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

内部资料

人机协同态势感知运行能力建设

安天 网络安全服务部

提纲

引子

- 为啥需要运行能力建设
- 人机协同态势感知的必要性

1 运行能力现状分析

- 现状调研与评估
- 推演评估运行能力不足

2 人机协同态势感知实战化运行能力建设

- 战术型态势感知中基础结构安全相关运行能力建设
- 态势感知与积极防御、威胁情报有关运行能力建设

3 实战化运行能力持续提升

- 运行能力提升方向
- 参考NICE框架提升网空安全防御人员素质
- 结合内外部力量持续提升战术型态势感知运行能力

引子

为啥需要运行能力建设

人机协同态势感知的必要性

战术型态势感知中人机协同的必要性

人机协同需求

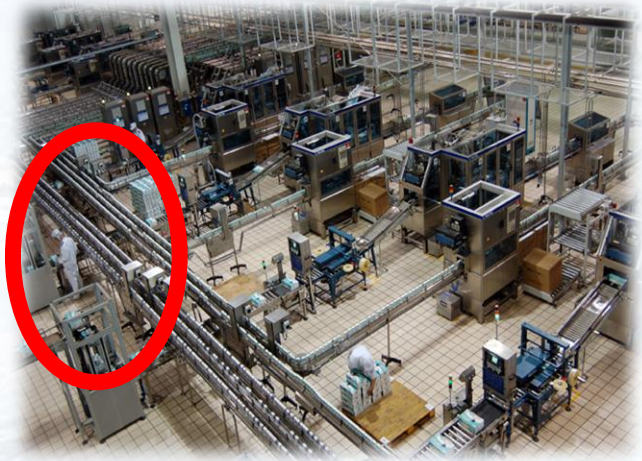
- 叠加演进网络安全能力模型基础结构安全中个别环节需人员介入
- 态势感知与积极防御中应存在分析人员对所处防御网络内的威胁进行监控、响应、学习和应用知识

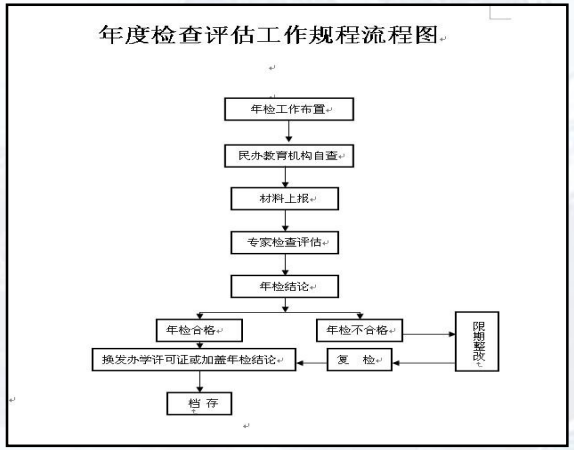
人机协同意义

- 防御模式上，应将网空安全防御人员视为获得态势感知所不可或缺的“系统组成部分”，并且使参与控制闭环的人员能够通过使用自动化工具而提高防御效果

人机协同实战化

- 结合用户侧人员配备与能力现状，设计安全运行规范、操作手册和流程
- 流程涵盖各项职责，对应角色能力要求，对能力要求高的角色可由外部人员承担





01 运行能力现状分析与评估

现状调研与评估

推演评估运行能力不足

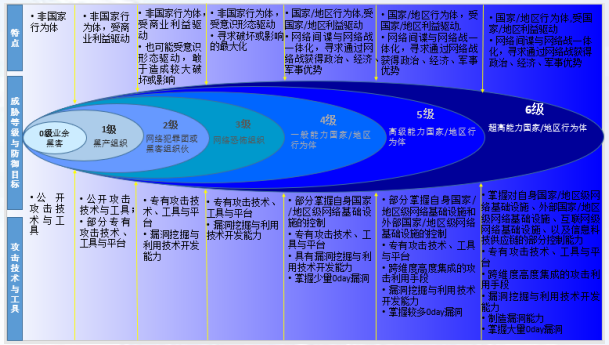
现状调研了解当前运行能力

建设前，安天对客户网络安全防御现状开展调研，调研内容包括管理、技术、运行三方面，对其成熟度与威胁对抗等级进行评估。在运行方面，调研内容包括规程建立与执行情况、角色职责等，进而了解当前网络内运行能力现状。

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

推演评估了解运行能力不足

为掌握当前网络防御能力与潜在威胁，应对客户当前网络防御能力进行威胁评估。传统方式中，一种是在模拟测试环境下进行渗透测试，导致威胁评估无法保证结果的全面性、准确性；另一种是在业务生产环境中进行威胁评估，存在影响业务系统稳定性和安全性等风险。面对以上难题，安天创新性提出推演评估方式。

