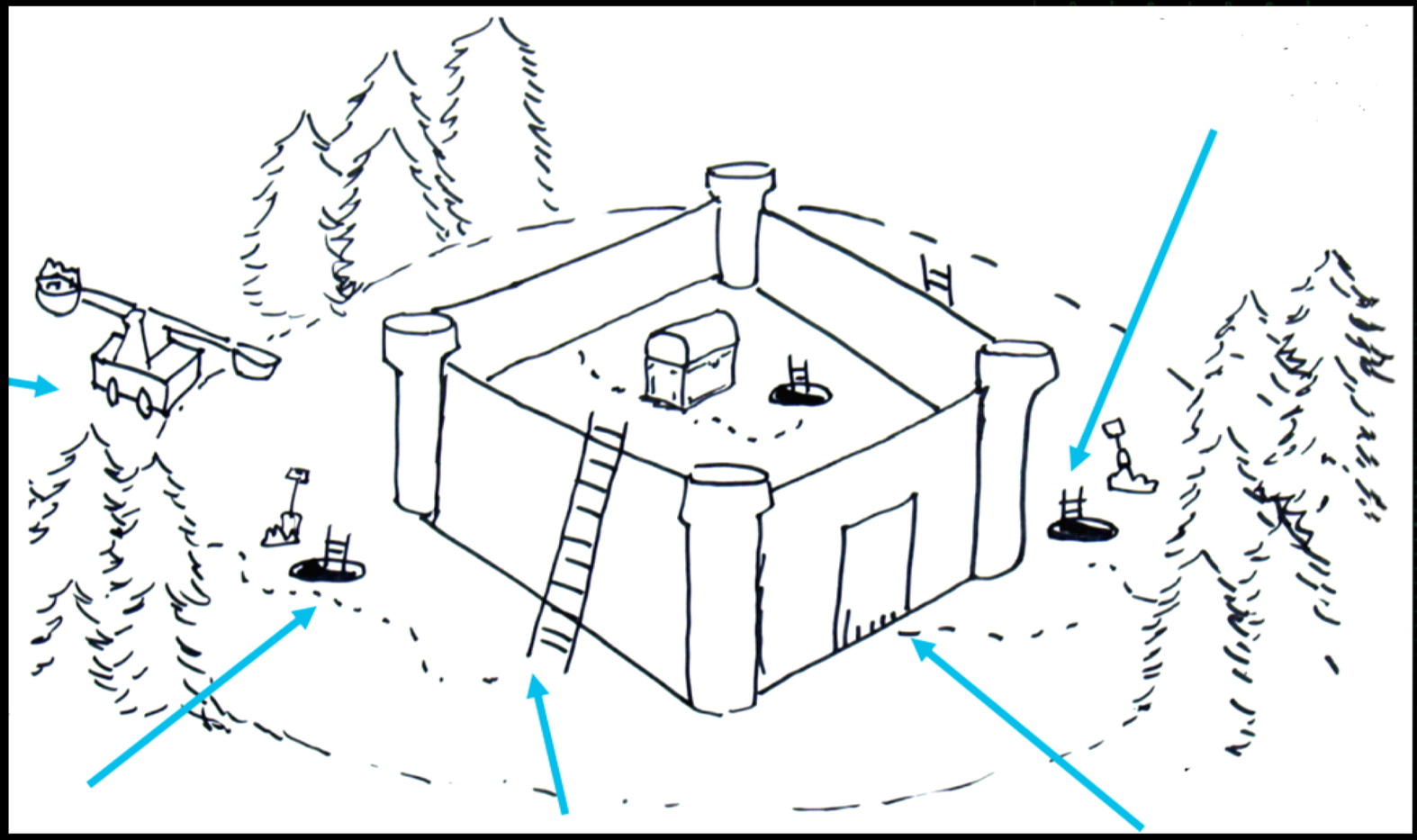
ISC 2019 7th
第七届互联网安全大会

从实战出发
提升网络安全的检测与响应能力

刘政平
亚信安全 副总裁

网络安全是攻与防的对抗



1、优先检测/缓解频繁使用的技术

2、进行对手模拟进攻

3、对当前防御进行差距分析

4、跟踪特定对手的技术集

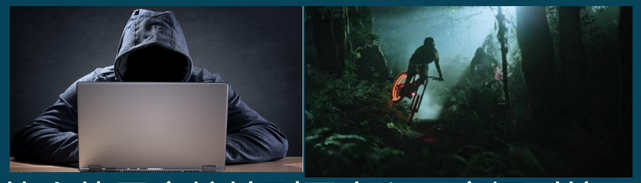
5、更好地评估新的安全技术

产业互联网时代的网络安全五大变化

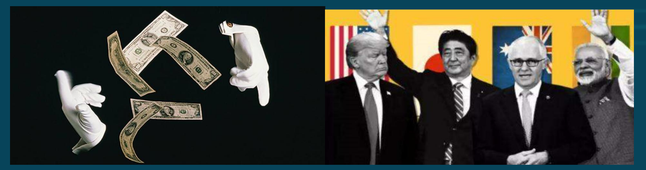
变化的战场

从网络和操作系统到“云大物移智+5G”

