黄石市住房和城市更新局

机房运维和网络安全服务项目

遴 选 文 件

二○二四年九月

黄石市住房和城市更新局机房运维和网络安全服务项目遴选的公告

 依据《黄石市住房和城乡建设局招标和采购管理办法》，拟就黄石市住房和城市更新局机房运维和网络安全服务项目，采用公开遴选方式选定服务合作公司，诚邀符合条件的服务单位参与遴选，具体内容及要求如下：

1. **项目基本情况**

**1、项目名称：**黄石市住房和城市更新局机房运维和网络安全服务

**2、采购内容：**

黄石市住房和城市更新局机房运维（网络运维、网络安全运维）和网络安全服务（具体服务内容见附件）。

**3、控制价：**50万元/年（其中运维费25万元/年，网络安全服务费25万元/年，需在报价明细表里分项报价）。

**4、服务期限：**自合同签订之日起1年。本项目服务期实行“1+2”模式，1年服务期满后，经采购人考核合格，成交供应商可续签合同。续签实行一年一签，最多可续签2年。

**二、资格条件及要求**

1、具备《政府采购法》第二十二条第一款规定的条件，提供下列材料：
 （1）法人或者其他组织的营业执照等证明文件，如供应商是自然人的提供身份证明材料；
 （2）2021年-2023年任意一年的财务审计报告，依法缴纳税收和社会保障资金的相关材料；
 （3）参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明；
 （4）具备法律、行政法规规定的其他条件的证明材料。

2、未被列入“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn ）失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

**三、投标文件审查**

招标人依据《黄石市住房和城乡建设局招标和采购管理办法（试行）》（黄建办[2022]35号）要求组建遴选小组。开标现场由遴选小组对各投标人进行审查，只有审查合格的投标人方能进入比价或评分阶段。

**1.资格性审查**

依据遴选公告和有关法律的规定,对投标文件要求提供的资格证明文件进行审查，采用资格评审入围办法，以确定投标人是否具备有效的资格。在资格性检查时,如有投标人资质及证明文件不满足遴选文件要求或过期失效情况的，经遴选小组认定，视为非实质性响应，将视为无效投标。

**2.符合性审查**

遴选小组从投标人递交的投标文件的有效性、完整性和对遴选文件的响应程度进行审查。经审查，如有以下情况之一的，属于无效相应文件：

2.1递交投标文件投标人法定代表或其委托授权人身份与投标文件不符的；

2.2未按照遴选文件规定密封、签署、盖章的；

2.3附有招标人不能接受的条件的；

2.4对无效投标文件须由遴选小组进行复核确认，确认为无效投标文件的投标人不予进入评分阶段。

**四、评分办法**

1.投标单位符合性审查家数少于5家（不含5家）的，现场采用比价方式确定投标人，根据合理低价中标原则确定中标候选人。

合理低价计算方法为：以评审合格的投标人投标报价的平均值作为基准价，报价最接近基准价的投标人为中标人，若有两家及以上投标人报价与基准价差值相等，则按报价较低、企业业绩数量较多进行逐项比优，选定中标人。

2.投标单位符合性审查家数多余于5家（含5家）的，本次遴选采用综合评分法的方式确定中标人。由遴选小组分别对投标人的投标报价、商务部分、技术部分进行综合评分，其中：报价评分占30%，商务评分占70%，最终得分为各部分得分之和（得分保留两位小数），综合评分第一名为中标候选人。

