**义乌市数据管理中心**

**网络安全全链路监管服务项目**

招标文件

**采购编号：YWCG2022039GK**

 **采购人：义乌市数据管理中心（盖章）**

**采购代理机构：义乌市政府采购中心（盖章）**

**日期：2022年10月18日**

**招标文件目录**

[第一章　采购公告 2](#_Toc32671)

[第二章　投标须知和投标须知前附表 5](#_Toc17086)

[第三章 招标项目要求 16](#_Toc9111)

[第四章 开标、评标和定标须知 59](#_Toc9757)

[第五章 投标文件的无效情形 63](#_Toc1097)

[第六章 评标办法 65](#_Toc31163)

[第七章 义乌市政府采购合同（样本） 70](#_Toc26103)

[第八章 投标文件部分格式 73](#_Toc1594)

# 第一章　采购公告

根据《中华人民共和国政府采购法》等有关规定，义乌市政府采购中心受委托，就义乌市数据管理中心网络安全全链路监管服务项目进行公开招标，欢迎国内合格的供应商参加投标。

**一、项目基本情况**

1.采购编号：YWCG2022039GK

2.项目名称：义乌市数据管理中心网络安全全链路监管服务项目

3.项目预算：1710万元 最高限价：1710万元

4.采购需求

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 项目内容 | 技术要求 | 数量 | 项目预算 | 最高限价 | 备注 |
| 1 | 网络安全全链路监管服务 | 详见招标文件第三章 | 一批 | 1710万元 | 1710万元 |  |

5.合同履约期限：详见招标文件第三章。

**二、投标人的资格要求，须同时满足以下条件：**

1.符合《中华人民共和国政府采购法》第二十二条供应商应当具备的条件或符合浙财采监【2013】24号《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定的供应商；

2.投标人无以下不良行为：在公开网站上能查到的被财政部或浙江省财政厅处理（或处罚）而处于暂停政府采购资格期的或处于暂停承接业务资格期的；或被国家级、浙江省级、义乌市级行业主管部门处罚处于暂停承接业务资格期的；或被义乌市政府采购监管部门列入不良行为还在公示期内的或者处于暂停政府采购资格期的；或被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、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的；

3.投标人自2019年01月01日起到中标公告期结束前无行贿犯罪记录；

4.根据《关于在全市公共资源交易活动中应用信用报告的通知》（义行服管〔2017〕17号）的规定，综合信用报告评级不属于D类或E类的（无信用评价供应商不受此项条件限制，查询结果以网站页面显示内容为准）；

5.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项（同一标项）下的政府采购活动；

6.为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动；

7.公益一类事业单位不属于政府购买服务的承接主体，不得参与承接购买服务采购项目；

8.本项目接受联合体参与投标。

**三、采购文件（即招标文件，下同）获取时间、地点及方式：**

1.时间：公告发布时间起至投标截止时间止。

2.地点：浙江政府采购网（http://zfcg.czt.zj.gov.cn/）。

3.方式：潜在供应商应按照浙江省政府采购网上所提示的方式免费获取采购文件。

潜在供应商未在规定的期限内按照上述方式获取招标文件的，采购人、采购代理机构可以不予受理其所提出的对招标文件的质疑。

**四、投标截止时间及地点：**

1.提交投标文件截止时间：2022年11月17日09:30（北京时间）

2.投标地点：用帐号登录政府采购云平台（简称“政采云”下同，https://www.zcygov.cn/），上传电子加密标书至“政采云”，逾期或未上传成功的将导致无法投标或投标无效。

3.开标时间：2022年11月17日09:30

4.开标地点：“政采云”（https://www.zcygov.cn/）

**五、公告期限：**

自本公告发布之日起5个工作日。

**六、其他补充事宜**

1. 质疑与投诉：供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起7个工作日内，以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

2.投标保证金：无

3.投标与开标注意事项：

①标前准备：本项目通过“政采云”实行在线投标（电子投标），各供应商在投标前应确保成为浙江政府采购网正式注册入库供应商，并完成CA数字证书办理。【办理流程详见电子投标工具链接：（[目前“政采云”仅支持浙江汇信或天谷CA锁，个体工商户投标仅支持浙江汇信CA锁）申领操作流程](file:///C%3A%5C%5CUsers%5C%5CAdministrator%5C%5CAppData%5C%5CRoaming%5C%5CMicrosoft%5C%5CWord%5C%5CCA%E7%94%B3%E9%A2%86%E6%93%8D%E4%BD%9C%E6%8C%87%E5%8D%97.pdf)”】。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。

②投标文件制作：投标人通过“政采云”电子投标工具制作投标文件，电子投标工具请供应商自行前往浙江省政府采购网(https://zfcg.czt.zj.gov.cn/)下载并安装，投标文件制作具体流程详见“政采云”供应商项目采购-电子招投标操作指南”（请投标供应商登录“政采云”政府采购电子卖场后，点击链接https://edu.zcygov.cn/luban/e-biding）以获取最新操作指南。

③投标文件上传：投标人应在投标截止时间（2022年11月17日09:30）之前上传投标文件，同时，投标人可在投标截止时间前将在 “政采云”上最后生成的具备电子签章的备份投标文件以电子邮件方式传送至义乌市政府采购中心邮箱（ywszfcgzx@163.com），传送的备份投标文件（文件名采用“采购编号+投标人名称+系统自动生成的后缀名”）需打包压缩并加密，加密密码由投标人自行保管。为了防止泄密，建议投标人在设置加密密码时采用大小写字母加数字的组合方式。**投标供应商仅递交备份投标文件的，投标无效。**

④开标与投标文件解密：本项目采用线上开标，供应商无需到开标现场，但应准时在线参加。开标时间后采购中心开启解密。开启解密后的1小时内，供应商应当登录“政采云”，用“项目采购-开标评标”功能解密投标文件。

如“政采云”上投标文件在规定时间内出现解密失败的，投标人可按照自身意愿确认同意提供加密密码，启用备份文件，并由采购中心把备份文件上传至“政采云”。如投标人未按照规定时间（2022年11月17日上午9:30前）及要求提供有效备份标书，同时政采云上投标文件解密失败的，将导致投标无效。

如果投标人发送两份以上备份文件的，以最后收到的那一份为准，通过“政采云”上传递交的“加密投标文件”已按时解密的，“备份投标文件”自动失效。

4. 参与在线投标时如遇平台技术问题详询400-881-7190，电子投标制作问题详询汪先生0579－85583800。

**七、对本次招标提出询问、质疑、投诉，请按以下方式联系。**

**1.采购人信息**

名  称：义乌市数据管理中心

地  址：义乌市城北路299号

项目联系人：王先生

项目联系方式：0579-85410120

质疑联系人：季女士

质疑联系方式： 13588679387

**2.采购代理机构信息**

名  称：义乌市政府采购中心

地  址：义乌市望道路300号4楼

传  真：0579-85570067

项目联系人：方先生

项目联系方式：0579-85583802

质疑联系人：洪艳

质疑联系方式：0579-85232979

**3.同级政府采购监督管理部门**

名  称：义乌市财政局

地  址：义乌市望道路300号5楼

联系人 ：骆女士

监督投诉电话：0579-89915066

义乌市数据管理中心

义乌市政府采购中心

2022年10月25日

# 第二章　投标须知和投标须知前附表

**投标须知前附表**

|  |  |
| --- | --- |
| **序号** | **内容规定** |
| 1 | 项目综合说明 | 项目名称：**义乌市数据管理中心网络安全全链路监管服务项目**，采购内容及数量:具体详见《第三章招标项目要求》 |
| 2 | 招标方式 | 公开招标 |
| 3 | 投标单位资格要求 | 详见采购公告 |
| 4 | 合同履约期限 | 详见第三章 |
| 5 | 招标文件获取时间、地点及方式 | 详见采购公告 |
| 6 | 现场踏勘时间 | 采购方不统一组织投标人前往项目实施场地踏勘，根据项目实际投标需求，投标人可自行前往项目实施场地进行现场探勘，以获取编制投标文件所需资料，如投标人因未现场踏勘原因导致投标文件出现错误或遗漏的，由投标人自行承担责任。 |
| 7 | 招标答疑 | 本项目不组织答疑会；招标方的答疑内容、书面澄清文件是招标文件的组成部份，招标方的书面澄清（更正）文件会在浙江政府采购网上发布公告，同时“政采云”会向所有已按招标文件规定方式获取招标文件的潜在供应商发送澄清（更正）提醒信息，潜在供应商请自行到浙江政府采购网上下载澄清（更正）文件，潜在供应商在收到该澄清（更正）文件后应于1日内，以书面或传真形式（签署意见并加盖公章）向招标代理机构回函给予确认。过期未回复的，视为默认接受。 |
| 8 | 投标有效期 | 自开标之日起90天（日历天） |
| 9 | 上传电子投标文件时间 | 投标人应在投标截止时间（2022年11月17日09:30）之前上传投标文件，同时，投标人可在投标截止时间前将在“政采云”上最后生成的具备电子签章的备份加密投标文件（文件名采用“采购编号+投标人名称+系统自动生成的后缀名”）以电子邮件方式传送至义乌市政府采购中心邮箱（ywszfcgzx@163.com），传送的备份投标文件需打包压缩并加密，加密密码由投标人自行保管。为了防止泄密，建议投标人在设置加密密码时采用大小写字母加数字的组合方式。**投标供应商仅递交备份投标文件的，投标无效。** |
| 10 | 履约保证金 | 无 |
| 11 | 开标时间、地点及电子投标文件解密 | 开标时间：2022年11月17日上午9:30开标地点：“政采云”（<https://www.zcygov.cn/>）本项目采用线上开标，供应商无需到开标现场，但应准时在线参加。开标时间后采购中心开启解密。开启解密后的1小时内，供应商应当登录“政采云”，用“项目采购-开标评标”功能解密投标文件。如政采云上投标文件在规定时间内出现解密失败的，投标人可按照自身意愿确认同意提供加密密码，启用备份文件，并由采购中心把备份文件上传至政采云。如投标人未按照规定时间（2022年11月17日上午9:30前）及要求提供有效备份标书，同时政采云上投标文件解密失败的，将导致投标无效。如果投标人发送两份以上备份文件的，以最后收到的那一份为准，通过“政采云”上传递交的“加密投标文件”已按时解密的，“备份投标文件”自动失效。 |
| 12 | 评标办法 | 综合评分法 |
| 13 | 付款方式 | 详见第三章招标项目具体要求 |
| 14 | 不良行为记录 | 投标人在公开网站上能查到的被财政部或浙江省财政厅处理（或处罚）而处于暂停政府采购资格期的或处于暂停承接业务资格期的；或被国家级、浙江省级、义乌市级行业主管部门处罚处于暂停承接业务资格期的；或被义乌市政府采购监管部门列入不良行为还在公告期内的或者处于暂停政府采购资格期的；或被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、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的，其投标将作无效标处理。 |
| 15 | 政府采购节能环保产品 | 1、根据财政部、发展改革委、生态环境部、市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知财库〔2019〕9号文件要求，投标人所投产品如属于节能产品政府采购品目清单或环境标志产品政府采购品目清单内的，投标人所投的相应产品须在中国政府采购网节能清单查询目录（http://www.ccgp.gov.cn/search/jnqdchaxun.htm）或环保清单查询目录（http://www.ccgp.gov.cn/search/hbqdchaxun.htm）中可查询到。 ★2、招标需求中要求提供的产品属于节能产品政府采购品目清单中强制采购的，投标人须提供该清单内产品，否则其投标将作为无效标处理。 |
| 16 | 中小微企业有关政策 | 1.根据财库[2020]46号《政府采购促进中小企业发展管理办法》和浙财采监[2022]3号《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》、浙财采监〔2022〕8号《浙江省财政厅关于进一步加大政府采购支持中小企业力度 助力扎实稳住经济的通知》的相关规定，未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分标段，在评审时对符合该办法规定的小微企业的投标报价给予20%的扣除，取扣除后的价格作为评审投标报价（此评审投标报价仅在评标时使用）。享受相关中小企业扶持政策的投标人，必须在投标文件中提供《中小企业声明函》。2.接受大中型企业与小微企业组成联合体的采购项目，对于联合协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体的报价给予 6 %的扣除，用扣除后的价格参加评审。3.根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函。4.根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的声明文件（格式自拟）。5.同一投标人，小微企业、监狱企业、残疾人福利性单位价格扣除优惠只享受一次，不得重复享受。6.本项目采购标的所属行业为：软件和信息技术服务业。(注：未提供以上材料的，均不给予价格扣除）。 |
| 17 | 是否接受进口产品参与投标 | 本项目不允许采购进口产品。详见投标须知7.1 |
| 18 | 政采贷 | 为支持和促进中小企业发展，进一步发挥政府采购政策功能，根据《义乌市政府采购支持中小企业信用融资暂行办法》，供应商若有融资意向，登录义乌市公共资源交易平台（http://ywjypt.yw.gov.cn/）“政采贷”专栏进行查询，查看信用融资政策文件及各相关银行服务方案。 |
| 19 | 失信行为处理 | 投标人发生下列情况之一时，除严格依法依规进行处理外，还将通报市信用管理部门，列入严重失信名单：（1）投标人在规定的投标有效期内撤回投标或放弃中标的；（2）有意串标或提供虚假材料的；（3）中标人在收到中标通知书后，因自身原因不能在投标有效期内和采购人签订合同。（4）中标供应商在标后履约过程中未按合同约定的期限和要求履约的。（5）因中标供应商原因在标后履约过程中擅自终止合同的。（6）不符合招标文件要求的其他失信行为。 |
| 20 | 质疑与投诉： | 1.供应商认为采购文件、采购过程、中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之起7个工作日内，以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。2.供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。3.提出质疑的供应商应当是参与所质疑项目采购活动的供应商。 |
| 21 | 其他 | 1.投标报价超过预算价或最高限价的，其投标为无效标。2**.**招标文件中要求投标人在制作投标文件时，提供的证明文件件必须根据评审细则对评审的内容要求完整、清晰可辨，否则在评审时以最不利于投标人原则评审。 |

**注：投标人须知前附表内容与本招标文件后述内容不一致的，以投标须知前附表为准。****投标须知**

## 一、说明

1.适用范围

1.1本招标文件仅适用于本次招标采购所叙述的货物和服务项目。

2.定义

2.1招标方：系指的是采购人和采购代理机构

2.2采购人：系指的是义乌市数据管理中心

采购（招标）代理机构：系指义乌市政府采购中心。

2.3投标人：系指响应招标、参加投标竞争的供应商。

2.4服务：系指招标文件规定投标人须承担的劳务及其它类似的服务。

2.5货物：系指按招标文件规定投标人须向采购人提供的设备及附件等。

2.6需方：即采购人，在招投标阶段称为采购人，在签订和执行合同阶段称为需方。

2.7供方：在招投标阶段称为投标人，中标后在签订和执行合同阶段称为供方。

2.8“原产地”是指货物开采、生长或生产、或提供有关服务的来源地。

2.9“★”标记系指必须满足不能负偏离或必须应答的条款。

3.合格的投标人

符合第一章采购公告中关于“投标人资格条件”规定的投标人。

**4.保证**

投标单位应保证所提交给采购代理机构和采购人的资料和数据是真实、有效的。

**5.投标费用**

不论投标过程中的作法和结果如何，投标人应承担所有与投标有关的全部费用。采购人和采购代理机构在任何情况下均无义务和责任承担上述这些费用。

**6.转包、分包、联合体**

6.1本项目不接受转包。

6.2本项目不接受分包。

6.3联合体采购相关规定

6.3.1除特定资格要求外，联合体各方均应符合本项目规定的其它资格要求及根据承担工作需要的相应资格。

6.3.2如本项目有特定资要求的，联合体中至少有一方应符合本文件规定的特定资格要求。但联合体中有同类资质的投标人按照联合体分工承担相同工作的，应当按照资质等级较低的投标人确定资质等级。

6.3.4以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他投标人另外组成联合体参加同一合同项下的政府采购活动。

6.3.5联合体参与的，必须提供《联合体协议》。

6.3.6如采购项目对供应商有业绩要求。联合体各方分别提供与联合体协议中约定的分工内容相应的业绩材料，业绩数量以提供材料较少的一方为准；如联合体协议中未进行分工约定的，联合体各方应就所有合同约定的工作内容提供业绩材料，有一方未能提供全部合同约定的工作内容的业绩材料的，视为联合体未提供业绩材料。

6.3.7联合体各方均为中小企业的，该联合体视同中小企业。

6.3.8以联合体形式参加政府采购活动的，其投诉应当由组成联合体的所有供应商共同提出。

6.3.9采购人或采购代理机构对联合体中任何一方的书面文件都对联合体各方具有约束力。

**7.政府采购政策**

**7.1进口产品采购规定**

7.1.1进口产品认定根据财政部财库[2007]119号和财政部办公厅财办库[2008]248号文件规定，“进口产品”系指通过中国海关报关验放进入中国境内且产自关境外的产品。但在海关特殊监管区域内企业生产或加工（包括从境外进口原料件）销往境内其他地区的产品，不作为政府采购项下进口产品。对从境外进入海关特殊监管区域，再经办理报关手续后从海关特殊监管区域进入境内其他地区的产品，应当认定为进口产品。

特殊监管区域包括：保税区、出口加工区、保税港区、珠澳跨境工业区珠海园区、中哈霍尔果斯国际边境合作中心中方配套区、综合保税区等区域。

7.1.2不允许进口产品参投的项目，投标人所投产品中有进口产品的其投标无效．

7.1.3允许进口产品参投的项目，同时也允许满足实质性需求的国内产品参与投标．

**7.2扶持中小企业政策**

7.2.1专门面向中小企业(具体情形详见招标公告资格要求中的情形)采购的项目或者标项，不再执行价格评审优惠的扶持政策。

7.2.2.非专门面向中小企业采购的项目(或标段)，执行价格评审优优惠。

7.2.2.1根据符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）要求，对小微企业报价给予 20% 的扣除，用扣除后的价格参加评审；对于接受大中型企业与小微企业组成联合体的采购项目，对于联合协议约定小微企业的合同份额占到合同总金额 30%以上的，对联合体的报价给予 6 %的扣除，用扣除后的价格参加评审。**享受相关中小企业扶持政策的投标人，应在投标文件中提供《中小企业声明函》。**

7.2.2.2根据财库[2017]141号的相关规定，符合该文件第一条规定的残疾人福利性单位，视同小型、微型企业，享受评审中价格扣除政策，但投标人应在投标文件中提供残疾人福利性单位声明函。

7.2.2.3根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受中小企业扶持政策，但投标人应在投标文件中提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的声明文件。

7.2.3对于采购标的中有不同属性(货物、服务、工程）的采购项目，应当根据采购项目的属性来执行中小企业政策。享受中小企业扶持政策的供应商应当满足下列条件：在货物采购项目中，货物应当由中小企业制造，不对其中涉及的服务的承接商作出要求；在工程采购项目中，工程应当由中小企业承建，不对其中涉及的货物的制造商和服务的承接商作出要求；在服务采购项目中，服务的承接商应当为中小企业，不对其中涉及的货物的制造商作出要求。

**7.3节能环保**

7.3.1根据财财库〔2019〕9号文件要求，采购人采购的产品中有属于节能产品政府采购品目清单或环境标志产品政府采购品目清单内的，投标人所投的相应产品应在中国政府采购网（http://www.ccgp.gov.cn）中可查询到，如属于强制采购节能产品的，未查询到的其投标无效。

## 二、招标文件

**8.招标文件的组成**

8.1招标文件包括下列内容：

第一章采购公告

第二章投标须知和投标须知前附表

第三章招标项目要求

第四章开标、评标和定标须知

第五章投标文件的无效情形

第六章评标办法

第七章合同主要条款

第八章投标文件部分格式

8.2除7.1内容外，招标人在投标文件递交截止日前以公告形式发出的对招标文件的澄清或修改内容，均为招标文件的组成部分，对招标方和投标人起约束作用。

8.3上述所列7.1及7.2条内容均以公告内容为准，招标方的任何工作人员对投标人所作的任何口头解释、介绍、答复，对招标方和投标人无任何约束力。

8.4投标单位应认真阅读投标须知、合同条件、规定格式、项目要求、报价要求等招标文件所有的内容。如果投标单位的投标文件不能符合招标文件的要求，责任由投标单位自负。实质上不响应招标文件要求的投标文件将被拒绝。

**8.5招标方在“政采云”上设定的内容与招标文件的内容如有不一致的，以招标文件为准。**

**9.招标文件的澄清**

9.1投标人若对招标文件有任何疑问，应于投标须知前附表规定的时间以书面形式送（传真）向采购人和代理机构提出。投标人应仔细阅读和检查招标文件的全部内容。如发现缺页或附件不全，应及时向招标方提出，以便补齐。如有疑问，应在投标人须知前附表规定的方式及时间前以署名书面或传真形式要求澄清问题的文件，要求招标方对招标文件予以澄清。否则，由此引起的损失由投标人自己承担。

9.2无论是招标方根据需要主动对招标文件进行必要澄清，或是根据投标人的要求对招标文件做出澄清，招标方的书面澄清（更正）文件会在浙江省政府网上发布公告，同时“政采云”会向所有已按招标文件规定方式获取招标文件的潜在供应商发送更正提醒信息，潜在供应商请自行到浙江省政府采购网上下载澄清（更正）文件，在收到该澄清（更正）文件后应于1日内，以书面或传真形式（签署意见并加盖公章）向招标代理机构回函给予确认。过期未回复的，视为默认接受。

