第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

态势感知全景能力构建

安天 监控预警产品中心

红旗漫卷

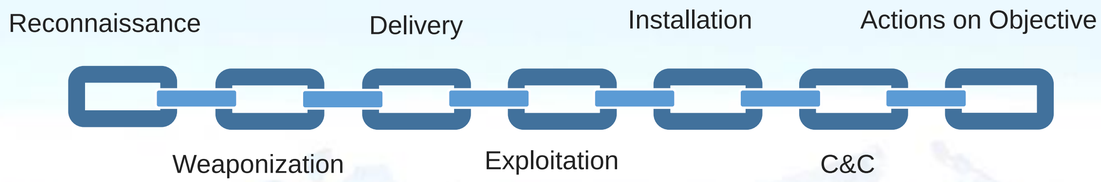
敌情想定是前提，网络安全实战化

提纲

- 威胁与挑战
- 态势感知能力全景
- 实战化态势感知
- 总结

1 威胁与挑战

背景



- 体系化的作业模式：“震网”事件、“乌克兰停电事件”、伪装“必加”事件等
- 商业军火扩散：商用攻击平台+恶意代码 为核心的军火扩散影响地区平衡
- 物理隔离：出现大量通过远程渗透入侵封闭的计算机网络或独立的安全隔离网形成的攻击事件

体系化防御

- 突发事件应急能力不足，针对 WannaCry 类似事件，缺乏人机协同的应急响应能力，无法做到及时止损
- 单点防御只能形成局部防御，应对体系化攻击无法有效进行能力组合
- 网络流量、网络边界、业务系统、主机端点相关安全数据与能力需要统一的汇聚、分析、协调、应用

上层指挥统筹能力

挑战

01 复杂多变的网络环境

- ✓ 网络结构变得复杂，增加了云平台架构、移动平台、工控网络、物联网等
- ✓ 计算与与安全技术飞速发展
- ✓ 信息资产的形式变得多样，实体资产之外增加了虚拟资产、信息资产

02 快速演化的网络威胁

- ✓ 攻击更有针对性，聚焦高价值资产
- ✓ 组合式的攻击方法，高级的攻击工具
- ✓ 更明确的攻击意图，为了成功达成攻击意图，可以在目标环境中长时间潜伏，期间所发生的行为均为正常的网络或者终端行为，无法被安全设备检出
- ✓ 实际攻击周期变短，且攻击成功后对目标造成“毁灭性”影响

03 相对威胁滞后的检测能力

- ✓ 面对复杂的攻击，传统安全防线很容易被绕过和规避，即由安全产品构成的安全防线很容易被突破
- ✓ 传统安全产品的防御能力滞后，通常只能在事后阶段进行检测，而不能在事前或者事中阶段进行发现，即对于用户来讲只能止损没有办法预防

态势感知引用的经典概念

在一定时间和空间内观察环境中的元素，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、处置的上层体系化防御系统

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

2 态势感知能力全景

叠加演进的建设思路

引入网络安全滑动标尺模型，采用叠加演进的建设思路

基础结构安全	被动防御	积极防御	情报	进攻性防御
在系统规划、建立和维护的过程中充分考虑安全防护	在无人员持续接入的情况下，附加在系统架构之上可提供持续防御或威胁洞察力的系统	分析人员监控和响应网络内部威胁并学习完善防御体系的过程	收集数据、将数据利用转换为信息，并将信息生产加工为评估结果，以填补已知知识缺口的过程	以法律反制措施等形式针对进攻者采取的自我防卫行动
合理的网络空间地形 合理的安全策略	全线防御体系	主动持续的威胁挖掘 流程化安全响应	情报管理 情报消费 情报生产	完善的安全服务机制

