APT 攻击检测
技术与观念

演讲人：韩志立

职务：天眼产品经理

日期：2014.09

目录

威胁已经发生变化

	过去	现在
攻击者	个人	团体
目的	挑战/声誉	政治/经济
目标	大范围目标	特定目标
工具	已知漏洞/工具	未知漏洞/工具
频率	一次	长久持续
特征	公开	隐秘

典型的攻击过程

	1	2	3	4	5	6	7	8	9	10	11
	锁定目标	组建队伍	构建或购买工具	研究目标	针对检测测试	部署实施	初始入侵	出局连接	建立立足点	盗取数据	掩藏踪迹持续渗透
黑客行动主义	■	■	■			■	■	■		■	
网络犯罪			■		■	■	■	■		■	
APT攻击	■	■	■	■	■	■	■	■	■	■	■

来源：Wikipedia

挑战一：高级恶意软件

54%

的恶意软件，传统AV无法检测

NTT Group《2014 Global Threat Intelligence Report》

基于签名技术的检测无法应对：

- 针对目标攻击无法提前取得样本；
- 零日漏洞无法得到利用特征；
- 定制工具无法得到攻击特征；
- 多态和变形使我们掌握的攻击特征总不及时；
- 数以亿计的规模使检测引擎无法承载。

挑战二：持续渗透内网