9.3投标人在前附表规定时间未提交疑问或质疑的，视作默认对本次招标过程中招标文件无异议，招标方对其提出的问题可以不予受理。

9.4招标文件澄清、变更、补充等内容均以浙江政府采购网公示的内容为准。当招标文件、招标文件的澄清、变更、补充等在同一内容的表述上不一致时，以最后在浙江政府采购网发出的公示内容为准。

## 三、投标文件

**10.投标文件的组成**

**10.1**投标文件由**资格响应文件**、**商务技术响应文件**和**报价响应文件**组成，以下的“格式”，指的是第八章投标文件格式中的表格；

**10.1.1资格响应文件：包含以下内容**

★①单位营业执照副本等经营资格证明文件扫描件（加盖电子签章）

★②义乌市政府采购项目投标承诺书（见格式）

③联合体协议（见格式）（★如供应商是联合体，则应提供本项材料）

④投标人实力与资信情况介绍或投标人认为需要提供的其他文件、说明等

**10.1.2商务技术响应文件：包含以下内容**

★①规范偏离表（见格式）

★②项目组成人员表（见格式）

③项目实施方案（格式自拟）

④根据评审需要、招标文件要求等，投标人自行考虑需提供的资料

**10.1.3报价响应文件：包含下列内容**

★①开标一览表（见格式）

★②项目成本报价表（见格式）

③中小企业声明函（见格式）（符合中小微企业有关政策的投标人需提供本项材料。投标人应根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准，填报企业规模类型。投标人也可在国务院客户端或工业和信息化部网站上，使用中小企业规模类型自测小程序识别企业规模类型。）

④残疾人福利性单位声明函（见格式）（符合残疾人福利性单位有关政策的投标人需提供本项材料）

⑤省级及以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的文件扫描件加盖电子签章（符合监狱企业有关政策的投标人需提供本项材料）

**11.投标文件编制要求**

11.1投标人应仔细阅读招标文件，了解招标文件的要求，在完全了解招标项目的技术要求和商务要求后，编制投标文件。

11.2在招标文件对技术要求中，投标人必须充分应答和满足用户的强制性的需求，如“★”等，否则将导致无效标。

11.3编制的投标文件对招标文件中有关条款未提出异议的，均被视为接受和同意。

11.4投标人应根据电子投标操作指南按本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。

11.5由于未按招标文件的规定要求编制投标文件，导致评审小组作出的对投标人的误判，责任由投标人自己承担。

**12.投标文件的语言及度量衡单位**

12.1投标文件和与投标有关的所有文件均应使用中文简体字。

12.2原版为外文的证书类文件，以及由外国人作出的本人签名、外国公司的名称或外国印章等可以是外文，但应当提供中文翻译文件并加盖电子签章。

12.3除工程规范另有规定外，投标文件使用的度量衡单位，均采用中华人民共和国法定计量单位。

**13.投标报价**

13.1投标人应根据国家的有关规定和招标文件要求并结合企业的实际情况进行投标报价。投标报价以人民币为结算货币，投标报价须包括因承包本次采购项目服务所需的服务费、线路租赁费（如有）、货物价款（备品备件）、项目软硬件费用、人员费用、运输费、装卸费、利润、税金、保险及不可预见费用等一切费用，应是招标文件确定的招标范围内的全部工作内容的价格表现，完成该项目的所有费用及各环节所必需的连带工作或服务、成果验收、以及政策性文件规定、合同包含的所有风险责任等所有费用。如有漏项，视同已包含在本报价中，投标单价及总价不做调整。

13.2投标人应在投标文件的《开标一览表》上写明投标报价项目的单价及总价。

13.3中标后，中标人所填写的报价在合同实施期间不因市场变化因素而变动，投标人在计算报价时应考虑一定的风险系数。

13.4投标人应按招标文件规定的报价格式进行投标报价。投标人对每种货物只允许有一个报价，招标方不接受任何有选择性的报价。

13.5招标方不接受低于成本的投标报价。

13.6投标人按照上述要求编制投标报价。一旦确认某一投标人中标，除合同规定的可调整内容外，中标人不得要求追加任何费用。

13.7须由中标单位开具正式发票。

13.8招标文件中规定由投标单位承担并支付的相关费用在投标报价时应一并考虑。

**14.投标文件格式**

投标人提交的投标文件应当使用招标文件所提供的投标文件格式，表格格式在不改变格式内容的情况下可自行制作。在所提供表格格式之外，投标人可以增加自行设计的表格及内容，以便更细致全面的说明其能力。

**15.履约保证金：**无

**16.投标有效期**

16.1投标文件从开标之日起，投标有效期为90天。

16.2特殊情况下，在原投标有效期截止之前，采购人可要求投标人同意延长有效期，这种要求与答复均应以书面形式提交。投标人可拒绝这种要求，接受延长投标有效期的投标人将不会被要求和允许修正其投标。

## 四、投标文件的递交

**17.电子投标文件上传的地点和截止时间**

投标人应在投标截止时间（2022年11月17日09:30）之前上传投标文件，同时，投标人可在投标截止时间前将在“政采云”上最后生成的具备电子签章的备份投标文件以电子邮件方式传送至义乌市政府采购中心邮箱（ywszfcgzx@163.com），传送的备份投标文件（文件名采用“采购编号+投标人名称+系统自动生成的后缀名”）需打包压缩并加密，加密密码由投标人自行保管。为了防止泄密，建议投标人在设置加密密码时采用大小写字母加数字的组合方式。**投标供应商仅递交备份投标文件的，投标无效。**

**18.投标文件的补充、修改与撤回**

18.1投标人在“政采云”上提交投标文件以后，在规定的投标截止时间之前，可以重新补充修改或撤回已上传的投标文件，补充、修改的内容为投标文件的组成部分。

18.2在投标截止时间之后，投标人不得对其投标做任何修改。

18.3从投标截止时间至投标人在投标书格式中确定的投标有效期期满这段时间内，投标人不得撤回其投标。

**19.投标文件解密**

本项目采用线上开标，供应商无需到开标现场，但应准时在线参加。开标时间后采购中心开启解密。开启解密后的1小时内，供应商应当登录“政采云”，用“项目采购-开标评标”功能解密投标文件。

如政采云上投标文件在规定时间内出现解密失败的，投标人可按照自身意愿确认同意提供加密密码，启用备份文件，并由采购中心把备份文件上传至“政采云”。如投标人未按照规定时间（2022年11月17日上午09:30前）及要求提供有效备份标书，同时政采云上投标文件解密失败的，将导致投标无效。

如果投标人发送两份以上备份文件的，以最后收到的那一份为准，通过“政采云”上传递交的“加密投标文件”已按时解密的，“备份投标文件”自动失效。

## 五、其它

**20.本招标文件解释权归“招标方”。**

# 第三章 招标项目要求

## **一、项目概况**

义乌信息经济发展迅速，信息基础设施、业务服务平台及智慧服务应用均走在省内前列，义乌“最多跑一次”改革跑出了新步伐，“义网通办”业务快速落地，各类政府数据资源充分整合，政务数据资源目录体系和交换体系初步建成，业务协同能力稳步提升。自然人、法人、地理信息和宏观经济等基础数据库基本建成，各类专业数据库建设有序推进，便民类智慧服务应用初显成效，数据安全管理和建设工作稳步推进，但顶层设计有待加强，标准规范不够健全，针对义乌数据资源中心信息共享和开放业务，缺乏统一的安全顶层设计和统筹规划，对于政务信息系统的架构、数据的分类分级、数据共享开放的渠道安全、数据共享开放的过程安全等缺乏统一的规范和指导。

义乌数据中心机房包括三个机房，江东机房、宾王机房、联通机房。目前江东机房已经完成了政务云安全资源的部署，保障委办局的业务数据。数据安全层面已经部署数据安全管控、数据分级分类、数据审计等安全产品，构建数据安全相应的安全能力。同时，包括政务外网、感知网等多个基础网络都规划网络安全建设体系，其他相关的安全基础建设、管理制度、运营体系正在逐步完善。

义乌市数据管理中心为健全自身网络安全以及数据安全防护和监测能力，拟于2022年启动全链路网络安全监管服务采购，汇聚全区各部门本地沉淀数据及相关部门的应用。一方面可大大提升基础资源的利用率，提高工作效率和服务能力；另一方面可以利用丰富的数据资源，结合行业业务将理论、业务、技术三方融合，为领导层决策提供依据、为政策制定提供建议、为政策落实提高精准度。

根据省大数据局下发的《浙江省电子政务外网安全评估指标体系》等工作要求，采用预防性建设为主、检测响应为辅的思路，以“安全能力服务化，安全服务集约化”为设计原则，构建覆盖义乌市、县（市、区）云、网、端、边界、数据全链路网络安全保障体系。以合规为基线，以业务流程为导向，建立完善的网络安全保障和监管措施。同时，将原本零散的安全数据变成统一规范的安全数据资源提供安全运营支撑能力。引入高水平网络安全运营服务，有效支撑日常安全运营管理工作，将安全运营工作与各个支撑单位与组织联动起来，建立立体化的安全运营模式。

## **二、项目采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务大类 | 服务子类 | 服务描述 |
| 1 | 全链路监管定制服务 | 立体化跟踪通报，多维度考核服务 | 详见“具体服务技术要求” |
| 2 | 政务云安全资源池服务 | 安全资源池管理服务及能力服务 |
| 3 | 网络安全数据分析服务 | 资产数据治理服务 |
| 网络威胁情报中心服务 |
| 4 | 政务数据安全防护服务 | 日志采集及审计分析系统预处理节点服务 |
| 数据分级分类服务 |
| 数据脱敏服务 |
| 数据管控服务 |
| 数据加密服务 |
| 数据安全态势感知服务 |
| 5 | 政务应用安全防护服务 | 应用防护服务 |
| 政务云应用监测服务 |
| 6 | 政务外网终端安全服务 | 终端安全主机防护服务 |
| 终端安全零信任控制服务 |
| 7 | 政务用户行为分析服务 | 用户行为分析（UEBA）服务 |
| 蜜罐系统服务 |
| 8 | 驻场人员安全运营服务 | 驻场服务 |

## **三、项目技术要求**

## **1.全链路监管定制服务**

## **1.1监管定制服务**

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 覆盖云、网、端、边界、数据、应用、行为，构建全链路防护、检测、预警、处置、反馈体系以及在数字化改革应用、关键信息基础设施等重要节点按照“四个同步”要求，建立覆盖边界、终端、数据、应用、行为全链路安全技术防控体系，并完成以下对接工作：1. 数据对接。根据省大数据局下发的《浙江省电子政务外网安全评估指标体系》等上级工作要求，协助采购人完成与上级安全监管平台的上述六个维度数据对接与数据上报工作。（须在投标文件中具体阐述数据对接方案及承诺书）

