



WHITE HAT FEST

2016乌云白帽大会·不插电

# 十年安全路

## 信息安全的从1到10

信息安全总监 凌云  
2016.4

# About Me

凌云 10年信息安全从业经验

待过乙方：绿盟科技

也待过甲方：1号店 中国平安等

目前在携程担任信息安全总监

关注电商业务安全，企业研发安全

信息安全，安全产品设计及合规审计

CISA、ISO27001LA认证



# 目录

- I. 信息安全的从1到10
- II. 运维安全之路
- III. 应用安全之路
- IV. 业务安全之路
- V. 一起在路上

# 信息安全的从1到10

## 先分类

- 运维安全
- 应用安全
- 业务安全
- 安全合规

## 再摸底

- 访谈
- 扫描
- 乌云

## 定目标

- 同行交流
- 我在哪里
- 我要去哪里

## 走起

- 招人
- 单点突破
- 预埋伏笔

# 信息安全的从1到10

携程一年时间20 +人 成长到 40人  
50%的人员会开发python, Java。

运维安全 运维安全工程师, 研发工程师  
应用安全 web安全工程师, 无线安全工程师  
业务安全 安全分析工程师, 安全开发工程师  
安全运营 安全运营人员, 安全合规

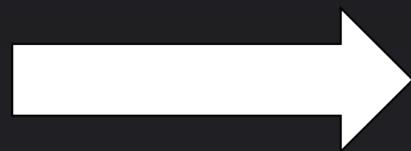
服务携程3000+人的技术团队。

# 目录

- I. 信息安全的从1到10
- II. 运维安全之路
- III. 应用安全之路
- IV. 业务安全之路
- V. 一起在路上

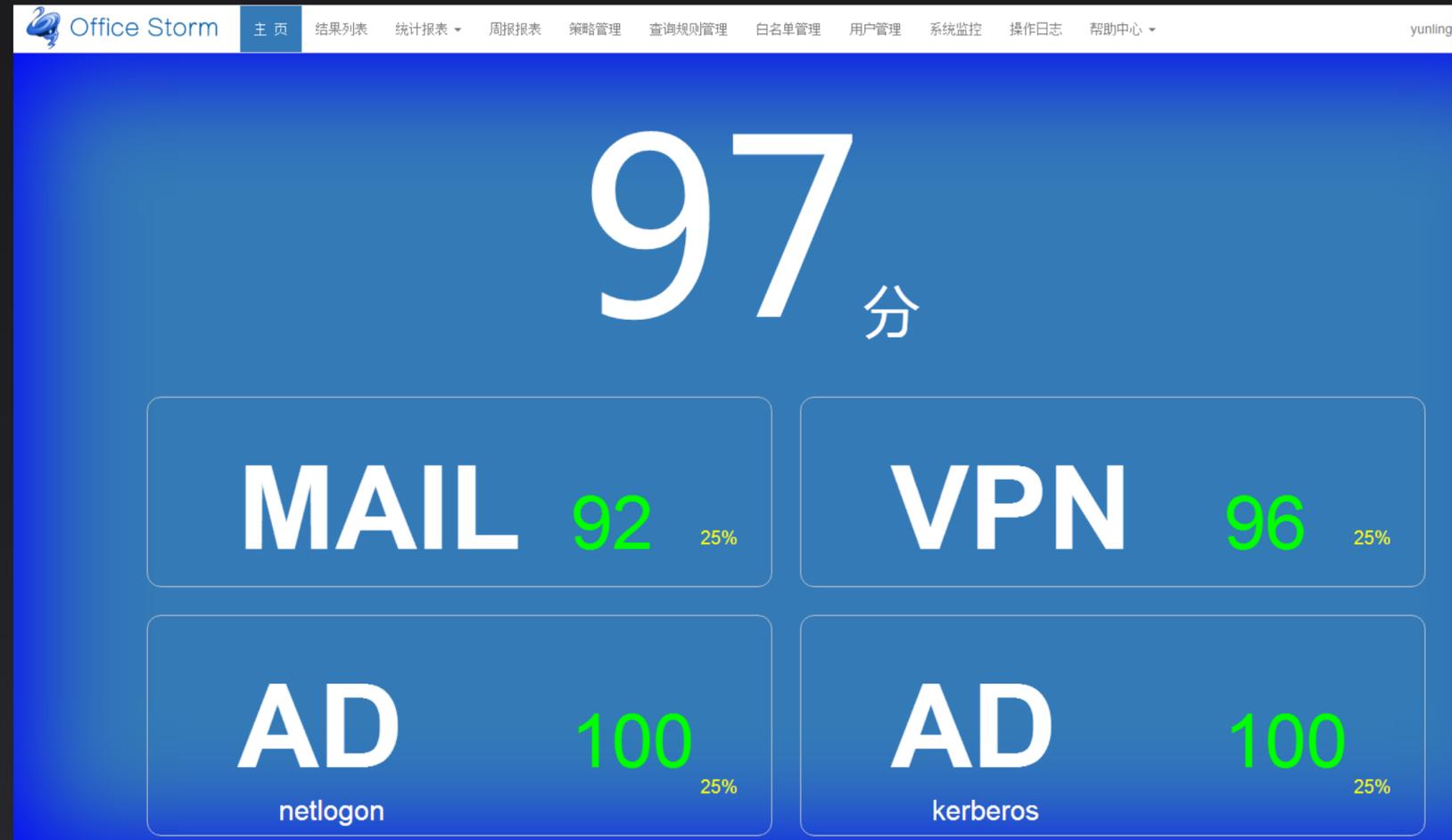
# 运维安全

- ✓ 定运维安全规范
- ✓ 安全域划分
- ✓ 巡检弱口令、漏洞
- ✓ 新增主机扫描
- ✓ 日志收集分析
- ✓ 蜜罐
- ✓ OSSEC
- ✓ APT防御
- ✓ .....