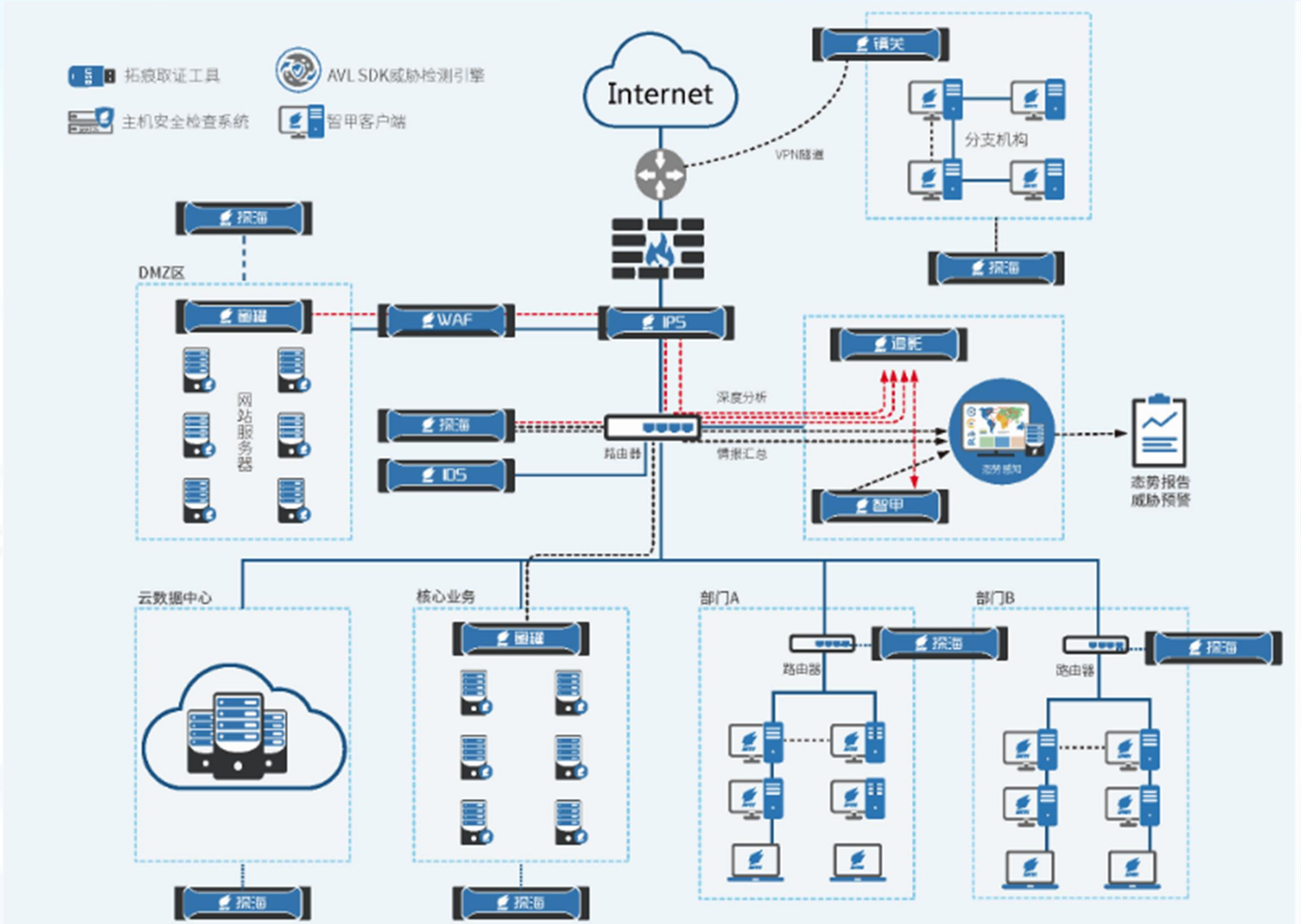
基础能力保障

基础能力提升

态势感知基础

◆ **态势感知必须依靠一定的基础防护能力，才能最大化地发挥作用，才能实现真正的有效防护：**

- 合理划分的网络结构
- 合理划分的安全域
- 定时的补丁机制
- 开启主机的防火墙设置
- 设置符合业务要求的白名单
- 关闭不常用的端口
- 关闭不常用的系统服务
- ...



