**采购包7-网络维修和安全防护服务**

**★一、商务要求**

1、服务期限：合同生效之日起12个月。

2、服务地点：用户指定地点。

3、采购资金的支付方式、时间、条件：

具体运维服务考核内容按三亚市公安局合同约定及业务单位下达的任务单，根据运维服务进度设置预付款、进度款、尾款比例进行支付。合同签订后15个工作日，采购人支付40%预付款，合同签订后6个月，根据服务考核情况，支付40%运维进度款，剩余款项在项目验收通过且按照三亚市财政局结算审核后的费用进行结算并支付。

4、验收要求：按招标文件和合同约定的内容以及国家、地方和行业的相关政策、法规实施。

5、其他要求

采购人根据业务需要，有权对中标后的办公网络及视频会议软硬件运维内容在签订服务合同之前进行调整，调整内容包括但不仅限于机房线路整理、配置交换机等，中标人必须无条件服从。

6、报价要求：本项目为包干制，应包括服务成本、法定税费和利润。由投标供应商根据招标文件要求自行测算投标报价；一经中标，报价总价作为中标供应商与采购人签定的合同金额，合同期限内不做调整。

★**二、技术要求【注：除2.2.2 安全保障服务内容和要求中服务工具作为技术评分项的性能指标外，供应商必须完全满足以下所有技术要求】**

1、采购清单

**1.1办公网络及视频会议软硬件清单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 运维对象 | 品牌型号 | 基本技术参数 | 单位 | 数量 | 验收时间 | 过保时间 |
|
| **1.1** | **三亚市公安局智能会议室配套设施运维** |  |  |  |  |  |  |
| **1.1.1** | **四楼第一会议室会议讨论与扩音系统** |  |  |  |  |  |  |
| 1 | 高集成数字会议系统主机 | ITC TS-0604M |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 2 | 高集成数字会议系统嵌入式讨论主席单元 | ITC TS-0624 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 3 | 高集成数字会议系统嵌入式讨论代表单元 | ITC TS-0624A |  | 台 | 22 | 2017-12-5 | 2019-12-5 |
| 4 | 高集成数字会议系统双音频主席单元接口盒 | ITC TS-0626 |  | 台 | 6 | 2017-12-5 | 2019-12-5 |
| 6 | 专业功放 | ITC TS-200PI |  | 台 | 2 | 2017-12-5 | 2019-12-5 |
| 7 | 高档会议天花喇叭（带分频器） | ITC TS-108R |  | 只 | 4 | 2017-12-5 | 2019-12-5 |
| 8 | 16路数字输出两编组USB录音实况调音台 | ITC TS-16P-2S |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 9 | 八进八出数字音频矩阵处理器 | ITC TS-P880 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 10 | UHF段液晶显示可调频真分集无线咪(双手持） | ITC T-521UH |  | 套 | 1 | 2017-12-5 | 2019-12-5 |
| 11 | 2通道反馈抑制器 | ITC TS-224 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 12 | 大功率电源时序器 | ITC TS-830 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| **1.1.2** | **四楼第一会议室无纸化会议系统** |  |  |  |  |  |  |
| 1 | 无纸化多媒体会议管理平台 | ITC TS-8300 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 2 | 无纸化会议终端软件 | ITC 无纸化会议终端软件 |  | 套 | 23 | 2017-12-5 | 2019-12-5 |
| 3 | 交互式多媒体无纸化会议终端 | ITC TS-8401A |  | 台 | 23 | 2017-12-5 | 2019-12-5 |
| 4 | 全数字多媒体会议控制主机 | ITC TS-8308 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 5 | 投影控制器 | 定制投影控制器 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 6 | 无线路由器 | H3C 无线路由 |  | 台 | 2 | 2017-12-5 | 2019-12-5 |
| **1.1.3** | **四楼第一会议室会议集中控制系统** |  |  |  |  |  |  |
| 1 | 网络中控主机 | ITC TS-9100D |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 2 | 10寸无线真彩色触摸屏 | 华为 16G\WIFI平板电脑 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 3 | 无线射频接收器 | ITC WS330 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 4 | 8键有线触摸防水墙上面板 | ITC TS-9109 |  | 个 | 1 | 2017-12-5 | 2019-12-5 |
| 5 | 8路串口分配器 | ITC TS-9232 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 6 | 8路手动、自动电源控制箱 | ITC TS-9101 |  | 台 | 3 | 2017-12-5 | 2019-12-5 |
| 7 | 红外发射棒 | ITC TS-9100D配带 |  | 根 | 8 | 2017-12-5 | 2019-12-5 |
| 8 | 无线路由器 | 华为 无线路由 |  | 个 | 2 | 2017-12-5 | 2019-12-5 |
| 9 | 编程软件 | ITC 按需编程 |  | 套 | 1 | 2017-12-5 | 2019-12-5 |
| **1.1.4** | **五楼第二会议室会议讨论与扩音系统** |  |  |  |  |  |  |
| 1 | UHF频段无线会议系统主机 | ITC TH-0590M |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 2 | UHF频段无线会议系统主席单元 | ITC TH-0591 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 3 | UHF频段无线会议系统代表单元 | ITC TH-0591A |  | 台 | 18 | 2017-12-5 | 2019-12-5 |
| 4 | UHF频段无线会议系统电池充电箱 | ITC TH-0595 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 5 | UHF频段无线会议系统专用锂电池 | ITC TH-0596 |  | 条 | 19 | 2017-12-5 | 2019-12-5 |
| 6 | UHF频段无线会议系统天线分配系统 | ITC TH-0597 |  | 个 | 1 | 2017-12-5 | 2019-12-5 |
| 7 | 专业功放 | ITC TS-500PI |  | 台 | 2 | 2017-12-5 | 2019-12-5 |
| 8 | 高档专业音箱300W | ITC TS-810 |  | 只 | 4 | 2017-12-5 | 2019-12-5 |
| 9 | 16路数字输出两编组USB录音实况调音台 | ITC TS-16P-2S |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 10 | 八进八出数字音频矩阵处理器 | ITC TS-P880 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 11 | UHF段液晶显示可调频真分集无线咪(双手持） | ITC T-521UH |  | 套 | 1 | 2017-12-5 | 2019-12-5 |
| 12 | 2通道反馈抑制器 | ITC TS-224 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 13 | 大功率电源时序器 | ITC TS-830 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| **1.1.5** | **五楼第二会议室会议集中控制系统** |  |  |  |  |  |  |
| 1 | 网络中控主机 | ITC TS-9100D |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 2 | 10寸无线真彩色触摸屏 | 华为 16G\WIFI平板电脑 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 3 | 无线射频接收器 | ITC WS330 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 4 | 8键有线触摸防水墙上面板 | ITC TS-9109 |  | 个 | 1 | 2017-12-5 | 2019-12-5 |
| 5 | 8路串口分配器 | ITC TS-9232 |  | 台 | 1 | 2017-12-5 | 2019-12-5 |
| 6 | 8路手动、自动电源控制箱 | ITC TS-9101 |  | 台 | 3 | 2017-12-5 | 2019-12-5 |
| 7 | 无线路由器 | 华为 无线路由 |  | 个 | 2 | 2017-12-5 | 2019-12-5 |
| 8 | 编程软件 | ITC 按需编程 |  | 套 | 1 | 2017-12-5 | 2019-12-5 |
| **1.1.6** | **三亚市公安局居住证制证一体机、拍照受理一体机等采购项目** |  |  |  |  |  |  |
| 1 | 多功能居住证制证一体机 | AG-FZ625 |  | 套 | 15 | 2019-10-21 | 2021-10-21 |
| 2 | 居民身份证自助拍照受理一体机 | XZ―FS21P |  | 台 | 17 | 2019-10-21 | 2021-10-21 |
| 3 | 熙卓居民身份证自助受理系统 V1.0 |  |  | 套 | 17 | 2019-10-21 | 2021-10-21 |
| **1.1.7** | **三亚市公安局执法办案中心设备采购合同** |  |  |  |  |  |  |
| **1.1.7.1** | **(一)入区登记** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 3 | 智能核验终端 | 天地伟业 TC-P820ZD-HY |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 4 | 手环读写卡器 | 天地伟业 TC-H607FK |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 5 | 指纹签章一体机 | 天地伟业 TC-P809Q-V2 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 6 | 全自动光盘刻印机 | 天地伟业 TC-P80SB |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 7 | 语音对讲主机 | 天地伟业NAS-8831V |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 8 | 办案自助终端 | 天地伟业 TC-P819ZD |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| **1.1.7.2** | **(二)人身安全检查、物品暂存、信息采集、尿检登记区** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 4 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 3 | 手环读写卡器 | 天地伟业 TC-H607FK |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 4 | 伤疤抓拍摄像机 | 天地伟业TC-NH9804S6-2MP-SD |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 5 | 指纹签章一体机 | 天地伟业 TC-P809Q-V2 |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 6 | 安检门 | 中科盾ME860 |  | 套 | 1 | 2021-9-23 | 2023-9-23 |
| 7 | 手持金属探测器 | 中科盾 MD3003b1 |  | 个 | 2 | 2021-9-23 | 2023-9-23 |
| 8 | 高拍仪 | 捷宇 V606 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 9 | 毒检管控终端 | 天地伟业 TC-P819ZD-DJ |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| **1.1.7.3** | **(三)候问室(按4间配置)、候问管理区** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 2 | 单目全景摄像机 | 天地伟业 TC-C8SMS |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 3 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 5 | 2021-9-23 | 2023-9-23 |
| 4 | 全景温湿度数码屏 | 天地伟业 TC-P819QW |  | 台 | 4 | 2021-9-23 | 2023-9-23 |
| 5 | 智能交互终端 | 天地伟业 TC-P811ZD |  | 台 | 4 | 2021-9-23 | 2023-9-23 |
| **1.1.7.4** | **(四)讯、询问室6间** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 12 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 3 | 室内高清智能全局球 | 天地伟业TC-A854D4-4K |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 4 | 智能审讯一体桌(左屏) | 天地伟业 TC-P819SZ |  | 台 | 4 | 2021-9-23 | 2023-9-23 |
| 5 | 智能审讯一体桌(右屏) | 天地伟业 TC-P819SZ |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 6 | 公安审讯主机 | 天地伟业 TC-I82HN |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 7 | 指纹签章一体机 | 天地伟业 TC-P809Q-V2 |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 8 | 示证展台 | 捷宇 V606 |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 9 | 全景温湿度数码屏 | 天地伟业 TC-P819QW |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 10 | 智能交互终端 | 天地伟业 TC-P811ZD |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 11 | 语音对讲分机 | 天地伟业NAS-8832V |  | 台 | 6 | 2021-9-23 | 2023-9-23 |
| 12 | 窗口对讲机 | 天地伟业 DWT-8805 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 13 | 生命体征检测椅 | 天地伟业 TC-P814 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| **1.1.7.5** | **(五)辨认室** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 5 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 3 | 辨认室特写球机 | 天地伟业 TC-NH9804S6-2MP |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 4 | 窗口对讲机 | 天地伟业 DWT-8805 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| **1.1.7.6** | **(六)走廊** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 4 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 4 | 2021-9-23 | 2023-9-23 |
| **1.1.7.7** | **(七)卫生间(按1间配置)** |  |  |  |  |  |  |
| 1 | 单目全景摄像机 | 天地伟业 TC-C85MS |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| **1.1.7.8** | **(八)手环定位系统** |  |  |  |  |  |  |
| 1 | 定位腕带(心率) | 天地伟业 TC-P806WH |  | 个 | 20 | 2021-9-23 | 2023-9-23 |
| 2 | 定位基站 | 天地伟业 TC-P806JZ |  | 台 | 25 | 2021-9-23 | 2023-9-23 |
| 3 | 定位引擎 | 天地伟业 TC-E801B-YO |  | 套 | 1 | 2021-9-23 | 2023-9-23 |
| 4 | 地图服务器 | 天地伟业 TC-S5148-DT |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 5 | 交换机 | 锐捷 |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| **1.1.7.9** | **中心机房** |  |  |  |  |  |  |
| 1 | 全景摄像机 | 天地伟业 TC-NH3204I |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 2 | 高保真拾音器 | 天地伟业 TC-H301TG-HZ |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 3 | 办案区管理模块 | 天地伟业 TC-H800R-GA |  | 套 | 1 | 2021-9-23 | 2023-9-23 |
| 4 | 应用服务器 | 天地伟业 TC-S5158-S2 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 5 | 地图3D模块(分局） | 天地伟业 TC-E801B-HJ |  | 套 | 1 | 2021-9-23 | 2023-9-23 |
| 6 | 流媒体服务器 | 天地伟业 TC-S9438 |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 7 | 数据中心服务器 | 天地伟业 TC-S5158-S2 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 8 | 即时通讯服务器 | 天地伟业 TC-S5158-S2 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 9 | 证据服务器 | 天地伟业 TC-U5224R-V3 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 10 | 48 盘位网络存储服务器 | 天地伟业 TC-U5248R-V4 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 11 | 6T 企业级硬盘 | 天地伟业 ST6000NM021A |  | 块 | 72 | 2021-9-23 | 2023-9-23 |
| 12 | 人脸识别主机 | 天地伟业 TC-S9A58-100L |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 13 | 对讲服务器 | 天地伟业 TC-S5144-S1 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 14 | 北斗校时服务器 | 天地伟业 TC-P818 |  | 台 | 1 | 2021-9-23 | 2023-9-23 |
| 15 | 强电控制器 | 天地伟业 TC-H610 |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| 16 | 网络交换机 | 华为 S1730S-L24T-MA |  | 台 | 5 | 2021-9-23 | 2023-9-23 |
| 17 | UPS 主机 | 科士达 YDC3315 |  | 台 | 2 | 2021-9-23 | 2023-9-23 |
| **1.1.7.10** | **门禁系统(交互终端人脸方式)** |  |  |  |  |  |  |
| 1 | 智能交互终端 | 天地伟业 TC-P811ZD |  | 台 | 6 | 2021-9-23 | 2023-9-23 |