能否加大入侵难度  
能否第一时间发现入侵

办公网日志入Storm  
规则实时分析  
数值化反映  
当前安全情况



Office Storm 主页 结果列表 统计报表 周报报表 策略管理 查询规则管理 白名单管理 用户管理 系统监控 操作日志 帮助中心

ID:  策略名称:  message:  日志来源: --choose-- 状态: --choose-- 开始时间:  结束时间:

ID	策略名称	发生时间	message	附加信息	日志来源	备注
84516	webmail同一个帐号登录失败-12302	2016-05-09 17:47:12	帐号(cn1.global.ctrip.com\CasterPy (!))120分钟内登录失败12次	[...]\CasterPy (!)	tmglog	
84515	webmail同IP登录失败-12302	2016-05-09 17:47:11	60分钟内IP120.132.51.31出现21次用户登录失败	[...ctrip.com\c (!), .../etc/rc.local (!)	tmglog	
84514	AD同一个帐号登录失败(8小时)	2016-05-09 17:54:11	帐号...失败292次		ad	
84513	AD同一个帐号登录失败(8小时)	2016-05-09 17:34:01	帐号...登录失败800次		ad	
84512	webmail同IP登录失败-12302	2016-05-09 17:49:31	...次用户登录失败	[...trip.com\zl... (!), .../etc/rc.local (!)	tmglog	
84511	AD同一个帐号登录失败(8小时)	2016-05-09 17:22:31	帐号(exam)...1次	[exam]	ad	
84510	webmail同IP登录失败-12302	2016-05-09 17:16:11	...分钟内IP...出现...用户登录失败	[...global.ctrip.com\c (!), .../etc/rc.local (!)	tmglog	
84509	webmail同一个帐号登录失败-12302	2016-05-09 17:16:12	...	...com\root (!)	tmglog	
84508	webmail同IP登录失败-12302	2016-05-09 17:10:51	...登录失败	[...emvd (!), ...com\wemvdjs (!)	tmglog	
84507	webmail同IP登录失败-12302	2016-05-09 17:05:12	60...失败	[...global.ctrip.com\wemvdjs (!), ...al.ctrip.com\root (!)	tmglog	
84506	webmail同一个帐号登录失败-12302	2016-05-09 17:15:12	帐号...20分钟内登录失败16次	[...global.ctrip.com\wemvdjs (!)	tmglog	

