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

“三高” 网络动态综合安全防御体系

安天 方案规划设计咨询部

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

提纲

1. 什么是“三高”网络？
2. 能力导向建设“三高” 网络动态综合防御体系
3. 夯实“三高”网络基础结构安全叠加纵深防御
4. 威胁情报驱动的战术型态势感知与积极防御
5. 实战化安全运行

01 什么是“三高”网络

- 定义
- 网空威胁
- 工作要求
- 几点思考

“三高”网络定义

“三高” 是安天与安全领域专家在技术探讨中定义的一种网络场景。特指一个网络系统中承载着**高信息价值资产**，该网络被规定为**高安全防护等级**，同时该网络受到**常态化高强度的网络威胁攻击**，具有这三种特征的网络统称为“三高”网络。

高信息价值　　**高防护等级**　　**高威胁对抗**

“三高”网络信息系统特征分析

高信息价值

- 具有极高信息价值，承载业务与国家安全紧密相关，不容有失。

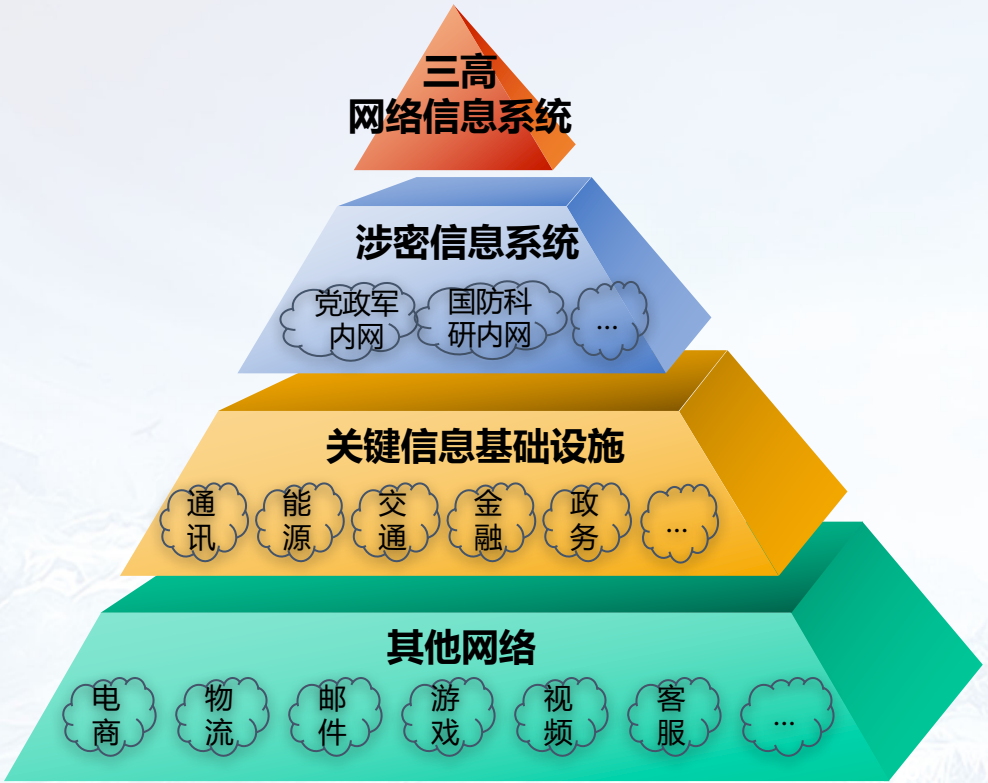
高防护等级

- 通常被规定较高安全防护等级，按照国家相关法律法规要求实施防护。

高威胁对抗

- 面临超高能力对手常态化、高强度、持续性的威胁攻击。

哪些是“三高”网络信息系统



- “三高” 网络信息系统是**关键信息基础设施、重要信息系统中具有“高信息价值、高防护等级、高威胁对抗”特征**的网络信息系统。

“三高”网络信息系统面临超高能力对手方持续性网空威胁

当前，国际形势日趋复杂，围绕关键信息基础设施的攻击、窃密、植入与干扰，已成为国际斗争的焦点。网络安全已上升成为关乎国家安全和国家发展的重大战略问题。“三高” 网络信息系统因其**具有极高的信息价值**，承载业务**与国家安全紧密相关，不容有失**。

因此，“三高”网络信息系统的安全防护工作，应充分**考虑“三高”网络信息系统的国家安全属性与攻防对抗特性**，根据业务特点确定主要面对的威胁来源，搞清楚到底“敌人是谁”，避免防御不足，并且要**充分考虑“三高”网络信息系统的平战结合特点**。

依据威胁对抗分级框架，“三高”网络信息系统面临威胁等级6级，也就是**面临超高能力国家/地区行为体的持续性网空威胁**。

威胁等级	防御目标	特点	攻击技术和工具
6级	5级目标+超高能力国家/地区行为体	• 国家/地区行为体, • 受国家/地区利益驱动， • 网络间谍与网络战一体化，寻求通过网络战获得政治、经济、军事优势 •	• 掌握对自身国家/地区级网络基础设施、外部国家/地区级网络基础设施、互联网级网络基础设施、以及信息科技供应链的部分控制能力 • 专有攻击技术、工具与平台 • 跨维度高度集成的攻击利用手段 • 漏洞挖掘与利用技术开发能力 • 制造漏洞能力 • 掌握大量0day漏洞
5级	4级目标+高级能力国家/地区行为体	• 国家/地区行为体， • 受国家/地区利益驱动, • 网络间谍与网络战一体化，寻求通过网络战获得政治、经济、军事优势	• 部分掌握自身国家/地区级网络基础设施和外部国家/地区级网络基础设施的控制 • 专有攻击技术、工具与平台 • 跨维度高度集成的攻击利用手段 • 漏洞挖掘与利用技术开发能力 • 掌握较多0day漏洞
4级	3级目标+一般能力国家/地区行为体	• 国家/地区行为体, • 受国家/地区利益驱动 • 网络间谍与网络战一体化， • 寻求通过网络战获得政治、经济、军事优势	• 部分掌握自身国家/地区级网络基础设施的控制 • 专有攻击技术、工具与平台 • 具有漏洞挖掘与利用技术开发能力 • 掌握少量0day漏洞
3级	1级目标+网络恐怖组织	• 非国家行为体，受意识形态驱动 • 寻求破坏或影响的最大化	• 专有攻击技术、工具与平台 • 漏洞挖掘与利用技术开发能力
2级	1级目标+网络犯罪团伙或黑客组织	• 非国家行为体，受商业利益驱动，也可能受意识形态驱动，敢于造成较大破坏或影响	• 专有攻击技术、工具与平台 • 漏洞挖掘与利用技术开发能力
1级	0级目标+黑产组织	• 非国家行为体，受商业利益驱动	• 公开攻击技术、工具与平台 • 部分专有攻击技术、工具与平台
0级	业余黑客		• 公开攻击技术与工具

威胁对抗分级框架

超级大国工程系统支撑下的体系化、全方位、全平台覆盖的进攻能力（1）

传统信号情报优势

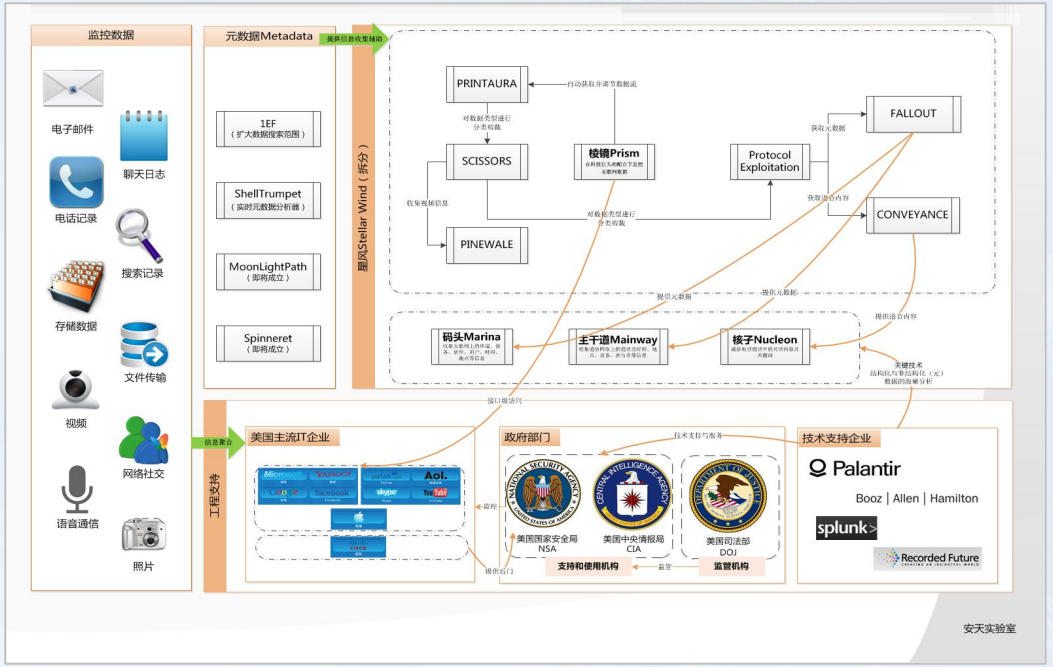
“梯队”是“五眼”情报联盟上世纪60年代开始建设的信号情报搜集网络。在全球范围内通过无线信号收集和海底光缆窃听等方式收集情报。