具体评分细则见下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 评审因素 | 得分 | 评分标准 |
| 投标报价总分30分 | 投标报价 | 30 | 价格评分的计算方法如下：基准价为评审合格的投标人投标报价去掉一个最高价、一个最低价的平均值。投标人报价比评标基准价每高出1%扣0.75分，扣完为止；投标人报价比评标基准价每低1%扣0.5分，扣完为止；由此得出各投标人的投标报价得分（保留小数点后两位数字，第三位四舍五入）。投标价得分的计算方法：30-丨（评标基准价-投标人报价）/评标基准价丨×100×E；E取值0.75或0.5； |
| 商务部分 总分70分 | 类似业绩 | 8 | 投标人需提供近三年（2021年1月-至今）通过等保测评的系统运维或网络设备维保项目经验证明（须提供合同及相关平台或系统的等保证书材料），每提供一份得2分；本项最高分8分。 |
| 财务能力 | 2 | 投标人须提供2021-2023年任意一年的财务审计报告，提供者的2分。 |
| 文件编制 | 3 | 投标人文件编制完整，逐页有连续页码、有详细目录、目录与有关材料装订顺序对应清晰、查阅方便。优得3分，一般得1分，未提供页码或编制不清晰不得分。 |
| 企业资质 | 6 | 投标人需提供以下企业资质，每提供一个得2分，满分6分。ISO9001质量体系认证证书信息安全管理体系认证证书信息技术服务管理体系认证证书 |
| 项目人员 | 6 | 投入本项目运维服务工作的技术团队成员具有运维和网络安全相关资质证书的，每提供1人得2分，满分6分。（需提供证书复印件并加盖投标人公章） |
| 服务方案 | 15 | 投标人应根据本项目的性质、特点、运维需求及服务内容，合理规划、设计运维服务方案。根据方案的合理性、科学性、规范性，进行综合评分：1.服务方案合理性、科学性、可扩展性强，完全满足需求，得11-15分；2. 服务方案合理性、科学性、可扩展性整体一般，较好满足需求，得6-10分；3、服务方案合理性、科学性、可扩展性整体可行，基本满足需求，得1-5分；4、服务方案合理性、科学性、可扩展性较差，无法满足需求，不得分。 |
| 网络安全服务工具 | 20 | 1.投标人提供的运维工具，应满足招标文件中的系统功能需求，此项评分，满分为20分；2.若标注为“▲”项的技术条款有负偏离，每一项负偏离，扣2分；若其它项目有负偏离，每一项负偏离，扣1分。注：对于“▲”项参数，投标人应提供第三方检测报告或资质证明材料，并加盖投标人公章；未提供证明材料投标人，视为该项参数为负偏离。 |
| 实施方案 | 10 | 投标人应充分了解服务工具的使用需求，根据本项目的实际情况，编写服务工具的实施方案。1.符合性：实施方案需对网络环境和网络拓扑进行充分调研，详细描述出服务工具部署位置，并充分考虑到服务工具部署可能对业务造成的影响。 2.完整性：实施方案应涵盖所有服务工具；3.科学性：实施方案应涵盖突发应急措施；服务工具实施方案中对各项服务的内容和范围描述准确，对现有基础网络、安全防护，可达状态描述准确，对项目内涵有较深的理解，有详细的网络逻辑部署拓扑图，有详细可实行的实施方案，对上述采购需求响应性进行评分，完全响应以上三个维度采购需求，表诉清晰、设计合理、证明充分，1.实施方案符合性、完整性、科学性，完全满足需求，得8-10分；2. 实施方案符合性、完整性、科学性整体一般，较好满足需求，得5-7分；3、实施方案符合性、完整性、科学性整体可行，基本满足需求，得1-4分；4、实施方案符合性、完整性、科学性较差，无法满足需求不得分。 |

**五、付款方式**

1.机房运维费：2024年底前支付运维费用的60%，合同期满后支付运维费余额。

2.网络安全服务费：网络安全服务提供的设备和软件，安装调试完成，经验收合格后支付网络安全服务费。

**六、工作要求**

1.服务方驻场工程师须具备计算机相关专业本科及以上学历，2年以上相关维护工作经验；驻场工程师服从用户的上班时间安排，全身心投入到机房运维和网络安全服务工作中，禁止做其它无关的事项；驻场工程师需与服务方就用户方的运维服务签署保密协议。

2.如遇重大问题，服务方需派技术团队上门服务，及时处理机房运维和网络安全服务中发现的问题，确保机房良好运行和全局网络安全。出现问题服务方应及时作出响应，并在4小时内解决问题。如服务方所派技术人员在运维服务中，出现失误给用户方工作造成影响，用户方按次在100-1000元范围内扣除运维服务费用。