登录失败IP关联分析

从 2016-05-08 18:07 至 2016-05-09 18:07

10.32.51.31 失败36次

从 2016-05-08 18:07 至 2016-05-09 18:07

10.32.17.138 失败19次

从 2016-05-08 18:07 至 2016-05-09 18:07

172.17.6.27 失败13次

从 2016-05-08 18:07 至 2016-05-09 18:07

10.32.51.145 失败11次

从 2016-05-08 18:07 至 2016-05-09 18:07

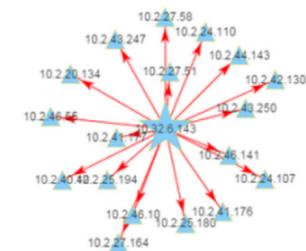
10.32.17.13 失败14次

10.32.17.13

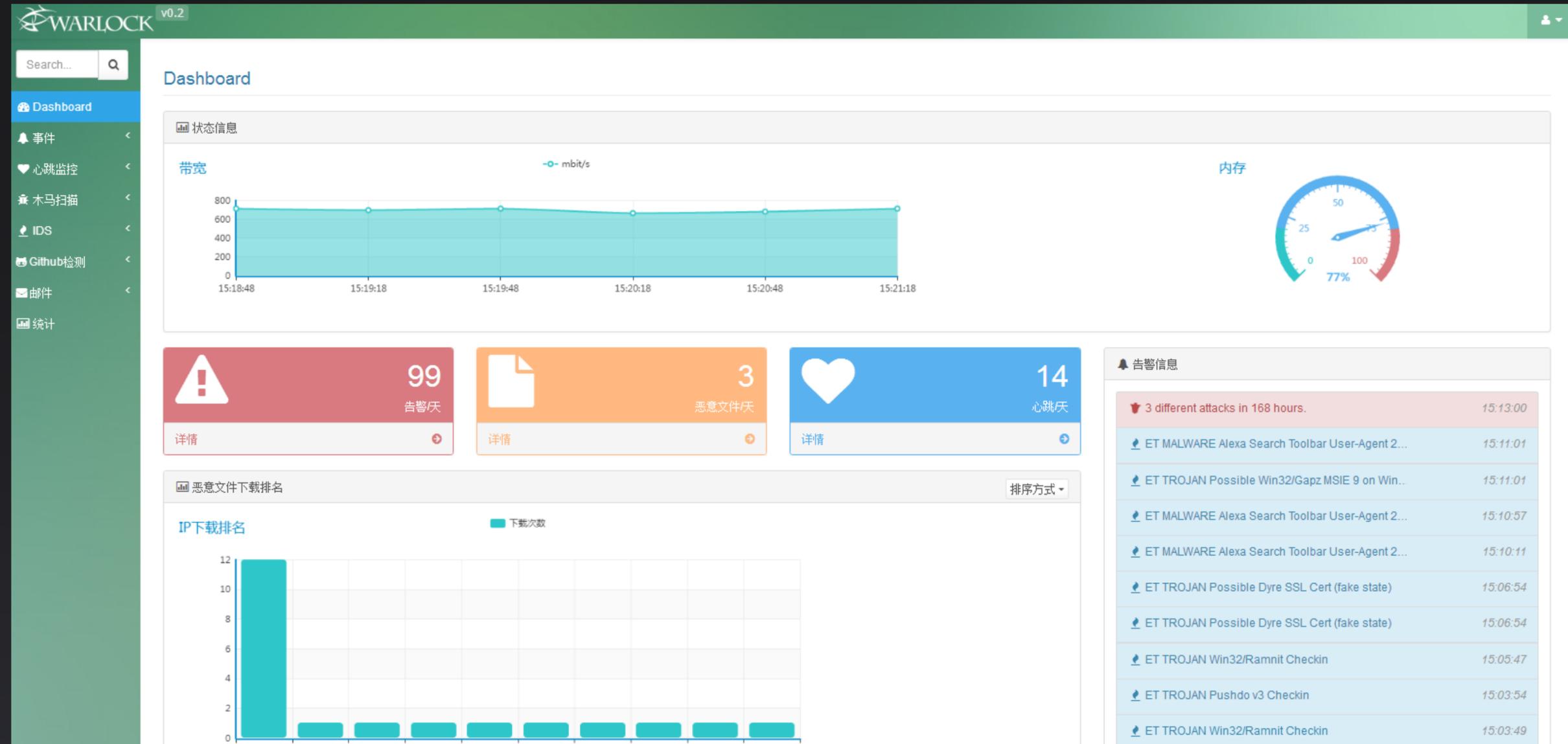


10.32.6.143 失败10次

10.32.6.143



# APT监控



# 目录

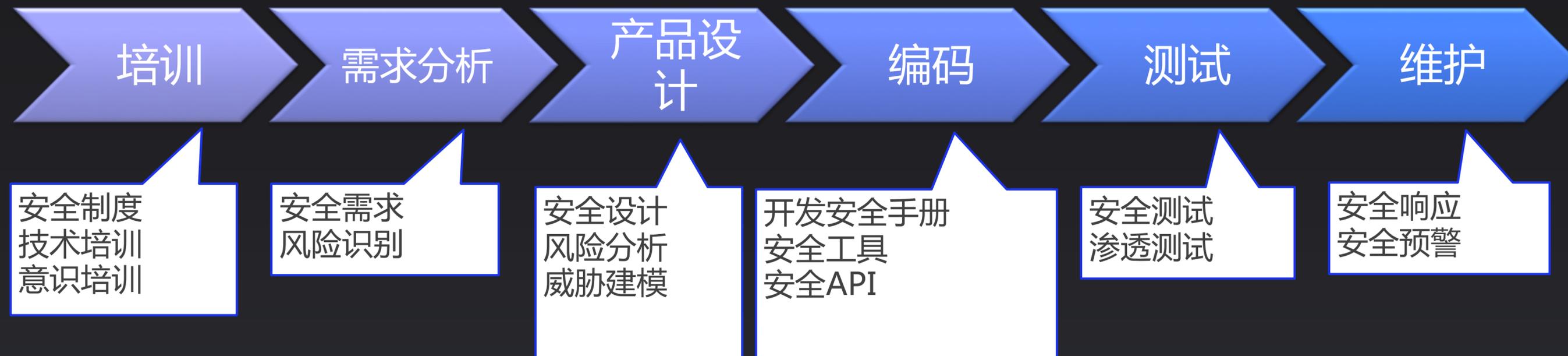
- I. 信息安全的从1到10
- II. 运维安全之路
- III. 应用安全之路
- IV. 业务安全之路
- V. 一起在路上

# 安全开发生命周期 SDL

什么是SDL？

Security Development Lifecycle from Microsoft

军事学说法：纵深防御 娱乐化解读：塔防



# 事前管控，抓大放小



1.身份鉴别	1.1密码支持
	1.2账户策略
	1.3辅助安全设备
2.授权管理	2.1 功能授权
3.访问控制	3.1 系统内访问控制
	3.2 系统外访问控制
4.系统安全审计	4.1 WEB应用访问日志完备性
	4.2 用户认证日志完备性
	4.3 应用操作日志完备性
	4.4 后台日志完备性
	4.5 日志信息安全存储
5.通信安全	5.1 通讯协议
	5.2 通讯安全认证
6.数据安全	6.1 用户数据的输入与输出
	6.2 用户数据保密性
	6.3 用户数据完整性鉴别
	6.4 用户数据的存储
7.抗抵赖	7.1 原发抗抵赖
	7.2 接收抗抵赖
	7.3 数字证书
8.软件容错	8.1 降级容错
	8.2 受限容错
9.资源控制	9.1 内部资源控制
	9.2 外部资源控制

# 登录注册风险

## 注册

1. 遍历已注册手机号
2. 允许弱密码注册
3. 抢注他人手机号
4. 绕过短信验证
5. 注册时可短信炸弹
6. 批量注册
7. 注册处存在SQL注入、跨站脚本、跨站请求欺骗类漏洞
8. 注册时图形验证码可绕过
9. 邮箱注册时验证值可猜解



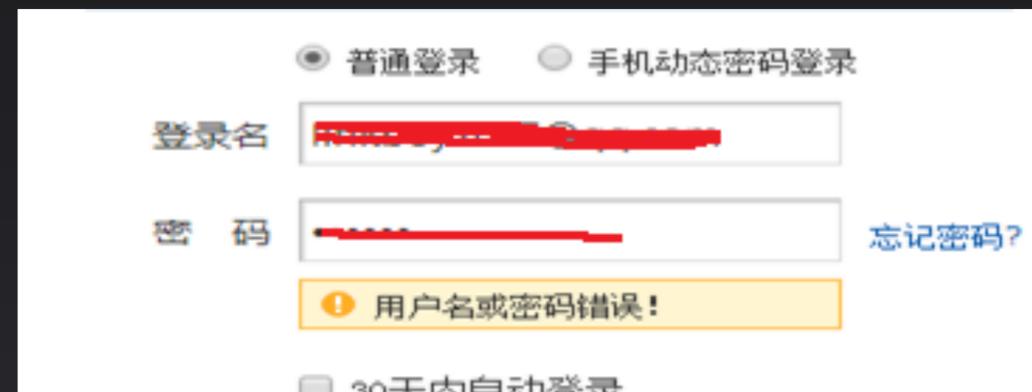
The image shows a registration flow diagram with three steps: 1. 设置登录名 (Set login name), 2. 设置密码 (Set password), and 3. 注册成功 (Registration successful). Below the diagram is a registration form where the phone number field contains '138' followed by redacted digits. A message on the right states: '该手机号已存在，您可以：' (This phone number already exists, you can:). The options listed are: '用此号码直接登录' (Log in directly with this number), '如忘记密码可用手机号找回密码' (If you forget your password, you can use your phone number to recover it), and '如你没用该号码注册过账号，可验证后重新注册' (If you haven't registered an account with this number, you can verify and register again).