“五眼情报联盟

美国
英国
加拿大
澳大利亚
新西兰

“梯队”项目全球站点分布

“星风计划”启动于2004年，是美国政府秘密开展的大规模搜集情报监控信息的计划。由于法律程序等敏感问题星风计划被拆分为“棱镜”(PRISM)、“主干道”(MAINWAY)、“码头”(MARINA)以及“核子”(NUCLEON)四大项目由NSA掌管。

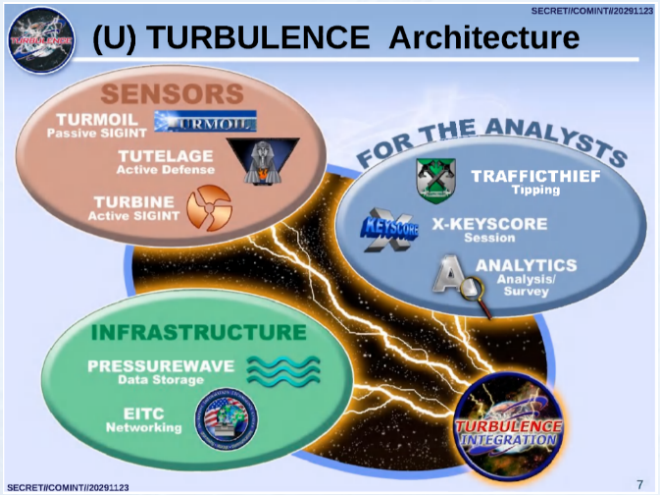


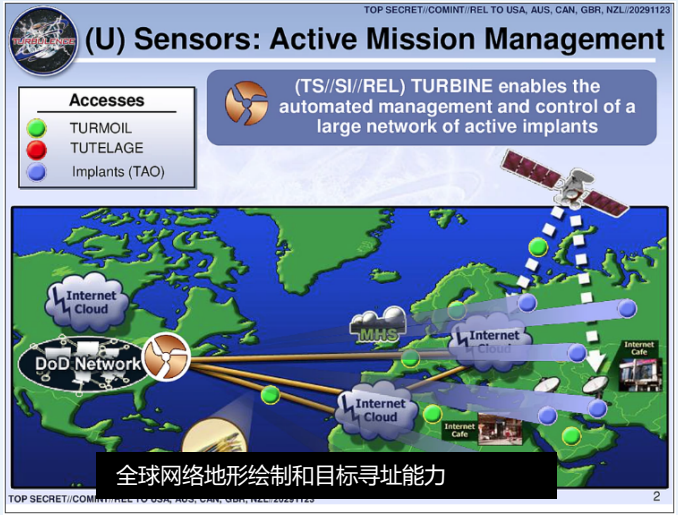
“星风”计划示意图

超级大国工程系统支撑下的体系化、全方位、全平台覆盖的进攻能力（2）

完备的进攻性能力支撑体系

- “湍流”是美国国家安全局（NSA）是NSA在21世纪信号情报（SIGINT）任务的核心作业框架，具有进攻性的网络战能力；
- 其综合考虑了感知获取、作业层面和后端分析，构成了对可精确打点、具有较好隐蔽性和反溯源性的支撑。



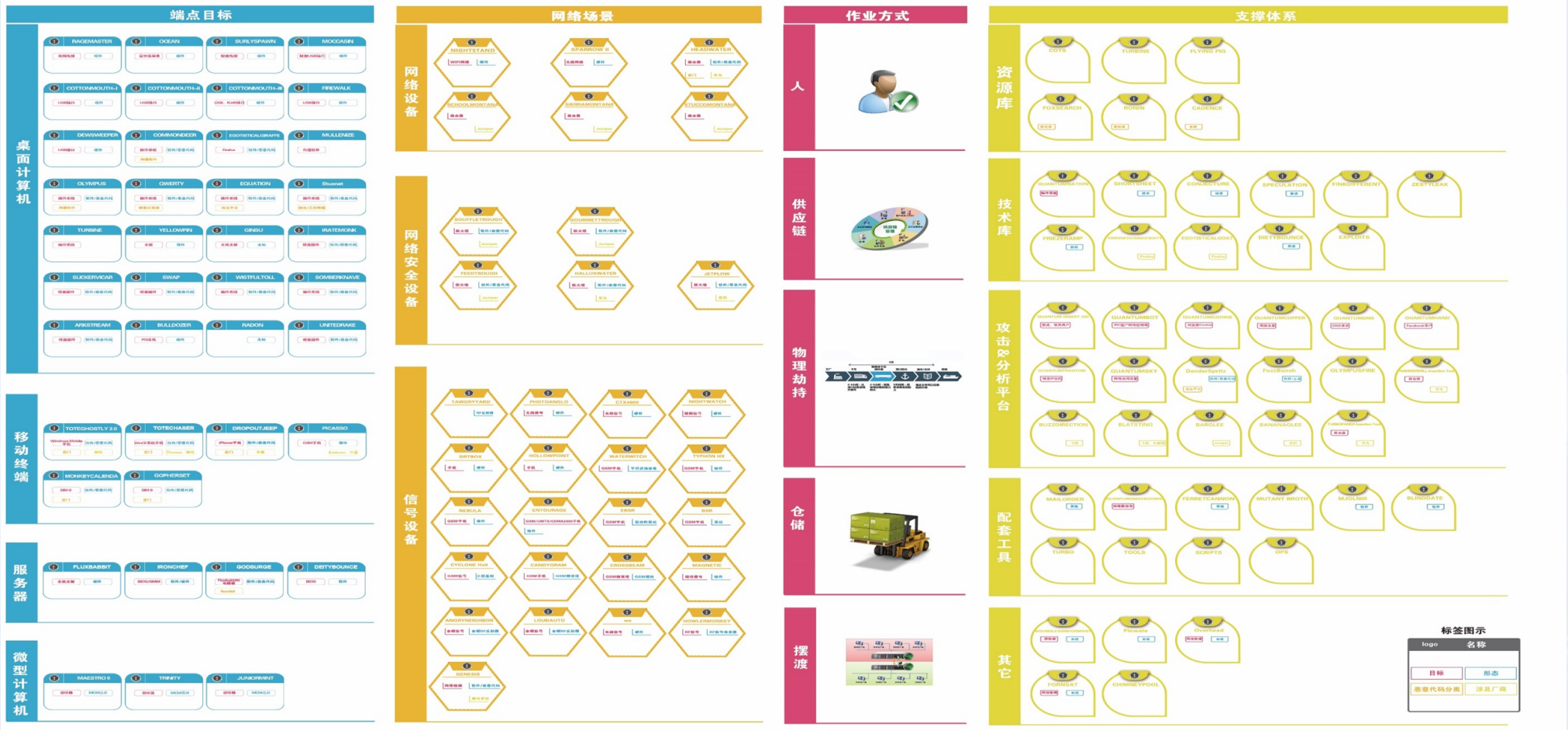


- 通过全球部署的被动收集系统Turmoil进行全球信号情报采集；
- 利用主动收集系统Turbine对互联网流量进行过滤，筛选出感兴趣的流量信息，并触发指挥控制模块；
- 指挥控制模块会将相关信息发送给TAO的节点，由TAO执行网络攻击。

- 通过情报分析定位目标，使用“量子”对目标进行网络攻击；
- 其中“量子之手”（QUANTUMHAND）主要针对的Facebook等可以识别身份的社交网站用户，当目标访问社交网站时，TURBINE系统可以先于真实的Facebook服务器给出反馈，发送诱骗数据包，将目标重定向至TAO的服务器，之后进行恶意代码植入等攻击。

