

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？

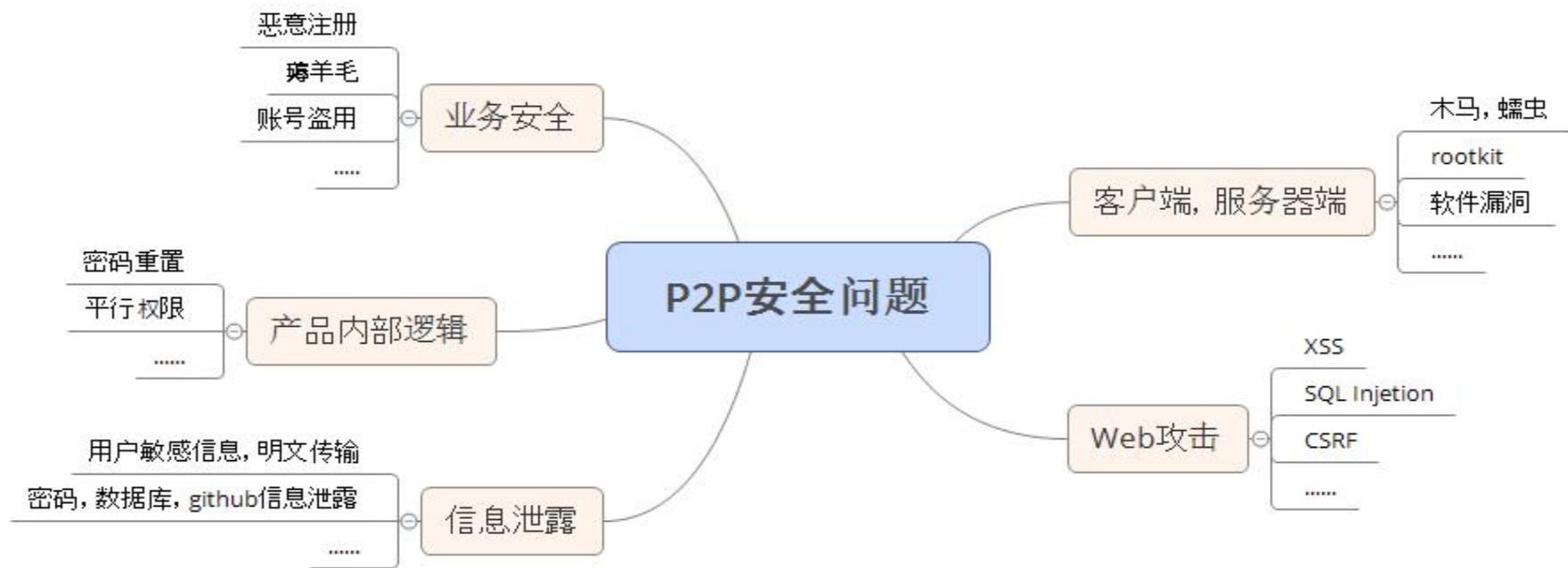
点融在做的一些事...



