

十面埋伏

-论大数据风控技术体系的构建

张新波 同盾联合创始人&技术VP

▪ 关于



中生代技术
FRESHMAN TECHNOLOGY



同盾科技
www.tongdun.cn

IT大咖说

• 同盾

- 国内领先的第三方大数据风控服务商
- 服务的客户数5000+，其中信贷类客户2500+
- 日均调用量4000万+，其中借款量300万+

• Me

- 2009年加入阿里巴巴AliExpress，从零开始参与建设国际支付风控体系
- 先后参与并负责AE、国际站、中文站、集团安全部的多个风控系统的建设
- 2013底参与创办同盾科技，从零开始打造了国内最大的独立第三方风控体系

- 两个捕头和一个歌姬的三角恋？



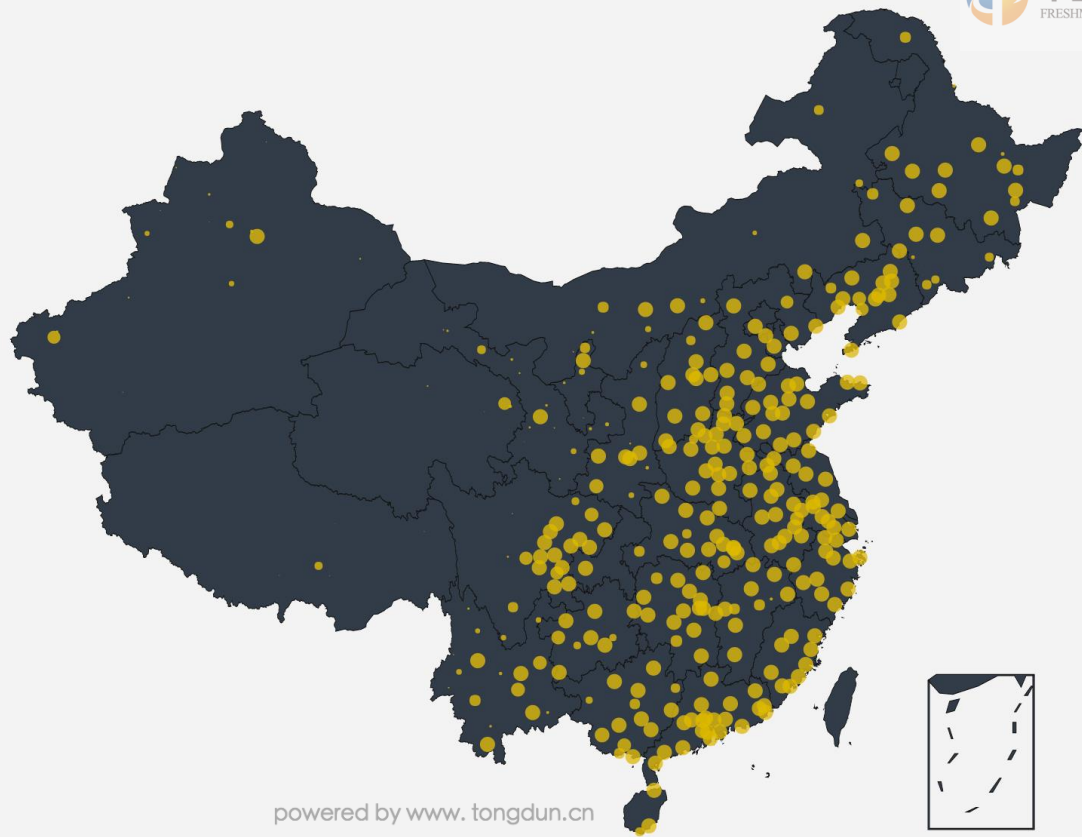
- 中国十大之一的琵琶曲？



- 楚汉争霸的垓下之战！！



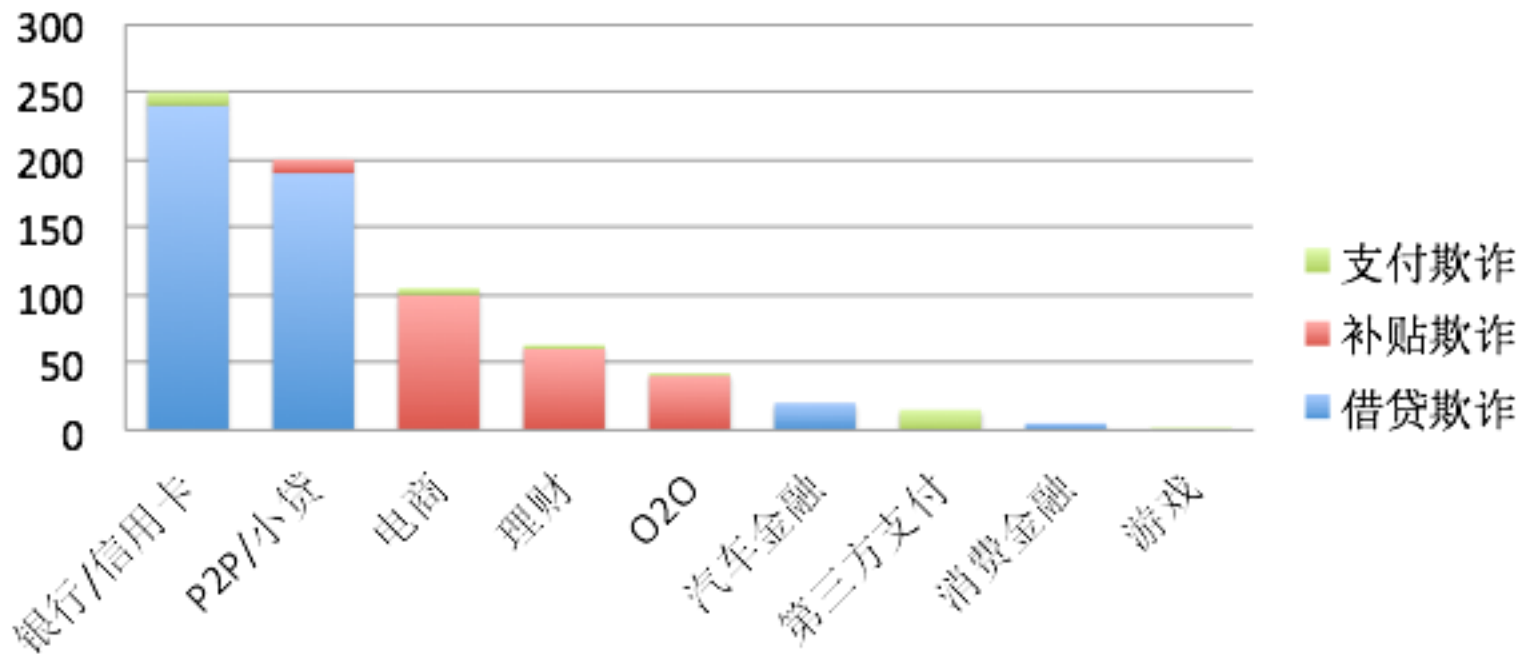
- 地下黑产猖獗，欺诈分布广泛



powered by www.tongdun.cn

