



翰海源  
VULNHUNT

南京翰海源信息科技有限公司

# 下一代威胁应对

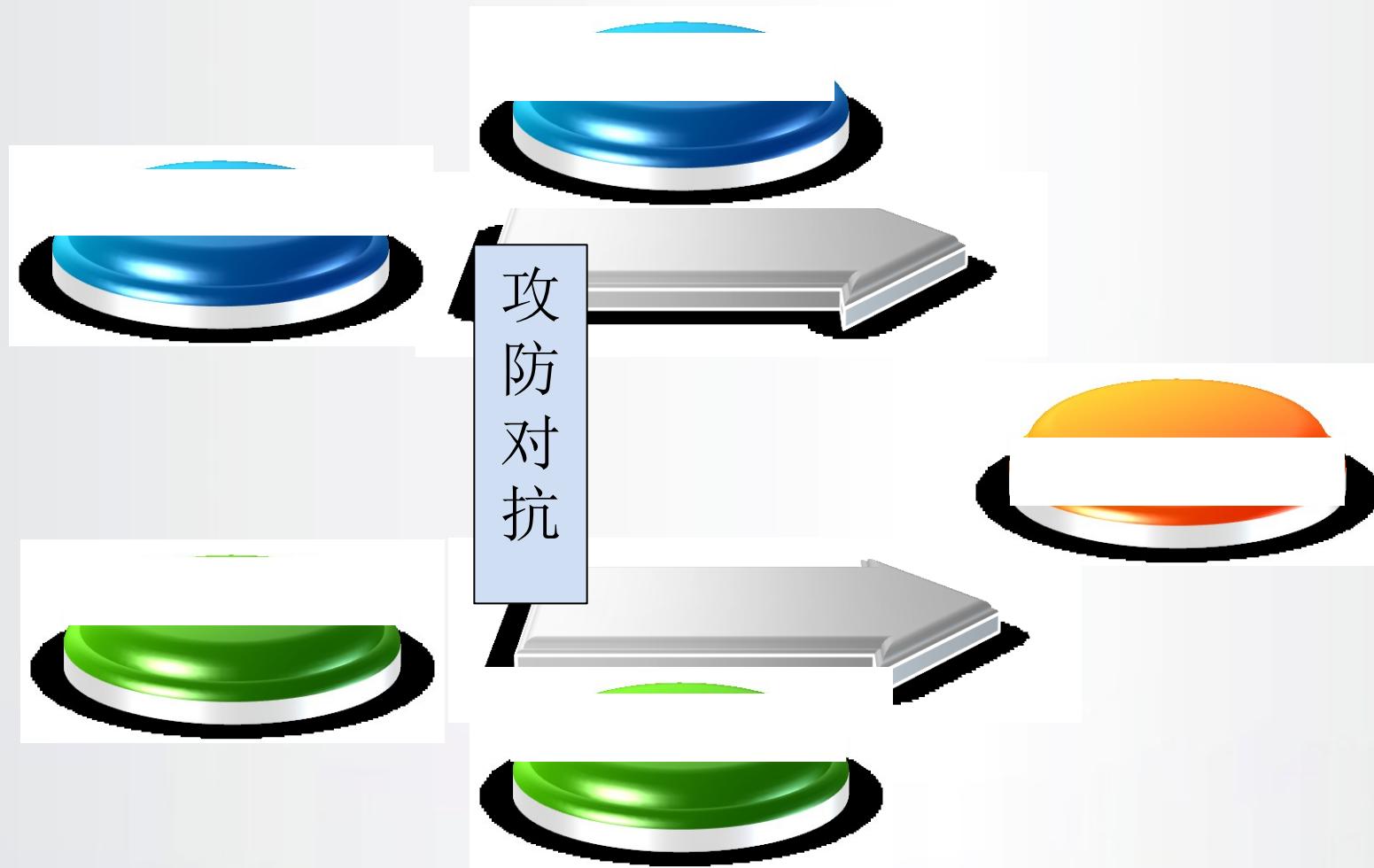


让安全成为IT的基础属性

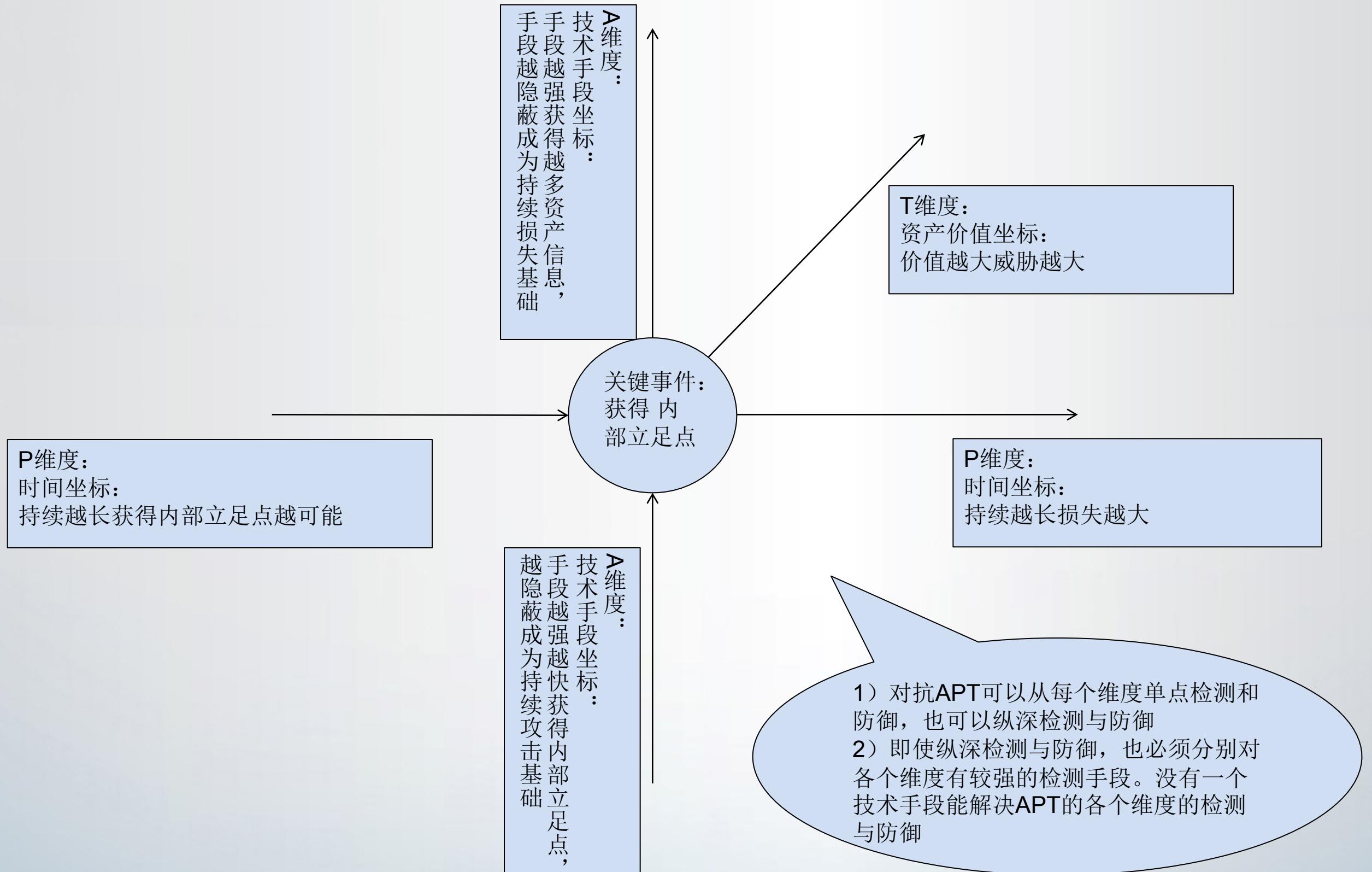
南京翰海源信息科技有限公司

---

# 攻防对抗：威胁要素的对抗



# 对APT的理解与维度



# P、T维度认知

- A维度很大程度上决定了P维度
  - ◆ P维度取决于意愿与能力
  - ◆ 在获得立足点前：
    - A与P都是为了获得立足点服务的
    - A维度决定了P维度实际需要时间
    - A维度决定了防御者警惕性间接决定了P维度价值与曝光损失
  - ◆ 获得立足点后：
    - P是为了获得更大威胁服务的
    - A维度决定了P维度可持续时间
  
- A、P维度又很大程度上决定了T维度
  - ◆ T维度取决于攻击者获取的资产（A维度、实际资产）、持续时间（P维度）

# A 维度认知

网络流量检测对抗

网络内容检测对抗

网络反取证

本地载体检测对抗

本地行为检测对抗

本地反取证

隐蔽、逃逸

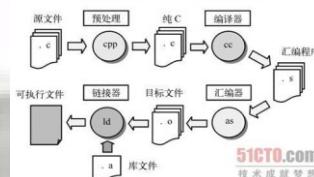
控制、渗透



# 防御者困境：沙堆上的城堡



自身安全：  
设计实现安全  
业务逻辑安全



开源、非开源库

依赖软件

应用软件



外部物理依赖

外部业务依赖



边信道信息辐射

# 后门的发展：沙子里藏坑

传统后门

漏洞

弱点

功能

数据

边信道

通道

算法

根（DNS、域名）

# 攻击手段发展：沙子里挖坑

技术对抗：漏洞组合、降维攻击、逻辑漏洞

半技术对抗：业务结合、供应依赖、手段组合，信赖或依赖劫持

非技术对抗：社工、环境依赖、猥琐流

新领域、物联网、工控



# 攻防维度的不对等性

攻击手法不断变化

沙堆里找点

