**南方科技大学医院网络安全服务项目**

**用户需求书**

## 项目背景

本项目要求：（1）通过对主机的暴露面梳理和持续威胁监测分析，可在第一时间精准发现服务器安全威胁及入侵事件，可提供服务器等保合规、勒索挖矿、弱口令及风险账号治理、恶意扫描、爆破登陆、提权、无文件攻击、Webshell/反弹shell、文件篡改、文件泄露、病毒横向扩散、补丁空窗期治理、软件漏洞等场景的统一解决与处置方案，并对原有终端管理系统进行续费维保。（2）原有终端管理系统已不满足现有终端数量，需新增终端管理系统。（3）建设终端集中管控平台，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过防病毒、漏洞管理、运维管控、基线合规检查、网络准入、终端审计、终端检测与响应（EDR）、终端数据防泄漏等安全功能，为业务终端提供体系化安全防护能力，并助力持续开展基于数字化指标的安全运营。（4）能够全面发现信息系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，能够快速定位风险类型、区域、严重程度，直观展示安全风险 ，能够在虚拟化环境、IPv6环境中部署和检测其脆弱性。（5）配合医院完成深圳市信息安全联合检查工作要求内容，提供信息安全联合检查中的各项服务，现场配合信息安全联合检查，保障医院在联合信息安全检查中的各项指标达到规定要求。

## 项目建设清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **建设内容** | **详细技术要求** | **数量** |
| 1 | 终端安全管理系统（续保） | 1. 【标准包服务】防病毒+补丁管理+主机防火墙+终端管控+移动存储+停服系统加固三年更新服务 | 1000个点 |
| 2 | 终端安全管理系统（新增） | 1. 【标准包三年】防病毒+补丁管理+主机防火墙+终端管控+移动存储+停服系统加固 含防病毒（不含第三方扩展引擎）、补丁管理、主机防火墙、终端管控、移动存储管理、Windows XP/7 停服系统加固功能。支持主流Windows PC客户端操作系统，默认包含三年更新服务。 | 1000个点 |
| 3 | 服务器安全管理系统 | 1. 服务器安全管理系统管理控制中心软件，可实现对客户端的统一运维管理、安全策略维护及全网安全日志分析、威胁溯源等。 2. 提供完整的服务器安全监测、防护和加固能力，包括资产管理、防病毒、微隔离、账号风险检测、安全基线、漏洞防护、入侵监测、webshell防护、系统防护、应用防护、网络防护等全功能模块，默认包含三年使用授权及升级维保服务。 | 150个点 |
| 4 | 漏洞扫描 | 1. 1U，含交流单电源，1\*RJ45串口，1\*GE管理口，4个10M/100M/1000M自适应以太网电口扫描口，1个网络扩展插槽，标准配置提供1路授权扫描端口；功能模块-Web应用扫描模块，对Web应用提供专业的漏洞、挂马检测和分析，授权许可-IP点授权（IP点数量），授权可扫描总数量不少于256个无限制范围的IP地址或域名。 | 1台 |
| 5 | 联合检查迎检服务 | 1. 配合医院完成深圳市信息安全联合检查工作要求内容，提供信息安全联合检查中的各项服务，现场配合信息安全联合检查，保障医院在联合信息安全检查中的各项指标达到规定要求。 | 1项 |