第十师北屯医院杀毒软件采购需求

**一、采购清单及采购需求**

|  |  |
| --- | --- |
| **功能项** | **详细描述** |
| 功能及授权 | 由一个控制中心统一管控，支持信创和非信创统一授权，提供不少于650点的终端杀毒模块、资产管理模块、漏洞管理模块、运维管控模块授权，提供不少于三年的维保服务。 |
| 风险洞察 | 支持对系统整体和单个终端进行安全风险评估，提供安全评分和等级 |
| 支持统计并折线图展示最近24小时、7天、30天的安全评分趋势 |
| ★评分标准按分数区间默认分为4个等级：高危、中危、低危、安全。支持用户自定义评分标准（提供产品界面截图并加盖公章） |
| ★按攻击面维度统计并展示已知资产、互联网暴露面资产的攻击点，攻击点包括：未安装的高危补丁、开放的高危端口、存在的弱口令账号、连接的外设资产（提供产品界面截图并加盖公章） |
| 支持按终端的风险等级统计核心资产、重要资产、普通资产和基础资产的占比 |
| 按安全威胁维度统计并分析系统内存在的安全威胁，分析维度包括：病毒风险、入侵检测、失陷检测 |
| ★支持统计并呈现最近24小时、7天、30天的不同来源的病毒入侵风险趋势折线图。病毒来源分为：本地或网络驱动器、Web、电子邮件、移动设备、其他来源。（提供产品界面截图并加盖公章） |
| 支持与上一周期的病毒入侵数量对比，并计算出环比。上一周期包括：前一次的24小时、7天、30天 |
| ★支持统计并呈现最近24小时、7天、30天的失陷检测事件趋势折线图。统计的事件类型包括：挖矿、勒索、APT攻击、僵尸网络、恶意软件等（提供产品界面截图并加盖公章） |
| 检测能力 | 提供自主知识产权的防病毒引擎 |
| 对所有平台均支持不少于三个杀毒引擎混合使用，包括云检测引擎、机器学习引擎、启发式引擎等，提供多引擎检测能力 |
| 提供对恶意代码有效检测与识别能力，对已知、未知病毒、病毒变种的全面检测、拦截和清除能力 |
| ★提供基于程序行为的独立恶意行为监控引擎，基于进程的操作行为和序列组合来应对未知威胁，包括：重复的系统文件，Hosets文件修改，可疑行为，新IE插件，IE设置修改，安全策略修改，动态链接库注入，Shell修改，新服务，系统文件修改，防火墙策略修改，系统进程修改，新启动程序等（提供产品界面截图并加盖公章） |
| ★具备机器学习检测技术，可检测可疑进程中或来自可移动存储、Web邮件等各渠道的文件中的新兴未知安全风险威胁。（提供产品界面截图并加盖公章） |
| 产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁； |
| 病毒策略 | 提供U盘扫描，可实时发现U盘里的病毒或恶意软件 |
| ★支持针对不同病毒类型针对性设置处置措施，处置措施包括“隔离”、“清除”、“删除”、“更名”、或“不予处理”等（提供产品界面截图并加盖公章） |
| ★支持设置病毒清除动作前备份文件（提供产品界面截图并加盖公章） |
| 支持扫描资源占用级别配置，包括高、中、低三个级别，满足在手动与预设扫描时低配置终端扫描防护性能要求，不影响生产办公，动态调整CPU占用以保证控制在CPU占用上限内，不影响生产办公 |
| ★具备爆发阻止功能，管理端可配置爆发阻止策略，封堵共享目录（提供产品界面截图并加盖公章） |
| 支持自定义SHA1、MD5本地威胁情报，黑名单可指定其动作包括（阻止，隔离，记录） |
| 支持设置扫描例外，包括自定义扫描例外文件目录、文件名、文件扩展名、间谍软件库 |
| 支持实时扫描模式下设置优先扫描用户态驱动 |
| ★支持配置客户端的隔离恢复权限，避免客户端可以随意恢复隔离的病毒文件，造成病毒感染和传播。 |
| ★具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新（提供产品界面截图并加盖公章） |
| 漏洞风险 | 支持对Windows、Linux系统及系统中的Web服务、数据库及其他应用的漏洞进行扫描，包括编号、漏洞名称、危险程度、CVE编号及修复参考建议； |
| 支持高价值漏洞、POC检测 |
| ★支持漏洞处置优先级(VPT)，依据漏洞风险，漏洞所在设备被攻击的可能性，漏洞所在资产的重要等级，漏洞可被利用的威胁情报等维度，筛选出立即修复，优先修复，稍后修复，延后修复，让补丁管理更有序从容。（提供产品界面截图并加盖公章） |
| 补丁管理 | 支持按照终端的维度统计终端补丁的安装情况，包括计算机名称，IP地址，连接状态，操作系统，已安装补丁，未安装补丁，对应的补丁信息。并支持导出统计报表。 |
| ★支持已安装补丁的卸载，和是否需要重启的状态统计（提供产品界面截图并加盖公章） |
| ★支持补丁包大文件的断点续传功能，减少误操作带来的问题（提供产品界面截图并加盖公章） |
| 资产管理 | 支持资产类型包括：主机，运行应用，安装软件，硬件，账号详情，账号登录历史，启动项，计划任务，端口 |
| 支持统计安装在终端上的数据库，Web服务，web站点，web应用，web框架，jar包和第三方中间件 |
| ★能够支持将windows客户端设置为探针，探测办公环境的windows设备（提供产品界面截图并加盖公章） |
| ★支持查看域账号和本地账号的账号详情（上次密码修改时间，密码有效期，账号分组），并支持按主机和时间范围查询（提供产品界面截图并加盖公章） |
| 弱口令检测 | 支持内置弱口令库，检测终端系统本地帐号中存在弱口令的账号 |
| 支持用户上传自定义的弱口令库，实时关注关键账户，跟踪关键账户风险 |
| 远程桌面 | 支持管理员向指定终端发起远程桌面连接，连接权限具备操作模式和仅查看模式。终端用户具备调整操作权限的权力。 |
| ★支持超级管理员配置远程桌面的模式：强制连接、询问连接，强制连接将无需终端接受直接连接成功，适用于无人看守的场景。同时支持在开启强制/询问连接模式下，配置例外的客户端列表。 |
| ★管理员通过 web 控制台直接发起远程连接，无需本地下载远程桌面的相关插件，使用场景更加灵活 |
| 违规外联 | 支持配置多种外联探测方式：DNS，Ping，TCP，Http/Https |
| 支持记录违规外联行为所使用的网卡信息 |
| ★支持禁用代理服务器，同时支持配置允许使用的代理服务器白名单，支持以IP或域名的方式添加白名单（提供产品界面截图并加盖公章） |
| ★支持禁用DNS域名解析服务，同时支持配置允许使用的DNS服务器白名单（提供产品界面截图并加盖公章） |
| 支持对违规外联的终端执行断开网络、消息通知的处置措施 |
| 支持消息通知内容的自定义 |
| **服务名称** | **服务内容** |
| 渗透测试服务 | 通过模拟黑客的攻击方法，检测医院业务应用系统的安全性，对程序可能存在的后门、陷阱、SQL注入、跨站漏洞、输入输出注入风险进行有效的加固封堵。 |
| 配合监管部门开展安全检查服务 | 协助制定安全自查计划并开展自查工作，在安全自查和安全整改以及国家相关部门的信息安全检查期间提供全过程的技术支持，帮助客户全面掌握信息安全现状，及时发现安全问题并进行完善性修复，切实提高信息安全保障水平，顺利通过安全检查工作。 |
| 安全培训服务 | 定期针对不同用户类型，设计有针对性的安全培训课程，协调有经验丰富的讲师授课，提升网络安全意识，课程内容包含但不限于：网络安全意识、安全开发、安全测试、实战技能培训等。 |

