****

**台州市政府采购招标文件**

**TZCG-2023-GK003号**

采购项目：台州市政务外网安全运营平台项目

采 购 人：台州市大数据发展中心（本级）

台州市政府采购中心

2023年 3 月 20 日

**目 录**

[第一章 投标邀请](#_Toc4350_WPSOffice_Level1) [3](#_Toc4350_WPSOffice_Level1)

[第二章 投标人须知 5](#_Toc25017_WPSOffice_Level1)

[第三章 招标需求 1](#_Toc13072_WPSOffice_Level1)4

[第四章 评标](#_Toc31173_WPSOffice_Level1) [22](#_Toc31173_WPSOffice_Level1)

[第五章 拟签订的合同文本](#_Toc27944_WPSOffice_Level1) [35](#_Toc27944_WPSOffice_Level1)

[第六章 投标文件格式](#_Toc5481_WPSOffice_Level1) [41](#_Toc5481_WPSOffice_Level1)

1. **投标邀请**

## 台州市政府采购中心受台州市大数据发展中心（本级）委托，就台州市政务外网安全运营平台项目进行公开招标，欢迎符合资格条件的国内投标人参加投标。

## 一、项目基本情况

项目编号：TZCG-2023-GK003号

项目名称：台州市政务外网安全运营平台项目

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **标项号** | **标项名称** | **数量** | **单位** | **预算**  **（万元）** | **最高限价**  **（万元）** |
| **1** | 台州市政务外网安全运营平台 | 1 | 项 | 600 | 576.5 |

## 二、投标人的资格要求

（一）满足《中华人民共和国政府采购法》第二十二条规定。

（二）本项目的特定资格要求：无。

（三）信用记录：未被列入“信用中国”失信被执行人或重大税收违法案件当事人名单；未处于“中国政府采购网”[政府采购严重违法失信行为信息记录中的禁止参加政府采购活动期间。](http://www.ccgp.gov.cn）政府采购严重违法失信行为信息记录中的禁止参加政府采购活动期间。)

（四）法律、行政法规规定的其他条件：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，不得同时参加同一项目投标；为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参与本项目投标（联合体投标的，联合体各方均须满足该条款）。

## 三、获取招标文件

（一）时间：2023年3月20日至2023年3月27日

（二）方式：浙江政府采购网（https://zfcg.czt.zj.gov.cn）免费下载

## 四、提交投标文件

（一）截止时间（开标时间）：2023年4月12日9点整（北京时间）

（二）投标网址：浙江政府采购云平台（http://www.zcygov.cn）

**五、发布公告**

（一）公告网址：浙江政府采购网（https://zfcg.czt.zj.gov.cn）、台州市公共资源交易网（https://tzztb.zjtz.gov.cn）

（二）公告期限：本公告期限自发布之日起五个工作日

## 六、注册报名

投标人需登录浙江省政府采购网（https://zfcg.czt.zj.gov.cn/）进行注册后报名。

## 七、联系方式

**（一）采购人（受理招标文件相关质疑及答复）**

名 称：　台州市大数据发展中心

地 址： 台州市椒江区市府大道市政府大楼347室

联系人：　　王先生　　　　　　 　　

联系电话：0576-88510380

**（二）采购组织机构**

名 称：台州市政府采购中心

地　址：台州市市府大道777号

项目联系人：谢女士

联系电话：0576-88685062

受理联系人：侯女士（受理注册、中标结果相关质疑及答复）

联系电话：0576-88685121

技术人员：徐女士

联系电话：0576-88685161

**（三）同级政府采购监管机构**

名 称：台州市财政局政府采购监管处

地 址：台州市财政局

联系人：陈女士

联系电话：0576-88206705

**（四）政采云平台**

联系电话：4008817190

台州市政府采购中心

2023年3月20日

1. **投标人须知**
2. **前附表**

|  |  |  |
| --- | --- | --- |
| **序 号** | **事 项** | **本项目的特别规定** |
| 1 | 是否允许联合体 | ☑ 是/□ 否 |
| 2 | 是否允许分包 | □ 是（但主体部分不得分包，详见招标需求内容）/☑ 否 |
| 3 | 是否需要提供预付款保函 | ☑ 是/□ 否 |
| 4 | 答疑会或  现场踏勘 | 无 |
| 5 | 投标文件的制作和投标 | 请投标人在投标前仔细阅读《政府采购项目电子交易操作指南》。  1.投标文件的制作：投标人按照本项目招标文件和政采云平台的要求，通过“政采云电子交易客户端”编制、加密并递交投标文件（下载网址：[https://zfcg.czt.zj.gov.cn/download/index.html）。](http://www.zjzfcg.gov.cn/bidClientTemplate/2019-09-24/12975.html）。)  2.投标：投标人应当在投标截止时间前（开标当天北京时间09:00）完成投标文件的传输递交，逾期上传的投标文件恕不接受。补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成上传的，视为撤回投标文件。  3.投标文件解密：投标人应在开标当天北京时间09:00至09:30完成解密。 |
| 6 | 备份投标文件的递交 | 备份投标文件是通过政采云电子交易客户端制作投标文件产生的备份文件，请投标人自行妥善保管。  1.使用前提：在解密截止时间前，投标人自行在线解密操作失败，又未能及时联系技术人员帮助解密，或者投标人寻求技术人员帮助仍无法完成解密。  2.递交截止时间：开标当天09:50（北京时间）。  3.投递邮箱：开标当天公布的指定邮箱。  4.未按上述要求递交备份投标文件或所提供的备份投标文件不符合要求的视同放弃投标，仅提交备份投标文件的，投标无效。  5.投标人未按时完成解密的，并符合备份投标文件使用前提的，投标人应提供备份投标文件，否则视为放弃投标。 |
| 7 | 不见面开标  (该项根据实际需求进行调整或删减) | 本项目开评标环节实行全流程电子化，采取政采云不见面开标大厅实现，投标人可自行登录政采云平台进入开标大厅观看现场直播画面。采购组织机构按照采购文件规定的时间通过电子交易平台组织开标、开启投标文件，所有投标人均应当准时在线参加。如未参加，造成无法响应或响应失败等后果由投标人自行承担。 |
| 8 | 远程询标/远程在线演示要求  要求 | 1. 评审小组可能向投标人发起远程询标，投标人需提前做好准备。 2. 本项目是否需要远程在线演示要求详见采购需求。 3. 远程询标/远程在线演示要求通过“政采云视频讲标系统”进行线上问答，投标人在接到政采云信息推送后登录政采云系统--进入开标大厅--进入本项目进行操作，单方面视频下回答评委询问。 4. 投标人进行远程在线演示可通过共享桌面来实现，具体操作指南在《政府采购项目电子交易管理操作指南-供应商》2.4.4项。 5. “政采云视频讲标系统”目前不支持手机端，投标人需配置带高清摄像头的电脑、音箱、麦克风等设备，以及足够的网络带宽保障远程询标顺利进行（建议用谷歌浏览器，网络带宽不少于50兆，有线网线、中档及以上摄像头，提前调试音响麦克风）。 |
| 9 | 投标与开标  注意事项 | 1.本项目实行电子投标，投标人自行承担投标一切费用。  2.标前准备：投标人在开标前确保成为浙江省政府采购网正式注册用户，并完成CA数字证书办理（办理流程详见本招标公告附件：政采云CA签章申领操作流程）。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投标人自行承担。 |
| 10 | 信用信息  查询渠道 | 信用中国（网址：<http://www.creditchina.gov.cn>）  中国政府采购网（网址：http://www.ccgp.gov.cn） |
| 11 | 中小企业预留  份额情况 | 根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）文件的规定，本项目(□ 是/☑ 否)属于专门面向中小企业采购的项目。 |
| 12 | 中小企业  优惠措施 | 1.项目属性： 服务类 。  2.中小企业划分标准所属行业（具体根据《中小企业划型标准规定》执行）：  采购标的： 台州市政务外网安全运营平台 ，所属行业：　软件和信息技术服务业 。  3.属于享受政府采购支持政策的残疾人福利性单位，应符合财库〔2017〕141号文件规定，视同小型、微型企业，在投标文件中提供《残疾人福利性单位声明函》（见附件），享受评审中价格扣除政策。  4.根据财库〔2014〕68号的相关规定，在政府采购活动中，监狱企业的视同小型、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证明文件（格式自拟）。  （注：未提供以上材料的，均不给予价格扣除） |
| 13 | 质疑渠道 | 政采云平台网上质疑系统。 |
| 14 | 实质性条款 | 带“▲”的条款是实质性条款，投标文件须作出实质性响应，否则作无效投标处理。 |
| 15 | 主要性能参数 | 带“★”的条款是主要性能参数。 |
| 16 | 书面形式 | 包括电子邮件、信函、传真。 |
| 17 | 解释权 | 本招标文件解释权属于采购人和采购组织机构。 |

**二、说 明**

**总则**

本招标文件依据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》（国务院令第658号）和《政府采购货物和服务招标投标管理办法》（财政部令第87号）及国家和浙江省有关法律、法规、规章编制。

投标人应仔细阅读本项目招标公告及招标文件的所有内容（包括变更、补充、澄清以及修改等，且均为招标文件的组成部分），按照招标文件要求以及格式编制投标文件，并保证其真实性，否则由此引起的一切后果应由投标人承担。

**适用范围**

本招标文件适用于本次项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

本招标文件仅适用于本次招标公告中所涉及的项目和内容。

**（三）当事人**

### 1.采购组织机构：是指采购人委托组织招标的集中采购机构或采购代理机构；

2.采购人：是指依法进行政府采购的国家机关、事业单位和团体组织；

3.投标人：是指响应招标、参加投标竞争的法人、其他组织或者自然人；

4.中标人：是指经评标委员会评审确定的对招标文件作出实质性响应，经采购人按照规定在评标委员会推荐的中标候选人中确定的或受采购人委托直接确认的，与采购人签订合同资格的投标人；

5.联合体：两个或两个以上法人或者其他组织可以组成一个联合体，以一个投标人的身份共同投标。

**（四）以联合体形式投标的，应符合以下规定**

1.联合体各方应签订联合体协议书，明确联合体牵头人和各方权利义务，并作为投标文件组成分部分；

2.联合体各方均应当具备《中华人民共和国政府采购法》第二十二条规定的条件，并在投标文件中提供联合体各方的相关证明材料；

3.联合体成员存在不良信用记录的，视同联合体存在不良信用记录；

4.联合体各方中至少应当有一方符合采购人规定的资格要求。由同一资质条件的投标人组成的联合体，应当按照资质等级较低的投标人确定联合体资质等级；

5.联合体各方不得再以自己名义单独在同一合同项中投标，也不得组成新的联合体参加同一项目投标；

6.联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任；

7.投标时，应以联合体协议中确定的主体方名义投标，对联合体各方均具有约束力。

**（五）语言文字以及度量衡单位**

1.投标文件以及投标人与采购组织机构就有关投标事宜的所有来往函电，均应以中文汉语书写，除签字、盖章、专用名称等特殊情形外。投标资料提供外文证书或者外国语视听资料的，应当附有中文译本，由翻译机构盖章或者翻译人员签名。

2.所有计量均采用中国法定的计量单位。

3.所有报价一律使用人民币，货币单位：元。

**（六）现场踏勘**

1.招标文件规定组织踏勘现场的，采购人按招标文件规定的时间、地点组织投标人踏勘项目现场。

2.投标人自行承担踏勘现场发生的责任、风险和自身费用。

3.采购人在踏勘现场中介绍的资料和数据等，不构成对招标文件的修改或不作为投标人编制投标文件的依据。

**（七）特别说明**

1.投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有且所提供的资料都是真实有效的。投标人投标所使用的采购项目实施人员必须为本法人员工。

2.本招标文件中关于电子招投标的内容、流程，如与政采云系统中最新的内容、操作不一致的，以政采云系统中的要求为准。

**三、招标文件**

（一）招标文件由招标文件目录所列内容组成。

（二）投标人在规定的时间内未对招标文件提出疑问、质疑或要求澄清的，将视其为无异议。

（三）对招标文件中描述有歧义或前后不一致的地方，评标委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

（四）采购组织机构对招标文件进行必要的澄清更正的，澄清或者修改的内容可能影响投标文件编制的，于投标截止时间的15日前在浙江省政府采购网上以更正公告的形式通知各潜在的投标人；不足15日的，采购组织机构应当顺延提交投标文件的截止时间。

**四、投标文件**

**（一）投标文件的编制**

投标人获取招标文件后，按照采购组织机构的要求提供：资格证明文件、商务与技术文件和报价文件。【特别提示：如在投标时有要求提供资料原件的，将原件扫描放入投标文件】若参与多标项投标的，则按每个标项分别独立编制投标文件。

**1.资格证明文件的组成（以联合体形式参加本项目投标的，联合体各方均应当提供如下资格证明材料。）**

（1）投标声明书；

（2）授权委托书或联合体授权委托书（法定代表人亲自办理投标事宜的，则无需提交授权委托书；以联合体形式投标时需提供联合体授权委托书）；

（3）联合体共同投标协议书（以联合体形式投标时需提供）；

（4）法人或者其他组织的营业执照等证明文件，自然人的身份证明；

（5）符合参与政府采购活动的资格条件并且没有税收缴纳、社会保障等方面的失信记录的承诺函；

（6）具备履行合同所必需的设备和专业技术能力的证明材料（根据项目性质提供）；

（7）提供采购公告中符合投标人特定条件的有效资质证书扫描件，以及需要说明的其他资料。

**2.商务与技术文件的组成**

**（1）技术方案描述部分（投标人视情制作）**

1. 投标人情况介绍（人员与技术力量、经营业绩等）；
2. 项目需求的理解与分析（投标人对项目现状及需求的理解状况，对项目现状和需求描述的全面性、准确性、针对性，项目功能设计完备、对系统各组成部分等功能进行准确的分析，对项目重点、难点的把握，解决方案及合理化建议）；
3. 总体设计（技术、服务）方案；
4. 功能设计方案；
5. 质量保证方案；
6. 项目实施方案（包括项目工期、确保项目进行的措施或方案、项目实施进度安排、项目实施人员及项目负责人的资质、类似经验及社保证明等）；
7. 项目分包方案；
8. 技术需求响应表；
9. 项目实施人员一览表；
10. 工程量/原材料、人工费清单（均不含报价）；
11. 项目负责人资格情况表；
12. 安装、调试及验收方案（包括项目验收标准和验收方法等）；
13. 实施服务与保障的能力及方案（包括服务方式、服务网点、技术培训、实施期与运维期服务的内容和措施等）；
14. 投标人需要说明的其他内容（包括可能影响投标人技术性能评分项的各类证明材料）。

**（2）商务响应及其他部分**

1. 证书一览表（与本项目相关的认证证书或文件）；
2. 近三年来类似项目的成功案例（投标人类似项目实施情况一览表、合同及其相应的发票、用户验收报告等）；
3. 商务需求响应表。

**3.报价内容的组成**

（1）开标一览表；

（2）报价明细表；

（3）中小企业、残疾人福利性单位、监狱企业等声明函；

（4）针对报价投标人认为其他需要说明的。

**（二）投标报价**

1.投标人应按照招标需求内容、责任范围以及合同条款进行报价。并按“开标一览表”和“报价明细表”规定的格式报出总价和分项价格。投标总价中不得包含招标文件要求以外的内容，否则，在评标时不予核减。

2.投标报价包括本项目采购需求和投入使用的所有费用，包括但不限于主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

3.投标报价不得为选择性报价和附有条件的报价。

**（三）投标文件的有效期**

1.投标文件有效期为投标截止日起90天。

2.在特殊情况下，采购人可与投标人协商延长投标文件的有效期。

3.中标人的投标文件自开标之日起至合同履行完毕均应保持有效。

**（四）投标文件的签署**

1.投标文件需由法定代表人或经其正式授权的代表签字或盖章（本项目如允许联合体投标且投标人是联合体的，联合体牵头单位应盖章，并签署联合体牵头单位法定代表人或经其正式授权的代表的全名）。授权代表须出具书面授权证明，其《法定代表人授权书》应附在投标文件中。

2.投标文件中所有的插字、涂改和增删，必须由法定代表人或经其正式授权的代表在旁边签字或盖章才有效。

3.投标文件中要求加盖公章处，可使用有效安全的电子签章替代。

**（五）投标文件的递交要求**

按照前附表要求提交，如采购组织机构顺延截止时间和开标时间，采购组织机构和投标人的权利和义务将受到新的截止时间和开标时间的约束。

**五、开标**

**（一）开标程序**

1.开标时间到后，主持人准时组织开标；

2.宣布采购组织机构工作人员；

3.投标人登录政采云平台，用“项目采购-开标评标”功能对投标文件进行在线解密，在线解密时间为开标时间起半个小时内；

4.采购组织机构工作人员当众宣布投标人名称、投标价格和招标文件规定的需要宣布的其他内容（以开标一览表要求为准）；

5.公布开标结果。

**（二）开标异议**

投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购组织机构相关工作人员有需要回避的情形的，应当场提出询问或者回避申请，开标会议结束后不再接受相关询问、质疑或者回避申请。

**（三）**投标人不足三家，不得开标。

**六、评标（详见第四章）**

**七、定标**

**（一）确定中标人**

评标委员会根据采购单位的《授权意见确认书》，推荐中标候选人或确定中标人。其中推荐中标候选人的，采购组织机构在评标结束后2个工作日内将评标报告送采购人，采购人自收到评标报告之日起5个工作日内在评标报告推荐的中标候选人中确定中标人。

**（二）发布中标结果公告**

采购组织机构自中标人确定之日起2个工作日内，在浙江省政府采购网和台州市公共资源交易网上公告中标结果，中标结果公告期为1个工作日。

**（三）发放中标通知书**

采购组织机构在发布中标结果公告的同时，通过政采云平台向中标人发出中标通知书。

**八、合同签订及公告**

**（一）签订合同**

1.采购人应当自中标通知书发出之日起30日内，按照招标文件和中标人投标文件内容要求，与中标人签订合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

2.采购人不得向中标人提出任何不合理的要求作为签订合同的条件。

3.中标人无故拖延、拒签合同的，将取消中标资格。

4.中标人拒绝与采购人签订合同的，采购人可以按照评标报告推荐的中标候选人名单排序，确定下一候选人为中标人，也可以重新开展政府采购活动。同时，拒绝与采购人签订合同的中标人，由同级财政部门依法作出处理。

5.询问或者质疑事项可能影响中标结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

**（二）合同公告及备案**

1.采购人应当自合同签订之日起2个工作日内，在省级以上财政部门指定的政府采购信息发布媒体及相关网站上公告。

2.采购人应当自合同签订之日起7个工作日内，将合同通过政采云平台提交至同级人民政府财政部门备案存档。

**九、询问、质疑与投诉**

**（一）询问**

投标人对政府采购活动事项（招标文件、采购过程和中标结果）有疑问的，可以向采购人或采购组织机构提出询问，采购人或采购组织机构将及时作出答复，但答复的内容不涉及商业秘密。询问可以口头方式提出，也可以书面方式提出。联系方式见第一章“投标邀请”中“采购人、采购组织机构的名称、地址和联系方式”。

**（二）质疑**

1.报名本项目的投标人认为招标文件、采购过程和中标结果使自己的权益受到损害的，通过政采云平台的质疑系统一次性向采购人或采购组织机构提出质疑：

（1）投标人认为招标文件的内容损害其权益的，应当自获取之日起（获取截止日之后收到招标文件的，以获取截止日为准）7个工作日内提出质疑；

（2）投标人对采购过程提出质疑的，应当在各采购程序环节结束之日起7个工作日内提出质疑；

（3）投标人对中标结果提出质疑的，应当在中标结果公告期限届满之日起7个工作日内提出质疑。

2.采购人或采购组织机构在收到投标人的书面质疑后7个工作日内作出答复，并以书面形式或政采云平台回复质疑投标人和其他有关投标人，但答复内容不涉及商业秘密。

3.投标人质疑应当有明确的请求和必要的证明材料，包括但不限于权益受损害的情况说明及受损害的原因、证据内容等，并对质疑内容的真实性承担责任（依据《中华人民共和国政府采购法实施条例》第五十七条，捏造事实、提供虚假材料或者以非法手段取得证明材料不能作为质疑、投诉的证明材料）。

