网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

战术型态势感知的探索与实践

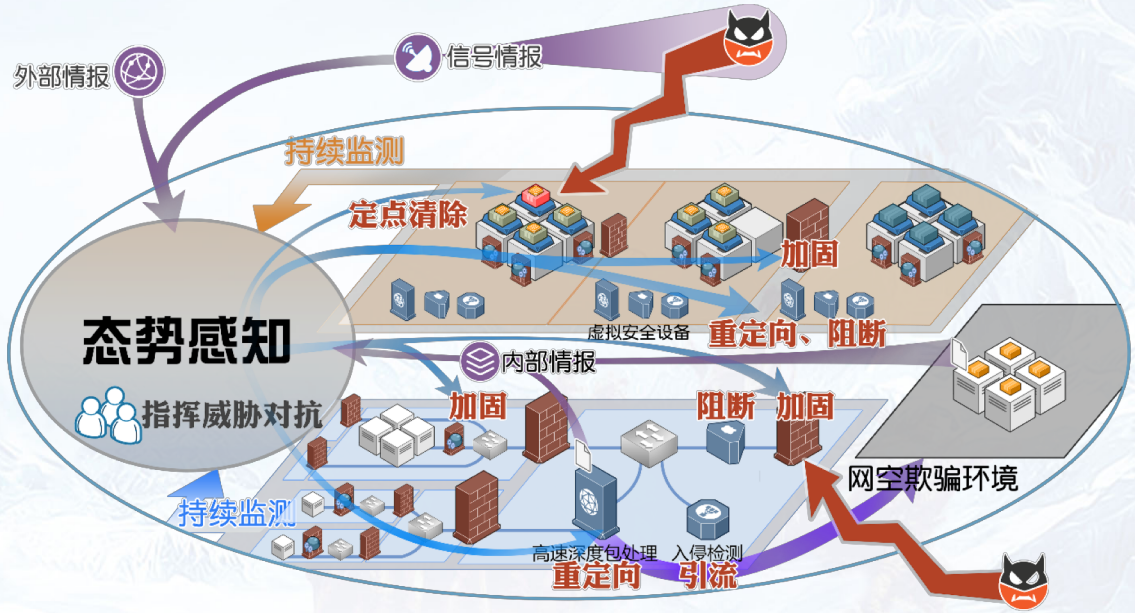
安天 态势感知工作组

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰

提纲

- 抵近战场——从监测型态势感知到战术型态势感知
- 战术型态势感知的关键能力要求
- 关键能力的解决方案实践
- 实际场景应用示例



01 抵近战场——从监测型态势感知到战术型态势感知

态势感知引用的经典概念

在一定时间和空间的观察环境中的元素，理解这些元素的意义并预测这些元素在近期未来的状态

——Endsley（1995）

时间：不受外界条件影响 、全天候、持续的

空间：网络空间地形形态，区分重点关注、持续跟踪

观察：网络空间全要素信息的有效记录

理解：对不同层面的元素进行分析、理解、知识转化

预测：基于情境模型，对于下一步攻击动作的短期猜测

态势感知是包含观察、理解、预测、响应、处置的体系化防御系统

微观

- 威胁元素（攻击载荷、C2…）
- 资产画像（属性、连接、人员组织归属）的

中观

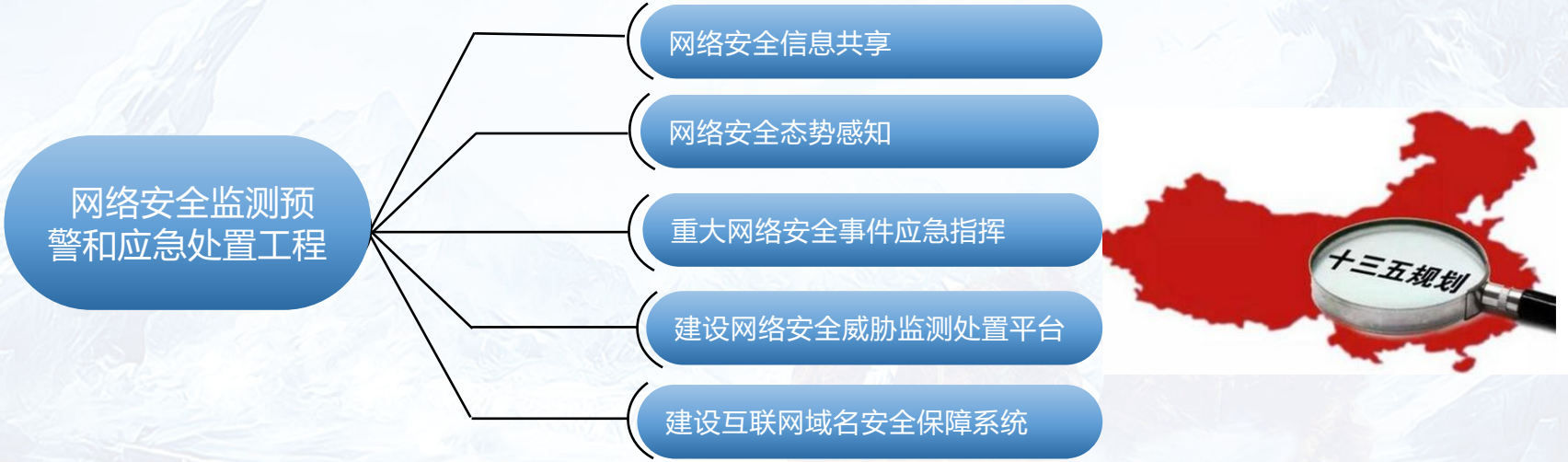
- 攻击路径（横向移动、载荷传输…）
- 事件分析（时间、地点、工具、漏洞、范围、影响、处置动作）

宏观

- 同类攻击追溯建立攻击模式情境模型
- 攻击战略意图
- 攻击对手画像

《“十三五”国家信息化规划》关于态势感知的要求

“**全天候全方位感知网络安全态势**，加强网络安全态势感知、监测预警和应急处置能力建设。建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。建立政府和企业网络安全信息共享机制，加强网络安全大数据挖掘分析，更好**感知网络安全态势**，做好风险防范工作。完善**网络安全检查**、风险评估等制度。”