2.业务流程对接。根据采购人实际业务需求，完成与上级监管平台的业务贯通工作，达到上级通报能直接流转至义乌各单位的目标。（须在投标文件中具体阐述业务流程对接方案及承诺书） |
| 公告栏服务 | 总体描述 | 提供立体化跟踪通报全流程周期，可以多维度展示通报工作开展情况，对网络安全工作进行监督考核。 |
| 事项看板服务 | 提供看板信息展示，包括通报、预警信息等，可以对整个信息发布过程进行跟踪记录。提供信息下钻，点击通报、预警信息，可以查看对应详情，如通报标题、创建时间等 |
| 通报总览服务 | 提供展示各个区域的通报情况，包括处置及时率、完结率、总量、逾期量，并以图表方式展示 |
| 预警中心服务 | 总体描述 | 提供对网络安全事件或威胁发出通知或者预警，以警示相关单位。 |
| 通知管理服务 | 通知中可记录通知名称、标签、级别、详情、通知对象和举证信息通知举证信息可一键溯源，包括溯源到资产档案、系统档案、情报信息、原始日志等。 |
| 预警管理服务 | 预警中可记录预警名称、标签、级别、详情、预警对象和举证信息 |
| 通报中心服务 | 总体描述 | 提供通过安全事件或风险隐患发布通报的服务，以督促相关单位妥善处置网络安全事件。 |
| 通报管理服务 | 提供通报流程统计的服务，可根据多维度查询展示通报信息。通报详情可显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等通报流程可配置，各流程的对应的处置单位可自动生成，并可自定义调整提供对通报进行超时设置的服务，针对截止时间一天内的通报进行截止时间醒目提醒；针对已超时的通报进行超时显示，并显示具体超时时间 |
| 互联网外发服务 | 通报外发审批服务 | 提供新增通报、预警、通知的服务 |
| 通报文件导入服务 | 提供导入通报、预警、通知信息的服，并且可查看。 |
| 防控中心服务 | 网络安全防护服务 | 可一键封禁IP、批量解禁/封禁IP。可查看有封禁历史IP的封禁历史详情服务；可展示指定时间范围内封禁和解封次数统计；可展示指定时间范围内封禁/解封操作的时间、封禁/解禁操作、操作用户名、阻断时间等 |
| 应用安全防护服务 | 可一键关停/开启、批量关停/开启应用。可查看应用的关停历史详情；可展示指定时间范围内关停和开启次数统计；可展示指定时间范围内关停/开启操作的时间、关停/开启操作、操作用户名等 |
| 等保自助服务 | 自主注册服务 | 管理端可对注册填报页面的字段开启关闭及是否必填、附件上传、附件别名设置、模版上传、模板下载等进行灵活设置注册账号可与单位关联，注册成功后等保自动创建单位信息并同步到全息档案，实现等保与全息档案及其他模块业务打通。 |
| 在线备案子系统服务 | 系统定级服务 | 提供单位端自主定级、在线填报定级信息及线上选取或抽取定级专家的服务。可开通定级专家账号，定级专家登录平台后查看系统定级信息，专家组长给出定级评审意见并确认提交 |
| 在线备案服务 | 提供系统定级、备案申请、提交测评结果、异地测评申请、发证申请、备案变更、备案撤销申请及管理端对各环节的审批等操作的服务。可对备案数据可视化流程查看，包括查看任意节点审批人对备案编号可手动修改，并可验证修改后的唯一性、合规性，且修改权限可通过配置页面进行控制。提供备案申请的多种导入方式，包括手动输入、备案表导入、测评机构rar包导入等多种方式。发证申请领取证明方式可以选择，包括邮寄填报地址及自取网点选择。对备案单位、系统流程操作环节形成历史记录，以方便回溯。 |
| 智库搜索服务 | 关键字搜索服务 | 提供精准搜、全库搜、场景搜，并可跳转到高级搜索。可对历史搜索记录进行保存并快速传入历史查询条件。提供对数据库的数据量统计，信息描述，数据入库更新时间以及快速入口。可对全平台业务资产数据的关系图谱展示。 |
| 全库搜服务 | 情报库服务 | 提供对情报数据信息的检索、展示。 |
| 黑客库能服务 | 提供对黑客库数据信息的检索、展示。 |
| 恶意IP库服务 | 提供对恶意IP库数据信息的检索、展示 |
| 恶意域名库服务 | 提供对恶意域名库数据信息的检索、展示。 |
| 案件库服务 | 提供对案件数据信息的检索、展示。 |
| 事件库服务 | 提供对安全事件数据信息的检索、展示。 |
| 网络资产库服务 | 提供对网络资产数据信息的检索、展示。 |
| 等级保护基础库服务 | 提供对等级保护基础（单位、系统）数据信息的检索、展示。 |
| 关基基础信息库服务 | 提供对关基基础信息（单位、系统、人员、机房）数据信息的检索、展示。 |
| 漏洞库服务 | 提供对漏洞库数据信息的检索、展示。 |
| 木马病毒库服务 | 提供对木马病毒库数据信息的检索、展示。 |
| 技战法应用服务 | 技战法模型服务 | 提供技战法模型所产生的数据集的服务，即技战法应用的检索，进入数据集之后可进行简单的查询。 |
| 可用性监测服务 | 资产可用性服务 | 可对资产监测任务、IP资产及监测业务系统进行管理。 |
| 高危端口监测服务 | 高危端口服务 | 提供对高危端口信息进行集中管控，可进行新增、删除操作。可根据各端口涉及的资产数量进行排序，按顺序从左到右换行展示，点击更多跳转至高危端口页面。 |
| 网络资产认领服务 | IP认领服务 | 资产认领页面用于扫描引擎发现当前资产列表中没有的数据时，进行展示处理。提供对单位名称（字符串）、资产IP、资产来源（按扫描引擎过滤）等相关字段查询。提供资产列表通过IP、所属单位、单位负责人、发现时间、资产来源、操作等字段展示。 |
| 网络安全知识库服务 | 知识库管理服务 | 可建立安全知识库，包括法律法规文件、标准规范文档、接口对接规范文档、标准解读等，且可以进行上传、下载。提供知识库文档权限设置，可设置完全公开、仅限本部门公开。 |
| 标准规范服务 | 提供新增制度规范，录入信息包括但不限于名称、附件、备注及制度制定单位。提供查看制度、编辑制度内容、以及删除操作的服务。对上传的png、doc、docx、pdf、jpg、jpeg文件可进行直接查看。可对文件开放范围进行完全公开或仅限部门公开权限控制 |
| 工作汇报服务 | 工作汇报服务 | 可通过标题、优先级、上报单位、上报时间、更新时间查询消息展示的消息包括标题、优先级、上报单位、上报人、上报时间、更新时间可对消息编辑，编辑内容包括消息标题、优先级、消息内容、接收人、可见范围，支持上传附件和发送消息消息详情显示标题、优先级、上报单位、上报人、接收人及单位、上报时间、更新时间、详情、已读、未读以及评论内容对工作汇报可进行标签，比如工作日报、工作周报、工作月报、会议纪要等。对工作汇报内容可指定接收人，并控制接收人是否可转发操作，支持对接收人进行汇报评论。（投标文件商务技术响应文件中提供佐证材料）对工作汇报可进行查询、新增、删除、查看等操作。 |
| 内生案例管理服务 | 内生隐患案例服务 | 提供通过隐患名称、标题、编号、简介查询相应案例。提供对已有的隐患案例进行编辑。提供对已有的隐患案例进行打标和编写批注操作。提供手动录入已有的隐患案例。 |
| 内生事件案例服务 | 可通过攻击描述、标题查询相应事件案例。对已有的事件案例可进行编辑。对已有的事件案例可进行打标和编写批注操作。可手动录入已有的事件案例。 |
| 内部归档管理服务 | 提供接入内部推送的事件信息并形成相应案例。 |
| 教育培训管理服务 | 教育培训管理服务 | 对宣传管理、教育培训可进行管理。内容包括：标题、时间、地点、与会内容、正文内容、接收人、通知方式等。教育培训消息通知方式可控制，可通过平台通知、短信通知。 |
| 检查总览服务 | 检查总览服务 | 提供根据检查计划筛选总览统计范围。提供对最新检查计划的进展进行实时跟踪呈现。提供对被检查单位的行业分布进行统计分析。提供对支撑单位的检查支撑情况进行统计和排序。 |
| 检查计划管理服务 | 计划执行详情页服务 | 提供相应的任务负责人、检查人员、被检查单位用户通过办理功能进行的计划的执行。提供对不同用户对处于不同状态的现场检查任务、远程检查任务、单位自查任务进行相应的处置操作。提供各种类检查负责人对自己负责的检查种类进行检查任务的新建、查看、删除等操作。 |
| 现场检查任务服务 | 现场检查任务至少包含待下发、任务签收、结果填报、结果签收、单位整改、整改审核和办结等状态。在同一个现场检查任务下发时可选择单位、系统等多个现场检查对象，同时可针对每一个对象配置相关检查表单提供在现场检查任务结果填写完毕提交时自动统计本次任务发现的各等级漏洞数量。对将检查通知书、检查记录表、整改通知书、单位整改报告等文书通过流程各环节上传到相应的现场检查任务可进行留档。在特殊情况下对现场检查的单条或多条任务可进行一键直接办结。 |
| 远程检查任务服务 | 远程检查至少包含待下发、任务签收、结果填报、结果确认、结果签收、单位整改、整改审核和办结等环节。对同一次远程检查任务新建时选择的属于同一个单位的多个系统自动合并成一个远程检查任务，在下发任务时支持选择特定的支撑单位。（投标文件商务技术响应文件中提供佐证材料）提供在远程任务结果填写完毕提交时自动统计本次任务发现的各等级漏洞数量。对将远程检查授权书、渗透设备信息、渗透报告通过流程各环节上传到相应的远程检查任务可进行留档。在特殊情况下对远程检查的单条或多条任务可进行一键直接办结。 |
| 单位自查任务服务 | 单位自查至少包含待下发、任务签收、结果填报、结果审核和办结状态。提供在同一个单位自查任务下发时选择单位、系统等多个自查对象的服务，同时实现对每一个对象配置相关检查表单。（投标文件商务技术响应文件中提供佐证材料）对单位自查相关的检查通知书、自查报告等文书通过流程各环节上传到相应的单位自查任务中可进行留档。在特殊情况下对现场检查的单条或多条任务可进行一键直接办结。 |
| 检查要素管理服务 | 检查模板管理服务 | 对检查项可进行独立管理，可对检查项进行新增、查看、编辑、删除等操作。对检查表可进行独立管理，可形成检查事项清单，可对检查表进行新增、查看详情、编辑、删除等操作。提供在同一张检查表下新建多个检查模块的服务，可为每个模块配置模块名称并导入相应的检查项。（投标文件商务技术响应文件中提供佐证材料）提供上移、下移等操作项服务，实现对检查模块下的检查项的顺序进行手动调整。在编辑已有检查表时可通过另存功能复制出一张相同的检查表。 |
| 检查对象管理服务 | 可通过列表展现检查对象库，展示内容包括单位名称、区域、单位类型、所属行业、单位标签等批量导入时可实现通过区域、行业、标签、类型等维度进行单位查询和选中。可通过查看动作对检查对象库中的单位关联的各类信息进行聚合展示。 |
| 支撑单位管理服务 | 可通过列表展示支撑单位清单，展示内容包括单位名称、所属区域、单位标签、单位联系人等。可通过导入功能将用户管理功能下已添加的支撑单位进行选择并导入到支撑单位清单中。可通过查看动作对支撑单位清单中的单位详情进行查看，信息包括单位名称、单位官网、单位标签、单位类型、单位行业、所属区域等。 |
| 检查人员管理服务 | 可通过列表展示检查人员库的服务，展示内容包括姓名、归属单位、用户标签、用户角色等。可通过导入功能将用户管理功能下已添加的支撑单位人员进行选择并导入至检查人员库中。可通过查看动作对检查人员库中的人员详情进行查看，信息包括真实姓名、归属单位、用户角色、用户标签、邮箱地址、手机号码、用户在线时段统计、用户登录情况等。 |
| 考评任务服务 | 考评任务服务 | 可管理考核评价任务，包括启动、编辑、查看、排名、办结、删除。可通过任务时间、创建单位、任务状态、标签、关键字（任务名称、联络人）查询考评任务。可通过单位名称、单位组、所属区域、所属行业、单位直属性质、单位类型选择评估对象。可通过专家名称、所属单位、专家组选择评分专家。可通过单位名称、单位任务状态查询考评任务的单位 可查看考评任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称。可展示单位任务状态及状态变更时间、总分、排名、材料完整度。可查看单位任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称和提交/操作的操作时间、操作账号。可对考评任务进行排名，提供柱状图展示考评任务单位排名、饼状图展示各分数等级分布；提供展示单位排名总分列表，包括单位名称、所属区域、单位类型、单位联系人、联系方式、单位直属性质、得分等；提供展示单位排名各项列表，包括单位名称及各一级评估项小计；可通过单位名称、单位直属性质查询单位；可下载排名明细，包括单位总分、排名情况及各评估项得分明细。（投标文件商务技术响应文件中提供佐证材料） |
| 考评配置服务 | 考评模板服务 | 可管理考评模板，包括新增、查看详情、编辑、删除。可展示模板名称、模板说明、创建人、最近修改时间。可编辑考评模板的模板名称、模板说明的服务。可识别并解析上传的表格，可预览考评表、编辑考评表单元格、增加行、删去行、上下移动行，可下载编辑的考评表。可查看考评模板的考评表内容，包括检查项内容、检查项等级、提示内容、总分、检查项类型。 |
| 考核对象服务 | 可管理单位组，包括新增、编辑、删除。可编辑单位组名称、说明以及选择、删除、批量删除专家组中的专家，可通过专家名称、所属单位、专家组查询并选择专家。 |
| 评分专家服务 | 可管理专家组，包括新增、编辑、删除。可编辑专家组名称、说明以及选择、删除、批量删除单位组中的单位的服务，可通过单位名称、单位组、所属区域、所属行业、单位直属性质、单位类型查询并选择单位。 |
| 考评填报服务 | 考评填报服务 | 可填报、查看考评填报任务。可展示考核评价任务的任务名称、任务时间、单位填报时间、单位任务状态、创建单位、总分、当前排名、材料完整度等信息。可通过任务时间、创建单位、单位任务状态、标签、关键字（任务名称、联络人）查询考评任务。可以暂存、提交、重复提交考评表材料项、备注项填报单位任务；可以根据填报情况自动计算预得分、材料完整度；可展示任务信息，包括任务状态、任务时间、单位填报时间、任务说明、任务联络人及其联系方式、任务附件；可展示单位任务状态及状态变更时间；可查看单位任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称和提交/操作的操作时间、操作账号。 |
| 考核评分服务 | 考核评分服务 | 可对考核评分任务进行评分。可展示考核评分任务的任务名称、任务状态、任务时间、单位填报时间、创建单位、任务联络人及其联系方式、考评进度。可通过任务时间、创建单位、任务状态、标签、关键字（任务名称、联络人）查询考评任务。 |
| 监测评估服务 | 评价报告服务 | 提供按照报告来源、统计时段、创建时间等维度对考评报告进行筛选。可一键展开报告，包括查看单位通报TOP10、评分分布情况。提供对考核对象的评分进行编辑时增加自定义的加分、扣分项并保存。可在考评报告列表和考评报告详情中导出相应考评的结果。提供创建实时考评任务，生成实时考评报告。可在实时考评报告中对考评规则进行优化调整。 |
| 评价任务服务 | 可通过关键字（任务名称、接收人）、考评范围、考评周期、启用状态等条件对考评任务进行搜索。可在新建考评任务时确定考核对象的类型和考评范围。可按不同周期进行考评，且可对考评起止时间点进行选择。提供自动订阅服务，且用户可以自主选择接收对象。可按照设定好周期、范围、规则，自动定期生成考评报告。 |
| 评价规则服务 | 可针对风险隐患、安全事件、通报情况三个维度设置考评规则表。可针对每一个维度的扣分上限进行设置。可按照风险隐患维度设定，至少包括对紧急、高危、中危、低危漏洞的扣分方案进行设定。可按照安全事件维度设定，至少具备对特别重大、重大、较大、一般网络安全事件扣分方案进行设定。可按照通报维度进行设定，至少具备对未处置、逾期、被退回通报扣分方案进行设定。 |
| 活动管理服务 | 单次活动管理服务 | 可新建活动，包括活动名称、活动地点、摸底、临战、备战、决战阶段的时间进度、活动负责人及联系方式、活动描述，同时对活动可进行编辑、删除、结束等操作。提供下钻到具体某个活动，查看活动详情。 |
| 作战台服务 | 可展示活动各阶段的进程并突出当前所处进程。可列表显示待办工作的服务，包括通报处置待办、指令待办，通报处置待办标识处置状态及通报类型，指令待办标识指令状态及指令类型。可列表显示跟进工作的服务，包括通报处置跟进、指令跟进，通报处置跟进标识处置状态及通报类型，指令跟进标识指令状态及指令类型。 |
| 里程碑管理服务 | 可按里程碑名称、里程碑时间查询里程碑。可对里程碑进行新增、修改、查看、删除操作。（投标文件商务技术响应文件中提供佐证材料） |
| 安保组织服务 | 指挥人员服务 | 提供说明指挥人员的作用，指挥人员是安保活动的组织领导人员，负责领导和决策安保活动的重大事宜，包括提供筹备组织、制度信息，指挥调度安保活动。可单个或批量设置指挥人员的角色，包括但不限于组长、副组长、组员。可通过人员名称、标签、单位名称、区域等条件查询人员列表。 |
| 指挥单位服务 | 提供说明指挥单位的作用，指挥单位是安保活动的组织领导机构，负责领导和决策安保活动的重大事宜，包括提供筹备组织、制度信息，指挥调度安保活动。可从已录入单位中批量选择指挥单位，单位信息包括但不限于单位名称、标签、上级单位、所属区域、单位类型。可通过行业类型、标签、所属区域、单位类型、单位名称、联系人、手机号等条件查询单位列表。 |
| 安保人员服务 | 提供说明安保人员的作用，安保人员是安保活动的被监管单位人员，负责安保系统的日常管理和维护，落实保障工作，参与应急演练和培训，以及处置安全事件和应急事件。可从已录入用户中批量选择安保人员，人员信息包括但不限于人员名称、标签、联系方式。可通过人员名称、标签、单位名称、区域等条件查询人员列表。 |
| 安保单位服务 | 提供说明安保单位的作用，安保单位是安保活动的被监管单位，负责安保系统的日常管理和维护，落实保障工作，参与应急演练和培训，以及处置安全事件和应急事件。可通过行业类型、标签、所属区域、单位类型、单位名称、联系人、手机号等条件查询单位列表。 |
| 安保系统服务 | 提供说明安保系统的作用，安保系统是安保活动的被监管单位的系统，在安保期间由安保人员保障系统的安全运行。可通过行业类型、标签、所属区域、系统重要性、系统类型、系统名称、访问地址等条件查询系统列表。 |
| 支撑人员服务 | 提供说明支撑人员的作用，支撑人员主要由安保技术人员和安保专家组成，负责制定安全事件应对方案、协同调度方案，提供技术支持等。可通过人员名称、标签、单位名称、区域等条件查询人员列表。 |
| 支撑单位服务 | 提供说明支撑单位的作用，支撑单位主要是各安服厂商或网络安保单位，负责制定安全事件应对方案、协同调度方案，提供技术支持等。可通过行业类型、标签、所属区域、单位类型、单位名称、联系人、手机号等条件查询单位列表。 |
| 安保驻点服务 | 提供说明安保驻点的作用，安保驻点是从指挥中心、安保目标、支撑力量三大角色的人员中选调到安保活动现场驻点，负责驻点的安全运行。（投标文件商务技术响应文件中提供佐证材料）可新增安保驻点，录入信息包括但不限于驻点名称、保障单位、驻点管理员、驻点人员、关联探针、标签、经纬度、驻点地址。可通过标签、驻点名称等条件查询驻点列表。 |
| 安保制度服务 | 信息公告服务 | 可新增信息公告，录入信息包括但不限于标题、正文、附件。指挥人员可发布正式的公开的信息至该次活动全部参与单位、人员以便实现重大安全事件信息的及时披露和共享。 |
| 安保制度服务 | 提供指挥人员维护该次安保活动的各项规章制度，安保活动各方参与人员可查看对应的规章制度。可新增安保制度，录入信息包括但不限于名称、附件、备注。 |
| 应急预案服务 | 提供统计服务，包括按不少于预案等级一级、二级进行统计，按不少于预案分类综合、现场、临时进行统计。可新增应急预案，录入信息包括但不限于预案名称、预案等级、预案分类、提交单位、预案描述、附件。 |
| 安保值守服务 | 安保驻点端服务 | 提供驻点管理员安排本驻点小组的值守排班日历计划，通过修改等操作可以设置该次安保活动的排班人员。可通过日历快速查看每天的驻点安全情况，通过切换日期可查看活动期间具体的驻点安全情况。可统计本驻点小组实时排班班次，比如驻点人员签到、签退情况的统计。 |
| 指挥中心端服务 | 提供指挥人员安排所有驻点小组的排班班次，通过修改等操作可以设置该次安保活动的排班班次的。可通过日历快速查看每天本次活动所有驻点的安全情况，通过切换日期可查看活动期间具体的驻点安全情况。可查看总体驻点报平安情况，包括查看驻点人员签到、签退情况。可查看单个驻点的具体安全情况，包括但不限于驻点基本信息、报平安情况、保障单位信息、驻点人员信息、关联探针信息。 |
| 值守移动端协同服务 | 驻点人员可在钉钉微应用上进行签到、签退和报平安等操作。驻点人员可在钉钉微应用上对指挥人员下发的指令进行回复，回复内容包括但不限于上报内容、附件。 |
| 指挥调度服务 | 指令发起服务 | 可向对应驻点小组下达调度指令，包括不少于签到、报平安、任务、其他等4种类型的调度指令任务，指令内容包括指令编码、调度类型、调度驻点、调度任务，并可以实现自定义下发应急预案。 |
| 通报发起服务 | 可直接在图上发布事件通报，当有事件发生时，通过发布事件通报以责令相关单位进行整改。 |
| 总览视图服务 | 可显示安保指挥部的负责人员，当日值班的指挥人员。提供支撑可视化展示安保活动的组织架构。提供安保单位、安保系统、安保人员、支撑人员、驻点小组、探针设备的数字信息，并且可通过对应名称进行筛选。提供监测、通报、值守、调度视图的总览信息，包括但不限于日志数据、攻击告警数、已发指令数、已发预案数、事件通报数、隐患通报数、报平安数、报事件数、指令列表、通报列表。 |
| 监测视图服务 | 可展示单位下安全监测情况，包括日志数据、攻击告警。可对发现的安全事件或风险隐患进行统计。地图突出显示有安全事件或风险隐患的单位，并且可查看具体单位情况。 |
| 通报视图服务 | 展示通报总数，以及对不少于处理中、已完成、今日新增等3种维度的统计。可对事件通报、隐患通报分别细化到状态维度统计。提供列表形式展示最近通报，并且可查看通报详情。地图突出显示有通报的单位，并且可查看具体单位情况。 |
| 值守视图服务 | 通过统计功能展示查看当天的驻点排班情况、签到、报平安情况。地图突出显示异常驻点，并且可查看具体驻点情况。可按时段统计驻点上报情况。 |
| 调度视图服务 | 提供按不少于报平安、签到、任务、其他等4个维度统计指令下发情况。可统计指令设计的驻点数及单位数。 |
| 活动快照服务 | 可按日期、时刻或里程碑选择某个时间点，可从该时间点开始回放历史大屏内容。提供开始、暂停、重新播放、结束活动回放。 |
| 大屏配置服务 | 可针对具体的单次活动提供详细的配置管理，包括活动名称、标题logo、标题颜色。可自定义维护该次活动的组织架构。提供配置大屏显示的在线人数。提供配置安保单位、安保系统、安保人员、支撑人员、驻点小组、探针设备的别名及是否显示。提供配置五大视图的数据、别名及是否显示。 |
| 总体描述 | 作为大数据态势感知平台的移动端延伸，满足独立性和安全性要求，完全自主可控，不依赖钉钉、微信等第三方平台，为用户提供便捷入口，具备查看平台和操作部分重要业务的能力。 |
| 整体参数 | 可将APP端和Web端横向打通，关联数据和业务。 |
| 工作台服务 | 提供“预警”、“通报”、“通知”数量统计，点击查看对应的详细信息。提供“最新通报”、“最新通知”、“最新预警”的提醒服务。可在移动端快速处置通报、完成相关操作。可通过标题、编号进行模糊搜索匹配。可对通报过程进行跟踪记录，完整记录任务流转过程详情并同步到Web端平台 |
| 掌上态势服务 | 可根据区域、行业、时间查看单位、系统监测情况。可通过地图查看实时监测情况，包括网络攻击、安全隐患、安全事件。可查看实时网络攻击情况、攻击趋势。可查看通报业务开展情况。 |
| 运营报告服务 | 可通过运营报告查看平台运行情况，包括实时监测、通报预警、全息档案等信息。可根据报告类型、报告标题、生成时间、阅读状态查看运营报告。可查看最新报告、实时报告、日报、周报、月报、季报、年报。 |
| 追踪溯源服务 | 具备实体间网络关系的多级钻取的能力，具备>10跳的流量关联关系分析的能力，具备通过端口、协议、异常访问类型过滤关联关系的能力。（投标文件商务技术响应文件中提供佐证材料）纵观全网IP资产和互联网服务，具备>2000个资产的实时风险评级和分析画像的能力。IP画像中时序型分析包括网络流量、访问频率>3个维度，统计型分析包括访问来源、访问目标、域名、服务端口等>5个维度。实体不同时间段内的风险行为记录和弱点信息，风险行为记录包括风险原理描述和处置建议。实体相关信息包括资产信息、情报信息、地理位置、运营商信息；具备结合云端数据，提供攻击者信息画像的能力，记录攻击者的IP所在地、首次作恶时间、上次活动时间、攻击次数、被攻击详情等信息。能够基于大数据分析及分析规则为用户提供严重后门入侵安全事件的分析回溯，实现对黑客攻击行为的完整分析回放。 |
| 可视化中心服务 | 具备可视化图表类型>=15种的能力，包括但不限于时序图、饼图、柱状图等。统计类图表具备展示升序或降序的TOP5到TOP100，可针对数据中任意字段的计数、平均值、求和、最大值、最小值、唯一值等>=5种算子的统计结果配置可视化图表的能力。可视化图表可通过拖拽配置组装成仪表盘，仪表盘不少于7种布局类型，每张仪表盘可包含>=50个可视化图表，可视化图表具备导出WORD、PDF的能力。仪表盘展示时具备时间范围自定义选择的能力，具备放大聚焦某个图表的能力。 |
| 报告中心服务 | 提供报告内容自定义的服务，包括标题、图表、报表自定义，其中支持的图表类型>=15种。可导出日报、周报、月报和自定义时间范围内的安全分析报告。报告订阅具备通过邮件方式在设定时间点发送日报、周报、月报到不同邮箱的能力，可配置订阅规则数量>=10条，报告格式支持WORD、PDF等。 |
| 知识库服务 | 内置漏洞知识库包含漏洞等级、漏洞名称、漏洞分类、CVE编号、CNNVD编号、漏洞解决方案、参考网址等信息。 |
| 共享总览服务服务 | 平台申请者对数据共享接口应用的整体概览情况：数据传输量、排名概况、数据共享趋势。提供时间筛选以及报表导出的服务。 |
| 标准接口服务 | 提供标准接口的信息展示的服务，包括基本信息、请求参数、返回参数、错误码等相关信息。标准接口包含且不限于执法检查现场检查新增任务接口、执法检查远程检查新增任务接口、执法检查对外新增计划接口、执法检查单位自查新增任务接口、安全情报上报接口、安全隐患数据上报接口、安全事件数据上报接口、通报预警归档上报接口、通报预警下发接口、通报预警反馈上报接口、业务指标共享接口、安全情报查询接口。提供标准接口对接说明文档的下载。提供标准接口检索的服务。 |
| 账号管理服务 | 提供接口账号申请管理，包括接口授权、账号鉴权等信息的服务。提供openAPI接口使用者画像管理。提供接口使用这检索的服务。 |
| 日志审计服务 | 提供账号调用数据共享接口的日志说明的服务。提供日志检索的服务。 |
| AI异常检测服务 | 具备UEBA、Bayes、随机森林等长周期高级机器学习算法的能力。（投标文件商务技术响应文件中提供佐证材料） |

## 2.政务云安全资源池服务

## 2.1安全资源池管理服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 为义乌政务云三个节点（即宾王节点、北苑节点、江东节点，以下简称三节点）提供云租户的网络安全资源服务。需完成云资源池部署，以及与政务云平台的对接工作，包括三节点安全资源池的硬件环境（预估为400个虚机体量的资源要求）部署，以及三节点的云内网络对接工作。预采购数量为70个租户，超过预采购数量的服务须承诺免费提供。（提供安全资源的软硬件集成实施方案及服务承诺书） |
| 云安全服务 | 能够利用虚拟化资源为用户提供一站式安全解决方案，至少包括下一代防火墙、web应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全（EDR）、APT等安全能力； |
| Web应用防火墙、主机安全、网站监测等虚拟安全组件支持多租户共享架构的，即通过一套虚拟安全组件向多个用户提供安全能力，产品使用时无需单点登录跳转，在管理平台界面即可直接使用产品。 |
| 提供用户认证统一的服务，被授权的用户可以直接通过管理平台登录到各个安全能力，包括下一代防火墙、web应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全（EDR）、APT等所有安全能力，无需二次认证； |
| 产品开通服务 | 用户可通过管理平台一键开通任意安全能力，安全能力成功开通后可自动获取计算、存储等虚拟化资源实现自动化部署和激活； |
| 提供安全能力开通关联工单审批流程的服务，普通用户申请开通安全能力，需要后台管理员审批通过后才能自动自动化部署和激活； |
| 安全能力具备提供多种服务规格和服务时长的能力，用户可根据业务规模和使用时间，按需选择开通不同规格的安全能力； |
| 安全能力具备试用开通功能的能力，试用的安全能力具备全量安全能力功能但不消耗安全能力授权，提升用户体验；（投标文件商务技术响应文件中提供佐证材料） |
| 管理员可通过后台界面直接为租户分配安全能力，如新能力开通和到期能力续费； |
| 云安全中心服务 | 云安全管理平台内置云安全中心，能够汇总展示租户资产面临的安全风险，并可以直接对安全风险进行响应处置。 |
| 云安全中心具备平台管理员视角的能力，管理员可查看平台整体安全态势，展示内容包括攻击次数态势、攻击源国家/地区TOP排名、主机/网站漏洞情况、风险网站数量、资产漏洞TOP排名、受攻击租户TOP排名、受攻击资产TOP排名、受攻击区域TOP排名、攻击事件详情等信息； |
| 云安全中心具备按照区域查看平台安全态势的能力，平台管理员既可以查看整体安全态势，也可以查看不同地市、区县的安全态势； |
| 云安全中心具备租户视角，具备以安全态势大屏和dashboard方式展示租户的安全情况的能力，包括资产总数、风险总数、风险资产TOP排名、安全风险TOP排名、防护事件TOP排名等信息； |
| 具备按照业务系统及单个资产两种维度展示资产的风险状态的能力，包括高危资产及已失陷资产； |
| 具备风险管理模块，租户可统一查看系统中存在的风险总数、高危风险及WEB安全事件，并具备基于安全产品及风险类型进行筛选查询的能力； |
| 具备日志查询模块，具备统一查看系统内产生的安全日志的能力，日志具备按照搜索语法进行搜索的能力，具备根据时间进行自定义筛选的能力； |
| 多区域管理服务 | 提供按照云安全管理平台支持省-市-区三级架构设置云安全区域服务，并将租户及管理员关联区域信息的服务，同一租户可关联多个区域，并根据不同区域的业务按需订购安全产品；区域管理员拥有本区域内的租户管理、产品管理、工单管理等权限。 |
| 用户管理服务 | 三权分立安全原则：平台内置多种身份角色，同时支持身份角色和权限的自定义设置，用户可根据业务需求对角色权限进行细粒度分配 。 |
| 提供设置临时成员的服务，可自定义账号有效期，到期后成员将被自动踢出租户团队 |
| 新建用户的初始密码具备指定密码和随机生成两种方式的能力，具备用户首次登陆强制修改密码的能力； |
| 订单管理服务 | 提供通过订单实现安全产品的订购统计的服务，用户可以查看订单创建时间、购买时长、订单状态、订单详情等； |
| 订单信息实现权限分离，管理员可以查看平台所有租户的产品订单，且具备按用户筛选产品订单的能力，对于云租户只能查看自己的产品订单； |
| 许可管理服务 | 云安全管理平台支持以通用授权许可的方式激活虚拟安全组件，管理平台只记录许可总数，通用许可将根据产品种类及规格进行按需扣减消耗，支持两个许可合并激活一个高规格的安全产品。 |
| 提供以许可文件包的方式批量导入许可的能力，通过扩展许可数量的方式扩展资源池可激活的安全产品数量； |
| 虚拟安全组件删除后，云安全管理平台支持将被占用的通用授权许可回收，并可继续用于开通新的虚拟安全组件。 |
| 运维监控服务 | 可通过管理平台查看物理机和安全虚拟机的资源占用信息，包含资源ID／别名，CPU使用率、内存使用率、磁盘使用率，网络流入流出速率，并用可视化图表的方式展示CPU、内存、磁盘占用趋势，网络总流入流出速率趋势； |
| 告警条件可自定义设置，管理员可自定义告警时间、告警阈值、告警持续时间，具备通过邮件方式发送告警信息的能力； |

