



# 从二维进化到立体：全息安全技术解析

演讲者：程岩（d4rkwind）

百度开放云 & 云安全 资深安全架构师

# 个人简介

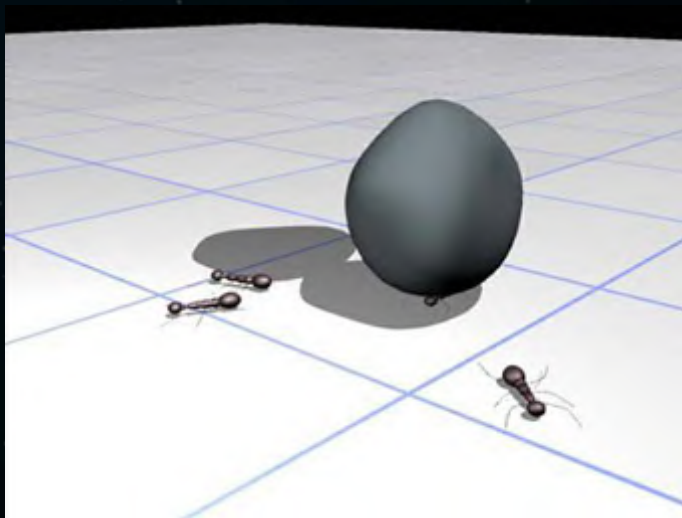
- 情怀：有感于安全不应该只为百度自身服务，转型致力于为互联网安全贡献自己一份力量
- 现在，百度开放云及云安全 资深安全架构师，专注于提供最安全的云计算平台+提供全息安全服务和解决方案
- 曾经，百度产品与业务安全团队安全架构师，带领团队建设百度安全体系、并攻克技术难题

