



我的电商安全观

——林鹏



个人介绍

当当网
dangdang.com

网信集团
NCF GROUP

飞凡
ffan.com

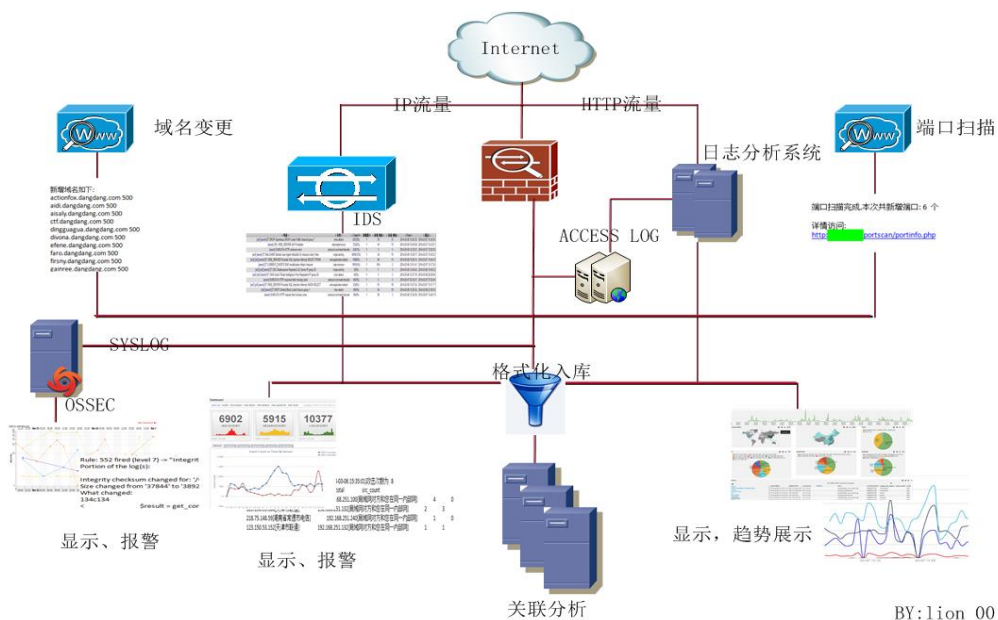
- 当当网

- 网信

- 飞凡



传统安全



□ E.L.K

□ SURICATA

□ OSSEC

□ 流程



传统安全-对外部攻击

规则配置

攻击规则管理 修改

Request.url

phpinfo.php

Request.user-agent

request.user-agent:特征匹配(需正则)

Request.body

request.body:特征匹配(需正则)

Response.body

response.body:特征匹配(需正则)

Response.code

200,404

Rule Description

phpinfo页面探测

Weight

1

Alert Name

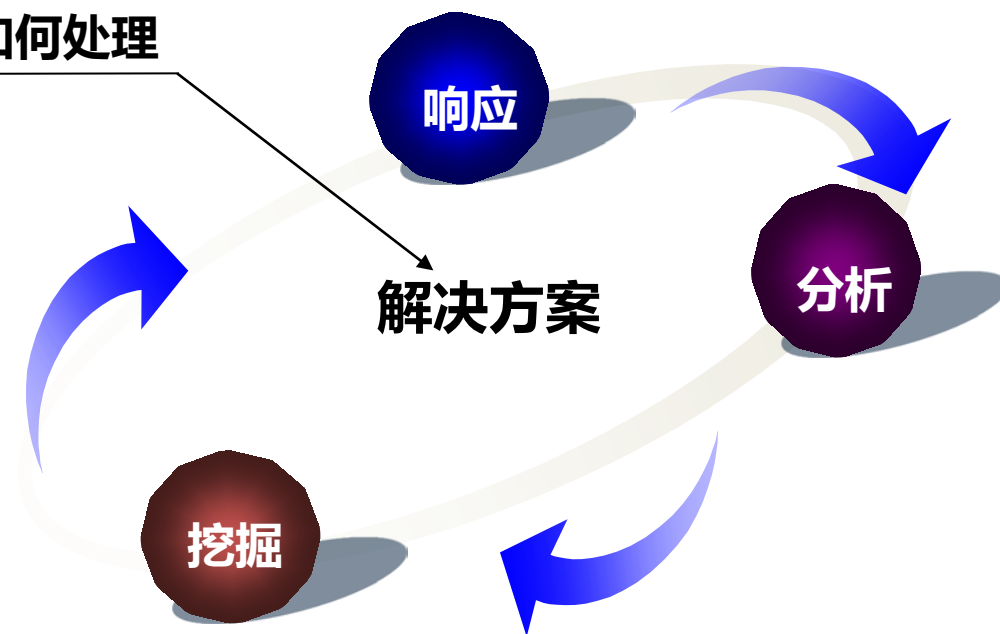
PHPINFO页面探测

告警内容

response.code	200
@timestamp	2016-06-18T01:11:24.666912
realIP	220.179.132.254
id	C12016061809110949592455325
request.host	fan.com
request.method	GET
response.content-encoding	gzip
dst	
request.user-agent	sqlmap/1.0.4.19#dev (http://sqlmap.org)
geo_longitude	117.281
realUrl	/zzq/h5/activity618/index.html
request.x-forwarded-for	220.179.132.254
geo_city	Hefei
request.hc	1
city	中国 安徽 滁州
geo_latitude	31.864
src	
response.body	
response.length	4
request.url	/zzq/h5/activity618/index.html?localCityId=310100&uid=15000000069286428
geo_country	China
time	2016-06-18 09:11:24



