**政府采购项目**

**公开招标采购文件**

**招标编号： NBGZZB123150**

**项目名称： 余姚市电子政务外网网络安全服务集成项目**

**采 购 人： 余姚市大数据发展管理局**

**采购代理机构：宁波国咨工程造价咨询有限公司**

**2024年1月**

**目 录**

[第一部分 采购公告 3](#_Toc520902391)

[第二部分 招标项目需求](#_Toc520902406) 9

[第三部分 投标资料表](#_Toc520902392) 119

[第四部分 投标人须知](#_Toc520902393) 122

[第五部分 评标办法](#_Toc520902405) 138

[第六部分 合同格式](#_Toc520902404) 146

[第七部分 附件（投标文件格式）](#_Toc520902407) 154

# 第一部分 采购公告

项目概况

余姚市电子政务外网网络安全服务集成项目招标项目的潜在投标人应在政府采购云平台（[www.zcygov.cn）获取（下载）招标文件，并于2024年](http://www.zcygov.cn）获取（下载）招标文件，并于2022年)2月21日14点00分（北京时间）前递交（上传）投标文件。

## 一、项目基本情况

项目编号：NBGZZB123150

项目名称：余姚市电子政务外网网络安全服务集成项目

预算金额（元）：4193800

最高限价（元）：4193800

采购需求：

标项名称：余姚市电子政务外网网络安全服务集成项目

 数量：1

简要规格描述或项目基本概况介绍、用途：余姚市电子政务外网网络安全服务集成，具体采购内容见第二部分招标项目需求。

备注：/

合同履约期限：自合同签订之日起至合同履约完成之日止。

本项目接受联合体投标。

## 二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

2.落实政府采购政策需满足的资格要求：无。

3.本项目的特定资格要求：无。

## 三、获取招标文件

时间：2024年1月17日至2024年1月24日，每天上午00:00至12:00，下午12:00至23:59（北京时间）

地点：政府采购云平台（http://www.zcygov.cn/）。

方式：本项目实行“政府采购云平台”（http://www.zcygov.cn/）网上获取。

（1）根据《浙江省政府采购供应商注册及诚信管理暂行办法》规定，已在“政府采购云平台”（www.zcygov.cn）或“浙江政府采购网”（ zfcg.czt.zj.gov.cn）注册的投标人获取路径：【用户登录】—【项目采购】—【获取采购文件】

（2）未注册投标人获取路径：【商家入驻】—完成政府采购供应商入驻注册—【项目采购】—【获取采购文件】

请注意注册所需时间。

注册入驻操作指南：https://service.zcygov.cn/#/knowledges/cm2eqWwBFdiHxlNd\_otq/w3Cd3GwBFdiHxlNd-BRD

注册咨询电话：95763

（3）供应商只有在“浙江政府采购网”完成获取采购文件申请并下载了采购文件后才视作依法获取采购文件（法律法规所指的供应商获取采购文件时间以供应商完成获取采购文件申请后下载采购文件的时间为准）。

通过本公告下方“游客，浏览采购文件”下载的采购文件仅供浏览，不视作参与本项目。

售价：免费。

## 四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2024年2月21日14点00分（北京时间），投标人应在投标截止时间前将电子加密投标文件上传到“政采云”平台，逾期上传或上传不成功的，其投标无效。

投标地点（网址）：政采云平台（https://www.zcygov.cn/）

开标时间：2024年2月21日14点00分（北京时间）

开标地点（网址）：政采云平台（https://www.zcygov.cn/）

## 五、公告期限

自本公告发布之日起5个工作日。

## 六、其他补充事宜

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

**2．其他事项：**

2.1 在线询问及在线质疑操作方式

2.1.1在线询问

潜在供应商获取采购文件后，对政府采购活动事项有疑问的，可对该项目进行在线询问及查看询问答复，访问路径如下：应用中心（登录首页）—项目采购—询问质疑投诉—询问列表；

2.1.2在线质疑

供应商认为采购文件、采购过程、中标或者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7个工作日内，对采购文件、采购过程、采购结果进行在线质疑（需在线签章）并查看质疑答复，访问路径如下：

应用中心（登录首页）—项目采购—询问质疑投诉—质疑列表。

2.2 供应商应于提交投标文件截止时间前将电子加密投标文件上传到政府采购云平台www.zcygov.cn，未上传电子投标文件，视为供应商放弃投标。

2.3 供应商在“政府采购云平台”完成“电子加密投标文件”的上传递交之外，还可以（邮寄形式或派人现场提交，以招标代理机构联系人签收时间为准）在投标截止时间前提交以介质（U盘或光盘）存储的数据电文形式的“备份投标文件”，备份电子投标文件递交可采用现场递交或邮寄的方式。

（一）现场递交方式，请供应商安排在投标截止时间前将电子备份投标文件送至余姚市公共资源交易中心（余姚市谭家岭东路2号，南雷大厦附楼4楼，详见开评标场所安排），投标文件递交时须同时递交供应商的法定代表人（或其授权代表）联系方式，并保证开标期间联系方式畅通。

（二）邮寄送达。供应商可以通过邮寄送达电子备份投标文件，送达地址宁波国咨工程造价咨询有限公司（宁波市鄞州区和源路510号宁兴国贸大厦2102室），联系方式：0574-87312175。供应商邮寄后须将邮件单号发送至代理机构电子邮箱（电子邮箱：625740900@qq.com），并致电采购代理机构，以便采购代理机构查询物流记录。各供应商应当确保投标文件的密封包装在邮寄过程保持完好，并在邮寄包裹上注明项目名称，因邮寄造成投标文件密封破损而不符合招标文件对投标文件的密封要求、或邮寄过程中导致投标文件未按时送达的，代理机构将拒绝其投标文件。各供应商自行考虑邮寄在途时间，投标文件送达时间以采购代理机构工作人员实际签收时间为准。电子备份投标文件邮寄送达截止时间为投标截止时间前一天17时00分。

2.4 开标时间后30分钟内供应商可以登录政采云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密。供应商按时在线解密投标文件的，以在线解密的投标文件作为评审依据，若供应商在规定时间内无法解密或解密失败，则以备份电子投标文件作为评审依据（若备份电子投标文件与政采云平台上传的投标文件被识别为不一致，仍以备份电子投标文件作为评审依据）。无论是否启用备份电子投标文件，备份电子投标文件均不退还供应商。若供应商在规定时间内无法解密或解密失败且未提供备份电子投标文件或所提供的备份电子投标文件无法读取的，视为投标文件撤回。

3．采购项目需要落实的政府采购政策：《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《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)、《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）。

4．投标与开标注意事项： 投标形式：本项目实行网上投标，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。 标前准备：各供应商应在开标前应确保成为浙江省政府采购网正式注册入库供应商，并完成CA数字证书办理（供应商CA申领操作指南：https://help.zcygov.cn/web/site\_2/2018/11-29/2452.html，完成CA数字证书办理预计一周左右，请供应商自行把握时间）。因未注册入库、未办理CA数字证书等原因造成无法获取采购文件、无法投标或投标失败等后果由供应商自行承担。

5．投标文件制作： 应按照本项目招标文件和政采云平台的要求编制、加密并递交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线95763或政采云服务专员电话0574-63917219。 投标人通过政采云平台电子投标工具制作投标文件，电子投标工具请供应商自行前往浙江省政府采购网下载并安装，下载网址：http://zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12946.html， 供应商投标文件制作及电子交易操作指南：https://help.zcygov.cn/web/site\_2/2018/12-28/2575.html （PDF操作指南）。制作电子投标文件的系统配置要求：请使用windows7及以上64位操作系统，不适用于mac或linux桌面系统。

 6．根据财库〔2016〕125号文要求，采购人或采购代理机构对投标人的信用记录进行查询并甄别：

6.1信用信息查询的截止时点：投标截止时间；

6.2查询渠道：“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）；

6.3信用信息查询记录和证据留存具体方式：打印查询网页并与其他采购文件一并保存；

6.4信用信息的使用规则：投标人存在不良信用记录的，其投标将被作为无效投标处理。不良信用记录指：被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

若在开标当天因不可抗力事件导致无法查询且一时无法恢复查询的，可在发布中标结果公告之前对中标候选人进行事后查询。中标候选人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的，采购人将依法取消其中标资格。

7、其他补充事宜

1） 《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 （浙财采监（2022）3号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号））、《浙江省财政厅关于进一步加大政府采购支持中小企业力度助力扎实稳住经济的通知》（浙财采监（2022）8号）已分别于2022年1月29日、2022年2月1日和2022年7月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

2） 根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监〔2021〕22号）文件关于“健全行政裁决机制”要求，鼓励供应商提起询问、质疑，质疑供应商对质疑答复不满意的，可在线提起投诉。

3）中小企业信用融资的相关政策:中小企业信用融资：供应商中标后也可在“政采云”平台申请政采贷：操作路径：登录政采云平台-金融服务中心-[融资服务]，可在热门申请中选择产品直接申请，也可点击云智贷匹配适合产品进行申请，或者在可申请项目中根据该项目进行申请。

## 七、对本次采购提出询问、质疑、投诉，请按以下方式联系。

1.采购人信息

名 称：余姚市大数据发展管理局

地 址：余姚市梨洲街道谭家岭东路2号

项目联系人（询问）：沈老师

项目联系方式（询问）： 0574-89553573

质疑联系人： 吕老师

质疑联系方式： 0574-89553568

2.采购代理机构信息

名 称：宁波国咨工程造价咨询有限公司

地 址：宁波市鄞州区和源路510号宁兴国贸大厦21楼2102室

项目联系人（询问）： 戴佳颖、黄一达、唐权勇、李莺

项目联系方式（询问）：0574-87312175

质疑联系人：王月

质疑联系方式：0574-87321998

电子邮箱：625740900@qq.com

3.同级政府采购监督管理部门

名称：余姚市财政局

地址：余姚市南滨江路118号；

联系人 ：303办公室

监督投诉电话：0574-89553033；

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线95763获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

# 第二部分 招标项目需求

项目需求前附表

| **序号** | **项目** | **采购需求内容** |
| --- | --- | --- |
| 1 | 采购内容 | 详见第一部分《采购公告》及本部分“技术要求” |
| 2 | 单位及数量 | 详见第一部分《采购公告》及本部分“技术要求” |
| 3 | 交付或者实施的时间和地点 | 详见商务要求表 |
| 4 | 需实现的功能或者目标 | 详见技术要求 |
| 5 | 采购标的需执行的标准 | 执行国家、地方、有关机构所有相关的技术规范与标准，且确保所采用的技术规范、标准必须是国家或有关机构发布的最新版本，无论此版本在此有无提及。 |
| 6 | 采购标的对应的中小企业划分标准所属行业 | 软件和信息技术服务业 |
| 7 | 技术规格要求 | 详见技术要求 |
| 8 | 物理特性要求 | / |
| 9 | 质量、安全要求 | / |
| 10 | 服务标准、期限、效率(培训等） | 服务质量必须执行国家相关标准、行业标准、地方标准或者其它标准、规范，按照就高原则执行。1、本项目必须达到现行中华人民共和国及省市行业的一切有关法规规范的要求。2、技术要求：按照相关图纸和相关的技术规范、验收规范。3、中标人应负责在项目现场进行服务直至该项目验收合格、交付使用，其费用应包括在项目总价中。4、项目验收：由采购人验收，依据为国家有关规定、采购文件、中标人的投标文件以及其他相关文件和资料。 |
| 11 | 验收标准 | 1、根据中华人民共和国现行技术标准，按采购文件以及合同规定的验收评定标准等规范，由采购人组织验收。2、中标人应对提交的服务成果作出全面检查和整理，并列出清单，作为采购人验收和使用的技术条件依据，清单应随提交的服务成果交给采购人。 |
| 12 | 现场踏勘 | 本项目不统一组织现场勘察，供应商可自行对本项目现场和周围环境进行勘察。勘察现场所发生的费用由供应商自己承担。不论何种原因所造成，在勘察过程中，供应商自行对由此次踏勘现场而造成的死亡、人身伤害、财产损失、损害以及任何其它损失、损害和引起的费用和开支承担责任。 |
| 13 | 演试时间及地点 | 无 |

**商务要求**

|  |  |
| --- | --- |
| **项目** | **要 求** |
| ★1.签订合同时间 | 中标通知书发出之日起30日内签订合同，具体签约时间以采购人通知为准。 |
| ★2.服务期 | 本项目工期为自合同签订之日起2个月内完成实施并进入试运行，试运行时间为3个月；服务期自项目通过交付验收之日起计算，服务期限叁年。 |
| 3.服务地点 | 招标人指定地点。 |
| ★4.付款条件 | 1-1）合同生效后7个工作日内支付合同总价的30%（中标人为非中小微企业）；1-2）合同生效后7个工作日内支付合同总价的40%（中标人为中小微企业）；2-1）第二年服务期结束前两个月，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的35%（如有违约金，在扣除第一年度违约金后支付）（中标人为非中小微企业）；2-2）第二年服务期结束前两个月，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的30%（如有违约金，在扣除第一年度违约金后支付）（中标人为中小微企业）；3-1）第三年服务期开始并完成资产移交后，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的35%（如有违约金，在扣除第二年度违约金后支付）（中标人为非中小微企业）；3-2）第三年服务期开始并完成资产移交后，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的30%（如有违约金，在扣除第二年度违约金后支付）（中标人为中小微企业）。注：约定的支付时间以政府财政性资金支付要求为准，如因财政等原因导致支付延迟，采购人不承担相应责任。 |
| ★5.履约保证金 | 1. 履约保证金金额：合同金额的1%；
2. 履约保证金形式：支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式；

（3）担保收件人：采购人；（4）提交时间：签订本项目合同后7个工作日内；（5）履约保证金的方式：合同履行完毕并经项目服务验收后退还。（6）履约保证金不予退还的情形：如中标人未履行或未完全履行合同规定的任何义务，给采购人造成损失的，采购人有权在其提交的履约保证金终获得相应赔偿，不足部分采购人有权继续向中标人赔偿。 |
| ★6.其他 | 1.在采购及合同执行过程中，供应商应承担由于其行为所造成的人身伤害、财产损失或损坏的责任，无论何种原因所造成，采购人均不负责。 |
| 2.在合同履行过程中，中标人不得存在与本项目实施有利害冲突，影响或可能影响考核公正的情形，一旦出现，采购人有权解除合同。 |

**采购需求**

**一、项目建设目标**

根据国家网络安全等级保护相关要求，在余姚市电子政务外网网络安全建设已有成果的基础上，充分分析余姚市电子政务外网网络的实际安全需求，结合其业务的实际特性，通过购买服务的方式，建立余姚市电子政务外网网络及数据安全保障体系框架，构建集约高效、具有特色的余姚市电子政务外网网络安全管理和运行平台，实现新形势下安全管理上台阶、安全技术见实效、综合实力有提升的建设成效，形成具有主动防御和协同运营能力的新一代网络安全保障体系，综合提升业务系统的安全保障能力和防护水平，确保入驻业务系统的网络和数据安全。

**二、项目建设需求**

为了保障余姚市电子政务外网网络数据安全，同时符合《网络安全法》、《数据安全法》、等级保护基本要求以及浙江省大数据发展管理局关于开展市县一体化智能化公共数据平台综合评价、公共数据安全体系建设指南所提出的数据安全要求，根据上述法律法规以及要求，平台需针对本地数据的分级分类管理和对数据库开展态势感知分析等数据安全内容进行全面建设。

以及面对余姚市关键信息基础设施网络安全防护需求，为了应对日趋严峻的网络安全威胁形势，需要通过对余姚市电子政务外网网络统一的安全建设和运营，提高对网络安全威胁事件的检测、发现、分析和处置能力，确保关键信息基础设施网络和信息系统的正常安全运行。面对余姚市网络安全防护建设、运行和应急处置能力参差不齐的现状，基于网络安全动态、开放、共同的特点，建立面向部门的网络安全管理和运营平台、技术工具、人员和服务业务，形成有特点、场景化的运营模式，统一提升余姚市网络安全防护能力，建立、完善余姚市电子政务外网网络安全联防联控体系，从而提升余姚市电子政务外网网络安全整体防控能力。

**三、项目建设内容**

本项目建设内容主要包括数据安全服务和网络安全服务购置，服务年限为三年。

1、数据安全服务

包含数据分级分类、数据安全态势感知平台、数据库加密扩展、数据安全管理系统和数据库软件等服务的购置。

2、网络安全服务

包含网络安全管理平台、网络安全运行平台和网络安全配套等服务的购置。

其中网络安全管理平台主要包括资产中心、威胁中心、分析中心、情报中心、工作指挥、报告中心、考核评估、态势感知等功能服务，以及配套的4台平台服务器。

网络安全运行平台主要包括监测中心、资管中心、感知中心、响应中心、web端工作台、移动端、大数据节点、大数据安全检测、云平台安全监测、资产数据治理、检查督查、指挥调度、IP定位、情报中心、分析研判、安全专项等功能服务，以及配套的2台平台服务器。

网络安全配套服务包括云端安全实时监测服务、漏洞扫描服务、基线检查服务、渗透测shi服务、风险隐患与事件通报服务、安全检查服务、安全工作报告服务、运营流程优化服务、运营文件编制服务、资产梳理服务、策略调优服务、重要时期安全保障服务、安全加固服务等。

**四、项目采购清单**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务名称** | **服务年限** |
| **一** | **数据安全服务** | 　 |
| 1 | 数据分级分类 | 3年 |
| 2 | 数据安全态势感知平台 | 3年 |
| 3 | 数据库加密扩展 | 3年 |
| 4 | 数据安全管理系统 | 3年 |
| **二** | **网络安全监管平台** | 　 |
| （一） | 安全管理子平台 | 　 |
| 1 | 子平台基础软件 | 3年 |
| 2 | 资产中心 | 资产脆弱性管理 | 3年 |
| 3 | 资产漏洞库管理 | 3年 |
| 4 | 资产风险评估管理 | 3年 |
| 5 | 威胁中心 | 安全事件管理 | 3年 |
| 6 | 分析中心 | 关联分析 | 3年 |
| 7 | 攻击链分析 | 3年 |
| 8 | 情报中心 | 具备根据情报侦察等方法获取攻击者情报信息、攻击方法手段、攻击目标等重要情报信息的能力，能录入和展示重要行业部门报送的情报信息、第三方收集报送的情报信息、上级部门下发的情报信息、下级报送的情报信息以及通过其他方式汇聚的情报信息的能力等。 | 3年 |
| 9 | 指挥中心 | 流程管理 | 3年 |
| 10 | 重要活动保障 | 3年 |
| 11 | 突发事件应急处置 | 3年 |
| 12 | 日常通报工作 | 3年 |
| 13 | 重大风险预警 | 3年 |
| 14 | 报告中心 | 　/ | 3年 |
| 15 | 考核评估 | 　/ | 3年 |
| 16 | 态势感知 | 　/ | 3年 |
| 17 | 子平台基础支撑硬件 | 子平台服务器（4台） | 3年 |
| （二） | 安全运行子平台 | 　 |
| 1 | 安全监管平台 | 3年 |
| 2 | 基础功能 | 监测中心 | 3年 |
| 3 | 资管中心 | 3年 |
| 4 | 感知中心 | 3年 |
| 5 | 响应中心 | 3年 |
| 6 | Web端工作台 | 3年 |
| 7 | 移动端 | 3年 |
| 8 | 大数据节点软件 | 3年 |
| 9 | 大数据安全监测 | 3年 |
| 10 | 云平台安全监测 | 3年 |
| 11 | 资产数据治理 | 3年 |
| 12 | 检查督查 | 3年 |
| 13 | 指挥调度 | 3年 |
| 14 | 分析研判 | 3年 |
| 15 | 安全专项 | 3年 |
| 16 | 威胁情报模块 | 3年 |
| 17 | 重大安保 | 3年 |
| 18 | 考核评价 | 3年 |
| 19 | 流量监测模块 | 3年 |
| 20 | 子平台支撑服务器（2台） | 3年 |
| **三** | **网络安全配套服务** | 　 |
| 1 | 云端安全实时监测服务 | 3年 |
| 2 | 漏洞扫描服务 | 3年 |
| 3 | 基线检查服务 | 3年 |
| 4 | 渗透测shi服务 | 3年 |
| 5 | 风险隐患与事件通报服务 | 3年 |
| 6 | 安全检查服务 | 3年 |
| 7 | 安全工作报告服务 | 3年 |
| 8 | 运营流程优化服务 | 3年 |
| 9 | 运营文件编制服务 | 3年 |
| 10 | 资产梳理服务 | 3年 |
| 11 | 策略调优服务 | 3年 |
| 12 | 重要时期安全保障服务 | 3年 |
| 13 | 安全加固服务 | 3年 |
| 14 | 宣传教育及培训服务 | 3年 |
| **四** | **国产化软件购置** | 　 |
| 1 | 国产数据库软件1套 | 3年 |
| 2 | 国产应用中间件1套 | 3年 |

**五、设备详细参数**

1. **数据分类分级服务**

**1.服务内容**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 服务内容 | 1、数据分级分类咨询服务：根据国家、行业相关要求梳理余姚市数据分级分类规范，输出余姚市分级分类标准；2、数据安全服务：做好省市飞检工作和数据安全一本账自查整改根据数据安全管理要求，开展周期性数据安全风险评估，并出具风险评估报告及整改建议。数据安全风险评估服务每年2次，并形成《数据安全风险评估报告》。按需提供，根据省、市数据安全相关绩效考核和工作要求，辅助用户完成上级数据安全检查项及考核指标解读、相关材料准备、不达标项整改等，并形成《数据安全考核评价检查记录》。提供数据安全咨询服务和数据安全相关建议；3、暗数据发现和分类分级系统：具备对于余姚市数据资产进行自动发现并进行分类分级，协助采购人全面梳理数据资产，具备数据安全治理和数据基础治理能力，含不少于2000张表40000个字段；4、数据分级分类实施服务：具备利用敏感数据发现分析出敏感数据后，再按照政务数据类型进行敏感数据分级分类，从敏感数据分类出发，选择敏感表格组成敏感数据集合，在保障安全的基础之上实现便捷管理。5、硬件配置，不低于下列参数及数量：CPU国产化不低于16核 /内存不少于DDR4 3200 16G\*2 /硬盘不少于480G 2.5 SATA 6Gb R SSD\*1 /硬盘不少于4TB 3.5 SATA 7.2K HDD\*2 /硬盘背板不低于4盘12G SAS /不少于8口SAS卡/不低于550W电源模块\*2 /双口10G（满配光模块）SFP+光纤网卡\*2 /10G SFP+多模光模块\*4 （满配光模块）/滑轨 /150cm 国标电源线\*2 / 整机三年保修且硬盘免回收。6、具备服务期内软件、硬件系统全功能免费升级服务。 |
| 服务范围 | 为余姚市电子政务数据中心提供三年期的数据分类分级服务。 |
| 交付物 | 服务期至少输出《数据资产发现报告》、《数据资产分类分级报告》、《数据源详情展示报告》。 |