## 2.2安全资源池能力服务

## 2.2.1云日志审计安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 帮助用户更好监控和保障信息系统运行，及时识别针对信息系统的入侵攻击、内部违规等信息，同时为安全事件的事后分析、调查取证提供必要的信息。 |
| 服务模式 | 审计工作不影响被审计对象的性能、稳定性或日常管理流程。 |
| 日志采集服务 | 可对Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集，以及阿里云SLS日志的采集。 |
| 可对主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等日志的收集。 |
| 日志分析服务 | ▲根据信息安全技术 日志分析产品安全技术要求（GAT 911-2019）、信息安全技术 信息系统安全运维管理指南（GB/T 36626-2018）等国家标准要求，可通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件（投标文件商务技术响应文件中提供国家权威检测机构检测报告或具有相关检测资质的第三方检测机构检测报告扫描件）。 |
| 日志查询服务 | 具备极高的日志查询性能，具备亿级的日志里根据做任意的关键字及其它的检索条件的能力，实现在秒级里返回查询结果 |
| 资产管理服务 | 资产拓扑支持根据实际的用户环境进行编辑发布并可以和资产进行绑定。拓扑可以显示资产采集的事件数量、被采集资产的状态等信息。 |

## 2.2.2云数据库审计安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 实时记录网络上的数据库活动,对数据库操作进行细粒度审计的合规性管理,对数据库遭受到的风险行为进行告警。对用户访问数据库行为的记录、分析和汇报,帮助用户事后生成合规搜索报告、事后追根溯源,同时加强内外部数据库网络行为记录,提高数据资产安全 |
| 服务部署 | 可在云环境操作系统中安装数据库审计软件代理。 |
| 协议支持服务 | 可对Oracle（包括21C版本）、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ、Vertica、Tidb、PolarDB、PolarDB-X等主流数据库进行审计； |
| 可对MongoDB、Hbase、Hive、Impala、Elastic Search、HDFS、Canssandra、greenplum、LibrA、graphbase、cache、Redis、HANA、ArangoDB、Neo4j、OrientDB等非关系型数据库进行审计 |
| 审计服务 | 审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集的。 |
| 查询分析服务 | 可基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询 |
| 安全审计服务 | 内置安全规则可通过规则包进行单独升级。 |
| 统计报表服务 | 提供多种报表模板库，报表类型不少于20种 |
| 三层关联服务 | 提供客户端访问Web服务器的URL和应用服务器访问数据库的SQL语句关联功能。 |

## 2.2.3云防火墙安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 帮助用户对网络的存取和访问进行监控，强化网络安全策略，有效防止客户内部信息的泄露以及各类安全威胁的入侵。 |
| 访问控制服务 | 提供一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，实现入侵防御、病毒防护、URL过滤、应用过滤等高级访问控制。 |
| 应用识别服务 | 提供应用智能识别，有效识别P2P和迅雷行为，识别模式可选择严格、适中、宽松，支持排除扫描端口 |
| 端口扫描服务 | 提供对IP、端口进行端口扫描，可选择立即执行或定期执行的服务；具备扫描结果的呈现的能力，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，并具备导出的能力 |
| 路由策略服务 | 提供静态路由、动态路由、ISP路由；提供基于入接口、源地址、目的地址、用户、服务、应用、时间、域名的策略路由；ISP路由具备联通、电信、教育网、移动等ISP服务商地址列表的能力，可根据运营商地址自定义 |

## 2.2.4云WAF安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 根据《浙江省电子政务外网安全评估指标体系》指标要求，提供与上级平台之间的热门漏洞等情报共享、漏洞修复、策略配置、防护验证等服务，保障网站及相关业务安全、可靠运行。（须提供联动服务方案及承诺书） |
| HTTPS防护服务 | 提供HTTPS站点SSL算法自动探测。探测时可以设置指定站点及端口，可以显示探测结果 |
| 机器学习服务 | 具有机器学习安全引擎，可以对用户web业务系统建立安全的访问模型 ，学习的内容包括URL地址、URL请求参数等信息；支持设定学习的周期，域名信息，可信任的客户端IP，不可信的客户端IP以及不学习的URL信息的能力；模型数据可以显示学习中的URL数量，学习完成的URL数量、检测中URL数量、学习失败的URL数量，同时可以显示各个阶段的占比情况；具有通用的机器学习模型，数据模型可实现在线更新； |
| 攻击检测服务 | 提供对跨站脚本(XSS)和注入式攻击（包括SQL注入、命令注入 、代码注入、文件注入、LDAP注入、SSI注入等）的检测防护 |
| CC功能防护服务 | 支持根据细粒度条件对CC攻击进行检测和防护；匹配条件由URL参数、请求头部字段、目的IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成；客户端检测对象由IP、IP+URL、IP+User\_Agent等参数组成；支持从请求头字段获取真实源IP地址。 |
| Webshell检测服务（语义分析） | 内置Webshell检测规则，可以对上传的文件内容进行检查，防止恶意Webshell文件上传，对已经上传的Webshell发起请求的行为进行拦截阻断 |
| 客户端安全防护服务 | 提供客户端安全防护，插入特殊的HTTP报头以保护客户端免受某些攻击包括但不限于增加以下安全报头：X-Frame-Options（用于防护客户端免受Clickjacking攻击）、X-Content-Type-Options（以防止浏览器将文件解释为内容类型声明以外的其他内容）、X-XSS-Protect（用于当检测到XSS攻击时，指示浏览器停止加载页面）、Content-Security-Policy（用于降低浏览器上的XSS风险和数据注入攻击） |
| 区域态势感知与阻断服务 | 按地理区域对攻击次数等进行统计，并通过地图展示；支持在地图上对某一地理区域设置阻断此区域IP的访问。 |

## 2.2.5云堡垒机安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 帮助用户保护网络设备和网络数据不受外部侵害,监测运维人员的工作状态,针对发现任何人有危害单位安全的行为,实现立即报警,并且审计定责。 |
| 用户管理服务 | 可根据用户部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等 |
| 设备管理服务 | 提供常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| 提供用户账号状态统计，包含用户账号上次登录时间、已禁用的用户账号、用户账号有效期等 |
| 工单流程服务 | 运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理 |
| 审计日志服务 | 提供对运维操作会话的在线监控、实时阻断服务；可实现录像回放、支持记录起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志； |

## 2.2.6云综合漏洞扫描安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登录操作；帮助用户准确发现网络中各主机、设备存在的网络安全漏洞，并给出详细的描述和解决方案，实现对整个系统进行安全评估的重要作用。 |
| 系统漏洞扫描服务 | 可对各种网络主机、操作系统、网络设备(如交换机、路由器、防火墙等)、常用软件以及应用系统进行识别和漏洞扫描。 |
| 基线核查服务 | 提供系统安全配置核查，能够对主流操作系统、中间件、数据库、网络设备、虚拟化设备的安全配置项目进行检查 |
| 网站漏洞扫描服务 | 提供常见Web漏洞类型的扫描，包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL跳转、文件包含、反序列化漏洞、文件上传、CSRF跨站请求伪造、信息泄露等。支持OWASP TOP10等主流安全漏洞；支持对漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级。 |
| 数据库扫描服务 | 提供Oracle、Mysql、SQLServer、DB2、informix、PostgreSQL、Sybase、达梦、人大金仓的授权数据库漏洞扫描 |
| 资产管理服务 | 提供授权管理，对已知用户名、密码的资产可预先进行配置存放至授权管理，再下发扫描任务时能对该部分资产的授权信息同步 |

## 2.2.7云主机安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 帮助用户保证主机在数据存储和处理的保密性、完整性，可用性，包括硬件、固件、系统软件的自身安全，为用户建立一个完整的主机安全保护环境。 |
| 系统性能监控服务 | 支持对防护资产的CPU使用率、内存使用率、磁盘使用情况、网络上下行流量进行性能监控，并支持对性能监控项设置阈值，达到阈值后告警；支持对CPU、内存达到一定阈值时客户端进行熔断 |
| 防病毒服务 | 提供专门的勒索风险评估、专门的挖矿风险评估服务 |
| 可对扫描发现的网马进行自动查杀设置 |
| 可对病毒立即处理，对于无法普通隔离的病毒文件进行处理并加入隔离区，或动态移动到信任区。 |
| 系统安全性服务 | 提供网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，具备资产自主切换不同网络访问域的能力 |

## 2.2.8云APT安全能力服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过深度威胁检测技术，帮助客户实现对流量深度解析，发现流量中的恶意攻击，包括不限于发现0day漏洞利用、未知恶意代码等高级攻击手段，提供全面的检测和预警的能力，为用户提供更高级的安全保障 |
| 检测风险类别服务 | 可检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、行为分析、DGA域名请求、SMB远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP欺骗、密码明文形式传输等行为 |
| 暴力破解检测服务 | 提供自定义启用/禁用暴力破解模型；提供自定义配置模型统计周期、登录次数、聚合维度等参数 |
| ARP欺骗检测服务 | 可根据MAC与IP地址的绑定关系，分析网络中的ARP流量，判断ARP应答包中的IP和MAC地址是否匹配的服务 |
| 文件检测服务 | 提供doc, xls, ppt, swf, pdf, rar, zip, rar, exe, vbs, scr、ps1、elf、mach-O等多种文件的解析 |
| 敏感信息管理服务 | 提供对自定义弱密码、暴力破解和密码明文形式传输等告警的密码查看权限 |
| 失陷主机检测服务 | 可根据威胁情报、DGA域名请求、IDS规则、用户配置数据，发现被远程控制的内部主机 |

## 3.网络安全数据分析服务

## 3.1资产数据治理服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 帮助用户摸清单位网络资产底数，建立网络资产档案库，在一个平台实现统一的资产探测、漏洞扫描、高危风险预警等功能，提供多维度安全态势可视化等一系列服务，可协助用户掌握本单位网站及业务系统的安全动态，提高整体的安全态势感知能力和安全水平。超出25000点位免费提供。 |
| 网络资产探测服务 | 资产探测发现服务 | 提供手工导入、主动扫描等多种信息资产发现方式，可通过域名、IP段等多种途径对资产进行探测和管理。 |
| 存活资产探测服务 | 提供资产存活状态自动发现，具备自定义端口存活探测的能力。 |
| 资产状态检测服务 | 提供资产状态检测服务，资产自动收集、识别并记录资产上线、下线和更新状态。 |
| 资产指纹服务 | 提供精准资产类型及指纹识别，能够识别的资产类型包括但不限于CMS网站应用、数据库服务应用、服务中间件、开源框架、网络及安全设备、物联网设备等，识别指纹种类不低于6000种。 |
| 资产探测任务服务 | 提供资产探测任务速率、端口范围和周期配置，包括自定义监控周期及检测时间（支持按照单次/日/周/月/）规则配置；端口范围具备通过常用场景模板快速选择端口范围的能力，模板包括企业应用、数据库、物联网等场景，支持自定义端口及全端口扫描。 |
| 域名/子域名发现服务 | 提供子域名的发现、多级域名自动发现。 |
| IP/IP段探测服务 | 提供IP/IP段的资产探测，发现存活的ip、开放的端口及服务类型等信息，具备基于IP的域名发现的能力。 |
| 内网资产探测服务 | 提供内网资产探测，能够采集局域网某网段内主机的MAC地址，用于硬件厂商的识别，对局域网资产进行分析。 |
| web资产拓展探测服务 | 提供对已知web资产的拓展探测，自动识别已有资产的域名和主机ip进行web资产和主机资产探测。 |
| 探测任务操作服务 | 提供资产探测任务的查看、修改、终止、删除等日常操作，可对单次任务进行再次探测，可查看每个任务的资产探测结果。 |
| 资产自动识别服务 | 提供单位资产的自动识别，可针对某一单位配置对应的ip段，在该ip段扫描发现的资产自动归属到该单位目录下，便于单位资产的管理。 |
| 网络资产管理服务 | 资产展示服务 | 可通过web、主机、域名、端口等多个类别和视角展示资产。具备以系统名称、IP、单位、联系人、首次发现时间、操作系统及版本、资产状态码、标签等信息实现资产的特征识别和过滤的能力。具备按URL、联系人、资产名称等多种搜索组合进行资产的检索能力。具备web、主机、域名、端口视角下资产批量导出的能力 |
| 可通过以单位组织架构视角和资产分类视角展示资产。组织架构视角可按单位名称展示本单位的资产；分类视角可根据资产属性和类别进行展示，如硬件、操作系统、服务类型、中间件、应用类型等。 |
| 资产管理服务 | 提供分类管理，资产可以按照单位和分组等基本属性进行分类管理，可自定义分组、标签和联系人（添加、编辑、删除）。 |
| 提供单位组织架构的管理，单位组织架构树状展示，可编辑、可搜索，可自定义展示排列先后顺序。 |
| 提供批量变更资产归属单位和分组，具备批量添加和变更资产安全联系人的能力，具备资产批量删除的能力。 |
| 弱点扫描及管理服务 | 弱点扫描模式服务 | 弱点扫描提供web漏洞扫描、主机漏洞扫描、弱口令扫描、安全事件扫描和内容风险扫描能力，并且具备登录扫描和非登录扫描两种模式。 |
| 自动匹配扫描服务 | 可根据用户选择或输入的资产，自动匹配资产的弱点扫描项，如选择web资产，自动匹配web漏洞扫描、安全事件、内容风险等扫描项；选择主机资产，自动匹配主机漏洞扫描、弱口令等扫描项。 |
| 弱口令扫描服务 | 提供弱口令扫描，提供多种弱口令扫描协议，包括SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS等协议进行弱口令扫描，允许用户自定义用户、密码字典。 |
| 主机漏洞扫描服务 | 提供主机漏洞扫描检测，漏洞策略库大于55000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国际CVE、国内CNNVD漏洞库标准兼容。 |
| 主机漏洞包括漏洞详情、影响端口、影响服务、CVE、CNNVD、CVSS，提供漏洞的修复及建议。 |
| web漏洞扫描服务 | 提供对web系统漏洞进行扫描检测，包括SQL注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞、隐藏字段、表单绕过、框架注入、0day漏洞等。 |
| 自定义扫描服务 | 提供自定义扫描参数和自定义扫描策略，提供自定义主机漏洞和web漏洞扫描模板。 |
| 暗链+V服务 | 提供暗链+V，加V表示该漏洞可靠性达到90%以上，可帮助用户快速的确认和处理漏洞。 |
| WEB漏洞+V服务 | 提供web漏洞扫描结果+V，加V表示该漏洞可靠性达到90%以上，可帮助用户快速的确认和处理漏洞。 |
| 扫描黑名单服务 | 提供扫描黑名单配置，已配置黑名单的web资产和主机资产不会被扫描。 |
| 漏洞详情服务 | 依据漏洞情报提供web漏洞VPT（弱点优先级）的能力，依据资产重要等级、是否互联网暴露、利用复杂度等维度进行VPT计算，各个维度的分值比重可自定义；通过VPT功能，可协助对漏洞重要程度分类，优先修复VPT高的漏洞。 |
| 漏洞详情提供漏洞描述、影响组件、CVE、CNVD、CVSS、漏洞修复及建议、修复方式、修复建议。 |

## 3.2网络威胁情报中心服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 具备云端威胁情报订阅模块：内置威胁情报离线库并支持更新；具备采用情报数据进行实时检测防御能力；具备在线查询与溯源能力：云端提供对IoC威胁类型、多源情报、WHOIS、开放端口、SSL证书等多维度的溯源分析；云端服务：提供订阅高级威胁分析情报，云端提供最新APT入侵、0day漏洞预警、病毒变种情况等分析报告订阅服务。 |
| 情报接入服务 | 提供原厂威胁情报云订阅API服务，可订阅IOC情报、APT情报、热点事件情报等。可在线或离线方式更新订阅情报。提供原厂威胁情报云查询API服务，可查询IP情报、域名情报、哈希情报等。提供至少10个开源情报源接入服务，如stopforumspam.com、otx.alienvault.com、greensnow.co、blocklist\_de等。提供任意第三方情报源的接入，可以通过自定义一键导入API插件方式实现，无需复杂的API配置。提供手工添加威胁情报，支持添加单个或批量导入的方式，并可以设置情报的分类、标签、红绿灯协议、可信度、威胁等级等字段格式。提供结构化情报导入服务，支持国内标准(GB/T36643-2018)、STIX、taxii、openioc、Excel等标准格式的威胁情报，并可以提供参考示例。 |
| 情报聚合服务 | 提供情报命中率聚合处理服务，对不同的情报源可以实现以威胁情报命中率的规则权重优先级来进行聚合处理。（投标文件商务技术响应文件中提供佐证材料）提供情报可信度聚合处理服务，对不同的情报源可以实现以威胁情报可信度的规则权重优先级来进行聚合处理。提供自定义情报源聚合处理服务，对不同的情报源可以实现以某个威胁情报源为优先聚合的规则权重进行处理。提供对情报源质量评价服务，对不同的情报源从时效性、价值性、关联性等威胁维度进行评估，并对不同的情报源进行综合排名。 |
| 情报检索服务 | 提供对单个情报的检索，检索结果至少包括威胁等级、威胁类型、威胁标签、可信度、有效状态、最后更新时间等。提供IP情报检索，查询结果至少包括运营商、ASN号、应用场景、地理位置等。提供域名情报检索，查询结果至少包括注册商、注册时间、更新时间等。提供对检索结果提供阻断等级服务，为威胁处置提供封禁支撑。对检索结果提供关联事件，为威胁分析提供更多情报支撑。对检索结果提供多情报源命中结果服务，实现多情报源检索结果的对比和判断。提供批量检索情报服务，支持IP和域名的混合批量检索，且批量检索的数量不低于1000个。提供批量检索情报结果服务，可显示命中数量、恶意数量、安全数量、未知数量、检索结果列表等，并将检索结果的列表批量导出查看。（投标文件商务技术响应文件中提供佐证材料） |
| 情报协同服务 | 提供本地情报查询API服务，为第三方平台提供本地威胁情报查询API接口，实现情报的快速比对与应用。提供丰富的情报API查询结果服务，具有返回是否恶意、威胁类型、威胁标签、可信度、可信度评分、是否APT、威胁名称、情报创建时间、情报更新时间、情报来源等内容。提供记录情报API调用情况服务，记录API调用时间、查询的IOC、是否命中、检索时间等内容，并可按条件过滤进行搜索。 |
| 威胁分析服务 | 提供Syslog查询情报服务，第三方安全产品可以以Syslog方式查询情报，本地日志与威胁情报进行快速比对。提供日志威胁分析服务，零规则方式实现自动分析Syslog日志能力，并展示命中的情报、威胁等级、情报标签、可信度、活动时间、命中数量、关联的事件等信息。提供威胁结果统计和搜索服务，显示近24小时的严重威胁数量、高威胁数量、中威胁数量，显示近7天和近30天的威胁数据。提供威胁日志关联服务，显示命中的威胁情报与日志来源的关系，并可导出及下载威胁分析列表以及原始日志。 |
| 情报统计服务 | 可统计情报数量，显示接入情报源的数量、情报数据总量、IOC数量、域名情报数量、威胁事件数量等。提供情报类型占比统计服务，显示IOC类型占比、威胁类型占比、情报可信度占比等情况。威胁类型至少包含白名单数据、C&C数据、恶意软件、漏洞利用、钓鱼情报、爬虫数据、伪造搜索引擎爬虫数据、扫描数据、垃圾信息传递机构数据、暴力破解信息、失陷主机信息、不受欢迎的主机信息等情报。提供威胁情报数据统计服务，显示以时间维度统计威胁类型数量、以威胁等级维度统计可信度数量。提供APT组织活动统计服务，显示APT组织历史活动情况，包括活动数据排名、APT组织位置分布等。 |
| 情报知识库服务 | 提供对热点威胁事件通告服务，可按所属行业、事件类型和关键词内容搜索热点事件。提供对热点威胁事件分析服务，事件的分析内容至少包括所属行业、事件标签、事件背景、事件过程、事件建议、事件关联的IOC情报等。提供对活跃APT组织的分析服务，APT组织的分析内容至少包括组织名称、组织别名、归属地、涉及行业、攻击事件等。 |
| 基础数据服务 | 威胁情报云端具备丰富的IP端口指纹数据，至少覆盖200种端口协议，包括OpenVPN、pptp、CS、HTTP、DNS、FTP、RDP、SSH等端口数据，每月更新数亿条网络资产数据。威胁情报云端具备威胁事件分析数据，且不低于2000个分析事件。威胁情报云端具备7年以上PDNS数据，且具备600万条ICP备案数据。威胁情报云端具备日均增量数亿条SaaS化防护中心中的网站访问日志能力，以支持云端威胁情报生产的基础数据。 |