3.驻场工程师服从用户方工作安排。做好日常巡检和常规维护工作，并做好台账记录。驻场工程师必须保持稳定，未经用户方同意，服务方不得对驻场工程师进行调整；用户方对驻场工程师不满意的，服务方必须无条件调换。

**七、投标文件要求、递交地点及时间**

1.遴选响应文件包含内容：投标报价、行业资质（营业执照）、法人授权委托书、类似项目业绩证明材料、服务方案、服务承诺、投标资料真实性、合法性、完整性承诺等原件（复印件）加盖公章。投标文件装订成册（一套），送达时应密封完好，并加盖公章。参加开标的代表须带有效身份证件原件。

2.遴选响应文件投标截止时间为 2024年 9月24日14时30分，地点为黄石市下陆区广州路21号市直集中办公区2号楼 317办公室。我局将于2024年 9月24日14时30分组织现场开标。

3.遴选响应文件逾期送达或未送达指定地点的将被拒绝；未按要求密封遴选响应文件，视同无效投标。

4.联系人：桂先生   电话：0714-6228576

**八、合同格式及主要条款**

甲方：黄石市住房和城市更新局 （以下简称“甲方”）

乙方： （以下简称“乙方”）

根据《中华人民共和国民法典》和国家的其他有关规定，现甲乙双方经友好协商，本着平等、自愿、诚实、信任、互惠互利的原则，就乙方为甲方提供机房运维和网络安全服务，签订如下协议：

**一、服务内容**

黄石市住房和城市更新局机房网络运维、网络安全运维、网络安全服务（具体服务内容见附件）

**二、工作要求**

具体内容见第六条

**三、费用及付款方式**

1、合同费用：合同总额为人民币 （￥ ）

2、付款方式：机房运维费：2024年底前,乙方提供正规增值税普票,甲方支付运维费用的60%，即 元。合同期满后，甲方支付运维费余额,即 元。

网络安全服务费：网络安全服务提供的设备和软件，安装调试完成，经验收合格后,乙方提供正规增值税普票,甲方支付网络安全服务费,即 元。

3、乙方账户信息资料

（1）开户银行：

（2）开户名称：

（3）帐 号：

四、合同服务期

1.合同期限：合同签订之日起12个月（2024年 月 日-2025年 月 日）；

2.合同续签：合同满一年后经甲方对服务进行考核评估，考核通过后，报请甲方领导同意，甲乙双方可以续签合同。

五、甲方责任

1、积极配合乙方工作，提供相应的工作环境。

2、配合协调各部门、各业务系统厂商、各供应商开展网络安全的加固和整改。

3、按合同规定及时支付服务费用。

六、乙方责任

1、服从甲方工作安排 ，严格遵守甲方有关规定。

2、乙方按照合同规定的内容严格执行合同，组织人员履行合同的服务内容，包括机房网络运维、网络安全运维、网络安全运维服务等。

3、遵守国家保密法律、法规、规章制度，履行保密义务，不记录、不存储、不复制、不留存机房网络中的一切信息。不以任何方式泄露在维护工作中接触和知悉的秘密或敏感信息，不擅自发表、谈论工作中未公开的信息内容。

七、保密条款

乙方应严格遵守甲方有关信息保密规定，不得向甲方索取或通过其他方式带走信息系统安全、网络运行、业务办公的有关敏感信息，包括但不限于以下信息：

1、《中华人民共和国保守国家秘密法》明确的保密内容；

2、应用系统中的业务数据；

3、所有带密级的文件；

4、服务期配置参数和操作系统、数据库系统及应用系统用户名及密码；

5、其他可能影响网络运行、业务办公、信息系统安全的信息。

八、安全条款

1、乙方服务人员不得利用为甲方服务期间从事危害国家利益或甲方利益的活动，在服务过程中不得危害甲方业务系统、机房、网络等安全。

2、乙方技术人员现场服务应遵守甲方机房管理制度，不得将无关人员带入机房，不得擅自将属于甲方的任何物品带出。

3、甲方如遇到事故、故障等紧急情况需乙方立即提供服务时，乙方按照甲方的要求开展相关工作，事后由甲方补办相关手续，乙方应予以协助。

4、更改系统设置、系统重新安装、应用程序升级、涉及数据库及核心网络设备等重要操作，乙方技术人员应编制工作方案、应急预案和安全措施报甲方审核同意，做好数据备份和安全措施后，方可开始工作，并接受甲方运行维护部门人员对工作全过程进行监护。工作完工后，乙方应填写服务工作记录，详细记录检修维护内容、操作步骤、变更情况、处理结果等交甲方监护人员签字确认。

