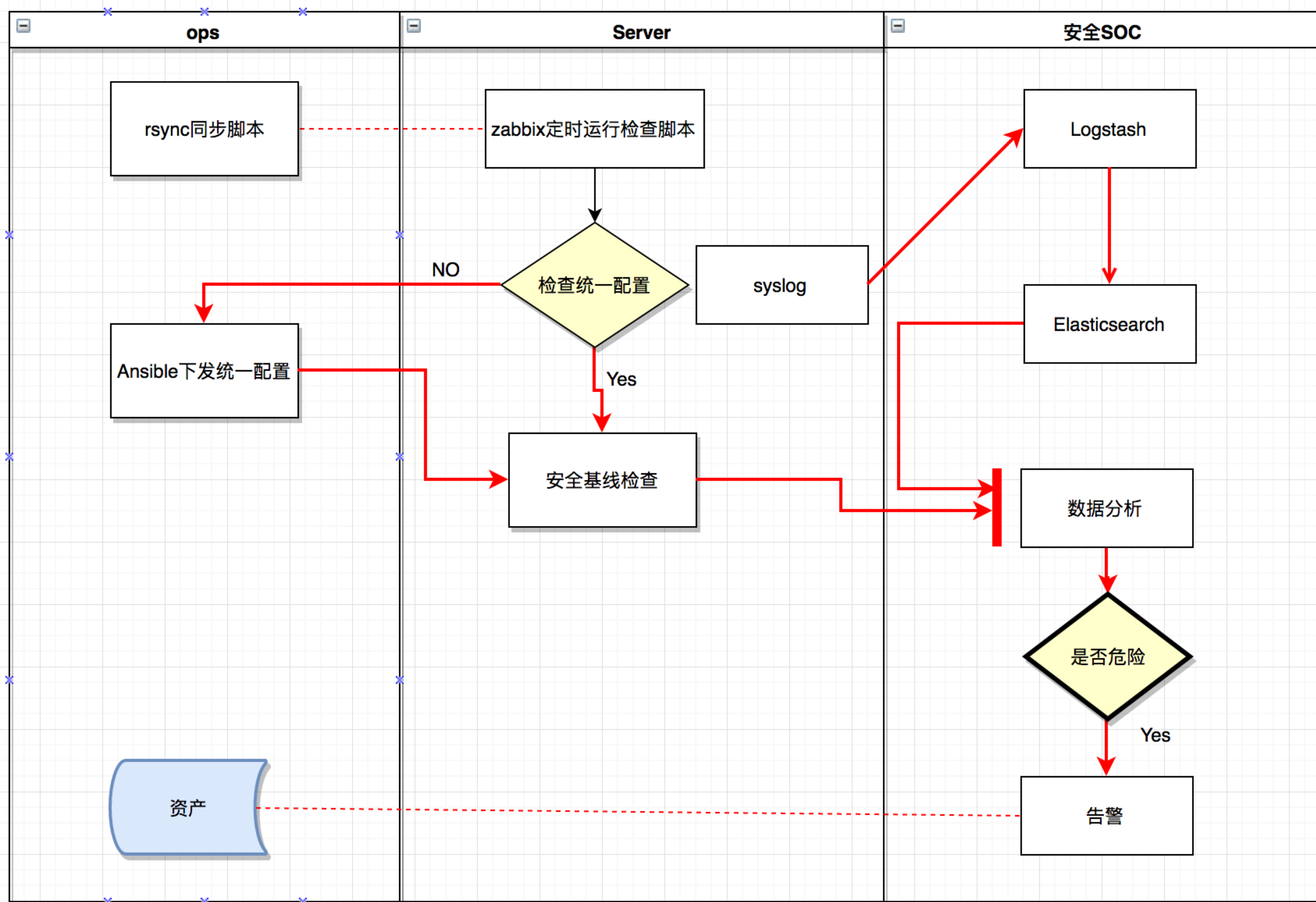
## 运维安全规范

Created and last modified by wuwenhao on 三月 03, 2017

- `/etc/hosts.allow`
- bash漏洞 (shellshock)
- DNS 域传送漏洞
- ElasticSearch安全配置
- FTP服务器安全配置
- Git导致文件泄露
- Memcached安全配置
- MongoDB安全配置
- MySQL安全配置
- NFS安全配置
- OPENSsl:心脏出血 (heart bleed) 漏洞
- Rsync安全配置
- 关于服务器的host绑定的不安全因素