推演评估

- 首先，调研了解网络安全防御现状。依托安天威胁对抗经验，结合对高能力对手网络攻击可用装备的了解，生成逻辑推演模型、设计攻击模板。
- 其次，由扮演攻击者的人员模拟每一步攻击步骤并生成攻击场景。针对攻击场景，分别由扮演攻击方和防御方人员陈述理由，由裁判组根据双方陈述、相关资料和专家经验判定是否攻击成功。
- 最终，根据各个场景下的判定结果，得出网络防御现状中存在的问题与必须的安全措施，评估威胁现状，得出管理能力、运行能力、技术能力的不足。

02 人机协同态势感知实战化运行能力建设

战术型态势感知中基础结构安全相关运行能力建设

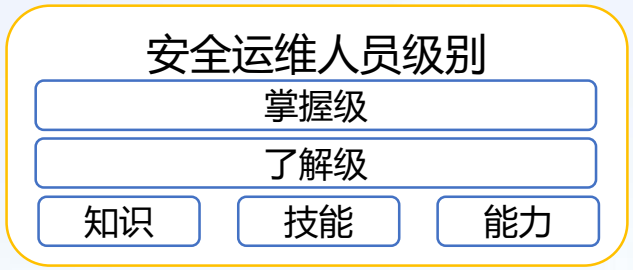
态势感知与积极防御、威胁情报有关运行能力建设

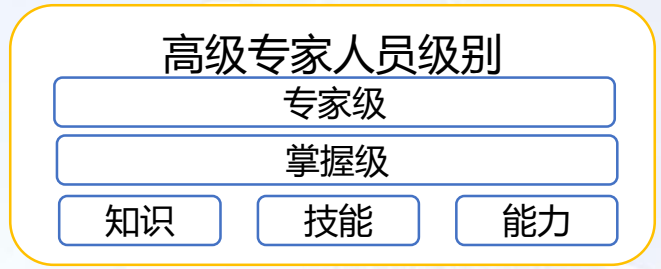
人机协同态势感知实战化运行能力建设思路

建设思路

围绕战术型态势感知，为实现客户侧网络安全防御实战化安全运行的目标。

- 建立完备、统一的安全运行管理流程，明确安全运行相关角色与职责，确定所需知识、技能、能力，编制所需方案指南。
- 组织对人员展开专业的安全知识和技能培训，并结合竞评演练和一线攻防对抗等形式，提升安全实战对抗能。





明确实战化运行的流程指南、角色职责与能力要求

建立流程

明确职责

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
	工作职责											
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

战术型态势感知中基础结构安全相关运行能力建设

态势感知依赖于全面且及时掌握网络与系统各方面情况的“知己”能力，这与网空测绘、资产管理、配置管理、漏洞管理与补丁管理等基础结构安全能力密切相关，而且直接影响着态势感知所必需的攻击轨迹聚合与攻击策略预测能力的水平

资产管理和网空测绘	漏洞管理和补丁管理	配置管理
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。	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。	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。

覆盖全生命周期的资产管理

资产入网前

资产管理角色

- 在态势感知资产管理表中记录资产信息与资产用途
- 通知配置管理角色开展初始配置管理流程
- 通知漏洞管理角色进行初始漏洞管理流程，必要时由补丁管理角色开展补丁管理流程

系统管理角色

- 资产达到入网基准后，将资产入网

资产入网后

资产管理角色

- 定期通过态势感知资产测绘功能并结合人工完善的方式记录所有软硬件资产技术信息与基本管理信息
- 技术信息包括机器名、MAC、IP、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。基本管理信息包括物理位置、所属部门、责任人等

