第三届
全国网络与信息安全防护峰会

对话·交流·合作

XDef 2014

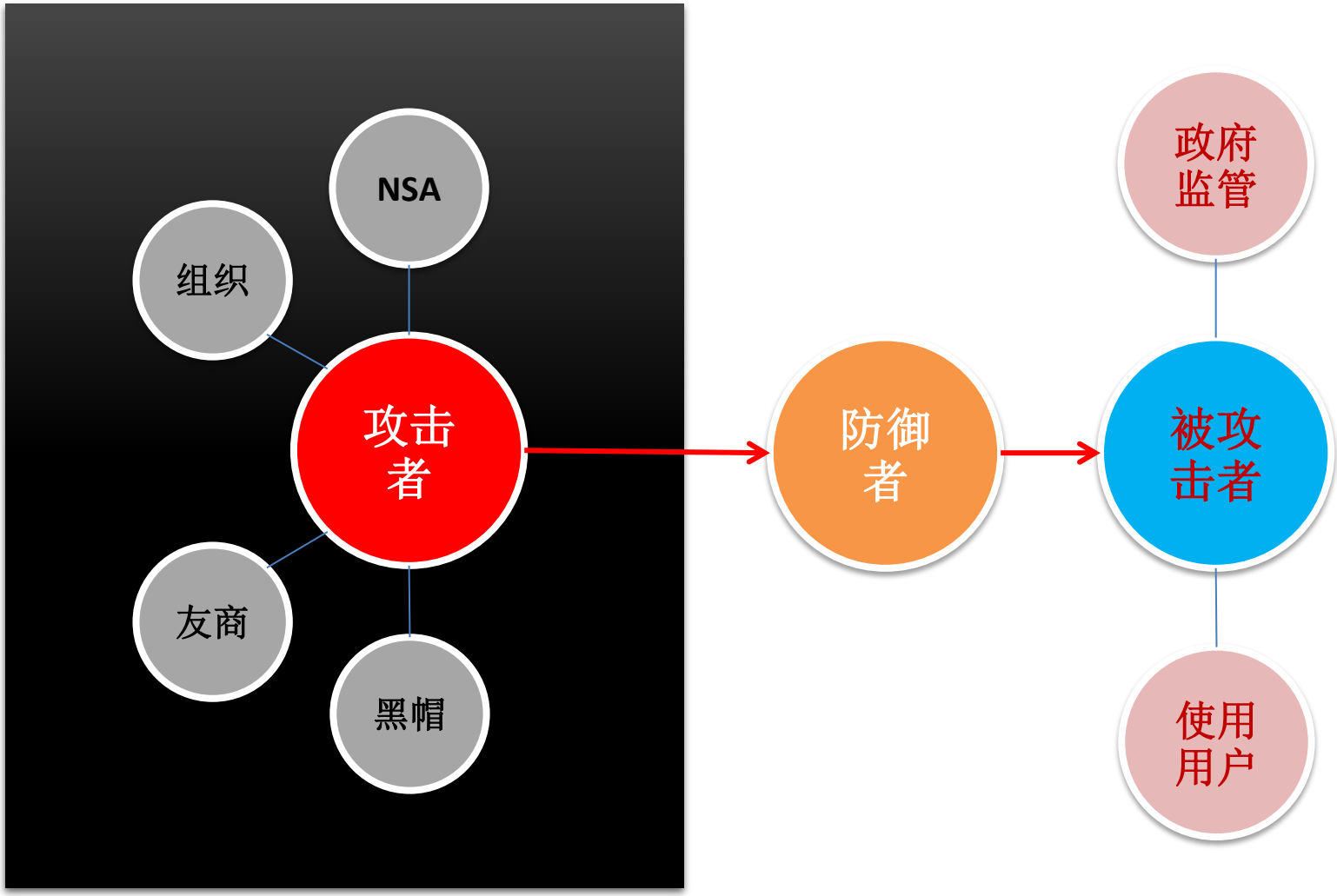
Defense Matrix

Alan Qian
华为技术有限公司

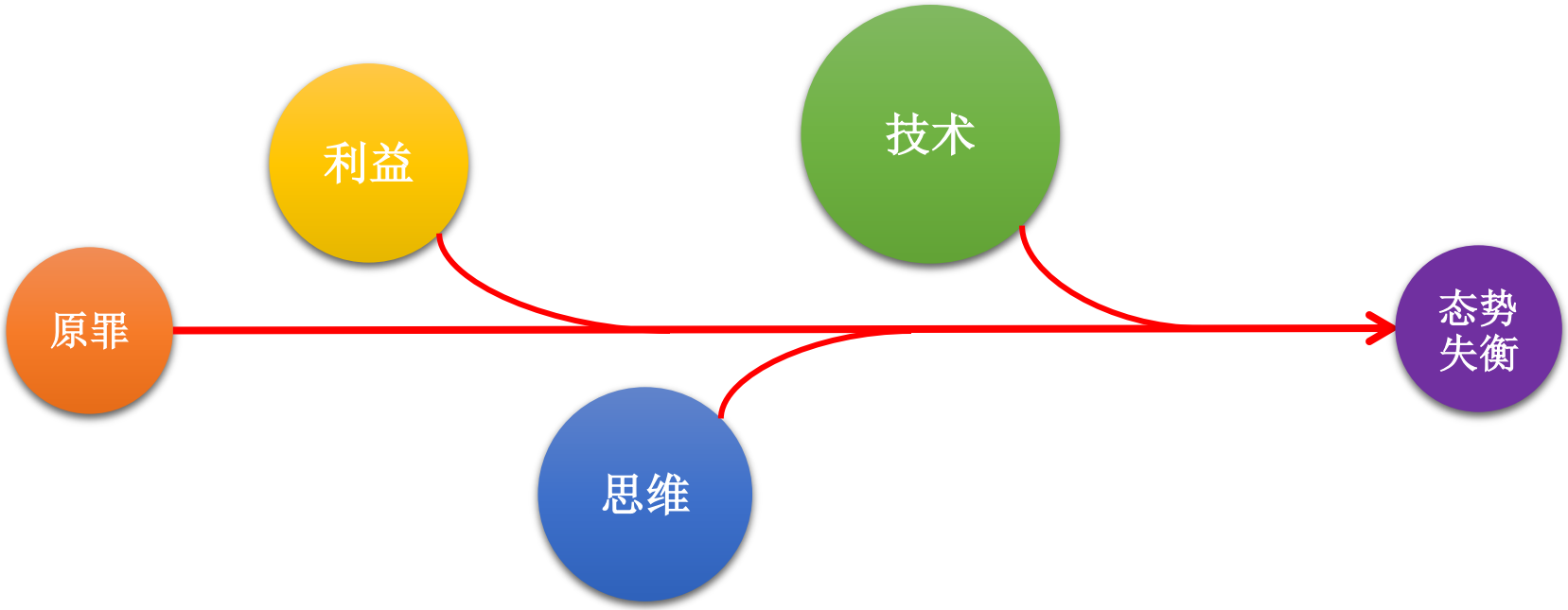
Agenda

- 攻防对抗中的难题
- 防御矩阵
- 安全智能

攻防对抗中的难题



攻防对抗中的难题

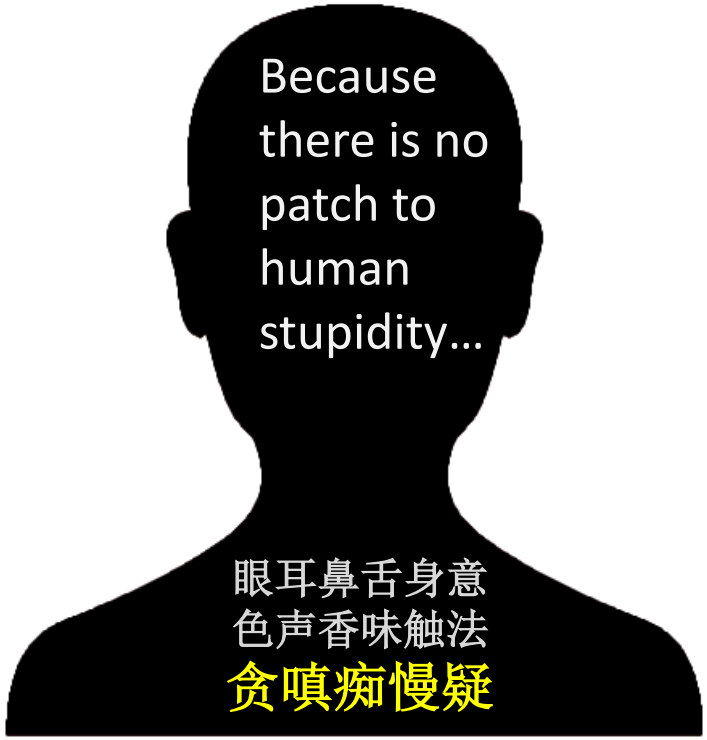


1、原罪：（系统 &人）的脆弱性
2、利益：预期收益 vs 预期风险
3、思维：主动与被动
4、技术：宏观策略、拥有信息、攻守界面、微观技术
5、失衡：攻防态势的不对称性

原罪：脆弱性（OS）


通用OS安全威胁分析
外部实体
网络服务端
spoofing
DHCP/DNS:服务端仿冒，返回错误IP地址欺骗控制
FTP/TELNEL:服务端仿冒，窃取隐私或敏感数据
NTP:返回错误的时间，扰乱业务运行
repudiation
ftp/sftp未做日志审计
登录、注销未做日志审计
外部设备
spoofing
设备是否物理安全，是否提供硬件安全功能
硬件固件被修改
无认证通道
存储
文件
tampering
文件内容被恶意修改
repudiation
日志文件被修改
Information Disclosure
业务数据未加密保存
DoS
文件系统存储空间占满
共享内存
tampering
恶意修改共享数据，造成程序运行异常
Information Disclosure
