# 广医附属番禺中心医院态势感知平台及云防护系统升级续保服务

用户需求书

# **项目背景**

 根据等保2.0政策要求，我院于2021年采购了态势感知平台及云防护系统，现需采购这套系统的3年维保升级服务，以完成对医院日志数据、流量数据、风险告警数据的集中收集、解析及审计等要求；并完成对医院门户网站接入云防护清洗服务，实现按需静态防护，确保重大节日期间对网站可持续访问及防篡改的要求。

# **服务内容**

## **服务清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **功能介绍** | **数量（年）** | **品牌** | **备注** |
|  | 云防护 | 包括：Web应用安全防护、CC攻击防护、区域访问控制、网站一键关停、网站永久在线、安全防护报告、安全可视化大屏，同时提供远程人工7\*24小时运维以及应急响应服务； | 3 | 安恒 |  |
|  | 态势感知 | 1. 基于实时流数据为用户提供安全分析能力和风险告警及多维度可视化展示。为企业安全提供决策依据、提高企业信息安全的纵深防御能力。包含以下引擎和模块： 1、智能化威胁检测引擎 2、多维度攻击溯源引擎 3、场景化威胁感知引擎 4、集成化联动响应引擎 5、启发式威胁狩猎引擎 6、安全运营工作台模块 7、可视化模型编排引擎 8、多租户运营管理模块 9、重大活动保障模块

 10、资产管理模块。1. 提供大数据分析和计算能力，包括基础大数据计算模块和分布式事件处理模块。支持横向平滑扩展，可以通过增加硬件服务器数量的方式增加平台集群的计算处理性能。包含以下引擎 1、BaaS 大数据平台 2、CDPS 分布式复杂事件处理引擎
2. 1、内置威胁情报订阅模块的能力，帮助产品实现实时定位、预警、降噪以及分析威胁趋势； 2、支持在线和离线更新威胁情报数据； 3、支持在平台中在线查询情报(如IP/域名)，查询结果包括：威胁类型、情报来源、WHOIS、开放端口、关联情报、SSL证书、样本分析等多个维度的溯源结果； 4、威胁情报云端能力：提供海量的威胁情报数据、持续更新IP情报、域名情报、哈希情报、漏洞情报、APT情报、事件情报等
 | 3 | 安恒 | 特征库升级，系统故障处理维护服务。 |
|  | 态势感知 | AI版本迭代升级服务 | 3 | 安恒 | 支持AI“恒脑”对接及联动 |

## **服务期限**

服务期：3年。

## **服务要求**

1. 应提供包含但不限于以下维保服务内容：
* ▲软件升级服务：提供维保设备的版本升级、特征库的升级，软件系统的故障处理及原厂400技术支持。
1. ▲服务响应时间：维保设备如出现故障需要维护，由招标人以电话或短信、微信、QQ等方式通知中标人，中标人应7×24小时受理，30分钟内响应。若不能远程排障，中标人应委派熟手工程师到现场排除故障，并保证所派人员在通知发出后2小时内到达现场。