让安全可见、可知、可控

人工智能在信息安全领域应用的
前世、今生、未来

瀚思科技产品VP 周奕

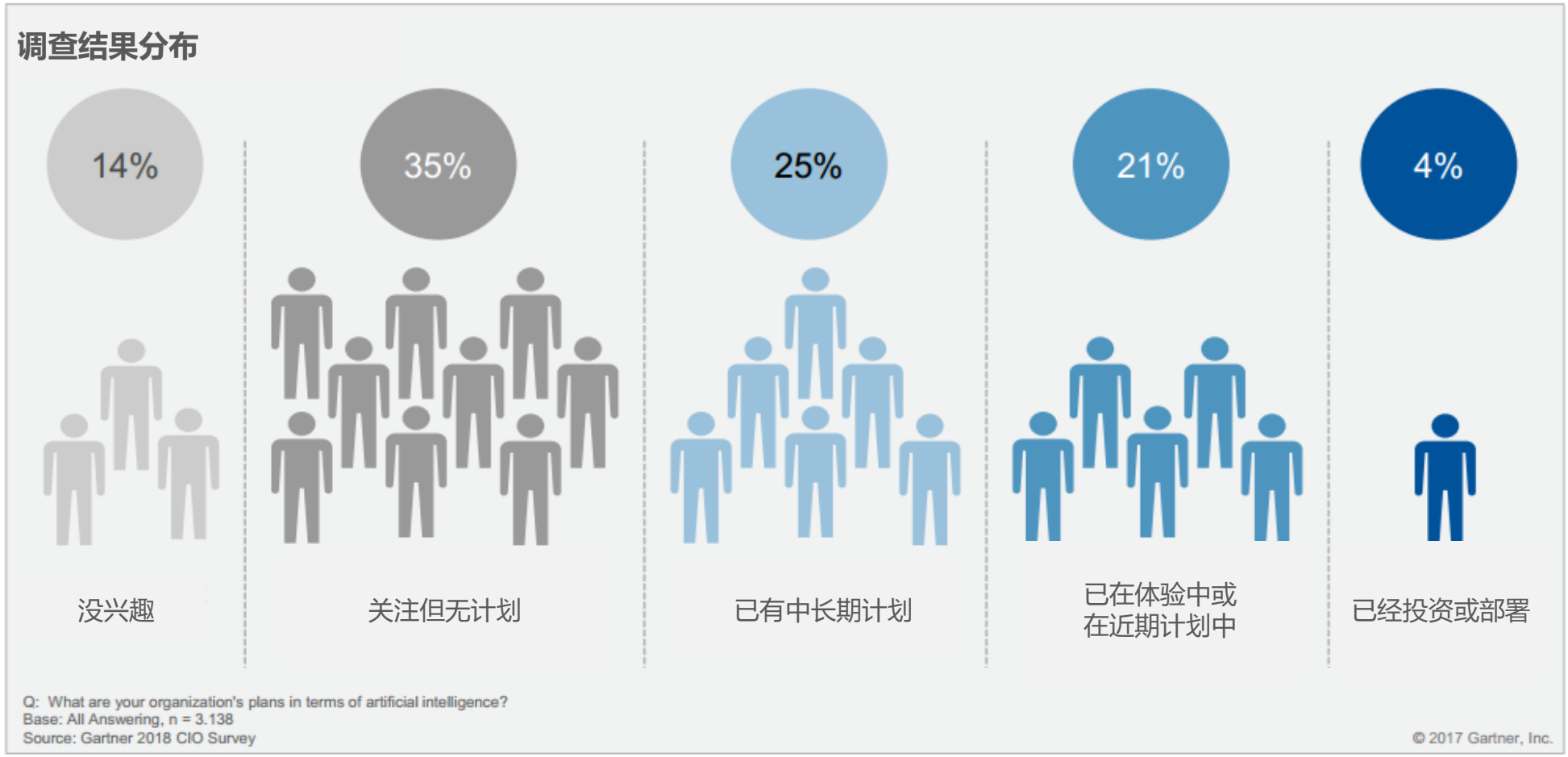
2018 年 12 月

Gartner 2018 CIO 调查：

请问您公司是否打算用AI？

AI 已经逐步被接纳

Gartner 2018 CIO 调查： 请问您公司是否打算用AI?