**2.技术服务工具要求**

|  |  |
| --- | --- |
| **指标项** | **详细功能要求** |
| 数据源适配 | 适配多种数据源，配置不少于以下主流关系型数据库（Oracle，Mysql，sqlServer，DB2，PostgreSQL，informix，MariaDB，TiDB，AS400等）、国产数据库（DM，GaussDB，浪潮K-DB，HotDB，Gbase 8a、Cache等）、大数据平台（hive，星环，Hbase，Greenplum等）、云数据库（ODPS，阿里云RDS - MySQL，阿里云RDS - SQL server，阿里云RDS - PostgreSQL，阿里云RDS - MariaDB等）、文件（txt、csv、xls、xlsx、数据字典等）。 |
| 可扩展性 | 提供完整的对接接口方案以及标准接口文档，能与其他系统进行交互。 |
| 数据源管理 | 配置手工新增、批量导入、数据源发现三种方式添加数据源的功能，可根据业务部门划分归属，页面支持查看数据源的关联用户、角色等。 |
| 数据源发现 | 配置根据网段范围自动探测网络中的数据库的能力，可扫描发现不限于Oracle、MySQL、SQL sever、DB2、postgresql、Sybase、 redis 、hbase、mongodb、informix等类型的数据库IP、端口、数据库类型等信息，配置支持仅对数据库常见的端口进行扫描以缩短扫描所用时间。 |
| 配置定时执行数据源发现任务的功能，可自定义定时周期和启动时间，启动时间可精确到小时、分、秒。 |
| 支持对任务进行跟踪，展示发现作业名称、扫描IP范围、开始时间、扫描用时、发现数据库数量、任务执行状态等信息。 |
| 数据源发现结果对比 | 配置用户选择两个不同的作业发现结果进行对比的能力，包括数据库类型分布、数据库IP分布、数据库新增或者信息变化情况，支持导出对比报告。 |
| 支持用户上传数据库台账文件，和扫描结果进行对比，并生成对比分析报告。 |
| 资产发现 | 配置用户创建资产发现作业的能力，支持按照schema或者表选择需要发现的数据范围。 |
| 配置选择发现模板自定义发现内容的能力。 |
| 配置自定义抽样行数范围、抽样行数（最小为10行）、输出命中率的能力。 |
| 配置定时开启资产发现作业的能力。 |
| 配置配置通过NLP技术对于字段注释进行分析的能力，自动识别数据业务类型，并支持相似度基线配置。 |
| 配置查看发现作业分析进度的能力，并可以对每一步的结果进行修改和确认。 |
| 资产关系梳理 | 配置用户根据schema或表格方式选择需要梳理关系的范围。 |
| 系统自动化对于数据关系进行梳理，并以关系图谱的方式进行展现。 |
| 支持手动对于待确定的数据关系进行确认，以及手动新增或删除数据关系。 |
| 字段业务类型分析 | 支持通过列内容匹配、列注释匹配、列名称匹配、函数分析等方式对数据语义内容进行自动识别，识别字段代表的业务类型。 |
| 支持自动分析字段数据内容是否为空数据和脏数据。 |
| 支持通过机器学习算法，自动梳理数据特征，并生成相应的数据发现规则。 |
| 支持通过重要数据识别规则，自动识别重要数据。 |
| 业务类型结果确认 | 字段业务类型分析完成后，会分组展示分析结果，支持用户分别查看、确认和修改识别等结果。 |
| 数据分类分级 | 配置在业务类型识别的基础上，根据分类分级标准自动化完成数据的分类分级。 |
| 分类结果确认 | 在自动完成数据分类分级时，支持用户对业务类型未分类的、字段对应业务类型存在多个分类的字段进行确认，确认完成后输出最终分类分级结果。 |
| 敏感字段识别 | 配置通过业务含义识别对多种敏感数据类型进行自动识别的能力；支持用户自定义需要发现的敏感类型，并对识别结果进行确认。 |
| 敏感表格发现 | 按照数据表内包含的敏感字段数量和敏感等级，提供敏感指数帮助用户快速确认表格敏感程度，支持查看表格包含的敏感字段信息。 |
| 配置对敏感表格发现结果进行导出的能力，格式为excel。 |
| 资产发现结果 | 支持以清单的形式资产发现的结果，包括字段业务类型、分类、分级、是否敏感等信息。 |
| 数据分类分级报告 | 配置导出资产发现清单的能力，格式为Excel、XML。 |
| 配置提供完整、直观、内容丰富的发现结果报告的能力，包括数据统计信息，敏感数据统计、数据分类统计等；配置用户进行导出，格式为pdf的能力。 |
| 分类分级总览 | 配置以分类分级目录形式查看数据资产的自动发现的结果和分类分级情况的能力。 |
| 资产总览 | 配置按照分组-数据源-schema-表的维度的能力，展示不同对象下的数据分类分级和敏感数据信息。 |
| 配置用户导出资产发现总览和敏感数据统计报告的能力，格式为Excel。 |
| 分类分级大屏 | ▲配置提供全部数据资产梳理及分类分级大屏的能力，包括数据资产的盘点、数据分类分级概况、数据敏感分析、数据库差异分析等，同时支持大屏显示内容配置界面。（提供功能截图） |
| 数据字典管理 | 配置通过手动新增和批量导入的方式添加规则配置中需要的数据字典。配置完成后可在“业务类型管理-规则配置”中进行选择的能力。 |
| 业务类型配置 | 配置用户维护和定义数据资产的业务标准的能力，支持用户自定义业务类型。 |
| 配置用户自定义发现规则的能力，包括列内容匹配、列注释匹配、字段名匹配等方式。 |
| 配置自定义业务类型的导入和导出的能力。 |
| 发现模版配置 | 配置用户按照资产发现的需求的能力，选择需要发现的业务类型，并以模板的形式进行管理。 |
| 分类分级管理 | 系统提供行业适配的数据分类分级标准，支持用户自定义分类层级和内容、自定义分级数量和名称。 |
| 配置表格分类分级配置的能力，表格分类包括分类集合和就多原则两种分类策略，表格分级支持就高原则和加权计算两种分级策略。 |
| 配置用户对字段业务类型的分类和分级信息进行编辑的能力。 |
| 产品资质要求 | 具备国家版权局颁发的《计算机软件著作权登记证书》具备信创适配实验室颁发的信创适配证书至少支持3种国产化数据库的适配兼容，提供相关数据库的兼容性互认承诺函并加盖公章。 |
| 原厂售后服务 | 本项目提供原厂项目管理和售后实施服务。 |
| 遇到产品自身问题时，可以提供2小时以内的上门服务。 |
| 原厂质保服务 | ▲中标后，合同签定时提供软件原厂商针对此项目三年7\*24原厂质保服务函，服务时间从交付验收后开始计算。 |

1. **数据安全态势感知服务**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 系统架构要求 | 支持Linux主流操作系统、国产化操作系统等。 |
| 数据源类型支持 | 产品应支持Oracle、SQL Server、MySQL、Sybase、DB2等主流关系型数据库，以及高斯、达梦、神通、金仓等国产数据库和Hive、HBase、HDFS、Elasticsearch、Kafka、Kudu等大数据关键组件。支持文件服务器、存储对象等多种形式的非结构化数据源接入。 |
| 数据源发现识别 | 产品配置多种类型数据库的自动发现的能力。包括但不限于余姚本地数仓、ODPS等。通过扫描解析方式，支持在指定IP地址和端口范围进行探测和扫描。能够梳理在线数据源类型、数量、分布等。 |
| 数据扫描方式 | 配置JDBC/ODBC直连采集和文件导入等不同数据资产梳理方式的能力，可绘制库、表、字段、文件等不同层次的数据目录，能形象地展示数据资产的分布、数量、归属等信息。 |
| 敏感数据识别 | ▲内置敏感数据特征库功能，包含不少于60类关键个人隐私的特征规则，包括姓名、身份证号、电话号码等关键个人隐私数据。（提供产品功能截图） |
| 配置通过智能算法、正则表达式、关键词、文档指纹、表格指纹等方式自定义数据特征的能力。 |
| 标签管理 | 配置标签库管理的能力，可建立多维标签体系。 |
| 配置自定义数据分级标签的能力，用户可自定义标签分级名称、标签颜色、标签权重。 |
| 配置标签模板管理功能，内置《GB/T35273信息安全技术个人信息安全规范》数据分类标准模板，并支持自定义添加分类标签库。（提供产品功能截图） |
| 分级分类 | 配置分类分级任务管理，任务支持自动化、定期进行分类分级打标。 |
| 支持通过数据识别规则对数据资产（表、簇、目录、字段、文件等）进行分类分级打标，并查看打标结果。 |
| 配置通过数据特征和资产属性构建识别规则的能力。可针对数据特征（特征项）、资产属性（表名、表注释、字段名、字段注释等）设定单一规则。也可针对多规则之间以“与”、“或”等逻辑关系进行组合形成规则集。 |
| 配置识别规则的批量导入和导出的能力。 |
| 标签核验 | 配置标签核验的能力，对打标结果进行校验，修正打标结果。 |
| 配置手动对打标结果进行调整的能力。 |
| 资产地图 | 配置以资产目录及资产索引方式直观展现数据资产的类别、分布、数量、归属的能力，描绘各数据源、数据库、数据表、字段、文件之间的关系和脉络，为用户提供翔实、直观的数据资产台账。数据资产以数据目录索引或数据映像等方式展现，产品不存储用户真实业务数据，敏感数据样例展现需采用遮蔽脱敏方式以防止泄露。 |
| 数据资产接口 | 配置数据资产API接口，包括数据源添加、分类分级字典、获取资产分类分级信息等接口。 |
| 数据动态监察 | 配置关联数据资产访问行为日志，实时监测目标数据的创建（生成）、修改（更新）、查看、删除等操作或使用行为。 |
| 大屏管理 | ▲提供安全应用运行大屏。能够体现不少于安全应用概览（如：安全设备总数、安全应用类型）、近一周的安全应用日志采集趋势、安全应用的实时告警、安全告警等级分布（支持不少于近7天、近30天、近半年时间选择）、安全应用的性能告警分布（支持不少于近7天、近30天、近半年时间选择）以及系统主机的性能监控（如：CPU的当前使用率/平均使用率，内存的当前使用率/平均使用率等）、具体安全应用的基本信息（版本、应用类别、持续运行时间、CPU使用率、内存使用率、剩余磁盘量）。 |
| 数据访问热度 | 可根据数据主体被访问的次数、分布等信息智能分析，生成数据对象调用次数、调用趋势、热度综合排名等分析图表。 |
| 配置对数据库中僵尸数据表、空数据表进行发现和统计的能力。（提供产品功能截图） |
| 配置资产热度分析的能力，统计数据资产使用情况，可覆盖表级，方便用户了解高频资产、低频资产、静默资产等。 |
| 接入管理 | 配置与现有系统中数据静态脱敏、数据动态脱敏、数据库加密、数据库水印等数据安全产品的接入集中管理的能力，可查看相关接入产品运行状态以及接入产品对接的数据资源状态。支持提供标准API接口供第三方接入。 |
| 统一策略 | ▲配置与现有系统中数据静态脱敏、数据动态脱敏、数据库加密、数据库水印等数据安全产品的统一数据安全策略制定、数据安全策略下发的能力。支持提供标准API接口供第三方接入。 |
| 安全能力融合 | 产品必须能够与现有系统中数据静态脱敏、数据动态脱敏、数据库加密、数据库水印等数据安全产品进行深度融合、联动工作，可支持产品间数据互通、信息共享等，使的本单位数据安全管理体系原生、融合、统一。（提供产品功能截图） |
| 数据风险模型 | 需提供数据风险识别模型库，能够有效识别用户异常访问、数据异常流转、数据异常操作等高危风险。 |
| 账号权限信息 | 支持数据库账号权限梳理、监测，用于数据资产关联及风险分析。 |
| 数据采集 | 配置数据安全日志的集中采集、标准化、存储、全文检索功能，如对数据动态脱敏、数据库加密等作业日志、其他数据安全设备的业务日志如数据库审计日志等。 |
| 数据分析 | 配置数据风险分析的能力，包括资产风险趋势，告警增量趋势、数据风险类型分布等。 |
| 配置场景化风险分析的能力，如数据库批量查询（不少于3级个人基本信息） |
| 告警管理 | 配置告警名称自定义的能力。告警支持通过风险等级与时间窗口进行归并形成事件，并且支持智能化批量处置，如根据“事件名称”、“风险类型”、“风险等级”、“客户端IP”、“关联资产类型”、“关联资产”等进行类似条件事件的处置。 |
| 告警定义 | 可以提供紧急、重要、警告、提醒多个级别告警级别，并用对应颜色显著标识区分。 |
| 配置通过时间段、告警级别、风险类型、资产名称等条件进行历史告警的组合检索的能力。 |
| 告警处置 | 配置可视化呈现告警概览的能力，并支持自定义告警的归并规则。 |
| 配置忽略、手工处理、工单处理、白名单等方式进行告警处理的能力。配置根据告警相关条件进行智能批量处理的能力。 |
| 告警通知 | 配置将告警信息以邮件方式发送给系统相关责任人的能力，支持syslog告警信息的定向输出。 |
| 工单管理 | 配置查看工单概览与工单列表的能力，对工单流程全程监管与处置，形成告警到工单的风险自闭环。 |
| 考核指标 | 配置对告警处理情况进行统计展示的能力，查看工单列表状态及详情。可通过创建人、工单状态维度，工单平均响应时长进行统计考核指标。 |
| 运维报表 | 支持查看，下载生成的报表，可创建报表定时任务，自定义报表。并对数十种参数进行自定义配置。 |
| 具备自定义报表功能，并能将自定义的报表保存为模板，方便后续的运维和汇报，作为固定审计模板。 |
| 管理分权 | ▲产品需支持分区域分部门多级管理模式，应支持通过角色为账号赋权，安全角色之间权限相互制约，重要功能(如用户/权限管理、审计记录管理)应由对应赋权角色用户才能执行。 |
| 敏感数据地图 | 配置对全网数据进行拉网式筛查和梳理的能力，并可依据数据的敏感度、敏感数据类型、敏感数据数量、敏感数据分布以及敏感数据占比等进行统计分析和展示。 |
| 数据资产报表 | 配置数据资产多维度统计分析的能力，可提供资产梳理统计报告、资产变化趋势分析报告、敏感数据报告、热度分析报告等专项分析报表。 |
| 日志源管理 | 配置对接第三方安全设备日志源进行管理的能力，支持便捷的字段解析设置，例如json、字符串、自定义形式（解析包上传）进行解析。针对日志，支持syslog、kafka的形式进行采集，并进行清洗补全、字段映射的方法进行归一化处理。 |
| 登录安全 | 产品应具备web安全访问（https）、密码长度复杂度校验、密码错误尝试锁定、动态验证码验证、账号超时登出以及IP限制管理等安全性自定义配置功能。 |
| 系统升级 | 产品应配置系统在线升级、查看系统历史版本补丁等升级管理功能。 |
| 操作日志 | 产品应配置记录用户操作日志，包含操作时间、操作用户、操作IP、操作对象、操作内容等的能力； |
| 用户角色 | 产品应配置用户角色权限管理等能力，可配置支持三权分立，提供系统管理员、安全管理员、审计管理员角色。 |
| 系统维护 | 产品应配置对系统自身运行状态进行实时监测（如CPU使用率、内存使用率、磁盘使用率、网卡流量等）及网络排查、网络地址配置维护等功能 |
| 数据库探针 | ▲配置数据库探针，支持数据库实例不少于45个，数据库流量不低于600Mbps，SQL峰值处理能力不低于60000条/秒，SQL日志存储数量不少于80亿条；配置在访问的数据库服务器上部署审计插件的能力，获取数据库访问的数据流量进行审计。并且支持在插件模式下，进行环回流量审计；审计采集插件支持自动休眠，当所在数据库服务器的CPU、内存消耗超过阈值时，临时暂停抓包工作，避免与数据库服务器抢占资源，并且支持插件抓取流量的阈值设置。支持插件过滤条件设置，包括IP过滤和端口过滤。支持插件更新与升级、远程推送、批量推送。 |
| 产品资质 | 1.计算机软件著作权登记证书。★2.由具备资格的机构安全认证合格或安全检测符合要求的检验检测报告，或已经获得《计算机信息系统安全专用产品销售许可证》，且在有效期内的。 |

1. **数据库加密扩展服务**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 配置及性能要求 | **▲**单机加密速率不少于25000单元格/秒、SM4最大加密速率不低于4Gbps、最大并发连接数不少于3000；最小同时百万级表加密；数据库实例不少于3个、最小同时加密列数不少于60列。 |
| 高可用 | **▲**配置与现有加密设备实现HA高可用方式部署的能力。支持主、从互备，防止主机故障、网络故障、程序故障引起的业务损失；双机设备数据库实例数各扩展不少于3个。 |
| 单机bypass | 配置单机bypass功能，当加密网关故障时，可通过bypass插件直接从应用侧加解密数据，绕过加密网关直接访问数据，保证业务访问正常。 |
| 操作系统 | 支持麒麟、UOS等所有国产化操作系统，支持鲲鹏、飞腾等所有国产处理器芯片。 |
| 国密浏览器 | 支持使用国密浏览器满足密评的要求。 |
| 数据库兼容性支持 | 支持MySQL、Oracle、达梦、Kingbase、PostgreSQL、SQLServer、HotDB、TDSQL、TBASE、MariaDB等数据库类型的加密。 |
| 读写分离 | 配置在数据库的读写分离场景下数据加密的能力。 |
| 数据库加密方式 | 配置应用免改造、数据库免改造的方式实现字段级别的数据加密的能力。 |
| 闲时加密 | 配置数据源主机的指标监控能力，并进行实时展现。超过阈值时降低加密系统对数据源主机的资源占用，实现“闲时加密”。 |
| 存量加密 | 配置存量数据加解密的能力。 |
| 实时加密 | 配置实时数据加解密的能力。 |
| 加密算法和完整性校验算法 | ▲配置使用SM4国密算法和AES国际算法进行加密的能力 ，支持SM2证书认证。 |
| 配置SM3-HMAC算法保证加密数据在解密前的完整性的能力，识别加密数据是否被篡改。 |
| 任务管理 | 提供加密解密队列任务管理，实现对加密解密队列任务的执行步骤可控化管理。 |
| 断点加密 | 配置加密任务的断点加密的能力，可以在数据表加密任务的中断点处继续执行加密任务。 |
| 用户授权 | 配置独立于数据库以外的用户访问控制的能力，未经数据库加密系统授权的数据库用户不能读取、插入、修改、删除敏感数据。 |
| 客户端授权 | 配置独立于数据库以外的客户端访问控制的能力，数据库指定用户、到期时间及多个ip段授权，防止非法访问数据库。 |
| 密文索引 | 配置创建密文索引的能力，提升数据加密后的查询效率。 |
| 密文模糊查询 | 配置密文列数据进行密文模糊查询的能力。 |
| 密文管理 | 配置自定义设置无权限访问密文的返回值的能力，配置设置为密文返回、空值返回、指定值返回的能力。 |
| 复杂查询 | 配置多表联合查询，子查询，嵌套查询，条件查询，组合查询，分组查询等复杂查询语句等能力。 |
| 行业模版 | 配置根据业务类型组合多种数据类型定制行业模板的能力，如企事业单位敏感信息等。 |
| 业务数据识别 | 配置帮助业务识别数据敏感字段和可加密字段的能力；支持扫描识别数据库姓名、地址、银行卡号、身份证号、车牌号等敏感数据及显示命中率。 |
| 业务仿真加密 | 配置帮助业务进行加密、解密仿真测shi的能力，提前模拟真实加密和解密过程。 |
| 业务分析 | 配置对加密的业务数据库进行分析测shi的能力，可自动生成数据加密对业务的影响结果报表；支持加密表的预分析，自动生成加密策略建议。 |
| 多级密钥 | 配置标准的主密钥(RK)、密钥加密密钥-库密钥(DSK)、数据密钥-列密钥(DEK)三级密钥管理技术保障密钥安全的能力。 |
| 密钥备份 | 配置密钥自动备份、手动备份至本地和FTP的能力；支持加密策略备份。 |
| 离线密文恢复工具 | ▲配置使用离线密文恢复工具将密文恢复成明文的能力，防止不可预测原因导致系统宕机后数据库数据不可解密。 |
| 运维排查 | 配置下载加密过程日志、数据库后台和系统后台日志供排查后台错误的能力。 |
| 应用访问代理记录 | 配置查看访问数据库的应用系统地址和与之对应的代理访问数据库端口的能力，当应用系统查询访问故障时，通过查询应用访问记录查看代理访问数据库的端口，进行网络排查。 |
| 登录安全 | 产品应具备web安全访问（https）、密码长度复杂度校验、密码错误尝试锁定、动态验证码验证、账号超时登出以及IP限制管理等安全性自定义配置功能。 |
| 系统升级 | 产品应配置系统在线升级、查看系统历史版本补丁等升级管理功能。 |
| 操作日志 | 产品应配置记录用户操作日志，包含操作时间、操作用户、操作IP、操作对象、操作内容等。 |
| 用户角色 | 产品应配置用户角色权限管理等，可配置支持三权分立，提供系统管理员、安全管理员、审计管理员角色。 |
| 系统维护 | 产品应配置对系统自身运行状态进行实时监测（如CPU使用率、内存使用率、磁盘使用率、网卡流量等）及网络排查、时间设置、网络地址配置维护等功能。 |
| 产品资质 | ★商用密码产品认证证书（二级）软件著作权证书 |

1. **数据安全管理系统**

|  |  |
| --- | --- |
| 资质要求 | ▲兼容国产操作系统及数据库，并提供兼容承诺函加盖投标人公章。 |
| 性能要求 | 单台服务器支持客户端数量≥6000个。本次项目客户端数量不少于200个,支持通过增加授权增加客户端数量。 |
| 功能要求 | 1. 文件识别：配置对doc、xls、ppt、docx、xlsx、pptx、pdf、txt等常见办公文档扫描识别的能力；
2. 配置ZIP、7z、RAR等压缩文件的能力，能识别不少于10层压缩文档，并对压缩文档中的文件进行扫描识别；配置JPG、JPEG、PNG、BMP图片文件扫描识别；配置PDF等电子出版格式扫描识别；配置对加密码格式识别；配置对文件内嵌套文件识别及多层嵌套格式扫描识别；配置对eml邮件格式扫描识别；配置文件名扫描识别。（2）文档加密：配置对Word、Excel、PPT、PDF、书生、OFD和WPS等类型文档进行透明加解密的能力；配置对指定文档针对指定用户进行手动点对点加密操作的能力，加密后的文档只有在已成功安装客户端程序，并且拥有权限的用户才可以使用；配置文件外带管控的能力，即对外发到未安装数据安全管理客户端的环境中的文档进行权限控制，权限包括：口令认证、打开次数、有效期、编辑权限、显示水印、打印次数等。（3）水印管理：配置在终端系统中显示屏幕水印的能力，水印内容支持文字、二维码和图片等，支持按时间显示水印。（4）移动存储设备管理：配置对U盘等移动存储设备进行管控的能力，权限包括：禁用、加密读写、只读明文、只读明文+密文、正常读写等。（5）应用程序外发管理：配置对终端用户通过QQ、微信、企业微信等应用软件外发文件的行为进行审计、内嵌水印外发、加密外发、禁止外发等管控的能力。（6）网页访问与外发管理：配置对终端用户通过浏览器查看网页的上网行为进行审计与管控的能力，管控的类型包括：允许或者禁止访问对应的网站，审计用户的一般上网记录；配置对特定网盘类型、Web邮箱类型的网址上传附件的行为进行拦截控制；配置下载文件自动加密的能力，上传文件自动解密的安全保护控制。（提供产品截图）（7）打印管控：配置正常\带水印\禁止打印的能力；配置根据扫描结果进行打印管控以及设置不同水印管控；配置禁止去水印\允许去水印\审批去水印配置。（8）明文外发管控：配置登记后直接明文外发、审批通过后直接明文外发或者禁止明文外发，实现外发通道加密管控方式下的文件明文外发控制的能力。（9）数据审计：配置对终端行为、终端报表、业务告警等日志数据进行审计的能力。
 |

1. **网络安全监管平台**

**1.安全管理子平台**

**1.1资产中心**

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 资产概况 | 配置不限于资产总量及各类资产数量的统计的能力；资产运营统计；资产重要程度统计；硬件资产分布统计；软件资产分布统计；系统资产分布统计；资产单位分布统计；行业资产分布统计。 |
| 资产检索 | 配置单位、设备、软件、服务、系统、网站、机房、网络的全局检索的能力，检索方式支持预置条件快速检索方式以及支持高级搜索模式；高级搜索模式支持查询语句的编写；配置保存搜索场景以及查看搜索历史的能力。 |
| 资产管理 | 单位维护 | 配置对单位实体的查看、新增、编辑、删除、查看详情、批量操作以及打标签的能力，配置单位画像，从单位维度分析安全状况、安全业务响应情况等能力。 |
| 系统维护 | 配置对系统实体的查看、新增、编辑、删除、批量修改和打标签以及详情查看的能力。 |
| 软件维护 | 配置对软件实体的查看、批量打标签和详情查看的能力。 |
| 设备维护 | 配置对设备实体的查看、新增、编辑、删除、批量打标签、详情查看以及多网卡融合的能力。 |
| 服务维护 | 配置对服务实体的查看、批量打标签和详情查看的能力。 |
| 网站维护 | 配置对网站实体的查看、新增、编辑、删除、批量修改和打标签以及详情查看的能力。 |
| 机房维护 | 配置对机房实体的查看、新增、编辑、删除、批量修改和打标签以及详情查看的能力。 |
| 底层资产关系模型 | 实现多源资产数据的汇聚、融合、运营流程以及基础的资产管理能力。 |
| 资产关系模型至少需要建立如下关系：设备能够关联软件；软件能关联服务；设备能关联系统；系统能关联网站；设备、系统、网站能关联到云平台、网络、单位、机房、人员等信息。 |
| 资产发现 | 原始资产查询 | 配置对原始资产使用快捷检索和高级检索两种模式进行检索的能力。快捷检索支持可选择要输入的快捷搜索字段进行数据检索。语句条件支持【=】【!=】【in】【range】【exists】【no exists】；高级检索支持输出高级检索、高级检索模式支持查询语句的编写； |
| 数据源管理配置 | 1 配置根据搜索条件查询当前接入的数据源情况以及对应数据源设备的连接状态的能力；2 配置数据源获取的启用停用状态的切换的能力；3 配置新增数据源配置（包括新增、编辑、删除）的能力。 |
| 扫描任务配置 | 1 配置对扫描任务的检索的能力；2 配置扫描任务的管理，包括创建、编辑和删除的能力；3 配置对扫描任务的批量启动和批量停止的能力；4 配置对扫描网段的基本管理，包括创建、编辑和删除的能力；5 配置对扫描网段的检索的能力。 |
| 资产运营 | ▲规则管理 | 配置运营规则进行资产的自动运营纳管，至少包含三类规则，归属规则、运营规则、忽略规则：1、归属规则中至少包括基于探针序列号判断归属单位；基于IP判断归属单位；基于域名判断归属单位；自动富化归属信息；基于系统判断关联设备的归属单位；基于设备判断关联系统的归属单位；2、运营规则中自动纳管规则至少包含自动纳管发现资产；自动更新已纳管资产数据；运营规则中冲突判断最少包含流量探针类发现数据冲突判断规则；主动扫描类发现数据冲突判断规则；运营规则中融合规则至少包含设备类资产基础融合规则；网站类资产基础融合规则；软件类资产基础融合规则；服务类资产基础融合规则。 |
| 资产归属管理 | 1 配置对资产归属设备根据检索条件进行数据检索的能力；2 配置对设备资产设置对应的单位的能力；3 配置对资产归属系统根据检索条件进行数据检索的能力；4 配置对系统资产设置对应的单位的能力； |
| 发现资产审核 | 1 配置对待处理新增和更新资产数据根据检索条件进行数据检索；2 配置对待处理新增和更新资产数据进行数据的纳管或者忽略；3 配置对被忽略发现数据根据检索条件进行数据检索；4 持对被忽略发现数据移出忽略列表。 |
| 脆弱性管理 | 资产脆弱性 | 配置接入云端脆弱性结果的能力，配置对接第三方漏扫设备的能力，包括不限于以下功能：1 配置通过已纳管与漏洞扫描告警数据和漏洞知识库数据进行关联检索当前的漏洞告警列表；2 配置点击单条漏洞的详情展示详细信息，包括漏洞的基本信息、关联资产信息、证据信息和变更记录；3 配置对告警状态标记修复状态；4 配置切换至“资产视角”界面，点击资产列表的下拉按钮，可查看当前资产对应的漏洞告警情况，点击“查看详情”跳转至该条告警的详情信息；点击资产列表的“查看详情”按钮，跳转至资产管理模块，展示该条资产的详情信息。 |
| 资产潜在漏洞 | 1 配置通过已纳管与漏洞扫描告警数据和漏洞知识库数据进行关联检索当前有潜在漏洞的资产列表的能力；2 配置查看当前资产对应的潜在漏洞列表的能力，下钻至该条漏洞知识库的详情信息展示界面；3 配置跳转至资产管理模块的能力，展示该条存在潜在漏洞资产的详情信息。 |
| 资产风险评估 | 风险模型管理 | 配置基于《信息安全风险评估规范》GB/T 20984国标规范的基础上进行风险评估模型的定义与评估参数设置的能力。1、资产的价值评估维度包括保密性、完整性、可用性等，可对这些维度进行等级定义设置；2、资产的威胁等级，可设置威胁评估范围；3、资产的脆弱性等级，可设置脆弱性评估范围；4、支持根据资产价值、威胁等级、脆弱性定期计算每个资产的风险等级；5、支持根据资产的风险等级计算总体、区域、单位等资产集合的风险等级；6、支持呈现资产风险评估模型的多个维度的定义、模型计算逻辑。 |
| 风险概况 | 配置各类风险评估维度统计的能力，包括不限于资产风险等级统计、网络区域风险统计、单位风险排名、总体风险趋势、资产风险排名、资产威胁等级统计、资产脆弱性等级统计、资产价值分级统计。 |
| ▲风险评级 | 1、配置以列表的方式呈现每个资产的风险评估情况的能力，显示内容包括不限于资产名称、资产ip、业务组、风险等级、资产价值、威胁等级、脆弱性等级；2、配置查看每个资产的风险评估详细依据的能力，包括显示该资产的基本信息、风险评估趋势、风险等级、评估时间；3、配置查看每个资产的风险过程数据的能力，包括资产价值评估过程数据、威胁等级评估数据依据、脆弱性等级评估数据依据；4、配置查看资产的价值评分的能力，并可对资产价值进行四个维度的打分，包括保密性、完整性、可用性、业务相关性；5、针对资产的脆弱性等级、威胁等级评估数据至少需要显示威胁及脆弱性的个等级数量统计、趋势、类型分布以及资产涉及的为处置整改的脆弱性和威胁。 |