5、未经甲方允许，乙方在提供服务的过程中不得对与工作内容无关的设备、软件系统进行操作、更改。

6、为方便乙方工作，甲方向乙方提供相关系统的用户帐号和临时密码。乙方工作结束后，甲方即修改密码。

7、乙方应建立甲方机房网络运维、网络安全运维、网络安全服务范围内的运维服务档案。

九、对不可抗拒力的处理规定

1、协议签订任何一方因战争、火灾、水灾、台风、地震等国际惯例视作不可抗力受阻，而无法履行其协议义务时，本协议可解除或经协商将执行时间延长与上述事故持续相等日数。

2、因不可抗力致使无法履行部分义务或全部义务一方应立即以书面形式通知对方无法履行义务的理由，在不可抗力发生后七天内，提交回主管机构核发的证明以证实该不可抗力之发生，允许延期履行、部分履行或终止合同，并根据情况可部分或全部免予承担违约责任。

3、因不可抗力致使无法履行义务一方应于该不可抗力事件终止或排除后，立即以书面形式通知对方。

4、因不可抗力影响协议执行超过50天，双方应就协议的进一步执行与否进行磋商并达成一致。

十、解决合同纠纷的方式

合同执行期内，任何一方有严重违反合同责任的行为，在协商未果的情况下，对方有权提出终止合同，同时责任方对由此造成的损失进行经济赔偿。

双方应友好协商处理争议，若协商不成时，可向甲方住所地仲裁机关申请仲裁。

十一、其它

1、合同组成：由本合同书包括附件一：黄石市住房和城市更新局机房运维和网络安全服务内容、附件二：安全保密协议、附件三：驻场人员安全背景审查资料。

2、本合同自双方签字之日起生效，合同执行期内，甲乙双方均不得随意变更或解除合同。

3、在本合同执行期内甲乙双方共同签定的有关协议与本合同具有同等效力。

4、本合同一式陆份，甲乙双方各执叁份, 具有同等法律效力。

**法定代表人授权委托书**

本授权委托书声明：我 （姓名）系 （投标人）的法定代表人，现授权委托 （单位） (姓名)为我的代理人,以本公司的名义参加 （招标人）的 投标。授权委托人在开标、评标、合同遴选过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委托权，特此委托。

投标人（盖章）

法定代表人（盖章）

代理人：姓名： 性别： 年龄：

身份证号码： 职务：

授权委托日期： 年 月 日

黄石市住房和城市更新局

                              2024年 9 月 18 日

# 附件：

**黄石市住房和城市更新局机房运维和网络安全 服务要求**

## 一、局机房和终端设备运维

黄石市住房和城市更新局机房现有设备主要包括：服务器、交换机、路由器、精密空调、UPS等设备，还包括大楼视频监控系统、会议系统、广播系统、机房环境监控系统、电力配送系统等设备。

