白山云科技
BAISHANCLOUD

AI重塑Web安全

白山云科技
丛磊
2017.10

云计算成为趋势

图 7　中国公共云市场规模及增速（单位：亿元人民币）

近3年云计算市场保持30%以上增速

近90%企业已经或者即将使用云计算服务（公有云、私有云、混合云）

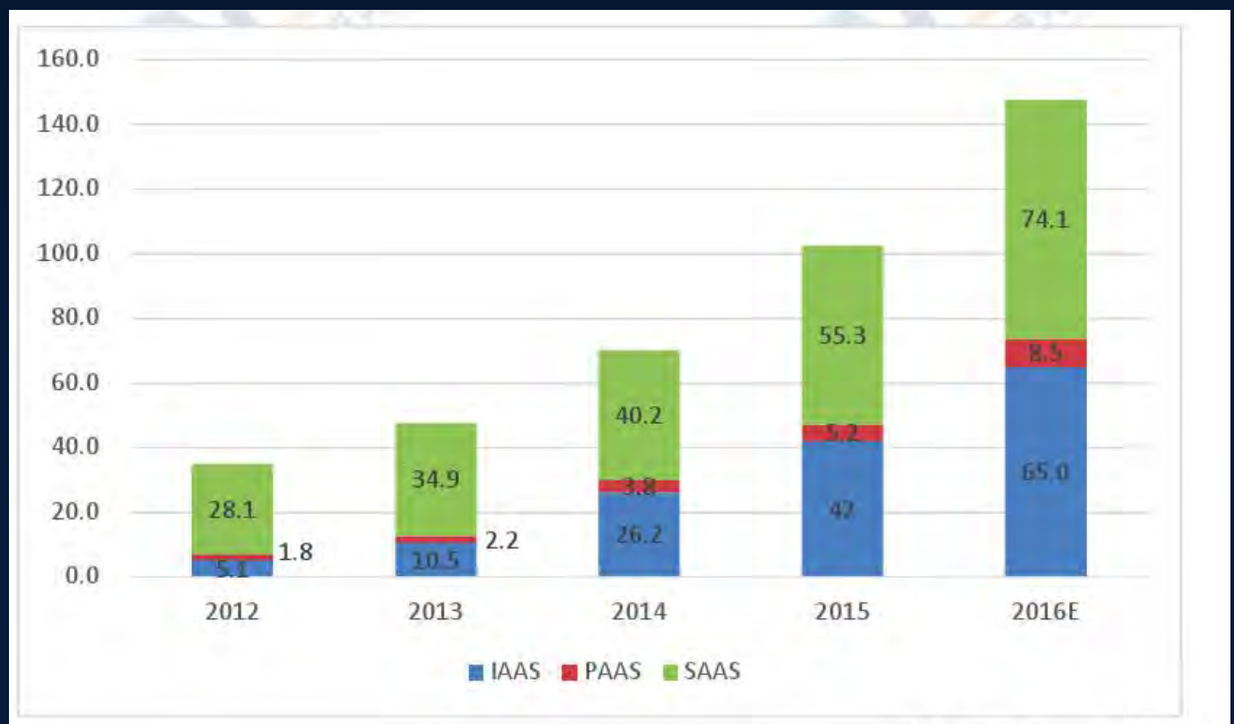


图 9　公共云细分市场规模（单位：亿元人民币）

云化导致安全风险严重

- 云化导致以硬件设备为主的传统安全方式失效
  - 公有云：A/T云
  - 私有云：OpenStack

- 云化导致攻击/作恶成本大大降低
  - 弹性IP 1RMB/天
  - Hypervisor 几RMB/天
  - Container…

云化导致安全风险严重

- 云化导致业务可控性降低，遭遇攻击的风险大大提高
  - 资源隔离技术

- 攻击手段越来越先进
  - 模拟浏览器行为（UA、Referer伪造）
  - JavaScript处理能力（PhantomJS）
  - 团伙作案

安全风险更多集中在应用层

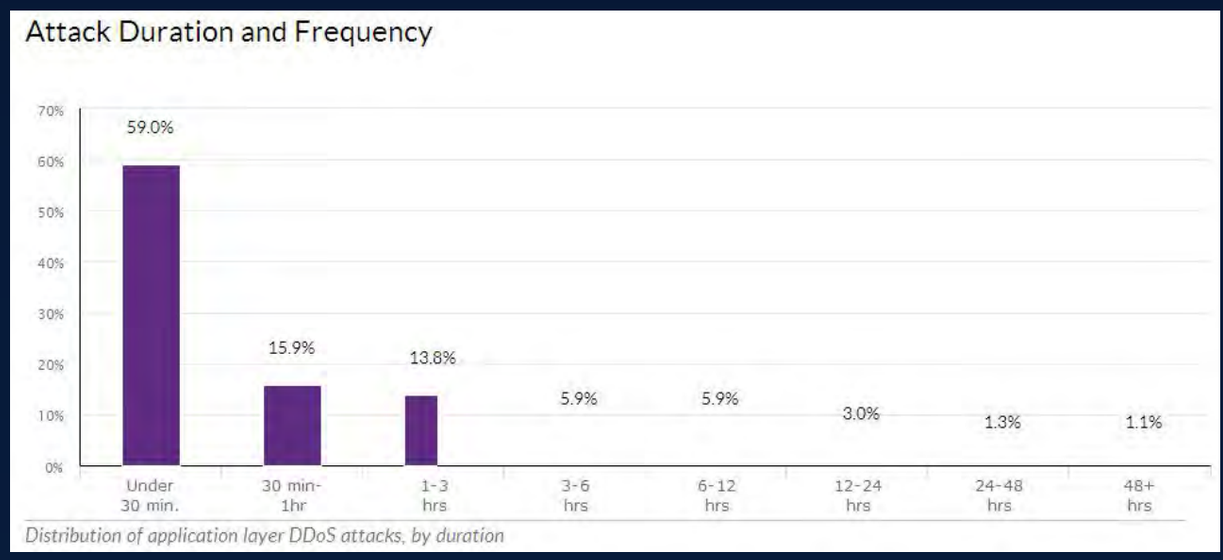
- 66%的流量由机器产生
- 90%的攻击是针对应用层
- 99%的应用层攻击是针对API
- 60%的应用层攻击/探测是短时低频