全要素采集能力

流量侧的全要素采集-改变对抗时空

19

全要素采集+全向量分析

基于可靠的基础采集能力和分析能力使攻击者从原有的对检测结果的绕过变为对分析机制的绕过。

控制攻击者对于向量绕过的手段

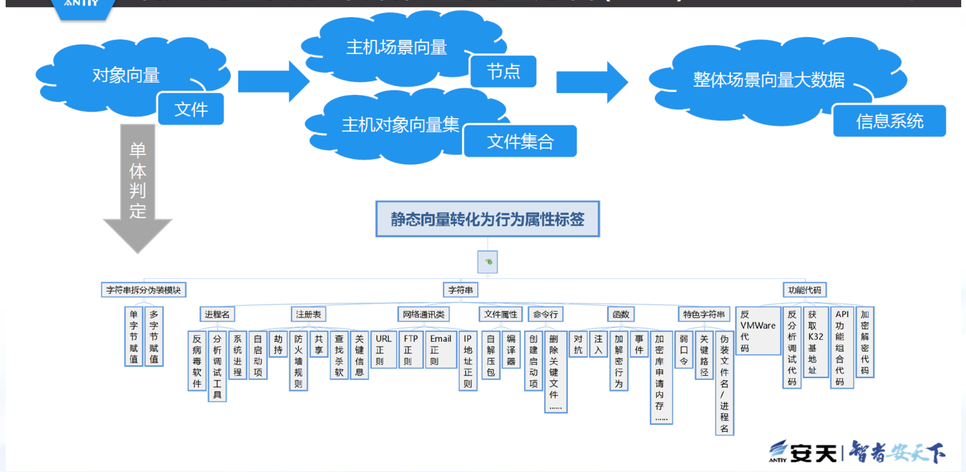
- 载荷或文件的解析能力；
- 流量侧的解析能力；
- 端点侧的解析能力。

以全量采集解析为基础能力，以定制采集为基本策略，以自适应的采集分析为努力方向。

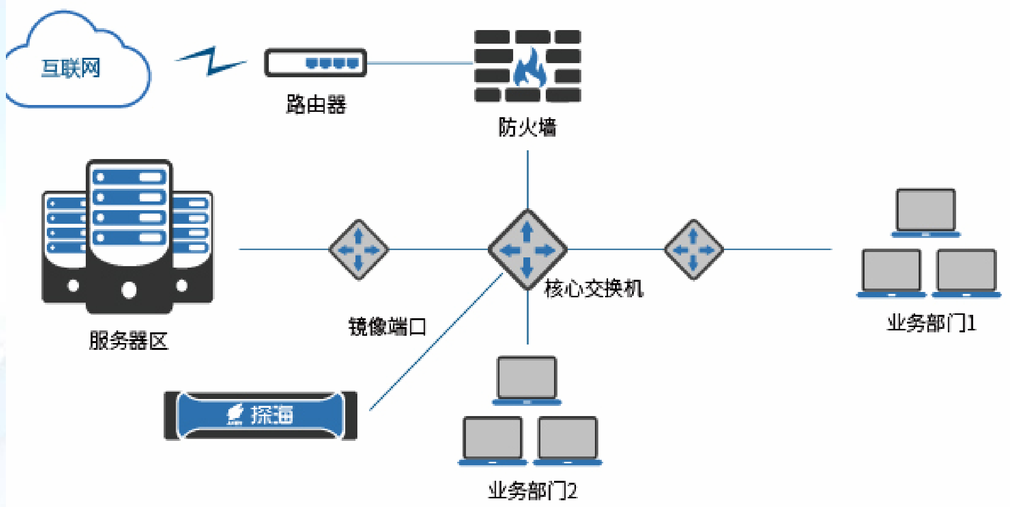
安天 | 智者安天下

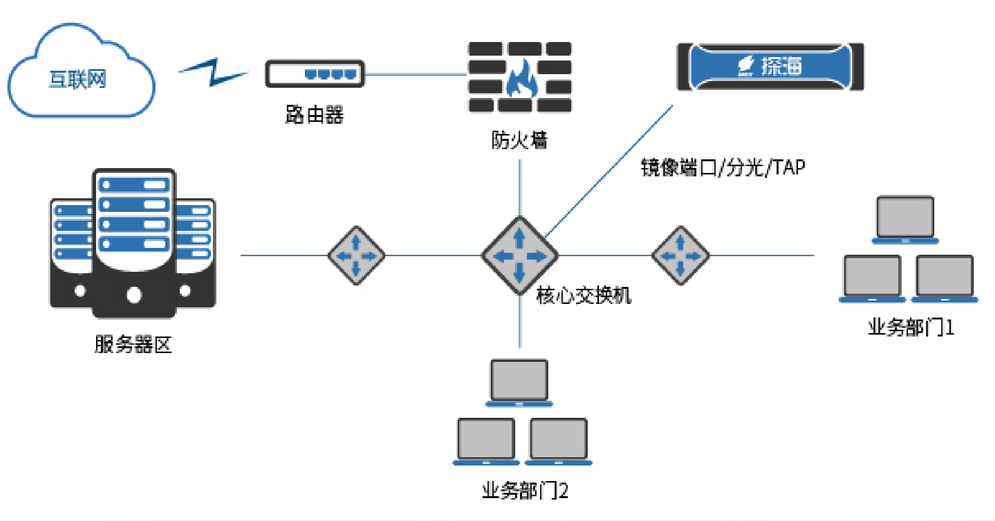
端点侧全要素采集和全向量分析(EDR)