**1.2安全保障服务清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | 单位 | 服务频率 |
| 1 | 边界安全防护及服务 | 年 | 1 |
| 2 | 运维安全和综合审计服务 | 年 | 1 |
| 3 | 网络安全威胁预警监控服务 | 年 | 1 |
| 4 | 业务全生命周期管控服务 | 年 | 1 |
| 5 | 主动防御体系建设服务 | 次/年 | 4 |
| 6 | 入网数字安全体检服务 | 次/年 | 4 |
| 7 | 渗透测试服务 | 次/年 | 2 |
| 8 | 网络安全加固服务 | 次/年 | 2 |
| 9 | 网站云监测 | 年 | 1 |
| 10 | 应急演练服务 | 次/年 | 1 |
| 11 | 网络安全驻点服务 | 年 | 1 |
| 12 | 特征库升级服务 | 年 | 1 |

**1.3其他运维服务清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 服务内容 | 单位 | 数量或工作量（人月） | **资质证书要求** |
| 1 | 运维驻场服务人员 网络通信保障服务 | 2名运维驻场服务人员；  服务地点：市局，各分局、各支队及各派出所； | 人月 | 2人\*12月=24人月 | **供应商在投标文件中提供2名人员的中级或以上职称证书复印件和2024年6月至今任意3个月在本单位缴纳的社保证明复印件加盖公章** |

**2、服务内容**

**2.1办公网络及视频会议软硬件运维服务**

根据公安局管辖范围及现有设备建设使用情况，中标单位负责电脑软硬件、服务器软硬件、公安内外网络以及其他网络、音频音响会议、机房环境动力等系统设备日常维修维护。

**2.1.1装备和人员资质要求**

中标单位要根据维修维护设备范围、主要维修维护项目及维修维护要求等情况，配备必要的人员（不少于4人，含项目经理和驻场运维人员）、备件、工具（含采购人通讯设备）及车辆。要求如下：

**（1）装备要求**

1）有箱式货车1辆（含）以上。

2）有维修维护作业机动车1辆（含）以上。

3）配备1 辆手动或者自动挡机动车，以及相应的通讯设备和智能化维修维护管理设备。

**（2）工作人员资质要求**

1）派驻1名项目经理具有本科（含）以上学历，具有计算机等级二级及以上证书。**（在投标文件中提供证书复印件和2024年6月至今任意三个月在本单位的社保缴纳证明加盖公章）**

2）中标单位签订合同时需确保配备维修维护技术人员不少于1个中级或以上运维驻场服务人员进行网络通信保障服务，大专学历（含）以上，工作态度端正、有责任心、口头和文字表达能力强，能够服从和配合采购人工作安排

3）按采购人需求配备服务队伍。项目团队人员需要能够胜任计算机、数据库类、网络类、电工类等设备的维修维护，其中，网络类不少于1人、计算机类不少于1人，人员可同时胜任多项工作，具有大专（含）以上学历，能够提供计算机、网络类等相关技能资格证书的；电工不少于1人，具有电工证书，有网络类、监控类、LED屏等设备的维修维护能力和经验；能够独立驾驶机动车不少于1人，具有C1或以上机动车驾驶资格证。（注：以上人员证书须在签订合同时提供，可1人多证）

**2.1.2工作内容**

中标单位按照采购人下达的任务和划定的范围负责各自区域范围内设备的日常巡检、维修维护及零星建设三类工作，具体如下：

**（1）日常巡检工作内容**

主要负责电脑软硬件、服务器软硬件、公安内外网络以及其他网络、音频音响会议、机房环境动力等系统软硬件，以及系统配套的供电设备设施、通讯设备设施及配套线缆、杆件、基础、管道、电缆井等的日常巡检和简易维护详见附表一，并将巡检工作结果按要求反馈给采购人。

**（2）维修维护工作内容**

各系统主要维修维护设备清单详见附表二（电脑、服务器、网络设备、视频会议、杆件、基础、管道、电缆井等附属设备在表中不再列出），并将维修维护工作结果按要求反馈给采购人。

