企业SaaS安全服务的瑞士军刀
---携程安全SaaS之路

凌云

目录

路的起点

楔子1

艺龙遭到黑客攻击，希望更方便的使用到携程已有的一些安全产品

楔子2

行业内黑名单数据交换，需要一个较好的互换机制和渠道

楔子3

乙方产品不接地气，造一些轮子给没有开发能力的甲方使用

谷歌、Facebook、雅虎共享IP黑名单

发布时间：2015-07-26 16:58:00 来源：论坛 作者：红黑联盟 dawner A+ A-

关键字：facebook 谷歌 新闻 雅虎

网络欺诈，尤其是广告欺诈行为很是令人恼火。近日网络科技巨头Google、Facebook、Yahoo公司携手启动了一个新计划，阻止黑名单中IP地址刷web流量。

谷歌将利用IP黑名单过滤爬虫机器人

现在的网络环境中，大部分数据中心流量都是非法流量或机器爬虫产生的。为了遏制这个问题，Trustworthy Accountability Group(TAG)宣布启动一项计划，利用Google内部数据中心的IP黑名单去过滤爬虫机器人。

Google的广告经理Vegard Johnsen表示，这个新的试点项目将使用黑名单过滤掉网络流量机器人和僵尸爬虫，这能减少数据中心很大一部分冗余流量。

像Google这样的科技大公司们都有自己的黑名单，上面列有计算机系统数据中心上可疑的IP地址，这些可疑IP地址会伪装成自然人点击广告等赚取流量费用。Google仅在5月份就阻止了将近8.9%的流量。

平台介绍

地址： https://security.ctrip.com

让我们一起做一些互联网公司喜欢的安全小工具

平台介绍

累计接入企业150+　核心活跃 40+

信息安全SaaS之路

创建历程

Github scan、风险库上线

2016.1.6

军火库上线

2016.3.31

天眼上线

2016.4.20

2015.12.9

启动立项

30+

2016.3.1

90+

2016.4.6

150+

2016.5.7

Github Scan

当前位置：WooYun >> 搜索结果

搜索关键字：github （共 772 条纪录） 将未公开漏洞纳入搜索结果

BUS365官方邮箱密码泄露40W+已发送邮件（姓名/身份证/手机号码/座位号/取票码等）

不知道重没重...https://github.com/chuanwang1993/hello-world/blob/24f3bd69cd7cf793c510689233b1b7a18af9ab1c/bus365mngr/conf/applicatio
mtp.bus365.com mail.smtp.user=bus365@bus365.com mail.smtp.pass=2013bus84365 mail.smtp.channel=smtp 可登陆 已发送邮件中，都是这样
... ...改密码, 来个20Rank吧

提交日期：2016-05-05 作者：路人甲

通卡网络账某处信息泄露（十多G数据数千万条数据）

...https://github.com/lifangzhen/BackEnd/blob/fdf273dca1e734157703e8
录 mongo未授权访问,无需输入账号跟密码 <mask>*******</mask> 十多G
享，到现在还没改密码，这可不行 求20Ra...

提交日期：2016-05-04 作者：路人甲

疑似众安保险某站源码泄露/数据库可直连/大量敏感信息

众安保险某站源码泄露/数据库可直连/大量敏感信息...code 区域https://gith
588bd4db7c2e0f750567743/src/main/resources/deploy.properties code
#database.user=root #database.password=Kingsley6 ... ...

提交日期：2016-04-21 作者：路人甲

乐友某站jboss存在后门漏洞

RT...http://wooyun.org/bugs/wooyun-2010-0196219 跟着前人的...github.
on: 1.0.7 [3;J * --- JexBoss: Jboss verify and EXploitation Tool --- * | | | @

提交日期：2016-04-21 作者：路人甲

东风本田某供应商交互平台getshell

rt工具 https://github.com/Xyntax/POC-T/blob/master/module/jboss.py...2
* | | | @author: João Filho Matos Figueiredo | | @contact: joaomatosf@gr

提交日期：2016-04-21 作者：路人甲


携程云安全
Dashboard
关键字配置
添加关键字
携程云安全
yunling
Dashboard
结果列表
安全服务
携程云安全
Dashboard
安全服务
GitHub Scan
结果列表
关键字配置
白名单配置
16
军火库
项目白名单
文件白名单
添加项目白名单
路径
创建时间
https://github.com/ctripcorp/hermes
2016-01-29 13:06:43
https://github.com/ctripcorp/
2016-01-22 15:41:17
github.com/ctripcorp/zeus
2016-01-18 19:08:35