刷单、刷优惠券、刷粉丝、刷评价、薅羊毛

撞库、爬虫、CC

SQL注入、XSS、慢速攻击、异常包攻击

流量攻击



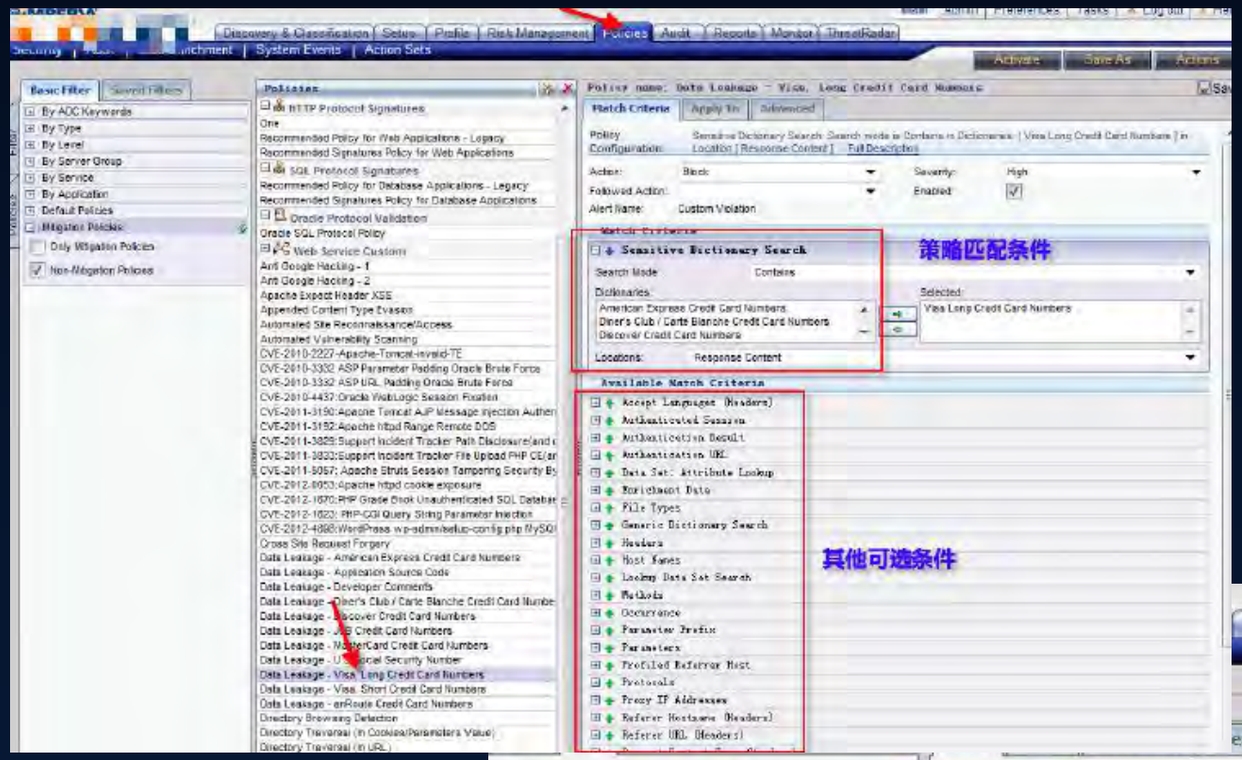
传统安全厂商需要被革命

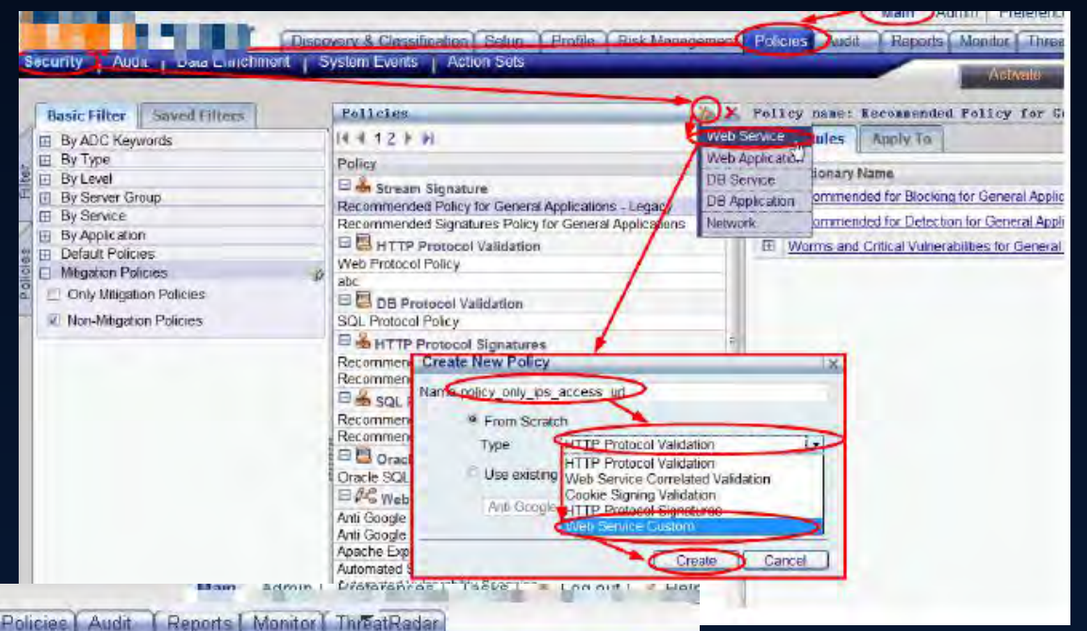
传统安全厂商在应对应用层威胁上非常无力

常见套路：

- 硬件模式：硬件是否我们需要？
- 强调准确率：怎么测试召回率？
- 混淆文本攻击==行为攻击
- 依赖policy

传统安全厂商需要被革命





“买了我们的产品不代表你的业务就安全了，你必须学会如何配置！”

- 史上最牛安全“布道师”

传统安全厂商需要被革命

我们真的会设策略吗？

我们真的依赖策略吗？

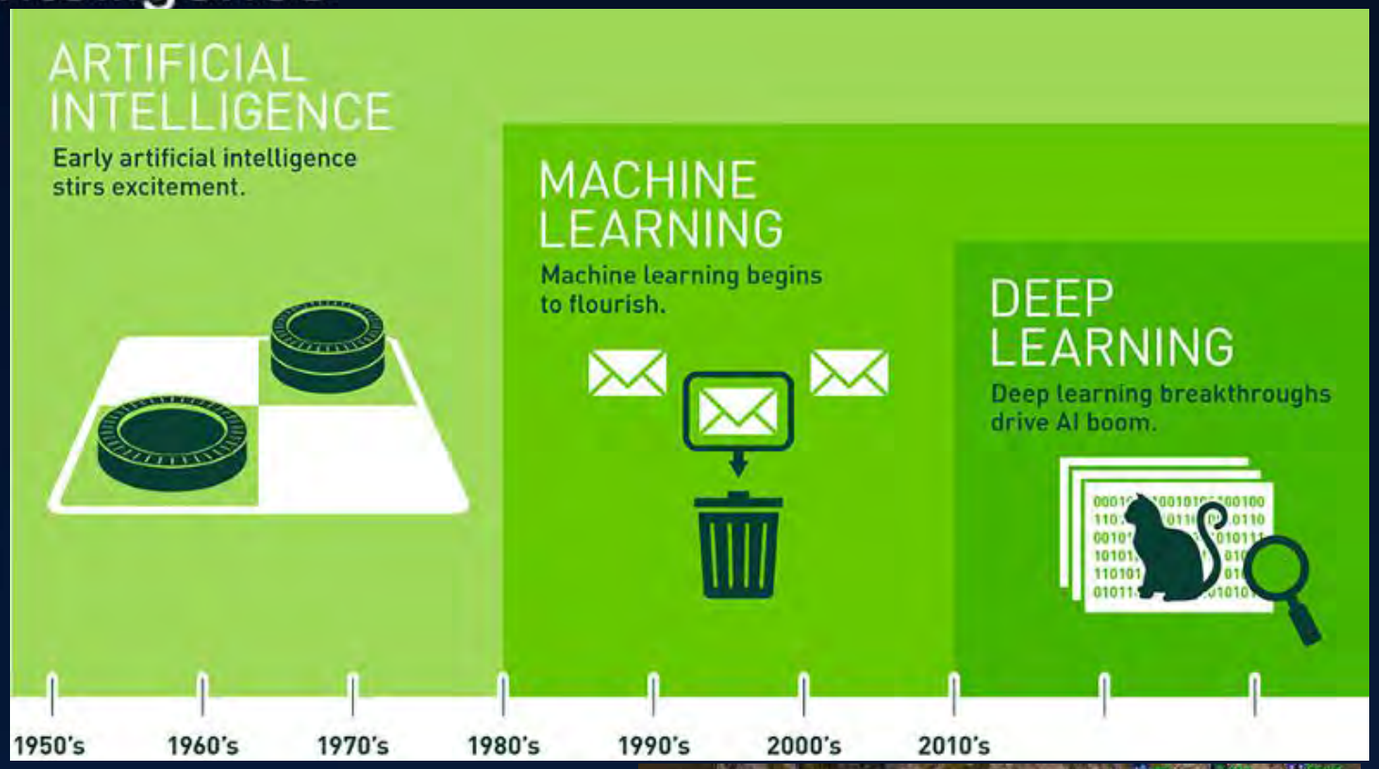
没有策略的世界会是怎样？

使用AI突破“策略瓶颈”

