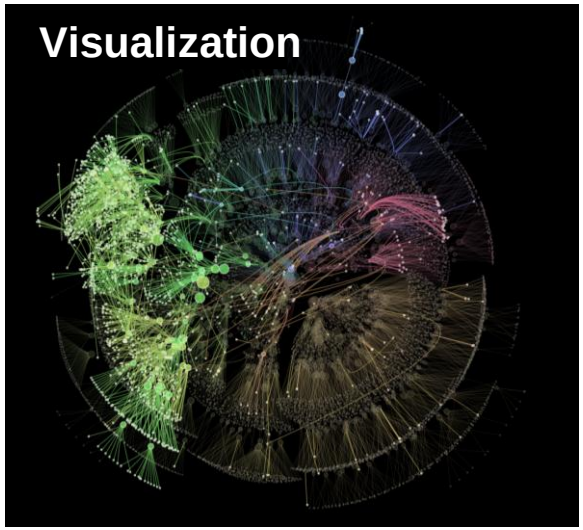
利用数据分析提高内部威胁防范能力

董靖 思睿嘉得 总裁

那些关于内部威胁的噱头热词

无处不见的高大上新技术



概念离落地成功还很遥远...

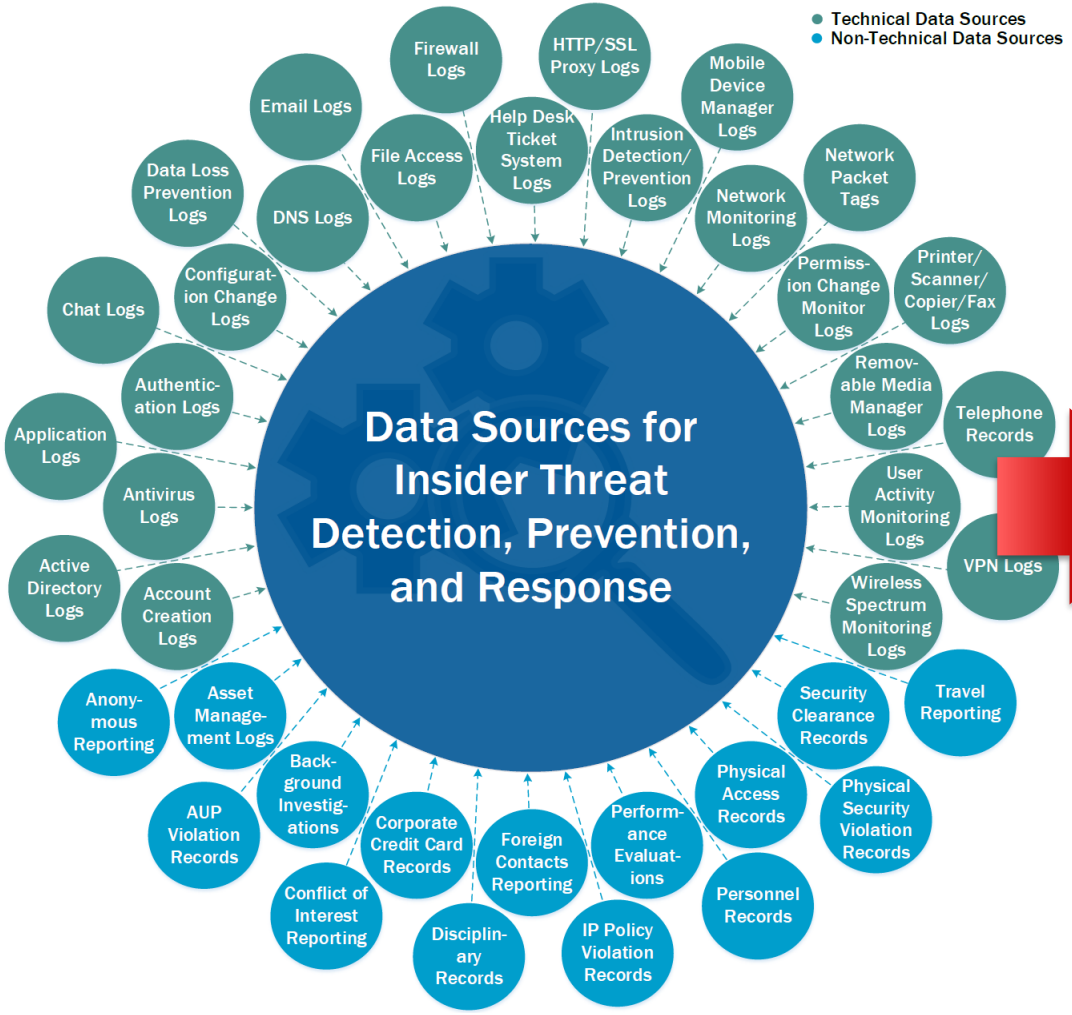
提高内部威胁防范能力 – 行动计划

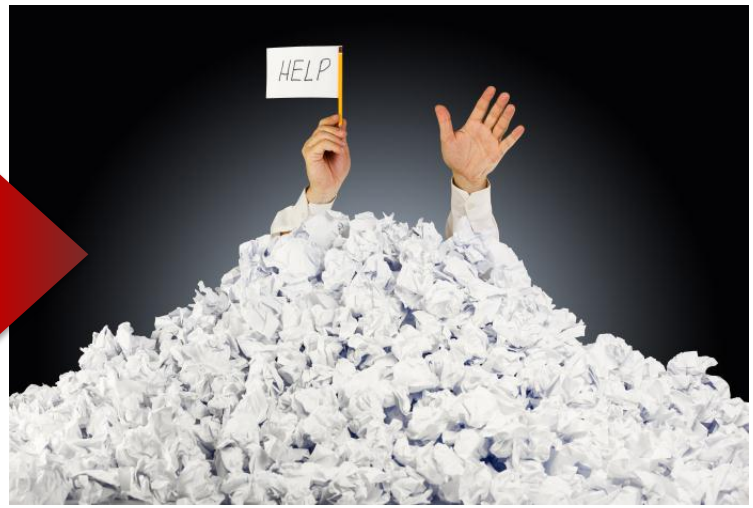
- 有的放矢 – 节制采集有效线索
- 循名覈实 – 语义理解预警威胁
- 数往知来 – 参照案例建立模型
- 操奇计赢 – 先进技术自动猎捕