各个办公室的终端电脑共有230余台，打印机共有90余台。

另外，包括多家银行、财政、不动产登记、民政、市民之家等20多条网络专线。

**运维服务目录清单：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **服务大类** | **服务小类** | **服务分类** | **服务名称** | **服务内容** | **服务频度** | **交付方式** | **交付成果** |
| 硬件运维服务 | 网络运维服务 | 例行操作 | 网络设备巡检 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/月 | 现场 | 巡检日志 |
| 网络设备资产管理 | 对设备资产进行登记管理，完成资产报表 | 1次/半年 | 现场 | 资产报表 |
| 网络专线检查 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 响应支持 | 网络设备安装调试 | 根据用户需求，提供搬迁服务 | 1次/季度 | 现场 | 服务日志 |
| 网络故障处理 | 及时响应用户需求，排除网络故障 | 6天\*8小时 | 现场/远程 | 服务日志 |
| 服务器运维服务 | 例行操作 | 服务器巡检 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 服务器资产管理 | 对设备资产进行登记管理，完成资产报表 | 1次/半年 | 现场 | 资产报表 |
| 服务器清洁保养 | 根据用户要求定期对设备进行清洁保养，完成保养日志 | 1次/年 | 现场 | 保养日志 |
| 备份一体机巡检 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 服务器系统故障处理 | 及时响应用户需求，处理服务器故障 | 6天\*8小时 | 现场 | 服务日志 |
| 备份故障处理 | 及时响应用户需求，处理备份故障 | 6天\*8小时 | 现场 | 服务报告 |
| 桌面运维服务 | 例行操作 | 桌面终端巡检服务 | 按规定巡检周期对桌面设备检查，完成巡检报告 | 1次/半年 | 现场 | 巡检日志 |
| 桌面终端资产管理服务 | 对设备资产进行登记管理，完成资产报表 | 1次/半年 | 现场 | 资产报表 |
| 办公设备资产管理服务 | 对设备资产进行登记管理，完成资产报表 | 1次/季度 | 现场 | 资产报表 |
| 办公设备现场故障排除 | 设备故障排除，配件更换 | 1次/季度 | 现场/远程 | 服务派工单 |
| 其他硬件运维服务 | 例行操作 | 机房设备巡检（精密空调、UPS) | 按规定巡检周期对设备检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 机房环境监控 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 公共广播系统内容更新 | 响应用户请求，及时更新播放内容 | 6天\*8小时 | 现场 | 巡检日志 |
| 监控安防设备巡检 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/周 | 现场 | 巡检日志 |
| 机房配电检查 | 按规定巡检周期对设备检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 电子屏显示内容更新 | 响应用户请求，及时更新显示内容 | 6天\*8小时 | 现场 | 服务派工单 |
| 响应支持 | 公共广播系统及设备故障处理 | 响应用户请求，及时排除故障 | 6天\*8小时 | 现场/远程 | 服务派工单 |
| 机房设备故障处理 | 响应用户请求，及时排除故障 | 6天\*8小时 | 现场/远程 | 服务派工单 |
| 电子屏故障处理 | 响应用户请求，及时排除故障 | 6天\*8小时 | 现场/远程 | 服务派工单 |
| 监控安防维护 | 响应用户请求，及时排除故障 | 6天\*8小时 | 现场/远程 | 服务派工单 |
| 视频会议系统运维 | 响应支持 | 视频会议技术支持 | 响应用户请求，为视频会议顺利召开提供技术支持 | 6天\*8小时 | 现场 | 服务派工单 |
| 会议相关设备故障处理 | 响应用户请求，及时排除故障 | 6天\*8小时 | 现场 | 服务派工单 |
| 指挥中心大屏系统运维 | 例行操作 | 硬件维护管理 | 根据客户要求对指挥中心各相关设备进行管理和调试 | 6天\*8小时 | 现场 | 服务派工单 |
| 大屏系统维护工作 | 响应客户要求对业务系统进行投屏或分屏演示 | 6天\*8小时 | 现场 | 服务派工单 |
| 响应支持 | 指挥中心设备故障处理 | 响应用户请求，及时排除故障 | 6天\*8小时 | 现场 | 服务派工单 |

## 网络安全运维

目前黄石市住房和城市更新局数据中心机房现有网络安全设备主要包括：4台防火墙、2台vpn终端、数据库审计、两台备份服务器、堡垒机、网闸、态势感知、日志收集分析等设备。以及二号楼、四号楼共30多台交换机和路由器等网络设备。

