点融网的一些安全实践

点融网高级安全工程师 李文吉

2016携程信息安全沙龙

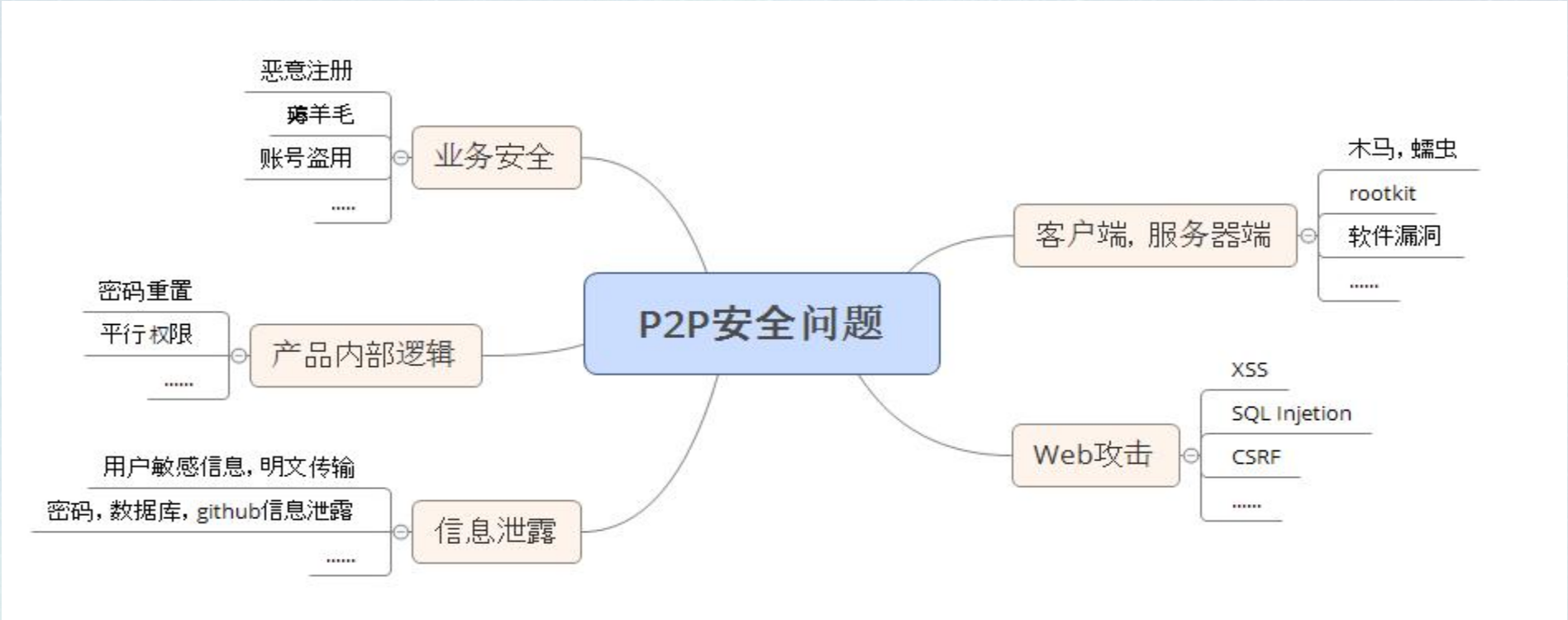
正在遭遇哪些威胁？

我们该怎么办？

点融在做的一些事...

正在遭遇哪些威胁？

P2P所遭遇的威胁


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

应用安全

- SQL注入
- 上传漏洞(getshell)
- 跨站脚本(XSS)
- 弱口令
- 无验证码或者验证码绕过
- 越权漏洞/平行权限
- 业务系统对公网开放
- 数据库未授权访问(mongodb)
- 第三方应用(wordpress, discuz)