敏感、隐私数据未加密
DoS
共享内存动态扩大，造成系统资源不足
数据流
网络流
网络数据篡改
tampering
ftp/telnet: 用户名密码泄漏
Information Disclosure
流量通道占用
DoS
系统调用
传递非法参数
spoofing
是否监控关键系统调用
repudiation
未做权限控制，未授权用户可以修改或者控制内核、外备行为
EoP
处理过程
进程
镜像篡改
同名进程
spoofing
缓冲区溢出
命令注入
tampering
关键事件没有审计
repudiation
镜像有明文密码
镜像有敏感数据
Information Disclsoure
数据报处理过载
进程过度占用内存资料
进程运行异常后无法恢复
DoS
进程运行在root权限
进程是否可以赋给更低级别的权限
EoP
内核模块
内核模块被篡改
spoofing
缓冲区溢出
tampering
镜像有明文密码
镜像有敏感数据
Information Disclsoure

原罪：脆弱性（人）


Because there is no patch to human stupidity…
眼耳鼻舌身意
色声香味触法
贪嗔痴慢疑

黑客思维

- 求异思维：寻求否定之否定
- 迷宫模式：入口_@$%&*出口
- 实用主义：“意有定向，招无定式”
- 反功能：misuse, abuse
- 隐藏与混淆
- 拟人拟态
- 社会工程学

编程大师说：“任何一个程序，无论它多么小，总存在着错误。”

初学者不相信大师的话，他问：“如果一个程序小得只执行一个简单的功能，那会怎样?”

