AsiaInfo | 亚信安全

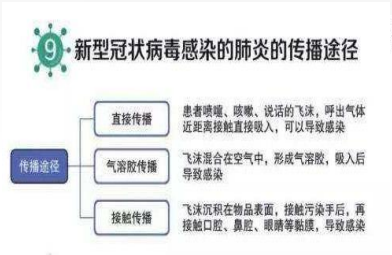
控制疫情需要速效隔离修复！

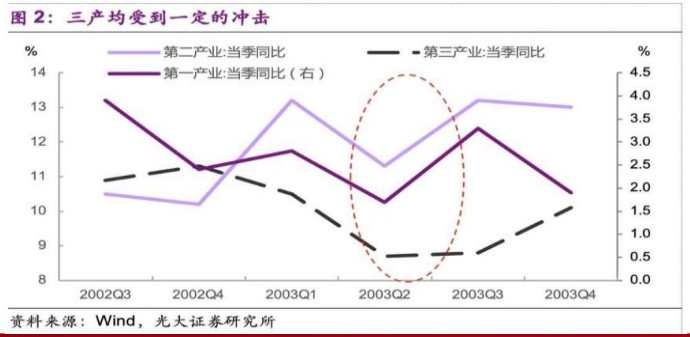
——亚信安全精密联动防治方案XDR

苏哲恒

2020.2.23

2020全民抗“疫”





为什么需要有应急机制?

为什么“疫情”难控制?

损失有多严重?

新冠病毒与高级威胁

AsiaInfo 亚信安全

病毒名称	新型冠状病毒	永恒之蓝（WannaCry）勒索病毒
传染源		—利用美军NSA网络攻击武器库工具
感染对象	人	服务器终端
传播途径		攻击微软SMB服务，通过139和445端口感染。
传染路线	人传人、人通过路网交通，各地爆发	机器之间互相传染，通过网络复制传播。
症状	发热	，桌面背景包含勒索语言和支付方式
传染强度	传染	，几个小时同网全部机器被加密。
严重性	严重，致死率目前在2~3%左右	严重，最核心数据全部被加密
易感群体	人群普遍易感。	"的，开放139、445端口的，后
特效药物	尚无	尚无很好的手段，被加密后破解难度很大
潜伏期	3~7天，最长14天	