DDOS/CC

来自
- 友商
- 敲诈

特点
- 低成本
- 低技术含量
- 高实效性

后果
- 用户流失
- 信誉下降

信息泄漏

- Github
- 非业务系统弱口令(Jira/Git/Mail)
- 默认口令
- 员工被社

业务欺诈

威胁

- 恶意注册
- 羊毛党(用户作弊)
- 恶意借款

影响

- 直接的经济损失

业务欺诈

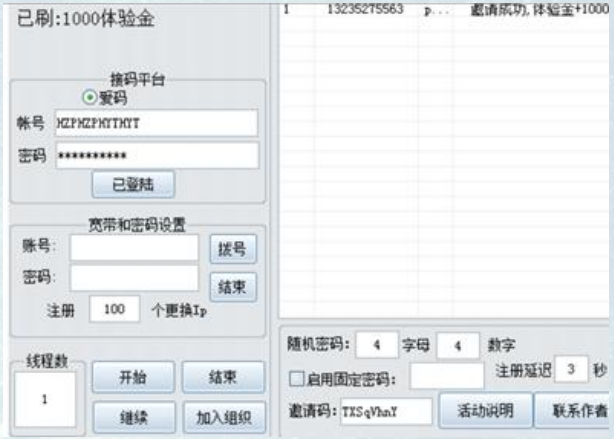
恶意注册

↓

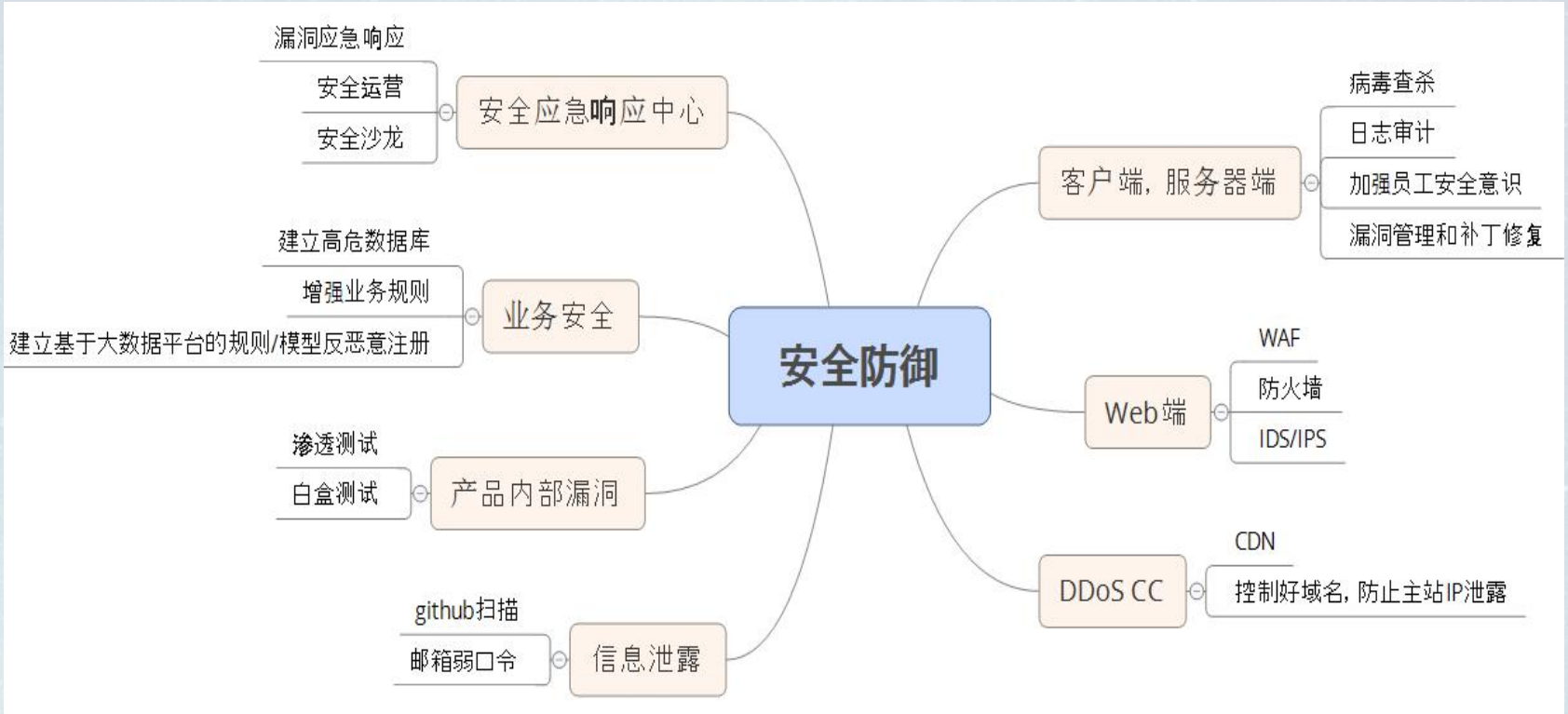
赚取奖励

↓

回收奖励



我们该怎么办？

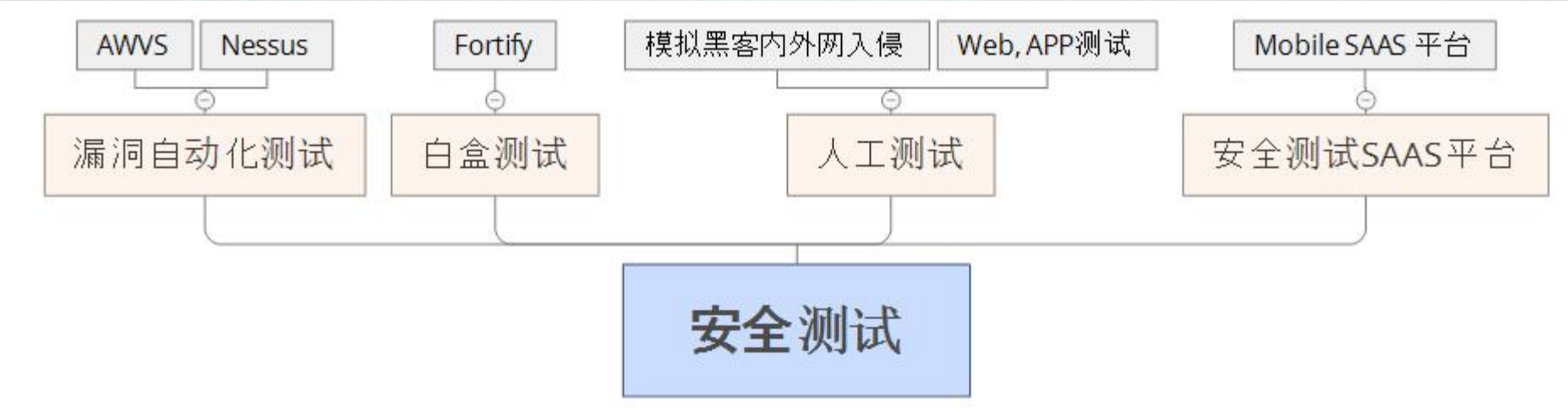

安全防御
安全应急响应中心
漏洞应急响应
安全运营
安全沙龙
业务安全
建立高危数据库
增强业务规则
建立基于大数据平台的规则/模型反恶意注册
产品内部漏洞
渗透测试
白盒测试
信息泄露
github扫描
邮箱弱口令
客户端，服务器端
病毒查杀
日志审计
加强员工安全意识
漏洞管理和补丁修复
Web端
WAF
防火墙
IDS/IPS
DDoS CC
CDN
控制好域名，防止主站IP泄露

面对传统的威胁

应用安全
- —WAF
- —渗透测试
- —代码审计

DDOS/CC
- —高抗设备
- —流量清洗

面对传统的威胁


AWVS
Nessus
Fortify
模拟黑客内外网入侵
Web, APP测试
Mobile SAAS 平台
漏洞自动化测试
白盒测试
人工测试
安全测试SAAS平台
安全测试