**（三）投诉**

投标人对采购人或采购组织机构的质疑答复不满意或在规定时间内未得到答复的，可以在答复期满后15个工作日内，向同级政府采购监督管理机构投诉。

1. **招标需求**

**一、招标项目一览表**

本次招标共 1 个标项，具体内容如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **标项号** | **项目名称** | **简要技术要求** | **数量** | **单位** | **总预算（万元）** | **最高限价（万元）** |
| 1 | 台州市政务外网安全运营平台 | 详见技术需求 | 1 | 项 | 600 | 576.5 |

**二、技术需求**

## （一）项目概况

### 1.建设背景

数字化改革是“最多跑一次”改革和政府数字化转型的迭代深化，是“数字浙江”建设的新阶段，是浙江立足新发展阶段、贯彻新发展理念、构建新发展格局的重大战略举措。数字化改革是围绕建设“数字浙江”目标，统筹运用数字化技术、数字化思维、数字化认知，把数字化、一体化、现代化贯穿到党的领导和经济、政治、文化、社会、生态文明建设全过程各方面，对省域治理的体制机制、组织架构、方式流程、手段工具进行全方位、系统性重塑的过程。数字化改革需要加快构建“1+5+2”工作体系，其中，“1”是一体化智能化公共数据平台；“5”是5个综合应用——党政机关整体智治综合应用、数字政府综合应用、数字经济综合应用、数字社会综合应用和数字法治综合应用；“2”是构建理论体系和制度规范体系。

台州市一体化智能化公共数据平台建设方案提出：提升严密可靠的网络安全防护体系。健全网络安全制度体系。健全安全等级保护、涉密信息系统分级保护、风险评估制度、预警和应急处置制度。健全政务外网安全保障体系。完善全市电子政务外网安全监管体系，完善一体化电子政务外网安全支撑体系，建设内外网公共安全组件，加强应用和移动端安全管理。

根据浙江省数字化改革总体方案、台州市数字化改革总体方案提出的支撑台州市数字化改革项目的要求，启动本项目建设。

### 2.建设目标

通过台州市政务外网安全运营平台建设，汇集台州市本级及县市区政务云、政务外网、终端及边界安全数据，建立从安全数据采集、治理、存储及安全综合分析服务全过程安全管理体系，构建网络安全协同处置多跨应用，实现安全问题综合分析、协同处置、闭环管理，提升台州市网络安全整体智治水平。

其中，平台提供全过程的数据安全采集、治理、计算、存储和分析能力，支持对接不同的安全数据源。支持在线存储、离线存储。根据数据类型和数据内容，对数据进行分类存储，构建安全数据主题库，对部分原始数据进行临时存储，供分析调用；各安全厂商可以根据安全数据仓提供的数据，结合数据分析工具，对安全数据进行分析，根据数据分析结果，为各部门提供安全服务。服务成果分发给台州市网信办网络安全协调指挥平台，通过该平台，将安全事件转发给市级部门和各县市区进行处置，处置完成后通过该平台将处置成果反馈到本平台。另外部分安全事件、安全问题信息将根据要求同步给浙江省电子政务外网安全监管平台和县（市、区）电子政务外网安全监测平台。

### 3.建设内容

本期项目将基于台州市电子政务云、台州市现有网络安全产品及服务进行建设。

具体建设内容包括安全数据采集系统、安全数据标准制定及对接服务、安全数据治理系统建设及服务、数据存储系统、数据仓、数据计算系统和网络安全综合分析服务，各模块建设内容如下：

安全数据采集系统：建设安全数据采集系统，实现数据接入、数据归集监控、数据源管理、策略配置管理、任务生成管理和执行管理等功能。

安全数据标准制定及对接服务：包括安全数据技术规范制定和系统对接服务，其中系统对接服务包括与大数据局现有的网络安全产品进行对接、与浙江省政务外网安全监管平台对接、与台州市网络安全协调指挥平台对接。

安全数据治理系统建设及服务：包括安全数据治理系统建设和安全数据治理服务。安全数据治理系统提供数据前置过滤、标准化过滤、增强过滤、数据回写、高级数据管理等功能。安全数据治理服务包括数据调研分析、数据治理规范的建立、数据人工处理、数据治理质量评估、安全数据共享、日常协调等工作。

数据存储系统：数据通过解析、映射以及数据处理增强模型后形成标准化数据，通过高可用高性能的分布式存储能力实现对数据采集系统已归集的安全数据进行存储管理。

安全数据仓：安全数据仓的数据共分为七大类，分别是边界安全数据、终端安全数据、日志管理数据、安全威胁数据、安全处置数据、安全资产数据、云端数据等。

数据计算系统：提供实时流计算、离线计算和分布式搜索等功能。

网络安全综合分析服务：提供安全事件分析、威胁感知、情报分析、热点情报预警、安全指数发布、安全报告及制度编制、安全策略制定、信息安全通报等服务。

## （二）采购清单

|  |  |  |
| --- | --- | --- |
| 序号 | 招标清单 | 具体内容 |
| 一 | 安全数据运营系统 | 安全指数管理、数据仓展示、业务流程管理、联动处置、可视化分析、资产管理 |
| 二 | 安全数据共享系统 | 安全数据采集模块、安全数据治理模块、数据存储模块、安全数字仓、数据计算模块 |
| 三 | 网络安全综合分析服务 | 威胁分析服务、态势感知服务 |
| 四 | 网络安全数据规范治理 | 安全数据技术规范制订、安全数据标准制订、信息资源编目服务、数据治理服务 |
| 五 | 对接服务 | 安全系统对接、安全数据采集 |

## （三）平台资源情况

### 1.资源情况

本期项目将基于台州市电子政务云、台州市政务外网现有网络安全产品及服务进行建设。

1.1计算存储资源

本项目所需的计算及存储资源，主要基于台州市电子政务云现有资源进行建设，包括ODPS、Flink、QuickBI、RDS、ECS、OSS等服务。政务云资源相关费用由采购人统一承担。

1.2安全资源

本项目涉及的安全数据基于现有的安全系统，包括政务终端安全管理系统、日志审计系统、县市区网络安全监测系统、漏洞扫描、政务云安全、边界安全等系统采集的数据。

### 2.性能需求

2.1数据处理能力

支持通过集群的方式弹性扩展平台规模，支持50台集群规模以上，满足PB级别的数据处理。

针对政务外网安全运营平台的数据仓，要求数据表管理数量不少于5万张，数据量处理能力不少于1PB，数据库容量可水平扩展。数据库系统和大数据计算服务系统的有效工作时间要求每年≥99.9%。

支持与离线计算有效对接，无需数据迁移即可支持TB级数据高并发实时写入实时查询，在线计算分析与离线大数据计算有效打通，为离线大数据计算提供交互式查询服务，让用户使用熟悉的工具以标准SQL查询分析离线大数据计算项目中的数据，快速获取查询结果。

2.2组件性能需求

系统要支持业务及后期扩展需求，结合业务场景，现有系统各类组件性能需满足如下指标：

流式计算：

根据上下游和处理逻辑的不同

（1）1CU 处理能力大约在2000条/秒 - 50000条/秒；

（2）简单 ETL 性能大约在20000条/秒/核；

（3）复杂计算性能大约在2000条/秒/核 - 8000条/秒/核；

分布式计算：

在4核16G资源配置下，采用TPC-DS基准测试规则（SQL99），数据集为5G配置的情况下：

（1）query33.sql三次测试的平均值不高于35秒；

（2）query66.sql三次测试的平均值不高于35秒；

（3）query99.sql三次测试的平均值不高于20秒；

搜索引擎：

（1）ElasticSearch组件在Operation默认维度下的平均吞吐量不低于50ops/s；

（2）ElasticSearch组件在Operation默认维度下的延迟不大于30ms；

（3）ElasticSearch组件在Operation默认维度下的服务时间不大于30ms；

2.3网络环境的性能

政务云各主机之间的传输满足万兆，政务外网和互联网的跨网传输满足千兆。要求数据传输网络畅通、快捷、安全、可扩展。

2.4兼容性

依据相关信创要求，本系统兼容国产操作系统和浏览器。

**（四）功能需求**

## 1.系统整体的描述

通过台州市政务外网安全数据运营平台（重点）、安全数据共享平台（重点）、网络安全综合分析平台（基础）建设，汇集台州市本级及县市区政务云、政务外网、终端及边界安全数据，建立从安全数据采集、治理、存储及安全综合分析服务全过程安全监测、防护和服务体系，构建网络安全协同处置多跨应用，实现安全问题协同处置、闭环管理，提升台州市网络安全整体智治水平。

## 2.安全数据运营系统

### 2.1安全指数管理

基于安全运营管理视角，结合相关安全管理要求设计对应的安全指标，形成相应的考核标准，从而根据运营工作阶段性要求，综合计算单位的安全状况，以实现对应的将安全运营工作量化评分。并通过系统展示整体安全评分、风险资产数及风险资产的资产类别、安全事件数及各等级安全事件数、流程流转数及各状态流程数、对应安全评分排名；并获得资产变化趋势与安全事件变化趋势的数据统计。安全指数的发布频率不低于每日一次；

### 2.2数据仓展示

数据仓展示主要针对安全数据共享系统中采集、治理与存储的数据进行展示，提供对应的检索工具快速展示在运营过程中所需的过程与结果数据；方便运营过程中对数据的分析和使用；提升数据使用的安全性，基于数据不同的类型与业务管理过程中不同角色进行区分，避免数据使用的权限过大，同时对数据使用过程中进行审计。

### 2.3业务流程管理

业务流程管理模块主要工作内容至少需要包含：情报预警、安全问题通报、安全问题预警、安全公告、安全问题上报。依靠安全业务流程机制，实现不同角色间的协同和流程化运维。依靠安全运维主管进行任务发起及归档，推动具体责任部门或下属单位的运维人员完成相关事件处置工作。

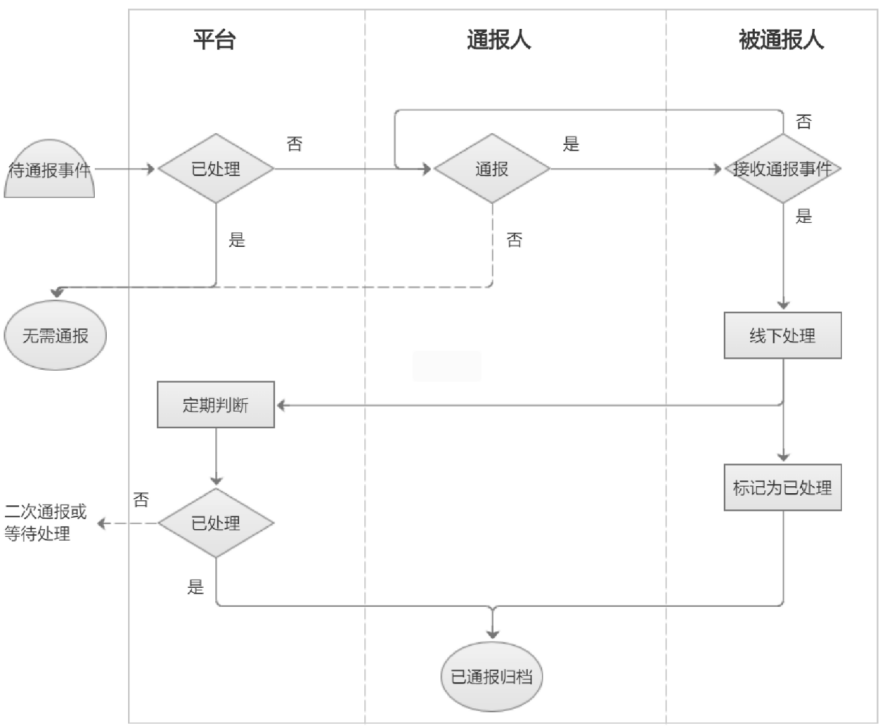
对安全问题进行流程化实现，可便于风险处置的协作和管理，避免无责任人管理导致的风险淹没。安全问题的来源主要基于安全设备日志、威胁情报匹配、多源异构的数据关联告警，通过对相关安全问题进行待流转设置，可针对性的进行通报、预警、上报，快速通知相关责任人进行安全事件的处置动作与归档。

对安全情报信息进行流程化实现，可快速拉齐信息同步，避免信息不同步导致的安全危害发生。安全公告、安全情报等主要基于多方厂商的线上信息，通过对相关信息发起通告流程，提前告知相关责任人威胁信息，快速做好预警防护工作。

* 流程模版编排

通过拖拉拽的方式，进行自定义流程的编排。为满足流程的全面性，流程动作应包含录入节点、审批节点，录入节点可满足流程中人工上传举证信息动作、审批节点可满足人工的选择与判断动作；

将定义好的流程进行保存，为安全业务的执行提供流程；安全业务的运营流程应从日常运维、通报预警、应急响应的维度进行多种流程编排。



流程设计应以满足可闭环的理念进行规划安排，流程应满足通报人发起、通报人归档的理念，且通报人在流程流转过程中可看到流程进展。

通过浙政钉通报支持查看所辖区域内安全事件发生情况，可查看事件详细信息。支持事件列表的查看，字段包括事件名称、事件类型、所属区域、事件发现时间、事件通报状态等信息。

### 2.4联动处置

安全编排自动化响应聚焦安全运维领域，重点解决安全响应问题，使得组织能够对事件分析与响应流程进行形式化的描述。SOAR具备自动执行能力，可以依据场景或案例制定执行计划或执行脚本。通过智能编排技术，SOAR可以让用户能够遵循特定的剧本，开展安全运营工作，并且支持剧本的自定义编排。通过灵活的剧本编排，实现基于不同业务场景的安全策略自定义，以适配不同应用场景和安全需求的安全能力灵活部署，帮助构建安全事件的标准处置流程。基于“人机协同共治”的理念，在标准工作流程的指引下，利用人机结合的方式帮助安全运维人员定义、排序和驱动标准化的事件响应活动。用户在剧本中定义相关流程，不仅可以实现处置自动化，同时可以借助安全专家的经验保障处置效果。

此外，安全编排自动化响应支持应用管理能力，能够集成各类协助处置的IT资源和设备（如防火墙、EDR、威胁情报系统、IT基础设施等），实现安全策略下发及设备联动处置，这可以避免在发生安全事件时，用户通过手工的方式操作各类资源设备进行事件处置，从而提升安全响应效率。

SOAR业务流框架如上图所示，通过数据关联分析或机器学习分析产生安全事件之后，SOAR事件接入模块从事件列表中查询新的事件，并根据剧本配置的条件进行匹配，选择相应的剧本进入自动化流程。剧本根据编排的画布流程对相应的事件进行响应处置。在流程运行中涉及到调用第三方资源平台来辅助安全处理时，通过应用管理中心调用相应的资源接口进行信息获取或者设备联动。

通过所画即所得的界面可配自定义剧本编排已经实现，让单位安全运营流程更加可视，能够更好的对不同事件进行及时有效地处置。

### 2.5可视化分析

可连接多种数据源，一键接入数据库表或导入Excel；可视化编辑数据，过滤合并计算，完全不需要SQL；内置10+可视化图表，可视化呈现数据。

以运营平台为支撑，建立政务网域的态势感知与通报预警系统，以网络安全、云安全、威胁风险管理为驱动，基于多维态势可视化技术，对网络空间安全相关信息进行汇聚融合，形成多维视图，从不同视角出发感知安全态势，为“一张网通览、一块屏通析、一朵云通防”建设目标提供可视化展示能力。

2.6资产管理

通过资产管理，解决资产分散、不集中等一系列管理问题。全面识别IT资产、梳理访问关系和建立责任人员组织架构的功能，实现资产的统一管理。可依照资产生命周期，对资产的新建、审核入库、风险识别、自动退库进行有序高效的管理，同时会优先展示活跃资产，让管理员更聚焦化地对活跃资产进行运维。通过资产关联到人，资产脆弱性管理与评估，方便管理者能够把控所有资产情况。通过资产视角与风险视角，快速了解当前风险情况，了解当前资产脆弱性情况，便于摸清家底。按信息系统重要、敏感程度纵向分级；按信息系统脆弱程度、可用程度纵向分级。自动发现未管控资产，并通知管理员及时安装防护软件，能够有效降低资产遭受攻击的风险，规避监控盲区。通过安全数据共享系统定期获取掉线资产列表，结合运维审计能力、自动化运维工具批量排查资产掉线原因，将结果反馈给对应问题处理团队。

## 3.安全数据共享系统

### 3.1安全数据采集模块

安全数据采集的对象主要为镜像的网络流量和终端的数据，在云、网、边、端上获取流量和日志数据。

1）云主要是指政务云，对接政务云安全监管现有的流量数据、日志数据；

2）网主要是指政务外网，采集政务外网的相关流量数据、日志数据和网络设备数据。

3）边主要是政务外网边界的安全，采集边界安全设备的安全数据。

4）端是指市内电子政务外网上的终端，分别与市县二级的终端管理和安全防护系统系统对接获取终端的安全数据。

除上述系统数据归集外，要求通过数据采集系统与其他网络安全监管平台对接，获取全大市外网网络攻击、有害事件数据和终端数据。

数据抽取范围包括原始流量监测数据、安全监测数据、主动监测数据、日志监测数据、端点监测数据、静态录入数据、动态推送数据、情报获取数据等。

数据采集的数据包括各类结果数据和原始数据。结果数据为各类安全系统的分析结果数据，原始数据为各类安全系统和安全设备的原始日志数据、网络流量数据。

系统要支持多元异构日志数据采集：包括但不限于主流安全设备、网络设备、主机、数据库、中间件、应用系统和虚拟化系统等数据的采集。可以通过自定义配置将用户不关心的日志过滤掉；可以对收集到的重复的日志进行自动的聚合归并，减少日志量；同时将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过日志转发功能将日志转发到其他日志存储设备；能够做到多种采集协议，以实现对各类数据的采集，包括不限于安全对象属性、运行状态、安全事件、评估与检测等数据。

系统要支持全流量数据采集：可以通过自定义配置将用户不关心的日志过滤掉；可以对收集到的重复的日志进行自动的聚合归并，减少日志量；同时将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过日志转发功能将日志转发到其他日志存储设备；能够做到多种采集协议，以实现对各类数据的采集，包括不限于安全对象属性、运行状态、安全事件、评估与检测等数据。

系统要支持通过第三方平台接口对接，采集第三方平台数据：从其他平台以接口同步的方式获取数据，如支持对互联网恶意程序、病毒、蠕虫、木马、僵尸网络等恶意程序事件数据的采集和导入第三方漏洞扫描结果。

数据采集必须能够满足系统数据库管理的需要，又要能保证不影响各业务系统的性能，所以进行数据抽取时应制定相应的策略，如使用缓存技术，降低数据采集时业务系统的影响。

支持分布式多节点部署。支持多采集节点存活、健康状态监控，发现节点异常后，及时告警；每个数据采集引擎支持配置不同的采集策略，保证每个数据采集引擎有针对性的采集数据。

支持对采集节点数据量级健康度监控，保证采集性能与数据量匹配，防止数据丢失；

支持数据汇聚。综合考虑网络传输性能的基础上，需满足将多个采集源到的数据传输汇聚。

数据接入实现内外部数据导入至安全数据仓的功能。数据接入支持结构化数据、半结构化数据、非结构化数据等多种数据类型。数据接入包括两大主要部分，流式数据接入、批量数据接入。

数据抽取能实现数据抽取策略的配置，包括数据抽取清单配置、数据回执策略配置等功能等。支持对设备的采集策略的管理，包括采集频率、采集协议、采集目标、过滤策略等。

可实现对数据采集的任务调度，通过数据采集作业策略的设置，提供定时执行的服务。根据数据采集系统的需求，在数据采集系统中任务生成方式有两种：自动任务和手动任务。自动任务调度周期包括：按秒、按分钟，按天，按周，按月，按年和实时。