“免疫系统”失效

应急手段有限

传播快、途径多，难发现

破坏不可逆，损失惨重

平时的防护容易被忽略

数据中心在抗“疫”中所面临的挑战

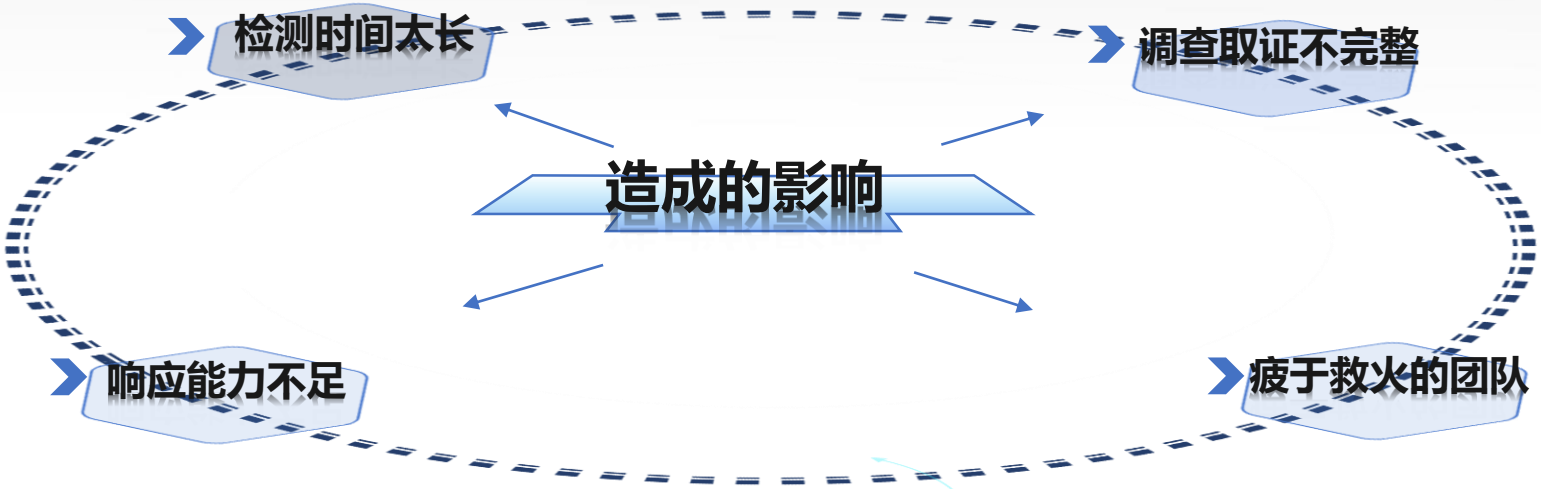
AsiaInfo 亚信安全

威胁检测日趋成熟，响应依旧落后

海量安全告警

沟通、人力成本

产品割裂



提升事件响应能力需要“速效隔离修复”