可组合攻击

无用户可用顾虑

单点突破、逐步渗透

技术处于暗处



产品固化

难以兼顾全面

单点防御

平衡用户易用顾虑

信息缺乏关联

技术处于明处

# 防御者的挑战：沙子里堵坑

阻击木马病毒植入

SDL 阻击漏洞?

阻击漏洞利用路径?

虚拟执行?

大数据

自主开发? 开源

签名技术滞后, 可对抗性增强

漏洞取决于人, 不可控; 后门也无法解决

路径繁复, 理论无法证明。非技术半技术组合难以防御, 误报

对抗无止境; 攻击者占优: 云、逻辑条件

数据不大, 滥用突出; 特马易溜, 需要专业运维

依赖无法保证可信; 能力无法保障安全

# 传统攻防类安全产品防御APT的困境

- 产品能力
  - ◆ 基于已有特征，无未知检测能力
  - ◆ 固化的知识，严重滞后，老旧知识影响判断
  - ◆ 产品检测能力受平衡性约束
  - ◆ 产品可用性缺乏：用户缺乏专家
  
- 知识生成
  - ◆ 不了解攻击者A攻击与对抗的技术知识
  - ◆ 缺乏安全相关的数据反馈
  - ◆ 缺乏专业分析提取知识能力
  
- 响应滞后
  - ◆ 新知识部署能力弱
  - ◆ 用户缺乏专业响应指导

# 换个维度思考防御

- ◇ 生命周期视角
  - ◇ 单一点不能有效防御；但传统防御缺乏关联
  - ◇ 针对一类威胁的攻击生命周期进行系统防御和关联
- ◇ 多维视角
  - ◇ 特征：已知
  - ◇ 内容：广谱 ->分析确认
  - ◇ 行为：已知+未知异常->分析确认
  - ◇ 现象：已知+未知异常->分析确认
- ◇ 大数据视角
  - ◇ 大数据是发现未知异常行为与现象的最好工具

# 大数据应用安全检测的思考

@盛科张卫峰 V

大数据应用实例: 有一位美国数学家最怕坐飞机。他研究了近20年的统计数据, 发现恐怖分子带炸弹上飞机的几率非常低。但他还是不放心的, 又做进一步研究, 发现两个人同时带炸弹上飞机的几率为零, 于是他坐飞机都自己携带一枚炸弹。

