AsiaInfo | 亚信安全

精密联动，智能运维，智慧护航

曹同玥

亚信安全资深安全顾问

关于亚信安全

AsiaInfo 亚信安全

2000年
发力安全领域

2008年
身份认证安全

2014年
大数据安全管控

2015
亚信安全成立
亚信科技收购趋势科技中国

2016年
成立 网络安全产业技术研究院
召开 C3安全峰会

2017年
成功抵御全球第一只勒索蠕虫WannaCry

2018年
连续三年蝉联中国网络安全企业十强

数据安全产品体系

AsiaInfo | 亚信安全

数据安全治理

数据过程管控

基础数据防护

数据安全管理与分析平台

MAXS

- 数据安全策略
- 数据分类分级
- 数据周期节点
- 数据安全事件
- 数据威胁分析
- 数据安全全景视图
- 数据安全资产
- 数据安全预警

数据发现系统	数据加密系统	数据泄露防护系统	数据脱敏系统	大数据管控系统	数据溯源
AI-DSG	AI-Encrypt	AI-SDG	AI-SDM	AI-BDS	AI-DPS
可监视	可隐密	可保护	可管控	可管控	可审计
生产	传输	存储	处理	使用	流通

AI-VMI 移动虚拟化数据安全

AI-TDA 深度威胁分析

AI-CTDI 数据泄漏调查取证

没有绝对的安全

AsiaInfo | 亚信安全

安全从业者与网络攻击者的博弈将会一直随着技术发展而持续下去，

任何个体、企业或者国家都不可能保证绝对的安全。

海量的安全事件

AsiaInfo | 亚信安全

>10000

超过55% 的IT安全专家每天收到海量安全告警

25+

超过50%企业使用多种独立安全技术

巨量的告警，难以发现未知的威胁

可视化孤岛导致对风险态势的理解有限

Source: 1. SC Media Survey, 2018, 2. ESG, OCT 2017

安全事件的处置响应要求

AsiaInfo | 亚信安全

- 《网络安全法》的要求
  - 第三章 **网络运行安全**
    - 第二十一条，第三十一条，第三十四条，第三十八条，强调了人员，制度，防治，容灾，应急预案，风险评估等要求
  - 第五章 **监测预警与应急处置**
    - 整章提出了对预警机制的建立要求，对应急处置，应急预案，应急演练的要求。
- 《国家网络安全事件应急预案》的要求

事件分级	描述
重大特别	**大面积**瘫痪，**丧失**业务处理能力，**特别**严重威胁，**特别**严重影响
重大	**长时间**中断或局部瘫痪，严重威胁、严重影响
较大	系统中断，**明显影响**系统效率，业务处理能力受到影响，**较**严重威胁，造成**较**严重影响
一般	**一定**威胁，造成**一定**影响

预警响应	描述
红色	联系专家和有关机构，跟踪研判，24小时值班，队伍进入待命状态
橙色	组织开展预警响应工作，密切关注事态发展，及时通报，队伍保持联络畅通
黄色	启动相应应急预案，指导组织开展预警响应
蓝色	启动相应应急预案，指导组织开展预警响应

应急处置	描述
Ⅰ级	成立指挥部，统一领导，24小时值班，跟踪事态，检查影响范围，处置进展汇报
Ⅱ级	进入应急状态，好应急处置，通报事态发展，应急技术支撑队支持配合
Ⅲ级	按相关预案进行应急响应
Ⅳ级	按相关预案进行应急响应

精密编排的事件响应

标准的预案：各种重大威胁的预案

AsiaInfo | 亚信安全

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：网络安全事件应急响应服务

AsiaInfo | 亚信安全

服务背景

网络安全应急响应是客户主机或网络在遭受入侵和破坏之后，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

应急响应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

利用专业产品和工具，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，利用专业产品获取关键信息。
并根据收集到的信息，找出完整的证据链。