AI 的价值

AI 技术发展提升数字化生活

AI 核心技术

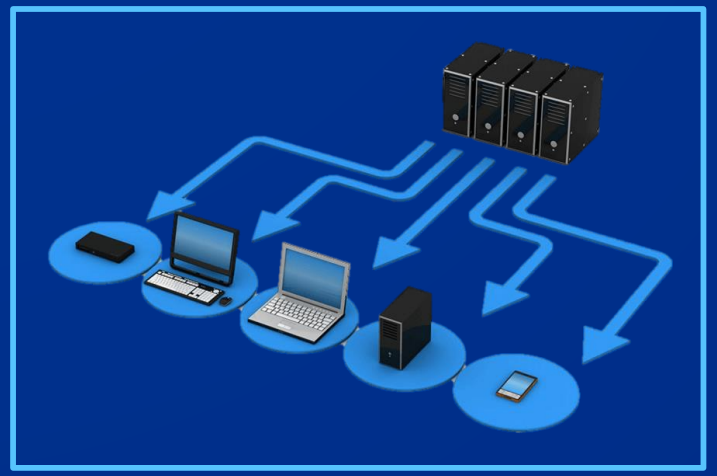
搜索	句法模式识别	客户细分	推荐系统
情绪识别	主题发现	机器翻译	机器人运动
信用卡欺诈检测	天气预报	医疗诊断	广告定位
垃圾邮件筛选	人脸检测	情绪分析	生物信息学
写作识别	金融衍生品交易	脑机接口	自动完成单词
语音理解	游戏竞赛	光学字符识别	DNA 序列分类
库存分析	软件即服务	健康监测	计算机视觉