“这样的一个程序没有意义，”大师说，“但如果这样的程序存在的话，操作系统最后将失效，产生一个错误。”

但初学者不满足，他问：“如果操作系统不失效，那么会怎样?”

“没有不失效的操作系统，”大师说，“但如果这样的操作系统存在的话，硬件最后将失效，产生一个错误。”

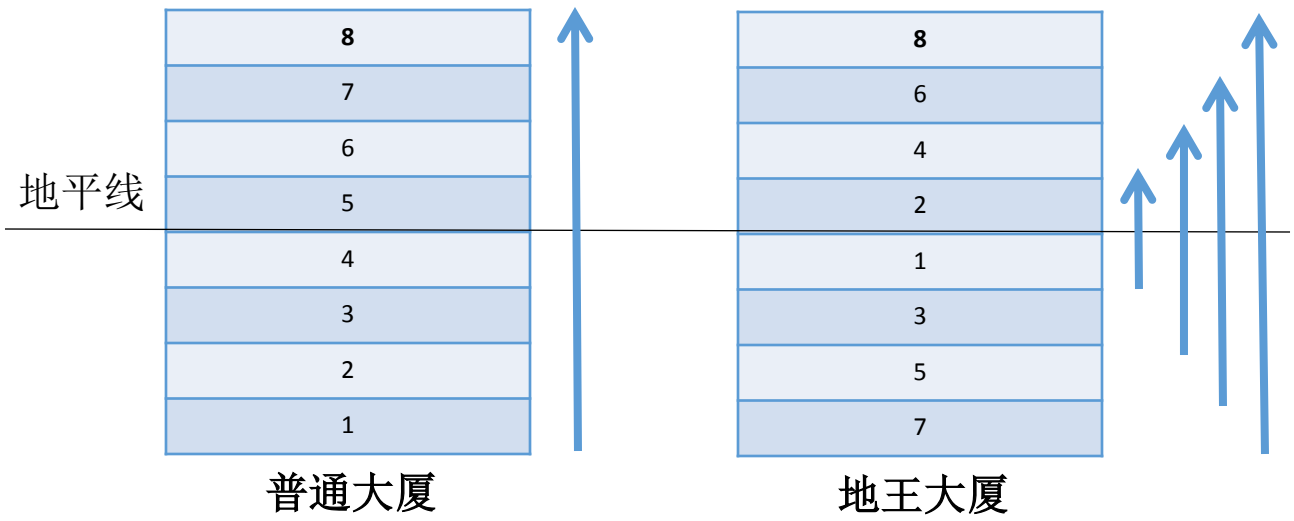
初学者仍不满足，再问：“如果硬件不失效，那么会怎样?”

大师长叹一声道：“没有不失效的硬件。但如果这样的硬件存在的话，用户就会想让那个程序做一件不同的事，这件事也是一个错误。”

没有错误的程序世间难求。

[Geoffrey James 1999 《编程之道》]