某省网信办网络安全态势感知应急处置平台

平台价值一：网站分级管理与态势呈现

- 重点监控、全面监测；
- 网站存活性验证；
- 篡改、黑链、挂马、钓鱼等威胁情况监测发现；
- 全省重点网站安全情况的态势呈现

对黑龙江全省2200余个重点网站的基本信息，单位归属情况进行归档、记录；

掌握网站存在的漏洞情况，尤其重点关注0day漏洞监测，人工验证漏洞数量105个；

100余个重点网站进行渗透测试，发现46个网站存在严重漏洞；

平台价值二：全方位威胁感知

从安天等厂商处获得了全省威胁数据、移动终端安全数据等威胁情报的推送；

形成PC与移动侧、终端与流量侧全方位的威胁感知能力；

利用大数据技术及情报信息库支撑，实时掌握网络攻击来源、攻击目标、攻击路径、攻击武器等情况，以及保护目标的安全状况

对比历史数据，形成趋势性、合理性判断，为用户决策提供支撑

平台价值三：实时告警与准确研判

A » 以安全实时防护为核心

聚焦安全，威胁准确定位

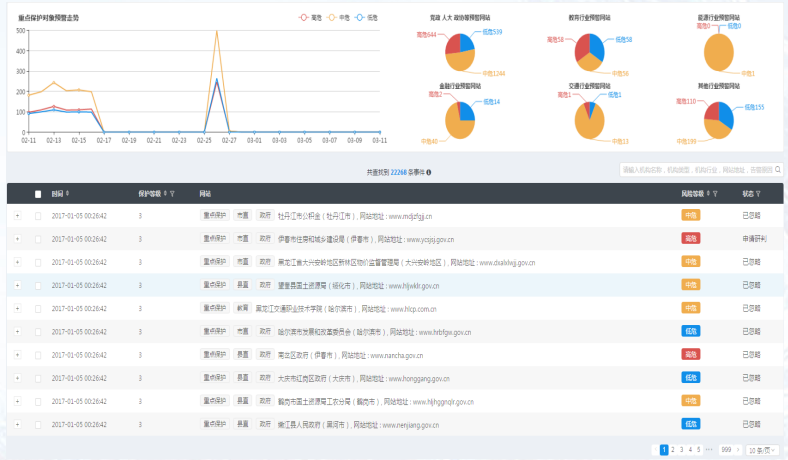
B » 以输出高价值告警为目标

多来源告警汇总研判，统一分级输出

C » 以安全业务为延展

开启安全业务流程的入口：

通报、预警、应急处置



平台价值四：贴合用户实际作业场景的安全闭环

实时告警

全量搜索
多层次过滤
针对隐患聚类
Whois信息查询
扫描历史对比

分析研判

重点保护
隐患分级
隐患对应威胁
近实时
多规则
告警历史对比

下发通知

自动生成整改通知
整改通知部分内容可配置
整改通知随时下载

通报审核

按条件集中处理
单条忽略
审核意见及时反馈

平台价值五：科学有效的应急响应

应急联动人员配置

应急响应资源支撑

平台建设预期效果

1、通过全面安全监测与威胁情报推送，精确、动态掌握全省病毒木马传播，网站安全遭受攻击情况

2、通过统一告警与综合研判，精准判断在哪里，什么时间，发生了什么威胁，提供清晰准确的风险判断

构建全天候全方位感知网络安全态势能力体系
切实帮助省委网信办履行监管职责

3、建立各信息系统与省委网信办的业务互通机制，提升重要信息系统的整体安全防御能力

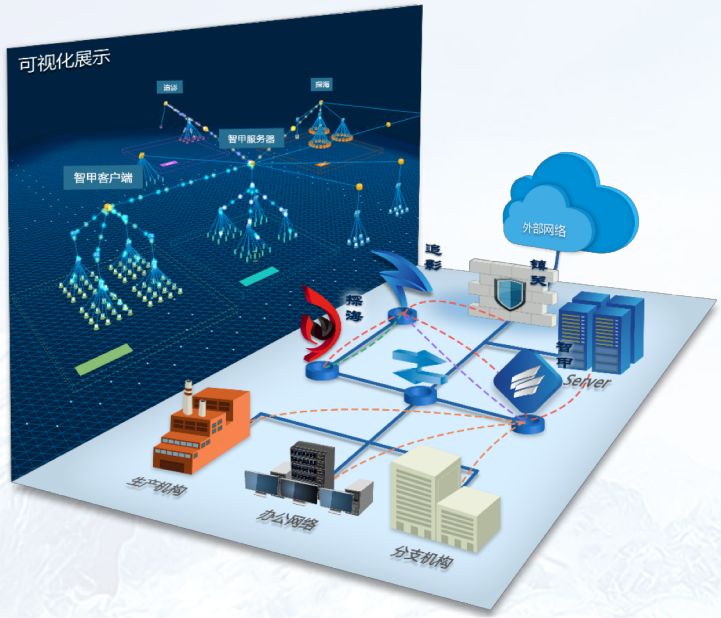
4、提供了“按需定向监测”、“按需定向鉴定”、“一键关停”等人机结合手段，提升应急处置工作效率

监管型态势感知与战术型态势感知的差异

	监管型	战术型
建设使用者	网络安全主管部门、职能部门、执法部门	重要信息系统和关键基础设施所有者
态势呈现	偏宏观，战略层面为主， 指导中观，提供部分战术指引	中观，战术层面的识别、理解、预测 提供微观线索指引猎杀、取证
与被监测资产关系	监管者	拥有者、运维者
感知范围	互联网**曝露资产**	**全部资产**
甄别研判	基于威胁认知和漏洞理解的泛化理解	结合资产“我情”的针对性分析研判
协同指控	偏重**体系间协同**	偏重**体系内指控**
威胁情报	基于通识的情报知识共享	**向量级情报适配**到具体环境指引猎杀
安全运维能力	第三方监管， 偏向合规检查、预警通报	与信息系统同步规划、建设、交付实施， 资产**安全运维一体化、全生命周期覆盖**
反馈、评估与改进	掌握被监管对象的整体能力 评估、引导规划方向	与自身业务情况深度结合、全面覆盖 基础结构和防御纵深的体系化持续改进
复杂度和实现难度	复杂单系统	超系统、复杂系统构成的体系

02 战术型态势感知的关键能力要求

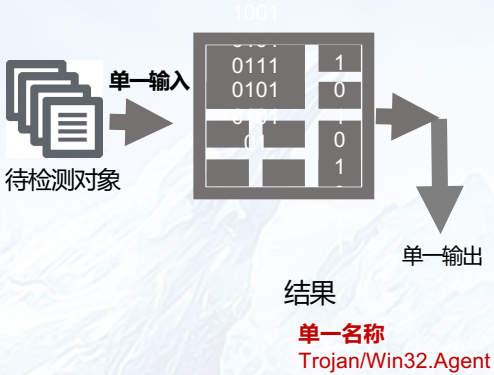
战术型态势感知需要以全面持续监测为基础



- 全局了解网络空间环境：网络空间地形（硬件、软件、服务）等
- 实时掌握环境中可能存在的脆弱点，将攻击面的窗口暴露最小化
- 面对发现的威胁，快速定位受害资产，及时止损