行动要点（一）

- 有的放矢 – 节制采集有效线索
- 循名覈实 – 语义理解预警威胁
- 数往知来 – 参照案例建立模型
- 操奇计赢 – 先进技术自动猎捕

如果你听从专家建议...将这些数据全部采集





如果你听从专家建议...对海量日志做行为分析

海量终端系统日志

```
Information 2016/7/22 12:54:42  Service Control Manager 7036    None    The Portable Device Enumerator Service service entered the stop state.
Information 2016/7/22 12:54:41  Service Control Manager 7036    None    The Windows Update service entered the running state.
Information 2016/7/22 12:54:40  Service Control Manager 7036    None    The Microsoft .NET Framework NGEN v4.0.30319_X64 service entered the stop state.
Information 2016/7/22 12:54:40  Service Control Manager 7036    None    The Microsoft .NET Framework NGEN v4.0.30319_X64 service entered the running state.
Information 2016/7/22 12:54:40  Service Control Manager 7036    None    The Microsoft .NET Framework NGEN v4.0.30319_X86 service entered the stop state.
Information 2016/7/22 12:54:40  Service Control Manager 7036    None    The Microsoft .NET Framework NGEN v4.0.30319_X86 service entered the running state.
Information 2016/7/22 12:54:18  Service Control Manager 7036    None    The Microsoft Software Shadow Copy Provider service entered the running state.
Information 2016/7/22 12:54:18  Service Control Manager 7036    None    The Volume Shadow Copy service entered the running state.
Information 2016/7/22 12:53:36  Microsoft-Windows-Application-Experience    206 None    The Program Compatibility Assistant service successfully performed phase
Information 2016/7/22 12:52:59  Service Control Manager 7036    None    The Software Protection service entered the running state.
Information 2016/7/22 12:52:48  Service Control Manager 7036    None    The Computer Browser service entered the stop state.
Information 2016/7/22 12:52:43  Service Control Manager 7036    None    The Windows Presentation Foundation Font Cache 3.0.0.0 service entered the running state
Information 2016/7/22 12:52:43  Service Control Manager 7036    None    The SSDP Discovery service entered the running state.
Information 2016/7/22 12:52:43  Service Control Manager 7036    None    The IPsec Policy Agent service entered the running state.
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Diagnostic System Host service entered the running st
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Portable Device Enumerator Service service entered th
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Windows Media Player Network Sharing Service service
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Computer Browser service entered the running state.
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Human Interface Device Access service entered the run
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Diagnostic Service Host service entered the running s
Information 2016/7/22 12:52:42  Service Control Manager 7036    None    The Application Experience service entered the running st
Information 2016/7/22 12:52:41  Service Control Manager 7036    None    The BaiduYunUtility service entered the stop state.
Information 2016/7/22 12:52:42  Microsoft-Windows-WMPNSS-Service    14204   None    Service 'WMPNetworkSvc' started.
Information 2016/7/22 12:52:41  Service Control Manager 7036    None    The Network List Service service entered the running
Information 2016/7/22 12:52:41  Service Control Manager 7036    None    The BaiduYunUtility service entered the running state
Error   2016/7/22 12:52:41  NetBT   4321    None    "The name ""ADMIN-PC       :20"" could not be registered on the interface
Information 2016/7/22 12:52:41  Service Control Manager 7036    None    The Windows Search service entered the runnin
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Background Intelligent Transfer Service s
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Application Information service entered t
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Disc Soft Lite Bus Service service entere
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Security Center service entered the runni
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Network Connections service entered the r
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The WinHTTP Web Proxy Auto-Discovery Service service
Error   2016/7/22 12:52:40  Service Control Manager 7026    None    "The following boot-start or system-start driver(s) failed
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Avira Web Protection service entered the stop state.
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Avira Mail Protection service entered the stop state.
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The VMware Workstation Server service entered the running
Error   2016/7/22 12:52:41  Server  2505    None    The server could not bind to the transport \Device\NetBT_Tcpip_{3C94C61D-BD7D
Information 2016/7/22 12:52:37  Service Control Manager 7036    None    The Avira Real-Time Protection service entered the runnin
Information 2016/7/22 12:52:35  Service Control Manager 7036    None    The SQL Server (SQLEXPRESS) service entered the running s
Error   2016/7/22 12:52:34  NetBT   4321    None    "The name ""ADMIN-PC       :0"" could not be registered on the interface with
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The Server service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The VMware USB Arbitration Service service entered the ru
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The VMware Authorization Service service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The World Wide Web Publishing Service service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The VMware DHCP Service service entered the running state.
Information 2016/7/22 12:52:30  Service Control Manager 7036    None    The QPCore Service service entered the running state.
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Avira Web Protection service entered the stop state.
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The Avira Mail Protection service entered the stop state.
Information 2016/7/22 12:52:40  Service Control Manager 7036    None    The VMware Workstation Server service entered the running state.
Error   2016/7/22 12:52:41  Server  2505    None    The server could not bind to the transport \Device\NetBT_Tcpip_{3C94C61D-BD7D-4E63-9C52-A7FF93CC5C05} beca
Information 2016/7/22 12:52:37  Service Control Manager 7036    None    The Avira Real-Time Protection service entered the running state.
Information 2016/7/22 12:52:35  Service Control Manager 7036    None    The SQL Server (SQLEXPRESS) service entered the running state.
Error   2016/7/22 12:52:34  NetBT   4321    None    "The name ""ADMIN-PC       :0"" could not be registered on the interface with IP address 192.168.20.246. T
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The Server service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The VMware USB Arbitration Service service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The VMware Authorization Service service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The World Wide Web Publishing Service service entered the running state.
Information 2016/7/22 12:52:32  Service Control Manager 7036    None    The VMware DHCP Service service entered the running state.
Information 2016/7/22 12:52:30  Service Control Manager 7036    None    The QPCore Service service entered the running state.
```

相信“海量日志关联分析发现未知威胁”?