Github Scan

使用统计

过滤： 请输入用户信息 搜索

用户名	厂商	爬取数	关键字
bourne	恒生电子	378	hundsun password, hundsun mysql, hundsun database, hundsun login, hundsun smtp pass
p[redacted]	完美世界	523	pwrd password, pwrd mysql, pwrd database, pwrd login, pwrd smtp pass, pwrd.com
sc[redacted]k1	Lenovo	774	lenovo password, lenovo mysql, lenovo database, lenovo login, lenovo smtp pass
s[redacted]	联想	776	lenovo password, lenovo mysql, lenovo database, lenovo login, lenovo smtp pass
xi[redacted]	厦门航空	14	xiamenair password, xiamenair oracle, xiamenair database, xiamenair login, xiamenair smtp pass, xiamenair, xiamenair.com, xiamenair.com.cn, mf.com
su[redacted]	UFreedom	295	duomi password, duomi mysql, duomi database, duomi login, duomi smtp pass
ar[redacted]ot	启明星辰	408	venustech.com password, venustech.com mysql, venustech.com database, venustech.com login, venustech.com smtp pass
o[redacted]	北京启明星辰	408	venustech.com password, venustech.com mysql, venustech.com database, venustech.com login, venustech.com smtp pass
a[redacted]	蚂蚁金服	473	alipay password, alipay mysql, alipay database, alipay login, alipay smtp pass
5[redacted]	武汉维佳置业有限责任公司	0	weigagroup password, weigagroup mysql, weigagroup database, weigagroup login, weigagroup smtp pass
lo[redacted]	福建新大陆科技集团	353	newland password, newland mysql, newland database, newland login, newland smtp pass

01 关键字定制

02 智能白名单

03 实时推送

04 多链路爬虫

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) 中华网财经

20万羊毛党大军 轻易薅于P2P 搜狐

安心贷大战羊毛党:撸羊毛不顺便到处宣扬... 浙江在线

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

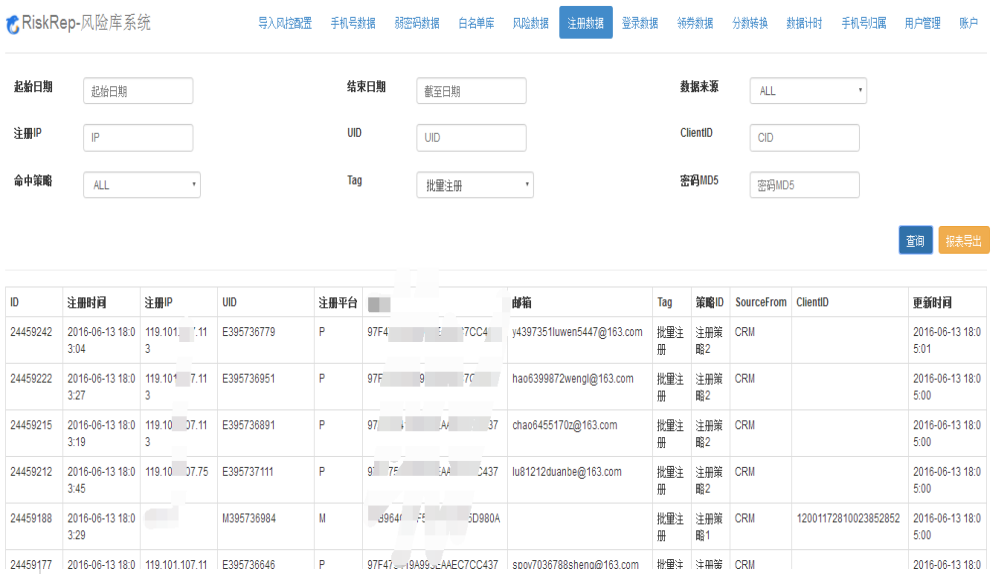
以薅羊毛为职业，团队作战，分工明确，拥有几百个手机号、身份证、银行虚拟卡，可对同一公司的活动狂薅。