■ 欺诈行业分布

2015年11个行业欺诈统计分布



欺诈损失~700亿人民币，增速~50%

■ 十面埋伏，围而歼之



中生代技术
FRESHMAN TECHNOLOGY

同盾科技
www.tongdun.cn

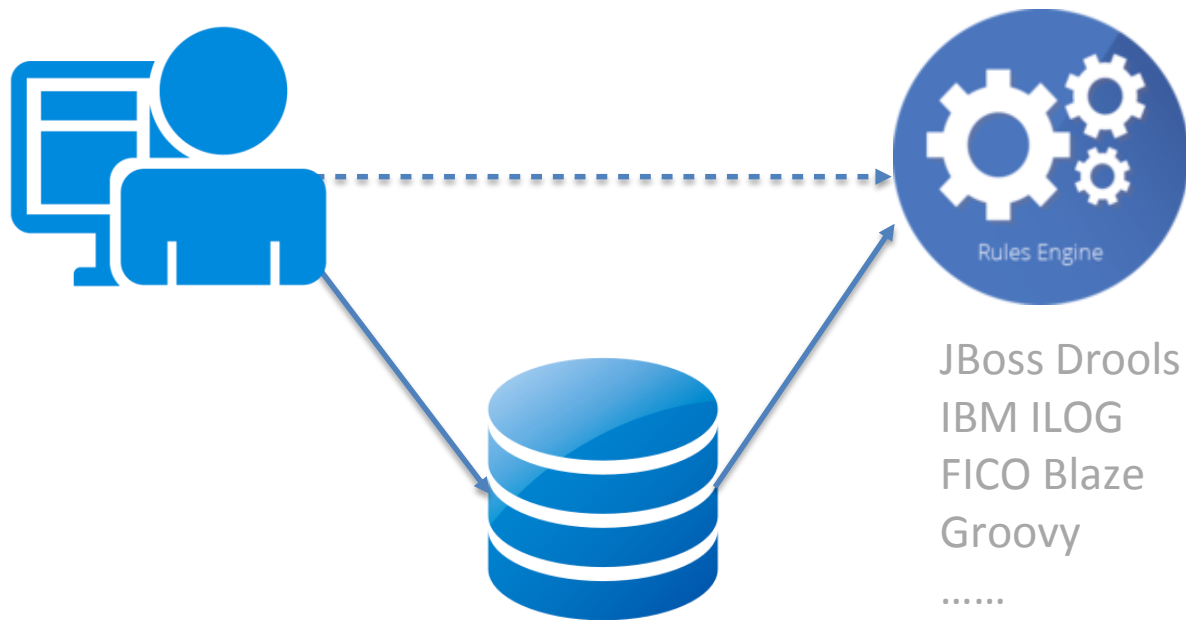
IT大咖说



▪ 决策引擎



中生代技术
FRESHMAN TECHNOLOGY



[编号:55610] 登录IP命中攻击性IP证据库

[编号:55612] 使用HTTP代理进行登录

[编号:55614] 使用SOCK4_5代理进行登录

[编号:55616] 使用VPN代理进行登录

[编号:55618] 登录设备标示缺失异常

[编号:55620] 登录IP与真实IP城市不匹配

[编号:55622] 在凌晨1点到5点进行登录

[编号:55624] 沉默账户登录

[编号:55626] 设备或账户两次登录的时间间隔极短

[编号:55628] 设备或账户短时间移动的位置距离异常

■ 经验总结



