**淳安县全链路网络安全监管平台（一期）建设采购项目**

**（电子招投标）**

编号: ZJCGZF[2021]149号

**招**

**标**

**文**

**件**

采购单位：淳安县人民政府办公室

代理机构：浙江辰光管理有限公司

二〇二一年十二月日

|  |  |
| --- | --- |
| 采购单位确认（公章）：  该采购文件已经我单位审核确认。  经办人（签名）：  日期：2021年12月日 | 代理机构审批（章）：  同意发布。  经办人（签名）：  日期：2021年12月日 |

目录

[第一部分招标公告](#__RefHeading___Toc13852)

[第二部分投标人须知](#__RefHeading___Toc28522)

[第三部分采购需求](#__RefHeading___Toc2895)

[第四部分评标方法及评分标准](#__RefHeading___Toc2910)

[第五部分拟签订的合同文本](#__RefHeading___Toc20075)

[第六部分应提交的有关格式范例](#__RefHeading___Toc16456)

**第一部分招标公告**

浙江辰光管理有限公司作为分散采购代理机构（以下简称代理机构）受淳安县人民政府办公室（以下称：采购单位）的委托，就淳安县全链路网络安全监管平台（一期）建设采购项目发布招标公告邀请符合条件的供应商参加投标**（电子招投标）**。具体如下：

1. **招标编号**：ZJCGZF[2021]149号

**2、项目名称：**淳安县全链路网络安全监管平台（一期）建设采购项目

**3、采购方式：公开招标**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 标项 | 项目名称 | 采购内容 | 单位 | 数量 | 预算总价(元) |
| 1 | 淳安县全链路网络安全监管平台（一期）建设采购项目 | 新建全链路一屏可视化展现模块，完成“云、网、端、边界、数据、应用”全链路网络安全监管平台的开发建设。 | 项 | 1 | 2000000.00 |

**4、采购人的采购需求：**详见招标文件。

**5、投标人的资格要求：**

**（1）基本条件：符合《中华人民共和国政府采购法》第二十二条第一款的规定；**

**（2）落实政府采购政策需满足的资格要求：无。**

**（3）特定条件：无。**

**6、本项目不接受联合体投标。**

**7、获取招标文件的时间期限、地点、方式及招标文件售价：**

（1）时间期限：发布至投标截止时；

（2）地点：**政采云平台（<https://www.zcygov.cn/>）**；

**（3）方式：使用账号登录或者使用CA登录政采云平台；进入“项目采购”应用，在获取采购文件菜单中选择项目，获取采购文件。（注册账号--点击“商家入驻”，进行政府采购供应商资料填写；申领CA数字证书--申领流程详见“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”。）**

（4）售价：免费

（5）供应商获取招标文件时须提交的文件资料：无；

（6）提示：**1）采购人、采购机构将依托政采云平台完成本项目的电子交易活动，平台不接受未按上述方式获取招标文件的供应商进行投标活动；**

2）对未按上述方式获取招标文件的供应商对该文件提出的质疑，采购人或采购代理机构将不予处理；

3）不提供招标文件纸质版。

4）获取招标文件的时间期限截止之日之后有潜在供应商提出获取招标文件的，采购机构将允许其获取，但该供应商如对招标文件有异议的，应于自采购文件公告期限届满之日起七个工作日内且在投标截止时间之前以书面形式向采购机构提出。

**8、投标截止时间与地点：**2022年01月20日上午09时30分00秒，地点：政采云平台。

**9、开标时间与地点：**2022年01月20日上午09时30分00秒，地点：淳安县千岛湖镇新安大街104号4楼综合财务室上5楼电子评标室，通过“政府采购云平台（https://www.zcygov.cn/）”实行在线开标。

**10、投标保证金：**本项目不需要交纳投标保证金。

**11、电子招投标的说明**

**（1）电子招投标：**本项目以数据电文形式，依托“政府采购云平台（www.zcygov.cn）”进行招投标活动，不接受纸质投标文件。

**（2）投标准备：**注册账号--点击“商家入驻”，进行政府采购供应商资料填写；申领CA数字证书---申领流程详见“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”；安装“政采云电子交易客户端”----前往“浙江政府采购网-下载专区-电子交易客户端”进行下载并安装。

**（3）招标文件的获取：**使用账号登录或者使用CA登录政采云平台；进入“项目采购”应用，在获取采购文件菜单中选择项目，获取招标文件。

**（4）投标文件的制作：**在“政采云电子交易客户端”中完成“填写基本信息”、“导入投标文件”、“标书关联”、“标书检查”、“电子签名”、“生成电子标书”等操作。

**（5）投标文件的传输递交：**投标人在投标截止时间前将加密的投标文件上传至政府采购云平台，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份。备份投标文的制作、存储、密封详见招标文件第二部分第15点—“备份投标文件”。

**（6）投标文件的解密：**投标人按照平台提示和招标文件的规定在半小时内完成在线解密。通过“政府采购云平台”上传递交的投标文件无法按时解密，投标供应商递交了备份投标文件的，以备份投标文件为依据，否则视为投标文件撤回。通过“政府采购云平台”上传递交的投标文件已按时解密的，备份投标文件自动失效。投标人仅提交备份投标文件，没有在电子交易平台传输递交投标文件的，投标无效。

**（7）具体操作指南**：详见政采云平台“服务中心-帮助文档-项目采购-操作流程-电子招投标-政府采购项目电子交易管理操作指南-供应商”。

**（8）政府采购云平台技术咨询电话**：400-881-7190。

**12、采购人、采购机构等：**

采购单位：淳安县人民政府办公室；

项目经办人：童伟传 联系电话：0571-65060036

质疑联系人：方友军 联系电话：0571-64813735

地址：淳安县千岛湖镇

代理机构：浙江辰光管理有限公司

联系人:高文峰联系电话：0571-64813937

质疑接收人：童国民联系电话：0571-64814245

地址：淳安县千岛湖镇新安大街104号

同级政府采购监督管理部门名称：淳安县财政局

联系人：方建宏监督投诉电话：0571-64818305

地址：淳安县千岛湖环湖北路695号

**13、本项目采购文件公告期限为：**本公告发布之日起五个工作日。

二○二一年十二月十四日**第二部分投标人须知**

前附表

| **序号** | **事项** | **本项目的特别规定** |
| --- | --- | --- |
| 1 | **报价要求** | 有关本项目服务所需的所有与项目实施有关的费用均计入报价。《投标（开标）一览表》是报价的唯一载体。投标文件中价格全部采用人民币报价。招标文件未列明，而投标人认为必需的费用也需列入报价。  **提醒：投标报价出现下列情形的，投标无效：**  **▲投标文件出现不是唯一的、有选择性投标报价的；**  **▲投标报价高于本项目采购预算或者最高限价的;**  **▲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质量或者不能诚信履约的，未能按要求提供书面说明或者提交相关证明材料，不能证明其报价合理性的;**  **▲《投标（开标）一览表》填写不完整或字迹不能辨认或有漏项的；**  **▲投标人对根据修正原则修正后的报价不确认的。** |
| 2 | **分包或转包。** | （1）采购人**不同意**分包。  （2）本项目不得转包。 |
| 3 | **投标人应当提供的资格、资信证明文件** | （1）资格证明文件：见招标文件第二部分11.1。  （2）资信证明文件：根据招标文件第四部分具体评标标准提供。  ▲**投标人未提供有效的资格证明文件的，视为投标人不具备招标文件中规定的资格要求，视投标无效。** |
| 4 | **开标前答疑会或现场考察** | 不组织。 |
| 5 | **样品提供** | 无 |
| 6 | **方案讲解演示** | **有方案讲解演示：有（方案演示20分钟内） 疫情期间：各投标单位演示视频请采用加密文件格式（不接受现场演示），与备份投标文件一起密封包装邮寄至代理公司。快件务必在投标截止时间前送达到招标代理公司指定接收人员处（确保开标前收到，合理安排时间），演示开始前，代理公司人员将联系供应商进行解密。收件地址：淳安县千岛湖镇新安大街104号4楼采购代理部 ，李梦0571-64813937。** |
| 7 | **是否适宜中小企业情况** | 无 |
| 8 | **中小企业信用融资** | 根据《杭州市政府采购支持中小企业信用融资管理办法》等规定，淳安县财政局与中国建设银行股份有限公司淳安支行、杭州银行股份有限公司淳安支行、中国工商银行股份有限公司淳安支行等银行签订了《政府采购支持中小企业信用融资合作备忘录》，本采购项目中标人与采购单位签订的政府采购合同适用于政府采购贷款政策，简称“政采贷”。 |
| 9 | **项目实施地点** | 淳安县行政范围内； |
| 10 | **采购服务费** | 采购服务费按照国家发展计划委员会计价格[2002]1980 号文《招标代理服务费管理暂行办法》及发改办价格[2003]857号文的收费标准计取。采购服务费为人民币￥23000.00元,由中标单位支付给采购代理公司。  收款单位（户名）：浙江辰光管理有限公司  开户行：中国工商银行淳安县支行  账号：  120 202 910 900 671 7573 |

**一、总则**

**1. 适用范围**

本招标文件适用于该项目的招标、投标、开标、资格审查及信用信息查询、评标、定标、合同、验收等行为（法律、法规另有规定的，从其规定）。

**2. 定义**

2.1 “采购人”系指招标公告中载明的本项目的采购人。

2.2 “采购机构”系指招标公告中载明的本项目的采购机构。

2.3 “投标人”系指是指响应招标、参加投标竞争的法人、其他组织或者自然人。

2.4 “负责人”系指法人企业的法定负责人，或其他组织为法律、行政法规规定代表单位行使职权的主要负责人，或自然人本人。

2.5“电子签名”系指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

2.6“电子交易平台”是指本项目政府采购活动所依托的政府采购云平台（https://www.zcygov.cn/）。

2.7 “▲”系指实质性要求条款，“★”系产品采购项目中单一产品或核心产品。

**3.采购项目需要落实的政府采购政策**

3.1 本项目原则上采购本国生产的货物、工程和服务，不允许采购进口产品。除非采购人采购进口产品，已经在采购活动开始前向财政部门提出申请并获得财政部门审核同意，且在采购需求中明确规定可以采购进口产品（但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人、采购机构不会对其加以限制，仍将按照公平竞争原则实施采购）。

3.2 节能环保要求

3.2.1采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。投标人须按招标文件要求提供相关产品认证证书。

3.2.2▲采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人未按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，投标无效。

**3.3支持中小企业发展。**

**3.3.1中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。**

**符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。**

**3.3.2在政府采购活动中，投标人提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：**

**（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；**

**（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；**

**（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。**

**在货物采购项目中，投标人提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。**

**以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。**

**3.3.3对于未预留份额专门面向中小企业的政府采购货物或服务项目，以及预留份额政府采购货物或服务项目中的非预留部分标项，对小型和微型企业的投标报价给予10 %的扣除，用扣除后的价格参与评审。**

**3.3.4接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购货物或服务项目，对于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，对联合体或者大中型企业的报价给予3%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。**

**3.3.5符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件）的残疾人福利性单位视同小型、微型企业；**

**3.3.6符合《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）规定的监狱企业并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证明文件的，视同为小型、微型企业。**

**3.3.7可享受中小企业扶持政策的投标人应按照招标文件格式要求提供《中小企业声明函》。**

**3.3.8中小企业享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。**

**3.4中小企业信用融资：根据《杭州市政府采购支持中小企业信用融资管理办法》等规定，淳安县财政局与中国建设银行股份有限公司淳安支行、杭州银行股份有限公司淳安支行、中国工商银行股份有限公司淳安支行等银行签订了《政府采购支持中小企业信用融资合作备忘录》，本采购项目中标人与采购单位签订的政府采购合同适用于政府采购贷款政策，简称“政采贷”。**

**4. 询问、质疑、投诉**

4.1供应商询问

供应商可以就采购文件中特定资格条件、采购需求、评分办法及采购过程中有关现场考察或开标前答疑会事项向采购人提出询问，采购人将对此作出答复；供应商可以就采购活动中的其它事项向采购机构提出询问，采购机构将对此作出答复。答复的内容不得涉及商业秘密。

4.2供应商质疑

4.2.1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。潜在供应商已依法获取其可质疑的采购文件的，可以对该文件提出质疑。

4.2.2供应商认为采购文件、采购过程和成交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日起七个工作日内，以书面形式向采购人或者采购机构提出质疑，否则，采购人或者采购机构不予受理：

（1）对采购文件提出质疑的，质疑期限为供应商获得采购文件之日或者采购文件公告期限届满之日起计算。采购文件在获取截止之日后获得的，应当自采购文件公告期限届满之日起计算，且应当在采购响应截止时间之前提出。对采购文件中特定资格条件、采购需求、评分办法提出的质疑，原则上由采购人负责答复；对采购文件中其他内容提出的质疑，原则上由采购机构负责答复。

（2）对采购过程提出质疑的，质疑期限为各采购程序环节结束之日起计算。对同一采购程序环节的质疑，供应商须一次性提出。对采购过程中有关现场考察或开标前答疑会事项提出的质疑，原则上由采购人负责答复；对采购过程中其它事项提出的质疑，原则上由采购机构负责答复。

（3）对采购结果提出质疑的，质疑期限自采购结果公告期限届满之日起计算。对采购结果提出质疑的，采购机构负责答复。

4.2.3供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

4.2.3.1供应商的姓名或者名称、地址、邮编、联系人及联系电话；

4.2.3.2质疑项目的名称、编号；

4.2.3.3具体、明确的质疑事项和与质疑事项相关的请求；

4.2.3.4事实依据；

4.2.3.5必要的法律依据；

4.2.3.6提出质疑的日期。

供应商提交的质疑函需一式三份。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。

质疑函范本及制作说明详见附件2。

4.2.4采购人或者采购机构应当在收到供应商的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他与质疑处理结果有利害关系的政府采购当事人，但答复的内容不得涉及商业秘密。

4.2.5询问或者质疑事项可能影响采购结果的，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。

4.3供应商投诉

4.3.1质疑供应商对采购人、采购机构的答复不满意或者采购人、采购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提出投诉。

4.3.2供应商投诉的事项不得超出已质疑事项的范围，基于质疑答复内容提出的投诉事项除外。

4.3.3供应商投诉应当有明确的请求和必要的证明材料。

4.3.5 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。

投诉书范本及制作说明详见附件3。

**二、招标文件的构成、澄清、修改**

**5．招标文件的构成**

5.1招标文件包括下列文件及附件

第一部分招标公告

第二部分投标人须知

第三部分采购需求

第四部分评标方法及评分标准

第五部分拟签订的合同文本

第六部分应提交的有关格式范例

5.2与本项目有关的澄清或者修改的内容为招标文件的组成部分。

**6. 招标文件的澄清、修改**

6.1已获取招标文件的潜在投标人，若有问题需要澄清，应于投标截止时间前，以书面形式向采购机构提出。

6.2采购机构对采购文件进行澄清或修改的，将同时通过电子交易平台通知已获取采购文件的潜在投标人。依法应当公告的，将按规定公告，同时视情况延长投标截止时间和开标时间。该澄清或者修改的内容为招标文件的组成部分。

**▲投标文件未按招标文件的澄清、修改的内容编制，又不符合实质性要求的，投标无效。**

**三、投标**

**7. 招标文件的获取**

详见招标公告中获取招标文件的时间期限、地点、方式及招标文件售价。

**8. 开标前答疑会或现场考察**

采购人组织潜在投标人现场考察或者召开开标前答疑会的，潜在投标人按前附表的规定参加现场考察或者开标前答疑会。**采购人不单独或分别组织只有一个供应商参加的现场考察和答疑会。**

**9. 投标保证金**

本项目不需要交纳投标保证金。

**10. 投标文件的语言**

投标文件及投标人与采购有关的来往通知、函件和文件均应使用中文。

**11. 投标文件的组成**

**投标文件的组成**

投标文件应当包括以下主要内容：**资格文件、报价文件、商务技术文件**。投标文件应当对招标文件提出的要求和条件作出明确响应。

11.1**资格文件**应包括以下内容（均需使用电子签名）：证明其符合《中华人民共和国政府采购法》规定的供应商基本条件和采购项目对供应商的特定条件（如果项目要求）的有关资格证明文件。**（以联合体形式进行政府采购的，参加联合体的供应商均应当提供）**

11.1.1营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，提供自然人的身份证明）；

金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构，以及个体工商户、个人独资企业、合伙企业，如果已经依法办理了工商、税务和社保登记手续，并且获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料（在投标文件中提供相关材料），证明其具备实际承担责任的能力和法定的缔结合同能力，可以独立参加政府采购活动，由单位负责人签署相关文件材料；

11.1.2 法人授权书（如法定代表人直接参加投标并对相应文件签字的，只需提供其身份证复印件正反面；如以联合体形式参加政府采购活动的，按招标文件有关格式范例提供联合体投标授权书）；▲**投标文件中法人授权书所载内容与本项目内容有异的，投标无效。**

11.1.3 授权代表的身份证（复印件）；

11.1.4 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；

11.1.5具有履行合同所必需的设备和专业技术能力的承诺函；

11.1.6参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明；

11.1.7具有良好商业信誉的特别声明；

11.1.8符合特定资格条件（如果项目要求）的有关证明材料（复印件）；

11.1.9以联合体形式投标的，提供联合体协议。

11.1.10本项目专门面向中小企业，货物全部由符合政策要求的中小企业制造，提供中小企业声明函；

11.2 投标人的**报价文件**应包括以下内容（均需使用电子签名）：

11.2.1投标响应函；

11.2.2投标(开标)一览表；

11.3 投标人的**商务技术文件应**包括以下内容（均需使用电子签名）：

11.3.1营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，须提供自然人的身份证明）；

11.3.2如以联合体形式参加政府采购活动的，联合体各方应当指定牵头人，授权其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，并应当向采购机构提交由所有联合体成员各方法定代表人签署的授权书，同时应当提交联合协议，载明联合体各方承担的工作和义务。联合体协议中应当注明由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。联合体协议中仅约定由牵头人或联合体成员中某一方与采购人签订合同的，或联合体协议中仅约定由牵头人或联合体成员中某一方就采购合同约定的事项对采购人承担责任的，视为联合体协议不成立，该联合体投标文件将被作无效投标文件处理；（**▲如以联合体形式参加政府采购活动的，联合体协议不符合招标文件规定的联合体协议要求的，投标无效。**）

11.3.3资信文件：见投标须知前附表所述；

11.3.4投标截止时间前三年投标人的主要业绩证明材料即合同和用户验收报告（联合体投标的，联合体各方分别提供与联合体协议中规定的分工内容相应的业绩证明材料，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，联合体成员各方应就所有合同约定的工作内容提供业绩证明材料，有一方未能提供全部合同约定的工作内容的业绩证明材料的，视为联合体未提供业绩证明材料；以分包方式履行政府采购合同的，还需提供其项目采购人同意分包的证明材料)；

11.3.5投标人认为需要的其他商务文件或说明；

11.3.6投标人应提供针对项目的完整技术解决方案；

针对本项目的完整技术解决方案和实施方案；详细阐述项目方案的实现思路及关键技术；符合本项目对当前和未来发展的要求；以及对功能设计和实施计划的建议；

**如果本项目涉及硬件设备采购，还需提供投标产品规格配置清单（设备名称、品牌及型号、规格配置详细说明、数量等）。所有技术指标表述均应采用中文，如当前公布的技术指标只有英文表述的，必须由投标人作出中文注释（评审时以中文注释为准）。否则任何含糊不清的表述导致评标委员会技术扣分直至认定为投标无效都将是投标人的责任**。

本项目如需采购政府强制采购的节能产品的或投标人提供的产品是环境标志产品，投标人按格式提供节能产品、环境标志产品认证证书复印件；

11.3.7投标人在投标文件技术偏离说明表中，应对采购需求中所提出各项要求进行答复、说明和解释。如果投标人在技术偏离表中注明无偏离，评标结束后、签订采购合同前又认为其实际产品与投标技术需求不一致的，并以此为由拒不与采购人按采购需求与投标承诺签订政府采购合同的，投标人有未按照采购文件确定的事项签订政府采购合同的情形，依照政府采购法第七十七条第一款的规定将被追究法律责任；

11.3.8针对本项目建设的详细实施计划。本项目详细工作实施组织方案，包括(但不限于)以下内容：组织机构、工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点；

11.3.9针对本项目的售后服务方案。项目验收之前、验收之后的维护方案；针对本项目的维护方案等。投标人应以书面形式完整准确地表述售后服务承诺(范围、标准及期限等)、投标人可能增加的服务承诺等。并明示服务承诺可能涉及的前提设定和费用，否则将被认为是无条件和免费的。承诺质保期内均提供免费上门服务；

11.3.10投标人为完成本项目组建的工作小组名单，每个专业人员的情况和人员数应该明确表示，明确各阶段投入人数，在提交的投标文件中安排的人员，须为公司的固定职员；每个参加项目人员的履历表主要内容包括学历、技术职称、工作特长、经验与业绩(包括从事相关项目的经验，对每一个项目有一个简要的描述，该人员参与的时间以及在项目中的责任)，资质情况等；

11.3.11优惠条件及特殊承诺；

11.3.12备品备件清单（含随机自带的备品备件和质保期后供采购人选择的备品备件及配套零部件，明细备品备件及价格，且供货价格不高于中标价格；中标货物设备应提供易损部件的备件和整机备品）；（如果有）

11.3.13培训计划；（如果有）

11.3.14投标人认为需要的其他技术文件或说明；

11.3.15关于对招标文件商务、合同中有关条款的拒绝声明（如果有）；

11.3.16政府采购供应商廉洁自律承诺书；

11.3.17廉政承诺书。

**▲投标文件组成漏项，内容不全或内容字迹模糊辨认不清的，投标无效；**

**▲投标文件含有采购人不能接受的附加条件的，投标无效；**

**▲投标人提供虚假材料投标的，投标无效。**

**12. 投标文件的编制**

12.1投标文件分为资格文件、商务技术文件、报价文件三部分。各投标人在编制投标文件时请按照招标文件第六部分规定的格式进行，混乱的编排导致投标文件被误读或评标委员会查找不到有效文件是投标人的风险。

**▲投标文件未按规定的格式编制的，投标无效；**

**12.2投标人进行电子投标应安装客户端软件—“政采云电子交易客户端”，并按照招标文件和电子交易平台的要求编制并加密投标文件。投标人未按规定加密的投标文件，电子交易平台将拒收并提示。**

**12.3使用“政采云电子交易客户端”需要提前申领CA数字证书，申领流程请自行前往“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”进行查阅。**

**13.投标文件的签署、盖章**

13.1投标文件按照招标文件第六部分格式要求进行签署、盖章。

**▲投标人的投标文件未按照招标文件要求签署、盖章的，其投标无效**。

**13.2为确保网上操作合法、有效和安全，投标人应当在投标截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用电子签名。**

**14. 投标文件的提交、补充、修改、撤回**

14.1 供应商应当在投标截止时间前完成投标文件的传输递交，并可以补充、修改或者撤回投标文件。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传输的，视为撤回投标文件。投标截止时间后递交的投标文件，电子交易平台将拒收。

14.2电子交易平台收到投标文件，将妥善保存并即时向供应商发出确认回执通知。在投标截止时间前，除供应商补充、修改或者撤回投标文件外，任何单位和个人不得解密或提取投标文件。

14.3采购机构可以视情况延长投标文件提交的截止时间。在上述情况下，采购机构与投标人以前在投标截止期方面的全部权利、责任和义务，将适用于延长至新的投标截止期。

**15. 备份投标文件**

15.1投标人在电子交易平台传输递交投标文件后，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份，**但采购人、采购机构不强制或变相强制投标人提交备份投标文件。**

15.2备份投标文件须在“政采云投标客户端”制作生成，并储存在U盘中。备份投标文件应当密封包装并在包装上加盖公章并注明投标项目名称，投标人名称(联合体投标的，包装物封面需注明联合体投标，并注明联合体成员各方的名称和联合体协议中约定的牵头人的名称)

**▲不符合上述制作、存储、密封规定的备份投标文件将被视为无效或者被拒绝接收。**

15.3直接提交备份投标文件的，投标人应于投标截止时间前在招标公告中载明的开标地点将备份投标文件提交给采购机构，采购机构将拒绝接受逾期送达的备份投标文件。

15.4以邮政快递方式递交备份投标文件的，投标人应先将备份投标文件按要求密封和标记，再进行邮政快递包装后邮寄。备份投标文件须在投标截止时间之前送达淳安县千岛湖镇新安大街104号4楼；送达时间以签收人签收时间为准（签收人：李梦，联系电话：0571-64813937）。采购机构将拒绝接受逾期送达的备份投标文件。邮寄过程中，电子备份投标文件发生泄露、遗失、损坏或延期送达等情况的，由投标人自行负责。