战术型态势感知需要以向量级情报指引猎杀

传统引擎

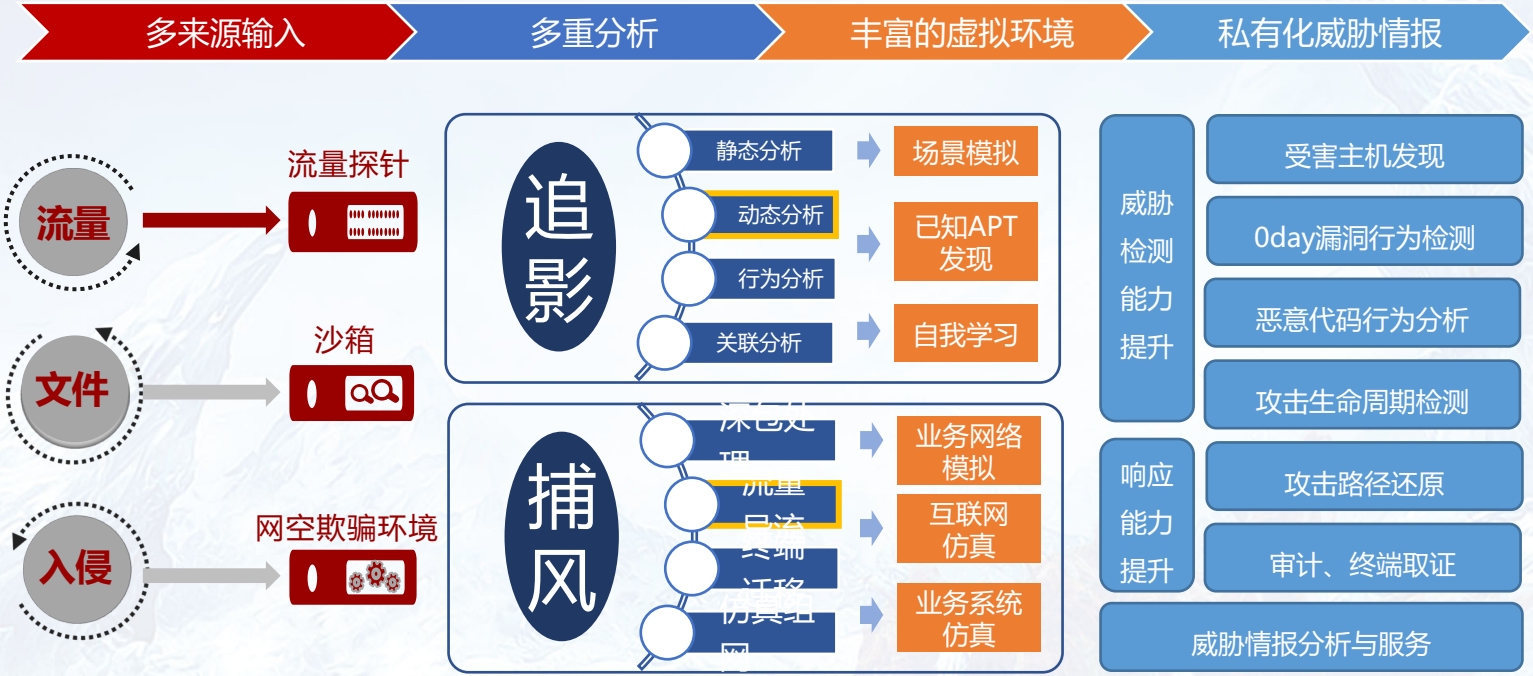


以单一对象为输入，以单一结果为输出。

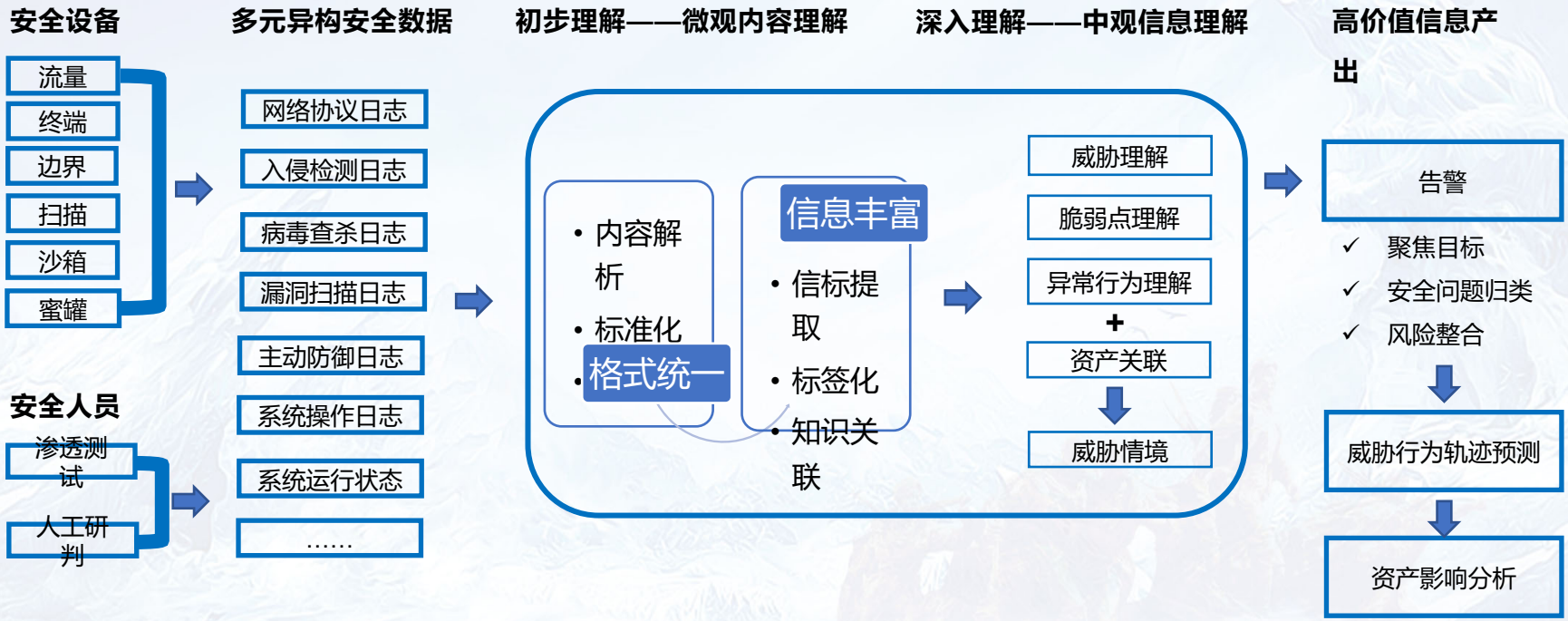
下一代威胁检测引擎

多种输入对象，多输出结果，威胁检测多样化。

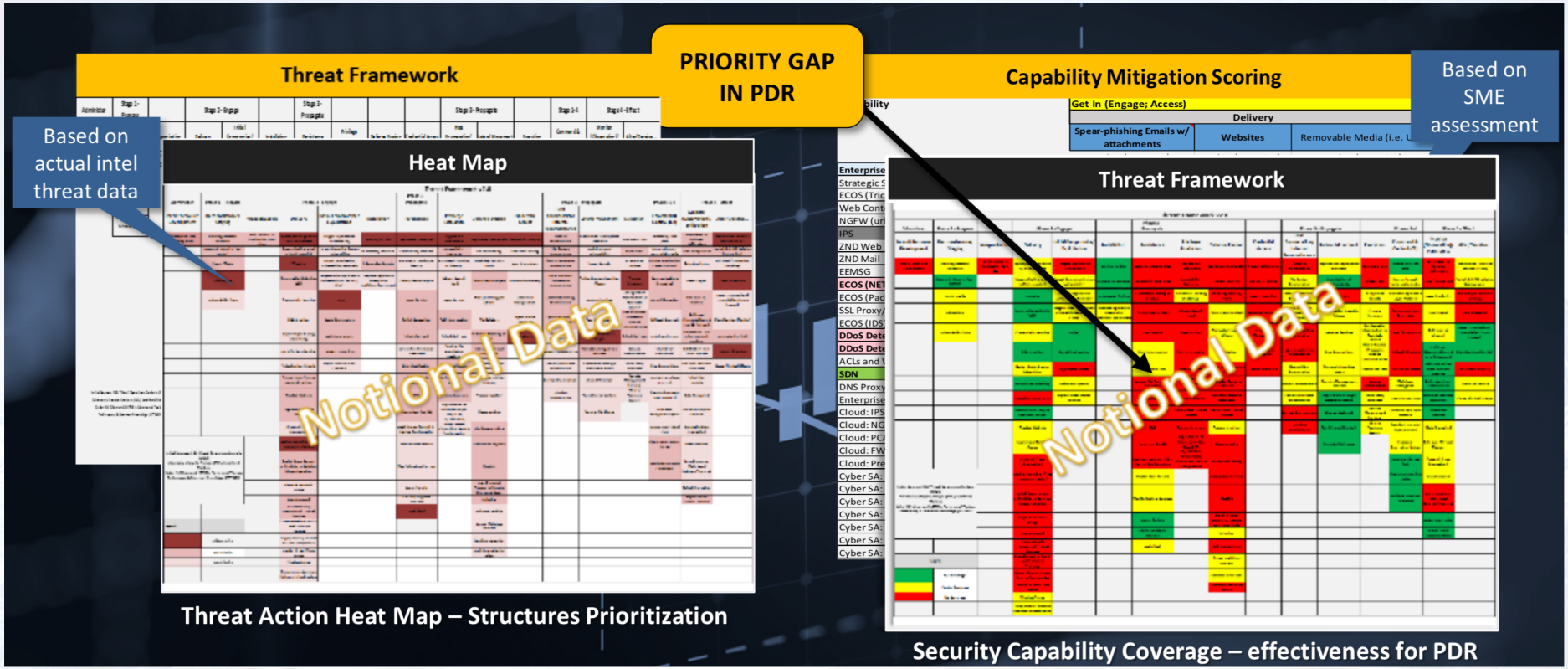
战术型态势感知需要基于我情的沙箱揭示线索



战术型态势感知需要基于威胁认知的信息融合



战术型态势感知需要对位对手的情报分析框架



引用自《DODCAR_-no class markings - Pat Arvidson.pdf》

态势感知对猎杀的平台支撑及现有能力分析

支撑网络威胁猎杀平台侧需要具备：

➢ 充分、细粒度的数据：

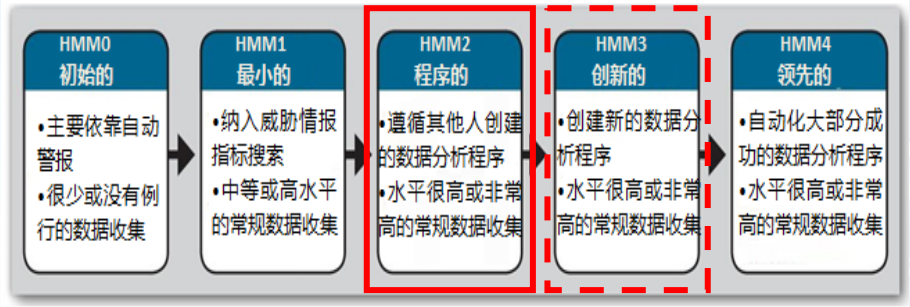
接收全要素采集数据，进行至少六个月数据留存，针对长期潜伏的威胁，为其建立攻击行为与攻击后果的关联提供充分的数据基础