新的挑战

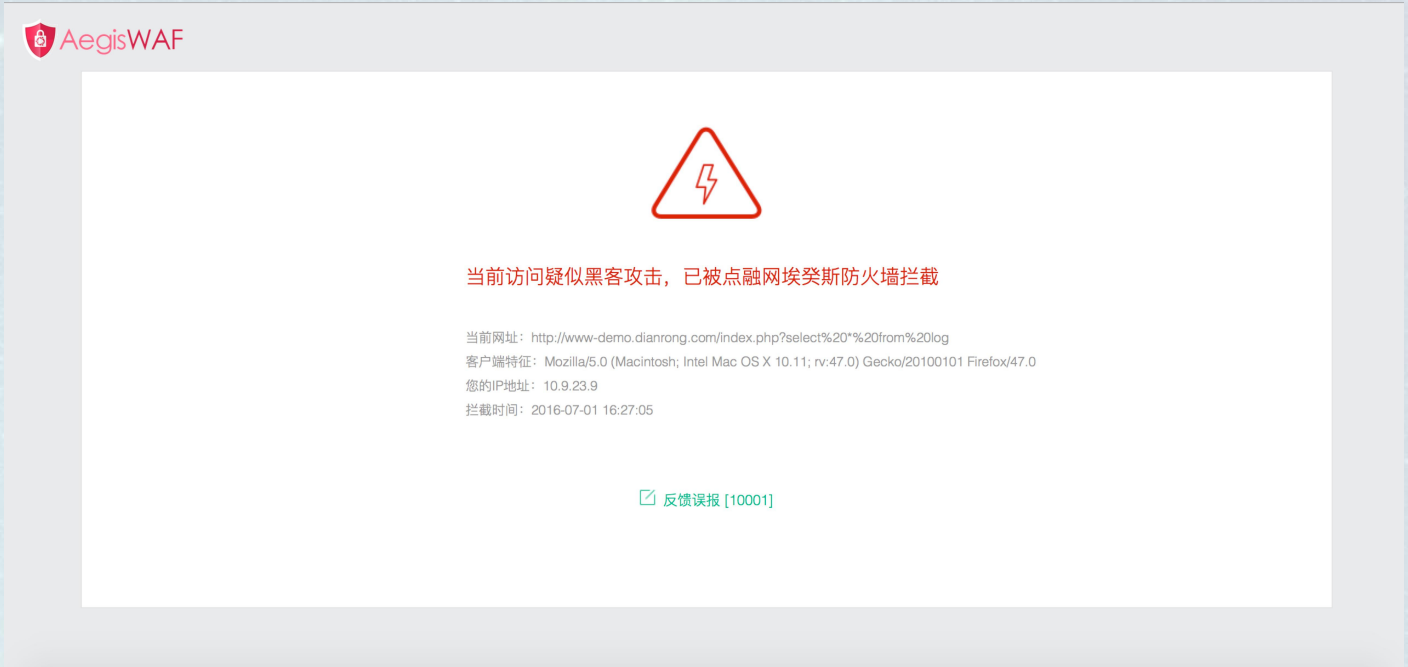
信息泄漏
- —Github爬虫
- —定期弱口令测试
- —定期员工安全培训

逻辑漏洞
- —渗透测试
- —白盒/黑盒测试

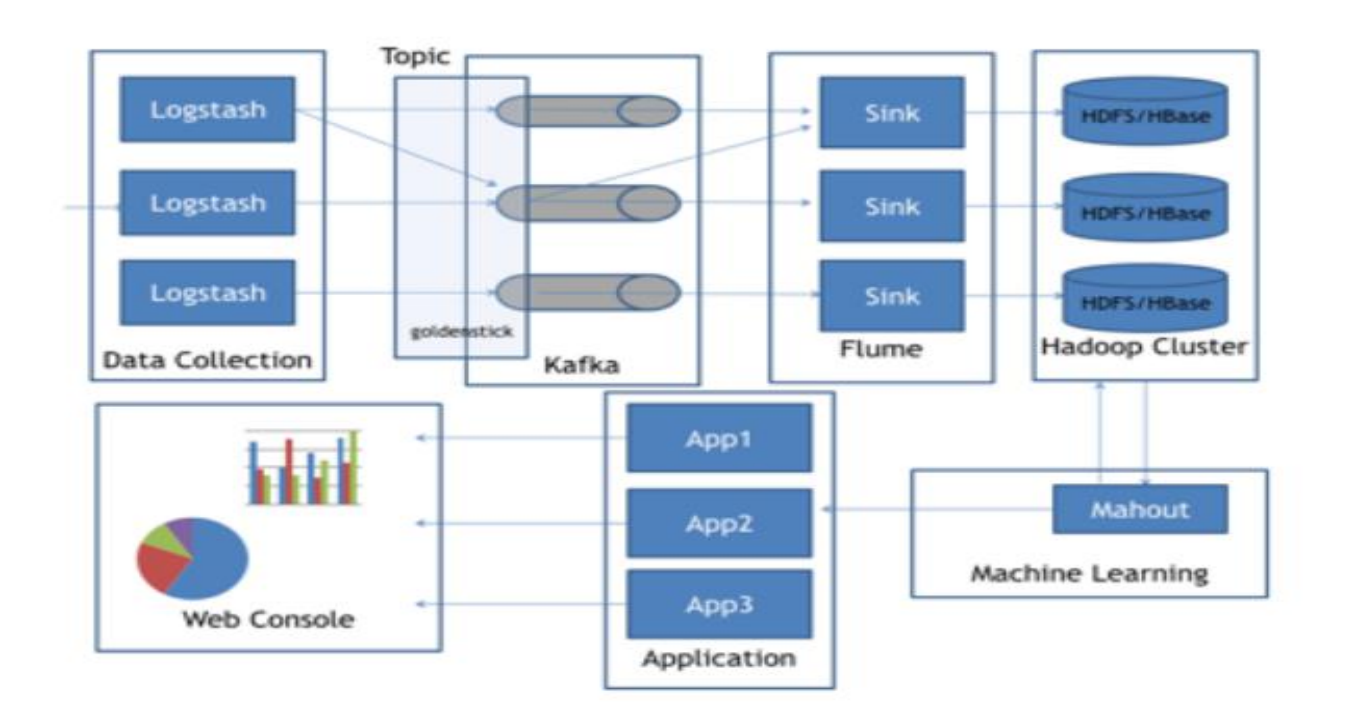
业务欺诈
- —建立反欺诈引擎

点融在做的一些事