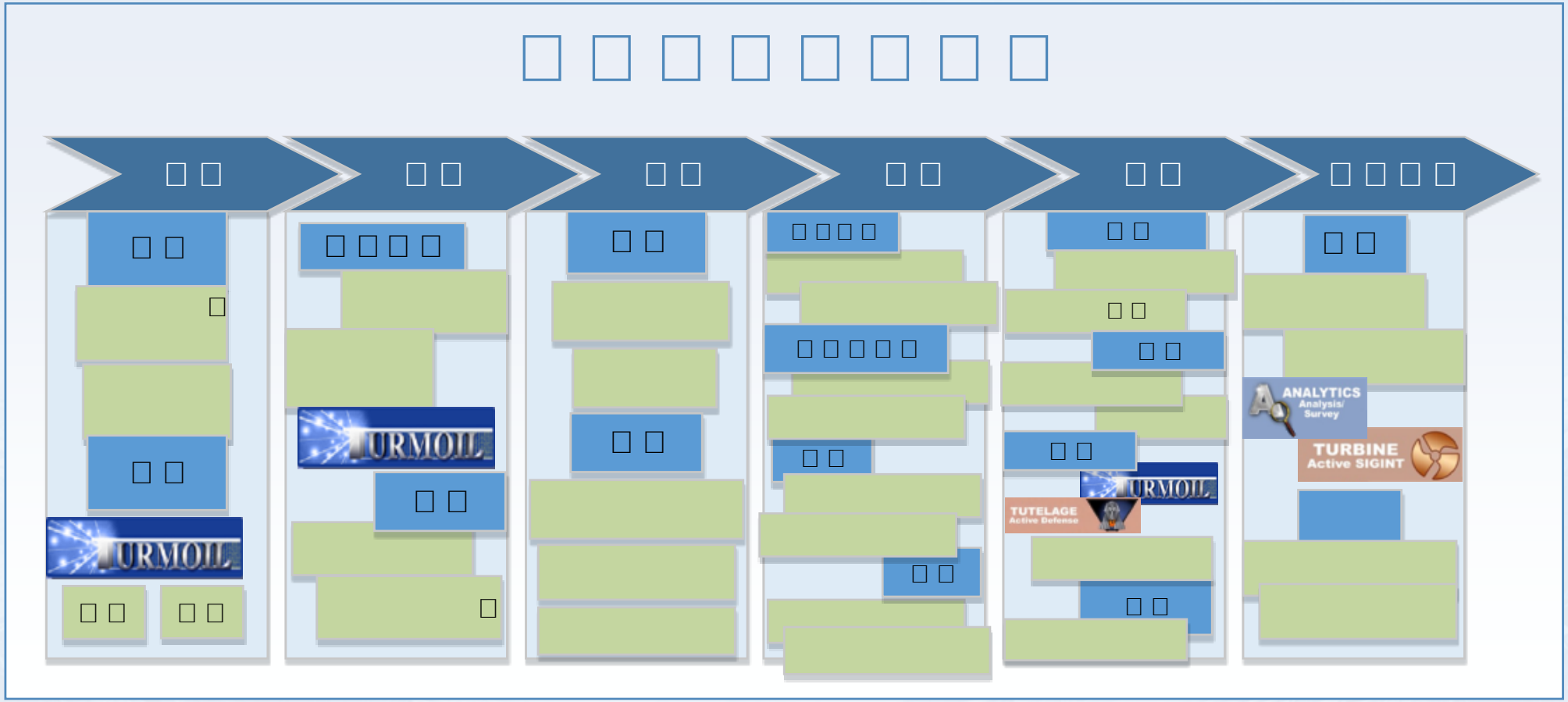
超级大国工程系统支撑下的体系化、全方位、全平台覆盖的进攻能力（3）

全场景网络攻击装备体系



超级大国工程系统支撑下的体系化、全方位、全平台覆盖的进攻能力（4）

成熟的网空威胁框架



从习近平总书记“4·19”讲话到“4·20”讲话——工作要求在不断提升

419

树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，**全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。**

217

要筑牢网络安全防线，提高网络安全保障水平，强化关键信息基础设施防护，加大核心技术研发力度和市场化引导，加强网络安全预警监测，确保大数据安全，**实现全天候全方位感知和有效防护。**

420

要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息系统统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，**做到关口前移，防患于未然。**

建立“三高”网络信息系统真实极限化的敌情想定

国家/政经集团行为体

民间复合行为体

传统民间行为体

外部信息环境

基础电磁（信号）环境处于对手广泛监听

关键链路设备被入侵和控制

互联网服务者、云和其他公共互联网基础设施供应商存在不可靠性

社会关系

所有关键系统的用户多数都是互联网用户。

所有社会关系可以从互联网定位摸底。

全民数据已经泄露。

敌已在内、敌将在内

内网已（将）被渗透，人员已（将）被策反，这是最基础和核心的想定

供应链

上游研发、生产、场景均可被控制和入侵。

物流仓储不能保证可靠。

运维、升级、更换等均不能保证可靠

对外信息交换

广泛的信息交换必须发生

威胁针对性的跟随信息交换

（平时）
持续性对抗
隐蔽性对抗

（战时）
高烈度对抗

（平战）
无底线对抗
高成本对抗

对手：层次化的攻击行为能力
具有其自身战略/利益意图的作业方向

敌情：真实极限化/的敌情想定

网空斗争的特点

“三高”网络信息系统安全防护工作模式需要演进

满足一系列信息安全标准与法律法规的相关防护要求，“**被动合规**”工作模式	**工作模式**	应立足于更加积极的合规驱动工作模式，并针对“三高”网络信息系统等重要领域实现**主动有效的全方位体系化防护**工作模式
信息安全**风险管理模式**，“突出重点、平衡风险、适度安全”	**防御理念**	根据网络与信息系统的国家安全、社会安全和业务安全属性，客观判断必须能够**有效对抗**哪些层级的网络空间威胁，并据此驱动网络空间安全防御需求
尝试罗列各种可能的网络威胁，并设计零散防御措施进行被动应对的传统式**“威胁导向建设模式”**	**建设模式**	全面建设必要的网络安全防御能力，并将其有机结合形成网络空间防御体系的“**能力导向建设模式**”

引自：黄晟《网络空间安全防御与态势感知》译者序

02 能力导向建设“三高” 网络动态综合防御体系

- 叠加演进模型
- 动态综合防御体系框架
- 覆盖面、结合面

铁流鏖戰
第六届安天网络安全冬训营

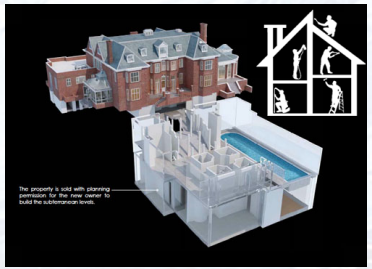
叠加演进的层次化网络安全能力模型

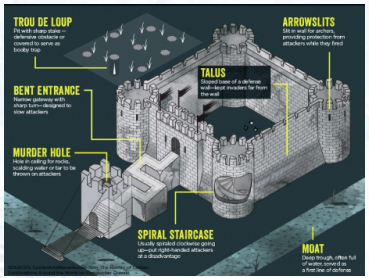
叠加演进

基础结构安全 Architecture	纵深防御 Defense in Depth	态势感知与积极防御 SA & Active Defense	威胁情报 Intelligence	反制 Counter
在网络与系统的规划、设计、建设和维护的过程中充分考虑安全防护	在无人员持续介入的情况下，融合在系统架构之上可持续提供威胁防御或威胁洞察力的系统	依托态势感知平台，由分析人员监控、分析、响应和猎杀网络内部威胁并对防御体系进行完善的过程	收集数据、将数据利用转换为信息，并将信息生产加工为威胁情报，以填补威胁知识缺口并驱动积极防	以采取法律反制措施等形式针对进攻者采取的自我防卫行动

深度结合、全面覆盖

掌握敌情、协同响应





叠加演进是安天从能力型安全厂商的公共模型滑动标尺演绎发展的一套模型，滑动标尺模型由SANS提出，由安天翻译引入国内，并与国内能力型厂商约定为公共安全模型。参见：《网络安全滑动标尺模型 —从架构安全到超越威胁情报的叠加演进 》中文译本，安天公益翻译组翻译。

基于叠加演进模型构建动态综合网络安全防御体系

总体思路

以基础结构安全和纵深防御为主体的综合防御体系为基础，叠加动态的积极防御以应对高级复杂威胁，同时结合威胁情报缩短防御响应周期并提高针对性，构建动态综合网络安全防御体系。

- **综合发展**：从前到后逐步加强、逐步演化，且前面的层次要为后面的层次提供基础支撑条件。
- **深度结合**：将安全能力落实到信息系统的各个实现层组件，逐层展开防御，为及时发现和响应赢得时间。
- **全面覆盖**：将安全能力最大化覆盖信息系统的各个组成实体，避免因局部能力短板导致整体防御失效。
- **动态协同**：依托持续监测和自动响应能力，结合大数据分析、威胁情报、专家研判，实现积极防御。