## From WooYun Wiki的备份

<https://github.com/13m0n/wooyun-wiki>



[登录安全](#)[基线检查](#)[操作历史](#)

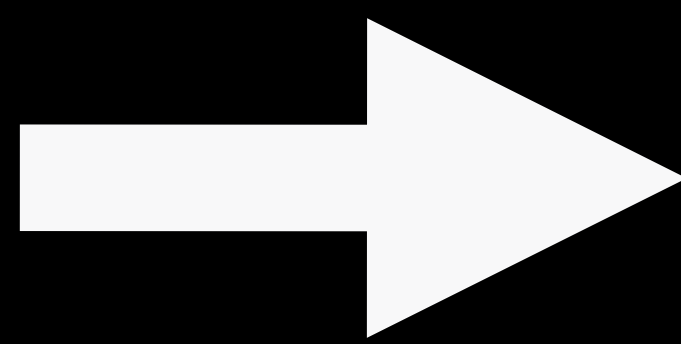
搜索命令

| 机器名     | 用户   | 命令内容                                    | time           |
|---------|------|---|----------------|
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 14:15:09 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 14:15:09 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 14:15:09 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 14:15:09 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 13:59:41 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 13:59:41 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 13:59:41 |
| pd-ci-1 | root | vim ./docker_build/golang1.6/Dockerfile | Apr 7 13:59:41 |



## 应用安全

- ✓ 渗透测试
- ✓ 落实代码规范
- ✓ 上线前的安全测试
- ✓ 部署WAF
- ✓ 漏洞生命周期管理 (SRC)
- ✓ 关注业界动态
- ✓ **事件推动安全！！**



在被外人搞之前  
自己先搞了





# 发布流程

- 安全开发白盒自检
- 安全部门黑盒测试
- 测试部门测试

- 安全部署自检
- 安全部门上线后自检

- IT服务管理
- 安全事件响应

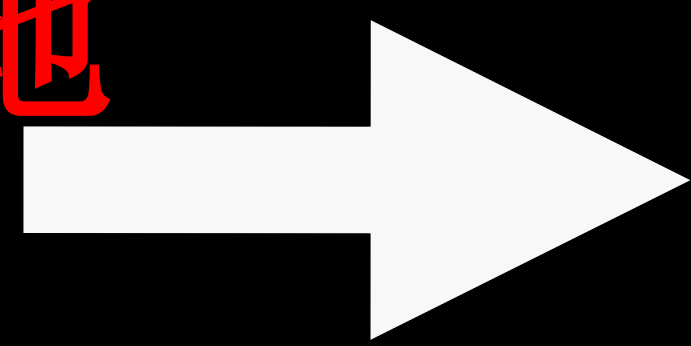
```
graph LR; subgraph Dev [开发]; direction TB; D1[开发]; D2[单元测试  
安全自检]; end; subgraph Test [测试]; direction TB; T1[测试部门测试]; T2[安全部门测试]; end; subgraph Deploy [上线]; direction TB; U1[上线]; U2[上线]; end; D2 --> T1; D2 --> T2; T1 --> U2; T2 --> U2; D1 -.-> D2; T1 -.-> T2; U1 -.-> U2;
```

开发提交《安全开发自检文档》



# 信息安全

- ✓ 办公网与生产网隔离
- ✓ 机密部门VLAN隔离
- ✓ 信息安全管理**的落地**
- ✓ SSO+双因子认证
- ✓ 办公网准入机制
- ✓ Github爬虫
- ✓ **员工安全意识！！**