资产退役时

资产管理角色

- 根据退役资产信息修改态势感知资产管理表

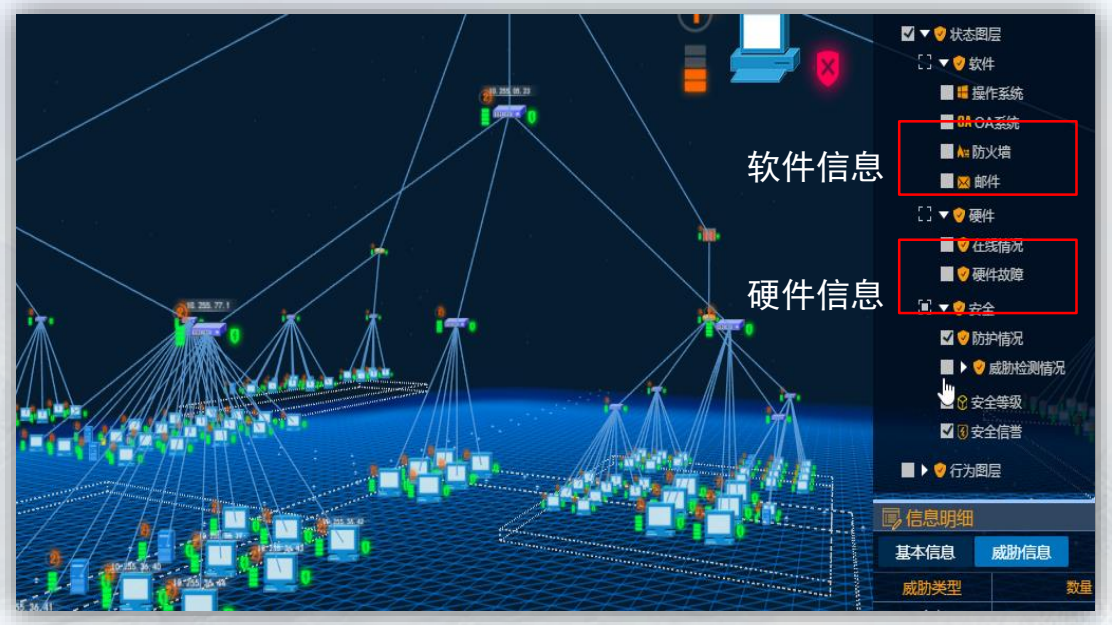
系统管理角色

- 将资产下线

注：资产管理流程均需要安全审计角色，对资产管理工作进行审核。

资产管理依托网络空间地形测绘，掌控全局软硬件资产信息

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。



- 高价值网络环境高度复杂，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

覆盖全资产的配置管理

配置管理

配置管理角色

- 根据资产信息与用途在态势感知方案库中选择并下发配置方案
- 通知配置开发角色开发配置方案，并组织配置方案测试
- 将经过测试的方案录入态势感知
- 资产配置信息录入态势感知配置表

配置开发角色

- 结合资产信息与用途开发方案，并协助测试方案

系统管理角色

- 测试与实施方案

安全审计角色

- 审核配置管理工作

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

注：由于配置开发角色需专家级能力，故建议由外部人员承担

了解级　掌握级　专家级

覆盖全资产的配置管理

配置方案开发

STIG(Security Technical Implementation Guides，安全技术实施指南）是美国国防部防务信息系统局支持发布的一系列安全加固实施指南。配置方案依据**资产信息与用途**。配置方案应参考STIG进行开发，并在测试环境中测试后方可使用。

- 操作系统加固项共15685 个，覆盖8 大类系统，168 个版本的操作系统，平均每个操作系统的配置点多达600 个以上
- 应用和服务加固项有4245 个，主要覆盖5大类应用和服务

(统计数据截至2018 年 9 月 4 日)