➢ 有效的信息分析工具：

提供高效、准确的数据检索能力，以及多维度的数据分析工具，能够实现从提出假设、动作预判、数据验证、模型迭代完整猎杀过程提供可操作环境

➢ 高素质经验丰富的分析团队：

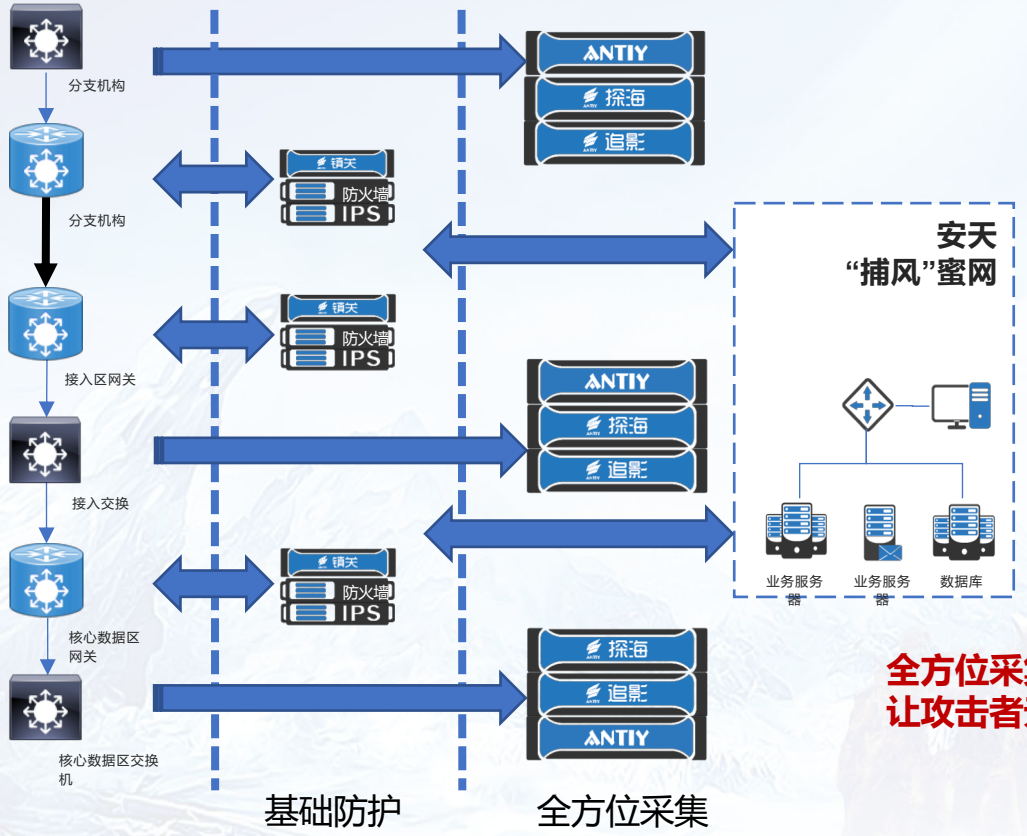
协调具有丰富经验的高素质分析团队，利用分析工具，基于积累数据，发现网络异常，逐步开展网内猎杀活动



现有猎杀能力应该至少位于成熟度模型的第二阶段，即可推荐假设，具备使用情境模型的能力，通过反复猎杀与分析人员经验与能力的提升，可达到成熟度模型的第三阶段，能够创建新的情景模型与分析方法

03 关键能力的解决方案实践

高防护等级网络，交叉火力全面覆盖持续监测

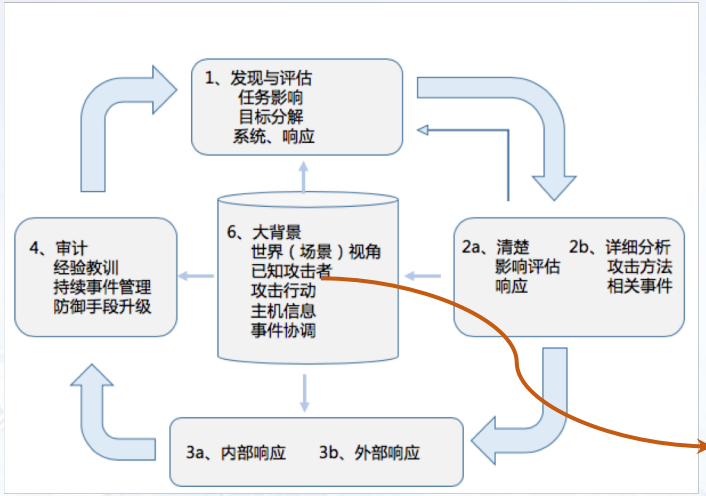


- 参考高价值目标构建合理分区
- 在抵达目标的路径上增加关隘
  - 业务路径
  - 数据路径
- 交叉火力**覆盖无死角**
  - **特别需要注意：设备管理流量**
  - **特别需要注意：包头记录**
- 被动防御能力是积极防御的基础