AsiaInfo 亚信安全

事件响应

专业的调查工具

终端检测及响应EDR

网络检测及响应NDR

高级威胁情报平台TIP

标准的工作手册

应对各种威胁的预案

安全响应专家

精密编排自动化

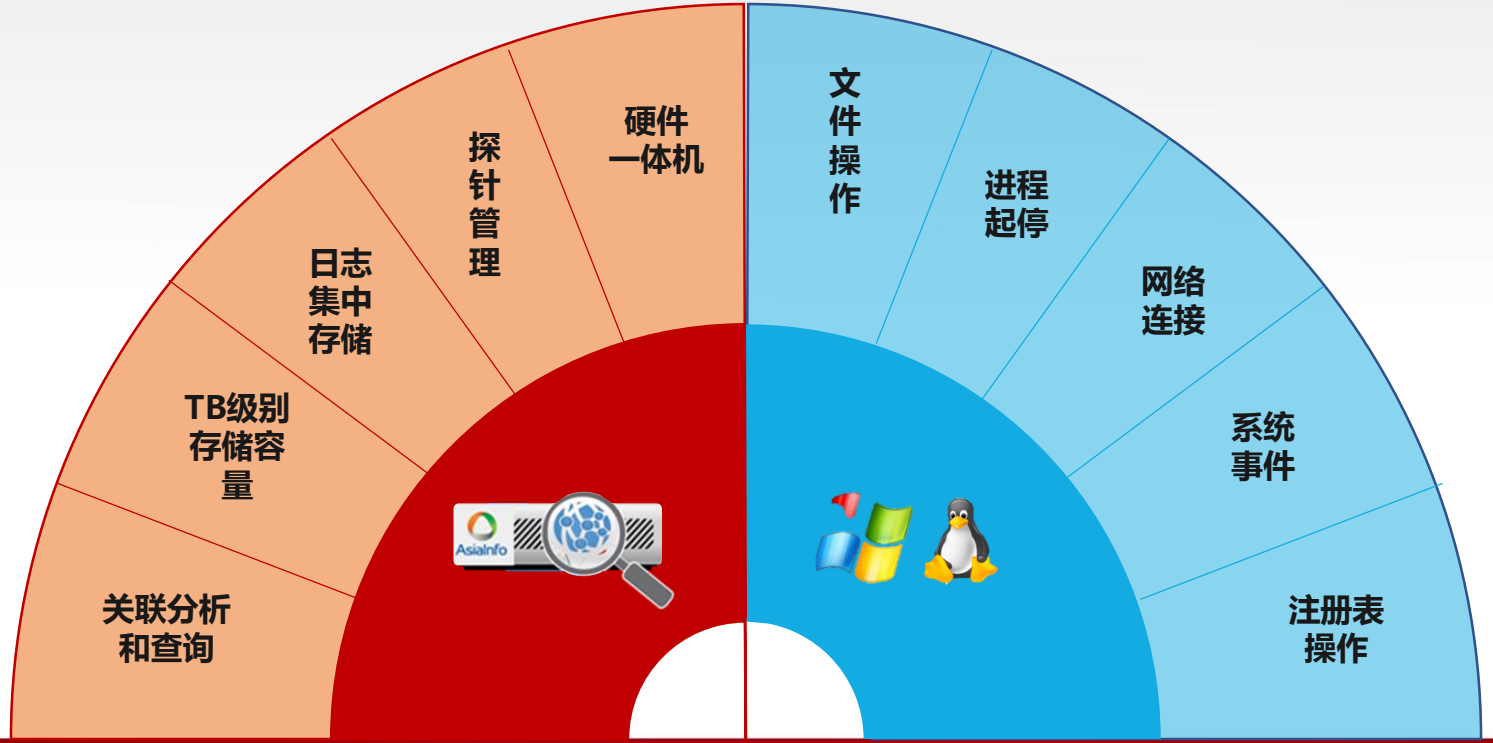
托管检测及响应MDR

专业的调查工具：高级威胁终端检测及响应系统

AsiaInfo 亚信安全

服务器端收集日志并进行关联分析

轻量级客户端高清记录系统行为

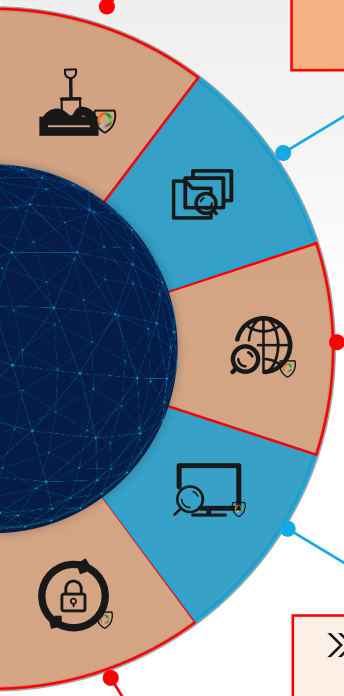


标准的工作手册：应对各种威胁的预案

层级	描述
1	准备
2	发现
3	分析
4	遏制
5	消除
6	恢复
7	优化

安全响应专家：精密编排自动化

AsiaInfo 亚信安全



服务背景

入侵应急响应是客户主机或网络在遭受黑客入侵之后，安全团队给客户提供的一系列安全服务，
包括但不限于定制威胁处理预案、阻断入侵、确定影响范围、帮助恢复生产、调查取证和给出整改建议等。

服务形式

通过充分调研客户的业务场景、安全需求和组织架构，帮助用户订制应对各类威胁的预案；
应急响应IR是在客户遭遇入侵后主动邀请和要求下，运维团队和攻防团队为阻断攻击，恢复业务甚至调查取证而提供的一次安全服务。