“ 不管什么来源的数据都采集进来自然有价值

...我也不知道这些数据能有什么用

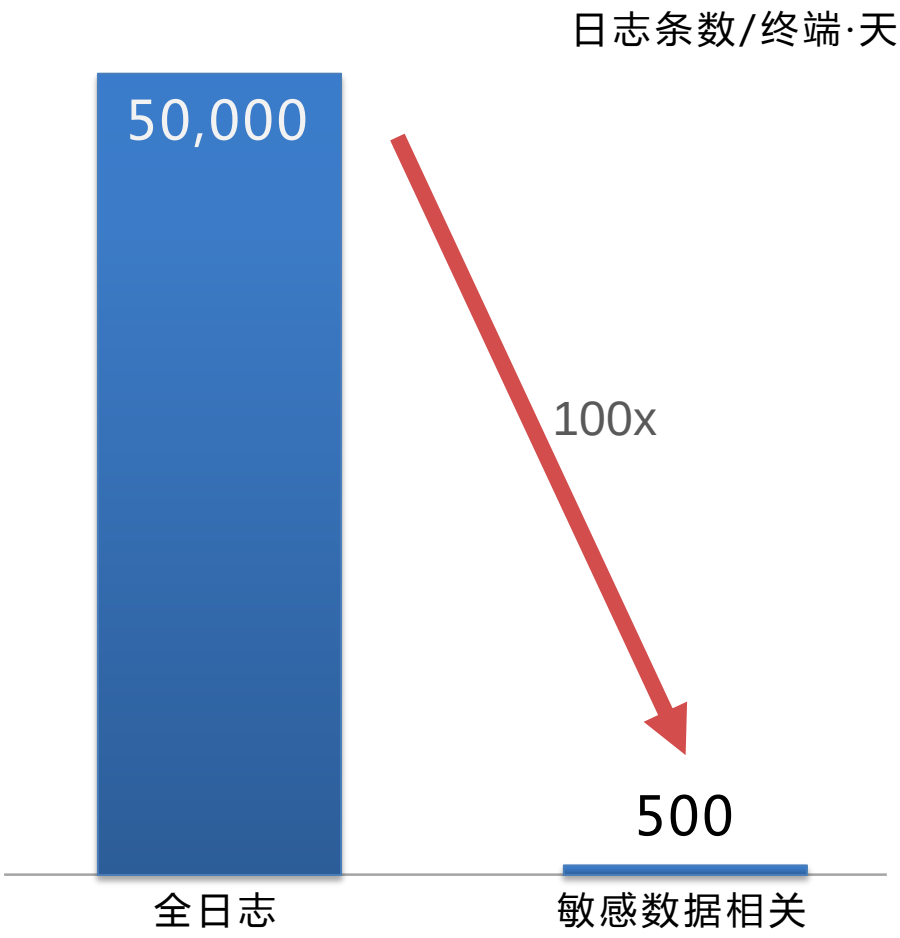
“ 只要数据够大就肯定能关联分析出威胁

...怎么处理数据做关联我也不知道,大家都这么说肯定没错

“ 机器学习和行为分析有很好效果

...我听说公司内有人能跑起来开源算法库

用户行为分析需要对数据有效降维



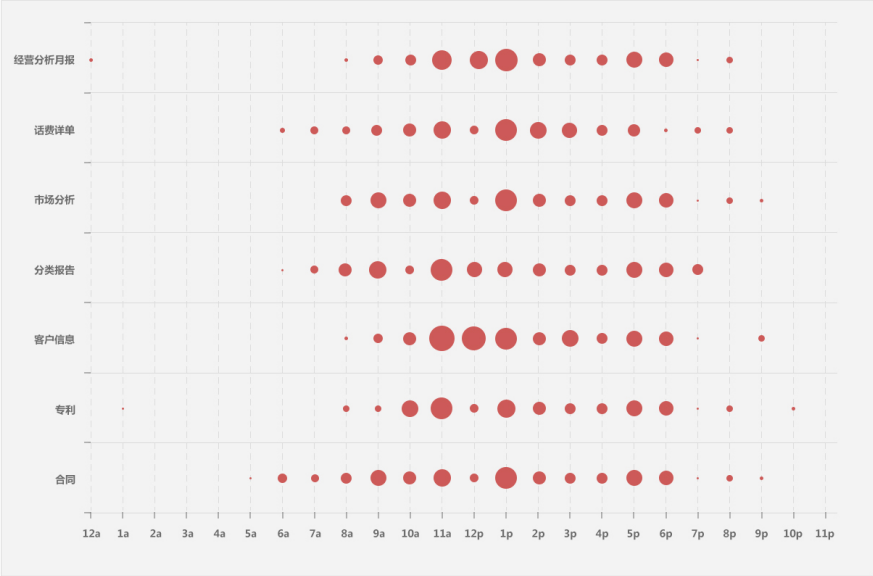
- 海量数据存储和计算的成本
- 日志处理和挖掘的难度
- 网络和服务器的负担
- 行为基线难以归纳
- 异常侦测模式复杂