黑客思维



前提	思考过程	结论
No 对某一个前提的否定	??? 努力思考	Yes / No 对自己的肯定或否定

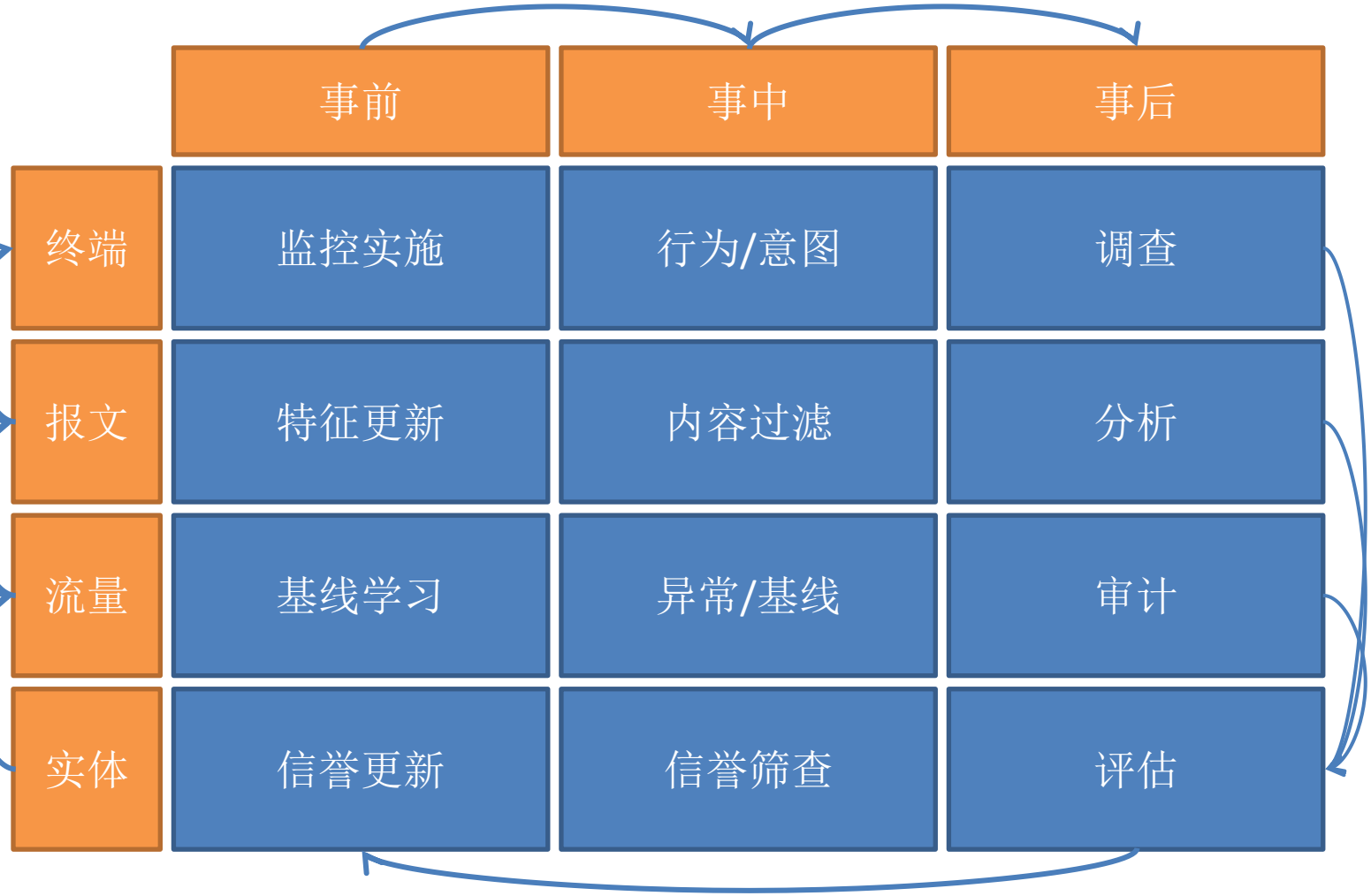
技术难点

- 人机分别
- 相似度判断
- 相关性分析
- 语义理解
- 信誉评估
- 自动化提取特征或生成模型

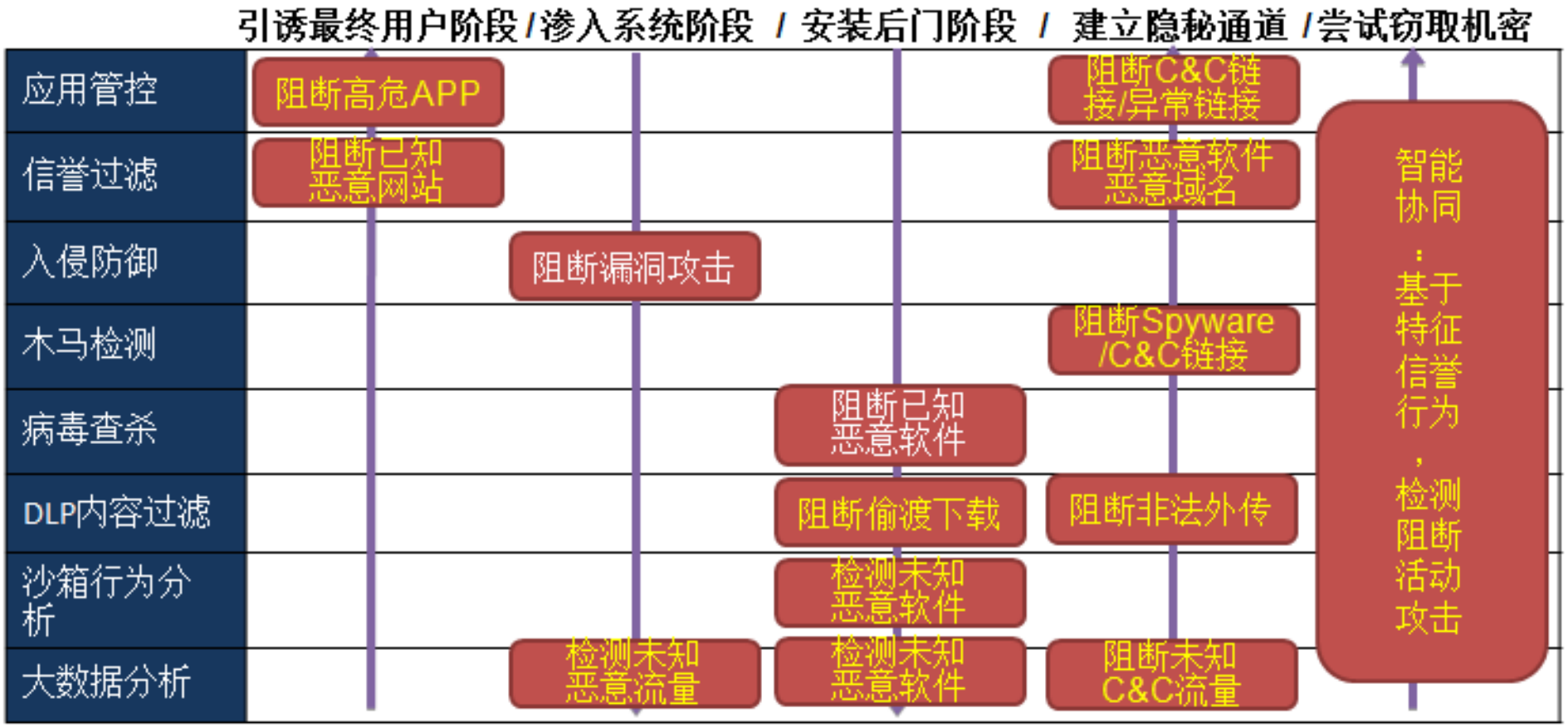
Agenda

- 攻防对抗中的难题
- **防御矩阵**
- 安全智能

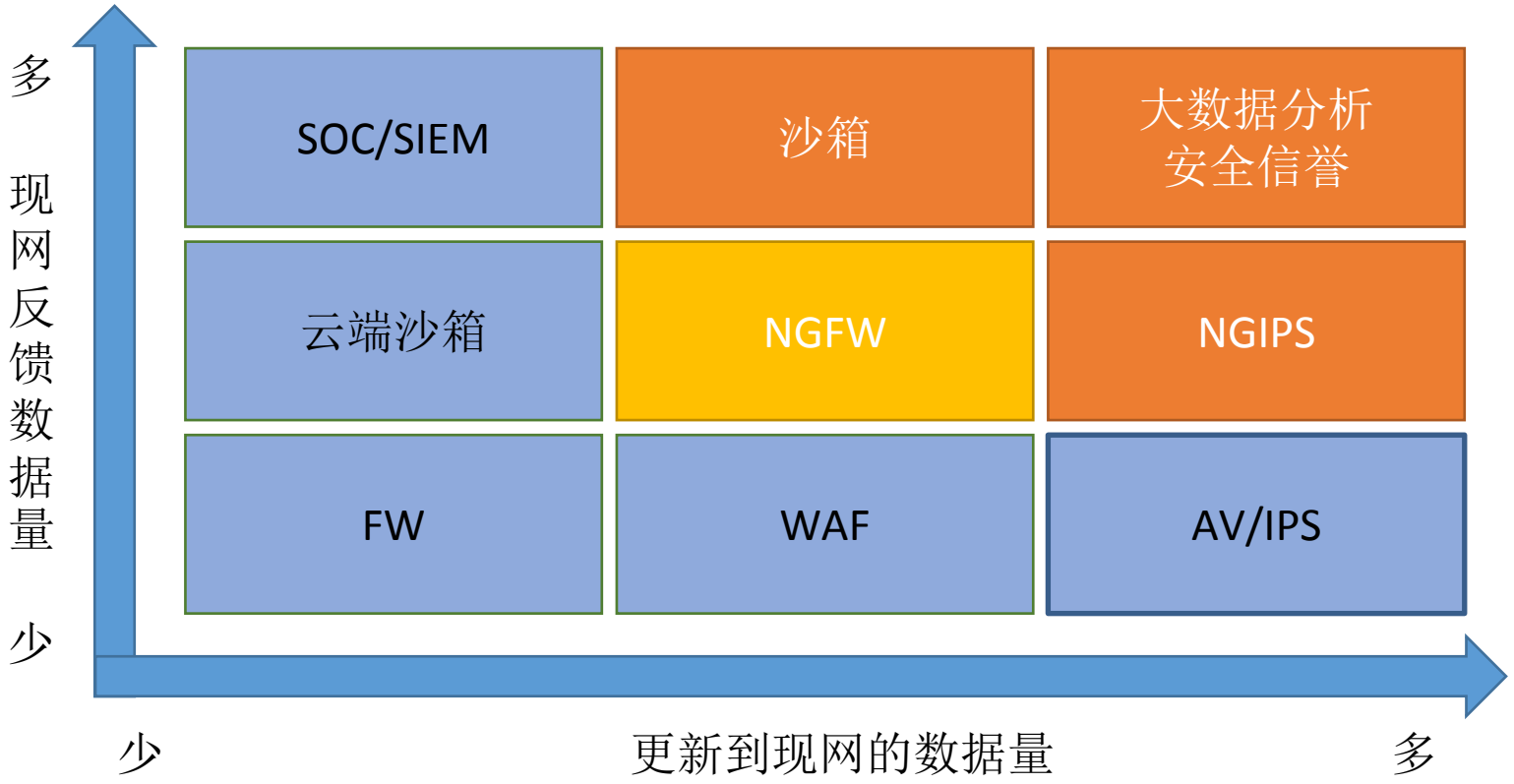
防御矩阵（时空纬度）


事前
事中
事后