# 目录

- 全息定义
- 企业全息安全理念
- 产品技术解析
- 未来及趋势

# 全息定义

- **全息：反映物体在空间存在时的全部情况的信息。**



# 柏拉图：洞穴之喻

- 投影：洞穴之中的世界相应于可感世界，而洞穴外面的世界则比作理智世界



# 理解全息误区

- 普通3D VS 全息



# 企业全息安全

- 首先，“企业”安全
- 其次，“全息”安全



# 企业的安全之痛

- 有用户 但不可达
- 有规则 但作弊/欺诈
- 有数据 但控制权沦陷
- 有品牌 但被黑
- 有安全 但投入的成本 = 保险

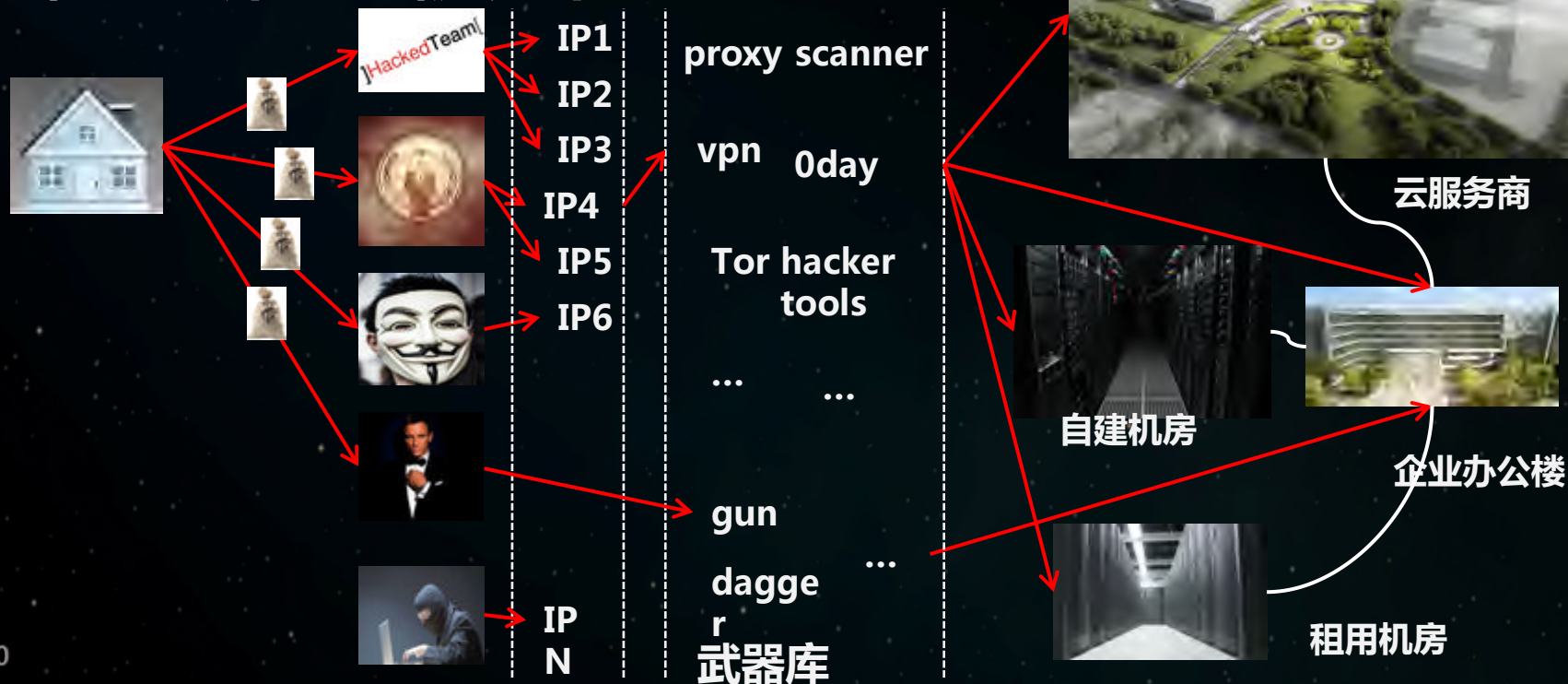


# 甲方安全团队之困

- 基于经验或拍脑袋的项目规划和建设
  - 繁琐重复的运维及响应
- } 安全团队
- 业务啥都不懂，也不鸟
- } 业务团队
- 不出事没人夸，一出事被责问
- } 老板