中生代技术
FRESHMAN TECHNOLOGY



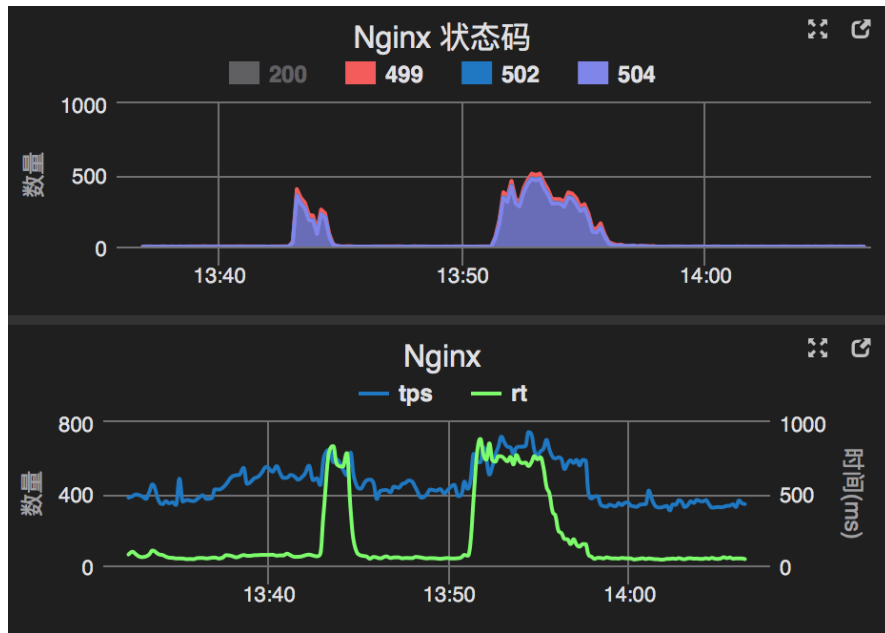
- 规则的可视化编辑能极大提升运营效率
- 规则变更实时生效可以快速应对风险的变化
- 针对不同的风险类型，需要配置不同的规则集
- 信贷等复杂场景需要支持复杂入参、决策流、决策表等高级功能
- 规则测试很重要但实现起来也比较复杂
- 历史数据按不同维度进行聚合存储，方便查询
- 规则配置的灵活性和处理性能是一对矛盾体
- 规则量太大时，单机已无法加载，需要进行集群拆分和路由处理
- 执行引擎用Drools、Groovy等差别不是很大，性能不在表达式执行本身
- 对第三方风控，需做好多租户支持并进行用户间的相互隔离

实时计算

- 秒杀、大促等高并发场景性能挑战很大
- 实时查询历史数据并计算
 - 网络IO压力过大
 - 延迟过高
- 数据预先分片聚合降低数据查询量
 - 流计算框架
 - STORM
 - SPARK STREAMING
 - 按时间片聚合
 - 合并计算
 - 增量计算