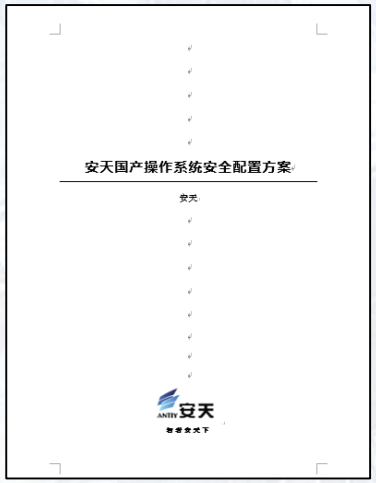
注意事项

- 配置方案并非按照资产信息“一刀切”编制
- 配置加固应支撑业务系统，而不能干扰业务系统的连续性和稳定性

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

国产操作系统安全配置示例



国产操作系统配置方案

结合威胁情报的漏洞管理

漏洞管理

情报分析角色

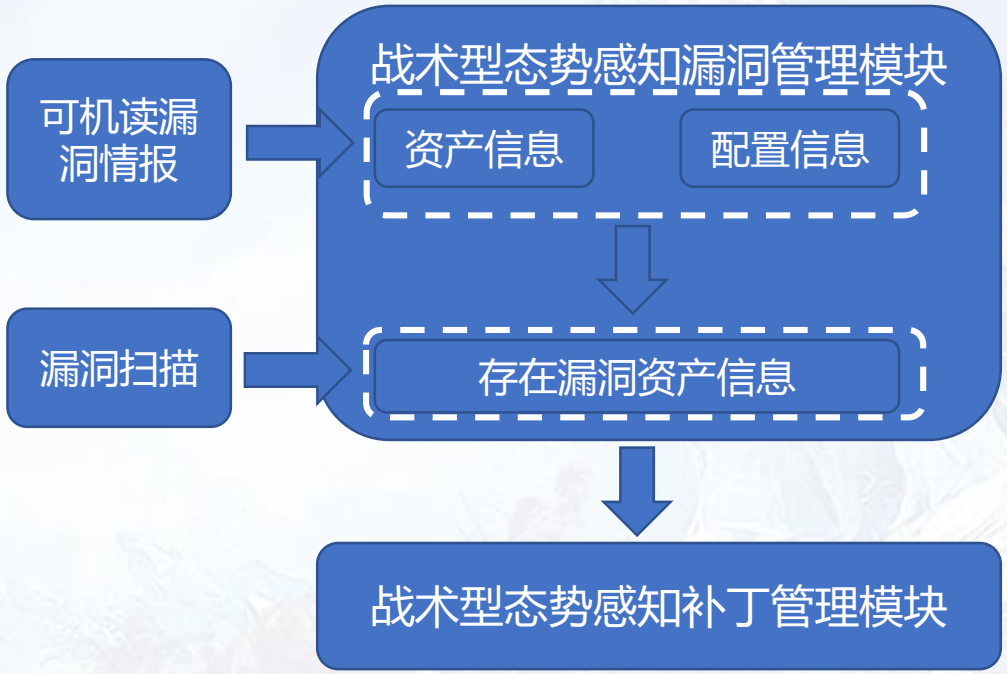
- 提供可机读漏洞情报给情报管理角色

情报管理角色

- 将情报信息录入态势感知的情报系统

漏洞管理角色

- 利用态势感知资产测绘或联动漏洞扫描设备(选择可扫描时段开展该工作)，生成待修补漏洞表，利用态势感知督促补丁管理员进行修补
- 利用态势感知资产测绘或联动漏洞扫描设备验证漏洞的修复情况
- 维护态势感知中漏洞表



结合安全性分析的补丁管理

补丁管理

补丁管理角色

- 通过态势感知接收待修补漏洞表，通知补丁开发角色提供新增漏洞对应补丁，在态势感知方案库中选择并下发已有补丁至系统管理角色

补丁开发角色

- 获取补丁并对补丁逆向进行安全性分析，判定是否可安装该补丁
- 开发缓解措施（包括虚拟补丁、增强监控）
- 协助系统管理角色在测试环境测试经过安全性分析补丁或缓解措施

注：该角色需要专家级知识技能，建议由外部人员承担

系统管理角色

- 在测试环境测试经过安全性分析补丁或缓解措施
- 实施补丁或缓解措施

感知态势资产漏洞与补丁信息

结合安全性分析的补丁管理——补丁安全性分析

- 补丁分析前后均需对补丁进行数字签名校验
- 人工结合设备动静态方式分析补丁
- 分析过程中对其中涉及的域名、特殊字符串等，应利用态势感知中情报系统对其进行关联分析
- 分析结果若发现存在安全威胁，建议将结果提交威胁情报流程情报分析角色

态势感知与积极防御、威胁情报有关运行能力建设

依托训练有素的网空安全分析人员的强大认知能力理解当前情境与发现那些隐藏的潜伏威胁和复杂的攻击行动，交由网空安全防御人员把控响应行动方案并监督响应行动执行过程，并在后续阶段利用系统的自动化响应执行能力对快速发生的已知攻击行动及时做出响应处置。

安全监测

在威胁情报能力驱动下，通过全面持续监控，网空安全分析人员发现威胁踪迹，并确定其影响节点范围

事件响应与处置

采用网空态势感知发现潜伏的高级威胁，指挥网空安全防御人员对所暴露威胁展开猎杀清除等响应行动

威胁情报

对信息获取与分析，从而识别、跟踪和预测网络空间威胁的网络作业能力、意图和行动，从而支撑网络防御的决策，并提供采取系列措施的建议

结合态势感知开展安全监测

日常安全监测

安全监测角色

- 查看态势感知告警信息，必要时通知深度威胁分析角色对可疑威胁进行人工研判
- 利用态势感知通知响应方案管理角色启动事件响应与处置流程

深度威胁分析角色

- 利用态势感知分析可疑威胁，结合资产对资产、可疑威胁、脆弱性、异常行为

注：由于该角色存在专家级能力要求，建议由外部人员承担

策略管理角色

- 生产按需监测规则，并利用态势感知向安全设备下发规则

查看告警信息 → **人工分析研判** → **事件响应与处置**

根据态势感知告警信息判断

- 若为已知威胁，启动事件响应与处置流程；
- 若为疑似威胁，通知深度威胁分析角色开展人工分析研判

利用态势感知分析

- 资产分析
- 可疑威胁分析
- 脆弱性分析
- 异常行为分析

在态势感知方案库中选择处置方案

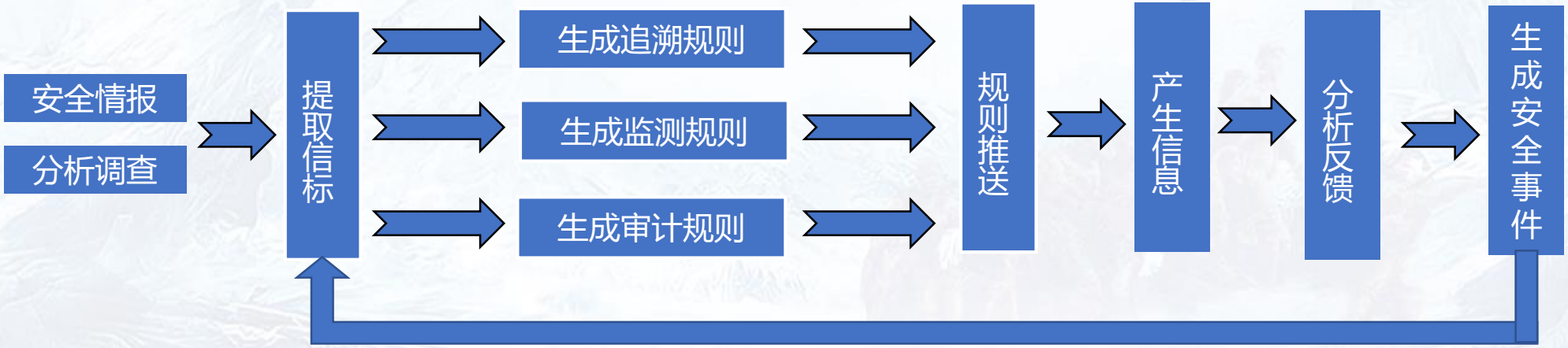
- 若存在，处置威胁；
- 若不存在，通知开发响应方案或联系外部专业应急团队处置