**运维服务目录清单：**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **服务大类** | **服务小类** | **服务分类** | **服务名称** | **服务内容** | **服务频度** | **交付方式** | **交付成果** |
| 网络安全运维服务 | 网络安全巡检 | 网络安全设备巡检 | 例行巡检 | 按规定巡检周期对网络设备例行检查，完成巡检报告 | 1次/天 | 现场 | 巡检日志 |
| 网络设备资产管理 | 对设备资产进行登记管理，完成资产报表 | 1次/半年 | 现场 | 资产报表 |
| 网络安全检查 | 每天对防火墙、堡垒机、网闸、数据库审计、VPN等设备运行日志查看分析，排查异常 | 1次/天 | 现场 | 巡检日志 |
| 响应支持 | 网络安全设备安装调试 | 根据用户需求，提供安装、调试、搬迁等服务 | 按需 | 现场 | 服务日志 |
| 网络安全故障处理 | 及时响应用户需求，排除网络安全故障，及时排除网络安全风险 | 6天\*8小时 | 现场 | 服务派工单 |
| 网络异常处理 | 及时分析异常情况，做好网络安全防护策略，消除安全隐患 | 6天\*8小时 | 现场 | 巡检日志 |
| 网络安全监测 | 例行操作 | 态势感知 | 实时监测网络攻击，分析网络安全风险，并进行整改处置 | 6天\*8小时 | 现场 | 网络安全威胁分析报告 |
| 日志审计和分析 | 实时对各设备及系统的警报信息进行分析，及时发现安全隐患 | 6天\*8小时 | 现场 | 日志收集分析报告 |
| 漏洞扫描 | 利用现有漏扫设备针对网络设备，安全设备，服务器和业务系统进行漏洞扫描，并出具漏洞扫描报告。 | 1次/月 | 现场 | 漏洞分析报告 |
| 渗透测试服务 | 针对局主要业务系统进行模拟攻击，发现核心业务的风险，消除潜在威胁 | 1个业务系统/年 | 现场 | 渗透测试报告 |
| 响应支持 | 安全隐患处理 | 根据网络安全监测报告、网络安全威胁分析报告、日志收集分析报告发现的安全隐患，找出漏洞原因，并提出整改意见，处理安全隐患 | 按需 | 现场 | 整改意见报告 |
| 安全加固 | 例行操作 | 漏洞修复 | 根据日常巡检对系统漏洞进行补丁修复，督促软件公司对业务系统及数据库进行修复 | 6天\*8小时 | 现场 | 服务派工单 |
| 策略加固 | 对网络安全设备策略进行优化加固 | 6天\*8小时 | 现场 | 服务派工单 |
| 病毒防护 | 办公电脑及服务器防病毒软件的安装，病毒库更新 | 6天\*8小时 | 现场 | 服务派工单 |
| 响应支持 | 紧急修复 | 发生紧急网络攻击事件时，对攻击行为进行阻断，及时查杀病毒和修复补丁 | 7\*24小时 | 现场和远程 | 服务派工单 |
| 备份与恢复 | 例行操作 | 数据备份检查 | 正确配置备份一体机备份策略，检查备份数据备份是否正常 | 6天\*8小时 | 现场 | 巡检日志 |
| 响应支持 | 数据恢复 | 数据出现异常时，能对业务系统数据及时恢复 | 6天\*8小时 | 现场 | 服务派工单 |
| 网络安全应急响应 | 例行操作 | 编制应急预案 | 编制网络安全预案，配合客户进行网络安全攻防演练，及时发现问题并进行整改 | 6天\*8小时 | 现场 | 服务派工单 |
| 应急响应 | 应急支持 | 响应用户请求，及时处理阻断攻击，处理恶意程序和信息破坏事件，清除网络入侵，进行网络安全加固 | 6天\*8小时 | 现场 | 及时报告处置安全事故 |
| 原厂服务 | 例行操作 | 护网服务 | 在护网期间，原厂工程师到现场提供网络保障和技术支持服务 | 5天/年，护网服务时间段由业主选择 | 现场 | 网络安全护网防守报告 |
| 例行操作 | 重保服务 | 重大活动期间，网络安全7\*24小时值守，原厂工程师驻场技术支持 | 7天/年，重保服务，时间段由业主选择 | 现场 | 重大活动网络安全服务报告 |
| 网络安全培训 | 例行操作 | 网络安全宣传 | 网络安全宣传周期间根据上级要求进行网络安全活动宣传 | 1次/年 | 现场 | 活动宣传记录 |
| 信息安全培训 | 对客户、相关技术及系统运维人员进行信息安全培训 | 1次/年 | 现场 | 培训方案、培训报告 |