**1.2全局检索**

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 底层技术 | 配置实时大数据OLAP引擎的能力，基于性能突出的Clickhouse，采用列式存储、稀疏索引、倒排索引、向量化执行等技术。 |
| 快速检索 | 配置可选择要输入的快捷搜索字段进行数据检索的能力。语句条件支持【=】【!=】【in】【range】【exists】【no exists】等。 |
| 检索结果 | 根据快速检索或者高级检索进行符合条件的数据呈现，数据呈现至少包含以下功能及内容：1、配置根据检索出的数据类别进行自动分组呈现，分组类型不限于告警日志、流量日志、终端日志、告警、事件的能力；2、配置根据搜索结果统计本次检索动作的耗时和查询的数据量以及根据搜索时间分析各时间点数据量的能力，呈现每个时间点的数量，统计支持在图表上选择时间段进行二次筛选；3、配置根据搜索的数据结果进行各类别数据的数据类型分类的能力，比如告警日志中可分为漏洞利用告警、攻击利用告警、情报告警等，用于快速二次筛选；4、配置数据字段展示配置功能，用户可自定义每种数据需要展示的字段以及数据列的展示顺序5、配置针对数据表中的常用字段（比如IP、告警类型、攻击结果等）进行添加到搜索、从搜索中排除、新建搜索等二次筛选操作的能力；6、配置检索结果的导出的能力；7、配置单条数据的详情查看的能力，数据详情最少支持键值对显示方式，针对数据字段过的的数据支持只看有值字段。 |
| 历史检索 | 配置保存最近不少于100条的历史检索条件的能力。检索范围、时间范围、检索条件和过滤语句。 |

**1.3告警管理**

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 告警管理 | 告警数据检索 | 1、配置可选择要输入的快捷搜索字段进行数据检索的能力。语句条件支持【=】【!=】【in】【range】【exists】【no exists】；2、配置输出高级检索类SQL语句进行数据检索；3、配置对多个检索条件使用AND或OR进行连接以及支持使用（）编辑逻辑连接顺序；4、配置将检索条件保存为常用检索条件的能力；5、配置保存最近不少于100条的历史检索条件的能力。检索范围、时间范围、检索条件和过滤语句；6、配置对检索任务的导出的能力。 |
| 告警标记 | 1、配置对告警列表中的数据标记为误报的能力；2、配置对告警列表中已经标记为误报的数据取消误表标记的能力；3、配置对告警列表中的数据进行已读、维度标记的能力；4、配置对告警数据进行关注标记的能力。 |
| 二次塞选 | 1、配置在搜索结果中快速选取结果字段进行二次快速搜索的能力，自动生成一个对应主界面搜索时间和搜索数据源，搜索内容为该字段的新的搜索任务；2、配置在搜索结果中的某条数据的某个字段进行快速排除操作的能力。 |
| 检索结果展示 | 根据快速检索或者高级检索进行符合条件的数据呈现，数据呈现至少包含以下功能及内容：1、配置根据搜索结果统计本次检索告警的告警类型分布情况、规则命中情况、告警数量趋势统计的能力；2、配置根据搜索的数据结果进行告警类型分类统计的能力，并可根据分类进行快速二次筛选；3、配置数据字段展示配置功能，用户可自定义每种数据需要展示的字段以及数据列的展示顺序；4、配置针对数据表中的常用字段（比如IP、告警类型、攻击结果等）进行添加到搜索、从搜索中排除、新建搜索等二次筛选操作；5、配置检索结果的导出的能力；6、对单条告警的操作至少包括查看详情、打标签、研判动作（误报、无需处置、查实需处置、转事件等操作）；7、单条告警显示内容根据告警类型的不同对告警信息进行信息分组显示。 |
| 事件管理 | 事件数据检索 | 1、配置可选择要输入的快捷搜索字段进行数据检索。语句条件支持【=】【!=】【in】【range】【exists】【no exists】；2、配置输出高级检索类SQL语句进行数据检索；3、配置对多个检索条件使用AND或OR进行连接以及支持使用（）编辑逻辑连接顺序；4、配置将检索条件保存为常用检索条件的能力；5、配置保存最近100条的历史检索条件的能力。检索范围、时间范围、检索条件和过滤语句；6、配置对检索任务的导出的能力。 |
| 事件管理 | 1、配置在新增事件界面输入基本信息、受害者信息、攻击者信息、攻击利用、举证信息的能力；2、配置对事件单条或者批量的进行删除操作的能力；3、配置对事件单条或者批量的标记无需处置状态信息的能力；4、配置在事件详情界面支持查看基本信息、受害者信息、攻击者信息、攻击利用、告警列表、举证信息的能力；5、配置在事件编辑界面支持查看基本信息、受害者信息、攻击者信息、攻击利用、告警列表、举证信息的能力。 |
| 主动防护配置 | 1、配置事件的一键封禁操作的能力，可对项安全设备发送管控数据；2、配置通过短信、邮件、蓝信、消息中心方式给运营人员发送的能力；3、配置联动安全设备进行告警、事件的联动处置的能力。 |

**1.4分析引擎**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 规则管理 | 分析规则可视化配置维护 | 1、配置规则名称的列表展示的能力，支持对规则名称、规则来源以及规则模版等检索条件的搜索；2、配置对单一数据的分析及多类数据的关联分析的能力；通过图形化配置、分步骤导航等形式，支撑关联分析策略的设计、发布、编辑；3、配置规则的导入、导出、批量发布的能力；4、配置流式和批式两种规则引擎的灵活配置的能力。 |
| 分析引擎 | 流式分析引擎 | 配置将在线数据（流式数据）的能力，把满足条件的数据提取并生成告警，能够将相同类型数据的单一字段进行标注，形成告警。数据类型包括但不限于：流量日志、系统日志、应用日志、告警日志等。 |
| 批式分析引擎 | 配置将离线数据（批式数据）的能力，把满足条件的数据提取并生成告警，能够将相同类型数据的单一字段进行标注，形成告警。数据类型包括但不限于：流量日志、系统日志、应用日志、告警日志等。 |
| 告警生成引擎 | 配置将满足条件的数据按照告警数据的结构的能力，填充和富化形成告警。字段操作提供最大值、最小值、输入、规则名、第一条、最后一条、字典映射、来源-威胁情报、生成当前时间。告警富化字段支持可视化配置。 |
| 归并引擎 | 配置将命中后的告警数据的能力，将相同特征的告警数据合并形成一条告警数据，减少告警冗余。字段操作提供最大值、最小值、第一条、最后一条、生成当前时间、合并为字符串、字典映射。 |
| 后置配置 | 配置将满足条件的告警的能力，统一打标签，并且能够对已经生成的告警字段再次手动更新告警信息。系统提供了后置配置规则模板对这类配置信息提供了固化模板，避免重复配置。 |
| 规则模版 | 威胁情报模板 | 配置将情报信息与流量特征对比和碰撞的能力，分析用户系统日志中是否存在命中威胁情报的攻击行为，并生成告警。 |
| 单表过滤模板 | 配置将内容匹配、正则匹配、静态资源引用以及相关逻辑条件组合满足条件后产生告警的能力；支持对日志进行过滤，过滤条件支持AND/OR/NOT等逻辑运算、多层级嵌套；支持引用资源对象和引用过滤器；支持条件表达式字段类型匹配，可使用等于/不等于、匹配/不匹配，包含/不包含、属于/不属于、大于/小于等逻辑； |
| 单表统计模板 | 配置将单个日志在某个时间窗口内且重复出现后产生告警的能力；针对单一数据源过滤，过滤条件支持AND/OR/NOT等逻辑运算、多层级嵌套；支持引用资源对象和引用过滤器；支持创建统计节点，通过统计节点建立规则，在指定的时间范围内，对符合过滤条件的字段进行计数、求和、求平均、最大值和最小值计算，将其与阈值进行比较以发现异常威胁告警；支持字段分组和去重； |
| 关联统计模板 | 配置将两类日志源中条件互相补充且满足条件后产生告警的能力；配置创建关联节点，通过日志字段关联匹配，在指定的时间范围内，对符合过滤条件的日志中进行统计，将其与阈值进行比较以发现异常威胁告警；配置字段分组和去重的能力； |
| 运行管理 | 规则分析任务管理 | 支持将运行的任务通过看板的形式展示，能实时展示任务运行中数量，运行失败数量，任务总数量，命中告警数量， CPU和内存使用率；并且能够对运行的任务人工干预， 批量停止，批量启动，批量删除操作。 |
| 资源管理 | 支持将IP地址，端口，时间， 字符串这些静态信息引入到命中规则中，可以被关联规则过滤或者加白使用，并且静态信息能够多次使用。 |
| 监测分析能力 | ▲提供不少于10份以上公开发布的APT报告作为证明；（提供相关截图证明材料） |

**1.5分析中心**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 云端实体分析 | 1、提供云端大网数据特征分析、包括不限于URL、文件MD5的分析，分析内容不限于所属行业、在线状态、所属国家、省市、地理经纬度等基础信息；2、配置分析IOC信息的能力，不限于提供ioc标识、主机名称、端口、标签；ioc风险信息，不限于提供风险等级、影响平台、是否定向攻击、恶意代码家族、威胁类型、解析事件、攻击链类型、攻击团伙名称、置信度、样本md5、协议类型、TTP等；IOC家族信息，不限于提供恶意家族名称、恶意家族详情、家族参考连接、风险等级、影响平台、威胁类型等;IOC利用者相关信息，不限于提供攻击事件/团伙名称、参考文档、检测事件、报告连接、攻击手法、报告发布时间、团伙所在国家、团伙别名、涉及行业、攻击者利用漏洞、受影响系统等；3、配置分析安全信誉的能力，提供不限于安全级别、恶意网站分类、网页地址、页面标题、检测发现地域、顶级域名、官网地址、仿冒对象等；4、配置分析whois信息的能力，显示内容不限于注册邮箱、注册组织、注册人名称、联系电话、更新时间、创建时间、注册服务商注册到期日期；5、配置分析备案信息的能力，包括网站主体域名、网站名称、开办主体、网站类别、开办者名称、公安备案号、备案地等。 |
| 多维分析 | 分析任务管理 | 1、配置对分析任务使用卡片和列表的方式进行呈现；2、配置多维分析任务的创建，创建字段任务名称、任务标签、任务描述与任务分组；3、配置对分析编辑功能，可以修改任务名称、标签、描述。可对分组进行变更；4、配置对分析任务按照创建时间、关键字以及标签进行检索；5、配置对分析任务新增、编辑与删除标签。配置对标签的检索；6、配置对分析任务新增、编辑与删除标签。配置对标签的检索。 |
| 可视化交互 | 1、配置以画布的方式进行人机交互的能力，以人、事、地、物、ip等元素在画布上进行关联关系描绘，直观的以图谱的方式展现各元素之间的关系；2、配置多维分析可视化画布交互方式的能力，不限于对检索结果的线索剪枝、对分析拓线结果进行截图、对分析结果一键清空、对分析结果一键清空、对分析任务按照分析时序进行标号，显示分析实体名称、对系统分析结果全局的缩略图展示与移动、多种分析布局方式、每次检索实体的最大数量限制、分析任务全屏和带有组件模式的切换等；3、配置将分析任务保存为分析案例的能力，可对案例进行二次分析；4、配置将每一步分析结果保存为分析快照的能力，并支持以时间轴的方式对分析历史进行数据回放。 |
| 攻击链分析 | 分析任务管理 | 1、配置对攻击链分析任务进行新增，修改，查询，删除，重启和查看；2、配置攻击链分析任务创建的能力，创建字段任务名称、攻击者ip，受害者ip，攻击者名称，告警时间范围，任务描述；3、配置分析任务的删除的能力，确认删除前需要对用户做明显提示；4、配置对攻击链分析任务编辑的能力，对未执行或完成的任务进行编辑，可对任务名称、攻击者IP,受害者IP,攻击者名称、告警时间范围和任务描述等内容进行修改；5、配置攻击链分析任务检索的能力，可按任务名称、任务状态、攻击者名称、攻击者IP和受害者IP条件进行模糊和精确检索；6、配置对未执行、完成状态的任务进行任务重启操作；7、配置对未执行、完成状态的任务进行任务重启操作。 |
| ▲攻击链分析引擎 | 1. 配置基于网络攻击链（Cyber Kill Chain）和MITRE ATT&CK模型进行安全事件攻击链分析的能力，分析展现侦查追踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成目标各阶段的攻击手法、攻击结果；最终已时间轴的方式将事件涉及的网络攻击进行攻击过程还原；2、配置以钻石模型分析展现攻击者、受害者、基础设施、攻击能力之间的关系；分析展示内容不限于原目的IP；基础设施中的邮箱、域名、ip；攻击能力的攻击手法和攻击技能等；
 |
| ▲APT攻击分析能力 | 配置APT攻击分析能力。 |

**1.5工作指挥**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 治理资源 | 单位实体维护 | 1、配置单位的增删改查的能力，维护信息不限于单位名称、单位简称、组织机构代码、单位类型、行业类别、网站URL、上级主管、单位地址、详细地址、单位标签、单位描述等；2、配置查看单位相关治理资源的能力，包括单位基本信息、关联人员信息、拥有装备情况、拥有手段情况；3、配置单位与其他治理资源之间的关系维护的能力，建立“单位-人员-装备-手段”关联关系，支持单位视角查看“拥有人员、装备、手段”情况；4、配置单位的关键词检索、排序、标签配置等的能力。 |

**1.7数据中心**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 元数据管理 | 数据标准管理 | 1、配置数据标准浏览功能，支持根据数据标准分类进行管理；2、配置基础主题标准维护的能力，配置对已梳理的基础主题数据标准的管理维护功能，包括修改、提交、发布等基础维护功能。数据标准定义信息不限于标准编码、数据长度、标准中文名称、数据精度、标准英文名称、度量单位、数据业务类型、样例数据、别名、描述、制定依据、业务规则、所属路径等；3、配置标准维护功能，支持对数据标准定义、关联字典的维护。 |
| ▲元数据管理（提供截图） | 1、配置丰富的元数据管理功能，包括元数据检索、采集、维护、应用分析等，沉淀企业数据知识，提高数据理解、定位、消费效率；2、配置业务元数据管理，管理业务元数据确定共同认可的词汇和对应的信息资产，确保领域知识的共同理解，保障行业元数据的标准化和归一化；3、配置数据业务类型管理，有助于数据被正确使用、重用并满足各种规范，打通数据孤岛并形成企业级知识传承平台；4、配置信息分类编码标准管理，创建并维护数据模型中使用的数据字典。制定并管理系统遵循的统一数据标准，统一数据口径；支持信息分类编码标准目录管理、内容多级管理，支持信息分类编码标准全文检索；5、配置信息分类编码标准批量导入/导出功能，以及导入校验功能；可对信息分类编码进行版本管理，历史版本对比。 |
| 数据质量管理 | 1、配置质量评估标准功能，建立系统数据质量评估标准，从完整性、一致性、准确性、及时性、唯一性评估数据质量；2、配置评分参数配置、质量检测任务配置、质量检测记录查看等统一的质量检测管理功能。 |
| 数据仓库 | 1、配置数据管理中接入的业务系统数据进行统一管理功能，以便于应用，支持可视化创建数据模型；2、配置展示数据库/数据表列表功能，支持添加、编辑、删除、检索数据库；3、配置批量导入导出数据表功能，批量创建数据表，包括字段、字段对应信息项和业务元数据等，支持创建结构体字段；4、配置查看数据库监控信息功能，包括数据存储趋势、数据产生消费趋势、业务元数据分析；支持查看数据模型以及数据库变更日志；5、配置查看数据表监控信息功能，包括数据表存储趋势、数据产生消费趋势、数据入库差值；数据表基本信息包括数据表存储量、字段数、记录数、数据表类型、存储路径、索引字段等；支持查看数据表字段数据，包括字段名称、中文名、描述、数据业务类型、数据标准等。 |
| 数据服务 | 数据消费服务 | 1、配置数据资源的统一市场化管理功能，用户可通过界面配置的方式选择API数据服务或文件数据服务，以满足不同的数据使用场景，降低数据使用的开发门槛，帮助企业实现数据应用价值最大化；2、配置API接口下载功能；可通过界面配置的方式选择API数据服务，高效创建API服务，接口开发时间缩短至分钟级；3、创建API服务后需要返回APIkey，APISecret,如果数据需要加密则还需要返回 加密秘钥；4、配置在线生成数据服务API使用文档功能。 |
| 数据服务安全管控 | 1、支持消费数据进行数据加密后再传输。2、支持对数据服务访问者进行安全认证授权管理3、支持对安全数据的消费进行记录，便于后续的安全审计工作。 |
| ▲联动处置 | 配置与现有防火墙进行联动处置功能； |
| 配置与现有服务器安全加固软件进行联动处置功能； |
| 配置与现有探针进行数据对接功能，采集流量信息； |

**1.8报告中心**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 报告总览 | 报告基本查询 | 1 配置查看系统中报告列表功能，包括名称、大小和时间；2 配置通过报告名称、报告类型对报告进行搜索查询功能。 |
| 报告操作 | 1、配置对指定报告的下载(word、pdf)和预览(pdf)功能；2、配置批量删除报告功能；3、配置报告按照自定义进行分组展示功能。 |
| 报告管理 | 快速报告 | 1、配置通过指定模板创建快速报告功能；2、配置报告列表查看功能，配置报告搜索功能；3、配置报告批量删除功能。 |
| 周期报告 | 配置创建周期报告任务功能，周期设置维度不限于周期报告名称、报告模板选择、执行频率（日、周、月、年）、容错机制（运行失败重启机制设置，重启间隔、重启次数）。 |
| 数据源管理 | 数据源 | 1、配置添加数据库、文件、api等方式创建数据源功能，不限于Excel、CSV、ElasticSearch、MySQL、Oracle、PostgreSQL、clickhouse、restful api等；2、配置在线预览数据源中的数据功能，不限于显示数据库表、文件解析内容、api返回数据等。 |
| 模板管理 | 模板可视化维护 | 1、配置新建模板功能，包括选择数据模型（包括维度和度量），数据表的字段作为XY轴数据，支持根据选择维度或度量进行筛选；2、配置模板编辑中用户自定义展示的图形方式的功能；3、配置模板编辑中用户定义展示画面中以图表、文本、图片或推荐模板进行展示的功能；4、配置模板编辑中的最后结果保存、预览和退出的功能；5、配置新建时点击或拖拽方式添加标题、图表、文本、推荐图表、图片等类型组件的功能；6、配置组件修改标题文字、字体颜色、字体大小、组件背景色等样式的功能；7、配置图表组件在线选择数据模型的功能，拖拽选择X轴数据及Y轴数据，并在Y轴数据选择后可定义数据的聚合方式：计数、最大值、最小值、平均数、求和等，配置拖拽选择筛选器，配置通过文本筛选、条件筛选、高级筛选等方式设置筛选器的具体内容对数据进行筛选；8、配置图表组件切换展示图形类型：饼图、柱图、折线图、表格等功能；9、配置组件右键编辑图层层级、组件删除、所在报告页位置移动等功能；图表组件和推荐组件还支持下载图行、导出CSV文件、编辑组件标签、保存到组件库等功能；10、配置模板报告新增报告页、报告页切换及可视画布区缩放等功能；11、在线模板预览即为实时数据报告、并支持预览模板导出pdf操作。 |

**1.9态势感知**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 综合态势 | 从分别从全球视角、全国视角、单位视角分析，当前的网络安全综总体风险、告警总体数量及类型占比、安全告警等级分布、通报整改质量、安全告警发展趋势以及告警实时监测列表。 |
| 资产态势 | 主视觉以余姚市电子政务外网网络区域逻辑视角展示每个网络区域的风险程度，并统计每个网络区域的高中低危的网络资产数量。资产相关的统计分析组件包括资产数量及类型统计、资产风险排名情况、资产业务分组安全分析、网络区域风险排名、设备及系统资产类型统计。 |
| 漏洞态势 | 可视化分析组件包括漏洞相关告警数量痛殴攻击、漏洞分类统计、漏洞等级占比、单位漏洞个数排名、风险评估趋势以及漏洞实时列表。 |
| 运行态势 | 提供对各类资产运行状态进行监控，满足实时查看当前网络中设备运行是否正常，从而及时发现设备故障等需要及时处理的问题。 |

**1.10平台基础环境要求**

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 国产化服务器 | 不少于2U标准上架设备；含滑轨。CPU: 不少于1颗64核国产处理器 主频2.2GHz；内存:不少于256G，DDR4 硬盘：不少于2块960G SSD固态硬盘+12\*4TB企业级SATA 3.5寸硬盘 ； 电源：冗余双电源 网口：不少于4\*GE管理电口，2\*GE光口；其他接口：不少于6\*USB3.0接口;1\*DB9 Console接口；1个IPMI接口。含所有国产化操作系统和所有用到的国产化软件、硬件，含三年产品原厂标准维保服务，硬盘不返厂服务。共需配置4台。 |
| ▲其它 | 为保障系统平台稳定运行，基础环境资源不得低于以上参数要求，若平台无法正常、有效运行，投标方需增加配置及设备，所有费用由投标方承担。 |