The image shows a login form titled '会员登录' (Member Login) with a link to '立即注册，享积分换礼、提现等专属优惠!' (Register now, enjoy exclusive benefits like积分换礼, 提现). There are two login options: '普通登录' (Normal login) and '手机动态密码登录' (Mobile dynamic password login), with the latter selected. The phone number field contains '138' followed by redacted digits. The verification code field is empty, and a button next to it displays '7400'. The password field contains '动态密码' (Dynamic password) and a button '发送动态密码' (Send dynamic password). At the bottom, there is a checkbox for '30天内自动登录' (Auto login within 30 days), which is checked.

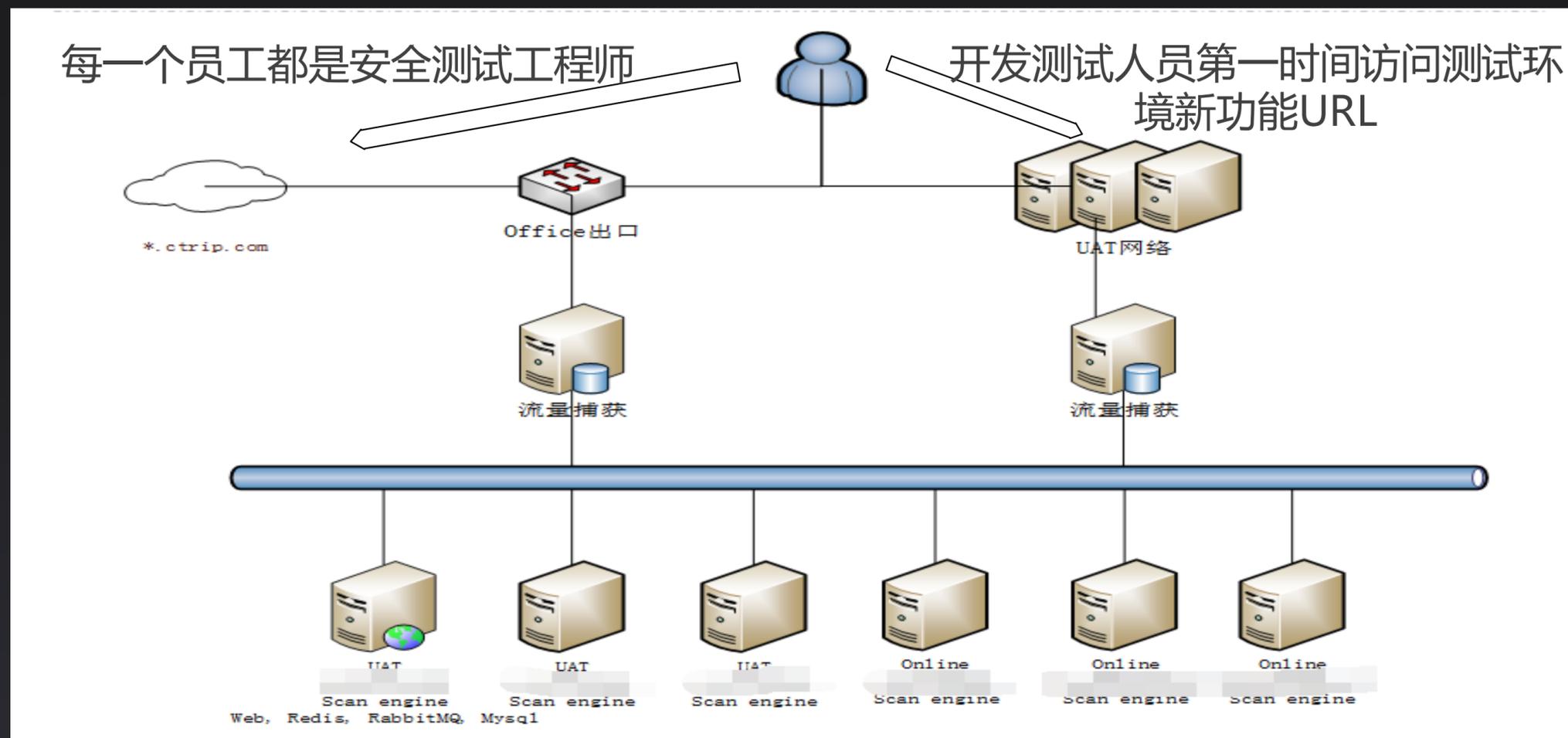
## 登录

1. 登录处可SQL注入
2. 登录处图形验证码可绕过
3. 登录时短信验证码各类问题，如正确的短信验证码在返回数据包中、爆破、短信轰炸、
4. **登录错误提示过于详细**