**15.5**▲**投标人仅提交备份投标文件，没有在电子交易平台传输递交投标文件的，投标无效。**

**16.投标文件的无效处理**

有招标文件第四部分第13项规定的情形之一的，投标无效。

**17.投标有效期**

17.1投标有效期为从提交投标文件的截止之日起90天。

▲**投标人的投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的，投标无效。**

17.2投标文件合格投递后，自投标截止日期起，在投标有效期内有效。

17.3在原定投标有效期满之前，如果出现特殊情况，采购机构可以以书面形式通知投标人延长投标有效期。投标人同意延长的，不得要求或被允许修改其投标文件，投标人拒绝延长的，其投标无效。

**四、开标、资格审查与信用信息查询**

**18.开标**

18.1采购机构按照招标文件规定的时间通过电子交易平台组织开标，所有投标人均应当准时在线参加。投标人不足3家的，不得开标。

18.2开标时，电子交易平台按开标时间自动提取所有投标文件。采购机构依托电子交易平台发起开始解密指令，投标人按照平台提示和招标文件的规定在半小时内完成在线解密。

18.3**投标文件未按时解密，投标人提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回。投标文件已按时解密的，备份投标文件自动失效。**

**19、资格审查**

19.1开标后，采购人或采购机构将依法对投标人的资格进行审查。

19.2采购人或采购机构依据法律法规和招标文件的规定，对投标人的基本资格条件、特定资格条件进行审查。

19.3投标人未按照招标文件要求提供与基本资格条件、特定资格条件相应的有效资格证明材料的，视为投标人不具备招标文件中规定的资格要求，其投标无效。

19.4对未通过资格审查的投标人，采购人或采购机构告知其未通过的原因。

19.5合格投标人不足3家的，不再评标。

**20、信用信息查询**

20.1信用信息查询渠道及截止时间：采购机构将通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道查询投标人投标截止时间当天的信用记录。

20.2信用信息查询记录和证据留存的具体方式：现场查询的投标人的信用记录、查询结果经确认后将与采购文件一起存档。

20.3信用信息的使用规则：经查询列入失信被执行人名单、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投标人将被拒绝参与政府采购活动。

20.4联合体信用信息查询：两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，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。

**五、评标**

**21.**评标委员会将根据招标文件和有关规定，履行评标工作职责，并按照评标方法及评分标准，全面衡量各投标人对招标文件的响应情况。对实质上响应招标文件的投标人，按照评审因素的量化指标排出推荐中标的投标人的先后顺序，并按顺序提出授标建议。**详见招标文件第四部分“评标方法及评分标准”**

**六、定标**

**22. 确定中标供应商**

采购人将自收到评审报告之日起5个工作日内通过电子交易平台在评审报告推荐的中标候选人中按顺序确定中标供应商。

**23. 中标通知与中标结果公告**

23.1自中标人确定之日起2个工作日内，采购机构通过电子交易平台向中标人发出中标通知书，向未中标人发出中标结果通知书，同时编制发布采购结果公告。采购机构也可以以纸质形式进行中标通知。

23.2中标结果公告内容包括采购人及其委托的采购机构的名称、地址、联系方式，项目名称和项目编号，中标人名称、地址和中标金额，主要中标标的名称、规格型号、数量、单价、服务要求，中标公告期限以及评审专家名单。

23.3公告期限为1个工作日。

**七、合同授予**

**24.** 合同主要条款详见第五部分拟签订的合同文本。

**25. 合同的签订**

25.1 采购人与中标人应当通过电子交易平台在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，并在规定时间内依法发布合同公告。

25.2中标人按规定的日期、时间、地点，由法定代表人或其授权代表与采购人代表签订合同。如中标人为联合体的，由联合体成员各方法定代表人或其授权代表与采购人代表签订合同。

25.3如签订合同并生效后，供应商无故拒绝或延期，除按照合同条款处理外，列入不良行为记录一次，并给予通报。

25.4中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标或者成交候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

**26. 履约保证金**

本项目不需要交纳履约保证金。

**八、电子交易活动的中止**

2**7. 电子交易活动的中止**

采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购机构可中止电子交易活动：

27.1电子交易平台发生故障而无法登录访问的；

27.2电子交易平台应用或数据库出现错误，不能进行正常操作的；

27.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

27.4病毒发作导致不能进行正常操作的；

27.5其他无法保证电子交易的公平、公正和安全的情况。

28.出现以上情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

**九、验收**

**29.验收**

29.1采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

29.2采购人可以邀请参加本项目的其他投标人或者第三方机构参与验收。参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。

29.3严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付条件挂钩。履约验收的各项资料应当存档备查。

29.4验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金。验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国合同法》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。**第三部分采购需求**

**一、建设背景**

2021年2月18日浙江省委召开全省数字化改革大会，全面部署数字化改革工作，其中提出必须坚持“系统安全观，强化政务网络安全体系”，强调三个重点：一是建立从云到端全链路的安全监测体系、防护体系，提升政务网络安全监测能力和主动防御能力；二是各市、县（市、区）、各部门要落实政务网络安全责任制，强化主体责任，加大检查、考核、通报力度；三是“构建完善数据全生命周期安全管理制度体系，落实安全主体责任，健全公共数据安全保障体系，提升数据安全防护能力，落实数据运营工作，建设政务网络和公共数据安全监测预警系统。”为贯彻落实数字化改革要求。

淳安县是杭州市全链路网络安全监管平台建设试点区县，淳安县数据资源中心（以下简称“淳安数据中心”）以此为契机，梳理现有网络安全架构，启动编制网络安全和数据安全（2021-2023）三年行动计划，加强网络安全防御的主动性和可持续性，提升网络安全防护与对抗能力，形成面向实战的安全运行机制，构建网络安全体系规划，提升网络安全规划建设的整体水平，助力淳安县数字化改革。

**二、现状描述**

杭州市数据资源管理局建设的数据安全管控平台为淳安县免费提供了子平台的部署与使用，进一步完善了市-区（县）两级一体化网络安全保障联动能力。

数据管控平台淳安子平台具备了安全数据采集和分析能力，能够对多维度的安全日志数据进行清洗和过滤，对数据进行标准化管理，同时基于SQL，提供高吞吐、高实时、高扩展、单易用的开放性数据分析能力；具备了网络安全监管监测能力，提供网络基础设施的脆弱性、外部威胁和运行情况的安全监管，及时发现安全漏洞和网络入侵行为，提高基础设施的安全可靠性；具备了数据安全监管能力，提供数据流和数据节点的建模工具，可基于建模工具构建业务应用，明确数据访问路径，实现数据流动安全监管；具备了网络安全态势感知能力，围绕网络安全提供总体网络安全态势分析。

数据管控平台淳安子平台的建设，已经完成了市-区（县）两级部门的平台数据打通，对安全事件形成工单下发处置和跟踪，形成工单处置闭环，实现可上传部分指标信息的功能。

当前淳安县数据资源中心是作为杭州市网络监管主平台的监管对象，子平台为杭州市局服务；为了能够充分利用子平台的能力，同时能够提升淳安县数据资源中心的监管职能，覆盖淳安县全域局委办、党政机关等各单位，通过淳安本地新建全链路安全监管平台，数据管控平台淳安子平台作为全链路安全监管平台的一部分整合进去，实现“云、网、端、边界、数据、应用”全链路网络安全监管。

**三、建设目标**

根据《浙江省数字化改革总体方案》和《浙江省一体化智能化公共数据平台建设方案》文件要求，围绕一体化智能化公共数据平台“四横四纵两端”总体架构，在数字化改革“1+5”、关键信息基础设施等重要节点按照“四个同步”要求下,采用预防性建设为主、检测响应为辅的思路，按照（2021-2023年）三年行动实施计划，构建覆盖淳安县云、网、端、边界、数据全链路防护、检测、预警、处置、反馈体系。三年规划如下：

**阶段一（2021年）：夯实基础，确立规则**

加强网络安全基础设施建设，淳安县数据资源中心新建全链路网络安全监管平台，无缝对接市局下发的数据管控平台淳安县子平台，新建全链路一屏可视化掌控模块，完成“云、网、端、边界、数据、应用”全链路网络安全监管平台的开发建设；加强网络安全基础设施建设，完成全链路安全监管平台部署，组建安全运营团队，以数字化改革为抓手，开展日常安全监测及运营工作，建立并逐步完善网络安全政策制度及标准，打造全网安全监测能力、预警能力、分析能力、处置能力为一体的全面治理体系。

**阶段二（2022年）：持续运营，优化提升**

加强县域网络安全人才培养，加强数据安全防护及监管能力，加强物联网感知领域安全治理能力，构建城市关键信息基础设施综合防御体系。建立联合安全监管工作，统筹协调网信办、公安等主管部门开展安全检查工作，形成工作考核机制，构建多方联动指挥体系。

**阶段三（2023年）：体系完善，迭代优化**

补齐基础设施安全能力，进一步完善县域数据安全政策制度，优化县域常态化一体化安全运营机制及工作考核机制，最终实现“看得见网络、防得住攻击、抓得住敌手、止得住危险”。

**四、建设原则**

本项目建设要着眼于用，务必达到管用、好用、实用的目标，以重点保护为原则，在方案设计中当遵循以下的原则：

**全县“一盘棋”原则**

在方案建设过程中，一要坚持全县“一盘棋”建设原则，统筹全县电子政务相关资源，统一建设、统一保护、统一监管。二要尽量利用现有的信息系统、网络基础设施、安全监控数据等，综合考虑对已有资源的共享和利用，避免重复建设和浪费。

**标准规划原则**

在方案设计和服务选择方面遵循国家以及行业内的相关标准，严格按照有关程序组织项目建设，并且建设标准符合国家及行业提出的接口规范和技术架构。根据关键信息基础设施安全保护条例征求意见、浙江省数据安全相关管理办法，结合信息系统的重要程度、业务特点，数据的重要程度、敏感程度实现不同强度的安全保护，集中资源优先保护涉及核心业务、关键信息资产的信息系统以及重要数据。

**技术先进原则**

整体方案设计立足先进技术，采用先进的系统结构、开放的体系架构，使系统在一个周期内保持技术领先水平，具备长足的发展能力，以适应未来网络技术和安全技术的发展和系统使用的科学性。

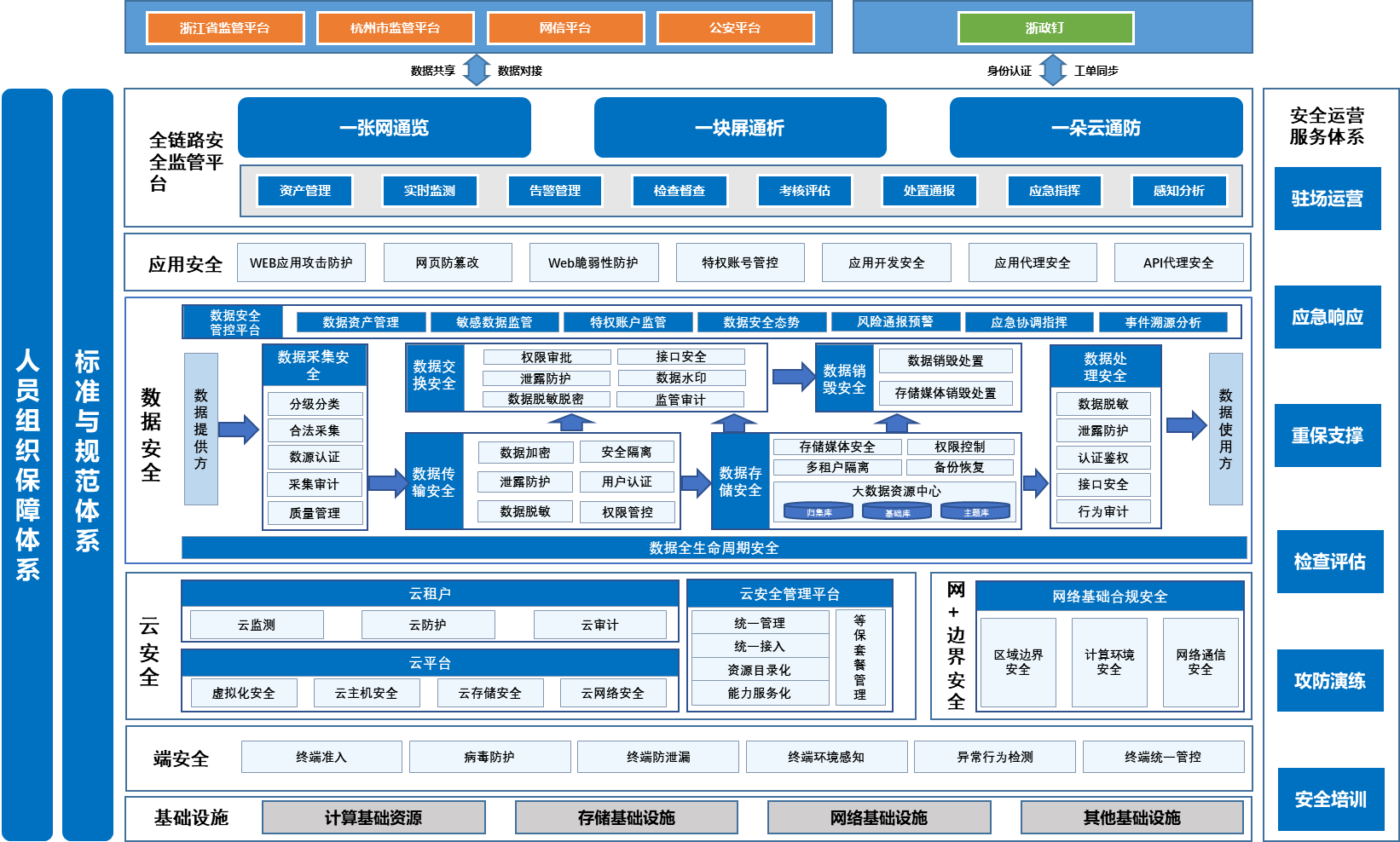
**实战实用原则**

本项目是淳安县数字化改革重要技术支撑项目，需要高质量实现全链路网络安全和数据全生命周期的实时安全监管能力，要为全县一体化智能化公共数据平台安全赋能，也要为全县数字化改革应用场景安全赋能。在管理维度和颗粒上要到边到点，要对现有的网络安全管理手段和方法进行全方位重塑。另外，本项目在服务期内需无条件免费与省市全链路网络数据安全监测平台实现无缝对接，实现向上充分兼容。

# 五、建设依据

本项目建设参考一系列国家法律法规、政策导向和省市数字化改革会议等相关要求：《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《浙江省数字政府建设“十四五”规划》、《杭州市数字政府建设“十四五”规划》、《省市两级公共数据平台建设导则（试行）》、《区县级公共数据平台建设导则（试行）》、《信息安全技术网络安全等级保护安全设计技术要求》（GB\_T 25070-2019）、《信息安全技术信息系统安全等级保护实施指南》（GB\_T 25058-2010）、《信息安全技术大数据服务安全能力要求》（GB\_T 35274-2017）。

# 总体框架设计



提供覆盖“云、网、端、边界、数据、应用”各环节网络安全纵深防护体系，汇聚挖掘全网安全风险数据、多源威胁情报数据等进行数据治理后，统一同步到全链路安全监管平台进行安全管理。全链路安全监管平台对淳安县域的政务云、网、终端、公共数据等政务信息基础设施和各类资产进行重点监测和分析，统一展示全网安全态势感知，形成全县一体化对云、网络、终端、数据、应用、边界安全监测、预警、防范、处置的闭环机制。依托大数据技术，建立安全风险感知分析能力，通过精准匹配、重点分析，提供可视化的大数据分析结果，为安全事件的研判、决策及安全重保工作提供有效支撑，加强对关键目标管控、风险识别的能力水平。并形成省、市、县纵向联动及横向与网信、公安等多部门进行安全风险联动指挥。同时全链路安全监管平台与浙政钉组织体系打通，将淳安电子政务相关各单位的责任人、管理人员及相关角色进行有效划分，安全事件、情报快速传达至相关单位处置。利用安全监管措施对安全处置流程各个阶段的安全保障工作和执行情况进行监督管理，确保安全策略在技术环节得到正确执行，相关规章制度在技术层面得到有效的支撑体现。

# 六、本期主要建设内容

**构建全链路网络安全监管平台，**加强网络安全基础设施建设，新建全链路网络安全监管平台，无缝对接浙江省大数据局、杭州市数据资管理局下发的数据管控平台淳安县子平台，新建全链路一屏可视化展现模块，完成“云、网、端、边界、数据、应用”全链路网络安全监管平台的开发建设。

**构建应用安全开发检测体系，**提供业务上云前的代码审计和渗透测试，构建源代码审计平台，通过源代码安全检测协助开发人员补齐测试能力，通过人工+自动化的方式对开发代码进行全面、深入测试，保障代码安全。通过政务业务系统上线前的安全检测确保应用安全补齐所有安全短板。防止先天代码漏洞，让后续的所有安全防护手段都丧失作用，导致数据泄露；以黑客视角进行全流程访问的攻击测试，最大限度发现目前安全建设薄弱点和入侵途径，协助运维人员整改发现的安全问题并进行安全复测。

**构建数据安全制度管理体系，**根据省市考核要求，建立健全公共数据安全制度规范体系，制定完善公共数据分类分级、访问权限、共享开放、脱敏销毁、日志审计、监督检查、安全事件应急处置、合作方及其人员管理等标准规范，指导各地各部门做好公共数据安全保障工作，促进公共数据安全管理工作标准化、流程化、规范化，使各项公共数据安全管理工作有规可依。

**构建数据安全运行管理体系，**建设部署数据安全运行管理平台与数据发现与分类分级平台，保障数据的运行环境稳定健康，提前预知隐患、问题快速定位、故障高效解决。

**构建平台整体运营服务体系，**通过专业的运营团队、配置专业安全服务，将平台运营使用起来，能够快速响应上级部门的考核与检查，也能够在安全事件发生后第一时间进行应急处置和通报。

1. **淳安县全链路安全监管平台建设**

淳安县数据资源中心建设全链路监管平台，基于当前淳安县全域一体化保障体系的现状和三年行动规划的设计，现需建设以下内容：

1. **数据采集分析模块**

数据采集分析服务用于采集覆盖淳安县全链路中的各种日志数据和安全数据，解决复杂环境下安全数据收集不全面，无法掌握整体安全状态的问题。

* + 1. **日志数据采集分析服务（日志探针）**

日志数据采集分析服务，主要采集政务云平台上部署的安全设备、系统产生的安全日志，并对日志进行解析和三维关联分析。建设全链路监管平台提供日志采集分析服务，满足三年行动规划冗余要求，便于业务扩展。

日志探针全面支持Syslog、SNMP、XML、FTP及本地文件等协议实现对各种资产进行日志采集，通过开放的标准接口，采集淳安县全链路中所有IT设施的审计日志如：操作系统、数据库、中间件、应用系统、数据库、网络设备等，形成安全数据仓，为上层应用提供分析基础。实现全维度、细粒度关联分析，内置众多的关联规则，支持网络安全攻防检测、合规性检测，及云计算租户间可轻松实现各资产间的关联分析。支持各种网络部署需要，包括日志聚合、日志过滤、事件过滤、日志转发、特殊日志格式支持(如单报文多事件)等。同时，收集通过漏扫或者其他第三方平台披露的漏洞数据，在整体平台安全运营过程中，基于资产数据对漏洞进行多维度的统计和分析，及时掌握系统内部缺陷，做到防范于未然。

* + 1. **流量数据采集分析服务（流量探针）**

当前淳安县缺少对恶意流量未知威胁的采集分析能力，本项目需部署流量数据采集分析能力探针。流量数据采集分析服务主要采集政务外网出口的流量，进行综合分析，发现流量中存在的木马、蠕虫、SQL注入、等各种威胁。

流量探针对采集数据的各类流量数据进行还原，通过对网络中流量的分析，经过关键标签索引和关联分析，可以发现网络中异常流量和异常访问，判断网络中流量访问是否存在异常，为后续事件分析处置做基础。通过流量发现等手段对网内资产的存活情况进行跟踪，一旦发现超出当前管理范围的IP，可以导出相关数据进行编辑后再录入资产数据库。而对于已经录入资产数据库的资产，可以通过分组、标记等方式对资产做更加细致的管理。

* + 1. **数据库数据采集分析服务（数据探针）**

当前已采购美创数据库审计系统，可以采集和审计政务云平台上的业务信息系统的数据库操作数据，开放提供平台标准化的API接口和现有数据安全已经建设的数据库审计、数据库运维、数据静态脱敏和数据水印等产品进行日志对接。

* + 1. **与现有安全数据源对接说明**

|  |  |
| --- | --- |
| **现有安全产品内容** | **对接要求** |
| 现有终端安全数据采集 | 对接现有终端安全管理系统，进行终端安装率、终端感染数、终端感染率和终端资产信息采集，进行统一分析监管 |
| 现有网络安全数据采集 | 支持天融信WAF、安恒WAF、思福迪SOC等网络安全设备进行对接，收集安全日志，进行统一分析监管 |
| 现有数据安全数据采集 | 支持与美创脱敏、美创防水坝等数据安全产品进行数据（数据脱敏、审计追查、访问控制等）对接，收集数据安全日志，进行统一分析监管 |

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 平台监控 | 支持监控当前接入数据的实时性能情况 |
| 支持监测数据中台节点信息以及集群的负载情况 |
| 支持监测采集器自身性能 |
| 数据接入 | 支持对当前采集器进行管理维护、以及采集器类型的统计 |
| 对每个采集器进行配置，包括SNMP Trap、文本格式日志、数据库日志、WMI日志、Netflow日志、Syslog日志的配置 |
| 数据处理 | 支持配置日志采集器的解析规则 |
| 支持统计没累采集器当前未解析的日志，并且可以查看未解析原始数据 |
| 规则管理 | 支持统计每种规则的个数，并以列表的方式展示规则，能够展示每个规则被引用的次数 |
| 支持添加编辑规则 |
| 规则能够支持正则表达式匹配、分隔符匹配、key-value匹配、json匹配 |
| 数据管理 | 支持可视化的配置页面，能够在页面上直观的验证规则是否正确 |
| 支持所有存储字段的管理维护 |
| 日志类型配置 | 支持自定义日志类型分组 |
| 支持自定义日志类型，包括存储的方式、数据保留天数，重要程度 |

1. **实时安全监测模块**

依托全链路监管平台建设数据安全和网络安全实时监测能力，实时监测整体安全情况，形成高价值的告警事件，对各类安全事件进行管理，包括形成监测任务及结果闭环。

收集平台数据采集设备集群的各类安全监测设备及策略和任务，能及时发现、识别网络攻击威胁，监测恐怖组织、黑客组织、不法份子等的攻击活动、攻击行为、攻击方法手段；监测重点保护对象所受的攻击威胁、破坏、窃密、渗透等情况，以及重点保护对象的网络、系统、大数据等安全状况、存在的漏洞、隐患等，为快速处置、通报等提供基础支撑。

实时监测对应用系统或设备提供安全监测能力，可自定义设置监测配置。包括可用性监测、脆弱性监测、篡改监测、敏感词监测、自动发现，对系统及设备进行全天后全方位监测。实时监测是建立在资产中心之上的功能模块，在建立资产基础信息后就会触发实时监测的各类除自动探测之外的监测任务。