**2.安全运行子平台**

|  |  |  |
| --- | --- | --- |
| **模块** | **指标项** | **技术参数** |
| 安全监管平台 | 平台硬件 | CPU不低于2颗24核国产处理器，内存不少于256G，硬盘不少于48T，网口不少于4个千兆电口，不少于2个万兆光接口（含光模块），不少于1+1热插拔冗余电源，国产化操作系统，具备配置网络安全平台部署所需的一切软件、硬件配件等。共需配置2台。含三年产品原厂标准维保服务，硬盘不返厂服务。 |
| 监测中心 | 具备监测云、网络、终端、应用、数据等在线网络资产的能力，具备根据资产分布、漏洞和指纹信息进行扫描探测和统一管理的能力，摸清区域资产总数。具备广域网流量、政务云出口流量、IDC机房流量的安全监测能力，实时发现和登记各类网络攻击、风险隐患、安全事件以及网络资产的能力。 |
| 平台提供事件成果解决方案，实现事件导入导出、事件/风险检索、事件/风险研判、事件/风险处置完整的事件处置流程。 |
| 配置通过事件/风险数据关联同类型事件/风险、同单位事件/风险、同终端事件/风险等联想方式等能力。（提供功能截图） |
| 事件类型、子类型展示，以矩阵形式展示事件所属类型以及子类型。 |
| 场景化验证，包括弱口令、挖矿、勒索病毒等场景，配置通过单位名称、IP地址、时间等多字段组合查询场景内容功等能。 |
| 场景自定义设置，自定义场景判断条件、分析周期、分析对象、场景标签，快速配置场景应用。 |
| 资管中心 | 具备监管终端、监控、WEB、在线业务系统等在线网络资产的能力，具备根据资产分布、漏洞和指纹信息进行统一管理的能力，摸清资产底数，具备形成统一的资产立体化监管能力。 |
| 配置按资产重要程度、资产区域和组织架构将资产分级分类管理功能。 |
| 平台配置不低于40种单位行业属性标签，不低于20种单位类型属性标签，并支持多属性标签联合检索。 |
| 配置单位详情信息快速浏览功能，信息至少包括单位信息、安全检测、人员信息、业务系统、资产等全部字段，并且能查看关联的历史安全事件、历史安全隐患和历史攻击告警，并一键展开事件详情进行处置或通报和支持进行系统画像快速浏览，信息同样包括系统信息、安全监测、等保信息、供应链、人员信息、单位信息等字段。 |
| 配置系统画像快速浏览功能，信息至少包括系统信息、安全监测、防护情况、基础网络、人员信息、单位信息等字段。（提供功能截图） |
| 配置在系统卡片中查看单位近期发生的安全事件和风险隐患信息功能，一键展开事件详情进行研判处置。 |
| 配置IP资产一键溯源功能，迅速定位资产风险。 |
| 配置在系统卡片中查看单位近期发生的安全事件和风险隐患信息功能，一键展开事件详情进行研判处置。 |
| 配置卡片式、表格形式展示数据源档案信息功能，展示内容包括数据库卡片显示数据库名称，数据库类型、所属单位、主机、端口、所属行业、是否敏感库、安全等级分级、数据来源、标记重要数据库，数据表、告警数、安全事件、安全隐患。 |
| 数据表卡片显示数据表中文名名称、表名、所属数据库、所属单位、主机、所属行业、最近更新以及是否是敏感库、安全等级分级、共享属性、更新周期，标记重要数据库，统计列数和告警。 |
| 接口档案显示接口名称，接口地址、所属单位、请求方式、所属系统、所属行业、数据领域、主题分类以及风险情况、共享属性、开放属性、更新周期，标记重要数据库，统计告警。 |
| 平台安全域卡片式管理和列表式管理，展示信息包含所属单位、IP范围、安全事件、安全隐患、攻击告警，安全域分配IP及已使用IP统计及安全域防护状况等。 |
| 平台配置根据探测任务状态标签对探测任务进行筛选功能，包括执行状态、完成、停止、异常等状态标签。 |
| 配置按区域、厂商域名数量统计CDN节点数量功能，按区域和运营商数量统计IDC节点数量，按区域和备案单位统计ICP节点数量。 |
| 配置在线自定义构建网络拓扑图功能。 |
| 平台提供人员档案管理解决方案，实现宏观人员态势展示、人员标签和人员详细管理功能。 |
| IP资产审核管理，支持通过页面操作、导入表等方式管理IP资产信息，支持批量申请入库、退库，支持批量审核入库、变更、退库的资产，支持批量导出IP资产审核信息，已退库的IP资产支持再次发起入库申请。（提供功能截图） |
| 配置多个用户角色、指定多个用户作为IP资产入库、变更、退库的审核人，支持分别为IP资产入库、变更、退库配置审核人，支持配置多级审核。（提供功能截图） |
| 感知中心 | 具备提供网络安全威胁可视化的入口的能力，具备基于全链路平台获取的各类监测数据及日常业务流转产生的业务数据的能力，具备以网络安全事件与威胁风险监测为驱动，对网络空间安全相关信息进行汇聚融合的能力，具备从不同视角感知网络安全态势的能力。 |
| ▲配置监测并展示不同类别资产安全情况功能，包括云、网络、数据、应用、终端等，并配置下钻功能。（提供功能截图） |
| 配置展示制度规范功能，并配置预览功能。 |
| 配置地图形式展示各区域安全告警和待办工单数量功能，并配置下钻功能。 |
| 配置单位、系统、资产、云平台、大数据平台、物联网、工业控制、移动APP的数据展示功能，并配置下钻功能。 |
| 配置预警中心、通报处置业务开展情况的数据统计功能。 |
| 配置在地图展示安全事件功能，支持与后台事件调查功能联动，一键进行事件调查。 |
| 配置大屏地图资产与后台信息发布一键联动功能，通过地图点击风险资产下发预警。 |
| 以列表形式统计以下内容并进行可视化呈现：网站区域访问量排行top5、访问IP排行top5、被攻击网站排行top50、攻击来源IP排行top10、攻击类型排行top10。 |
| 响应中心 | 具备支持将监测到的漏洞隐患或安全事件按照信息系统网络安全事件隐患分级标准进行下发通报的能力，具备预警提醒或限期整改的通知能力，具备显示被通报的单位反馈处置结果的能力，具备实现通报预警工作流程化管理的能力；具备支持其他通报方式的能力，包括但不限于短信、网站、浙政钉通知等的能力；具备支持对通报情况和处理情况进行统计展现和提供不同类型的通报报告的能力。 |
| 配置信息下钻功能，点击通报、预警信息，可以查看对应详情，如通报标题、创建时间等。 |
| 配置展示各个区域的通报情况功能，以图表方式展示。 |
| 新增通知可以输入文字、图片、超链接、表格、代码片段等多种信息类型，其中文字支持设定字体大小、文字颜色，文字高亮、加粗、倾斜等不少于5种配置。 |
| 通知举证信息支持一键溯源，包括溯源到资产档案、系统档案、情报信息、原始日志等。 |
| 预警详情可以输入文字、图片、超链接、表格、代码片段等不少于5种信息类型，其中文字支持设定字体大小、文字颜色，文字高亮、加粗、倾斜等不少于5种配置。 |
| 通报详情支持显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等。 |
| 配置通过通报下发单位及业务系统的信息补全任务功能，通报接收单位补全信息返回后支持将已补全的信息直接入库。 |
| 配置通报流程可配置功能，各流程的对应的处置单位可自动生成，并支持自定义调整。 |
| 通报支持进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒；针对已超时的通报进行超时显示，并显示具体超时时间。 |
| Web端工作台 | 具备提供本系统安全监管平台所有子模块的Web端工作台应用的能力。 |
| 配置对通报过程进行跟踪记录功能，完整记录任务流转过程详情并同步到Web端平台。 |
| 移动端 | 具备浙政钉进行通报下发或处置流转的能力，具备对通报过程进行跟踪记录的能力，具备完整记录任务流转过程详情并同步到Web端平台的能力。 |
| 配置移动端和Web端横向打通功能，关联数据和业务。 |
| 配置在移动端快速处置通报、完成相关操作等功能。 |
| 大数据节点软件 | 具备大数据分析和计算能力，包括并不限于基础大数据计算模块和分布式事件处理模块。具备支持横向平滑扩展的能力，具备通过增加硬件服务器数量的方式增加平台集群的计算处理性能的能力。包括并不限于以下内容：1、具备大数据平台能力；2、具备分布式复杂事件处理引擎的能力；性能要求：1. 支持不少于1000个用户同时在线并发查询。2. 10亿数据关键字查询结果响应时间小于2秒。3.单节点数据采集和处理性能不低于15000EPS。 |
|  | 大数据安全监测 | 具备对重要的大数据平台进行统一的监测的能力，具备摸清全市重点大数据平台数据状况及其使用情况的能力，包括并不限于同时实现对涉大数据平台的单位管理、大数据信息系统管理、大数据平台安全防护情况管理、涉大数据平台或信息系统的人员管理等的能力。平台提供完整的单位管理解决方案，帮助用户直观、清晰、便捷的完成单位资产录入、资产概况总览和细分单位管理。 |
| 云平台安全监测 | 具备云平台的日常网络安全监管的能力，包括并不限于监控、感知、应急全流程的安全监管机制功能。具备建立云平台全息档案的能力，具备实时感知云平台当前安全态势与外部安全威胁感知的能力。 |
| 资产数据治理 | 具备基于网络规划的资产主动探测的能力，包括并不限于明确到单位与责任人的能力。具备网络环境包括政务外网、互联网暴露面、兼顾行业专网提供系统可用性和无故障运行时间评估等的能力。具备资产普查一体化流程、自动发现、下发确认、信息补全、审核、归档、联动控制的能力，具备政务网的信息资产与安全资产的全面梳理的能力。 |
| 平台配置资产数据摸底解决方案功能，实现资产检索、探查、研判分析和源头分析。 |
| 资产检索，配置多种SQL语法组合检索功能，包括“与”、“或”、“等于”、“存在”、“包含”等语法，配置语法不少于14种，且具备语法示例，方便用户快速上手使用。 |
| 资产展示，支持资产名称、资产类型、资产大类、资产小类、资产标签、单位名称、所属行业、地理位置、安全等级、事件名称、风险隐患名称、受攻击名称、等保等级等多个字段展示，并可自定义删减字段。 |
| 资产详细信息，资产详细信息包括最后更新时间、有效性、服务商、注册名等不少于40个字段。 |
| 配置资产数据多层研判功能，用户可根据展示字段进行过滤和排除完成初步研判，同时可根据详细信息和原始数据进行深度研判。 |
| 平台配置资产探测任务管理功能，支持探查任务新增、执行、停止、编辑、删除等功能。 |
| 平台配置任务名称和时间范围对探测任务进行检索功能。 |
| 平台配置根据探测任务状态标签对探测任务进行筛选功能，包括执行状态、完成、停止、异常等状态标签。 |
| 平台配置查看探测任务结果查看功能，一键查看任务详情、任务结果以及存在问题。 |
| 检查督查 | 具备实现线下检查、线上填报两个业务流程的能力，具备实现检查数据的在线采集和结果分析的能力，具备促进各单位积极开展安全管理工作和定期反馈资产情况的能力，具备配合专项线下检查工作任务的能力。 |
| 配置对单位自查、现场检查、远程检查任务发布情况、完成情况和逾期情况进行统计等功能。 |
| 配置用户新建检查计划功能，输入内容包括计划名、计划联络人、计划时间、计划标签等字段，同时配置手动新建标签并为计划打标功能。 |
| 配置在同一个现场检查任务下发时选择单位、系统等多个现场检查对象等功能，同时支持针对每一个对象配置相关检查表单。 |
| 配置对同一次远程检查任务新建时选择的属于同一个单位的多个系统自动合并成一个远程检查任务等功能，在下发任务时支持选择特定的支撑单位。 |
| 配置在同一个单位自查任务下发时选择单位、系统等多个自查对象等功能，同时支持对每一个对象配置相关检查表单。 |
| 配置在同一张检查表下新建多个检查模块等功能，可为每个模块配置模块名称并导入相应的检查项。 |
| 提供上移、下移等操作项，支持对检查模块下的检查项的顺序进行手动调整。 |
| 配置通过查看动作对检查对象库中的单位关联的各类信息进行聚合展示等功能。 |
| 指挥调度 | 具备构建网络空间全息地图的能力，包括并不限于实现网络安全态势挂图展示、网络安全通报预警、安全检查、指挥调度等业务挂图作战等。 |
| 分析研判 | 具体包括规则模型、关联模型、统计模型、情报模型、离线模型等在内的不少于5大类安全分析模型的能力，具备实现AI高级分析、实体间网络互访关系的多级钻取能力，具备威胁关系一键溯源的能力。 |
| 配置界面化交互式完成安全建模等功能，模型类型包括统计模型、规则模型、情报模型、关联模型、AI模型 不少于5种；模型支持标签化管理，支持单个模型的启用禁用控制，支持一键查看模型的输出结果；多个模型可以形成串并联关系，前一个模型的输出结果可以作为后一个模型的输入。 |
| 安全分析模型支持自定义新增，新添加的模型可选择适用的作用域，如全局通用、单选机构，如选择单选机构即选择应用的组织架构，可通过字段映射、静态值、模板、表达式等多种方式自定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。 |
| 实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展； |
| 配置报告内容自定义等功能，包括标题、图表、报表自定义，其中支持的图表类型不少于15种。 |
| 安全专项 | 具备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安全专项分析的能力，包括并不限于对可能受到影响的资产、行业、受影响的重要单位进行分析的能力，具备给各区域监管单位提供相关安全威胁隐患的数据的能力。 |
| 2.情报专刊正文部分包含威胁隐患的发现背景介绍、影响范围评估和安全修复建议，影响范围评估通过图表形式展示影响行业、影响资产等信息。 |
| 情报专刊详情数据支持界面化展示和导出Excel文件，数据内容包括漏洞类型、影响资产IP、端口、协议、厂商、IP区域、归属者、用户场景、资产单位、发现时间等信息，支持一键验证和发起通报等功能。 |
| 配置手动录入自身发现及第三方厂商的情报专项报告等功能，录入项包括但不限于报告名称、编号、专题大类、专题小类、发现厂商、标签、背景介绍、安全建议、附件，并配置编辑、删除等操作等功能。 |
| 配置手动录入自身发现及第三方厂商的流量分析报告等功能，录入项包括但不限于报告名称、编号、分析类型、事项类型、攻击类型、受害目标、发现厂商、标签、概述、安全建议、附件，并支持编辑、删除等操作。 |
| 配置接入人工分析推送的情报专项报告和流量分析报告等功能。 |
| 威胁情报模块 | 具备云端威胁情报订阅功能模块：包括并不限于内置威胁情报离线库及更新功能；具备采用情报数据进行实时检测防御等能力；具备在线查询与溯源的能力：包括并不限于云端提供对IoC威胁类型、多源情报、WHOIS、开放端口、SSL证书等多维度的溯源分析的能力；具备云端服务的能力：包括并不限于订阅高级威胁分析情报、云端提供最新APT入侵、0day漏洞预警、病毒变种情况等分析报告订阅的能力。 |
| 配置用户自建行业情报库等功能，自建情报库支持增删改查、导入、导出。 |
| 情报库支持不少于4种IOC类型，IP、域名、文件HASH、邮箱。 |
| 情报类型>=4种，包括恶意、监管、黑客组织等，支持的情报标签类型>=10种，包括安全事件、行为、威胁主体、攻击目标、应对措施、观测数据、可疑的、事件、家族、组织、攻击方法、攻击活动、攻击指标、其他等，每条情报支持包含多个情报标签。 |
| 情报查询配置通过IOC同时跨越多个情报源查询等功能，结果汇总展示。 |
| 情报查询结果配置跳转到云端和第三方威胁情报库交叉验证等功能。 |
| 情报IOC配置与原始日志和威胁告警中的源IP、目的IP、域名等>20个字段进行碰撞并产生告警。 |
| 碰撞情报IOC配置通过情报源、IOC类型、标签、置信度筛选等功能。 |
| 情报告警名称配置修改等功能，无效情报配置单条禁用等功能。 |
| 情报碰撞结果配置聚合方式查看威胁来源等功能。 |
| 配置统计情报源碰撞命中情报数量等功能。 |
| 重大安保 | 具备实现重大活动保障前期、中期、后期分阶段的任务管理的能力，具备保障预案管理的能力，包括并不限于对重点单位/系统、技术支撑单位、人员、探针、驻点排班等静态数据的管理以及对安保检查、通报处置、应急处置、安保巡检、指挥调度等业务支撑能力。 |
| 配置新建活动等功能，包括活动名称、活动地点、摸底、临战、备战、决战阶段的时间进度、活动负责人及联系方式、活动描述，同时支持编辑、删除、结束活动。 |
| 说明指挥人员的作用，指挥人员是安保活动的组织领导人员，负责领导和决策安保活动的重大事宜，包括提供筹备组织、制度信息，指挥调度安保活动。 |
| 配置说明指挥单位的作用等功能，指挥单位是安保活动的组织领导机构，负责领导和决策安保活动的重大事宜，包括提供筹备组织、制度信息，指挥调度安保活动。 |
| 配置说明安保人员的作用等功能，安保人员是安保活动的被监管单位人员，负责安保系统的日常管理和维护，落实保障工作，参与应急演练和培训，以及处置安全事件和应急事件。 |
| 配置说明安保驻点的作用等功能，安保驻点是从指挥中心、安保目标、支撑力量三大角色的人员中选调到安保活动现场驻点，负责驻点的安全运行。 |
| 配置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等功能。 |
| 配置查看总体驻点报平安情况，驻点人员签到、签退情况等功能。 |
| 配置查看单个驻点的具体安全情况等功能，包括但不限于驻点基本信息、报平安情况、保障单位信息、驻点人员信息、关联探针信息。 |
| 考核评价 | 具备构建常态化网络安全综治考核、日常考核工作机制等能力，包括并不限于针对不同被监管对象建立对应的网络安全检查指标库，实现管理统计、工作质量考核、安全评价、综治考评等功能，具备按不同时间周期提供考核报告的能力。 |
| 配置对考评任务排名等功能，支持展示考评任务单位排名、展示各分数等级分布；支持展示单位排名总分列表，包括单位名称、所属区域、单位类型、单位联系人、联系方式、单位直属性质、得分等；支持展示单位排名各项列表，包括单位名称及各一级评估项小计；支持通过单位名称、单位直属性质查询单位；支持下载排名明细，包括单位总分、排名情况及各评估项得分明细。 |
| 考评项类型支持自动填报、多选、单选、填写、附件上传等；自动填报的考评项来源包括监测事件、监测风险、资产管理、通报处置等，并支持自定义自动填报考评项条件。 |
| 配置暂存、提交、重复提交考评表材料项、备注项填报单位任务等功能；支持根据填报情况自动计算预得分、材料完整度；支持展示任务信息，包括任务状态、任务时间、单位填报时间、任务说明、任务联络人及其联系方式、任务附件；支持展示单位任务状态及状态变更时间；支持查看单位任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称和提交/操作的操作时间、操作账号。 |
| 配置对风险隐患、安全事件、通报情况三个维度设置考评规则表等功能。 |
| 具备构建常态化网络安全综治考核、日常考核工作机制等能力，包括并不限于针对不同被监管对象建立对应的网络安全检查指标库，实现管理统计、工作质量考核、安全评价、综治考评等功能，具备按不同时间周期提供考核报告的能力。 |
| 配置对考评任务排名等功能，支持展示考评任务单位排名、展示各分数等级分布；支持展示单位排名总分列表，包括单位名称、所属区域、单位类型、单位联系人、联系方式、单位直属性质、得分等；支持展示单位排名各项列表，包括单位名称及各一级评估项小计；支持通过单位名称、单位直属性质查询单位；支持下载排名明细，包括单位总分、排名情况及各评估项得分明细。 |
| 考评项类型配置自动填报、多选、单选、填写、附件上传等功能；自动填报的考评项来源包括监测事件、监测风险、资产管理、通报处置等，并支持自定义自动填报考评项条件。 |
| 配置暂存、提交、重复提交考评表材料项、备注项填报单位任务等功能；支持根据填报情况自动计算预得分、材料完整度；支持展示任务信息，包括任务状态、任务时间、单位填报时间、任务说明、任务联络人及其联系方式、任务附件；支持展示单位任务状态及状态变更时间；支持查看单位任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称和提交/操作的操作时间、操作账号。 |
| 配置对风险隐患、安全事件、通报情况三个维度设置考评规则表等功能。 |
| 机器学习 | 配置市场主流的长周期高级机器学习算法等功能 |
| 全链路流量监测模块 | 硬件规格 | 网口：千兆电口不少于4个，万兆光口不少于2个（含2个万兆多模光模块） 吞吐率：网络层不少于5Gbps；硬盘容量： 不少于12T ；内存：不少于64G ，USB口：USB2.0口不少于2个，电源：1+1热插拔冗余电源。国产化操作系统，具备配置全链路流量监测模块部署所需的一切软件、硬件配件等，含三年产品原厂标准维保服务，硬盘不返厂服务。 |
| 全流量检测 | 配置全流量检测，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 |
| 弱口令风险检测 | ▲配置对HTTP、IMAP、SMTP、POP3、Redis、Telnet、FTP等协议的弱口令检测等功能（提供截图证明）配置自定义弱口令规则配置（最短口令长度、最少字符类型数）等功能，自定义新增弱密码及其检测类型 |
| WEB登录 | 配置自定义HTTP登录行为关键字等功能，包括用户名和密码配置自定义HTTP登录行为的用户名获取来源等功能，包括但不限于请求头、URL、Cookie、POST-body；配置自定义配置状态码、返回内容与登录成功/失败状态的绑定关系（提供截图证明） |
| 暴力破解检测 | 配置HTTP、SMB、SMTP、IMAP、POP3、FTP、TELNET、RADMIN、SSH、RDP、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PGSQL、LDAP等协议的暴力破解等功能，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 |
| 密码明文形式传播 | 配置HTTP密码明文传输和HTTP 密码Base64传输检测等功能，能识别出登录页面URL、账户和明文密码 |
| ARP欺骗检测 | 配置根据MAC与IP地址的绑定关系等功能，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 |
| 协议解析 | 配置Websocket通信的HTTP、HTTPS（需要导入服务器私钥证书）协议解析等功能，检测WEB攻击 |
| 双向审计 | 配置双向审计等功能，对请求和响应都进行审计 |
| 攻击检测 | 配置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、服务错误攻击检测等功能配置通过智能语义分析引擎等功能，对XSS跨站脚本、SQL注入攻击和OGNL注入攻击进行检测配置通过智能语义分析引擎等功能，检测JSP脚本文件上传和PHP脚本文件上传 |
| 深度检测 | 包含30种以上的深度检测模块，可支持市场主流远程管理工具的检测能力，且能识别市场主流的隧道通信工具 |
| WEBSHELL检测 | ▲配置WEBSHELL检测功能，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） |
| 解析协议 | 配置 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等功能 |
| 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 |
| 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，分析其安全风险配置沙箱逃逸检测功能，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、国产化系统多种检测环境。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 |
| 资产识别和管理 | 配置对流量中的IP地址、端口等进行统计功能，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） |
| 一键登录排错 | 产品内置的排错平台可对系统进行深度配置和排错，配置一键检测故障、配置核对、表分区检查、表检测、信息收集等功能。 |
| 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） |
| 配置kafka、短信、邮件、syslog、ftp、sftp、钉钉等数据外送方式等功能syslog、kafka、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 |

1. **网络安全配套服务**

**1.云端安全实时监测服务**

|  |  |
| --- | --- |
| **服务名称** | **服务要求** |
| 云端安全实时监测服务 | 1、提供不少于50个资产的综合安全托管服务授权，协助用户完成日常安全运营工作。在运营服务期内提供7x24小时的安全威胁监测服务，持续监测网络内的安全隐患情况并进行分析，包括对外部网络攻击网络漏洞利用情况、恶意软件活动情况、以及内网安全情况，对安全监测发现的安全隐患及高危事件在服务规定时间内进行通告，同时能够每日同步安全状况。1. 运营服务期内基于平台提供服务资产识别与梳理服务，包括但不限于服务资产IP地址、端口、资产类型、操作系统类型及版本等属性，同时能够分析现有资产漏洞信息，包括但不限于SQL注入、XSS、命令注入、反序列化、越权访问等漏洞信息，同时提供可落地的专业漏洞修复指导。
2. 基于平台，持续监测用户侧漏洞利用情况，对监测发现的安全漏洞进行分析验证，同时持续跟踪整改情况。

4、基于网络安全监管平台的资产和漏洞情况，结合威胁情报信息，提供资产漏洞预警服务5、要求能够在运营服务期内提供网络安全监管平台的设备巡检和维护，巡检包括但不限于本地的平台CPU、存储情况、系统事件、授权情况、功能模块以及本地探针的运行状况和特征库版本，并发现设备故障后，能够协调原厂售后服务并跟踪直至设备故障修复。6、安全事件快速响应，基于本地网络安全监管平台对各类安全数据及日志数据进行关联分析与深入挖掘，及时发现各类安全事件并通知客户，同时协助客户开展通报、处置等响应动作。7、提供每年不少于四次对具体安全事件的深度分析，包括攻击复现、追踪溯源定位攻击者等内容，从多维度对安全事件进行分析，精准定位威胁根源。针对重点高危事件输出事件分析报告。8、▲提供事件跟踪管理服务，通过分析研判确认后的安全事件，对事件处置过程进行跟踪形成闭环，每周输出工作周报。9、提供每月主动分析服务，服务人员定期综合所发现的安全事件、攻击情况进行主动分析，包括但不限于告警趋势分析、威胁类型分布分析、高威胁攻击者分析，同时进行场景化安全分析，包括APT告警分析、恶意软件情况分析、网络攻击情况分析、WebShell情况分析、内网安全情况分析、数据库安全情况分析、爆破行为分析、弱口令分析等，每月输出运营月度报告。10、提供定期的运营汇报解读服务，综合所发现的安全事件结合客户网络环境，评价客户侧整体网络安全态势，同时输出问题事件的分析说明，并给出针对性建议和方案，让客户更加了解网络安全现状和当前安全趋势。11、运营问题解答服务，提供对于网络安全监管平台的使用故障问题、平台漏报/误报、安全事件分析问题提供原厂工程师处理和跟踪闭环。 |