中生代技术
FRESHMAN TECHNOLOGY

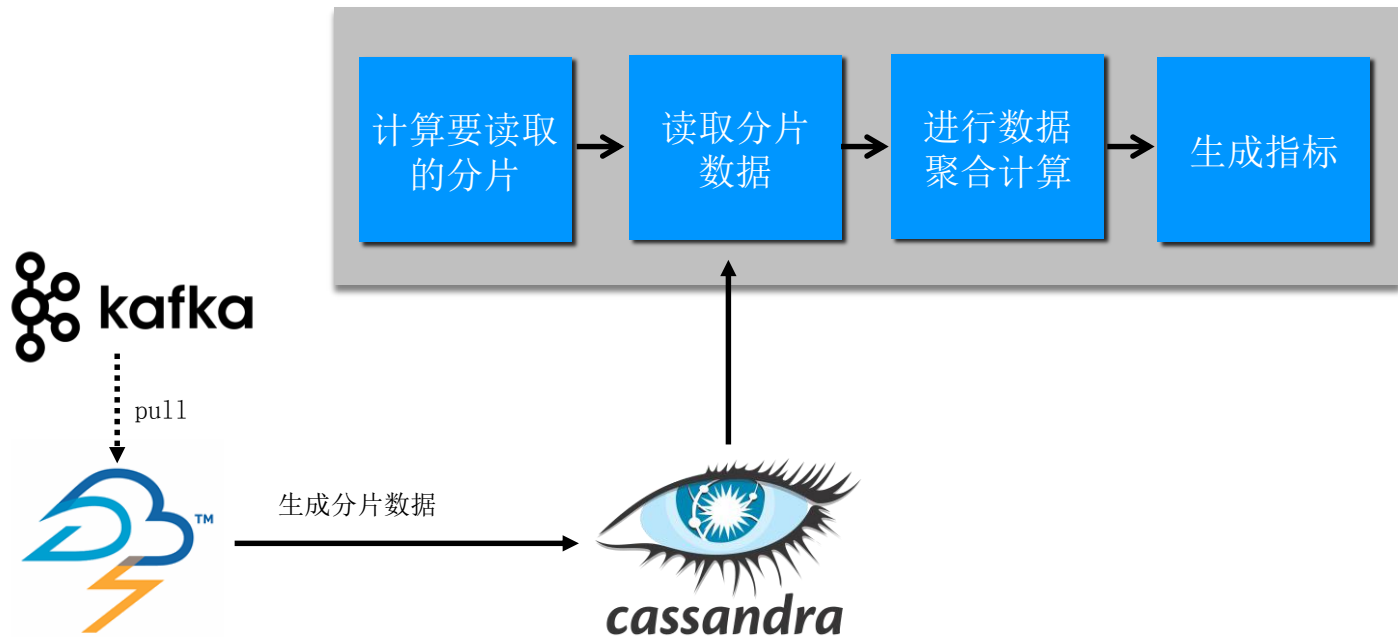


基本架构



中生代技术
FRESHMAN TECHNOLOGY

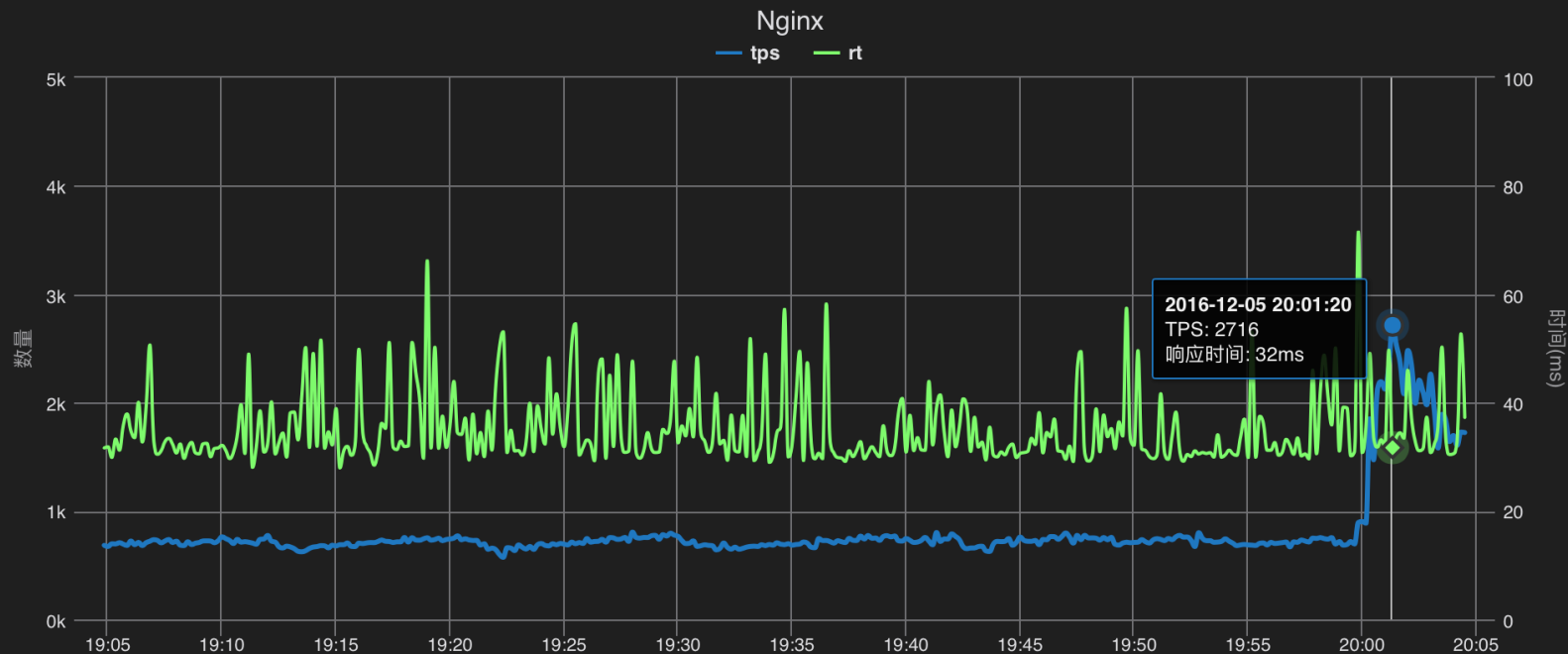
同盾科技
www.tongdun.cn
IT大咖说



■ 使用后的效果

Nginx

● 最近1小时 ● 最近3小时 ● 最近6小时 ● 最近12小时 ● 最近24小时 ● 最近3天 ● 最近7天



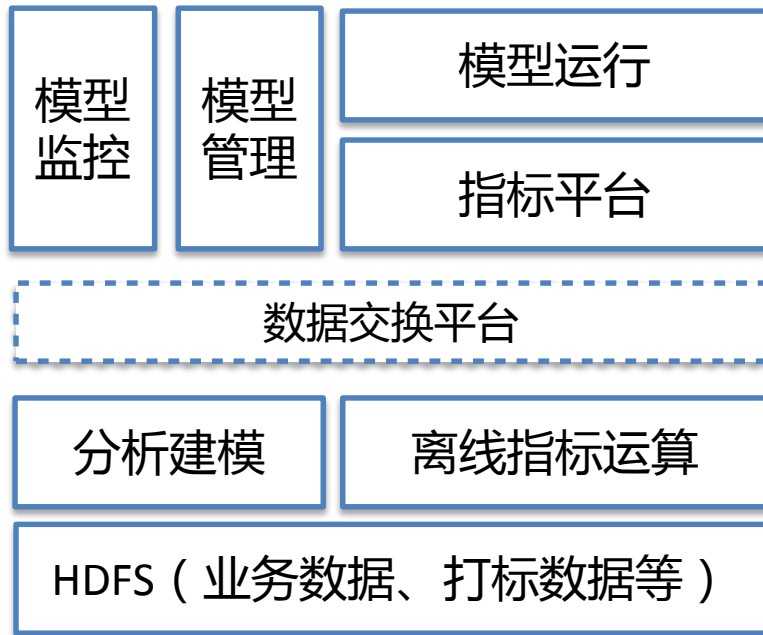
■ 模型平台



中生代技术
FRESHMAN TECHNOLOGY



- 模型常用的算法
 - 逻辑回归
 - 决策树
 - 随机森林
 - 神经网络
 - SVM
 - 深度学习
- 编程语言的支持
 - PMML
 - Java
 - Python



中生代技术
FRESHMAN TECHNOLOGY

- | 设备精准ID | 事件时间 | 注册手机 | 手机归属省份 | 来源ip | 来源ip归属省 |
|--------------------|-----------------|-------------|--------------|-----------------|---------|
| b37ef4f2ad5beb8dbd | 3/30/2016 12:38 | 13202849135 | 广东省 | 27.50.137.27 | 河南省 |
| | 3/30/2016 12:40 | 13129023054 | 广东省 | 115.47.36.209 | 北京市 |
| | | | | 115.47.36.209 | 北京市 |
| | | | | 182.125.151.228 | 河南省 |
| | 3/30/2016 12:42 | 13245826641 | 江苏省 | 115.62.89.239 | 河南省 |
| | 3/30/2016 12:44 | 18219171691 | 广东省 | 115.47.36.209 | 北京市 |
| | | | | 118.26.117.112 | 山东省 |
| | | | | 171.15.71.244 | 河南省 |
| 3/30/2016 12:45 | 18319994083 | 广东省 | 115.28.83.30 | 山东省 | |