使用**内容**与**情境**
实现有效降维

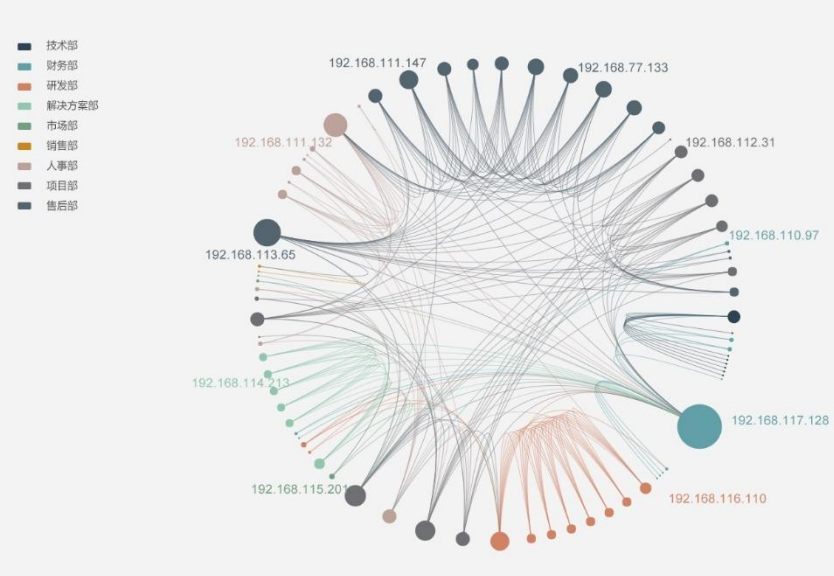
根据内容和情境降维，显著降低数据分析难度

场景：降维后可视化特权用户使用关键数据行为的实例

服务器下载关键数据行为



关键文档传输行为



行动要点（二）

- 有的放矢 – 节制采集有效线索
- 循名覈实 – 语义理解预警威胁
- 数往知来 – 参照案例建立模型
- 操奇计赢 – 先进技术自动猎捕

内部威胁实践的第一准则

以“用户”(人)为终极分析对象

- 改变以“事件”为主的惯常做法
- 预警和检测同样重要
- 员工心理活动成为重要指标

在内部邮件中发现员工心理风险

From: Hu, Rui [mailto:Hu_Rui@emc.com]
Sent: 2006年4月10日 13:48
To: Loke, Soon Choo
Cc: China All (Beijing); China All (Chengdu); China All (Guangzhou); China All (Shanghai); Lai, Sharon
Subject: FW: Do not assume or take things for granted
Soon Choo,
首先，我做这件事是完全正确的，我锁门是从安全角度上考虑的，北京这里不是没有丢过东西，如果一旦丢了东西，我无法承担这个责任。
其次，你有钥匙，你自己忘了带，还要说别人不对。造成这件事的主要原因都是你自己，不要把自己的错误转移到别人的身上。
第三， 你无权干涉和控制我的私人时间，我一天就8小时工作时间，请你记住中午和晚上下班的时间都是我的私人时间。
第四，从到EMC的第一天到现在为止，我工作尽职尽责，也加过很多次的班，我也没有任何怨言，但是如果你们要求我加班是为了工作以外的事情，我无法做到。
第五，虽然咱们是上下级的关系，也请你注重一下你说话的语气，这是做人最基本的礼貌问题。
第六，我要在这强调一下，我并没有猜想或者假定什么，因为我没有这个时间也没有这个必要。

From: Loke, Soon Choo
Sent: Saturday, April 08, 2006 1:13 AM
To: Hu, Rui
Cc: Ng, Padel; Ma, Stanley; Zhou, Simon; Lai, Sharon
Subject: Do not assume or take things for granted
Rebecca, I just told you not to assume or take things for granted on Tuesday and you locked me out of my office this evening when all my things are all still in the office because you assume I have my office key on my person.
With immediate effect, you do not leave the office until you have checked with all the managers you support - this is for the lunch hour as well as at end of day, OK?

愤怒时发泄情绪的邮件

向外界发送恶意诋毁公司的内容

恶意中伤或攻击性用词

对公司制度和业务的冷嘲热讽

讨论不恰当的私人事务

在员工社交媒体中检测负面言论

不满当前状况想离开

7-21 17:47 from 华为G7 Plus

唉，我这人比较恋旧，不愿意挪窝，但是你也不能登鼻子上脸吧，用拿绩效考核考核来搪塞我，老子不干了。。。

7-21 16:47 from iPhone 5s

我一点也不喜欢这里，工资低的可怜，物价高的吓人，还他妈的屁事特别多，关键是好多东西这里都没有卖的，现在还请不准假了，妈的，老子不干了可以吗，老子再也不想在这么个鸟不拉屎的地方呆了

7-21 16:36 from iPhone 6 Plus

他妈的，给那么点工资，还到我这里逼烦逼烦的，老子我还不干了，什么东西嘛！

被猎头说服计划跳槽

7-15 23:16 from iPhone客户端

四十岁这一年 以为没戏了也正中下怀。结果临下班接到猎头电话，说是对方对我还是很满意的，但现在CFO还没到无法下一轮面试。首先肯定我的自信心得到加强，但如果后续面试我成功，我真的要去珠海吗？面试走了一趟，有点打退堂鼓了，公司岗位还不错，但交通实在不方便，我人品又不好经常晚点，犹豫啊。

7-19 16:07 from Android客户端

【区别】面试了两家公司的专业对口岗位，第一家外企，从猎头到中国区经理再到美国经理三次面试，中规中矩客客气气，一周搞定～第二家民企（所谓上市公司，后来发现网上负面消息很多），简历发过去一周没消息，打电话问，回答说还在用人部门那，会尽快返回消息，现在一周又过去了，估计悲催了.....囧...

认为领导对自己有恶意

7-21 09:32 from vivo智能手机

妈的智障！我觉得我公司那个总监就是有病，老跟我过不去，什么屁大点事儿都给我打电话，网站续费协议你自己不会汇报吗非得通过我？说是让我了解，了解你妹啊？！这关我吊事？有的时候让我做啥第二天就忘记了？excuse me？工资那么少并且还没发要求还挺多，有本事你现在发工资或者给我涨工资啊？

6-23 13:52 from iPhone 6

我被我们领导出卖了。我觉得受到了森森的桑害。。。

5-20 18:14 from iPhone 6 Plus

原来世界不公平处处存在不公平待遇，原来之前以为看清的人比雾还模糊，人心果然易变。人往上走，但是你这样出卖自己我心疼你同时看不起你。一个连续作业了28小时的人在什么情况下才能保持正常心态去面对一个背叛者，面对最信任的以为最好的朋友，面对无情的领导对你的施压。用职权欺压，我无话可说。