## 三、网络安全服务

### 3.1、网络安全态势感知服务

在黄石市住房和城市更新局机房免费部署网络安全态势感知服务设备，通过运用威胁情报、文件虚拟执行、智能规则引擎、机器学习等技术，检测和发现内网高级网络攻击和新型网络攻击，涵盖：APT 攻击、勒索软件、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等高级攻击进行人工专业分析，发现网络流量中的安全风险，在对安全威胁和安全事件深度分析后，给出事件处置和整改建议。

设备技术要求：

|  |  |  |
| --- | --- | --- |
| 工具名称 | 数量 | 配置要求 |
| 网络安全态势感知系统 | 1套 | 1、所提供的服务工具需为国产化工具，≥6\*GE电口，≥4\*GE光口，≥1TB SATA 企业级硬盘； |
| 2、需包括网页漏洞利用检测、webshell上传检测、网络攻击检测、威胁情报检测功能，提供离线pcap包导入检测、基础旁路阻断和基础SSL解密功能和高级扩展功能模块（包括威胁感知，威胁狩猎，响应处置，态势大屏等高级功能）； |
| 3、支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs 等。 |
| 4、支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力 |
| 5、威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含： DNS 解析、TCP 流量、UDP 流量、WEB 访问、文件传输）等。 |
| 6、支持对任意线索的自定义拓线及溯源取证分析，支持以可视化分析画布形式展示拓线过程并支持结果快照导出；支持对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。 |
| 7、应用安全的细分维度包括：WEB 安全、数据库安全、中间件安全系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为设备安全等。 |
| 8、▲支持与云端威胁情报中心联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（需提供威胁情报官网链接、软件著作权等证明文件并加盖投标人公章） |
| 9、▲服务工具需具备海光CPU7000、5000、3000合作认证证书，（提供相关证明材料并加盖投标人公章） |
| 10、▲为保证工具能力，服务工具制造商应具备强大的漏洞发现能力和漏洞挖掘能力，需具备自主研发的漏洞响应平台，同时，在最近三年度国家信息安全漏洞共享平台（CNVD）支撑单位工作贡献排名中获得过前三名的成绩；（需提供漏洞响应平台官网链接、软件著作权等证明文件并加盖投标人公章） |
| 11、▲为保证服务质量，所提供的网络安全态势感知服务需由工具生产厂商提供原厂服务，投标人提供服务承诺函。 |

### 3.2、日志收集与分析服务

在黄石市住房和城市更新局机房免费部署日志收集与分析服务设备，实时不间断地将不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实时地对日志和事件信息进行标准化（归一化）、关联分析、行为分析，通过统一的仪表板和报告进行实时动态、可视化的呈现，协助安全管理人员迅速准确地识别安全事故，消除了管理员在多个控制台之间来回切换的烦恼，提高工作效率，降低工作强度。