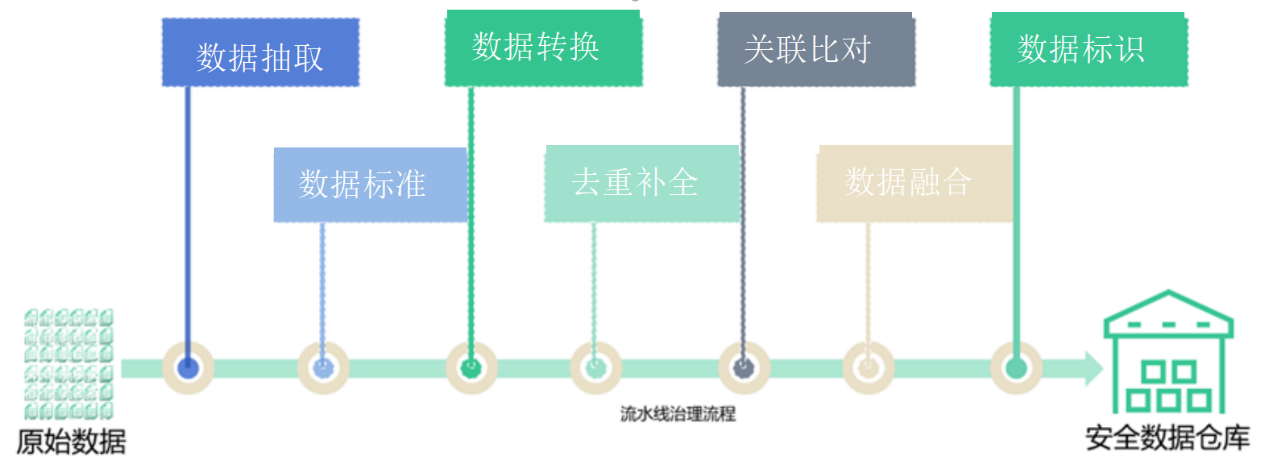
### 3.2安全数据治理模块

安全数据从采集端采集后，通过高级数据管理、数据标准、数据可视化清洗对数据进行标准化处理，为后续的数据存储和分析提供支撑。

数据治理系统主要包含数据治理功能和数据管理功能，通过该系统可以对归集至安全数据仓原始层的数据进行管理和加工处理，实现数据加工过程和结果可管理可看。具体功能包含数据标准管理、元数据管理、数据地图、数据血缘管理、可视化数据清洗、租户管理、运维管控等

数据解析与映射的目标是对原始安全数据提供标准进行转换，并最终生成符合系统要求的标准化数据。数据治理流程将原始层数据进行标准化治理后存入成果层。

数据经过抽取后，还需要将不同来源，不同结构的数据按照业务需要解析为目标数据结构，并按照需要进行计算汇总。安全数据的治理加工过程将在以下几个环节中具体实现：



数据抽取和元数据管理支持将多源异构业务系统和计算引擎的元数据通过统一的采集机制采集到 数据治理系统中集中管理，对元数据进行加工整合后，为数据接入、数据质量提升、数据加工处理、日常运行维护和业务应用提供基础能力支持。

数据标准支持建立数据治理系统中的统一的数据标准体系，使用户能够充分利用国家、行业、企业等相关的标准，对各类安全数据进行统一的标准化改造，在平台中形成单一的对数据的理解视图，并能够借助统一的标准化数据定义，帮助用户实现数据质量的监控和提升。

数据标准管理支持标准数据元管理、标准字典表管理。

在数据治理过程中，数据会经过大量功能模块的处理和传递，业务用户经常需要分析数据的转换关系。通过数据血缘模块以历史事件的方式记录每项数据的来源、处理过程等，可以快速进行影响分析，以数据流向为主线进行血缘追溯，从而提升报表信息的可信度，为企业数据的合规性提供验证手段。

数据治理过程中需要数据地图解决数据工程师“ 有哪些数据可用 ” 、 “ 到哪里可以找到数据 ” 的难题，提升数据资源的利用率。数据地图支持查看与操作数据表结构定义、数据预览、标准清洗、数据血缘等信息。

### 3.3数据存储模块

采用分布式架构，存储能力可横向扩展。 数据存储采用分布式文件系统， 支持多种存储格式，具有高可靠性和高性能，支持列式存储，具有高压缩比。支持与常见数据源如传统数据库、Hadoop、HDFS和文件进行数据导入导出，以及流式数据导入。具有高吞吐高性能的数据处理能力。

具备分布式文件系统：为安全数据提供持久化分布式存储。

具备分布式列存数据库：为安全数据提供结构化数据的高速写入和读取。

具备分布式存储，实现数据冗余备份；

数据存储系统所有数据三副本存储 ，保障数据高可靠性；具备服务全HA ，无单点故障， 保障服务高可用

数据通过解析、映射以及数据处理后形成标准化数据，通过数据存储模块存入安全数据仓。

数据存储负责将标准化的最终数据写入到存储中或者转发到其他系统中。支持以不同的协议方式输出数据，兼容大多数协议(http、redis、kafka、syslogAPI)，支持将数据写入到不同的数据存储系统中，支持根据不同入库配置规则将数据写入到指定存储空间，满足不同的输出、存储速率、支持不同规模的数据量。

存储的数据分两大类：数据存储和文件存储。其中数据存储用来存储各种数据，包括日志类、告警类、元数据类数据等；文件存储用来存放文件。数据存储支持elasticsearch、HDFS、HBASE等存储；es适用于检索、聚合，可用来保存近期的热点数据；HDFS适用于离线数据存储，关联、统计分析，可用来保存全量数据，用于大数据量的分析。

按照数据的访问频度需求，数据分别存储在Kafka消息队列、HDFS、Hbase离线计算存储、ElasticSearch中。

安全数据需要复用现有的台州市政务云各类存储资源，相关费用由采购人承担。

### 3.4安全数据仓

安全运行数据仓是综合各种数据资源进行提炼加工，形成公共数据集合，对各项业务工作都具有支撑作用，可以脱离任何业务而独立存在，也与每一项业务相关。安全运行数据仓是在原始库上对所有汇聚数据，按照一定的规则进行清洗、标准化，并按业务使用规则或属性规则等进行整合加工与汇总，为政务外网安全运营平台提供基础数据资源支撑的数据集合。

安全运行数据仓的数据共分为七大类，分别是边界安全数据、终端安全数据、日志管理数据、安全威胁数据、安全处置数据、安全资产数据、云端数据等。

从各安全数据源采集的数据存入数据库，原始数据存入临时数据库，分析结果数据保存在成果库中。

数据源采集的数据同步到原始库中。各类业务系统、安全相关设备、网络设备系统和平台，都会产生日志数据，这些日志数据描述了当前网络空间中已经发生或正在发生的一系列行为，而这些行为包含着与安全威胁相关的信息。

原始库汇集的数据来自于多个业务系统、多种数据形态。安全数据接入系统能够针对异构的数据源，利用其灵活便捷的特性快速的集成各类数据。

通过数据接入系统从本地文件、syslog、外发数据等多样数据源采集数据到原始库中。

原始库的数据经解析、数据提取、数据质量处理、数据标准转换等处理过程，将数据加工成符合标准规范的数据。

成果库的数据经过数据融合、数据标识、数据管理、对比、建模加工、数据分发的处理过程，将数据映射到云安全、终端安全、网络安全等信息分类中，并详细对应到各信息分类中的主题库中。

数据共享交换服务为应用开发商提供标准的数据接口，应用在经过授权后可以按需取用安全数据仓库中的原始库、主题库中的数据资源，实现与其他业务的数据分析成果和知识共享。

### 3.5数据计算模块

提供实时流计算、离线计算和分布式搜索等功能。考虑到安全数据计算和城市大脑提供的相关数据计算组件存在差异，经过对市场主流安全厂商的调研，考虑到系统的成熟和可靠性，拟采用安全专用数据计算组件提供相关计算服务。

* **流数据计算系统**

流计算作为一类针对流数据的流计算模型，可有效地缩短全链路数据流时延、实时化计算逻辑、平摊计算成本，最终有效满足实时处理大数据的业务需求。

流计算需要包括以下功能：

1.实时数据接入

支持秒级或亚秒级将业务生产的数据即时归集至实时数仓中，支持多源异构的流式数据接入。

2.实时数据ETL

支持对多种数据库类型数据进行SQL灵活加工，对流式安全数据进行实时清洗处理、融合加工，作为离线数仓有效的补充和优化。

3、实时报表

实时化采集、加工流式数据源，实时监控和展现业务、客户各类指标，让数据化运营实时化。

4、监控预警

对系统和用户行为进行实时检测和分析，实时监测和发现异常情况。

5、在线系统

流计算各类数据指标，并利用实时结果及时调整在线系统相关策略。

* **离线计算系统**

提供针对TB/PB级别安全数据、实时性要求不高的批量处理能力，主要应用于日志分析、安全数据仓库、安全数据挖掘等领域。主要能力包括：

* 能基于SQL构建大规模数据仓库；
* 具备调度管理功能，包括一次性调度与周期性调度，其中周期性调度应支持按分钟、小时、日、周、月、年调度，工作流可跨周期依赖；
* 具备启停功能，支持工作流重跑；支持补数据，可通过设置工作流运行的起止时间，来达到导入历史数据的目的；
* 能搭建数据仓库。

通过分布式计算系统，实现数据的分区、数据表统计、表的生命周期等功能。

具有数据进出离线大数据计算服务的标准接口，用户可以通过上传数据到平台中或从平台下载数据，通过并发的方式来保证高吞吐量的服务，IO的能力可以通过添加节点的方式水平扩展。可以基于SDK开发和任意数据源对接的工具，对于常见的数据源（比如Oracle/MySQL），需要有相关工具可以使用。

安全数据离线计算能力需要复用现有的台州市政务云大数据计算能力，相关费用由采购人承担。

* **分布式搜索系统**

提供实时搜索和分析能力，支持实时更新索引数据及快速检索。分布式搜索引擎要求具备分布式、高扩展、高实时的搜索与数据分析能力，支持TB级别数据量实时分析和检索。具有大量数据搜索、分析和处理的能力，满足全文检索、结构化搜索、分析、聚合、高亮等需求。

（1）数据查询

提供开放的 API 接口，支持通过API 编程接口实现大数据搜索服务的索引建立、数据检索等；

（2）索引管理

基于索引服务，展示各索引的健康状态、主分片数、副分片数、中文文档总数、主分片大小以及主分片和副分片大小相关信息。

（3）监控平台

部署索引监控系统，可以通过浏览器页面监控ES运行情况，包括CPU、内存、硬盘等系统资源占用情况，还有每个服务器节点的系统负载情况。

分布式搜索引擎将全文检索、数据分析以及分布式技术结合起来，提供全文检索，同义词处理，相关度排名，复杂数据分析等功能，能够达到海量安全数据的近实时搜索，稳定，可靠，快速响应的要求。

通过搭建ElasticSearch集群，建立大数据搜索引擎，将各种类型、来源的数据全部存入大数据搜索引擎，统一管理，实现资源共享，提供搜索服务。

## 4.网络安全数据综合分析服务

### 4.1威胁分析服务

威胁分析服务，通过原生的流量采集与端点采集工具，将关键数据聚合分析，准确生成安全事件并自动回溯完整攻击链，在检测的同时收集研判数据，实现快速研判，精准还原安全事件故事线，快速溯源，提高安全事件流转处置效率。

威胁分析模块整体建设内容分为四个层面，分别为数据接入层、数据存储层、安全能力层、安全业务管理层，通过四个层面的能力构建，形成统一、高效的网络安全协同联动、预警通报、情报共享、研判处置和应急响应机制。

4.1.1数据接入层：数据采集的类型分为三种，分别为网络侧遥测数据，终端侧遥测数据以及第三方数据，采集的数据以JSON或文件的格式上报；由于上传的数据形式各异，为了实现数据解析、ETL的标准化过程，平台需提供功能强大的解析算子、逻辑处理算子和标签算子。其中，解析算子需支持多种格式的数据解析，包括CSV、KV、JSON、grok、正则、XML等格式，格式覆盖大多数数据分析的使用场景；数据过滤支持多字段、多条件进行组合，形成复杂的过滤条件，满足分析场景中灵活的需求；标签算子，可结合地理位置、资产信息、黑白名单和威胁情报等信息，为不同应用场景提供不同的选择，给原始数据添加对应的标签，富化形成结构化数据。

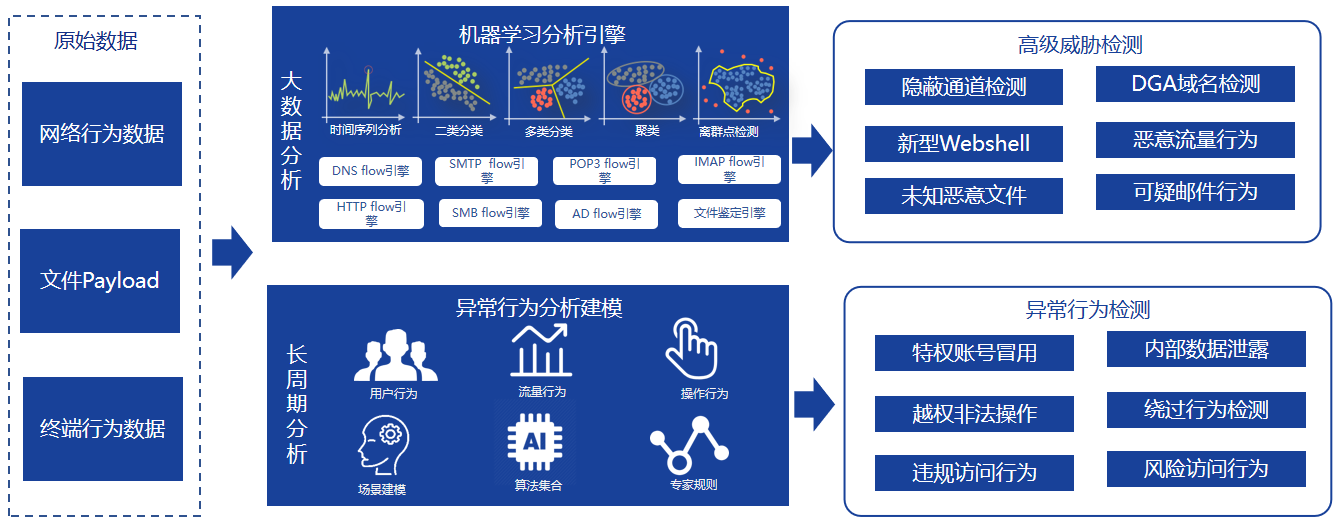
4.1.2数据存储层：采用分布式存储架构，构建全局、统一的数据湖数据信息平台，为威胁分析模块平台的安全能力提供强有力的数据基础，并提供多种数据模型，构建应用、查询数据更加灵活。

4.1.3安全能力层：整体建设内容分为二部分，分别为威胁检测能力、关联分析能力；

* 威胁检测能力

终端侧高级威胁检测能力通过在端侧采集全面的数据，包括终端、用户、文件、进程、行为等数据。数据在本地做分层，聚合有效数据上传至平台。结合用户真实环境做上下文强关联分析，提升攻击研判精准度。行为检测基于多事件复杂关联规则匹配算法，依靠泛化行为规则提高已知和未知高级威胁攻击检测能力，补充复杂行为关联检测领域空白，构建行为检测防御层级，增强多层次纵深防御检测能力，有效抵御已知和未知高级威胁攻击。

网络侧基于流量采集和日志采集，通过防火墙\入侵防御\漏洞检测\威胁情报等规则进行初步分析做数据标记和特征检测，之后再结合AI中基础的威胁检测模型来进行匹配，快速定位出场景威胁如流行病毒、黑客工具、爆破、扫描、等，针对一些更复杂的不规则的一些组合威胁攻击手段如攻击成功识别、自定义工具、0day漏洞利用、代理转发工具、隐秘隧道等，基于整个会话流量进行检测，包括对流量的请求回显、特征异常关联、异常行为利用、多阶段攻击利用等行为进行完整回溯关联，最终定位出来异常风险。最后是基于优化算法模型，对一些典型的加密流量、0day漏洞利用特征进行优化检测，实现高检出低误报。



* 关联分析能力

将终端侧和网络侧收集的数据，与云端威胁情报、资产、时间等因子做复杂关联，最终生成平台侧的关联事件。

对与组件强加强的告警信息，平台提供可视化和高可见性，结合精准详尽的处置响应建议，帮助安全运营人员提高效率。

对于组件弱加强的告警信息，平台通过多因子关联提升检测精度，有效降低告警误报量，针对原本单一网络侧或终端侧无法精准检测的攻击，如Webshell上传成功、RDP爆破成功等，网络和终端数据相互印证，互为补充，提升检测精度。

对于组件弱加弱的告警信息，平台对于二者进行整合，提升威胁检测的覆盖广度。

4.1.4安全业务管理层：

* 脆弱性管理

在资产梳理清晰后，通过平台对资产进行脆弱性评估和管理，包含主动扫描、被动流量识别、以及主机Agent等发现的资产脆弱性信息进行有效的整合，实现对资产脆弱性进行统一的生命周期管理。同时可结合漏洞全生命周期机制，对漏洞全生命周期进行管理，包括：发现漏洞、审核漏洞、漏洞处置、漏洞复测、处置完成，实现漏洞全生命周期状态闭环跟踪，确保重要的漏洞及时处置。支持紧急漏洞评估，可以快速按照使用者视角了解紧急漏洞的分布情况，快速了解指定的漏洞当前的影响范围。通过自定义的快速扫描可快速排查资产，系统，应用漏洞，弱口令等。关键字涵盖主机名、MAC地址、IP、责任人等基础信息的同时，还包含操作系统、服务应用、端口等信息。筛选支持根据资产类型、标签、重要级别、状态等关键字段进行搜索。同时支持输入关键字进行搜索。

* 安全事件管理

通过威胁分析服务对安全事件进行集中管理分析，将所有孤立的网络安全事件集中化，进行统一管理分析。对安全事件进行统一管理和基于设置资产、状态、类型、等级和时间等的条件对安全事件进行查询。可以按照资产类型、事件状态、事件等级、事件类型等依据需求设置不同的条件进行筛选，并且数据统计区可以清晰的显示出对应事件的统计信息。可通过平台针对各类安全事件分析提供的工具和流程，实现了不同事件不同分析处置过程规范性的跟踪管理，形成闭环。

### 4.2态势感知服务

采用分层的大数据处理结构设计，从数据的采集，数据预处理、大数据分析、数据存储、数据服务等五个层面，利用大数据并行计算框架支撑关联分析、流量检测、机器学习等计算检测模块，从而实现对安全数据共享平台数据分析协同的全方位检测服务；

* 日志采集与关联分析服务

对主流的网络设备、安全设备、操作系统、中间件、应用系统等设备的日志进行采集，采集方式支持Webservice、Syslog、WMI、Agent、JDBC、FTP等接入方式，同时平台的日志采集具备良好的可扩展性，可支持自定义正则，快速兼容新的设备类型。平台接收到日志后，使用与上报日志设备匹配的范式对日志内容提取、整理为统一标准格式，如日志生成时间、IP端口信息、用户信息、协议、日志等级、日志内容等。可识别日志中各类安全威胁，同时通过大数据和深度挖掘等技术提取有效安全告警，关联生成安全事件，并以可视化形式展示。

* 情报关联与智能分析服务

结合云端以及第三方威胁情报库，通过多维度信息融合实现基于攻击场景的事件关联、交叉关联和启发式关联，从而评估安全事件的可信度、威胁度和风险值。通过大数据关联分析发现网络中的失陷主机、安全威胁，识别业务潜在安全风险和高级APT攻击行为。

* 多维度威胁检测服务

根据网络流量的正常行为轮廓特征建立正常流量模型，判别流量是否出现异常，可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描、端口扫描、ARP欺骗。同时深度检测能力还应包含口令暴力破解检测、弱密码扫描检测、黑链检测、终端病毒/恶意软件检测等。同时利用机器学习进行建模，对用户和主机等实体进行分析（UEBA）、识别出用户对业务系统的异常访问，进而发现客户凭据被盗、用户主机失陷等潜在威胁。有具体的请求响应信息，可以直接在平台进行分析研判；提供了事件URL、攻击者受害者信息、事件的举证信息、具体描述信息并支持图片、文件的上传。

* 威胁分析与处置服务

针对检测出来的安全威胁，结合日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害；针对明确的安全事件进行处置，清除恶意文件、快速恢复业务，同时深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径，最后根据事件发生根因、影响范围，针对性给出安全加固方案。