正在遭遇哪些威胁？



P2P所遭遇的威胁





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

已刷:1000体验金

1 13235275563 p... 邀请成功, 体验金+1000

接码平台
☒ 爱码

帐号: 9ZPKZPKYTHYT

密码: *****

已登陆

宽带和密码设置

帐号: [input] 拨号

密码: [input] 结束

注册 100 个更换IP

线程数

1 开始 结束 继续 加入组织

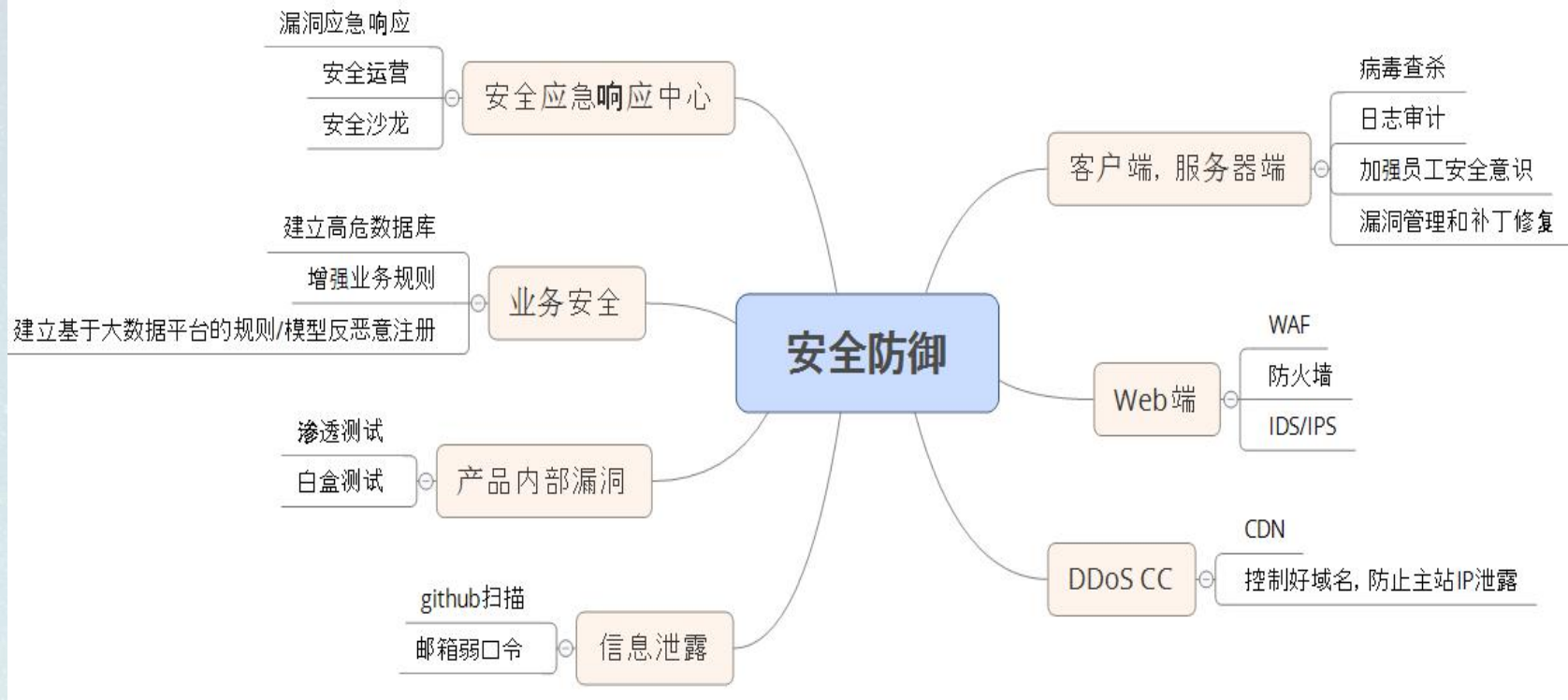
随机密码: 4 字母 4 数字

☐ 启用固定密码: [input] 注册延迟 3 秒

邀请码: TKSqVhaY 活动说明 联系作者



我们该怎么办？





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





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



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