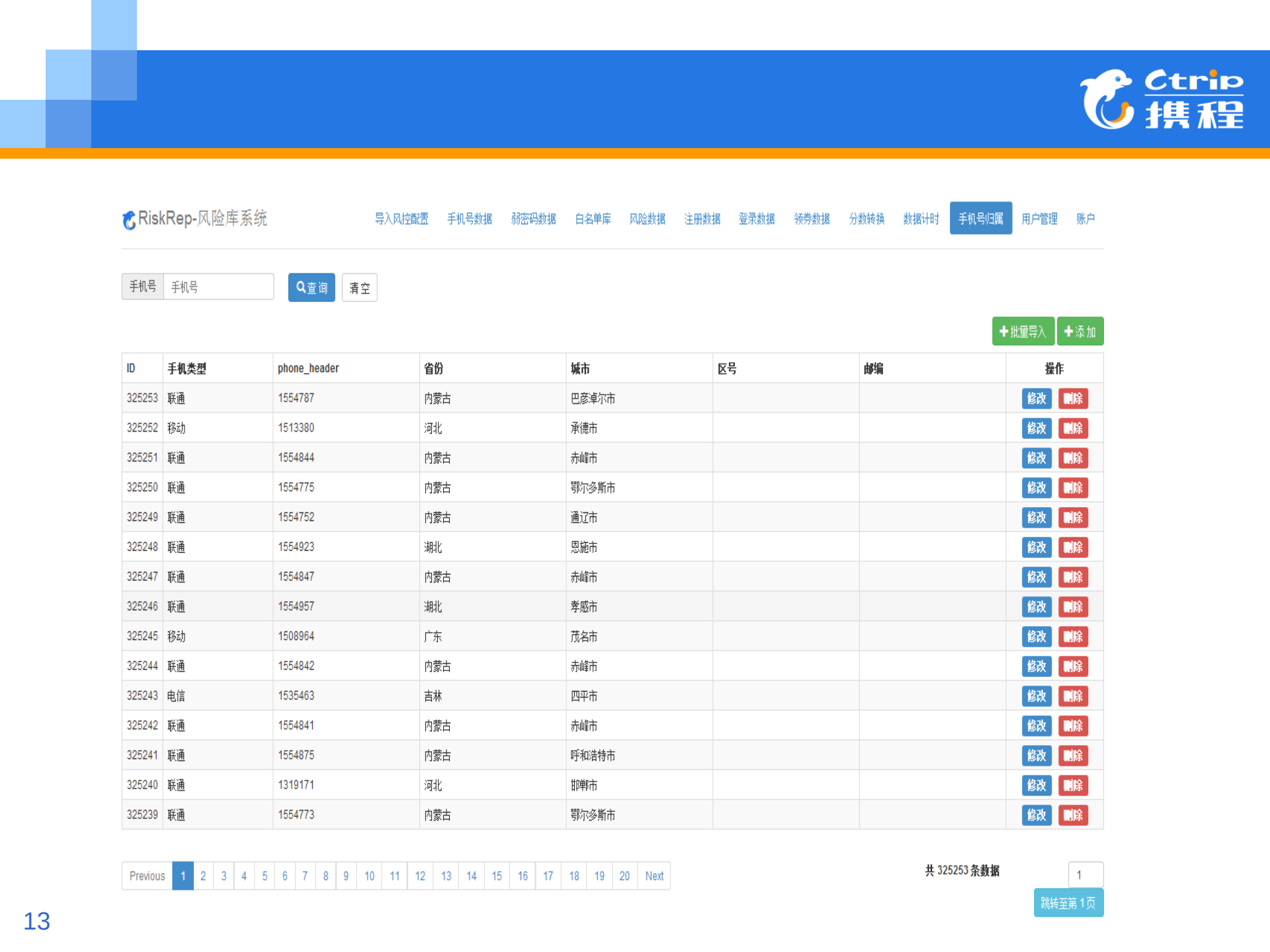
集团作战

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

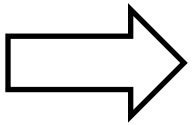



RiskRep-风险库系统
导入风控配置
手机号数据
弱密码数据
白名单库
风险数据
注册数据
登录数据
领券数据
分数转换
数据计时
手机号归属
用户管理
账户
手机号
手机号
查询
清空
批量导入
添加
ID
手机类型
phone_header
省份
城市
区号
邮编
操作
325253 联通 1554787 内蒙古 巴彦淖尔市 修改 删除
325252 移动 1513380 河北 承德市 修改 删除
325251 联通 1554844 内蒙古 赤峰市 修改 删除
325250 联通 1554775 内蒙古 鄂尔多斯市 修改 删除
325249 联通 1554752 内蒙古 通辽市 修改 删除
325248 联通 1554923 湖北 恩施市 修改 删除
325247 联通 1554847 内蒙古 赤峰市 修改 删除
325246 联通 1554957 湖北 孝感市 修改 删除
325245 移动 1508964 广东 茂名市 修改 删除
325244 联通 1554842 内蒙古 赤峰市 修改 删除
325243 电信 1535463 吉林 四平市 修改 删除
325242 联通 1554841 内蒙古 赤峰市 修改 删除
325241 联通 1554875 内蒙古 呼和浩特市 修改 删除
325240 联通 1319171 河北 邯郸市 修改 删除
325239 联通 1554773 内蒙古 鄂尔多斯市 修改 删除
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地理地址	UID	UserName	手机号归属地	[illegible] (ms)	[illegible] (ms)	[illegible]	[illegible]	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	[illegible]9016B BCE4 9DAD		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	[illegible]9016B BCE4 9DAD		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	[illegible]9016B BCE4 9DAD		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	[illegible]9016B BCE4 9DAD		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/9.2.5748.400	/mobilecouponws/json/Participate