老板衡量安全做得好不好  
的重要因素

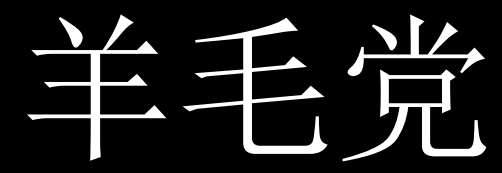
# 业务安全与风控



羊毛党

- 养帐号
- 领定时礼物
- 刷直播抽奖
- 刷直播在线观看数
- 刷游戏初始帐号







🏠 主页

🔍 漏洞生命周期管理

👁 安全审计

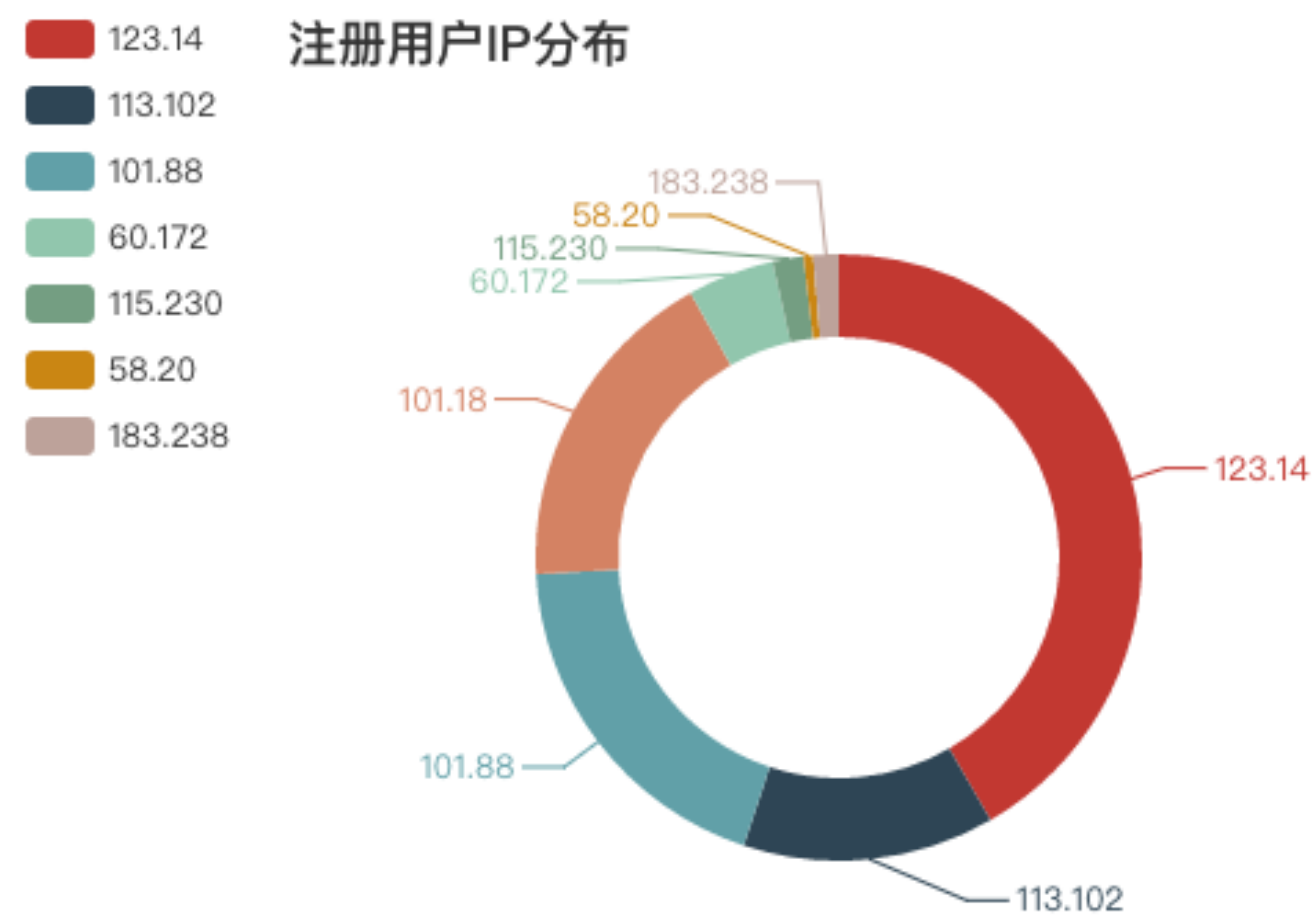
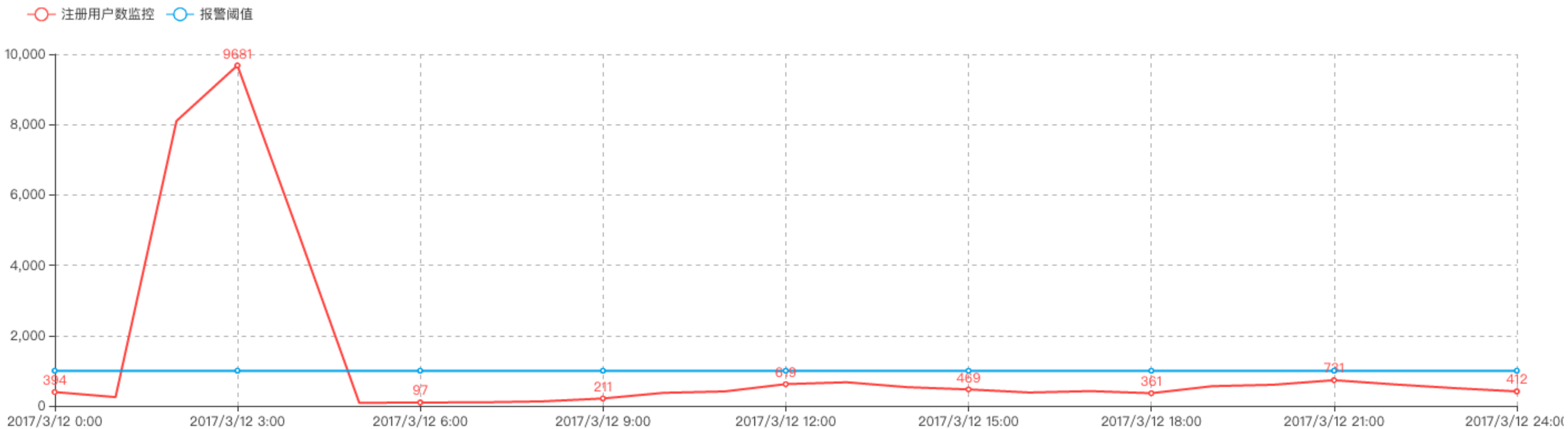
☁ 服务器安全