AI 应用场景

- 大大提高速度和效率
- 更好的数据分析和处理
- 增强客户体验和参与度

AI 应用效果

I U T 驱动安全演进



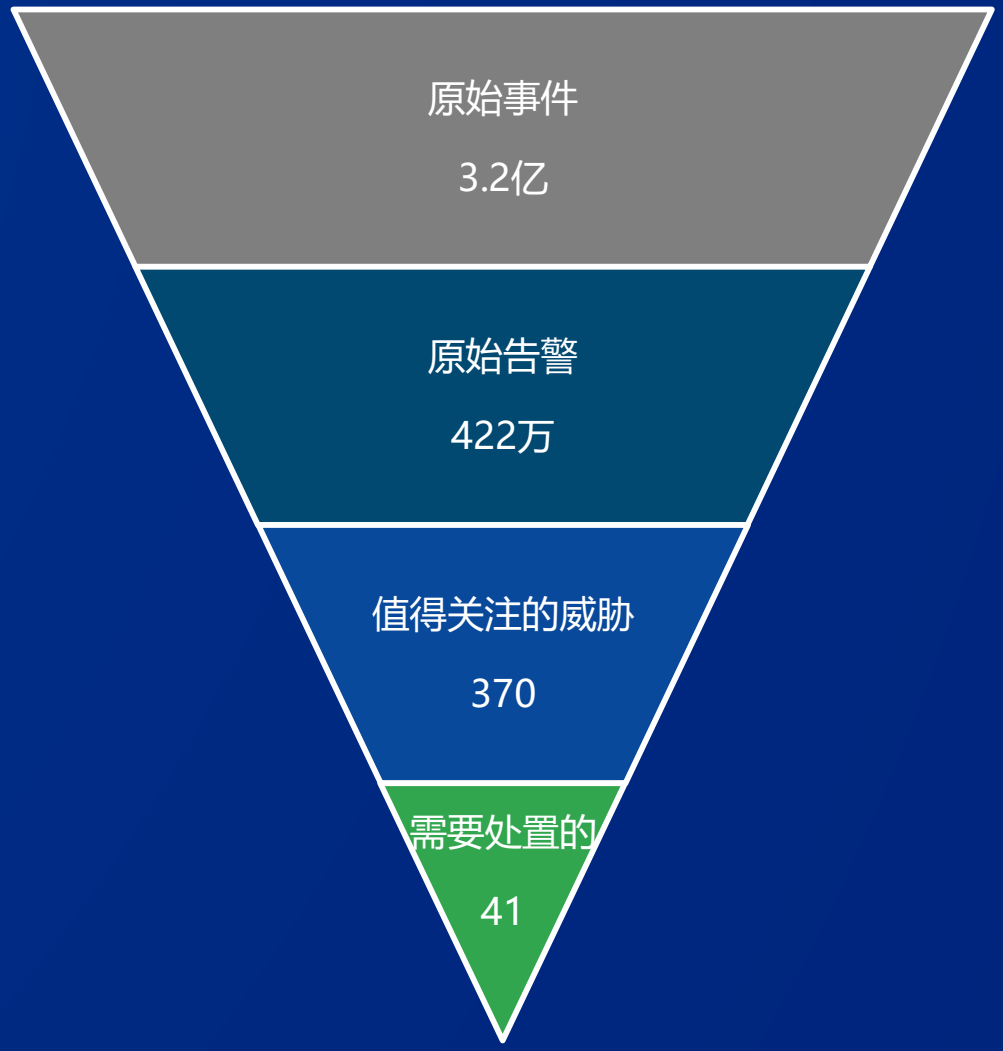
Infrastructure

User

Threat

> 信息安全已经成为智能大数据分析的问题。

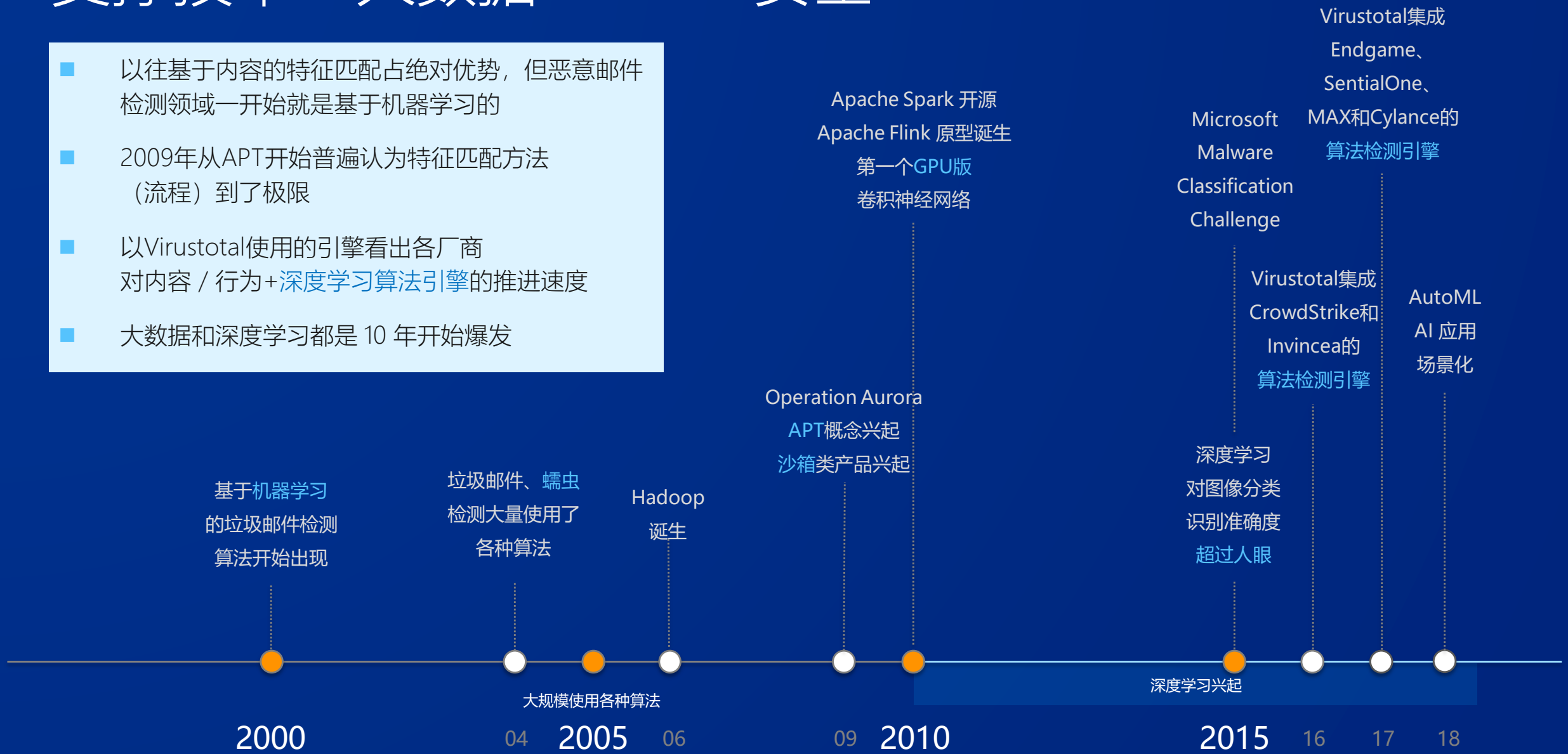
Anton Chuvakin
Distinguished VP Analyst
Gartner