实时监测可针对资产下发各类安全方面的监测且能将监测结果接入到系统中形成监测任务及结果的闭环，且监测任务是周期性的，保证了监测的时效性，也提供自动发现功能。监测结果更有助于安全管理人员掌握资产的安全情况，根据监测结果进行更详细的安全感知，从而处理解决安全问题，为后续处置、通报提供支撑。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 监测概况 | 支持根据时间段统计分析整体安全状况，默认统计最近一天的数据，并支持未匹配单位告警统计 |
| 支持告警各维度分析统计，维度 包括攻击结果、事件级别、告警类型、 事件类型 |
| 支持单位安全事件发生 TOP5统计 |
| 支持按照时间度段分析网络安全风险趋势，包括告警趋势、事件趋势、时间可精确到小时 |
| 支持按照数据来源统计时间周期内每种告警的数量 |
| 支持按照告警受影响资产统计涉及单位、涉及网站、涉及IP的排名情况 |
| 支持威胁来源top100分析，并可通过威胁IP下钻到具体的告警列表 |
| 支持按照单位视角统计每个单位涉及的每类告警的数量 |
| 告警列表 | 支持多种类型的漏洞发现能力，漏洞类型包括：  SQL注入, 跨站脚本攻击（XSS）, 文件包含, 代码执行, 命令执行, 文件上传, 任意文件操作, 权限绕过, 跨站请求伪造（CSRF）, 路径遍历, 配置错误, 逻辑漏洞, 弱口令, 后门, 信息泄露, 后置链接, 数字错误, 信任管理, 竞争条件, 授权问题, 代码问题, 资源管理错误, 输入验证, 缓冲区错误, 格式化字符串, 命令注入, 操作系统命令注入, 代码注入, 失效的访问控制, 访问控制错误, 加密问题, 未充分验证数据可靠性, 安全特性问题, 失效的身份认证, XML外部实体（XXE）, 不安全的反序列化, 使用含有已知漏洞的组件 |
| 支持网页漏洞利用告警发现，主要类型包括：  SQL注入, 跨站脚本攻击（XSS）, 文件写入, 文件下载, 文件上传, 文件读取, 文件包含, 弱口令, 配置不当/错误, 目录遍历, 默认配置不当, 命令执行, 敏感信息/重要文件泄漏, 逻辑/设计错误, 跨站请求伪造（CSRF）, 后门程序, 非授权访问/权限绕过, 代码执行, URL跳转, 系统/服务配置不当, WEBSHELL利用, WEBSHELL上传, 隧道, 电脑病毒, 网络蠕虫, 特洛伊木马, 窃密木马, 僵尸网络, 远控木马, 挂马, 键盘记录, 用户自定义, 间谍软件, 恶意广告, 勒索软件, 挖矿木马, 黑市工具, 流氓推广, 协议异常, 应用异常, SYN Flood, UDP Flood, ICMP Flood, ACK Flood, DNS Flood, HTTP Flood, HTTPS Flood, 溢出攻击, 浏览器劫持, 端口扫描, 网络钓鱼, 网络扫描, 暴力猜解, 高级威胁, 黑链, 内容变更, 热点钓鱼, 信息泄露, 违规内容, 访问状态异常, DNS解析异常, Webshell利用, WEB扫描, 网络爬虫, 敏感操作, Webshell上传, 代理通道, 拒绝服务, 网络欺骗 |
| 支持恶意软件的发现 |
| 支持DDOS攻击告警的发现，主要类型包括：  SYN Flood, UDP Flood, ICMP Flood, ACK Flood, DNS Response Flood, Http Flood, LAND Flood, IGMP Flood, TCP Flag NULL, TCP Flag误用, Protocol NULL Flood, Https Flood, DNS Request Flood, SIP Flood, DARK IP, PRIVATE IP, NTP REFLECTION Flood, SSDP REFLECTION Flood, SNMP REFLECTION Flood, CHARGEN REFLECTION Flood, TRAFFIC ABNORMAL, cc攻击, 拒绝服务, 协议异常, SIP-IP-Flood, SIP-ACK-Flood, SIP-SYN-Flood, SIP-Frag-Flood, SIP-UDP-Flood, SIP-ICMP-Flood, Frag-flood |
| 支持多种网络攻击的发现，主要包括：  网络欺骗, 端口扫描, 溢出攻击, 拒绝服务, 代码执行, 信息泄露, 黑市工具, SQL注入, 网络钓鱼, 恶意广告, 暴力猜解, 间谍软件, 后门程序, 浏览器劫持, 键盘记录, 窃密木马, 僵尸网络, 网络蠕虫, 电脑病毒, 协议异常, 网络扫描, WEB扫描, 应用异常, SYN Flood, UDP Flood, ICMP Flood, ACK Flood, DNS Flood, HTTP Flood, HTTPS Flood, 违规内容, 网络爬虫, 敏感操作, 代理通道, 特洛伊木马, 远控木马, 挂马, 用户自定义, 勒索软件, 挖矿木马, 流氓推广, URL跳转, 非授权访问/权限绕过, 跨站脚本攻击（XSS）, 跨站请求伪造（CSRF）, 逻辑/设计错误, 命令执行, 目录遍历, 配置不当/错误, 文件包含, 文件读取, 文件上传, 文件下载, 文件写入, 高级威胁, 黑链, 内容变更, 热点钓鱼, 弱口令, 访问状态异常, DNS解析异常, Webshell利用, Webshell上传, 隧道 |
| 支持恶意文件检测告警发现能力，主要包括：  僵尸网络, 勒索软件, 黑市工具, 远控木马, 窃密木马, 网络蠕虫, 流氓推广, 电脑病毒, 特洛伊木马, 间谍软件, 恶意广告, 挖矿木马 |

1. **综合分析模块**

依托全链路监管平台对采集的“云、网、端、边界、数据、应用”的数据进行统一综合分析，精准识别攻击和威胁，为各级指挥员和基层防御人员提供有价值的决策支撑，完善全链路网络安全监管数据多维综合分析能力。

对本项目整个安全监管功能要求来说，数据服务是基础，安全分析是核心，通报处置是目标。没有丰富完善、准确详实的数据，就无法进行准确的数据分析，从而也得不到正确的结果，无法为各级指挥员和基层防御人员提供有价值的决策支撑。没有正确的结论，就无法指导后续的通报处置。

网络攻击和威胁变得越来越复杂，安全分析方法也在随着攻击和威胁的演变而不断演进。当前已有的众多安全分析方法和手段，无法解决所有的安全问题，任何一种单一的安全分析方法只能解决某一类或某些特定的安全问题。本项目要求针对复杂的安全问题，采取多种安全分析方法进行综合分析，精准识别攻击和威胁，提供精准的溯源攻击链，协助安全运维人员快速定位到问题源头，从根本上解决安全问题。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 攻击链分析 | 分析任务管理：系统支持对溯源任务进行管理，支持溯源任务的创建、删除、任务重启等操作  分析任务创建：系统支持从任一安全事件做为线索创建分析任务  分析任务查询：系统支持对溯源任务进行查询，查询条件包括但不限于任务名称、创建者、攻击者名称、攻击IP、受害设施、受害IP  任务分析：系统支持用可视化的方式进行展示；系统支持在分析过程中人工加入攻击者或受害者线索；支持以时间轴的方式展示攻击过程；支持以攻击链阶段的方式展示攻击过程 |
| 账号安全 | 支持发现异地账号登录行为，通过流量发现非本地账户登录行为，检测SMTP、POP3、SSH、RDP、FTP、MSSQL、MYSQL、REDIS、ES、ORACLE协议，判断内网资产（目的IP :dip）是否被外网IP（源IP :sip）尝试登录过，按照源IP(sip)、目的IP(dip)，协议(proto)，账号（user），hour时间进行归并。呈现内容包括源ip、源ip归属地、账号、登录资产、协议、登录次数、登录成功率，以及通过世界地图的呈现方式展示登录IP的地域分布情况 |
| 支持发现暴力破解行为，通过流量发现暴力破解行为，在1分钟以内，按照源IP(sip)，目的IP(dip)，目的端口(dport)，协议类型(proto)，为四元组判断数值相同，连续登录失败超过100次以上，就属于暴力破解行为。呈现内容包括攻击源ip爆破次数top10统计，爆破次数时间段内的出现次数统计，爆破账号时间段内出现的次数统计，以及暴力破解行为数据，包括源ip、源ip归属地、登录资产ip、协议、目的端口、爆破次数、爆破结果、最近爆破时间等 |
| 支持发现存在弱口令的系统，通过流量检测存在弱口令的系统，测SMTP和POP3的协议的登录数据，并且只对登录成功的账号做检测。匹配内置的弱口令正则匹配，看是否命中。呈现内容包括弱口令、受影响账号、受影响资产、最近访问时间，以及通过词云的方式呈现弱口令出现的频率 |
| 行为分析 | 支持发现业务资产主动外联场景，通过TCP流量日志、UDP流量日志进行分析判断、源IP是内网IP，目的IP是外网IP，并且源IP属于业务资产的IP满足这些条件的属于业务资产主动外联，呈现内容包括外联IP、外联IP归属地、服务商、业务资产ip、流量。并以地图的方式呈现外联IP地理位置分布情况以及在地图上热力图的方式表示各外联地理位置流量的大小 |
| 支持通过机器学习模型发现DGA域名，读取dns解析日志里面的host字段，取出域名（例如： www.google.com, google.com为域名），通过机器学习模型判断该域名是DGA产生的概率，如果概率大于0.9(90%) 可以配置，则作为DGA域名。呈现内容包括源ip、请求域名、请求次数、准确率、最近访问时间等 |
| 支持发现HTTP代理，在tcp流量中发现http代理请求，判断在tcp载荷里面是否有特殊HTTP代理的特征码，如果有就是HTTP代理，呈现内容包括源ip、http代理ip、端口、使用次数、最近访问时间，以及通过词云等方式展示代理IP的出现频率 |
| 支持发现socks代理，在tcp流量中发现socks代理请求，判断在tcp载荷里面是否有特殊socks的特征码，如果有就是socks代理，呈现内容包括源IP、socks代理ip、端口、使用次数、最近访问时间，以及通过词云等方式展示代理IP的出现频率 |
| 支持发现异常DNS服务器，通过DNS解析记录发现异常内网中的异常DNS服务器，通过判断发往该DNS服务器解析的请求的主域名不超过阈值个数，则判定为异常服务器，呈现内容包括dns服务器地址、端口、响应次数、上级dns服务器地址、解析异常地址，以及通过饼状图的方式展现异常dns服务器响应次数分布情况。 |
| 支持DNS隧道发现，通过NDS解析记录发现隧道连接，请求DNS host的总长度超过50，并且子域名长度占总长度的一半以上（倒数第二个“.”以前的部分按照“.”分割成多个子域名）。同时以源IP（sip）、目的IP(dip)、根域名(host)为三元组，判断在3分钟内连续10次以上的相同数值，呈现内容包括源ip、请求地址、请求次数、最近访问时间等 |
| 支持reGeorg隧道发现，通过流量日志分析reGeorg隧道连接，判断web访问日志里面是否有命令语句符合reGeory请求特征的数据，呈现内容包括源ip、tunnel地址、最近访问时间等。 |
| 支持多种扫描工具识别，包括：  AWVS、Empire PowerShell 渗透攻击框架、SQLMap、antSword、BugScan、CaiDao、webinspect、netspark、w3af、nessus、SharinGan\_Scanner、WindowsPowerShell、WebVulnScan、masscan等 |
| 关联分析 | 新建场景分组 |
| 删除场景分组，分组内有关联任务的时候进行提示 |
| 修改场景分组的名称 |
| 新建任务，可指定任务名称、描述以及对该任务打标签 |
| 任务展示分为卡片和表格两种。展示任务名称、创建人、创建时间、标签以及任务的描述 |
| 通过任务创建时间搜索任务。点击搜索后展示过滤后的任务卡片或者列表信息 |
| 任务可选择不同的场景管理分组 |
| 点击删除，对任务进行删除，删除前有明显的提示信息 |
| 编辑任务的名称以及标签 |
| 支持块状布局、树状布局、横向树状布局、引力布局以及环状布局的五种布局模式，点击使分析任务结果按照对应的布局进行展示 |
| 设定每次返回的最大数量 |
| 点击清空画布按钮，清空当前任务分析得到的实体节点 |
| 点击将画布中的所有节点选中 |
| 点击显示名称按钮画布中分析结果实体显示对应的名称 |
| 点击显示序号按钮画图中分析结果实体显示分析顺序的序号 |
| 显示任务的整体图，鼠标拖动画图中跟随移动展示缩略图视窗中的内容 |
| 根据选择时间窗口选择查询的对应IP。时间窗口可以选预置的最近一天、最近七天、最近三十天以及自定义时间窗口选择。默认选择最近七天进行查询 |
| 根据不同的分析实体展示对应类型的详细信息 |
| 根据实体的发现时间将实体在时间轴上进行分布打点 |
| 可以将当前的分析结果保存为案例。或者将已保存的案例导入到当前的分析任务中 |

1. **处置通报模块**

目前具备市局平台通报给子平台的能力，依托全链路监管平台实现安全事件通报，满足后续三年规划的管辖颗粒度，实现覆盖局委办、乡镇等要求，真正做到安全事件落实到具体人员，做到安全处置闭环，同时能够将落实情况上报给市局平台。

根据告警管理模块获取的攻击、漏洞、风险、隐患等情况，利用处置通报模块进行汇总，并及时将情况上报、通报、下达，进行预警及快速处置。

当全链路网络安全监管平台获取到重要信息系统运营、使用单位的系统存在重大风险威胁隐患，或受到攻击、入侵、已被植入后门、篡改、植入暗链、拖库等形成重大安全事件时，根据谁使用、谁管理原则，通过平台将事件情况通过预警、通报处置等流程手段进行通报下发，业主单位反馈处置结果。

平台需具备多种方式的通报，包括浙政钉、网页等。在发生严重情况时，如突发的安全事件、重大漏洞等，可立即通过浙政钉、网页的方式进行传达；当系统监测到存在轻微的安全隐患时进行预警提醒、或限期整改等。通报完成后，通报成员单位及时的处置结果反馈。

* + 1. **通报预警机制**

将发现到的各类中高危漏洞、数据库脆弱性等安全风险通过通报预警模块快速下发到各委办局单位及相关负责人，各局委办负责人可快速查看本单位存在的风险。当爆发重大漏洞时也可以通过预警功能对各区域、各单位进行安全预警，督促相关单位修复安全隐患，避免安全隐患成为安全事件。

* + 1. **工单处置机制**

平台可通过工单处理流程，对发现的高危漏洞和事件，进行工单下发处置，处置任务的内容包括任务名称、事件描述、事件类型、事件级别、发现时间、涉及单位、单位联系人、单位联系人电话等。对下发的工单进行跟踪，负责人对工单的处理过程及结果进行记录，实现对整个工作处理过程进行跟踪，形成工单处置闭环，对逾期未处置的进行提醒。

还可以支持对扫描发现的资产弱点、告警事件等一键生成工单，使其进入工单处理流程。

另外处置通报已和浙政钉完成对接，跟浙政钉的对接方式按照《浙政钉2.0应用上架迁移流程》进行申请上线。

**从用户维度上，本项目需支持接收省市级工单，以及县级下达到乡镇、部门的工单管理功能，实现省、市、县、乡镇四级一体化互联互通能力。**

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 安全事件分析 | 支持通过单位视角展示漏洞事件、网站可用性事件、网站篡改事件、网页仿冒事件、威胁情报事件、攻击利用事件、恶意软件事件、拒绝服务攻击事件数量统计列表 |
| 支持对选择确定单位后统计该单位下各类资产的安全事件分布（按事件类型进行统计），并可下钻查看各类安全事件详情 |
| 支持对确认的安全事件进行忽略处理；并可通过单位名称、行业进行单位检索，查看对应单位的忽略数据，并进行安全事件忽略数据的恢复操作 |
| 日常通报 | 支持对待需要处理的安全事件可选择进行通报，通报类型包括：隐患告知、限期整改、行政处罚，可配置通报时间、处理时限、系统自动附带《网络安全隐患告知书》《网络安全检测报告》《网络安全整改报告》 |
| 支持对于通报反馈情况、整改情况及处罚情况的跟踪和记录 |
| 应能够通过移动端应用、短信、邮件方式提醒被通报单位的相关责任人及时受理及处置 |
| 综合通报 | 支持根据用户设置的各类通报模板，按照指定的周期完成对于指定行业、单位、行政区域的网络安全综合数据分析，并形成通报文件 |
| 支持通过手工方式导出通报文件利用其他方式完成专项分析通报 |
| 支持配置以周、月、季、年为维度生成综合通报，具备启用/停用功能 |
| 通报预警移动端应用 | 移动端应用应能支持本地部署，且各项应用可根据需要支持相应的数据钻取 |
| 应能够接入态势感知组织机构基础数据和重保单位基础数据，并支持分级管理、分权管理、人员属性管理、可见性设置等功能 |
| 专项通报 | 支持针对多个通报主体的专项通报任务，任务类型支持体检类、综合类，能够设置任务名称，任务时间，模板选择，监控类别、重点监控单位 |
| 任务模板支持行业/区域视角报告、单位视角报告 |
| 公开预警 | 支持创建公开预警，能够设置预警来源、预警名称、预警等级、风险评级、标签、预警时间，支持pdf格式附件上传 |
| 预警等级支持红色、橙色、黄色、蓝色四级 |
| 风险评级支持危急、高危、中危、低危四级 |

1. **资产管理模块**

依托全链路监管平台梳理“云、网、端、边界、数据、应用”多维度资产，实现一屏通管的需求，形成本地资产知识图谱。

“云、网、端、边界、数据、应用”多维度资产一屏通管作为淳安县全域的数据来源，需要明确资产的种类、数量以及位置，才能明确安全防护的对象及后续安全策略的制定。

**网络资产管理：**按照浙政钉规范形成单位组织架构树，通过对接获取包括主机、云平台基础设施、安全设备、网络设备等数据，形成网络资产目录，进行统一的管理。

**数据资产管理：**按照浙政钉规范形成单位组织架构树，通过平台对接明确数据在哪里、敏感数据存在哪里、敏感数据有多少，形成数据资产地图。

**应用资产管理：**应用资产管理模块可通过对接数据安全支撑平台同步用户的应用服务，对用户的应用服务、接口进行统一梳理。对应用服务的流量和日志进行监测，对接口访问进行统计，结合业务规则对高频的访问行为进行及时的告警。

**物联感知网管理：**通过物联感知网安全支撑平台同步感知网中的物联网终端厂商品牌、设备类型、操作系统类型、协议、平台等信息，根据识别的资产建立设备指纹库，实现资产智能检索和资产统计。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 资产概况 | 支持资产总量及资产分类数量统计，支持待明确资产统计以及下级单位上报资产数量统计 |
| 支持未知资产发现趋势统计，包括流量发现、下级单位上报 |
| 支持软件资产类型分布统计 |
| 支持设备资产类型分布统计 |
| 支持按照单位、区域进行资产分布统计 |
| 资产发现 | 支持未知资产导出 |
| 支持未知资产二次运营后形成本地资产库 |
| 资产管理 | 支持对单位信息按地区、统计和筛选 |
| 支持按列表的方式统计展示单位信息，展示信息包括单位名称、单位简称、地区、网络数量、业务系统数量、IP数量、监管单位、主管单位、标签 |
| 能够对单位资源按单位名称、单位简称、标签字段进行查询 |
| 能够对单位资源进行添加、批量删除、导入、导出 |
| 支持按软件资产、硬件资产、IP资产分类展示资产信息，支持资产数据的批量导入、导出 |
| 支持资产自定分类 |
| 一键搜索 | 支持输入关键字对资产数据进行一键搜索，一次最多支持查询10个词组 |
| 支持显示历史检索条件 |
| 支持检索结果以资产实体的形式呈现 |

1. **告警管理模块**

依托全链路监管平台，实现考量云平台局委办租户的个性化告警管理、一屏通览的要求，打通数据分析和通报机制，确保平台租户环境安全。

* + 1. **告警事件对接服务**

可将监测发现的漏洞或安全隐患及时将情况上报到全链路网络安全监管平台，经过预处理之后的安全数据以结构化的形式分布式存储在系统大数据库中，对外提供数据查询与统计服务，从而实现海量数据检索与挖掘。

平台支持对安全告警的分类检索。支持数据搜索输入框，可输入关键字包括不限于设备IP、日志发生时间、原始信息等进行检索；支持输入时间段、表达式等条件进行检索；支持快速选项卡检索；可指定多个查询条件进行组合查询；搜索结果以列表方式实现清晰展示，可在前端页面直接导出检索结果。

* + 1. **通报方式**

多种方式的通报，包括浙政钉、网页等。在发生严重情况时，如突发的安全事件、重大漏洞等，直接通过电话的方式进行传达；当系统监测到存在轻微的安全隐患时可通过浙政钉或网页进行预警提醒、或限期整改等。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 数据归一处理 | 能够接受数据接入的数据过滤计算任务，进行数据的过滤、归并 |
| 分布式计算 | 能够提供分布式计算资源，支持流式计算任务、批量计算任务，为数据分析提供支撑 |
| 分布式存储 | 能够提供分布式存储方式，能够快速建立数据索引，并能支持快速检索 |
| 日志检索 | 支持查询检索范围选择日志类型，类型包括：告警原始库、告警资源库、流量原始库、HIVE查询库、审计日志库； |
| 选择索引后，点击搜索语句框会下拉展示通用字段、流量通用字段，以及该索引特有字段； |
| 支持搜索条件提示字段编辑 |
| 支持多值搜索，可连续选择多字段，编辑多个胶囊 |
| 支持日志列表中字段的过滤或排除 |
| 支持lucene语句搜索，定义语句进行英文搜索语句检索数据 |
| 日志展示 | 支持在字段区域可操作字段在“已选字段”、“可选字段”间变更、展开查看字段信息 |
| 支持字段二次搜索，在原搜索基础上可以根据字段值二次搜索 |
| 支持日志内容以“键/值”、“JSON”格式展示 |
| 通报对接 | 要求通报与浙政钉进行对接，通过浙政钉通知到具体责任人进行签收反馈整改处置 |

1. **检查督查模块**

依托全链路监管平台，满足浙江省大数据发展管理电子政务安全监测相关指标要求以及浙江省一体化智能化公共数据平台建设方案当中建立全链路安全监管机制要求，实现对各委办局的检查督查。

检查督查是数据局定期开展检查工作的主要机制，主要包括现场检查、安全自查两个部分，通过线上系统管理检查工作，收集检查数据，评价检查结果。检查督查系统支持与网络安全检查工具箱实现数据对接和业务管理闭环。

检查督查形式包括现场检查和安全自查两种模式。

* + 1. **现场检查**

现场检查是由淳安县数据资源中心协同网信、公安组织技术支撑单位，制定检查计划并开展现场检查的过程，主要包括以下功能：

现场检查情况统计：现场检查模块从不同维度对工作情况进行统计说明，主要包括检查资产总数、发现的漏洞数量、年度检查的任务信息、渗透测试的情况、检查队伍评价等。

建立检查任务：提供创建检查任务的功能入口，支持创建检查任务（包括任务名称、负责人、任务时间、检查对象、任务模板、支撑队伍等信息）。

任务清单：任务创建成功后在任务清单中存档，支持任务的基本管理，编辑、删除、查询、查看详情、提交报告、评价任务情况等。

* + 1. **安全自查**

支持各单位定期自我检查并上报检查结果。检查任务由淳安县数据资源中心统一设计、安排，并经过通知系统下发自查通知。

自查统计：自查统计主要针对安全自查的工作维度进行数据统计，显示整体工作情况，主要维度包括自查任务的数量统计、自查任务的进度情况显示、自查单位数量、自查渠道提交的漏洞数量、资产数量、测试报告数量。

发布自查任务：用户可以创建自查任务，并通过通知系统通知相关单位。创建自查任务可选择检查模板、填写任务目标说明、填写任务期限、选择接受单位（行业、单位、区域）。

任务清单：任务创建成功后在任务清单中存档，能够查看单位用户自查结果提交情况及查看任务详情（包括任务基本信息以及单位提交自查状态，分两个群组，已提交自查结果的和未提交自查结果）；对已提交自查结果的单位可以点击单位名称查看、下载自查结果。

提交自查结果：系统在单位端开放自查模块，接收自查任务，自查任务提供自查清单，对自查任务可以下载检查模板，查看检查要求。完成自查工作后，可以根据模板上传自查结果。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 检查任务管理 | 支持创建检查任务，可选择多个被检查单位，检查任务类型支持 年度安全检查、专项检查、经费情况、软件正版化情况等 |
| 支持检查附件上传 |
| 支持检查任务通过浙政钉的方式发布，并可在app上下载检查附件 |
| 支持检查任务催办 |
| 分析报表 | 支持安装检查任务状态进行统计 |
| 支持检查任务填报率统计 |
| 支持检查任务催办率统计 |
| 支持检查任务按时填报率统计 |
| 网络安全检查任务 | 支持检查任务在线填报 |

1. **考核评估模块**

考核评估模块是作为淳安县数据资源管理中心对所辖各委办局等单位的重要管理措施，也是进一步提升各单位安全防范意识的重要手段。依托全链路监管平台对各单位多维的考核评价、指标质量考核，明确当前薄弱点及需重点关注加固的单位，提升淳安县全域整体安全智治。

为了有效开展网络安全防护工作，了解网络安全现状，分析存在问题，统筹指引系统通过态势分析、工作指引以及工作考评等直观展示内容为网络安全主管部门提供数据决策支持。

考核评估服务设计依据国家级和市级相关政策文件，结合网络及数据安全建设要求，建立网络及数据安全检查指标库。实现以查代促、以查促改、以查促管、以查促防，达到有效推动各级政府机关单位落实网络安全工作目标任务。