**2.1.3工作要求**

**（1）日常巡检工作基本要求**

1）巡检工作按采购人下达的任务或划定的区域要求，以及设备构成和特点，结合设备常发故障等情况，制定详细的巡检计划报采购人审核后执行。

2）采购人可根据设备的故障率、常发故障情况和工作需要，调整各中标单位巡检频次或者针对单项设备进行专项巡检；以及根据重要活动及恶劣天气等情况，对主要路线和机房（中标后由采购方提供）选定中标单位进行针对性的设备巡检。

3）中标单位要对每次巡检工作内容进行详细的文字记录、拍照和录像记录，列出详细的巡检清单，并做好具体的巡检台帐，以备检查和抽查。

4）中标单位的专业巡检队伍中，应配备专用巡检工具及车辆。中标单位必须配备至少1辆箱式货车和1辆维修维护作业机动车用于到采购人指定地区维修工作。

5）中标单位必须于每月15日前将上月巡检报告，由巡检人员与项目经理签字后报采购人审核。

6）中标单位应按照巡检工作内容项目逐一开展巡检工作，不得有漏检、漏巡现象。对于巡检中发现的紧急情况（如服务器报警、网络异常、ups电池异常等）应当按照相关处置要求进行临时处理或简易处理，需产生费用的必须提前报告并请示采购人。

7）中标单位应具备维修电脑、服务器等设备能力，以及能恢复硬盘数据能力。

8）中标单位应在恶劣天气之后和节假日等重大活动前组织专门力量对机房设备、网络设备、ups、空调设备、通讯线路等设备进行巡检，并形成专项巡检报告，由巡检人员与项目经理签字后报采购人审核。

**（2）维修维护工作基本要求**

**1）维修维护质量要求**

A.计算机机房集中监控用户要求

B.《计算机场地安全要求》

C.《计算机站场地技术条件》GB2887-89

D.《工业企业通信接地设计规范》GBJ79-85

E.《安全防范工程程序与要求》 GA/T75-94

F.《智能建筑设计规范》(GB/T 50314－2000)

G.《低压配电设计规范》(GB 50054－95)

H.《中华人民共和国公共安全行业标准》(GA 247-2000)

**2）维修维护人员、设备要求**

中标单位要根据维修维护设备范围、主要维修维护项目及维修维护要求等情况，配备必要的专业维修维护备件、工具（含采购人通讯设备）及车辆。

中标单位的专业维修维护队伍白天(8时-20时）不得少于1人，可同时兼顾巡检工作，夜间(20时-次日8时）不得少于1人，可同时兼顾巡检工作，白天和夜间可根据设备故障情况报采购人同意后动态调整队伍数量，确保及时修复设备故障；在恶劣天气、重大安保工作等情况下，专业维修维护队伍数量同时在岗数量至少可增加到4组人。

配备专用维修维护工具及车辆用于日常巡检和维修维护工作，1 辆手动或者自动挡机动车派驻采购人，并保障所有车辆燃油或电力充足；配备至少2个信号机检修工具、4台维护手持电脑和通讯设备，并按维修维护人员数量（不少于4人）配备1人1套专用维修工具。

**3）维修维护质保要求**

所有更换设备质保期36个月，质保期内设备再次故障中标单位必须无条件修复，采购人不再支付维修维护费用。另外，新更换设备在质保期内因质量问题再次更换的，从再次更换日期起重新计算质保期36个月。

**4）其他要求**

A.服从采购人工作安排，按照规定的期限及时维修维护并保证工期。

B.搞好文明施工，安全施工。中标单位应遵守工程建设安全生产有关管理规定，严格按安全标准组织施工，采取必要的安全防护措施，消除事故隐患。由于中标单位措施不力造成事故的责任和因此发生的费用，由中标单位全部承担。

C.中标单位应派遣具有一定资质的维修维护人员进行维修作业，所有本项目维修维护人员应当报采购人备案登记和考核，中标单位未经采购人方同意不得随意变更维修维护人员。

D.中标单位应按采购人要求准备适量充足的常用配件（不少于3%），报采购人审核备案。

E.中标单位应对巡检及维修维护过程进行详细记录拍照或录像摄像等，形成充分的证据链，按照采购人要求定期及时报送维修维护相关资料。

F.维护过程中，中标单位应随时接受采购人的监督。

G.维护过程中，中标单位应遵守采购人的有关规定。

H.维护过程中，若采购人财产被中标单位人为损坏且确认后，中标单位应按现值赔偿或免费更换。

**2.1.4应急响应要求**

**（1）响应时间**

中标单位应做到全天候7\*24小时提供运维保障服务，对于故障抢修涉及的响应时间和故障处置时间的要求如下：

1)普通故障响应时间：普通故障在接到采购人抢修通知后，应在5分钟内做到响应，具有处理故障能力的维修人员到达故障服务现场的时间应不大于60-90分钟。具体为：工作日白天（8时至20时）的最大到达故障现场时间为60分钟，工作日夜间（20时至次日8时）、郊区乡镇最大到达故障现场时间为90分钟。

2)紧急故障响应时间：采购人要求的紧急事件，应即时做到响应，30分钟内到达故障现场。

**3）如遇到早、晚高峰期，路段积水等因素引起交通拥堵，应确保及时到达现场处置。**

**（2）故障恢复时间**

按故障严重程度分3级。

特别紧急（1级）故障：重大活动或者全局公安网络发生中断的，或者综合布线恢复时间在工作时间内（工作日8时至20时）不超过2小时，非工作时间内不超过4小时。（不可抗力因素除外）

紧急（2级）故障：部分分局或者派出所网络发生中断的，恢复时间在工作时间内（工作日8时至20时）不超过4小时，非工作时间内不超过6小时；采购人指定的网络类或者音响类外场设备发生故障的，恢复时间在工作时间内（工作日8时至20时）不超过2小时，非工作时间内不超过6小时；郊区乡镇故障恢复时间可适当放宽到8小时。（不可抗力因素除外）

一般（3级）故障：某个单位的某个办公室区域网络故障但未影响业务办理和办公的，恢复时间不超过24 小时；其他网络存在故障但不影响业务办理和办公的，恢复时间不超过48小时（不可抗力因素除外）。

2级以上故障（一个点位一个月内发生3次以上）除提交故障处置报告以外还应提交问题分析报告，深度分析故障产生的原因，并提出预防性改善建议。

如确因特殊原因无法在指定处置时间内修复故障的，需将故障原因、过渡方案等和恢复计划在故障发生后的8小时内向采购人书面上报，并在此期间积极制定和采取过渡方案，全力保证网络通畅。在故障修复期间，如需要其他运维单位配合的，应提前向采购人提出。

**（3）应急人员、设备和其他要求**

1）安排足够的应急抢修人员、车辆、工具、备品备件24小时值班待命，同时应确保车辆、工具和备品备件的充足与完好。

2）在节假日（元旦、春节、清明、五一、端午、中秋、十一等）、恶劣天气（台风、暴雨/雷电、高温等）和重大安保工作（由采购人指定）前及其期间，根据采购人的要求，进行驻点保障服务。同时，应提前安排人员做好应急抢修准备，并将应急抢修人员名单、联系方式等报采购人备案，必要时，赴指定地点驻场保障。

3）在气象预报即将发生台风、暴风雨或其他恶劣天气、节假日及重大交通保卫工作之前，对外场设备进行维护保养和维修巡检，重点检查外场设备运行情况、设备安装牢固性，网络是否正常，尽量避免和降低恶劣天气对外场设备的破坏，发现问题及时解决。