## 4.政务数据安全防护服务

## 4.1日志采集及审计分析系统预处理节点服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过部署日志采集及审计分析系统预处理节点，对主机、数据库、数据平台、堡垒机、vpn、安全设备等日志进行采集与适配。完成全量日志采集与接入工作，同时对接市日志采集与审计分析系统，满足义乌市对安全监管要求，实现全量日志接入。 |

## 4.2数据分级分类服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过网络嗅探技术对指定范围内的数据源进行扫描发现，动态发现数据资产，防止遗漏，通过内置识别规则将数据抽取进行分级比对计算，将符合敏感数据特征的数据项自动定级梳理。 |
| 数据源资产管理服务 | 可对数据库类型包括但不限于MySQL、Oracle、PostgreSQL、Hive、SQLServer、IPMALA、MongoDB、ElasticSearch、ClickHouse、Greenplum、INFORMIX、SYBASE、DM7、ODPS、DB2、GBASE8A（南大通用）、KINGBASE8(人大金仓)、POLARDB、Teradata、VERTICA、CacheDB等数据库的数据源进行资产管理。 |
| 创建数据源时，提供数据源绑定对应的部门、责任人的服务。每个数据源都可以使用不同的行业模板，达到不同行业模板的多数据源并行执行分类分级任务。 |
| 可手动添加数据源，可以编辑数据源名称、数据源类型、主机及端口、库名/实例名、版本号、账号、密码等信息，也可以批量导入数据库，进行数据资产管理。可通过指定的IP段、端口段，定时扫描发现当前环境下的数据库资产 |
| 提供数据源展示，至少包括但不限于数据源名称、数据源类型、主机及端口、创建用户、创建时间等数据源基本信息，同时可展示具体每个数据源的库、表、字段信息。 |
| 提供数据源“一键删除”。当数据源删除后，对应数据源关联的数据分类分级任务、数据资产目录、数据库账号信息、数据风险检测任务都将被自动删除，系统其他模块自动感知数据源环境变化，无需手动再次更新。 |
| 分类分级服务 | 提供分类分级任务管理，包括对任务的启动、终止，并展示任务的执行进度情况。提供任务的定时启动服务，自动发现敏感数据的动态变化。 |
| 提供分类分级任务信息的列表展示。包括但不限于任务名称、数据源名称、发现结果、状态、次数、操作等信息，同时支持扫描任务结果的导出。 |
| 提供至少几十种常见敏感字段识别规则，且具备自定义创建识别规则的能力。自定义规则包括但不限于正则、字典等。具备结合算法识别能力以保障敏感数据识别精准度，至少包括但不限于正则+luhn、NER算法等（投标文件商务技术响应文件中提供佐证材料） |
| 可根据不同规则之间进行组合，识别复杂的复合字段，如“姓名”、“手机号”规则组合后可识别“联系人”业务含义的字段。 |
| 可通过对发现字段的敏感级别进行逻辑计算，通过多种策略实现对表的分类分级。提供表分类策略，表分类策略具备分类合集（使用去重后所有已识别数据字段的类别集合，作为表分类）和就多原则（使用数据字段所属最多的分类，作为表分类）两种维度定义表类别的能力 |
| 看对系统自动分类分级的结果手动梳理和调整，提高准确性，也可以通过配置匹配度的阈值实现自动确认，提高效率，且手动确认的结果优先级高，再次执行任务后，无需再次确认。 |
| 提供自动推荐引擎，当同一列中识别出多种字段信息时，需提供该列数据的规则命中列表，并给出精确的较高的推荐结果，便于用户根手工修改确认梳理，实现迅速、高效的手动确认。（投标文件商务技术响应文件中提供佐证材料） |
| 可通过对字段内容、字段名称和字段注释进行模糊匹配，并可通过调整权重配比，提高数据自动分类分级准确性。 |
| 可对相似表、相似字段进行聚合并在页面中统一展示，以便于人工二次确认或修改分类分级结果 |
| 数据资产和分类分级结果展示服务 | 可在多个视角下查看当前数据分类分级情况。数据视角至少包括但不限于：数据源视角、行业模板视角、敏感数据视角。展示的内容，至少包括敏感字段表级别分布、字段级别分布、敏感表数目、敏感字段数目、梳理字段占比。并可以增量展示一定周期的敏感数据变化情况。具备以图表形式展示结果的统计和分析的能力。 |
| 可对梳理后的分级分类结果进行导出，并提供分类分级报表，报表内容至少包括但不限于：资产分布、分类分级结果、敏感数据分布和占比等，且提供具体数据的图示。 |
| 以列表形式展示分类分级的详细结果，包括但不限于列名、表名、是否新增、规则名称、是否梳理、识别字段、分类结果、分级结果、操作等信息，同时提供查询服务，自动展示数据源内相关候选项 |

## 4.3数据脱敏服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过数据脱敏服务，使数据库中的原始数据，经过系统清洗后离线分发至测试环境，所有敏感数据全部在内存中处理，可保证整个环节敏感数据不落地。 |
| 敏感数据发现服务 | 提供数据源管理服务，主流数据源类型包括但不限于MySQL、Oracle、Db2、MSSQL、PostgreSQL、Greenplum、SybaseASE、Informix、Hive、ODPS、MariaDB、Clickhouse、Elasticsearch、MongoDB、MariaDB、达梦、GBase8A、Kingbase，同时具备新增本地文件xls、xlsx、csv、txt、SFTP\FTP数据源的添加能力。 |
| 提供自动数据识别发现敏感项的服务，包括敏感表和敏感列以及敏感项的动态变化 |
| 需提供数据目录，可以查看数据的分布情况，包含表级别分布和列级别分布；同时提供包括数据库梳理、敏感表数量、识别字段数、敏感列数和已经梳理占比情况等信息 |
| 提供数据分级分类任务任务的管理服务，包括但不限于务名称、数据源名称、主机、发现结果、状态、次数、周期、创建时间、最新发现时间、操作。提供查看任务详情，可以查看以图表形式展示当前数据源分类分级的概况。 |
| 敏感数据脱敏服务 | 支持主流字符集如gbk、gb2312、gb18030、utf8、utf8mb4等 |
| 提供自定义脱敏算法模板库服务，用户可将若干脱算法略组合成为适用于该场景的脱敏算法模板库，脱敏模板库定后，可被重复利用。 |
| 提供脱敏任务的配置服务，具备数据库到数据库、数据库到文件、文件到数据库、文件到文件流程的脱敏任务新增能力，具备数据处理配置和脱敏算法的配置能力。 |
| 提供脱敏任务的展示服务，包括但不限于任务名称、脱敏流程、任务状态、执行次数、执行周期、新增时间、最近执行时间、执行耗时和操作等信息，同时可对任务进行编辑、查询等操作。 |
| 开启脱敏任务审批后，用户提交脱敏任务审批后，权限管理员可以进入该界面进行脱敏任务的审批，审批通过后方可执行脱敏任务。 |
| 提供水印配置服务，水印配置界面可直观展现水印的使用状态，具备添加1000w+的水印数量的能力，具备在水印中自动附加时间信息，提供方便便于维护管理水印的能力。（投标文件商务技术响应文件中提供佐证材料） |
| 用户可制定要脱敏的表，自由选择全量或增量抽取数据，可基于字段自由配置增量条件 |
| 提供自动同步源数据表主键、索引、唯一约束至目的表的服务 |
| 提供覆盖原表脱敏服务 |
| 数据溯源服务 | 提供伪行水印、伪列水印、脱敏水印、内容修改水印等多种水印方式的服务 |
| 可通过数据上传和数据输入两种方式溯源，定位水印处理后数据的单位信息 |

## 4.4数据管控服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过数据管控服务，可基于IP、MAC、客户端主机名、操作系统用户名、客户端工具和数据库账号六个维度认证身份，实现用户的多维度身份认证和敏感数据的细粒度访问控制。 |
| 服务数据库类型 | 支持Orcal、MySQL、Mariadb、PostgreSQL、DB2、MSSqlserver、hive、hbase、kingbase、gbase8a、sybase、informix、MongoDB、达梦（DM）、人大金仓（KingBase）、ODPS、vertica等数据库 |
| 敏感数据扫描服务 | 可扫描发现14种敏感信息，包括身份证、银行卡、手机号、座机号、军官证、护照号、车牌号、MAC地址、日期、时间、港澳台通行证、台胞证、邮箱、中文姓名等，同时支持自定义敏感数据扫描规则。可和数据分类分级服务结合，调用分级分类的结果。 |
| 访问控制服务 | 提供多种数据来源筛选管控，包括IP、客户端主机名、操作系统用户名、客户端工具名、数据库账号 |
| 对于越权的动作可以选择：阻断、脱敏、仅告警 |
| 可阻断未经授权的逻辑备份操作，如mysqldump、oracleexp、pg\_dump等 |
| 运维审批服务 | 可申请运维任务通过邮件发送且通过邮件正文的链接审批提供运维申请手动配置运维对象或者选择对象组 |
| 安全防护服务 | 内置的特征策略包含缓冲区溢出、SQL注入、提权、数据库内核入侵探测等常见攻击特征，内置多种数据库安全规则 |
| 自定义规则支持根据账号、数据库名、客户端工具、操作系统用户名、客户端IP、操作类型、SQL关键字等制定防护策略 |
| 可基于一定时间范围内基于同一会话、同一ip、同一用户、同一工具等维度对数据库访问频次及返回行数的限制 |
| 规则动作具备允许访问、命令阻断、会话阻断和动态脱敏的能力 |
| 提供数据库防护虚拟补丁技术服务，防护未升级数据库，并可以更新维护 |
| 动态脱敏服务 | 自定义敏感数据规则，敏感信息发现结果的在线新增、修改和删除 |
| 多种脱敏算法，如字符串取整、遮蔽等 |
| 提供自定义策略脱敏服务，关键字、正则表达式、字符长度等。 |
| 提供动态脱敏效果预览服务 |
| 对于越权的数据访问进行动态脱敏，防止数据泄露 |

## 4.5数据加密服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 采用SM2、SM3、SM4国家标准加密算法提供存储加密服务，有效防止数据存储环节可能出现的泄露风险，保证敏感数据的机密性、真实性、完整性。 |
| 算法服务 | 加密算法：▲根据《信息安全技术 信息系统密码应用基本要求》等国家标准（GB/T 39786-2021），加密工具支持国产SM2、SM3、SM4标准加密算法，具备相关的《商用密码产品认证证书》。（投标文件商务技术响应文件中提供国家权威机构检测报告或具有相关检测资质的第三方检测机构检测报告扫描件）。 |
| 数字签名算法：支持国产SM2、SM3、SM4数字签名算法。 |
| 服务工具要求 | 提供硬件密钥管理设备，基于物理噪声源生成真随机数；部署在用户本地，密钥由用户自主掌控。 |
| 密文密钥分离机制，如果“黑客”获取数据库密文，密钥也无法解密查看明文数据，确保数据库数据的安全性。 |
| 密钥可根据周期自动更新，密钥管理模块后台保留密钥更新记录功能，确保密钥使用安全。 |
| 加密工具需支持应急告警机制，提供报警邮箱设置功能，实现系统故障时可向指定内部人员邮箱发送告警邮件。 |
| 具备SQL、PL/SQL、JDBC、ODBC的透明性能力，不需要改造；具备现有Oracle维护工具的透明性能力，数据库管理员依然可以使用RMAN等现有工具实现备份恢复和数据库维护；硬件密钥管理设备可独立部署。 |
| 基本能力服务 | 提供安全访问控制，除数据库原有权限控制外，可限制访问数据库的具体进程等。基于进程与数据库用户绑定进行访问控制增强，同一用户只能通过指定的进程访问密文，而无法使用命令行等其他方式访问密文数据，可有效防止合法用户违规操作引发的数据安全隐患。 |
| 提供系统管理员、安全管理员和审计管理员三权分立。其中安全管理员完成日常的加密数据配置、数据库用户的密文权限控制等安全维护和管理操作；审计管理员进行审计开关的控制，检索、分析密文访问操作的审计信息工作；系统管理员则负责进行系统配置，如IP，端口等的配置。 |
| 数据加密后，对于数据库的IO性能损耗可控制在10%~15% |
| 以表为单位进行数据加密，加密表的数据以密文形态存储在磁盘中。 |
| 对数据库系统加密后，可进行密文数据索引。 |
| 提供随机加密策略，防止相同的数据的加密结果一致而导致的数据泄密。 |
| 兼容性服务 | 加密工具需支持多种数据库类型，覆盖用户单位所使用的数据库类型，包括MySQL、Oracle、SQLServer等；支持主流的Linux、Windows等类型操作系统。 |

## 4.6数据安全态势感知服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过数据安全态势感知服务开展安全监控和审计，建立相关的措施对非法采集、未授权访问、数据滥用、数据泄漏进行监控、预警和审计，通过数据分析来支撑有效的安全、合规决策，从而降低数据安全风险。为实现与市数据安全日志采集与审计系统对接，实现义乌市大数据局对数据安全统一监管要求，需要在各下级单位部署日志采集及审计分析系统预处理节点。实现对下级单位日志汇聚及预处理，实现下级单位全量日志接入。 |
| 数据接入服务 | 可通过多种类型的安全、泛安全类数据接入采集，应包括但不限于日志数据、流量数据、资产人员数据等；可通过流量采集设备采集接入全流量数据，包含流量中的请求包和返回包等信息，并可在数据检索中体现包信息； |
| 资产梳理服务 | 可梳理的资产类型包括网络资产、数据资源、应用接口、应用服务、账号权限等；提供EXCEL等格式的文件数据，可通过模板文件的填写导入实现资产数据的导入和管理的服务；提供流量中分析和自动发现资产，至少包括网络资产、应用服务和应用接口等。 |
| 业务建模服务 | 围绕业务场景开展的数据流动安全监管，将业务场景分解到数据流和数据节点进行细粒度的监控，实现基于业务规则的数据流动安全监管；基于业务的数据建模：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组建包含应用服务、数据服务、账号、接口、表等； 基于拓扑建模基础，生成业务大屏，对业务相关风险进行可视化展现，包括SQL注入、漏洞攻击、账号安全、数据泄露、违规操作、可疑通信等。 |
| 安全监管服务 | 提供数据全流程安全监控服务：数据从归集、治理、共享、交换全流程的数据安全风险监测预警，包括敏感数据访问监控预警、数据流转监控预警、基于业务场景数据安全监控预警等；数据接口安全监控：数据共享接口的健康状况进行实时监控，对接口访问进行统计，包括高密访问、越权访问、访问高延时、返回报错、404异常访问实现对异常或高风险操作的识别和预警；提供特权人员安全监控服务：对第三方运维服务人员的数据访问操作行为进行监督审核，包括特权账号的越权行为及高危操作等。 |
| 安全告警服务 | 可对数据库、应用服务告警进行统一的跟踪管理；提供安全事件场景研判的服务，展示攻击者和受害者的资产信息，可联动会话详情，点击查看不同溯源维度的会话详情，通过请求头，payload等详情字段定位攻击。 |
| 安全管理服务 | 数据权限服务 | 可基于用户角色的数据权限控制，不同的角色只能查询与用户角色相关联的安全告警信息和工单信息等。 |
| 数字字典服务 | 提供管理系统中异常记录、安全告警的所有字段和取值服务，每个字段均有清晰的说明；提供数据标准管理，用户可以根据实际需求，对字典进行编辑，可进行手动修改、增加或删除相应的字段的操作；提供数据字典，数据字典支持管理系统中原始日志和告警数据中所有字段的类型、取值范围、字段说明，支持数值、字符串、枚举、ip等≥9种字段类型。 |
| 采集模块服务 | 日志采集服务 | 日志采集方式应具备但不仅限于Syslog、kafka、ftp、部署代理等4种方式；提供采集异构设备的日志数据的服务，实现包括但不限于安全类、网络类、应用服务器类、操作系统类等至少4大类、50种设备的日志接入采集； |
| 应用性能监控：通过在目标主机上安装Agent程序，监测目标主机的CPU利用率、内存使用率、磁盘使用率、流量等信息。 |
| 无需配置解析规则与设备日志对应关系，自动完成解析；提供日志细粒度解析服务，可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息，≥30个字段； |
| 具备三维关联分析能力：通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件。 |
| 资产管理：资产拓扑可按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息（投标文件商务技术响应文件中提供国家权威检测机构检测报告或具有相关检测资质的第三方检测机构检测报告扫描件）。 |
| 流量采集服务 | 提供行为审计与可疑通信检测服务：违规操作、违规访问、违规应用、违规外发等300种以上行为审计检测规则，支持隧道通信、可疑内容、恶意IP、恶意域名、恶意证书、远程控制等3000种以上可疑通信检测规则，可针对任意单条规则进行启用和禁用；提供漏洞利用检测服务：SMB漏洞、RDP漏洞、软件漏洞、设备漏洞、系统漏洞、拒绝服务漏洞、shellcode等7000种以上漏洞利用检测规则，可针对任意单条规则进行启用和禁用；提供恶意文件检测服务：挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell等25000种以上恶意程序检测规则，可针对任意单条规则进行启用和禁用；提供配置风险检测服务：弱口令风险、明文传输风险、HTTP配置风险、中间件配置风向、数据库配置风险、服务配置风险等100种以上配置风险检测规则；提供Web攻击检测服务：Webshell请求、XSS攻击、SQL注入、远程代码执行、命令注入、远程文件包含、本地文件包含、文件上传、路径遍历、信息泄露、越权访问、XXE注入、网页篡改等13类、6000种以上web攻击检测规则，对任意单条检测规则可启用和禁用。 |
| 数据采集服务 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计；提供对Oracle、SQLServer、DB2、Informix、Sybase、MySQL、MariaDB、PostgreSQL、GuassDB、HANA、greenplum、librA、graphbase、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、Redis等数据库进行审计的服务；提供数据库操作表、视图、索引、存储过程等各种对象的所有SQL操作审计的服务。 |
| 审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集。 |
| 可依据探针客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志。 |

## 5.政务应用安全防护服务

## 5.1政务云应用防护服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务要求 | 保障义乌全域党政机关应用安全，具备两地三中心的服务体系架构，要求10分钟内完成快速切换，涉及服务过程中的机柜租用、线路租用、软硬件运维等所有费用（如有）由中标单位自行承担。（请在投标文件中详细阐述政务云三节点的建设方案与联动处置机制及承诺书） |
| 云应用防护服务 | 可检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等；可识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入、Cookie注入等）、跨站请求伪造等应用攻击行为的服务；可对用户上传的文件后缀名和文件内容进行全方面检查，以杜绝Webshell的上传和访问； |
| 提供区域访问控制，限制国外用户或者国内以市为最低行政单位的区域进行访问控制。 |
| 提供流量监测，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现暗链、Webshell等问题，或作为网站防护的补充功能，更精准地挖掘出网站存在的问题与风险。 |
| 提供一键关停，当网站出现紧急安全事件时，可在一分钟内通过浏览器、微信公众号一键完成关停，防止产生恶劣影响 |
| 攻击态势可视化服务 | 整体网站群攻击态势可视化分析，包括访问与攻击流量趋势、受攻击网站排行、攻击源IP排行、攻击类型排行等 |
| 单个网站可视化分析，包括防扫描告警、总体访问/攻击趋势、攻击源实时分析、IP追踪、访问量排行、防御能力分析等数据展示与挖掘 |
| 威胁告警服务 | 根据不同告警级别发送邮件、短信、电话等多种告警方式。 |

## 5.2政务云应用监测服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 提供义乌重要应用的实时可用性监测服务，具备两地三中心的服务体系架构，涉及服务过程中的机柜租用、线路租用、软硬件运维等所有费用（如有）由中标单位自行承担。（请在投标文件中详细阐述政务云三节点建设方案与联动处置机制及承诺书） |
| 操作系统类型 | Microsoft Windows 2000/XP/Vista/7/8/10 等主流操作系统 |
| 告警服务 | 提供告警信息服务，告警信息包含用户故障判断的主要要素，以及异常发生时间、监控对象、单位、监控类型、当前状态、事件信息、持续时间等可对告警信息的分类显示，包括可用性类、深度巡检类、域名劫持类；发生故障类、已恢复类。 |
| 监控服务 | 提供对单个监控主体，保留历史异常情况，以做长时间的故障问题分析的服务；提供对每条监控异常情况，保留深度巡检结果的服务提供深度关联监控主体和相关的历史异常情况及深度巡检结果的服务，且操作简单方便，易学易用，人性化，简洁。 |