**2.网络安全配套其他服务**

|  |  |  |
| --- | --- | --- |
| **模块** | **指标项** | **技术参数** |
| 网络安全配套服务 | 漏洞扫描服务 | 具备提供现场驻场服务人员使用漏洞扫描工具，对余姚市电子政务网或者被指定的网络主机漏洞、Web应用扫描、指定网站的所有文件进行安全扫描，通过人工验证扫描结果后，给出整改意见，输出《XX年XX月漏洞扫描报告》。每年提供不少于4次全网漏洞扫描服务。 |
| 基线检查服务 | 针对操作系统、数据库、网络设备等配置合规性进行检查，评估发现潜在风险点。每年提供不少于4次基线检查服务。 |
| 渗透测shi服务 | 每年提供不少于6个系统渗透测shi服务。 |
| 风险隐患与事件通报服务 | 具备现场驻场服务人员使用网安运营平台能力，发现安全风险隐患后，主动向存在风险隐患的系统责任单位进行隐患通报，通过平台梳理安全风险隐患，统一下发，建立安全隐患事件，统一管理安全事件。 |
| 安全检查服务 | 根据国家、省市下发的相关考核与监督检查要求，驻场服务人员配合招标人或相关单位开展网络安全检查工作，完成相关考核要求。提供每年不少于4次设备安全巡检服务。 |
| 安全工作报告服务 | 现场驻场服务人员每月度对发现的安全问题与处置情况进行综合汇总，形成安全态势分析与工作报告，输出《XX年XX月安全工作报告》 |
| 运营流程优化服务 | 根据已有安全运营流程或制度，从可行性、落地性和规范性上进行相应评估，形成余姚市具备特色、具备落地性的安全通报流程和制度。 |
| 运营文件编制服务 | 常态化安全检查期间，驻场服务人员对网络安全专项检查通知文件进行编制，整合、沉淀相应模板文件材料，作为安全监管平台中的知识库，供相关单位或运营人员参考。 |
| 资产梳理服务 | 现场驻场服务人员定期对余姚市政务外网进行资产梳理，更新资产信息库，实现资产归属动态清单，定期输出《电子政务网资产清单》、《余姚市互联网网站资产清单》等。 |
| 策略调优服务 | 对已有网络安全运营平台、SOAR、防火墙、APT等设备，以及本期新建设设备进行策略调优等服务，包括并不限于白名单、黑名单、设备联动、模型优化、规则优化等策略的调优，保证策略最新，保障具有实在的安全能力。 |
| 重要时期安全保障服务 | 服务期间驻场服务人员结合技术工具对指定的信息系统、网站、服务器等资产进行实时监测，及时按操作流程处理系统安全隐患及事件。 |
| 安全加固服务 | 现场驻场服务人员使用网络安全运营平台能力，监控所有业务系统，对漏洞扫描、基线核查、安全监管监测、安全运维过程当中发现的安全问题提供处置建议，指导和修复业务系统的漏洞，协助和处置服务器、网络设备、安全设备等的安全加固工作。 |
| 宣传教育及培训服务 | 提供组织本地区，每年不少于2次，包括信息安全方面培训、人员安全意识培训、运维操作安全技能等宣传培训活动。 |

1. **国产化软件购置**

|  |  |
| --- | --- |
| 国产数据库软件 | 具备对数据分区管理能力，配置对表进行范围分区、列表分区、哈希分区等分区机制等功能。支持混合负载应用场景，既支持事务处理，也支持分析处理。同时支持bytea、oid、clob、blob等数据类型，能够存储大型非结构化数据，如：文本、图像、视频、空间数据等。支持GIS地理功能，支持面向LBS位置的数据分析和处理能力。数据库存储模式支持：本地存储、共享存储、分布式存储。支持分布式大规模并行处理集群150个节点以上。支持高可用模式的数据库集群，可在线管理集群节点（增删改）；支持应用程序的透明访问能力，在数据库节点发生故障时，可自动切换到其它节点。支持AES、DES等及国密SM算法等。支持对同构、异构数据库的监控，包括其他国产主流数据库、ORACLE、PostgreSQL、DB2、MySQL、SQL Server等，监控信息包括：CPU、内存、文件系统、网络情况、系统运行状态等。支持国产操作系统：统信UOS、麒麟系列等主流操作系统。支持MIPS系列（龙芯）、ARM系列(飞腾、鲲鹏)、Alpha系列（申威）、X86系列（兆芯、海光、Intel、AMD）等。支持Tomcat、Weblogic及信创平台认证的东方通、金蝶、中创……等中间件。支持Java、C/C++、.NET、Node.js、PHP、Python、Perl、Tcl、Go等程序开发语言或工具。支持JDBC、ODBC、Node.js、C API、OLEDB、OCI等多种开发接口。提供多种过程语言包括：PL/Perl、PL/Python、PL/Tcl、PL/JAVA等。兼容大部分Oracle、MySQL等常用语法。 |
| 国产应用中间件 | 具备web应用、ejb应用、虚拟主机、应用服务器集群、身份验证、日志审计等基本工作，提供类库管理、图形化监控、jvm配置、垃圾回收配置等工具，支持实例部署、数据库连接服务，为业务系统提供运行环境。 |

**六、详细功能要求**

本项目建设内容主要包括数据安全服务和网络安全服务购置，年限为三年。其中数据安全服务包含数据分级分类、数据安全态势感知平台、数据库加密扩展、数据安全管理系统和数据库软件等服务的购置；网络安全服务包含网络安全管理平台、网络安全运行平台和网络安全配套等服务的购置。具体功能要求如下：

**（一）数据安全服务**

本项目通过购买服务的方式，建立余姚市电子政务外网数据安全防控能力，服务购置期限为三年。

本次数据安全服务购置主要包括数据分级分类、数据安全态势感知平台、数据库软件、数据库加密扩展和数据安全管理系统。

1. **数据分级分类**

本次项目需提供数据分级分类服务一项，服务年限为三年。

数据分级分类服务具体包含内容如下：

（1）数据分级分类咨询服务

根据国家、行业相关要求梳理余姚市数据分级分类规范，输出余姚市分级分类标准。

（2）数据安全服务

建立健全的组织架构是数据安全治理工作的基础，制定部门职责与人员角色及动态协同机制，制定并不限于规章制度、管控办法、奖惩机制、技术规范等，制定并不限于由分管领导、数据安全人员、数据管理人员以及相关人员等组织层面的数据管理制度规范；协同业主单位处置数据安全问题、常态化数据安全风险发现和处置；全年开展 2 次数据安全培训（包括但不限于政策规范制度解读、接口和批量数据使用安全、第三方管理等）；全年开展 2 次数据安全应急演练（包括但不限于数据篡改、数据泄露等）；协同业主单位开展本地区各单位数据安全相关检查工作，形成检查报告，配合业主单位指导相关问题责任单位闭环处置且提供书面整改报告。

（3）暗数据发现和分级分类

具备对于余姚市数据资产进行自动发现并进行分级分类，协助采购人全面梳理数据资产，具备数据安全治理和数据基础治理能力，含不少于2000张表不少于40000个字段。

（4）数据分级分类实施服务

具备利用敏感数据发现分析出敏感数据后，再按照政务数据类型进行敏感数据分级分类，从敏感数据分类出发，选择敏感表格组成敏感数据集合，在保障安全的基础之上实现便捷管理。

（5）硬件配置

不低于下列参数及数量：国产CPU 16核\*2 /散热片\*2 /DDR4 3200 16G\*2 /480G 2.5 SATA 6Gb R SSD\*1 /4TB 3.5 SATA 7.2K HDD\*2 /横插04盘12G SAS 硬盘背板 /8口SAS卡/550W电源模块\*2 /双口10G（满配光模块）SFP+光纤网卡\*2 /10G SFP+多模光模块\*4 （满配光模块）/滑轨 /150cm 国标电源线\*2 / 整机三年保修且硬盘免回收。

（6）具备服务期内软件、硬件系统全功能免费升级服务。

1. **数据安全态势感知**

本次项目以购买服务的方式，建立余姚市电子政务外网的数据安全态势感知平台，服务购置年限为三年，具体要求如下：

（1）具备敏感数据资产管理能力，包括并不限于敏感数据识别、分级分类等。

（2）具备数据安全设备管理能力，包括并不限于数据安全设备接入、统一策略管理、设备运行监控等，兼容已有加密、动静态脱敏及水印设备。

（3）具备安全日志接入能力，包括并不限于安全日志采集接入，兼容已有加密、动静态脱敏及水印设备等。

（4）具备统一告警管理能力，包括并不限于支持统一告警、工单管理，兼容已有加密、动静态脱敏及水印设备等。

（5）具备支持数据源数不小于200，具备接入数据安全设备数不小于50；具备全场景安全风险事件集中收集、清洗、分析、预警，日志和数据解析、静态风险监测、动态风险检测、数据安全态势、数据安全大屏，实现数据安全可视化，可量化，可感知和可追溯的能力；包含数据库探针设备，具备支持数据库实例不少于48个，数据库流量不小于600Mbps，SQL峰值处理能力不小于60000 条/秒，SQL日志存储数量不小于80亿条；具备扩展选配API接口、网络流量解析等探针组件的功能。

1. **数据库加密扩展**

数据库加密系统是基于网关代理加密技术实现敏感数据加密存储，系统支持采用SM2证书对身份进行认证，使用国际主流加密算法AES和国产加密算法SM4对敏感数据加密，使用SM3-HMAC对敏感数据进行校验，能满足等保、分保等评测要求，能满足商用密码系统应用与安全性评估的存储数据完整性和机密性保障的评测要求；在此基础上增加独立于数据库的访问授权机制。

数据加密系统主要功能包含：

（1）数据源管理

数据源管理主要用于对各种数据库类型数据源的配置，包括添加数据库信息、对数据库主机监控的阈值配置等。

（2）敏感数据发现

系统内置丰富的敏感数据类型特征库，特征库里包含常见的敏感数据类型，例如：中文姓名、身份证号、固定电话、手机号码、银行卡号、电子邮箱、中文地址、邮政编码、企业单位名称、组织机构代码、营业执照代码、税务登记代码、企业三证合一代码等共二十余种。支持以正则表达式的方式扩展自定义敏感数据特征，添加至自定义敏感类型特征库。

（3）数据加密

数据加密的目的是保证数据的机密性，防止未经授权的人员查看敏感数据，保证不会因为存储介质的丢失、被盗等因素造成泄密。数据库加密系统对数据列进行加解密，对不同字段采用不同的工作密钥，系统支持AES等国际标准算法的同时还支持SM4等国密算法。

（4）访问授权

提供独立于数据库的访问授权机制，限制部分用户的增删改查操作，同时对访问的客户端的IP、时间等进行限制，从而防止内部特权用户或突破边界防护的外部未授权人员查看敏感数据。

（5）密钥管理

数据库加密系统采用标准的三级密钥管理机制：主密钥由安全管理员存储于加密卡中，通过查找索引号将其调用。库密钥被主密钥保护，由系统自动产生，并执行自动更新机制。列密钥由高度随机算法或量子密钥发生器生成，通过国密算法对数据进行加密处理且与密文进行数据封装被库密钥保护。多级密钥对数据进行了多重防护符合行业标准内对密钥管理的要求。

（6）备份与恢复

系统备份功能将关键数据和配置信息进行打包导出并上传到加密服务器作为备份，导出信息栏中会增加备份文件的描述、导出时间、导出类型和文件，也可下载到本地。当需要恢复配置时，选择备份包恢复即可回退配置。

（7）审计管理

记录系统的敏感操作，并可用于事件追溯。审计功能记录各用户进行登入、登出、加密、解密、客户端授权、用户授权操作的具体信息生成操作日志。可以使用用户名称、操作类型、起止时间对操作日志进行筛选。操作日志和操作日志副本独立于应用之外的安全审计子系统。无法从应用自身发起删除行为。

本次项目在原有单机数据加密系统的基础上扩展为双机模式，提供方式为服务购置的方式，年限为三年，具体要求如下：

数据加密系统扩展为双机模式；加密速率不低于25000单元格/秒；SM4加密速率不低于4Gbps；并发连接数不低于3000个；不低于百万级表加密；数据库实例不低于3个；加密列数不低于60列；双机设备实例数扩展不低于3套。具备服务期内软件系统全功能免费升级服务。

1. **数据安全管理系统**

本次项目设计以购买服务的方式，建设数据安全管理系统，服务年限为三年。

数据安全管理系统主要技术参数要求如下：

具备通过加密、审批、阻断和审计等手段，为不同架构不同操作系统（同时支持所有国产系统）的电脑终端提供数据扫描、文档加密、权限管理、外设管控、屏幕水印、文档审批等安全防护的能力。包含不低于200个客户端永久授权。具备服务期内软件系统全功能免费升级服务。

（1）文档加密管理

文档加密管理提供针对办公终端用户文档的加解密以及权限管理功能。

文档手动加密：文档手动加密提供单个文档和多个文档的主动加密功能，同时配置文档自动加密/强制加密功能。

文档自动加密：文档自动加密提供整个文档夹加密功能，文档目录可由使用者自行设置，并可设置该文档夹中的文档使用权限。用户可以通过拷贝、拖拽方式将文档放入文档夹中，文档自动加密及设置权限。

文档强制加密：文档强制加密功能提供根据策略配置内容，终端电脑全盘或者指定目录配置针对特定格式、特定名称的文件强制加密功能，支持配置加密密级以及例外免除加密的路径。

文档透明解密与权限管控：支持至少Windows平台，文档的权限控制包括读、写、另存、脱密、截屏、拷贝、文档水印、无水印打印、带水印打印、离线使用等十种基本文档权限。管理员可以通过控制台设置不同密级对应的文档权限，文档在使用指定密级加密后具有该密级设定的使用权限。

文档加解密：文档透明加密，可对Word、Excel、PPT、PDF、书生、OFD和WPS等类型文档进行透明加密，不改变用户的任何操作习惯，不改变原有文档信息的格式；文档透明解密，配置对密文办公文档利用Office、WPS、书生、Adobe、福昕等软件透明解密打开使用等功能，并进行对应的读、写、另存、水印等权限管控;

授权用户访问，文档被加密后，只有授权用户才能正常访问，否则文档打开是乱码形式显示；系统集中审计，系统可以审计加密文档的相关信息，如：时间、电脑名称、用户名、文档名、解密文档内容等，便于事后追踪。

文档点对点加密：点对点加密功能配置管理员在控制台配置点对点加密模版功能，支持配置目标用户、操作权限集合、使用期限、密文打开次数等。用户在终端执行点对点加密功能时，可以直接选择管理员配置的公共模版，也可以在终端自己手动创建和维护加密模版。点对点加密后的文件只有原作者和对应有操作权限的目标用户才可以打开阅读并使用。

配置用户手动开启点对点加密的文件自动分享给目标操作用户等功能，点对点加密的文件支持用户通过提权流程向文件作者扩展申请延期使用或者其它权限。除此之外还支持用户作者针对点对点加密的密文进行权限编辑修改，方便用户操作。

文档外带功能：文档外带功能在Windows平台配置对外发到未安装数据安全管理客户端的环境中的文档进行权限控制等功能，支持管理的文档权限包括：访问口令、打开次数、使用时间、编辑、显示水印、打印次数、打印水印等。配置针对用户制作外带文件的行为进行审批流程控制等功能，支持强制用户在制作外带文件时开启特定权限的配置。文档外带功能在信创平台支持访问口令权限的控制。

安全U盘功能：安全U盘功能是结合国产化第三方的安全U盘特殊硬件设备组合使用，在安全可控的基础上设计安全U盘中文件读写的操作日志。安全U盘的性能参数如下：存储容量：4G/8G/16G/32G/64G/128G；加密存储算法：AES-256、SM4，硬件芯片加密支持；大文件读/写速度：12Mbps；安全访问功能：配备专门的安全U盘生产管理软件工具，支持安全U盘访问口令控制（支持错误超次锁定）、文件存储加密、分区隐藏、防病毒、文件读写日志的审计。

（2）移动存储介质管理

移动存储介质管理针对计算机客户端移动存储设备进行管理，实现了U盘、移动硬盘等移动存储设备完整的生命周期（注册、授权、使用、挂失、注销）管理与管控，既保证了计算机移动存储设备的正常使用，又能有效防止随意使用移动存储设备造成的资料外泄等安全隐患。

移动存储设备注册：配置针对在用的移动存储设备进行注册、授权、挂失等统一管理等功能，配置在控制台进行统一管理等功能。根据U盘是否已在系统中注册，可以分为已注册U盘和未注册U盘，并支持设置不同的策略，兼顾安全性和易用性的统一。

移动存储介质管控：该功能通过策略设置，对PC客户端的U盘操作权限进行管控，包括禁用、加密读写、只读明文、只读明文+密文、正常读写等五种权限。

为了便于管理，可统一给未注册的移动存储设备下发策略；如禁止使用未注册的U盘，该策略将禁止使用员工私自插入的U盘。为了减少管理员注册大量U盘的工作量，系统支持用户通过客户端进行远程注册或通过注册工具进行注册。

（3）网络访问行为管控

配置对终端用户访问网络资源、实时通讯及外发文件的行为进行审计管控等功能，根据网络中不同的访问协议支持的业务管控类型主要包括：

1）网页访问与外发管控

可对终端用户通过浏览器查看网页的上网行为进行审计与管控，管控的类型包括：允许或者禁止访问对应的网站，审计用户的一般上网记录，并支持对特定类型网盘类型、Web邮箱类型的网址上传附件的行为进行拦截控制。支持基于内容扫描的登记外发/审批外发管控。

配置对常规第三方基于Web的业务系统保护功能，即下载文件自动加密，上传文件自动解密的安全保护控制。

配置对网站地址资源库进行统一增、删、改、查管理等功能。根据网站的业务属性的不同和管控方式的区别进行分类管理，根据网站的业务属性可以对网站地址分类成新闻、财经等进行管理；根据网站的管控属性可以对网站地址分类成黑名单网址、白名单网址和普通网址。

2）基于FTP/FTPS协议的外发管控

可对终端用户通过FTP/FTPS协议外发文件的行为进行管控，配置根据目的FTP服务地址的不同对FTP外发行为进行不同方式的管控处理等功能。管控的类型包括审计允许外发行为、内嵌水印外发、加密外发文件、禁止外发行为。配置对通过资源管理器、命令行以及第三方FTP工具等外发文件的行为进行审计与外发管控等功能。

3）基于SMB共享协议的外发管控

配置对终端用户将文档发送到局域网共享目录的行为进行审计、内嵌水印、加密外发与禁止外发的管控等功能。配置管控的局域网共享目录协议为SMB2.0功能；

配置针对终端本地开设共享目录的行为进行检测和提示等功能。

4）针对应用程序外发文件管控

配置对终端用户通过QQ、微信、企业微信、钉钉、飞书、RTX、向日葵、Teamviewer、百度网盘、腾讯微云等应用软件外发文件的行为进行审计、内嵌水印外发、加密外发、禁止外发的管控等功能；配置对通过360安全/急速浏览器、IE浏览器、chrome浏览器、Firefox浏览器、Edge浏览器、搜狗浏览器外发文件的行为进行审计、内嵌水印外发、加密外发、禁止外发的管控等功能。

对部分其他第三方应用程序外发文件进行扫描审计外发、扫描阻断外发管控。

（4）打印管控

对用户打印文档的事件进行审计与管控，管控的方式分为正常打印、带水印打印和禁止打印，其中带水印打印的控制方式支持用户自定义配置打印水印模版的内容。打印管控的过程中对发起打印的文档内容进行扫描，并根据扫描的结果是否命中进行灵活的管控，对用户的文档打印行为进行日志和附件进行审计。

配置用户在打印过程中手动发起去水印打印的流程等功能，策略配置用户禁止去水印打印、直接去水印打印或者审批去水印打印的管控方式。

（5）终端数据防泄漏

通过对终端本地文档和外发文档内容的扫描，根据预先定义的规则对文档进行内容扫描，进而对文档进行分级分类以及后续的审计、加密、审批或阻断外发等处理。支持文档规则的与、或、非等逻辑运算。

根据行业特点和客户需求，对关键数据按照重要性进行梳理和划分，制定数据安全性由高到低的数据分级分类规则。按照数据分类规则，已包含在行业预置规则库中的类别可直接选用规则，制定出对应的扫描文档规则，然后对规则库进行验证，确保规则库的准确性和易用性。采用文档内容扫描引擎，对组织复杂信息环境中的不同非结构化数据进行分析，根据文档内容的语义特征和格式，将文档业务策略进行智能匹配。现已支持所有主流格式的办公文档和部分网络协议格式。

配置根据设置不同的扫描模式等功能：一种是以效率优先的快速扫描模式；一种是以扫描内容更全面的详细扫描模式。用户可以根据关注业务的类型选择不同的扫描模式。

1)全盘智能扫描

全盘智能扫描功能可根据预先定义的规则和策略，对用户终端的本地文档进行全盘扫描，并对含敏感数据的文档做审计、隔离、添加文档标密标签/隐形数字水印标签、加密管控处理，从而对终端敏感数据进行安全防护。

管理员可配置全盘扫描的条件，例如配置扫描执行路径、扫描跳过路径、文档类型、文档大小、允许全盘扫描启动和执行的终端性能指标等。系统也可以智能判断终端是否满足扫描条件，当终端锁屏或者终端性能指标（如CPU占用率、内存占用率、笔记本电池电量、磁盘IO读写使用率等）达到指定条件，才启动扫描。扫描过程中会根据终端性能自动停止，尽可能减少对终端用户操作的影响。模块支持文档增量扫描，仅对未扫描或扫描后有变更的文档进行扫描。

模块配置根据预置的策略等功能，对敏感文档做加密/隔离/内嵌水印管控处理；同时支持记录扫描日志、上传附件，以便于事后审计。

在增量扫描模式支持的基础上，配置设置为单次任务扫描模式等功能，单次任务扫描模式主要是以检查的模式统计敏感数据资产信息在组织内部不同终端、不同用户的分布情况，并支持纵向的检查对比。控制台下发一次策略终端对应执行一遍全盘扫描任务，并根据进度上报终端本次全盘扫描任务的统计结果到服务器；控制台支持展示任务的进度与结果统计数据信息。协助客户摸底掌握组织内部敏感数据资产的分布（终端、等级、用户），并为后续的管控奠定基础。

2)外发途径扫描

系统配置对通过网络途径如邮件smtp协议、FTP协议、HTTP/HTTPS、SMB、蓝牙协议、第三方应用程序（IM类、网盘类）进行外发的过程等功能，以及通过硬件外发文件的途径如拷贝文件到移动存储设备，打印文件的过程进行文档内容扫描，并根据扫描命中的结果和严重性等级动态的确定管控方式是允许放行、内嵌水印外发、加密外发或者禁止阻断。

3)明文外发功能

在对应外发通过管控方式为固定文件加密的前提下，明文外发功能为终端用户提供了一条便捷通道。配置设置固定的登记/审批控制等功能，或者根据文件内容扫描的文档敏感程度动态实现登记后直接明文外发、审批通过后直接明文外发或者拒绝明文外发的控制。

4)预置标签外发管控

在各外发通道对文件进行扫描外发管控时，产品会首先检测待发文档中是否包含全盘智能扫描策略中添加的数字水印标签，如果有的话直接按照此预置标签中的级别信息进行对应的管控，减少在外发过程中实时扫描的业务耗时，提升用户使用体验的同时保持相同级别的安全管控措施。

5)终端证据文件流转审计

在原有针对终端用户操作审计日志的基础上，增加了以证据文件为核心维度的日志展示与分析功能。配置展示所有证据文件相关的日志记录等功能，并针对记录了文件流转ID文档支持展示其来源和外发目的对象的分析图示。

6)支持文档规则类型

关键字：根据预先定义的敏感数据关键字，扫描待检测数据，通过是否被命中来判断是否属于敏感数据；

正则表达式：由于有些识别特征无法以关键字来表示，如身份证、银行卡号等，需要通过正则表达式来定义敏感数据识别特征，并根据这个特征是否命中来判断数据是否属于敏感数据；

数据字典：配置对应的关键词组等功能，并支持设置其中每个关键词的权重分值，在策略中设置命中达到指定分数阈值时判定为命中并进行后续的处理；

隐写文件：配置对特殊文件格式后通过命令拼接的文件进行识别等功能，如JPG/JPEG等特殊图片格式；

文档属性：配置根据文件格式、文件大小、文件名称、文件所有者、文件创建时间/最后修改时间等属性对文档进行分类管控等功能；

文档分类特征：利用自然语言处理和机器学习技术对组织文档进行智能分级分类，对分级分类后的文档进行深度内容分析后，提取文档分类特征；

文档指纹：基于内容的文档指纹，不受文档格式、文档编码，文档类型的影响；利用局部敏感哈希，文档局部更改，在相似度差别容许范围内，文档指纹不变；文档相似度阈值调整可容许文档的改变范围；适合内容复制、嵌入广告或文档少量修改。

7)支持解析格式类型

针对文档内容识别的功能支持主流数据格式，支持简繁体识别。系统采用模块化架构设计，预置支持多种格式的解码和转换引擎，可以在数据抓取时自动识别文件格式，并转化成可理解的文本，然后送入自然语言处理模块进行分析和归类。预置格式分析模块组能解读以下常见数据格式：

Microsoft Word/Excel/PowerPoint、Openoffice、WPS等办公文档；

ZIP、ISO、RAR、gz、tar、EML等压缩文件；

JPG、JPEG、PNG、BMP、TIFF图片文件

PDF等电子出版格式；

其它以文本形式存储的格式。

针对文档属性识别的功能在支持上述格式的基础上，还支持识别以下格式：

Wav、mp3、mid、ogg、mp4a、wma等音频类格式；

Mp4、avi、flv、mp4、mpg、mpeg、mov、mkv等视频类格式；

Dwg、dws、dxf、dwt、dwf、ics、pcb、brd、max、mdb、gdb、shp、mxd、sbn等制图类格式；

Vb、c、java、jsp、go、python、sh等代码类格式；

系统控制台支持查看扫描文档所包含的敏感快照信息，并支持高亮展示。

8)文档接收扫描

针对通过浏览器访问网页下载文件，从局域网共享目录下载文件到终端本地的行为进行监测，对文件内容进行扫描，根据命中的敏感级别进行放行下载、加密下载、内嵌水印下载、禁止下载的管控。

（6）终端行为管理

1）显示水印

系统配置在Windows终端系统和国产化终端系统中展示屏幕水印等功能。屏幕水印是指终端电脑启动后在电脑桌面最顶层展示水印；显示水印的内容支持文字、二维码和图片三种。支持配置水印内容包括的信息和自定义信息，支持配置文字的字体类型，颜色、位置、间距信息等。支持同时生效文字和图片水印的叠加显示满足项目定制化的需求。