# 事中自动化，扩大覆盖面

CMDB Git代码库 JIRA DNS服务器 监控？  
我们来点更高大上的黑科技 —— 被动扫描，主动感知

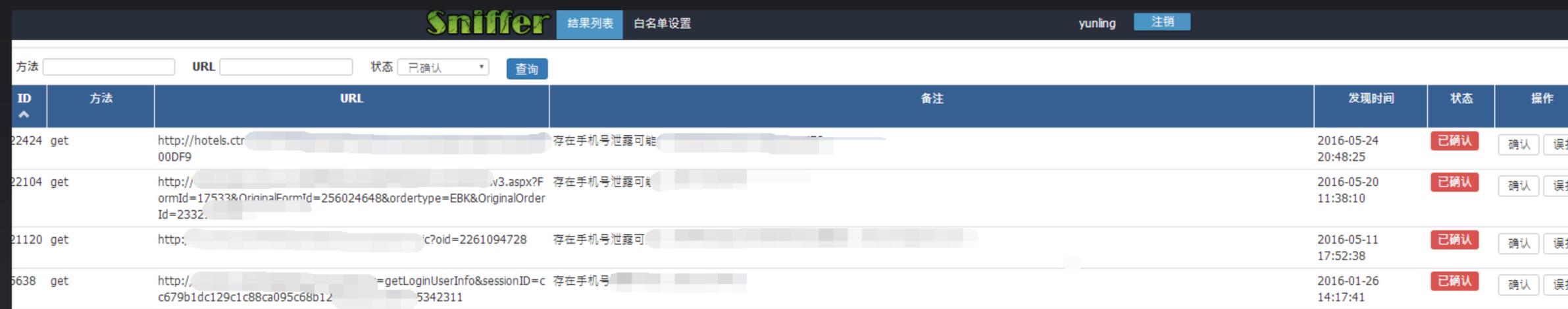


# 抓住每一个新功能



# 水平权限自动化检测

通过自定义Cookies访问含有订单信息的页面  
自动化检测水平权限问题



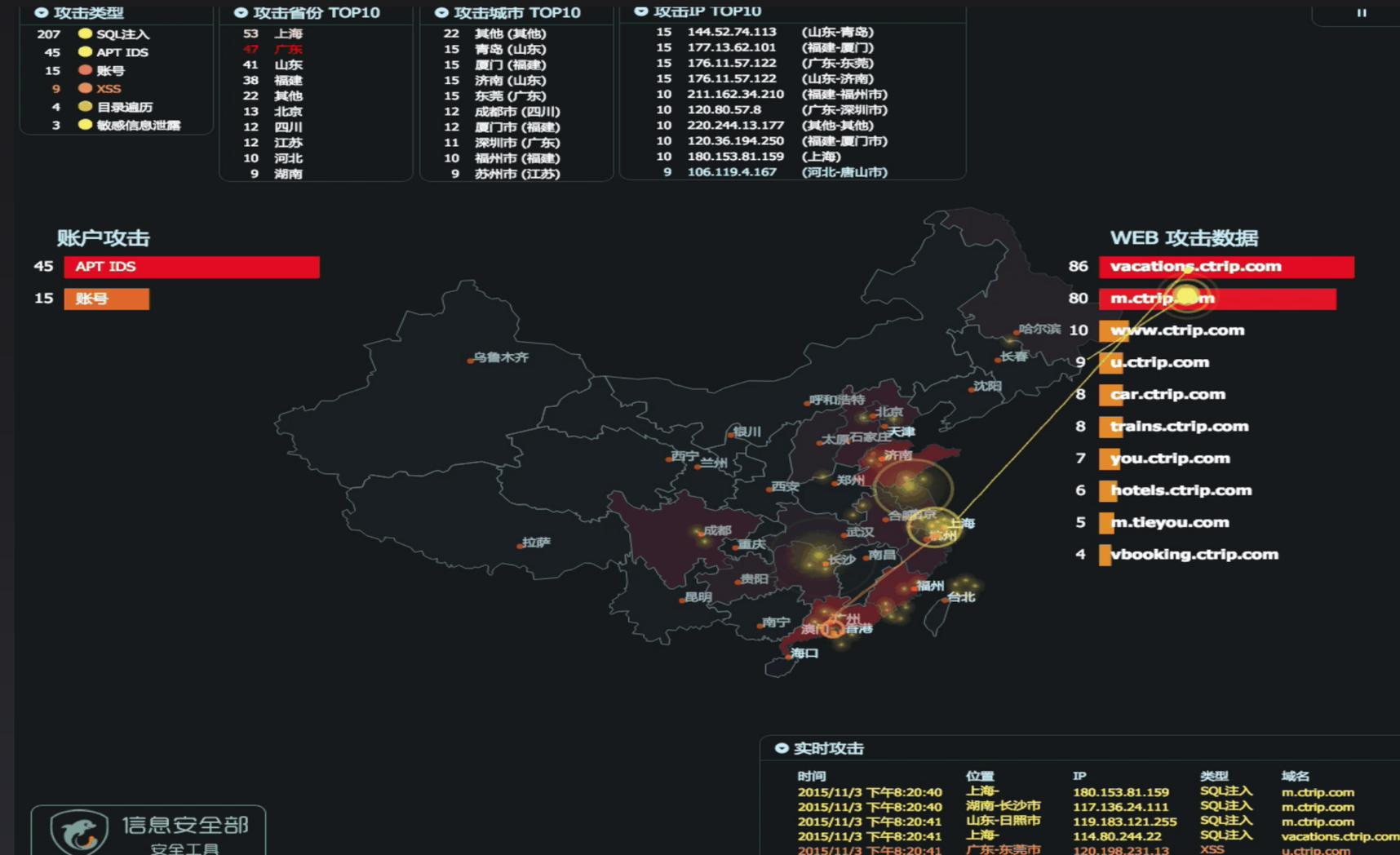
The screenshot shows the Sniffer tool interface with a table of detected vulnerabilities. The table has columns for ID, Method, URL, Remark, Discovery Time, Status, and Action. Four vulnerabilities are listed, all marked as 'Confirmed' (已确认).