87%

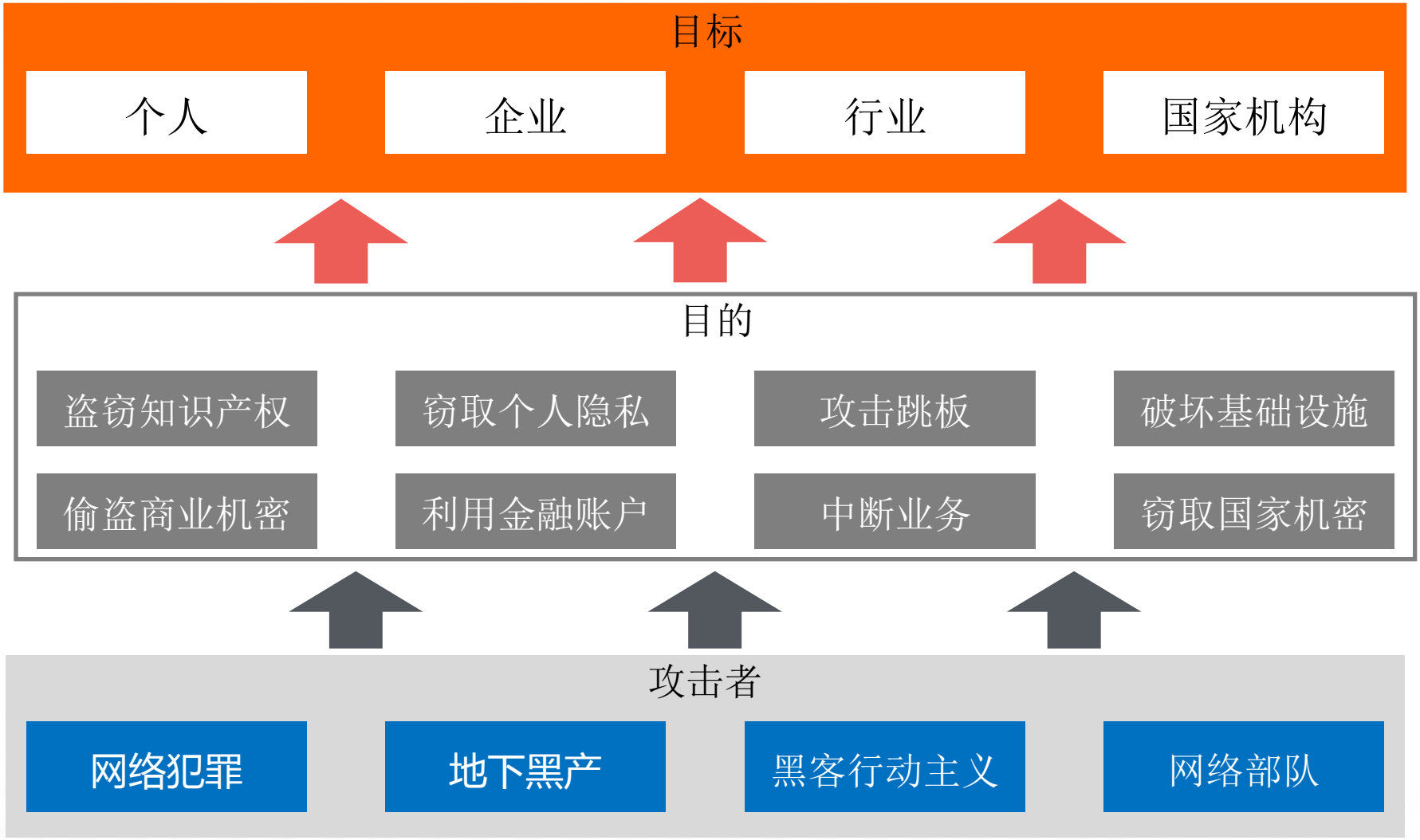
数据泄露事件，传统检测技术无法发现

Verizon：《2013 Data Breach Investigations Report》

传统内网检测方案无法监控内网持续渗透：

- 攻击者具备内网合法权限，无需使用攻击手段；
- 攻击者针对现有监控措施，有意识规避；
- 攻击者采用内容层面的高级恶意软件攻击；
- 攻击者采用社交工程等多重攻击手段。

没有幸免者


目标
个人
企业
行业
国家机构
目的
盗窃知识产权
窃取个人隐私
攻击跳板
破坏基础设施
偷盗商业机密
利用金融账户
中断业务
窃取国家机密
攻击者
网络犯罪
地下黑产
黑客行动主义
网络部队


拿什么来拯救我们？

目录

APT背景下的新挑战

对抗高级恶意软件

检测内网持续渗透

变革：技术与观念

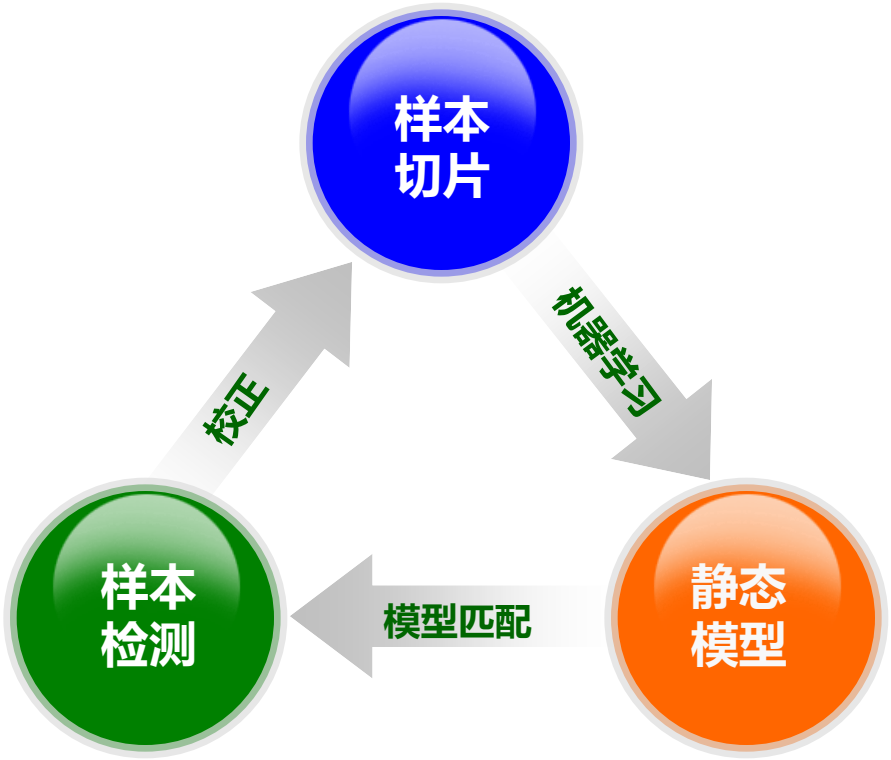
传统沙箱检测的不足

- PE类文件检测
- 专门针对沙箱检测的逃逸技术
  - 运行环境检测
  - 检测沙箱技术
  - 环境锁
  - 延时执行
- 应用环境限制
- 针对C&C检测的逃逸
- 防御能力的实时性问题