**（五）服务需求**

## 1.平台服务

### **1.1安全数据规范制订服务**

以服务咨询形式，提供台州市政务外网安全大数据平台的安全数据标准规范制订，该标准规范制订需要充分考虑平台自有的格式规范标准，同时兼顾台州市政务外网相关安全设备厂商的安全数据标准规范、浙江省政务外网安全监管平台安全数据标准规范、台州市网络安全协调指挥平台安全数据标准规范等，在此基础上制定安全数据技术规范，包括台州市政务外网安全运营数据的采集技术规范、处理技术规范、存储技术规范、建库技术规范等。为安全数据的采集、处理、存储、共享及分析利用提供支撑。

收集相关国家标准、省级标准和行业标准，本项目的需求，制定《台州市政务外网安全运营平台数据标准》，相关标准提交大数据局审核，经过初步审核后，组织相关安全厂商进行讨论，根据反馈的意见对标准进行修改和完善，修改后的标准提交大数据局进行最终审核，市大数据局从数据标准的合理性、是否能落标、是否符合业务发展等多个角度对标准进行审核，最终得到定版标准。

《台州市政务外网安全运营平台数据技术规范》需要涵盖业务数据标准、参考数据和主数据标准、数据元标准、指标数据标准等内容。

1.1.1台州市政务外网安全运营平台业务术语标准

台州市政务外网安全运营平台业务术语是被批准、管理的安全运营平台业务概念定义的描述，需要根据平台运营的需要明确相关术语定义。

1.1.2台州市政务外网安全运营平台参考数据标准

安全运营平台参考数据是将其他相关数据进行分类或目录整编的数据，是台州市政务外网安全运营平台的数据字典，政务外网安全运营平台主数据标准。主数据是安全运营平台的核心数据，需要明确主数据的定义。

1.1.3台州市政务外网安全运营平台数据元标准

数据元是用一组属性描述其定义、标识、表示和允许值的数据单元，是描述数据的最基本单元。数据元由3部分组成:对象类、特性、表示值域和数据类型的组合。

1.1.4台州市政务外网安全运营平台指标数据标准

指标数据是衡量台州市政务外网安全情况的数据，由指标名称、指标解释、时间限定、其他条件限定、指标数值等组成，如政务外网安全事故发生率等。《台州市政务外网安全运营平台安全数据技术规范》需要覆盖安全告警、安全事件、资产信息、漏洞信息等内容：

1. 安全告警数据规范标准

台州市政务外网范围内的安全设备根据制定的安全告警数据规范标准上报对应数据字段，保障安全运营平台最终汇总的安全告警的数据统一标准；以便于支撑安全运营管理过程中整体安全态势统计与分析；

1. 安全事件数据规范标准

台州市政务外网安全运营平台分析产生的安全事件数据形成统一标准规范，保障在运营管理过程中信息传递的一致性，并能够支撑统一的处置决策。

1. 资产信息数据规范标准

台州市政务外网安全运营管理过程中形成统一的资产信息数据标准，保障运营管理过程资产可以准确和快速的定位。

1. 漏洞信息数据规范标准

台州市政务外网安全运营管理过程中形成统一的漏洞信息数据标准，保障运营管理过程漏洞信息传递和处置准确性，尽量减少信息不全和不准确导致的重复处置或处置不到位的问题。

### **1.2安全数据治理服务**

数据是一切安全工作的基础，保证安全数据质量是安全分析的相关人员日常需要对台州市电子政务外网安全数据进行综合的安全数据治理，用以辅助资产、威胁、脆弱性、事件的管理工作及其他一切的安全服务相关工作。

安全数据的治理在充分遵循国家、省、市的相关数据标准和治理规则的前提下，开展本地数据数据的清洗治理工作，逐步形成标准统一、质量可靠、纬度全面的本地数据，同时，将本地归集的个性数据制定成本地特色标准发布，作为后续该个性数据的治理标准规范等。

完成安全数据的综合治理之后，借助安全数据仓支撑安全运营工作，同时为相关单位的数据使用提供数据共享。

**1.2.1服务周期**

数据治理的服务年限为从项目竣工验收后两年。

**1.2.2服务内容**

按照“应归尽归”原则，本项目数据归集的范围为台州市相关安全数据。通过对安全数据的持续治理构建安全数据仓，安全数据的治理包括数据解析、数据标准化等相关工作。数据治理服务范围和本项目数据归集范围保持一致，治理的数据包括但不限于：边界安全数据、终端安全数据、日志管理数据、安全威胁数据、安全资产数据、安全处置数据、云端数据等。

数据治理的服务内容包括数据调研分析、数据治理规范的建立、数据人工处理、数据治理质量评估、安全数据共享、日常协调等工作。通过安全治理系统提供的工具，通过可视化配置方式对多种来源的数据进行数据人工治理，支持内置数据标准化的解析规则和灵活的自定义解析规则。包括：数据元管理、字典表管理、标准智能关联、数据对标、打标签等。通过数据治理为后续的大数据分析建模、上层应用提供数据支撑。

**1.2.3服务方式和要求**

需要根据治理服务的需要，派驻人员参与数据治理工作。派驻的数据治理人员未经建设单位同意，不得随意更换。

经过治理后的安全数据，准确性、完整性应满足台州市政务外网安全运营平台正常运行的需要，满足网络安全综合分析服务的需要。数据处理过程需要形成数据血缘，记录每项数据的来源、处理过程、应用对接情况等，记录数据表在建仓过程中的全链路血缘关系，帮助数据监管部门实现便捷地问题数据溯源查询和影响分析。

如治理后的安全数据存在准确性和完整性缺陷，项目服务单位需要及时进行整改，直至满足验收要求。

### **1.3安全数据归集服务**

安全数据归集的对象主要为云、网、边、端部署的安全产品。

1）云主要是指政务云，对接政务云安全资源池现有的流式数据、日志数据；

2）网主要是指政务外网，采集政务外网的相关流式数据、日志数据和网络设备数据。

3）边主要是政务外网边界的安全，采集边界安全设备的安全数据。

4）端是指市内电子政务外网上的终端，与市级的终端管理和安全防护系统对接获取终端的安全数据。

除上述系统数据归集外，要求通过数据采集系统与其他网络安全监管平台对接，获取全市外网网络攻击、有害事件数据和终端数据。

**1.3.1终端安全数据归集**

通过标准数据接口方式与市级的终端管理系统进行对接，获取台州市终端安全数据。获取终端主机操作系统、应用系统（如：Web、邮件，操作系统等）所产生的海量日志信息，具体获取的数据内容如下：

1）终端概况

包含已安装终端管理软件终端数量、存在非法接入的终端数量、已安装防病毒软件终端数量、已按要求更新病毒库终端数量、存在病毒但是无法清除的终端数量、打齐规定补丁的终端数量。

2）终端病毒攻防

杀毒趋势、病毒查杀分组、病毒查杀、病毒感染种类情况、病毒实时事件。

3）终端漏洞数据概况

漏洞概况数据、漏洞修复与发现趋势、漏洞及时事件提示、PC与服务器修复漏洞情况、分组漏洞修复情况。

4）终端常用端口

终端端口开放情况、特定端口（如X86的3389、国产的21等）开放情况、特定端口连接情况。

5）终端系统日志信息

各类日志信息、包括系统日志、应用日志。

**1.3.2政务外网安全数据归集**

通过主动探测、标准数据接口对接等方式采集分析电子政务外网流量、网站、系统、主机、安全设备等，同时对接获取台州市的相关政务外网安全数据，政务外网安全数据包括：

安全威胁：威胁事件等级和数量。

网络攻击数据：包含信息收集、拒绝服务、SQL注入、XSS攻击、密码破解、网络欺骗、漏洞攻击、后门攻击、会话劫持、域名劫持、黑市工具、目录遍历。

有害程序数据：包含计算机病毒、蠕虫、木马程序、僵尸网络、混合攻击程序、网页嵌入恶意代码。

流量日志：协议审计日志、登录日志和文件审计日志等；

安全日志：网络安全、应用安全、主机安全和数据安全等；

主机日志：系统日志、应用日志、服务器日志等；

其他日志：安全运维、网络设备等日志；

**1.3.3云安全数据归集**

台州市政务云已经部署台州市电子政务云安全资源池，建设内容包括安全感知系统，终端检测与响应系统,安全日志存储，安全威胁情报。通过主动探测、标准数据接口对接等方式采集分析云平台安全风险，并最终汇总后通过数据融合治理生成相应的主题库数据。

防火墙的安全日志有：DOS攻击日志、WEB应用防护日志、漏洞攻击防护日志（IPS）、僵尸网络日志、内容安全日志、应用控制日志以及安全事件日志等。

EDR的安全日志有：病毒查杀日志、漏洞扫描日志、基线检查日志、入侵检测日志、安全加固日志联动日志、运维日志等

业务系统：部署在云区域内的主要业务系统系统日志。

威胁感知数据：攻击事件、攻击源、攻击目标、攻击类型、危害级别、时间、类型、严重等级、动作、区域、IP、用户、特征/漏洞ID。

安全告警：主机防护、web应用安全、边界防护、漏洞扫描这些安全设备发现的告警数量，包括、主机防护事件数量和趋势，应用防护事件数量和趋势，边界防护事件数量和趋势。

**1.3.4边界安全数据归集**

归集政务外网边界安全数据。常见的网络边界安全管控包含访问控制、网络攻击监测/拦截等，对应的常见安全产品包含防火墙、入侵监测/防护设备（IDS/IPS），WEB应用防火墙等。

1.3.4.1防火墙相关信息

防火墙访问控制类日志：指的是防火墙的允许放行策略和禁止访问策略产生的日志。

关键信息：包含会话信息、源ip、目的IP等的五元组信息；通讯的流量信息；以及策略信息。

1.3.4.2 IDS相关信息

主要归集IDS设备的五元组信息、设备信息、证据信息、规则信息、其他信息。

1.3.4.3 WAF字段信息

主要归集web应用防火墙的五元组信息、设备信息、规则信息、动作信息等

1.3.4.4数据归集标准化

基于实时计算系统的实时处理能力，对数据采集模块采集的消息队列数据并进行标准化治理。上游的安全业务数据通过定时上报及实时抽取汇聚至消息队列，通过配置标准化治理规则、目的表和问题表，将订阅获取到的消息数据进行标准化和治理，并将规范后的数据写回到消息队列或者落盘到各种结构化数据库。

1.3.4.5数据共享可定制化

基于实时计算系统的实时处理能力，对需要通过数据共享模块共享给不同安全厂商的数据进行个性化数据处理。上游的安全业务数据通过定时上报及实时抽取汇聚至消息队列，通过配置个性化处理规则、目的表和问题表，将订阅获取到的消息数据进行个性化处理，并将调整后的数据写回到消息队列，共享给不同的安全厂商。

数据归集服务是利用数据采集模块的能力，将分散在各安全系统中的不同数源、不同格式、不同标准、不同更新情况等的各种个性化数据，按照不同的数据采集方式配置数据采集任务，将数据归集至安全数据仓进行数据标准化。

### **1.4安全数据共享服务**

数据安全共享服务是利用平台安全数据共享能力，将进行标准化治理后的数据，根据浙江省政务外网安全监管平台、台州市网络安全协调指挥平台等数据需求方要求，提供标准化安全数据共享对接服务，将数据以接口、批量、文件或其他方式按需要的调度周期进行共享。

## 

## 2.网络安全综合分析服务

提供2年的综合安全分析服务，主要负责对安全事件研判、安全隐患验证和事件/隐患通报等日常工作，实现对网络安全事件、安全隐患等网络安全数据从产生、验证、通报业务发起到处置闭环全生命周期的管理，从而实现台州市政务外网“底数摸得清、告警报的准、重点抓得到、成效看得见、情报促协同、源头看得见”。

**2.1安全事件分析服务**

提供安全事件发现、定位与溯源、安全事件处置建议等服务。

安全事件发现：基于威胁情报，发现高级威胁、APT攻击、异常流量行为、僵尸木马攻击等安全事件；

定位与溯源：对发现的安全事件定位到具体的IP地址并且能够进行攻击链还原及攻击入口定位 ，识别攻击威胁实体（域名、IP、进程等）；

安全事件处置建议：对发现的安全事件进行深度分析后给出事件处理建议，并提出解决方案。

**2.2威胁感知服务**

通过对安全数据进行分析，运用威胁情报、规则引擎、文件虚拟执行、机器学习等技术，精准发现网络中针对主机与服务器的已知高级网络攻击和未知的新型网络攻击的入侵行为，利用平台对流量日志和终端日志进行存储和查询，结合威胁情报IOC、攻击特征线索、特种攻击特征（如对美暗网等），初步检测网络中存在的攻击行为，定位流量中存在的异常和未知攻击行为，对安全威胁进行感知。

**2.3情报分析服务**

提供情报分析服务，依托安全大数据能力以及本地安全分析人员，对高级威胁事件进行跟踪、研判，并最终发现威胁事件。在威胁分析的各环节，通过公开情报收集、数据处理、恶意代码分析、网络流量解析、线索挖掘拓展，为威胁分析提供了强大的基础数据、威胁研判支撑。

**2.4热点情报预警服务**

提供热点情报预警服务，内容包括漏洞安全预警通告、安全热点周报、月度安全通告。

从海量的安全事件提炼最受关注的热门威胁事件，如漏洞、恶意样本、数据泄露事件等，提供深度分析并结合内外的情报数据进行高效的关联分析，对未知威胁进行预测，例如IP情报（扫描IP、僵尸网络、垃圾邮件服务、恶意IP等）、URL情报（钓鱼、欺诈、篡改、挂马等）、漏洞、文件等并进行内部资产或者量关联分析，形成近期热点安全事件列表。

**2.5安全指数发布**

综合安全事件、威胁感知、情报预警等情况，结合各单位、各县（市、区）情况，编制台州市政务外网综合安全指数和地区安全指数。

**2.6安全报告及制度编制**

相关安全服务商需要对台州市电子政务外网安全运营工作定期出具安全监测分析报告，对发现的问题和采取的措施进行说明，分析存在的问题和改进的措施。配合台州大数据局进行安全制度的编写，安全制度要求具备可执行性。

**2.7安全策略制定**

综合安全事件、安全威胁、安全情报等内容，结合台州市现有的网络安全防御情况，提出网络安全防范措施，定期制定网络安全策略。网络安全策略需要具有指导性、针对性和可实施性。

## 3.系统对接服务

要求实现与浙江省政务外网安全监管平台和台州市网络安全协调指挥平台的对接。

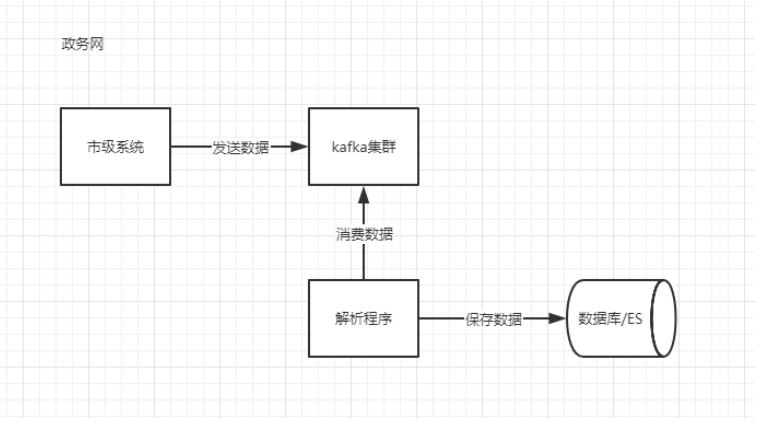
提出数据对接共享标准，包括频率要求等，县市区系统管辖范围内的网络基础数据，包括单位组织信息、硬件设备信息、网站/系统信息、IP信息。系统应在本地新增基础数据或更新基础数据后同步将新增数据记录或含修改内容的数据记录上报给台州市级。同时县市区系统能根据市级级系统的上报基础信息的核验反馈指令，对存在异常的记录及时进行补正并重新上报。其中指令通道通过http方式下达，数据通道通过数据采集系统接入（kafka、sysolog等）。台州市网络安全运营平台根据要求，将相关数据共享给市委网信办网络安全协调指挥平台和浙江省政务外网安全监管平台，通过这种方式实现省、市相关系统对接。

与市委网信办网络安全协调指挥平台和浙江省政务外网安全监管平台对接的接口免费开放，由采购人负责相关接口的协调工作，接口上的技术问题由中标公司负责处理。

**3.1与浙江省安全监管平台对接**

浙江省电子政务外网安全监管平台系统包含了省级平台和地市级平台，省市系统之间需要数据传输，数据、流程对接暂定地市级平台向省级平台报送数据，分别为：流量元素数据、设备日志、资产数据、告警数据、威胁情报数据以及安全事件等，需要实现与浙江省平台需要按照《浙江省电子政务外网安全监管平台地市对接标准规范》进行对接。

数据传递流程如下：



本次对接采用Kafka进行异步数据上报，由于本次对接涉及到不同类型数据，因此对各类型数据定义单独的topic。

**3.2与市委网信办网络安全协调指挥平台对接**

与台州市委网信办的网络安全协调指挥平台进行对接，将安全隐患与安全事件传送给台州市委网信办网络安全协调指挥平台进行安全隐患与安全事件的通报预警，通报的内容包括：对各委办局的安全评估通报、对突发事件的通报、对专项威胁与事件的通报和综合定期通报。

获取台州市委网信办网络安全协调指挥平台回传的网络事件处置结果数据并进行展示

情报共享协同：提供订阅威胁情报功能，按照行业、IP、域名、区域等订阅内容，并能推送告警通知。同时能够提供通过WEB接口、Syslog、API等方式进行情报分发共享。