# 回归企业安全本质

## 物理世界 企业被攻击的全息



# 用全息理念做安全

- 扬长：高维优势
- 避短：单点/兵器库对抗



# 说起来简单，但面临？

- Known Knowns
- Known Unknowns
- Unknown Knowns
- Unknown Unknowns

“极端” case : juniper 某事件和fireeye 某事件

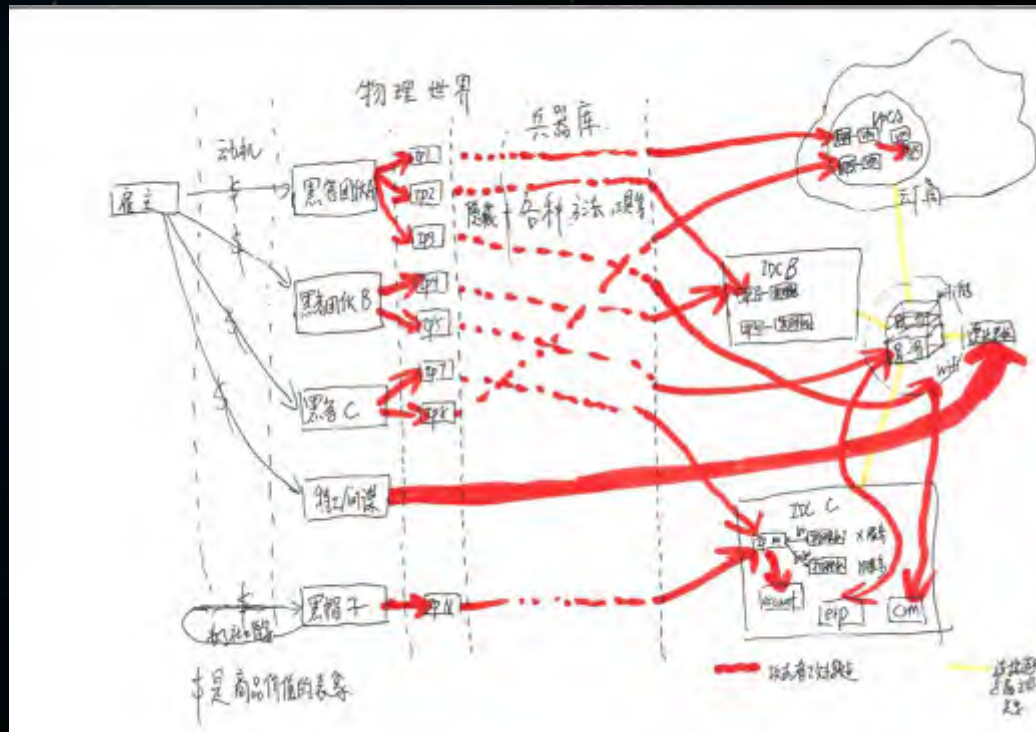
# 让企业掌握其全息安全信息



# 全息安全技术解析

一定维数时空的全息性完全等价于少一个量子位的排列数全息性

- 资产收集及识别
- 风险预警及确认
- 攻击感知及溯源
- 威胁情报及告警



# 资产收集及识别

## 可见资产

- 主机、网络、域名、IP、服务、应用、代码
- 员工

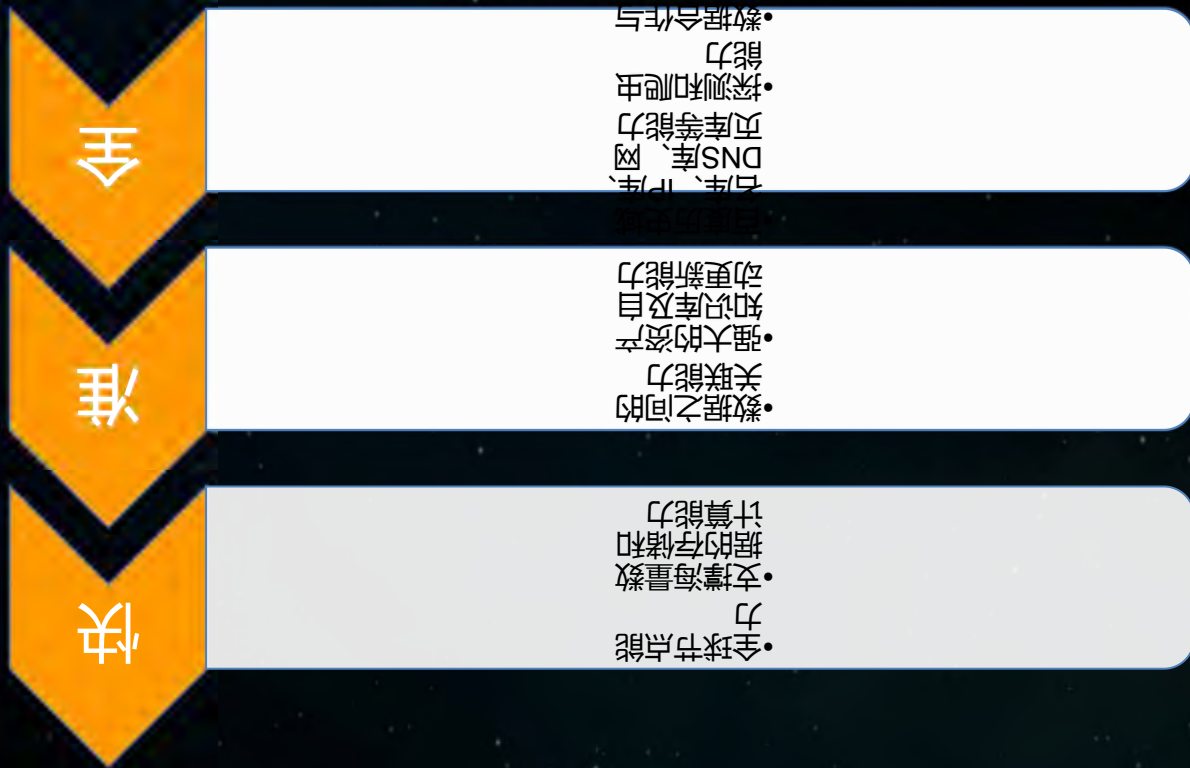
## 不可见资产，什么样？在哪？

- 入口通道
- 员工钥匙
- 关键数据



# 资产收集及识别

How?



# 风险预警及确认

## 风险预警

- 基于0day情报的预警
- 基于漏洞知识库的预警和打分

## 风险确认

- 通用和第三方漏洞的安全扫描
- 基于攻击感知捕获的0day和0day收集计划的安全扫描
- 自动化模拟渗透测试而非Fuzz：举个简单弱口令识别case
- POC => 可控的EXP=》实际后果

# 攻击感知及溯源

基于事件的大数据分析，利用高维优势：



# 攻击感知及溯源

## 异常感知解析

- 基于参数异常
- 基于路径异常
- 基于Session异常

基于传统安全模型（但可以是弱规则）+机器学习等

# 攻击感知及溯源

## 相关感知解析

- 同种类型攻击数据间相关性
- 不同类型数据间相关性（如，HTTP $\leftrightarrow$ SQL）
- 攻击人员间相关性（包括IP）
- 攻击人员与攻击数据间相关性

# 攻击感知及溯源

## 因果感知解析

- 基于时间轴的数据串联
- 基于安全知识库的推论

# 威胁情报及告警

本次大会其他议题讲了很多，这里只举个骗子诈骗的例子

- 环境
- 动机
- 骗子
- 骗术
- 察言观色



# 未来及趋势

- **结合云计算：软件定义+共享经济，大幅降低成本，并提高易用**
  - 事件驱动
  - 灵活调度
  - 弹性伸缩
- **全息+决策+响应**

- **Q&A**