服务结束

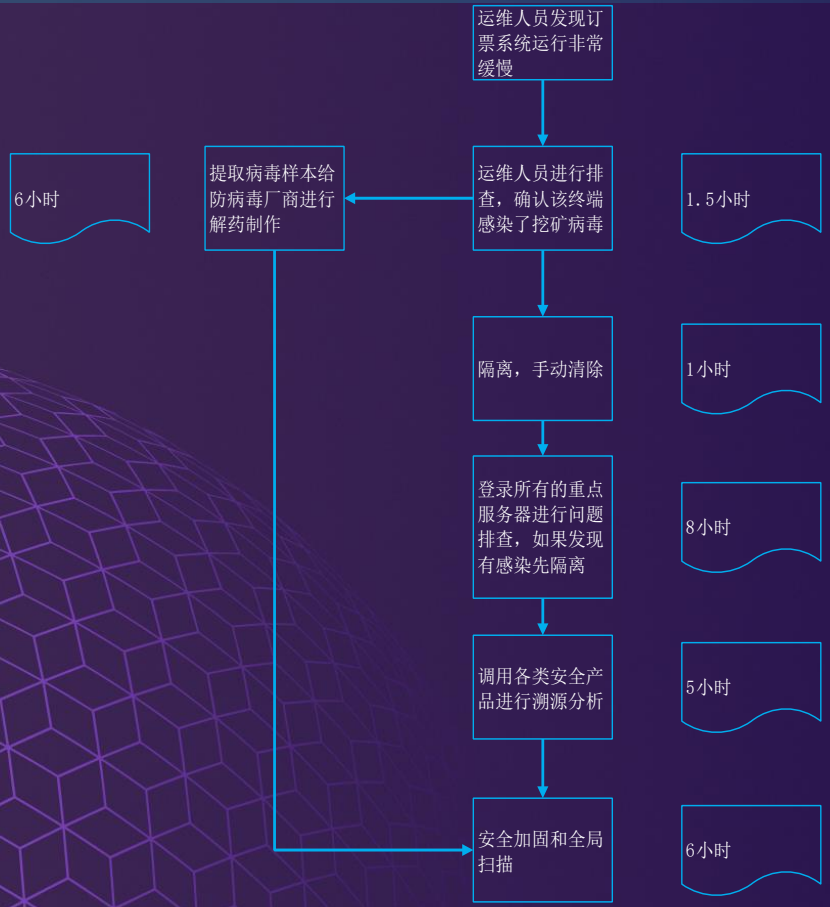
服务结束后，服务团队需告知客户，提供完整的黑客入侵报告。原始数据和取证数据留档保存。
给出后续整改方案，防止再次出现同类攻击。

专业的工具：亚信安全的防护体系

AsiaInfo | 亚信安全

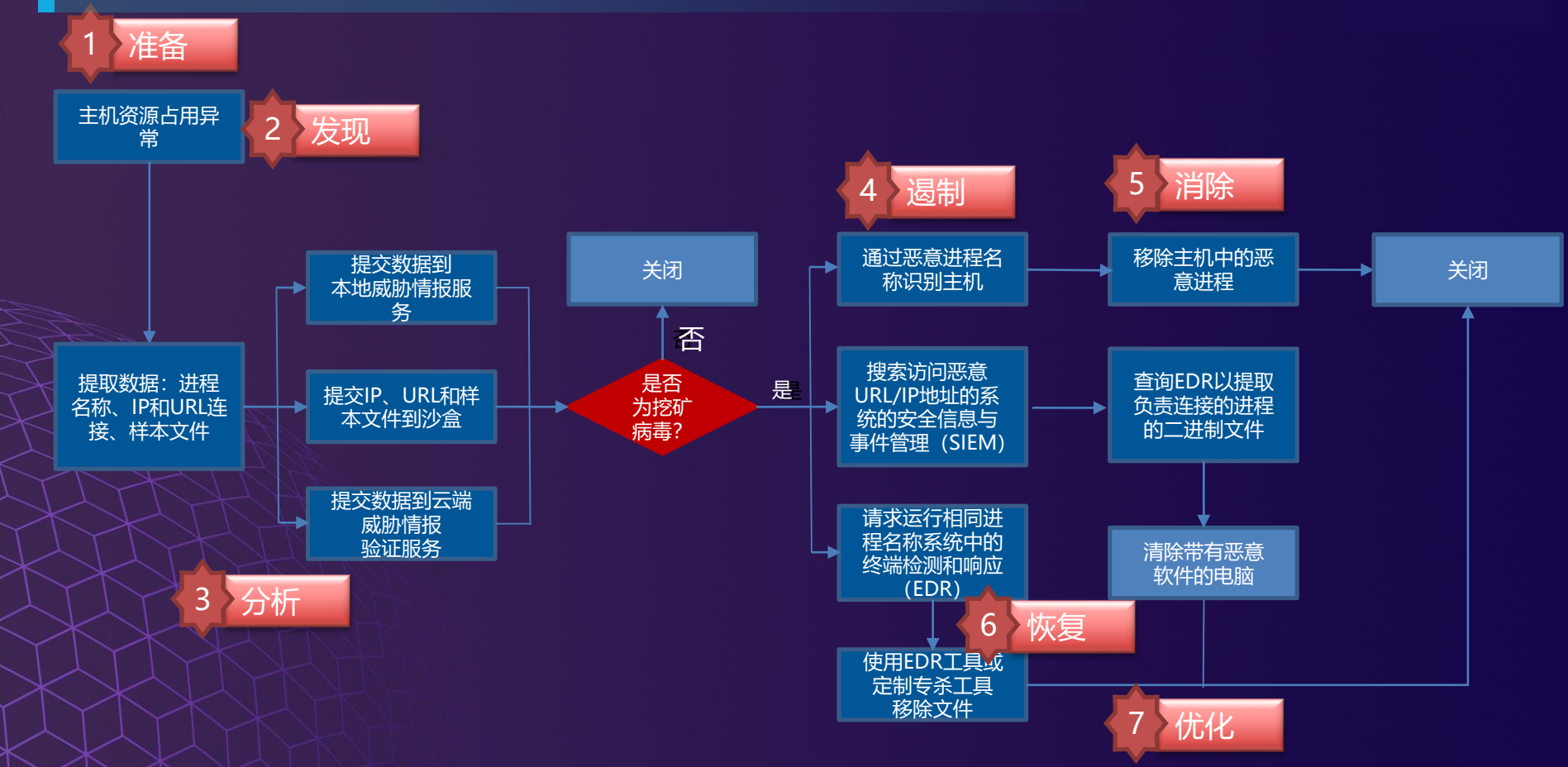
阶段	早期阶段（2010之前）	进阶阶段（2010开始）	高级阶段（2017开始）	智能阶段（TBD）
产品	云：DS 管：DE、DDEI 端：OSCE	TIP TDA、DDAN、 NTA（发现、存证） SIEM、SOC	CTDI、NDR （验伤、取证） SOAR	SOAR （TBD）
职能	基于已知威胁的检测、拦截、告警	基于未知、新型、可疑威胁的检测、分析、告警、存证	确认威胁的真实性、本质及意图、回溯攻击场景、评估影响和范围、自动下发并执行响应策略	预防机制 风险评估