## 6.政务外网终端安全服务

## 6.1终端安全主机防护服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 对所有终端部署杀毒软件，实现全域安全数据可视预采购数量为10000个点位，超过预采购数量的服务须承诺免费提供。 |
| 操作系统类型 | Windowsserver2003、Windowsserver2008、Windowsserver2012、Windowsserver2016、Winxp、Win7、Win8、Win10、Centos5.0+、Redhat5.0+、Suse11+、Ubuntu14+。 |
| Web服务器类型 | Apache2.0-2.4、IIS6、IIS7、IIS8、IIS10、Java系列(JBoss、Tomcat、Weblogic、Websphere)等 |
| 数据库类型 | MSSQL，Oracle、Sybase、Informix、DB2、MySQL等关系型数据库；Mongodb、Cassandra等非关系型数据库。 |
| 全网风险可视服务 | 可对当前待处理高危风险进行展示，包括弱口令、待处理病毒、待处理漏洞数据，并可一键跳转到对应处理页面 |
| 可查看当前top5风险资产、top5威胁ip、top5威胁区域的服务 |
| 系统安全服务 | 提供防端口扫描服务，可锁定恶意的端口扫描，并记录告警。 |
| 可对系统登录行为进行一定的限制，可设置单个IP请求时间、登录失败次数、IP临时锁定时间。 |
| 违规外联支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断。 |
| 提供内核级防火墙（业务间流量东西向隔离）服务，实现对包括IP、端口、协议、流向等细粒度权限控制。 |
| 提供流量画像服务，实现全网流量可视化 |
| 提供登录防护服务，包括以系统账号为粒度的异常登录防护、支持五个任意维度（任意IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 |
| 可显示隐藏的系统账户 |
| 可对顽固流行病毒进行智能拦截。 |
| 针对Windows系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程 |
| 提供专门的勒索风险评估服务。 |
| 提供专门的针对已知、未知勒索病毒的防御引擎，并提供功能开关项。对于已知勒索病毒确保进程无法启动。 |

## 6.2终端安全零信任控制服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 对所有终端首次入网推行安装终端管控软件，并打通“浙政钉”手机扫码实现身份实名制接入，零信任架构结合终端安装软件，可对政务网络环境的多层NAT的穿透，实现对身份精准定位和管控，避免如私接路由、地址转换后的终端管控盲区。预采购数量为10000个点位，超过预采购的服务须承诺免费提供。 |
| 网络隐身服务 | 提供启用网络隐身的服务，开启后默认不向任何用户及终端开放任何TCP端口 |
| 可启用并配置IP白名单，在白名单中的源IP地址可以直接访问控制台的TCP端口 |
| 提供SPA单包授权种子凭证的签发，凭证支持激活次数、激活时间、使用时间限制，凭证提供二维码类型、文件类型 |
| 终端管理服务 | 可对接入零信任控制台的终端进行管理，具备查看终端操作系统、CPU等硬件信息、进程信息、端口开放信息等的能力 |
| 提供用户与终端的一对一、多对一绑定管理的服务，具备为特定用户独立设置绑定设备数量上限的能力 |
| 提供管理配置终端环境监控项的服务，包括但不限于：网络信息、进程信息、软件安装信息、服务运行信息等 |
| 客户端功能服务 | 提供配套的零信任安全接入客户端的服务，客户端可在Windows、MacOS、Android、iOS等操作系统运行 |
| 身份管理服务 | 提供用户、组织、用户分组的统一管理服务，包括用户及组织信息增删改查、导出、用户状态管理、用户同步等服务 |
| 提供用户身份信息字段自定义扩展服务，具备定制外部身份目录对接模板，并可按秒、分、时、日、月、年等条件灵活设置同步任务 |
| 可向第三方应用系统提供身份同步接口，接口支持访问认证及授权保护的服务 |
| 可信身份认证服务 | 提供本地账号密码、手机APP扫码、手机动态令牌方式，内置LDAP、微信扫码、钉钉扫码、短信验证码、邮箱验证码等认证对接方式 |
| 提供维护多个不同优先级的用户认证策略，根据配置关联不同的用户及认证因子，可引入安全基线判定条件，当用户登录的安全基线不达标时，不允许用户登录或要求用户执行二次认证 |
| 提供维护应用认证策略，根据配置关联不同的用户、应用及认证因子，可引入安全基线判定条件，当用户访问应用的安全基线不达标时，要求用户执行二次认证 |
| 权限管理及动态授权服务 | 提供应用分组管理，将应用授权到资源角色（应用安全组），应用安全组支持划分安全等级，安全等级分级可自定义 |
| 提供提供应用级鉴权，可从用户、用户组、组织机构视角，维护主体到应用的授权关系 |
| 提供提供应用页面级鉴权，可从用户、用户组、组织机构视角，维护主体到应用页面的授权关系 |

## 7.政务用户行为分析服务

## 7.1用户行为分析（UEBA）服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 通过统计特征学习、动态行为基线和时序前后关联等多种形式场景建模，最终为用户提供包含正常行为基线学习、风险评分、风险行为识别等功能的安全分析能力。 |
| 用户总体风险评估服务 | 提供解决方案视角服务，通过切换解决方案视角，用户可以查看在不同解决方案（主机安全、数据库安全、账号安全及通用解决方案）下的用户总体风险情况。 |
| 提供已录入的用户/数据中发现的所有用户的切换服务。选择已录入的用户，即当前页面展示当前用户在用户信息管理中所录入的用户对应的风险情况。选择数据中发现的所有用户，即当前页面展示当前所接入数据中所有用户的风险情况。 |
| 提供用户风险评分服务，综合考虑用户的所有特征权重、风险信息、历史趋势等维度，进行的自适应算法综合计算评分，以宏观视角审视全网用户，将异常高风险用户呈现出来。 |
| AI模型服务 | 提供AI模型增删改查服务 |
| 提供AI模型列表服务，以查看包括但不限于模型名称、模型分组、模型描述、所用特征名称、所选算法、算法参数、实时检测周期、创建人、状态、创建时间和近运行时间等信息，同时支持全文搜索 |
| 创建AI模型，应包括但不限于up/down异常、daily周期性异常、weekly周期性异常、新出现实体异常、阈值异常和潜伏型异常等算法 |
| 时序异常探索服务 | 提供单时序异常探索服务，可针对AI模型进行特征时序异常探索，可以查看标记列表、异常列表和同时段异常等信息，同时应具备钻取原始日志操作的能力 |
| 提供预测服务，预测时长应包括但不限于一天、一周和一月等 |
| 提供综合异常探索服务，可针对多个AI模型进行交集或并集综合异常探查，可以查看异常排名、异常时间线、标记列表和异常列表等信息，同时可实现快捷标签和实体过滤等操作 |
| 风险评分服务 | 提供用户风险评分服务，能够根据个体的异常、群组对比和历史趋势等维度，按照100分风险最高评分标准综合进行用户风险评分 |
| 提供用户总体风险概览服务，能够直观展示包括但不限于活跃用户总数、最近一周活跃用户数、最近一周高风险用户数、日志总数、用户风险排行、关注用户、最近一周趋势图、用户风险分布图和风险类型分布等信息 |
| 提供自定义调整用户总体风险刷新周期服务，绝壁最小1分钟调度周期的能力，可选择基于历史多少天的风险数据进行用户总体风险评分。 |
| 提供风险阈值调整服务，能够针对高、中、低和无4个风险级别进行区间调整 |
| 可针对特定用户进行用户行为画像，能够从风险趋势和全局画像两种模式进行用户行为画像 |
| 态势大屏 | 提供用户行为风险态势可视化大屏服务，应能够清晰展示活跃用户总数以及变化趋势，高风险用户数以及变化趋势，无风险、低风险、中风险和高风险各类用户风险分布，日高风险用户数最近一周趋势，风险类型文字云等信息；并且在大屏中央可以展示正常用户和高风险用户分布情况；同时对于特定的高风险用户，可以轮播展示用户名、职务、工号、账号、邮箱账号、风险评分、较上次风险浮动、当前风险排名、风险趋势以及各类异常图表信息。 |
| 提供账号安全态势感知大屏服务，包含日志量、告警量、活跃账号数和高风险账号数，账号风险排名TOP5，登录失败TOP5，账号日志量趋势、24时账号数量分布、部门日志量TOP5、账号日志量TOP5，风险事件和风险类型等信息。分析时间范围可选24小时、最近7天、本日、本周、本月或者半年；分析视角可以在整体关联视角，或者单独的数据源视角进行切换，单独的数据源视角包括但不限于VPN日志、AD域日志、上网行为审计日志、堡垒机日志、邮件审计日志和零信任日志等。 |

## 7.2蜜罐系统服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| 服务总体要求 | 布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。 |
| 伪装诱捕服务 | 具备Windows、Linux类操作系统蜜罐能力，提供不低于7种蜜罐，包括但不限于：CentOS7、SUSE12、SUSE12sp2、RedHat7、Windows7、Windows10、WindowsServer2008等。 |
| 具备Web类蜜罐能力，提供不低于13种蜜罐，包括但不限于Jenkins、WordPress、Zabbix、OA、Nginx、Discuz论坛、DokuWiki、渗透、邮箱、Webmin、Struts2、SugarCRM、Joomla等。 |
| 具备中间件类蜜罐能力，提供不低于3种蜜罐，包括但不限于Tomcat、Weblogic、JBoss等。 |
| 具备数据库类蜜罐能力，提供不低于8种蜜罐，包括但不限于MySQL、Oracle、PostgreSQL、MongoDB、Redis、MemCached、Hive、HBase等。 |
| 具备工控类蜜罐能力，可仿真S7Comm、Modbus、Bacnet、SNMP等6种工控协议。 |
| 具备物联网类蜜罐能力，提供不低于6种蜜罐，包括但不限于Linksys路由器、D-Link摄像头等。 |
| 具备系统服务类蜜罐能力，提供不低于8种蜜罐，包括但不限于DNS、ARP、SSH、扫描检测、Samba、FTP、Telnet、VPN等。 |
| 具备综合型服务蜜罐能力，提供不低于4种服务，如：Redis、Web、Mongo、imitator等。（投标文件商务技术响应文件中提供佐证材料） |
| 具备5G网元仿真服务能力，提供不低于5种蜜罐，包括但不限于UPF、UDR、SMF、NRF、AMF等。 |
| 攻击分析服务 | 可基于攻击事件聚合攻击行为，捕获某一攻击者对某一蜜罐/蜜饵产生的所有攻击，并按照时间轴形式详细展示攻击内容。 |
| 可基于攻击者聚合攻击事件，展示所有该攻击者的攻击事件，且可对攻击者添加标签。 |
| 提供解析/下载流量包、下载爆破字典、查看攻击截图、查看攻击视频、还原攻击日志等内容的服务。 |
| 提供系统自动比对攻击源IP溯源信息的服务，可根据内置算法模型判断是否/可能为同一攻击者使用的不同IP。 |
| 可捕捉、下载可疑落盘文件，并通过在线和离线两种方式进行云端情报库/沙箱深度检测分析，获得HTML格式的分析报告。报告内容包括文件的基本信息、静态分析、软件环境、威胁情报、动态行为、可疑行为、进程行为、网络行为、文件行为、注册表行为、其他行为、内存字符串、截屏信息等。（投标文件商务技术响应文件中提供佐证材料） |
| 可对攻击者进行溯源，识别出攻击者设备信息和网络身份信息，包括但不限于：设备类型/名称/品牌/显卡/声卡/屏幕分辨率/字符集编码、操作系统类型/版本/系统语言/时区、应用程序类型/版本等信息，以及至少12种主流社交平台账号信息（包括社交平台logo/用户ID/用户名/用户昵称/用户头像等）等。 |

## 8.驻场人员安全运营服务

## 8.1驻场服务

|  |  |
| --- | --- |
| 服务能力指标 | 具体服务技术要求 |
| ★服务总体要求 | 组建不少于4名工程师的义乌市网络安全运营团队，需驻点在甲方指定场所，以“驻场人员总体牵头，专家团队在线支撑”的模式进行义乌市数据管理中心网络安全保障。安全运营团队组建以“能力多样、体系完善”为原则，打造一个能力全面、响应迅速的本地化专业技术服务团队。依托专业厂商网络安全服务团队，其中包括安全运维工程师、应急响应工程师、渗透测试工程师以及安全制度编写人员，主要承担义乌市全链路监管体系驻场运营服务工作，以及重保活动期间突发网络安全服务响应等工作任务。 |

## 四、投标演示要求

1.本项目需要演示：投标方需在投标文件解密成功后，进入政采云平台开标大厅，等待通知演示。政采云平台会以投标文件解密时间的先后顺序以短信的形式通知演示，每个投标人演示前的调试准备时间不超过15分钟，演示时间不超过20分钟，不包含评标委员会提问解答时间。演示的方式通过“开标大厅”（建议选择谷歌浏览器）的屏幕共享方式进行演示，其中涉及需要安装的软件投标人应在开标前自行下载安装，确保网络、麦克风、演示环境等演示所需设备和系统正常稳定，并提前熟悉操作和使用。由评委对各投标人针对招标文件中演示部分进行评定打分。

2.演示形式：投标方针对招标文件需要演示的内容，需使用成熟或DEMO软件进行演示，不演示或者使用PPT,WORD等文本形式演示者不得分。提供第三人视角方式进行连续拍摄，拍摄画面中需包含时间计时器或其他方式以表明其拍摄过程不存在剪切编辑情况存在，请依照招标文件要求进行演示，演示过程中需语音介绍目前演示的内容是什么，演示时长不超过20分钟。

## **五、项目考核要求**

**1.月度考核指标**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 一级指标 | 二级指标 | 三级指标 | 指标定义 | 赋分方法 |
| 1 | 服务能力（60分） | 全链路监管服务（10分） | 监管定制程度（10分） | 定制覆盖云、网、数据、应用、端、行为六个维度的网络安全监管服务 | 1.六个维度都涉及10分； 2.缺少一个维度扣2分，扣完为止； |
| 政务云安全资源池服务（10分） | 资源池能力（5分） | 安全资源池安全能力至少包括下一代防火墙、web应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全（EDR）、APT等安全能力 | 1.安全资源池全部包含指标安全能力，得5分； 2.若不满足指标安全能力，每少1项扣1分 |
| 云租户数量（5分） | 为市党政机关提供至少70个单位的安全资源池服务 | 1.满分5分； 2.若发现云安全资源池服务数量不满足要求，每一个数量扣1分 |
| 网络安全数据分析服务（10分） | 数据安全能力覆盖（5分） | 提供包含数据分级分类、数据脱敏服务、数据管控服务、数据加密服务、数据安全态势感知服务等能力 | 1.完成5项数据安全能力实现，得5分； 2.若部署安全能力的过程中，每少1项扣1分 |
| 数据安全管控质量（5分） | 可基于IP、MAC、客户端主机名、操作系统用户名、客户端工具和数据库账号六个维度认证身份 | 1.完成6个维度认证身份，得5分； 2.若发现数据认证身份维度缺少，每次缺少1个维度扣1分，扣完为止； |
| 政务应用安全防护服务（10分） | 应用防护服务（5分） | 针对应用防护能够实现一键关停、区域访问控制、流量监测等能力 | 1.能够对应用防护能力进行实现，得5分；2.若发现有不能实现能力，每个能力扣2分，扣完为止； |
| 应用监测服务（5分） | 采用模拟访问方式实现故障实时自动发现，对故障情况自动分析并精准定位故障点并实现自动记录； | 1.能够对应用监测能力进行实现，得5分；2.若发现有不能实现能力，每个能力扣2分，扣完为止； |
| 政务外网终端安全服务能力（10分） | 终端安全主机防护（5分） | 对所有终端部署杀毒软件，实现全域安全数据可视，超过10000个点位免费提供。 | 1.能够对所有终端部署杀毒软件，得5分。2若发现有拒绝安全终端，每个终端扣1分，扣完为止； |
| 终端安全零信任控制（5分） | 通过零信任控制终端，实现浙政订扫码、终端环境感知、网络管控、违规外联监测、准入控制等。 | 1.能够对零信任控制能力进行实现，得5分；2.若发现有不能实现能力，每个能力扣1分，扣完为止； |
| 政务用户行为分析服务能力（10分） | 用户行为分析（5分） | 统计特征学习、动态行为基线和时序前后关联等多种形式场景建模 | 1.能够对用户行为分析能力进行实现，得5分；2.若发现有不能实现能力，每个能力扣2分，扣完为止； |
| 诱捕行为分析（5分） | 作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析 | 1.能够对诱捕行为分析能力进行实现，得5分；2.若发现有不能实现能力，每个能力扣2分，扣完为止； |
| 2 | 服务质量（30分） | 驻场人员安全运营（10分） | 驻场要求（10分） | 安排不少于4名驻场人员安全运营 | 1.安排4名及以上驻场人员,得10分； 2.安排3名驻场人员，得7分； 3.安排2名驻场人员，得5分；  |
| 重保时期服务质量（10分） | 重保要求（10分） | 重保时期（如亚运）安排3个安全工程师24小时轮值安全保障 | 1.重保时期安排3个人轮值，得10分； 2. 重保时期安排2个人轮值，得7分；3. 重保时期安排1个人轮值，得5分 |
| 有效投诉（6分） | 部门投诉情况（6分） | 部门对驻场团队的投诉情况 | 1. 无投诉，得6分；

2.若出现投诉情况，每个有效投诉扣2分 |
| 操作规范（4分） | 操作合规情况（4分） | 驻场团队在日常工作中的安全操作情况 | 出现违规或者不规范操作情况，每人每次扣1分 |
| 3 | 服务保障（10分） | 服务响应（5分） | 响应指标（5分） | 安全处置7\*24小时服务，15分钟内响应，半小时内到达现场 | 1. 完全满足相应指标，得5分；

2.有一项响应指标不满足，扣2分； |
| 服务效率（5分） | 甲方交办的工作效率（5分） | 按时完成安全运营、网络安全调整、文档整理等甲方交代的工作 | 1.根据甲方要求，按时完成安全运营、网络安全调整、文档整理等工作，得5分； 2.未及时完成的，每超期一个工作日扣2分 |

**2.年度考核：**

根据每月考核情况，得出年度考核分：95（含）分以上，按当年计划支付金额的100%支付年度运维费用；90-94分，按当年计划支付金额的95%支付年度运维费用；85-89分，按当年计划支付金额的88%支付年度运维费用；85（不含）分以下，按当年计划支付金额的80%支付年度运维费用。若连续三个月得分在85分以下，甲方有权单方解除本合同，双方按实际服务量进行结算，甲方已支付费用超过结算价的，乙方应在结算后20个工作日内退还超额支付的价款。

## **★六、商务要求**

**1.项目服务期限：**合同签订正式生效以及具备项目服务条件后三年整。

**2.为确保服务质量，服务要求如下：**

（1）合同签订完成后，根据采购人提供的接口文档，在20个工作日内协助采购人完成横向平台（义乌市网信办）与纵向平台（金华市大数据局）的情报共享、事件流转、数据上报等数据流、业务流对接工作。

（2）常态化安全运营，包括通报、考核、核查、周报、月报等日常工作，协助采购人指导各单位做好网络安全整改工作。

（3）重大活动时期安保，安排不少于3名安全工程师，提供7\*24小时现场值守工作。

（4）提供7\*24小时应急响应上门服务，要求15分钟内响应，30分钟内到达现场。

（5）服务期内，做好全链路监管平台的运维工作，硬件按需更新或扩容，软件及时升级至最新版本。

**3.报价要求**

投标人应根据国家的有关规定和招标文件要求并结合企业的实际情况进行投标报价。投标报价以人民币为结算货币，投标报价须包括因承包本次采购项目服务所需的服务费、线路租赁费（如有）、货物价款（备品备件）、项目软硬件费用、人员费用、运输费、装卸费、利润、税金、保险及不可预见费用等一切费用，应是招标文件确定的招标范围内的全部工作内容的价格表现，完成该项目的所有费用及各环节所必需的连带工作或服务、成果验收、以及政策性文件规定、合同包含的所有风险责任等所有费用。如有漏项，视同已包含在本报价中，投标单价及总价不做调整。按国家规定由中标方缴纳的各种税收已包含在投标总价内，由中标方向税务机关缴纳。

**4.验收要求：**根据中华人民共和国现行技术标准，按招标文件以及合同规定的验收评定标准等规范，由采购人根据《政府采购合同履约和验收管理办法（暂行）》（义招管办【2008】32号）文件要求和《义乌市关于规范政府采购管理的若干意见》（义政办发【2017】102号）要求和行业相关的规定，组织验收。

**5.结算和付款方式：**

（1）在合同生效以及具备项目服务条件后7个工作日内，采购人向中标人支付第一年度计划支付金额的40%作为年度预付款（在签订合同时，中标方明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不支付或减少预付款支付比例）。采购人可以要求供应商提交银行、保险公司等金融机构出具的预付款保函或其他担保措施。
 （2）项目第一年服务期结束后7个工作日内，采购人根据考核结果进行实际结算后向中标人支付第一年度的剩余支付金额及第二年度计划支付金额的40%作为年度预付款（中标方明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不支付或减少预付款支付比例）。采购人可以要求供应商提交银行、保险公司等金融机构出具的预付款保函或其他担保措施。