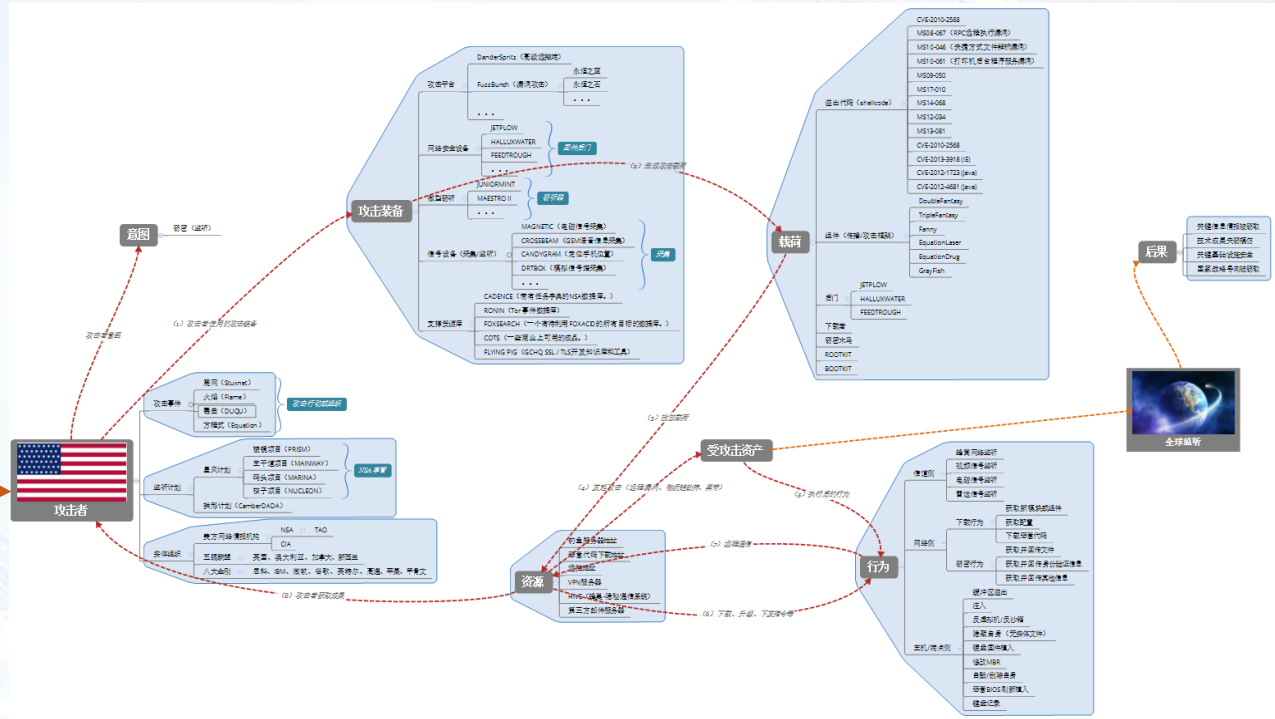
全方位采集、智能化响应
让攻击者无所遁行、无处可逃、无计可施

面向任务、基于知识，是有效理解能力的基础

- 系统落地的关键 ： 有重点、分阶段的分析支撑
- 系统可用的关键 ： 细粒度的资产信息和安全知识信息
- 系统好用的关键： 基于任务的模板库



来源：网空指挥控制任务流程（Erbacher 等人，2010）



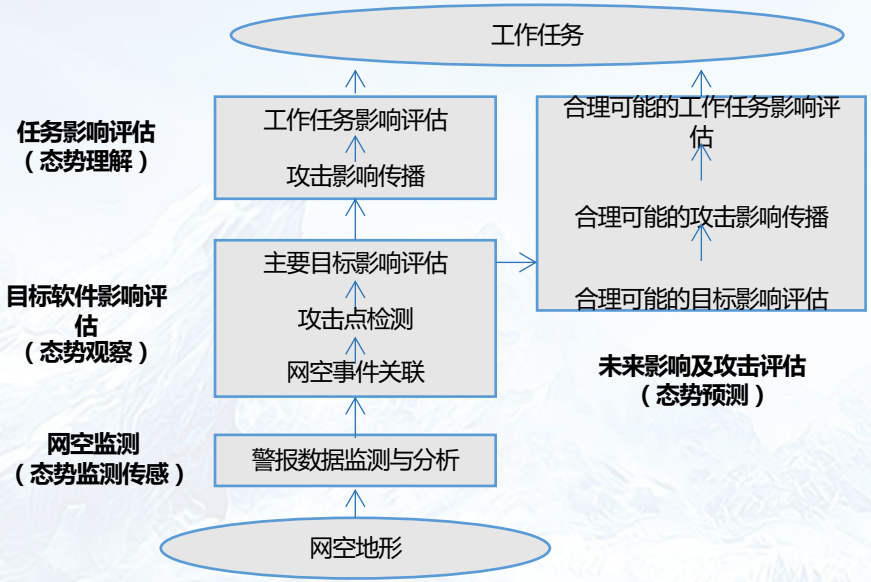
从任务目标分解，看地图炮式态势感知的价值和局限

价值

- 揭示严峻情况
- 避免盲目自信
- 持续推动防御体系完善

局限

- 虚假的安全感：“我可以看到一切”
- 放大认知偏差：乐观偏差、易得性偏差、幸存者偏差等

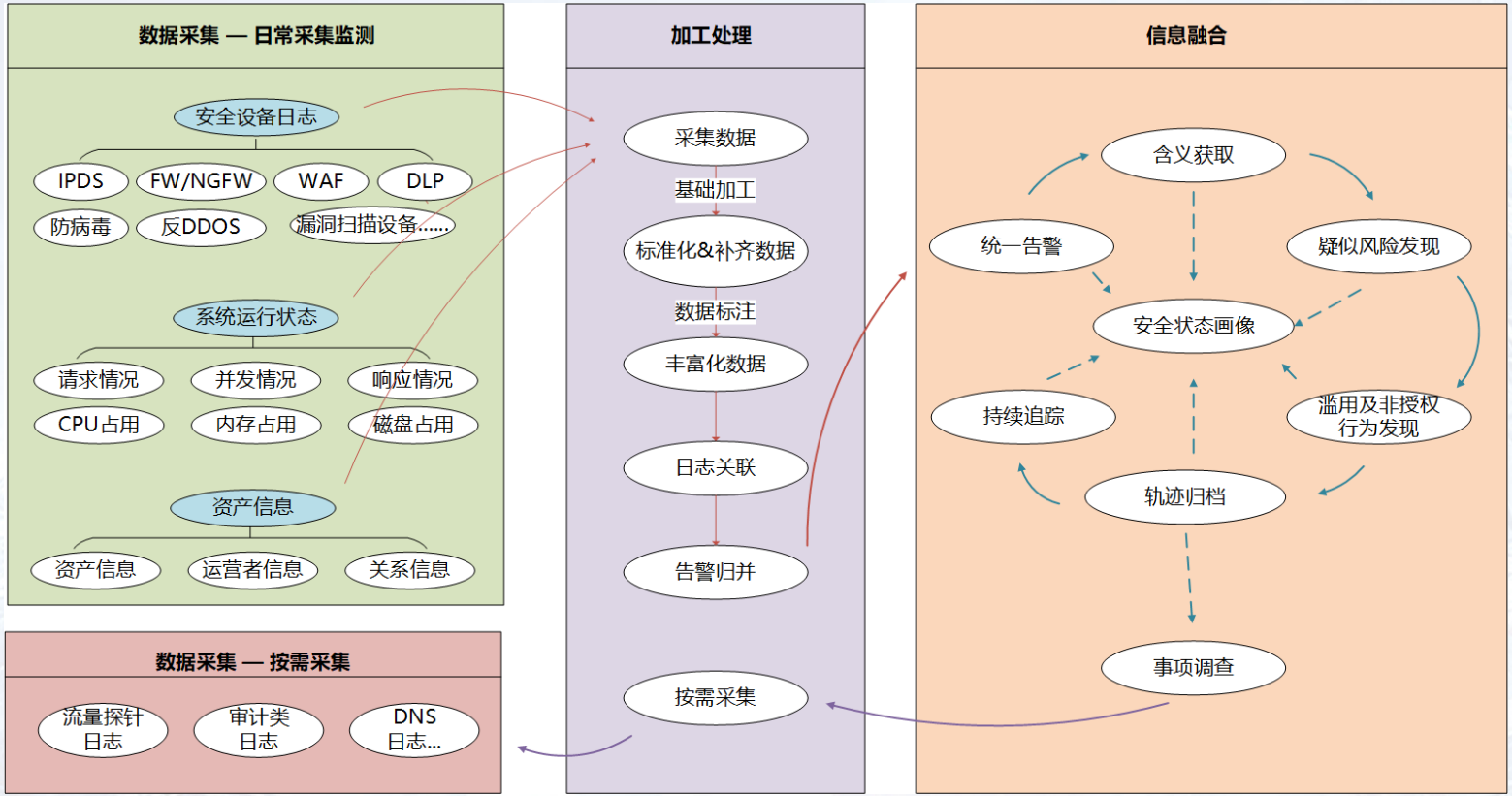


网空态势感知通用过程

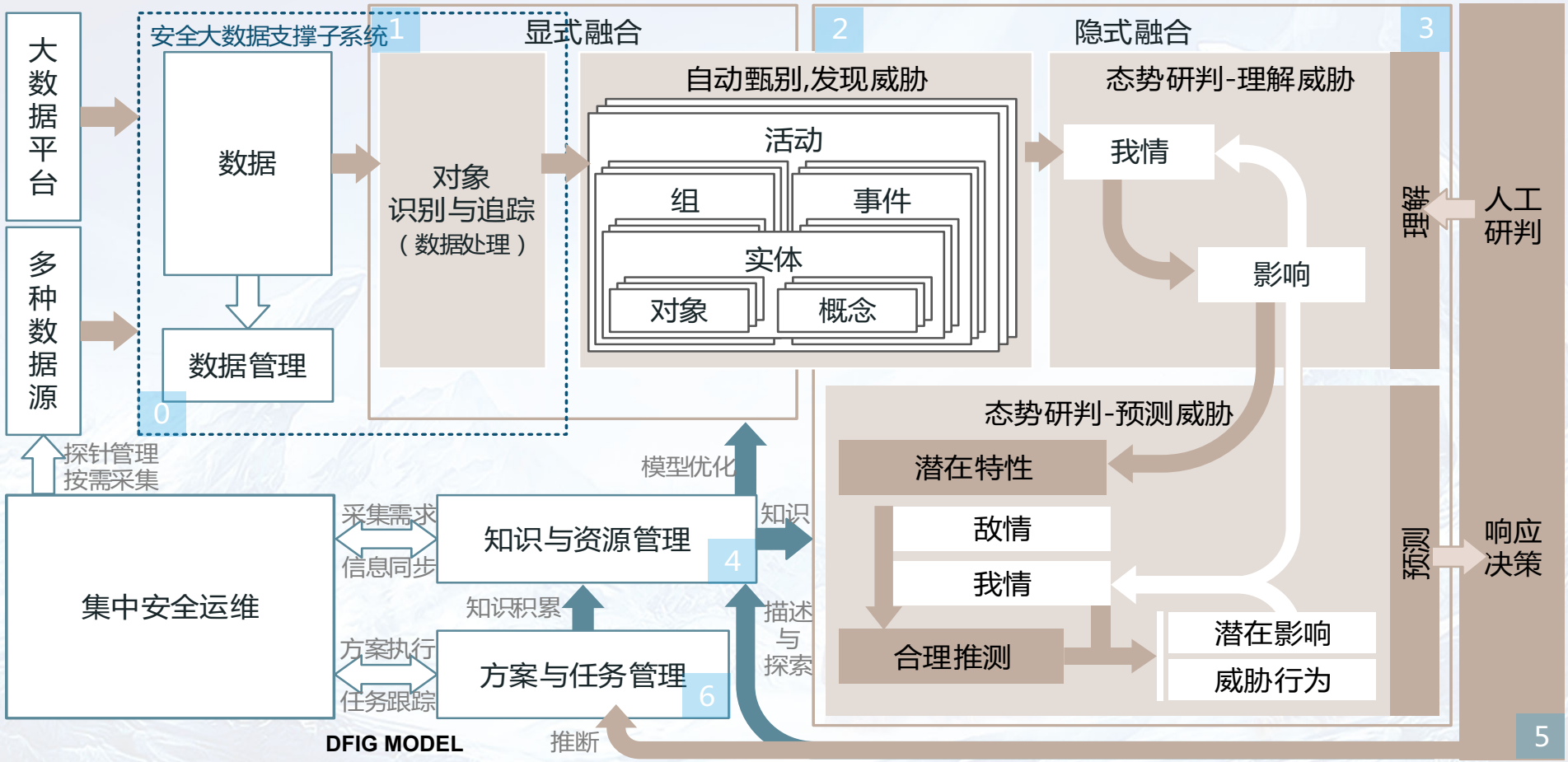
来源：工作任务的弹性恢复能力（G . Jakobson）

常见态势感知可视化模式

态势感知的数据基础 = 全面监测 + 高价值信息融合

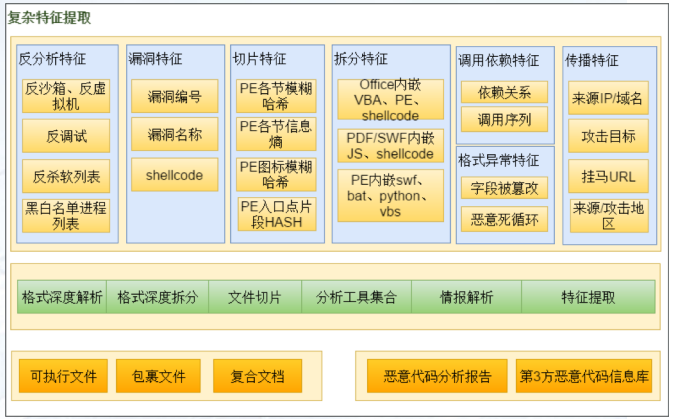


态势感知的数据基础 = 全面监测 + 高价值信息融合

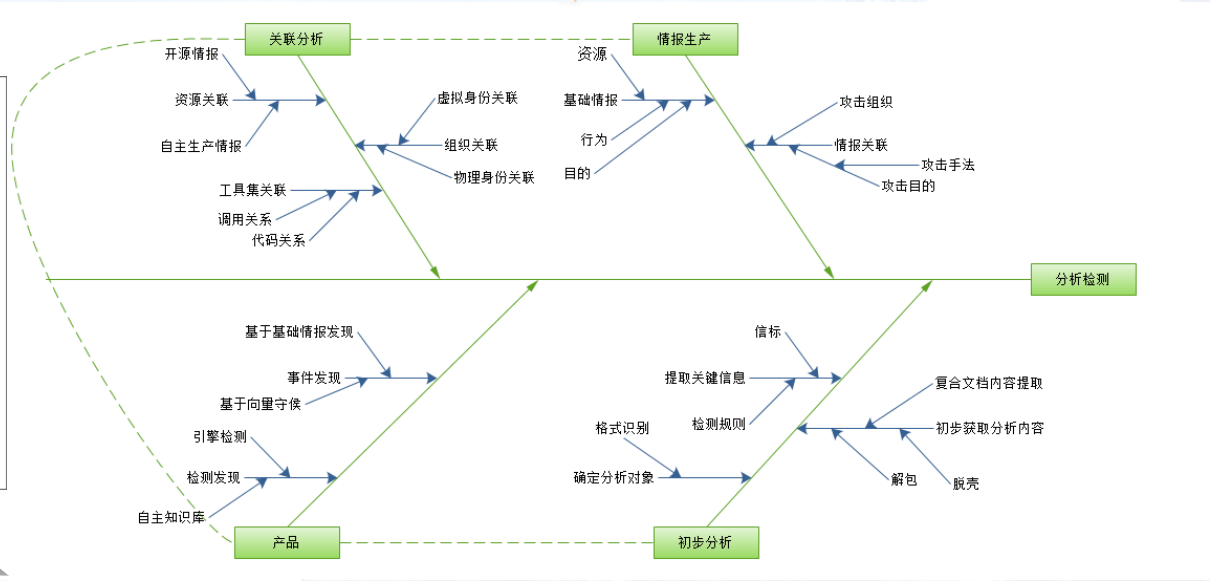