ID	方法	URL	备注	发现时间	状态	操作
22424	get	http://hotels.ctr00DF9	存在手机号泄露可能	2016-05-24 20:48:25	已确认	确认 误报
22104	get	http://...v3.aspx?FormId=17533&OriginalFormId=256024648&ordertype=EBK&OriginalOrderId=2332	存在手机号泄露可能	2016-05-20 11:38:10	已确认	确认 误报
21120	get	http://...c?oid=2261094728	存在手机号泄露可能	2016-05-11 17:52:38	已确认	确认 误报
5638	get	http://...=getLoginUserInfo&sessionID=c679b1dc129c1c88ca095c68b12...5342311	存在手机号	2016-01-26 14:17:41	已确认	确认 误报

# 攻击可视化

通过storm  
实时抓取攻击数据  
分析“黑客”爱好

并反向验证  
网站安全情况



# 自研WAF

状态监控

规则策略

统计功能

报表功能

日志明细

变更日志

发布日志

漏报分析

误报分析

攻击日志

切换主题

3D可视化

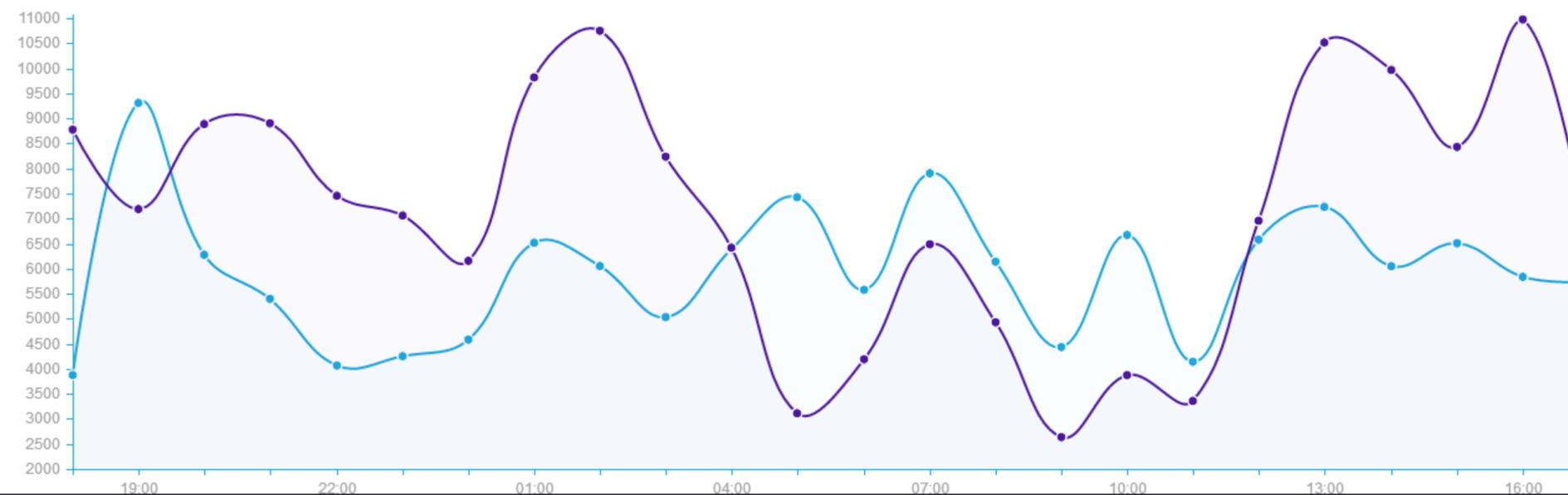
DASHBOARDS

## 状态监控

运行状态



攻击趋势



# 目录

- I. 信息安全的从1到10
- II. 运维安全之路
- III. 应用安全之路
- IV. 业务安全之路
- V. 一起在路上

# 业务安全

1. 扫号撞库
2. 广告劫持
3. 薅羊毛
4. 虚占位/库存
5. 爬虫

## xKungFoo2013

| xKungFoo | 会议日程 | 赞助商 | 演讲者 | 往届会议 | 注册 | 联系我们 |



2013年3月23日星期六 第一天

时间	演讲者	议题
08:00-09:30	会议注册	
xKungFoo开始		
09:30-10:30	王云翔	Oday快速分析 - 预知未来, 通晓过去
10:30-11:00	魏兴国	CC攻击防御基础介绍
11:00-11:10	休息	
11:10-12:10	杨哲	2013:后无线Hacking时代
12:10-13:30	休息	
13:40-14:10	崔孝晨	From 1 day to forensic
14:10-15:10	林鑫	虚拟机入侵与内存取证
15:10-15:20	休息	
15:20-15:50	魏兴国	动态cookie缓解APP时代的CC攻击
15:50-16:50	凌云	电商安全那点事
16:50-17:00	幸运抽奖	

2013年3月24日星期日 第二天

时间	演讲者	议题
09:30-10:30	胡文君	基于Android程序通信机制的攻击及防御方法
10:30-11:00	商广明	Android网络安全
11:00-11:10	休息	
11:10-12:10	何晓杰	Android的组件管控与安全
12:10-13:30	休息	
13:40-14:10	方兴	APT攻击的过去、现在和将来
14:10-15:10	潜伏鹰	先进匿名通信网络的设计及其在敏感行动中的应用
15:10-15:20	休息	
15:20-15:50	Benjurry	SDN 改变网络安全格局
15:50-16:50	于畅 (TK)	浏览器和本地域
16:50-17:00	幸运抽奖 & xKungFoo 闭幕辞	