QVM

精确查杀PE文件格式的未知恶意软件。全球多家权威测评机构的测试中，均检出率最高、误报率最低

- 依赖数十亿的样本
- 通过大数据挖掘找出正常、恶意两类软件最具有区分度的特征
- 建立机器学习模型，使用机器学习算法
- 得到恶意软件的识别模型



漏洞利用检测

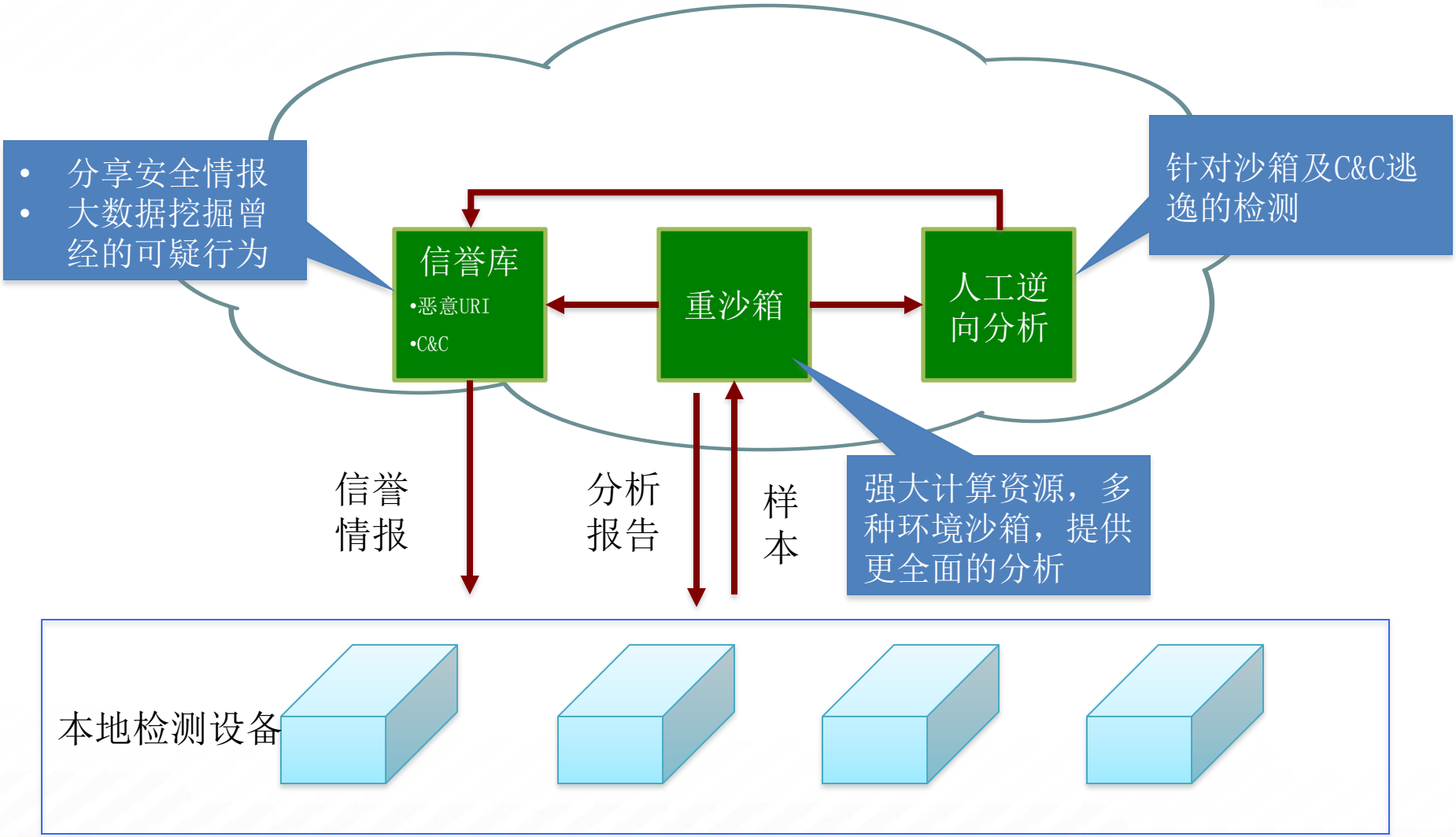
内存、指令监控

- 是否在栈上执行了二进制代码
- 是否在堆上执行了二进制代码