动态综合网络安全防御体系框架

□□□□□□

□□□□

□□□□□

□□□□□□

□□□□□□

□□□□□□

□□□□□□

□□□□

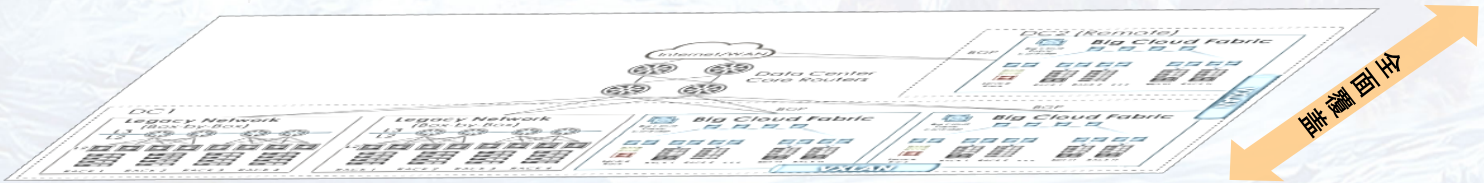
□□□□

□□□□

□□□□□□□□

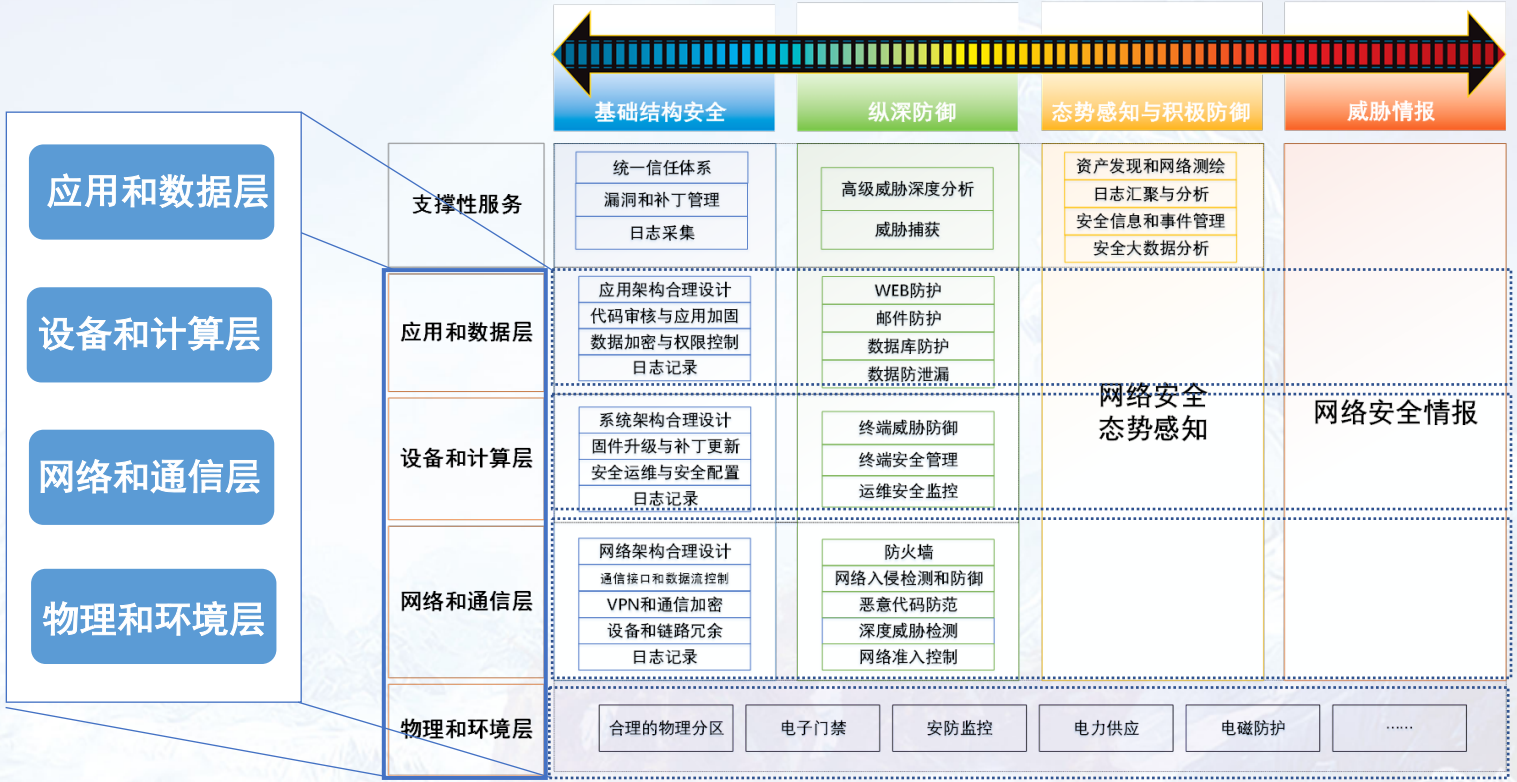
基础结构安全	纵深防御	态势感知与积极防御	威胁情报
漏洞与补丁管理 配置管理 资产管理	安全设备管理 深度威胁分析设备 漏洞扫描设备	日志汇聚与分析 安全数据存储与处理	网络安全 威胁情报
漏洞和补丁管理 应用安全配置与更新 数据加密 日志记录等	WEB应用防护 数据库审计系统 安全认证网关	网络安全 态势感知	
设备固件升级 漏洞和补丁管理 安全配置 日志记录等	态势感知终端探针 统一终端安全管理 应急处置工具		
网络合理架构设计 传输加密 设备固件升级 安全配置 通信接口和数据流控制 日志记录	单向导入系统 深度威胁检测探针 IDS/IPS 网络准入控制 防火墙		

合理的物理分区 | 电子门禁 | 安防监控 | 电力供应 | 电磁防护 | ……



动态综合网络安全防御体系框架——结合面

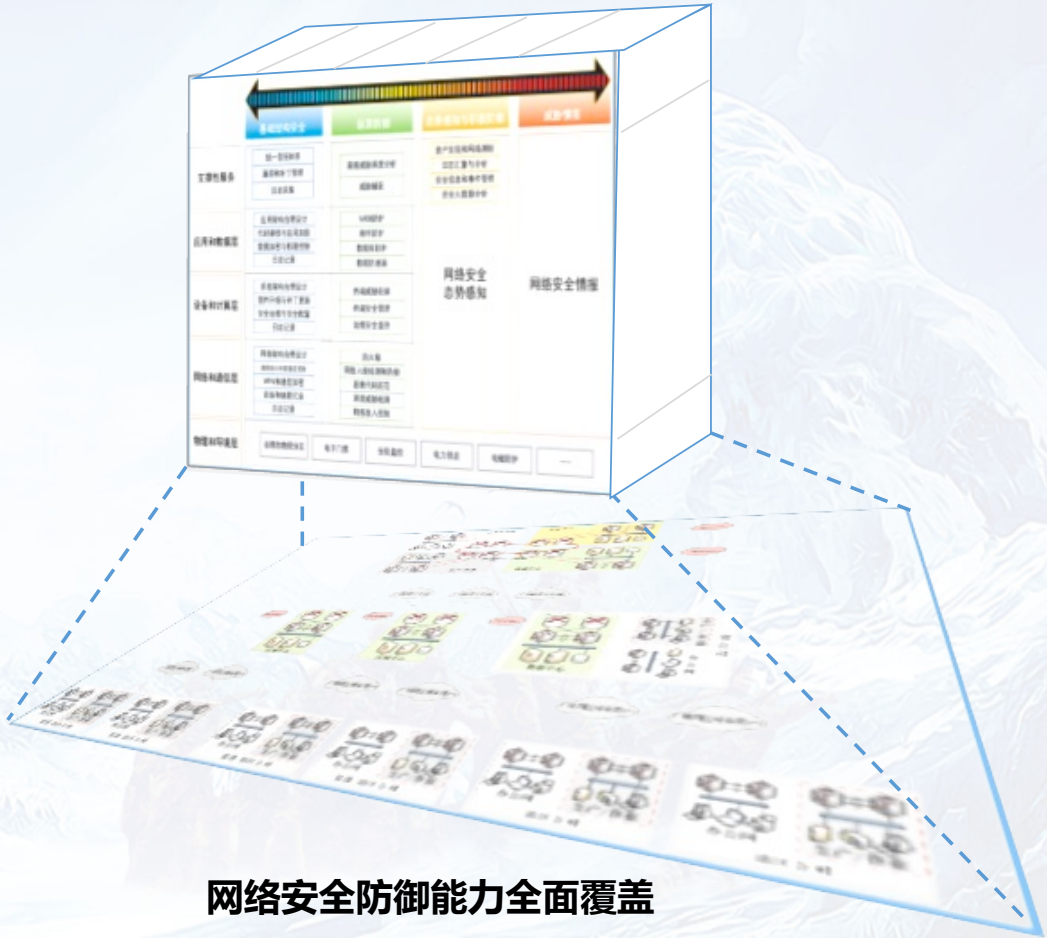
- 在“三高”网络信息系统的规划设计以及后续项目建设实施、运行维护的过程中，以“敌情想定”为前提、“面向失效的设计”为基本原则，在构成“三高” 网络信息系统的物理和环境、网络和通信、设备和计算、应用和数据等各个层面实现与网络安全防御能力的深度结合。



网络安全防御能力深度结合

动态综合网络安全防御体系框架——覆盖面

- 要将网络安全防御能力部署到信息基础设施和信息系统的“每一个角落”，力求**全面覆盖构成“三高”网络信息系统的各个组成实体**，包括桌面终端、服务器系统、通信链路、网络设备、安全设备、以及供应链、人员等，**避免由于存在局部的安全盲区或者安全短板**，而导致整个网络安全防御体系的失效。