结合态势感知开展安全监测

按需监测

策略管理角色根据威胁情报流程，事件响应与处置流程、日常安全监测产生中获取信息，结合深度分析角色经验与态势感知情报系统系统提取信标，产生并下发规则至态势感知，按需监测结果终汇入态势感知系统进行综合分析

生成规则

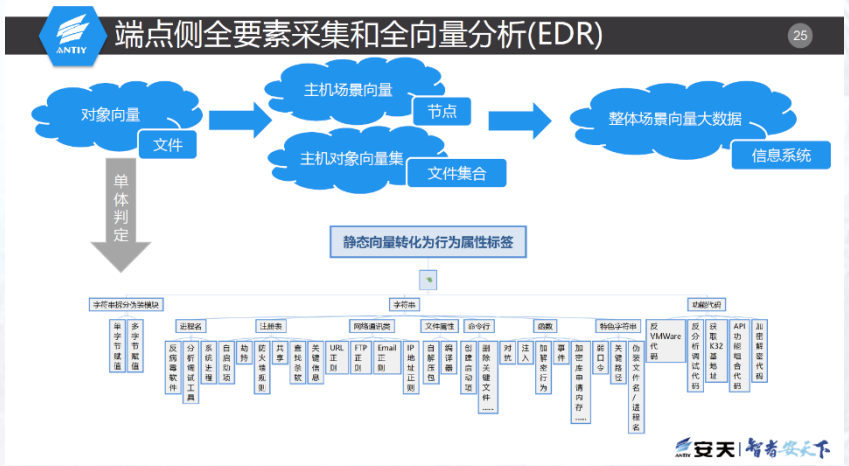


安全监测流程依赖态势感知采集能力与提供的分析功能

态势感知平台对安全分析人员配备多种安全分析功能

- 统计分析功能：数据层面特征分析、数据趋势分析
- 可视化分析功能：与实际网络地形对应，直观清晰呈现分析过程
- 交互式分析功能：分析过程与结果自由切换与对应，搜索、过滤、关联、聚合多种分析方式相互组合

态势感知提供的分析功能



终端、网络侧信息采集

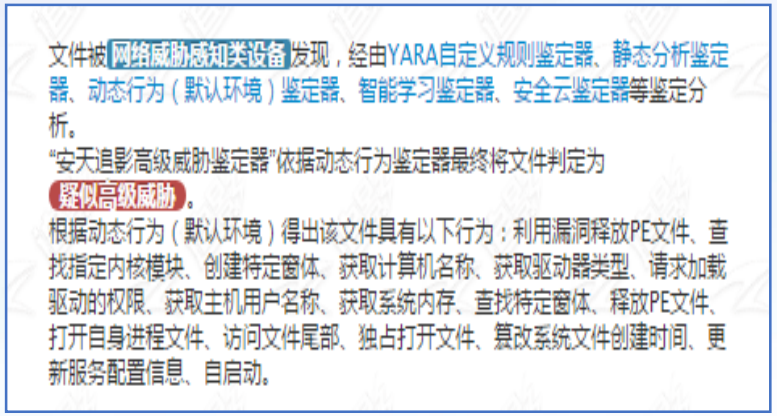
利用态势感知提供的深度威胁分析功能

可疑威胁分析：根据告警信息，结合对关键信标向量进行查看，逆向分析可疑文件与关联分析C&C等。

资产信息分析：查看可疑资产注册表、进程、服务等信息，查看端口开发、数据执行保护(DEP)等配置信息。

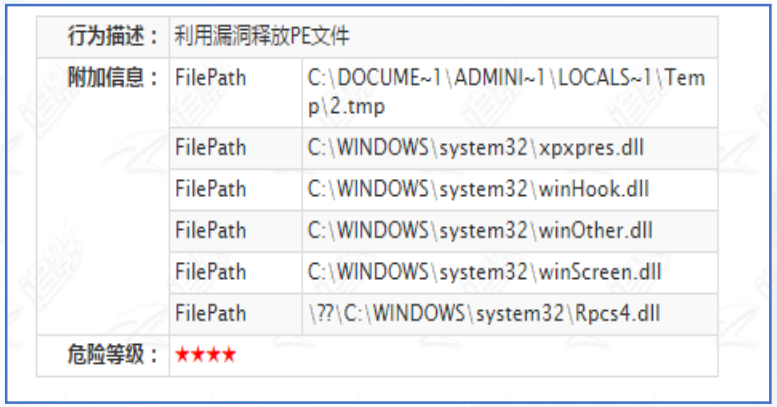
漏洞利用分析：利用配置表与漏洞表匹配查看有关漏洞，关联APT组织历史漏洞利用信息。