🐱 github监控

📊 态势感知

📊 大数据风控

⚙ 系统设置



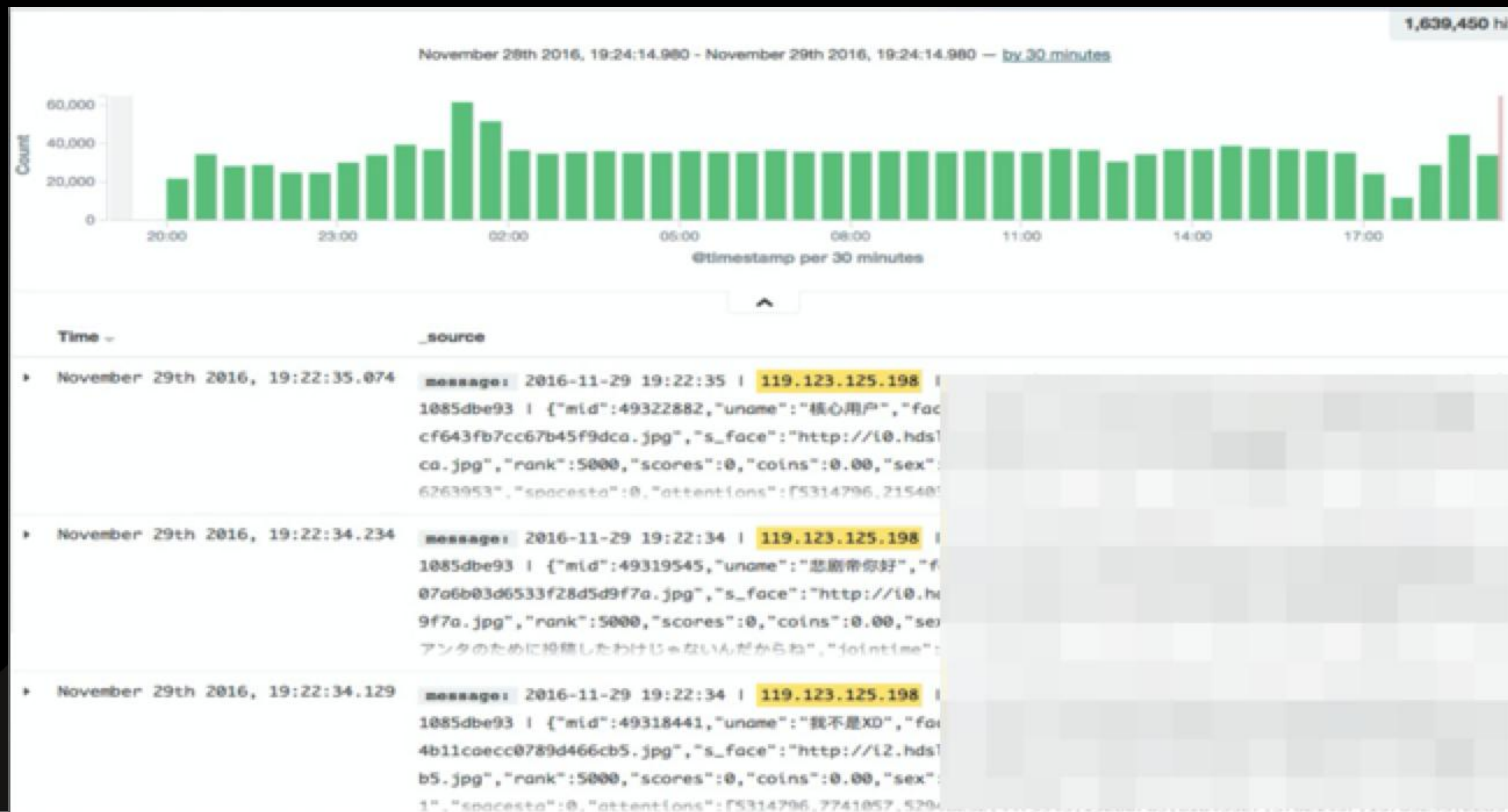


# 羊毛党

该ip在4小时内登录了 8579 个账号, mid相邻账号 5107 个, 绑定了手机的账号个数为 0 个, 注册时间间隔不到1小时的账号个数 8579 个

→ /tmp

→ /tmp python test.py 180.153.242.22







183. 在刷passport登录接口 ☆

发件人 @bilibili.com>

时 间: 2017年3月2日(星期四) 下午3:43

收件人 @bilibili.com>

您好, 绝对不是程序的我发现 1.11.57 在刷登录接口

该ip在1分钟内登录了 347 个账号,mid相邻账号 347 个

请相关负责人获知后及时确认状态、并对mid

[67966712,67475270,67798997,67554119,67541289,67734591,67498353,67507898,67381213,67712513,67790282,67109473,67770505,67565919,67779842,68012166,67874327,67746567,67546624,67865424,67392884,67654669,67103131,67402138,67789499,67387810,67397263,67746853,67204151,67647347,67795726,67312171,67654307,67609100,67602617,67139112,67238222,68004532,68094184,67763922,67225845,67984581,67805192,67905720,67296039,67819789,67385538,67622922,67895305,67905625,68078737,67936473,67718369,67919604,68079784,68052553,67951437,67261573,67521636,67116821,67459246,67791501,67562093,67798516,67202479,67966887,67577911,67336703,67849250,67375287,67386473,67248483,67751818,67513870,67199337,68037428,67926023,67987896,68049730,67737227,67420690,67762966,68091850,67470429,67362315,67390838,67197595,67795987,67443592,67895857,67875405,67258810,67840274,67117971,67974219,68089612,67981167,67293335,67402145,67520479,68104525,67275785,67989967,67997104,68026941,67548695,67673318,67496456,67786822,67630991,67657169,67836084,67190312,67234839,68106994,67951247,67882088,67948903,67783351,67172390,67750247,67807757,67681631,67206659,67190321,67808299,67845587,67713139,67630725,67879878,67668525,67326819,67824084,67866031,67443322,67494331,67224597,67296971,67996199,67937208,67108167,67549605,67650075,67580509,67324582,67136457,67594561,67258429,67673358,67958786,67256104,67185689