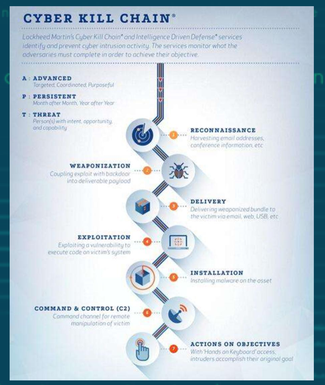
变化的对手



从个体黑客炫技到黑产和国家间对抗



变化的武器



勒索、挖矿、杀伤链

……

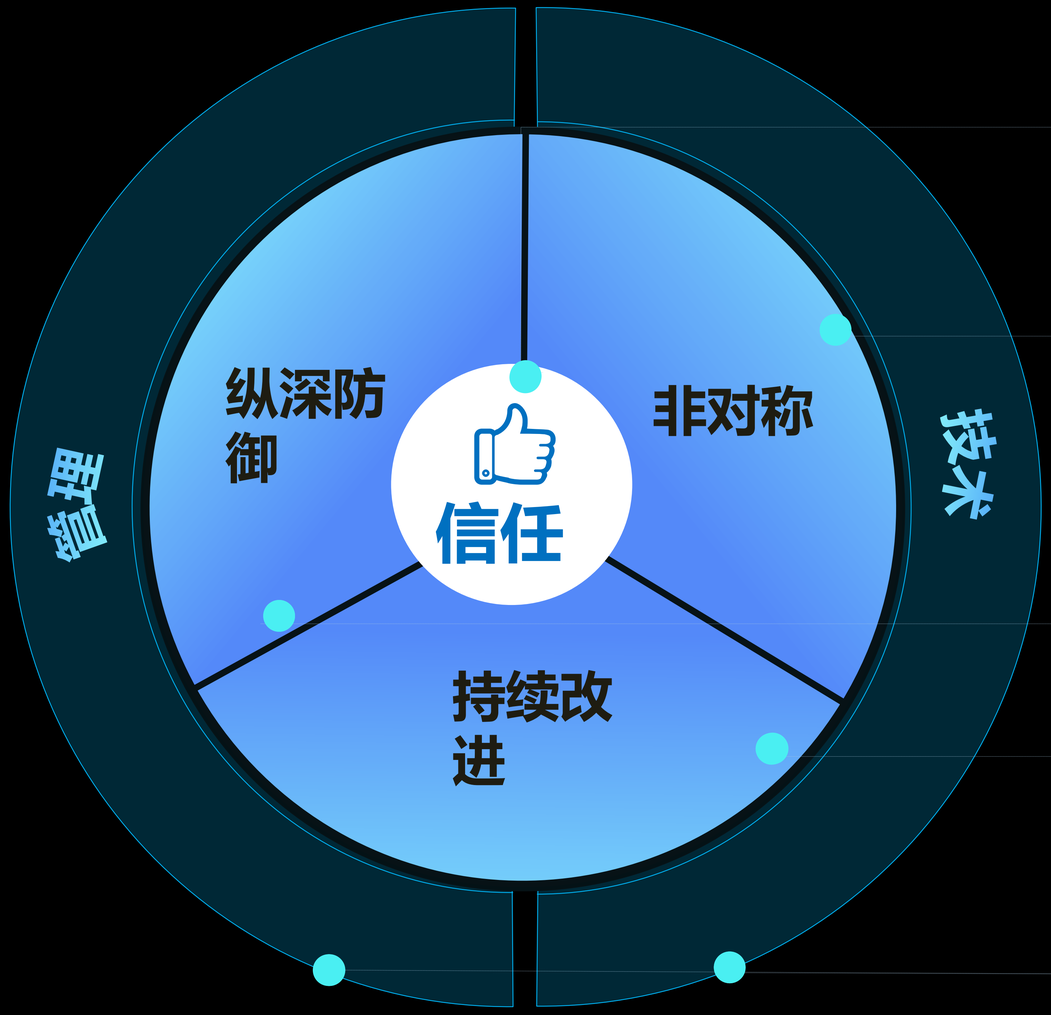
变化的目标

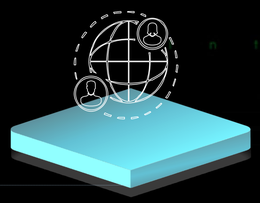
从网络和操作系统到窃取数据和破坏应用

变化的监管力度

国家战略、法律法规等级保护、护网行动

网络安全的本质及特点