**（六）** **技术指标要求**

## 1.安全数据运营系统

|  |  |  |
| --- | --- | --- |
| **指标能力** | **指标项目** | **指标要求** |
| 安全指数管理 | 安全指数发布 | 结合各单位、各县（市、区）情况，编制台州市政务外网网络综合安全指数，发布市级部门及县市区安全指数。 |
| 自定义指数，系统支持基于安全状况定义指标，和用户可自定义评估指标两种模式； |
| 评分任务调度 | 基于设计的安全指数定义评分项目，并下发基于安全指数的评估项目；系统可自定义评估对象与评估频率； |
| 数据仓展示 | 数据仓展示 | 将丰富、多样的安全数据资源通过资产盘点进行资产的定义，并进行资产的分类梳理，形成数据仓展示界面，充分摸清安全数据家底，能够直观的展现安全数据资产整体情况，帮助持续不断的提升和挖掘安全数据的应用价值。支持安全数据仓资产、安全数据归集情况、安全数据治理等安全数据资产的统计呈现，实现对安全数据资产的轻松全盘掌握。具备安全数据仓数据分层分类统计呈现，包括原始库、成果库、主题库等各种维度的全盘呈现，掌握安全数据资产在安全数据仓中的来龙去脉。 |
| 运营流程管理 | 安全运营流程自定义 | 可通过安全运营工具，创建安全运营流程用以辅助日常安全运营工作，如：资源申请、公文下发等。（需提供软件界面截图等证明材料） |
| 支持针对用户安全运营业务流程，可进行图形化的方式进行自定义工单流程（至少包含录入节点和审批节点），并可以根据业务不同内容进行工单的自定义；灵活的表单配置能力；支持自定义控件，包括：基础字段：单行文本、多行文本、日期、附件、单项选择、多项选择、下拉菜单、富文本、表格、高级字段：组织架构、选择人员、选择告警、选择脆弱性、选择资产、选择动作、选择剧本、脆弱性状态、告警状态、资产属性审核、资产入库审核等。 |
| 工单支持多种附件类型，满足各流程节点的推动所需的相关信息，提供多种附件类型的支持与限制，包括:文档、图片、压缩包；单流程节点不小于上传10个附件的能力。 |
| 支持结合用户工单流转情况进行统一展示，包括工单总数、流转中、超时工单、责任人超时工单TOP5、超时工单TOP5、已结束工单、已撤销工单等。 |
| 工单支撑考核 | 支持基于运营管理过程的流程工单闭环情况，进行对应的评分的记分统计，包括工单完成情况、待处理超时工单等维度； |
| 安全运营流程节点自定义 | 可对新增或已有的安全运营流程各个节点进行新增、删减、顺序调整等操作，匹配安全运营流程节点中各个组织、责任人的加签、处置、跳转等场景。（需提供软件界面截图等证明材料） |
| 公共字段自定义 | 可对各安全运营流程节点的公共字段（内容）进行调整，如：名称、内容、通知放、抄送方、附件添加、建议、评价等，满足各流程节点的推动所需的相关信息。 |
| 工单任务下发 | 监测的各类网络安全隐患及事件、通报反馈情况、整改情况及处罚情况可以支持浙政钉客户端、短信、邮件等通报通知方式 |
| 可与第三方工单系统进行集成对接，将监测的各类网络安全隐患及事件、通报反馈情况、整改情况及处罚情况形成工单模版，下发到相关责任单位。 |
| 消息通知 | 通过浙政钉支持查看所辖区域内安全事件发生情况，可查看事件详细信息。字段包括事件名称、事件类型、事件发现时间、处置状态等信息 |
| 联动处置 | 自动化风险处置编排 | 自动化风险处置编排流程，不同类型安全事件的分析处置响应流程，平台管理员可自定义安全编排剧本。 |
| 可通过类似Visio的拖拽方式灵活自定义编排威胁的响应处置流程。 |
| ★支持灵活自定义编排威胁的响应处置流程，并支持多种执行节点包括：动作调度、剧本应用、决策器、过滤器、人工审批、人工录入、并行分支等必要的关键节点。（需提供软件界面截图等证明材料） |
| 在自动化安全响应中，可基于事件主体类型（攻击源、账号、目标资产、域名等）、风险等级、安全威胁场景、安全规则等定制联动指挥场景全自动调用剧本；可基于满足某个数据过滤条件周期性执行剧本；（需提供软件界面截图等证明材料） |
| 联动支持台州大数据局现网已有的安全设备，包括：2台政务外网出口防火墙和4台政务云出口防火墙等设备的安全策略下发； |
| 流程处置剧本 | 可设置不少于50个自动化处置的playbook剧本的运行能力，能够在部分安全场景下实现自动化或半自动化的对威胁进处置。 |
| 能够新建剧本并关联事件，提供手动执行和自动执行触发剧本执行，具备动作、过滤、决策、文本、人工介入审批等，可通过图形拖拽连线形成完整事件处置流程剧本。支持and、or、not、==、！=、in、not in、>、>=、<、<=、else if、纯文本等方式添加过滤规则。 |
| 告警联动处置 | ★支持文件、邮件、勒索、挖矿相关安全事件专项页面展示，且所有专项告警支持直接进行联动处置，联动处置支持自动调用内置处置策略模板，也支持自动化编排的自定义处置流程策略。  （需提供截图打印加盖投标人公章） |
| 自动化编排 | 同时支持自动化编排的自定义处置流程策略的设置，灵活剧本设置，融入事件自动处置流程，节省运维处置时间，根据客户实际需要对接所需同品牌或者第三方品牌安全设备进行安全事件处置。  支持前端拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于数据源、分析组件、处置响应等，可自动判断策略编排是否合理并弹窗提示  （提供界面截图并加盖投标人公章） |
| 可视化分析 | 技术指标 | 可连接多种数据源，包括但不限于MySQL ，Oracle，hive，MaxCompute，Hologres，Hbase； 内置10+可视化图表模板，可视化呈现数据。 |
| 安全报告及规范编制 | 安全报告及规范编制 | 相关安全服务商需要对台州市电子政务外网安全运营工作，定期出具安全监测分析报告，对发现的问题和采取的措施进行说明，分析存在的问题和改进的措施。支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种方式呈现。 |
| 资产管理 | 资产信息管理 | 支持通过对接资产探测发现设备资产，识别操作系统、开放的服务与端口、在线离线状态、资产类型等信息。支持资产维度包括IP地址、所属资产组、主机名、责任人、所属业务、MAC、地理位置、操作系统、服务与端口、最近上线时间等信息。（需提供截图证明并加盖投标人公章） |
| 资产指纹定义 | 支持基础信息、开放端口、风险信息、账号信息、应用软件信息、访问权限、硬件信息、数据来源维度进行资产信息展示。其中基础信息包括关联IP、设备信息、地理位置、资产责任人、操作系统、虚拟机、业务服务、自定义属性等维度。其中支持手动自定义属性的填报，支持定制更多属性信息进行填报。 |
| 资产识别 | 可识别并展示资产信息，识别IP地址、主机名、MAC地址、操作系统、资产类型、终端接入状态等信息。 |
| 资产总览 | 支持展示资产统计、资产来源、资产防护统计、Agent防护状态统计、资产互联网暴露、指纹信息、高风险应用软件统计、特殊账号TOP5统计、端口TOP5统计、应用软件TOP5统计、数据库TOP5统计。 |
| 资产管理 | 支持以资产组视角、业务视角的纬度展示资产详细台账，  资产组支持自定义，支持新增、编辑、删除等操作，可配置资产组的基本信息、资产组范围（可自动识别IP属性）和资产责任人。  业务组支持自定义，支持新增、编辑、删除等操作，可配置业务名称、业务所属上级、业务的资产范围（支持以资产组的快速批量筛选和手动输入筛选）、责任人、重要级别和备注等。  支持资产的高级筛选功能，内置的筛选条件，包括资产类型、终端接入状态、数据源、操作系统、资产重要性、标签、首次发现时间、最近更新时间等，并支持手动输入IP/资产ID/主机名/资产名称/MAC地址/责任人，进行精确搜索 |
| 资产详情 | 支持展示资产基础信息、关联IP、操作系统、设备信息、地理位置、资产责任人；  支持展示资产指纹包括、开放端口、应用资产、web资产、账号信息、运行进程。  支持展示硬件信息包括CPU、内存、硬盘、分区、主板、网卡。  支持展示数据来源。 |

## 2.安全数据共享系统

|  |  |  |
| --- | --- | --- |
| **指标能力** | **指标项目** | **指标要求** |
| 安全数据采集模块 | 适配多种数据资源 | 【流式数据接入】  ★支持基于开源组件Kafka深度优化后的流式数据接入。  （提供具有CMA（中国计量认证）标识或CNAS（中国合格评定国家认可委员会认证）标识的测试报告关键页（含首页、盖章页及对应功能描述页）等证明材料并加盖投标人公章） |
| 【批量数据接入】  ★系统需适配各种关系型数据接入，包括但不限于Oracle、MySQL、SQL Server、PostgreSQL、MongoDB、Sybase、Teradata和DM、GBase、GaussDB、kingbase等。  具备主流大数据平台对接，包括但不限于Hadoop、FusionInsight、MaxCompute等大数据平台。  系统需支持文件的搬移与解析功能，文件夹或目录增量同步功能；具备针对文件夹的子文件夹及文件增、删、改操作的实时增量同步功能。［提供具有CMA（中国计量认证）标识或CNAS（中国合格评定国家认可委员会认证）标识的测试报告关键页（含首页、盖章页及对应功能描述页）等证明材料并加盖投标人公章］ |
| 【文件数据采集】  对海量文件（10000+以上文件），具备批量操作功能，具备批量选择传输文件，自动进行文件传输的功能。 |
| 【其他数据接入方式】  支持通过Syslog等方式，对相关设备和系统日志数据进行采集。 |
| 关键功能特性 | 【易用性】  具备Web页面的拖拉拽式数据交换管理。  具备系统配置导入和导出功能。 |
| 【安全性】  具备加密传输功能：具备国密算法（如AES、SM2、SM4等）数据加密交换功能，能够实现数据加解密；具备数据日期类型、 INT类型等非字符串类型字段的数据加解密；具备数据传输通道加密功能(SSL) |
| 【兼容性】  ★采用的软件产品需能兼容国产芯片，需提供与龙芯、众志海光、神威等任意一个国产芯片兼容性互认。  （要求提供相关认证证书扫描件并加盖投标人公章）  ★采用的软件产品需能兼容国产数据库，需提供与达梦、人大金仓、OceanBase等任意一个国产数据库兼容性互认证明材料。  （要求提供相关认证证书扫描件并加盖投标人公章） |
| 【基础功能】  可实现对数据采集的自定义频率任务调度，通过数据采集作业策略的设置，提供定时执行的服务。定时调度方式有：手动，按秒、按分钟，按天，按周，按月，按年和实时。  ETL组件库具备数据抽取、关联、排序、清洗转换、聚合、装载等功能。  具备批量创建作业功能；具备在ETL任务同步时，批量作业通过一个任务管理多张表的数据同步；具备同步至目的库时增加入库时间。 |
| 安全数据治理模块 | 高级数据管理 | 支持各种主流类型的数据存储和处理平台，包括但不限于MySQL、Hive、Oracle等，可提供元数据信息展示和动态更新。  具备元数据变化通知功能，通知内容应包括变更的具体内容  具备元数据继承功能，可进行克隆表、接入转换任务配置。 |
| 数据血缘 | 具备自动数据血缘生成功能，包括但不限于数据集成、清洗、SQL加工、数据共享的自动血缘生成。 |
| 数据地图 | 具备多种建表方式，包括但不限于可视化建表、DDL建表。  具备以目录形式对数据表进行管理的能力，包括如收藏数据表等功能。  具备按照多种条件组合查询数据表的功能，查询条件包括但不限于数据表描述、业务标签、创建者、生命周期、大小、项目空间名称、分区表属性等。  具备表信息查看功能，包括但不限于表的元数据信息，例如主键信息、分区信息，表数据预览，表血缘详细信息。  具备管理数据元、字典表、限定词的能力。 |
| 数据标准 | 数据标准支持多租户（工作空间）实例，每租户实例可以使用独立的数据标准模板。  具备定制安全行业标准模板功能。系统支持预置行业模板，并支持用户自定义扩展  具备按照标准的发布状态进行数据元版本管理的能力，提供版本变更支持在线审批等功能。  具备批量导入和导出数据标准定义功能。 |
| 数据回写 | 具备内置的数据清洗和过滤组件。数据过滤组件应包括但不限于长度过滤、正则过滤、标准值域过滤、空值过滤、比较过滤；数据清洗组件包括但不限于字典标准化、JS自定义清洗。  具备规则库相关功能，能提供去除空白、空值过滤、全角半角转换、正则校验、长度校验、去重等内置规则，并支持规则自定义。  具备智能清洗功能，能够智能推荐清洗规则，实现自动配置。 |
| 过程监控 | 具备调度管理功能，包括一次性调度与周期性调度，其中周期性调度应支持按分钟、小时、日、周、月、年调度，工作流可跨周期依赖。  具备数据运维大盘功能，能够直观的展示各空间工作流运行情况，包括但不限于任务运行情况、任务出错排行和空间任务数量排行等，从各个维度展示系统的过去一段时间内的运行情况。  具备数据接入任务运维功能，管理任务实例、状态、关联工作流，支持查看数据抽取、写入数据量等指标；支持对接多套数据集成环境。 |
| 数据存储模块 | 数据存储 | 具备多副本高可靠的分布式文件存储能力，具备结构化、半结构化、非结构化文件，具有高吞吐量和低延时的访问能力。 |
| 具备全文搜索服务能力，基于分布式全文搜索引擎，支持TB级别数据量实时分析和检索。 |
| 安全数据存储需复用台州市政务云各类存储服务资源，包括但不限于MaxCompute存储空间、OSS等。 |
| ★安全数据复用现有的台州市政务云各类存储资源。 |
| 运维监控 | 具备消息队列引擎的多集群运维、管控、指标统计分析能力  具备全文搜索引擎的多集群运维、管控、指标统计分析能力 |
| 安全数据仓建设 | 数据仓建设 | 平台可根据用户需求与场景，支持基于数据特征进行抽取各种层次的库类型。设置层次至少三层，分为原始库、成果库、主题库。 |
| 原始库存储从各安全设备和各数据源采集的原始数据，原始库中的数据是系统最基础的数据，需要对数据设置不同的生命周期和存储份额，从而保障数据的可用性和鲜活性。 |
| 成果库的数据是由原始库的数据经过解析、清洗和标准治理等数据处理过程后形成的标准数据。成果库同时也保存着安全数据分析后的结果数据。 |
| 主题库对上游的成果库数据打散重构形成主题表，对下游的专题层提供了标准化、一致性的数据。 |
| 数据计算模块 | 流数据计算 | 具备实时开发功能，能处理Kafka源数据，支持Oracle、华为GaussDB，Mysql，DM，Kafka输出 |
| 具备实时数据运维功能，支持查看Flink SQL和application的任务状态；可以查看任务运行实时指标，可自定义运维指标。 |
| 具备实时开发工作台功能，能提供基于FlinkSQL的可视化SQL编辑器，应支持实时SQL任务的管理、启动、暂停、取消等操作 |
| ★具备实时清洗功能，能够完成实时数据清洗过滤、实时数据转换、内置规则组件调用、自定义清洗规则、配置问题数据处理方式、清洗流程试运行。  （提供具有CMA（中国计量认证）标识或CNAS（中国合格评定国家认可委员会认证）标识的测试报告关键页（含首页、盖章页及对应功能描述页）等证明材料并加盖投标人公章） |
| 分布式计算 | 【开发环境】  提供一站式集成开发环境，满足大数据环境下的开发、调度、运维等需求。  具备开发、生产空间隔离，可以对空间中数据、资源、代码和配置进行隔离功能。  具备团队协同开发功能，能够实现代码版本管理、多人协同模式下的代码锁管理和冲突检测机制。  具备通过图形化的拖拉拽方式、零编码交互完成数据的转换、过滤以及工作流开发功能，便于自主管理作业的部署以及生产监控运维。  采用多点部署方式，具备弹性扩容能力，能避免单点故障导致整个系统不可用，保证系统的高可靠性  具备在腾讯云、华为云、阿里云等多云、跨云环境中运行的能力。 |
| 【数据开发】  支持多种数据传输插件，例如：Kafka、ElasticSearch、Fluentd、JSON、ActiveMQ，RabbitMQ等。  适配MaxCompute、FusionInsight HD、TDH等大数据平台引擎，支持SparkSQL、Spark、数据清洗、SubWorkflow（子工作流）等数据开发类型节点。  ★具备工作节点开发功能，包括但不限于数据集成类型节点、数据开发类型节点、数据清洗类型节点。（提供具有CMA（中国计量认证）标识或CNAS（中国合格评定国家认可委员会认证）标识的测试报告关键页（含首页、盖章页及对应功能描述页）等证明材料并加盖投标人公章）  具备工作流运行管理功能，能够管理工作流执行路径，包括但不限于串行、并行、分支条件，并应具有从此处开始运行功能。  具备智能化依赖推荐功能，能够基于工作节点的输入输出表，自动推荐上下游依赖关系。  具备工作流的导入导出功能，包括但不限于工作流、自定义函数、资源文件和模型等，可实现离线备份和异地发布。  具备版本管理功能，能提供工作流和工作节点的版本查看及版本回滚。  可对已删除的工作节点或工作流进行恢复。 |
| 【任务调度】  具备调度管理功能，包括一次性调度与周期性调度，其中周期性调度应支持按分钟、小时、日、周、月、年调度，工作流可跨周期依赖。  具备启停功能，支持工作流重跑；支持补数据，可通过设置工作流运行的起止时间，来达到导入历史数据的目的。  具备模型任务管理功能，能对数据模型中一键生成的映射加工任务节点进行统一管理，包括但不限于保存、提交、运行、版本比较、版本回滚等；构建工作流后可实现周期调度。 |
| 【数据运维】  具备数据运维大盘功能，能够直观的展示各空间工作流运行情况，包括但不限于任务运行情况、任务出错排行和空间任务数量排行等，从各个维度展示系统的过去一段时间内的运行情况。  具备作业管理功能，能实现作业状态查询、启停操作，并支持引擎告警和工作流告警策略配置，可通过邮件方式发送告警。  具备数据接入任务运维功能，管理任务实例、状态、关联工作流，支持查看数据抽取、写入数据量等指标；支持对接多套数据集成环境。 |
| 【安全性】  具备用户角色权限控制功能，包括系统管理员、空间拥有者、空间管理员、开发人员和测试人员，不同的角色拥有不同的运维权限，用户只能查看到自己拥有权限的空间相关的运维信息。  具备基于SQL节点的加密功能。 |
| ★安全数据离线计算能力复用现有的台州市政务云大数据计算能力。 |
| 分布式搜索模块 | 【数据查询】  提供开放的 API 接口，支持通过API 编程接口实现大数据搜索服务的索引建立、数据检索等； |
| 【索引管理】  基于索引服务，展示各索引的健康状态、主分片数、副分片数、中文文档总数、主分片大小以及主分片和副分片大小相关信息。 |
| 【监控平台】  部署索引监控系统，可以通过浏览器页面监控数据库运行情况，包括CPU、内存、硬盘等系统资源占用情况，还有每个服务器节点的系统负载情况。 |