考核评估模块根据网络及数据安全检查指标库内的标准，对各类安全检查任务进行安全检查指标对比，形成统计分析、安全评价和工作质量考核。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 考核统计分析 | 支持统计每个考核任务的考核概况统计，包括考核单位数、考核任务权重、考核指标数量、最高评分、最多评分、评分top5、单项指标最低评分top5 |
| 支持按照单位过滤筛选考核任务统计页面 |
| 考核任务管理 | 支持创建考核任务，选择考核单位 、选择考核指标 ，制定考核评分上线以及各考核指标权重 |
| 支持考核模板引用保存 |
| 考核评分管理 | 支持考核评级等级分数区间自定义规则 |
| 支持考核指标的主观指标设置、自评指标设置 |
| 支持安全业务类指标的系统自动评分规则设置 |
| 支持被考核单位自评 |
| 支持考核单位对被考核单位进行主观评分 |
| 考核指标 | 支持系统内置考核指标 |
| 支持自定义考核指标 |

1. **事件案例模块**

依托全链路监管平台构建淳安县本地事件案例库，为淳安县全链路网络安全数据分析提供本地的威胁情报数据。事件案例库可以很有效的提供事件发生的类别、频率、应对方式，为所辖各单位提供了快速处置安全应急事件的方式方法。

事件案例服务用于总结已发生的攻击事件与行为，对事件发生及处置经过进行分类梳理，形成事件案例库。为后续的网络安全工作开展提供借鉴。事件案例的产生，由发现攻击行为为起点，经过关联分析、扩线分析，产生威胁分析拓扑以及攻击画像，通过专家或平台结合受攻击系统的等级情况，进行影响评价与定性，对于事件的处置进行跟踪记录，最后产生事件案例的最终说明。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 安全事件管理 | 事件列表数据呈现内容主要包括事件编号、事件标题、事件分类、上报时间、威胁程度、攻陷结果、持续时长、影响实体类型、影响范围、影响实体数量、攻击者/组织、攻击者国家、关联告警数量、利用恶意代码数量、利用漏洞数量、利用工具手段数量等。 |
| 基本信息维护包括事件编号、发现单位、事件类型、事件等级、事件描述、事件解决方案，事件的附件信息等 |
| 添加、编辑，详情功能从事件的四类信息进行维护与展示包括基本信息、受害者信息、攻击者信息、黑客能力、举证信息 |
| 基本信息维护包括事件的编号、发现单位、事件标题、上报时间、事件分类、事件发生起至时间、时段描述、事件描述、事件等级、解决方案。 |
| 受害者信息维保包括事件的影响范围、受害实体数目、受害者实体类型、受害者实体的数据添加删除维护，其中受害者实体信息包括实体名称、实体编码、实体描述。 |
| 攻击者信息维护包括攻击者的攻击动机、是否是攻击组织、攻击者组织名称、攻击者组织国家、攻击者组织分类、攻击者组织描述。 |
| 事件举证信息维护，包括流量的上行、下行维护、PCAP包文件上传、说明文件上传、图片上传、图片描述信息，是否被攻陷、危害信息、攻击链阶段、事件包含的告警列表 |

1. **应急指挥模块**

淳安县数据资源管理中心作为全县网络安全事件应急总指挥，通过应急指挥模块迅速定位事件发生源，已经当前各单位的处置响应情况，一屏掌控全链路监管。

通过全链路网络安全监管平台安全监测的事件向应急指挥推送基础数据，基础数据通过事件管理模块进行汇聚。

报送的事件通过研判和决策，确定为应急事件后，通过应急任务管理，启动应急响应任务，同时通过预警、通报和应急处置启动应急响应流程。

在重要会议或重大活动期间，加强网络安保人员调度，全方位全天候掌握淳安县电子政务外网网络、系统和网站安全状况，安全情况实时监测，以及重保任务的全生命周期管理，覆盖筹备阶段、临战阶段、决战阶段、战后总结等多个环节，及时通报预警网络安全隐患，高效处置网络安全事件，并对监测过程所产生的数据及结果进行管理，协同多家技术支撑单位、互联网安全厂商及网络安全专家保障整个过程的网络安全和数据安全，提升重大活动的安全保障能力。

技术指标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 单次活动管理 | 支持用户新增安保活动并对该活动进行管理，支持下钻到具体某个活动，查看活动详情 |
| 作战台 | 展示活动进程、信息公告、待办工作/跟进工作、快捷方式、个人信息 |
| 里程碑管理 | 支持对单次活动的里程碑进行管理 |
| 指挥中心 | 提供安保活动指挥单位和人员的选择添加、查看、退出活动、查询功能 |
| 安保目标 | 提供安保活动重点保障单位、人员和系统的选择添加、查看、退出活动、查询功能。 |
| 支撑力量 | 协助安保组完成该次安保活动的单位和人员，提供选择添加、查看、退出活动、查询功能。 |
| 信息公告 | 提供以指挥人员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 | 支持指挥人员维护该次安保活动的各项规章制度，并支持安保活动各方参与人员查看对应的规章制度。 |
| 应急预案 | 应急预案支持针对预先定义的预案名称、预案等级、预案分类、提交单位、提交时间和对应的操作项进行相应操作，并可以查询统计 |
| 安保驻点端 | 系统提供驻点小组安排本小组的值守排班计划的功能。对于驻点小组主要需要管理安保期间，每一天，每一个班次的人员，因此该部分模块展示的该小组每一天、每一个班次的值守人员通过修改等操作可以设置该次安保活动的排班频率，并可以对各个安保驻点上报驻点的排班计划， |
| 指挥中心端 | 安保组视角，对于安保组主要需要查看每一天每个驻点是由谁值守，并能查看该驻点当天的排班计划支持宏观查看活动期间的排班数量情况、报平安数量情况，以及深度查看安保期间每天，每个驻点每个班次的人员值班情况、签到签退时间、报平安状态、每个驻点在安保期间的排班计划等情况。 |
| 值守移动端协同 | 平台支持安保值守人员使用在手机APP钉钉上完成确定驻点各个班次的人员及签到、签退和报平安等操作。上述信息会同步到平台，并进行统计。 |
| 指挥调度 | 指挥中心通过切换总览、监测调度、通报、值守视图，来统筹协调赛事期间的网络安全事件处理。 支持查看战前各重点保障单位的安保检查情况，战时回复和处置报平安情况、安全事件上报及通报情况、查看下发的应急处置任务进展情况，战后通过活动快照查看历史活动成果。 借助视图切换，一键下发通报、检查、指令，联动移动端组织调度，运用应急预案响应应急处置。 |

1. **与杭州市主平台对接开发**

**本项目需满足浙江省大数据发展管理局下发的《浙江省政务外网安全运行监测指标（试行）》的全链路安全监测体系要求，支持满足后续五年杭州市数据资源管理局对于市-区（县）数据安全管控平台区县对接指标规范，**满足相关考核指标，采用接口的方式，将相关安全数据推送至杭州市数据安全管控平台，满足杭州市对下属区县的监管要求。同时，预留开放“云、网、端、边界、数据、应用”六大维度数据对接的接口，为后续全面对接提供技术保障，对接接口根据杭州市局指导按需合规设计开发。

1. **浙政钉安全协同对接开发**

对接浙政钉，以展示淳安县全域的安全风险情况、事件总数、事件分类、事件处置情况、及时处置率等方面，支持展示各单位安全风险及处置情况和TOP 10排名。此外，处置通报信息可通过移动驾驶舱下发到各责任人，实现态势呈现集约化，事件通报便捷化，安全运营移动化。

通过浙政钉相关规范主要了解其组织架构，全链路网络安全监管平台根据浙政钉的组织架构形成平台内部组织架构树，方便资产、告警管理和组织架构的关系对应，后期在通报及工单处置时可通过浙政钉为主要方式进行传达，以及各单位处置后的反馈。

移动端安全驾驶舱通过URL链接对接方式内置在浙政钉里，利用驾驶舱主要方便让领导一眼就能看明白网络安全及数据安全重点风险在哪里、哪些单位安全做的更好、接下来一段时间的安全形势走向，以便及时做出精准判断，有效决策。

通报、工单处置及移动端安全驾驶舱应用跟浙政钉的对接方式按照《浙政钉2.0应用上架迁移流程》进行申请上线。

1. **全链路可视化大屏开发建设**

淳安县全链路网络安全监管平台可视化大屏是根据浙江省大数据发展管理电子政务安全监测相关指标要求以及浙江省一体化智能化公共数据平台建设方案当中建立全链路安全监管机制的要求进行设计。

全链路网络安全监管平台以网络安全、云安全、数据安全、物理感知网安全以及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，形成针对人、物、地、事、数据、资产的多维视图，从不同视角出发感知安全态势，为三年规划的“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。

全链路网络安全监管平台（数据安全管控淳安子平台）向上对接杭州市数据安全管控主平台，向下对接“云、网、端、边界、数据、应用”子平台。横向对接云内安全相关资产的告警信息，并对资产从“云、网、数、用、端”等维度进行整体展示。

全链路可视化大屏展现指标如下：

1. **云内安全监测**

云内安全监测，监测主要包括目前目前淳安县全域云内活动资产（各类型实例）平台可用率（省里要求），以及云内安全事件近期发展趋势,点击更多跳转查看专项云安全态势。

1. **应用系统监测**

应用系统监测，监测内容包括淳安县全域政务云上应用、互联网应用、政务外网应用，主要从应用的脆弱性进行安全指标的展示，并对系统新增与否进行监测（省里要求）。

1. **网络安全监测**

网络安全监测，主要从两个维度，会跳动，包括设备告警趋势，以及资产的数量与类型分布占比。点击更多跳转查看应用安全态势。

1. **数据安全监测**

数据安全监测情况，主要包括数据资产（数据库、数据表、API）数量情况，并对告警数量趋势、数据库可用率（省要求），以及各类类型的分布进行展示。点击更多跳转查看数据安全态势。

1. **终端安全监测**

终端安全监测，监测不同终端类型的安全资产安装情况以及违规外联情况（省要求），点击更多跳转查看终端安全态势。

1. **监管中心**

大屏中心是监管中心，主要从安全监管、技术防御、防控运营、应急指挥、制度规范等维度进行下钻，可下钻至不同的板块进行详细功能的展示。

1. **实时通报情况**

实时通报情况，实时轮播展示淳安县全域未处置的工单情况，并对逾期工单进行标签提醒，确保事件闭环。点击该板块可以下钻至流程板块，该板块可以通过浙政钉进行通报和事件整改的通知。

1. **制度建设情况**

制度建设情况，检查淳安县全域考核排名，制度规范建设和人员情况（人员主要是运营人员保密协议签订等信息）

1. **应用安全开发检测体系设计**
2. **业务上云前源代码审计**

为了解决因开发人员能力不足、存在开发陋习等问题，可能导致代码存在算法、逻辑等漏洞，所以淳安县政务业务系统上云前前需要进行源代码安全测试审查。由于测试人员、测试工具、测试标准、测试环境等种种原因，代码测试结果中往往存在一定的误报。导致应用存在先天安全漏洞，因此需要建立一套行之有效的代码安全测试体系，解决后续业务上线存在大量漏洞无法修复或不能修复的问题。

本项目通过构建源代码审计平台，提供源代码安全检测能力，协助开发人员补齐测试能力，通过人工+自动化的方式对开发代码进行全面、深入测试，保障代码安全。通过安全检测确保上线应用安全补齐所有安全短板。防止先天代码漏洞，让后续的所有安全防护手段都丧失作用，导致数据泄露。

应用开发过程以及系统上线之前源代码安全分析技术对应用源代码进行自动化分析，从源代码层面发现软件中的安全缺陷。不同应用开发人员采用的开发语言可能多种多样，平台实现多种编程语言开发的软件源代码的缺陷检测。

通过多套源代码分析引擎技术，能在分析精度，速度，深度等方面均衡得到较好的分析结果。能够自动寻找软件的编码错误，无需构造测试用例，无需人工干预，在发现缺陷的同时还能给出问题的触发过程。这样可以让程序员迅速理解和修复问题，从而投入更多的时间到创造性的工作中。帮助企业在软件的开发环节中和程序员密切交互，在软件制造早期帮助开发人员集中精力完成开发进度的同时提高软件质量，大幅减少生产成本，提高研发效能。

**在本项目服务周期内，提供源代码审计次数不限。**

技术指标要求：

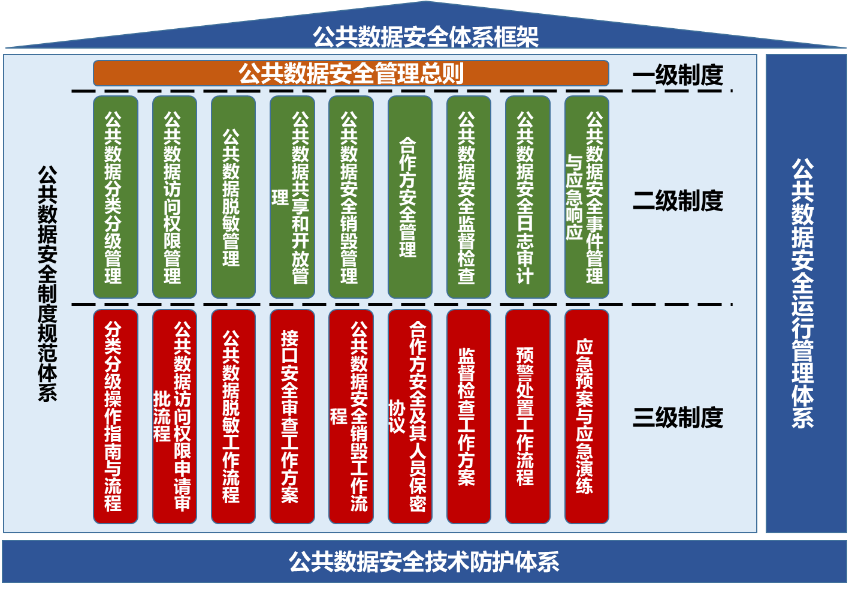
|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 部署方式 | 支持无服务化运行；支持虚拟化部署；支持 Linux 部署；支持容器化部署；支持集群部署。 |
| 源代码缺陷分析功能 | 支持 C、C++、Java、JavaScript、JSP、PHP、Android、 Python、Shell、GO、SQL等主流编程语言开发的软件源代码的缺陷检测。 |
| 支持代码注入、跨站脚本、输入验证、危险函数、代码质量、API 误用、密码管理、异常处理等常见安全缺陷问题的检测 |
| 支持用户对源代码缺陷分析模板的灵活配置。 |
| 支持函数白名单功能 |
| 支持文件/文件夹白名单功能，可以对多个文件或文件夹进行过滤，不统计该文件和文件夹下检测的问题结果，提高系统检测精准性。 |
| 支持对检测失败的任务重新发起检测，无需重新上传代码。 |
| 支持单个检测任务的检测日志下载。 |
| 检测完成后，系统能够自动以邮件方式将检测结果通知到指定人员。 |
| 源代码缺陷审计功能 | 能够对源代码安全扫描结果进行汇总，并按照问题的严重性和可能性进行威胁级别的划分，如高、中、低等多个级别。 |
| 能够迅速定位某一特定源代码安全问题所在源代码行，对问题产生的整个过程进行跟踪。 |
| 能够提供中文的源代码安全问题分类、问题描述及修复建议。 |
| 能够对当前问题进行审计，修改问题等级以及修改问题状态为是问题、不是问题、遗留问题。 |
| 能够记录结果的审计信息，包括人员、时间和审计信息等。 |
| 能够对检测结果按照缺陷类型、审计状态、文件名进行过滤查询。 |
| 项目管理功能 | 支持项目目标的设定，项目目标应包括缺陷类型、缺陷密度项。 |
| 支持配置自动化检测策略，能够按天或周进行自动化周期性检测。 |
| 能够对项目中每次检测结果与项目目标以及多次检测的结果进行对比，形成趋势分析。 |
| 支持自动化审计信息携带，能够将上一次的审计结果携带到下一次的检测结果中，降低审计成本。 |
| 能够对项目中源代码缺陷检测结果按照源代码提交者信息进行自动化分配，开发人员可查看自己的缺陷。 |
| 统计分析功能 | 能够根据检测时间、检测方式、任务类型、缺陷等级选择一至多个检测任务进行统计，统计显示任务数、总代码行数、缺陷总数、平均缺陷密度等信息。 |
| 统计结果以柱状图显示，分别展示缺陷总数和缺陷密度最高和最低的 TOP10 部门。 |
| 能够以饼状图显示所有统计数据缺陷次数出现最多的 TOP10类型及数量。 |
| 系统管理功能 | 系统为 B/S 架构，支持多用户同时使用浏览器访问。 |
| 支持自定义角色权限。 |
| 能够对检测队列进行管理，如删除正在执行的任务，调整任务优先级等。 |
| 能够提供系统操作日志，记录用户的关键操作；能够提供系统错误日志，记录关键的错误信息。 |
| 可支持通过系统界面下载系统日志和引擎日志。 |
| 界面要求 | 要求中文界面，易操作，具有中文问题描述、修复建议 |
| 服务要求 | 提供三年的平台免费升级质保服务，提供平台使用现场培训 |
| 支持并指导驻场人员日常源代码审计的平台使用 |

1. **业务上云前渗透测试**

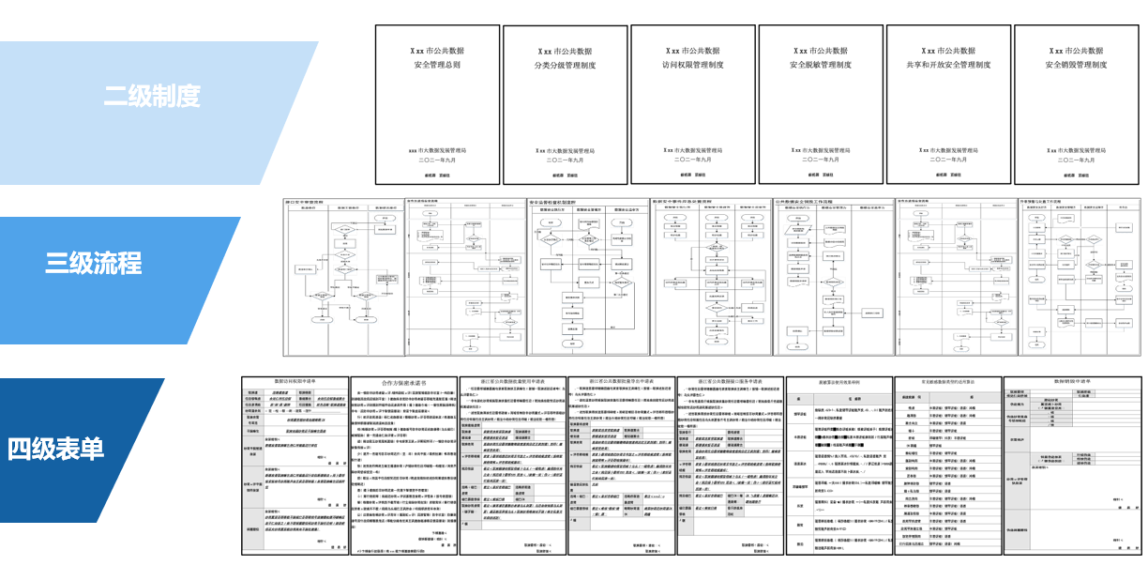
为了保障淳安县政务业务系统上云前的系统处于安全的状态，依据等保的安全性要求，由专业的网络安全驻场人员和实施单位以黑客视角进行全流程访问的攻击测试，最大限度发现目前业务系统薄弱点和入侵途径，协助运维人员整改发现的安全问题并进行安全复测，确保安全漏洞被修复，形成安全闭环。**在本项目服务周期内，业务上云前渗透测试次数不限。**

1. **数据安全制度管理体系设计**

结合淳安县本地实际，建立健全公共数据安全制度规范体系，制定完善公共数据分类分级、访问权限、共享开放、脱敏销毁、日志审计、监督检查、安全事件应急处置、合作方及其人员管理等标准规范，指导各地各部门做好公共数据安全保障工作，促进公共数据安全管理工作标准化、流程化、规范化，使各项公共数据安全管理工作有规可依。



积极响应上级领导指示与要求，通过制定二级、三级制度以及配套的四级表单，完善数据安全制度管理体系；并作为后续整体中心运营提供理论流程依据。



1. **数据安全运行管理体系设计**
2. **数据安全运行管理平台**

数据运行安全的稳定性主要从隐患监控、日常运维、安全检测、集中告警、可视化展示几大维度定义。数据库承担数据的存储、读取等功能，是信息系统内极其重要组成部分，数据库故障可能导致信息系统全面瘫痪，对运营和安全生产的威胁极大，数据资产的丢失也会造成不可挽回的影响，保障数据的运行环境稳定健康，提前预知隐患、问题快速定位、故障高效解决是必要的。

数据运行安全监控管理平台主要包括以下内容：

1. 健康度监控：从5大健康指数（可用性、错误、性能、变化和可靠性）、SQL执行生命周期（登录、解析、执行、提交）的监控以及关联资源（数据库资源如：process\session\jobs等，锁资源，主机资源）的监控，实现精准定位影响数据库健康和性能缓慢的根因。
2. 智能自动运维组件：工具箱提供诸如：性能分析、锁处理等、错误日志多种多样的数据库运维工具，诸如：性能分析、TOP SQL、SQL诊断、锁处理、容量预测、表空间扩容、归档日志清理等等，方便运维人员快速完成日常数据库运维工作，提升运维效率。帮助数据库运维人员能够简单而又高效快捷的完成日常的数据库运维工作，以保证数据库能够稳定运行，从而为整个数据管理中心的信息化业务系统稳定可靠的运转提供保障。
3. 安全检测：对用户、变更、主机链接、DB-Link图谱、SCN、比特币等数据库常见运行安全隐患进行检测，保证数据库的平稳运行。
4. 可视化展示：支持平台内已配置的所有对象聚合监控及单一对象的详细监控。聚合监控从：最近24小时告警数量、最近24小时变更数量、过去7天可用性、会话数、繁忙度、健康度等多个维度，实现全面、丰富、深度地数据库聚合监控。利用聚合监控大屏，运维人员可以直观清晰地了解到各数据库对象及其对应的业务系统整体运行情况，确保业务系统的连续稳定可用。
5. 数据风险事件告警：威胁信息主要包括外部第三方威胁，如最新的SQL注入病毒，数据库漏洞，系统漏洞，勒索病毒等，要求数据安全管控平台对外提供接口，能够及时发现这些漏洞，并能提供报警能力，外部威胁信息分析库支持离线以及在线两种方式进行更新，保证系统可用可靠。实时展示数据风控系统最新发现的敏感数据泄露风险告警事件，内容包含：敏感内容、敏感级别、访问账号、业务系统等。
6. **数据发现与分类分级平台**

在数据安全治理过程中，数据分类分级是基础工作，并且至关重要，只有将数据资产有效分类分级，发现敏感数据、重要数据、个人信息等类型及其重要级别，盘点清楚有什么，需要保护什么，保护程度是什么，才能在数据安全防护中实施更合理和精细化的措施，进而在数据全生命周期中实现动态、开放、可视的数据安全治理。

数据分类分级是确定数据保护和利用之间平衡点的重要依据，为后续数据应用和安全措施落地奠定了基础。数据分类分级涉及组织全部数据，在工作开启之前，需要明确该项工作的实施流程，包括建立组织保障、数据资源梳理和识别、数据分类、数据分级、数据分类分级策略、数据分类分级落地，具体如下所示：

文本  描述已自动生成

根据省厅《数字化改革公共数据分类分级指南》的要求，需要从数据产生频率、数据产生方式、数据结构化特征、数据存储方式、数据质量要求、数据应用领域、数据共享属性、数据开放属性、数据使用频率、安全保护维度、数据对象纬度等十一个维度来对现有的数据进行分类分级。

**构建数据发现与分类分级平台，面向数据挖掘并进行自动化数据识别、分析、分类、分级。**平台可接入淳安县数据资源中心内网，盘点数据资产，认识数据，实现自动化的元数据采集、识别数据格式和语义内容、实现敏感数据发现和分类分级。

对于数据在哪里，平台提供手动添加、批量导入、自动发现三种方式。对于连接成功的数据源，支持用户开展资产发现作业。对于数据管理中心归集的数据规模、格式不一的各部委数据，可使用数据发现与分类分级平台定期通过扫描IP范围的方式去自动化发现政务数据网内部有多少数据库，确保对完整数据源的统一管理。

对于有那些数据数据发现与分类分级平台可实现通过数据库用户，扫描用户名下数据表、字段，并获取相关元数据信息。发现结果确认之后可同步到总览中进行查看，也可以通过接口提供给其他平台，包括一体化智能化公共数据，安全产品以及数据资产管理等工具。

采用数据发现与分类分级平台对现有的所有数据表和字段进行逐个字段的分类分级实施有可能出现工具无法正常识别的情况，需要人工对表和字段进行发现和分类分级以及对分类分级的结果进行人工确认，保障分类分级工作的准确和质量。