,67157848,67213439,67587631,67429278,67163108,67825436,67288291,67728125,67978759,67588783,67792058,67832146,67494141,67177301,67671036,67970455,67180891,67549385,67753017,67804292,67829776,67643751,68026537,67963811,67123370,67613829,67139627,68078710,67765333,67705192,67665942,67357956,67726293,67773434,67677508,67603515,67445153,67905831,67542760,67707461,67980792,67368043,67661173,68042017,67433514,68069094,67924117,67986805,67771019,68020693,67684000,67879296,68056256,68037912,67123693,67276325,67464439,67851462,67799884,67489798,67417097,67784141,67327962,67788399,67208594,67689053,67648008,68041528,68066267,67633500,67473635,67249772,67956434,67769932,68096228,67325706,68065218,67563354,67666895,67953031,67442869,67875269,67469212,68111626,67500922,67756506,67849412,67505746,67784299,67180808,67398860,67548138,67626073,67723099,67171534,67268223,67838224,67543438,67827054,67381411,67458883,67323243,67580690,67854163,67228300,67717386,67978688,67422126,67412177,67505089,67334844,67520180,67570869,67998861,67921281,67261756,67714930,67418717,68000127,67313555,67163518,67152370,68109086,67173998,67841083,67146900,67654314,67278443,67100605,68092194,67861494,68029183,67474435,67309840,67542240,67544900,67290423,67713758,67601789,67366127,67758925,67244168,67766933,67594171,67768668,67582304,67388875,67724271,67785699,67579066,67466423,68036101,67394228,68053674,67574816,67169858,68102247,67486630,67772953,67839089,67846283,67368652,67776333,67909260,67161777,68069082,67526507,67205926,68121838,67176365,67596442,67980195,67136476,67371722,67403790,67184546,67672002,67906940,67685245,67379639,67393432,67349275,67653670,67632999,67253898,67712744,67490975,67285885,67469014,67260462,68014874,67906843,67988433,67540965,67408932]进行封号踢登录操作