深度分析，支撑有效理解能力的持续提升

复杂特征提取



多向量关联



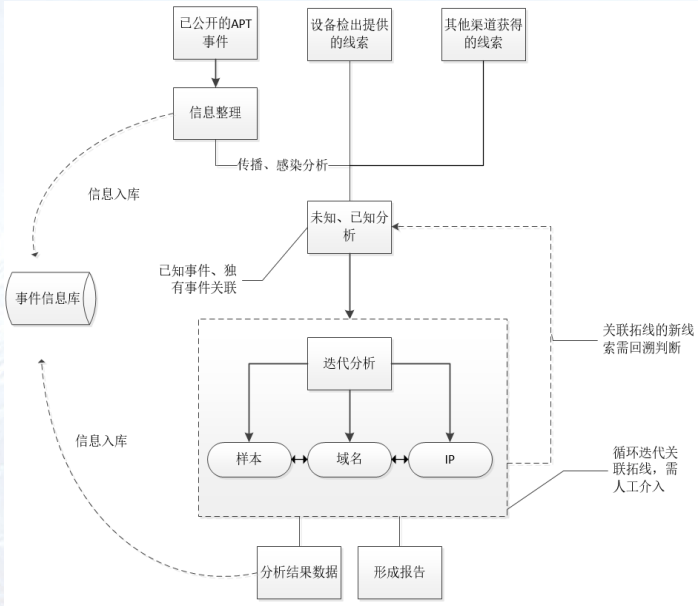
达成合理预测能力的几种典型姿势

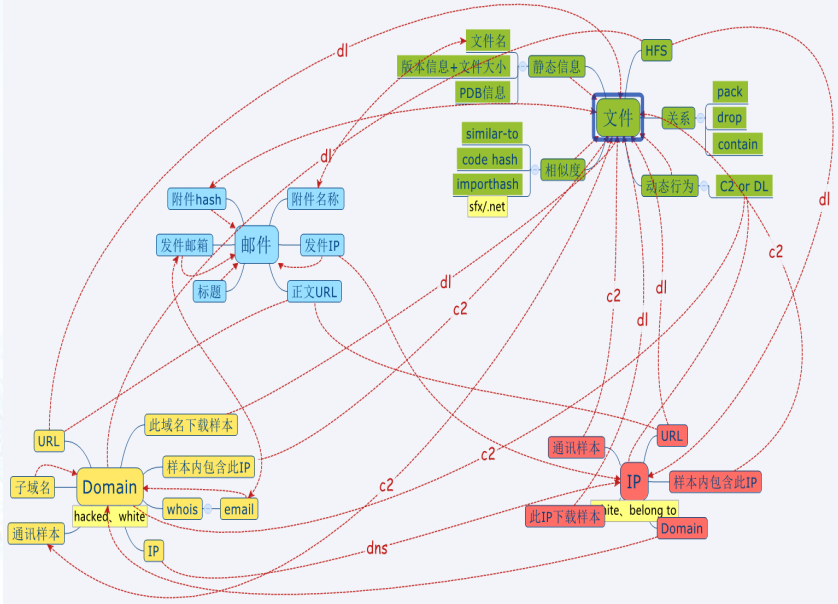
基础姿势

- 基于漏洞利用、目标资产
- 基于攻击行动
- 基于相关事件

增强姿势

- 面向业务运行影响
- 面向工作任务影响



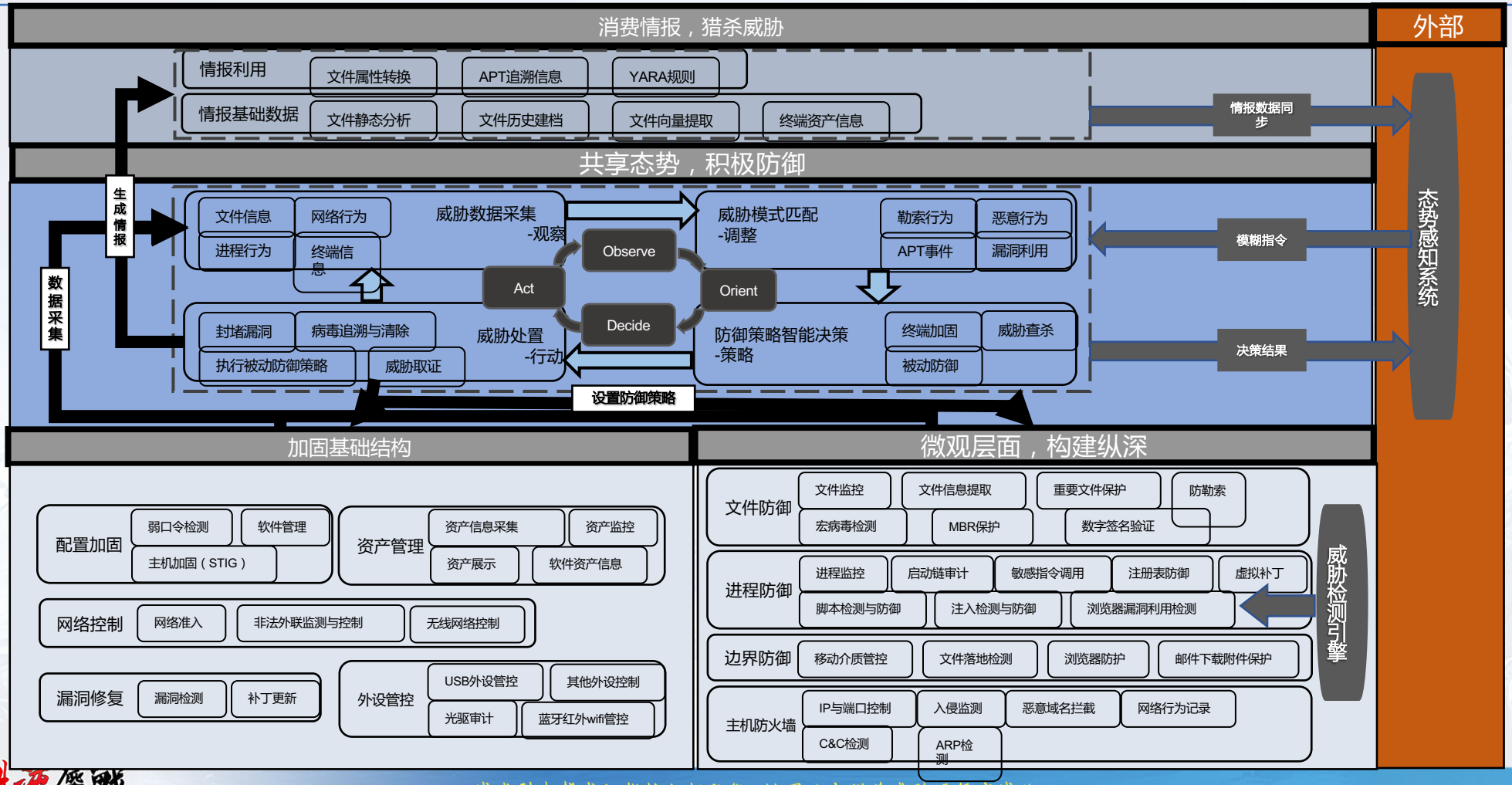


四种类型的联动响应能力

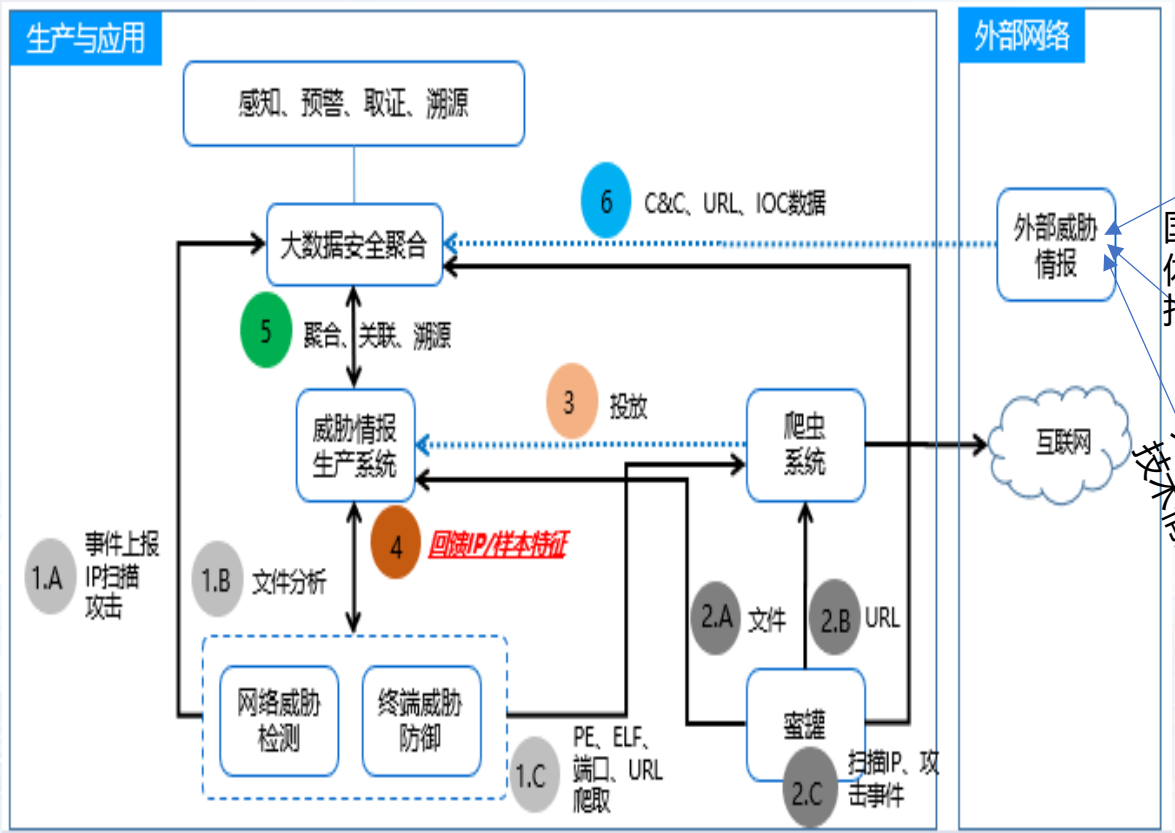
态势感知的指挥协同响应能力

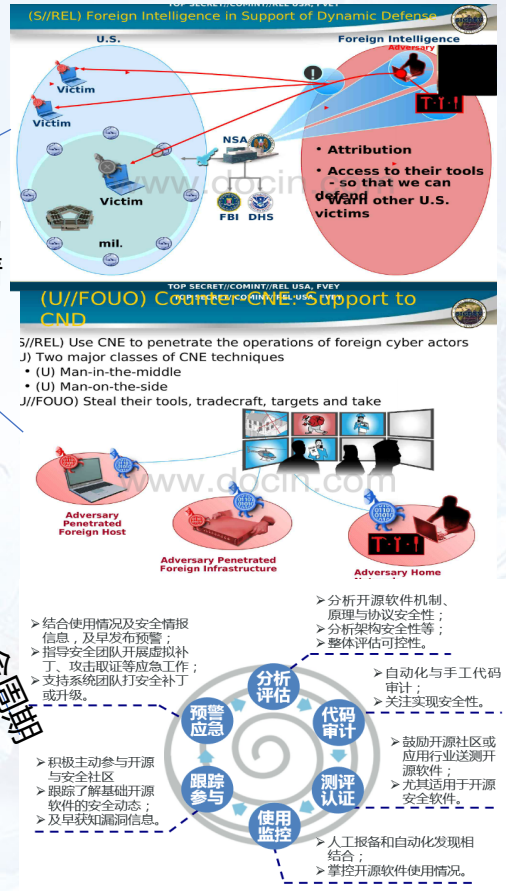
安全设备的被协同能力

态势感知的联动响应，必须推动防御体系能力提升



从“情报驱动”能力，到“情报协同”能力

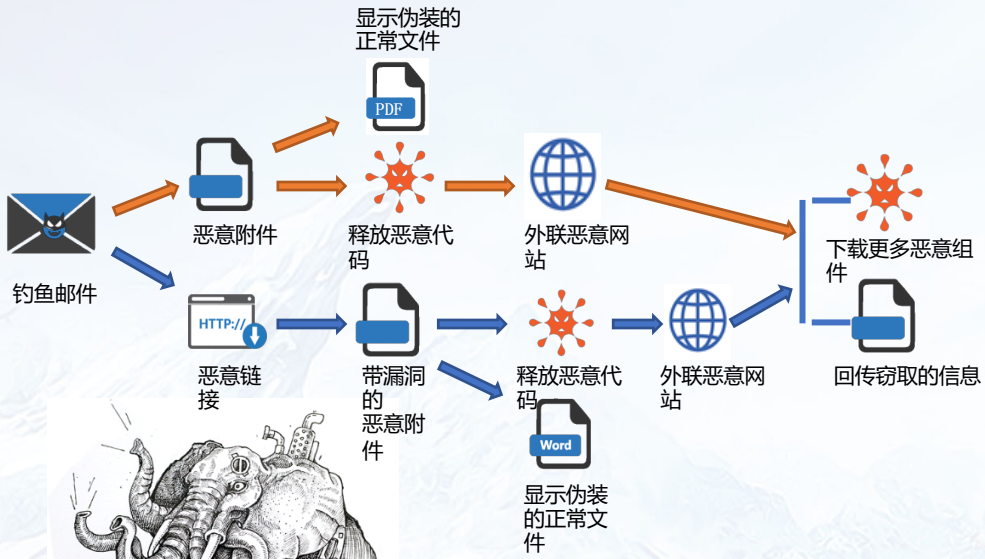




04 实际场景应用示例

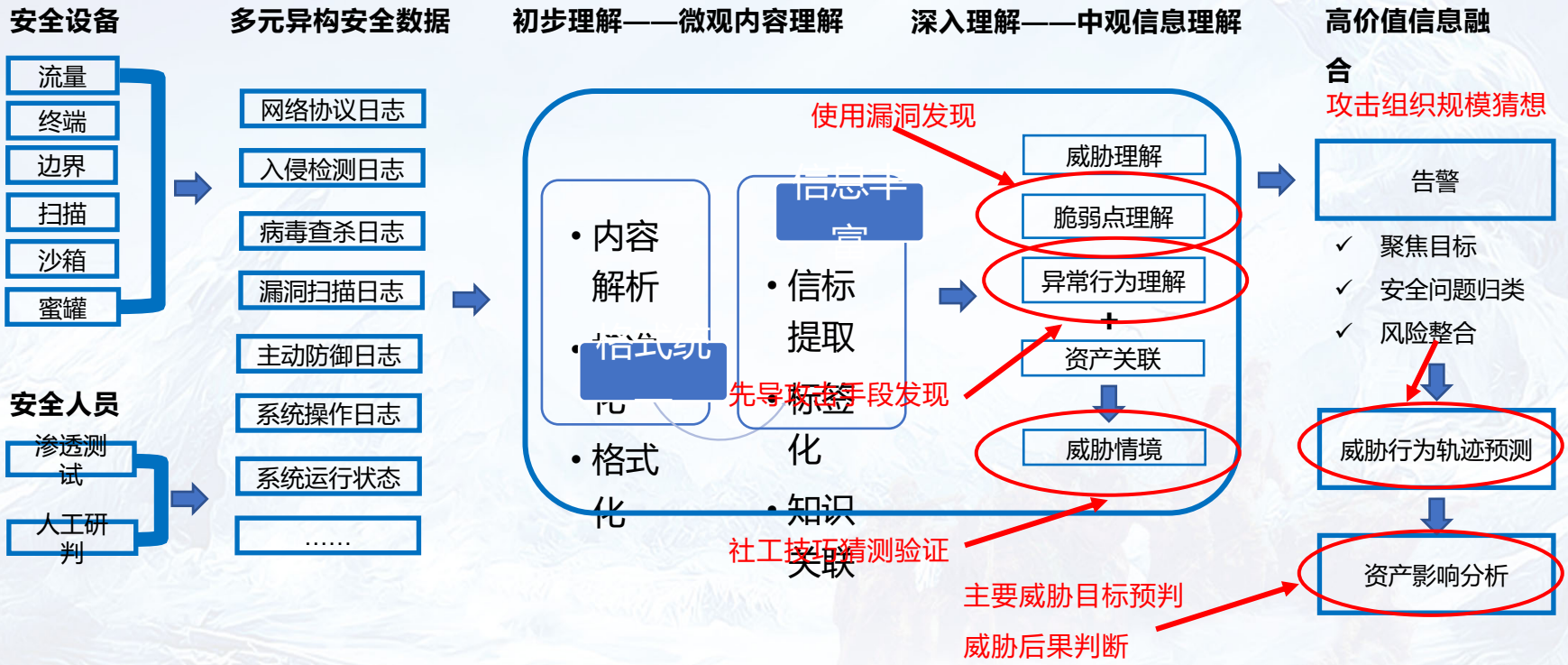
白象攻击的检测防御：1- 背景

“白象”技术、战术分析

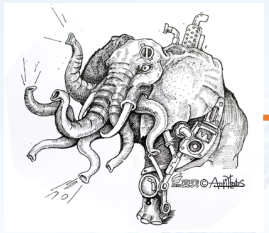


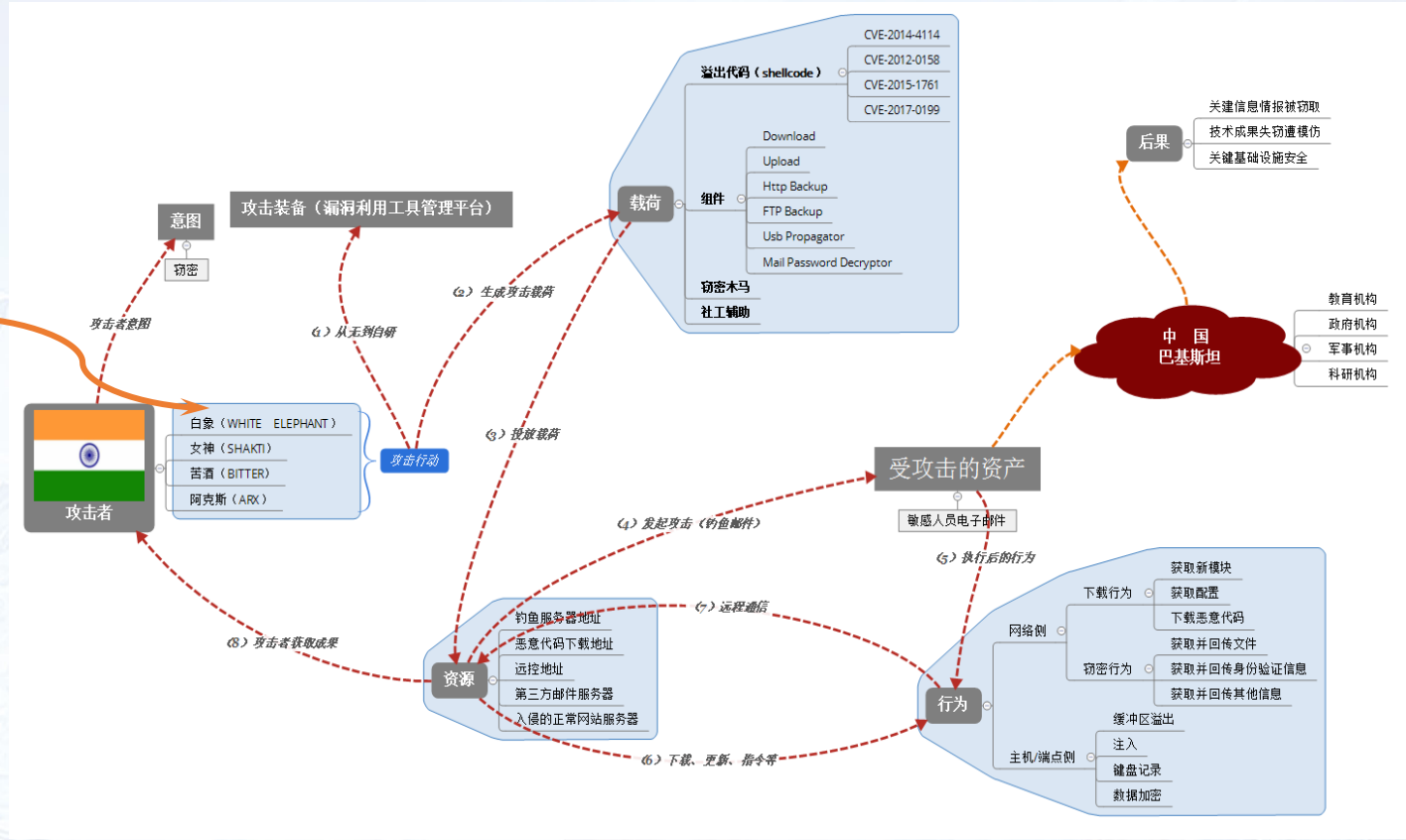