网络安全防御能力全面覆盖

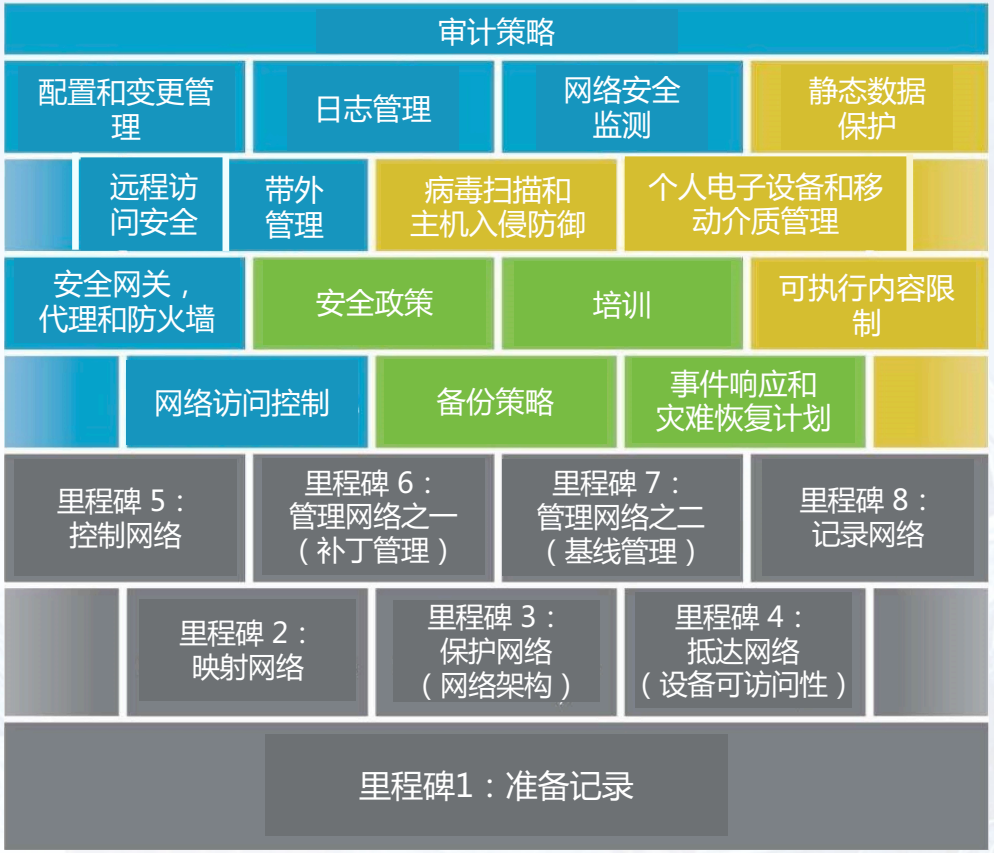
03 夯实“三高”网络基础结构安全叠加纵深防御措施

- 强化网络可管理性
- 全面覆盖的资产安全运维管理
- 合理网络结构上叠加纵深防御
- 全生命周期的漏洞与补丁管理
- 实施配置加固形成基准

强化“三高”网络的可管理性

“三高”网络必须具备可管理性，可管理网络才具有可防御性。

- 可管理网络特点
  - 完整准确记录网络及其中的设备、协议、配置等信息并保持持续更新
  - 具有健全的网络安全架构、访问控制规程、设备管理流程及用户权限约束
  - 具备完善的补丁管理流程和基线状态管理措施等
- 可管理网络的效果
  - 更有效的网络管理
  - 防范恶意软件
  - 保障运行
  - 防止数据丢失
  - 阻止非授权访问
  - 确保可用性等



规划可管理网络的路线图

注：参考美高等级网络的防护方法《可管理的网络计划指南V4. 0》

强化“三高”网络的可管理性——路线图

叠加纵深

纵深防御

基于“面向失效的设计”原则，综合利用多样化的防御手段，在多样化的纵深维度上布置层层防线。

里程碑1	里程碑 2	里程碑 3	里程碑 4	里程碑 5	里程碑 6	里程碑 7	里程碑8
准备记录	**测绘网络**	**网络架构**	**网络可达**	**控制网络**	**补丁管理**	**基准管理**	**记录网络**

夯实基础

资产和拓扑测绘

通过资产识别、拓扑绘制掌握网络结构和业务连通关系的全局信息。

分区分域

对网络进行合理、细粒度的区域划分以及通信接口和数据流定义。

漏洞和补丁管理

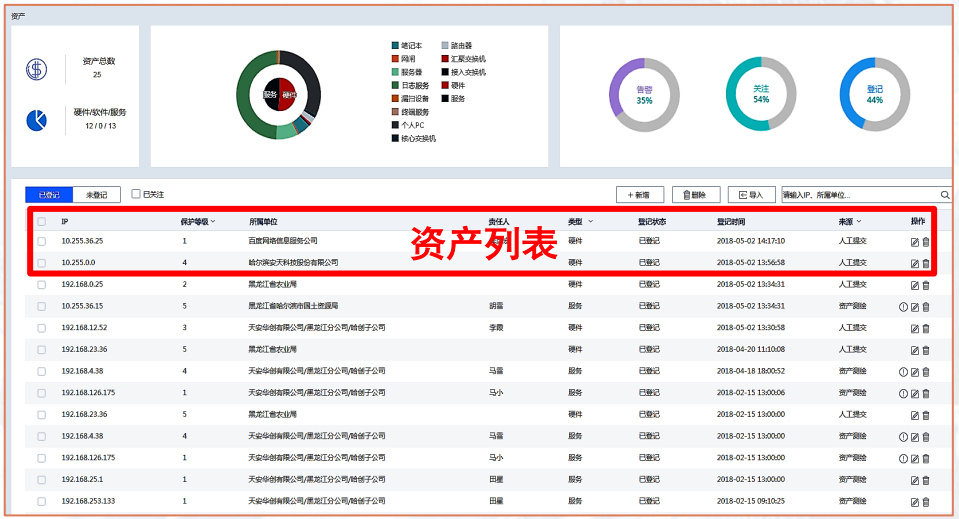
同步漏洞信息、感知漏洞存在，实施漏洞修复和补丁管理，防御和缓解漏洞利用。

配置与加固

通过合理配置和全面的安全加固，可以增加攻击者入侵成本、提高对威胁的防御能力。

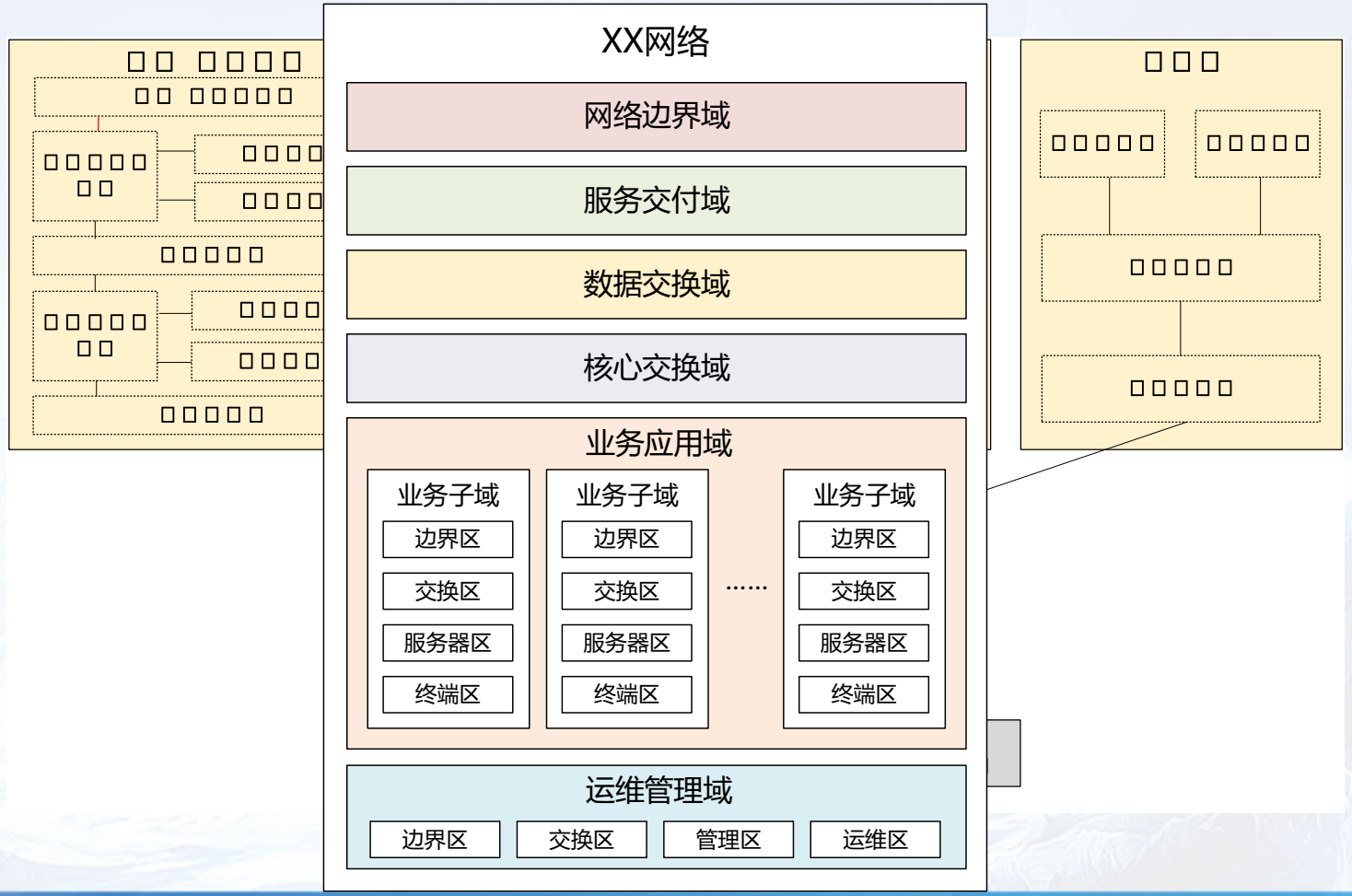
全面覆盖的资产安全运维管理

- 全面记录“三高”网络资产信息，并作为态势感知平台的基础数据源之一，同时可通过态势感知平台提供的主动探测、被动检测、端点上报、手工填报等方式进行网络空间资产测绘；
- 记录的资产信息包括：技术信息（机器名、MAC、IP、通联关系、设备类型、制造商、型号、序列号、硬件规格、操作系统或固件、软件版本、软件许可、安全证书等）以及基本管理信息（物理位置、所属部门、责任人等）；
- 资产安全运维管理应覆盖资产全生命周期：从规划设计阶段，建设阶段到运行阶段全面覆盖。