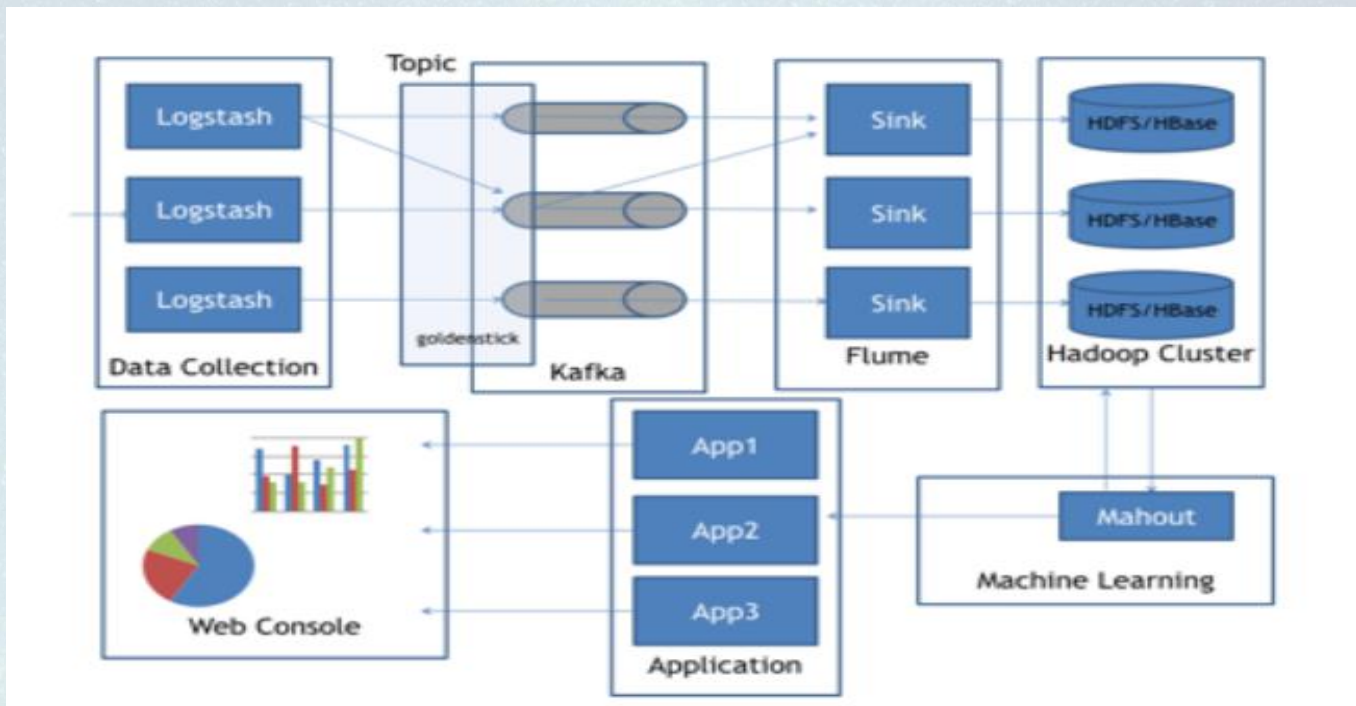
您的IP地址：10.9.23.9

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



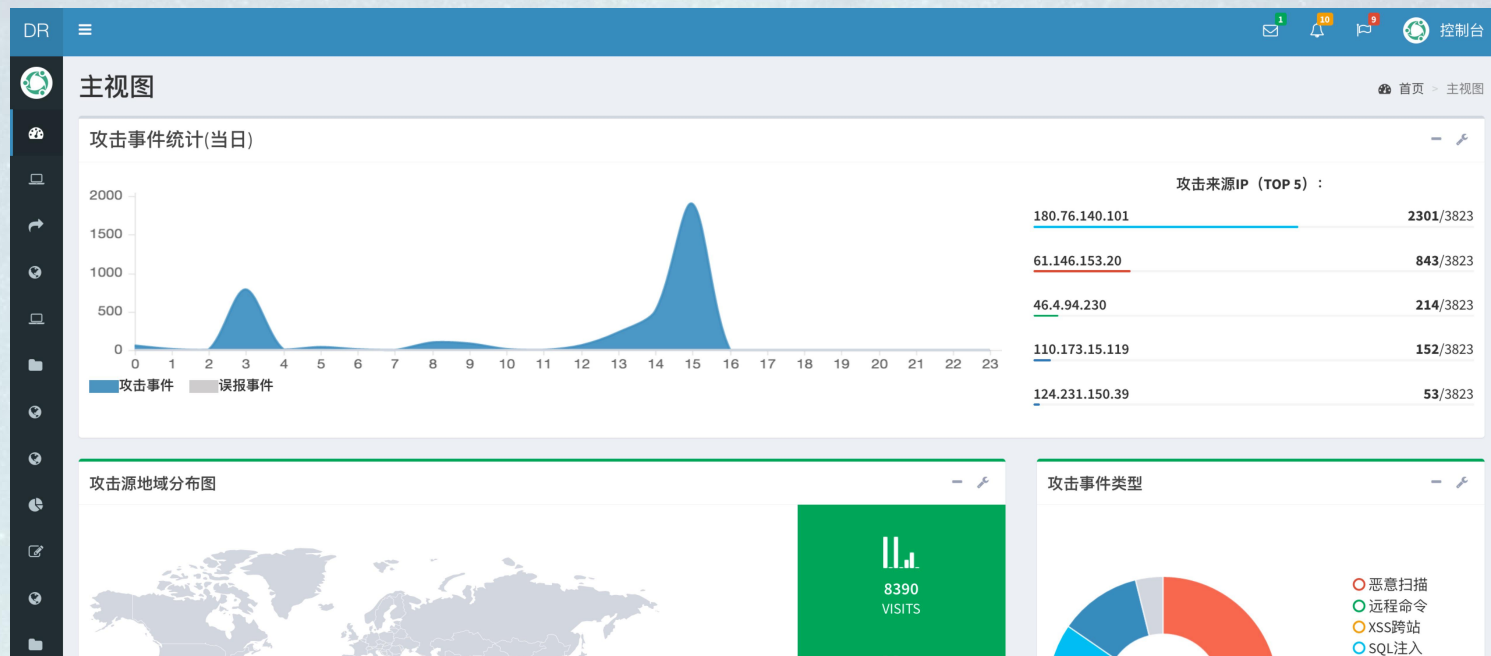


反欺诈(谛听系统)一建模逻辑



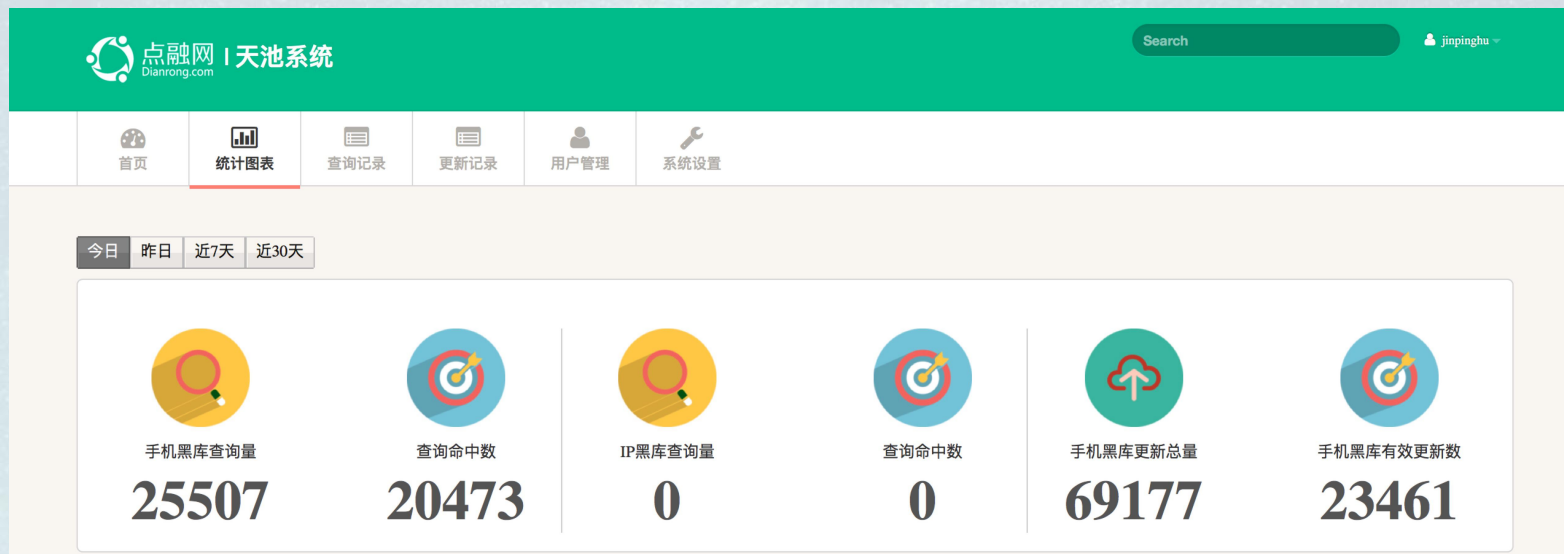


安全中心(SC)





