**网络安全设备特征库及软件升级服务项目需求**

基本情况：

医院在用的部分网络安全设备特征库和软件即将到期，需要采购相应的升级服务，从而确保信息系统等级保护测评要求，及医院信息网络环境的安全可靠，保障医院医疗服务的正常稳定运行。

技术参数：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务/货物名称** | **数量** | **单位** | **参数描述** | **技术要求** |
| 1 | 防火墙系统升级服务 | 3 | 台 | IPS+AV+URL特征库1年升级服务许可； | **服务需提供如下功能：** **1.侵防御特征库和恶意域名特征库升级功能**:通过分析网络流量，检测入侵(包括缓中区溢出攻击、木马、蠕虫等)，并通过一定的响应方式，实时地中止入侵行为，保护医院信息系统和网络架构免受侵害。  **2.反病毒特征库升级功能**:通过识别和处理病毒文件来保证网络安全，避免由病毒文件而引起的数据破坏、权限更改和系统崩溃等情况的发生  **3.URL远程查询升级功能**: 使用URL远程查询功能需要先加载URL远程查询组件包 |
| 2 | 入侵防御系统升级服务 | 2 | 台 | IPS特征库1年升级服务许可； | **服务需提供如下功能：**  **1.侵防御特征库和恶意域名特征库升级功能:**侵防御是一种安全机制，通过分析网络流量，检测入侵(包括缓中区溢出攻击、木马、蠕虫等)，并通过一定的响应方式，实时地中止入侵行为，保护医院信息系统和网络架构免受侵害。 |
| 3 | 漏洞扫描升级服务 | 1 | 台 | 漏洞扫描特征库升级服务1年 | **服务需提供如下功能：** **1.动态漏洞特征库升级服务**：标准化漏洞库：持续集成CVE、CNVD、NVD等权威漏洞库。 **2.风险矩阵服务：**基于CVSS评分、业务影响、漏洞可利用性（如ExploitDB数据）生成风险矩阵 |
| 4 | 日志审计升级服务 | 1 | 台 | 日志审计扩容升级服务 | **服务需提供如下功能： 1.日志分析功能：**对全面支持通过Syslog、Agent、FTP、SFTP、TCP、SNMP、Trap、Kafka、WMI、HTTP等方式对院内网络安全设备、交换设备、路由设备、操作系统、应用系统、数据库等资产所产生的日志信息进行收集。 |
| 5 | 技术支持服务 | 1 | 项 | 技术支持服务 | **服务须提供如下功能：** 针对于医院HiSec联防方案配套的安全运维与响应服务。包括但不限于：特征库配置与调优、安全事件分析研判、攻击溯源深度支持、应急处置指导、定期安全态势报告及必要的现场技术支持等。 |