- 是否在数据区执行了二进制代码

系统调用监控

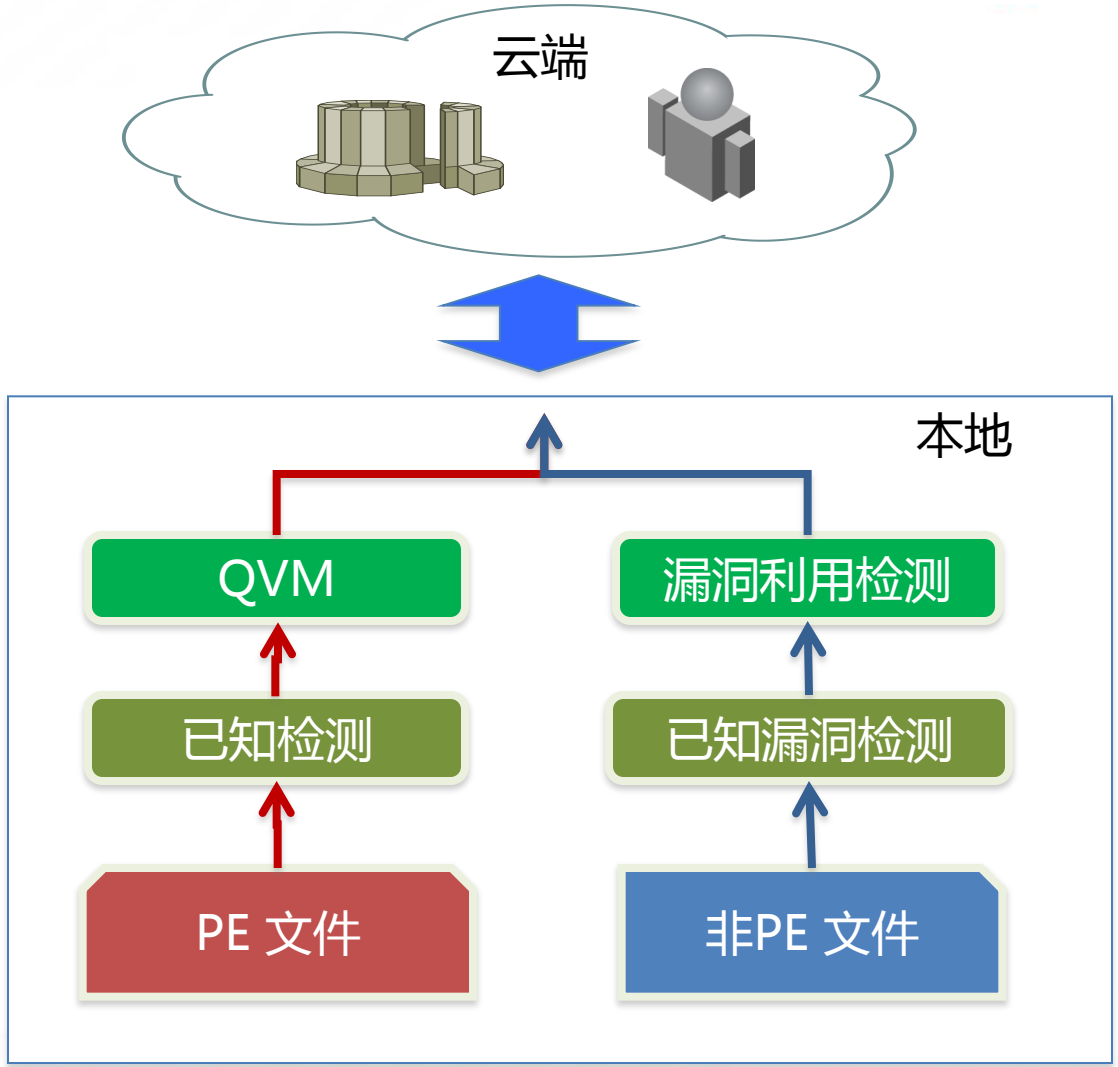
- 是否释放可疑文件
- 是否创建可疑进程或线程
- 是否修改注册表

云端检测平台与信誉情报共享



小结

- 提供支持漏洞利用检测的沙箱技术；
- 检测PE和非PE类文件均提供未知威胁检测能力
- 基于高性能的云端沙箱及人工分析平台
- C&C通信检测
- 提供云端情报收集、共享机制，供实时防御设备使用；