（3）项目第二年服务期结束后7个工作日内，采购人根据考核结果进行实际结算后向中标人支付第二年度的剩余支付金额及第三年度计划支付金额的40%作为年度预付款（中标方明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不支付或减少预付款支付比例）。采购人可以要求供应商提交银行、保险公司等金融机构出具的预付款保函或其他担保措施。

（4）项目第三年服务期结束后7个工作日内采购人根据考核结果进行实际结算后向中标方支付第三年度的剩余支付金额。

（5）采购人根据考核结果进行实际结算。

（6）合同款凭发票、合同、中标通知书、考核结果和政府采购资金结算单由义乌市财政支付。

## **★七、其它说明**

1.本项目设有一个标项，对于同一标段内的产品或服务不允许拆分参投，否则其投标无效。

2.中标之后，如发现投标人的投标文件内容有不一致的，以有利于采购人和使用单位的原则执行。

# 第四章 开标、评标和定标须知

## 一、开标

1.本项目实行电子开评标，投标人无需前往开评标现场，应在规定时间内在“政采云”上上传电子投标文件和准时在线参加开标。

2.电子开评标及评审程序

2.1采购中心开启解密后的1小时内，由各投标人自行对电子投标文件进行解密（请各投标人务必在规定时间内完成电子投标文件的解密工作，在电子开评标期间，投标人（授权代表）需确保在各自所在的区域具备上网的技术条件并保持网络及联系方式畅通；

2.2.评标委员会对投标人的资格和商务技术响应文件进行评审；

2.3评标委员会对报价响应文件进行评审；

2.4在系统上公布评审结果。

**特别说明：“政采云”如对开评标程序有调整的，按调整后的程序操作。**

## 二、评标

**3.评标小组**

招标方将根据招标采购项目的特点确定评标委员会（即评标小组）。其成员由评审专家和采购人代表共5人及以上单数组成。评标小组对投标文件进行审查、质疑、评估和比较。

**4.评标原则**

4.1评标小组将遵循公开、公平、公正的原则，严格遵守评标工作纪律。

4.2先评资格及商务技术响应文件，再评报价响应文件。

4.3客观公正对待所有投标人，对所有投标评审均采用相同的程序和标准。评标的依据为招标文件和相关法律、法规及政策文件。

4.4异常或特殊情况处理：

4.4.1在评标过程中，如发现招标文件中内容有不一致的（招标文件中其它地方另外规定的除外），经评标委员讨论认为不影响评标的，可以继续评标。

评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，应当停止评标工作，与采购人或者采购代理机构沟通并作书面记录。采购人或者采购代理机构确认后，应当修改招标文件，重新组织采购活动。

4.4.2在评标过程中，出现其它异常或特殊情况时，由评标小组集体讨论决定。

4.5评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

**5.评标过程的保密**

5.1开标后，直至授予中标人合同为止，凡属于对投标文件的审查、澄清、评价和比较等有关的资料以及中标候选人的推荐情况等与评标有关的任何情况均严格保密。

5.2中标人确认后，采购人不对未中标人就评标过程以及未能中标原因作出任何解释。未中标人不得向评标小组人员或其他有关人员索问评标过程的全部情况。

5.3为保证定标的公正性，在评标过程中，评标成员不得与投标人私人交换意见。在招标工作结束后，凡与评标情况有接触的任何人不得也不应将评标情况扩散出评标成员之外。

**6.投标文件的澄清**

6.1为有助于投标文件的审查、评价和比较，评标委员会应当在“政采云”在线询标或采用其他有效形式要求投标人对同一份投标文件含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容（招标文件其它地方有另有规定处理方法的除外）作必要的澄清或说明，投标人应采用在线回复或其他有效形式在询标规定时间内进行澄清或说明（需盖电子签章或实体公章），但不得超出投标文件的范围或改变投标文件的实质性内容。根据本须知第8条规定，凡属于评标小组在评标中发现的计算错误并进行核实的修改不在此列。

6.2如果投标人代表拒绝按评标委员会要求在“政采云”作出在线回复且无其他有效回复方式的，评标委员会可以对其作出无效标处理。

**7.投标文件的资格性和符合性评审**

7.1评标时，评标小组将首先评定每份投标文件是否实质上响应了招标文件的要求。所谓实质上响应，是指投标文件应与招标文件的所有实质性条款、条件和要求相符，无显著差异或保留。

7.2如果投标文件出现第五章规定的内容，即为实质上不响应招标文件的各项要求，评标小组将予以拒绝（或作为无效标），并且不允许投标人通过修改或撤销其不符合要求的差异或保留，使之成为具有响应性的投标。

7.3在投标文件的评审和比较、中标候选人推荐以及授予合同的过程中，投标人向采购人和评标小组施加影响的任何行为，都将会导致其投标被拒绝。

**7.4评标小组在作出任何一项无效标决定前，都应当严格遵循以下程序：**

7.4.1要求当事投标人作相应的答辩。

7.4.2在充分讨论的基础上集体表决。

**8.投标文件计算错误和不同文字文本的修正**

8.1修正原则如下：

8.1.1对不同文字文本投标文件的解释发生异义的，以中文文本为准；评标委员会可以拒绝接受不是中文版的投标文件以及与投标相关的资料。

**8.1.2投标文件的商务技术响应文件中，同类内容表述不一致的处理：彩页、官网下载资料、检测报告等证明性资料中描写的技术性能指标与投标文件中其它地方内容描述不一致的，应以上述证明性资料为准；规范偏离表等偏离表的内容与投标文件中其它地方内容有描述不一致的，应以投标文件中其它地方内容的描述为准。其它情形的，评标委员会以在线询标或其他有效形式要求投标人作必要的澄清或说明。**

8.1.3投标文件报价出现不一致的，除招标文件另有规定外，按照下列规定修正：

（1）客户端填写的报价与以pdf格式上传文件中的报价不一致的，应以pdf格式上传文件中的报价为准。

（2）投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准；

（3）投标文件的大写金额和小写金额不一致的，以大写金额为准。

（4）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

（5）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价通过“政采云”经投标人确认后产生约束力，投标人不确认的，其投标无效。

**9.评标办法**

**本项目采用综合评分法（具体评标办法见第六章）。**

**10.决标**

评标小组依据本招标文件规定的评标标准和方法，对投标文件进行评审和比较，向招标方提交书面评标报告。

 **11. 在招标采购过程中，有下列情形之一的，应对采购项目予以废标：**

（1）通过资格审查或评审后有效投标人不足三家的；

（2）出现影响采购公正的违法、违规行为的；

（3）因重大变故采购任务取消的；

（4）招标文件另有规定情形的。

## 三、定标

**12.中标通知**

12.1投标人自2019年1月1日起到中标公告期结束前无行贿犯罪记录（评标结束后，发放中标通知书前，由采购人通过中国裁判文书网（http://wenshu.court.gov.cn/）按照招标文件约定，对拟中标（成交）单位及其拟派项目负责人的行贿犯罪记录进行查询，查询结果以网站页面显示内容为准）,经查实，中标人有前述行贿犯罪记录的，取消其中标资格，采购人依法重新组织采购。

12.2评标结束后，采购结果公告期限为1个工作日，发布采购结果公告的媒体为：浙江政府采购网站、义乌市公共资源交易平台。

12.3由义乌市政府采购中心通过 “政采云”签发《中标通知书》，《中标通知书》一经发出即发生法律效力。

**13、合同签订**

13.1中标人自接到《中标通知书》后应在三十天内与采购人签订合同。

13.2招标文件、中标人的投标文件、评标过程中投标人在询标时作出的承诺及其澄清文件等，均为签订合同的依据。

13.3中标人不遵守招标文件和投标文件的要约及承诺而擅自修改报价，或在接到《中标通知书》后借故拖延、拒签合同而造成超过规定时间的，取消该投标人的中标资格。在此情况下，采购人和招标代理机构重新招标，对受影响的投标人不承担任何责任。

13.4采购人变更数量的权利

采购人在授予合同时有权对“第三章 招标项目”要求中规定的货物数量和服务予以增加或减少，但必须符合《中华人民共和国政府采购法》及义乌市政府采购的相关规定。

**四、质疑和投诉**

14.1开标过程中，投标人对开标有异议的，应当在“政采云”上及时提出，评标委员应对异常情况制作相关记录。

14.2开评标结束后，投标人或者其他利害关系人对依法必须进行招标的项目的评标结果有异议的，应在采购结果公告期限结束之日起的7个工作日内，依据政府采购相关法律法规向采购人、采购代理机构提出质疑。采购人或招标代理机构将在收到书面质疑后7个工作日内对质疑内容作出答复。若投标人对采购人或采购代理机构的答复、处理结果不满意，应在收到书面答复后十五个工作日内向同级政府采购监督管理部门投诉。

14.3质疑投诉的相关规定质疑应当包括下列内容：

（1）供应商的名称（或姓名）、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据及相关证据材料；

（5）必要的法律依据；

（6）提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

质疑投诉存在以下情形之一的，将不予受理：

（1）质疑投诉人不是参加本项目的供应商；

（2）供应商自身权益未受到损害的；

（3）已超过法定质疑投诉提出期限的事项；

（4）质疑未提供书面质疑或未按要求签署或盖章的；

（5）质疑已经处理并答复后，质疑人就同一事项再次提起质疑且未提供新的有效证据的；

（6）质疑投诉的事项已经进入行政复议或者行政诉讼程序的；投诉事项应先提出质疑而没有提出质疑的；

（7）不符合《政府采购质疑和投诉办法》（财政部令第94号）等有关规定的投诉。

# 第五章 投标文件的无效情形

**1.有下列情形之一的，招标方将不予受理投标文件：**

1.1逾期上传电子投标文件至“政采云”的。

1.2电子投标文件在规定时间内解密未成功的，且未提供备份投标文件或提供的备份投标文件无法上传打开的。

**2.投标文件在资格性评审或技术响应性评审出现下列情形之一的，由评标委员会审核后按无效投标文件处理：**

2.1.资格响应文件或商务技术响应文件中包含商务报价的；

2.2招标文件关于投标文件组成内容商务技术响应文件要求中打“★”的内容，投标人的投标文件内容未提供完整的，或关键字迹模糊、无法辨认的，或未按其规定的格式及要求填写、签字、盖章，或提供的投标文件内容不符合招标文件的中有关打★号的条款的规定；

2.3投标人的投标资格不符合招标文件的资格要求规定；

2.4投标人所投产品的数量不符合招标文件规定的；

2.5投标人借用或冒用他人名义或证件、涂改文件、伪造或编造投标文件的；

2.6投标中不同投标单位的投标文件出现雷同或相似（包括部分雷同或相似），对所有雷同或相似投标人按废标处理，招标方将保留进一步追究责任的权利；投标人串标的；

2.7其它对本招标文件中打★号的条款未完全响应的；

2.8经评标委员会认定，投标文件附有采购人不能接受的条件；

2.9评标委员会要求投标人澄清或说明的，如果投标人拒绝按照招标文件规定进行澄清或说明的。

**3.报价响应文件评审出现下列情形之一的，由评标委员会审核后按无效投标文件处理：**

3.1.招标文件关于投标文件组成内容报价响应文件要求中打“★”的内容，投标人的投标文件内容未提供完整的，或关键字迹模糊、无法辨认的，或未按其规定的格式及要求填写、签字、盖章，或提供的投标文件内容不符合招标文件的中有关打★号的条款的规定；

3.2投标报价高于最高限价或低于项目成本总价的；

3.3投标人的所投产品的数量不符合招标文件规定的；

3.4投标人的投标报价未明确的，或者对同一采购项目提供两个或两个以上报价且未声明哪一个有效的，或者对同一采购项目提供两个或两个以上成本价且未声明哪一个有效；

3.5经评标委员会审议认为投标文件附有采购人不能接受的条件的；

3.6评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品服务或者不能诚信履约的，要求其通过“政采云”在规定的时间内提供CA签章的材料，投标人不能证明其报价合理性的；

3.7其它对本招标文件中打★号的条款未完全响应的；

3.8当投标人由于报价计算错误，投标人拒绝接受按招标文件的规定进行的修正处理。

**4.在资格审查及评审过程中，符合中华人民共和国财政部令第87号《政府采购货物和服务招标投标管理办法》第三十七条情形之一的，视为投标人串通投标，其投标无效，并移送采购监管部门：**

（1）不同投标人的投标文件由同一单位或者个人编制；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（5）不同投标人的投标文件相互混装；

**5.其他法律法规规定的投标文件无效的情况。**

**6.评标过程中，非上述所罗列的情况，不得以无效标处理。**

# 第六章 评标办法

根据《中华人民共和国政府采购法》及相关法律的有关规定，为更好地做到公开、公平、公正，结合本次招标的特点，特制定本评标办法，本项目的评标办法为综合评分法。

**一、评审程序**

评标小组以开标、评标、询标情况为基本依据，按照招标文件的规定，对各投标人的投标文件按资格部分、商务技术部分和报价部分顺序进行分析、评议，具体按以下程序进行评审：

（一）对所有投标人的资格响应文件进行审查，并以开标当日为准，对投标人“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）信用记录情况进行查询，根据（义行服管〔2017〕17号）的规定，对投标人的综合信用报告评级进行查询。

（二）对通过资格性审查合格的投标人的商务技术响应文件进行符合性审查。

（三）对通过符合性审查有效的投标人的商务技术响应文件进行技术评分（详见三、评分细则）。

（四）上述投标人的评分结束后，评标委员会对上述投标人的报价文件进行评审；评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响服务质量或者不能诚信履约的，应当要求其通过“政采云”在规定的时间内提供加盖投标人CA签章的材料，必要时提交相关佐证材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

（五）对通过报价评审有效的投标人,由“政采云”计算出其报价分及总得分，并由评标委员会进行确认。

（六）确定中标人

1.首先，评标委员会按综合得分从高到低顺序进行排列；得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按技术分从高到低顺序排列；技术分也相同的，投标报价相同的由采购人代表采用公共资源交易中心抽取程序随机确定。

2.其次，评标委员会直接确定排名第一的投标人为中标人。

（七）完成评标报告

评标委员会根据评审相关情况作出评标报告。

**二、确定的中标人放弃中标等情况的处理**

当确定的中标人放弃中标，因不可抗力提出不能履行合同，或者质疑投诉成立，取消中标人资格的，都不再确定其余投标人作为中标人**。**

1. **评分细则**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分内容 | 评分细则 | 分值 | 备注 |
| 一 | 商务技术分 | 评标委员会根据评分细则，对各投标人的技术标进行书面审核和评论后，由各成员独立给分，打分时保留小数1位，每人一份评分表，并签名。在统计得分时，如果发现某一单项评分超过评分细则规定的分值范围，则该张评分表无效。投标人技术分的最终得分为评标委员会组成员的有效评分的算术平均值。计算结果保留小数2位(第三位四舍五入)。 | 90分 |  |
| 1 | 同类业绩（1分） | 投标人提供近3年内（2019年1月1日至今，以合同签订日期为准）类似项目业绩，每提供一个得0.5分，最高得1分。投标文件商务技术响应文件中提供合同扫描件加盖投标单位电子签章，提供的合同扫描件清单内容能体现类似项目情况，否则不得分。 | 0-1 | 客观分 |
| 2 | 投标人能力体现（4分） | (1)投标人具备能力成熟度模型集成（CMMI）认证证书：5级及以上的得2分；(2)投标人具备数据安全能力成熟度证书得2分。不具备不得分。投标文件商务技术响应文件中提供证书扫描件。 | 0-4 | 客观分 |
| 3 | 技术服务方案(14分) | 投标人对本项目的业务现状和安全需求提供详尽的需求分析，结合本项目的实际情况，对需求分析的合理性进行评议，0-2分，不提供不得分。 | 0-2 | 主观分 |
| 根据本项目的整体解决方案的先进性、合理性进行打分，包括具备构建覆盖“云、网、端、数据、应用、行为”的安全技术防护能力，可将多维度的数据进行汇聚整合、联动及安全管理，形成“1+4”的监管模式（一个服务—全链路网络安全监管服务，四项监管成果—补短板、强基础、严考核、重闭环）等情况，1-4分，不提供不得分。 | 0-4 | 主观分 |
| 根据投标人针对本项目实施过程中可能出现的紧急情况是否提供详细的应急措施方案（应急方案目的、风险分析、应急措施等）是否全面合理、科学可行进行打分，0-3分，不提供不得分。 | 0-3 | 主观分 |
| 根据投标人针对关于安全管理、安全监测、安全防护等指标的优化提升方案内容进行打分，须详细阐释问题现状、提升路径、落地措施、结果预估等内容，2-5分，不提供不得分。 | 0-5 | 主观分 |
| 4 | 项目实施团队(10分) | 项目经理具有注册信息安全专业人员证书（CISP）、信息安全保障人员认证证书（CISAW）、网络安全应急响应工程师（CCRC）、网络与信息安全管理员证书、零信任安全认证证书（CZTP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、数据库大师认证证书（OCM）或相关专业（网络专业、安全专业）其他高级证书的,每本证书得1分，本项最高5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。 | 0-5 | 客观分 |
| 技术负责人具有信息技术基础构架库认证证书（ITIL）、工信部软件服务IT服务项目经理证书、华为认证网络资深工程师（HCIP）、麒麟操作系统应用工程师认证证书、Oracle数据库管理员认证专员证书（OCP）、高级工程师（传输与接入）认证证书、大数据建模与分析师认证证书、系统架构设计师（高级）认证证书或相关专业（网络专业、安全专业）其他高级证书的，每本证书得1分，本项最高得5分。投标文件商务技术响应文件中提供证书扫描件及近3个月的对应投标单位的社保佐证材料扫描件，不提供不得分。 | 0-5 | 客观分 |
| 5 | 项目实施方案（6分） | 根据投标方在服务内容上详细、清晰、合理，管理机构设立完善，措施保证，运作流程清晰等情况评分，0-2分，不提供不得分。 | 0-2 | 主观分 |
| 根据投标人提供与上级单位纵向协同（包括但不限于资产数据、安全事件、安全隐患、安全情报、通报数据、系统等保备案率、系统等保测评通过率、终端安全防护软件安装率、高危漏洞及端口、弱口令、高危外联、攻防演练等工作)的建设性举措方案，以及与本地网络安全监管单位（如公安、网信办）横向协同（包括但不限于情报共享、隐患/事件协同等工作）的建设性举措方案进行评分，1-4分。不提供不得分。 | 0-4 | 主观分 |
| 6 | 项目服务保障措施(5分) | 根据投标人服务保障的过程管理的可行性、完整性进行评分，0-1分。 | 0-1 | 主观分 |
| 根据投标人服务保障的结果保证的可行性、完整性进行评分，0-1分。 | 0-1 | 主观分 |
| 根据投标人驻场服务人员的运营职责定位合理性进行评分，要求明确规范但不限于资产运维组、数据分析组、协同核验组、考评规范组、重保应急组等工作职责，落实标准的安全运营流程，引入高阶安全专家，持续、动态、主动地落实安全运营工作进行评分，0-3分，不提供不得分。 | 0-3 | 主观分 |
| 7 | 服务能力指标(30分) | 加“★”号的技术指标为强制性要求指标，必须满足，不得负偏离；除加“★”号强制性要求指标外，完全响应招标文件“项目技术要求-具体服务技术要求”中所有指标或完全响应且有正偏离的得30分；标“▲”标记参数系指重点参数，投标指标每负偏离一项扣2分；其他技术指标每负偏离一项扣1分。本项评分最高得30分，最低得0分。投标人仅在规范偏离表中作出响应但没有提供指标项所要求的佐证材料或检测报告等相应材料的，视为负偏离项。 | 0-30 | 客观分 |
| 8 | 演示讲解(20分)（备注：录屏须体现连贯性，以计时器为背景。） | **1全链路态势感知展示服务，围绕大数据局考核要求的“云网数用端”多个维度进行展示呈现。** | 0-4 | 客观分 |
| （1）支持以下功能：对接网络安全、数据安全、云安全、应用准入、边界安全等领域的安全管理中心，展示各中心部署引擎数和上报数据数；统计并展示选定任意日期和时间范围内的互联网暴露面，包括域名、IP、开放端口等；统计并展示安全运营现状，包括存在的高危漏洞、高危端口、高危违规、弱口令、防火墙阻断、安全处置等，得1分，否则不得分。 |
| （2）支持以下功能：展示实时保障力量，包括团队规模、安全值守、机关单位、安全支撑单位、安全指挥长、总联络人。展示全链路安全监管对象，包括监管单位、监管系统、监管终端、安全设备、数据资产、用户档案等信息，得1分，否则不得分。 |
| （3）支持以下功能：在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反应三层之间的关联关系，将攻击行为从网络空间映射到地图空间，再到单位拓扑，得1分，否则不得分。 |
| （4）支持以下功能：在地理、网络、行为主体等不同图层上以地图打点方式展示单位、系统、人员信息，点击查看详情，得1分，否则不得分。 |
| **2、全链路处置通报流程，结合大数据局事件场景，实现事件同步和分析研判。** | 0-3 | 客观分 |
| （1）支持以下功能：展示网络和数据安全事件场景化验证，包括弱口令、挖矿、勒索病毒等场景；展示通过单位名称、IP地址、时间等多字段组合查询场景内容；展示事件信息联想，通过事件数据关联同单位事件、同类型事件、同终端事件等联想方式，得1分，否则不得分。 |
| （2）支持以下功能：展示通过“与”、“或”、“包含”等不低于15种语法分析研判，根据攻击类型和攻击信息进行数据聚合分析，不低于13种攻击类型分类，自定义攻击信息字段，详细展示攻击趋势、攻击链、攻击流向、实体信息等，得1分，否则不得分。 |
| （3）支持以下功能：展示事件通报，事件关联通报中心，一键生成通报信息，得1分，否则不得分。 |
| **3构建全链路安全专题库，根据安全数据和业务关系，落实网络和数据安全专题库，形成数据沉淀积累。** | 0-2 | 主观分 |
| （1）根据以下情况，评委进行评分，0-1分：展示管理不少于10个安全专题库，展示专题库中安全数据与安全业务的关系图谱。 |
| （2）根据以下情况，评委进行评分，0-1分：展示对全库进行模糊搜索，并分别展示各专题库相关数据，支持以资产为主体的模糊搜索，通过关联关系展示专题库中与该资产相关的信息。 |
| **4重大活动安全保障能力，可根据重要时期，建立专项保障任务，调度保障资源，适配保障场景的需求。** | 0-2 | 主观分 |
| （1）根据以下情况，评委进行评分，0-1分：展示对保障人员、保障单位、安保制度、安保组织、支撑单位、驻点小组等应急力量和物资的管理，展示重大活动保障前、中、后不同阶段里程碑节点管理，展示回放复盘历史保障过程。 |
| （2）根据以下情况，评委进行评分，0-1分：展示通过应急作战台展示活动信息和近期重点工作，快速查看通报详情并处置，按不同等级的应急预案响应指令并联动移动端调度人员，驻点每日分班次上报平安情况。 |
| **5重要应用系统资产梳理，可根据IRS重点应用系统，进行应用系统安全画像呈现。** | 0-2 | 主观分 |
| （1）根据以下情况，评委进行评分，0-1分：展示系统安全画像包括系统信息、系统拓扑、安全检测、防护情况、供应链、安全检查、等保信息、基础网络、人员信息、单位信息、档案时光轴等内容。 |
| （2）根据以下情况，评委进行评分，0-1分：展示卡片式、缩略图方式展示系统信息，一键标记重要系统，一键查看系统事件隐患详情，快速下发系统扫描评估任务，支持系统域名到期提醒。 |
| **6注重过程考评机制，提供多种安全风险评估工作方式，可以定义考评的相关细项分值、权重等内容。** | 0-2 | 主观分 |
| （1）根据以下情况，评委进行评分，0-1分：展示现场检查、单位自查、远程检查三种方式开展安全风险评估工作，界面创建检测表单，上移下移调整检查项顺序，支持检查项类型包括填写、单选、多选、附件上传等。 |
| （2）根据以下情况，评委进行评分，0-1分：展示设定考评范围的地区和行业、考评周期、考评起始时间、考评规则，将发生的安全事件、风险隐患级别和处置情况纳入考评并设定分值和权重。 |
| **7全链路通报预警能力，针对安全事件和风险隐患，进行信息获取并实现通报流程打通。** | 0-2 | 主观分 |
| （1）根据以下情况，评委进行评分，0-1分：展示安全事件和风险隐患一键生成通报信息，通报详情显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。 |
| （2）根据以下情况，评委进行评分，0-1分：通报可进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒，针对已超时的通报进行超时显示，并显示具体超时时间。 |
| **8满足数据安全考核评估指标，实现数据分类分级能力，提供行业法规标准，实现综合评价指标内容达标。** | 0-1 | 客观分 |
| （1）支持以下功能：需内置不少于9种行业法规标准，包括但不限于网络安全法、金融、证券、电信、GDPR、CCPA、等保、数据安全法和个人信息安全规范等，同时应可进行自定义增删修改，得1分，否则不得分。 |
| **9数据安全态势感知展示服务，实现与政务云环境进行部署对接，满足政务云监管、对接、建模等能力。** | 0-2 | 主观分 |
| （1）根据以下情况，评委进行评分，0-1分：业务数据建模功能：通过简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑建模，组件包含应用服务、数据服务、账号、接口、表等； |
| （2）根据以下情况，评委进行评分，0-1分：数据安全监管功能：需详细展示数据资源信息，包括但不限于部门数、主机数、应用数、数据库数等；同时需详细展示安全告警分析、访问统计分析、以及工单状态分析等。与ODPS日志对接：对ODPS访问日志、下载日志等两种类型的日志进行相关采集、存储、查询、统计及分析。具备丰富的查询条件，实时查询ODPS访问日志及下载日志。查询条件包括云账号、来源IP、目的IP、项目名称、操作类型、涉及资产、访问时间等。 |
| 二 | 报价分 | 1、以符合招标文件要求且投标价格最低的投标报价为评标基准价，其报价得分为满分。2、其他投标人的报价分统一按照下列公式计算：报价分＝（评标基准价／投标报价）×10，计算结果保留2位小数（第三位小数四舍五入）。（注：对于小型和微型企业产品的价格给予20%的扣除，对于符合条件的联合体的报价给予6%的扣除，用扣除后的价格参加评审，是否给予价格扣除按第二章投标须知7.2条要求认定。） | 10分 |
| 三 | 综合得分 | 投标单位综合得分=商务技术分+报价分 | 100分 |