服务准备

利用**终端检测及响应EDR**和**网络检测及响应NDR**工具，了解黑客攻击过程和攻击路径，找到关键攻击线索。

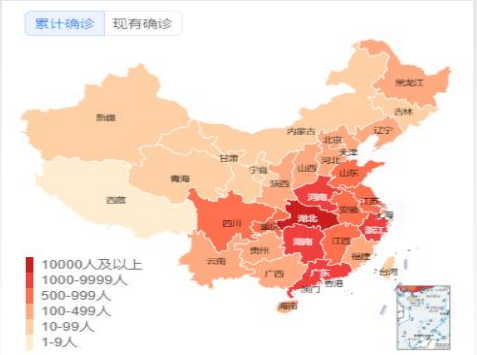
服务执行

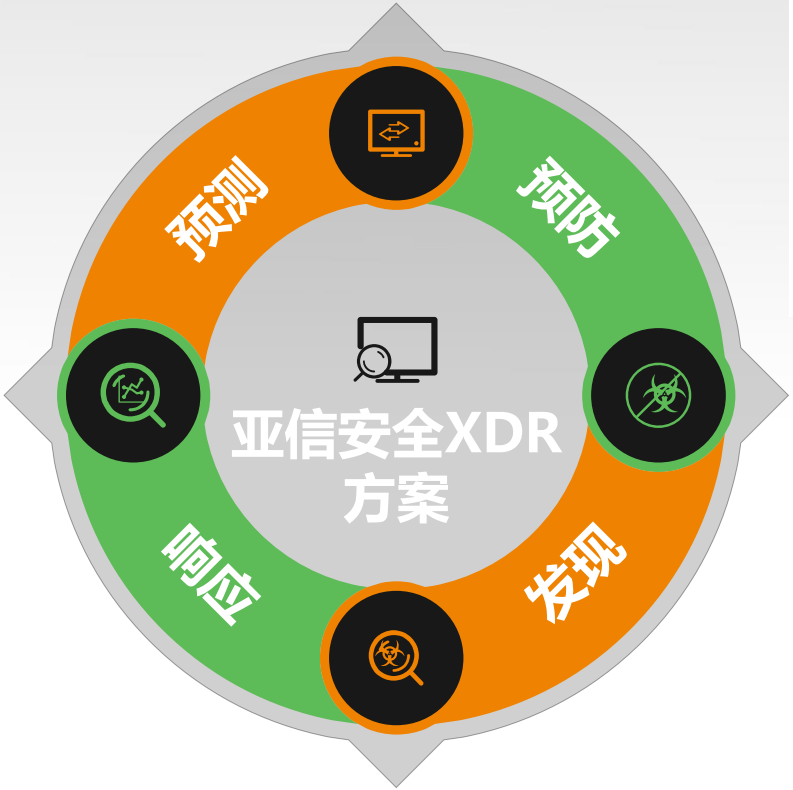
确定影响范围后，服务团队现场搜集数据，利用取证产品获取关键信息。
并根据收集到的信息，找出完整的证据链。

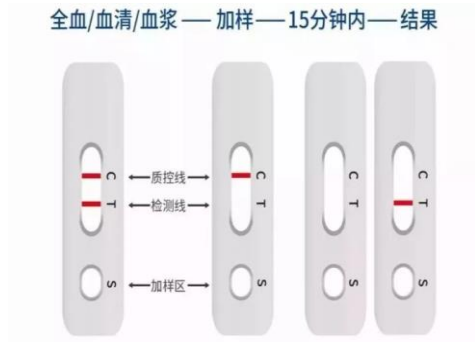
服务结束

服务结束后，服务团队需告知客户，提供完整的黑客入侵报告。原始数据和取证数据留档保存。
给出后续整改方案，防止再次出现同类攻击。

亚信安全精密联动防治方案——XDR







为数据中心打造全套的预防设备

——“一两“威胁防御价值远大于”一斤”的威胁检测

AsiaInfo 亚信安全

端点防护

云和服务器防护

电子邮件防护

网络防护

云、管、端全方位的安全威胁防护

缩短“疑似”到“确诊”的时间

——沙盒、取证溯源等技术提升高级威胁发现的效率

AsiaInfo 亚信安全

新冠肺炎出现“假阴性”病例 什么是假阴性_旅泊网

2020年2月10日 - 新冠肺炎疫情发展至今,随着核酸咽拭子的检验方法越来越成熟,现在病毒感染的确诊速度也越来越快了。但是目前各地通报的“假阴性”病例,让大家又有着不...