Aegis WAF

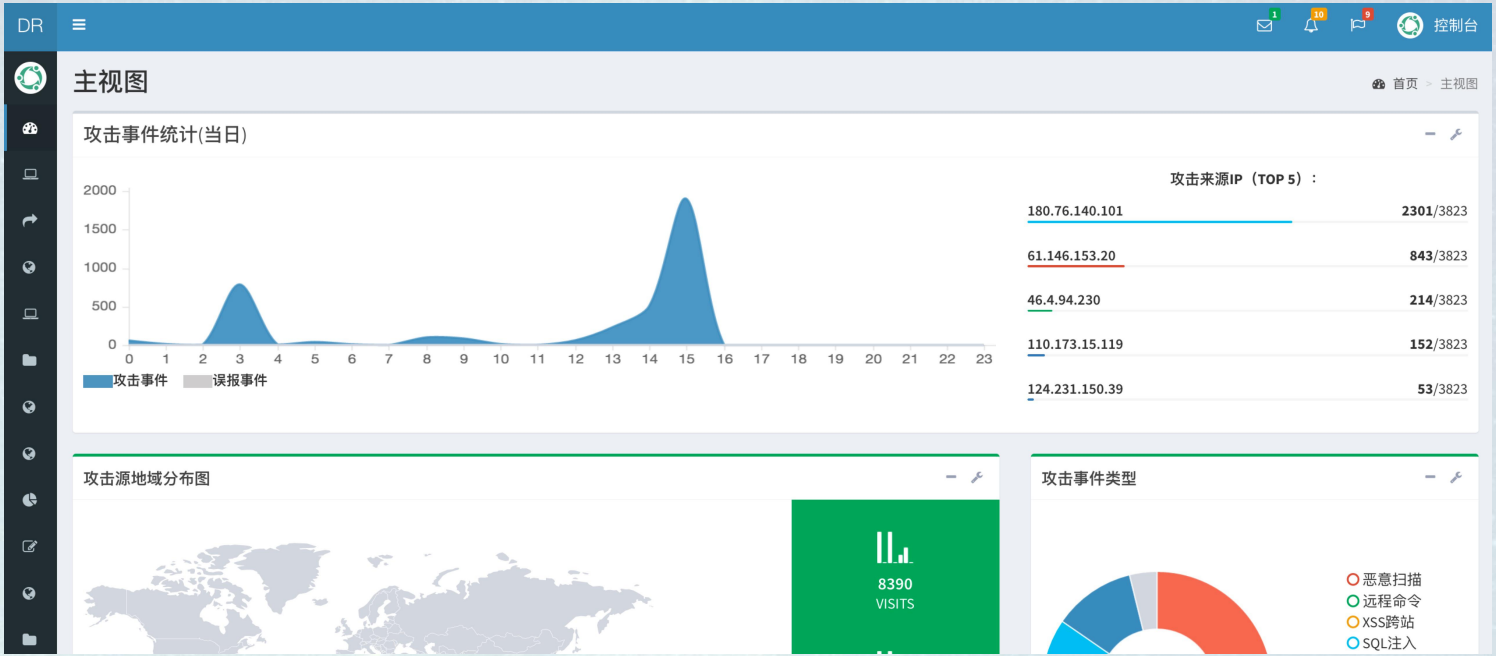

AegisWAF
当前访问疑似黑客攻击，已被点融网埃癸斯防火墙拦截
当前网址：http://www-demo.dianrong.com/index.php?select%20*%20from%20log