- 何为AI？
  Artificial Intelligence != Human Intelligence

- 何为Machine learning？
  Data + Learning

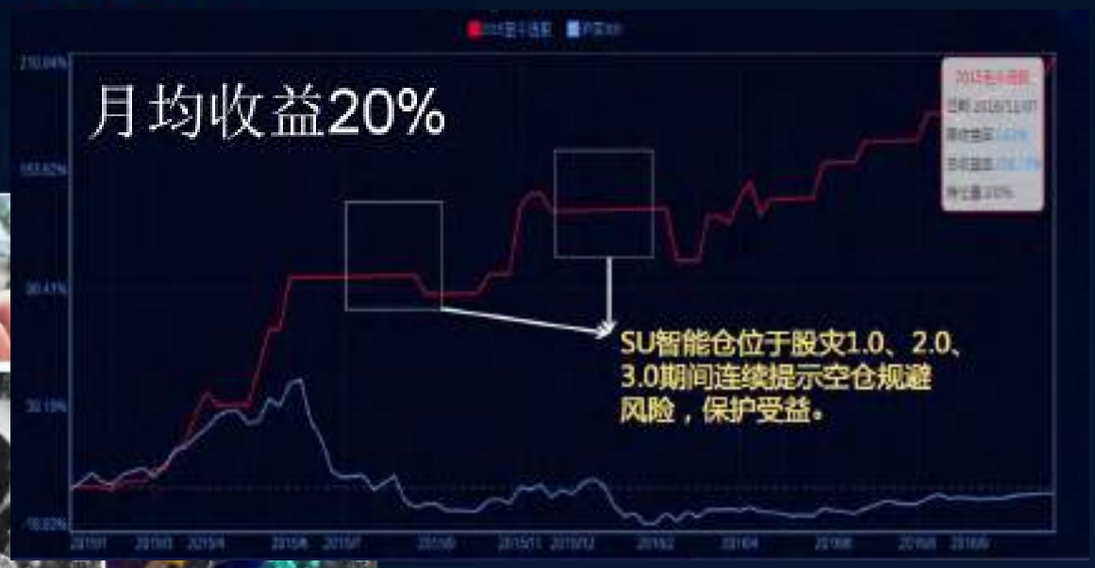
- 何为AI ^ Machine Learning
  - αβ
  - greedy
  - A*
  - ...



使用AI突破“策略瓶颈”

- AI三步走
  信息识别=》信息理解=》信息反馈

- AI太强了



- AI还很弱：深度学习 vs 两岁小孩
  is AI not HI

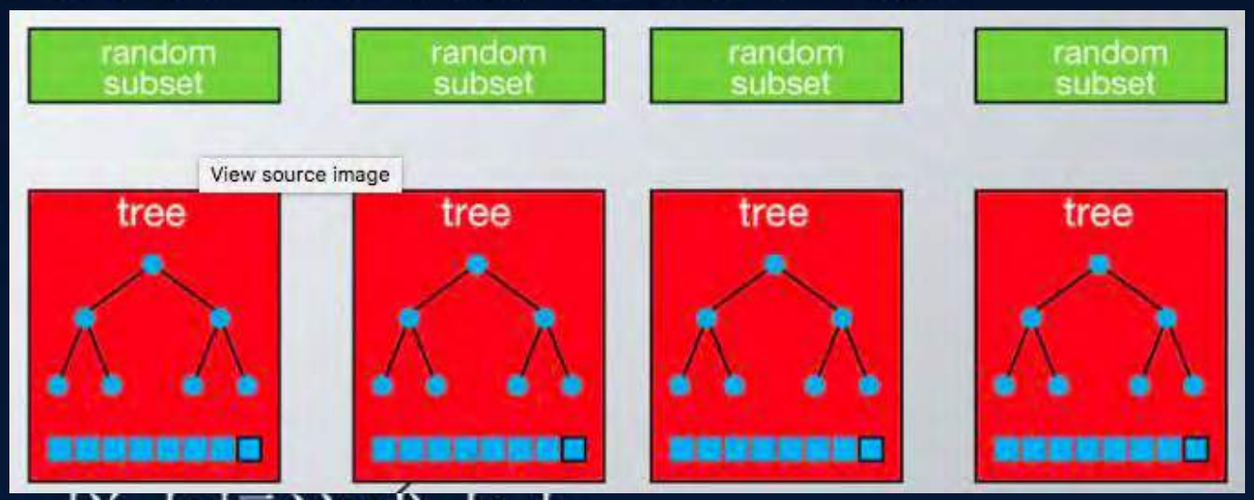
- AI适合什么领域？

使用AI突破“策略瓶颈”

- AI非常适合安全
  - 安全属于特定领域
  - 安全属于识别问题
- 为什么目前AI&安全还是处于蓝海
  - 难

使用AI突破“策略瓶颈”

- AI&安全的“难”
  - 安全领域场景差异大
  - 文本型攻击特征空间不均衡

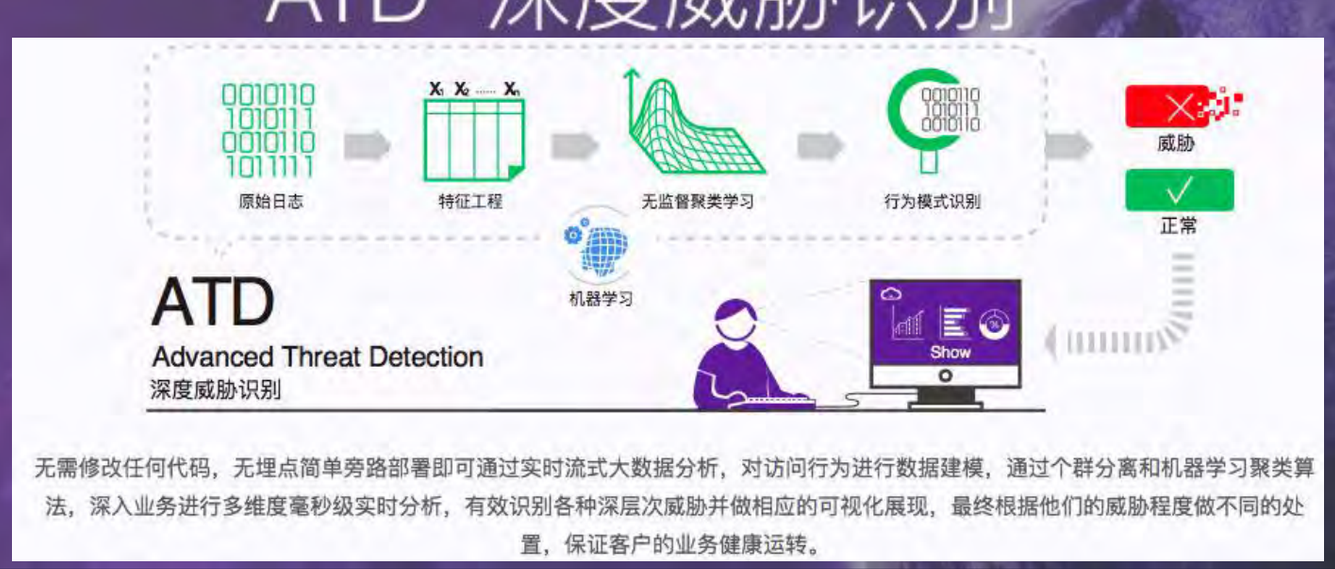


  - 样本标注成本大

[redacted] "GET /test/test.php?id=1%df%27%2F%2A%21aNd%2A%2F3922%3D%2F%2A%21iF%2A%2F%28%280
RD%28MID%28%28%2F%2A%21SelEcT%2A%2F%2r%2A%21iFNULL%2A%2F%28Cast%28CoUNt%28%2F%2A%21dIStinCT%2A%2F%28grantee%29%29%2F%2A%21
aS%2A%2F%2F%2A%21ChAr%2A%2F%29%2C0x20%29%2F%2A%21fROM%2A%2FINFORMATION_SCHEMA.USER_PRIVILEGES%29%2C1%2C1%29%29%3E181416%29
62CSLEEP%285%29%2C3922%29--%20mUZT%20anD%20%270haVInG%27%3D%270haVInG%27 HTTP/1.1" 200 378