## 3.网络安全综合分析服务

* 威胁分析服务

|  |  |  |
| --- | --- | --- |
| **指标能力** | **指标项目** | **指标要求** |
| 数据采集 | 网络侧数据采集 | 支持网络侧遥测数据采集20种，包含脆弱性、服务探测、主机探测、网站攻击、后门通信、账号爆破、攻击利用、邮件攻击、DOS攻击、黑客工具、异常流量、漏洞攻击、业务风险、DOS攻击、勒索挖矿、僵尸网络、网络协议、NetFlow、Payload、可疑日志。 |
| 终端侧遥测数据采集 | 支持终端防护遥测数据采集：包含传统杀毒类日志、IOA类日志；  Windows系统上支持18种系统事件的遥测数据采集：包含进程销毁、文件创建事件修改、文件重命名、文件删除、远程线程注入、注册表删除、进程调用API、驱动加载、模块加载、WMI Filter创建、WMI Consumer创建、WMI Binding创建、计划任务创建、符号链接创建、命名管道创建、命名管道打开、VolumeSnapshot删除、敏感进程访问。  Linux系统上支持8种系统事件的遥测数据采集：进程创建、文件删除、文件重命名、文件创建、文件修改、DNS请求、网络链接、TCP端口监听。 |
| 第三方数据采集 | 支持第三方数据采集，可对接第三方开放的一手数据，或现网安全设备日志、网络设备日志、操作系统日志、应用日志、数据库日志、VPN/堡垒机等审计日志；  接入方式包含Syslog、Kafka、SNMP Trap、JDBC、FTP、SFTP；  解析类型包含正则、kv、csv、grok正则。 |
| 威胁检测 | IOA行为检测 | 支持攻击指标检测，对攻击者的攻击手法进行检测，指标覆盖ATT&CK所有阶段攻击手法，以检测攻击准确性为目标，通过采集的网端数据进行研判、挖掘。可以发现高级威胁。  支持自定义IOA规则。 |
| 特征检测 | 支持IOC失陷指标检测，包含WAF、IPS、威胁情报、黑客工具、攻击利用成功、僵尸网络多种规则库。  支持16种分析检测引擎，包含AD域行为分析、DNS流量分析、HTTP流量分析、邮件检测、SMB协议流量分析、SIEM日志关联分析、 威胁情报关联分析、文件威胁检测、脆弱性检测、 UEBA分析、内网安全检测、 账号安全检测、恶意脚本分析、 HTTPS加密流量检测、攻击溯源分析、视频设备安全检测。  支持自定义IOC规则。 |
| 异常行为检测 | 支持UEBA异常行为检测，通过对内部用户和资产的行为分析，进行持续的学习和行为画像构建，以基线画像的形式检测易于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常行为，对用户/资产进行综合评分，识别已入侵的潜伏威胁、外部入侵行为提前预警，应用场景有账号登录异常、数据库异常、外联异常、外发数据异常、访问异常、账号爆破。 |
| 关联分析 | 支持将终端侧和网络侧收集的数据，与云端威胁情报、资产、时间等因子做时间线关联、因果推断，最终生成平台侧的关联事件。  支持内置分析规则104条，支持自定义分析规则。 |
| 监控管理 | 监控总览 | 支持首页展示风险总览、包括安全事件总览、资产统计、接入设备展示包括不仅限于防火墙、探针、EDR、CWPP，待处置安全事件TOP5、云端威胁狩猎报告总览、攻击面TOP5、脆弱性资产TOP5、风险资产分布及风险资产发生趋势、待处置安全事件分布及安全事件发生趋势。可清楚明晰下一步处置方向。 |
| 监控大屏 | 支持不同安全视角展示2个独立的大屏展示功能 ，包括安全告警态势大屏、资产态势大屏等，支持自定义大屏。 |
| 安全调查 | 安全事件 | 支持对事件等级、威胁标签、数据源、处置状态等进行快速筛选，并提供简易模式和专家模式两种调查方式，简易模式可基于字段名称进行检索、专家模式采用SPL语句检索。支持保存检索条件。（需提供截图证明并加盖投标人公章） |
| 支持安全事件详情总览，包括安全事件名称，安全事件等级、数据源、处置状态、事件编号、告警举证数、资产IP、事件描述等，同时提供ATT&CK命中次数缩略图、攻击故事线、告警详情、响应处置、攻击入口还原、历史攻击回溯、业务攻击面分析的展示，可在详情总览实现一键遏制。 |
| 支持查看ATT&CK攻击矩阵攻击命中全景图并匹配对应告警，可清晰了解安全事件中被黑客技战术利用的情况，提升研判效率。同时可查阅命中技术ID、命中次数、技术描述和参考来源。（需提供截图证明） |
| 支持通过安全事件详情查看攻击故事线。安全事件按照攻击入口和进程树的视角进行安全分析。可详细点开进程链中任意进程查看进程详情，包括基础信息、威胁告警、网络连接行为、文件行为、域名访问行为、模块加载行为，并且自带解码工具。 |
| 支持对安全事件推送处置和响应建议，响应建议包括原理介绍、危害影响、处置建议。通过建议描述、业务影响标签和安全效果标签清晰明确指导下一步响应动作，可一键封禁IP、隔离主机等。（需提供截图证明） |
| 风险资产 | 支持风险资产总览，对包括影响资产、风险等级、威胁标签、资产类型、事件数、漏洞/弱密码攻击面情况、最近检测时间等进行展示。可自定义编辑风险资产统计图。可通过风险等级、标签、重要级别、资产类型、数据源对资产进行筛选。可导出风险资产列表。 |
| 安全告警 | 支持安全告警的高级筛选功能，可对告警的名称、告警等级、攻击标签、处置动作、主机IP、源IP、目的IP、攻击结果、处置动作、等进行告警筛选，可对重点关注资产、重点关注告警类型、重点关注攻击者进行设置筛选和标示，支持数据导出。支持对安全告警的处置操作，包括标记处置状态、封堵地址、隔离主机、处置文件、信任文件、加白名单等。 |
| 安全日志 | 支持对收集的日志进行检索，包括网端安全检测日志、端点安全检测日志、流量审计日志以及第三方日志。 |
| 操作日志 | 支持区分账号用户记录平台操作记录，记录包括操作时间、用户名、IP地址、操作类型、操作对象、执行结果、操作描述。 |
| SIEM数据接入 | 可支持以标准Syslog、Kafka、SNMP Trap、JDBC、FTP、SFTP接收第三方设备日志并存储，如防火墙、上网行为审计、应用交互、态势感知、扫描器、抗DDoS、DLP、UTM、IPS、网站入侵检测、数据库防火墙、沙箱、蜜罐等，解析规则不低于800种，涵盖安全设备、网络设备、操作系统、中间件、服务、应用系统等，采集数据多维丰富。支持新增、编辑、启用、禁用解析规则，并监控日志源连通状态，当日采集、解析日志数。 |
| SIEM数据分析 | 支持内置CC通信、VPN安全、主机异常、堡垒机安全、恶意软件、扫描探测、拒绝服务、暴力破解、漏洞利用、网站攻击、邮件安全等维度的数据分析规则不低于100条。可自定义新增匹配或统计规则，可启用或禁用解析规则。 |
| 攻击面 | 脆弱性 | 支持以资产视角，对终端遥测及网络遥测扫描到的资产脆弱性进行展示，可对资产修复优先级、风险类型、风险资产及资产组名、责任人等标签进行筛选，并通过图表进行统计展示资产修复优先级情况、脆弱性统计情况、资产脆弱性TOP5 |
| 支持以风险视角，对脆弱性风险进行展示，可对脆弱性类型、威胁标签、修复优先级、检测方式、脆弱性名称、数据源等标签进行筛选，并通过图表进行展示脆弱性修复优先级情况、弱密码类型TOP5，影响主机数TOP5等 |
| 资产脆弱性详情基于漏洞和弱密码展示不同资产的脆弱性总览；漏洞会展示漏洞名称、CVE-ID、标签、等级、数量、扫描原理等信息，并可以基于修复优先级、威胁标签、扫描原理等进行高级筛选。  单个漏洞展开会展示基础信息、漏洞介绍、解决方案、影响组件、攻击情报、举证信息等。  弱密码展示不同账号的弱密码信息，包括修复优先级、互联网暴露、弱密码类型、数据源、发现时间等。 |
| 风险应用检查 | ★支持针对风险应用查看是否有资产安装该应用，并查看该资产上风险应用的数量及风险应用的介绍。（需提供截图证明并加盖投标人公章） |
| 响应策略 | 封禁IP管理 | 支持配置规则可按IP/域名/url联动防火墙设备进行封堵，封禁时长可按天/时/分细粒度进行设置。可对封禁对象进行删除、解封、再次封禁等操作 |
| 隔离主机 | 支持联动EDR/CWPP进行隔离主机，支持隔离主机的管理，展示隔离主机的详细信息，包括主机名、操作人、处置时间、隔离状态和联动设备等，可对已隔离的主机进行解除隔离。 |
| 白名单 | 配置规则支持按源IP、源端口、目的IP、目的端口、告警规则ID、日志规则ID、域名、X-Forwarded-F、CVE-ID等字段，进行=或in加白，支持配置加白时长。已添加的规则支持搜索和批量删除（需提供截图证明并加盖投标人公章） |
| 阻断进程记录 | 支持阻断进程记录的展示，包括匹配条件、参数、所属资产、关联告警、关联事件、处置人、处置时间、联动设备等。并支持检索。（需提供截图证明并加盖投标人公章） |
| 拦截域名 | 支持拦截域名记录的展示，包括匹配方式、生效资产、处置状态、关联告警、关联事件、处置人、处置时间、联动设备等。并支持检索。（需提供截图证明并加盖投标人公章） |

* 态势感知服务

|  |  |  |
| --- | --- | --- |
| **指标能力** | **指标项目** | **指标要求** |
| 日志采集与关联分析服务 | 异常流量分析 | 支持按照对外业务流量可视、横向流量可视、外联流量可视等开放的业务流量情况，展示服务器流量排行、最活跃源主机的内网服务器的流量情况，支持全球地图展示整体外联流量情况。 |
| 潜伏威胁黄金眼 | ★支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息；帮助管理人员及时了解威胁的影响，并找到攻击入口点。（需提供截图证明并加盖投标人公章） |
| 第三方日志接入 | 支持对700+网络安全设备规则，包括网络设备、安全设备、中间件、操作系统等；接入方式支持文件、数据库、API、Syslog、FTP、Snmp trap、Kafka、wmi、webservice、winlogbeat等方式进日志行接入，并支持用户对日志进行自定义解析规则，支持接入设备自动发现功能。 |
| 情报关联与分析服务 | 情报威胁检测 | 支持APT 情报告警、Rootkit 告警、感染型病毒告警、木马病毒、挖矿病毒、蠕虫病毒、勒索病毒、恶意下载、DGA病毒等情报威胁检测并产生告警。（需提供截图打印并加盖投标人公章） |
| 威胁感知模块赋能态势感知 | 支持通过网络侧（N）与终端侧（E）关联聚合，可以实现进程级取证，失陷主机定位更精准，并以可视化图谱直观清晰地展示出完整的攻击链，帮助用户快速找到症结，避免全盘查杀对业务产生影响。 |
| 威胁情报共享 | 支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。 |
| 多维度威胁检测服务 | 主机行为UEBA分析 | 支持利用EBA技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。并支持用户对EBA基线进行自定义调整，优化模型。（需提供截图打印加盖投标人公章证明） |
| 入侵威胁检测 | 支持端扫描探测攻击、口令爆破攻击、Web 通用攻击、通用组件漏洞攻击、恶意邮件、横向移动攻击、隧道攻击、紧急应用漏洞、黑客工具攻击、漏洞攻击、 WebShell、数据库安全、AD 域安全等攻击检测并产生告警。（需提供截图打印加盖投标人公章证明） |
| 告警消减 | 支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。支持根据自身业务和安全运维经验自定义告警/事件，以便提高告警的精确度，减少运维成本。 |
| 威胁分析与处置服务 | 溯源中心 | 支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。 |
| 流量采集服务 | 基本要求 | ★提供不少于5套流量采集服务 ；其中2套（市府大楼核心、应急核心）支持不低于 8Gbps 的数据采集分析服务:3套（政务云)支持不低于 3Gbps 的数据采集分析服务； |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等,  具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。 |
| 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号 |
| 异常会话检测 | 可实现对外联行为分析、间歇会话连接分析、加密通道分析、异常域名分析、上下行流量分析等在内 的多场景网络异常通信行为分析能力。 |
| 深度监测能力 | 可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型; |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解检测功能； |
| 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测 |
| 高级检测 | 支持DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；SMB审计日志，主要用于平台SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于平台Mail flow分析引擎进行安全分析，同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析 |
| Web应用安全检测能力 | 支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测； |
| 支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测 |
| 支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤； |
| 违规访问检测 | 能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式 |

## 

## 4.网络安全数据规范治理

|  |  |
| --- | --- |
| 安全数据技术规范制订 | 制定安全数据技术规范，包括台州市政务外网安全运营数据的采集技术规范、处理技术规范、存储技术规范、建库技术规范等。为安全数据的采集、处理、存储、共享及分析利用提供支撑 |
| 安全数据标准制订 | 日志数据接入，日志平台供应商需要按平台数据要求与平台对接，按要求提供相关数据，根据接入安全业务系统的数据评估结果，结合国标、行标、地标以及不同安全厂商的不同类型标准，梳理符合安全业务字段数据的数据元，然后基于数据标准对安全业务系统数据进行数据治理，由于数据标准直接决定数据治理后的数据质量，所以需要对大量标准集中梳理后持续迭代优化，保证清洗后的数据质量。 |
| 政务云安全数据接入，政务云安全开发单位需要按平台要求与平台对接，提供平台需要的数据，根据接入安全业务系统的数据评估结果，结合国标、行标、地标以及不同安全厂商的不同类型标准，梳理符合安全业务字段数据的数据元，然后基于数据标准对安全业务系统数据进行数据治理，由于数据标准直接决定数据治理后的数据质量，所以需要对大量标准集中梳理后持续迭代优化，保证清洗后的数据质量。 |
| 政务外网边界安全数据接入，边界安全系统提供单位或相关设备供应商需要按平台要求与平台对接，提供平台需要的数据，根据接入安全业务系统的数据评估结果，结合国标、行标、地标以及不同安全厂商的不同类型标准，梳理符合安全业务字段数据的数据元，然后基于数据标准对安全业务系统数据进行数据治理，由于数据标准直接决定数据治理后的数据质量，所以需要对大量标准集中梳理后持续迭代优化，保证清洗后的数据质量。 |
| 政务外网终端数据接入，政务外网终端安全系统或设备提供单位需要按平台要求与平台对接，提供平台需要的数据，根据接入安全业务系统的数据评估结果，结合国标、行标、地标以及不同安全厂商的不同类型标准，梳理符合安全业务字段数据的数据元，然后基于数据标准对安全业务系统数据进行数据治理，由于数据标准直接决定数据治理后的数据质量，所以需要对大量标准集中梳理后持续迭代优化，保证清洗后的数据质量。 |
| 漏扫数据接入，漏扫系统或设备提供商需要按平台要求与平台对接，提供平台需要的数据，根据接入安全业务系统的数据评估结果，结合国标、行标、地标以及不同安全厂商的不同类型标准，梳理符合安全业务字段数据的数据元，然后基于数据标准对安全业务系统数据进行数据治理，由于数据标准直接决定数据治理后的数据质量，所以需要对大量标准集中梳理后持续迭代优化，保证清洗后的数据质量。 |
| 其他安全数据接入，包括安全资产、安全处置信息等相关安全系统或设备提供商按要求与平台对接，提供平台需要的数据，根据接入安全业务系统的数据评估结果，结合国标、行标、地标以及不同安全厂商的不同类型标准，梳理符合安全业务字段数据的数据元，然后基于数据标准对安全业务系统数据进行数据治理，由于数据标准直接决定数据治理后的数据质量，所以需要对大量标准集中梳理后持续迭代优化，保证清洗后的数据质量。 |
| 信息资源编目服务 | 结合相关信息共享目录要求，对数据资源名称、数据资源摘要、数据资源提供方、数据资源分类、数据资源共享属性、数据资源公开属性、数据资源标识符、元数据标识符、数据项描述等元数据信息进行明确，对已注册的基础数据按照业务、层级等进行编目、发布，形成《台州市政务外网安全运营平台数据资源目录》。将编制好的数据资源目录，根据IRS的相关要求，上传到IRS平台。 |
| 数据治理服务 | 提供安全数据治理人工服务，建立数据治理工作规范，明确数据治理工作流程，通过安全治理系统提供的工具，支持通过可视化配置方式对多种来源的数据进行数据人工治理，支持内置数据标准化的解析规则和灵活的自定义解析规则。包括：过滤、解析与标准化、关联补齐、打标签等。对相关安全数据进行业务数据价值挖掘，对业务数据标签化处理。对安全数据数据资产进行业务标签配置，可以新增和删除标签，每类数据资源可以设置多种标签，可根据业务标签对安全数据资源进行检索筛选。在主题库建设的过程中，存在大量需要人工维护（添加，修改，删除）的信息。此类数据主要是在数据清洗和数据比对过程中产生的大量需要进行人工判断、维护的数据。服务单位需要对这些数据进行人工维护，与相关部门进行对接沟通，将问题数据反馈到相关部门，确定每条数据的处理方案，数据处理方案确定后，由人工进行处理，人工处理方式包括但不限于字段补全、数值修改等，相关人工处理需要进行记录。 |

## 5.系统对接

|  |  |
| --- | --- |
| 安全系统对接 | 与浙江省政务外网安全监管平台系统对接 |
| 与台州市委网信办的网络安全协调指挥平台对接 |
| 安全数据采集 | 支持Kafka\Api\Syslog等多种采集方式。支持对接不同的安全数据源。  支持多元异构日志数据采集,基于现有的安全系统，包括但不限于政务终端安全管理系统、日志审计系统、县市区安全风险数据、政务云安全、漏洞扫描、边界安全等系统采集的数据  数据采集过程中，针对不同厂商、不同系统、不同标准的源数据，对接相关厂商，按照既定的安全数据规范设置不同的解析规则，定义不同的数据字段标准化规则，添加不同的业务属性信息，并输出至安全数据采集模块，实现数据标准化采集。 |

**（六）其他要求**

## 1.项目进度要求

合同签订后 90 天内完成台州市政务外网安全运营平台建设并上线试运行，试运行

3个月后通过项目竣工验收。

供应商应按照上述时间安排，制定相应的项目实施详细进度计划，确定每个实施阶段的时间表及工作目标。

## 2.项目组织及实施要求

2.1供应商中标后需要在台州市大数据发展管理局成立工作团队，向采购人提供项目管理人员和技术人员配置情况，并指定一名专职的项目经理，负责项目协调和调度工作。除项目经理外，项目组须配备专职的技术负责人，并按照项目实施的要求，配置相应的项目管理、系统设计、开发、测试、集成、培训、质量保证等人员。

2.2本项目分为建设期服务及运维服务，实施阶段要求按照项目实施进展合理安排驻场服务，要求供应商明确各分项建设内容实施阶段的人员驻场安排，项目经理要求在项目建设各阶段在现场开展相关工作，并保证一定的到场率。

2.3项目小组团队成员在实施各阶段至少安排6人进驻现场开展各项工作，并在验收后提供不少于2人2年驻场服务的驻场服务。

在项目建设与运维过程中，供应商应严格遵守并落实采购人制定的网络和数据安全管理制度。

2.4参与此项目的技术人员必须具有承担过相同类型项目实施的经验，能够与用户进行良好的沟通，掌握相关领域的相关基础知识，具备相关应用和开发的能力。

2.5供应商在项目合同签订后，需组织相关实施人员在该项目招标需求的基础上进行深入调研，编制需求规格说明书。需求规格说明经采购人、供应商确认后作为项目验收的依据。

2.6要求供应商在各阶段及时提供相应的项目管理文档、开发类文档及实施类文档，以便采购人及时了解项目进展情况。

2.7对上述安排供应商应列出详细实施方案，包括但不限于项目管理计划、项目服务流程、项目实施流程、项目进度计划、项目验收计划、项目组织结构（人员姓名、经验、学历和在本项目中的职责分工等，项目小组成员须提供社保证明）等。

2.8本方案对项目提出的主要需求，是供应商编制投标文件和报价的主要依据，但不应作为编制正式实施方案的完整的详细要求。在编制正式的项目建设实施方案和详细设计时，供应商应深入分析和充分考虑采购人对本项目现在及未来发展的需求，设计出完整的优质方案。方案中要体现开放接口，便于系统功能的扩充和完善。

2.9中标后供应商所作的详细设计应完全满足用户的需求。

2.10安全保密要求。本次项目要求供应商建立可行的安全保密措施，提供对本项目的保密承诺，实施过程中接触的所有秘密，包括(但不限于)技术方案、过程文档及其他资料，无论是书面的、口头的、图形的、电磁的、光介质的或其他任何形式的信息，包括(但不限于)数据、模型、样品、草案、技术、方法、仪器设备和其他信息，同时承诺不向任何第三方透漏。为保障相关数据及应用安全，将在遵循国家相关法律法规的基础上，严格遵守台州市关于数据安全和保密的要求。

## 3.安装、测试及系统集成要求

3.1负责本项目范围内应用软件的现场安装部署、集成、测试和调试，保证系统功能、性能要求的实现，提供售后服务。同时负责对应用于该项目的软硬件设备的系统集成。在安装、配置和测试、调试过程中，供应商应对最终用户技术人员所提出的技术问题，给予满意的答复。

3.2要求有完整的安装和配置程序，具有详细的系统安装、部署及配置说明手册、用户使用说明书和系统维护说明书。系统实际安装与操作必须与说明书描述一致。

3.3要求具有完整的系统测试计划，包括根据用户需求编写的测试用例，合理的测试方案和测试方法。要求保留完整的测试报告。

3.4项目实施过程中，如果牵涉到与第三方产品集成工作，供应商应与系统集成商及其他供应商通力合作，并提供必要的技术支持。

3.5供应商负责解决系统建设中全部技术问题，对用户单位项目建设中碰到的其他技术问题，有责任和义务提供咨询和帮助。

## 4.售后服务要求

4.1供应商应保证对本项目提供3年的质量保证期。

4.2在保修期内由于系统本身质量原因造成的软硬件故障，供应商须做好系统运维工作。

4.3质量保证期自项目正式验收合格之日开始计算。由于本项目的特殊性（必须满足业务7\*24小时不间断工作），质量保证期内，在接到系统故障通知后，供应商必须在15分钟内响应。对于影响平台系统正常运行的严重故障，供应商工程师及其它相关技术人员必须在在接到故障通知后2小时内赶到现场，查找原因，提出解决方案，并工作直至故障修妥完全恢复正常服务为止，一般要求保证系统在4小时之内修复，并需要提供确保承诺实现的措施。

4.4为保证系统正常、安全地运行，技术支持力量和优良的服务是系统正常、安全运行的保障。供应商应据此制定系统详细的技术支持与服务方案，包括服务内容、服务方式、服务响应时间、应急措施及组织结构等。

4.5供应商须做出无推诿承诺。即供应商应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，并在得到采购人通知后，立即派工程师到场，全力协助系统集成商和其他供应商，使系统尽快恢复正常。

4.6保质期内因系统本身缺陷造成各种故障应由供应商免费技术服务和维修。系统保质期内故障时间不得超过5天，如达不到要求，每超过一天，质保期相应延长10天。

4.7在质量保证期结束前，须由供应商工程师和采购人代表进行一次全面检查，任何缺陷必须由供应商负责修改。在修改之后，供应商应将缺陷原因、修改内容、完成修改及恢复正常的时间和日期等报告给采购人。