以身份为基础

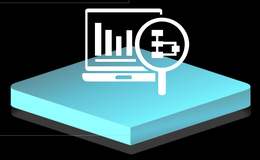
构建网络空间信任体系

以攻防为视角

提升全方位主动防御能力

以联动为策略

提升网络安全事件智能响应能力



以运维为关键

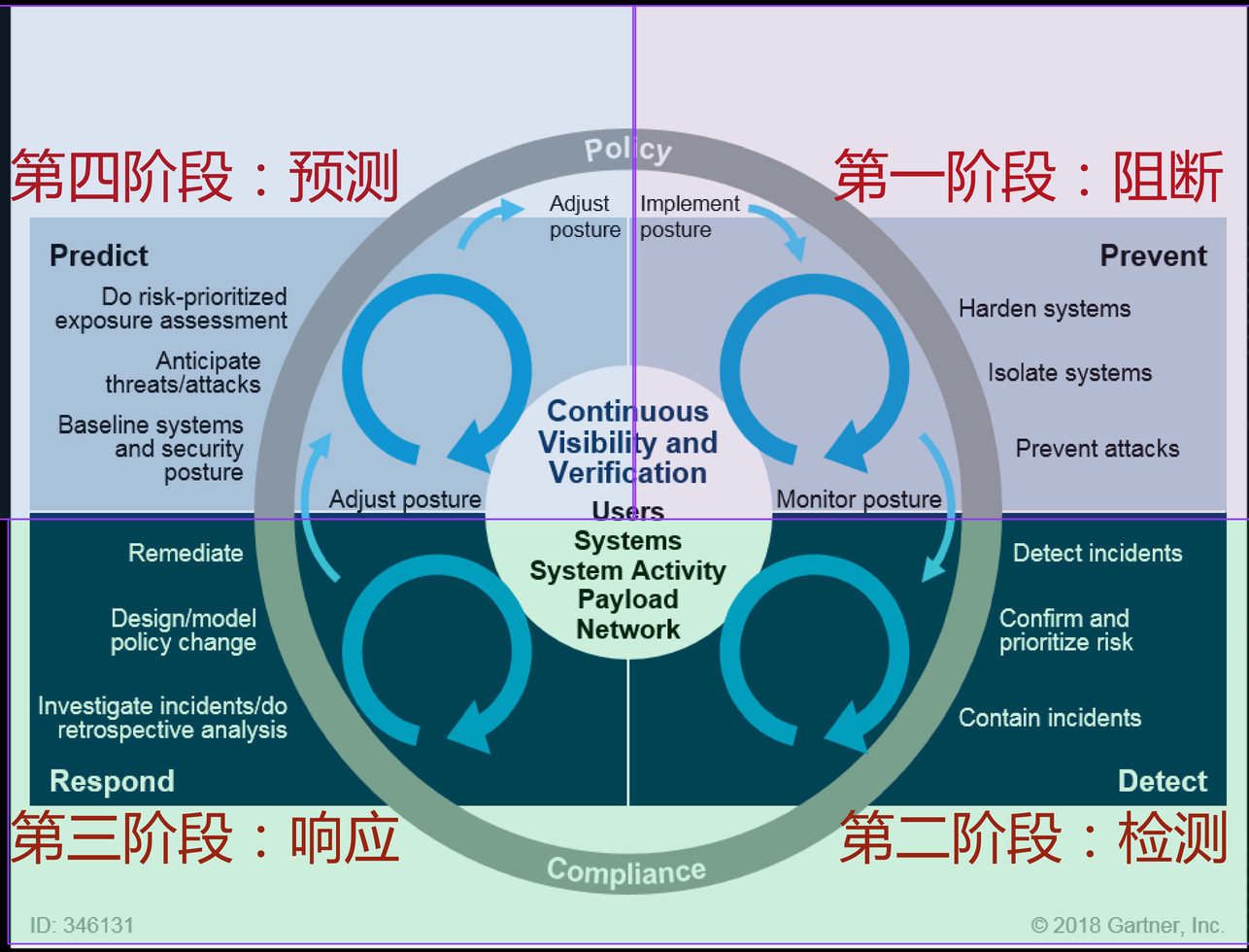
加强统一集中管控平台建设

从实战出发

建设自适应安全体系

网络安全技术阶段演进--自适应安全架构

- 未来安全由威胁情报驱动
- 代表技术包括**MDR**、TI、Deception和UEBA



- 传统安全基于黑白名单对“已知威胁”进行阻断
- 检测率和响应速度无法有效应对新型“高级威胁”
- 代表技术包括传统EPP、防火墙和入侵检测系统

- 新型安全基于“行为特征”有效检测“高级威胁”
- 强调快速响应和恢复补救
- 代表技术包括**EDR**、**NDR**、APT监控设备和沙箱

政策法规的要求

- 《**网络安全法**》中提出了**应急预案**、**应急演练**和**应急处置**的要求
- 《**国家网络安全事件应急预案**》中给出了**应急响应**的具体指导意见