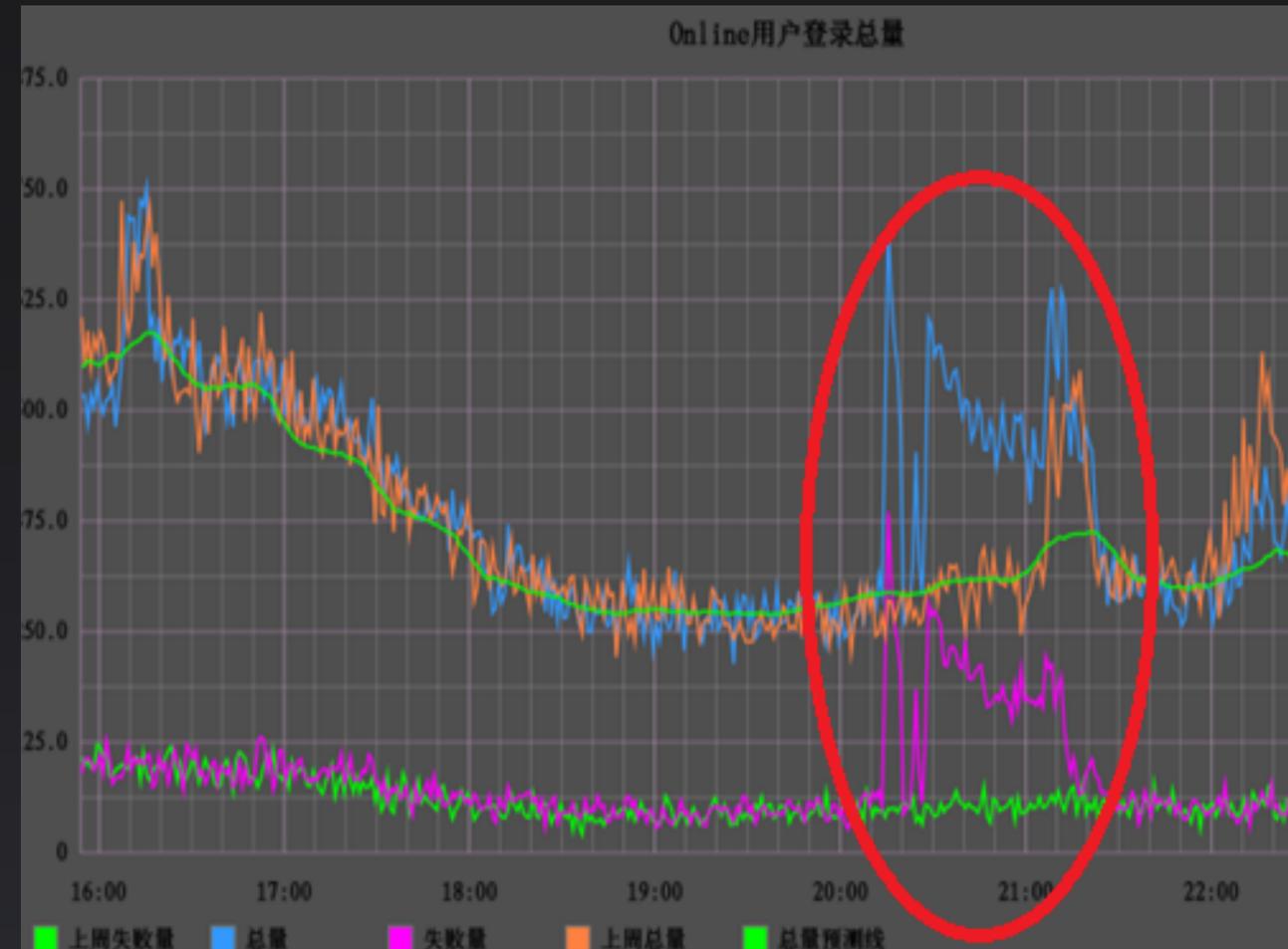
扫号：

威胁用户账号安全的源头

- ◆ 资金盗用
- ◆ 信息泄漏
- ◆ 恶意欺诈

特征：

- ◆ IP使用量巨大，可以做到1号1IP
- ◆ 使用外部社工库，密码正确率高
- ◆ 可以根据安全措施及时更换策略
- ◆ 设备指纹基本伪造，无明显特征



# 薅羊毛与风险库

“羊毛党”调查：日入数万元，美团饿了么都被薅



在线下时代，他们常常为抢打折商品、“限时特供”而排长龙；在电商时代，他们紧盯各电商的优惠券和秒杀，到了网贷兴起时代，因为羊毛丰厚、操作简单，羊毛...  
腾讯财经 3月2日

P2P羊毛党调查：团伙出战，日入数万元(1) 中华网财

20万羊毛党大军，轻易薅干P2P 搜狐

安心贷大战羊毛党，撸羊毛不顺便到处宣扬... 浙江报

羊毛党惹的祸，借贷宝这样躺枪有点冤 和讯网

个人羊毛客

凡有活动就薅，不计风险。



羊毛团伙

以薅羊毛为职业，团队作战，分工明确，拥有几百个手机号、身份证、银行虚拟卡，可对同一公司的活动狂薅。



集团作战

当羊毛党结集10个以上羊毛团伙，资金达到5000万以上时，可利用提现绑架平台，进行“接管”，甚至“搞垮”平台。



## 谁是小号?

eud7282038da@163.com  
pgcf77045140haos@163.com  
qhz77413593jiaos4@163.com  
xd63576160haoyi6@163.com  
zhuoji9683@163.com  
lting520@hotmail.com

RiskRep-风险库系统

导入风控配置 手机号数据 弱密码数据 白名单库 风险数据 注册数据 登录数据 领券数据 分数转换 数据计时 手机号归属 用户管理 账户

起始日期:  结束日期:  数据来源:

注册IP:  UID:  ClientID:

命中策略:  Tag:  密码MD5:

ID	注册时间	注册IP	UID	注册平台	邮箱	Tag	策略ID	SourceFrom	ClientID	更新时间
24459242	2016-06-13 18:03:04	119.101.113	E395736779	P	y4397351luwen5447@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:01
24459222	2016-06-13 18:03:27	119.101.713	E395736951	P	hao6399872wengl@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:00
24459215	2016-06-13 18:03:19	119.101.713	E395736891	P	chao6455170z@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:00
24459212	2016-06-13 18:03:45	119.101.75	E395737111	P	lu81212duanbe@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:00
24459188	2016-06-13 18:03:29		M395736984	M		批量注册	注册策略1	CRM	12001172810023852852	2016-06-13 18:05:00
24459177	2016-06-13 18:03:29	119.101.107.11	E395736646	P	spw7038788sheng@163.com	批量注册	注册策略	CRM		2016-06-13 18:05:00