海量安全告警

信息孤岛

攻防特性

业内领先的沙盒技术

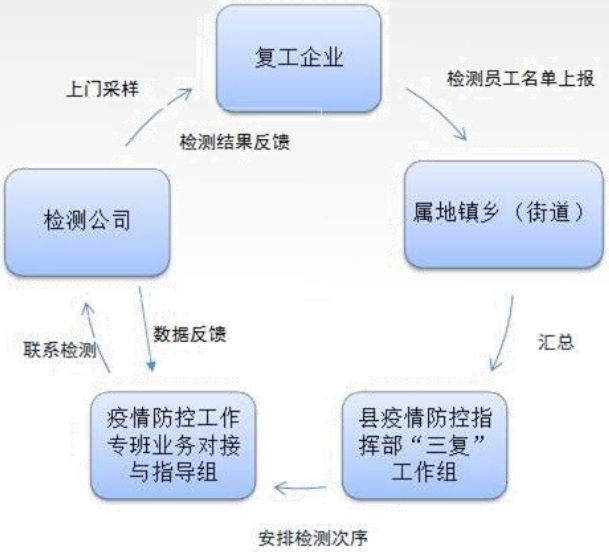
基于IOA分析能力

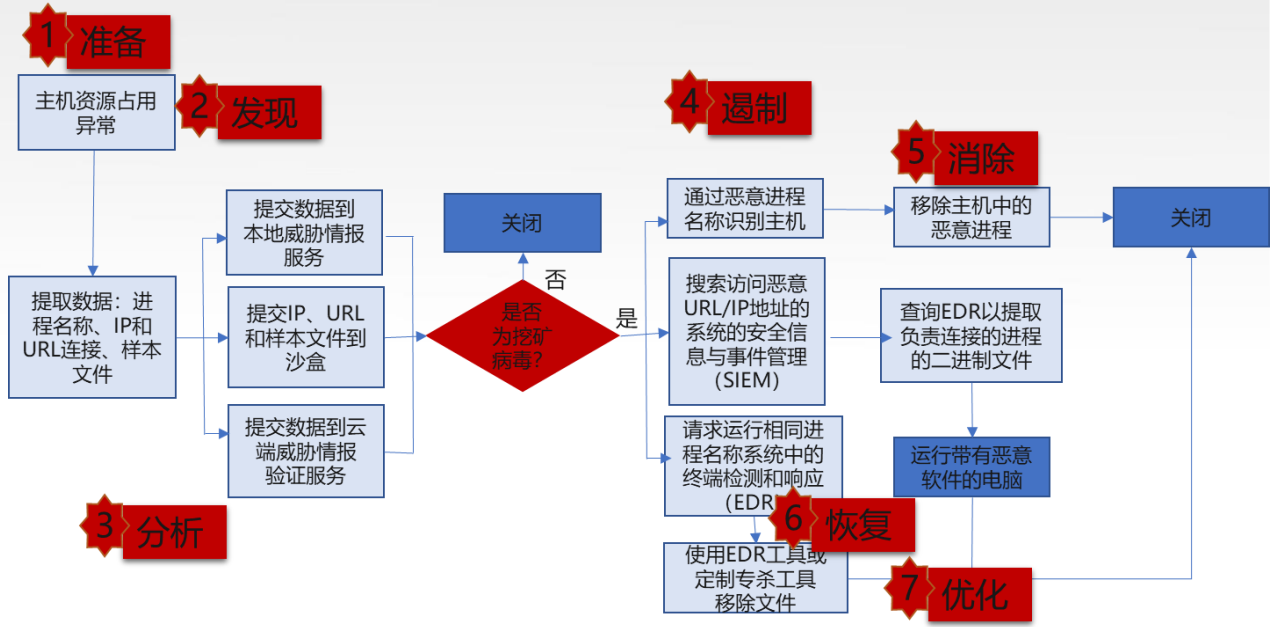
稳定的取证溯源能力

网络终端联动验伤能力

精密联动，缩短应急处置时间

——高级威胁的根因分析、范围判定、取证溯源、联动处置，一站式运维

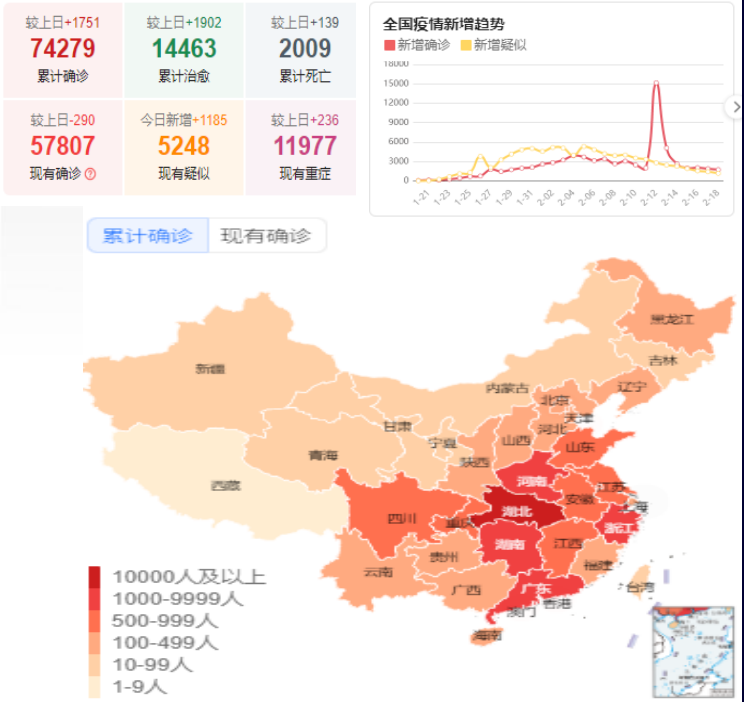




威胁“新增” “疑似” “确诊”全面感知

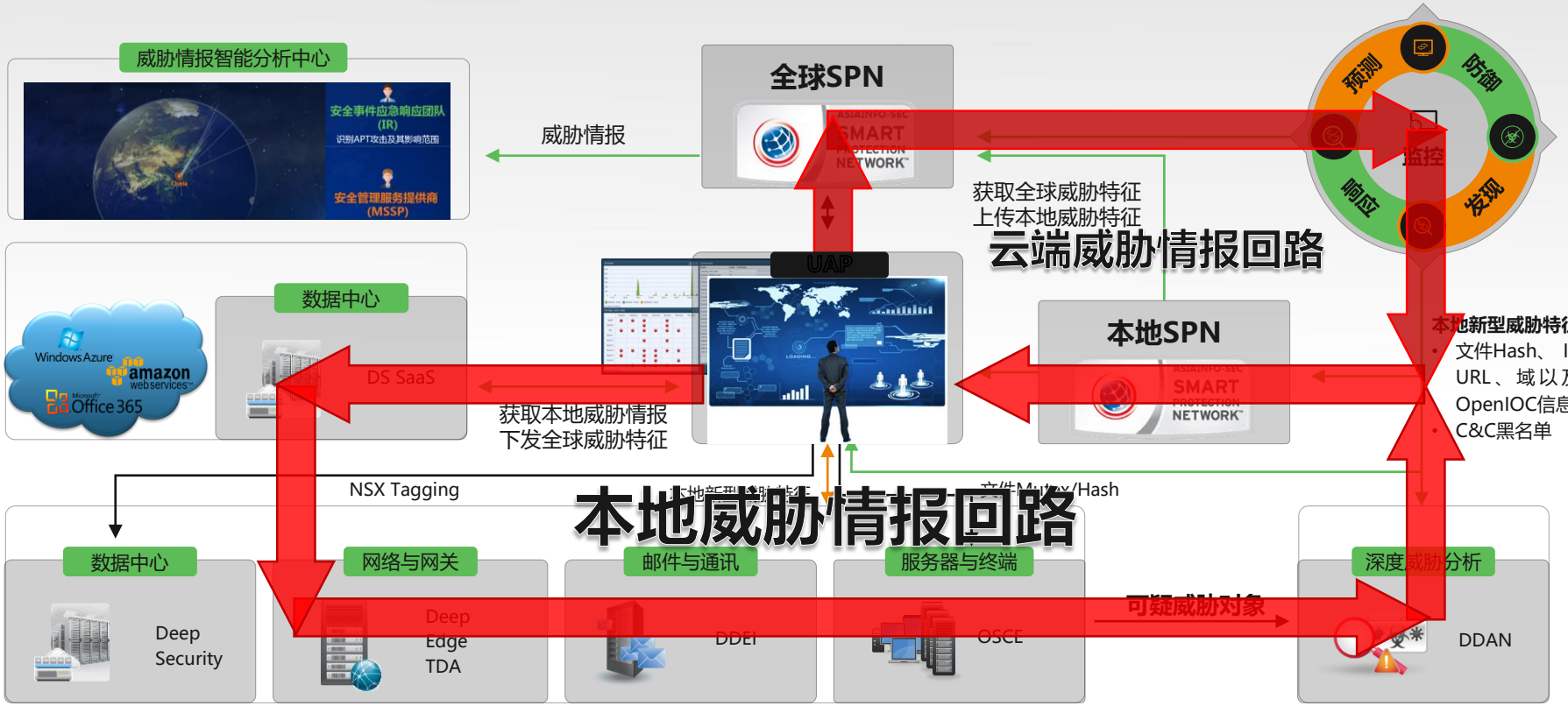
——随时掌握“疫情”局势

AsiaInfo 亚信安全



快速生成“疫苗”并自动部署

——基于本地威胁情报建立免疫机制



亚信安全 XDR 方案全景

AsiaInfo 亚信安全

检测

高级威胁发现

Deep Security

TDA
Deep Edge
DDEI

OSCE

CTDI

产生可疑威胁日志

分析

安全运营
事件管理

态势感知
UAP
SIEM
SOC

高级威胁分析

ASIAINFO-SEC SMART PROTECTION NETWORK

TIP
DDAN

主机取证

CTDI (EDR)