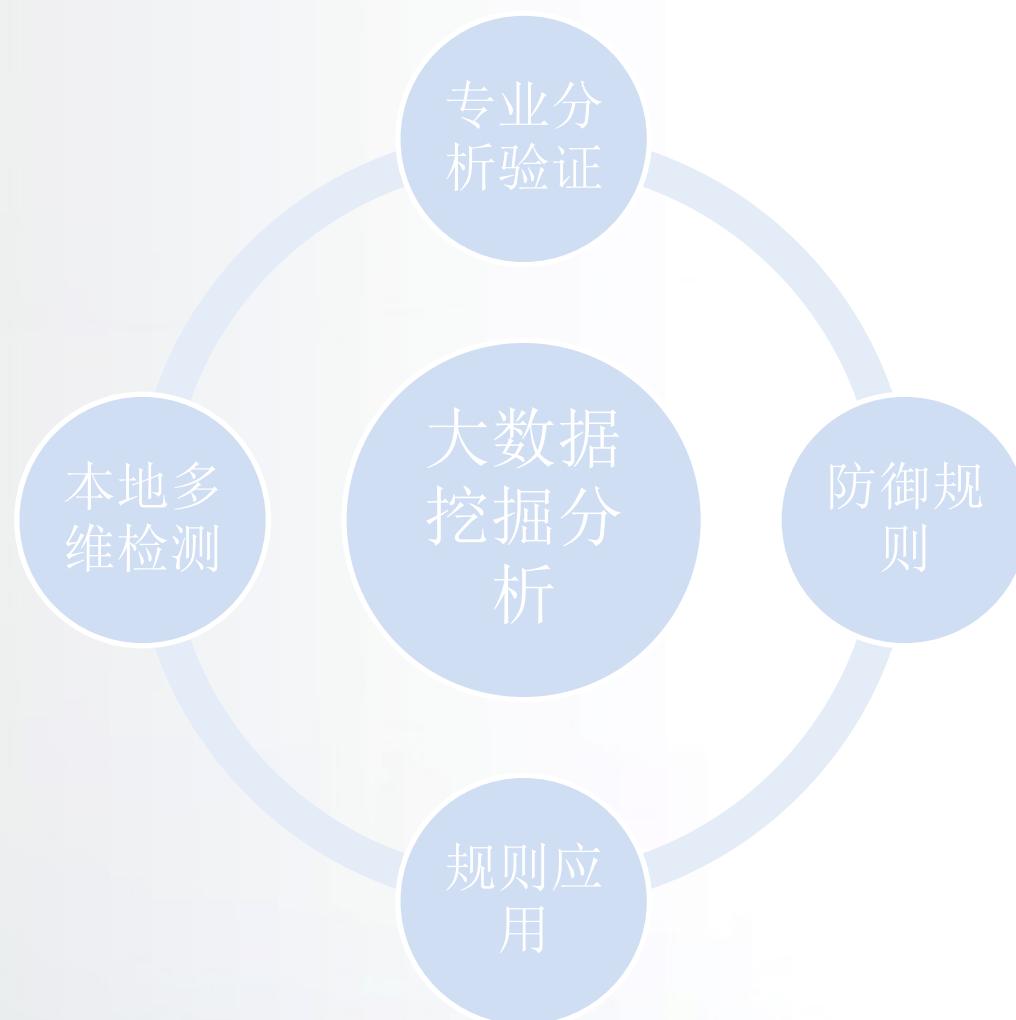
大数据是揭示客观相关性的

- 1) 如果相关性可以被有意识针对性的主观改变, 大数据将陷入尴尬
- 2) 而安全攻防正属于有意识针对性对抗的领域

大数据应用安全检测的价值

- 1) 攻击者未意识到发起对抗阶段
- 2) 对攻击者对抗技术发展的预测
- 3) 通过前期积累的大量攻击者知识进行跨维度对抗

# APT对抗本质：攻击者知识对抗



## A维度:

- 多维度协防
- 攻防对抗知识
- 信息共享
- 专业分析团队共享
- 快速知识分发

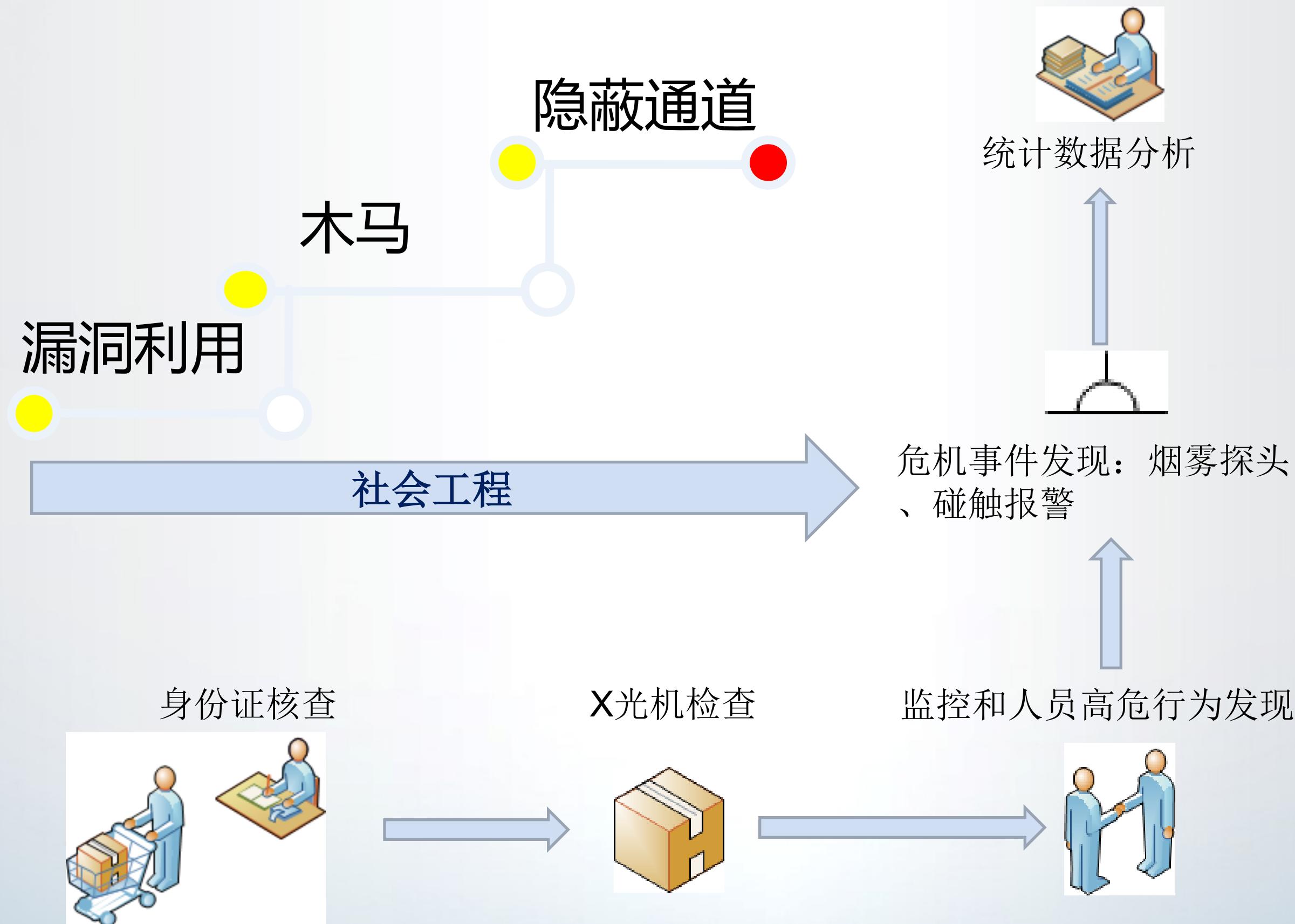
## P维度:

- 数据集合需求
- 数据隐私冲突
- 攻击（普通攻击、APT攻击）的差异
- 攻击者对抗视角

## T维度:

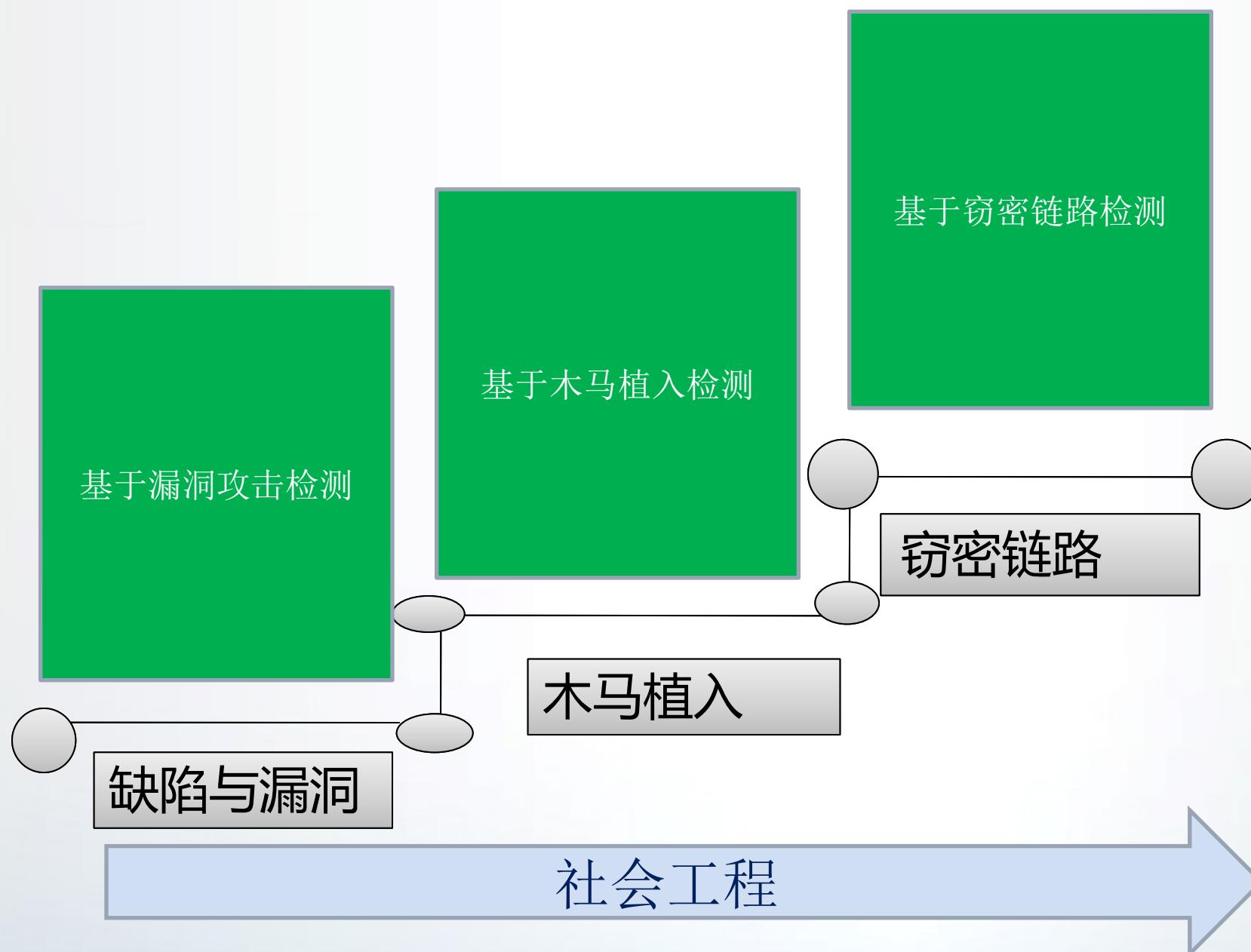
- 资产管理角度

# 翰海源的思考：多维度检测思想



# 翰海源的思考：全生命周期纵深覆盖

APT攻击是由多个环节多个攻击手段组合而成  
针对每个环节每个手段形成纵深检测体系，可以最大限度发现APT攻击，提高攻击者门槛



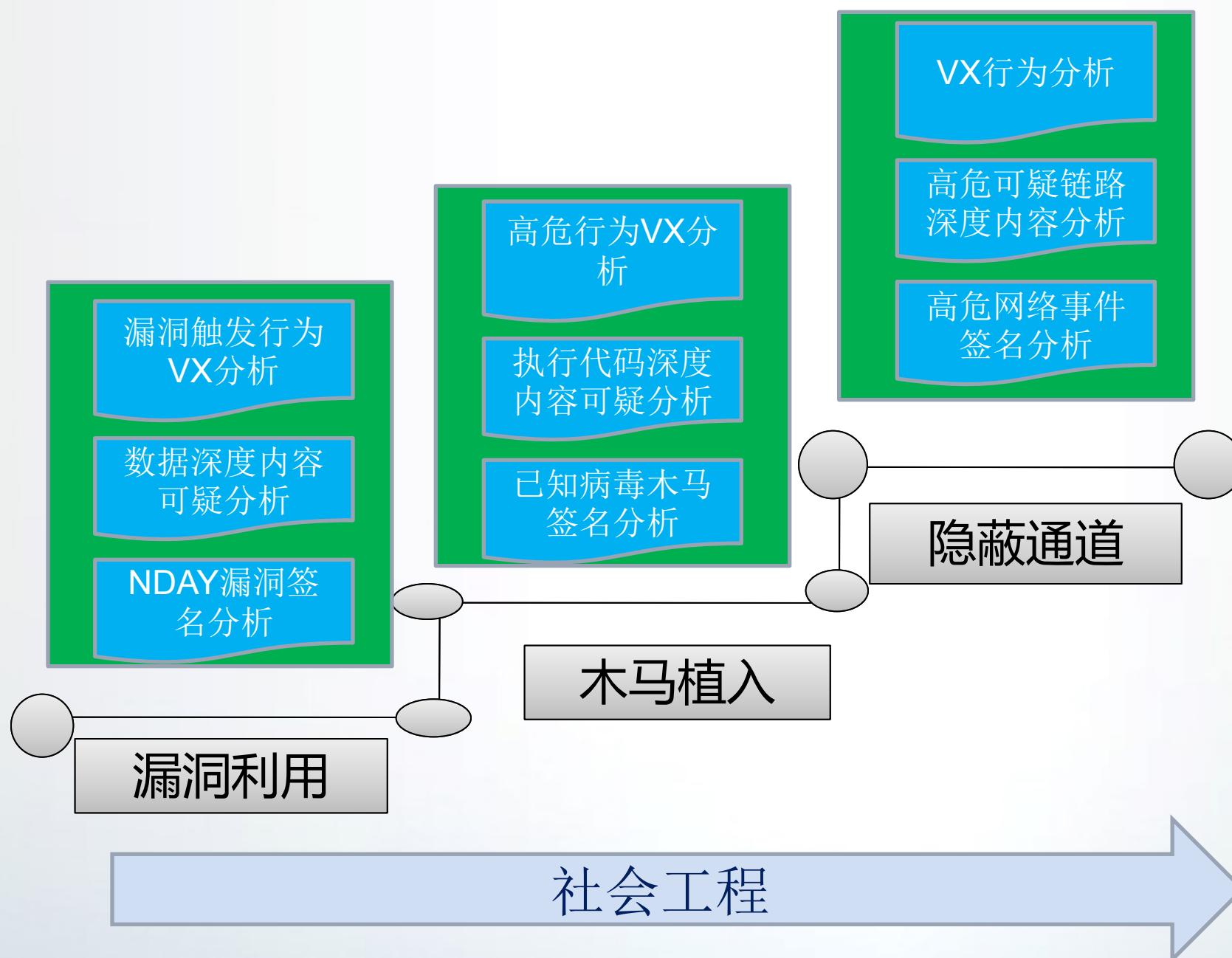
翰海源星云多维度威胁检测体系

# 翰海源的思考：多维度监测

APT攻击每个检测手段都因为原理性能易用性误报率等因素都存在对抗技术

针对每个APT攻击手段手段用多种检测方法形成多维度检测体系，可以最大限度检测APT攻击手段

纵深覆盖\*多维度形成网状检测体系



翰海源星云多维度威胁检测体系

# 多维度全生命周期检测体系

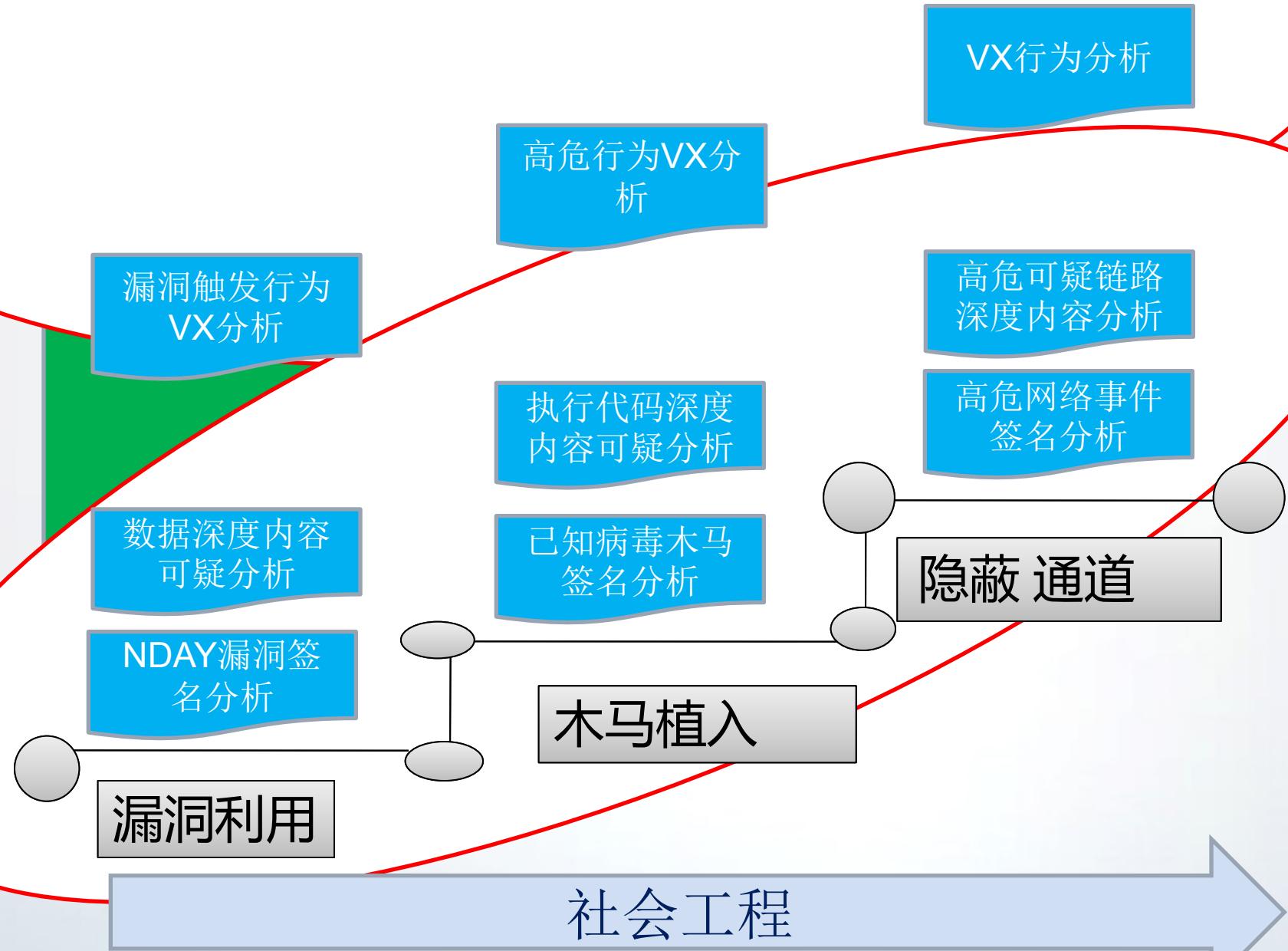
翰海源公有云

云端数据分析：攻击共享、攻击者归组特征、攻击者资源特征

企业私有云

智能事件关联分析：攻击确认、事件关联可疑发现、因果溯源

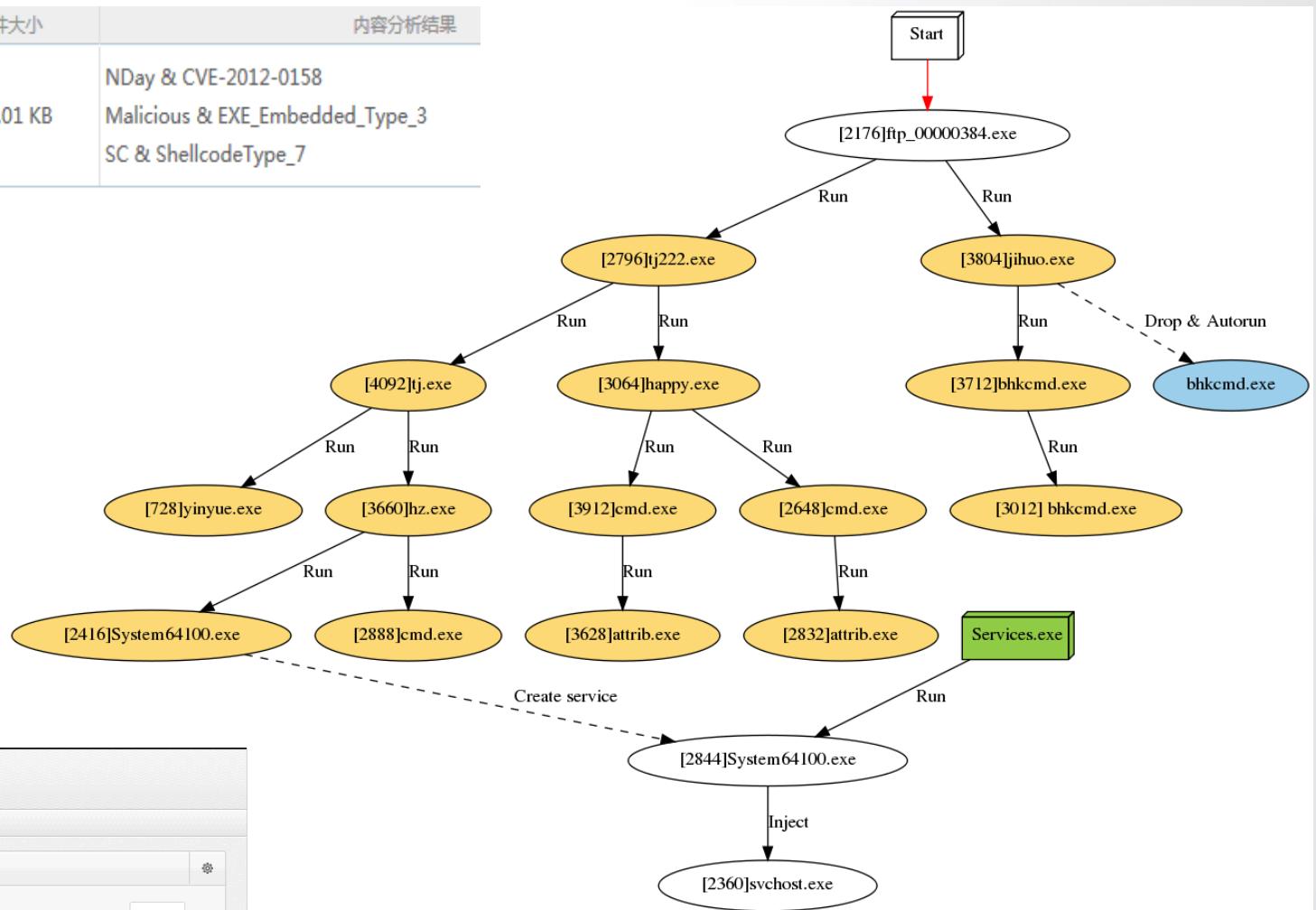
端点探头设备