发现结果确认包括：

* 1. 确认业务类型识别结果：确认已识别的业务类型，确认空数据和脏数据，确认自动字典和自动规则的业务类型，确认未识别和其他类型的业务类型，
  2. 新增业务类型及发现规则，新增业务类型，新增发现规则，
  3. 分类结果确认，给未分类的字段添加分类分级，给业务类型对应多个分类的字段确认唯一分类，
  4. 再次运行和规则完善，将新增的业务类型添加到发现模版，导出自定义的数据字典和发现规则，提供给研发完善发现模型。

**与数据安全系统联动，可通过API方式为数据治理和数据安全治理提供分类分级成果和规则，为数据业务和数据安全提供必要基础安全能力。**

1. **整体平台安全运营服务设计**
2. **驻场运营**

本项目要求安排一名驻场运营服务人员进行淳安县全链路网络安全监管平台安全运行及维护保障。具体的驻场服务包括但不限于：

1. 日常处理与全链路网络安全监管平台的对接工作，包括但不限于需求讨论、问题协助处理等；
2. 根据全链路网络安全监管平台获取到的漏洞及安全事件数据信息，向相关负责人汇报，汇报完成后，根据相关负责人指示授权开展进一步工单处置及协助复核工作；
3. 对系统进行维护时，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
4. 定期对全链路网络安全监管平台相关数据进行日常巡检及问题发现，以便及时发现异常行为。
5. 定期对全链路网络安全监管平台进行报告输出，报告内容包括但不限于安全事件情况、处置情况、考核情况等。
6. **驻场人员需具备渗透测试、漏洞扫描、协助安全加固、应急服务、普通安全重保服务的能力，工作频次根据淳安县数据资源管理中心的实际工作评估要求完成。**
7. **驻场人员的工作作息时间与淳安县数据资源管理中心一致，由淳安县数据资源管理中心进行人力管理。**
8. **渗透测试**

本项目要求实施单位以黑客视角进行全流程访问的攻击测试，最大限度发现目前安全建设薄弱点和入侵途径，协助运维人员整改发现的安全问题并进行安全复测，确保安全漏洞被修复，形成安全闭环，增强平台业务安全对抗能力。由驻场人员实施，要求每年不少于4次（平均每季度一次）渗透测试。

1. **安全加固与演练**

基于构建的全链路网络安全监管平台，通过自动化的安全编排，将安全风险发现的问题及时进行处置，将安全流程或预案，利用数字化管理起来形成安全剧本。联动业务环境当中已经部署的安全防护措施，用自动化完成其中所有可能自动化的动作，无法自动的仍然交由人来处理，通过可视化编排工具将人、技术和流程有机的结合起来，形成标准统一的、可重复的、更高效的安全运营流程。同时对分析、响应处置过程中各种复杂的分析流程和处理平台进行整合，形成自动化的能力集成，实现从静态事件响应到动态工作流跟踪的转变，提升整体的协调及决策能力。

本项目要求每年不少于4次（平均每季度一次）的定期对安全设备、安全产品进行巡检，分析其运行参数和运行结果，发现、研判、清除设备故障风险点，预防设备运行异常和宕机罢工，维持安全设备、安全产品的长效稳定运行。

根据安全巡检结果，针对所发现的安全漏洞及安全风险，安全运营人员提出可操作性强、效果佳的整改建议，并协助用户完成安全整改。

业务应用在在一体化智能化公共数据平台上线后，应定期对应用系统进行风险评估，通过漏洞扫描、渗透测试、访谈调研、安全审计等手段，主动识别技术、管理安全风险并协助加固整改，完善应用安全体系。

1. **应急响应支撑**

本项目要求实施单位结合省市县应急预案要求，在省市规定应急演练次数基础上，另外增加每年两次以上的应急演练，明确安全责任分工，控制安全事件范围，消除安全事件影响，确保指挥渠道畅通、响应部门高效处置，防止可能发生或已发生的事件影响相关业务及平台平稳、稳定运行。

打造一支能力突出的应急处置团队，引入第三方安全服务商做好应急响应支撑工作，基于全链路网络安全监管平台，借助网络安全态势感知和通报预警技术及管理手段，将通报预警体系与应急响应体系进行有效整合，逐步建设成覆盖全县政务系统的应急响应及通报预警机制，实现全县安全事件的统一预警通报和应急指挥。

建立安全事件联动共享的机制，统一管理应用安全事件通报预警与应急响应。制定CC攻击、网站篡改、不良信息传播、系统入侵等安全事件的应急预案以及应急演练方案，并定期开展应急演练。

1. **安全重保服务**

本项目需要实施单位加强安全防护措施、开展专项安全检查、抓好重点单位排查，制定多项网络安全应急保障预案，形成重大活动期间7\*24小时安全保障机制。通过建立保障队伍和制定保障计划，确定保障时间、管理范围、负责人及参与者、制定检查工作计划、制定保障演练计划、制定应急预案等。在重大活动保障期间，定期开展网络攻防应急演练，检验网络安全防御、监测预警及应急响应能力，做到“实战对抗、能力进化”。

重大活动保障时期对平台业务系统可能存在的安全风险以及安全防御体系可能存在的薄弱环节，指导修复，以提升被保障单位信息系统安全防御能力。同时为重保期间网络安全提供有力保障，加强信息系统生命周期安全管理、协助淳安县建立全面的主动安全运营机制、提升淳安县数据驱动的威胁对抗能力。

重大活动包括国家法定节期日和国家、省、市、县主办的重大活动，重大活动保障次数不限，以淳安县数据资源中心实际需求为准。

1. **安全创新能力探索**

淳安县数据资源中心拟与省内著名重点科研院所、承建单位三方联合打造服务于淳安县特别生态功能区的“全链路网络安全联合创新实验室”，实验室为开放性实验室，根据研究方向和路径可根据需要引入不同的优秀信息安全软硬件企业及业务建设类企业加入实验室，共建共创，共同打造国内一流水平集数据治理、安全管控与城市数字化安全保障一体的创新型实验室。实验室在淳安县落地，共同就网络安全和大数据安全进行创新探索，沉淀安全创新能力，打造具有淳安特色安全场景。

网络安全创新探索：探索区块链、边缘计算、可信接入等新的技术理念，解决物联网设备发现、识别、接入、监管、告警等安全防护问题，达到“信任接入、接入可知、接入可管”，打造淳安县生态环境保护等领域物联感知体系，强化物联感知网络数据安全保障机制，孵化物联感知数据的分类分级与敏感数据鉴别打标工具，落地物联网数据区块链全流程审计平台，从而实现物联网云、端、数据、网络全链路的安全保障与监管机制。

大数据安全：落地本地数据治理团队，开展数据异构融合和治理能力。形成异构数据融合安全治理规范，并按照标准完成本地异构数据融合工作。同时对淳安县一体化智能化公共数据平台数据安全进行全生命周期防护，打造“安全监管+政务数据”的智慧监管新模式，提高安全管理科学化、专业化、智能化、精细化水平，赋能淳安县安全监管，提升安全监管的数字化水平，初步形成一屏掌控全县安全的监管模式。

**具体要求：**联合创新实验室要紧紧围绕淳安县社会发展需要，项目验收前每年举办一次全县网络安全领域专题培训，承担市级课题研究一项以上，发表SCI（或EI）类高质量论文不少于三篇，网络与数据安全领域孵化技术工具成果每年至少落地一项，并成果获得省市认可，成果可发布于浙江省数字化改革专刊或全国政务一体化平台建设专刊。

# 全链路网络安全监管平台能力对接说明

淳安县全链路网络安全监管平台作为顶层架构，为后续“云、网、数、用、端、边界”六大维度提供了一体化全链路统一监管平台，通过多维异构的安全厂商能力，构建整体完善的淳安县一体化智能安全防护体系。

各个体系的对接说明如下：

1. **云安全---对接云安全防护平台**
2. **漏洞扫描数据**

对接扫描淳安县政务网内Web、数据库、基线核查、操作系统、软件存在的弱口令、端口与服务探测为辅助的漏洞检测信息。

1. **主机安全及管理**

对接日志集中化管理功能和多种类型的关联分析，为淳安县提供持续性安全监控能力和高效的攻击溯源分析技术平台。

1. **日志审计能力**

对接政务网内各类日志包括访问记录、潜在的威胁，起到追根索源的目的，并且记录服务器返回的内容，便于取证式分析，以及作为案件的取证材料。

1. **数据库安全审计**

对接淳安县进出核心数据库的访问流量进行数据报文字段级的解析操作，完全还原出操作的细节，并给出详尽的操作返回结果，以可视化的方式将所有的访问都呈现在管理者的面前，数据库不再处于不可知、不可控的情况，数据威胁将被迅速发现和响应。

1. **网、边界安全---对接云防护平台、网络安全大数据平台**
2. **对接云防护平台**
3. **白名单接口对接**

将全链路网络安全监管平台推送过来的白名单IP加入云防护平台白名单，实现大数据平台和云防护平台策略下发的同步和联动。

1. **黑名单接口对接**

将全链路平台推送过来的黑名单IP加入云防护平台黑名单，实现大数据平台和云防护平台策略下发的同步和联动。

1. **告警数据处理对接**

将云防护平台的攻击日志和拦截告警数据发送到全链路平台，全链路平台经过建模分析后进行展现，可提取出高风险攻击信息，提醒安全运维人员进行处置。

1. **网络安全大数据平台**

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 风险上报接口 | 上报频率至少为10分钟一次，含安全域名称、风险值和风险等级。 |
| 2 | 告警上报接口 | 网络安全一体化支撑平台应将本平台发现的告警信息通过告警上报接口向安全监管平台进行上报。含市级编码、告警时间、数据来源等。 |
| 3 | 安全事件上报 | 网络安全一体化支撑平台通过安全事件上报接口向安全监管平台进行安全事件上报。含事件等级、源目IP、文件hash等。 |
| 4 | 资产上报接口 | 安全监管平台定时将资产信息上报到市级平台。含名称、IPv4/IPv6、MAC、责任人、操作系统、部门等。 |

1. **对接市数据安全管控平台**

淳安县全链路网络安全监管平台按照国家有关标准规范、结合《浙江省电子政务外网安全监测平台地市对接标准规范》，完成与杭州市数据安全管控平台的对接，逐步建立安全风险报告和情报共享机制。

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 级联认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成安全监管平台至市级平台的注册功能，保证平台之间通信的安全性。由市级平台进行平台间级联的注销，市级平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 市级平台对安全监管平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 风险上报接口 | 上报频率至少为10分钟一次，含安全域名称、风险值和风险等级。 |
| 4 | 告警统计上报接口 | 安全监管平台向市级平台上报前一天发现的告警统计数据信息。含告警数量、总数、漏洞病毒高中低危告警总数等。 |
| 5 | 告警上报接口 | 安全监管平台应将本平台发现的告警信息通过告警上报接口向市级平台进行上报。含市级编码、告警时间、数据来源等。 |
| 6 | 安全事件上报 | 安全监管平台通过安全事件上报接口向市级平台进行安全事件上报。含事件等级、源目IP、文件hash等。 |
| 7 | 案例上报接口 | 安全监管平台以文档方式进行安全事件汇总上报。含案例时间、标题、关键字、创始人、附件等。 |
| 8 | 案例知识库查询接口 | 安全监管平台可查询市级平台的知识库共享内容。含关键字、开始、结束时间等。 |
| 9 | 报表上报接口 | 安全监管平台应按要求向市级平台汇报本平台的月报报表汇总信息。含报表id、名称、类似等。 |
| 10 | 预警通报下发接口 | 市级平台定时将通报信息发送到安全监管平台中。含通报类型、描述、创建时间、附件等。 |
| 11 | 威胁情报共享接口 | 安全监管平台可向市级节点查询威胁情报信息。含行政区划码、情报IOC、IP地址、文件hash、情报类型级别等。 |
| 12 | 漏洞上报接口 | 安全监管平台定时将漏洞信息上报到市级平台。含漏洞发布时间、级别、处置建议、参考链接等。 |
| 13 | 漏洞信息共享 | 安全监管平台可向市级节点查询漏洞信息，实现漏洞信息的共享。含关键字、开始、结束时间。 |
| 14 | 资产上报接口 | 安全监管平台定时将资产信息上报到市级平台。含名称、IPv4/IPv6、MAC、责任人、操作系统、部门等。 |
| 15 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，市级平台获取时需要获取文件授权（授权有时效性）再获取文件，含状态码、返回消息、存储路径等。 |

1. **自动编排与分析**

通过自动化编排，把人、过程和技术整合起来，大幅提升安全运营工作效率，将分析人员从耗时且重复的分析工作中解放出来。

拖拽式交互设计安全风险分析研判策略和联动响应剧本，多种策略编排动作，包括但不限于关联验证、告警聚合、联动、阻断。

可以设置剧本的触发方式，包括事件触发（当系统监测到选中的事件发生时，则触发绑定的剧本），定时周期，定时单次（比如需要设置定期扫描等任务，可选择定时触发方式）三种，通过不同的触发方式触发绑定的剧本从而产生不同类型的案件，执行自动化的响应过程。

1. **应急处置联动**

对接云防护平台、防火墙、EDR等防护设备，实现一键封堵，支持输入单个IP封堵、输入网段封堵、上传文件批量封堵等封堵操作。

能够配合自动化响应剧本，实现告警触发后自动识别受攻击资产，联动对应防护设备进行阻断。

1. **终端安全---对接终端一体化安全平台**
2. **网络终端**

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 告警事件上报接口 | 将发现的终端告警信息通过告警上报接口向安全监管平台进行上报。含告警类型、告警内容、告警等级、来源信息、目的信息、访问信息、告警时间、数据来源等。 |
| 2 | 终端资产上报接口 | 定时将终端资产信息上报到安全监管平台，含名称、类型、主机:端口、责任人、部门等。 |

1. **感知网终端**

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 级联认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成安全网络安全支撑平台至安全监管平台的注册功能，保证平台之间通信的安全性。由安全监管平台进行平台间级联的注销，安全监管平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 物联感知网资产上报接口 | 物联网安全支撑平台定时将物联网终端资产信息上报到安全监管平台，含厂商品牌、设备类型、操作系统类型、协议、平台等信息。 |
| 3 | 感知网终端设备运行状态上报接口 | 安全监管平台对物联网安全支撑平台的上报感知网终端设备实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 4 | 风险上报接口 | 上报频率至少为10分钟一次，含安全域名称、风险值和风险等级。 |
| 5 | 告警统计上报接口 | 物联网安全支撑平台向安全监管平台上报前一天发现的告警统计数据信息。含告警数量、总数、漏洞病毒高中低危告警总数等。 |
| 6 | 告警上报接口 | 物联网安全支撑平台应将本平台发现的告警信息通过告警上报接口向安全监管平台进行上报。含市级编码、告警时间、数据来源等。 |
| 7 | 安全事件上报 | 物联网安全支撑平台通过安全事件上报接口向安全监管平台进行安全事件上报。含事件等级、源目IP、文件hash等。 |
| 8 | 案例上报接口 | 物联网安全支撑平台以文档方式进行安全事件汇总上报。含案例时间、标题、关键字、创始人、附件等。 |
| 9 | 案例知识库查询接口 | 物联网安全支撑平台可查询安全监管平台的知识库共享内容。含关键字、开始、结束时间等。 |
| 10 | 报表上报接口 | 物联网安全支撑平台应按要求向安全监管平台汇报本平台的月报报表汇总信息。含报表id、名称、类似等。 |
| 11 | 预警通报下发接口 | 安全监管平台定时将通报信息发送到物联网安全支撑平台中。含通报类型、描述、创建时间、附件等。 |
| 12 | 威胁情报共享接口 | 物联网安全支撑平台可向安全监管平台查询威胁情报信息。含行政区划码、情报IOC、IP地址、文件hash、情报类型级别等。 |
| 13 | 漏洞上报接口 | 物联网安全支撑平台定时将漏洞信息上报到安全监管平台平台。含漏洞发布时间、级别、处置建议、参考链接等。 |
| 14 | 漏洞信息共享 | 物联网安全支撑平台可向安全监管平台查询漏洞信息，实现漏洞信息的共享。含关键字、开始、结束时间。 |

1. **数据安全---对接数据安全管控淳安子平台**

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 告警事件上报接口 | 数据安全管控淳安子平台应将本平台发现的告警信息通过告警上报接口向安全监管平台进行上报。含告警类型、告警内容、告警等级、来源信息、目的信息、访问信息、告警时间、数据来源等。 |
| 2 | 数据资产上报接口 | 数据安全管控淳安子平台定时将数据资产信息上报到安全监管平台，含名称、类型、主机:端口、责任人、部门等。 |
| 3 | 元数据分级分类接口上报接口 | 数据安全管控淳安子平台定时将元数据资产信息上报到安全监管平台。含表分级分类梳理结果、列敏感识别梳理结果等。 |
| 4 | 应用服务资产上报接口 | 数据安全管控淳安子平台定时将应用服务资产信息上报到安全监管平台。含名称、主机:端口、URL、系统重要性、责任人、所属系统、部门等。 |
| 5 | API接口资产上报接口 | 数据安全管控淳安子平台定时将API接口资产信息上报到安全监管平台。含接口名称、接口地址、应用服务IP：端口等。 |
| 6 | 人员账号资产上报接口 | 数据安全管控淳安子平台定时将人员账号资产信息上报到安全监管平台。含账号名、资产、使用人、部门等。 |
| 7 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，安全监管平台获取时需要获取文件授权（授权有时效性）再获取文件，含状态码、返回消息、存储路径等。 |

# 第三方监管单位对接说明

平台同时具备与第三方监管单位对接的能力，为后期整体智治提供相应的统筹协调能力。对接接口清单与接口描述如下：

1. **对接网信监管平台**

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成安全监管平台至网信平台的注册功能，保证平台之间通信的安全性。由网信平台进行平台间级联的注销，网信平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 网信平台对安全监管平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 工单列表信息获取接口 | 安全监管平台定时将工单列表信息上报到网信平台。含工单主题、状态、优先级、时间、受理部门、人员、创建人等。 |
| 4 | 工单详情信息获取接口 | 安全监管平台定时将工单详情信息上报到网信平台，含工单基本信息、工单详情、工单流程信息等。 |
| 5 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，网信平台获取时需要获取文件授权（授权有时效性）再获取文件。含状态码、返回消息、存储路径等。 |

1. **对接公安监管平台**

|  |  |  |
| --- | --- | --- |
| 序号 | 接口名称 | 接口描述 |
| 1 | 认证接口 | 包括级联注册接口和级联注销接口。级联注册接口完成安全监管平台至公安平台的注册功能，保证平台之间通信的安全性。由公安平台进行平台间级联的注销，公安平台上注销后，停止与安全监管平台的通讯。含注册节点IP、端口等。 |
| 2 | 运行状态上报接口 | 公安平台对安全监管平台的上报接口实施周期检测。含运行状态、内存使用、CPU使用、硬盘使用等。 |
| 3 | 工单列表信息获取接口 | 安全监管平台定时将工单列表信息上报到公安平台。含工单主题、状态、优先级、时间、受理部门、人员、创建人等。 |
| 4 | 工单详情信息获取接口 | 安全监管平台定时将工单详情信息上报到公安平台，含工单基本信息、工单详情、工单流程信息等。 |
| 5 | 文件上传接口 | 各接口附件内容通过文件上传接口进行上传，各级平台通过HTTP接口方式上传接口，公安平台获取时需要获取文件授权（授权有时效性）再获取文件。含状态码、返回消息、存储路径等。 |

