**响应文件**

**（正或副本）**

**项 目 名 称：**

**供应商名称：**

**日 期：**

1. **法人代表证明文件**

应答人名称：.

单位性质：.

地址：.

成立时间：.

经营期限：.

姓名：性别：年龄：职务：

系（应答人名称）的法定代表人。

特此证明

附：法定代表人身份证复印件（需同时提供正面及背面）

|  |  |
| --- | --- |
|  |  |

应答人：（盖单位章）

年月日

**二、营业执照**

**三、报价清单**

货币单位：人民币元

项目名称： 江苏有线盐城分公司堡垒机等项目

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **品牌及型号** | **数量** | **单价** | **合计** | **备注/说明** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| …… |  |  |  |  |  |

投标单位名称：（公章）

投标人代表签字：

说明：

1. 投标人须按照招标文件要求， 开具增值税专用发票。

1. 投标人须严格按照格式进行报价，不得对表格条目进行增删和改动。
2. 付款期限及方式：按合同约

附件

堡垒机等项目招标清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名 称** | **参数说明** | **数量** | **单位** |
| 1 | 堡垒机 | 性能参数：默认包含运维授权数：50，最大可扩展资产数：150，图形运维最大并发数：100，字符运维最大并发数：200。  硬件参数：规格：1U，内存大小：8G，硬盘容量：2T SATA，电源：单电源，接口：6千兆电口。  功能描述：.运维安全管理系统（堡垒机OSM），将运维人员离散维护主机及网络设备的行为统一到该平台进行，加强对系统安全以及运维的控制力。一方面通过集中运维，减少因离散操作导致的失误，提高工作效率，如新的安全策略在主机上的统一应用等；另一方面通过对所有用户在主机上的操作行为进行监控与记录，实时了解用户的操作行为，发现风险及时中止用户的操作，并记录下用户所有的操作行为，便于进行事后的审查与取证。  OSM-1000-B1150标准产品,每台含：  1套\* 运维安全管理系统软件  3年\* 产品质保;  3年\* 软件升级服务; | 1 | 台 |
| 2 | 杀毒软件及网络监控设备 | 性能参数：安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出，管理账号分权分域，总分平台级联控制.  PC:  周密预防：系统漏洞扫描，补丁修复管理、终端基线检查，资产盘点，资产主动发现，轻补丁漏洞免疫；  全面防护：文件实时监控、勒索诱饵防护、静态文件AI引擎、动态勒索行为AI引擎、勒索攻击对抗、无文件攻击防护、RDP二次认证、可信进程防护、关键目录加固  灵敏检测：恶意文件检测、暴力破解检测、网端联动杀毒（SIP、AC、AF、XDR）  深度检测：终端行为数据采集、（单品）高级威胁行为检测（IOA）、（单品）攻击进程链可视化展示（单品）威胁狩猎、内存马检测等  快速响应：文件急速隔离、终端一键隔离、感染文件修复、病毒处置响应、域名隔离、进程阻断、网端深度联动（与SIP、AC、AF、XDR）、全网威胁定位  简便运维：外设管控、违规外联检测、远程桌面、广告弹窗拦截（高级版）、屏幕水印、应用管控  服务器：  服务器全量版（主机安全）包含服务器侧所有能力，适用于主机安全专业保护场景  周密防护：系统漏洞扫描、补丁修复管理、终端基线检查、资产盘点、资产主动发现、轻补丁漏洞免疫、弱密码检测  全面防护：文件实时监控、勒索诱饵防护、静态文件AI引擎、动态勒索行为AI引擎、勒索攻击对抗、无文件攻击防护、RDP二次认证、SSH二次认证、可信进程防护、关键目录加固、Webshell防护、无文件攻击防护  灵敏检测：恶意文件检测、暴力破解检测、网端联动杀毒  深度检测：终端行为数据采集、（单品）高级威胁行为检测（IOA）、（单品）攻击进程链可视化展示（单品）威胁狩猎、内存马检测等  快速响应：文件急速隔离，终端一键隔离，感染文件修复，病毒处置响应，网端深度联动（SIP、AF、AC、XDR），全网威胁定位、主机流量采集 | 1 | 套 |
| 3 | 二级等保测评 | 智慧乡镇平台系统二级测评服务费 | 1 | 套 |