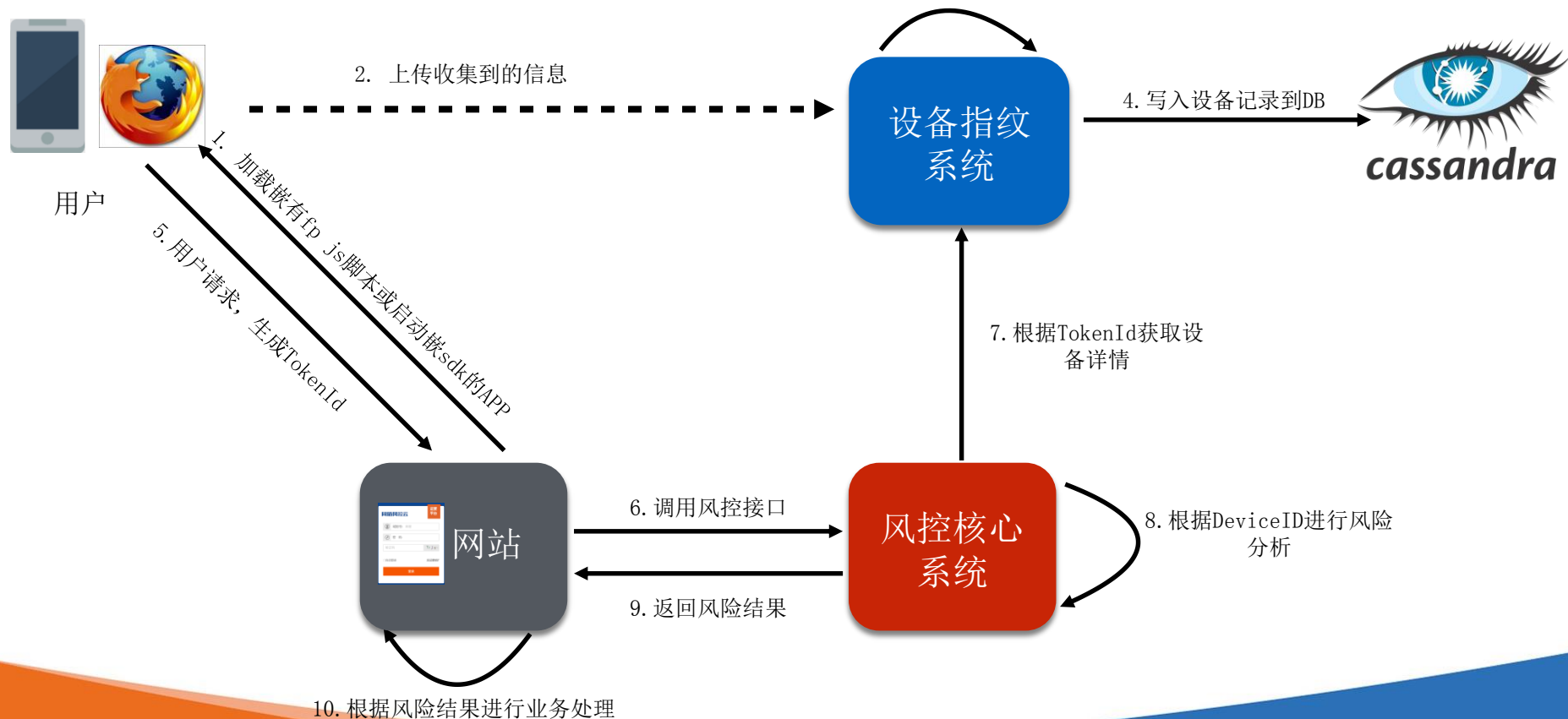
设备指纹的基本原理



中生代技术
FRESHMAN TECHNOLOGY

同盾科技
www.tongdun.cn

IT大咖说



IP画像

IP画像报告



IP地址

183.129.232.234

详细信息

类型: 企业办公网络

端口: 22,443

程序: SSH,SSL,VPN

位置: 中国, 浙江 杭州滨江区 海创园(30.2936,120.1614)