AI重新定义Web安全

ATD 深度威胁识别



无需修改任何代码，无埋点简单旁路部署即可通过实时流式大数据分析，对访问行为进行数据建模，通过个群分离和机器学习聚类算法，深入业务进行多维度毫秒级实时分析，有效识别各种深层次威胁并做相应的可视化展现，最终根据他们的威胁程度做不同的处置，保证客户的业务健康运转。

新一代基于AI的深度威胁识别产品

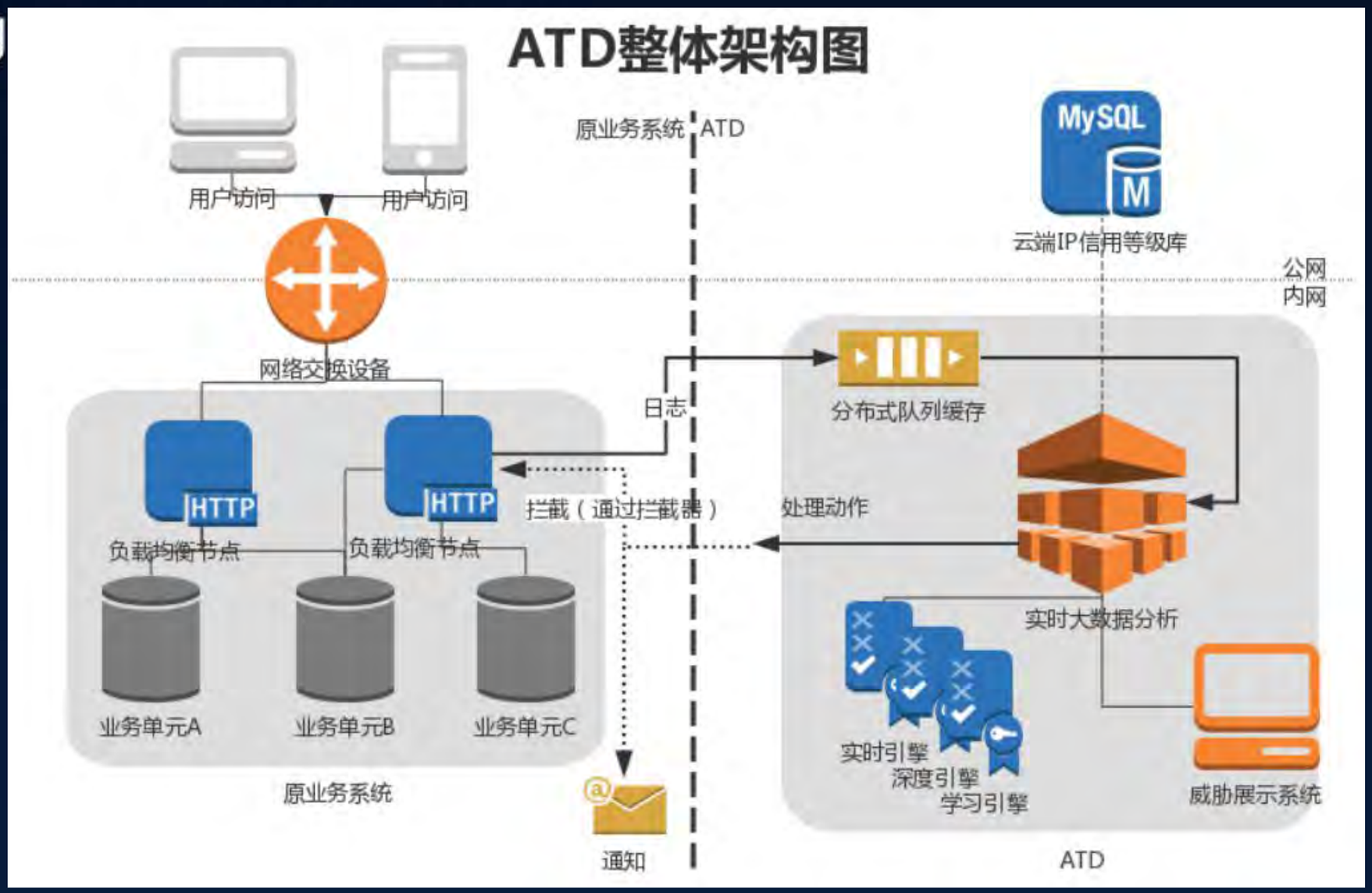
AI重新定义Web安全

- 我们的思路：
- 【学习】业务内在规律
- 【个群对比】突破策略瓶颈
- 【无监督学习】破解样本标注问题

白山ATD

- 机器学习的前提 - 流式大数据分析
  - Spark Streaming
  - Storm
- 构建特征模型
  - URI
  - Request Time
  - User Agent
  - Refer
  - Response Code
  - Request Length
  - Cookie
  - Token

……



白山ATD - 三大引擎

实时引擎

深度引擎

学习引擎

- 实时引擎 - 个群对比
- 深度引擎 - 无监督聚类
- 学习引擎 - 概率置信区间

白山ATD - 实时引擎

request length

response code

uri

path

http method

request time

user agent

referer

...

X

最大值

最小值

平均值

标准差

中位数

四分位数

重复环占比

最大占比

LCS

...

主要分析维度	该IP	群体行为
每分钟请求数	55	3
路径最大相似占比	100.00%	0.16%
路径最大重复环占比	100.00%	0.00%
Referer最大相似占比	100.00%	0.16%
危险UA占比	0.00%	10.30%
UA最大相似占比	100.00%	0.16%
UA集合空间	1	1
404状态码占比	0.00%	0.00%
5XX状态码占比	0.00%	1.43%
请求响应时间	3	0
请求响应长度 (B)	320	51
请求返回长度 (B)	330	15906

个群对比 - 毫秒级分析

白山ATD - 深度引擎

威胁事件回溯

demouse

演示应用 / demo.baishancloud.com

2017-10-13 至 2017-10-13 确定

请输入查询的IP 搜索 导出

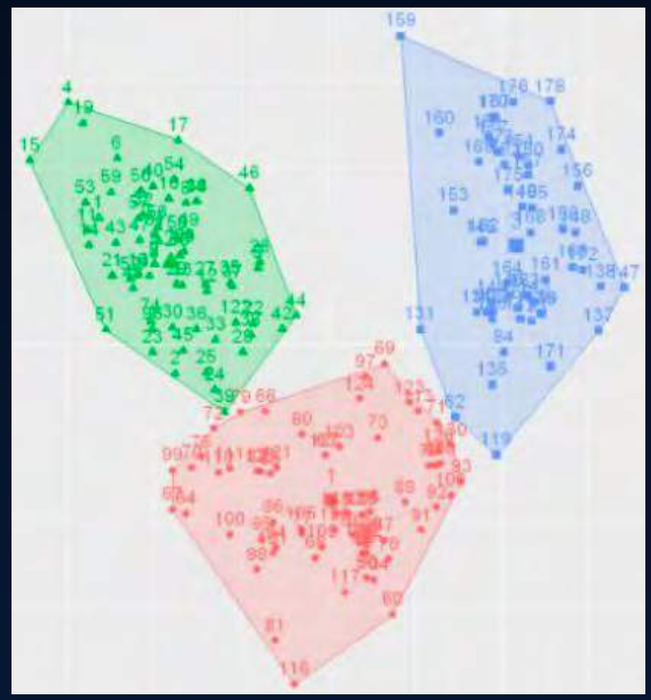
原因 全部 (8425) 爬虫 (4200) CC攻击 (2698) 危险UA (854) SQL注入 (365) 异常流量包攻击 (286) 命令注入 (17) 跨站脚本 (5) 刷单类 (0) 展开