**二、合同履约期限**

签订合同后20日内完成全部采购内容实施上线工作。

**三、项目验收**

**1、设备到货验收**

本项目要求交货期为合同签订后20天，交货地点为采购人要求的地点。按采购需求文件规定的型号、技术参数、数量、产地，并根据制造商签发的《License授权书》进行现场验收，并由甲、乙双方签署验收报告。验收不合格，招标人有权更换产品或退货。

**2、项目验收**

本项目完成合同内约定货物到货安装调试，符合项目验收标准（安全设备特征库升级授权期限），经由采购人验收合格后，双方签署《验收报告》。

**3、售后服务及要求**

供货商应详细阐述在质量保证期内的技术支持和售后服务的内容、方式与范围。为确保售后服务的稳定性和快速响应，供货商须提供售后服务能力证明：包括售后服务机构、售后服务流程、售后服务响应程度等多方面证明。

设备运行过程中如果出现严重技术故障，中标方应保证对用户提供解决此类问题的紧急预案，使设备及时得到修复，并正常运行。

**四、投标须知**

**投标商需响应以下要求：**

1、为保证货物原厂正品，需提供厂商授权及售后服务承诺函；

2、保修期内提供提供7\*24小时售后服务，接到医院电话后30分钟响应，2小时内解决，特殊紧急情况6小时内需上门。承诺函并加盖投标单位公章。

3、投标总价包含货物到达采购人指定地点并能正常使用所需的一切费用，包括不限于包装费、运输费、装卸费、保险费、安装调试费、技术服务费、培训费以及保修费、税费等，采购人不再额外支付任何费用。承诺函并加盖投标单位公章。

4、如果投标单位提供的货物不能满足与现有终端安全管理系统兼容使用的，应当将其作为无效投标处理。承诺函并加盖投标单位公章。

5、供货商承诺其根据本合同提供的服务没有任何权利瑕疵，没有侵犯任何第三方权利，采购人在使用该服务的任何一部分时，免受第三方提出的侵犯其权利等任何权利主张。如果任何人对采购人使用该服务主张权利，由供货商负责处理一切纠纷及相关事宜。由此给采购人造成的损失，由供货商承担，其承担范围包括但不限于：赔偿费、律师费、诉讼费或仲裁费、鉴定费、调查取证费和其他一切相关的费用。

6、合同正式签订后，杀毒软件安装、调试、运行正常，且验收合格后五个工作日内支付合同总额的95%既：运维质保期结束后无息支付余款。

7、采购需求中技术参数均为参考指标，并不局限于某一品牌或规格型号。投标人在投标中可以选用替代指标，但这些替代技术指标要实质上相当于或优于采购需求中的要求。以上所供内容不少于参数内容，但可增加，以保证达到正常使用。