**平台建设功能要求指标清单**

1. **全链路网络安全监管平台功能指标要求**

|  |  |  |
| --- | --- | --- |
| **模块名称** | **功能名称** | **功能要求** |
| **资产管理** | 单位档案 | 通过单位卡片提供单位问题情况一览，形成单位组织架构树，并支持按照架构树控制数据可见范围；提供单位的详细档案，刻画维度包括：单位信息、安全监测信息、人员信息、业务系统信息、IP资产信息等 |
| 系统档案 | 通过系统卡片提供系统事件、隐患、被攻击情况概览，按照系统所属单位形成组织架构树，支持按照架构树控制数据可见范围；提供系统的详细档案，刻画维度包括：系统信息、安全监测信息、防护情况信息、供应链信息、基础网络信息、人员信息等。 |
| IP档案 | 通过IP资产卡片提供IP相关事件、隐患和攻击情况概览，按照系IP资产所属单位形成组织架构树；提供IP资产的详细档案，刻画维度包括：风险详情、访问关系、行为画像等 |
| 机房档案 | 支持对机房信息进行增、删、改、查。 |
| 大数据平台档案 | 支持对大数据平台信息进行增、删、改、查；配置经纬度信息后，大数据平台将可在相应大屏的地图上进行打点 |
| 云平台档案 | 支持对云平台信息进行增、删、改、查；配置经纬度信息后，云平台将可在相应大屏的地图上进行打点 |
| 物联网档案 | 支持对物联网LED设备信息进行增、删、改、查。 |
| APP画像 | 展现相应APP所有详情信息，包括基础信息、关联资产和境外风险、APK威胁、APK漏洞、关联权限等。 |
| 业务全景 | 用户可通过拖拽方式形成各种样式和内容的网络拓扑图，支持画布尺寸、主题色的自主设置。 |
| 人员档案 | 用户可通过本菜单对本辖区涉及到网络安全的人员进行统一管理。提供增删改查功能，并支持将人员与单位、系统等资产进行关联。通过详情信息可查看该人员的具体档案，包括个人基础信息、关联业务系统信息和所属单位信息等。 |
| 设备档案 | 对安全设备和引擎的数据接入情况进行统一管理和监控。 |
| 待核验 | 待核验单位、系统、IP数据展示，单位、系统、IP数据检索、新增、删除、核验、编辑、导入、导出等功能 |
| 已核验 | 已核验单位、系统、IP数据展示，单位、系统、IP数据检索、新增、删除、核验、编辑、导入、导出等功能 |
| 无效数据 | 无效单位、系统、IP数据展示，单位、系统、IP数据检索、新增、删除、核验、编辑、导入、导出等功能 |
| 治理模型 | 资产治理模型管理 |
| **数据分析** | 模型管理 | 可对所有安全模型进行管理，具体可进行新增、删除、启用、告警等具体操作 |
| 指标管理 | 指标管理主要是将安全数据以某些条件过滤后进行统计，生成的指标信息可以作为大屏、统计模型及AI模型的模型指标项。可对指标进行新增、查询、删除等操作。 |
| 黑白名单 | 具备“检测项”和“过滤项”两种匹配原则，“检测项”仅分析（统计、模型）检测项配置匹配的数据，“过滤项”，不分析（统计、模型）过滤项配置匹配的数据，数据分析流程：数据（日志、流量）先通过“检测项”，后通过“过滤项”。“检测项”不配置时，所有数据通过“过滤项” |
| 数据字典 | 数据字典统一管理平台上的字段信息包括：数据来源、数据的标准化字段格式说明、目标存储平台等基础信息以及攻击链、告警字典等数据。通过数据字典可以查询接入的数据对应的字段信息，包含表名，表字段信息。支持数据字典中数据信息的维护，包括数据信息的录入、修改、删除。 |
| 资产概况 | 对资产的概况信息进行展示 |
| 访问关系 | 展示资产的网络关系 |
| 行为画像 | 展示资产的流量趋势、访问趋势等信息 |
| 服务端口 | 展示资产开放的端口详情 |
| 访问端口 | 展示资产访问的端口详情 |
| 图表管理 | 通过图表方式对数据进行展示，具体支持报表查询、报表类型、报表新增、报表导出等操作。 |
| 仪表盘管理 | 支持由多种图表组成的仪表盘进行展示和管理，具体包含仪表盘新增、仪表盘删除、仪表盘预览等操作 |
| **实时监测** | 事件成果 | 展示平台的事件成果，支持展示事件等级、攻击者、威胁等级、发现厂商、事件来源、危害程度、事件报警源文件等信息 |
| 风险成果 | 展示平台风险成果，支持展示漏洞等级、URL、漏洞类型、发现厂商、风险来源等信息。 |
| 事件/风险检索 | 多字段组合检索，事件检索，支持按事件名称、受害者、处置状态、起始时间、单位名称、威胁级别、数据来源、所属区域等字段进行事件组合检索 |
| 事件/风险导入导出 | 根据模版进行事件/风险导入、导出 |
| 事件处置 | 事件/风险通报、批量处置 |
| 事件/风险详情展示 | 展示事件/风险详细信息，包括受害者、攻击者、poc信息、原始信息等 |
| 事件/风险联想 | 同类型、同单位事件/风险联想 |
| 事件验证 | 展示带验证事件详情，包括事件名称、单位名称、威胁级别、发生时间、数据来源、验证状态和事件操作等信息 |
| 风险验证 | 展示带验证风险详情，包括漏洞资产、单位名称、漏洞等级、发现时间、数据来源、验证状态、风险操作等信息 |
| 弱口令 | 弱口令场景风险聚合，展示事件名称、单位名称、威胁等级、涉及账号、高危账号、登陆密码、api等信息 |
| 挖矿 | 挖矿场景事件聚合，展示系统名称、单位信息、威胁级别、事件名称、来源IP、来源端口、目的IP、目的端口、传输协议、应用协议等信息 |
| 勒索病毒 | 勒索病毒场景事件聚合，展示系统名称、单位信息、威胁级别、事件名称、来源IP、来源端口、目的IP、目的端口、传输协议、应用协议等信息 |
| 事件/风险检索 | 多字段组合检索，支持按单位名称、漏洞资产、验证状态、结束时间、漏洞名称、漏洞等级、数据来源、所属区域等字段进行组合检索 |
| 事件/风险验证 | 事件/风险批量验证 |
| 事件/风险导入导出 | 根据模版进行事件/风险导入、导出 |
| 事件搜索 | 展示事件信息，支持展示事件名称、威胁等级、受害者、模型名称、事件标签、单位名称、单位类型、所属行业、地理位置、事件时间、事件等级、资产域名、URL等字段信息 |
| 风险搜索 | 展示风险信息，支持展示漏洞名称、漏洞类型、漏洞等级、漏洞IP/域名、地理位置、更新时间、地址经纬度、省份、城市、区县、单位类型、资产域名、数据来源等字段信息 |
| 攻击搜索 | 可以使用不同查询条件对安全告警进行查询。当用户为租户时，只显示根据来源安全域过滤后的数据。具体可进行告警查询、检索保存、告警聚合、时序图查看、字段显示、告警导出、告警详情查看等功能 |
| 原始日志 | 可以使用不同查询条件对日志信息进行查询。当用户为租户时，只显示根据来源安全域过滤后的数据。具体可进行告警查询、检索保存、可视化、时序图查看、字段显示、日志导出、日志详情查看等功能 |
| 数据检索 | 通过AiSQL检索所有数据，包括“与“、“或”、“包含”等不低于15种语法检索。 |
| 自定义字段展示 | 自定义展示字段，可进行自主配置 |
| 生成风险/事件 | 从攻击数据中生存事件和隐患 |
| **告警管理** | 信息对接 | 通过与各类探针对接，获取相关的攻击、漏洞、风险、隐患等告警数据并进行汇总，经过预处理之后的安全数据以结构化的形式进行存储，对外提供数据查询与统计服务，从而实现海量数据检索与挖掘。 |
| 通报方式 | 浙政钉、网页等。在发生严重情况时，如突发的安全事件、重大漏洞等，直接通过电话的方式进行传达；当系统监测到存在轻微的安全隐患时可通过浙政钉或网页进行预警提醒、或限期整改等。 |
| **检查督查** | 检查总览 | 可按照用户需要针对某一次计划或者全部检查计划的任务信息进行统计，主要展现 三类检查任务的总量、进行中数量、逾期数量；展示备件差对象的行业分布情况，展示最新一次检查计划的进度，展示支撑单位对检查任务的支撑情况。 |
| 计划本身管理 | 用户可针对具体的检查工作新建检查计划，并对计划下的各种任务分派具体负责人；同时支持用户手动将检查计划进行归档办结。计划创建人、计划联络人、任务负责人可在计划详情页面进行各类检查任务的新增和检查任务的推进。 |
| 现场检查任务 | 现场检查任务功能支持监管方用户在现场检查中直接通过页面填写检查表并出具检查结果，也支持用户现场检查完毕之后向系统录入检查结果；若需要整改的还可将任务流转给被检查单位，由其完成相应的整改动作后将检查任务闭环。 |
| 单位资自查任务 | 单位自查任务功能支持监管用户将任务直接对自查单位进行下发，自查单位可通过平台页面直接填报自查表，也可线下提交检查表给监管方由监管方统一录入；结果提交后由任务负责人进行审核，通过后任务办结。 |
| 远程检查任务 | 远程检查任务支持监管用户将任务直接下发给支撑单位，由支撑单位对指定系统进行渗透测试并反馈漏洞发下情况；由监管用户确认检查结果后，由漏洞系统归属单位进行整改和结果提交，若整改审核通过则任务办结。 |
| 检查模板管理-检查项管理 | 用户将检查表中的每一个检查项通过该页面维护至系统内，以支持后续组成相应检查表。 |
| 检查模板管理-检查表管理 | 每一张检查表由若干检查模块组成，每一个检查模块又有相应检查项组成；每张检查表可配置是针对单位或是系统，同时可多选检查表对应的检查任务类型。 |
| 检查对象管理 | 监管用户可根据实际检查业务对象范围，将被检查单位导入到检查对象管理中进行信息维护。支持检查对象的导入、查询、详情查看和移除。 |
| 支撑单位管理 | 监管用户可根据实际业务支撑厂商情况，将厂商导入到支撑单位管理中进行信息维护。支持支撑单位的导入、查询、详情查看和移除。 |
| 检查人员管理 | 监管用户可根据实际业务支撑人员情况，将厂商侧网安专家导入到支撑人员管理中进行信息维护。支持支撑人员的导入、查询、详情查看和移除。 |
| **考核评估** | 考评报告 | 考评报告检索、查看、下载、删除，报告想起展示。 |
| 考评任务 | 创建考评任务，展示任务详情，多字段任务检索，考评任务维护。 |
| 考评规则 | 考评规则打分设置。 |
| **处置通报** | 事项看板 | 展示当前用户相关的通报和预警信息，包括待我处置、我跟踪的、抄送我的通报以及已读、未读的预警通知信息。 |
| 通报总览 | 多维度统计展示通报预警工作开展情况，支持地区、行业、单位等维度统计展示。 |
| 通知管理 | 对日常工作相关事件发出通知信息，告知相关单位，可以索要已读回执。 |
| 预警管理 | 对网络安全事件或威胁发出预警信息，警示相关单位，可以索要已读回执。 |
| 通报管理 | 根据安全事件或风险隐患发布通报，督促相关单位妥善处置网络安全事件。 |
| 规范文件 | 展示通报预警模块相关法律规范依据文档。 |
| 通报外发审批 | 可以通报外发审批功能，支持新增事件通报、隐患通报、预警、通知等操作。 |
| 通报文件导入 | 导入加密的通报文件并查看，支持多维度列表查询。 |
| 上级督办 | 展示上级下方的督办信息，支持对督办信息进行查看、督办等操作。 |
| 督办管理 | 展示安全事件、风险隐患督办信息展示，可以查看详情，进行督办或者通报操作。 |
| 通报归档 | 对已完成的上下级平台通报进行归档，支持第三方通报归档。 |
| 上级通报系统对接 | 汇总展示上级平台下发通报、预警信息的。 展示上级平台发布的安全事件或风险隐患通报。 展示上级发出的通报信息，可以多维度检索、开启关闭通报信息。 展示上级发出的预警信息，可以多维度检索和开启关闭预警信息。 |
| **事件案例** | 智慧搜索 | 全平台数据资源的搜索和展示，支持全库搜、精准搜、场景搜等搜索方式。 |
| 情报库 | 情报数据信息的检索、展示。 |
| 事件库 | 安全事件数据信息的检索、展示。 |
| 案件库 | 案件数据信息的检索、展示。 |
| 关基基础信息库 | 关基基础信息（单位、系统、人员、机房）数据信息的检索、展示。 |
| 网络资产库 | 网络资产数据信息的检索、展示。 |
| 木马病毒库 | 木马病毒库数据信息的检索、展示。 |
| 恶意IP库 | 恶意IP库数据信息的检索、展示。 |
| 恶意域名库 | 恶意域名库数据信息的检索、展示。 |
| 等级保护基础库 | 等级保护基础（单位、系统）数据信息的检索、展示。 |
| 漏洞库 | 漏洞库数据信息的检索、展示。 |
| 情报专刊 | 根据互联网上的最新爆发的安全漏洞或者其他影响较大的安全隐患进行分析，对可能受到影响的资产进行分析，给各区域监管单位提供相关安全威胁隐患的数据 |
| 情报查询 | 通过输入IP、域名、文件HASH(MD5/SHA1/SHA256)、邮箱进行情报查询，展示查相关情报类型、情报源、情报标签、地理位置、置信度、运营商及组织名称信息。 |
| **应急指挥** | 单次活动管理 | 支持用户新增安保活动并对该活动进行管理，支持下钻到具体某个活动，查看活动详情 |
| 作战台 | 展示活动进程、信息公告、待办工作/跟进工作、快捷方式、个人信息 |
| 里程碑管理 | 支持对单次活动的里程碑进行管理 |
| 指挥中心 | 提供安保活动指挥单位和人员的选择添加、查看、退出活动、查询功能 |
| 安保目标 | 提供安保活动重点保障单位、人员和系统的选择添加、查看、退出活动、查询功能。 |
| 支撑力量 | 协助安保组完成该次安保活动的单位和人员，提供选择添加、查看、退出活动、查询功能。 |
| 信息公告 | 提供以指挥人员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 | 支持指挥人员维护该次安保活动的各项规章制度，并支持安保活动各方参与人员查看对应的规章制度。 |
| 应急预案 | 应急预案支持针对预先定义的预案名称、预案等级、预案分类、提交单位、提交时间和对应的操作项进行相应操作，并可以查询统计 |
| 安保驻点端 | 系统提供驻点小组安排本小组的值守排班计划的功能。对于驻点小组主要需要管理安保期间，每一天，每一个班次的人员，因此该部分模块展示的该小组每一天、每一个班次的值守人员通过修改等操作可以设置该次安保活动的排班频率，并可以对各个安保驻点上报驻点的排班计划， |
| 指挥中心端 | 安保组视角，对于安保组主要需要查看每一天每个驻点是由谁值守，并能查看该驻点当天的排班计划支持宏观查看活动期间的排班数量情况、报平安数量情况，以及深度查看安保期间每天，每个驻点每个班次的人员值班情况、签到签退时间、报平安状态、每个驻点在安保期间的排班计划等情况。 |
| 值守移动端协同 | 平台支持安保值守人员使用在手机APP钉钉上完成确定驻点各个班次的人员及签到、签退和报平安等操作。上述信息会同步到平台，并进行统计。 |
| 指挥调度 | 指挥中心通过切换总览、监测调度、通报、值守视图，来统筹协调赛事期间的网络安全事件处理。 支持查看战前各重点保障单位的安保检查情况，战时回复和处置报平安情况、安全事件上报及通报情况、查看下发的应急处置任务进展情况，战后通过活动快照查看历史活动成果。 借助视图切换，一键下发通报、检查、指令，联动移动端组织调度，运用应急预案响应应急处置。 |
| **全链路可视化** | 综合态势 | 以监管运营视角出发，通过对管辖区域内单位、业务系统、IP资产、新业态资产摸底，结合多方安全数据情报、本地安全数据治理成果、业务开展情况数据，实现一张屏看清资产底数，实时掌握安全事件、风险隐患处置效率，并支持从区域、行业、境内、境外多维度展现安全情况。 |
| 网络空间安全监测 | 通过可视化的大屏展示辖区内设备部署情况、安全监测情况，方便用户掌握辖区内设备运行情况。 |
| 大数据平台安全态势 | 以大数据平台为切入点，通过对大数据平台资产、用途分类、服务范围、行业分布情况等多维度展示，全面解析全网大数据资产，实时监控大数据安全情况，达到全方位掌控大数据的安全情况。 |
| 云平台安全态势 | 以云平台为切入点，通过对云平台资产、用途分类、服务范围、行业分布情况等多维度展示，实时监控云平台安全情况，达到全方位掌控云平台的安全情况。 |
| Web业务系统态势 | 数据大屏直观展示Web业务系统态势，实时统计分析当天Web业务系统态势相关数据，包括进出流量、访问量、攻击量、网站区域访问量、访问区域、访问IP排行、访问攻击路线、详细攻击信息、网站攻击趋势、被攻击网站排行、攻击IP排行、攻击类型排行等数据。 |
| 攻击者追踪溯源 | 攻击者可视化溯源分析大屏，为安全运维人员提供包括攻击行为分析、团伙分析、攻击取证信息、攻击趋势、攻击手段，攻击影响范围等信息；以攻击IP为中心，对该IP产生的告警类型、所攻击的受害主机IP，以及使用攻击手段类似相似IP等信息进行展示。支持任意攻击者信息查询，可生成详细的攻击者溯源报告，并能够一键导出报告。 |
| 资产威胁溯源 | 资产威胁溯源大屏从资产的角度考虑，为安全运维人员提供包括被攻击行为分析、影响资产范围分析、攻击取证信息等；可呈现被访问趋势、被攻击趋势、被攻击手段、资产状态，资产评分等信息。帮助用户分析现有资产安全状况，了解资产被攻击详情，帮助事后取证溯源。 |
| 行为轨迹溯源 | 追踪网络实体的连接关系，发现访问行为的蛛丝马迹。大数据标签画像分析寻找相似的受害团体和黑客组织，AI算法加持发现观测指标中隐藏的未知威胁，情报、弱点信息辅助异常记录的追根溯源。 |
| AI异常分析 | 通过模型管理支持针对不同类型的数据采集与处理（全部日志soc接收解析后统一放入原始日志中），配置对应的监控模型策略（规则模型、统计模型、关联模型、AI模型、其他）及告警策略（处理结果统一放入异常记录中，当模型中标记为安全时放入安全告警中）。在元数据统一管理下，用户可以根据不同的关注领域灵活操作，包括告警时，放入异常记录中同对数据处理逻辑的新增、删除、修改、查询、启动、停止等。 |
| **全链路可视化-全局概览** | 地理环境 | 以地理图谱为基础支持单位打点，并能对存在风险的单位进行特殊打点，点击支持查看单位概览信息 支持对单位进行统计展示，包括风险单位量、重点单位量、全部单位量、单位行业统计信息，同时支持重点、风险单位切换功能 支持查看单位档案详情信息，包括单位名称、所属行业、单位类型、所属监管单位、单位负责人、负责人职务等基本描述字段，同时支持对单位衍生内容的补充包括人员信息、等保相关信息、实时监测信息、归属系统、归属IP资产 |
| 网络环境 | 支持系统、设备两类内容的打点 支持系统进行地图打点，并能对其进行统计展示，包括重点系统量、全部系统量、系统风险变化趋势 支持设备进行地图打点，并能对其进行统计展示，包括括设备在线情况、安全专项情况 支持对系统进行全方位的描述，包括系统名称、系统域名、业务类型、归属单位、使用时间等基本描述字段，同时支持对系统衍生内容的补充包括人员信息、单位信息、等保相关信息、实时监测信息以及基础网络信息 支持对设备进行全方位的描述，包括设备基本信息、部署单位信息、上报日志量、上报攻击量、上报趋势、覆盖系统信息、发现攻击列表信息、发现原始日志列表信息 |
| 行为主体 | 支持人员打点，点击支持查看人员概览信息 支持对人员进行统计展示，包括重点人员量、风险人员量、全部人员量、人员行业分布、人员标签 支持对人员进行全方位的描述，包括姓名、固定电话、移动电话、身份证号、曾用名等不少于12个基本描述字段，同时支持对人员衍生内容的补充包括网络身份、人物标签、所属单位、所负责系统 |
| 业务环境 | 支持安全事件、风险隐患、通报管理、侦查调查四类内容的打点 支持通报打点，点击支持查看通报概览信息并支持统计展示，包括通报总数、完成效率、平均耗时、通报状态情况 支持调查打点，点击支持查看调查概览信息并支持对调查进行统计展示，包括调查总数、完成效率、平均耗时、调查状态 支持事件打点，点击支持查看事件概览信息并支持对事件进行统计展示，包括事件总数、各级别事件数量、事件类型情况、事件趋势情况 支持隐患打点，点击支持查看隐患概览信息并支持对隐患进行统计展示，包括隐患总数、各级别隐患数量、隐患类型情况、隐患趋势情况 |
| **系统管理** | 运维告警 | 运维告警管理，告警趋势、告警详情展示，告警检索 |
| 健康检查 | 对平台自身健康进行展示，对平台使用情况、组件节点状态、集群状态、接口开放状态等进行巡检，巡检结果以不同的图标进行展示，并加以结果描述及处置建议，使用户可精确定位系统故障并对其进行修复 |
| 存储管理 | 对平台存储情况进行展示，展示磁盘使用情况和磁盘使用趋势 |
| 故障日志 | 可对系统日志进行下载，支持不同组件的区分下载。 |
| 系统配置 | 平台通用配置中心，包括对应系统配置、内部IP配置、钉钉微应用配置、界面配置、工作台配置、级联配置和门户配置 |
| 数据配置 | 用于平台数据存储的生命周期管理。 |
| 推送配置 | 用于对告警信息的推送方式，支持邮件、短信、钉钉三种方式。 |
| 升级管理 | 展示平台版本信息，导入升级包进行升级，查看平台升级历史 |
| 许可证 | 用于系统许可导入。 |
| 监测总览 | 监测数据总览，累计上报数据统计、检索 |
| 分级部署 | 平台分级部署设置 |
| 上级协同 | 注册上级单位，制定数据推送策略 |
| 下级协同 | 注册下级单位，制定数据推送策略 |
| 流计算任务 | 对系统当前的流计算任务进行管理与监控 |
| 定时任务 | 系统内置的定时任务，可对任务状态进行查询。 |
| 数据推送 | 启动、关闭数据推送服务 |
| 数据加载 | 启动、关闭数据加载服务 |
| 数据同步日志 | 数据同步日志展示、查询 |
| 数据安全大脑 | 安全数据大脑对接配置和数据推送配置 |
| 移动互联网 | 第三方厂家app数据对接配置 |
| 业务流程配置 | 业务流程节点开关配置 |
| 网站监测 | 网站监测平台对接配置和数据推送配置 |
| 账号审批 | 单位账号申请审核 |
| 注册配置管理 | 注册服务、短信验证配置管理 |

1. **日志采集探针功能指标要求**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发  支持ka\*\*a日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能，Ka\*\*a收发支持SSL加密  支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器  支持通过界面自定义字段方式实现与第三方平台的数据共享，快速满足第三方平台个性化分析和对接需求。  支持配置平台信息，包括logo、名称及版权信息。 |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集，提供截图证明。  可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。  支持目前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；  支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 日志分析 | 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展；  内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景  三维关联分析；支持通过资产、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，提供截图证明。 |
| 性能监控 | 支持监控设备自身CPU、内存、磁盘等工作运行状况；  通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息 |
| 地理安全系统 | 内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图；  支持用地理地图展示来源威胁的趋势；  支持用地理地图展示目的威胁的趋势； |
| 综合查询及报表管理 | 内置合规性报表1000+种；  内置SOX、ISO27001、WEB安全等解决方案包；  内置完善的等级保护合规报表； |
| 用户管理 | 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户  提供一键式故障排除功能；  提供自助式的升级接口，支持对产品升级、规则升级。 |