终端
监控实施
行为/意图
调查
报文
特征更新
内容过滤
分析
流量
基线学习
异常/基线
审计
实体
信誉更新
信誉筛查
评估

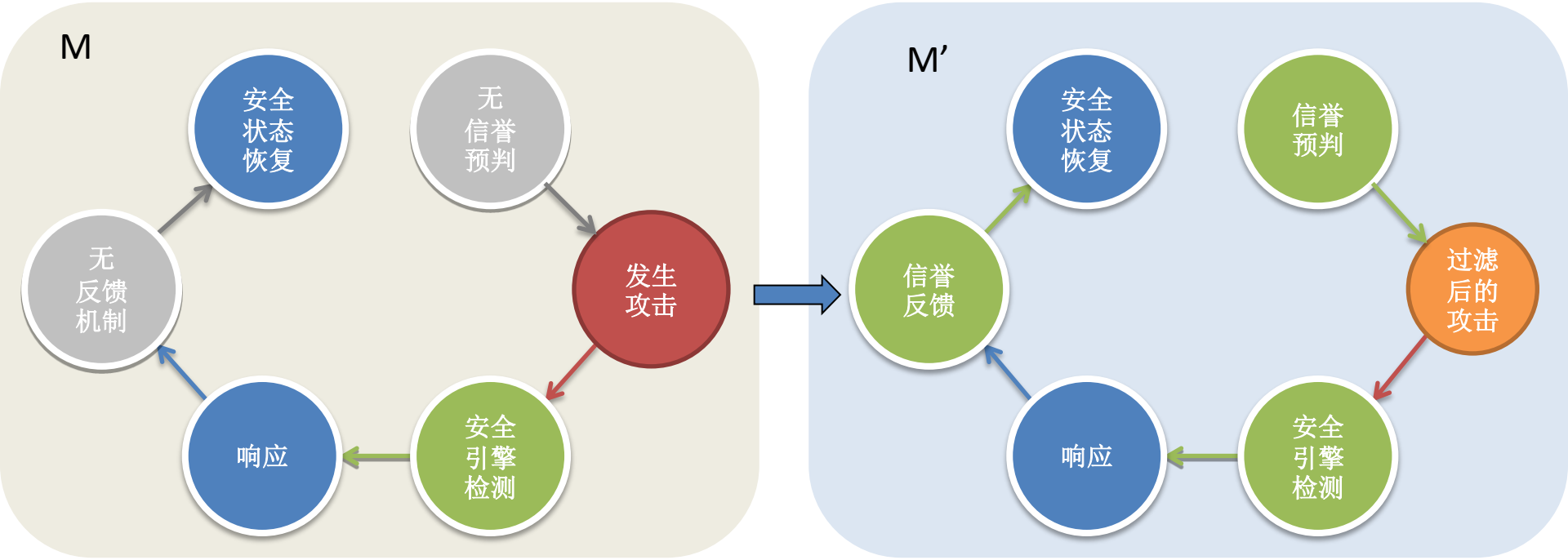
防御矩阵（KillChain纬度）



防御矩阵（信息流纬度）


多
现网反馈数据量
少
SOC/SIEM
沙箱
大数据分析
安全信誉
云端沙箱
NGFW
NGIPS
FW
WAF
AV/IPS
少
更新到现网的数据量
多

防御矩阵（演进实例）



#	信誉模型	特征库模型
时间成本	**低。**依据访问对象的可信程度进行预判，在检测链上的最前端起作用。	**高。**根据数据内部特征进行检测。在检测链上的中段起作用。