4）安排不少于1辆应急机动车在采购人进行驻场保障，负责系统后台设备的维修检测、联络、信息收集、数据统计等工作。

**附表一：日常巡检工作内容**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **巡检项目** | **巡检具体内容** | **备注** |
| **机房环境以及设备巡检内容** | 检查和测试动力环境集中监控系统 | 温度范围是否正常 |  |
| 湿度范围是否正常 |  |
| 烟雾情况是否正常 |  |
| 摄像头监控情况是否正常 |  |
| 水浸情况是否异常 |  |
| 门禁情况是否正常 |  |
| 三相电量监控是否正常 |  |
| 单相电量监控是否正常 |  |
| UPS监控是否正常 |  |
| 精密空调是否正常 |  |
| 区域漏水是否正常 |  |
| PDU是否正常 |  |
| 多路负载电流是否正常 |  |
| 配电开关是否正常 |  |
| 市电断电是否正常 |  |
| 蓄电池阻是否正常 |  |
| 普通空调是否正常 |  |
| **机房环境以及设备巡检内容** | 机房机柜 | 机柜基础是否稳固、机柜是否密封完好、  机柜内电缆走线、设备接线是否整齐。 |  |
| 柜门锁头是否完好及正常锁闭，  有无生锈无法正常开闭现象 |  |
| 机柜侧面手动警卫控制开关是否具备正常  手动控制功能，锁头有无生锈现象 |  |
| 柜内环境是否清洁干净，是否存在垃圾或动物残渣 |
|  | **巡检项目** | **巡检具体内容** | **备注** |
| **机房环境以及设备巡检内容** | 机房内  清洁 | 机房内是否干净、少尘、无悬浮颗粒 |  |
| 机房内是否积水 |  |
| 机房内是否有异味 |  |
| 检查机房内是否有蜘蛛网尘土 |  |
| 机房内是否有食物存放 |  |
| 机房视频监控线缆 | 线缆是否完好，有无破损和断裂现象 |  |
| 线缆是否有短路或漏电现象 |  |
| 线缆接头处是否铰接完好，有无短路漏电 |  |
| 线缆接头处及破损处是否采用热塑管套接 |  |
| 机房防火  设施 | 是否存在，是否有破损 |  |
| 是否过期，是否能正常使用 |  |
| 消防器材是否符合规范 |  |
| 机房的应急照明设施是否正常 |  |
| 网络、电话线缆线头 | 线缆是否完好，有无破损和断裂现象 |  |
| 线缆线头是否做详细标签标示 |  |
| 线缆接头处及破损处是否采用套接 |  |
|  | **巡检项目** | **巡检具体内容** | **备注** |
| **机房环境以及设备巡检内容** | 服务器  设备外观  检查 | 检查电源、光纤、网络连线是否稳固、  线缆有无过度折弯或破损 |  |
| 服务器运行的声音是否异常 |  |
| 检查各部件LED工作状态指示灯是否正常 |  |
| 服务器设备外表是否清洁、  风扇及空气过滤网是否积尘 |  |
| 空调设备  巡检 | 检查管路、阀门是否有掺水、漏水现象 |  |
| 检查冷水机组、泵、风机控制箱电气连接点是否有发热现象 |  |
| 注意电机、水泵、接触器等是否声音异常 |  |
| 检查电子水处理器运行是否正常，  并保持设备表面及地面干净整洁，无垃圾灰尘 |  |
|  | 机房视频  监控线缆 | 线缆是否完好，有无破损和断裂现象 |  |
| 线缆是否有短路或漏电现象 |  |
| 线缆接头处是否铰接完好，有无短路漏电 |  |
| 线缆接头处及破损处是否采用热塑管套接 |  |
|  | **巡检项目** | **巡检具体内容** | **备注** |
| **网络运行整体巡检内容** | 网络结构 | 网络拓扑是否异常，设计编写数据 |  |
| 网络拓扑分析，修改拓扑图，  优化网络结构，稳定数据传输 |  |
| 网络拓扑建议 |
| 网络属性 | 根据各个部门的业务需求，  增大网络带宽及优化网络链路类型 |  |
| 了解所有的链路信息，增加或减少链路的需求 |  |
| 二级网络 | 检查二级网络是否正常、通畅 |  |
| 检查二级网络延迟时间和异常 |  |
| 检查二级网络线路是否异常 |  |
| 三级网络 | 检查三级网络是否正常、通畅 |  |
| 检查三级网络延迟时间和异常 |  |
| 检查三级网络线路是否异常 |  |
| 互联网络 | 检查互联网络网络是否正常、通畅 |  |
| 检查互联网络网络延迟时间和异常 |  |
| 检查互联网络网络线路是否异常 |  |
| 其他专网  网络 | 检查其他专网网络是否正常、通畅 |  |
| 检查其他专网网络延迟时间和异常 |  |
| 检查其他专网网络线路是否异常 |  |
| **LED屏设备巡检内容** | LED屏显示内容 | LED屏显示内容是否正确，  内容是否按照正常顺序切换显示； |  |
| 显示内容是否完整及颜色是否正确 |  |
| LED屏有无非正常显示或花屏现象，  显示频率是否正确。 |  |
| LED屏线缆 | 线缆是否完好，有无破损和断裂现象 |  |
| 线缆是否有短路或漏电现象 |  |
| 线缆接头处是否铰接完好，有无短路漏电 |  |
| 线缆接头处及破损处是否采用热塑管套接 |  |
|  | **巡检项目** | **巡检具体内容** | **备注** |
| **视频会议系统设备巡检内容** | MCUR服务器 | 工作状态 |  |
| 网络状态 |  |
| 告警状态 |  |
| 会议终端 | 能否正常开机 |  |
| 能否进入系统 |  |
| 系统功能是否完整 |  |
| 视频输入、输出是否正常 |  |
| 音频输入、输出是否正常 |  |
| 网络通道是否正常 |  |
| 摄像机 | 是否有视频输出 |  |
| 镜头变焦、变倍状态 |  |
| 镜头左右、上下旋转状态 |  |
| 显示设备 | 能否正常开机 |  |
| VGA AV等输入状态 |  |
| 分辨率、切换、色彩等是否正常 |  |
| 调音台 | 音频输入状态 |  |
| 音频输出状态 |  |
| 音量调节状态 |  |
| **视频会议系统设备巡检内容** | 混音器 | 音频输入状态 |  |
| 音频输出状态 |  |
| 音量调节状态 |  |
| 音频矩阵 | 切换是否正常 |  |
| 音质情况 |  |
| 麦克风 | 音频输出状态 |  |
| 视频网络通道 | 第一通道到第十通道状态 |  |
| 通道切换情况 |  |
|  | **巡检项目** | **巡检具体内容** | **备注** |
| **各系统设备供电设施及通讯设施的巡检内容** | 各系统电源供电线路 | 各系统电源线缆接头处是否铰接完好及有无漏电短路或潮湿现象，并进用热塑管套接进行简易的  绝缘和防潮处理 |  |
| 供电线路的管道走向分布图 |  |
| 各系统通讯设备设施 | 各系统通讯传输设备是否完好及正常工作 |  |
| 检查通讯光纤光路通断情况及光路衰减情况 |  |
| 检查各系统通讯传输数据是否有丢包等现象 |  |
| 各系统电源取电点 | 各智能系统取电位置处电表、  空气开关及熔断器是否完好和正常工作 |  |
| 各系统取点处电压值是否在设备正常工作范围内，有无电压变化不稳定等现象 |  |
| 各系统供电线路是否有破损现象  及是否有短路等情况 |  |
| 各系统电源取电点 | 各智能系统取电位置处电表、  空气开关及熔断器是否完好和正常工作 |  |
| 各系统取点处电压值是否在设备正常工作范围内，有无电压变化不稳定等现象 |  |
| 各系统供电线路是否有破损现象  及是否有短路等情况 |  |
| **（以上巡检内容具体以合同约定为准）** | | | |

**附表二：维修维护内容明细表**

|  |  |  |
| --- | --- | --- |
| **维护项目** | **维修维护项目类别** | **备注** |
| **主要维修维护项目列表** | 电脑、服务器硬件  维护维修 | 对所有的电脑和服务器的运行、故障、性能进行检测，并对其检测的结果做出相对的维修维护更换，如果出现储存故障时并能恢复其数据。 |
| 电脑、服务器软件  维护维修 | 在保证客户的资料不丢失的情况下，对电脑和服务器的崩溃系统，进行重新安装或调试系统，并安装对应的驱动程序保证跟其相连的设备正常使用。 |
| 交换机数据设计编写以及维护维修 | 对专网的网络结构、网络拓扑进行优化、检测和设计，对交换机进行数据设计和编写，并对所有的网络进行IP规划分配，杜绝网络的环路，网络风暴等等维修维护更换。 |
| 设备通讯线路维护 | 含光端机维护及更换、光路运行情况检测（光功率、光路通断等）、通讯线缆及接头更换、各类通讯线  （RS232、RS485、以太等）制作及更换等工作 |
| 线路整理以及  综合布线 | 对办公室、机房、落井口、走廊里的线路进行梳理整理，并对发现出现线路故障的要及时维修维护更换。对新装修的办公室、机房、落井口、走廊，按照业务需要、按照国家标准和涉密要求、对其对应综合布线，并对其遗留的垃圾进行清理。 |
| 软件指导以及  使用和调试 | 对所有的电脑和服务器里的软件进行检测并对出现错误的软件进行修复，安装对应的插件等等或者重新安装或调试，并指导客户使用工作上使用的软件和工具。 |
| 视频会议系统的  维护以及维修 | 含一体化枪机、球机外壳及各模块，摄像机外壳及各模块，信号灯具、灯芯及灯罩，LED 屏，行人按钮设备，盲人钟提示器，信号显示倒计时器，光端机各模块，信号控制接线端子，继电吸合器，变压器，保险管等零部件的维护更换 |
| 各类专网和互联网的维护调试维修 | 对各类专网和互联网的维护调试维修，对存在的网络风暴、网络环路、网络延迟以及网络故障要及时处理恢复。 |
| **维护项目** | **维修维护项目类别** | **备注** |
| **主要维修维护项目列表** | 设备主机板件及主  机模块维护及更换 | 含监控、电脑、服务器、LED、交换机路由器及各类模块，云台及控制模块等设备的维护和更换 |
| 设备辅助设施加装 | 含加装备用电源设备、网络中控、LED接收发送器、多媒体控制器、音频转换线、视频转换线、无线路由器、、插排、USB转换器、硬盘、主板、内存条、CPU等等 |
| 运送、迁移和存放 | 含所有各类通讯线、前端设施、主机柜箱等 |
| 设备设施 | 取电设施、通讯设施的运送、迁移和存放等 |
| 前端设备运行  情况调试 | 含监控、电脑、服务器、LED等前端程序刷新和调试，供电设备、通讯设备、检测设备及辅助设施设备等的运行情况调试 |
|  | 日报、周报、月报 | 按采购人要求报送工作日报、周报、月报。 |
| 维修维护的  其他内容 | 采购人业务范围内维修维护的其他内容 |