一个典型金融客户一周的安全数据

支撑技术：大数据 + AI + 安全

- 以往基于内容的特征匹配占绝对优势，但恶意邮件检测领域一开始就是基于机器学习的
- 2009年从APT开始普遍认为特征匹配方法（流程）到了极限
- 以Virustotal使用的引擎看出各厂商对内容 / 行为+深度学习算法引擎的推进速度
- 大数据和深度学习都是 10 年开始爆发



AI 在安全领域的成功应用

垃圾邮件识别

异常行为检测

自然语言处理

安全智能分析

AI 在安全领域应用的演进

有统一方法
有预定义模型

有统一方法
无预定义模型

无统一方法
无预定义模型

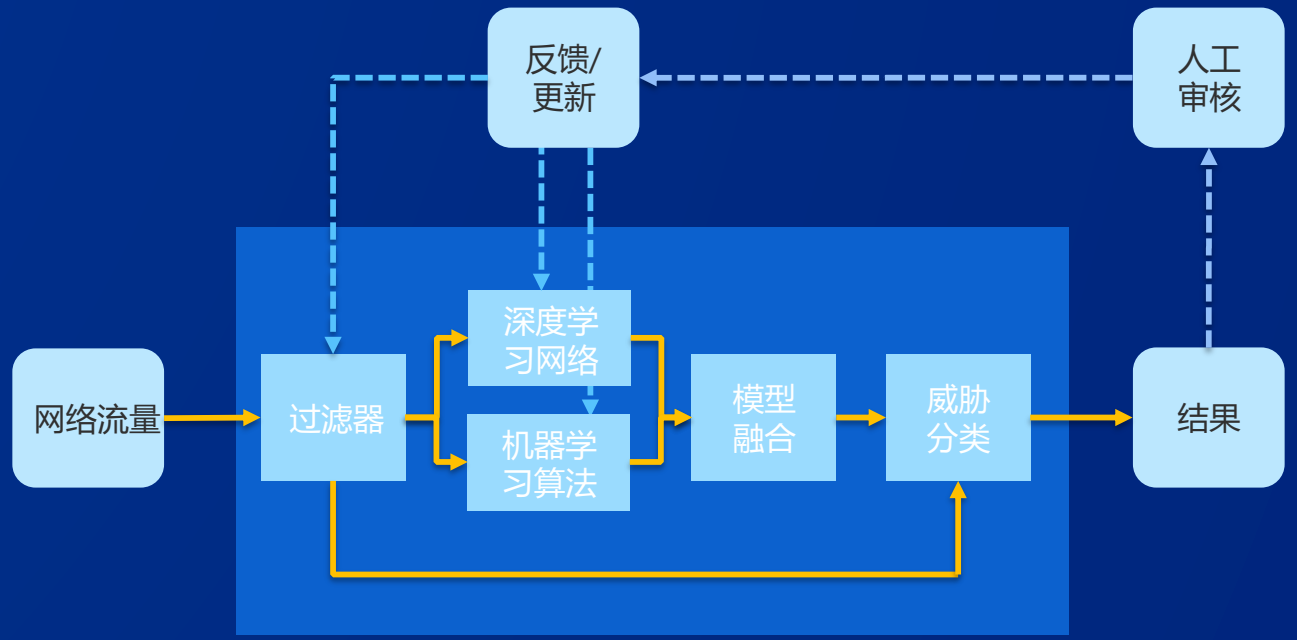
AI 应用在瀚思的实践

HanSight 瀚思

传统流量检测手段

- 固化的规则、语义分析
- 难以平衡误判和漏判
- 规则情景适配度低

自学习、自进化、自适应

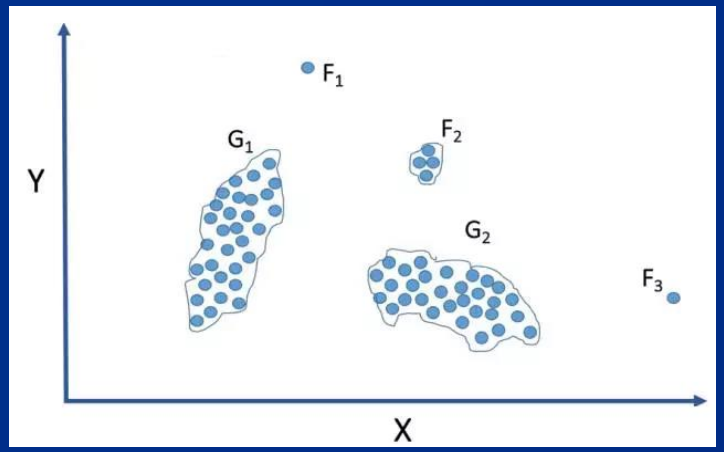