资源成本	**低。**基于最少的信息量作决策，资源最节约。可处理大部分常见的可信与不可信链接。	**高。**需要解析报文内容，需要大量的CPU与内存。较难适应流量模型的变化。
智能协同	**好。**检测结果通过信誉反馈对防御能力形成贡献。	**差。**缺少信誉反馈，防御能力无法闭环提升。

Agenda

- 攻防对抗中的难题
- 防御矩阵
- **安全智能**

安全智能

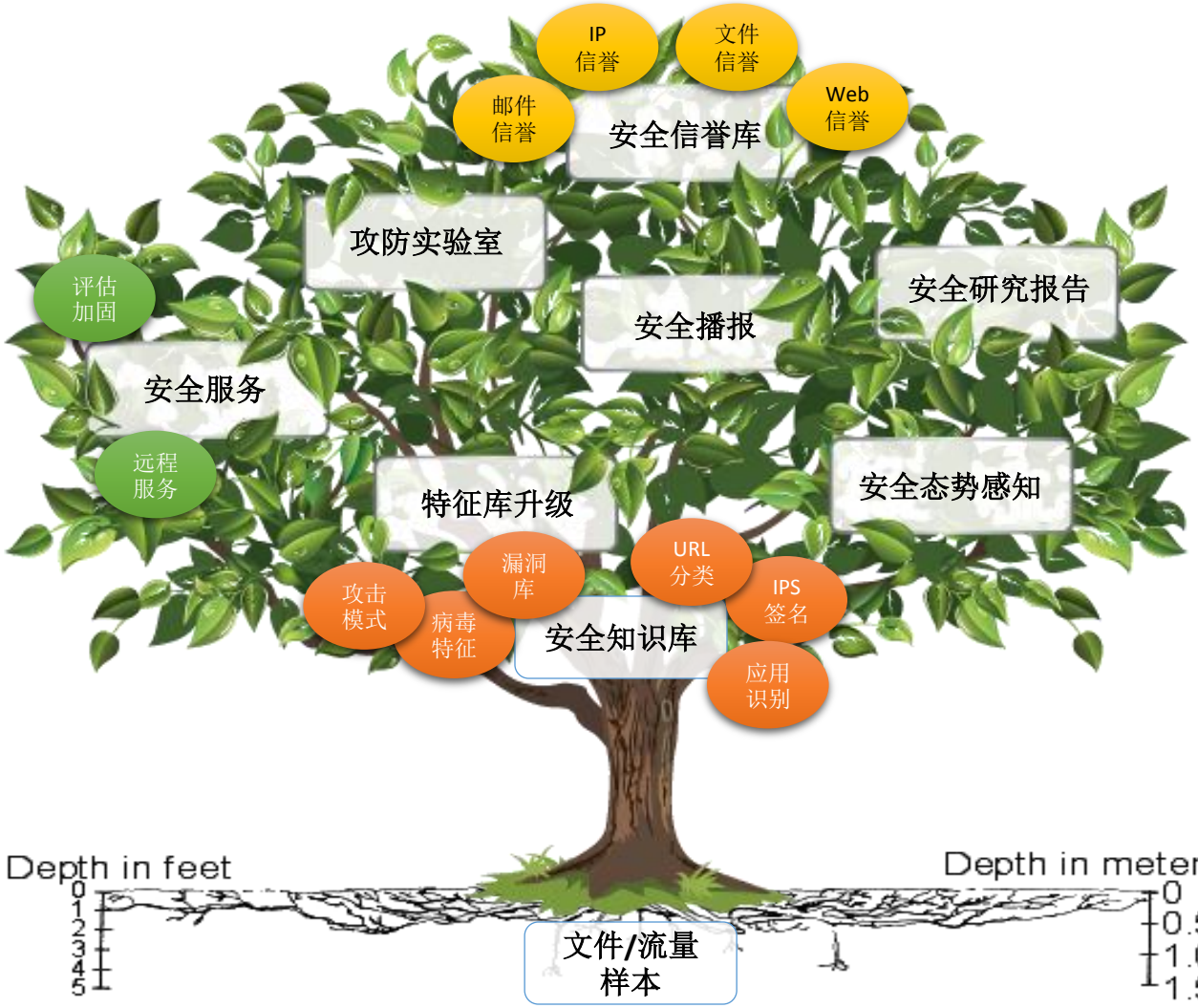
1、安全的服务对象是“被攻击者”，安全能力的服务对象是“攻击者”。
服务的内容是提供知识与防护手段。