网络类型: 电信骨干网络, 静态地址

组织信息: 暂无



WHOIS信息

更新时间: 2019年11月29日

注册人: CHINANET-ZJ Zhongxin node network

注册组织: CHINANET-ZJ-ZX

国家和地区: China

电子邮箱: antispam@ch.hz.zj.cn

ASN编号: AS4134

AS Path: 4134

风险事件历史

风险类型	来源	威胁评分	时间
机器人登录	漏洞命中-机器人登录识别	80	2018-05-12 11:48:34
垃圾注册	漏洞命中-机器人登录识别	20	2018-05-12 11:48:34
垃圾注册	漏洞命中-机器人登录识别	80	2018-05-12 11:48:34
漏洞	漏洞命中-识别	80	2018-05-12 11:48:34
垃圾注册	漏洞命中-垃圾登录识别	80	2018-05-12 11:48:34

第三方情报

类型	来源	威胁评分	时间
web攻击	IBM	80	2018-05-12 11:48:34
木马程序	公开渠道	20	2018-05-12 11:48:34
木马程序	Brexit	80	2018-05-12 11:48:34
垃圾邮件	CTX	80	2018-05-12 11:48:34
钓鱼	IBM	80	2018-05-12 11:48:34

代理检测

类型	端口	首次出现时间	最后出现时间
VPN	1723	2018-05-12 11:48:34	2018-05-12 11:48:34
HTTP	8080	2018-05-12 11:48:34	2018-05-12 11:48:34

域名历史

类型	端口	首次出现时间	最后出现时间
VPN	1723	2018-05-12 11:48:34	2018-05-12 11:48:34
HTTP	8080	2018-05-12 11:48:34	2018-05-12 11:48:34

■ IP模拟器



■ 地址服务

- 地址标准化
 - 国家/省/市/区县/乡镇街道/道路...
- 地址模糊匹配
- 地址真实性验证
- 地址分团
- 地址画像



福建福州市连江县 10区贵安新天地慕尔鸣东路737号太阳国际公馆2号楼2102	表
福建福州市连江县 15区贵安新天地丁香中路267号华夏花园2号楼1302	043680
福建福州市连江县 17区贵安新天地吉雪北路905号黛珍棋牌室	043680
福建福州市连江县 19区贵安新天地蒙自西路773号嘉融玩具超市	043680
福建福州市连江县 23区贵安新天地丽园北路729号澜黛西饼屋	043680
福建福州市连江县 26区贵安新天地西爱威斯中路89号卡布其诺8栋2101	043680
福建福州市连江县 32区贵安新天地雷上达东路451号朝阳新城8号楼2203室	043680
福建福州市连江县 39区贵安新天地华达北路736号城市月光8号楼2001室	043680
福建福州市连江县 46区贵安新天地安和寺东路861号国瑞城2号楼2303	043680
福建福州市连江县 66区贵安新天地颛桥南路406号威海翠海明珠小区2号楼1203	043680
福建福州市连江县 74区贵安新天地富锦西路407号林顺汽车服务中心	043680
福建福州市连江县 76区贵安新天地深圳迎春北路148号华贸中心4栋1301室	043680
福建福州市连江县 81区贵安新天地湖滨北路895号澜畔湘菜馆	043680
福建福州市连江县 83区贵安新天地建安一路753号政国理发店	043680
福建福州市连江县 第15区贵安新天地大冲路261号月亮城堡7栋1502	043680
福建福州市连江县 第15区贵安新天地茭白园西路114号辉士休闲吧	043680
福建福州市连江县 第17区贵安新天地昙花庵北路775号东方太阳城4号楼2402室	043680
福建福州市连江县 第19区贵安新天地迎宾东路885号风格与林6号楼1702	043680
福建福州市连江县 第1区贵安新天地双菱东路346号顶秀青溪5幢1501室	043680
福建福州市连江县 第26区贵安新天地茄勒北路994号谦茂粤菜馆	043680
福建福州市连江县 第28区贵安新天地青年中路496号回龙湾8号楼1601室	043680
福建福州市连江县 第2区贵安新天地茂海路591号翔胜大饭店	043680
福建福州市连江县 第36区贵安新天地环镇南路440号枫晶大饭店	043680
福建福州市连江县 第43区贵安新天地爱国西路985号枝墨酒吧	043680
福建福州市连江县 第53区贵安新天地怀德北路428号鸣波茶业店	043680
福建福州市连江县 第56区贵安新天地永嘉北路324号影宁音响专卖店	043680
福建福州市连江县 第60区贵安新天地南京东路651号义若玩具超市	043680
福建福州市连江县 第67区贵安新天地保德北路677号心庆西餐厅	043680
福建福州市连江县 第72区贵安新天地江宁中路440号东润枫景3号楼1002室	043680
福建福州市连江县 第82区贵安新天地东兰中路614号航伟茶餐厅	043680
福建福州市连江县 第82区贵安新天地卡德西路921号汤泉逸墅2幢2002	043680
福建福州市连江县 第97区贵安新天地黄金南路180号新城国际7号楼1101	043680
福建福州市连江县 第97区贵安新天地通济东路298号世纪城3幢1503室	043680