手机号

手机号

查询

清空

+ 批量导入

+ 添加

ID	手机类型	phone_header	省份	城市	区号	邮编	操作
325253	联通	1554787	内蒙古	巴彦淖尔市			<a href="#">修改</a> <a href="#">删除</a>
325252	移动	1513380	河北	承德市			<a href="#">修改</a> <a href="#">删除</a>
325251	联通	1554844	内蒙古	赤峰市			<a href="#">修改</a> <a href="#">删除</a>
325250	联通	1554775	内蒙古	鄂尔多斯市			<a href="#">修改</a> <a href="#">删除</a>
325249	联通	1554752	内蒙古	通辽市			<a href="#">修改</a> <a href="#">删除</a>
325248	联通	1554923	湖北	恩施市			<a href="#">修改</a> <a href="#">删除</a>
325247	联通	1554847	内蒙古	赤峰市			<a href="#">修改</a> <a href="#">删除</a>
325246	联通	1554957	湖北	孝感市			<a href="#">修改</a> <a href="#">删除</a>
325245	移动	1508964	广东	茂名市			<a href="#">修改</a> <a href="#">删除</a>
325244	联通	1554842	内蒙古	赤峰市			<a href="#">修改</a> <a href="#">删除</a>
325243	电信	1535463	吉林	四平市			<a href="#">修改</a> <a href="#">删除</a>
325242	联通	1554841	内蒙古	赤峰市			<a href="#">修改</a> <a href="#">删除</a>
325241	联通	1554875	内蒙古	呼和浩特市			<a href="#">修改</a> <a href="#">删除</a>
325240	联通	1319171	河北	邯郸市			<a href="#">修改</a> <a href="#">删除</a>
325239	联通	1554773	内蒙古	鄂尔多斯市			<a href="#">修改</a> <a href="#">删除</a>

Previous

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

Next

共 325253 条数据

1

跳转至第 1 页



# 批量领券拦截

ID	请求时间	用户IP	用户IP地理位置	UID	UserName	手机号归属地	注册时间间隔时间 (ms)	重置密码间隔时间 (ms)			Tag	策略ID	更新时间	UA	URL
1695	2016-03-30 11:08:02	112.102.69.27	黑龙江	M354847129	15665808142	济南	1000	121161	9016B BCE4 A9DAD		批量刷券	活动领券策略1	2016-03-30 11:11:13	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.154 Safari/537.36 LBBROWSER	/mobilecouponws/json/Participate
1694	2016-03-30 11:09:06	1.58.55.80	黑龙江	M354847693	15665758642	济南	1000	62244	9016B BCE4 A9DAD		批量刷券	活动领券策略1	2016-03-30 11:11:12	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36	/mobilecouponws/json/Participate
1693	2016-03-30 11:08:21	1.58.55.80	黑龙江	M354847284	15665764069	济南	1000	68641	9016B BCE4 A9DAD		批量刷券	活动领券策略1	2016-03-30 11:11:12	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36	/mobilecouponws/json/Participate
1692	2016-03-30 11:08:11	112.102.69.27	黑龙江	M354847215	15665807486	济南	1000	114238	9016B BCE4 A9DAD		批量刷券	活动领券策略1	2016-03-30 11:11:12	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.87 Safari/537.36 QQBrowser/9.2.5748.40	/mobilecouponws/json/Participate

沉淀恶意手机号	1000W +	➔	上线3个月
国人常用弱密码	2500+		羊毛党拦截1,219,341次
手机归属地分类	32W+		爬虫拦截689,561次

每张卷平均价值20，使用率2%，被刷优惠券损失倍数3

$1219341 * 20 * 2\% * 3 = 1,463,209$  元

# 目录

- I. 信息安全的从1到10
- II. 运维安全之路
- III. 应用安全之路
- IV. 业务安全之路
- V. 一起在路上

# security.ctrip.com

抓痛点，接地气。  
有情怀，不收费。

你的想法，我来实现

携程云安全 安全产品 · 帮助中心 登录 注册

## 携程业务安全防护

千万级手机号码库，让羊毛党无处遁形

登录即可体验

立体防护  
风险分类评估  
实时告警  
风险用户识别  
机器人行为拦截

[01.06]携程信息安全云平台上线 [03.31]军火库功能闪亮登场~

### 让我们一起做一些互联网公司喜欢的安全小工具

- Github Scan**  
监控github代码库，及时发现员工托管公司代码到Github行为并预警，降低代码泄露风险。
- 风险库**  
根据不同层面的恶意行为计算风险值，多年沉淀，千万级别手机号码库，帮助企业有效防御羊毛党。
- 军火库**  
监控常用软件漏洞发布，对存在POC的漏洞及时预警，帮助用户提早发现高风险安全漏洞。
- 天眼**  
跟踪最新互联网泄密事件，发现企业隐私数据被泄露行为，并及时预警。
- 更多功能，敬请期待！
- 更多功能，敬请期待！

接入用户

平安好贷 猫眼 艺龙 中国南方航空 网银科技 Lenovo 联想 NEYTEAM 202-193-7132 Dunsun.Com JD 京东 招财 爱奇艺

唯品会

合作厂商

# 四大金刚



## Github Scan

监控Github代码库，及时发现员工托管公司代码到Github行为并预警，降低代码泄露风险。



## 风险库

根据不同层面的恶意行为计算风险值，多年沉淀，千万级别手机号码库，帮助企业有效防御羊毛党。

## 军火库

监控常用软件漏洞发布，对存在POC的漏洞及时预警，帮助用户提早发现高风险安全漏洞。



## 天眼

跟踪最新互联网泄密事件，发现企业隐私数据被泄露行为，并及时预警。



# THANKS



乌云 WooYun



乌云白帽大会·2016  
不插电