2、安全的价值在于迅速将不安全的状态转换为安全，并尽量提高攻击成本。
对已知威胁根据风险与成本取舍。
对未知威胁提升免疫力降低风险。

3、安全是模式的科学，其核心工作是构建安全知识系统。
安全技术通过模式的挖掘，把潜在的威胁呈现出来。

4、大数据改变了安全知识挖掘的方式，从实验模拟发展到密集计算，进一步完善了安全知识的积累手段，是安全智能化的基础。

安全智能



安全信誉

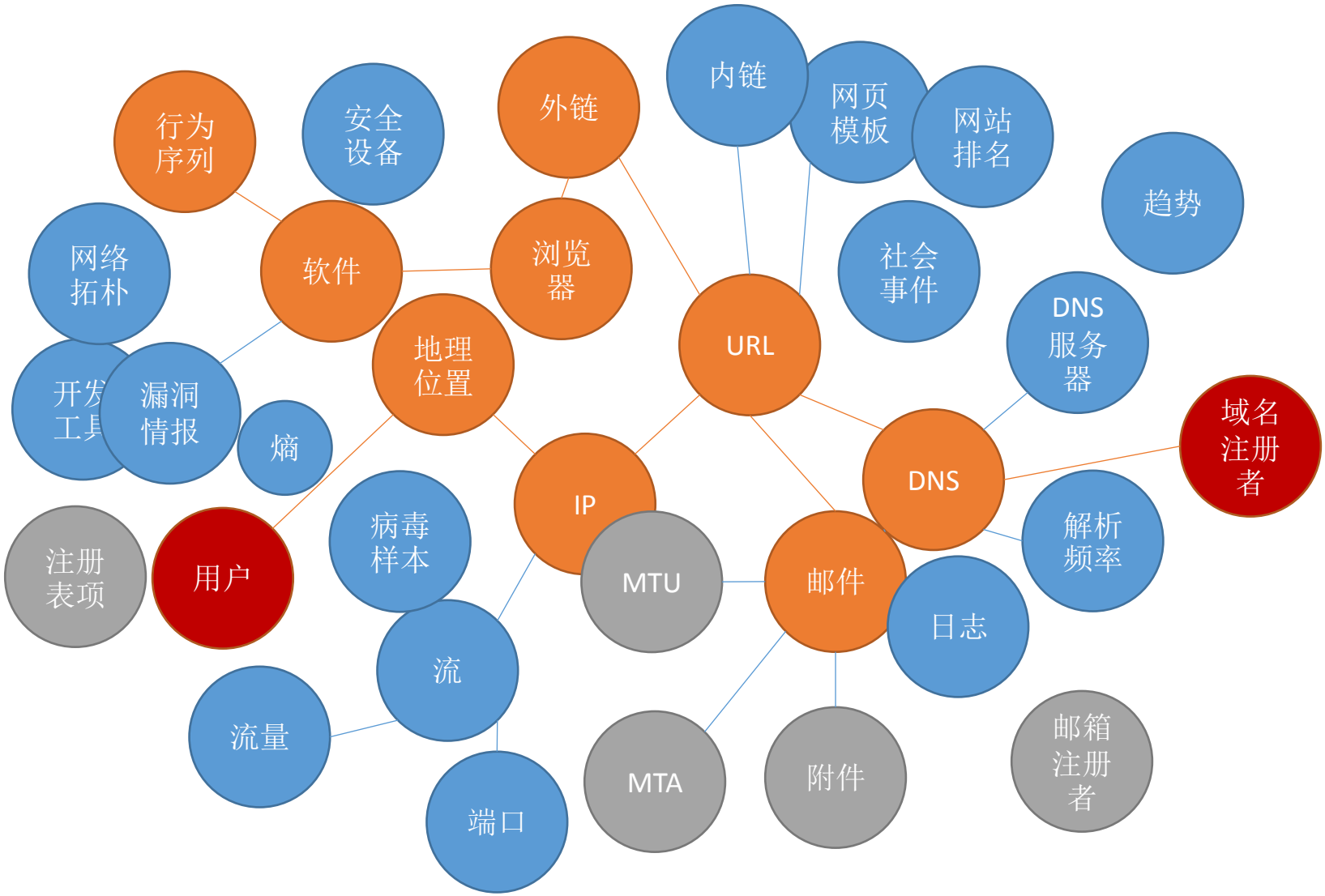
安全模型

安全特征

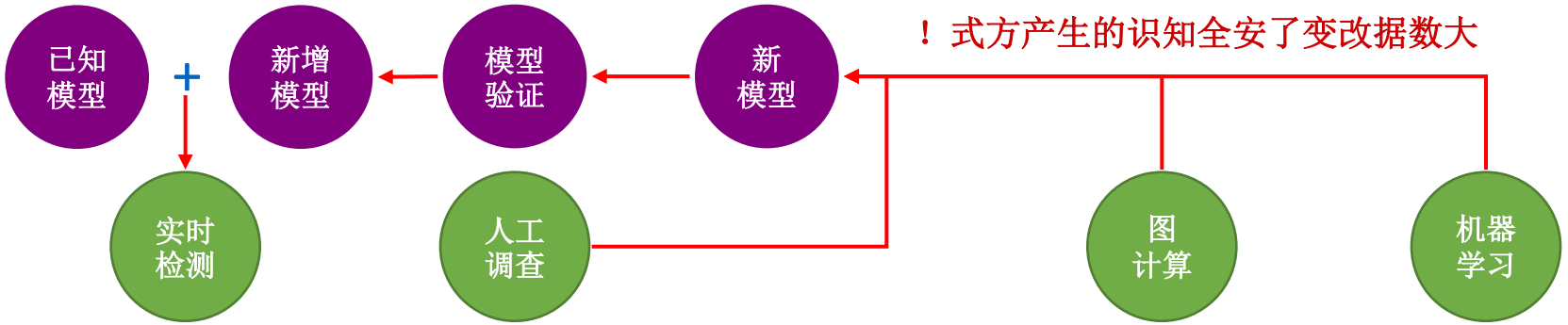
威胁分析

样本

知识的涌现

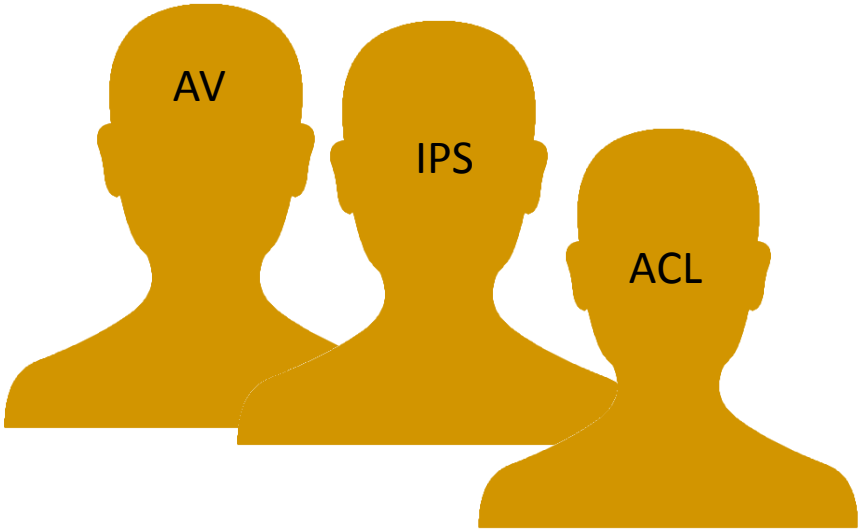

行为序列
安全设备
外链
内链
网页模板
网站排名
趋势
网络拓朴
软件
浏览器
社会事件
DNS服务器
开发工具
漏洞情报
地理位置
URL
域名注册者
熵
DNS
解析频率
注册表项
用户
病毒样本
IP
MTU
邮件
日志
流
流量
MTA
附件
邮箱注册者