25



安天 | 智者安天下

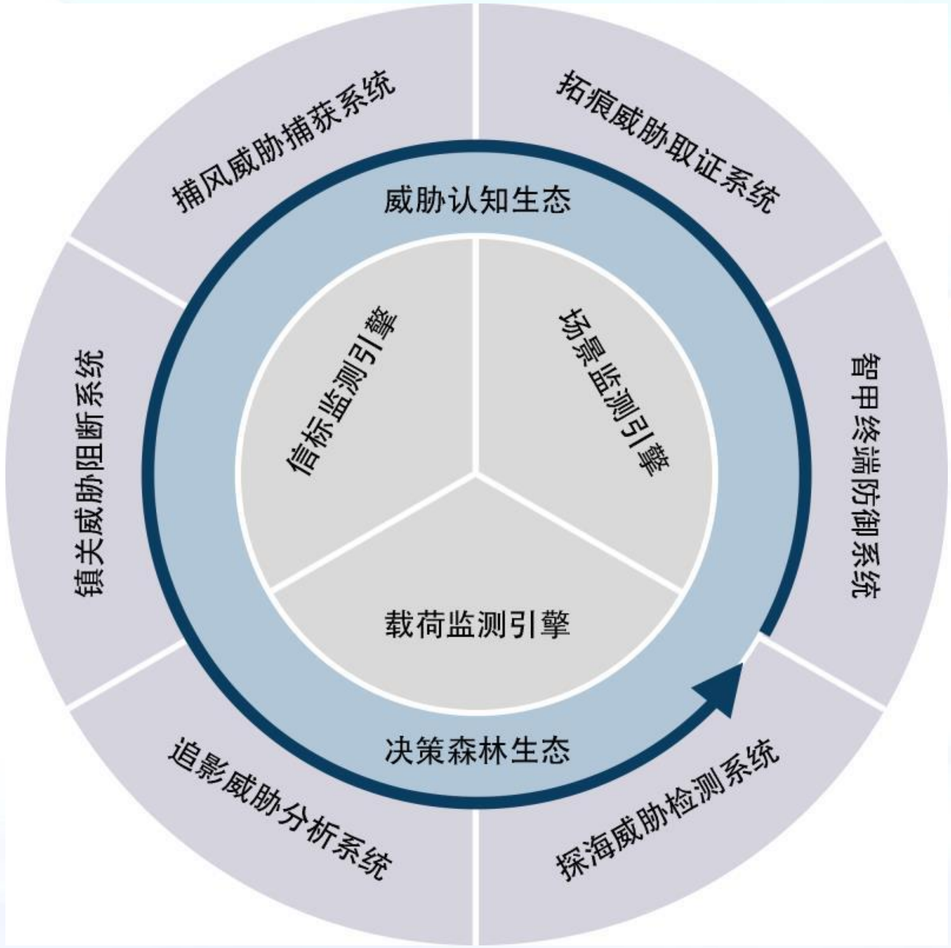




终端、网络侧信息采集

内网、互联网出口采集

多层次、按需检测能力



多层次检测能力

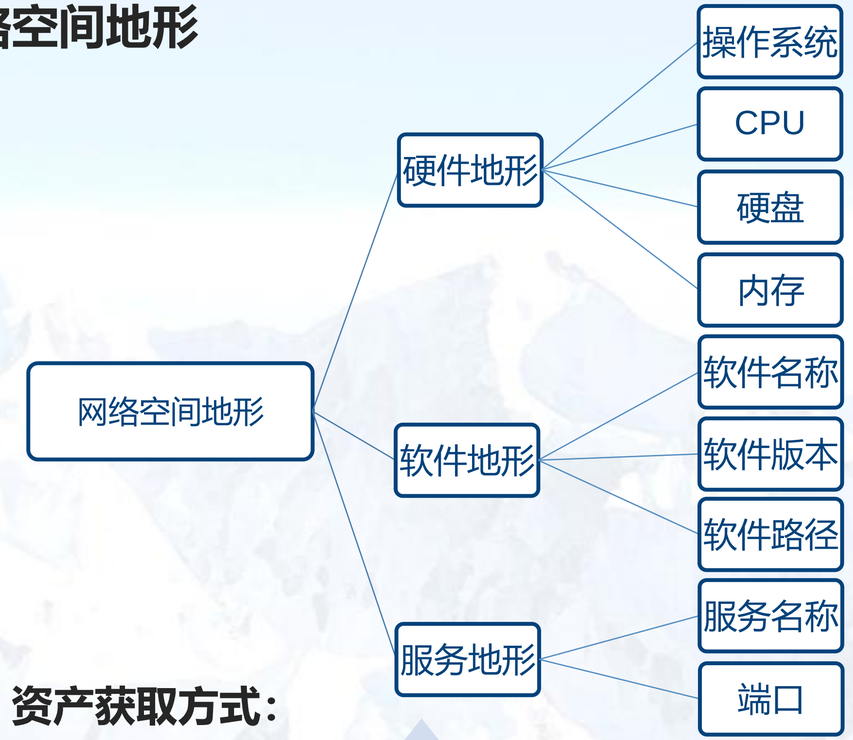
- 检测设备：流量、端点、网关
- 分析设备：文件分析、流量分析、主机行为分析
- 威胁捕获与取证：威胁诱捕、终端取证