**2.2 安全保障服务**

网络安全保障服务是落实网络安全等级保护制度的核心和落脚点，安全保障服务是在等级保护对象定级工作基础上深入开展的一项工作，使网络系统可以满足保护等级的要求进行设计、规划和实施，并且达到相应等级的基本保护水平和保护能力。

**2.2.1 安全保障服务目标**

依据网络安全等级保护相关标准和指导规范，本次安全保障服务总体安全目标如下：

保障基础网络安全、保障业务应用安全，实现等级保护对象安全稳定运行，同时符合国家相关法律法规要求。

具体目标描述如下：

1. 基础网络安全

安全的基础网络能够为系统提供稳定的IT基础设施环境，保障设备和线路冗余，同时为业务应用系统提供稳定、可靠的运行环境；保障网络和系统运行处于可控状态，统一实施对各类网络设备、服务器设备、控制终端设备等的管理，确保业务系统IT基础设施的安全稳定运行。

1. 业务应用运行安全

通过统一的安全管理措施，统一的访问控制策略，统一的安全审计、网络监控措施，及统一的授权、认证措施，保障业务系统不受恶意攻击的影响，防止业务中断。

1. 满足国家相关法律法规要求

三亚市公安局信息系统属于国家重要的信息系统，按照国家等级保护工作的要求确定了安全保护等级，需要按照国家等级保护相关技术标准和规范开展等级保护工作，实施相应等级强度的安全保护，满足国家等级保护要求。

**2.2.2 安全保障服务内容和要求**

**（1）网络边界安全防护及服务**

服务内容：通过安全服务人员使用相关配套工具来实现以下服务

1）提供基于应用协议和应用内容的细粒度安全访问控制措施。

2）提供边界入侵防护防止或限制从内、外部发起的网络攻击行为，对内、外部发起的网络攻击行为实时监测和拦截。

3）提供边界病毒防护防止恶意代码（蠕虫、挖矿等）在内网传播传播

4）提供对应的工具或安全策略加固，要求至少针对两个网络边界进行防护及保障，并且满足业务性能，在服务期内，服务商确保所提供的工具或设备系统版本为最新版本。

服务对象：公安网、视频网、互联网、PDT对讲专网。

服务周期：一年，7\*24小时不间断。

服务交付：包括但不限于以下交付成果：

①《网络安全边界防护报表》

服务工具：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务工具名称** | **技术指标** | **数量** | **单位** |
| 1 | 视频网下一代防火墙 | 1、2U机型，含交流冗余电源，≥1\*RJ45串口，≥1\*RJ45管理口，≥2\*USB接口，≥6\*GE电口（Bypass）,≥4\*SFP光口（含4个光模块），≥2个万兆SFPP插槽（不含光模块）。≥2个接口扩展槽位，≥256G固态硬盘。网络吞吐量≥20G，IPS+AV吞吐量≥18Gbps，最大并发会话数≥800w，每秒新增会话数≥15w。含传统防火墙、入侵防护、防病毒、流量管理、应用管理、IPSec VPN、资产识别功能。  2、支持批量绑定IP/MAC地址，可通过文件形式和非文件形式批量导入；  3、支持对二层协议进行访问控制，针对BPDU、802.1Q、SLOW协议、PPPoE、QinQ、MPLS等协议进行屏蔽；  4、支持基于策略的双向NAT、动态/静态NAT、端口PAT;支持ALG(支持协议包括FTP、SIP、H.323、TNS、PPTP等)；  5、通过对每个接口进行探测，测试接口的可达性和有效性，协议方式包括ICMP/TCP/UDP；  6、Ipsec vpn支持在不改变用户网络架构的情况下，机型虚拟线部署方式，以达到Ipsec vpn改造效果；  ▲7、内置应用过滤器，可通过应用过滤器分析、筛选出结果，自动生成模板，便于用户直接使用和管理；(提供工具系统功能截图并加盖工具厂商公章)  ▲8、内置应用过滤器，可通过不同角度（应用种类、技术方式、风险级别、标签备注等）进行过滤；(提供工具系统功能截图并加盖工具厂商公章)  9、支持至少2000条规则数的web服务器的安全策略模板；  10、支持预置风险级别，包括操作系统、浏览器、杀毒软件等；  11、可基于应用、源/目的IP、用户、攻击事件等维度，对安全事件进行关联分析；  12、提供工具厂商针对该项目下一代防火墙工具的使用授权。 | 1 | 台 |
| 2 | 互联网、PDT对讲专网下一代防火墙 | 1、1U机型,双电源,1\*管理口,≥16\*千兆电口,≥4\*Combo口,≥6\*SFP（含2个光模块）,≥2\*SFP+（不含光模块）,≥2\*扩展插槽,≥64G SSD，网络吞吐量≥12G，IPS+AV吞吐量≥8Gbps，最大并发会话数≥400w，每秒新增会话数≥8.6w。含传统防火墙、入侵防护、防病毒、流量管理、应用管理、IPSec VPN、资产识别功能。  2、支持一对一、多对一、多对多等多种方式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能；  3、具备各类VPN技术，支持IPSec、L2TP、GRE VPN、SSL VPN等功能方式；  4、支持安全域划分，访问控制列表，配置对象及配置策略，数据包动态过滤，黑名单，IP/MAC绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能；  5、支持策略风险优化，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略优化，可根据流量、应用、风险类型等不同维度进行展示，用户可以根据总体安全平台更好的对安全策略进行管理；  6、支持至少6000条以上的软件应用发现识别，用户可根据提示风险类型及风险级别进行上网行为管理；  ▲7、僵尸网络分析，支持攻击链分析及资产安全风险等级的可视化呈现；(提供工具系统功能截图并加盖工具厂商公章)  8、发现病毒发送的告警日志，用户可对告警日志进行修改；  9、智能路径选择，支持基于链路权重、带宽、配置优先级、链路质量、用户业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权HASH等智能选路方式；  10、支持包括轮询及加权轮询、最小连接及加权最小连接、随机及加权随机、源/目的地址Hash、源地址端口哈希值、优先级等负载均衡调度算法；  ▲11、能够防范DOS/DDOS攻击：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP分片报文、ARP欺骗、ARP主动反向查询、TCP报文标志位不合法、超大ICMP报文、地址及端口扫描等攻击防范，还包括针对SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood等常见DDoS攻击的检测防御；(提供工具系统功能截图并加盖工具厂商公章)  12、提供工具厂商针对该项目下一代防火墙工具的使用授权。 | 2 | 台 |

1. **运维安全和综合审计服务**

服务内容：通过安全服务人员使用相关配套工具来实现以下服务

1）提供对多种方式收集各主机系统产生的告警日志，并进行集中存储、解析与范式化，通过先进的关联算法可对告警日志进行关联分析与统计展示，支持对综合日志的检索与查询。

2）提供对各类用户的操作行为审计，以及网络中重要安全事件的记录审计等内容，且审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，对违规越权操作、违规访问网络等用户行为进行分析告警。