客户端特征：Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
您的IP地址：10.9.23.9
拦截时间：2016-07-01 16:27:05
反馈误报 [10001]

反欺诈(谛听系统)—基础计算平台

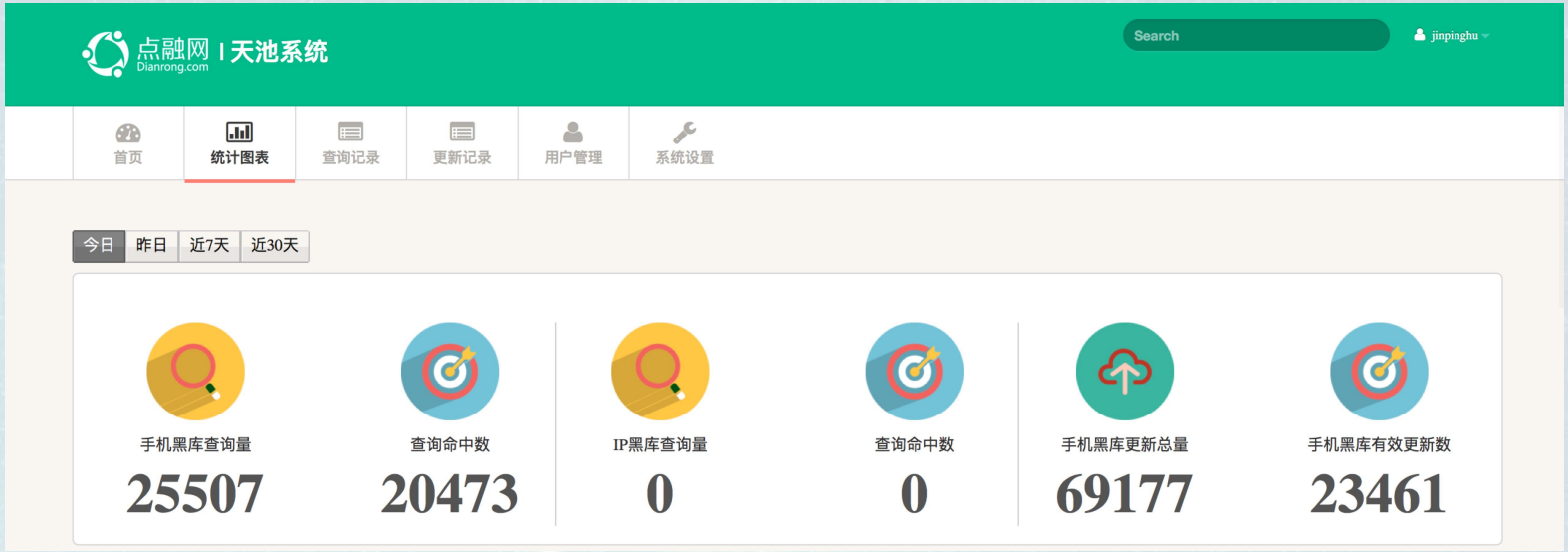


反欺诈(谛听系统)—建模逻辑

安全中心(SC)