网络结构调整和增强

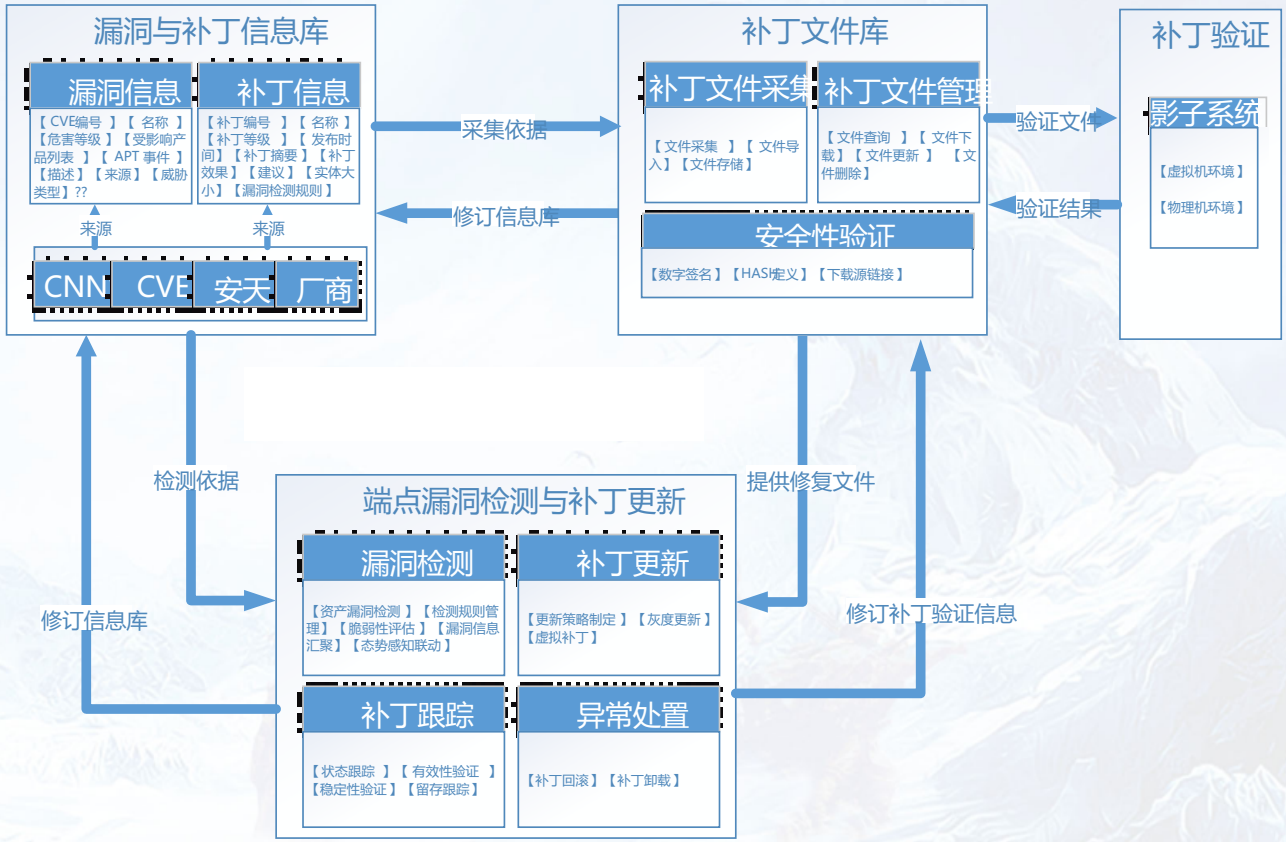
- **功能内聚**，将维持功能运行的组件纳入**最小化的安全区域**；
- 根据不同系统的重要程度、资产类型、保护需求等**细化划分安全区域**，进行**逻辑隔离和数据流控制**；
- 不同业务**应用系统之间逻辑隔离**；
- 设置**独立的运维管理区域**，避免管理与业务通信相互影响；
- **日志和管理数据也属于高价值信息**，存放于运维管理区域，需要**加强访问控制**，防止泄露。



全生命周期漏洞与补丁管理

“三高”网络漏洞与补丁管理要点：

- 关注漏洞平台信息并结合威胁情报、测试环境漏洞扫描等方式**及时发现漏洞信息**；
- 根据全面记录的资产信息验证测试漏洞是否存在，**分析漏洞影响**，并对可能已存在的**攻击行为进行自查**；
- 根据分析结果按需进行**修复或缓解方案开发**；
- 对补丁或升级文件实施**安全性分析、测试验证和灰度升级**；
- 同时可根据相应**威胁情报实施快速响应处置**；
- 建立漏洞与补丁管理响应跟踪机制，实施效能评估，**持续优化和改进**处置措施、管理流程等



内部补丁升级设计的基本原理

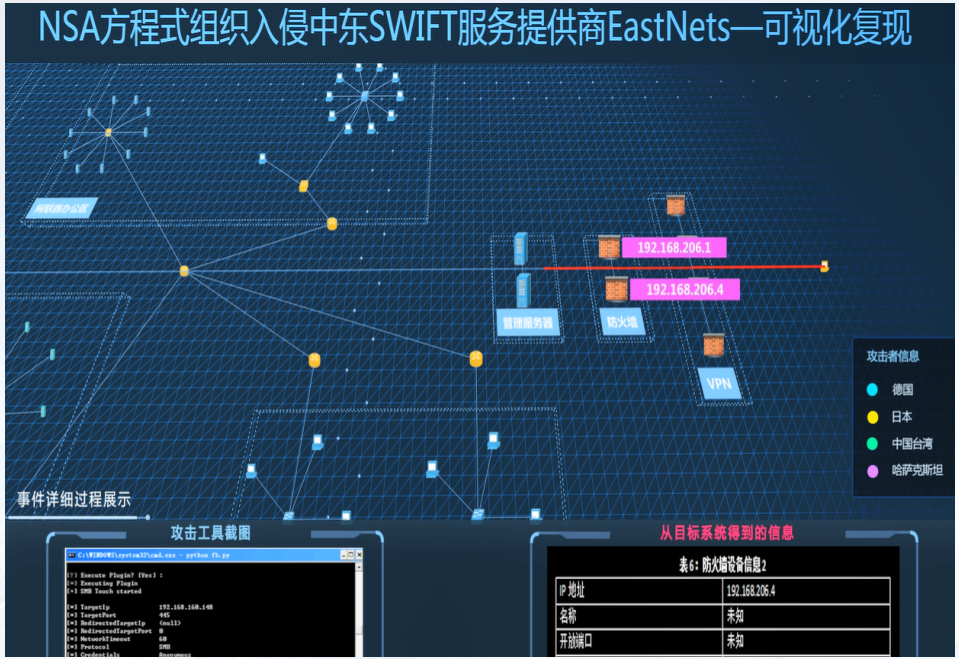
实施配置加固形成基准

- 结合网络实际情况
- 应覆盖所有的资产，避免盲点加固盲点
- “三高”网络信息系统软硬件资产建议参考安全技术实施指南（STIG）的加固措施集进行编制
- 能清晰明确地指导实施人员开展工作
- 应在测试环境中进行测试验证后实施配置加固
- 将安全加固配置形成基准，实现面向应用场景的配置管理

类别	名称	配置要求	配置措施
Windows-XP 示例			步骤1：选择“控制面板” 步骤2：选择“管理工具”
Windows-7 示例			步骤1：选择“控制面板” 步骤2：选择“管理工具”
国产操作系统 示例			
帐户与口令	禁止默认帐户	系统中除root帐户以外的默认账号应被禁止	步骤1：打开命令行 步骤2：查看系统中所有帐户名称， awk -F: '$1 !~ /^root$/ && $2 !~ /^[!*]/ {print $1 ":" $2}' /etc/shadow 步骤3：关闭帐户， passwd -l 帐户名
帐户与口令	口令过期设置	系统应强制密码X天更新	步骤1：打开命令行终端 步骤2：使用 vi /etc/login.defs 步骤3：查找PASS_MAX_DAYS参数所在行 步骤4：修改PASS_MAX_DAYS参数后的值为X
帐户与口令	口令过期提示	口令过期前Y天提示用户	步骤1：打开命令行终端 步骤2：使用 vi /etc/login.defs 步骤3：查找PASS_WARN_AGE参数所在行 步骤4：修改PASS_WARN_AGE参数后的值为 Y，建议Y为7