按需检测能力

- 威胁检测：根据攻击（或疑似攻击）者信息、攻击（或疑似攻击）行为信息、潜在定向攻击目标，更新检测的规则，进行按需检测
- 脆弱点检测：根据漏洞利用特征更新检测的规则，进行指定漏洞在监测目标网络内的利用情况按需检测

资产测绘能力

建立多层次的信息结构，按照感知获取的信息，如实还原具体场景下所描述的网络空间地形



资产获取方式：

场景化分析能力

1、建立情境模型

（1）情报消费、知识利用、经验积累

（2）机器学习、知识图谱、人工智能

（3）基于实际攻击场景

（4）不断优化、迭代

2、使用情境模型

安全要素观察 -> 套用情境模型 -> 下一步工作短期预测 -> 全量数据关联 ->关键线索挖掘 -> 形成攻击路径

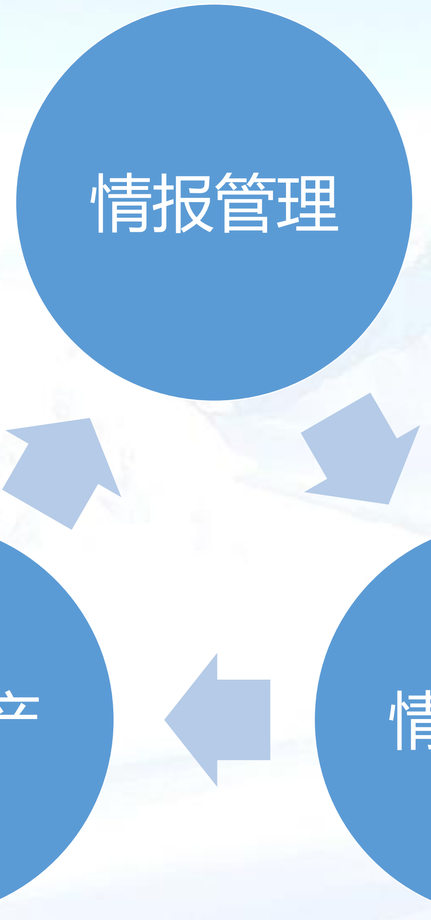
3、分析工具

（1）统计分析工具

（2）可视化分析工具

（3）交互式分析工具

情报消费与生产能力



- 情报获取：主动采集、被动获取、厂商交换
- 情报分析：信誉度评定、情报分类、安全要素提取
- 情报存储：分类分级集中存储，关键信息记录
- 情报检索：根据级别、类型、用途、关键信息检索