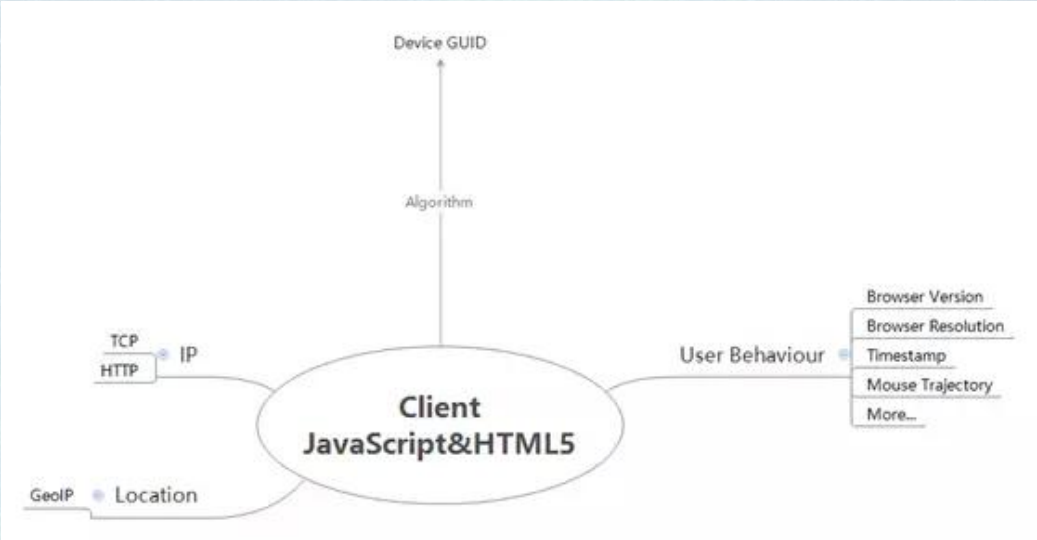

DR
控制台
主视图
首页 > 主视图
攻击事件统计(当日)
2000
1500
1000
500
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
攻击事件
误报事件
攻击来源IP（TOP 5）：
180.76.140.101 2301/3823
61.146.153.20 843/3823
46.4.94.230 214/3823
110.173.15.119 152/3823
124.231.150.39 53/3823
攻击源地域分布图
8390
VISITS
攻击事件类型
恶意扫描
远程命令
XSS跨站
SQL注入