1. **流量采集探针功能指标要求**

|  |  |
| --- | --- |
| **技术指标** | **技术要求** |
| 全流量检测 | 支持全流量检测，可根据需求打开或关闭全流量检测功能 |
| IPv4 & IPv6网络 | 支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6网络流量分析检测 |
| 风险数据包保存 | 支持风险数据包保存功能，可存留会话的请求和相应数据包，帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置wireshark组件在线预览风险数据包 |
| 数据包去重 | 支持数据包去重功能，在原始流量存在重复包的情况下能够自动剔除重复的数据包，确保分析结果的准确性，数据包去重功能不影响设备的处理性能 |
| 审计协议 | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；  支持识别QQ、WEB、LDAP、FTP、TELNET、邮件、SMB、RADMIN、ORACLE、MSSQL、SYBASE、MYSQL、DB2、postgreSQL、REDIS等登录行为；  支持多层 VLAN、VXLAN、MPLS、GRE、VN-Tag等网络流量的解析检测 |
| 协议自动识别 | 支持非标端口下的常规协议自动识别、解析和威胁检测功能，包括HTTP/FTP/IMAP/SMTP/POP3/SSL/SMB/RDP等；可自定义是否启用该功能 |
| 检测风险类别 | 支持检测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 |
| 弱口令风险检测 | 支持对HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP等协议的弱口令检测  支持自定义弱口令规则配置（最短口令长度、最少字符类型数），自定义新增弱密码及其检测类型  支持对HTTP协议请求头中用户认证弱口令、对JSON格式(逗号分割和冒号区分键值)的用户信息提取和弱口令、明文口令和MD5加密口令碰撞的弱口令、BASE64加密口令的弱口令等进行检测 |
| WEB登录 | 支持自定义HTTP登录行为关键字，包括用户名和密码  支持自定义HTTP登录行为的用户名获取来源，包括但不限于请求头、URL、Cookie、POST-body；支持自定义配置状态码、返回内容与登陆成功/失败状态的绑定关系 |
| 暴力破解检测 | 支持HTTP、SMB、SMTP、IMAP、POP3、FTP、TELNET、RADMIN、SSH、RDP、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PGSQL、LDAP等协议的暴力破解，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态  支持自定义启用/禁用暴力破解模型；并支持自定义配置模型统计周期、登录次数、聚合维度、检测机制等参数 |
| 扫描行为检测 | 支持IP、端口、SMB、Radmin、ICMP、ARP、传输层协议和漏洞扫描行为检测  支持自定义启用/禁用扫描行为模型；并支持自定义配置模型统计周期、访问次数等参数 |
| 拒绝服务攻击检测 | 支持UDP FLOOD、DNS FLOOD、NTP FLOOD、Chargen FLOOD、SNMP FLOOD、SSDP FLOOD、 Memcached FLOOD、SYN FLOOD、RST FLOOD、FIN FLOOD、ACK FLOOD、HTTP FLOOD、ICMP FLOOD、SEANET\_FLOOD  检测  支持自定义启用/禁用拒绝服务攻击模型；并支持自定义配置模型统计周期、单包长度阈值、统计周期内包数量阈值等参数 |
| 密码明文形式传播 | 支持HTTP密码明文传输和HTTP 密码Base64传输检测，能识别出登录页面URL、账户和明文密码 |
| ARP欺骗检测 | 支持根据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 |
| IP检测配置 | 支持IP过滤配置，可配置IP、端口或IP对和端口的方式对网络流量进行过滤；可通过新增、批量导入等方式完成IP过滤的配置  支持对指定IP进行流量检测，可通过新增、批量导入等方式完成指定IP检测的配置 |
| UDP端口过滤 | 支持UDP端口过滤配置，对指定端口的网络流量不做分析检测 |
| 告警详细展现 | 支持详细展现风险等级、时间、威胁名称、攻击状态、攻击方向、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、端口、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度、ATT&CK矩阵等信息，并提供相应的数据包下载链接 |
| 主机威胁分析 | 支持对内网主机进行主机威胁分析，详细展示具体的威胁等级、威胁次数、攻击开始时间、攻击结束时间、威胁性指数统计等（提供截图证明）  可按攻击链阶段（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）详细展示主机相关事件数量 |
| 可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析  支持攻击路径可视化，直观展示攻击过程和扩散过程，可呈现从外向内、从内向外和内部之间的攻击事件 |
| 可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示 |
| 攻击者视角分析 | 可基于该页面，快速获悉攻击者IP、攻击手段和攻击资产，并支持导出攻击者列表，便于威胁分析人员快速应对和处置 |
| 受害者视角分析 | 可基于该页面，快速获悉受攻击的资产，及其对应的攻击者数量、攻击手段、攻击次数等，并支持导出受害者列表，便于威胁分析人员快速应对和处置 |
| 脆弱性分析 | 从脆弱性角度，详细展示资产存在的弱口令、密码明文形式传输风险，以及自定义配置的特权账户是否存在弱口令风险  支持导出资产IP、资产标签、被请求域名、首次发生时间、最近一次发生时间等信息，便于威胁分析人员快速统计和上报资产脆弱性风险 |
| 威胁情报检索 | 支持对IP、域名、恶意文件SHA256进行威胁情报检索，或跳转第三方链接（Whois、VirusTotal）进行检索 |
| 敏感信息分析 | 支持识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置 |
| 攻击地图展示 | 可通过攻击源和目的的地理位置信息，以世界地图和中国地图的形式展示，并可切换世界地图和中国地图以直观展示攻击路径 |
| PCAP文件上传 | 支持上传PCAP包进行回放分析 |
| **WEB攻击检测** | |
| 协议解析 | 支持HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测WEB攻击 |
| 双向审计 | 支持双向审计，对请求和响应都进行审计 |
| 攻击检测 | 支持SQL注入、命令注入、跨站脚本、代码注入、WEB扫描或爬虫、网页篡改、服务错误攻击检测  支持通过智能语义分析引擎，对XSS跨站脚本、SQL注入攻击和OGNL注入攻击进行检测  支持通过智能语义分析引擎，检测JSP脚本文件上传和PHP脚本文件上传 |
| WEBSHELL检测 | 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功（提供截图证明） |
| 自定义规则 | 支持根据规则类型、协议、源IP/端口、目的IP/端口、流量方向、流量状态、风险类别、风险等级、风险阶段、攻击者、攻击状态、阈值、Flowbits、规则内容等自定义审计规则  支持自定义配置旁路阻断规则，阻断TCP会话 |
| 动态分析 | 自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等 |
| 场景化分析 | 支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警。 |
| DNS协议分析 | 具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为。 |
| 与WAF联动 | 支持将分析到的WEBSHELL攻击、木马回连和恶意攻击行为同步到WAF，实现APT深度威胁分析与WAF联动阻断（提供截图证明） |
| 与防火墙联动 | 支持将分析到的SMB远程溢出攻击、扫描行为、Web后门访问、隧道通信、暴力破解、挖矿、远控工具利用等攻击成功事件同步到防火墙，实现APT深度威胁分析与防火墙联动阻断（提供截图证明）  支持自定义防火墙阻断时长，并展示最新联动状态、状态更新时间  支持查看阻断信息，阻断信息包括阻断IP、阻断开始时间、阻断结束时间、阻断状态等  支持自定义添加防火墙阻断IP白名单 |
| **Mail攻击检测** | |
| 协议解析 | 支持解析webmail、SMTP、POP3、IMAP、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）类型报文 |
| 社工类攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接（提供截图证明） |
| 恶意附件检测 | 支持邮件恶意附件行为检测 |
| **文件攻击检测** | |
| 解析协议 | 支持HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测 |
| 文件类型 | 支持doc, xls, ppt, swf, pdf, rar, zip, rar, exe, vbs, scr、ps1、elf等多种文件解析 |
| 自定义分离文件类型 | 可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP可进一步按GET、POST来配置） |
| 恶意文件MD5 | 支持自定义新增或批量导入恶意文件MD5值进行文件威胁检测，可配置内容包括文件MD5、恶意信息描述和参考链接 |
| 文件分析 | 支持自定义上传文件样本进行威胁分析  支持批量上传文件 |
| 特征检测 | 对文件进行特征匹配，利用已知的特征库发现恶意的可执行文件及非可执行文件。 |
| Shellcode检测 | 通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击（提供截图证明） |
| 多引擎在线检测 | 与国际领先的反病毒引擎深度结合，支持对文件的MD5值进行多引擎在线检测，检测结果中包括MD5、扫描时间、病毒引擎总数、引擎检出数、SHA1、SHA256和引擎检出列表 |
| 动态沙箱检测 | 对存在恶意行为的文件输出完整的二进制动态分析报告  动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险（提供截图证明）  可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容  可展示ROP行为检测  可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、返回结果、返回值等信息  可显示文件运行过程中企图访问的IP、域名，以及域名及对应的IP  支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现  采用多并发沙箱检测技术，集成主流的操作系统winXP、win7、win10、linux等多种检测环境，结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析 |
| 子文件扫描 | 对文件内部嵌入的子文件可进行二次扫描，分析安全性（提供截图证明） |
| 检测结果复用 | 文件MD5值相同时，支持自定义配置检测结果是否复用 |
| 压缩文件子文件格式识别 | 支持自定义配置是否识别压缩文件中子文件的真实格式 |
| 自定义YARA规则设置 | 支持导入自定义YARA规则，可从静态文件和运行内存中检测文件威胁  支持单个规则或多个规则累加告警  支持从规则状态、类型、等级、描述等方面进行自定义配置 |
| 沙箱操作系统设置 | 支持自定义配置不同沙箱操作系统的超时时间和检测文件类型 |
| 攻击样本提取 | 可以提取出攻击的完整样本文件，并提供对该文件下载的能力 |
| 文件威胁指数 | 可展示威胁程度最高的文件样本MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容 |
| 根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告（提供截图证明） |
| 根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等 |
| 回连域名/IP | 支持提取恶意文件在沙箱虚拟机中运行时回连的域名和IP，并支持将回连域名和IP添加进威胁情报 |
| **失陷主机检测** | |
| 远程控制检测 | 支持根据威胁情报、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 |
| DGA域名请求检测 | 具备DNS协议解析功能，发现发起DGA域名请求的失陷主机 |
| 挖矿行为检测 | 可发现利用失陷主机挖矿的行为 |
| 失陷主机分析 | 支持以失陷主机维度进行分析，分析内容包括失陷主机IP、MAC地址、攻击类型、访问次数、攻击开始时间、攻击结束时间 |
| **威胁情报与APT云端** | |
| 本地威胁情报 | 设备集成离线的高可用威胁情报库，支持离线环境下，根据威胁情报进行检测，增量威胁情报随策略升级包升级 |
| 威胁情报检索 | 支持对IP、域名、恶意文件SHA256进行威胁情报检索，或跳转第三方链接（Whois、VirusTotal）进行检索  支持在告警详情页面直接查询与告警IP、域名相关的威胁情报，获取样本通信记录、情报画像等信息 |
| 云端威胁情报 | 支持自动从APT云端获取最新威胁情报  支持域名白名单同步云端 |
| 代理服务 | 支持使用代理服务器访问云端；支持代理服务器认证 |
| **抓包检测功能** | |
| 抓包任务 | 同时支持至少16个抓包任务抓包，每个抓包任务可配置抓包规则，按照IP、端口、协议等信息进行抓包，将抓取的原始流量包保存于本地以供后续分析和取证使用 |
| **管理功能** | |
| 资产识别和管理 | 支持对流量中的IP地址、端口等进行统计，快速识别未登记资产。可基于特定应用或服务对内部资产进行梳理（系统类型、IP、域名、端口等），查看资产端口暴露情况，特别是以非标端口提供的服务情况；可深入识别运行在资产上的设备类型、应用、服务信息详细情况（类型、版本、服务名称等） |
| 三权分立用户管理 | 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色 |
| 敏感信息管理 | 支持自定义弱密码、暴力破解和密码明文形式传输等告警的密码查看权限 |
| 风险处理 | 支持根据需要对风险状态进行处理，包括处理中、处理完成、延迟处理、拒绝处理等至少四种选择模式，并支持对处理情况进行备注 |
| NAT地址解析 | 支持自定义NAT转换前的IP字段名和字段位置，最多支持5个，并支持对字段名进行优先级排序；可配置不会被NAT转换的代理服务器资产IP |
| 一键登录排错 | 支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、信息收集等功能。  支持在页面实时查看物理内存、共享内存、硬盘分区、硬盘I/O、监听端口、内存占用TOP10进程、CPU占用TOP10进程，无需登录后台，提高设备安全性  支持自定义时间查询和导出设备内存、CPU、磁盘空间的使用状态日志 |
| 设备状态监控 | 支持对设备的CPU、内存等状态进行监控，可查看1个月内的系统资源数据，并通过折线图在界面中展示 |
| 数据外送至第三方平台 | 具备风险数据外送至第三方平台的能力，支持以KA\*\*A、FTP、SFTP、SYSLOG数据接口输出风险信息  具备元数据外送至第三方平台的能力，支持以KA\*\*A、FTP、SFTP、SYSLOG数据接口输出审计信息、会话应用识别信息、会话应用流量统计信息、传输层流量统计、应用层统计信息、登录行为统计信息和文件检测信息  支持元数据按照服务器配置、发送配置、发送情况进行设置。KA\*\*A发送配置可以按照发送状态、主题、服务器列表、服务器响应、服务器版本、加密认证方式、是否需要压缩。支持字段名称禁用和启用进行配置  支持分离流量中的原始文件并通过KA\*\*A方式发送原始文件和文件审计数据  支持根据流量方向选择发送的元数据，包括外网到外网、外网到内网，内网到外网、内网到内网流量  支持根据流量属性选择发送的元数据，包括是否发送白名单IP流量数据、非告警流量数据等 |
| SNMP | 支持通过SNMP协议对设备的系统资源进行监控，包括内存、交换空间、CPU、系统分区、数据分区、探测器分区和入库缓冲分区 |
| **日志报表** | |
| 告警与报表 | 告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、ATT&CK矩阵、报文内容（URL、请求头、请求参数、请求内容） |
| 支持语音告警播报功能，可自定义播报告警的风险类别、风险级别、攻击状态等 |
| 支持ka\*\*a、短信、邮件、syslog、ftp、sftp、钉钉等数据外送方式  syslog、ka\*\*a、sftp和ftp外送方式支持配置多个服务器，分别发送不同业务数据 |
| 支持对ka\*\*a、syslog发送的风险信息进行AES、SM4加密传输  KA\*\*A服务器配置中协议类型支持明文、SSL、SASL认证+明文、SASL认证+SSL、Kerberos认证+SSL等方式 |
| 支持同时发送多人、单条发送、发送统计等高级告警功能； |
| 支持在线预览报表，以及WORD、PDF、HTML等格式导出  设备内置多种维度的报表模版，可从外部攻击、内部主机、样本投递等维度生成报表，并支持自定义选择报表生成的时间范围、报表类型、报表格式  支持批量导出报表及报表订阅功能，可自定义单位名称和Logo，报表订阅的时间纬度包括日报、周报、月报 |
| 日志数据管理 | 审计数据保留策略应至少满足天数和百分比两个控制参数，支持web界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，无法通过撞库、混淆还原等方式解密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间。  设备产生的数据重要程度至少分为3级，可自定义配置不同级别数据的清理比重 |
| **服务要求** | |
| 产品成熟度 | 软件著作权证书 |
| 销售许可证（必须是APT安全监测类） |
| 售后服务 | 3年质保，提供3年免费升级与维护服务 |
| 提供24小时支持热线； |
| 提供高级技术分析服务 |

**六、商务条款**

1、付款方式：在合同生效以及具备实施条件后15日内预付合同总价的30%，项目完成并验收合格后30个工作日内支付合同总价的65%，其余5%作为质量保证金（不计息），在质保期满后无质量问题一个月内结清余款（余款不支付利息）。

2、项目交货期：签订合同后60天内完成设备安装，调试，达到验收条件。

3、安装及验收

（1）交货及安装地点：用户指定地点与位置。

（2）供货时间：签订合同后60天内完成设备安装，调试，达到验收条件。

（3）安装标准：符合国家有关安全技术标准，以及所属行业通用技术要求。

（4）验收标准：相关货物据需提供原厂合格证或相关证明，设备包装完好,设备为原包装以确保正品；系统必须经第三方检测，试运行后合格后，出具验收报告。

**第四部分评标方法及评分标准**

**一、评标方法**

**1.综合评分法。**

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。

**二、评标委员会的组成**

**2.评标委员会的组成。**

评标委员会由采购人代表和评审专家组成，成员人数为5人以上单数，其中评审专家不少于成员总数的三分之二。

**3.评标委员会的组成人员的回避。**

在政府采购活动中，评标委员会的组成人员与供应商有下列利害关系之一的，应当回避：

3.1参加采购活动前3年内与供应商存在劳动关系；

3.2参加采购活动前3年内担任供应商的董事、监事；

3.3参加采购活动前3年内是供应商的控股股东或者实际控制人；

3.4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；

3.5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。

**三、评标委员会的职责**

**4.评标委员会负责具体评标事务，并独立履行下列职责：**

4.1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；

4.2要求投标人对投标文件有关事项作出澄清或者说明；

4.3对投标文件进行比较和评价；

4.4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；

4.5向采购人、采购机构或者有关部门报告评标中发现的违法行为；

4.6法律、法规、规章、招标文件等规定的其它事项。

**5.评标委员会及其成员不得有下列行为：**

5.1确定参与评标至评标结束前私自接触投标人；

5.2接受投标人提出的与投标文件不一致的澄清或者说明，本办法第五十一条规定的情形除外；

5.3违反评标纪律发表倾向性意见或者征询采购人的倾向性意见；

5.4对需要专业判断的主观评审因素协商评分；

5.5在评标过程中擅离职守，影响评标程序正常进行的；

5.6记录、复制或者带走任何评标资料；

5.7其他不遵守评标纪律的行为。

评标委员会成员有5.1-5.5行为之一的，其评审意见无效，并不得获取评审劳务报酬和报销异地评审差旅费。

**四、评审程序**

**6.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。符合投标无效情形的，投标无效。

**7.投标人澄清、说明或者补正。**

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需要投标人作出必要的澄清、说明或者补正的，评标委员会和投标人通过电子交易平台交换数据电文，投标人提交使用电子签名的相关数据电文或通过平台上传加盖公章的扫描件。给予投标人提交澄清、说明或补正的时间不得少于半小时，投标人已经明确表示澄清说明或补正完毕的除外。投标人的澄清、说明或者补正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。

**8.比较与评价。**

评标委员会应当按照评标标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

**9.汇总（商务技术得分情况）。**

评标委员会各成员应当独立对每个投标人的商务和技术文件进行评价，并汇总商务技术得分情况。

**10.报价审核。**

对经商务和技术评审符合采购需求的投标人的报价的合理性、准确性等进行审查核实。

10.1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，有可能影响产品质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料。

10.2根据财政部发布的《政府采购促进中小企业发展暂行办法》规定，对于非专门面向中小企业的项目，对小型和微型企业产品的价格给予一定的扣除，用扣除后的价格参与评审。

10.3投标价格的修正原则。投标文件报价出现前后不一致的，按照下列规定修正：

10.3.1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;

10.3.2大写金额和小写金额不一致的，以大写金额为准;

10.3.3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;

10.3.4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。

10.3.5同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照财政部第87号令《政府采购货物和服务招标投标管理办法》第五十一条第二款的规定经投标人确认后产生约束力。

▲**投标人对根据修正原则修正后的报价不确认的，投标无效。**

**11.汇总得分。**

评标委员会各成员应当独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。

**12.顺序排列与中标候选推荐。**

12.1评标结果按评审后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，按技术指标优劣顺序排列。得分最高的投标人为排名第一的中标候选人。

12.2多家投标人提供相同品牌产品（单一产品采购项目中的该产品或者非单一产品采购项目的核心产品）且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

**13.投标无效。**

有下列情况之一的，投标无效：

13.1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参加同一合同项下的政府采购活动的（均无效）；

13.2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再参加该采购项目的其他采购活动的；

13.3投标人不具备招标文件中规定的资格要求的（投标人未提供有效的资格证明文件的，视为投标人不具备招标文件中规定的资格要求）；

13.4如以联合体形式参加政府采购活动的，联合体协议不符合招标文件规定的联合体协议要求的；

13.5投标文件未按规定的格式编制的；

13.6投标文件未按招标文件的澄清、修改的内容编制，又不符合实质性要求的；

13.7投标文件组成漏项，内容不全或内容字迹模糊辨认不清的；

13.8投标文件中法人授权书所载内容与本项目内容有异的；

13.9投标文件未按照招标文件要求签署、盖章的；

13.10招标文件要求提供样品（含小样），投标人没有提供样品（含小样）的；

13.11采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人未按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的；

13.12投标文件含有采购人不能接受的附加条件的；

13.13投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的；

13.14投标人所投内容不符合采购需求中实质性要求的；

13.15投标文件出现不是唯一的、有选择性投标报价的;

13.16投标报价高于本项目采购预算或者最高限价的;

13.17报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，未能按要求提供书面说明或者提交相关证明材料，不能证明其报价合理性的;

13.18《投标（开标）一览表》填写不完整或字迹不能辨认或有漏项的；

13.19投标人对根据修正原则修正后的报价不确认的；

13.20投标人提供虚假材料投标的（包括但不限于以下情节）；

13.20.1使用伪造、变造的许可证件；

13.20.2提供虚假的财务状况或者业绩；

13.20.3提供虚假的项目负责人或者主要技术人员简历、劳动关系证明；

13.20.4提供虚假的信用状况；

13.20.5其他弄虚作假的行为。

13.21投标人有恶意串通、妨碍其他投标人的竞争行为、损害采购人或者其他投标人的合法权益情形的；有下列情形之一的，属于或视为恶意串通，其投标无效：

13.21.1供应商直接或者间接从采购人或者采购机构处获得其他供应商的相关情况并修改其投标文件或者响应文件；

13.21.2供应商按照采购人或者采购机构的授意撤换、修改投标文件或者响应文件；

13.21.3供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

13.21.4属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

13.21.5供应商之间事先约定由某一特定供应商中标、成交；

13.21.6供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标、成交；

13.21.7供应商与采购人或者采购机构之间、供应商相互之间，为谋求特定供应商中标、成交或者排斥其他供应商的其他串通行为。

13.21.8不同投标人的投标文件由同一单位或者个人编制；

13.21.9不同投标人委托同一单位或者个人办理投标事宜；

13.21.10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；

13.21.11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；

13.21.12不同投标人的投标文件相互混装；

13.22投标人仅提交备份投标文件，没有在电子交易平台传输递交投标文件的，投标无效；

13.23法律、法规、规章（适用本市的）及省级以上规范性文件（适用本市的）规定的其他无效情形。

**五、评标报告**

**14. 评标报告与推荐中标候选人。**

评标委员会根据原始评标记录和评标结果编写评标报告，并通过电子交易平台向采购人、采购机构提交。

**15. 评标争议事项处理。**

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。

**六、废标**

**16.废标。**

根据《中华人民共和国政府采购法》第三十六条之规定，在采购中，出现下列情形之一的，应予废标：

16.1符合专业条件的供应商或者对招标文件作实质响应的供应商不足3家的；

16.2出现影响采购公正的违法、违规行为的；

16.3投标人的报价均超过了采购预算，采购人不能支付的；

16.4因重大变故，采购任务取消的。

废标后，采购机构应当将废标理由通知所有投标人。

**七、重新组织采购**

**17.修改招标文件，重新组织采购活动。**

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，将停止评标工作，并与采购人、采购机构沟通并作书面记录。采购人、采购机构确认后，将修改招标文件，重新组织采购活动。

**18.重新开展采购。**

有政府采购法第七十一条、第七十二条规定的违法行为之一，影响或者可能影响中标、成交结果的，依照下列规定处理：

18.1未确定中标或者成交供应商的，终止本次政府采购活动，重新开展政府采购活动。

18.2已确定中标或者成交供应商但尚未签订政府采购合同的，中标或者成交结果无效，从合格的中标或者成交候选人中另行确定中标或者成交供应商；没有合格的中标或者成交候选人的，重新开展政府采购活动。

18.3政府采购合同已签订但尚未履行的，撤销合同，从合格的中标或者成交候选人中另行确定中标或者成交供应商；没有合格的中标或者成交候选人的，重新开展政府采购活动。

18.4政府采购合同已经履行，给采购人、供应商造成损失的，由责任人承担赔偿责任。

18.5政府采购当事人有其他违反政府采购法或者本条例规定的行为，经改正后仍然影响或者可能影响中标、成交结果或者依法被认定为中标、成交无效的，依照18.1-18.4规定处理。

**八、评审过程的保密与录像**

**19.保密。**

评审活动在严格保密的情况下进行。评审过程中凡是与采购响应文件评审和比较、中标成交供应商推荐等评审有关的情况，以及涉及国家秘密和商业秘密等信息，评审委员会成员、采购人和采购机构工作人员、相关监督人员等与评审有关的人员应当予以保密。

**20.录音录像。**

采购机构对评审工作现场进行全过程录音录像，录音录像资料作为采购项目文件随其他文件一并存档。

**九、具体评标标准**

**21、本项目采用综合评分法**

评标委员会将对各投标人的投标报价、技术和服务方案、投标人提供的资质和业绩情况等方面进行综合评审，评标委员会各成员应当独立对每个有效投标人的投标文件进行评价、打分。经统计，得出各投标人的最终评审分,按最终评审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，按技术指标优劣顺序排列，并形成评标意见。

**公示结束后，经采购人确定，原则上选择第一中标候选人为成交供应商，如第一中标候选人出现无法履约等情形，可选择第二中标候选人为成交供应商。**

**22、分值的计算**

报价得分 = （基准价/报价）×价格权值× 100(精确到小数点后二位，由采购机构当场统一计算)

技术、资信、商务及其他分按照评审小组成员的独立评分结果汇总后的算术平均分计算，计算公式为：技术、资信商务及其他分 = 评审小组所有成员评分合计数/评审小组成员组成人数

**各投标人综合得分 = 投标价格分 + (技术 + 资信商务及其他分)**

**23、评审内容及标准**

**23.1 价格部分（ 15 分）**

价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分按照下列公式计算：

价格分=（评标基准价/投标报价）× 15%×100

**23.2 技术资信商务部分（85分）**

|  |  |  |
| --- | --- | --- |
| **评审因素** | **分值** | **评分细则** |
| **商务分（25分）** | | |
| **投标人实力要求** | **5** | 1.为保障项目质量，在本项目售后服务与维护期间，针对于本项目所产生的数据、模型以及各项成果，投标人具有CMMI 5证书，具备得1分；具有CMMI 4证书，具备得0.5分; 具有CMMI 3证书，具备得0.2分。（1分）  2.投入本项目的项目团队需要具有ISO 27001 主任审核员认证证书、CISSP信息系统安全专业认证证书、CCSK云安全人才认证证书、CISP-BDSA大数据安全分析师认证证书，每提供1项得1分，本项最高得4分。  （提供以上证书原件扫描件加盖投标单位公章，相关人员提供近6个月公司缴纳的社保证明加盖投标单位公章，不加盖公章不得分） |
| **创新研究能力要求** | **3** | 1.因本项目需要和淳安县数据资源中心及第三方共建网络安全创新实验室，投标人需具备一定的创新研究能力，对投标人实验室核心成员参与过市级以上地方标准建设的进行评分，参与过省级及以上标准的，每个得1分；参与过市级地方标准的，每个得0.5分；（1分）  2.对投标人承担过市级及以上科研项目进行评分，参与过省级及以上重大科研项目的，每个得1分；参与过市级重大科研项目的，每个得0.5分。（1分）  3.对投标人建有市级及以上科研载体进行评分，市级及以上重点企业研究院、市级技术研究中心，每个得0.5分。（1分）  （提供以上相关证明材料原件扫描件加盖投标单位公章，不盖公章不得分） |
| **项目建设能力成熟度要求** | **5** | 为保证投标人充分理解并深度参与数据主管部门的业务体系，提供实现省市县三级贯通的同类合同的，每个得3分；提供实现市县二级贯通的同类合同，每个加2分，最高得5分；  （证明材料：提供合同及验收证明材料复印件加盖公章，同一用户不累计得分。） |
| **制度建设能力要求** | **4** | 结合本项目制度建设要求，投标人需提供对应的制度建设经验证明，包括但不限于数据安全制度验收清单，数据安全类合同（涵盖数据安全制度建设）等，每提供一项得2分，不提供不得分，本项最高得4分。 |
| **售后服务** | **4** | 投标人提供的售后服务方案、售后服务承诺的可行性、完整性以及服务承诺落实的保障措施，维护期内外的后续技术支持和维护能力情况等；对服务承诺的保障措施，是否满足采购人的要求等。4分 |
| **3** | 投标人安排驻场人员工作履历情况及售后服务方案的响应时间、人员安排方案，根据投标人提供的售后服务承诺是否切实可行。3分 |
| **1** | 投标人承诺驻场人员具备两年以上同类工作经验，并获得国家软考网络工程师证书或CCRC证书或HCNP或同等级别证书。得1分 |
| **技术分**（60分） | | |
| **投标产品响应程度** | **18** | 根据投标人提供的技术方案，与招标文件要求的技术标准要求符合性进行打分。满足招标文件明确的全部技术条款要求的得满分18分：产品截图等证明材料低于产品功能指标要求的（负偏离）的每项扣1分，扣完为止。  注：技术偏离表技术要求中响应规格与技术支持资料不一致的经评标委员会讨论后可被认定为负偏离。 |
| **技术服务方案** | **11** | 投标人提供的技术服务方案中是否详细阐述了以下内容：  1.依据《浙江省政务外网安全运行监测指标（试行）》要求，从资产监测、可用性监测、事件监测、隐患监测、监测周期、监测方式几方面判定能否要求，服务方案能满足上述要求的得5分，服务方案能基本满足上述要求的得2分，服务方案不能满足上述要求的得不得分。（6分）  2.为保障满足市局的数据安全监管要求，本项目需提供与上级数据管控平台的数据对接方案。对接要求的阐述全面、合理、针对性强的得5分，阐述理解不全面、针对性一般的得3分，有明显缺陷或理解上有明显的逻辑性错误的得1分，不提供者不得分。（5分）  （根据以上每一项内容的合理性和响应程度进行打分） |
| **服务质量** | **5** | 投标人是否按招标人要求提出了明确的服务质量目标、服务质量保证措施等内容，由评审专家进行综合评议。 |
| **项目进度计划** | **5** | 投标人是否提出了详细的组织实施方案和实施进度计划，含工作时间进度计划、工作程序和步骤、管理和协调方法、关键步骤的思路和要点等，由评审专家综合评议。 |
| **培训计划** | **3** | 投标人是否提出了详细的培训计划，含课程概要、课程目的、培训对象、教学方式、师资力量等，由评审专家综合评议。 |
| **服务承诺、响应** | **3** | 投标人提供的售后服务方案、售后服务承诺的可行性、完整性以及服务承诺落实的保障措施，维护期内外的后续技术支持和维护能力情况等内容进行综合评价。 |
| **系统演示** | **15** | 投标人需对全链路网络安全监管平台进行演示，根据投标人演示的相应内容，由评审专家根据演示情况是否满足招标需求进行判定评分，最高得15分。演示时间不超过15分钟。（本项不接受图片、PPT、Axure等高保真演示。）1.一屏掌控能力：根据可视化演示“指令直达、层层钻钻、闭环处置”能力进行评分。（３分）  2.监测指标维度：根据监测的“云、网、数、用、端”等维度进行评分。（３分）3.一体化能力：根据与省市级网络安全管控平台融合能力、与县级部门和乡镇向下颗粒度细化能力进行评分。（３分）4.网络安全应用能力：根据提供的全链路网络安全实战、实用、实效能力进行评分。（3分）  5.数据安全应用能力：根据提供的全生命周期数据安全实战、实用、实效能力进行评分。（3分）  注：演示视频20分钟内。 |