设备技术要求：

|  |  |  |
| --- | --- | --- |
| 工具名称 | 数量 | 配置要求 |
| 日志收集与分析 | 1套 | 1、所提供的服务工具需为国产化工具，≥6个千兆电口，≥4个千兆光口，配置不少于2个扩展插槽，≥4TB硬盘。日志处理性能≥3000EPS，日志采集处理均值≥6000EPS；配置≥135个日志源授权。 |
| 2、支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；支持审计各种主机操作系统（包括Windows\Solaris\Linux\AIX\HP-UX\UNIX\ AS400）配置日志、运行日志、告警日志等；支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic等）配置日志、运行日志、告警日志等支持各种应用各种应用系统（邮件，Web，FTP，Telnet等）配置日志、运行日志、告警日志等；以及用户自己的业务系统的日志、事件、告警等安全信息。 |
| 3、▲系统日志审计平台内置等保大屏展示，等保大屏界面支持查看设备运行天数、日志源数量、原始日志数、关联事件数、告警总数、等保合规情况、本地最早日志产生时间、已保存日志天数、平均每天日志存储量、存储空间情况、日志源列表、登录失败用户分布、等信息。（需提供相关检测报告证明材料并加盖投标人公章） |
| 4、转发支持TCP、UDP协议，支持按照Syslog-NG标准及自有格式原始日志进行转发，可根据IP类型转发；支持范华日志转发，范华日志可根据字段（内置150字段，包含IP、设备类型、事件等级等，支持自定义添加字段）需求选择性转发。支持转发加密，转发时包含原始日志源IP地址，可与NGSOC、态势感知等产品进行数据对接。 |
| 5、支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示。 |
| 6、能够在世界地图和中国地图上实时定位事件源/目的IP地址（内网IP）的地理位置； |
| 7、▲支持通过机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成；（需提供相关检测报告证明材料并加盖投标人公章） |
| 8、支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图（世界地图、中国地图）、3D地球等形式的统计信息可视化展示，并可将统计结果保存为统计条件、仪表板和报表等。图表数据支持数据下钻。 |
| 9、支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告； |
| 10、▲系统内置安全知识库，包括事件库、案例库、应急预案库、日志采集配置库和端口库等，支持自定义增加安全知识内容。（需提供相关检测报告证明材料并加盖投标人公章） |
| 11、▲产品具有《信息技术产品安全测试证书》，未发现该产品中存在漏洞库中已知中、高风险漏洞。（需提供有效证明复印件并加盖公章并加盖投标人商公章） |
| 12、▲工具需具备中国网络安全审查技术认证与技术中心《网络关键设备和网络安全专用产品安全认证》及《中国国家安全产品认证证书》增强级认证，需提供相关证明文件并加盖投标人公章。 |
| 13、▲为保证服务质量，所提供的日志收集与分析服务需由工具生产厂商提供原厂服务，投标人提供服务承诺函。 |

### 3.3病毒库授权：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **服务类别** | **服务名称** | **服务内容** | **服务频度** | **交付方式** | **交付成果** |
| 病毒库授权 | 原厂软件授权 | 对住更局机房内的3台防火墙提供病毒库升级授权（单台防火墙授权有效期为一年） | 1次/年 | 现场/远程 | 系统授权到期时间 |

## 服务要求

1.总体要求

根据国家监管部门以及行业监管部门下发的关于行业信息安全技术指引，提炼指引中涉及到的重点安全要素，结合企业信息安全现状分析，制定相应的基线标准。

根据行业制定的标准对信息系统安全要求、漏洞、病毒等进行安全评估及差距分析，以评估系统现状与监管部门技术要求标准存在的差距。

除监管部门的要求外，当业内出现监管部门通报的重大安全事件时，运维单位会协助客户验证系统中是否存在爆发相同的安全事件及潜在因素，并协助客户解决问题。

2.驻场要求

承担运维服务的公司需组建运维服务团队，不少于3人的专业技术人员组成，驻场人员不少于1人，驻场工程师须具备计算机相关专业本科及以上学历，2年以上相关维护工作经验；驻场工程师服从用户的上班时间安排，在黄石市住房和城市更新局现场上班，全身心投入到机房运维和网络安全服务工作中，禁止做其它无关的事项；驻场工程师需与服务方就用户方的运维服务签署保密协议；如遇重大问题，承担运维服务的公司需派技术团队上门服务，及时处理运维中发现的问题，确保设备和网站的正常运行。如服务公司所派技术人员，不能完成运维服务工作，黄石市住房和城市更新局有权通知服务公司换人；如公司所派技术人员运维服务中，出现失误给黄石市住房和城市更新局工作造成影响，用户方按次在100-1000元范围内扣除运维服务费用。

3.运维目标

（1）保证黄石市住更局取得全市护网网络安全攻防演练优秀防守单位。

（2）不能出现特别重大的网络安全事件（客观因素除外），比如局网络大面积中断、主要业务系统瘫痪、重要业务数据泄露及损坏、敏感信息事件造成不良政治影响。