3）提供对系统管理员、审计管理员和安全管理员，通过集中化运维管控、统一运维管理、身份认证与权限控制、运维访问合规性控制、运维过程实时监看、自定义应用发布等功能，

4）提供对应的服务工具（日志审计、数据库审计、堡垒机），满足业务性能，在服务期内，免费提供工具的规则库和软件升级，确保规则库为最新版本。

服务对象：公安网、视频网、互联网、PDT对讲专网。

服务周期：一年，7\*24小时不间断。

服务交付：包括但不限于以下交付成果：

①《安全运维分析报表》

②《网络日志统计分析报表》

③《数据库安全统计分析报表》

服务工具：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务工具名称** | **技术指标** | **数量** | **单位** |
| 1 | 视频专网、互联网、PDT对讲专网日志审计 | 1、标准2U机箱,≥6个千兆电口，≥4个千兆光口,双电源,≥2个扩展槽位,综合采集处理均值≥8000EPS，含100日志源授权，≥32G内存，≥256G固态硬盘，存储容量≥6T；带液晶屏；  2、支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据；  ▲3、支持对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集；  4、支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数；(提供工具系统功能截图并加盖工具厂商公章)  5、支持为不同类型日志设置不同的查询条件和显示条件；  6、支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果；  ▲7、支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息；(提供工具系统功能截图并加盖工具厂商公章)  8、系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；  9、系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置；  10、提供工具厂商针对该项目日志审计工具的使用授权。 | 3 | 台 |
| 2 | 互联网堡垒机 | 1、标准1U机箱,≥6个千兆电口，≥2个千兆光口，≥1个console口；单电源,≥2个扩展槽位,配置100资源授权，用户数不限制；  ▲2、认证管理支持双因子认证；认证方式支持OTP动态口令认证、短信认证、数字证书认证、USB-KEY认证、人脸识别等双因素认证方式；内置人脸识别功能，无需与第三方人脸识别系统对接开发；(提供工具系统功能截图并加盖工具厂商公章)  3、支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令TOP10等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况；  ▲4、支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填；(提供工具系统功能截图并加盖工具厂商公章)  5、自动对Linux、Windows、安全设备、数据库等资产进行账号改密，改密支持手动和定期自动改密；支持改密结果可通过邮箱、FTP方式外发，密码采用密码信封加密保存，以保证安全性；支持密钥加密和明文分段发送；  6、提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系；  7、支持会话请求远程协助，且协同会话保持实时同步；  8、支持Xshell、Xftp、SecureCRT客户端的session文件导出；  ▲9、审计管理支持全文审计检索；可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯；(提供工具系统功能截图并加盖工具厂商公章)  10、提供工具厂商针对该项目堡垒机工具的使用授权。 | 1 | 台 |
| 3 | PDT对讲专网堡垒机 | 1、标准1U机箱,≥6个千兆电口，≥2个千兆光口，≥2个万兆光口；1个console口；单电源,≥2个扩展槽位,配置100资源授权，用户数不限制；  ▲2、认证管理支持双因子认证；认证方式支持OTP动态口令认证、短信认证、数字证书认证、USB-KEY认证、人脸识别等双因素认证方式；内置人脸识别功能，无需与第三方人脸识别系统对接开发；(提供工具系统功能截图并加盖工具厂商公章)  3、支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令TOP10等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况；  ▲4、管理隔离，支持管理口与业务口分离，启用管理隔离后，实现管理和运维操作的分离；  5、自动对Linux、Windows、安全设备、数据库等资产进行账号改密，改密支持手动和定期自动改密；支持改密结果可通过邮箱、FTP方式外发，密码采用密码信封加密保存，以保证安全性；支持密钥加密和明文分段发送；(提供工具系统功能截图并加盖工具厂商公章)  6、提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系；  7、支持会话请求远程协助，且协同会话保持实时同步；  8、支持Xshell、Xftp、SecureCRT客户端的session文件导出；  ▲9、审计管理支持全文审计检索；可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯；(提供工具系统功能截图并加盖工具厂商公章)  10、提供工具厂商针对该项目堡垒机工具的使用授权。 | 1 | 台 |
| 4 | 视频网数据库审计 | 1、标准2U机箱,≥6个千兆电口，≥4个千兆光口,冗余电源,≥2个扩展槽位,审计处理能力≥2Gbps,峰值SQL处理能力≥15000条/秒，日志存储能力≥40亿条，≥4T存储空间；  2、支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统；支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统；支持KingBase、DaMeng、Oscar、GBase、Inspur\_KDB、Highgo、GaussDB等国内主流数据库系统；  3、支持数据库请求和返回的双向审计，特别是返回字段和结果集、返回码、SQL错误信息、返回行数、执行时长等内容；  4、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息；  ▲5、支持会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节；(提供工具系统功能截图并加盖工具厂商公章)  6、支持以姓名、部门、域名、主机名、源MAC、邮箱、电话、数据来源等要素为条件的实名审计；  7、支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低了存储空间和无用信息的堆砌，白名单内容包括但不限于SQL语句、数据库类型、业务URL地址、数据库名、HTTP访问域等；  8、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括以下几种： WinSer2003/2008/2012/2016、Centos、opensuse、redhat、Ubuntu、中标麒麟SV1.2-龙芯、银河麒麟SV1.3-飞腾、银河麒麟server-飞腾等、AIX5/6；  ▲9、多个维度展示错误占比及趋势，从源IP维度以柱状图展示SQL错误数（TOP10），以饼图展示正常SQL与慢SQL占比情况、TOP10慢SQL的详细分析：TOP排名信息、事件ID、数据库名、目的ip、协议类型、源ip、sql响应时间、操作类型、具体sql语句等要素；(提供工具系统功能截图并加盖工具厂商公章)  10、提供工具厂商针对该项目数据库审计工具的使用授权。 | 1 | 台 |
| 5 | 互联网数据库审计 | 1、标准2U机箱,≥6个千兆电口，≥4个千兆光口,双电源,≥2个扩展槽位,审计处理能力≥600Mbps,峰值SQL处理能力≥4000条/秒，日志存储能力≥20亿条 ，≥1T存储空间；  2、支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统；支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统；支持KingBase、DaMeng、Oscar、GBase、Inspur\_KDB、Highgo、GaussDB等国内主流数据库系统；  3、支持数据库请求和返回的双向审计，特别是返回字段和结果集、返回码、SQL错误信息、返回行数、执行时长等内容；  4、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息；  ▲5、支持会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节；(提供工具系统功能截图并加盖工具厂商公章)  6、支持以姓名、部门、域名、主机名、源MAC、邮箱、电话、数据来源等要素为条件的实名审计；  7、支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低了存储空间和无用信息的堆砌，白名单内容包括但不限于SQL语句、数据库类型、业务URL地址、数据库名、HTTP访问域等；  8、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括以下几种： WinSer2003/2008/2012/2016、Centos、opensuse、redhat、Ubuntu、中标麒麟SV1.2-龙芯、银河麒麟SV1.3-飞腾、银河麒麟server-飞腾等、AIX5/6；  ▲9、多个维度展示错误占比及趋势，从源IP维度以柱状图展示SQL错误数（TOP10），以饼图展示正常SQL与慢SQL占比情况、TOP10慢SQL的详细分析：TOP排名信息、事件ID、数据库名、目的ip、协议类型、源ip、sql响应时间、操作类型、具体sql语句等要素；(提供工具系统功能截图并加盖工具厂商公章)  10、提供工具厂商针对该项目数据库审计工具的使用授权。 | 1 | 台 |
| 6 | PDT对讲专网数据库审计 | 1、标准1U机箱,≥6个千兆电口，≥4个SFP插槽,单电源,审计处理能力≥200Mbps，峰值SQL处理能力≥2000条/秒，≥1T存储空间；  2、支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统；支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统；支持KingBase、DaMeng、Oscar、GBase、Inspur\_KDB、Highgo、GaussDB等国内主流数据库系统；  3、支持数据库请求和返回的双向审计，特别是返回字段和结果集、返回码、SQL错误信息、返回行数、执行时长等内容；  4、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息；  ▲5、支持会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节；(提供工具系统功能截图并加盖工具厂商公章)  6、支持以姓名、部门、域名、主机名、源MAC、邮箱、电话、数据来源等要素为条件的实名审计；  7、支持白名单审计：系统使用审计白名单将非关注的内容进行过滤，降低了存储空间和无用信息的堆砌，白名单内容包括但不限于SQL语句、数据库类型、业务URL地址、数据库名、HTTP访问域等；  8、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括以下几种： WinSer2003/2008/2012/2016、Centos、opensuse、redhat、Ubuntu、中标麒麟SV1.2-龙芯、银河麒麟SV1.3-飞腾、银河麒麟server-飞腾等、AIX5/6；  ▲9、多个维度展示错误占比及趋势，从源IP维度以柱状图展示SQL错误数（TOP10），以饼图展示正常SQL与慢SQL占比情况、TOP10慢SQL的详细分析：TOP排名信息、事件ID、数据库名、目的ip、协议类型、源ip、sql响应时间、操作类型、具体sql语句等要素；(提供工具系统功能截图并加盖工具厂商公章)  10、提供工具厂商针对该项目数据库审计工具的使用授权。 | 1 | 台 |