埋怨体制 负面情绪

4-25 22:52 from iPhone 6 Plus

工作中最难搞的几类人：窝囊上司，不敢出头。年轻manager，以为有个title就牛逼上天了。中年妇女秘书，啥都不想干 啥都往外推，能闲着就闲着。马屁精，跪舔上级 你不强就鄙视你 比他强就讽刺你。其余的找到软的硬的手段都能解决。这几类我是服了。

15-7-9 23:09 from iPhone 5s

加班不算职能部门，抗台风倒要全员待命，请问我一个做工资的待命个什么鬼，领导总是用屁股想问题，自己想跪舔上级拜托别连累我的双休，再见好吗！

大规模实时文本分类是识别风险的基础技术

内容识别技术发展

关键字/指纹

- 入门级

正则表达式组合

- 通配符
- 简单逻辑描述
- 简单关联、序列等

人工智能

- 自然语言处理
- 先进数据挖掘（聚类、分类等）
- 机器学习（无监督、有监督）

支持特征数

- < 5
- 或与关系

- < 20
- 布尔运算

- > 300
- 语义相似度

引入内部非传统IT数据源需要评估其有效性

通讯

- Email
- 聊天
- 电话记录
- 卷宗传递

人力

- 辞职/开除
- 未升职/降职
- KPI考核差
- 病假/事假

交易记录

- 异常交易
- 账户异动
- 异常对手
- 一般风险

安防日志

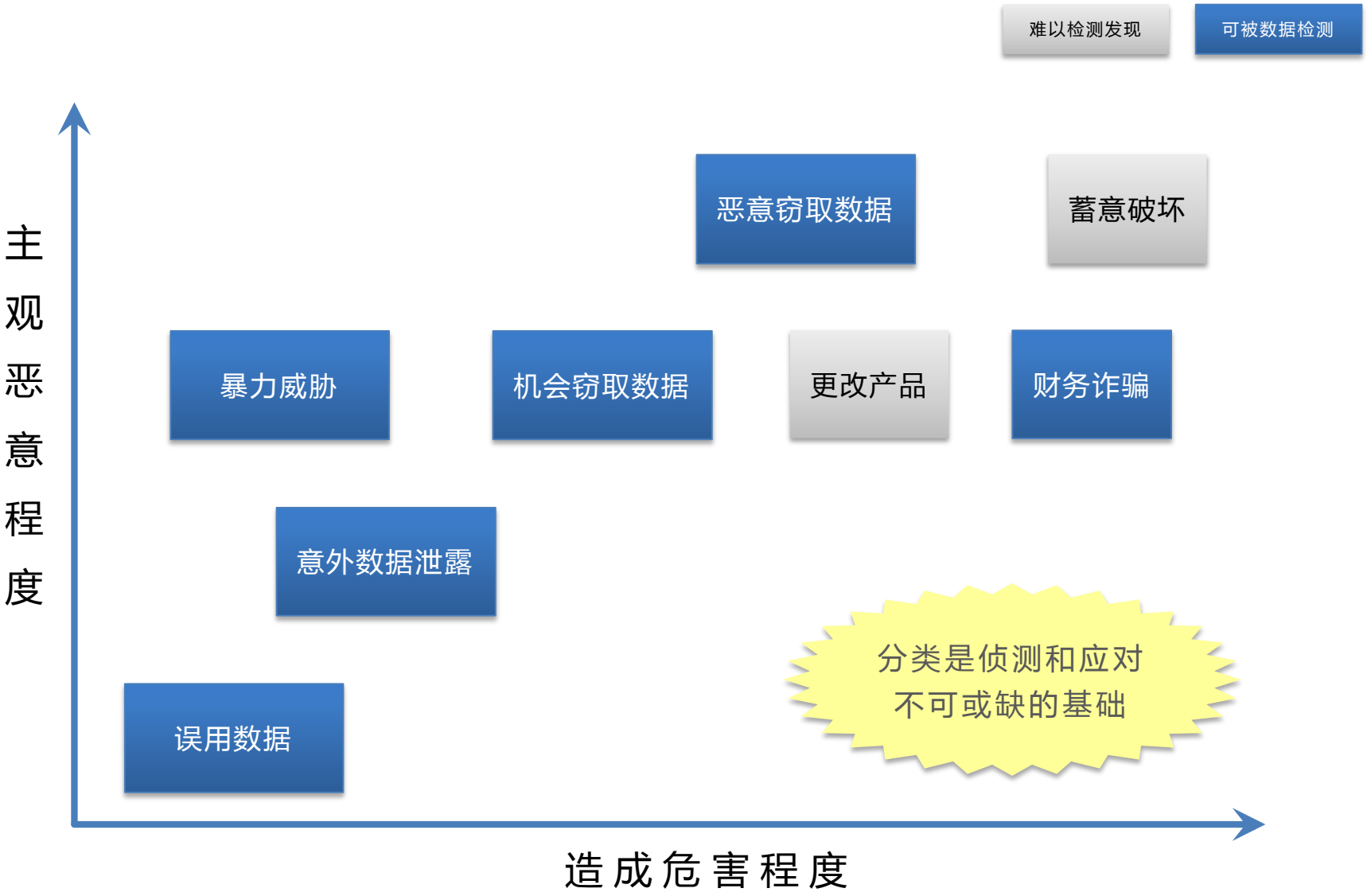
- 门禁刷卡
- 进出记录

- 保密考虑不能获取所有数据，即使有权限采集仍需先脱敏
- 最佳实践：只获取表示风险的指标，否则不采集
- 需要数据接触界面拥有行为分析和机器学习能力

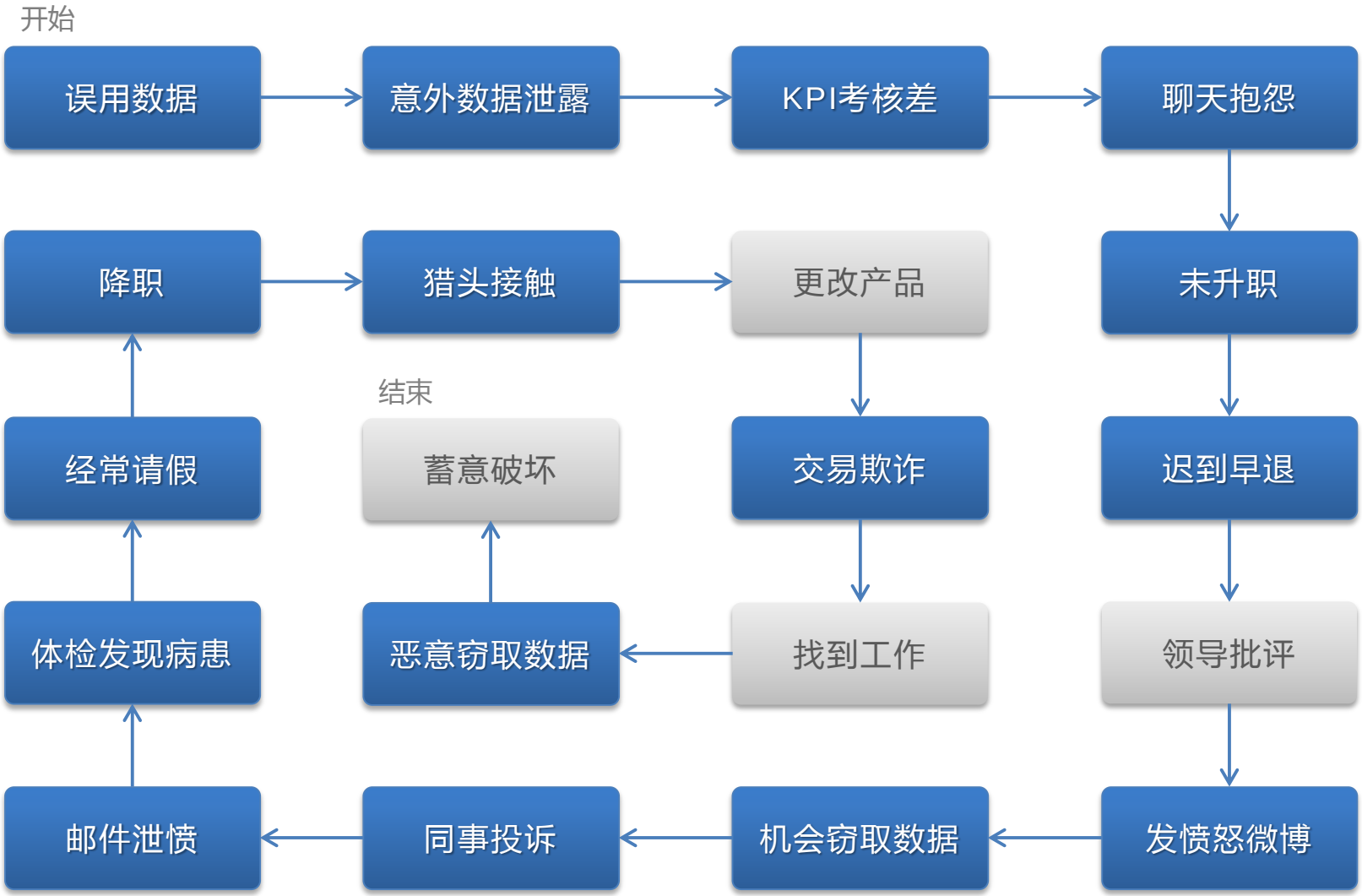
行动要点（三）

- 有的放矢 – 节制采集有效线索
- 循名覈实 – 语义理解预警威胁
- 数往知来 – 参照案例建立模型
- 操奇计赢 – 先进技术自动猎捕

内部威胁分类，是数据分析的基础



行为时序画像是机器学习建模基础



人工选取特征可提高机器学习准确度和性能

高效特征实例

直接

- 发送敏感数据至私人邮箱、大量打印关键文档

行为

- 下载超量敏感数据、频繁换用他人账号登录业务系统

时序

- 生活事件+同事投诉+泄愤邮件、奖金发放+组织变更+猎头接触

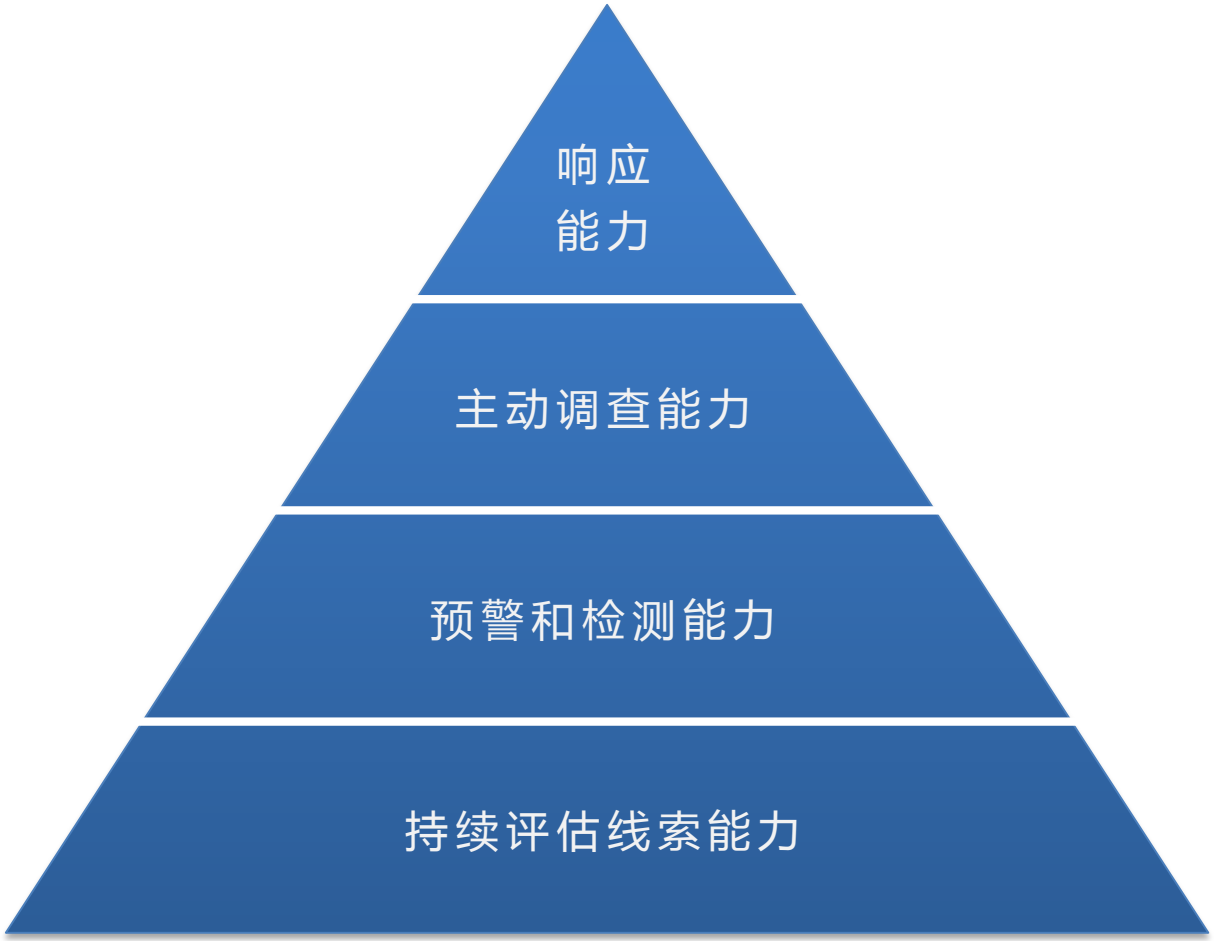