异常行为分析：查看NSA/CSS对应阶段，查看原始日志并结合威胁情报查询接口进行异常行为分析。



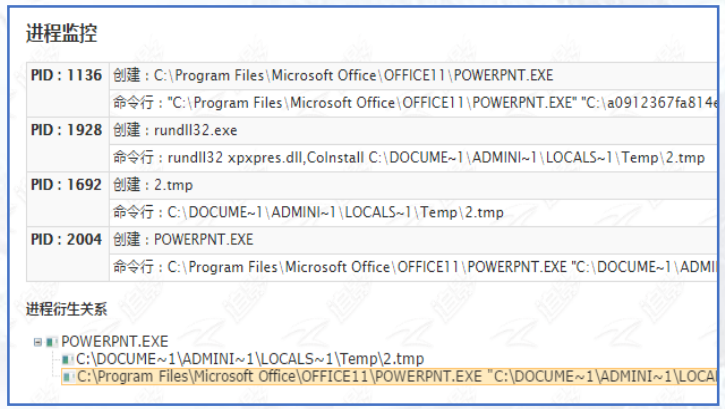
可疑威胁分析

资产信息分析



行为描述：	利用漏洞释放PE文件	
附加信息：	FilePath	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\2.tmp
	FilePath	C:\WINDOWS\system32\xpxpres.dll
	FilePath	C:\WINDOWS\system32\winHook.dll
	FilePath	C:\WINDOWS\system32\winOther.dll
	FilePath	C:\WINDOWS\system32\winScreen.dll
	FilePath	\??\C:\WINDOWS\system32\Rpcs4.dll
危险等级：	★★★★	

漏洞利用分析



异常行为分析

态势感知协同事件响应与处置流程

事件响应与处置

事件管理角色

- 启动事件处置流程；维护态势感知事件管理表

响应方案管理角色

- 根据态势感知告警信息匹配方案库中处置方案；通知方案开发角色开发处置方案；将维护态势感知方案库

方案开发角色

- 开发处置方案与配套处置工具；协助在测试环境中对测试方案

注：由于该角色存在专家级能力要求，建议由外部人员承担

取证分析角色

- 利用安天拓痕处置工具或人工方式进行固证，并对证据进行分析

注：由于该角色存在专家级能力要求，建议由外部人员承担

系统管理角色

- 结合态势感知与接收方案开展处置

安全角色配置

态势感知协同事件响应与处置

处置方案

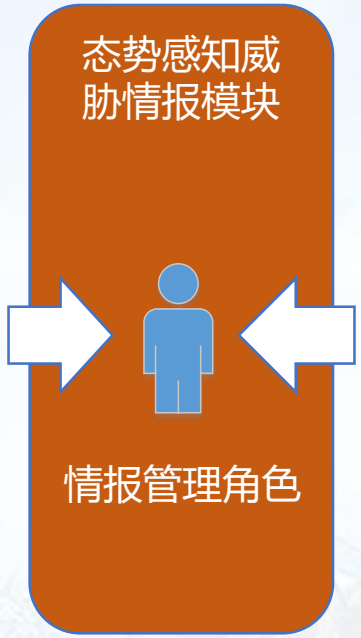
处置方案应根据知识情报、人工经验与告警信息开发，并开发配套处置工具；应在测试环境测试；应录入态势感知，通过审核后正式录入方案库。

针对攻击不同威胁，方案中覆盖相应应急响应动作，如：

- 定点清除：后门植入、恶意代码下载/运行
- 阻断连接：后门植入、远程连接、加密传输
- 增强监控：远程连接、主机提取
- 应用加固：主机提权
- 文件深入分析：加密传输

驱动战术型态势感知的威胁情报流程

厂商赋能的情报



客户自有的情报

态势感知中威胁情报支撑多个流程运行

情报分析角色

- 通过主动采集、被动获取、厂商交换、客户自有情报获取情报
- 通过信誉度评定、情报分类、安全要素提取、开源情报综合分析生成情报

情报管理角色

- 将情报录入态势感知威胁情报系统

部分其他流程角色

- 深度威胁分析角色：发现未知威胁、深入分析已知告警、深度分析可疑文件
- 策略管理角色：生成按需监测规则
- 配置开发角色：基础网络架构薄弱点加固的策略参考
- 漏洞管理角色：根据情报信息发现存在漏洞的资产
- 方案开发角色：评估潜在威胁，开发安全事件的处置方案

