**南方科技大学医院网络安全加固项目**

**用户需求书**

## 项目背景

本项目要求：（1）利用主动拨测技术，发送检测任务，精确定位链路故障位置，减少定位所需时间。（2）深入探测资产细节，通过技术探测手段，获取详尽资产指标。包括域名资产对应的IP资产、IP资产上开放的业务端口、端口上运营的服务应用，并可通过应用指纹、web指纹精确识别应用组件资产的详细版本。精确的版本信息可以和1day漏洞情报等威胁情报进行高效匹配，在充分揭示系统脆弱性的同时，尽可能降低误报率和漏报率，减少对安全运营工作的不利影响。（3）内、外网打通通信链路后，由于外网相对安全风险较高，而内网的业务重要性较高，因此必须要采取一定的隔离措施，来限制外网对内网的访问，特别控制从外网交换到内网的数据，需要对数据进行深入检查，对攻击数据包，或者病毒进行过滤。（4）作为信息系统核心的数据库管理系统,保存着大量敏感信息，需要采取有效措施防止非法用户的访问。（5）提升医院敏感数据保护能力，有效防止敏感数据被窃取、盗用、违规使用，对敏感数据的流转实现安全保护，提升敏感数据防泄漏能力，提升数据流通访问过程的安全管理能力。（6）面对攻击者的访问，医院需要对APT组织攻击及0day漏洞等未知威胁攻击进行有效检测与发现。

## 项目建设清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **建设内容** | **详细技术要求** | **数量** |
| 1 | 网络应用监控分析系统 | 硬件平台，标准2U机架式设备；处理性能1Gbps；硬盘4T，4\*RJ45，600W单电源；流量处理能力：1G；对所有业务应用的网络通讯数据实时分析，实现对业务网络访问行为和运行状态的全面态势感知，快速定位网络及应用访问故障；通过主动拨测的功能，模拟真实用户访问，感知真实用户的访问体验；通过远程控制拨测探针进行主动故障排查。 | 1台 |
| 2 | 资产威胁与漏洞管理系统 | 支持内外网资产管理与威胁探测（2000IP以内），Intel 至强八核十六线程E5-2620V4，2U机架，C612主板，2个千兆电口和不少于4个扩展插槽，售后服务期限36个月，包含三年漏洞库、指纹库版本升级。提供硬件（含系统软件）三年维保服务,包括故障判断、报修登记、设备修复、提供升级系统版本的服务,7x24小时电话咨询服务，5x8小时远程技术支持服务。 | 1套 |
| 3 | 防火墙 | 6个千兆电口，2个千兆光口，2U标准机架，网络吞吐率12Gbps，并发连接：800万，具备3年的防病毒、防攻击、上网行为管理、Web安全防护、威胁情报、系统升级服务。 | 2台 |
| 4 | 数据库防火墙 | 实现核心数据库的敏感数据访问控制，规范数据库运维管理、危险操作访问控制、数据库合规接入控制等数据内部权限控制系统，可以有效管控高权限管理人员的违规使用、恶意使用，有效防止隐私数据泄露。 | 1台 |
| 5 | 数据静态脱敏系统 | 数据静态脱敏系统针对系统开发中测试用数据，对敏感数据提供去隐私化处理，通过脱敏规则进行数据变形，漂白和替换，有效防止隐私/敏感数据的泄露。 | 1台 |
| 6 | 蜜罐 | 标准2U机架式设备，接口默认不少于4个千兆光口和8个千兆电口，扩展插槽不少于2个，设备硬盘不少于4T，内存不少于32G，双电源；支持混合探针模式，直连部署和探针部署两种模式同时运行，用于适应不同网络环境的部署；具备防逃逸技术。 | 1台 |