IP 全部 出口IP 搜索引擎IP 其他IP 处理结果 全部 已拦截 自定义 无 决策引擎 全部 实时引擎 深度引擎 威胁等级 全部 高 中 低

返回 218.61.196.123同一簇IP 加入白名单 加入黑名单

IP	时间	原因	请求数	位置 | 运营商	处理结果	决策引擎	威胁等级	操作
218.61.1	2017-10-13 14:43:44	爬虫	7	大连 | 联通	已拦截	深度引擎	中	
211.149.2	2017-10-13 14:43:44	爬虫	7	- | 电信	已拦截	深度引擎	中	
45.114.11	2017-10-13 14:43:44	爬虫	7	雅加达 | dediserve.com	已拦截	深度引擎		
118.186.220	2017-10-13 14:43:44	爬虫	7	北京 | 联通	已拦截	深度引擎		

查找聚类周期内同一簇IP



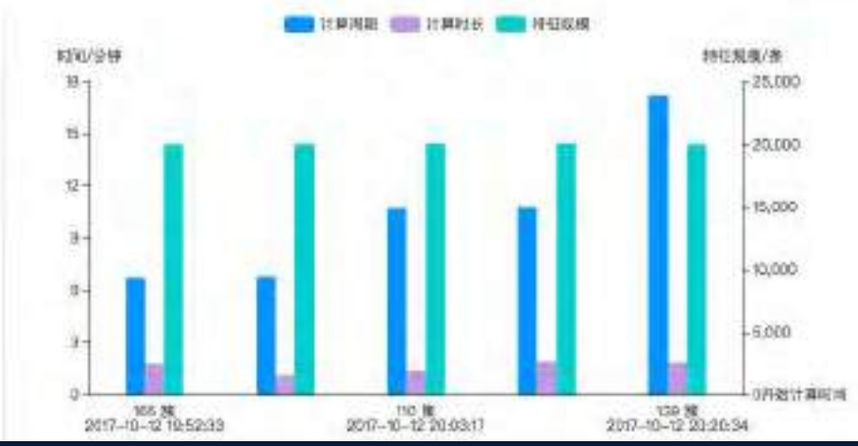
聚类算法

编辑

计算周期 分钟

最大聚类特征规模 条

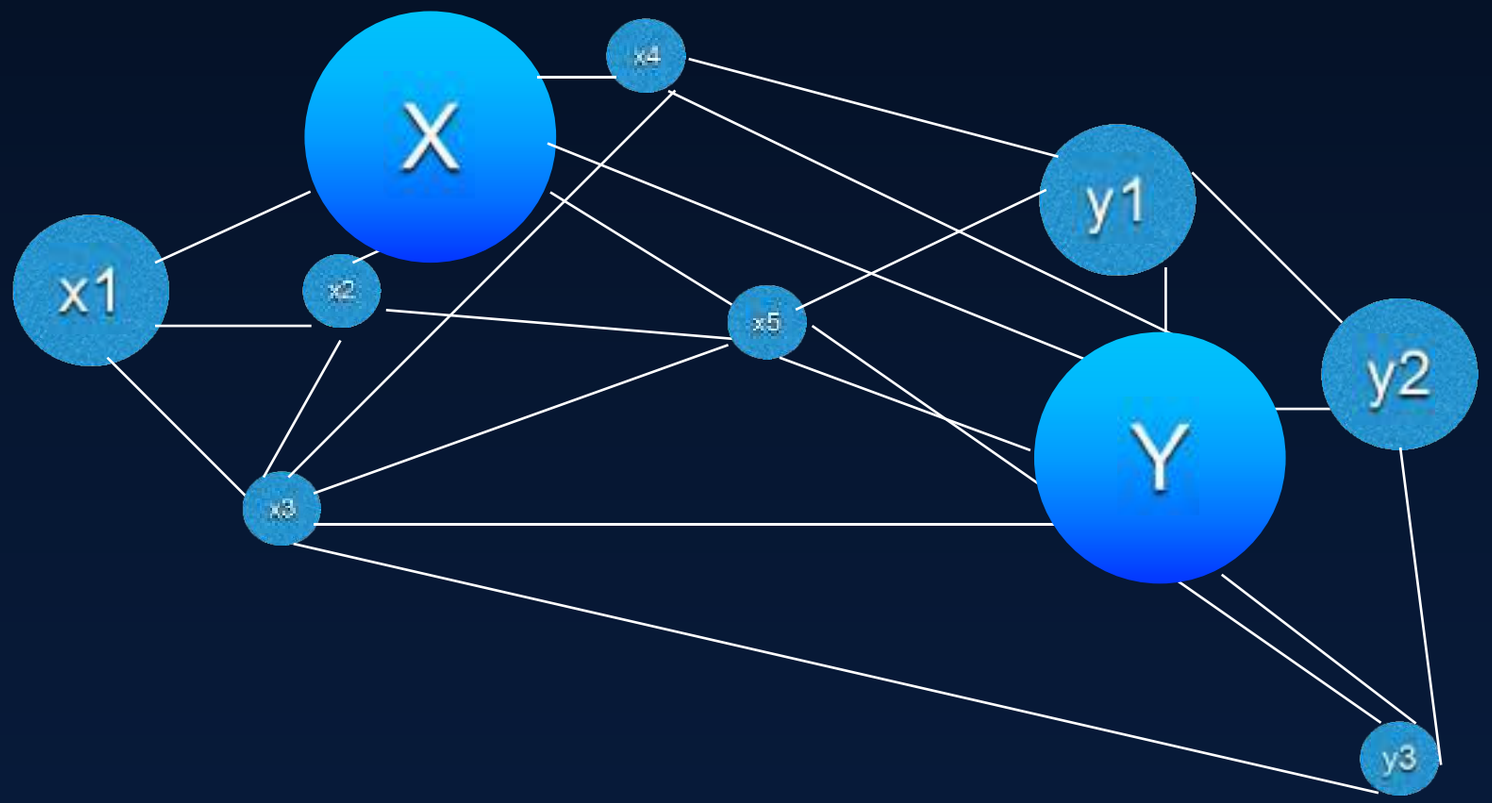
攻击IP最小请求数



无监督聚类 - 无标注样本

白山ATD - 学习引擎

- 学习规律
  - 行为规律
  - 文本规律
- 关键节点
  - 访问矩阵

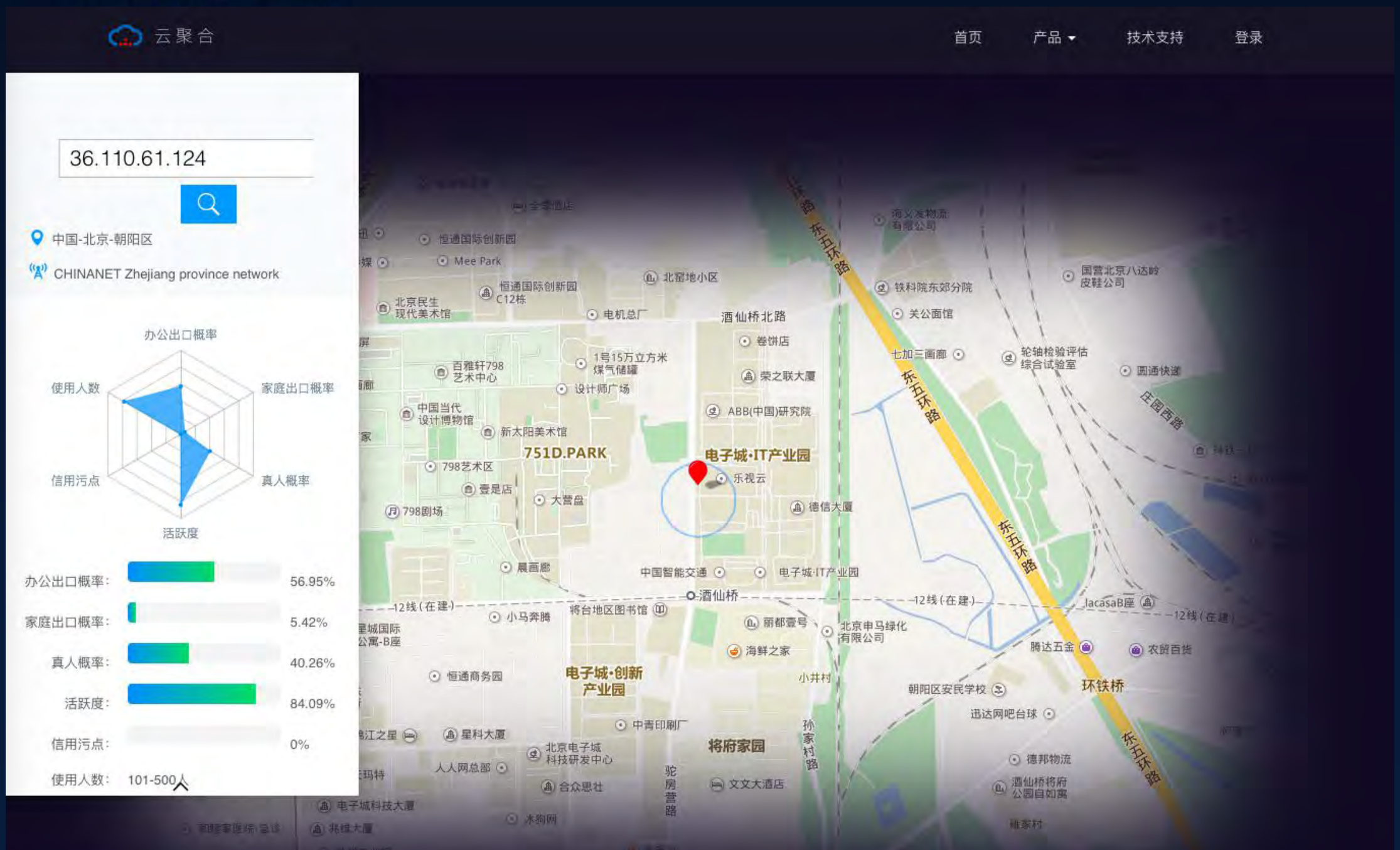


白山ATD - 产品展现


云聚合
首页
产品
联系购买
登录
ATD 深度威胁识别
控制台
ATD
demou...
创建
演示应用
域名(3)
攻击情况
demo.baishancloud.com
最近1小时
www.baidu.com
最近24小时
www.baishancloud.com
最近24小时
2017 - ATD v1.6.3
域名分析
威胁事件回溯
实时防护状态
决策引擎设置
基础配置
实时引擎
深度引擎
导出
总览
基本信息
接入的域名: 3
被防护的主机: 1
管理员: 3
2017-08-29 ~ 2017-08-29
威胁情况
演示应用
攻击IP
已处理IP
威胁情况
导出
攻击源数
攻击次数
拦截流量
流量 (KB)

白山ATD - 实用功能

- IP信用等级



白山ATD - 实用功能

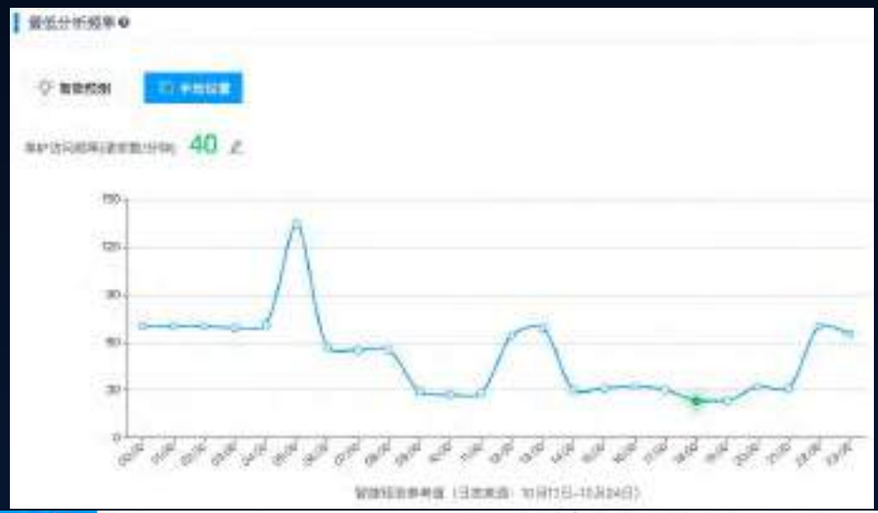
- IP信用等级
- 覆盖全球41亿+IPv4地址
- 识别真人概率/机器概率
- 识别住宅/企业使用人数
- 识别日常活跃度/信用度
- 精确到街道级IP坐标