目录

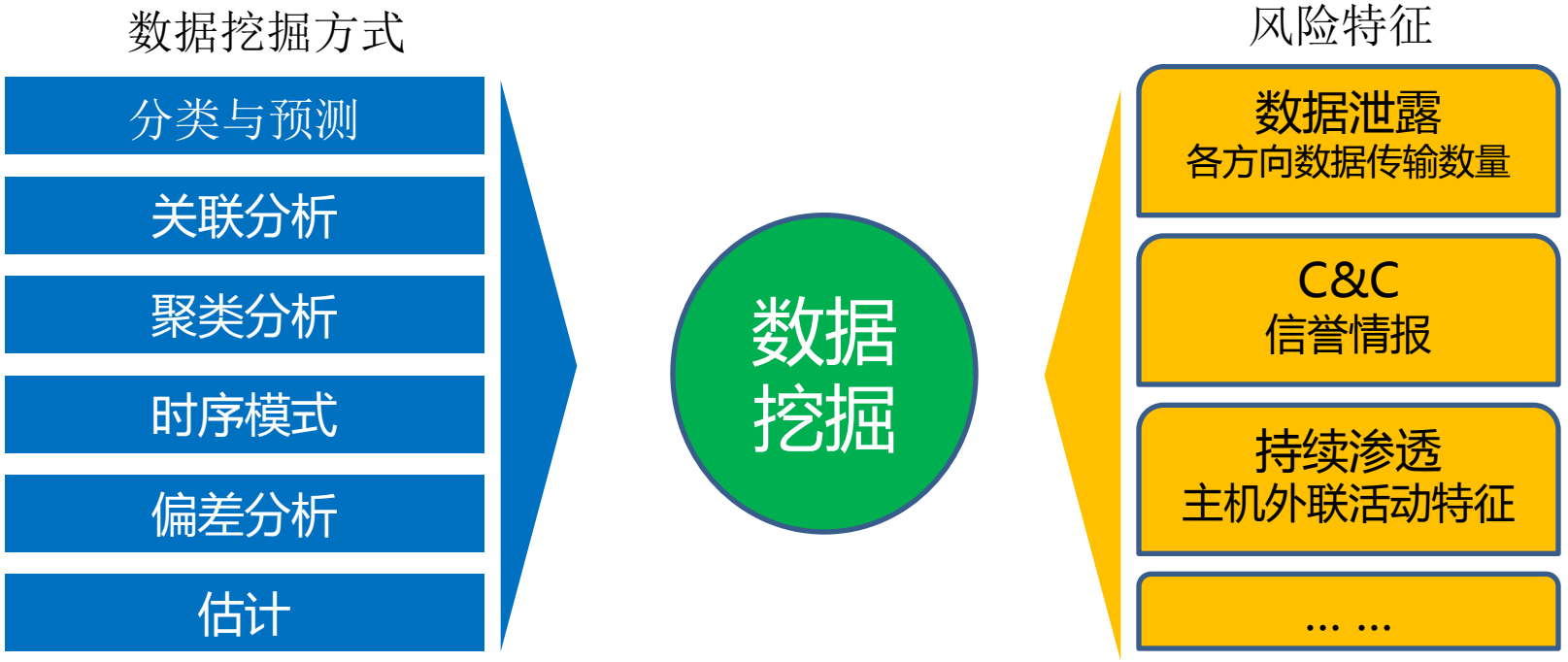
基于异常的内网持续监控

- 当前内网渗透行为往往不具备传统网络攻击特征，因此IDS等设备很难发现
- 基于行为异常的检测成为关键业务资产防护的必要技术手段

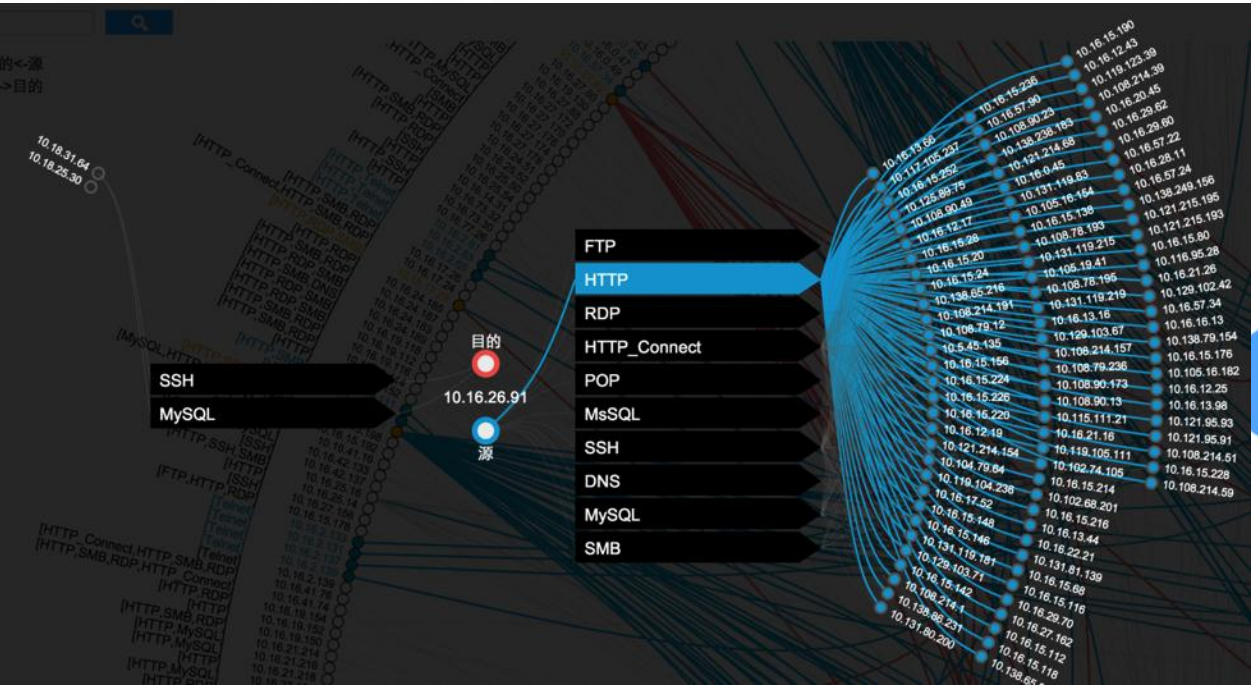
基于已知特征	基于行为异常
识别已知攻击或恶意行为	检测正常的偏离来发现新型攻击
• 针对特定环境往往需要预定义规则 • 无法检测未知威胁与APT威胁	• 更适合于可信网络环境 • 需要通过调整来达到更准确的告警