网络取证

TRA (NDR)

终端取证

CTDI (EDR)

响应

云

Deep Security

管

Deep Edge
DDEI

端

OSCE

1. 提交威胁告警

2. 确认威胁真实性、本质及意图

3. 调查取证、验伤、评估

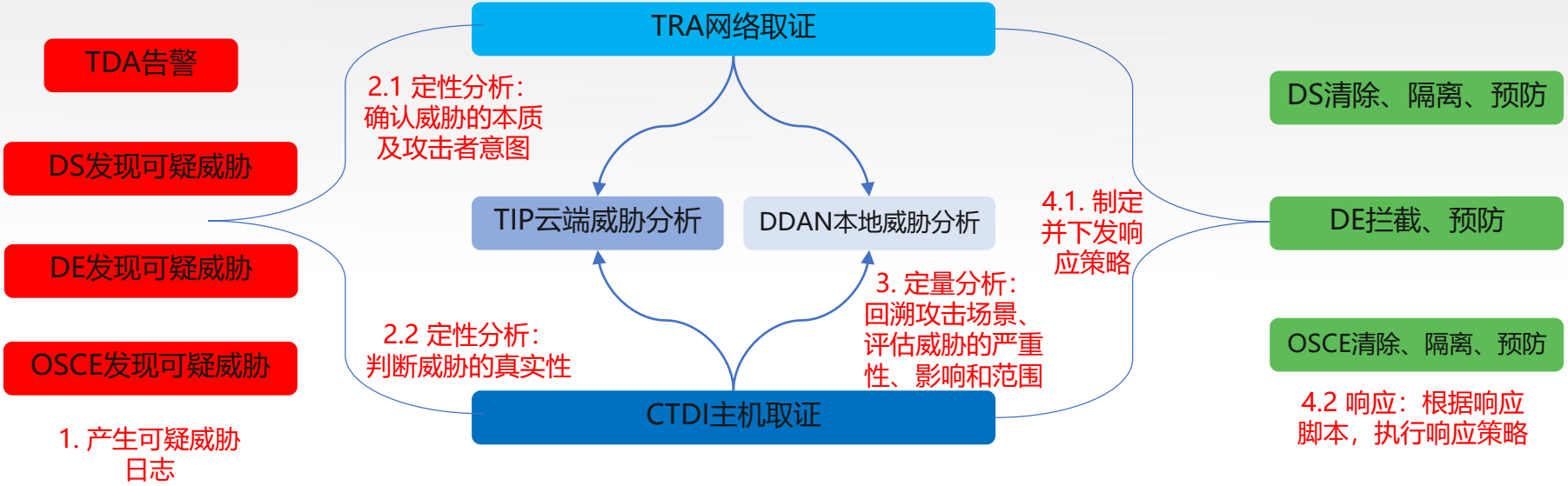
4. 自动化下发并执行响应策略

预测

XDR

精密编排的快速恢复补救

亚信安全 XDR 方案原理



亚信安全 XDR 方案亮点

AsiaInfo 亚信安全

解决的问题

- **云、管、端、邮全面防护**
  ——减少应急事件的发生
- **全网威胁可视化**
  ——全面掌控风险
- **全球领先的威胁分析技术**
  ——摆脱日志DOS，降低人力成本
- **精密联动**
  ——缩短应急响应时间、提高运维效率
- **自动建立安全免疫机制**
  ——避免下次中招

优势

- **“全”：云管端邮，全方位安全感知**
- **“准”：沙盒溯源，根因分析定位准**
- **“快”：精密联动，一站运维效率快**

AsiaInfo | 亚信安全

谢谢