部分操作系统安全加固示例

在合理网络结构上叠加纵深防御



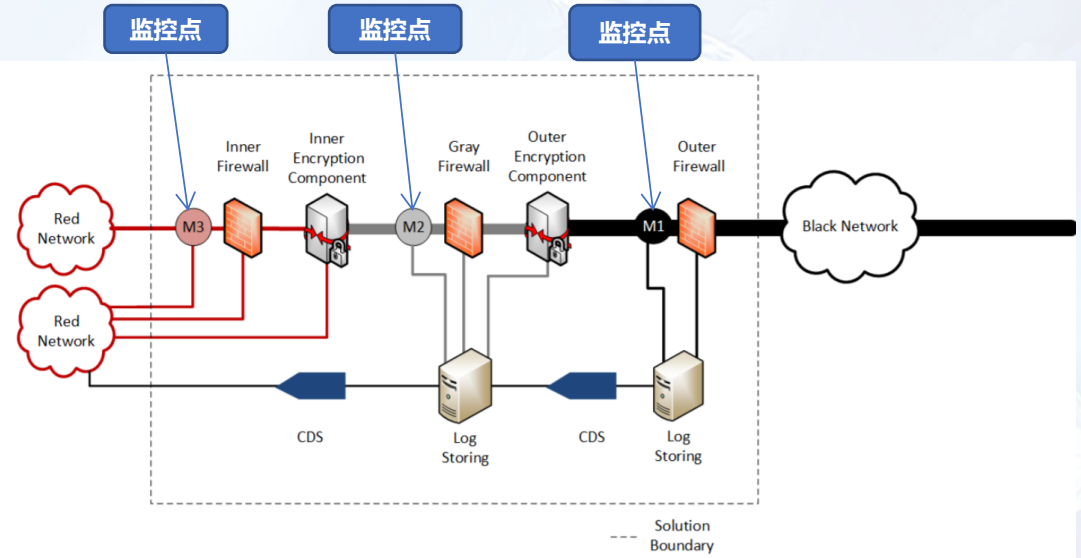


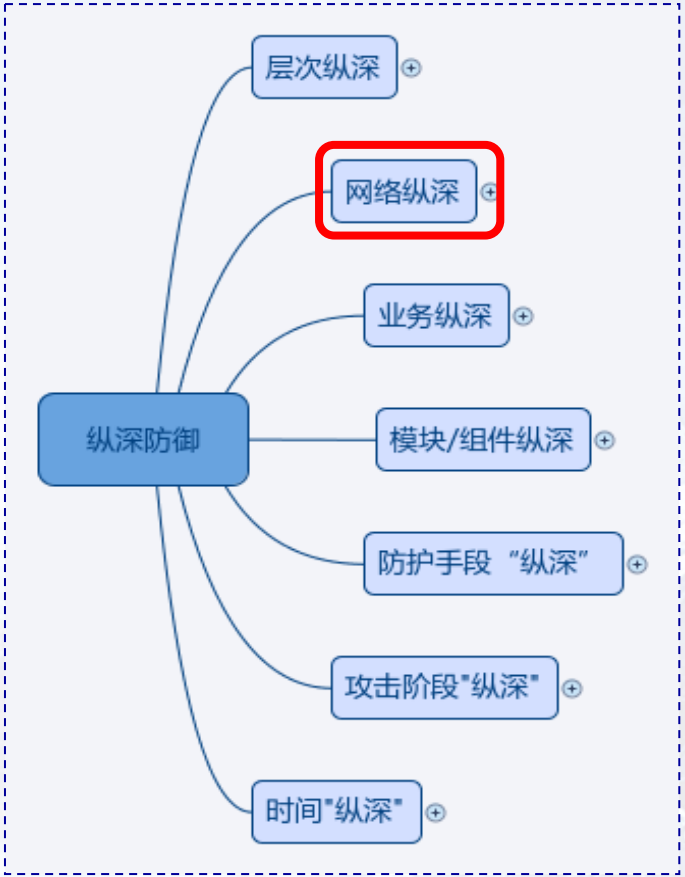
Figure 10. MSC Solution Continuous Monitoring

面对超高能力网空威胁行为体的攻击，边界防火墙、区域防火墙的边界防护，依然存在被打穿的可能。

根据业务工作特性和威胁情况，在合理规划的网络结构（或经过合理化调整的网络结构）上部署安全措施/设备，达到控制网络行为并收缩资产攻击面的作用。

“三高”网络应该在各个方面考虑防御手段的纵深覆盖

- 为了对抗体系化的攻击，防御体系的设计应利用好“先发优势”，针对威胁行为模式，**在各个方面考虑防御手段的纵深覆盖。**
- 在**网络纵深**方面，应有针对性地设计网络拓扑架构，从而限定攻击者可利用的潜在进攻路径，并**基于“面向失效的设计”原则**，综合利用白名单网络访问控制、IDS/IPS、已知与未知恶意代码检测、Web应用防火墙、VPN与数据加密、系统与应用加固和持续安全监控等多种安全机制，设计多样化多层次的防御体系，并**着重考虑其中任何一道防线被绕过后的防御“后手”**，最终强化防御者的先发优势，有效控制复杂的安全威胁。



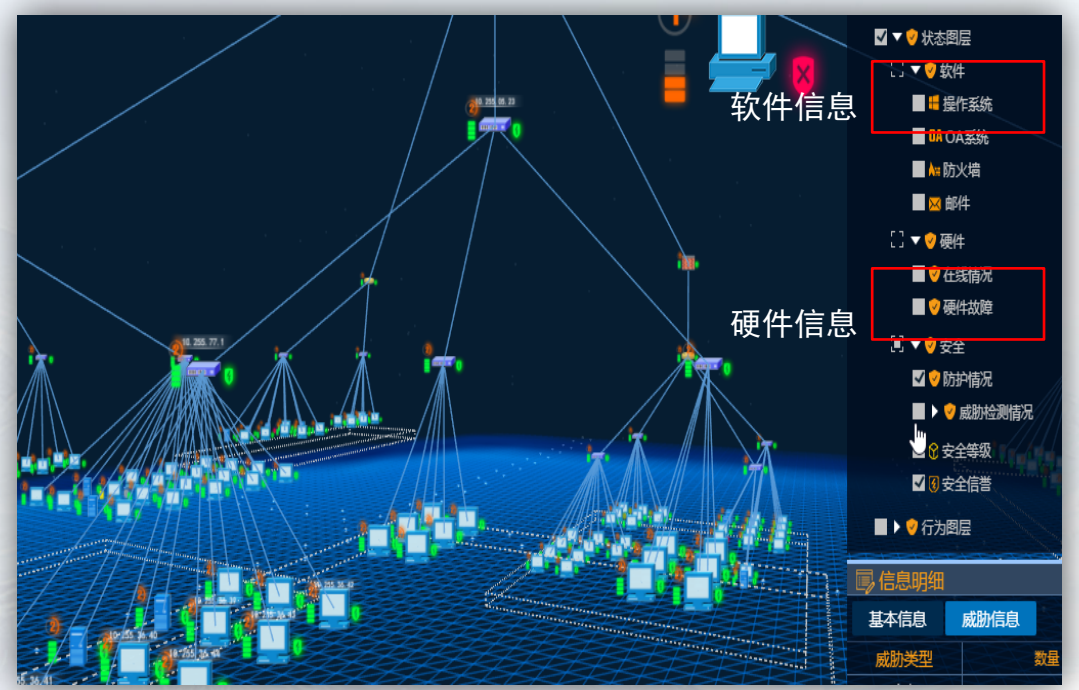
引自：第二届冬训营——黄晟《关于网络纵深防御的思考》

04 威胁情报驱动的战术型态势感知与积极防御

- 通过“三高”网络空间地形测绘掌握全局信息发现安全隐患
- 高价值信息融合理解进行威胁发现
- “套模板”式开展响应动作与过程跟踪
- 依托平台猎杀潜伏网络威胁
- 指挥协同响应实现积极防御

通过“三高”网络空间地形测绘掌握全局信息发现安全隐患

- 通过网络空间地形测绘掌握全局信息，并通过端点采集、探测发现、被动监测、人工上报等多途径持续获取资产信息，构架多层次的信息资产结构，如实还原现网场景下网络空间地形，建立全局能见度及感知能力，尽早发现脆弱点。为快速消除隐患，收缩攻击窗口提供有效支撑。



- “三高”网络信息系统的网络环境高度复杂，需要掌握网络结构整体情况，了解硬件地形、软件地形、服务地形等基本信息
- 及时进行脆弱点提醒，提供相关修复工具，同时协同终端防护设备进行修复，快速消除安全隐患
- 建立脆弱点修复任务，全程跟踪修复效果，最大限度排除安全隐患

高价值信息融合理解进行威胁发现

安全设备

- 流量
- 终端
- 边界
- 扫描
- 沙箱
- 蜜罐

威胁情报知识

多元异构安全数据

- 网络协议日志
- 入侵检测日志
- 病毒查杀日志
- 漏洞扫描日志
- ……
- 主动防御日志
- 系统操作日志
- 系统运行状态

初步理解——微观内容理解

- 内容解析
- 标准化
- 格式化

格式统一

信息丰富

- 信标提取
- 标签化
- 知识关联

深入理解——中观信息理解

- 威胁理解
- 脆弱点理解
- 异常行为理解
- ＋
- 资产关联
- 威胁情境

高价值信息产出

告警

- ✓ 聚焦目标
- ✓ 安全问题归类
- ✓ 风险整合

威胁行为轨迹预测

资产影响分析

“套模板”式开展响应动作与过程跟踪

1、按照响应预案操作设备或者系统，完成具体的响应动作

2、对事件建立响应任务

3、定期查看任务中每一步响应动作的完成情况

4、对于设备自动响应失败的动作，进行人工处置

5、以wannacry告警为例，作为已知威胁，搜索ms17-010漏洞所有影响主机，提供修复建议与措施，同时对所有网络设备下阻断指令，经过管理员确认，全网推送

面对威胁行动，根据所匹配的“情境模型“，对应响应行动模板，开展”组合拳”式响应，协调网络阻断、定点查杀、调整白名单策略等单点能力，流程化进行响应操作，集中记录、跟踪、评估响应效果。

依托平台猎杀潜伏网络威胁

支撑“三高”网络威胁猎杀平台侧需要具备：

- 充分、细粒度的数据：

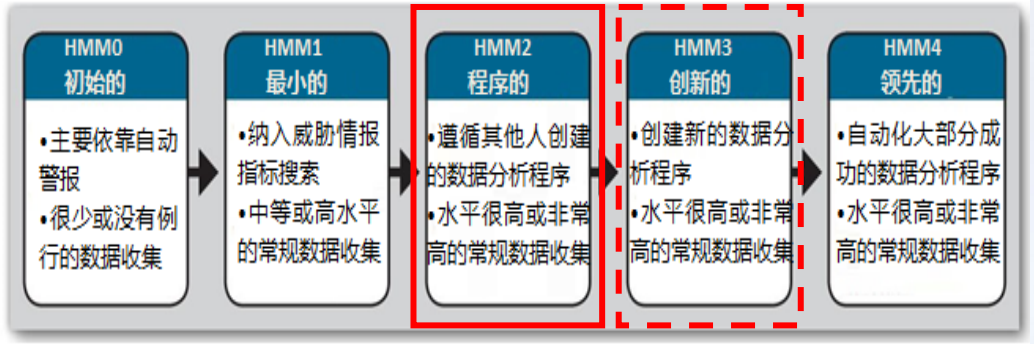
接收全要素采集数据，进行至少六个月数据留存，针对长期潜伏的威胁，为其建立攻击行为与攻击后果的关联提供充分的数据基础