威胁情报驱动态势协同响应猎杀威胁运行实战化

第1步：情报管理角色将可机读威胁情报录入态势感知

1、情报管理角色接收可机读威胁情报

- ◆ 低级：哈希、域名、 URL等
- ◆ 中级：网络行为、主机行为等
- ◆ 高级：攻击者/组织信息等

2、情报管理角色将情报信息录入态势感知威胁情报系统

第2步：安全监测人员查看态势感知威胁告警

1、查看告警信息，若告警信息为可疑威胁，向深度威胁分析角色（建议由外部人员承担）下发分析任务

2、深度威胁分析角色利用威胁情报模块、人工经验与知识等进行分析，完成后反馈安全监测人员

3、安全监测人员判定威胁情况

威胁情报驱动态势感知，协同响应猎杀威胁运行实战化

第3步：安全监测角色将告警信息提交事件管理角色

1、安全监测角色确认告警信息，如：

- ◆ 资产信息：软硬件信息、配置情况等
- ◆ 检测信息：检测规则、原始日志等
- ◆ 威胁信息：发起者、威胁行为、样本信息、C2等

2、安全监测角色通知事件管理角色启动事件处置与响应

3、事件管理角色更新安全事件表，通知响应方案管理角色

第4步：响应方案管理角色选择处置方案

1、响应方案管理角色利用告警信息匹配处置方案与配套工具

2、响应方案管理角色根据告警信息，完善处置方案中受害资产、处置人员、处置资产等信息，随配套工具下发相应系统管理角色。

注：若无法匹配处置方案，通知方案开发角色（建议由外部人员承担）进行开发或外部安全团队进行处置。

处置方案

威胁情报驱动态势感知，协同响应猎杀威胁运行实战化

第5步：系统管理角色处置威胁

1、系统管理角色根据处置方案需要，通知取证分析角色进行**固证与分析**，分析结果反馈系统管理角色

2、系统管理角色根据处置方案与配套工具处置威胁，如：

- 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、白名单更新、配置优化**等响应操作
- 联动**镇关**，实现**网络阻断**等响应操作
- 使用处置工具，实现威胁处置与猎杀

3、处置完成后，系统管理角色填写处置记录表单与取证分析结果，通知安全审计角色开展审计，完成后，反馈事件管理角色

第6步：事件管理角色关闭事件处置与响应流程

1、事件管理角色根据处置记录表单信息更新态势感知事件管理表，关闭事件处置与响应流程

2、事件管理角色将威胁信息、告警分析记录、处置记录表单、取证分析结果提交情报分析角色，进入情报分析流程

人机协同猎杀威胁

威胁情报驱动态势感知，协同响应猎杀威胁运行实战化

第7步：情报分析角色对响应过程信息进行分析

1、情报分析角色（建议由外部人员承担）对威胁信息、告警分析记录、处置记录表单、取证分析结果关联分析，生成可机读威胁情报与高阶威胁情报，并提交情报管理角色

- ◆ 威胁源信息：攻击者、攻击组织、来源IP、攻击装备等
- ◆ 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、攻击工具等
- ◆ 攻击目标信息：组织、行业、人员、设备等
- ◆ 关联事件报告：历史事件

第8步：情报管理角色将可机读威胁情报录入态势感知（转至第1步）

1、情报管理角色将可机读威胁情报作为客户自有情报录入态势感知，提升态势感知威胁捕获与威胁猎杀能力

- 攻击事件：“魔窟”勒索蠕虫事件
- 攻击利用装备：永恒之蓝（Eternalblue）
- 装备来源：影子经济人曝光的美方攻击装备（方程式组织）
- 影响平台：Windows系统
- IOC信息：

域名特征

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

样本HASH

F107A717F76F4F910AE9CB4DC5290594

DB349B97C37D22F5EA1D1841E3C89EB4

5BEF35496FCBDBE841C82F4D1AB8B7C2

……

魔窟事件情报信息

03 实战化运行能力持续提升

运行能力提升方向

参考NICE框架提升网空安全防御人员素质

结合内外部力量持续提升战术型态势感知运行能力

运行能力提升方向

安全运行

物理管理、资产管理 、配置管理 安全监测、日常巡检、事件管理、身份管理与访问控制、第三方人员管理、桌面安全、漏洞管理、补丁管理、数据保护、网络安全、网络可达、容灾备份、变更管理、态势感知、威胁情报、风险评估、安全审计与验证、安全培训、安全测试、安全开发、升级管理

运维

物理运维、资产运维、配置实施、监控与巡检、事件响应、身份与访问控制、第三方人员安全、漏洞确认补丁实施、升级管理、数据维护、网络运维、备份和恢复、变更维护、态势感知、审计、安全培训、测试运维