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

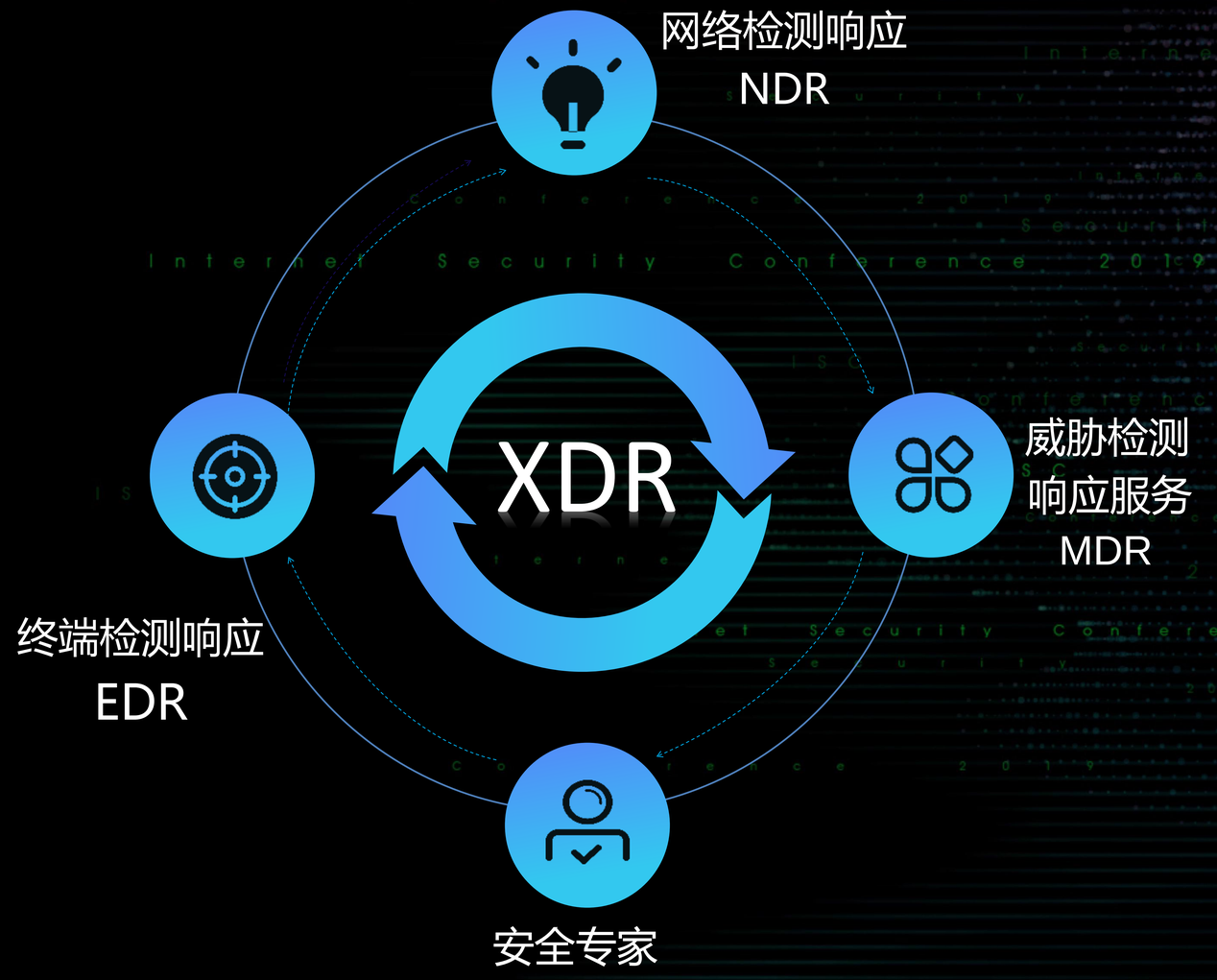
基于XDR的威胁检测与应急响应体系

XDR =

EDR + NDR + MDR

&

应急响应



精密编排XDR解决方案提升事件响应能力

XDR

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：超洞察威胁情报平台TIP

China unicom中国联通

中国电信 CHINA TELECOM

中国移动 China Mobile

公共通讯和信息服务　能源　交通　水利　金融　公共服务　电子政务

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

安全响应专家服务：精密编排自动化

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。

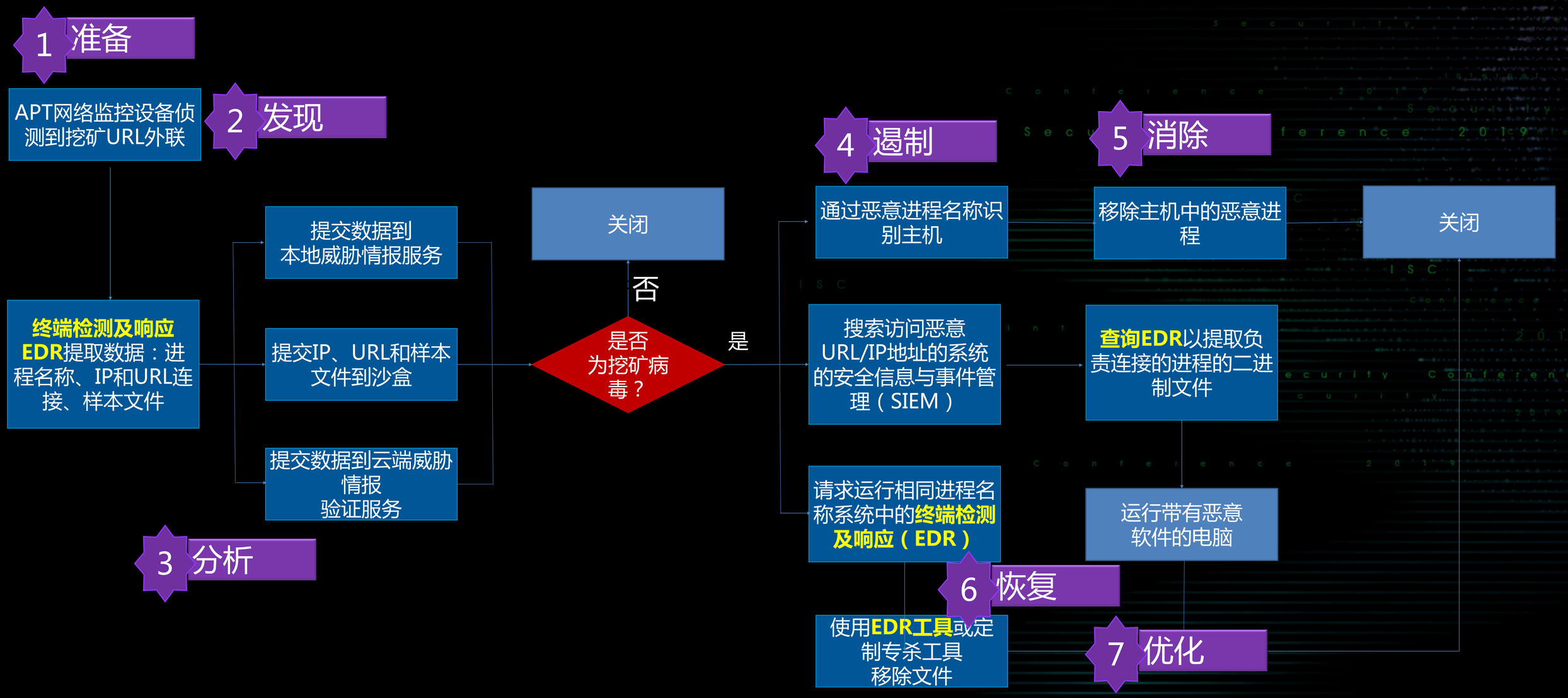
服务执行

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。

挖矿病毒安全事件的预案



精密编排的挖矿病毒应急响应

云端威胁情报平台

互联网

DMZ区

EDR 客户端 Web 服务器

EDR 客户端 Email 服务器

EDR 客户端 应用 服务器

进程名称

IP&URL

样本文件

EDR 服务器端

APT 监控设备

核心交换机

本地威胁情报平台

1 准备

2 发现

3 分析

大数据存储服务器集群

管理区

沙箱系统

生产区

EDR 客户端 应用 服务器

EDR 客户端

EDR 服务器端

APT 监控设备

办公区

EDR 客户端 文件 服务器

EDR 服务器端

APT 监控设备

4 遏制

5 消除

6 恢复

7 优化

亚信安全XDR 精密联动方案

产生可疑威胁日志

检测

阻断

高级威胁发现

Deep Security

TDA
Deep Edge
DDEI

OSCE

CTDI

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)

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

响应

XDR

SOAR

精密编排的快速恢复补救

亚信安全重保实战的经验分享

预案

- 标准预案（7个步骤）
- 场景化

流程

- 结合用户环境定制处置流程
- 跨部门的协作流程

装备

- 多维度的阻断和发现设备
- 精密编排的产品联动XDR
- 自动化处置、响应设备

专家

- 提前发现漏洞
- 熟悉黑客的攻击思路和手法
- 利用线索分析和响应

ISC 2019 7th
第七届互联网安全大会

Thank You

2019.7.15