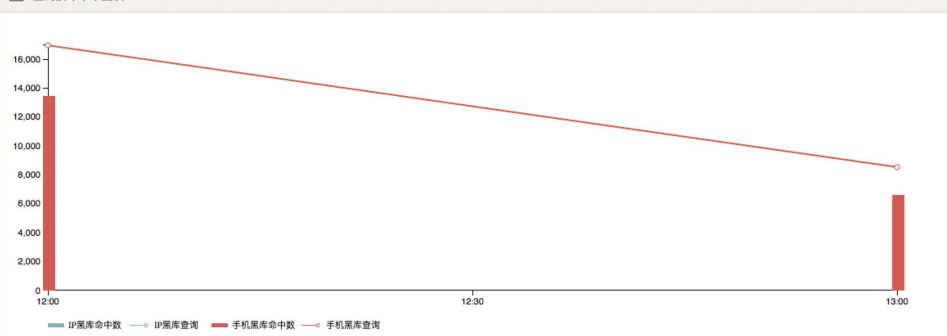
反欺诈(谛听系统)一天池组件



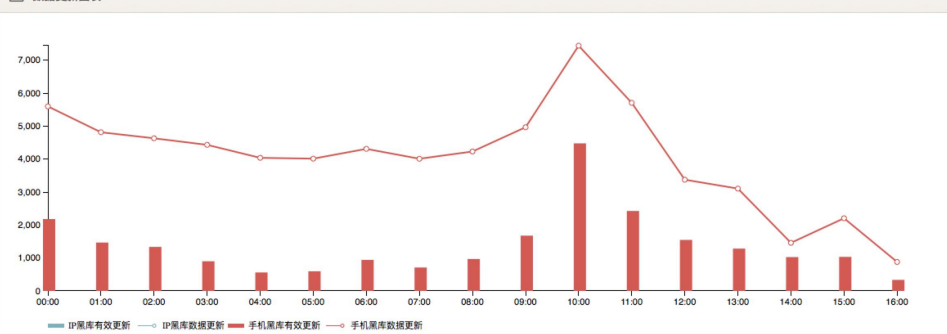


反欺诈(谛听系统)一天池组件

查询及命中率图表

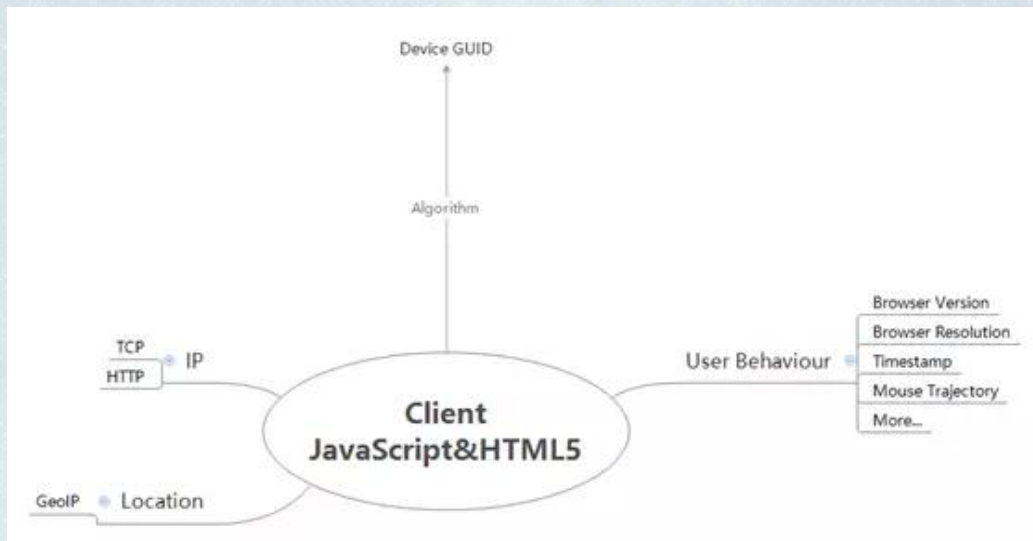


数据更新图表



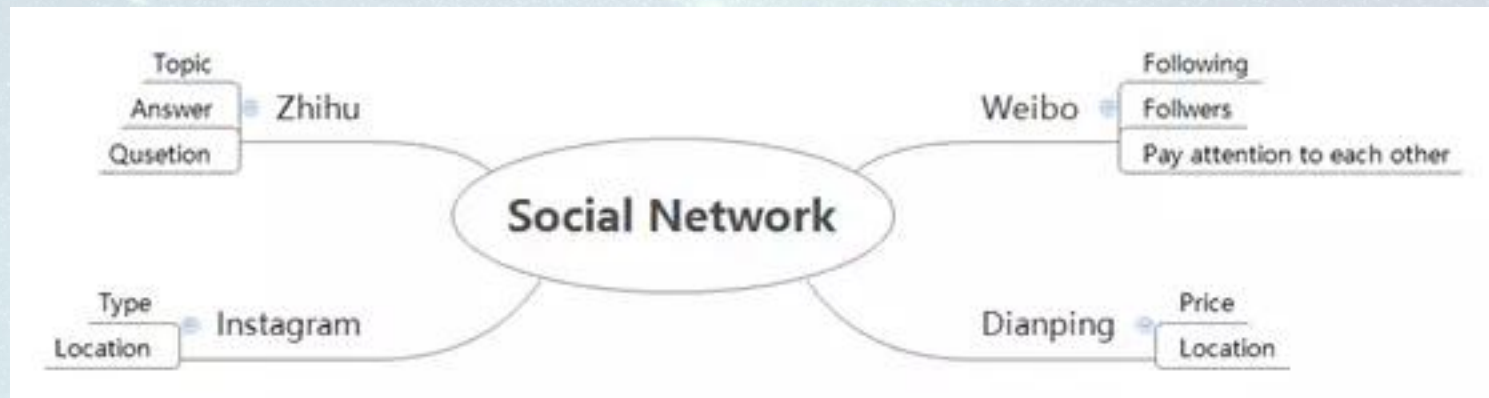


反欺诈(谛听系统)-客户端



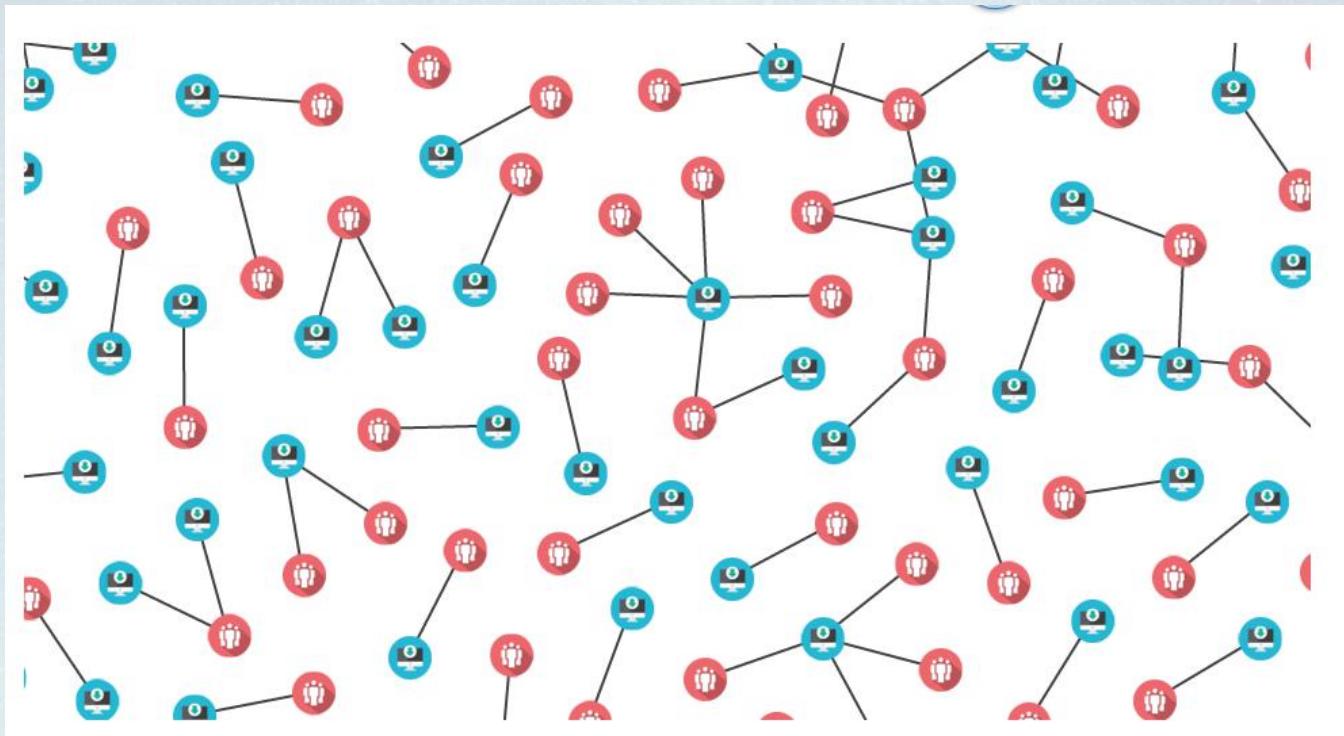


反欺诈(谛听系统)-社交关系图谱





反欺诈(谛听系统)一模型应用一异常用户





反欺诈(谛听系统)一规则引擎一单IP多次调用注册接口

DASHBOARDS			ANALYSIS		ENVIRONMENT		REPORTS	
	11 hours			WebServer Attack	Common web attack	1		114.5
	11 hours			C&C Communication	Username(phone number) detection API	1		113
	11 hours			C&C Communication	Username(phone number) detection API	1		117
	11 hours			C&C Communication	Username(phone number) detection API	1		115
	11 hours			C&C Communication	Username(phone number) detection API	1		115
	11 hours			C&C Communication	Username(phone number) detection API	1		115
	11 hours			C&C Communication	Username(phone number) detection API	1		115
	12 hours			C&C Communication	User Login API	1		115
	02:30:29	open		C&C Communication	Username(phone number) detection API	1		115
	02:06:20	open		C&C Communication	Username(phone number) detection API	1		115
	02:03:32	open		C&C Communication	Username(phone number) detection API	1		115
	01:17:29	open		WebServer Attack	Common web attack	1		114.5



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

The background is a deep teal and blue space scene. It is filled with numerous small, bright white stars of varying sizes. A prominent comet with a long, bright yellow-green tail streaks diagonally across the lower half of the image, pointing towards the bottom left. The overall texture is grainy, giving it a cosmic, high-tech feel.

THANKS
Q&A