翰海源星云多维度威胁检测体系

# 展示静态、动态、行为关联

样本文件名	样本MD5	文件大小	内容分析结果
100004976.rtf	E21676D7367952AE0B8B5B858722568E	135.01 KB	NDay & CVE-2012-0158 Malicious & EXE_Embedded_Type_3 SC & ShellcodeType_7



**警告管理**  
Warning query

- 警告查询
- 事件视图
- 样本视图
- 受害者视图
- 攻击源视图
- 警告记录导出
- 警告记录清除
- 样本导入
- 手动提交样本测试

**受害者视图**  
Warning query

首页 > 警告管理 > 受害者视图

受害者视图

攻击时间: [ ] 被攻击者: [ ] 所属国家: [ ] 所属地区: [ ] 样本md5: [ ] 搜索 [ ] 自定义列 [ ]

被攻击者	所属地区	受害严重程度	可疑样本数	可疑图片数	恶意IP/URL数	C&C IP/URL数	首次被攻击时间	最近被攻击时间
192.168.0.126	局域网	■	1	0	0	1	2013-11-11 13:38:37	2013-11-11 13:49:29
192.168.0.115	局域网	■	0	0	0	1	2013-11-11 13:29:25	2013-11-11 13:29:25
192.168.0.107	局域网	■	0	0	0	1	2013-11-08 15:07:24	2013-11-08 15:07:24
192.168.0.203	局域网	■	0	2	0	0	2013-11-08 11:39:01	2013-11-08 14:23:12
info@aoucaagliari.it	意大利	■	1	0	0	0	2013-11-07 16:54:49	2013-11-07 16:54:49
192.168.0.56	局域网	■	0	2	0	0	2013-11-07 11:27:25	2013-11-11 11:22:01
5145672@qq.com	局域网	■	1	0	0	0	2013-11-07 10:45:32	2013-11-07 10:45:32
192.168.0.103	局域网	■	0	2	0	0	2013-11-06 16:22:34	2013-11-08 12:54:49
119.147.193.115	广东省	■	1	0	0	0	2013-11-06 14:54:39	2013-11-06 14:54:39
192.168.0.202	局域网	■■	0	29	0	15	2013-11-06 13:42:36	2013-11-11 14:14:42