- 威胁发现的重要线索
- 安全设备的检测规则更新
- 基础网络架构薄弱点加固的策略参考
- 敌情分析的可靠依据

- 未知威胁挖掘生成
- 已知告警深入分析生成
- 文件深度分析生成
- 开源情报综合分析生成

常态化响应能力

人机结合的协同响应

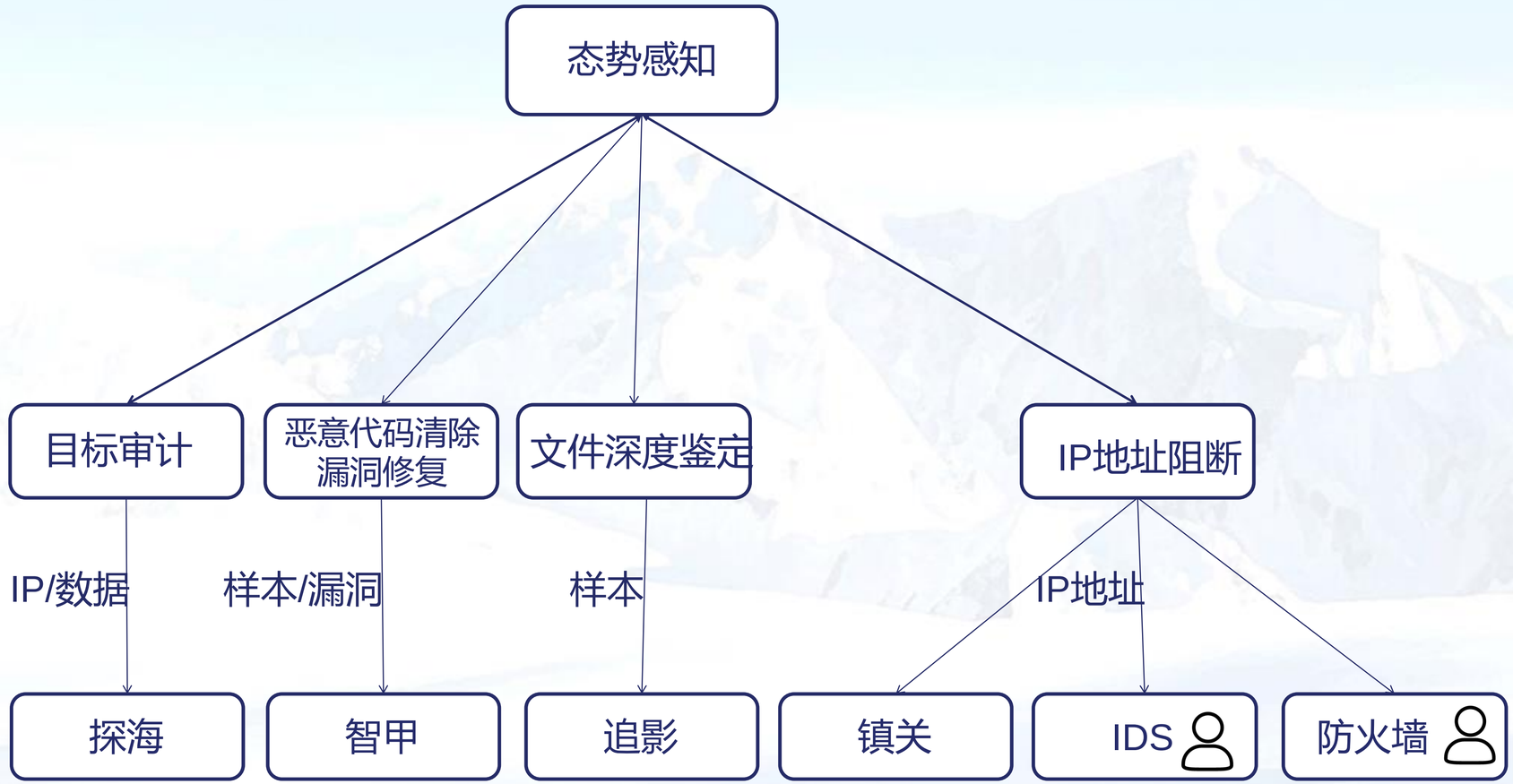
联动探海，实现威胁定点守候数据按需采集等响应操作

联动追影，实现文件深度分析，全方位获取文件鉴定结果和行为信息等响应操作

联动智甲，实现系统漏洞修复、恶意代码清除、文件全网追溯等响应操作

联动镇关，实现网络阻断等响应操作

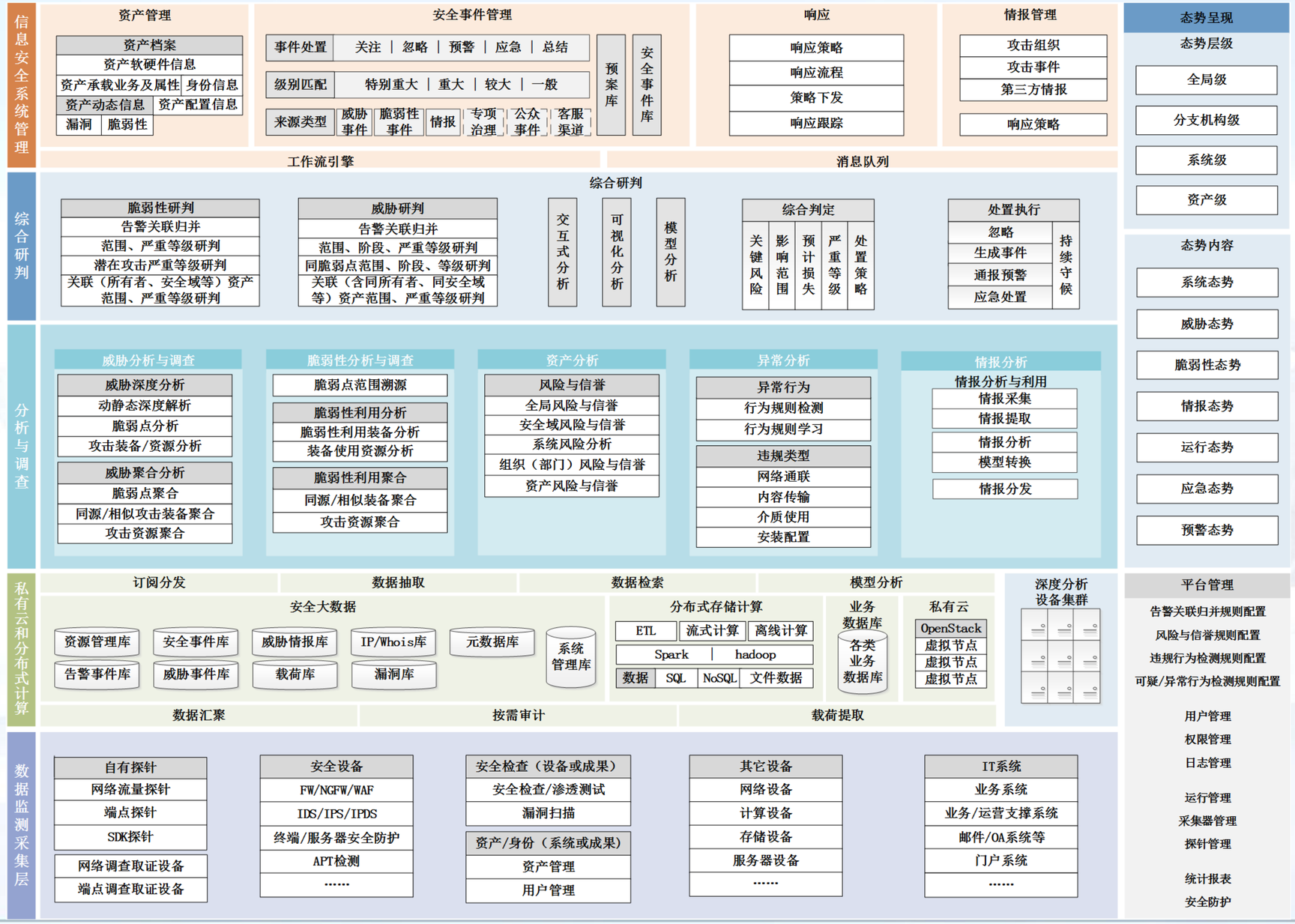
自动协同动作人工进行确认



通过对各类设备进行联动实现主动的威胁对抗能力

态势感知能力全景

- 全要素数据采集能力
- 多层次、按需检测能力
- 资产测绘能力
- 场景化分析能力
- 情报消费与生产能力
- 协同联动能力
- 常态化响应能力



3 实战化态势感知

实战化态势感知的任务与人员配置

1、演示任务

- 演示信息安全态势显示内容和含义
- 演示攻击流程、处置过程

2、常态安全对抗

- 日常威胁处理
- 输出日常安全报告
- 监控安全态势，发现异常行为

3、突发事件应急

- 积极响应突发事件
- 根据应急预案开展应急处置

4、网络安全的战略决策

- 全览全网安全态势，指挥设备操作
- 应急处置开展等安全决策
- 监控安全态势、安全事件处置过程和结果
- 模型推送、事件通报

实战化态势感知的流程

基于资产的威胁发现与响应

情报驱动的威胁发现与响应

未知威胁的发现与响应

基于资产的威胁发现与响应

对于存在敏感数据、承担关键业务的资产进行重点关注，在完善的基础防护基础上，发现资产存在的已知威胁在全线的检测能力和防护目标为核心的基础上，对资产告警进行自动化响应

基于资产的威胁发现与响应

第一步：查看资产告警（安全值守员）

1、查看关注的资产是否有新的告警产生