IP长串

3箱



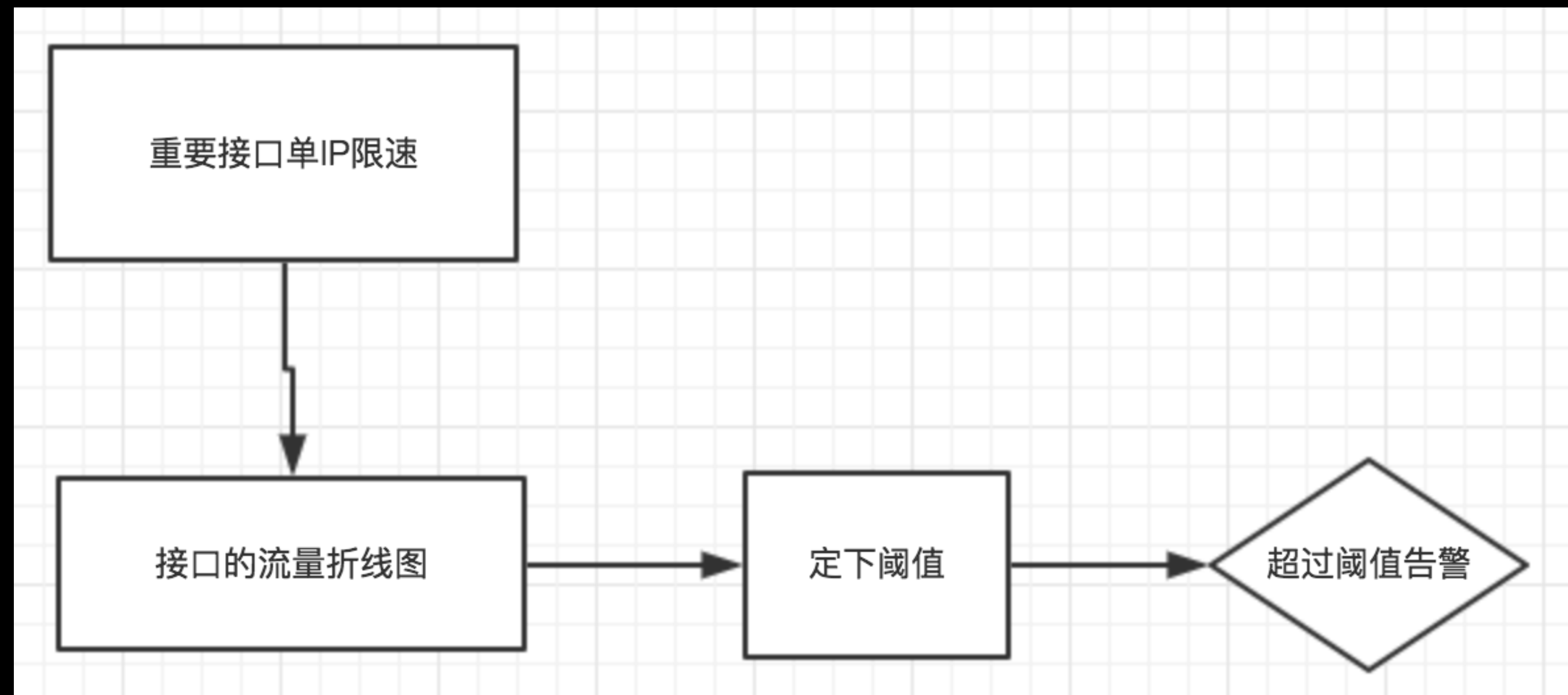


- 爬弹幕，爬用户公开资料
- 做“数据分析”
- 什么都不做,就是想练习下代码
- 员工利用爬虫高效完成工作



# 爬虫的危害都有啥

- 协程+多线程+分布式 == CC攻击
- Redis , memcached缓存存满



# 汇报安全工作



# 世界三大难题

- 欧洲的债务
- 非洲的难民
- 中国  的高
- 还有一个安全汇报工作



# 漏洞生命周期

SRC、应急响应事件、已知待解决的安全风险

## 覆盖率

上线前安全测试、安全基线、资产、灰色地带

## 主动检出率

渗透入侵、常见漏洞、安全测试、薅羊毛、违规员工



## 安全自研

SOC、安全产品

## 成本

买了什么第三方、投入和效果

## 数据

有图有表(都要下降趋势)





关注QCon微信公众号，  
获得更多干货！

# Thanks!



主办方 **Geekbang** **InfoQ**  
极客邦科技