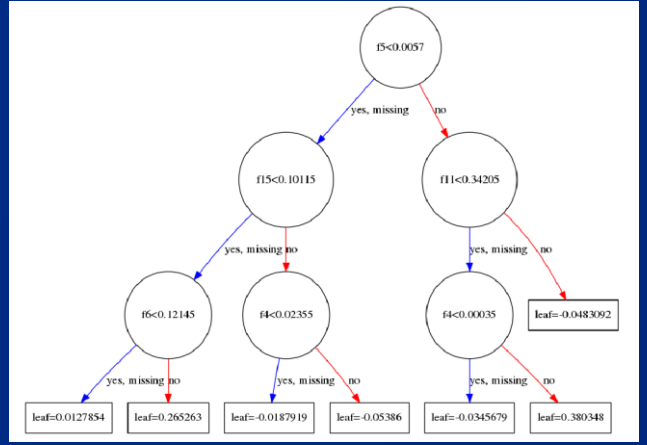
AI 应用在瀚思的实践

HanSight 瀚思

UEBA —— 结合无监督、有监督机器学习算法识别互联网异常访问

- 注册
- 登录
- 交易
- 访问
- 搜索
- 。。。





爬虫

羊毛党

正常

数据解析 → 无监督算法聚类 → 训练有监督算法模型 → 有监督模型检测结果

用户网站访问等网页行为转化为多维度特征值

根据访问网页行为，有相同行为的聚成一类

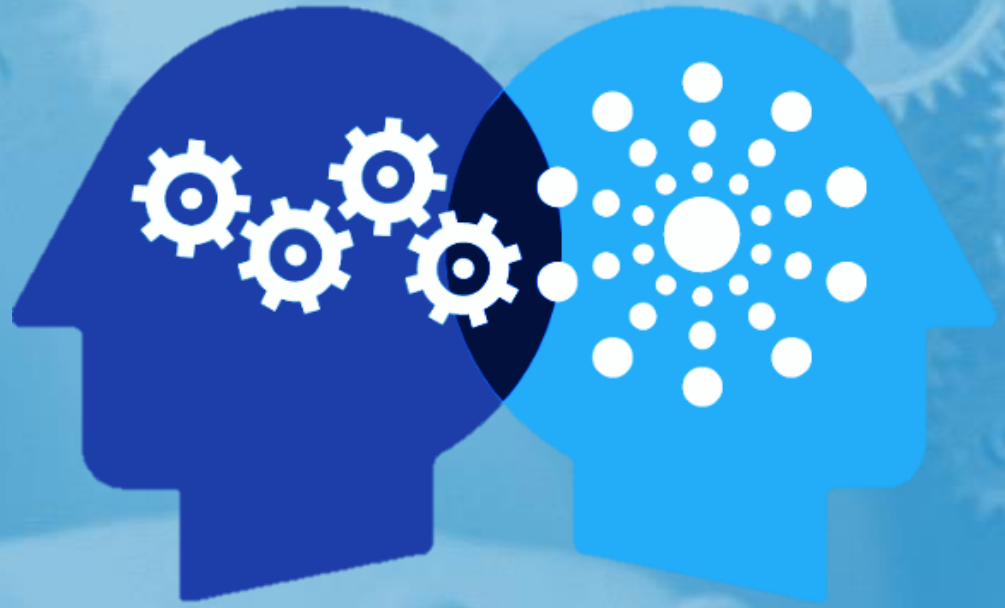
区分正常行为和异常行为，基于分类结果进行有监督模型训练

多算法投票，自动识别出爬虫、羊毛党、正常用户

管理创新是人工智能在安全领域成功的关键

Predicable

提升和革新已知领域



Exploratory

探索和实验解决新的问题

谢谢 |  HanSight 瀚思

www.HanSight.com

微信公众号：HanSight瀚思

北京市海淀区中关村软件园9号楼2区306A