昌吉职业技术学院漏洞扫描服务项目采购需求

**一、项目信息**

项目名称：昌吉职业技术学院漏洞扫描维保服务项目

预算金额：人民币13500元

需求部门及经办人联系方式：信息中心 赵子钰 13779269615

单位联系人及联系方式：虞老师 0994-2331451 \13899634567

供应商基本要求：必须上传营业执照、法定代表人授权委托书原件(法定代表人本人投标时除外)及被授权人（或法定代表人）《居民身份证》原件或具有同等法律效力的证明文件（发证机关或公证机关出具的证明材料原件）、报价单、技术参数、售后服务承诺函及要求上传的其他证明资料并加盖投标人公章；以上资料必须以PDF格式做在一个文档里上传（不要分别上传），否则以“未按要求上传资料”审核为“不符合”。

**二、商务要求及说明**

1.完成时间：维保期1年。

2.付款方式：合同签订后60个日历工作日内一次性支付。

3.质保期：壹年。

4.项目地址：昌吉职业技术学院

5.其他说明：此采购项目为交钥匙项目，报价含发票税费、运输、安装、调试、培训指导及其它所有费用。

**三、履约验收**

（一）验收内容

1、提供1年的软件更新服务、产品保修服务、远程支持服务升级；

2、设备维保情况：提供1年的硬件保修服务，7×24小时技术支持服务，提供原厂保障漏洞扫描设备相关硬件设备维修保障，包括但不限于设备的开机状态、指示灯情况、硬件接口连接是否松动等，确保设备稳定开机率达到 100%。

3、提供原厂1年售后服务承诺原件。

4、提供现有设备原厂商授权函。

功能有效性：利用漏洞扫描工具扫描企业内部网络或系统，查看是否能准确检测出存在的漏洞并提供修复建议；确保各项功能正常有效。

（二）履约验收标准：

服务响应时间：在设备出现问题或软件出现故障时，维保服务提供商应在接到通知后的[1] 小时内做出响应，并在 [2] 小时内到达现场进行问题排查和解决，响应及时率达到95% 以上。

故障修复率：对于设备硬件故障，应确保一次性修复率达到 85% 以上，维修后的设备在一个月内不出现同一故障；软件故障修复率要求达到 90% 以上，保证系统稳定运行。

服务记录完整性：维保服务过程应有详细的服务记录，包括设备巡检记录、软件升级记录、故障维修记录等，记录内容应准确、完整，便于查阅和追溯，服务记录完整率达到 100%。

**四、售后服务**

1.售后服务方式

多渠道技术支持 ：构建全方位的技术支持体系，涵盖电话、邮件、在线客服以及现场服务等多种高效沟通方式。配备原厂专业且经验丰富的技术支持团队，确保用户在遭遇网络安全设备相关问题时，能够依据自身偏好与实际需求，迅速、便捷地与技术支持专家建立联系，获取精准、专业的技术咨询服务，切实保障业务连续性不受影响。

深度技术咨询：提供原厂的技术服务，支持团队成员均具备深厚的网络安全技术功底，对入侵防御、漏洞扫描等各类网络安全设备的架构、原理及应用场景有深刻的理解。在提供咨询服务过程中，能够迅速理解用户问题核心，运用专业知识与实践经验，提供切实可行的解决方案。

解决设备及相关软件故障

快速响应：建立严谨、高效的故障响应体系，针对设备运行过程中突发的各类故障，如设备宕机、系统崩溃、数据错误、功能异常等。在接到用户故障申报后，原厂的技术支持团队即刻启动应急响应流程，迅速调配资源，第一时间与用户取得联系，初步诊断故障类型与严重程度，确保在最短时间内开启故障修复工作。

精准故障修复：运用先进的故障诊断工具与方法，实现对故障的精准定位。结合丰富的实战经验与完善的故障修复预案，制定针对性、可操作性强的修复方案，高效实施修复操作，确保设备快速恢复正常运行状态。同时，对故障处理全过程进行详实记录与深入分析，总结经验教训，为用户打造坚如磐石的网络安全保障防线。

三、协助用户维护网络安全设备

维护支持 ：每季度派遣专业技术工程师上门，为用户提供引擎、漏洞扫描仪、防毒墙等设备执行深度巡检，细致检查设备硬件状态、系统参数配置、网络连接状况等关键指标；对各类网络安全软件开展功能测试，确保防护功能完备、响应及时、更新顺畅。同时，结合最新网络安全威胁态势，为用户实施软件升级服务，及时更新病毒特征库、漏洞补丁、防护策略等，全方位加固设备防护能力，保障系统时刻处于最佳运行工况。

专业配置指导：通过现场演示、远程协助、专题培训等多种形式，深入浅出地向用户传授设备配置技巧、策略制定原则、安全防护最佳实践等关键知识，引导用户深度参与设备管理与维护工作，提升用户自主运维能力与安全意识。在用户独立配置与操作设备过程中，提供实时在线的专家支持服务，及时纠正用户操作失误，解答技术疑问，确保用户精准、高效地掌控网络安全设备，使其充分发挥防护效能。

**附件1：昌吉职业技术学院采购报价单**

附件1

**昌吉职业技术学院采购报价单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 品名 | 规格型号 | 单位 | 数量 | 单价（元） | 金额（元） | 备注 |
| 1 | 漏洞扫描维保服务 | 绿盟 RSASNX3-HDBX | 年 | 1 | 13500 | 13500 | 原厂维保服务 |
| 合计 | | | | | | 13500 |  |

### **附件2：**

**详细技术参数一览表**

|  |  |  |
| --- | --- | --- |
| **序号** | **品名** | **技术参数** |
| 1 | 漏洞扫描维保 | 1. 提供现有设备原厂商授权函。 2. 支持检测的漏洞数大于330000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供CVE Compatible证书。（提供功能截图） 3. 品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。（提供功能截图） 4. 支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统，提供详细漏洞列表。（提供功能截图） 5. 支持扫描主流云主机机管理系统的安全漏洞，如：VMWareESX/ESXi、KVM、Xen，要求能够扫描大于5000条相关漏洞，并提供功能截图和支持的漏洞列表。 6. 支持扫描容器镜像存在的漏洞，支持扫描互联网上公开仓库中的镜像以及私有仓库中的镜像。支持对扫描出的漏洞提供取证性质的验证并输出报告，直观展示漏洞利用过程和危害性，（提供功能截图） 7. 支持通过在目标资产部署终端代理agent方式，实时精准获取资产信息，进一步完成漏洞分析扫描，（提供功能截图） 8. 支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测；（提供功能截图） 9. 支持智能端口挖掘，可以智能发现非默认端口启动的服务，（提供功能截图）   支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行，（提供功能截图） |