白山ATD - 实用功能

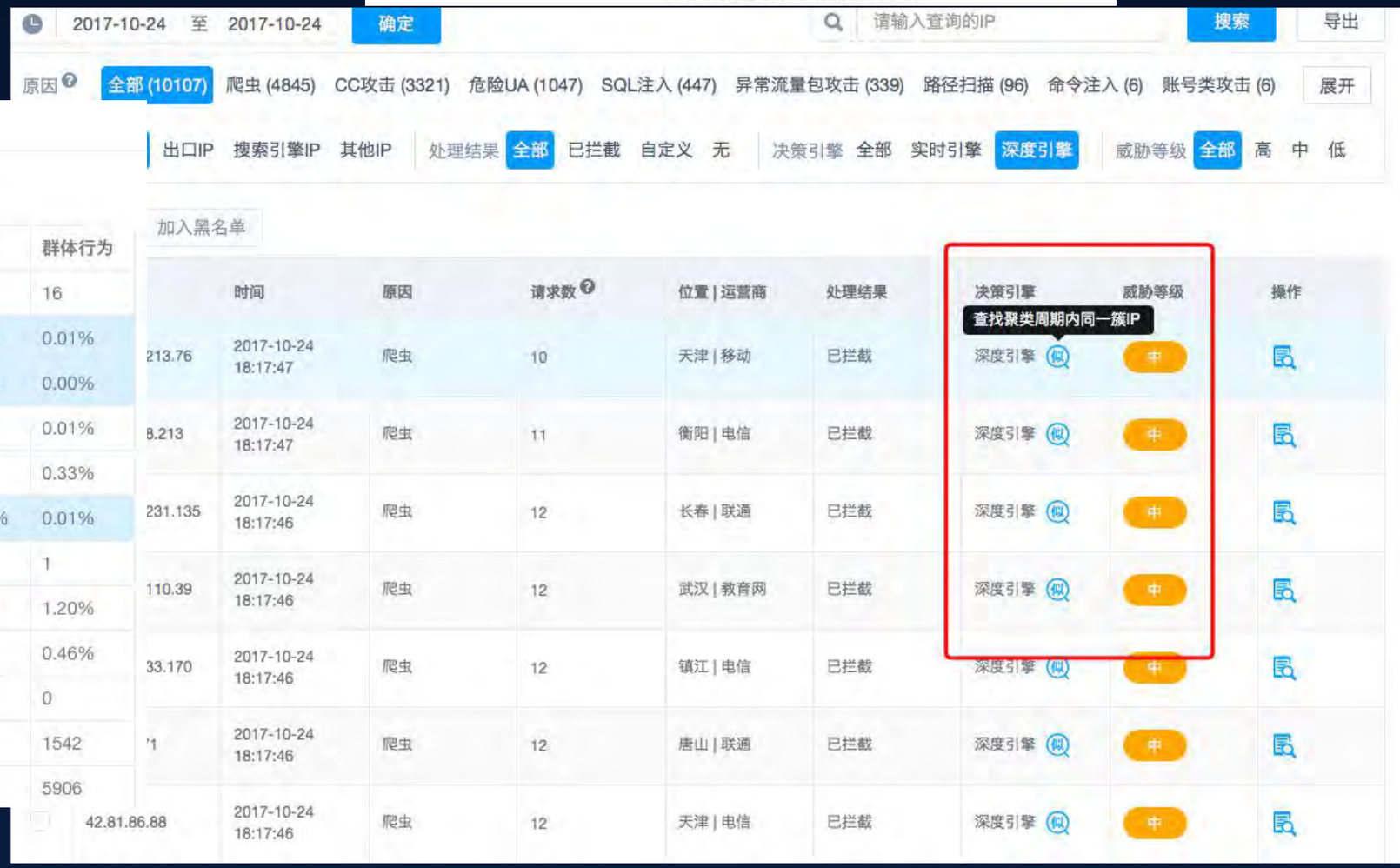
- 拦截惩罚模式
- 区分善恶搜索引擎
- 过滤人群出口

白山ATD - 实用功能

- 智能访问频率分析
- 个群行为对比
- 同簇威胁识别

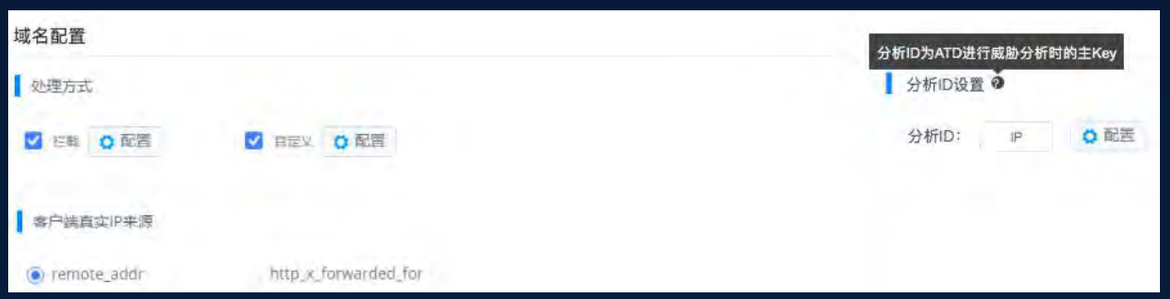


主要分析维度	该IP	群体行为
每分钟请求数	173	16
路径最大相似占比	13.87%	0.01%
路径最大重复环占比	78.49%	0.00%
Referer最大相似占比	9.83%	0.01%
危险UA占比	0.00%	0.33%
UA最大相似占比	100.00%	0.01%
UA集合空间	1	1
404状态码占比	0.00%	1.20%
5XX状态码占比	0.00%	0.46%
请求响应时间	0	0
请求响应长度 (B)	1508	1542
请求返回长度 (B)	4399	5906