系统配置在windows终端系统上打开的文档窗口文字区域展示水印内容等功能，文档水印的内容会随着进程窗口的放大、缩小、隐藏等变化而随动展示。

系统配置在屏幕水印和文档水印类型中等功能，配置添加隐形水印。在显示隐形水印的终端上用户无法观察到水印内容，但是通过专门工具可以查看其中的水印信息，主要包括用户名、IP/MAC地址、时间信息等。

2）进程管控

管理员可通过设置进程管控策略，对终端进程进行启动/停止/网络访问（配置的范围主要是IP地址和端口信息，配置设置允许访问网络范围/禁止访问网络范围两种方式）/截屏的权限进行管控等功能，并记录对应的审计日志。

3）外设管控

管理员可通过设置外设管控策略，以实现对终端常见类型外设的禁用控制功能。配置管控的外设类型包括：

Windows平台下：通用串行控制器、网络适配器、DVD/CDROM驱动器、磁盘驱动器、蓝牙设备、PCMCIA卡、智能卡读卡器、指纹设备、便携设备、图像设备、SD控制器。

国产化平台下：移动U盘存储设备、手机MTP设备、无线网卡设备、蓝牙设备、刻录机设备（CD/DVD）、打印机设备。

另外，对于非常用外设，可通过在系统外部设备资源库配置中定义设备关键字（设备类型或驱动）来对外设进行禁止管控功能。

4）非法外联管控

对于内网隔离的终端环境，本系统配置定时检测终端是否可以通过非法途径连接到互联网上等功能，配置设置检测的频率等功能，并配置告警与自动断网、关机处理等功能。

5）异常行为管控

系统配置自动检测终端用户在一定时间段阈值内触发的文件打印、内容截屏与密文打开的操作次数等功能，并根据设置的阈值次数自动对终端用户指定类型的行为进行锁定；并配置自动解锁管理等功能。

对终端敏感数据缓慢泄漏行为、外发加密码文件、压缩超限文件、嵌套超限文件、分片压缩文件或者隐写文件的行为进行监测与阻断，支持监测指定的终端外发通道与敏感信息命中的文档规则类型。并支持触发了阈值次数后可以自动对外发通道进行锁定与超时自动解锁的管控。

对终端用户的异常行为上报告警事件到控制台，管理员可以查看告警事件的对应信息并进行闭环管理。

6）文档操作审计：

系统配置对PC终端本地硬盘和移动存储U盘内明文文件的新建（打开）、删除、移动、复制、重命名、文件内容拷贝操作类型进行审计等功能。

配置终端用户手动打开标记数字隐形标签文件的明文文档进行敏感级别冒泡提示等功能，配置终端用户手动打开密文文件进行对应的密级的冒泡提示等功能。

（7）文档审批

用户在执行业务操作时，根据需要可以调用文档审批系统来执行审批流程，系统具有配置灵活、可执行、可跟踪等特点。

文档审批配置的审批模式包括单人审批模式、会签模式、审批优先级模式等功能，支持申请人手动取消审批申请。支持的审批类型包括文档提权审批、文档外发审批、虚拟安全桌面之间的文件共享审批等。审批者根据实际情况，可以手动执行审批，同时系统支持审批者设置自动审批模式以及委托他人审批模式。

**（二）网络安全服务**

建设单位以8项重点任务推进网络安全系统工程建设，构建适应余姚市电子政务外网的网络安全保障体系，其中已完成建设的包括任务一、任务七和任务八，分别是优化基础安全防护能力、深度融合实战化安全运行与评价服务、优化数字化业务的安全管理机制。本次项目需要建设的任务包括推进数字化终端统一安全防控、建设平战结合的安全监测与运营指挥中心。

本项目通过购买服务的方式，建立余姚市电子政务外网网络安全防控能力，服务购置期限为三年。

网络安全服务购置主要包括包含网络安全管理平台、网络安全运行平台和网络安全配套等服务的购置。

其中网络安全管理平台和网络安全运行平台可实现交叉验证，确保网络安全的隐患排查和事件处置不会出现遗漏，保障余姚市电子政务外网的安全运行。

**1.网络安全管理平台**

（1）系统架构



系统架构分为监管对象层、采集层、数据中台层、分析引擎层、应用层以及安全运营保障和标准规范保障。其中具体内容如下：

监管对象层：主要监管内容为余姚市级政务外网、余姚市级政务终端。

采集层：通过具体的采集器对各类数据进行采集，包括政务外网终端数据采集，政务外网出口网络采集，数据中心流量采集，余姚市节点设备日志、漏洞、单位基础数据采集、外部情报数据。

数据中台层：基于采集的数据，形成采集、管理、开发和服务等业务，能够对数据进行开发利用，能够对第三方提供服务。

分析引擎层：对数据进行计算，找出异常的数据，分析引擎包括关联引擎、行为引擎、专项引擎、交互式分析引擎、流式计算引擎等。

应用层：包括资产中心、威胁中心、分析引擎、分析中心、情报中心、工作指挥、报告中心、考核评估和态势感知。

安全运营保障：平台使用的基础，建立有组织的安全运营保障体系，能够安全监管平台的使用效果。

标准规范保障：在平台的对接过程中需要对数据采集、事件上报、通报下发、数据上报等信息进行规范，以保障数据、流程的标准化、规范化。

（2）信息流转



电子政务外网出口和数据中心通过部署流量采集器和标准接口对接获取流量数据，余姚市节点数据通过标准数据规范接口与市级监管平台对接。数据采集完成后进入数据中台，进行数据的存储、计算，通过数据开发和服务向外提供数据；安全事件通过分析引擎中的规则形成安全监测事件，事件通过研判分析，确认后进行通报预警，此时需要调用监管对象数据，确认通报预警对象；县级监管平台也会根据安全监测、研判分析的积累，形成内生的威胁情报和漏洞情报进行信息共享。

（3）监管对象

监管对象主要包括电子政务外网、数据中心和政务终端等，搭建余姚市的监管平台，通过对其云、网、端的监管，发现网络安全事件、有害程序事件；管理节点设备、终端上的漏洞、风险；最终降低整个政务外网的风险。

（4）数据采集处理设计

1）架构设计

数据采集处理，分为数据采集、数据处理、数据存储、管理平台、监控平台等模块设计，为分析型应用提供多源大数据的采集、处理、存储、查询等基础能力。

数据采集、数据处理、数据存储三大环节依次运行，完成数据接入、并存储到系统。

数据采集是整个环节的最前端，完成多种不同类型、不同协议数据的采集封包，并发送到下一个环节。

数据处理模块完成格式化、富化等操作，将不同来源的数据归一化到业务需要的格式。

数据存储则完成数据最终的存储动作，控制数据的保存位置、形式，根据不同的业务需求，还可以将数据分发一份到流处理，让处理完的结果再进入存储。

管理平台和监控平台负责对整个采集、处理、存储过程的管理配置和运行监控。

2）技术能力

数据接入，配置流式、批量两种方式，主要用于数据采集中数据接入阶段的数据处理。数据接入统一使用Kafka作为数据总线进行数据的写入与消费。

存储方式，采用集群化分布式存储结构。

数据计算，实现对已经保存至大数据平台的数据计算功能。数据计算能够对所有已保存至本平台内数据进行计算，并且提供相应的计算调用接口，能够满足外部分析系统的调用。数据计算包含五个主要部分，分布式资源调度系统，批处理计算系统，流式计算系统，高性能计算系统，迭代计算系统。

数据分析，在大数据环境下，通过数据分析能够实现数据价值。组件管理提供众多的数据分析能力，通过这些数据分析能力，可以对下层数据进行分析挖掘工作，同时为上层分析应用提供可调用接口。

基础管理，主要提供组件管理模块的可视化交互管理功能，包括运维、监控、安全设置等。

智能化运维，自动监控大数据环境，根据数据量自动运维，计算合适的kafka\ES的分片参数，自动扩展，减少运维人员难度，提高系统性能。

（5）数据治理设计

1）架构设计

数据治理，做为安全能力基座的核心模块，实现多源异构安全数据的标准化融合落地、数据仓库管理、数据质量监测、数据治理管理等。

2）技术能力

通用安全数据标准制定，包括但不限于：各类设备原始日志、告警数据、脆弱性数据。

所有公共元数据在线管理，信息分类编码、业务元数据、数据检测规则等元数据统一管理。

建设安全数据仓库，并提供一切数仓管理使用能力支撑，包括但不限于详情监控、质量监测、数据查询接口等。

将安全数据接入并标准化，通过可靠信道推送至本地。

接入各类数据，进行解密、解析，写入数据仓库并通过Kafka通知各数据订阅方。

（6）数据存储设计

1）架构设计

数据存储设计对海量数据进行存储、计算、查询和分析。提供海量数据的数据存储、实时流数据处理与离线批数据处理、高性能的检索与统计分析能力。

提供数据的多副本高可用、服务的高可靠与故障容错恢复能力。

提供大规模集群的自动化安装部署、扩容、监控告警、服务管理、节点管理、平滑升级等能力。

技术能力

2）提供多种标准协议接口，便于应用系统的开发，便于第三方系统的对接；

服务安全：可通过防火墙策略，对主机和端口进行安全加固；

准入认证：支持使用ldap和kerberos进行认证；

访问控制：实现用户组、用户、角色、权限的细粒度管控；

单节点故障不影响整体平台的服务运行；

Kafka/ES /HDFS等组件支持数据；

多副本存储，保证数据高可用；

支持单节点不低于2万EPS的写入；

百亿级数据检索分钟级响应；

自动化安装部署，系统线性增加服务器数量即可实现存储空间动态扩容；

实时监控硬件与服务，异常情况可及时排查。

（7）资产中心

1）整体架构



资产中心提供通用的资产运营和管理的能力。主要功能包括，资产概况、资产发现、资产管理、资产运营、资产脆弱性管理、资产漏洞库管理、资产风险评估管理、拓扑管理、资产检索等功能。

2）资产概况

资产概况展示安全运营大脑中资产数据的整体情况，并从不同维度对资产进行分析和统计，包括资产数据的概要统计（数据总量、分类别的数据量统计），以及分类统计图表，分别统计展示发现资产（发现资产中的操作系统分布、软件类型分布、使用的协议分布、端口分布、应用TOP10分布、发现源趋势、发现设备资产分布）、单位统计（单位地区分布、行业分布、类型分布）、设备信息统计（设备资产类型、设备使用操作系统分布）、软件信息统计（软件类型分布、软件使用的协议统计、软件使用的端口统计、软件应用统计）以及资产重要程度统计（重点资产等保备案占比、关基资产等保备案占比）。

通过BI分析工具形成资产相关维度的图表，形成资产管理分析仪表盘，对资产模型进行整体宏观分析，包括资产的发现情况、资产运营情况、资产管理维护情况。

通过多维度（重要程度、资产总量，资产发现总量），多状态（已运营、待运营、已归档、未归档）、多类型（系统、软件、设备、ip）进行整体数量情况展示。

根据资产的协议和端口分类展示总量饼分析排名，并且根据资产类型（操作系统与应用），提供各分类以及端口、协议的top10进行柱状图的数据分析展示。

按照资产的类型（软件、设备），以及资产的重要程度（重点资产与关基资产），用环形图的方式展现总量和其分布占比。

根据资产的单位所属的地区、行业、类型进行分布展示，支持环形图与块图的方式。

3）资产发现

配置将不同方式（流量探测、资产探查）所汇报的资产进行统一的管理等功能，并且配置人工导入未运营资产等功能，以软件资产和设备资产两种类型进行分类展示，并且可以选择具体细分类型进行展示（如网站、数据库软件等）。

资产发现子模块分为资产发现、发现配置、资产扫描、服务发现、快速扫描五个部分，资产发现页主要展示各个发现源发现的资产（软件、硬件）；发现配置页用于对发现源进行配置；资产扫描可结合资产探测引擎，扫描网络中的存活主机；服务发现可结合资产探测引擎，扫描目的主机上开放的服务；快速扫描支持快速发起扫描任务，结合资产探测引擎可进行存活主机、开放服务的扫描，结合漏洞扫描引擎可进行目标主机的漏洞扫描并导入扫描结果。

资产发现通过与资产扫描器的对接，进行扫描任务的创建，然后对对资产扫描器结果进行解析后发送至源数据管理平台进行数据的清洗、归一化处理，最后形成资产发现库。

4）资产检索

资源管理子系统为资产检索提供一键检索功能，配置关键字检索和全文检索，提供搜索历史查阅功能，便于用户操作使用。

配置多维度（单位名称、资产名称、资产类别、ip、操作系统、域名、端口、协议等）的模糊与精准数据查询等功能，并且可以多个关键词一起搜索，查询不同状态下的实体，包括：资产发现、已核实（资产管理）等状态，以实体的形式进行结果呈现。

一键搜索提供资产数据综合查询功能，支持输入检索条件进行查询，使用特定的语法能够获得更加精确的查询结果；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，只要满足检索条件，都能查看到相应的实体及详情。

搜索框，支持多个关键词用空格隔开，每次搜索多个关键词，点击搜索后同时搜索历史展示当前用户搜索的最近的多个关键词。

搜索历史，可以删除历史关键词，也可点击垃圾桶删除全部。

搜索展示内容，分为设备、网站/系统、软件3个维度展示列表点击列表后跳转至相应的管理功能中。

5）资产管理

系统提供对资产按照不同类型的实体进行管理和维护，用户可通过对不同功能界面进行操作，实现不同类型资产的管理，管理包括新增、编辑、删除、导入、建立关联关系等操作。

可以按照不同的维度对资产进行分类统计。平台提供资产的清单，包括：设备、网段、域名和网站等，支持查看资产信息的详细属性，对资产进行编辑、新增和删除。

除去资产的基本属性（名称、IP、地理位置、责任人、资产价值）外，还应当包括资产的组件（组件是构成资产的最小软件单元。例如：Web服务器上常用的Linux、Windows、IIS、Apache等组件）、组件状态（各组件对外提供服务的端口号、协议类型等）、资产弱点（脆弱性、暴露程度等）等安全属性。

6）资产运营

资产运营提供两种资产运营模式，自动运营和手工运营，自动运营是系统根据预置好的规则自动将原始发现资产通过运营规则进入资产纳管库，系统自动解决运营中的冲突处理，人工运营是指在运营过程中，对于冲突数据，需要人工进行确认处理后进入资产纳管库中。功能包括：规则管理、资产归属管理、发现资产审核；

规则管理是包括归属规则、运营规则、忽略规则，其中归属规则描述的是目前资产的单位匹配规则、运营规则描述的是资产运营中资产冲突的处理逻辑、忽略规则描述的是对不关注的资产进行忽略处理规则逻辑；

归属管理提供对无主资产或者有单位冲突资产的统一管理，在该功能下可以进行单位的设置和资产详情的跳转；

发现资产审核提供人工审核冲突资产的功能，在该功能下可手动处理冲突资产并进行纳管和忽略操作，发现资产根据发现资产与已纳管资产的对比，区分是更新资产数据或新增资产数据；

在资产运营管理中，可对运营规则进行修改编辑、对冲突资产进行人工审核等操作。

7）资产脆弱性管理

通过关联已纳管的资产数据与漏洞告警数据生成资产脆弱性数据，借之实现对资产脆弱性的管理。支持纳管资产和漏洞告警数据的关联。

资产脆弱性：配置通过漏洞视角查看受影响的资产情况等功能，配置对资产漏洞告警的修复状态提示和设置等功能，支持对各资产漏洞告警次数的统计；支持通过资产视角查看资产的漏洞告警情况，支持在纳管资产和漏洞告警数据的关联后，对资产详情和漏洞告警详情的查看。

资产潜在漏洞：通过关联纳管的资产数据与漏洞知识库生成资产潜在漏洞数据，实现对资产潜在漏洞情况的管理。系统配置纳管资产和漏洞知识库数据的关联等功能，支持通过资产视角查看资产的潜在漏洞情况，支持对纳管资产和漏洞知识库数据的关联后，对资产详情和漏洞知识库详情的查看。

8）资产漏洞库管理

资产漏洞库管理模块提供漏洞知识库的管理功能，包括公共漏洞库和我的漏洞库。公共漏洞库提供了的漏洞列表查看查询功能。

我的漏洞库为用户提供对自身维护的漏洞知识库的管理功能，配置对接入漏洞知识库数据的查看和统计等功能。支持对接入漏洞知识库数据与已纳管资产的管理、支持对接入漏洞知识库数据漏洞影响面的评估，支持对人工维护漏洞知识库的管理，支持对人工维护的漏洞知识库的新增、修改、删除、查看等基础管理功能。同时支持对人工维护的漏洞知识库数据的查看和统计、支持对人工维护的漏洞知识库数据与已纳管资产的管理，及支持对人工维护的漏洞知识库数据漏洞影响面的评估。

9）资产风险评估管理

资产风险评估管理，主要是对风险的组成要素进行识别、汇总和评估，确定组织面临的风险的大小，并对风险进行评价，以选择适当、合理的安全处置方法和安全措施进行风险控制。资产风险评估贯穿了信息安全风险评估的设计、实施、检查、改进等整个周期，覆盖了组织、人员、技术、管理等各个方面。而信息安全风险评估在信息安全建设过程中是非常重要的，它是该过程的起点和基础，是信息安全管理持续完善、改进的推动和指引，是信息安全管理绩效的衡量及工作考核的方法和手段。其目的是全面、系统的分析客户业务所面临的信息安全风险，以采取有效措施进行风险处置和应对，提升信息安全保障能力。

风险概况：风险概况统计信息，包括针对资产风险、网络区域风险、单位组织风险、业务系统风险评分排名、并显示风险评分，并可查看风险计算详情等。

风险评级：根据资产风险评估模型计算出具体资产（设备/系统/网站）的风险总体情况，及风险相关数据分析。并据此计算出资产风险等级，从而分级显示资产风险相关信息，具体包括资产的类型、基本信息以及资产价值、重要性等。

风险模型管理：提供资产价值分级评价模型配置功能，权重包括资产的保密性、完整性、可用性以及业务相关性等。

提供资产威胁等级模型配置功能，权重包括资产涉及的安全事件、脆弱性出现频率等。

配置资产风险等级模型配置功能，权重包括资产价值、威胁、脆弱性三个基本要素进行资产的风险计算。

10）拓扑管理

通过流量、网络设备日志进行网络资产关系分析，形成拓扑图，并在拓扑图上体现资产的风险相关信息。

拓扑引擎通过网络流量的五元组数据、以及结合网络这边日志中的路由关系，分析出网络资产之间的逻辑关系与业务访问关系，并结合资产库将拓扑节点与资产进行绑定，形成基础拓扑图，然后经过运营人员的细化完善，最终形成重点网络资产的逻辑拓扑关系图与重点系统的业务关系图，并结合脆弱性告警库、网络告警库、风险评估结果在拓扑节点上直观的展示每个节点安全状况。

（8）威胁中心

威胁中心主要提供告警管理和安全事件管理两大功能。

告警管理配置安服人员或业务人员对接入平台数据源生成的告警进行管理等功能，支持安服人员或业务人员对归并后的告警做进一步研判。实现对网络安全情况的实时监测，及时发现国际敌对势力、黑客组织等不法分子的攻击活动、攻击手段和攻击目标，全面监测重保单位信息系统和网络，实现对安全漏洞、威胁隐患、高级威胁攻击的发现和识别，并为通报预警和侦查调查等业务系统提供强有力的数据支撑。

安全事件管理支持安服人员或业务人员对系统自动生成的事件或人工录入的事件进行管理操作。识别重点网络安全事件并依据研判结论决定后续业务流转，并启动相应的处置动作。在告警管理中提供转事件、转处置等业务快速入口，并可通过自动处置策略进行对高可信告警进行自动处置。

1）告警概览

对告警整体情况进行概要性的统计展示，包括告警分类、告警趋势、告警排名、告警同比/环比分析等，支持按照时间范围筛选，按照危急程度分类统计等。

2）告警管理

告警管理向安服人员或业务人员提供了对接入平台的数据源生成的告警进行管理，支持安服人员或业务人员对归并后的告警进行进一步研判。

告警管理展示告警的详细信息。系统能够根据自定义的时间范围，和不同的字段对告警进行查询，用户还可根据实际业务需求，进行告警编辑、导入导出、自定义表头和手动输入告警的操作功能。

告警查询：系统能够根据选择的相关字段以及告警事件级别进行告警数据查询。查询条件支持历史保存，查询字段包括但不限于时间、等级、一级（或二级）分类、单位、行业、告警简介、受影响资源、威胁源、数据源、区域和通报状态等内容，其中部分字段（告警简介、受影响资源、标签、威胁源）支持模糊查询。查询后，根据自定义的表头字段展示相应的内容，用户可对单条告警信息进行详情查看和人工编辑。

告警编辑：告警编辑功能实现对告警的状态批量的进行人工确认，和标签编辑管理。导出功能，支持以Excel格式导出搜索返回的告警，内容包含所有告警字段。导入功能可以通过模板填报来人工导入告警数据。

3）安全事件管理

安全事件管理向安服人员或业务人员提供了系统自动生成的事件或者人工手动录入的事件，并支持对其进行管理操作。

通过事件研判模块评估研判后的事件，以列表的形式在事件管理模块进行展示。同时可以对海量的事件进行归并，提炼更高的业务价值。

配置事件检索功能，内置快捷检索和高级模式；支持事件转通报。

通报管理：配置通报全流程管理功能。

4）事件研判

配置按照所需的过滤条件进行综合筛选等功能，得出目标事件，并对事件做进一步研判，适时触发应急响应动作。

5）主动防护配置

主动防护配置，可以配置综合的触发条件，打开主动防护开关，并在其被触发后，自动封禁安全事件中的威胁IP。

配置灵活配置消息中心邮件告警、短信告警等多种告警方式等功能，满足用户多种场景告警需求。

（9）分析引擎

分析引擎是对各种类型的分析规则、分析策略、分析模板进行综合管理，包含对这些规则、策略、模板下发生效后的运行管理，以及对同这些因素相匹配的支撑资源进行管理调配。

分析引擎管理采用多层次的安全事件分析技术，内置多种安全分析规则模型，可通过界面化的安全规则模型定义方式，支持逻辑关系、大小判断、字段匹配、频率统计、通配符、黑白名单等多种设置算法。可结合用户实际的运营场景需求，帮助用户实现基于规则算法和参数条件的规则自定义。主要分为规则管理、策略管理、运行管理和资源管理。

1）规则管理

规则管理模块，能针对系统网络安全分析规则，提供新建、编辑、复制、删除、批量删除、批量下发等功能，并能够对系统用户提供编辑后的规则导入功能，和选中的规则导出功能。

系统预置基于网络安全设备日志、原始流量分析的200多种“开箱即用”的告警分析规则，包括但不限于：有害程序、攻击利用、安全隐患、可用性、内容安全、拒绝服务、异常活动、信息破坏、信息收集等告警类型。

2）策略管理

策略管理，是对告警生成和告警归并两个阶段的告警规则，做统一的策略约束与维护管理。对在一定时间窗口内的日志匹配、规则识别生成告警的动作过程，可以令其使用同类的规则模板，从而大大减少了模板数量。告警归并则是对多起告警（相同特征的一类告警）归并为一条，减少告警数量，提高告警分析效率。

策略管理包含告警生成策略模板、告警归并策略模板、后置配置模板管理。

系统配置告警生成策略模板的新增、修改、删除、启用、停用、查看等功能。对于一些特定字段能够自定义设置告警生成策略。此外还配置告警生成模板的导入和导出等功能，提升规则配置效率。

配置告警归并策略模板的新增、修改、删除、启用、停用、查看等功能。对于一些特定字段能够自定义设置告警归并策略。配置告警归并模板的导入和导出等功能，提升规则配置效率。

配置后置配置模板的配置添加和管理等功能，包括配置的名称、说明、响应配置、响应动作、设置全局生效或无效等。

3）运行管理

运行管理，配置对规则运行情况进行监控等功能，支持对运行占用资源数量进行监控，并且支持对告警信息明细进行查询（产生告警），以及对任务资源占用情况的统计等。

主要包含任务仪表盘、告警仪表盘、实时占用资源图表以及任务列表。其中任务列表可对任务进行查询、启动、停止、删除、查看等操作。

配置对发布规则的启动、停止、删除等操作。

配置对基于规则的CPU利用率、内存占用等计算资源的消耗监控。

配置实时查看规则\模型的运行状态，包括任务数量分类统计（总数、运行中、运行失败、运行结束），命中告警数量统计（归并前、归并后）等内容。

4）资源管理

资源管理的主要功能，包括资源的新增、编辑、删除、查看、复制、导入/导出等。其中，当前资源管理中包含的资源为IP地址资源、端口资源、时间资源、字符串资源和表资源。

对象资源，是命中规则过滤条件所引用的数据，对其进行统一管理从而形成的相应数据对象，其可被命中规则条件过滤。用户可以对多处引用的对象资源进行统一的维护，避免在命中规则环境重复编辑定义自定义字段或数据，减少人工干预的频次，一次设置可多次引用。

资源管理包括对IP地址资源、端口资源、时间资源、字符串资源、表资源等资源进行管理。IP类型对象资源可以记录特殊的IP地址列表，端口类型对象资源可以记录特殊的端口列表，时间类型对象资源可以记录工作时间、登录时间等，字符串类型对象资源可以记录URL、域名列表，表资源可以配置表字段，生存时间，最多资源数等内容。

针对黑白名单等场景，配置定义各类静态资源等功能，在流式分析或离线分析的过程中，引用相关资源定义进行规则模型构建。

配置新增、删除、修改自定义对象资源等功能，包括IP地址、端口、时间、字符串，可与日志数据进行关联分析时引用；支持写入对象资源，如源IP、目的IP；

系统配置过滤器的新增、删除、修改、查看等功能，并支持过滤器的导入和导出，具体如下图所示。

（10）分析中心

分析中心主要包括关联分析、攻击链分析等分析手段，输出源IP大网行为、源IP攻击特征、攻击IP同源分析等分析结果，输出安全分析的概况及具体安全事件信息，支撑起系统的告警和事件分析。

