态势感知项目说明

为提高我院的工作效率，我院已陆续完成HIS系统、电子病历系统、LIS、PACS等医院信息系统的建设工作。为响应国家、行业主管们有关信息安全政策法规要求，按照卫生行业等级保护工作指导意见，我院已将HIS系统定级为等级保护三级系统。

随着《网络安全法》的发布施行，国家网络安全保障制度和标准体系也在逐步完善，2018年6月，由公安部牵头制定的《网络安全等级保护条例》发布征求意见稿，与此同时，等级保护核心系列标准也基本修订完成，此外，针对关键信息基础设施的相关制度和标准也在加紧制定中。

2019年12月1日起，《信息安全技术 网络安全等级保护基本要求》（以下简称“等保2.0”）正式实施，标志等保工作进入到2.0阶段，为进一步落实等保2.0要求，完善网络安全体系、提升网络安全服务能力、保障业务系统正常稳定运行，需要对我院对网络安全态势感知ß系统进行建设。

本次态势感知项目需要满足如下要求：

满足《网络安全法》相关要求

“负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领 域的网络安全监测预警和信息通报制度， 并按照规定报送网络安全监测预警信息”；

“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件。”

满足《网络安全等级保护基本要求》

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

应在关键网络节点处检测和限制从内部发起的网络攻击行为；

应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；

当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警

外网数据采集

在外网核心交换旁路部署IDS采集探针，采集数据。

内网数据采集

内网部署采集代理服务器，收集IDS采集探针的数据。对数据进行预处理后，通过防火墙将数据发送至外网态势感知平台。

部署态势感知平台

态势感知平台集中汇总内、外网采集的数据，进行统一存储、分析、展示。可实现对已知、未知的新型网络攻击行为进行发现及预警。对恶意IP可实现自动下发策略给外网防火墙，阻断恶意IP地址。同时可下发策略给EDR，实现对全网终端病毒的查杀防御。

总体提升医院的整体网络安全风险识别分析和监测预警处置能力，满足监管单位要求，能够实时、准确、及时的处置威胁，保证我院信息系统的健康、稳定运行。

为医院进行的决策提供有效的数据支撑，为新时代医疗保障事业高质量发展提供强有力的信息化支撑。

保证医院安全运营处置工作和安全设备状态监控工作能够被集中管控，能够实现防火墙、EDR、入侵检测等设备的联动、管控、自动封堵风险终端、策略的统一下发等，提高信息系统运维效率。

逐步完善医院信息安全运维管理体系，推动我院信息安全体系的全面建设。

深入贯彻落实国家、北京市及行业主管单位的信息安全政策法规要求，从管理和技术上保证各项信息安全措施的落地执行。