**注：响应方所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有（且在有效期内）。**

**第五部分拟签订的合同文本**

**（以最终合同为准）**

淳安县政府采购合同

**（本合同为合同样稿，最终稿由双方协商后确定）**

**合同编号：**

根据《中华人民共和国政府采购法》和《中华人民共和国合同法》等相关法律、法规和政策，在平等、自愿、协商一致的基础上，就采购人委托中标人（经评审最终确定的成交供应商）对淳安县全链路网络安全监管平台（一期）建设采购项目订立本合同。

**第一条定义**

1.“合同”即由采购人、中标人共同签订的合同格式中的文件，包括所有的附件、附录和组成合同部分的所有其他文件。

合同将由采购人淳安县人民政府办公室（以下简称甲方）与经评审最终确定的中标人（以下简称乙方）结合本项目具体情况协商后分别签订。以下为甲方提出涉及乙方的主要条款，乙方在投标文件中应对其进行确认或拒绝。如乙方在其投标文件中未做拒绝或提出修改要求的，甲方将视作认同。

2.“合同价格”系指根据合同规定，在乙方全面正确地履行合同义务时，甲方应支付给乙方的款项。

3.“技术服务”系指乙方按投标文件规定，结合本项目的性质特点，对淳安县全链路网络安全监管平台（一期）建设采购项目运行管理定位、目标，为甲方提供优质的服务。

4.“验收”系指甲方依据国家有关规定接受合同所依据的程序和条件。

**第二条适用范围**

本合同条款适用于本次采购活动。项目实施范围详见附件——投标文件和投标文件及补充文件、承诺书等。

**第三条委托事项**

（具体内容详见招标文件）。

**第四条服务期限**

**第五条费用结算方式**

第六条履约保证金

本项目不需要交纳履约保证金。

3. 投标文件规定的其他内容。

**第八条乙方对甲方作出如下承诺**：

**第九条甲方对乙方作出如下承诺：**

**第十条合同生效**：

本合同经甲乙双方法定代表人或其授权代表签字盖章后生效。

**第十一条双方权利义务**

**1. 甲方权利义务**

**2. 乙方权利义务**

**第十二条乙方的人员配置**

**第十三条争议处理**

1．合同在履行过程中发生争议时，甲方与乙方及时协商解决。协商不成时，提请淳安仲裁委员会根据仲裁规则仲裁。

2．对于因违反或终止合同而引起的损失、损害的赔偿，由甲方与乙方友好协商解决，经协商仍未能达成一致的，提交淳安仲裁委员会仲裁。

**第十四条其他**

1．未经过甲方的书面同意，乙方不得转让其应履行的合同项下的义务，和将部分合同项下的义务分包给其他单位完成。

2．乙方不得参与可能与合同规定的与甲方的利益相冲突的任何活动。

3．乙方人员在甲方场地工作时，应遵守甲方相关规章、制度。

4．本合同任何一方给另一方的通知，都应以书面或电传/传真/电报的形式发送，而另一方应以书面形式确认并发送到对方明确的地址。

5．合同履行期内甲乙双方均不得随意变更或解除合同。合同若有未尽事宜，需经双方共同协商，订立补充协议，补充协议与本合同有同等法律效力。

6．投标文件（编号：号）、投标文件及评标过程中形成的文字资料、询标纪要均作为本合同的组成部分，具有同等效力。

7．本合同一式份，甲方执份、乙方执份、采购代理机构执一份。

8．适用法律：本合同应按照中华人民共和国的法律进行解释。

甲方（盖章）：乙方（盖章）：

法定代表人或受委托人（签字）：法定代表人或受委托人（签字）：

联系人：联系人：

地址：地址：

电话和传真：电话传真：

开户银行：开户银行：

帐号：帐号：

签约地点：

签约日期：2021年月日

鉴证方（盖章）：

法定代表人或受委托人（签字）：

★此仅为合同书样本，中标单位需根据实际情况和采购人签订相应的合同！

**第六部分应提交的有关格式范例**

投标人按照以下格式编制投标文件。

▲**资格文件部分**

**目录**

（1）营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，须提供自然人的身份证明）………………………………………………（页码）

（2）法人授权书………………………………………………………………（页码）

（3）授权代表的身份证（复印件）………………………………………………（页码）

（4）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…………………………………………………………………………（页码）

（5）具有履行合同所必需的设备和专业技术能力的承诺函……………………（页码）

（6）参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明（页码）

（7）具有良好商业信誉特别声明…………………………………………………（页码）

（8）符合特定资格条件（如果项目要求）的有关证明材料（复印件）………（页码）

（9）以联合体形式投标的，提供联合体协议；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……………………………………………（页码）

**一、营业执照或事业法人登记证证明材料（复印件）**

投标人名称(电子签名)：

日期：年月

**二、法人授权书**

淳安县人民政府办公室、浙江辰光管理有限公司：

兹委派我公司先生/女士(其在本公司的职务是：，联系电话：手机：传真：)，代表我公司全权处理淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：】政府采购投标的一切事项，若中标则全权代表本公司签订相关合同，并负责处理合同履行等事宜。

本授权书有效期：自年月日起至年月日止。

特此告知。

投标人名称(电子签名)：

签发日期：年月日

**联合体投标授权书（适用联合体投标）**

兹委派公司先生/女士(其在该公司的职务是：，联系电话：手机：传真：)；……，代表本联合体全权处理淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：】政府采购投标的一切事项，若中标则全权代表本联合体签订相关合同，并负责处理合同履行等事宜。

本授权书有效期：自年月日起至年月日止。

特此告知。

单位：（电子签名）单位：（电子签名）

日期：年月日日期：年月日

……

**三、授权代表的身份证（复印件）**

身份证件扫描件：

|  |
| --- |
| 正面：反面： |

投标人名称(电子签名)：

日期：年月

**四、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**

淳安县人民政府办公室、浙江辰光管理有限公司：

我方郑重承诺，我方符合参与淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：】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。

投标人名称(电子签名)：

日期：年月

**五、具有履行合同所必需的设备和专业技术能力的承诺函**

淳安县人民政府办公室、浙江辰光管理有限公司：

我方郑重承诺，我方具有履行淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：】合同所必需的设备和专业技术能力。如中标，我方将保证合同顺利履行。

投标人名称(电子签名)：

日期：年月日

1. **参加政府采购活动前三年内，在经营活动中**

**没有重大违法记录的声明**

淳安县人民政府办公室、浙江辰光管理有限公司：：

我方声明投标截止时间前三年，在经营活动中没有重大违法记录。

投标人名称(电子签名)：

日期：年月日

**七、具有良好商业信誉特别声明**

淳安县人民政府办公室、浙江辰光管理有限公司：：

截至投标截止时间，我方具有良好的商业信誉，不存在下列情形（包括但不限于）。否则，我方将承担在资格审查时不被通过的后果。

1**、**按照招标文件规定的信用信息查询渠道及截止时间，经查询列入失信被执行人名单、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；

2、截至投标截止时间，因违反《浙江省政府采购供应商注册及诚信管理暂行办法》而被列入‘黑名单’，在处罚有效期内。

投标人名称(电子签名)：

日期：年月日

**八、特定资格条件要求的资质文件（复印件）**

（由投标人根据招标公告合格的投标人应具备的特定资格要求编制；如果本项目没有设置特定资格条件，则不需要提供）

**九、联合体协议**

（以联合体形式投标的，提供联合体协议；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）

甲方：

乙方：

……

各方经协商一致，决定组成一个联合体，以一个投标人的身份就淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：】共同投标。

一、各方一致决定，指定方牵头人，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：甲方承担的工作和义务为：；乙方承担的工作和义务为：；……

四、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。

五、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。

甲方单位：（电子签名）乙方单位：（电子签名）

日期：年月日日期：年月日

▲**报价文件部分**

**目录**

（1）投标响应函……………………………………………………（页码）

（2）投标（开标）一览表…………………………………………（页码）

（3）提供中小企业声明函；………………………………………（页码）

**一、投标响应函**

淳安县人民政府办公室、浙江辰光管理有限公司：

(投标人全称)授权(全权代表姓名)(职务、职称)为全权代表，参加贵方组织的淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：**号**】招标的有关活动，并对此项目进行投标。为此：

1、我方同意在投标人投标人须知规定的开标日期起遵守本投标文件中的承诺且在投标有效期满之前均具有约束力。

2、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的条件：

(1)具有独立承担民事责任的能力；

(2)遵守国家法律、行政法规，具有良好的信誉和商业道德；

(3)具有履行合同的能力和良好的履行合同记录；

(4)良好的资金、财务状况；

(5)产品及生产所需装备符合中国政府规定的相应技术标准和环保标准；

(6)没有违反政府采购法规、政策的记录；

(7)没有发生重大经济纠纷和走私犯罪记录。

3、我方中标后拟在中标后将工作分包，分包承担主体是，我方承诺分包承担主体具备相应资质条件，且不再次分包。（不再将工作进行分包或本项目不允许分包的，下划线处填写“/”。）

4、提供投标人须知规定的全部投标文件。具体内容为：

(1)投标(开标)一览表；

(2)投标技术文件和商务文件；

(3)投标人须知要求投标人提交的全部文件；

(4)按招标文件要求提供和交付的货物和服务的投标报价详见投标(开标)一览表；

(5)保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务；

(6)保证遵守招标文件中的其他有关规定。

5、我方承诺投标有效期从提交投标文件的截止之日起天，不少于招标文件中载明的投标有效期（从提交投标文件的截止之日起90天）。

6、我方完全理解贵方不一定要接受最低价的投标。

7、我方愿意向贵方提供任何与该项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

8、我方已详细审核全部招标文件，包括招标文件修改书(如果有)、参考资料及有关附件，确认无误。

9、我方将严格遵守《中华人民共和国政府采购法》第七十七条规定，供应商有下列情形之一的，处以采购金额5‰以上10‰以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动；有违法所得的，并处没收违法所得；情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

a)提供虚假材料谋取中标、成交的；

b)采取不正当手段诋毁、排挤其他供应商的；

c)与采购人、其它供应商或者采购机构恶意串通的；

d)向采购人、采购机构行贿或者提供其他不正当利益的；

e)在招标采购过程中与采购人进行协商谈判的；

f)拒绝有关部门监督检查或提供虚假情况的。

供应商有前款第a)至e)项情形之一的，中标、成交无效。

投标人名称(电子签名)：

日期：年月日

联系人：联系电话：

联系地址：

邮政编码：传真号码：

**注：未按照本投标响应函要求填报的将被视为非实质性响应投标，从而可能导致该投标被拒绝。**

**二、投标(开标)一览表**

淳安县人民政府办公室、浙江辰光管理有限公司：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下投标(开标)一览表的价格完成淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：**号**】的实施。

项目名称：项目编号：

单位：元

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 投标报价（元） | 项目负责人 | 服务期限 |
| 1 | 淳安县全链路网络安全监管平台（一期）建设采购项目 |  |  |  |

注: 1、报价一经涂改，应在涂改处加盖单位公章或者由法定代表人或授权委托人签字或盖章，否则其投标作无效标处理。

2、凡需用专用耗材的专用设备类采购项目，应按招标文件规定的耗材量或按耗材的常规试用量提供报价。

3、投标总价包括项目实施所需的人工费、服务费、运输费、购买及制作标书费、税费、**中标服务费、**及其他一切费用。

4、以上报价应与“投标报价明细表”中的“投标总价”相一致。

投标人名称(电子签名)：

日期：年月日

**投标报价明细表**

投标人全称（公章）：

项目编号：

单位：元

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **服务内容（规格型号）** | **数量** | **单位** | **金额（元）** | **备注** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | …… |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 投标总价 | | | 小写： | | | |
| 大写： | | | |

注：**上述表格中各项费用可根据标项实际情况增减(不得少于采购需求中的采购内容)，若需进一步细分，栏数不够可自加。**

投标人名称(电子签名)：

日期：年月日

### 三、中小企业声明函

**中小企业声明函(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（采购单位名称）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（软件与信息技术服务业）；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](file:///C:\\Users\\lenovo\\Documents\\WeChat%20Files\\wxid_gjllf995igxo21\\FileStorage\\File\\2021-12\\淳安县应急管理局乡、村级防汛应急物资（汽油发电机、4寸排水泵（含水带））采购项目---招标文件（发布）.docx" \l "_bookmark0)，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。

企业名称（盖章）：

日期：年月日

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。

注：投标人提供的中小企业声明函与实际情况不符的，投标价格不可享受价格扣除。符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，投标人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证明文件的，视同为小型和微型企业。

▲**商务技术文件部分**

**目录**

（1）营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为然人的，提供自然人的身份证明）………………………………………………（页码）

（2）联合体协议……………………………………………………………（页码）

（3）资信文件复印件（如果要求提供）…………………………………（页码）

（4）主要业绩证明…………………………………………………………（页码）

（5）其他商务文件或说明…………………………………………………（页码）

（6）技术解决方案…………………………………………………………（页码）

（7）技术偏离说明表………………………………………………………（页码）

（8）组织实施方案…………………………………………………………（页码）

（9）售后服务方案…………………………………………………………（页码）

（10）项目小组人员名单……………………………………………………（页码）

（11）优惠条件及特殊承诺…………………………………………………（页码）

（12）备品备件及供选择的配套零部件清单………………………………（页码）

（13）培训计划………………………………………………………………（页码）

（14）认为需要的其他技术文件或说明……………………………………（页码）

（15）关于对招标文件中商务、合同有关条款的拒绝声明………………（页码）

（16）政府采购供应商廉洁自律承诺书……………………………………（页码）

（17）廉政承诺书……………………………………………………………（页码）

注：以上目录是基本格式要求，各投标人可根据自身情况进一步细化。

**一、营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，提供自然人的身份证明）**

投标人名称(电子签名)：

日期：年月日

**二、联合体协议**

甲方：

乙方：

……

各方经协商一致，决定组成一个联合体，以一个投标人的身份就浙江辰光管理有限公司组织实施的淳安县全链路网络安全监管平台（一期）建设采购项目【招标编号：】共同投标。

一、各方一致决定，指定方牵头人，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法定代表人签署授权书，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：甲方承担的工作和义务为：；乙方承担的工作和义务为：；……

四、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。

五、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。

甲方单位：（公章）乙方单位：（公章）

日期：年月日日期：年月日

**三、资信文件复印件（如果要求提供）**

（由投标人根据采购需求及招标文件要求编制）

投标人名称(电子签名)：

日期：年月日

**四、主要业绩证明**

**附表 :相关项目建设业绩一览表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | 项目  类型 | 简要描述 | 项目  投资  （万元） | 开竣工日期 | 项目地址与建设单位联系电话 | 所在页码 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**注：投标人可按上述的格式自行编制，须随表提交相应的合同复印件和用户单位验收证明并注明所在投标人商务技术文件页码。**

投标人名称（电子签名）：

日期：年月日

**五、****其他商务文件或说明**

（其他商务文件或说明由投标人根据采购需求自行编制）

投标人名称（电子签名）：

日期：年月日

**六、技术解决方案**

（由投标人根据采购需求及招标文件要求编制）

**（一）投标产品规格配置清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **投标品牌及型号** | **规格配置详细说明** | **数量** | **备注** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| …… |  |  |  |  |  |

**注：如果本项目涉及硬件设备采购，须在技术文件中提供此配置清单。**

**（二）节能产品认证证书复印件（电子签名）**

**（三）环境标志产品认证证书复印件（电子签名）**

供应商名称（电子签名）：

日期：年月日

**七、技术偏离说明表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 采购要求 | 投标响应 | 偏离 | 说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称（电子签名）：

日期：年月日

**八、组织实施方案**

（由投标人根据采购需求及招标文件要求编制）

**附表:项目实施进度计划表(以生效日算起)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 工  作  日  内容 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | … |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**注：投标人可按上述时间表的格式自行编制切合实际的具体时间表。**

投标人名称（电子签名）：

日期：年月日

**九、售后服务方案**

（由投标人根据采购需求及招标文件要求编制）

**附表A:售后服务机构情况表**（按此格式自制）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **机构名称** | **机构性质** | **注册地址** | **服务技术人员数量** | **联系电话** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**注：关于项目涉及的所有售后服务机构均在本表注明，包括投标人本单位和符合条件的第三方服务机构；**

**附表B：售后服务人员情况表**（按此格式自制）

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 类别 | 姓名 | 性别 | 年龄 | 学历 | 专业 | 职称 | 本项目中的职责 | 响应时间 | 到达现场时间 |
|  | 总协调人 |  |  |  |  |  |  |  |  |  |
|  | 售后人员 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

投标人名称（电子签名）：

日期：年月日

**十、项目小组人员名单**

（由投标人根据采购需求及招标文件要求编制）

**附表A:本项目的项目经理情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 |  | 页码 | 投标截止时间前三年业绩及承担的主要工作情况，曾担任项目经理的项目应列明细 |
| 性别 |  |  |  |
| 年龄 |  |  |
| 职称 |  |  |
| 毕业时间 |  |  |
| 所学专业 |  |  |
| 学历 |  |  |
| 资质证书编号 |  |  |
| 其他资质情况 |  |  |
| 联系电话 |  |  |

**注：须随表提交相应的证书复印件并注明所在投标技术文件页码。**

**附表B:本项目的项目小组人员情况表**（按此格式自制）

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 性别 | 年龄 | 学历  (页码) | 专业  (页码) | 职称  (页码) | 本项目中的职责 | 项目经历 | 参与本项目的到位情况 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

**注：投标人可按上述的格式自行编制，须随表提交相应的证书复印件并注明所在投标技术文件页码。**

**附表C:本项目的项目经理和小组人员近3个月交纳社保记录情况表**（以社保局缴纳凭证作附件）

投标人名称（电子签名）：

日期：年月日

**十一、优惠条件及特殊承诺**

（由投标人根据采购需求自行编制）

投标人名称（电子签名）：

日期：年月日

**十二、备品备件及供选择的配套零部件清单**

（由投标人根据采购需求自行编制）

投标人名称（电子签名）：

日期：年月日

**十三、培训计划**

（由投标人根据采购需求自行编制）

**附表: 培训日程及费用**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | 提供的资料 | 持续时间 | 授课教师 | 培训对象 | 培训地点 | 课程费用 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 费用总计 |  |  |  |  |  |  |

注解:A 课程清单按时间顺序排列，并提供以下详细资料：

* 课程概要
* 课程目的
* 教学方式
* 先决条件
* 教材目录

B 按照附表A提供授课教师的简历

**注：须随表提交相应的证书复印件并注明所在投标技术文件页码。**

投标人名称（电子签名）：

日期：年月日

**十四、认为需要的其他技术文件或说明**

（由投标人根据采购需求自行编制）

投标人名称（电子签名）：

日期：年月日

**十五、关于对招标文件中有关商务、合同条款的拒绝声明**

（由投标人根据采购需求自行编制）

投标人名称（电子签名）：

日期：年月日

**十六、政府采购供应商廉洁自律承诺书**

淳安县人民政府办公室、浙江辰光管理有限公司：

本单位合法参加               项目（编号：       ）政府采购活动，就有关廉洁自律和公平竞争事项郑重声明如下：

一、本单位与采购人之间不存在利害关系，不存在行贿、串通等违法行为。

二、本单位与其他当事人之间不存在直接控股、管理关系等情况，不存在法定的不允许投标情形，不存在行贿、串通等违法行为。

三、本单位清楚知道并严格遵守政府采购法律法规、政策文件和相关纪律。

投标人名称（电子签名）：

日期：年月日

**十七、廉政承诺书**

（单位名称）：

我单位响应你单位项目招标要求参加投标。在这次投标过程中和中标后，我们将严格遵守国家法律法规要求，并郑重承诺：

一、不向项目有关人员及部门赠送礼金礼物、有价证券、回扣以及中介费、介绍费、咨询费等好处费；

二、不为项目有关人员及部门报销应由你方单位或个人支付的费用；

三、不向项目有关人员及部门提供有可能影响公正的宴请和健身娱乐等活动；

四、不为项目有关人员及部门出国（境）、旅游等提供方便；

五、不为项目有关人员个人装修住房、婚丧嫁娶、配偶子女工作安排等提供

好处；

六、严格遵守《中华人民共和国政府采购法》《中华人民共和国招标投标

法》《中华人民共和国民法典》等法律法规，诚实守信，合法经营，坚决抵制各种违法违纪行为。

如违反上述承诺，你单位有权立即取消我单位投标、中标或在建项目的建设资格，有权拒绝我单位在一定时期内进入你单位进行项目建设或其他经营活动，并通报市财政局。由此引起的相应损失均由我单位承担。

投标人名称（电子签名）：

法定代表人或其授权代表（签字）：

日期：年月日

**政府采购支持中小企业信用融资相关事项通知**

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《杭州市政府采购支持中小企业信用融资管理办法》等规定，淳安县财政局与中国建设银行股份有限公司淳安支行、杭州银行股份有限公司淳安支行、中国工商银行股份有限公司淳安支行等银行签订了《政府采购支持中小企业信用融资合作备忘录》，本采购项目中标人与采购单位签订的政府采购合同适用于政府采购贷款政策，简称“政采贷”。

# 附件

**附件1：**

**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。

单位名称（电子签名）：

日期：

**附件2：质疑函范本及制作说明**

**质疑函范本**

一、质疑供应商基本信息

质疑供应商：

地址：邮编：

联系人：联系电话：

授权代表：

联系电话：

地址：邮编：

二、质疑项目基本情况

质疑项目的名称：

质疑项目的编号：包号：

采购人名称：

采购文件获取日期：

三、质疑事项具体内容

质疑事项1：

事实依据：

法律依据：

质疑事项2

……

四、与质疑事项相关的质疑请求

请求：

签字(签章)：公章：

日期：

**质疑函制作说明：**

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体分包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

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

**附件3：投诉书范本及制作说明**

**投诉书范本**

一、投诉相关主体基本情况

投诉人：

地址：邮编：

法定代表人/主要负责人：

联系电话：

授权代表：联系电话：

地址：邮编：

被投诉人1：

地址：邮编：

联系人：联系电话：

被投诉人2

……

相关供应商：

地址：邮编：

联系人：联系电话：

二、投诉项目基本情况

采购项目名称：

采购项目编号：包号：

采购人名称：

代理机构名称：

采购文件公告:是/否公告期限：

采购结果公告:是/否公告期限：

三、质疑基本情况

投诉人于年月日,向提出质疑，质疑事项为：

采购人/代理机构于年月日,就质疑事项作出了答复/没有在法定期限内作出答复。

四、投诉事项具体内容

投诉事项 1：

事实依据：

法律依据：

投诉事项2

……

五、与投诉事项相关的投诉请求

请求：

签字(签章)：公章：

日期：

**投诉书制作说明：**

1.投诉人提起投诉时，应当提交投诉书和必要的证明材料，并按照被投诉人和与投诉事项有关的供应商数量提供投诉书副本。

2.投诉人若委托代理人进行投诉的，投诉书应按照要求列明“授权代表”的有关内容，并在附件中提交由投诉人签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.投诉人若对项目的某一分包进行投诉，投诉书应列明具体分包号。

4.投诉书应简要列明质疑事项，质疑函、质疑答复等作为附件材料提供。.

5.投诉书的投诉事项应具体、明确，并有必要的事实依据和法律依据。

6.投诉书的投诉请求应与投诉事项相关。

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