开发

开发流程规范、产品设计

产品测试、发布和部署

运行和维护（售后支持）

开发要求、项目管理

信息化建设

规划设计

开发

集成与采购

系统实施

测试验收

系统交付

结合NICE框架指导网空安全防御人员知识、技能与能力建设

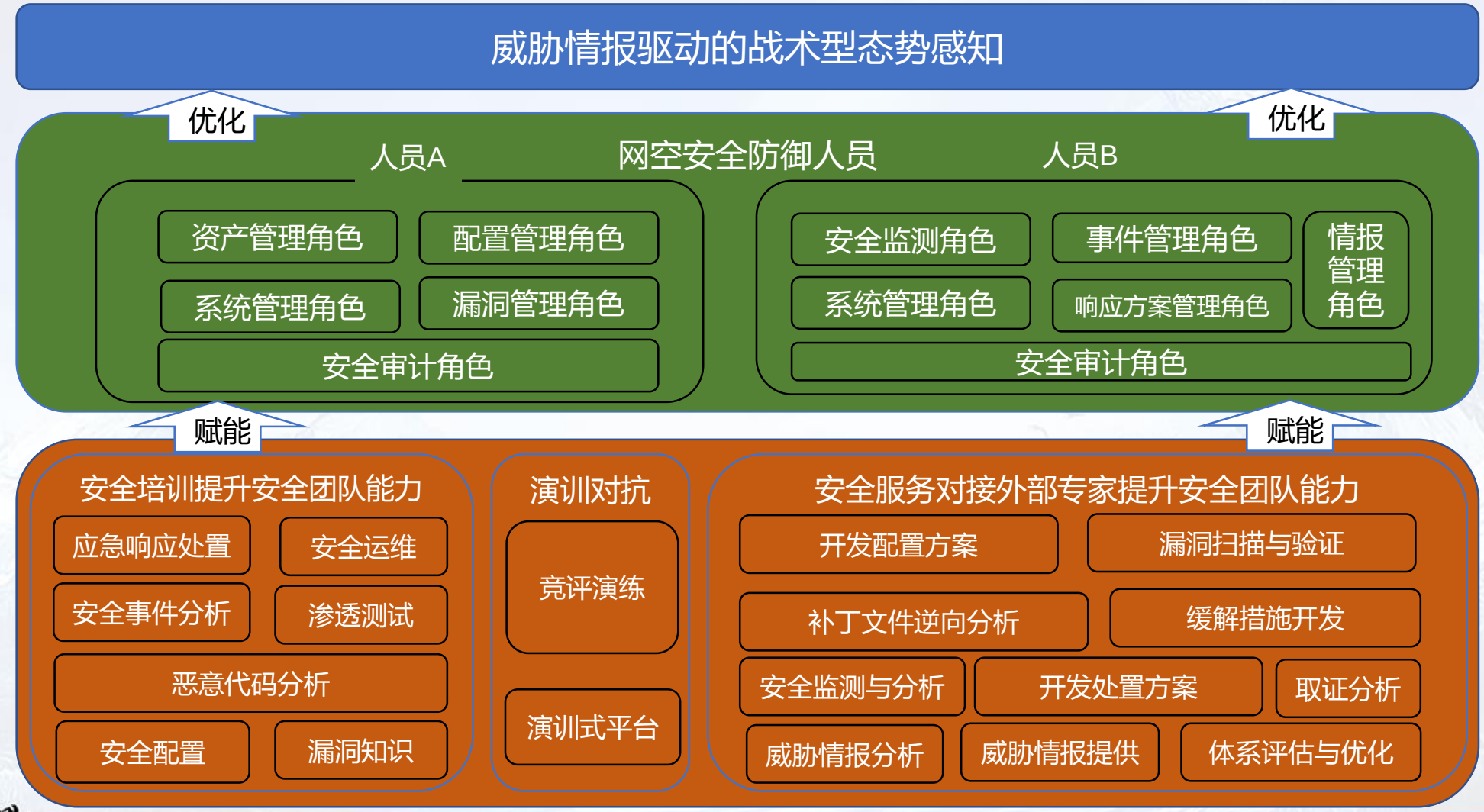
美国国家网空安全人才队伍框架是一个基本的参考资源，用于描述实现网空安全工作角色、职责及其所需的知识、技能和能力（KSA），可协助安全团队确定网空安全人才队伍需求，招募和聘用高技能的网空安全人才，指导网空安全人才队伍的教育和培训等

NICE框架

- 7大类别：由专业领域和工作角色组成
- 专业领域：32个专业领域，每个专业领域代表着网空安全和相关工作中功能类似的领域
- 工作角色：网空安全相关工作最详细的分组，其中包括执行该角色所需的属性列表（KSA）、该角色执行的任务

- 安全供应：概念化、设计、采购或构建安全信息技术系统，负责系统和/或网络开发的各个方面
- 运行和维护：提供必要的支持，管理和维护，以确保有效和高效的信息技术系统性能和安全性
- 监督和治理：宣传，以便组织机构可以有效和开展网络安全工作
- 保护和防御：识别、分析和减轻对内部信息技术系统和/或网络的威胁
- 分析：对传入的网络安全信息进行高度专业化的审查和评估，以确定其对情报的有用性
- 收集和操作：提供专门的拒绝和欺骗操作，收集可用于开发情报的网空安全信息
- 调查：调查与信息技术系统、网络和数字证据相关的网空安全事件或犯罪

人机协同战术型态势感知运行能力持续优化与提升



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

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