2、查看告警的资产信息，包含资产的归属、基本属性、基本配置情况

2、查看告警原因：

（1）恶意代码：病毒名、家族、样本哈希、样本类型等

（2）远程控制：持续时长、跳板机、控制端地址等

（3）网站挂马：恶意链接、病毒名、家族、样本哈希等

3、根据威胁类型在系统的预案库中选择响应预案

第二步：响应处置与结果跟踪（设备操作员）

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，对ms17-010漏洞进行修复，对wannacry相关样本进行全网追溯和定点清除，对连接开关域名的连接进行阻断

第三步：定期的资产维护（安全值守员）

1、根据业务变化动态维护关注资产：存在敏感数据、承担关键任务

2、定期检查资产的漏洞修复情况，发现未修复的漏洞及时协同智甲或者通过人工下载补丁进行修复

3、动态维护资产白名单

（1）可访问应用

（2）可访问主机

情报驱动的威胁发现与响应

需要稳定的情报供应，后续分析的结果与质量依赖于初始情报的信誉与完整度

能够发现同源、同类型的未知威胁

情报驱动的威胁发现与响应

第一步：情报查看与推送（安全值守员）

1、通过系统界面提醒发现有待处理的威胁情报

2、浏览情报信息，重点关注：

（1）情报源：判断情报信誉

（2）获取途径：外部共享还是内部通告，判断情报优先级

（3）类型：IOC还是TTP

（4）内容

3、根据情报源和获取途径，将情报内容向安全分析员进行分类推送，按照情报的等级由高到低依次选择电话、短信、邮件进行通知

第二步：IOC分析与检测规则落地（安全分析员）

1. 阅读IOC情报，提取关键字
2. 将信息进行分拣：
   1. 低级：哈希、域名、 URL
   2. 高级：网络行为、主机行为
3. 将单条IOC或者多条IOC进行组合，根据IOC的内容，选择符合条件的安全设备，将IOC转化为符合安全设备检测规则格式的检测规则
4. 指定规则的适用安全区域
5. 指定规则的使用时长
6. 向安全指挥员提交网内应用申请