1. 网络安全威胁预警监控服务

服务内容：通过安全服务人员使用相关配套工具来实现以下服务

1）对网络安全的病毒特征检测、行为检测、威胁情报、AI/机器学习对信息化系统实时检测及预警分析，及时分析及相应的处置措施等。

2）提供对应的服务工具（高级威胁监测系统），满足业务性能，在服务期内，免费提供工具的规则库和软件升级，确保规则库为最新版本。

服务对象：公安网、互联网、视频专网、PDT对讲专网。

服务周期：一年，7\*24小时不间断。

服务交付：包括但不限于以下交付成果：

①《安全威胁监测分析报表》

服务工具：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务工具名称** | **技术指标** | **数量** | **单位** |
| 1 | 公安网高级持续性威胁预警系统 | 1、软硬一体化，2U标准机架式设备，MTBF大于65000小时，吞吐率：网络层≥2Gbps，WEB检测：HTTP最大并发数≥6万/秒，邮件检测：邮件处理数: ≥145万封/24小时，文件检测：≥12万个/24小时，支持分布式管理节点≥10个；电源：冗余电源，内存≥64G，硬盘容量≥4T；接口数量：管理口≥2个、千兆RJ45网口≥4、千兆业务SFP光口≥4（标配千兆多模光模块2个），接口扩展插槽≥2个；  2、支持风险数据包保存功能，以帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置wireshark组件预览风险数据包；  3、支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、邮件钓鱼、DGA域名请求、SMB远程溢出攻击、WEB行为分析、非法数据传输、弱口令、隐蔽信道通信、暴力破解、挖矿、远控工具利用、密码明文形式传播、扫描行为等风险；  4、支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB风险特征白名单进行设置；  5、支持对HTTP、IMAP、SMTP、POP3、Telnet、FTP等协议的弱口令检测。支持敏感信息管理，可自定义弱密码、暴力破解和密码明文形式传输等告警的密码查看权限；  6、可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等；  7、可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析；  8、支持全流量检测，可根据需求打开或关闭全流量检测功能；  9、支持IP、端口、SMB、Radmin、ICMP、ARP、传输层协议和漏洞扫描行为检测；  10、支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功；  11、支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级；  ▲12、具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为，具备DNS重绑定攻击检测能力，分析域名与IP地址间的获取关系，并记录DNS解析返回的多个IP与时间；(提供工具系统功能截图并加盖工具厂商公章)  ▲13、对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接；(提供工具系统功能截图并加盖工具厂商公章)  14、支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现；  15、采用多并发沙箱检测技术，集成主流的操作系统winXP、win7等多种检测环境，可结合平台内置的反病毒引擎和静态分析技术、动态模拟技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析；  16、提供工具厂商针对该项目威胁预警系统工具的使用授权。 | 1 | 台 |
| 2 | 互联网、PDT对讲专网高级持续性威胁预警系统 | 1、软硬一体化，标准机架式设备，吞吐率：网络层≥500Mbps，文件检测：≥8万个/24小时，支持分布式管理节点≥5个；电源：单电源，内存≥32G，硬盘容量≥2T；接口数量：管理口≥2、千兆RJ45网口≥4，网络接口扩展槽位≥2个。  2、支持风险数据包保存功能，以帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置wireshark组件预览风险数据包；  3、支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、邮件钓鱼、DGA域名请求、SMB远程溢出攻击、WEB行为分析、非法数据传输、弱口令、隐蔽信道通信、暴力破解、挖矿、远控工具利用、密码明文形式传播、扫描行为等风险；  4、支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB风险特征白名单进行设置；  5、支持对HTTP、IMAP、SMTP、POP3、Telnet、FTP等协议的弱口令检测。支持敏感信息管理，可自定义弱密码、暴力破解和密码明文形式传输等告警的密码查看权限；  6、可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等；  7、可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析；  8、支持全流量检测，可根据需求打开或关闭全流量检测功能；  9、支持IP、端口、SMB、Radmin、ICMP、ARP、传输层协议和漏洞扫描行为检测；  10、支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功；  11、支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级；  ▲12、具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为，具备DNS重绑定攻击检测能力，分析域名与IP地址间的获取关系，并记录DNS解析返回的多个IP与时间；(提供工具系统功能截图并加盖工具厂商公章)  ▲13、对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接；(提供工具系统功能截图并加盖工具厂商公章)  14、支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现；  15、采用多并发沙箱检测技术，集成主流的操作系统winXP、win7等多种检测环境，可结合平台内置的反病毒引擎和静态分析技术、动态模拟技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析；  16、提供工具厂商针对该项目威胁预警系统工具的使用授权。 | 2 | 台 |
| 3 | 视频网安全威胁预警系统 | 1、软硬一体机产品；管理资产数量：≥3000个；数据处理性能：≥20万并发会话；内存：≥2\*32G；硬盘≥2\*240G SSD（Raid 1）+2\*4TB SAS（Raid 1）；单电源；网络接口：≥2个千兆电口，≥4个USB2.0接口，≥2个USB3.0接口,≥1个CONSOLE口。  2、工具具有主动安全监测、网络空间测绘、资产安全识别、边界安全检测、违规行为分析、网络攻击预警、信令安全审计以及取证、溯源等功能；  ▲3、可进行自定义监测频率设置，并对全网设备进行安全检测；(提供工具系统功能截图并加盖工具厂商公章)  4、支持对网络摄像机的IP、品牌、型号、操作系统等资产属性进行监测；支持设备在线与离线状态监测；  5、支持对PC设备的系统类型、系统版本、服务类型、端口等信息进行监测；  6、支持对在网资产的设备类型、品牌型号、操作系统、应用名称、版本、端口等信息进行识别；  7、支持对资产的在线状态、资产变更进行监测；  8、支持对视频设备进行安全漏洞扫描检测，分析设备安全风险状况；  9、实现对全网视频设备进行不间断的视频信令安全检测，包括：信令审计。支持对ONVIF、GB28181视频信令审计；  ▲10、高危信令监测：对可能对视频设备、视频数据等造成影响的高危信令进行安全监测、分析与告警；(提供工具系统功能截图并加盖工具厂商公章)  11、异常信令监测：对信令的来源、时间、频繁度等不同的角度进行综合分析，及时发现信令异常情况；  ▲12、违规外联监测——可监测范围内终端的两网互通（同时连接内网和互联网）的行为，并可在两网互通监测平台子模块中定位其终端地址（内网IP和互联网IP）；(提供工具系统功能截图并加盖工具厂商公章)  13、提供网中网分析，可监测视频网中存在的包括NAT设备等的私有局域网情况；  14、边界安全监测：可显示网闸设备、小型路由器、代理服务器等边界安全设备的监测信息；  15、实现对网络中存在的网内攻击行为进行检测；  16、恶意扫描检测：监测网络中频繁或大规模的访问其它主机设备、服务端口的行为，提供发起扫描的设备地址、被扫描最多主机、被扫描最多端口等详细信息；  17、敏感端口扫描：监测通过专网对全网设备特定端口或特定设备全端口扫描的行为；  18、监测病毒或木马程序利用已知漏洞进行大规模传播的行为。提供病毒木马对应的详细通信记录以及特征信息，包括开始时间、结束时间、病毒源（地址、端口）、被攻击目标（地址、端口）等信息；  19、监测对特定业务系统的进行频繁访问的异常行为，提供频繁访问业务系统的终端设备地址、所在位置、被访问系统的地址、端口、名称等详细信息；  20、监测在一定时间段内对大范围网络IP发起访问连接请求，或频繁地试图访问连接特定的IP等的异常行为，提供发起访问连接的源地址、目的地址、时间、端口等信息；  21、脆弱性：对使用弱口令、设备端口的安全风险隐患进行监测和发现。用户可以自定义扫描目标、类型、扫描时间策略。系统会根据设备类型进行漏洞扫描；  22、对内网的终端设备持续互联网DNS异常请求进行监测；  23、监测网络违规设备（移动设备/Windows 8系统）接入，提供设备接入地址、设备类型、所在地市位置等信息；  24、可监测网络中存在的FTP服务器，并提供服务器地址、FTP软件类型、匿名登录状态、服务器位置等信息；  25、可监测用户访问FTP服务器的行为，并提供用户终端地址、FTP服务器地址、上传下载文件名、文件大小、用户名、密码等信息；  26、提供告警事件类型、类别、等级、内容、告警时间、持续等告警事件管理。提供告警事件名称、类型、状态、级别、告警时间、签收时间、处理时间、处理人、处理结果等告警事件处置管理；  27、提供工具厂商针对该项目威胁预警系统工具的使用授权。 | 1 | 台 |

1. 业务全生命周期管控服务

服务内容：通过安全服务人员使用相关配套工具来实现以下服务

1）漏洞利用入侵模拟阶段通过人工+工具的方式，识别互联网侧系统漏洞，对识别出的漏洞进行深入分析，了解漏洞的具体细节和利用条件，根据漏洞特点编写或获取现有的载荷，在控制的环境中执行载荷，测试漏洞利用的有效性，从而记录漏洞对入侵内网提供入口。

1. 提供对应的服务工具，基于全生命周期管控思路，对漏洞、管理、配置等风险进行系统化的全生命周期管理，同时巩固数字健康检查结果，跟进风险修复进度，回放测试载荷，加载热修复方案；

服务对象：公安网、互联网、视频专网。

服务周期：一年，7\*24小时不间断。

服务交付：包括但不限于以下交付成果：

①《业务全生命周期检测报告》

服务工具：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务工具名称** | **技术指标** | **数量** | **单位** |
| 1 | 数字风洞测试评估平台 | 一、数字风洞测试评估中心平台  1、容错：支持本地双机实时热备，保证平台稳定性；  2、稳定性：有效工作时间≥99%  3、规格：2U标准机架式，CPU≥2颗Xeon 处理器，内存≥64G 内存，硬盘容量≥12TB存储,配置RAID卡，网口数量≥2个千兆网卡  4、并发量：同时支持≥500人同时登录  5、系统容量：支持≥3万用户，支持GB及数据，支持数据库表≥100万行；  ▲6、平台需内置勒索病毒专项检查任务模板，内置常见的易引起勒索病毒事件的载荷，任务下发后检测人员可利用勒索病毒载荷集进行检查。检测过程中发现的未入库资产支持补充信息后加入资产库，已加入资产库的资产支持查看本次任务关联的风险。(提供工具系统功能截图并加盖工具厂商公章)  二、数字风洞测评终端  6、规格配置 CPU≥8核，内存≥8G  7、URL最大数量≥300个  8、站点最大数量≥300个  9、IP最大数量≥1270个  10、IP-C段最大数量≥5个。  11、提供工具厂商针对该项目数字风洞测试评估工具的使用授权。 | 1 | 套 |