# 第七章 义乌市政府采购合同（样本）

需方：

供方：

供、需双方根据2022年 月 日义乌市数据管理中心网络安全全链路监管服务项目（招标编号：YWCG2022039GK）项目中标结果和投标文件的要求，依据《中华人民共和国民法典》并经双方协调一致，订立本采购合同。本合同（□是 □否）为可融资合同。

**一、合同文件组成：**招标文件及其补充更正文件、询标承诺、询疑答复、投标响应文件、双方来函。合同文件组成的所有内容是构成合同不可分割的部分，与合同具有同等法律效力。

**二、合同金额**

合同金额:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_（价款以人民币进行结算，大写）。合同价款中包括\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_等所有费用。

单位：人民币元

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 采购项目 | 数量 | 单价 | 总价 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| ... |  |  |  |  |
| 合计 | ￥：大写： |

**三、服务内容：**

**四、服务期限：**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**五、付款方式：**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**六、技术资料**

1.供方应按招标文件规定的时间向需方提供使用货物的有关技术资料。

2.没有需方事先书面同意，供方不得将由需方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员（项目经办人）提供，也应注意保密并限于履行合同的必需范围。

**七、知识产权**

供方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**八、产权担保**

供方保证所交付的货物的所有权完全属于供方且无任何抵押、查封等产权瑕疵。

**九、履约保证金：**无

**十、转包或分包**

1、本合同范围的服务，应由供方直接供应，不得转让他人供应；

2、供方不得将本合同范围的服务全部或部分分包给他人供应；

3、如有转让和分包行为，需方中止合同，并追究供方的违约责任。

**十一、需、供双方权利和义务：**

需方的权利和义务

供方的权利和义务

**十二、违约责任：**

1．需方无正当理由拒收接受服务的，需方向供方偿付合同款项百分之 作为违约金。

2．需方无故逾期验收和办理款项支付手续的,需方应按逾期付款总额每日万分之 向供方支付违约金。

3．供方未能如期提供服务的，每日向需方支付合同款项的千分之 作为违约金。供方超过约定日期个工作日仍不能提供服务的，需方可解除本合同。供方因未能如期提供服务或因其他违约行为导致需方解除合同的，供方应向需方支付合同总值百分之 的违约金，如造成需方损失超过违约金的，超出部分由供方继续承担赔偿责任。

4.如果供方提供的服务项目的质量未达到本合同规定标准的，则需方有权拒绝，供方需向需方偿付合同款项的百分之 的违约金。如造成需方损失超过违约金的，超出部分由供方继续承担赔偿责任。

**十三、税费**

本合同执行中相关的一切税费均由供方负担。

**十四、不可抗力事件处理**

1.在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2.不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3.不可抗力事件延续\_120\_天以上，双方应通过友好协商，确定是否继续履行合同。

**十五、诉讼**

本合同项目所在地为义乌市，本合同发生争议产生的诉讼，应向项目所在地有管辖权的法院提起诉讼。

**十六、合同双方确认，本合同及合同约定的其它文件组成部分中的各项约定都是通过法定招标过程形成的合法成果，如果中标单位的投标文件与招标文件要求不一致的，履约时应以有利于采购人的条款执行。如果不一致条款不是合同双方真实意思的表示，对合同双方不形成任何合同或法律约束力。合同双方也不存在且也不会签订任何背离合同实质性内容的其他协议或合同。如果存在或签订背离本合同实质性内容的其他协议或合同，也不是合同双方真实意思的表示，对合同双方不构成任何合同或法律约束力。**

**十七、合同生效及其它**

1.合同经双方法定代表人(或负责人)或授权代表签字并加盖单位公章后生效。

2.本合同一式八份，供需双方各执三份，义乌市财政局和义乌市政府采购中心各执一份，均具同等法律效力。

3.本合同未尽事宜，遵照《民法典》有关条文执行。

**十八**、本合同一式 份，需供双方各执 份，义乌市财政局和义乌市政府采购中心各执一份，均具同等效力。

**十九**、本合同在合同签订之日起报义乌市财政局备案。

需 方：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 供 方：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

地 址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 地 址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人(或负责人)：\_\_\_\_\_\_\_\_\_\_\_\_ 法定代表人(或负责人)\_\_\_\_\_\_\_\_\_\_\_\_\_\_

授权代表：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ 授权代表：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

电 话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 电 话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

帐户名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 帐户名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

开户银行：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 开户银行：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

帐 号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 帐 号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

签约时间：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 签约地点：

# 第八章 投标文件部分格式

一、封面格式

二、资格响应文件部分格式：

1、义乌市政府采购项目投标承诺书

2、联合体协议

二、商务技术响应文件部分格式：

3、规范偏离表

4、项目组成人员表

三、报价响应文件部分格式：

5、开标一览表

6、项目成本报价表

7、中小企业声明函

8、残疾人福利企业声明函

封面格式

 项目

投标文件

采购编号：\*\*\*\*\*\*\*\*\*

投标文件内容：（资格、商务技术或报价响应文件）

投标人： （电子签章）

日期： 年 月 日

**义乌市政府采购项目投标承诺书**

致：采购人名称和代理机构名称

1、我单位已认真阅读了义乌市数据管理中心网络安全全链路监管服务项目（采购编号：YWCG2022039GK）招标文件、技术要求、图纸、招标补充（答疑）文件及相关资料，对其全部内容和要求有实质性了解，并对这些内容表示理解且无任何异议，接受其全部内容及要求，承诺我单位的投标文件已经完全响应并符合其全部条件和要求，愿意参加投标并愿意中标。

2、自愿接受义乌市财政局的管理，并严格遵守义乌市财政局制定的招投标管理制度、规范和纪律。

3、我单位承诺参与本次投标的资格符合《中华人民共和国政府采购法》的规定，并承诺近三年内，在经营活动中没有重大违法记录。我单位承诺财务状况良好，并已依法按时缴纳税收和社会保障资金。我单位承诺具备履行本项目合同所必需的设备和专业技术能力。如我单位中标，我单位承诺不转包和分包该项目。

4、积极主动配合义乌市财政局的调查。及时、如实、全面地回答义乌市财政局提出的问题，并在调查笔录中签字确认。如拒绝签字确认的，则视为我单位及有关工作人员认可调查笔录中的全部内容，并对最终的调查结果无任何异议，且自愿放弃一切救济途径。

5、不转让、出借、涂改、伪造资质（资格）证书或者以其他方式允许其他单位（个人）以我单位（本人）名义承接业务。

6、不与采购人或者其他投标人相互串通投标，围标，不以行贿等不正当手段谋取中标。

7、在招标、投标、开标、评标、询标、中标、签订合同等招投标预备和进行的全过程中提供的资料均真实、有效，不弄虚作假。

8、我单位已详细审核全部招标文件，包括更正文件(如果有的话)，及有关附件，我方同意放弃提出含糊不清或误解的权力。

9.投标文件中未明确的内容一律按招标文件规定执行。

10、我单位同意招标文件要求的投标有效期，如我方中标，我方将受此约束。

11、我单位相信贵方的招标结果是公正、合法的，无论我单位中标还是落标，我方将接受这一结果。

12、一旦我单位中标，我单位将严格依照招标文件和投标文件的规定与采购人签订合同。

13、不低于企业成本价投标，不恶意过高报价，不扰乱招投标的正常秩序。

14、严格遵守开标纪律，不在开标现场吵闹、滋事，服从工作人员指挥。

15、按照法律法规和本项目招标文件规定的程序和方式进行异议和投诉，不越级投诉，不无理投诉。如捏造事实、伪造材料或者以非法手段取得材料进行投诉，给他人造成损失的，依法承担赔偿责任。

**15、指定我单位人员(姓名: \_\_\_\_\_\_\_\_\_\_\_\_\_ 身份证号码：\_\_\_\_\_\_\_\_\_\_\_联系电话：\_\_\_\_\_\_\_\_\_\_\_\_\_)全权代表我方联系和协调处理投标过程中的有关事项。**

上述承诺事项已认真逐项核对，均表达我单位真实意见，愿承担任何责任。若有任何弄虚作假内容或未遵守上述约定的，经查实后，愿意放弃投标及中标资格，如由此给采购人造成损失的，我方愿意承担赔偿责任。如我单位违反上述承诺事项，无条件接受义乌市财政局或相关监管部门作出的任何管理和处理决定，并自愿承担一切不利的后果。

投标人（电子签章）： 年 月 日

**联合体协议**

**（以联合体形式投标的，提供联合协议；本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）**

（联合体所有成员名称）自愿组成一个联合体，以一个投标人的身份参加（项目名称）【招标编号：（采购编号）】投标。

一、各方一致决定，（某联合体成员名称）为联合体牵头人，代表所有联合体成员负责投标和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据招标文件规定及投标内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合投标各方产生约束力。

三、本次联合投标中，分工如下：

（联合体其中一方成员名称）承担的工作和义务为： ；……。

四、（联合体其中一方成员名称）提供的全部货物由小微企业制造或服务全部由符合政策要求的小微企业承接，其合同份额占到合同总金额 %以上；……。（未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，接受联合体投标的，联合体其中一方提供的货物全部由小微企业制造或服务全部由符合政策要求的小微企业承接，且其合同份额占到合同总金额 30%以上，对联合体报价给予6%的扣除）

五、如果中标，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

六、有关本次联合投标的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

联合体成员名称(盖公章)： 联合体成员名称(盖公章)：

……

 日期： 年 月 日

**规范偏离表**

采购编号：YWCG2022039GK

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 序号 | 内容 | 招标文件规范要求 | 投标文件对应规范 | 偏离情况详细说明 |
| 商务偏离 |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 技术偏离 |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称（电子签章）：

日 期： 年 月 日

备注：1、投标人应仔细对第三章招标项目要求进行逐条分析，如投标内容与招标文件内容有不一致的，则须在上表中列明并详细填写。

2、如招标文件内容与投标文件内容都一致的，则本表可以在相关的盖章后，不需要填写其它内容或在“偏离情况详细说明”栏内只填写一个无字。

3、此表在不改变表式内容的情况下可自行制作。

**项目组成人员表（格式）**

**项目经理简历表**

**投标人：（电子签章）\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** 采购编号：YWCG2022039GK

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 |  | 性别 |  | 年龄 |  | 学历 |  | 职称 |  |
| 职务 |  | 参加工作时间 | 年 月 日 | 从事类似工作年限 |  |
| 近三年负责完成的类似主要项目情况 |
| 序号 | 业主单位 | 项目名称 | 项目内容 | 项目金额 | 委托日期 | 联系人 | 联系电话 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |

**注：1.如有技术等级或职称证书，需将证书扫描件附于表后；**

 **2.在投标文件中需提供相关证书扫描件和个人社保缴费清单（社保缴费清单要求是持证人员近三个月的在投标单位缴纳的个人社保缴费清单，如投标单位新成立不足三个月的，按实际缴纳情况提供持证人员在该单位的社保缴费清单，社保缴费清单需加盖缴费当地社保机构公章或业务章。近三个月指的是从2022年5月01日至投标截止时止期间中任何一个连续3个月）。**

**3.此表在不改变格式内容的情况下，可自行制作。**

**技术负责人简历表**

**投标人：（电子签章）\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** 采购编号：YWCG2022039GK

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 姓名 |  | 性别 |  | 年龄 |  | 学历 |  | 职称 |  |
| 职务 |  | 参加工作时间 | 年 月 日 | 从事类似工作年限 |  |
| 近三年负责完成的类似主要项目情况 |
| 序号 | 业主单位 | 项目名称 | 项目内容 | 项目金额 | 委托日期 | 联系人 | 联系电话 |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

**注：1.如有技术等级或职称证书，需将证书扫描件附于表后；**

 **2.在投标文件中需提供相关证书扫描件和个人社保缴费清单（社保缴费清单要求是持证人员近三个月的在投标单位缴纳的个人社保缴费清单，如投标单位新成立不足三个月的，按实际缴纳情况提供持证人员在该单位的社保缴费清单，社保缴费清单需加盖缴费当地社保机构公章或业务章。近三个月指的是从2022年5月01日至投标截止时止期间中任何一个连续3个月）。**

**3.此表在不改变格式内容的情况下，可自行制作。**

**项目组成主要成员表**

**投标人：（电子签章）\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** 采购编号：YWCG2022039GK

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **性别** | **技术等级或职称** | **岗位** | **从事该岗位时间** | **从事过类似主要项目** | **备注** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**注：1.如有技术等级或职称证书，需将证书扫描件附于表后；**

**2.在投标文件中需提供相关证书扫描件和个人社保缴费清单（社保缴费清单要求是持证人员近三个月的在投标单位缴纳的个人社保缴费清单，如投标单位新成立不足三个月的，按实际缴纳情况提供持证人员在该单位的社保缴费清单，社保缴费清单需加盖缴费当地社保机构公章或业务章。近三个月指的是从2022年5月01日至投标截止时止期间中任何一个连续3个月）。**

**3.“从事过类主要项目”栏中注明每个参与的项目名称、内容、金额、参与项目的时间、业主联系人、联系人的联系电话、手机等内容。**

**4.此表在不改变格式内容的情况下，可自行制作。**

**开标一览表**

项目名称：义乌市数据管理中心网络安全全链路监管服务项目

采购编号：YWCG2022039GK

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **运维服务内容** | **单位** | **数量** | **单价** | **总价** |
| 1 | 全链路监管定制服务 | 年 | 3 |  |  |
| 2 | 政务云安全资源池服务 | 年 | 3 |  |  |
| 3 | 网络安全数据分析服务 | 年 | 3 |  |  |
| 4 | 政务数据安全防护服务 | 年 | 3 |  |  |
| 5 | 政务应用安全防护服务 | 年 | 3 |  |  |
| 6 | 政务外网终端安全服务 | 年 | 3 |  |  |
| 7 | 政务用户行为分析服务 | 年 | 3 |  |  |
| 8 | 驻场人员安全运营服务 | 年 | 3 |  |  |
| 合计 | 大写： 小写￥：  |

投标人名称（电子签章）：

 日 期： 年 月 日

备注：1、投标报价以人民币为结算货币，投标报价须包括因承包本次采购项目服务所需的服务费、线路租赁费（如有）、货物价款（备品备件）、项目软硬件费用、人员费用、运输费、装卸费、利润、税金、保险及不可预见费用等一切费用，应是招标文件确定的招标范围内的全部工作内容的价格表现，完成该项目的所有费用及各环节所必需的连带工作或服务、成果验收、以及政策性文件规定、合同包含的所有风险责任等所有费用。如有漏项，视同已包含在本报价中，投标单价及总价不做调整。投标报价为投标人所能承受的最低、最终报价。只允许有一个报价，有选择的报价将不予接受。

2、项目投标总价不得超过项目预算价及最高限价，不得低于投标人自报的成本价，否则投标无效。

3、此表在不改变表式的情况下，可自行制作。

**项目成本报价表**

|  |  |
| --- | --- |
| 项目名称 | 项目成本总价 |
| 义乌市数据管理中心网络安全全链路监管服务项目（采购编号：YWCG2022039GK） |  (大写)： 元(小写)￥: 元 |

投标人名称（电子签章）：

 日 期： 年 月 日

备注：

1、投标单位应按照招标项目内容要求，根据项目特点和企业条件确定该项目成本报价，项目成本总价不得高于投标总价，否则投标无效。

2、此表在不改变表式的情况下，可自行制作。

**中小企业声明函（工程、服务）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46号）的规定，本公司（联合体）参加*（单位名称）*的*（项目名称）*采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.*（标的名称）*，属于*（采购文件中明确的所属行业）*；承建（承接）企业为*（企业名称）*，从业人员\_\_\_\_\_\_人，营业收入为\_\_\_\_\_\_万元，资产总额为\_\_\_\_\_\_万元，属于*（中型企业、小型企业、微型企业）*；

2.*（标的名称）*，属于*（采购文件中明确的所属行业）*；承建（承接）企业为*（企业名称）*，从业人员\_\_\_\_\_\_人，营业收入为\_\_\_\_\_\_万元，资产总额为\_\_\_\_\_\_万元，属于*（中型企业、小型企业、微型企业）*；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业（投标人）名称（盖章）：\_\_\_\_\_\_\_

日 期：\_\_\_\_\_\_\_

备注：

1.从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2.本项目采购标的所属行业：软件和信息技术服务业。

**残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（电子签章）：

 日 期： 年 月 日