情报驱动的威胁发现与响应

第三步：TTP分析与情境模型落地（安全分析员）

1、阅读TTP情报，提取关键字

2、将信息进行分拣：

（1）战术：攻击方法

（2）技术：攻击工具、攻击平台、攻击资源

（3）过程：攻击过程

3、根据TTP的内容，形成情境模型，输出探海（网络）和智甲（终端）的高级检测规则

4、指定规则的使用时长

5、向安全指挥员提交规则下发申请

第四步：查看守候的威胁告警（安全值守员）

1、查看告警资产信息，确认告警范围与告警对象特征

2、查看告警原因：

（1）告警匹配的规则

（2）告警的威胁类型：恶意代码、网络入侵、横向移动、远程控制等

3、如果匹配了情境模型，能够查看告警后续动作的预判，针对每一步的预判动作触发后续的分析调查

4、如果告警中发现了未分析样本，投放追影，并向样本分析员发起样本分析申请

5、对于已经确定的部分动作，查看处置建议，在系统中完成相应操作

情报驱动的威胁发现与响应

第五步：威胁调查与安全事件研判（安全分析员）

1、查看告警威胁相关联元素的属性与关联关系，图形化了解告警基本情况

2、基于情境模型对于下一步攻击动作的预测，通过关联分析，全量数据搜索、聚合分析，挖掘威胁攻击路径，还原单点威胁全貌，即威胁源在哪里做了什么事情

3、在单点威胁的基础上，进一步分析历史相关联事件和由该威胁可能引发的潜在风险

4、在相关联威胁分析的基础上，对应知识库、情报库，针对攻击组织的分析，归纳总结攻击组织画像、同源事件行为模型提取，完整针对对手的分析

情报驱动的威胁发现与响应

第六步：输出响应预案（安全分析员）

1、根据分析结果完善预案的基本信息：标题、单位、时间、人员、告警或者安全事件描述

2、根据针对事件的分析，协调单点防御能力，配合人工作业，形成流程化的响应预案

（1）网络侧：网络阻断、目标审计等

（2）主机侧：定点清除、漏洞修复、全盘扫描、全网追溯等

（3）业务系统：网络隔离等

3、生成预案文件并派发（邮件、内部IM、纸质版等)

第七步：响应处置跟踪（设备操作员）

1、收到新的响应预案

2、按照响应预案操作设备或者系统，完成具体的响应动作

3、对事件建立响应任务

4、定期查看任务中每一步响应动作的完成情况

5、对于设备自动响应失败的动作，进行人工处置

第八步：生成威胁情报（安全分析员）

分析结果、响应过程、响应结果总结生成威胁情报：

1、威胁源信息：攻击者、攻击组织、来源IP、事件发生未知、攻击装备等

2、威胁检测信息：静态检测特征、动态检测特征、HASH、IP、域名、攻击资源、攻击工具、网络环境信息等

3、攻击目标信息：组织、行业、人员、设备、环境等

4、利用漏洞信息

5、关联事件报告：历史事件

6、响应方式与结果：处置建议、响应预案、响应结果等

未知威胁发现与响应

在配备高级安全分析人员的，全要素数据采集的基础上，能够对网络、主机的正常行为进行建模

发现异常后，能够有足够的数据储备进行未知威胁的挖掘

未知威胁发现与响应

第一步：查看发生异常的告警（安全值守员）

1、查看告警资产信息，确认告警范围与告警对象特征

2、查看告警原因：

3、如果匹配了情境模型，能够查看告警后续动作的预判，针对每一步的预判动作触发后续的分析调查

4、对于已经确定的部分动作，查看处置建议，在系统中完成相应操作

未知威胁发现与响应

第二步：异常点调查与安全事件研判（安全分析员）

1、查看存在异常点资产的属性与关联关系，图形化了解告警基本情况

（1）资产节点属性：类型、安全域、资源归属、业务意义、软硬件配置

（2）节点间网络连接关系

2、基于情境模型，通过关联分析，全量数据搜索、聚合分析，挖掘未知威胁，进行安全事件研判

（1）行为关联

（2）漏洞利用关联

（3）历史数据中相同行为攻击挖掘

（4）历史数据中相同脆弱点利用攻击挖掘

（5）……

第三步：输出响应预案（安全分析员）

第四步：响应处置跟踪（设备操作员）

4 总结

感攻击于须臾 定源头于一瞬

拢态势于眼底 挫威胁于指尖

第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

关注安天冬训营官网

关注安天微信公众号

红旗漫卷

敌情想定是前提，网络安全实战化