对于告警的信息，如何处理





传统安全-对信息的收集与处理1

攻击IP

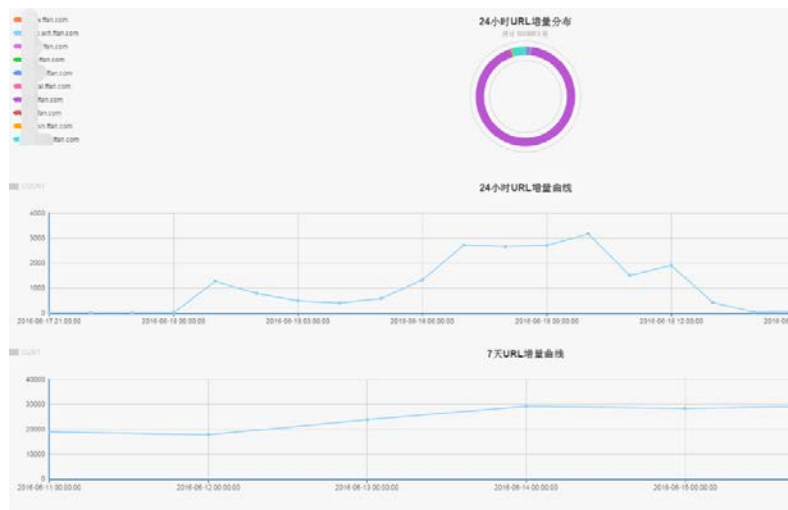
total_score	
5, 13:52:45.374	16
June 18th 2016, 13:52:45.374	2015-11-26
AVViEWMr2mkdCFR1Wrh0	2015-11-26
logstash-sec-login-detect-2016.06	2015-11-26
test-type	2015-11-26
中国吉林长春	
3	70781 攻击IP列表 1 2 ... 704 705 706 707 708
异地登录:3.0	
攻击IP:2.0	
vn	
time	
2016-06-18 13:50:28	
Version 2.0	
Copyright © 2015-2017 security.intraffan.com All Rights Reserv	

代理IP



传统安全-对信息的收集与处理2

记录新增URL



被动扫描

ID	域名	请求方法	漏洞类型	入库时间	扫描节点	操作
3e04416f8e2d0a33	https://ffan.com/imageController/requestRegImgInfo.do	GET	XSS跨站	2016/06/16 15:45:51	127.0.0.1	详情
3e04416f8e2d0a33	https://ffan.com/imageController/requestRegImgInfo.do	GET	XSS跨站	2016/06/16 15:45:51	127.0.0.1	详情
f61dfafda86a1481	https://ffan.com/imageController/requestRegImgInfo.do	GET	XSS跨站	2016/06/16 15:44:50	127.0.0.1	详情
83611ccd8ea3155a	http://ffan.com/ap	GET	XSS跨站	2016/06/16 09:18:02	127.0.0.1	详情
977d25901ca1422a	http://ffan.com/ap	GET	XSS跨站	2016/06/16 09:13:56	127.0.0.1	详情