情境

- 角色（供应商、外包商、合同工）、竞争强度、薪酬水平

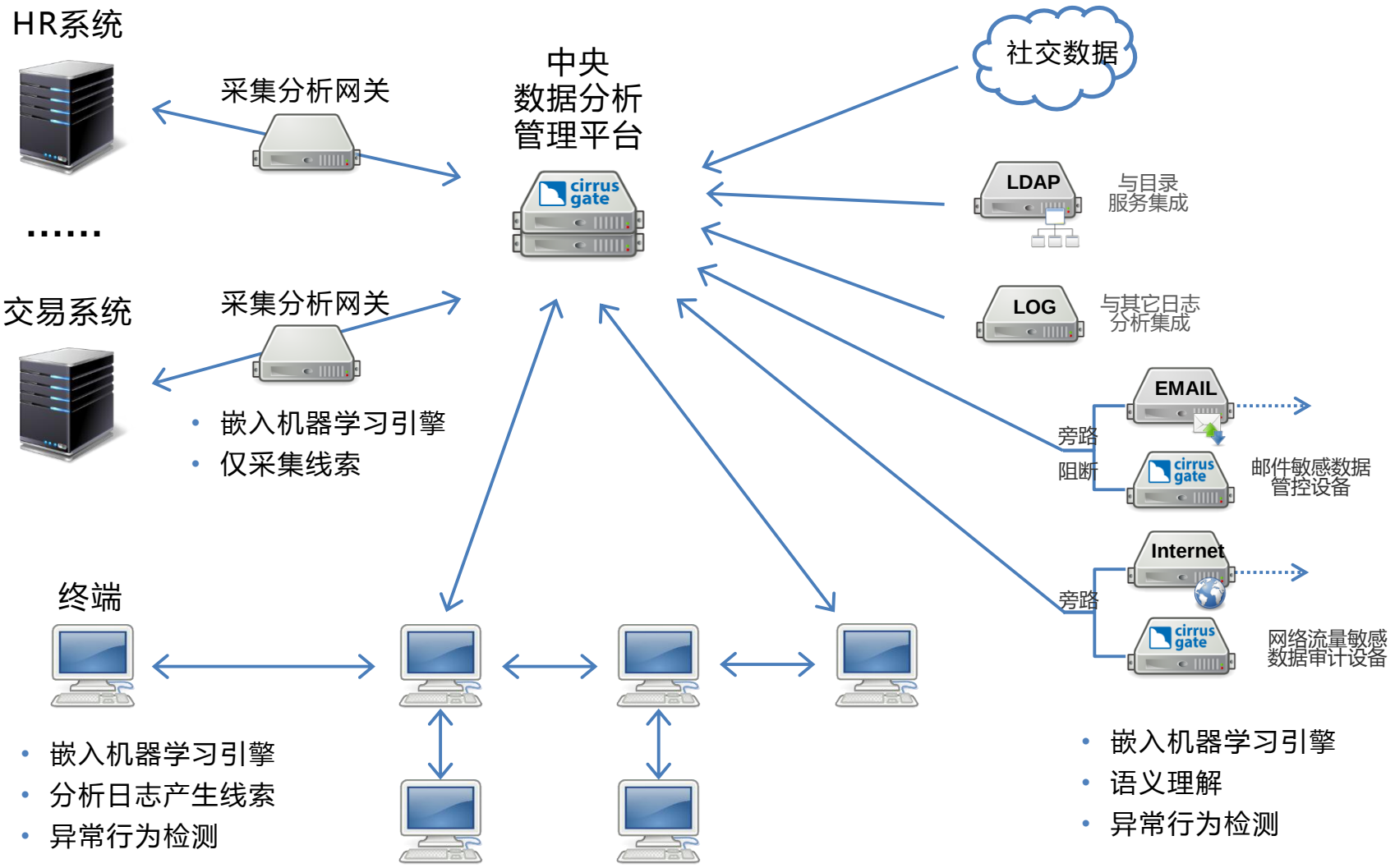
行动要点（四）

- 有的放矢 – 节制采集有效线索
- 循名覈实 – 语义理解预警威胁
- 数往知来 – 参照案例建立模型
- 操奇计赢 – 先进技术自动猎捕

内部威胁防范体系的重要构成



持续监控部署示意图



大数据平台是必须，前端能力亦重要

机器学习和数据挖掘分析也发生在前端接触点

集中式后置

大数据安全分析平台

- 海量数据
- 大规模基础设施
- 强计算能力且可扩展
- 严重依赖开源代码库

分布式前置

终端、IoT

- 少量流数据
- 轻量化嵌入式
- 能适应弱计算能力限制
- 自有算法和代码实现

按用户和实体进行基线统计归纳

遵循“以人为终极分析对象”的原则

端点自身亦拥有检测行为异常能力

基线

- 终端用户行为历史，如A部门用户每天平均访问220次关键数据
- 外发敏感数据行为历史，如用户、设备、时间、频率、和目的地等
- 内部业务系统和服务器敏感数据访问历史
- 业务系统之间、端点设备之间、子网络之间的敏感数据传输