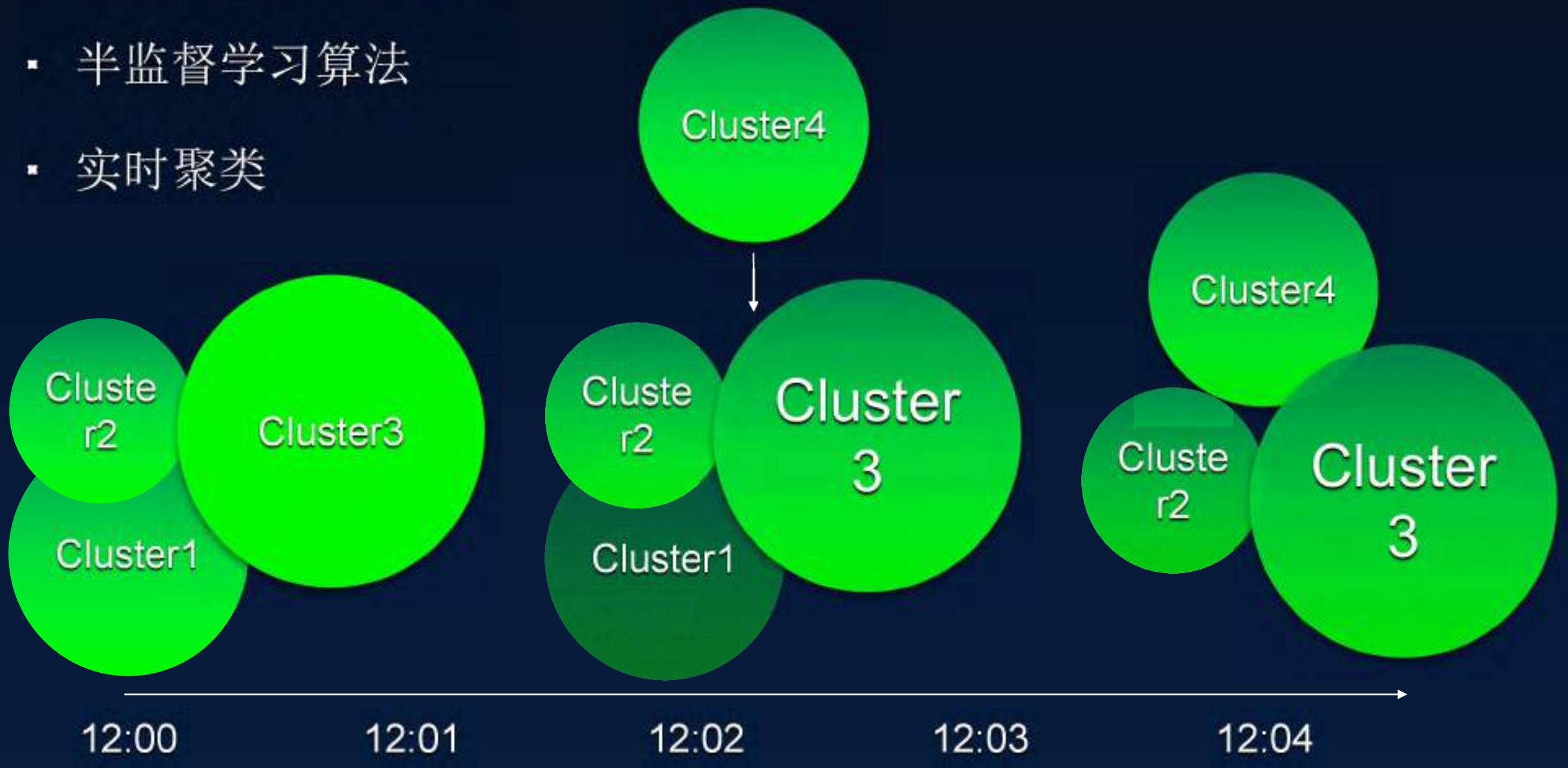
白山ATD - 实用功能

- 大屏/报表展现
- 用户界面自定义分析维度



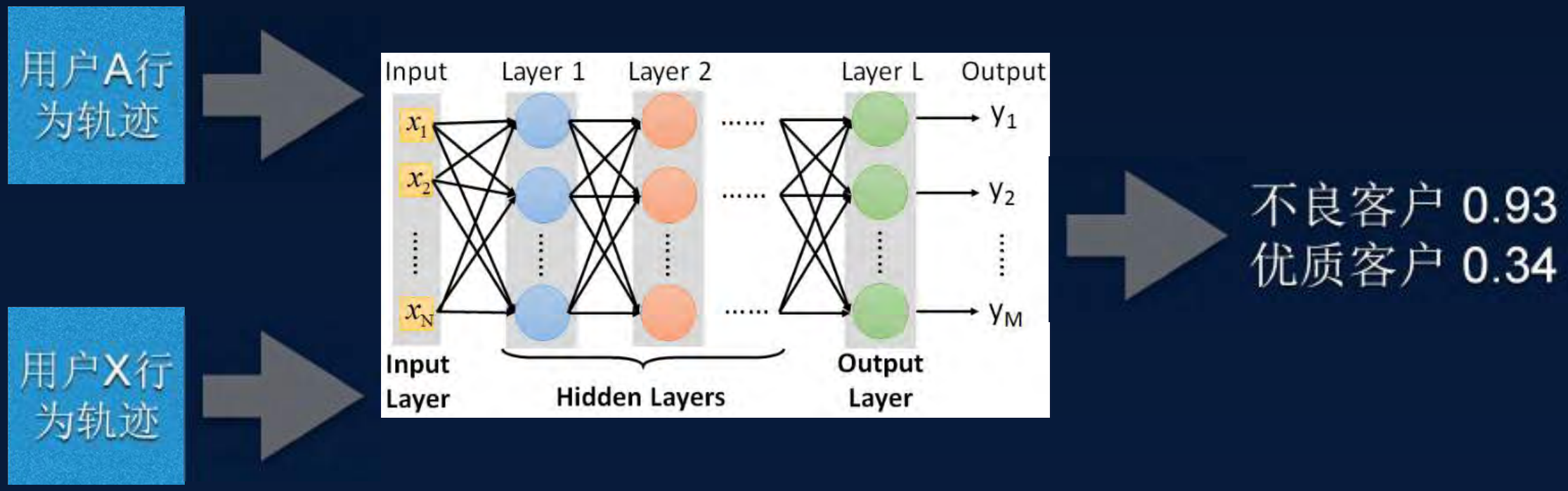
白山ATD - 未来

- 全新的漏洞识别算法
- 半监督学习算法
- 实时聚类



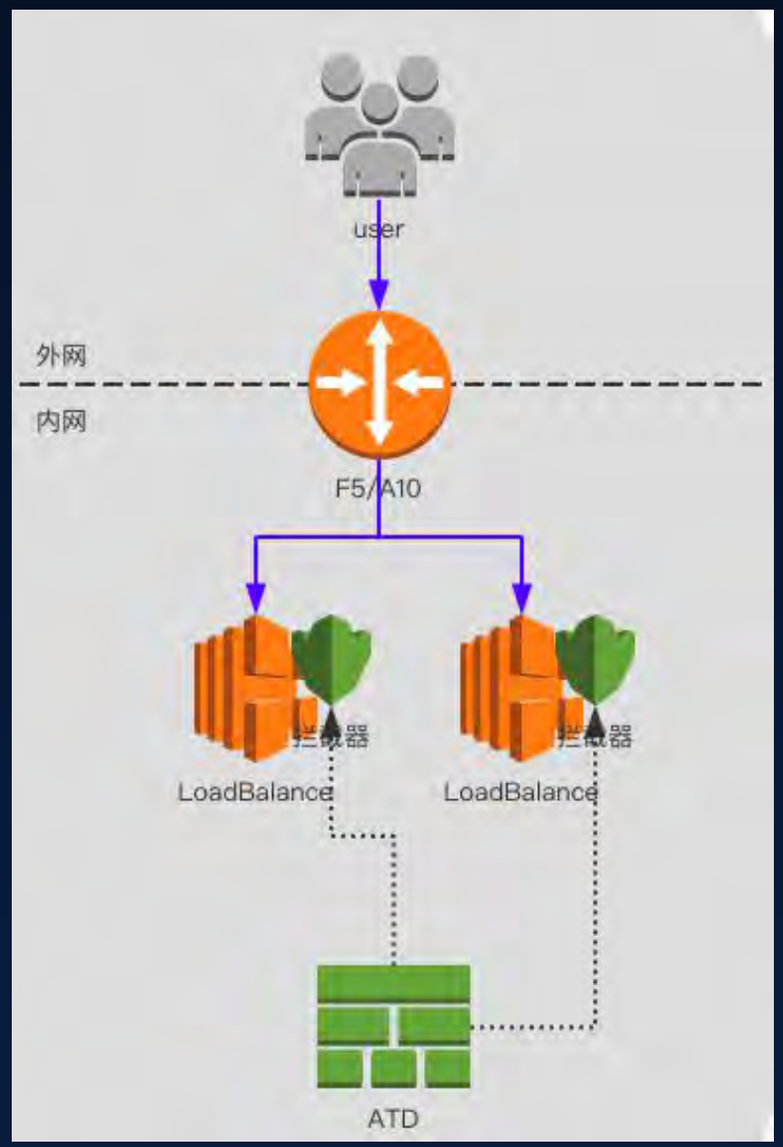
白山ATD - 未来

- 深度学习 Deep Learning
- 深度学习和传统机器学习的本质区别
- 深度学习可以应用在安全的什么领域？为什么这些领域特别需要深度学习



白山ATD - 案例

- 某航空公司



模式A

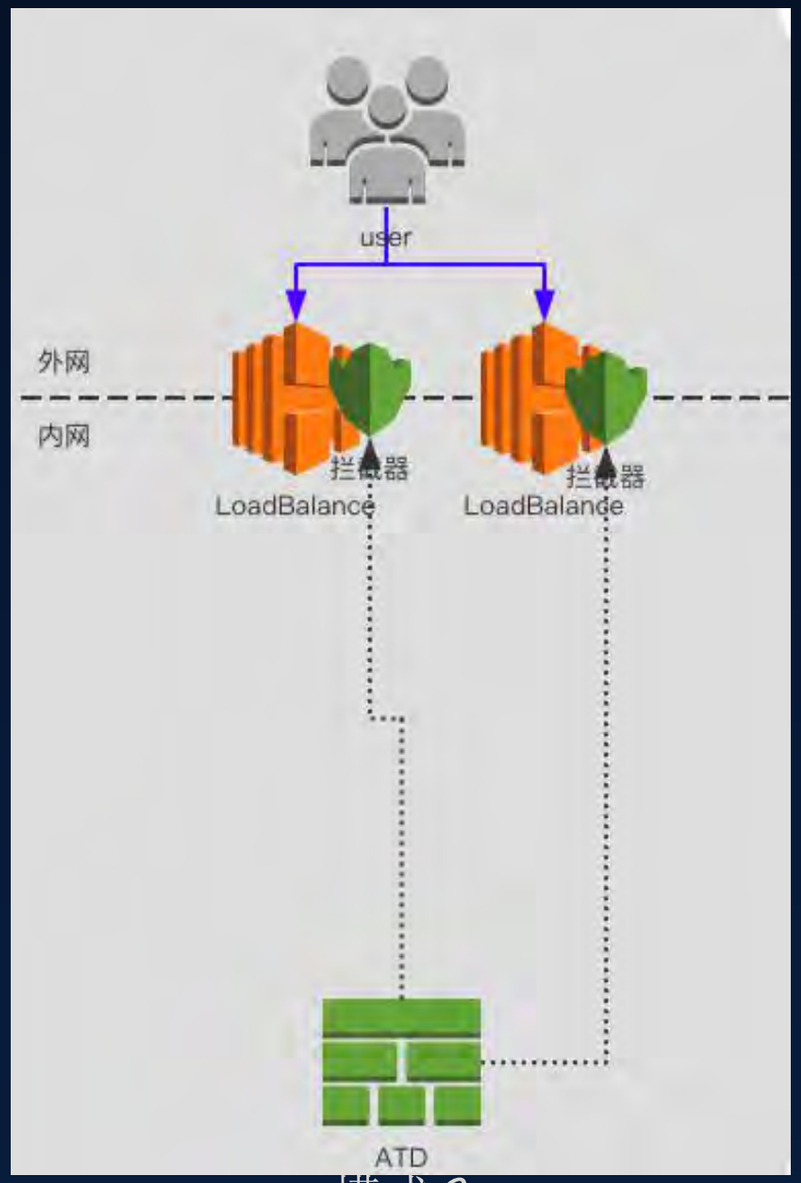
客户场景特点：
- 已有Imperva安全产品
- 机票信息被外界爬取，查定比低，并且影响服务质量
- 会员信息被外界爬取，核心用户数据泄露
- 金卡会员接口存在被第三方非法调用情况

解决方案：
- 阶段1，ATD运行在Imperva后面，发现有大量爬虫行为未被Imperva识别
- 阶段2，停掉Imperva相关策略，独立运行ATD，发现识别召回率提升400%，准确率保证100%
- 阶段3，通过学习引擎学习金卡会员接口的访问行为，屏蔽第三方非法调用，拦截准确率100%

最终效果：
- 成功识别对于机票信息的爬虫行为，准确率100%，召回率提升400%
- 成功拦截对于会员接口的非法第三方调用

白山ATD - 案例

- 某Top1自由行旅游公司



模式C

客户场景特点：
- 大量爬虫非法收集数据，爬虫行为各异
- 用户主要采用云主机，传统安全产品无法使用
- 用户采购高防IP，但高防IP无法解决业务被爬的问题

解决方案：
- 采用模式C方式部署，部署规模5台高配机器
- 利用机器学习分类对爬虫行为进行识别
- 为了避免误拦，结合IP信用等级处理出口IP
- 针对爬虫类别进行分类

最终效果：
- 精确识别了非法爬虫
- 有效阻拦非法恶意访问