每页显示: 10 共 56 条记录

首页 上一页 1 2 3 4 5 下一页 末页 1



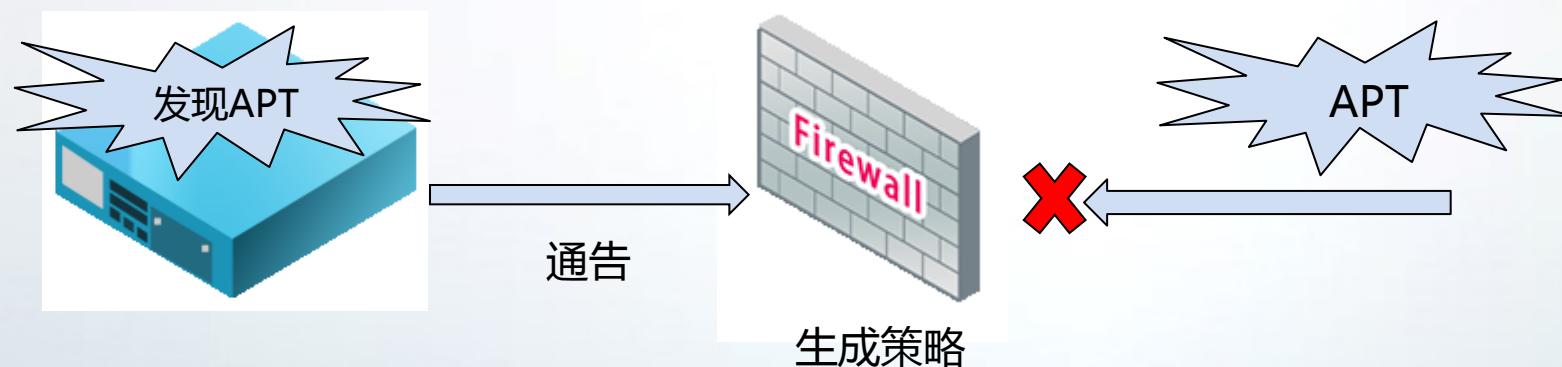
# 与传统FW对接

星云可以与传统FW对接

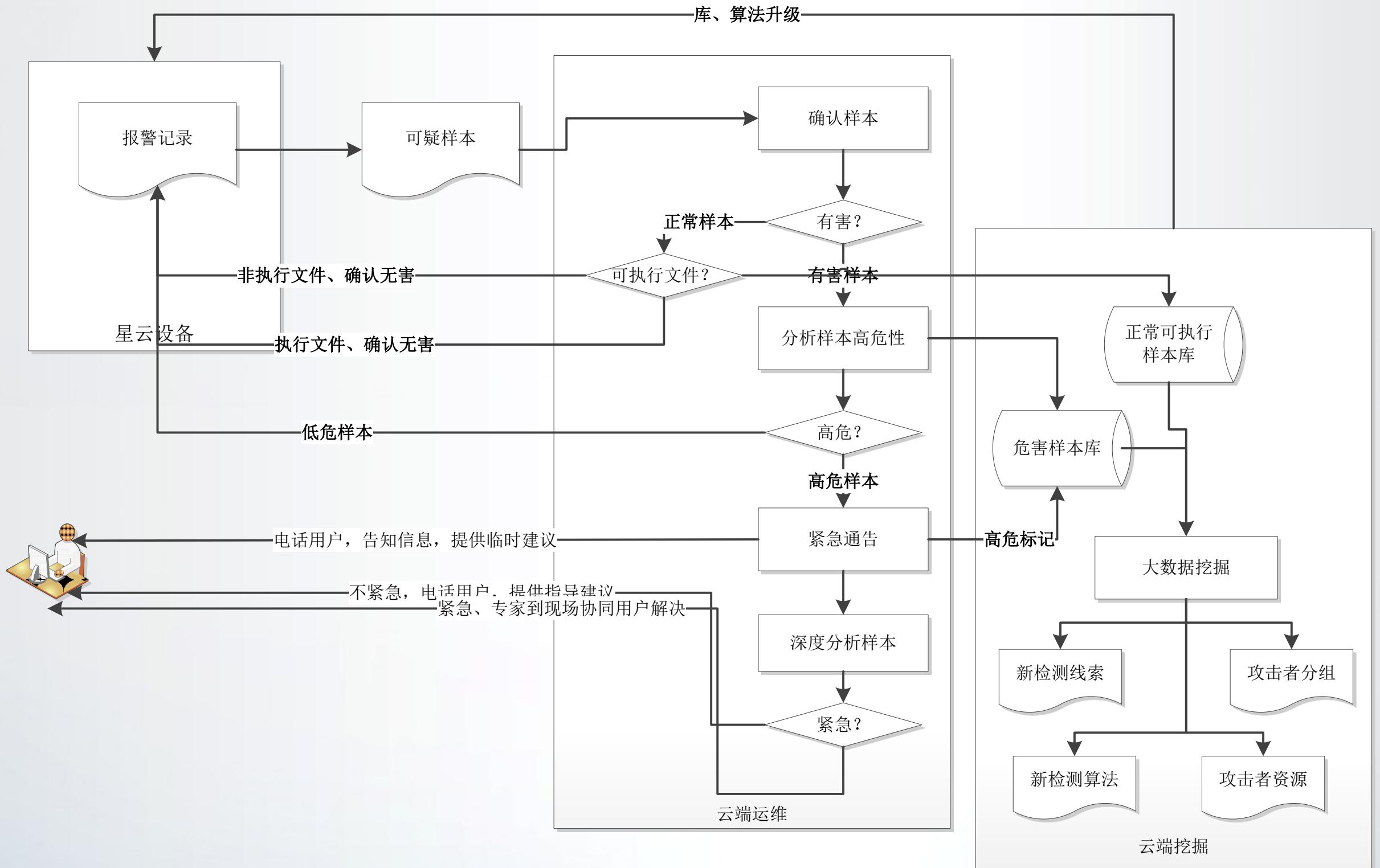
- FW注重传统攻击，并提供了阻截能力
- 星云专注基于0DAY、变种病毒、高级木马的APT攻击防御
- 两者相辅相成，互为补充