举例：某次挖矿病毒处理过程



- 如何在资源被耗尽，影响业务运行之前提早发现挖矿病毒的植入和执行?
- 到底是什么种类的挖矿病毒，是否具备强烈的传播性以及破坏性?
- 是否还有某些服务器上仍然潜伏着此类挖矿病毒?
- 如何快速清除病毒并恢复所有服务器的运行?
- 如何最大限度的避免同样问题不会再发生?

举例：处理挖矿病毒安全事件的预案



精密编排的事件响应与联动防护体系

AsiaInfo | 亚信安全

侦测

威胁发现与拦截


Deep Security


TDA
Deep Edge
DDEI


OSCE


CTDI

分析

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)

响应

云


Deep Security

管


Deep Edge
DDEI

端


OSCE

威胁
线索

威胁
线索

确认的
威胁

确认的
威胁

影响的
范围

威胁
情报

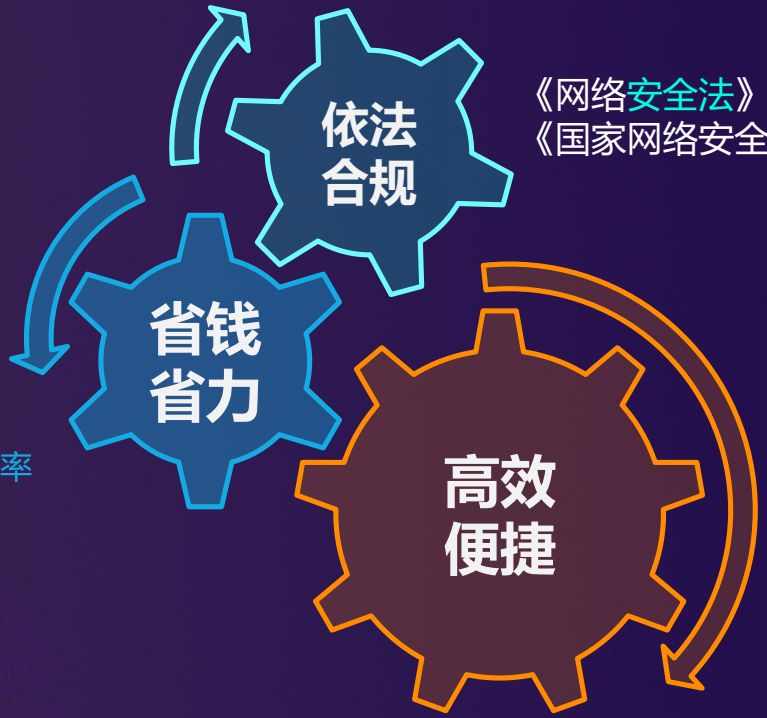
监控

UAP

威胁感知运维中心

精密编排运维体系的价值

AsiaInfo | 亚信安全



《网络安全法》
《国家网络安全事件应急预案》

“正规军” 的装备
摆脱对高精尖人才的依赖
提高应急响应安全事件的效率
超强的溯源分析功能
高效定位问题源头

“高清摄像头” 内核态证据全收录
高效的机器智能关联分析
通过培训提高用户安全运维人员的战斗力
厂家的安全服务专家团队提供后台支持

AsiaInfo | 亚信安全

Thank You