1）关联分析

关联分析通过分析流量中的行为，结合开源情报信息，挖掘网络安全事件背后的攻击者。利用流量日志、安全事件、PCAP包等信息，结合开源威胁情报（包括但不仅限于恶意域名、IP、恶意软件、设备指纹、攻击者\组织）以及网络攻防知识库，基于本体论的思想，从网络空间人、地、物、事、组织的角度，提取关键实体（攻击事件、攻击方法、IP、域名、设备、文件、地址、邮箱、电话...），并构建实体之间的关系网络，通过攻击者同源、IP通联、虚实映射等分析方法，结合布控等手段，找出重点网络安全事件后面隐藏的真实攻击者，定位其位置、身份、意图，形成攻击者\组织。

分析任务创建：点击添加任务，弹出窗口对分析任务进行创建。包括任务名称、任务标签、任务描述与任务分组。其中任务名称不能为空且不能与现有任务重名。

 任务分析-单线索拓线：实体节点右键选择“数据源”类的查询，在用户所选择的数据源范围中对与该节点有关系的ip进行查询。如图所示，用户可选择并配置数据源。其中，对于端口类型的节点进行“数据源”类查询时，得到的结果为与当前ip的当前端口有联系的ip。

 数据查询：对外接口提供告警，事件等流量日志的查询能力。形成查询结果，查询结果支持拖拽，根据不同的实体类型在画布中显示对应的图例和统计。

 经验模型拓线：模型拓线只支持IP实体类型进行查询。

 “IP通联关系模型”将筛选与当前ip之间有联系（TCP连接）的ip，用户可以配置想要查询的通联ip之间使用的端口和协议（默认80端口和http协议）。

 “IP资产模型”将查询当前ip所属的行业、单位、运营商、位置、开放的端口等资产信息。

 “攻击者画像模型”将查询当前ip背后的攻击者，具体的攻击者画像信息可通过单击画布上的攻击者节点来查询节点的详细信息。

2）攻击链分析

攻击链分析基于洛克希德·马丁定义的“网络杀伤链”，来进行网络攻击全生命周期的分析，从侦查跟踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成目标七个攻击阶段，对攻击手法以攻击链的形式进行可视化呈现。

在系统的攻击链分析过程中，系统支持以时间轴的形式展示攻击过程，呈现攻击过程中分析出的相关结果，展示内容包括：首次发现时间、最近发生时间、威胁名称、受害IP、攻击IP、威胁级别、确信度、攻击结果和分析结果。

任务管理：对攻击链分析的任务进行管理，可以创建、编辑、重启、查看、删除分析任务。任务列表页面可以按任务名称，状态，攻击者名称，攻击者ip,受害者IP等条件进行任务精确和模糊查询。任务列表展示任务序号，创建时间，任务名称，创建者，攻击者名称，攻击者IP,受害者IP，任务描述，状态，分析消耗时长和操作列。

任务创建：选择创建自定义分析任务，包括任务名称，攻击者IP,受害者IP为必填项，攻击者名称,起止时间，告警发生时间和任务描述非必填。任务名称有重复名称校验，攻击者IP和受害者IP支持多个IP，告警发生时间默认为当前系统时间，起止时间开始时间为告警发生时间-7天，结束时间为告警发生时间。

选择创建系统告警分析任务，在该页面默认展示近7天所有可进行攻击链分析的任务的告警，默认按告警发生时间倒序排序展示，可以对单条告警或多条告警进行批量分析。支持通过告警发生时间，攻击者IP,受害者IP，告警一级分类，告警二级分类，攻击结果代码，危害等级等条件进行过滤出系统告警，然后在对过滤出的结果进行分析，支持对告警发生时间，攻击者IP,受害者IP,攻击结果代码和危害等级升序/降序排序。

 任务编辑：在任务列表中选择任务，并选择“编辑”，对该项调查任务进行编辑。在编辑成功状态的分析任务时，修改ip或时间任意内容时，鼠标点击ip和时间条件时，提示"修改攻击者IP、受害者IP或起止时间任意一条件保存任务时，会清除该任务的历史分析结果，请慎重操作!"。新建创建的分析任务，处置未执行状态。以下是任务状态对应的操作项。

分析结果：对攻击链分析的任务进行管理，可以创建、编辑、重启、查看、删除分析任务。任务列表页面可以按任务名称，状态，攻击者名称，攻击者ip,受害者IP等条件进行任务精确和模糊查询，。任务列表展示任务序号，创建时间，任务名称，创建者，攻击者名称，攻击者IP,受害者IP，任务描述，状态，分析消耗时长和操作列。以图形的形式展示攻击者的攻击过程，分析人员可以很直观的看出攻击者的攻击路径，使用了哪些攻击手段，以及当前处于哪个攻击链阶段。每个攻击链阶段球颜色从侦察跟踪到达成目标渐变展示。并且从阶段模式，时间模式和关系模式三个维度来具体分析攻击过程。

（11）情报中心

情报中心配置对情报信息的采集、录入、标定、存储、检索、分析、关联、挖掘、应用、展示等功能，并可进一步向有关监管单位推送情报信息。本系统所含情报信息，可供安全分析人员检索分析，并能和系统其它模块进行内部业务联动，为平台挖掘深层次线索或对线索进行追踪溯源，提供数据支撑。

情报中心汇聚多方来源的威胁情报，并对这些情报进行统一的维护和管理。情报中心主要包括情报查询、情报管理、威胁资源库、情报升级管理等功能。

1）情报查询

情报总览：在情报总览查询页面中，顶部展示内容为威胁情报总数、云端威胁情报数及版本号、本地威胁情报数及生效情报数进行查看。

威胁情报总数：本地威胁情报数量+云端威胁情报数据。

云端威胁情报数：来源于威胁情报中心提供的活跃威胁情报数。

本地情报数据：本地运营创建的威胁情报数量。

在情报搜索部分，配置按照全部情报和本地情报两个搜索范畴进行情报信息的搜索等功能。其中，全部情况搜索范畴，配置按照IP、DOMAIN、 URL、MD5、SHA1、SHA256、情报名称等条件进行搜索等功能；本地情报搜索范畴，支持按照创建时间、风险等级、情报置信度、情报状态、情报名称、检测指标等条件进行搜索。

用户只需要输入关键词，立刻能检索到符合条件的情报信息和失陷主机情况，其查询结果按照第三方威胁情报和本地情报进行分类展示。

2）情报管理

本地情报：可以对最近创建或导入的情报信息进行查看，支持对情报进行检索、创建、编辑、删除、启用、停用、导入、导出等操作。

情报检索：在本地情报管理页面顶部为情报检索区域，支持按照情报创建时间、威胁类型、风险等级、置信度、状态、情报名称进行单条件检索或组合检索。在本地情报管理页面列表中通过详情按钮，页面跳转到情报详情页面。

指示器：指示器模块作为平台情报的知识库模块，提供威胁关联分析适用的IOC基础信息的维护。用户可以自行从指示器模式类型、攻击链阶段、生效日期、失效日期等维度创建并维护指示器信息。

3）威胁资源库

攻击者信息库：攻击者信息库配置进行攻击者信息填报和分类查看等功能，攻击者和攻击组织信息均以列表化进行管理，可以对最近创建或导入的攻击者信息进行查看，配置对攻击者进行检索、创建、编辑、删除等操作等功能。在攻击者管理页面顶部为情报检索区域，配置按照攻击者名称进行检索。录入检索指标，点击【搜索】按钮，在下方列表中展示搜索结果。

恶意软件库：恶意软件库包括各种病毒木马等，可根据恶意软件名称、类型、是否恶意家族、实现语言、处理器架构、第一次发现时间、最后出现时间、能力、标签、描述等字段进行手动新增，可按照时间和名称等进行模糊搜索。

4）升级管理

通过升级管理功能，可查看云端情报升级历史，并可对云端升级模式进行配置。

自动升级：在升级管理页面，开启自动升级功能，在联通外网的情况，会在每天0点、6点15分、12点30分、18点45分自动从云端获取最新的热点威胁情报。

手动升级：在升级管理页面，关闭自动升级功能，可以通过立即升级功能按需实时拉去最新的云端情报，在升级管理页面，通过手动升级，导入离线云端威胁情报升级包，即可进行离线升级。

（12）工作指挥

工作指挥提供日常通报、重大风险预警、重要活动保障、突发事件应急处置、流程管理等功能，实现与同级党政机关、事业单位、相关重点企业等协同处置网络安全事件的能力。

1）流程管理

流程管理模块，包括预案管理和工作方案管理两个子功能。

a.预案管理

预案管理可实现预案场景管理、个性化预案编排、预案流程管理，解决了传统纸质预案战时“用不上”的问题。平时，相关人员可根据不同场景制定不同等级的预案，在战时，可依据预案快速调配相关资源，实现平时向战时的迅速切换。由此，预案管理模块可针对网络安全突发事件应急处理等相关工作，支持执行流程编排配置、调阅管理等业务动作。

预案管理默认进入预案的统计页面，展示预案类型的统计和预案卡片列表及预案组分类统计信息。

预案统计信息，配置对当前预案总数以及不同类型预案的数量做统计等功能。还支持对整体预案状态的统计，包括待提交、待审核、已启用、已停用等状态。点击不同分类下的统计数字，对下面预案的卡片进行过滤显示。预案卡片支持分页，可进行标准的翻页，以及选择每页数量的操作。

预案卡片中展示预案的信息以及基本操作，包括编辑、复制、删除操作，并支持在此页面点击创建按钮进行预案的创建。

预案组分类统计，支持预案组的创建和配置，按照不同的预案组来分类展示每个预案组下的方案数量，并可点开具体查看。

b.工作方案管理

工作方案管理模块针对日常事件通报、重要活动保障等业务工作进行编排配置、调阅管理。默认进入工作方案的统计页面，展示工作方案的分类型统计和工作方案卡片列表及工作方案组分类统计信息。工作方案卡片中展示预案的信息以及基本操作，包括编辑、复制、删除操作，并支持在此页面点击创建按钮进行工作方案的创建。

工作方案统计信息，配置对当前工作方案总数以及不同类型工作方案的数量做统计等功能，具体的工作方案类型划分为“日常事件通报、重要活动保障”等。此外支持对整体工作方案状态的统计，包括待提交、待审核、已启用、已停用等状态。点击不同分类下的统计数字，对下面工作方案的卡片进行过滤显示。工作方案卡片支持分页，可进行标准的翻页，以及选择每页数量的操作。

工作方案组分类统计，配置工作方案组的创建和配置等功能，按照不同的工作方案组来分类展示每个工作方案组下的方案数量，并可点开具体查看。

2）重要活动保障

重要活动保障主要用于在重要会议或重大活动期间，加强网络安保人员调度，全方位全天候掌握活动相关的单位、系统和网站安全状况，重保单位网络安全情况的实时监测，以及重保任务的全生命周期管理，配置设定筹备阶段、临战阶段、决战阶段、战后总结等多个环节等功能，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，可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保障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。

a.重保工作管理

重保工作管理配置将平台中的重保工作通过卡片的形式进行展示等功能，可体现各个任务的基础信息及当前状态。支持通过工作名称、执行状态、工作类型、工作分级等条件对重保工作列表进行筛选过滤。

业务协同：单击【业务协同】，可在此页面收发重保任务指令，指令自动关联该重保任务。

事件风险：配置对网络安全事件、风险的针对性查询等功能。具体分为快捷模式和高级模式。快捷模式支持关键字的“胶囊式”查询；告警模式支持多种类的检索语句查询。通过网络安全风险事件的查询，可以获得目标性的网络安全事件、风险信息。

工作流程：图形化编排、展示重保工作引用预案的进展情况，其中每个节点依据执行情况进行标记，实现重保业务的全流程可视化记录。

b.值班值守

值班值守，配置选取不同的重保业务起止日期来添加业务阶段等功能。而且，设定值班值守的功能，支持指挥部值班安排、重保目标选择和重保目标值班安排等子功能。

c.会商研判

会商研判，配置添加记录重保活动期间的业务会商情况等功能，添加后以列表的形式展现，表头信息有会商主题、参会人员、会商形式、会商状态、会商时间、操作等。并且支持按照会商时间、会商主题、会商形式等进行筛选查询。

d.方案/报告

重要保障活动保障期间，需对各类相关报告进行报送，系统支持在线添加的方式，结果以列表形式展现。如果上传的报告是pdf格式，则支持报告直接预览。word可以通过转换为pdf格式后直接预览，其他格式不可直接预览，此情况下「预览」功能置灰。支持按照报告类型做统计，具体包括：工作方案、进展简报、进展详报、每日日报、综合报告、总结报告、调查分析报告、安全检查报告、事件处置报告等类型，相应统计每种类型下的报告数量，并做列表化展示。

e.指令创建快捷入口

指令创建，以下图蓝色圆底白色信封状快捷入口的形式，贯穿了重保工作管理的全部处理环节，点击后支持重保业务指令的创建、提交，以卡片的形式概要展示指令当前状态，包括审核中、进行中、已归档等。

3）突发事件应急处置

突发事件应急处置，通过可编排可执行的数字化应急预案和可机读的威胁情报，针对重大网络安全事件，实现对预警响应流程和应急响应流程的全方位支撑，支持对各类资源的统筹调度、情报共享、协同联动，提高在突发网络安全事件期间的应急响应能力。

a.应急处置工作管理

应急处置工作管理，通过卡片列表的形式展示当前系统中所有应急处置工作。应急处置工作管理展示的基本信息包括：工作名称、处置类型、启动响应时间、持续时间、当前状态、采用预案名称、标签。搜索条件包括工作名称、处置类型、当前状态、响应级别、标签等。

b.信息报送

信息报送配置相关单位在突发事件应急期间的信息上报等功能，可手动添加待通报的网络安全业务信息。上报列表内容包括标题、报送时间、状态、标签，相关操作包括详情、编辑和删除等。

c.报告报送

重要突发事件应急处置期间，对各类相关业务报告进行报送，系统配置在线添加的方式，结果以列表形式展现。如果上传的报告是pdf格式，支持报告直接预览。word可以通过转换为pdf格式后直接预览，其他格式不可直接预览，此时「预览」功能置灰。报告类型包括：工作方案、每日日报、综合报告、总结报告、事件处置报告等等。

d.应急装备报送

应急装备报送，配置展示应急处置过程中等功能，本单位和下级单位创建或提交的应急装备信息，支持应急装备的添加、搜索。

4）日常通报

日常通报将网络安全监测分析产生的网站漏洞、木马、僵尸网络、网站篡改、网站仿冒、网站挂马、暗链、APT攻击等安全事件数据，及手工导入的外部获取的安全事件，及时通报到相关的涉事单位，并协调涉事单位完成对网络安全隐患及网络安全事件的处置工作。通报流程要做到透明化，能对通报流程进行全程跟踪，涉事单位整改后予以反馈，再由运营人员验证确认，最终完成业务归档闭环。

a.通报处置工作管理

通报处置工作管理模块，以列表形式直观展示当前日常处置通报数量，进行中数量，待启动数量及已结束梳理，支持以事件列表及人工录入事件两种方式新建通报，支持对通报进行查询，处置等操作。同时列表状态栏展示每个通报当前执行情况，用户做到心中有数。

b.通报处置

通报处置功能，统计不同类型任务的通报列表，展示内容包括编号、标题、类型、状态、发送方、签收人、发送时间、任务名称和操作等，支持通过状态和类型两个维度进行统计，支持通过任务类型，任务名称，签收人等多个维度进行检索。

c.通报配置

通报配置模块配置从基本信息等功能，受害者信息，攻击者信息，攻击利用，举证信息等多个维度配置通报字段。

d.自动通报预警规则

自动通报预警规则，支持通过配置资产价值、事件级别、事件类型等条件，实现自动预警通报。其通报触发条件，包括资产价值条件和事件类型条件。此外，支持通报信息模板的创建；支持通报方式的选择；完成上述设置后，可以选择打开自动通报的开关，启动自动通报。

5）重大风险预警

a.预警工作管理

实现对于重大风险预警工作（例如，重大漏洞、重大安全隐患、重要攻击事件预警）的全流程任务调度和管理功能，风险预警工作流程需依次包含研判评估、预警整编呈报、预警指令下发、预警反馈和预警解除呈报等必要任务环节。

实际业务中，根据制定的重大风险预警工作完成相对应的工作流程，包括指令制定下发、指令审核、进度推进及报告、反馈回复、整体工作跟踪处理，实现重大风险预警业务工作的闭环。

b.预警响应处置

预警响应处置功能，统计不同类型预警列表，展示内容包括编号、标题、类型、状态、发送方、签收人、发送时间、任务名称和操作等，支持通过状态和类型两个维度进行统计，支持通过任务类型，任务名称，签收人等检索条件进行检索。

c.预警业务审核

重大风险预警通报必须经过严格的检查与审核，该模块展示当前已审核和待审核的重大风险预警通报任务，支持根据审核时间，工作名称，标签等检索条件进行检索。展示内容包括工作名称，状态，标签，风险等级，发送方，提交审核时间，审核处理时间等。

（13）报告中心

报告中心包括报告总览、报告管理、数据源管理、模板管理、组件管理等相关功能组成，可快速生成各类报告以支撑相关安全事件以及业务分析工作报告。

1）报告总览

报告总览支持对系统中生成的报告进行管理，以卡片形式呈现当前已配置的报告任务，整体上支持按照快速报告和周期报告做分类筛选；具体支持对其进行查询、预览、删除以及下载等工作。并以列表的形式对全部报告进行分组统计，支持按照不同分组对报告进行分类查看。

2）报告管理

a.快速报告

快速报告，是通过灵活的选取时间范围、快速生成所需要的报告，并提供了报告的增删改查操作。支持用户按需选择哪一份报告模板来生成相应报告，支持自定义所要统计报告内数据的时间范围等。

创建好的快速报告以列表的形式呈现在页面上，显示了快速报告的名称、创建人、开始时间、结束时间、创建时间和任务状态。其中开始时间和结束时间显示了该快速报告的统计时间区段。创建时间显示了该快速报告的创建（生成）时间。任务状态包含两种：等待和成功，是根据实际报告的生成状态来进行显示的。由于报告的生成时间是根据报告的内容多少成正比的，当报告的篇幅很多、统计的数据量非常大时，在2s内不能及时生成将会呈现生成中状态，在2s内如果报告生成完毕则是已生成的状态。无论报告的篇幅和数据有多大，报告的生成时间不会超过20s。

快速报告的下载和查看也与报告管理的方式相同，支持以Docx及PDF两种格式下载到用户本地，查看则是以Pdf的格式在网页上显示。

b.周期报告

周期报告，是可配置周期性的时间范围和生成时间用来生成报告，生成报告的调度类型有日、月、周。用户可以根据自己的需求来每天/每周/每月生成自己想要的报告。周期性的好处之一就是无需重复，仅一次配置就可每天/每周/每月固定时间得到生成的报告。

支持对查询数据量比较大的任务创建调度任务。包括任务的名字、使用的模版、报告生成周期等功能。可以对调度任务进行查询、删除、新增以及编辑等基本操作。

3）数据源管理

报告中心的数据源包括：数据连接和数据模型两部分，解决系统接入多元数据库的问题，给系统带来了数据选择的灵活性。

数据连接支持EXCEL、CSV、ElasticSearch、MySql、PostgreSQL等多种类型。

数据模型模块有常用的增、删、改、查等功能，新建数据模型前可以新建数据模型文件夹、再新建数据模型文件或直接新建数据模型文件，使得文件有分类，便于查找。新建数据模型过程为：选择数据连接后选取连接的数据库以及拖拽选择数据库的表，根据数据库的数据内容选择单张表或者多张表，选择多张表的情况下可设置表间关联关系及字段关系筛选等，进而得到数据模型的维度、度量数据信息，同时用户可手动添加数据的字段映射、值映射。

a.模板管理

模板管理，是对报告涉及的各种模板进行管理，其中模板列表是对报告模板进行列表化管理，并支持报告模板的新建、删除、详情查看、编辑等,即实现报告模板的增、删、改、查等功能。

b.组件管理

组件管理模块是对业务组件的数据展示，功能包括删除、查看详情、编辑标签等，编辑标签页面包括标签选择和自定义标签两个部分，方便给组件标签做编辑。

（14）考核评估

考核评估，是网络安全主管单位及部门，对下级或同级单位/部门进行网络安全类相关业务内容，进行针对既定考核指标的综合考核评价。通过系统，对考核进行全流程管理和配置，实现考核全流程的信息化管理，保障考核过程的可管可控可追溯。网络安全管理部门通过系统，对相关网络安全政策和法律法规的落地效果进行检验和评估，不断完善落地制度和配套措施，不断提高网络安全管理水平。

考核评估主要包括考核统计分析、考核任务管理、考核评分管理和考核指标管理。

1）考核统计分析

通过对相关覆盖区域的网络安全监测、检查、整改和应急处置数据，进行过滤、排列与关联、跟踪和识别，根据多源网络安全感知和数据的特性，与知识库、指纹库的信息聚合碰撞出横向、纵向相关关系，从而得出并展现当前网络安全工作的考核评估开展情况。

2）考核任务管理

考核任务管理模块，是对考核任务从创建考核任务，选择对应的考核指标到评分的全生命周期的管理。本模块支持考核任务的创建，可针对被监管单位的综合安全通报时效性、安全检查时效性、现场抽查数量、督促整改时效性等多项指标进行设定、评分。

3）考核评分管理

考核评分管理，展示由专家队伍根据指标体系进行综合评分后的结果，客观的对当前各被考核单位的网络安全工作进行综合评价。且在考核评分管理模块，可对当前考核的得分情况，进行审核。

4）考核指标管理

为了更好地衡量安全监管工作的有效性，可通过考核指标管理模块进行多项工作的指标制定，包括被监管单位的网络安全技术保障能力、网络安全应急响应能力、网络安全防护能力、网络安全教育培训效果等多个维度评价指标。借此，可有效促进网络安全检查工作落实，逐步提升党政机关单位网络安全工作水平。

（15）态势感知

提供完备的综合态势感知能力，利用大数据分布式集群下的计算、存储和分析技术，实时对重保单位的资产状况、受威胁攻击、安全事件处置等情况进行全方位评估，并以地图、柱状图、曲线图、环状图等多维可视化形式进行展现，帮助监管部门直观了解辖区内整体网络安全态势。

态势感知是整个监管平台的分析与呈现中心，在本次项目中，包含了综合态势、攻击态势、资产态势和运行态势。

系统通过对恶意代码检测、异常流量分析、威胁分析等技术进行宏观分析后，以监管单位为视角，对本项目监管范围下的单位安全状态进行监测；并且根据系统内置的风险评估算法给出当前被监管单位的整体安全评估；并实现对余姚市电子政务外网网络内存在的威胁有效感知并实现可视化呈现。

1）综合态势

综合态势站在决策视角对整体网络安全状况进行态势分析展现，可从不同视角进行分析展现，可查看当前的网络安全总体风险、告警总体数量及类型占比、安全告警等级分布、通报整改质量、安全告警发展趋势以及告警实时监测列表等。

在综合态势大屏上，可开启自动巡检模式，逐个去巡检每个受保护单位的网络资产风险情况，并可随时停止巡检操作。

2）资产态势

资产态势以网络资产作为切入点，为网络安全业务决策做资产相关的可视化分析。

可展示每个网络区域的风险程度，并统计每个网络区域的高、中、低危的网络资产数量。相关具体的统计分析项包括：资产数量及类型统计、资产风险排名情况、资产业务分组安全分析、网络区域风险等级统计、设备及系统资产类型统计等。

还可切换至某单位网络区域的设备/系统关系视角，支持展示重点网络资产关系，呈现单个网络资产风险程度以及网络资产之间的关联关系等，支持更进一步的资产安全分析。

3）漏洞态势

漏洞态势，以资产脆弱性为切入点，对网络资产相关的漏洞进行可视化分析。

漏洞态势大屏的分析展示项，包括漏洞相关告警数量、风险等级评分、低危单位统计、中危单位统计、高危单位统计、漏洞分类统计、漏洞等级统计、单位风险个数排名、风险评估趋势以及漏洞实时列表等。

4）运行态势

运行态势大屏，是站在运维视角对系统的数据采集、数据处理、数据存储等阶段进行性能监控，并对支撑平台正常运行的服务器、中间件、服务组件等进行性能监控。

运行态势大屏的分析展示项，包括数据流监控、平台集群状态监测、平台服务监测、平台数据库监测、平台组件监测、平台性能告警实时监测列表等。

（16）硬件支撑配置

网络安全管理平台运行需配置4台平台服务器，用于平台分布式部署。

平台服务器主要技术参数要求如下：

不少于2U标准设备；含滑轨等配件。CPU: 不低于1颗64核飞腾2000+处理器 主频2.2GHz；内存:不少于256G（总容量）DDR4；硬盘：不少于2块960G SSD固态硬盘（组成Raid 1），不少于12\*4TB企业级SATA 3.5寸硬盘 （总容量不少于48T）；电源：冗余双电源；网口：不少于4\*GE管理电口，不少于2\*GE光接口，不少于2个万兆光接口；其他接口：不少于6\*USB3.0接口；配置网络安全平台部署所需的一切系统、软件、硬件配件等；具备服务期内软件、硬件系统全功能免费升级服务，并配置介质保留服务。