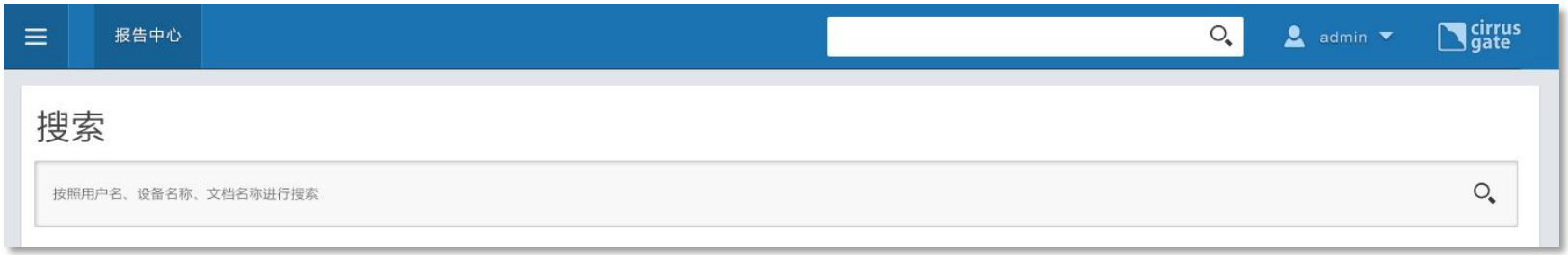
异常检测

- 超过正常访问敏感数据次数5倍以上
- 使用压缩软件RAR打包大量敏感数据
- 向USB设备中密集大量拷贝敏感数据
- 用户或设备频繁外发加密文件
- 从内部服务器下载大量表单等数据
- 大量访问恶意域名 (DNS隐蔽信道点滴外传)

机器学习进行数据分析的实践经验

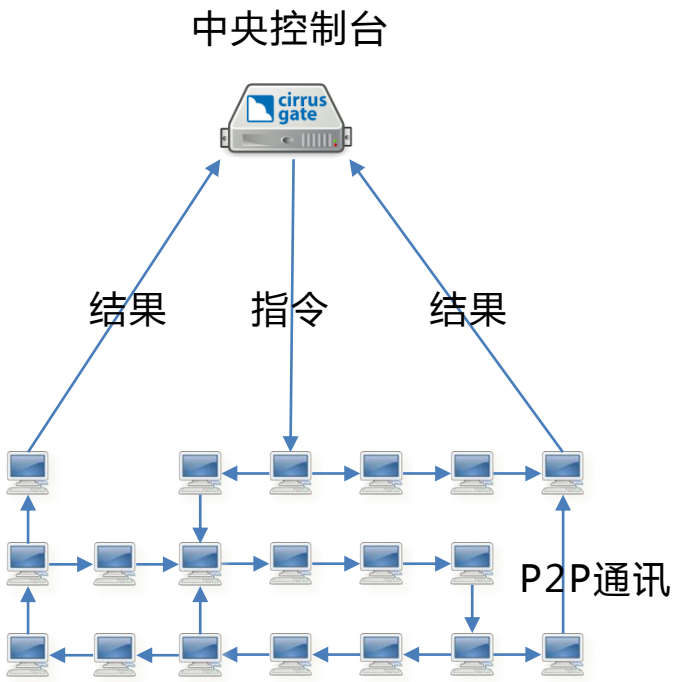
- 降低误报，是现阶段机器学习应用落地亟需解决的问题
- 缺少针对性的数据采集，难以挖掘出有用成果
- 垃圾输入数据，只会造成挖掘难度和成本指数上升
- 未针对场景优化的机器学习，实际效果堪忧
- 特征选择，值得投入资源的提升关键点
- 提高算法效率和准确率，往往需要理解并修改算法的能力
- 自动化，持续处理海量数据实现监控的必备手段

敏捷应答端点信息查询支持调查与响应



- 输入设备名、用户名、文件信息(名称、哈希、类型、日期等)、数据分类、日志关键字、行为特征(打印、U盘拷贝等)、图片等进行搜索
- 快速返回结果列表，用户使用体验良好
- 调查潜在内部威胁，获取详细信息，第一时间做出正确应对

P2P通讯的控制架构保证敏捷应答



- 中央控制服务器只会有选择地向某些终端下发指令
- 终端Agent自动向其它终端通过P2P信道发送指令，完成指令任务后自动将结果汇总传向下一个终端
- 遍历一定规模数量端点后向服务器上传结果
- 算法保证遍历效果
- 极大节约了用于通讯的带宽，并降低服务器负载

逐渐积累高级调查能力形成优势

场景：全局文件追踪溯源分析

- 监控文件流转路径，记录进出终端行为，辅以网关设备更可描绘在网络中扩散路径和关键时间点
- 基于内容识别，少量更改数据仍可有效追踪
- 借助敏捷响应架构和数据分类，快速发现敏感文件并全局定位
- 是调查、取证、与应急响应的核心能力基础

提高内部威胁防范能力 – 行动计划

- 有的放矢 – 节制采集有效线索
- 循名覈实 – 语义理解预警威胁
- 数往知来 – 参照案例建立模型
- 操奇计赢 – 先进技术自动猎捕


cirrus
gate
思睿嘉得
ISC
2016
中国互联网安全大会
360互联网安全中心
展台：A28