端口

知识的涌现



流处理与CEP Storm / Truviso / Spark Steaming	交互式SQL Impala / Drill / Splice Machine	GraphiLab / GraphX (Graph Analysis)	Titan / Gremlin (Graph DB & traversal)	Mahout / 0xdata (Batching ML)
	Spark (Fast memory-optimized execution engine)		MapReduce	
YARN / Mesos (Multi-memory Resource Management)				
MapR-FS / MapR Table				

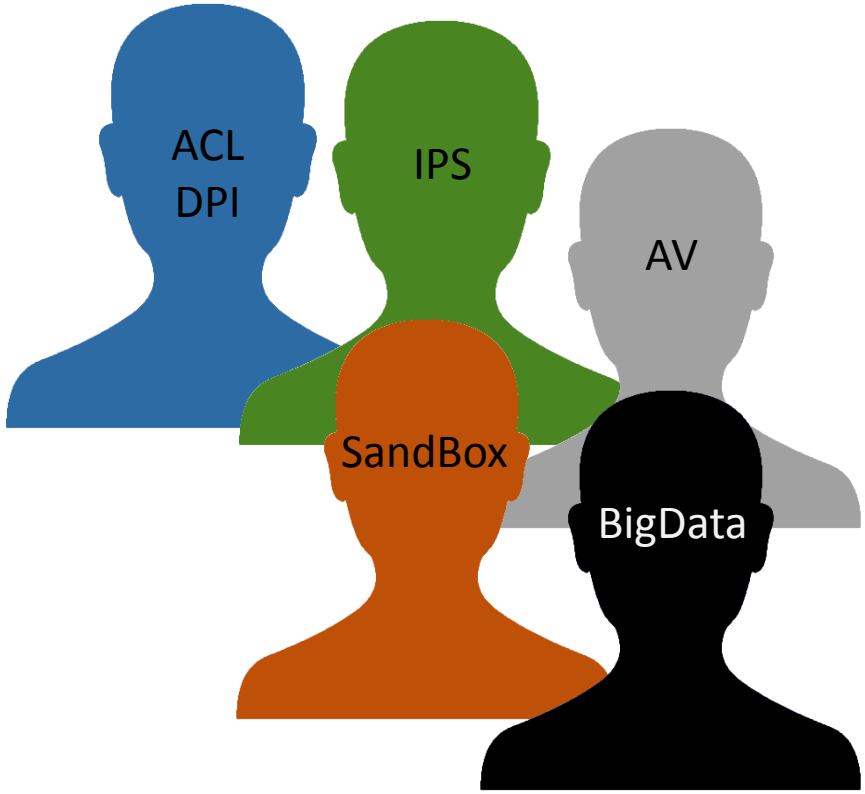
上一代与下一代



流 → 应用

特征 → 行为意图

黑白名单 → 安全信誉



关联分析 → 大数据

固态执行 → 环境感知

下下一代：HumanWall？

Q&A

Thanks!