**需求**

全面掌握和实时监测本院网络资产的总体情况，知道风险在哪里，是什么样的风险，什么时候会发生风险，提供网络资产管理和安全监管的技术核心支撑平台，实现资产数据、脆弱性分布、安全威胁状况、安全防御状态等数据信息的全面深度掌控；在重大安全事件爆发时，能够明确了解到该事件对医院信息系统的影响面以及发展趋势。通过指挥决策指导安全运营人员对安全事件进行应急处置，并组织各部门组织配合协同，保证安全事件第一时间进行精准定位并处置。

每日针对异常流量、攻击日志进行分析，通过关联规则告警聚合发现安全事件。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | | 产品 | | 功能 | | 数量 | | 单位 | |
| 网络安全分析监测指挥平台 | | 安全分析管理与运营系统+监测运营服务 | | 1、平台综合功能：  1.1平台硬件：2U标准上架设备，含滑轨；CPU: ≥2颗10核 主频≥2.2 GHZ ；内存：≥ 256G（总容量）DDR4 ；硬盘1：≥2块960G SSD固态硬盘组成Raid 1；硬盘2：≥12\*4TB企业级SATA 3.5寸硬盘 总容量≥48T；电源：冗余双电源；网口：≥4\*GE电口; ≥2\*SPF+插槽；≥3\*USB3.0接口。  1.2平台软件基础功能：包含威胁检测、分析中心、响应中心、资产中心、统计报表、仪表板、系统管理、态势感知（综合安全态势、安全运营态势、外部威胁态势、内网威胁态势、威胁预警态势、攻击者态势、资产态势、资产风险态势、脆弱性态势）等功能，包含≥50个日志数据源的采集授权。  2、包含内网流量传感器1套（4G吞吐量），外网流量传感器1套（1G吞吐量）。  3、监测服务包含：（1）每日针对异常流量、攻击日志进行分析，通过关联规则告警聚合发现安全事件。（2）威胁情报实时升级。（3）出现重要规则更新时，及时推送消息以告知医院升级检测能力。（4）根据前期导入的资产，结合攻击流量以及最新公开漏洞情况，判断资产漏洞并形成资产漏洞管理清单，持续跟踪漏洞状态，出具漏洞整改建议，及时告知医院。（5）根据医院前期导入的资产，通过运营，协助医院在平台中完善资产信息。（6）运行状态监测，每周每月安全运营分析周报，月报。 | | 1 | | 套 | |
| 虚拟化主机安全 | | 虚拟主机安全防护：包含AV+FW+IPS+防暴力破解。 | | 45 | | 套 | |
| 服务器监测与防护探针 | | 功能包括内核探针和应用探针，实现系统权限及应用的控制与隔离，并持续对业务服务器上的流量和行为进行监控，有效抵御恶意程序执行，提权等已知未知APT攻击，实现提供整体的安全加固。 | | 20 | | 套 | |