过去：GB
现在：TB、PB
日志、告警
• 环境配置信息
• 网络流量信息
• 用户信息
• DNS活动
• 邮件活动
• Web活动
• SQL活动
• 业务数据
• 外部风险情报
大数据存储、处理能力是基础

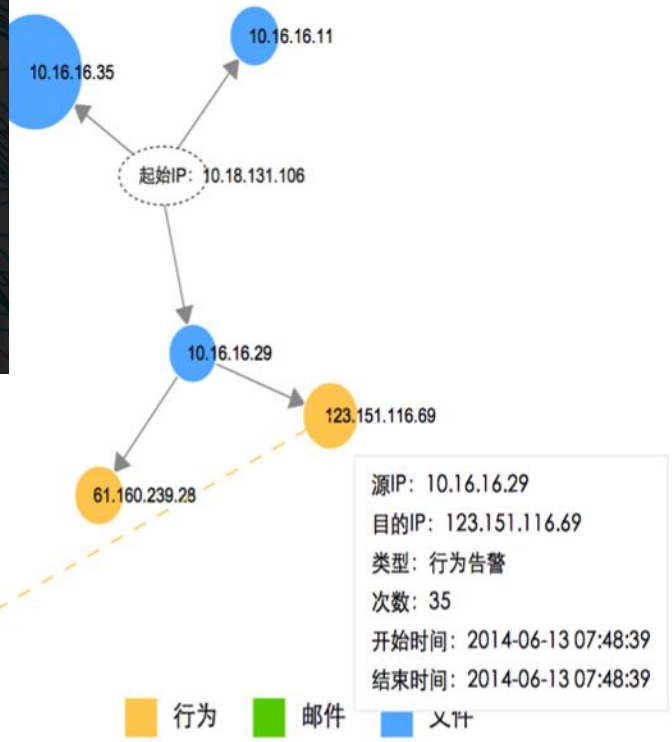
基于数据挖掘的安全检测



基于可视化的异常监控



服务器行为可视化



事件关联展示

基于安全情报的数据分析

- 利用其它位置的检测结果，增强自身防御；
- 利用数据挖掘，查找疑似攻击流量

安全情报
恶意地址，C&C、域名等

攻击或疑似攻击的网络流量

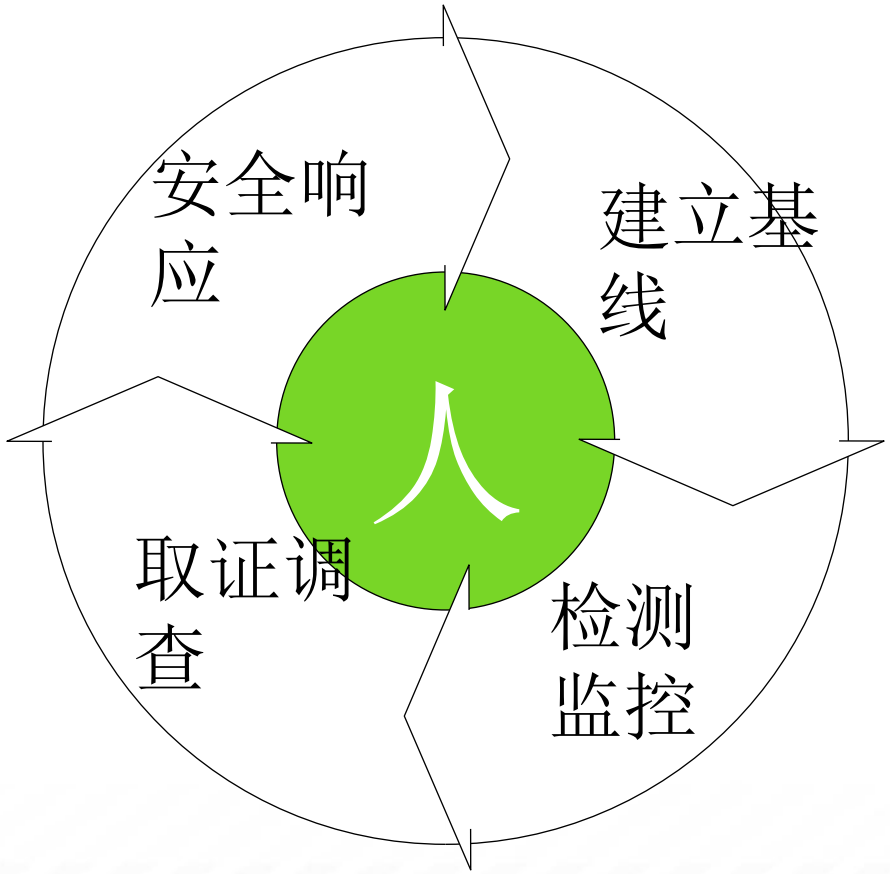
当前及历史流量数据

取证及溯源分析

- 异常检测需要人工方式调查、确认，需要保留必要的原始信息以供调查使用：
  - DNS查询日志
  - URL访问日志
  - 会话日志
  - 数据库访问行为日志
  - 主机行为日志
  - 资产信息：设备MAC、IP、设备名称、归属人员、归属部门、更新时间等
  - 其他设备日志