	白象一代	白象二代
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标（如高等院校）	巴基斯坦和中国的大面积目标，包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件，发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114 CVE-2012-0158 CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIt	Visual C#、AutoIt
二进制攻击载荷加壳情况	少数使用UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

白象事件的检测防御：2 - 发现与影响评估



白象事件的检测防御：3 - 威胁预测与猎杀





基于多向量关联分析的Cobalt Strike的事件发现

影响分析

事件发现

发现事件主机A
IP:192.168.23.220

事件样本
MD5:6D13119B42C
2CA71491E26A42B
CDB352

主机B
IP:192.168.34.133

样本B
MD5:FD217A7993E
B699E4C986D95321
6FAFF

利用已提取的向量检索其它主机，发现主机B中存在哈希不同于原事件样本A的样本B

向量提取

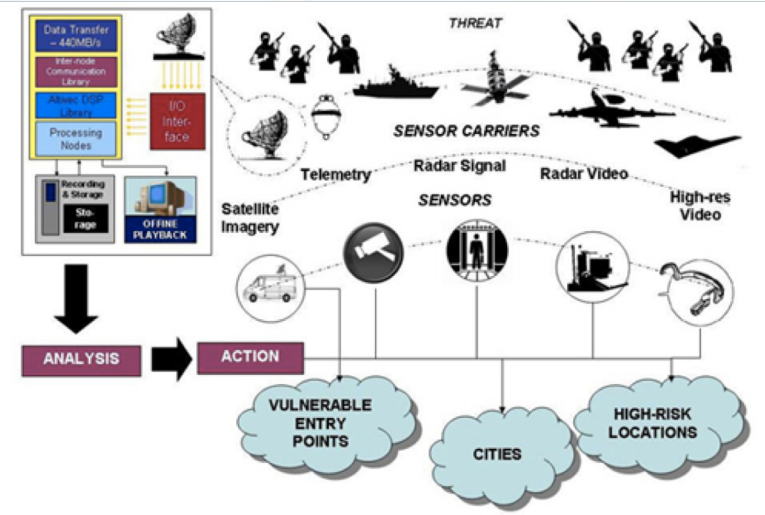
加密解密	网络通讯	进程操作	反调试	提权	获取信息	服务操作
• **RSA加密** • **AES加密**	• HTTP通讯 • IP:146.0.XX.107	• 枚举进程 • **进程注入**	• **检测调试器** • 显示调试字符串	• **查看系统权限的特权值** • **启动或禁止权限**	• **获取机器名称** • **获取用户名称**	• 创建服务 • 打开服务 • 启动服务

事件分析：Cobalt Strike v2.4（后门的商用平台）

态势感知的更多价值达成，依赖各方的共同努力

定位于体系化、实战化的态势感知解决方案，其独特价值在于

“既能支撑安全防御体系、也能推动安全防御体系建设”



更多态势感知相关的启示（推荐书籍）

网络空间安全防御
与态势感知

［美］ 亚历山大·科特 克利夫·王 罗伯特·F. 厄巴彻 著
（Alexander Kott） （Cliff Wang） （Robert F. Erbacher）

黄晟 安天研究院 译 黄晟 审校

- 系统介绍网络空间安全态势感知的基础理论
- 全面解析网络安全态势感知的内涵、实现框架和前沿问题
- 重量级序言深入解读领域研究成果和产业实践

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