星云与FW的联动形成完整的APT攻击响应

- 星云发现APT攻击事件，提供攻击链路、攻击者和受害者信息
- FW结合星云，有的放矢，生成相应的防护策略，阻断APT攻击路径

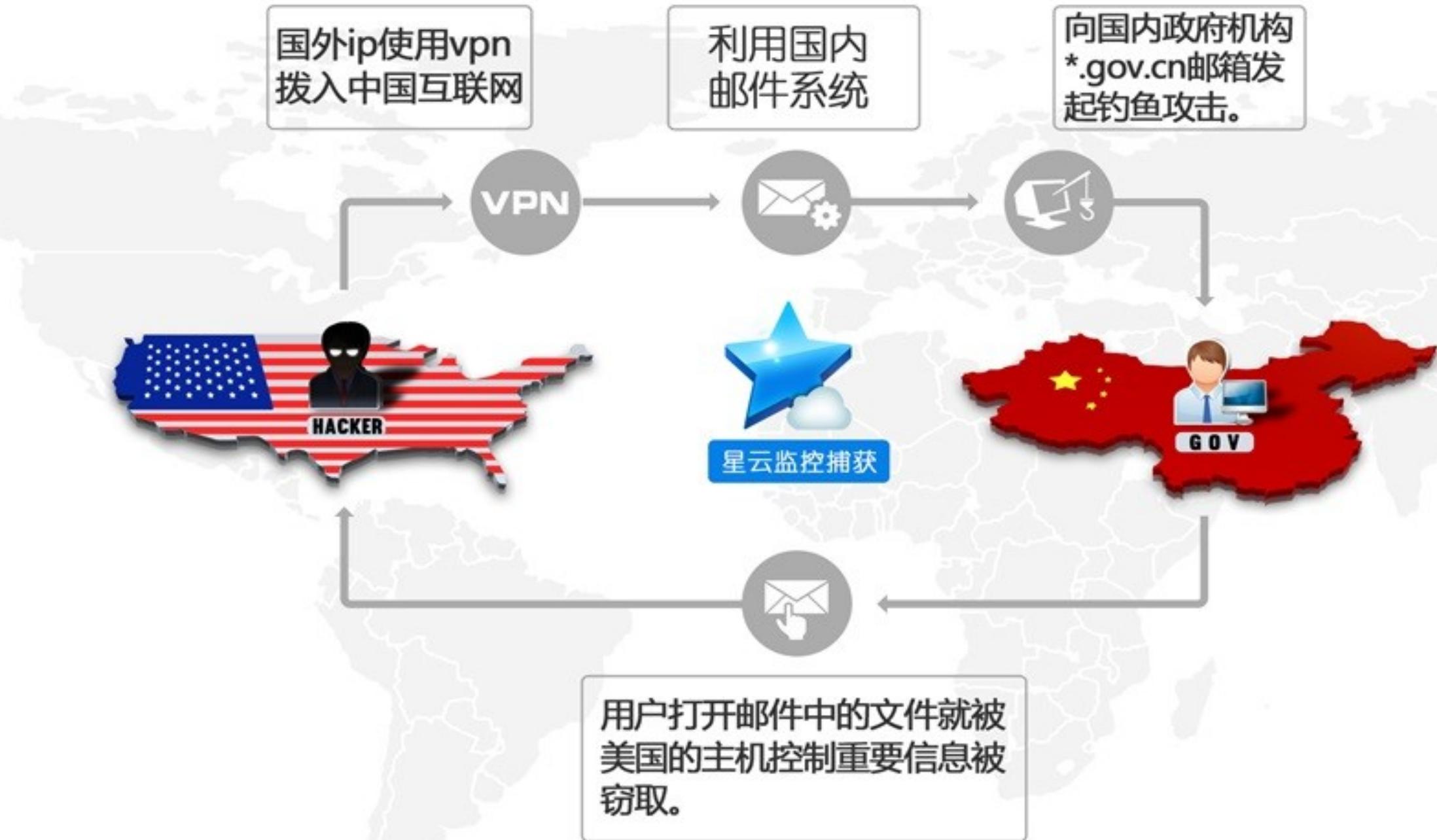


# 云端运维



# 案例：WPS 0DAY

- 2013年12月星云是国内唯一捕获WPS漏洞APT攻击



# 具体的捕获内容

发件人 2014中国经济形势解析高层报告组委会 < > ☆

← 回复

← 全部回复

主题 **Fw:2014中国经济形势解析高层报告会**

各位专家，各位老师：

经国务院发展研究中心批准，由国务院发展研究中心信息中心主办一年一度的“中国经济形势解析高层报告”于2013年12月21-22日在北京举办。将邀请中央有关部委的高层人士和权威专家，解读“十八届三中全会”，政府政策取向，把脉中国经济走势，有助于企业制定发展规划，明确投资方向。

附件含本次会程详细内容，请您查收。

▶ 1 个附件： 2014中国经济形势解析高层报告会.rar 136 K

使用MS office 2010打开会提示使用让用户下载wps 2012打开该文件，诱惑用户下载并使用有0day漏洞的wps 2012。

# 案例：高级特马

- 近期星云捕获一个高级特马

状态	事件产生时间	来源设备	攻击者	被攻击者	内容分析结果	行为分析结果	协议	类型	样本文件	等级
	2014-03-13 ...	10.200.0.99 ...	211.149.19...	10.200.8.17	Normal		HTTP		prdiskuploa...	高

- 大多数杀毒软件无法检测



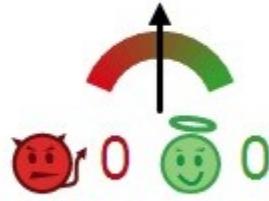
**virustotal**

SHA256: 8c3660d0c528a8848d36e5747d0f8830c9ed965df7b9e6e9613ba63be5d62dee

File name: 0f6466501756c98c1ca38a38a313898997c398b5

Detection ratio: 2 / 50

Analysis date: 2014-03-04 15:22:26 UTC ( 1 month, 3 weeks ago )



- 利用博客来获取C&C地址



基本资料

个人简介: WM70F8E777772E69746278772E636F6D1A83UWM

在线

q22223344

私信

# 案例：高级特马

## ➤ 可疑行为

category	PID	进程名	行为[英文]	行为发生次数
FILESYSTEM	1676	prdiskupload.exe	Drop PE File in File System C:\Documents and Settings\All Users\Application Data\WSTRKHPKY\STRKH PKY.exe 关闭UAC	1
REGISTRY	1676	prdiskupload.exe	Disable Windows UAC Settings ,Registry Key Set \REGISTRY\MACHINE\SOFTWARE\Microsoft\Window s\CurrentVersion\policies\system,[ValueName:ConsentPromptBehaviorAdmin]=0	1
REGISTRY	1676	prdiskupload.exe	Disable Windows UAC Settings ,Registry Key Set \REGISTRY\MACHINE\SOFTWARE\Microsoft\Window s\CurrentVersion\policies\system,[ValueName:EnableLUA]=0	1
SERVICE	1676	prdiskupload.exe	Try to Create Services (NVidiaPRKWSrv),Display Name:NVidiaPRKWSrv Manager ,ServiceType:SERVICE _WIN32_OWN_PROCESS,StartType:SERVICE_AUTO_START,lpBinaryPathName:"C:\Documents and Sett ings\All Users\Application Data\WSTRKHPKY\STRKHPKY.exe" /assrv 创建服务	1
LPC	1676	prdiskupload.exe	Open Mutex :Local\c!\documents and settings!administrator!cookies!	1
NETWORK	1676	prdiskupload.exe	Try to access or download url <a href="http://www.baidu.com/p/q22223344/detail">http://www.baidu.com/p/q22223344/detail</a>	1
FILESYSTEM	1676	prdiskupload.exe	Try to Search File From Disk 搜索磁盘	9

# 案例：云端运维

翰海源星云私有云系统软件

客户监控 | 系统管理 | 警告查询 | 统计报表

主菜单 << 实时数据 警告记录查询

警告上传时间: [ ] 至 [ ] 选择客户: 不限 选择设备: 不限 未读:  筛选重复样本:  搜索 基本筛选

扫描类型: 不限 来源类型: 不限 Sensor扫描结果: 不限 Vx扫描结果: 不限 是否为威胁样本: 不限

样本类型: [ ] 样本MD5值: [ ]

样本攻击来源 样本影响范围 导出当前页 导出所有记录 收缩 自定义显示列

状态	Sensor扫描时间	Sensor扫描结果	Vx扫描结果	扫描类型	来源类型	样本类型	样本来源	漏洞等级	是否为威胁样本
	2014-04-28 11:22:12	Virus(Virus.MSExcel Ignore)	Ignore	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	尚未未确认
	2014-04-28 11:22:12	Virus(Virus.MSExcel Ignore)	Ignore	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	尚未未确认
	2014-04-28 08:39:10	Virus(Virus.MSExcel Ignore)	Ignore	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-28 07:44:36	SC(ShellcodeType_ Normal)	Normal	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-28 04:04:45	SC(ShellcodeType_ Normal)	Normal	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-28 01:45:54	SC(ShellcodeType_ Normal)	Normal	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-28 00:38:11	Virus(Virus.MSExcel Ignore)	Ignore	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-27 23:27:51	Virus(Virus.MSExcel Ignore)	Ignore	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-27 21:49:58	SC(ShellcodeType_ Normal)	Normal	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报
	2014-04-27 21:45:38	SC(ShellcodeType_ Normal)	Normal	邮件附件	邮件附件	自动捕捉	自动捕捉	Medium	确认为误报

每页显示 10 条,共85500条

目标来源 样本信息 扫描信息

来源类型: 邮件附件  
样本来源: 自动捕捉  
样本类型: xls

W首页 < 上一页 1 2 3

联合云端，厂家联合用户做运维

事件确认及时 (新攻击 < 2小时)

# 结语

## 下一代威胁的应对之法

- 生命周期纵深覆盖 VS 多路径攻击
- 多维度检测 VS 攻防对抗
- 大数据分析、云端管理 VS 快速发现及相应威胁

# THANK YOU

- 产品与服务联系方式
  - 电话：400-086-9086
  - 邮箱：[support@vulnhunt.com](mailto:support@vulnhunt.com)