4.8质量保证期结束后，供应商应保证以优惠价格优先对采购人进行系统技术支持和维护。

## 5.等保及第三方测评

系统定级为等保三级，供应商有义务作好等保测评配合工作，并对测评过程中出现的问题或缺陷进行整改，直至通过第三方安全等保测评。

平台要根据信创的需求进行适配，新建设的系统要求满足信创环境部署需求。新建系统要求适配信创终端，满足信创终端和非信创终端访问的需求。系统不单独采购信创硬件设备，相关安全系统采用软件化部署，应用系统部署在台州市政务云平台，通过现有的资源服务，满足应用部署需求。

本项目还需要进行商用密码应用安全性评估（简称“密评”），在采用商用密码技术、产品和服务集成建设过程中，对其密码应用的合规性、正确性、有效性进行评估。测评要参照《商用密码应用安全性评估管理办法（试行）》、《信息安全等级保护商用密码管理办法》《信息系统密码测评要求》等办法，邀请具有密评资质的第三方测评单位进行测评。

项目验收前，系统须由第三方评测机构对系统功能、性能和密评测试，供应商有义务作好配合工作，并对测试过程中出现的问题或缺陷进行整改，直至通过第三方测评。

## 6.软件版权要求

6.1本项目所采购的软硬件产品。供应商须保证采购人及其用户对供应商所提供的软硬件产品享有合法的使用权。供应商就本项目所使用软硬件产品，保证其合法性。

6.2供应商须保证采购人及其用户单位在使用过程中不受到第三方关于侵犯专利权等知识产权的指控。任何第三方如果提出指控，供应商须与第三方交涉并承担可能发生的一切法律责任和费用。

6.3供应商在项目定制化开发过程中取得的专利、软件著作权与采购人共同所有。

6.4源代码定制开发部分，源代码版权属于采购人。

6.5 系统运行中所产生的数据，所有权归业主所有。

## 7.培训要求

在项目进行的过程中，供应商需要对用户提供全面的培训。根据业务分工特性，可以将培训分为以下三类：

7.1日常操作培训

面向市大数据发展中心、县（市）区大数据管理部门、市级部门主管信息化的处室。负责管理平台的相关工作人员，主要是政务外网安全运营平台操作培训。由具有丰富经验的培训师主讲，对工作人员进行系统的操作培训，配以实际操作的指导，并提供全部详细的培训资料，保证工作人员可以迅速并正确掌握相关系统的使用。

7.2系统管理培训

各级平台的管理员需要对相关系统进行配置、对用户进行管理、对流程进行设置，需要面对更加负责的操作，因此需要针对性的培训，主要包括以下四个方面：

7.2.1系统日常维护培训。对安全运营平台管理人员进行系统的日常维护培训，包括对微小系统故障的排除等。保证系统运行的可靠性及持续性。在系统扩展时，也提供对系统管理人员的后续培训。

7.2.2系统相关技术培训。对安全运营平台管理人员进行相关技术的培训，包括安全数据采集、安全事件处理、安全数据分析和数据治理等相关技术的培训，有利于系统管理人员对系统的日常维护。避免管理操作不当引起的系统故障。

7.2.3系统架构培训。除了进行普通系统操作培训外，还进一步向系统管理人员介绍安全运营平台总体设计及其各部分之间的关系，使系统管理人员全面地了解安全运营平台，以便为其他用户提供技术支持。

7.2.4系统二次开发培训。对系统管理人员进行系统二次开发的培训，以利于系统功能的扩展及完善。

7.3高级技术培训

对部分高级用户进行系统中关键功能（安全数据分析）培训，使用户对功能及其相关技术有深入的掌握，了解功能在本系统中所处的位置和起到的作用，从而对系统架构有更深层次的理解，使这些系统能够发挥出最大的效益。

## 8.交付要求

供应商应按照招标文件所约定的内容和时间进行交付。按照计算机软件工程规范国家标准分阶段交付应用系统的文档，所交付的文档与文件应该是电子版式及纸质形式。交付的文档包括但不限于：需求规格说明书、概要设计说明书、详细设计说明书、数据库设计说明书、项目测试方案、项目测试报告、用户操作手册、管理与维护手册、安装部署手册、总结报告及采购人认为需要的其他材料。

## 9.项目验收要求

项目的验收包括初步验收、试运行和竣工验收，验收相关费用由供应商承担。

9.1项目初验

项目初验前，供应商应首先对系统进行自测，并将系统自测报告提交甲方和监理方审查。供应商依本合同约定向采购人提交成果及相关文档，并向采购人提出初验申请。采购人接到供应商初验申请后，组织相关单位进行初验，初验合格后联合签署初验报告。

9.2试运行

初验合格后，系统进入试运行，试运行时间为3个月。

9.3竣工验收

系统通过试运行后，供应商向采购人提出竣工验收（即终验）申请，采购人组织相关单位进行系统的终验。系统终验通过，进入正式运行阶段。系统终验收合格的条件必须至少满足以下三个要求：已提供了合同要求的全部设备、软件和资料，试运行时性能满足合同要求，性能测试和试运行验收时出现的问题已被解决。

1. **报价要求**

投标报价：包括需求调研、开发设计、系统集成、测试、实施部署、培训、维护、税费、密评（1年）、等保测评（1年）等费用，即一直到整个系统调试验收合格交付业主使用，采购人不再另行支付费用。

供应商在总报价基础上按采购清单的各子系统分别报价，采购人在今后系统扩展需增加建设时，若采购供应商子系统内容，供应商不得超过本次投标报价。

**11.演示**

投标人应提前做好演示准备（包括演示设备）。投标人需依照安全数据运营功能、安全数据共享功能、安全数据综合分析功能三个部分内容提供真实系统的操作录屏，配有人员讲解。录屏总时长不超过20分钟（录屏文件需通过“政采云视频讲标系统”进行线上实时在线播放，播放结束后发至公共交易中心指定邮箱）。PPT、图片演示的，不得分。

**三、商务需求**

**（一）维保期：**免费维保期至少\_3\_年（产品技术需求栏中有特别注明的除外）。

**（二）服务时间及地点：**

1、项目工期：自签订合同之日起\_90\_个天内完成项目建设。

2、交货地点：台州市大数据发展中心。

**（三）付款条件：**合同签订后20个工作日内预付合同款项的40％（需提供预付款保函），初验合格后20个工作日内支付合同款项的40％,验收合格后20个工作日内支付合同款项的20％。

**（四）履约保证金：**合同签订前，中标人应先缴纳合同总金额1%的履约保证金，合同期满无违约情形的，将在15个工作日内退还。（供应商以电汇、转账、或者金融机构、担保机构出具的保函等形式提交履约保证金，注明用途为“履约保证金”。）

1. **评标**

**一、评标原则**

（一）评标活动遵循公平、公正、科学和择优的原则，以招标文件和投标文件为评标的基本依据，并按照招标文件规定的评标方法和评标标准进行评标。

（二）任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员应不带任何倾向性和启发性，不得向外界透露任何与评标有关的内容，不得私下与投标人接触。

**二、评标方法**

综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

**三、评标委员会**

（一）本项目评标委员会由采购人代表和评审专家组成。

（二）评标委员会成员与参与投标的供应商有下列情形之一的，应当回避：

1.参加采购活动前3年内与供应商存在劳动关系；

2.参加采购活动前3年内担任供应商的董事、监事；

3.参加采购活动前3年内是供应商的控股股东或者实际控制人；

4.与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

5.与供应商有其他可能影响政府采购活动公平、公正进行的关系；

6.法律法规规定的其他情形。

（三）评标委员会负责具体评标事务，并独立履行下列职责：

1.审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

2.要求投标人对投标文件有关事项作出澄清或者说明；

3.对投标文件进行比较和评价；

4.确定中标候选人名单，以及根据采购人委托直接确定中标人；

5.向采购人、采购组织机构或者有关部门报告评标中发现的违法行为；

6.法律法规规定的其他职责。

**四、无效标情形**

（一）在资格证明文件或商务与技术文件中出现投标报价的，或者报价文件中报价的服务跟商务与技术文件中的投标服务出现重大偏差的；

（二）不具备招标文件中规定的资格要求的；

（三）投标文件含有采购人不能接受的附加条件的；

（四）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，投标人在限定的时间内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）报价超过招标文件中规定的预算金额/最高限价或未填写投标报价的；

（六）主要性能参数指标负偏离 8 项（含）以上的；

（七）投标参数未如实填写，完全复制粘贴招标参数的；

（八）投标文件存在虚假材料的；

（九）有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。

（十）实质性要求（招标文件中打“▲”内容）不响应的；

（十一）商务条款不响应的；

（十二）投标文件有效期不足的；

（十三）逾期或未按要求提交投标文件的；

（十四）未按要求提供资格证明文件的；

（十五）其他不符合法律法规相关规定的。

**五、废标情形**

（一）出现影响采购公正的违法、违规行为的；

（二）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；

（三）因重大变故，采购任务取消的；

（四）法律、法规和招标文件规定的其他导致评标结果无效的。

**六、评标过程的监控**

本项目评标过程实行全程录音、录像监控，政府采购监管部门视情进行现场监督，投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

**七、政府采购政策落实**

**（一）政府采购政策：**

1.关于小型、微型企业（简称小微企业）投标：小微企业投标是指符合《中小企业划型标准规定》的投标人，通过投标提供本企业制造的货物、承担的工程或者服务，或者提供其他小微企业制造的货物。本项所指货物不包括使用大、中型企业注册商标的货物。小微企业投标应提供、《中小企业声明函》（见附件14），投标人未提供以上资料或者经评标委员会核查不符的，将不能享受相应的小微企业优惠政策。

2.监狱企业参加政府采购活动时，应当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证明文件，视同小型、微型企业，享受小微企业政府采购优惠政策。

3.残疾人福利性单位在参加政府采购活动时，应提供《残疾人福利性单位声明函》（见附件14），视同小型、微型企业，享受小微企业政府采购优惠政策。

**（二）政府采购政策优惠措施：**

经主管预算单位统筹后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：对小微企业报价给予10%-20%的扣除，用扣除后的价格计算评标基准价和投标报价。联合体各方均为小微企业的，联合体视同为小微企业，对报价给予10%-20%的扣除；联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对报价给予4%-6%的价格扣除，用扣除后的价格计算评标基准价和响应报价。同一投标人（包括联合体），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。

**八、评标程序**

**（一）资格审查**

投标文件解密后，采购人或采购组织机构依法对投标人的资格进行审查，对审查发现无效的进行必要的询问，在政采云平台公布无效投标的投标人名单、投标无效的原因。

|  |  |
| --- | --- |
| 具有独立承担民事责任的能力 | 在中华人民共和国境内注册的法人或其他组织或自然人，投标时提交有效的营业执照（或事业法人登记证或身份证等相关证明）扫描件，法定代表人委托办理招标事宜的请提交授权委托书（根据附件2-1《授权委托书》填报）。 |
| 具有良好的商业信誉和健全的财务会计制度 | 提供具有良好的商业信誉和健全的财务会计制度的承诺函。 |
| 履行合同所必需的设备和专业技术能力 | 按投标文件格式填报设备及专业技术能力情况（根据附件4《投标人基本情况表》和附件6《项目实施人员一览表》填报）。 |
| 有依法缴纳税收和社会保障资金的良好记录 | 提供没有税收缴纳、社会保障等方面的失信记录的承诺函。 |
| 参加采购活动前3年内，在经营活动中没有重大违法记录 | 参加本次采购活动前3年内，在经营活动中没有重大违法记录（根据附件1《投标声明书》）。 |
| 信用记录 | 1.截止时点：开标后评标前。  2.信用信息查询记录和证据留存的具体方式：由采购组织机构在规定查询时间内打印信用信息查询记录并归入项目档案。  3.使用规则：投标人未被列入“信用中国”失信被执行人或重大税收违法案件当事人名单；未处于“中国政府采购网”政府采购严重违法失信行为信息记录中的禁止参加政府采购活动期间 |
| 必须符合法律、行政法规规定的其他条件 | 1.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，不得同时参加本项目投标。  2.为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参与本项目投标。  3.投标（报价）文件相关承诺要求内容。 |
| 联合体投标 | 1.若以联合体形式投标，请提交联合体授权委托书（根据附件2-2《联合体授权委托书》填报），并载明联合体各方承担的工作和义务（根据附件3 《联合体共同投标协议书》填报）。  2.若以联合体形式投标，联合体各方均须满足上方条款，并提供相应承诺或说明。 |
| 落实政府采购政策需满足的资格要求 | 根据实际情形设置。 |

**（二）符合性审查**

评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求，对审查发现无效的进行必要的询问，在政采云平台公布无效投标的投标人名单、投标无效的原因。

|  |  |
| --- | --- |
| “▲”实质性条款 | “▲”实质性条款必须满足招标文件要求。 |
| 串通投标 | 未出现财政部87号令《政府采购货物和服务招标投标管理办法》第三十七条规定的串通投标情形。 |
| 附加条件 | 投标文件未含有采购人不可接受的附加条件。 |

**（三）商务技术及价格评审**

**1.评分标准**

本项目评标方法为综合评分法，总计100分，评标按以下标准及要求进行：

|  |  |  |  |
| --- | --- | --- | --- |
| **评分项目** | **评分细则** | | **分值** |
| 技术响应  63分 | 根据投标文件响应招标文件的程度进行评分：基础分20分，参数负偏离1项扣1分；招标文件中标“★”的条款，负偏离1项扣2分，扣完为止。（注：主要性能参数指标负偏离 8 项（含）以上的，投标无效） | | 20 |
| 总体建设方案 | 根据投标人对采购人案需求的理解、提供的项目实现思路、体系构架、功能模块等进行综合打分：  ①对项目的实现思路、体系架构齐全，包含了招标需求中的全部内容，对具体的实施方案作出了详细、准确的阐述，且项目方案贴合实际的，得4-5分；  ②对项目的实现思路、体系架构较齐全，包含了招标需求中的大部分内容，对具体的实施方案作出了详细、准确的阐述，但方案没有针对项目的实际情况的，得2.1-3.9分；  ③对项目的实现思路、体系架构只包含了招标需求中的部分内容，实施方案不明确，没有针对实际情况的，得0-2分；  ④未提及此项的不得分。 | 5 |
| 建设方案 | 根据投标人提供的安全数据运营方面的建设方案是否能满足采购需求进行打分：  ①方案逻辑清晰、完整详实、可操作性强，得4-5分；  ②方案合理、内容常规、操作性一般的得2.1-3.9分；  ③方案粗糙、内容缺漏、操作性差的得1.1-2分。  ④方案差的得1-0分，未提及此项的不得分。 | 5 |
| 根据投标人提供的安全数据共享方面的建设方案是否能满足采购需求进行打分：  ①方案逻辑清晰、完整详实、可操作性强，得4-5分；  ②方案合理、内容常规、操作性一般的得2.1-3.9分；  ③方案粗糙、内容缺漏、操作性差的得1.1-2分。  ④方案差的得1-0分，未提及此项的不得分。 | 5 |
| 根据投标人提供的网络安全数据综合分析方面的建设方案是否能满足采购需求进行打分：  ①方案逻辑清晰、完整详实、可操作性强，得3.1-4分；  ②方案合理、内容常规、操作性一般的得2.1-3分；  ③方案粗糙、内容缺漏、操作性差的得1.1-2分。  ④方案差的得1-0分，未提及此项的不得分。 | 4 |
| 根据投标人提供得项目建设方案，综合评估以上3个系统对接方案得合理性、耦合性等方面否能满足采购需求：  ①方案逻辑清晰、完整详实、可操作性强，得2.1-3分；  ②方案合理、内容常规、操作性一般的得1.1-2分；  ③方案粗糙、内容缺漏、操作性差的得0-1分。  ④未提及此项的不得分。 | 3 |
| 根据投标人提供安全数据仓存储方案，从独立性、先进性、合理性等方面由专家判定是能否足采购需求:  ①方案逻辑清晰、完整详实、可操作性强，得2.1-3分；  ②方案合理、内容常规、操作性一般的得1.1-2分；  ③方案粗糙、内容缺漏、操作性差的得0-1分。  ④无方案无措施的不得分。 | 3 |
| 根据投标人提供得项目建设方案，综合评估本项目数据归集方案能否满足采购需求：  ①方案逻辑清晰、完整详实、可操作性强，得2.1-3分；  ②方案合理、内容常规、操作性一般的得1.1-2分；  ③方案粗糙、内容缺漏、操作性差的得0-1分。  ④未提及此项的不得分。 | 3 |
| 产品演示 | 安全数据运营功能演示：  1.支持灵活自定义编排威胁的响应处置流程，并支持多种执行节点包括：动作调度、剧本应用、决策器、过滤器、人工审批、人工录入、并行分支等必要的关键节点（1分）；  2.支持结合用户工单流转情况进行统一展示，包括工单总数、流转中、超时工单、已结束工单、已撤销工单等（1分）；  3.支持针对用户安全运营业务流程，可进行图形化的方式进行自定义工单流程（至少包含录入节点和审批节点），并可以根据业务不同内容进行工单的自定义；具备灵活的表单配置能力（1分）。  4.支持基于运营管理过程的流程工单闭环情况，进行对应评分的记分统计，包括工单完成情况、待处理超时工单等维度；  5.支持通过浙政钉（或钉钉）进行业务通知告警（1分）。  上述5项中每一项功能点完全实现的，每项得1分；部分实现的，每项得0-0.5，不能实现的不得分。 | 5 |
| 安全数据共享功能演示：  1.支持元数据版本管理，记录元数据历史版本、差异比较（1分）；  2. 演示异构数据库（无目的表的情况下）自动建表能力（1分）；  3.具演示多种条件组合查询数据表的能力，查询条件包括但不限于目录名称、数据表名、数据表描述、业务标签、创建者、大小等（1分）；  4. 演示数据全链路血缘的能力；展示细粒度的数据血缘关系，包括不限于数据表级、字段级数据血缘关系展示（1分）；  5. 演示数据标准清洗能力，集成提供去除空白、空值过滤、全角半角转换、正则校验、长度校验、去重等清洗能力，并支持规则自定义，支持配置问题数据处理方式（1分）。  上述5项中每一项功能点完全实现的，每项得1分；部分实现的，每项得0-0.5，不能实现的不得分。 | 5 |
| 安全数据综合分析功能演示：  1．支持安全事件详情总览，包括安全事件名称，安全事件等级、数据源、处置状态、告警举证数、资产IP、事件描述等（1分）；  2.支持通过安全事件详情查看攻击故事线。安全事件按照攻击入口和进程树的视角进行安全分析。可详细点开进程链中任意进程查看进程详情。（1分）；  3.支持以时间轴视角，对风险资产上的终端及网络告警进行关联，同时支持向前、向后进行全局调查，展现内网影响面分析。（2分）  4.自动化提取安全事件中需要响应处置的“IP、域名、主机、进程、文件”等信息，可查看相关威胁情报、同时针对精准威胁可开启失陷实体自动遏制。（1分）  上述4项中第1、2、4项：每一项功能点完全实现的，每项得1分；部分实现的，每项得0-0.5，不能实现的不得分。  第3项：每一项功能点完全实现的，每项得2分；部分实现的，每项得0-1，不能实现的不得分。 | 5 |
| **实力信誉与售后服务**  **15分** | 项目经理及团队成员 | 评估本项目实施团队的人员质量、数量及合理性情况进行综合评分，团队质量高，完全招标文件要求的，得2.1-3分；团队合理，基本满足招标文件要求的，得1.1-2分；团队质量差，得0.1-1分。  注：需提供该人员在投标人处近三个月的社保证明及相关证书扫描件证明，不提供或提供不全的不得分。 | 3 |
| 资质资信 | 根据投标人的专业资质认证情况进行评分：  1.投标人为国家信息安全漏洞共享平台CNVD用户组成员得1分；  2. 投标人具备ITSS 信息技术服务运行维护体系认证证书，一级得2分，二级得1分，其他不得分；  3. 具备国家信息安全测评信息安全服务资质证书（安全运营类一级）要求的得1分；  4.具备大数据服务能力评估数据工程专项认证证书，三级及以上得2分，二级得1分，其他不得分。  5.具备国家互联网应急响应中心网络安全应急服务国家级支撑单位证书得1分。  注：提供相关证书复印件并加盖投标人单位公章，证书获得日期须在本项目招标公告发布日期之前，否则不得分。 | 7 |
| 软著 | 投标人取得相关领域软件著作权证书，且证书名称中包含以下关键词之一的：“数据治理”、“数据采集”、“数据标准”、“数据可视化”、“数据安全”。每具有一项上述证书得1分，最多得4分。同一证书只计一次，不得重复计分；不同证书具有相同的关键字，只算为一项满足，计1分。  注：提供相关证书扫描件并加盖投标人单位公章，证书获得日期须在本项目招标公告发布日期之前，否则不得分。 | 4 |
| 案例 | 根据投标人提供的自2020年3月1日以来（以合同签订时间为准）类似项目建设、服务或运维的业绩情况，每提供一个得0.5分，最多可得1分。（建设、服务或运维需同时提供合同，同一合同不重复计分）  注：提供原件备查。 | 1 |
| **售后服务承诺**  **7分** | 售后服务：根据投标人提供的驻场人员，售后服务方案、售后服务承诺以及售后服务保障措施等打分：  ①人员优秀，方案完整详实、可操作性强，措施有力的，得3.1-4分；  ②方案合理、内容常规、操作性一般的得2.1-3分；  ③方案粗糙、内容缺漏、操作性差的得1.1-2分。  ④方案差的得1-0分，未提及此项的不得分。 | | 4 |
| 培训服务：综合评定投标人提供得业务培训方案：①培训时间安排科学、合理，培训课程内容完整丰富，操作性强的，得0.8-1分；②方案合理、内容常规、操作性一般的得0.4-0.7分；  ③方案粗糙、内容缺漏、操作性差的得0.1-0.3分，无不得分。 | | 1 |
| 其他优惠承诺 | 根据投标人给出的优惠条件（除价格外）和特色服务承诺进行评分： ①与本项目完全契合，具有实质性、科学性，重点突出得2分； ②与本项目契合，基本具有实质性、科学性，得1分； ③与本项目不契合，或未提供不得分。 | 2 |
| **价格**  **15分** | 以合格投标人/供应商有效总报价中的最低价为基准价，基准价为15分。报价得分＝（评标基准价/最终报价）×15%×100（小数点后保留2位小数）。（注：对于小型和微型企业产品的价格给予20%的扣除，用扣除后的价格参与评审。) | | 15 |