沉淀恶意手机号　1000W +
国人常用弱密码　2500+
手机归属地分类　32W+



上线3个月
羊毛党拦截1,219,341次
爬虫拦截689,561次

每张卷平均价值20，使用率2%，被刷优惠卷损失倍数3

1219341*20*2%*3=1,463,209 元

通过SaaS接口方式

进行风险值调用

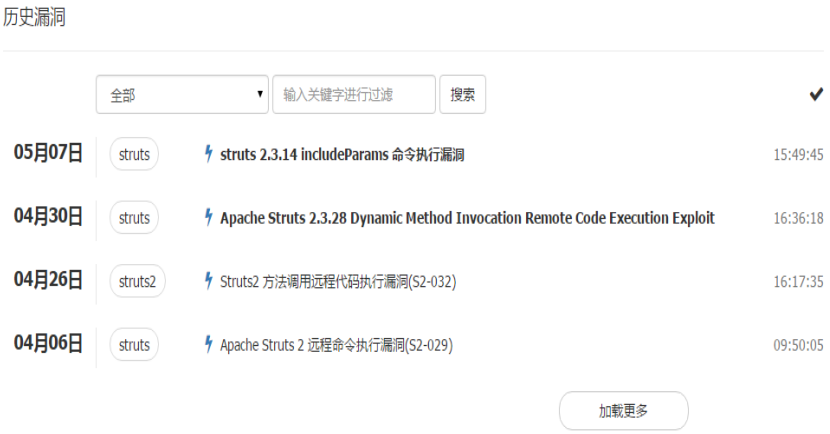
对外闭源黑名单

为乌云提供底层数据

欢迎合作

军火库

自定义关键字，有POC的漏洞才通知
避免劳烦运维频繁打补丁



天眼

思考

大量泄漏信息中
是否保护企业用户？

黑客获取这些信息
会攻击哪些地方？

CSDN600万数据泄露

考生信息泄露

天涯网4000万用户隐私信息泄露

机锋被泄露2300万用户信息

iCloud账号被盗引发“好莱坞艳照门”事件

酒店开房记录泄露

12306大量用户数据泄露并在网上传播售卖

海康威视监控设备存在严重漏洞被境外控制

支付宝前员工出售数据

超30省过5000万社保信息泄露

人寿10万保单信息泄露

美国人事电脑遭受黑客入侵，2150万人的信息被窃取

大麦网600万用户信息泄露

.....

天眼

ai @ctrip.com	1qaz2wsx3	6745****
bi en@ctrip.com	beni_shen	a06e****
bo en@ctrip.com	yizhi928	f339****
cj @ctrip.com	wuhero11	ilov****
ck @ctrip.com	lornally	9911****
cs ng@ctrip.com	hock	357c****
cy n@ctrip.com	gcy0015	gcy1****
cy n@ctrip.com	ycy290	3dbc****
cz ctrip.com	czji	904e****
d l@ctrip.com	hktk200216	dd48****
d l@ctrip.com	hktk200216	f4df****
d o@ctrip.com	N/A	MAHO****
d ng@ctrip.com	shdita11979	6720****
d eng@ctrip.com	shdita	805b****
zhang@ctrip.com	zdwfhxy	e9e6****
ngj@ctrip.com	yogosuny66	e915****
hang@ctrip.com	saphiresky1	7953****
ang@ctrip.com	fyang	49ba****
ec@ctrip.com	gec	0435****

总计 96 条

首页 上一页 1 2

跟踪最新泄露事件，识别隐私数据

1 动态更新

2 智能清洗

3 免操作

4 实时推送

信息安全SaaS之路

未来展望

蜜罐： docker形式开放，SaaS主控台

扫描器： docker形式开放， SaaS主控台

WAF： docker形式开放， SaaS主控台

机器学习： 在线提交

有情怀的安全工具平台

https://security.ctrip.com

首席客服 yunling@ctrip.com

谢 谢