1. 主动防御体系建设服务

服务内容：通过安全服务人员使用相关配套工具来实现以下服务

1. 主动防御分析针对受保护网络的威胁状态进行感知分析与监视，对攻击者的行为和状态进行监控和分析，包括:攻击溯源、主动反制、威胁来源、事件分析、行为分析。
2. 提供对应的服务工具（主动攻击诱捕系统），构建主动防御体系提升：1.识别和预警病毒入侵和传播，2.精准发现高危攻击行为，3完善网络安全监测与防御体系，4.实时掌握攻击态势，支持快速取证溯源。

服务对象：公安网、互联网、视频专网以及PDT对讲专网的应用系统、操作系统、服务器、数据库及其他设备，如路由器、交换机、防火墙等的运行状况、资源利用情况、网络连接情况等进行检查，检查系统健康状态。。

服务周期：一年，每季度一次，总共四次。

服务交付：包括但不限于以下交付成果：

①《季度主动防御分析报告》

服务工具：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务工具名称** | **技术指标** | **数量** | **单位** |
| 1 | 主动攻击诱捕系统 | 1、2U机架式服务器；CPU≥2\*Intel Xeon 4210R 10核 2.4GHz；内存≥2\*32GB DDR4；硬盘≥4\*2TB；电源：1\*550W单电源；网口≥4\*千兆电口。  ▲2、威胁监测场景采用虚拟防火墙仿真网络入口，采用虚拟网络仿真DMZ区，并在DMZ区构建VPN、邮件系统、办公自动化系统等10个蜜罐，内置RCE、反序列化、文件上传、弱口令、WebShell执行等多种漏洞，不仅能监测对于网络的威胁，还能基于沙箱技术监测对于主机的各类威胁行为，全方位记录、分析及复现黑客的整个攻击过程。(提供工具系统功能截图并加盖工具厂商公章)  3、溯源反制场景采用虚拟防火墙仿真网络入口，采用虚拟网络仿真DMZ区，并在DMZ区构建JSONP溯源、文档类溯源反制、协议类溯源反制、扫描工具类溯源反制等蜜罐，通过多种不同类型的手段对黑客进行溯源或反制。  4、支持通过在线爬取、上传网站源码方式进行网站伪装仿真，并支持自定义设置网站logo、网站名称、系统版权、网站背景等。  5、支持仿真网站实时预览，以验证伪装是否准确完成。  6、支持数据库伪装仿真，包括仿真账号密码及数据；支持自定义设置数据库的账户、密码；支持通过上传SQL脚本创建和更新数据库表、数据记录。  7、支持域名诱饵，将用于诱饵的域名解析到蜜罐场景入口IP上，从而将攻击者引入蜜罐。  ▲8、支持14种威胁手法识别，包括端口扫描、尝试访问、文件操作、注册表操作、代码执行、暴力破解、账号操作、建立连接、漏洞利用、进程操作、登录操作、系统控制、中间人攻击、本地提权等手法的识别。(提供工具系统功能截图并加盖工具厂商公章)  9、提供工具厂商针对该项目主动攻击诱捕系统工具的使用授权。 | 1 | 台 |

1. 入网数字安全体检服务

服务内容：通过入网数字安全体检服务开展1、深度数字健康检查模拟黑客攻击针对系统进行安全检查，配置核查和漏洞扫描，发现网络层面安全重大风险及隐患，跟进消除风险，2、围绕重要信息系统开展季度数字健康巡检，巩固安全检查成果，结合信息系统建设和使用近况，防范化解风险，通过人员驻场加远程服务的方式对重要系统进行常态检测。

服务对象：针对公安网、互联网、视频专网、PDT专网上的业务系统开展入网数字安全体检工作。

服务周期：一年，每季度一次，总共四次。

服务交付：包括但不限于以下交付成果：

①《入网数字安全体检报告》

1. 安全渗透测试服务

服务内容：针对单位的相关信息系统提供一年2次的渗透测试工作，精通渗透测试技术的资深安全专家，在客户授权范围内，参考PTES(渗透测试执行标准)对客户信息系统进行模拟黑客攻击的商业化测试服务，用于帮助客户评估信息系统当前的安全性。提供包括外网渗透测试、内网渗透测试、黑盒测试、灰盒测试等多种测试方法，覆盖信息系统中包含的网站、APP、服务器、数据库、中间件、网络设备、终端等相关软硬件资产。

服务对象：针对公安网、互联网、视频专网、PDT专网以及政务外网（雪亮工程综治共享分平台）上部署的系统（总共13个系统）进行安全性渗透测试。

服务周期：一年，每半年一次，总共两次。

服务交付：包括但不限于以下交付成果：

①《渗透性测试报告》

②《渗透性测试复测报告》

1. 网络安全加固服务

服务内容：根据漏洞扫描评估或渗透测试中发现的问题开展安全加固服务，提供主机层面漏洞修复以及策略加固和网络安全层面配置加固，针对现有操作系统中存在的系统问题，提供漏洞修复服务，针对主机和网络安全设备配置中存在问题，进行相关配置层面的优化，确保满足等级保护的安全基线，加固范围为网络环境中的所有网络设备，安全设备，服务器，包括交换机、路由器、防火墙、主机等。

服务对象：针对公安网、互联网、视频专网及PDT专网上的主机、网络设备、安全设备进行安全加固，对雪亮系统进行加固指导服务。

服务周期：一年，一年两次，总共两次。

服务交付：包括但不限于以下交付成果：

①《系统加固指导书》

②《系统加固报告》

③《系统加固复查报告》

9、网站云监测服务

服务内容：以保障网站安全“持续有效”为目标，围绕漏洞、威胁、事件三个要素，通过云端安全监测中心和安全专家团队有效协同的“人机共智”模式7\*24H持续性开展网络安全保障工作，与用户一同构建持续（7\*24小时）、主动、闭环的网站安全监测。

服务对象：大厅排队叫号管理平台（户政预约服务系统）

服务周期：一年。

服务交付：包括但不限于以下交付成果：

①《网站安全监测报告》

10、应急演练服务

服务内容：根据国家法律法规要求，针对单位开展一次信息安全事件应急演练，应急演练以演示或者模拟的环境的形式，以通信故障、系统安全、软硬件故障几大类进行编制再结合用户场景定制，应急演练结束后出具总结报告。

服务对象：三亚市公安局。

服务周期：一年，一年开展一次。

服务交付：包括但不限于以下交付成果：

①《应急演练方案》

②《应急演练总结报告》

11、网络安全驻点服务

服务内容：派驻1名运维驻场安全服务人员，对市局安全设备进行安全运维，对相关信息系统进行安全监测，通过查看相应配套支撑工具的日志，及时响应安全事件，制定相关的应急预案，提供应急处置。

服务对象：三亚市公安局

服务周期：一年。

服务交付：包括但不限于以下交付成果：

①《安全专项检查月报》

②《安全专项检查季报》

③《重要时期保障报告》

④《应急预案》

⑤《应急响应报告》

12、特征库升级服务

1. 公安网上联边界防火墙

IDP攻击规则特征库1年升级许可；专业版快速扫描查杀病毒库1年升级服务许可。

1. 公安网下联边界防火墙

IDP攻击规则特征库1年升级许可；专业版快速扫描查杀病毒库1年升级服务许可。

1. 公安网上联边界防毒墙

1.防病毒AV防护特征库升级授权，自授权导入生效后起1年有效期，由原厂工程师提供升级授权实施服务。

2.系统版本升级授权，当系统更新版本时，可以进行版本升级。包含日志分析/配置策略定期优化服务，原厂工程师定期上门现场巡检服务，以保障系统更稳定运行，自合同生效起1年。

1. 公安网运维审计系统

1.系统版本升级授权，当系统更新版本时，可以进行版本升级。包含日志分析/配置策略定期优化服务，原厂工程师定期上门现场巡检服务，以保障系统更稳定运行，自合同生效起1年。

1. 视频网边界防火墙

IDP攻击规则特征库1年升级许可；和专业版快速扫描查杀病毒库1年升级服务许可。

1. 视频网运维审计系统

1.系统版本升级授权，当系统更新版本时，可以进行版本升级。包含日志分析/配置策略定期优化服务，原厂工程师定期上门现场巡检服务，以保障系统更稳定运行，自合同生效起1年。

1. 互联网边界防火墙

IDP攻击规则特征库1年升级许可；专业版快速扫描查杀病毒库1年升级服务许可。

1. 互联网Web防火墙

1.WEB应用防护特征库升级授权，自授权导入生效后起1年有效期，由原厂工程师提供升级授权实施服务。

2.系统版本升级授权，当系统更新版本时，可以进行版本升级。包含日志分析/配置策略定期优服务，原厂工程师定期上门现场巡检服务，以保障系统更稳定运行，自合同生效起1年。

**2.3 其他运维服务**

**2.3.1 人员驻场运维服务**

（1）1名运维驻场服务人员提供网络维修服务 ；1名运维驻场服务人员提供安全保障服务。

1. 服务地点：市局，各分局、各支队及各派出所；
2. 服务周期：服务周期为1年。