- 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

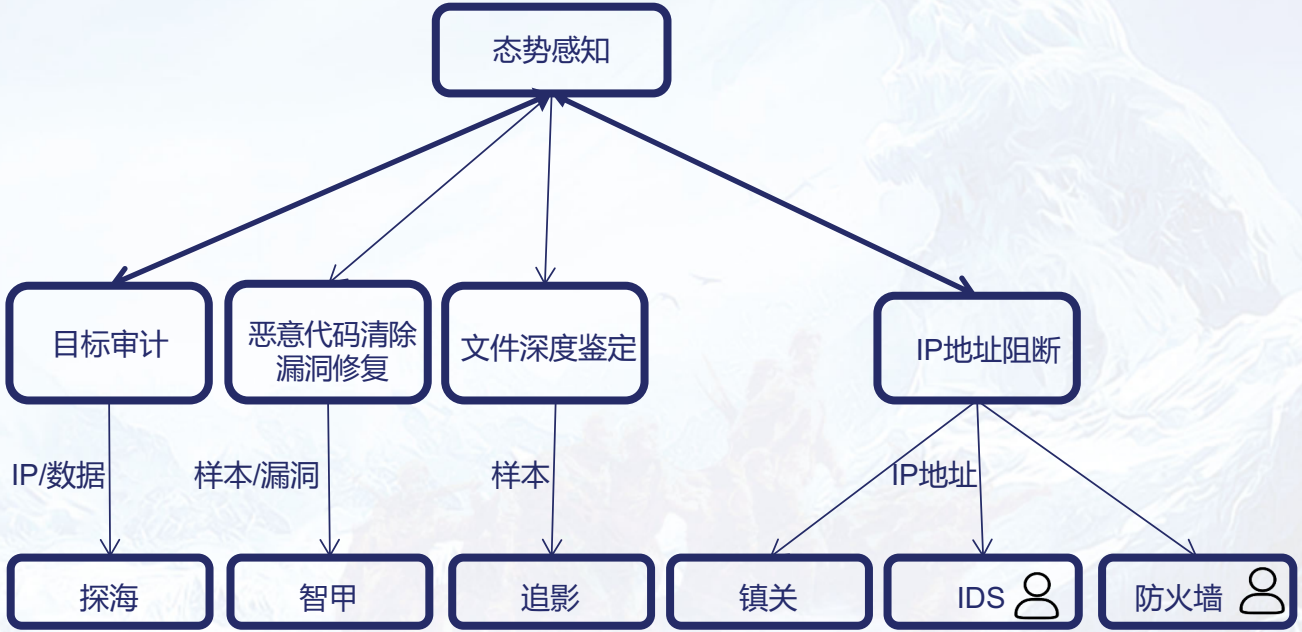


现有猎杀能力应该至少位于成熟度模型的第二阶段，即可推荐假设，具备使用情境模型的能力，通过反复猎杀与分析人员经验与能力的提升，可达到成熟度模型的第三阶段，能够创建新的情景模型与分析方法

人机结合协调指控响应与处置，形成主动化威胁对抗能力

基于敌情的复杂性、动态性、隐蔽性，单点安全能力不足以形成“三高”网络信息系统资产安全的有效保障，需要能够协调统筹各安全设备、处置工具、安全人员、网络环境等资源的上层态势感知实现威胁的积极防御。

需要态势感知的指挥协同响应能力



态势感知协同指控安全设备示例

05 实战化安全运行

- 通过全面调研了解现状、分析差距
- 根据调研结果设计安全运行流程
- 明确实战化运行的流程、角色职责与能力要求

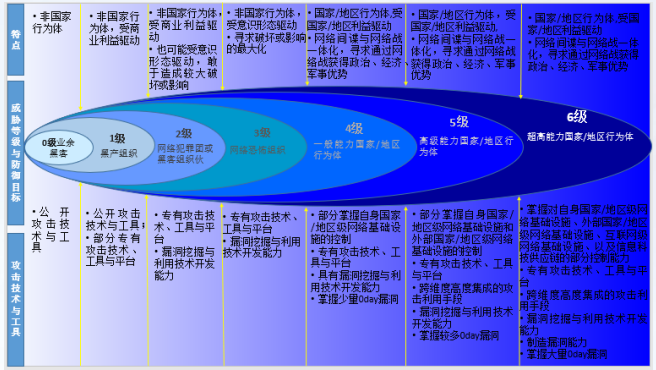
通过全面调研了解现状、分析差距

从对客户网络安全防御现状开展调研入手，调研内容包括管理、技术、运行三方面。在运行方面，调研工作内容、执行情况、人员职责、能力要求等，进而了解当前网络内安全运行能力现状。

成熟度等级

成熟度	含义
1级	初始化
2级	发展中
3级	明确定义
4级	可被管理
5级	持续优化

威胁对抗等级



准备调研

- 技术方面
- 管理方面
- 运行方面

开展调研

- 访谈方式
- 调研问卷
- 资料收集

现状评估

- 成熟度评估
- 威胁对抗等级评估

网络安全运行能力现状

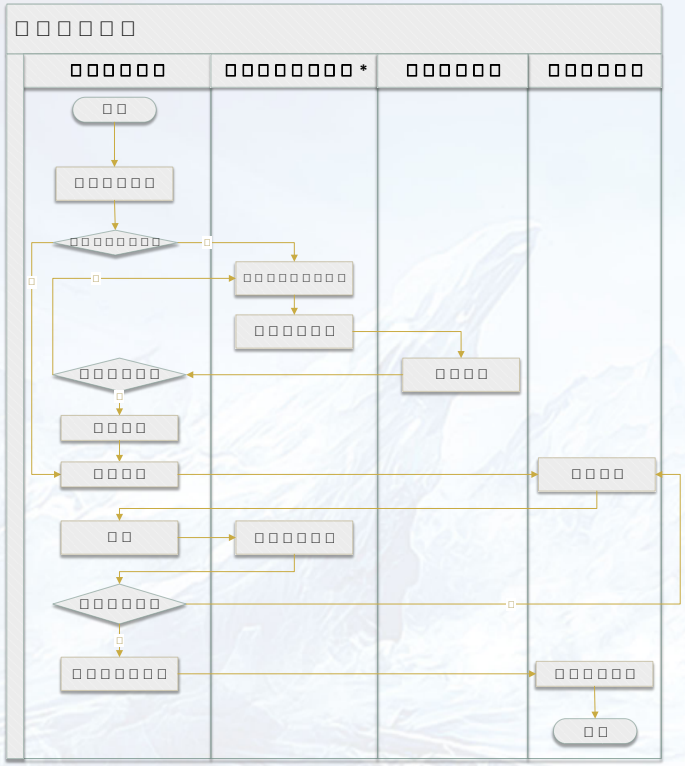
根据调研结果设计安全运行流程

结合客户场景设计安全运行流程

“三高”网络环境建议参考《美国国家安全体系黄金标准框架》

明确实战化运行的流程、角色职责与能力要求

建立流程



角色职责

角色职责表 - 配置管理

职责与配备 / 人员 · 角色	通知配置管理角色	通知系统管理角色	组织开展测试工作	选择安装配置方案	查看配置核查表	登记安装配置方案	登记配置核查表	测试安装配置与方案	修改并更新配置表	开展安全加固服务	实施配置	查看操作日志
配置管理角色		√	√	√	√	√	√					×
系统管理角色								√	√		√	×
配置开发角色										√		×
安全审计角色	×	×	×	×	×	×	×	×	×	×	×	√

注：√ 代表此项工作由相应角色承担；× 代表此项工作不能由此角色承担；* 代表此项工作可由外部人员承担。

注：同一人员可承担多个角色

能力要求

角色能力要求表 - 配置管理

能力 / 角色	信息安全知识	安全运维	计算机网络	操作系统软件	安全检查与安全加固	信息安全风险检查与风险评估
配置管理角色	了解级				了解级	
配置开发角色 *	专家级			掌握级	专家级	
系统管理角色		了解级	了解级	了解级		
安全审计角色	了解级					了解级

注：标 * 项可由外部人员承担

了解级 掌握级 专家级

“三高”网络动态综合网络安全防御体系建设总结

- 以“敌已在内、敌将在内”的敌情想定为基本前提；
- 遵循三同步原则，在网络信息系统的规划设计、建设实施、运行维护过程中充分考虑安全因素；
- 从网络与系统的规划设计开始，必须充分考虑基础结构安全，增强网络可管理性、提升可防御性，做好大量扎实演进的基础环节、基础能力支撑工作；
- 在此基础上，基于 “面向失效的原则” ，叠加可提供持续威胁防御和洞察能力的纵深防御，融合在系统架构之上，并与之深度结合；
- 进一步建设威胁情报驱动的战术型态势感知指控积极防御；
- 在叠加演进各个安全能力方面、网络信息系统的全生命周期均应配套实战化的网络安全运行。

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