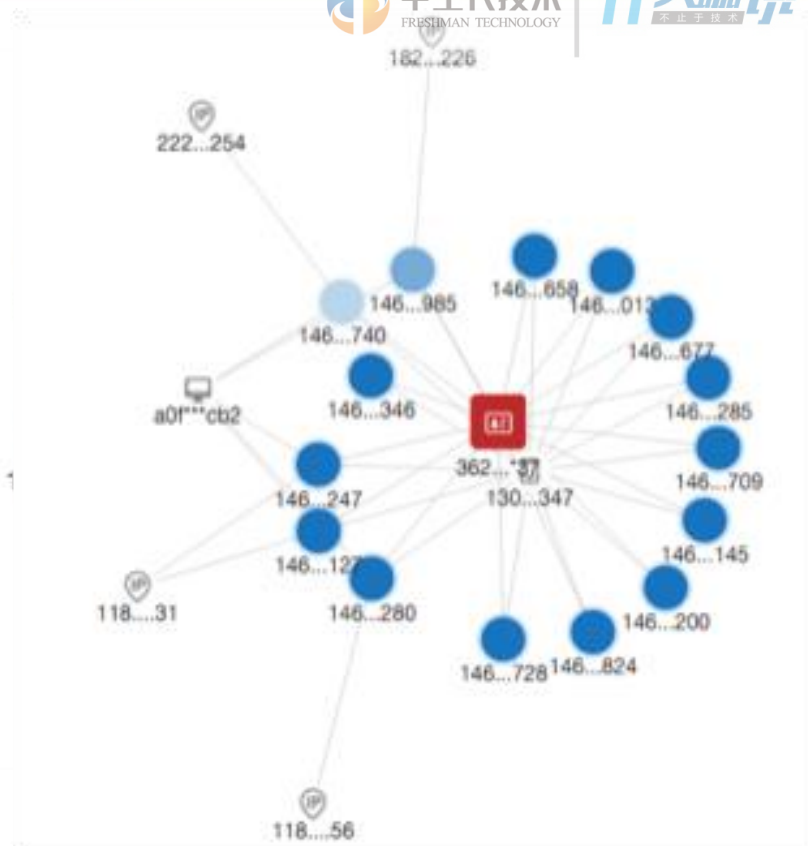
■ 复杂网络

- 通过设备、IP、手机号、身份证号、地址等多个维度建立不同主体之间的关联关系
- 打通信贷、理财、电商、支付、航旅、租赁等不同行业数据，彻底实现联防联控
- 提供数据挖掘与分析工具，方便风险核查
- 嵌入到风控决策流程，实时进行风险决断



团伙作案

- 通过对嫌疑的用户信息的周边进行关联调查，找出关联作案团伙。
- 在复杂网络输入手机号130****2347
- 关联查询展示出来事件都是借款事件，且都是拒绝的，事件关联身份证命中信贷逾期名单



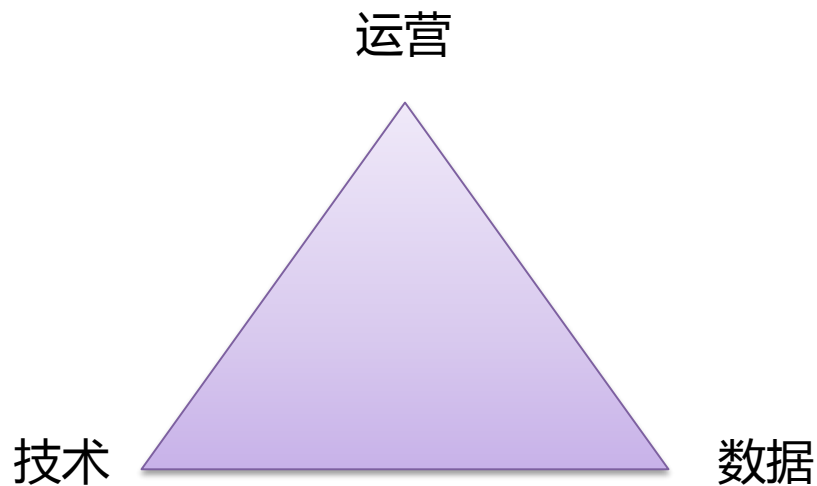
- 总结



中生代技术
FRESHMAN TECHNOLOGY

同盾科技
www.tongdun.cn

IT大咖说
不止于技术



跨行业联防联控

THANKS