反欺诈(谛听系统)—天池组件

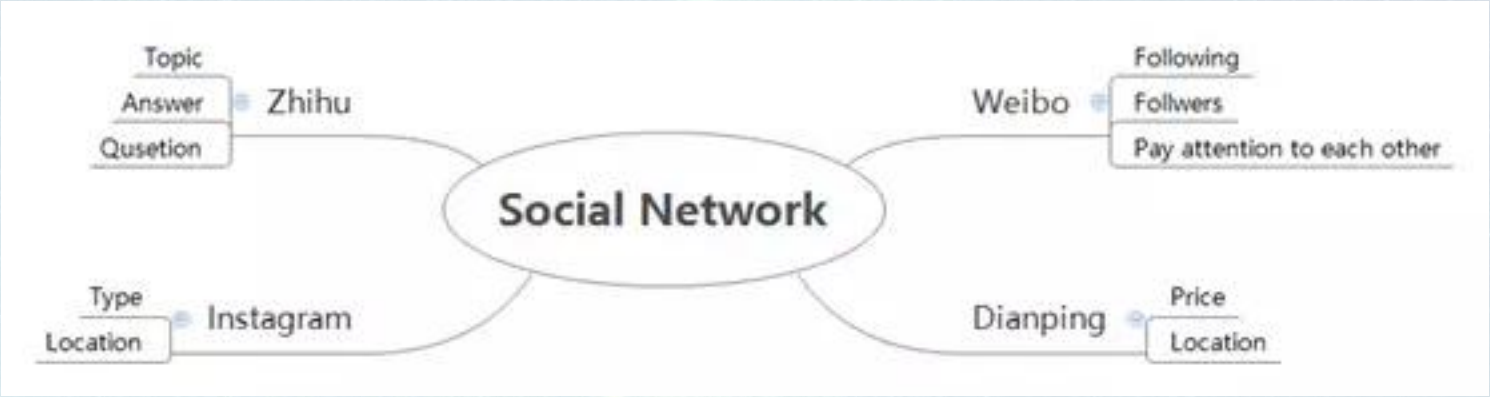


反欺诈(谛听系统)—天池组件

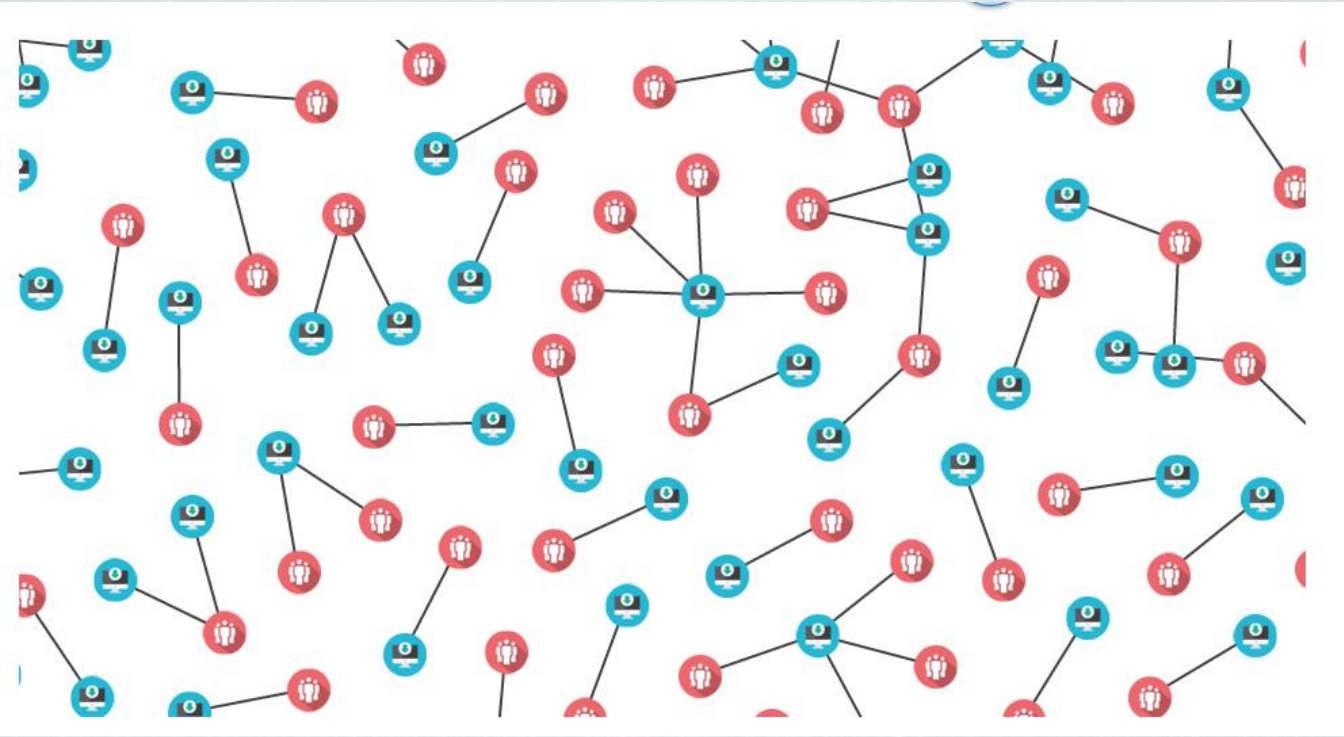
反欺诈(谛听系统)—客户端


Device GUID
Algorithm
TCP
HTTP
IP
GeoIP
Location
Client
JavaScript&HTML5
User Behaviour
Browser Version
Browser Resolution
Timestamp
Mouse Trajectory
More...

反欺诈(谛听系统)—社交关系图谱



反欺诈(谛听系统)—模型应用—异常用户



反欺诈(谛听系统)—规则引擎—单IP多次调用注册接口

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


THANKS
Q&A