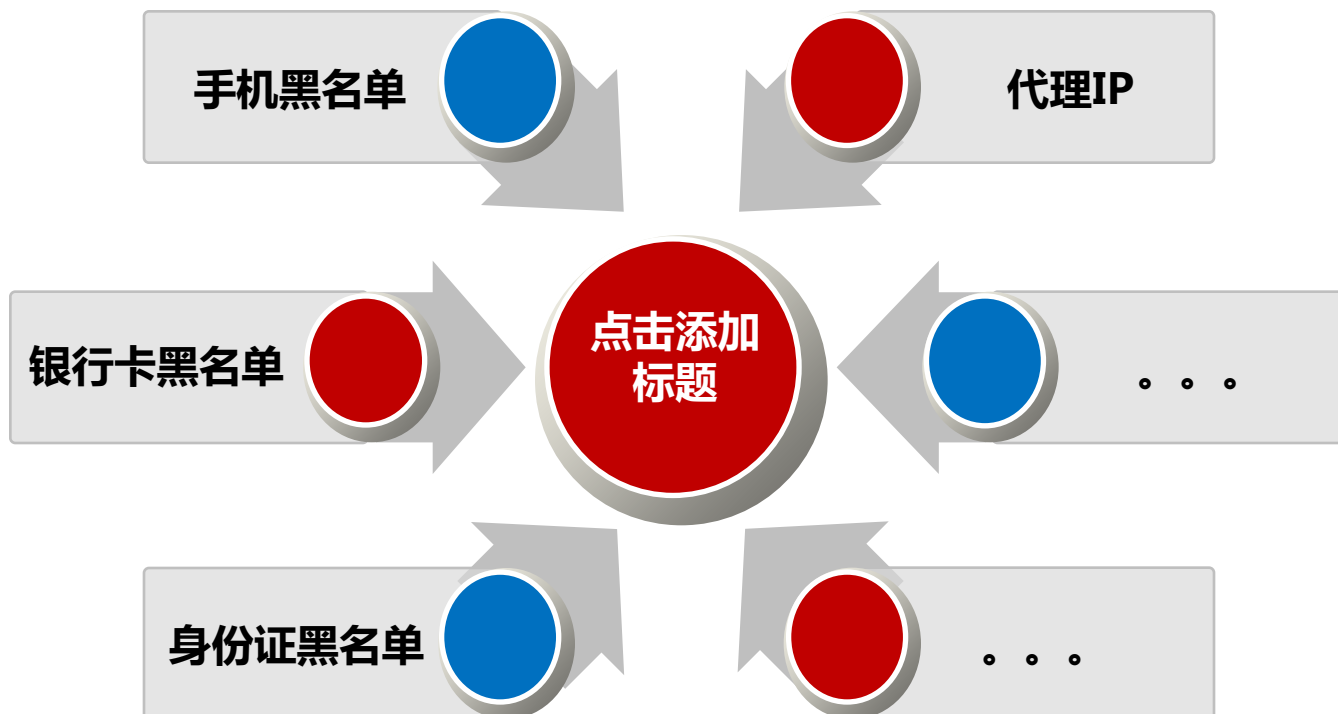


业务安全



业务安全问题







- 活动的接口与APP的版本
- 活动的内容与风控
- 执着的刷单者



APP 第一天下午更新第二天下午14点39分被破解



kibana Discover Visualize Dashboard Settings Today

ef8180c 18406ac

logstash-sec-rebate-YYYY.MM.DD

Data Options

Top 5 request.user-agent.raw

	Count
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)	51,410

netrics

统计学

```
+-----+
| cnt | hours |
+-----+
| 16 | 2016-06-16 10 |
| 301 | 2016-06-16 11 |
| 804 | 2016-06-16 12 |
| 524 | 2016-06-16 13 |
| 2266 | 2016-06-16 14 |
| 7574 | 2016-06-16 15 |
+-----+
6 rows in set (3.89 sec)

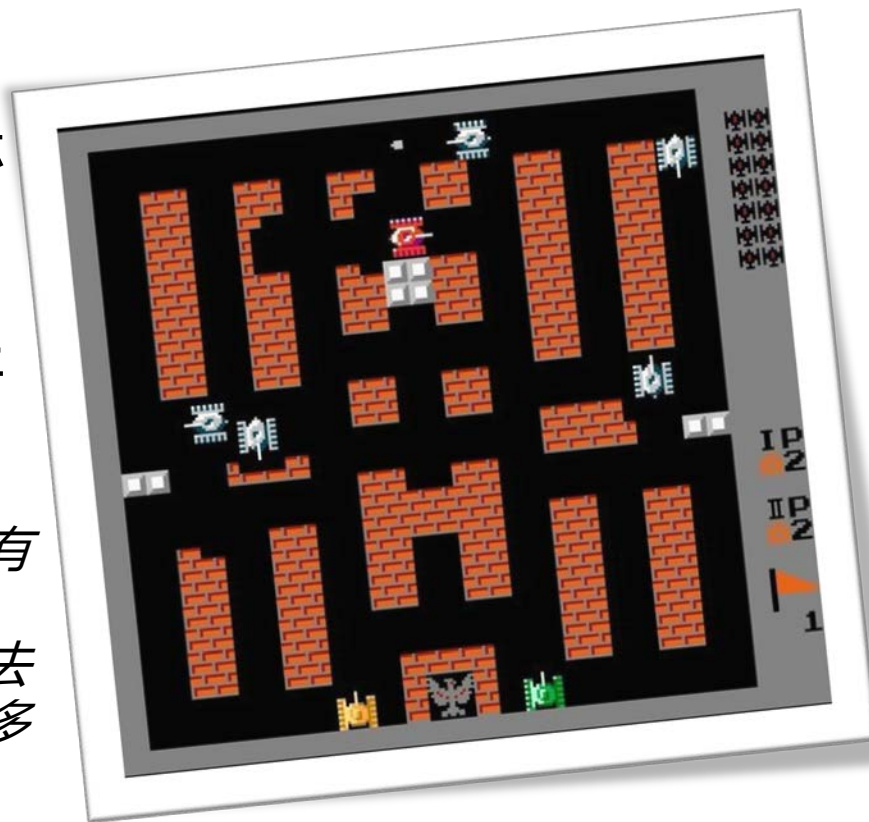
mysql>
```



- 我们身后有要保护的目标
- 我们要保证业务不被影响
- 我们要尽量使用户体验好

每制定一条策略，一定要对策略有100%的了解；

一定要100%了解技术原理，一定要去验证，无论在什么情况，也无论有多忙





谢谢！