**注**：①请扫描上传合同、证书、报告及其他相关证明材料的原件扫描件至投标文件，并加盖公章。

②原件备查，采购机构在项目评审直至合同签订、履约期间，有权要求投标人出具投标文件中的合同、证书、报告及其他相关证明材料，予以确认其的真实性和有效性，如出现与事实不符等情况，将根据有关规定以“提供虚假材料谋取中标（成交）”予以处理。

**2.评审要求**

（1）评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件的商务部分和技术部分进行综合比较与评价，其中客观评分项的分值应当一致。

（2）对于投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

①“政采云平台”上开启的投标报价与电子投标文件中开标一览表（报价表）内容不一致的，以电子投标文件中开标一览表（报价表）为准；

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

③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。修正应当采用询标的形式，并加盖公章。

（3）对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或者补正。

（4）投标人的澄清、说明或者补正采用书面形式，并加盖公章或者由法定代表人或授权代表签字，且不得超出投标文件的范围或者改变投标文件的实质性内容。

**（四）结果汇总及排序**

评标结果按评审后综合得分由高到低顺序排列。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并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

**（五）评标报告撰写**

评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。

**第五章 拟签订的合同文本**

以下为成交后签订本项目合同的通用条款，中标人不得提出实质性的修改，关于专用条款将由采购人与中标人结合本项目具体情况协商后签订。

项目名称： 项目编号：

甲方：（采购单位） 所在地：

乙方：（中标人） 所在地：

甲、乙双方根据××(采购组织机构名称）关于××项目公开招标的结果，签署本合同。

**一、合同文件**

（一）合同条款

（二）中标通知书

（三）更正补充文件

（四）招标文件

（五）中标人投标文件

（六）其他

上述所指合同文件应认为是互相补充和解释的，但是有模棱两可或互相矛盾之处，以其所列内容顺序为准。

**二、合同内容及服务标准**

（具体见项目需求）

**三、合同金额**

本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元（￥\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元）人民币。

**四、甲乙双方责任**

（一）甲方责任

（根据招标结果确定）

（二）乙方责任

（根据招标结果确定）

**五、技术资料**

（一）乙方应按招标文件规定的时间向甲方提供有关技术资料。

（二）没有甲方事先书面同意，乙方不得将由甲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提供，也应注意保密并限于履行合同的必需范围。

**六、知识产权**

（一）乙方应保证提供服务过程中不会侵犯任何第三方的知识产权。

（二）若侵犯，由乙方赔偿甲方因此遭受的损失（包括但不限于应对及追偿过程中所支付的律师费、差旅费、诉讼费、保全费、鉴定费、评估费等）。

**七、履约保证金**

本项目履约保证金为合同金额的\_\_\_\_%。[合同签订前交至采购人处，服务期满 年后及时退还]

**八、转包或分包**

（一）本合同范围的服务，应由乙方直接供应，不得转让他人供应。

（二）除非得到甲方的书面同意，乙方不得将本合同范围的服务全部或部分分包给他人供应。

（三）如有转让和未经甲方同意的分包行为，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

**九、服务期 (选用)**

（一）服务期 年。（自合同签订之日起计）

**十、合同履行时间、履行方式及履行地点**

（一）履行时间：

（二）履行方式：

（三）履行地点：

**十一、款项支付**

付款方式：

**十二、税费**

本合同执行中相关的一切税费均由乙方负担。

**十三、质量保证及后续服务**

（一）乙方应按招标文件规定向甲方提供服务。

（二）乙方提供的服务达不到合同文件要求的，根据实际情况，经双方协商，可按以下办法处理：

1.赔偿处理；

2.解除合同。

（三）如在使用过程中发生问题，乙方在接到甲方通知后在 小时内到达甲方现场。

（四）在服务期内，乙方应对出现的质量及安全问题负责处理解决并承担一切费用。

**十四、违约责任**

（一）甲方无正当理由拒收接受服务的，甲方向乙方偿付合同款项百分之五作为违约金。

（二）甲方无故逾期验收和办理款项支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

（三）乙方未能如期提供服务的，每日向甲方支付合同款项的千分之六作为违约金。乙方超过约定日期\_\_\_\_个工作日仍不能提供服务的，甲方可解除本合同。乙方因未能如期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

**十五、不可抗力事件处理**

（一）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。

（二）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。

（三）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。

**十六、解决争议的方法**

如双方在履行合同时发生纠纷，应协商解决；协商不成时，可提请政府采购监管处调解；调解不成的通过以下第（ ）方式解决：

（一）提交台州仲裁委员会仲裁。

（二）依法向人民法院提起诉讼。

**十七、合同生效及其它**

（一）合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

（二）本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

（三）本合同一式两份。甲、乙双方各执一份。本项目未尽事宜以招标文件、投标文件及澄清文件等为准。

甲方（盖章） 乙方（盖章）

法定代表人： 法定代表人：

委托代理人： 委托代理人：

联系电话： 联系电话：

开户银行： 开户银行：

账号： 账号：

地址及邮编： 地址及邮编：

签订时间： 年 月 日

**第六章 投标文件格式**

项目名称

项目编号：（标项）

投

标

文

件

（**资格证明文件）**

投标人全称（公章）：

地 址：

时 间：

**资格证明文件目录**

1. 投标声明书（附件1）
2. 授权委托书或联合体授权委托书（法定代表人办理投标事宜的，则无需提交授权委托书；以联合体形式投标时需提供联合体授权委托书）（附件2-1、附件2-2）
3. 联合体共同投标协议书（以联合体形式投标时需提供）（附件3）
4. 法人或者其他组织的营业执照等证明文件，自然人的身份证明
5. 符合参与政府采购活动的资格条件并且没有税收缴纳、社会保障等方面的失信记录的承诺函
6. 具备履行合同所必需的设备和专业技术能力的证明材料
7. 本项目要求的特定资质证书

**附件1**

**投标声明书**

台州市政府采购中心：

（投标人名称）系中华人民共和国合法企业，经营地址。

我（ 姓名 ）系（ 投标人名称 ）的法定代表人，我公司自愿参加贵方组织的（招标项目名称）（编号为）的投标，为此，我公司就本次投标有关事项郑重声明如下：

1. 我公司声明截止投标时间近三年以来：未被列入失信被执行人、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，以及不存在其他不符合《中华人民共和国政府采购法》第二十二条规定的条件【说明：投标人在截止投标时间近三年以来，如有上述所列情形，但限制期届满的，可按实陈述，并提供相应证明文件】。
2. 我公司在参与投标前已详细审查了招标文件和所有相关资料，我方完全知悉并认为此招标文件没有倾向性，也没有存在排斥潜在投标人的内容，我方对招标文件的所有内容没有任何异议，不申请澄清和质疑。
3. 我公司不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。
4. 我公司保证，采购人在中华人民共和国境内使用我公司投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任由我方承担。我方的投标报价已包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。
5. 我公司严格履行政府采购合同，不降低合同约定的产品质量和服务，不擅自变更、中止、终止合同，或拒绝履行合同义务。
6. 以上事项如有虚假或隐瞒，我公司愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

投标人名称（公章）：

法定代表人或授权委托人签字：

日期：××年 ×× 月 ×× 日

**附件2-1**

**授权委托书**

台州市政府采购中心：

（投标人全称） 法定代表人（或营业执照中单位负责人） （法定代表人或营业执照中单位负责人姓名） 授权 （全权代表姓名） 为全权代表，参加贵单位组织的 项目的采购活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对全权代表的签字事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。全权代表在授权委托书有效期内签署的所有文件不因授权的撤销而失效。

全权代表无转委托权，特此委托。

法定代表人签字或盖章：

投标人全称（公章）： 日期：

**附：**

|  |
| --- |
| **法定代表身份证** |

法定代表人姓名：

传真：

电话：

详细通讯地址：

邮政编码：

|  |
| --- |
| **全权代表身份证** |

全权代表姓名：

职务：

传真：

电话：

详细通讯地址：

邮政编码：

**附件2-2**

**联合体授权委托书**

台州市政府采购中心：

（联合体牵头人公司全称） 法定代表人（或营业执照中单位负责人）、 （联合体成员1公司全称） 法定代表人（或营业执照中单位负责人）、（联合体成员2公司全称） 法定代表人（或营业执照中单位负责人） 组成的联合体，现共同授权 （全权代表姓名） 为全权代表，参加贵单位组织的 （项目名称） （项目编号： ）的采购活动，并代表我方全权办理针对上述项目的投标、开标、评标、签约等具体事务和签署相关文件。我方对全权代表的签字事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。全权代表在授权委托书有效期内签署的所有文件不因授权的撤销而失效。

全权代表无转委托权，特此委托。

联合体牵头人全称（公章）：

法定代表人签字或盖章：

联合体成员1全称（公章）：

法定代表人签字或盖章：

日期：

**附：**

|  |
| --- |
| **法定代表身份证** |

联合体牵头人法定代表人姓名：

传真：

电话：

详细通讯地址：

邮政编码：

|  |
| --- |
| **法定代表身份证** |

联合体成员1法定代表人姓名：

传真：

电话：

详细通讯地址：

邮政编码：

|  |
| --- |
| **全权代表身份证** |

全权代表姓名：

职务：

传真：

电话：

详细通讯地址：

邮政编码：

**附件3**

**联合体共同投标协议书**

（联合体所有成员名称） 自愿组成联合体，以一个投标人的身份共同参加贵单位组织的 （项目名称） （项目编号： ）的投标。现就联合体投标事宜订立如下协议：

1. （某联合体成员名称） 为联合体的牵头人。
2. 联合体牵头人合法代表联合体各成员，负责本采购项目投标文件编制和合同谈判活动，并代表联合体提交和接受相关的资料、信息及指示，并处理与之有关的一切事物，负责合同实施阶段的主办、组织和协调工作。
3. 联合体将严格按照招标文件的各项要求，递交投标文件，履行合同，并对外承担连带责任。
4. 本次联合投标中，分工如下：（联合体牵头人名称）承担的工作和义务为： ；（联合体成员1名称）承担的工作和义务为： 。 ……
5. 本次联合投标中，各方对于分享项目成果和知识产权的约定为：

。

1. 各方具体的责任、权利、义务，在中标后经各方协商后报采购人同意后在合同中明确。
2. 联合体各方不得再以自己的名义参加本项目的投标。联合投标的项目负责人不能作为其他联合体或单独投标单位的项目组成员。因发生上述问题导致联合体投标无效的，联合体的其他成员可追求违约行为。
3. 未中标，本协议自动废止。

联合体牵头人名称（盖单位公章或电子签章）：

法定代表人（签字）：

联合体成员1名称（盖单位公章或电子签章）：

法定代表人（签字）：

签订日期： 年 月 日

（注：联合体各方成员应在本协议上共同盖章，不得分别签署协议书）

项目名称

项目编号：（标项）

投

标

文

件

（商务与技术文件**）**

投标人全称（公章）：

地 址：

时 间：

**商务与技术文件目录**

**第一部分 技术方案描述部分**

1. 投标人情况介绍（附件4）
2. 项目需求的理解与分析
3. 总体设计（技术、服务）方案
4. 功能设计方案
5. 质量保证方案
6. 项目实施方案
7. 项目分包方案
8. 技术需求响应表（附件5）
9. 项目实施人员一览表（附件6）
10. 工程量/原材料、人工费清单（均不含报价）
11. 项目负责人资格情况表（附件7）
12. 安装、调试及验收方案（包括项目验收标准和验收方法等）
13. 实施服务与保障的能力及方案（包括服务方式、服务网点、技术培训、实施期与运维期服务的内容和措施等）（附件8）
14. 投标人需要说明的其他内容（包括可能影响投标人技术性能评分项的各类证明材料）

**第二部分 商务响应及其他部分**

1. 证书一览表（附件9）
2. 近三年来类似项目的成功案例（附件10）
3. 商务需求响应表（附件11）

**附件4**

**投标人基本情况表**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 企业名称 |  | | | | | | 法人代表 | | |  | |
| 地址 |  | | | | | | 企业性质 | | |  | |
| 股东姓名 |  | 股权结构（%） | |  | | | 股东关系 | | |  | |
| 联系人姓名 |  | 固定电话 | |  | | | 传真 | | |  | |
| 手机 | |  | | |
| 1.  企  业  概  况 | 职工人数 |  | | 具备大专以上学历人数 |  | | 国家授予技术职称人数 | | |  | |
| 占地面积 |  | | 建筑面积 | 平方米  □自有  □租赁 | | 生产经营场所及场所的设施与设备 | | |  | |
| 注册资金 |  | | 注册发证机关 |  | | | | | 公司成立时间 |  |
| 核准经营范围 |  | | | | | | | | | |
| 发展历程及主要荣誉： | | | | | | | | | | |
| 2．  企业有关资质获证情况 | 企业获得其他资质认证情况 | | 资质名称 | | | 发证机关 | | 编号 | 发证时间 | | 期限 |
|  | | |  | |  |  | |  |
| 企业获得专利情况 | |  | | | | | | | | |

**要求：**

1.姓名栏必须将所有股东都统计在内，若非股份公司此行（第三行）无需填写。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件5**

**技术需求响应表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **招标参数** | **投标参数** | **偏离说明** | **备注** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**要求：**

1. 本表的名称须与《报价明细表》一致。

2.本表参照本招标文件第二部分“招标需求”内第二条“具体技术需求”填制，投标人应根据投标设备的性能指标、服务指标，对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

3.对于所投服务的技术偏离情况需严格按照招标文件的技术要求一一比对给出，未达到技术要求中规定的数值应以负偏离标注。若因技术实现方式等其他问题而导致的理解不同未标注负偏离的，需在备注中具体说明；若未按要求标注负偏离又未予以说明的，评标委员会将视偏离程度给予扣分或认定为虚假应标。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件6**

**项目实施人员一览表**

（主要从业人员及其技术资格）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **职务** | **职责** | **专业技术资格** | **证书编号** | **参加本单位工作时间** | **劳动合同编号** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**要求：**

1.在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

2.附人员证书。

　　3.出具上述人员在本单位服务的外部证明，如：投标截止日之前六个月以内的代缴个税税单、参加社会保险的《投保单》或《社会保险参保人员证明》等。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件7**

**项目负责人资格情况表**

|  |  |  |
| --- | --- | --- |
| **姓名** |  | **近年来主要工作业绩** |
| **性别** |  | 注：业绩证明应提供旁证材料  （供货合同或中标通知书）。 |
| **年龄** |  |
| **职称** |  |
| **毕业时间** |  |
| **学校专业** |  |
| **联系电话** |  |
| **最近一年工作状况** |  |
| **拟在本项目中担任主要工作** |  | |

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件8**

**服务实施情况表（视情制作）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **投标人承诺** | **备注** |
| 1 | 服务实施期内服务情况(服务方式、服务的内容和措施等等，可用附页和宣传材料)。 | 生产厂商售后服务情况： |  |
| 投标人售后服务情况： |  |
| 2 | 运维期服务情况(服务方式、服务网点、服务的内容和措施等等，可用附页和宣传材料)。 |  |  |
| 3 | 培训方案（可用附页）。 |  |  |
| …… | …… |  |  |

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件9**

**证书一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **证书名称** | **发证单位** | **证书等级** | **证书有效期** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**要求：**

1.填写投标人获得资质、认证或企业信誉证书。

2.附所列证书或其他证明材料。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件10**

**投标人类似项目实施情况一览表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **项目地址** | **合同总价** | **实施时间** | **项目质量** | **项目单位名称及其联系人电话** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**要求：**

1.业绩证明应提供证明材料（合同可只提供首页、含金额页、盖章页并加盖投标人公章）。

2.投标人可按此表格式复制。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件11**

**商务需求响应表(第 标)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **内容** | **招标需求** | **是否响应** | **投标人的承诺或说明** |
|  | 维保期 |  |  |  |
|  | 服务时间及地点 |  |  |  |
|  | 付款条件 |  |  |  |
|  | 备品备件及耗材等要求 |  |  |  |
|  | …… |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

项目名称

项目编号：（标项）

报

价

文

件

投标人全称（公章）：

地 址：

时 间：

**报价文件目录**

1.开标一览表（附件12）

2.报价明细表（附件13）

3.中小企业声明函、残疾人福利性单位声明函（附件14）

4.针对报价投标人认为其他需要说明的

**附件12**

**开标一览表**

**项目编号：**

**项目名称：** [货币单位：人民币元]

|  |  |  |
| --- | --- | --- |
| 投标总报价 | 大写 |  |
| 小写 |  |

**填报要求：**投标报价包括本项目采购需求和投入使用的所有费用，包括但不限于主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件13**

**报价明细表**

**项目编号：**

**项目名称：** [货币单位：人民币元]

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **报价名称（成本组成内容）** | **小计** | **备注** |
| 1 | 安全数据运营系统 |  |  |
| 2 | 安全数据共享系统 |  |  |
| 3 | 网络安全综合分析服务 |  |  |
| 4 | 网络安全数据规范治理 |  |  |
| 5 | 对接服务 |  |  |
| 6 | 等保测评 |  |  |
| 7 | 密评 |  |  |
| 8 | 运维驻场 |  |  |
| 9 | ...... |  |  |
| **合计人民币：大写 小写** | | | |

**要求：**

1.本表为《开标一览表》的报价明细表，如有缺项、漏项，视为投标报价中已包含相关费用，采购人无需另外支付任何费用。

2.“报价明细表”中的报价合计应与“开标一览表”中的投标总报价相一致，不一致时，以开标一览表为准。

投标人名称（公章）：

投标人代表签字：

职 务：

日 期：

**附件14**

**中小企业声明函**

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，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（招标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①，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（招标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。

信息查询网址为：

企业名称（盖章）：

日 期：

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本声明函将随中标结果公开，接受社会监督。

**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 台州市政府采购中心 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。

单位名称（盖章）：

日 期 ：