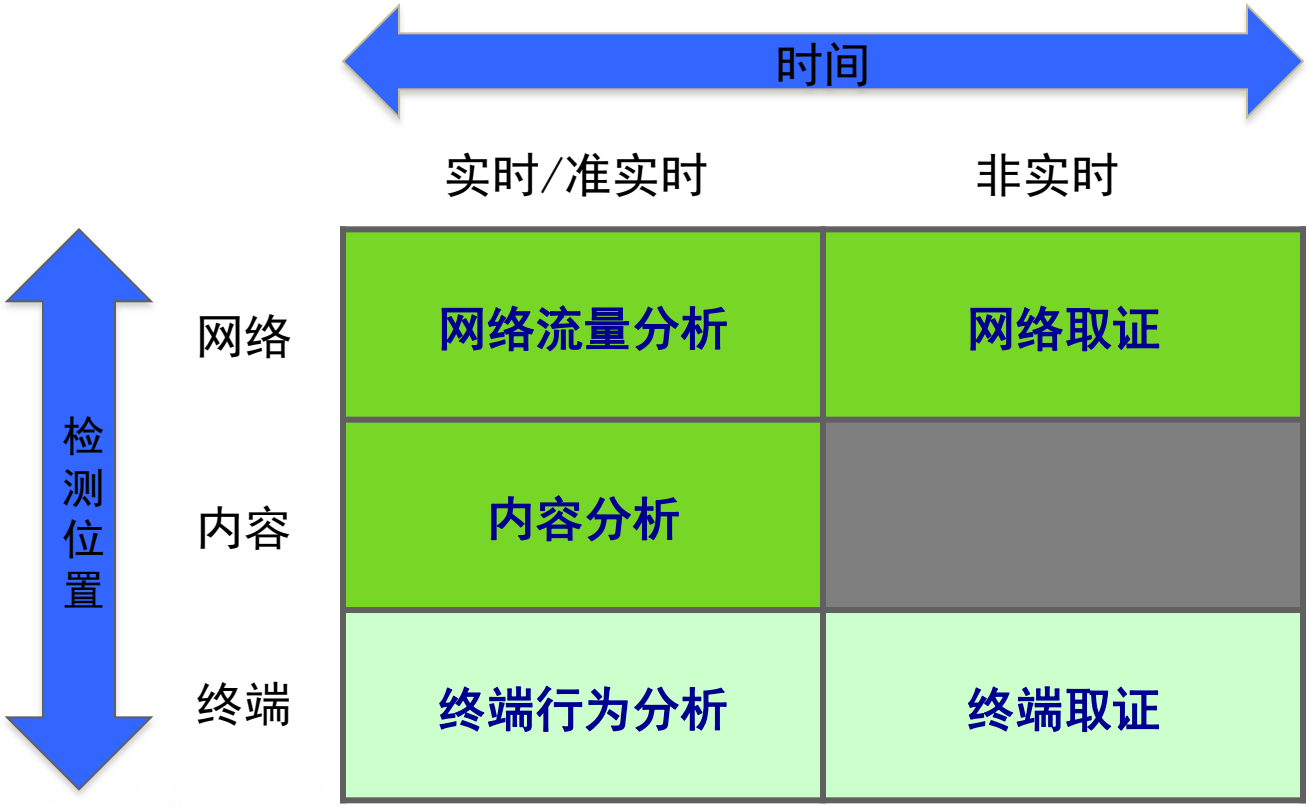
小结

安全最终是人与人的对抗，行为异常监控是依赖专业安全人员的持续监控服务



目录

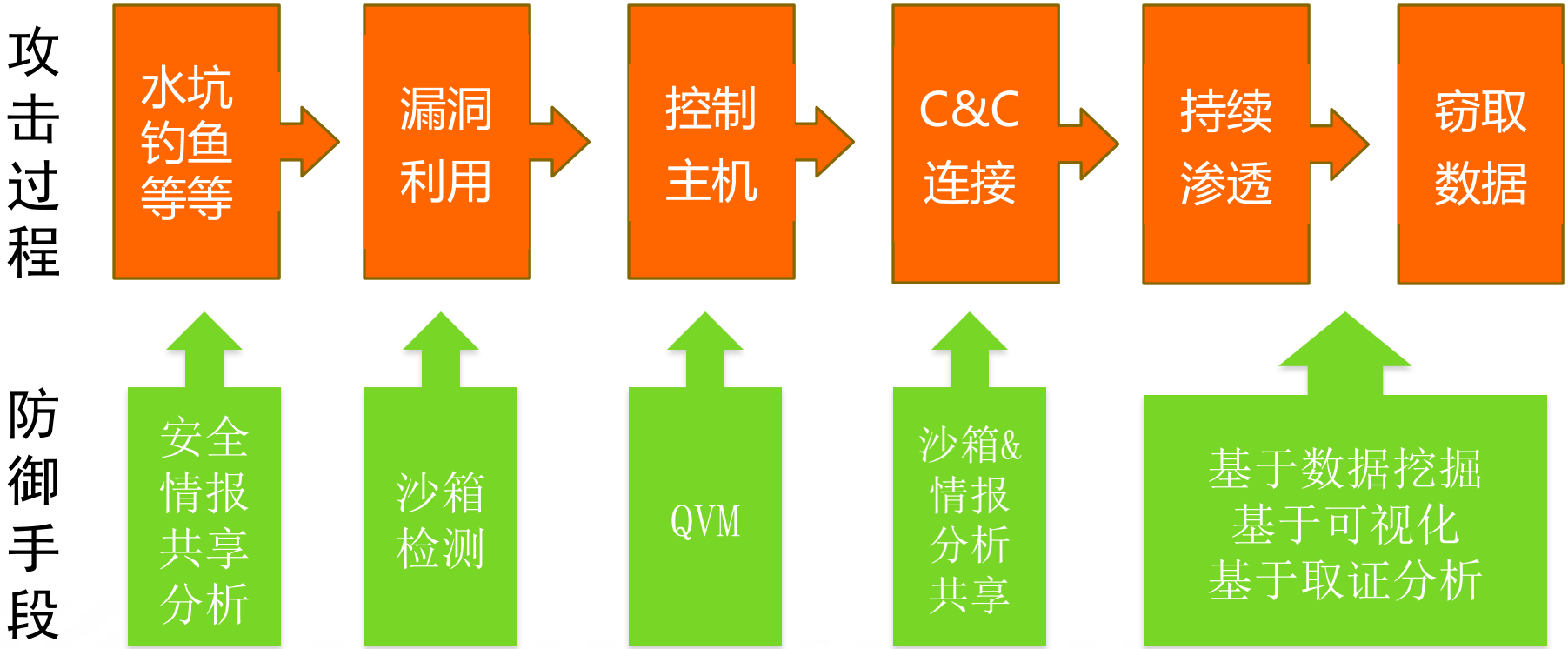
多维度检测



来源：Gartner

纵深防御

- 针对APT攻击的任一阶段均提供检测手段



技术&观念

- APT检测需要的不仅是技术的更新，更需要观念的变革
- 安全观念与技术同时进步，才有可能真正应对APT

技术	观念
检测漏洞利用的沙箱技术	云端：计算能力、专家
基于行为异常的检测	设备与服务一体化
大数据存储、处理、分析	安全情报共享

Thanks!