**2.网络安全运行平台**

（1）监测中心

监测中心子系统针对云、网络、终端、应用、数据等暴露面资产的风险隐患、网络攻击和安全事件进行统一管理，摸清风险资产底数。针对网络出口流量进行安全监测，及时发现各类网络攻击、安全事件以及网络风险资产。同时，为更快捷的实现安全态势三要素（隐患、攻击、事件）和三对象（单位、系统、IP资产）的全面管理，设置监测任务中心、搜索中心、验证中心、成果中心，形成针对安全事件、风险隐患、网络攻击从支撑人员（安服人员、安全专家）精准验证到客户精准通报处置的业务闭环。

1）网络安全监测

通过高级行为检测功能，可以识别用户的行为特点，区别机器行为和人工渗透行为。能够分析出普通的扫描器扫描、大量数据获取（拖库行为）、手工渗透等大量的基于行为特征分析。

通过解码所有进入的请求，检查请求是否合法或合乎规定。仅允许通过正确的格式或RFC遵从的请求，已知的恶意请求将被阻断。（例如：跨站点脚本攻击、缓冲区溢出攻击、恶意浏览、SQL注入攻击等。）解码所有进入的请求，检查请求是否合法或合乎规定。仅允许通过正确的格式或RFC遵从的请求。已知的恶意请求将被阻断。（例如：跨站点脚本攻击、缓冲区溢出攻击、恶意浏览、SQL注入攻击等。）

通过对WEB上传和下载的文件进行检测，发现WEBSHELL、可执行文件、非执行文件检测（office、pdf、flash等大量可能被利用直接攻击客户端的文件）。

通过对邮件协议进行深度分析，对已知、未知攻击漏洞的扫描和动态分析的方式检测邮件内容及附件是否含有APT安全威胁。通过分析邮件中的内容可分析出欺骗链接、挂马页面、伪造发件人等各种常见攻击手段。分离邮件中的附件，使用深度的检测手段找到邮件附件中可执行文件攻击和非可执行文件攻击。主要防护内容包括：伪造发件人攻击检测、欺骗挂马检测、伪造欺骗链接检测、 恶意文件检测、WEBmail攻击检测、

通过对内部网络流量进行抓包分析，捕获APT攻击行为，实现APT预警。在检测过程中会分离流量中的各种协议的文件，对文件进行检测。发现文件中的恶意代码，并及时进行预警。

通过对分离出的文件进行快速扫描，内部集成全面的多引擎特征库，及时检测其中存在的各种病毒木马文件，并对文件的来源、目的、详细信息进行分析，便于进一步的进行处理。

通过静态二进制文件安全分析技术可发现常见格式文件的异常特征，如：PDF、DOC、EXE、XLS等。并根据其异常格式、文件异常特征、异常代码来判断文件的可疑特征进行Shellcode静态行为分析。

通过动态沙箱系统，可针对文件进行动态行为分析，通过建立恶意代码行为模型分析恶意文件的运行时行为来确定文件是否存在恶意代码。

2）终端安全监测

支持通过终端探针代理软件持续采集终端动态行为数据，包括样本投递、内存活动、进程行为、网络访问、注册表修改、文件下载行为、进程注入行为和账户变更行为等数据。终端进行全量存储和分析，将数据实时推送到安全数据中台，为威胁狩猎、调查分析、追踪溯源提供数据基础。支持持续采集终端动态行为数据，以威胁行为规则驱动和ATT&CK行为数据模型，结合动态基线检测、机器学习等技术发现高级威胁。

终端管理将已安装终端探针代理软件的终端信息进行展示，包括终端名称、策略组、IP地址、MAC地址、操作系统、系统版本、最近在线时间、7天告警、终端版本、状态、安装时间以及对应时间线和响应中心。

对于终端响应，支持对终端体检，计算系统评分，终端风险列表展示，体检项目包含：系统信息、磁盘信息、环境变量、应用程序、启动项、计划任务、驱动信息、服务信息、进程信息、网络信息、文件信息，支持以其他体检结果为基线做基线对比，分析系统状态变化。支持多种终端处置动作，如进程隔离、文件隔离、进程结束、网络隔离等，支持命令行方式操作终端操作系统。

3）数据安全监测

通过对数据库进行自动扫描发现数据库服务后，进一步对数据库服务进行数据资产盘点，同步数据库的数据库表、字段等元数据，并基于内置的数据特征识别模型。对数据进行识别，例如姓名、身份证、邮箱定义为个人信息，身份证、社保号定义为证件号码等，可对已经发现的数据进行分类管理和数据打标。同时对某个场景下固定开发使用的SQL语句，平台将进行SQL模板和SQL组管理，清晰呈现其所属用途、相关数据库、操作类型、是否触发告警情况。

通过对用户的应用服务进行统一梳理和对应用服务（如API接口服务、应用服务等）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。对接口的健康状况进行实时监测，包括高延时、返回报错、404异常访问进行监测和记录并及时告警，从而发现各类数据安全风险，帮助安全人员进行分析研判。

汇总用户相关的历史、档案、行为得出个体和群体在一个长期时间范围内稳定的数据特征，从而描绘出用户的信息全貌。用户画像和异常行为分析系统根据用户的历史使用行为习惯来画像和定义行为模式。用户行为模式通过机器学习算法生成，在用户当前实时行为模式与其对应的历史模型模式存在一定程度的差异时识别用户行为是否为异常。通过对数据进行分割、审查、交叉分析，周期性地为每个用户依次创建行为模型，形成用户在特定时间内容的行为基线，实时地识别出异常行为，包括但不限于下列分析场景：账户异常行为分析、账户权限变更行为分析、资产被访问异常分析、账户异常分析、越权访问分析等。

4）应用安全监测

自动归档、整理获取到的本地安全监测、情报中心等模块产生的应用安全信息以及上级通报、下级报告的应用安全问题，支持对网站资产进行探测发现、检测状态、追踪变化情况。支持通过事件名称、攻击者、受害者、目的端口、应用协议等条件聚合，系统全面地感知应用安全态势。

a、安全漏洞检测

可对目标站点进行网站漏洞检测，包括SQL注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞以及新发现的0Day漏洞等，及时发现漏洞，并进行人工审核、取证确认，支持网站脆弱性检测，可对目标站点历史风险进行追踪监测，提供漏洞的新增、遗留与修复情况。

b、敏感内容监测

可对接入互联网的重要网站或业务系统做7\*24小时的敏感关键词监测，监测网站页面是否有敏感内容或涉政、涉暴恐、涉黄赌毒等不良信息，将监测发现的信息安全风险或问题及时反馈并协助处置，并提供整改方案。

c、篡改变更监测

可对页面篡改情况进行实时监测，实时发现网站中发生的黑页、暗链等各类篡改事件，帮助用户尽快得知当前网站被篡改情况，能够在事发产生恶劣影响前尽快恢复系统正常。

d、挂马和后门监测

支持网页挂马监测，能有效的检测出网站已知和未知的webshell和挖矿脚本等后门文件。

5）成果中心

a、监测总览

针对验证后的安全事件、风险隐患情况进行总体展示，可根据事件情况进行安全通报预警，相关信息在通报预警模块中可以智能带出，避免繁琐操作，提高工作效率。针对事件类型、子类型进行展示，以矩阵形式展示事件所属类型以及子类型。

b、安全事件

安全事件成果中心基于发现的挖矿、勒索、弱口令、网站篡改（黑链/暗链）、远程控制、WEBSHELL和访问异常等安全事件进行统一管理和汇总展示，包括事件名称、IP地址、单位名称、威胁级别、区域、发生时间、数据来源、处置状态和事件操作等信息。

实现事件导入导出、事件检索、事件研判、事件通报、处置完整的流程，可根据事件情况进行安全通报，相关信息在通报预警中可以智能带出，避免繁琐操作，提高工作效率。

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、所属区域等进行任意字段的聚合分析和快速组合检索。支持在搜索结果中批量下发安全通报或针对安全事件选择任务处置场景下发自动化处置任务，支持事件溯源分析。

提供事件信息联想功能，支持通过事件数据关联同类型事件、同单位事件、同终端事件等联想方式。

c、风险成果

风险成果中心基于发现的主机漏洞、WEB漏洞、基线漏洞、弱口令、数据库漏洞、渗透漏洞、填报漏洞等漏洞风险进行统一管理和汇总展示，包括风险名称、单位名称、风险等级、发现时间、数据来源、处置状态和关联监测任务等信息。

实现风险导入导出、风险检索、风险研判、风险通报、研判完整的流程，可根据风险情况进行安全通报，相关信息在通报预警中可以智能带出，避免繁琐操作，提高工作效率。

配置按风险资产名称、单位名称、发生时间、处置状态、风险名称、所属区域、漏洞等级、数据来源、关联监测任务等进行任意字段的聚合分析和快速组合检索。支持在搜索结果中批量下发安全通报或针对安全事件选择任务处置场景下发自动化处置工单任务，支持漏洞研判分析。

提供风险信息联想功能，支持通过风险数据关联同类型风险、同单位风险、同终端风险等联想方式。

6）验证中心

a、安全场景

提供场景自定义设置功能，自定义场景判断条件、分析周期、分析对象、场景标签，快速配置场景应用。用户可自定义当前热点安全场景，如外部攻击者、挖矿、弱口令、勒索病毒、WEBSHELL等，支持通过单位名称、IP地址、时间等多字段组合查询场景内容。

b、告警监控

告警监控对自动化归并的安全告警数据进行汇总统计，并通过告警列表条目颜色区分“已读告警”和“未读告警”；支持查看归并告警基本信息、规则详情、原始告警列表、全部字段、PCAP包详细信息，并支持下载PCAP包；支持在归并告警页面进行告警快速处置，包括忽略告警、误报处置、联动处置、人工处置等；支持按照时间、告警类型、威胁等级、源/目的IP、攻击方向、攻击阶段、攻击结果，IoC、处置状态、域名、状态码等字段自由组合检索。

c、事件验证

实现事件管理、事件检索、事件分析、事件研判、事件验证等功能。支持按事件名称、受害者、验证状态、结束时间、单位名称、威胁级别、数据来源、所属区域等字段进行组合检索。事件批量处置，支持事件新增、导入/导出、批量验证、批量删除等功能，提交验证描述完成事件验证。事件展示信息，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。支持事件详细信息查看，展示事件等级、受害者、单位名称、资产名称、事件报警源文件等信息。事件信息联想，支持通过事件数据关联同类型事件、同单位事件、同终端事件等联想方式。

d、风险验证

实现风险管理、风险检索、风险分析、风险研判、风险验证等功能。支持按风险名称、单位名称、风险等级、发现时间、数据来源、处置状态和关联监测任务等字段进行组合检索。风险批量处置，支持风险新增、导入/导出、批量验证、批量删除等功能，提交验证描述完成风险验证。风险展示信息，包括风险资产名称、单位名称、发生时间、处置状态、风险名称、所属区域、漏洞等级、数据来源、关联监测任务等信息。支持风险详细信息查看，展示风险等级、风险来源、单位名称、资产名称、风险等级、是否验证等信息。风险信息联想，支持通过风险数据关联单位信息、IP信息、同类型风险、同单位风险、同终端风险等联想方式。

e、风险资产

配置对风险资产进行精细化评级评分计算等功能，资产风险等级包括已失陷、高风险、中风险、低风险，资产评分为百分制，具备资产评级标签；支持按不同字段检索并查看资产历史风险对比、组织架构风险资产数排行和导出风险资产报告。

7）检索中心

a、事件检索

运营平台基于发现的僵尸网站、网站挂马、网站篡改（黑链/暗链）、钓鱼网站和访问异常等安全事件，对辖区内重要信息系统及重点网站的安全进行实时掌控，支持安全事件的统一管理、展示、检索。

b、风险检索

用于查看风险的详细信息，除网络安全运行平台自身存储的风险详细描述和修复建议之外，还提供了相关的外部链接作为参考，为风险研判、修复漏洞提供便利，便于管理人员掌握最新的相关信息。通过对风险漏洞统一管理，支持新增、导入/导出和按照不同字段或组合字段检索，列表式展示漏洞名称、漏洞等级、漏洞类型、CVE编号、漏洞状态、IP、端口、发现时间、涉及服务、涉及单位等多种信息，支持按照不同字段自定义展示。

提供漏洞生命周期跟踪，从披露漏洞开始，持续监控资产变化，实时获取漏洞披露情报，对漏洞发现、分析、修复和审核过程进行跟踪。通过对整个管理过程的评估、对比，达到持续优化弱点管理的要求。

c、原始日志检索

配置灵活自定义检索时间段，可选本日、本周、本月、本年、最近24小时等功能。

配置对所有标准化日志数据和异常记录进行检索等功能，支持通过关键字、条件表达式、时间范围等对告警进行快速检索；此外，支持多条件组合检索。

以图表方式对检索结果进行可视化呈现，图表类型包括但不限于柱状图、折线图、面积图、表格、数值图、饼状图等。

d、原始告警检索

配置灵活自定义检索时间段等功能，可选本日、本周、本月、本年、最近24小时等。

配置根据不同分析变量进行告警聚合等功能，安全日志中所有标准化的字段，都可以作为聚合的变量，告警聚合帮助减轻基于海量告警检索调查的负担。

配置通过关键字、条件表达式、时间范围等对告警进行快速检索等功能，帮助用户快速定位到起关注的威胁和上下文数据；此外，配置多条件组合检索等功能，帮助用户快速转化其分析思路，做到所想即所得。

对检索结果进行时间维度统计，并以时间轴方式可视化呈现。

配置对检索结果进行追加检索等功能，将检索结果字段值一键添加至检索条件中，快速对字段值进行过滤或排除。

配置对检索结果展示字段灵活自定义等功能，可根据特定需求选择显示字段信息。

配置将自定义检索条件存储为检索模板等功能，提供检索条件复用能力，方便用户多次使用同一检索条件。

配置以xlsx或csv格式导出检索结果等功能。

8）监测任务

a、风险监测成果

针对风险监测结果进行统一管理，配置风险检索、风险分析、风险处置等功能。风险检索配置漏洞名称、漏洞等级、漏洞类型、漏洞状态、扫描器类型、IP/域名、端口、服务、CVE编号、CNNVD、关键字等字段检索等功能，实现多字段组合检索。风险类型展示，支持展示漏洞类型、漏洞等级、漏洞名称、IP/域名、端口、服务、CVE编号、漏洞状态、扫描器和发现时间。配置查看风险详情，包括资产信息、关联监测任务、风险状态、数据来源、威胁等级、生命周期，标签，并提供相应的资产关联链接。配置风险处置一键联动通报预警平台，实现风险处置。

b、监测任务管理

漏洞监测功能可统一调度不同种类的弱点扫描器，实现扫描任务的创建、下发、任务状态监控、任务启停、报告取回、报告归一化等一系列集中管理功能。同时，通过对报告的自动解析和漏洞归一化，并实现与资产脆弱性关联，形成本地区资产风险的统一管理。

监测任务类型包括主机扫描、WEB扫描、基线扫描、弱口令扫描、数据库扫描等；对于已建立的任务，支持进行执行、停止、编辑、删除操作；任务详细界面可以查看当前任务历次执行的结果统计；同时，基于通报预警流程，实现漏洞闭环管理、持续分析和预控安全风险。

c、引擎调度

安全监测模块可对不同种类的扫描器实现自动调度。构建扫描器管理调度中心，实现扫描任务的创建、下发、任务状态监控、任务启停，降低各类扫描器差异化导致的学习使用成本。

d、监测报告

配置将任务执行的结果进行统计分析形成统一规格的漏洞报告和整改报告等功能，并支持其他系统报告导入等一系列集中管理功能。

（2）资管中心

资产管理是整个网络安全运行平台建设的关键组成部分，多源融合云、网、数、用、端等不同层面的资产数据，并对数据进行归一化去重以及资产分布、漏洞和指纹信息进行统一管理，摸清资产底数，形成统一的资产立体化监管，针对暴露面资产进行深度调查与分类、分级，形成更加细化的信息系统资产数据：按所属行业、机关横向分类；按所属地域、组织架构横向分类；按信息系统重要、敏感程度纵向分级；按信息系统脆弱程度、可用程度纵向分级，完成资产从发现、导入、存续管理、风险分析、变更监控及下线退库等全生命周期的管理，即有主资产自动匹配责任部门，无主资产自动发现、走认领流程补充确认后上线入库，支持资产字段灵活扩展，关键信息全局检索。

1）全息档案

a、单位档案

单位档案子系统提供单位监测和刻画能力，以网络空间地理信息图谱实现对单位的全面掌控。并为每个单位构建起档案，基于多方采集的数据，对单位进行全方位管理和刻画。同时，提供可视化档案呈现和档案管理功能，支持通过单位名称、单位行业、单位类型、单位标签、单位简称、单位状态、联系人、备案号等信息进行单位检索和根据类型统计单位资产信息，包括但不限于单位总数、风险单位个数、风险单位行业分布和风险单位排名。

单位档案主要内容包括单位基本信息、安全检测、人员信息、业务系统、资产、供应链、档案时光轴等。

b、系统档案

系统档案子系统提供系统监测和刻画能力，以网络空间地理信息图谱实现对业务系统的全面掌控，真正反应网络资产的安全状态，从而打破信息壁垒，消除信息孤岛，为网络安全事件调查处置提供基础数据支撑，为重点活动期间网络安保业务提供重点系统关注能力。同时，提供可视化档案呈现和档案管理功能，支持通过单位名称、系统域名、风险系统、系统名称、系统类型、系统标签、系统IP、服务组件等信息进行系统资产检索，支持卡片式、缩略图方式展示系统信息，展示内容包括系统名称、官网IP、详细地址、安全事件、网络攻击、风险隐患等。

系统档案支持系统画像快速浏览，信息至少包括系统信息、安全监测、供应链、基础网络、人员信息、单位信息、档案时光轴等。

c、IP资产档案

IP资产管理覆盖云主机、服务器、终端等资产类型，通过快速筛选地区信息和监管组织架构，筛选出被监管的资产，支持通过所属单位、行业、IPv4、IPv6等属性对资产进行精确定位，从安全事件、网络攻击、风险隐患对资产进行综合安全评估。

资产管理以资产卡片、资产缩略图、资产管理三种方式进行显示，直观展示IP资产的详细信息，并对IP相关重点信息进行提取显示，如对应单位名称、资产标签、对应的安全事件情况、网络攻击情况和风险隐患情况等。

可以通过单位名称、资产类型、资产标签、资产评级、资产来源等条件进行灵活筛选查看详情。对资产的安全情况进行评级，支持已失陷资产、高风险资产、低风险资产的数量统计，并可通过风险系统变化趋势管控趋势图查看资产风险变化情况。

现对资产信息的管理维护，通过“新增”功能可增加资产信息，输入字段包括资产名称、单位名称、资产类型、资产标签、责任人、资产重要性等基本信息和是否国产化、是否物联网设备等扩展字段信息，并支持资产的批量导入导出功能。

2）数据资产

数据资产管理提供完整的数据源管理功能，帮助用户直观、清晰、便捷的完成数据源档案过滤、检索、全局分析和数据库专项分析。支持展示不同区域或组织架构的数据源情况。支持通过数据库名称、数据库类型、主机、数据库标签查询，支持通过安全等级、行业等标签过滤检索，根据检索结果统计分析并显示数据库概览，包括数据库总数和敏感库总数；支持根据单位统计敏感库top10；支持根据数据库安全等级统计数据库敏感分布情况。

支持卡片式、表格形式展示数据源档案信息，展示内容包括数据库卡片显示数据库名称，数据库类型、所属单位、主机、端口、所属行业、否是敏感库、安全等级分级、数据来源、数据主题信息，标记重要数据库，统计敏感表、数据表、告警数、安全事件、安全隐患。

a、数据源档案

数据源档案子系统包括数据源概览、基本信息、数据表信息、隐患信息、安全事件信息、威胁告警信息。

b、数据表档案

数据表档案子系统包括数据表概览、基本信息、数据项信息、隐患信息、安全事件信息、威胁告警信息。

c、接口档案

包括接口概览、基本信息、隐患信息、安全事件信息、威胁告警信息。

3）网络规划

网络规划用于管理网络规划的安全域网段信息，对安全域的网络环境、IPv4网段、IPv6网段、防御设备、负责人等信息进行结构化管理，提供安全域信息新增、编辑、删除、检索，导入、导出、批量操作功能，提供卡片式快速预览安全域中IP分配数、已使用IP数、存在的事件和隐患，提供安全域全息档案详细展示安全域名称、归属单位、所属网络、IP网段分配、防御设备部署、联系人等信息。

支持单位网络规划管理，可定义安全域名称、单位名称、网络环境、安全域重要性、安全域属性标签、等级保护、是否政务云、是否关基资产、否归属地区归属行业、是否固定IP、经纬度、安全防御、联系人等信息。

4）网络管理

网络管理包括CDN数据、IDC数据、ICP备案数据，网络安全运行平台将各个数据来源收集到的数据进行归纳整理，便于查询检索本地基础网络相关数据。

CDN数据包括CDN厂商名称、IP地址、运营商信息、地理位置信息，可按照多种条件进行组合查询，并对CDN厂商、CDN节点分布情况进行统计展示。

IDC数据包括IP范围、运营商、地理位置、关联机房等信息，并支持查看某个IDC的安全状况。维护IDC信息时，可新增IDC所包括的机房信息。

ICP数据包括域名、备案单位、单位行政归属、ICP备案号、备案有效性等信息，可按照多种条件进行组合查询，并对区域分布情况、单位性质分布情况进行统计展示。

5）业务全景

实现以业务资产视角，辅助用户以资产为核心的工作层面之上构建一个面向业务部门和管理层的业务资产模型。业务全景功能主要管理用户的业务支撑系统，实现业务资产拓扑和资产安全等级评价等功能，为用户提供业务的实时监控能力，保障用户业务的可持续平稳运行。

主要功能如下：

提供安全资产拓扑视图，支持根据网络架构自定义资产拓扑，支持拓扑的模板导入和编辑好的资产拓扑文件导出；用户可以根据具体的业务流程构建相应的业务模型，支持业务模型的管理功能。

6）人员管理

人员管理可实现对具备网络安全能力的人员情况的全面掌控，对其是否就职于网络安全企业或参加过网络安全大赛等信息进行分析，并对其网络行为日志进行监控与审计，及时了解重点人员情况，为网络安全业务从业人员评估提供参考依据，为重点活动期间网络安保业务提供重点人员关注能力。系统既提供可视化档案呈现能力，同时提供人员档案管理系统。

a、人员统计

人员档案子系统基于多方采集的数据，对涉网人员进行全方位刻画，直观显示重点人员数量统计，对其基本信息、网络身份、涉网技能、教育情况进行全息刻画，形成辖区内涉网安全相关重点人员库，并根据业务需求划分多个子库。

b、标签统计

针对入库重点人员进行打标签，标签类型包括前科人员库、涉关基人员库、安全服务人员库、系统开发人员库、网络安全专业人员库、特殊技能（网络安全）人员库、CTF人员库等。

c、分布统计

采用地图画域方式展示该地区重点人员数量或通过饼状图、柱状图形式按照前科人员、职业、年龄、行业等维度显示重点人员占比情况。

（3）感知中心

安全感知中心提供网络安全威胁可视化的入口，基于网络安全运行平台获取的各类监测数据及日常业务流转产生的业务数据，以网络安全事件与威胁风险监测为驱动，对网络空间安全相关信息进行汇聚融合，从不同视角感知网络安全态势。

感知中心系统以单位数据、资产数据、网络安全事件与威胁风险监测为驱动，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，从不同视角出发感知网络安全态势，包括但不限于安全运营态势、综合监管态势、外部攻击态势、资产态势、应用系统态势等视角。

1）安全运营态势

按照本日、本周、本月、本年、近7天、近30天维度进行统计，支持政务云实例、骨干网设备、入网终端、应用系统、数据库的数据展示，可展示制度规范，并支持预览。支持统计安全运营机构、安全联络员、首席安全运营官，支持展示安全值守联络员和今日值班人员。支持安全事件、风险隐患、网络攻击事件的展示，并支持下钻。支持地图形式展示各区域安全告警和待办工单数量，并支持下钻。

2）综合监管态势

综合监管态势汇聚单位、资产、威胁风险、网络攻击、安全事件、预警处置等总体情况，通过多维图形可视化方式及实时更新的动态趋势数值进行综合呈现。

综合监管态势大屏通过“网络空间-地图空间-单位拓扑”三层映射关系，可直观了解本地资产情况、网络安全监测成果、黑客动态、通报情况、资产分布和网络攻击趋势等，多维统计数据全部支持查看详情，针对隐患情况、事件情况、网络攻击情况可直接下发通报处置任务，实现“一张屏”协调指挥。

通过综合监管态势实现网络安全保障措施从网络虚拟空间到城市地理空间和企业网物理空间的互联互通全面贯彻，让监管者能够一张屏看清资产底数，探明风险隐患，下发整改通知，协同追捕攻击者。

3）资产失陷态势

资产失陷态势汇集重要信息系统、网站、终端等不同资产信息，实时获取和分析当前失陷资产总数、分布区域、外联类型、危险等级等情况。结合地图、表单、趋势曲线并通过大屏进行生动呈现，可查看资产失陷事件详情，包括资产所属IP或IP段、远控地址、攻击类型等。

4）威胁态势

威胁态势通过分析漏洞、木马、病毒、篡改、非法关键字等不同威胁类型，结合对重要信息系统的监测、第三方威胁情报数据、历史积累数据等多方数据来源，实时获取和分析当前安全威胁总数、类型数量、区域分布、数据来源分布、典型漏洞分布等信息，以及最新监测发现的威胁详情，如存在威胁风险的URL、监测发现时间、等级、详细描述及威胁处理建议等信息。

5）隐患态势

隐患态势展现当前各类隐患数据统计及分布情况，具体包括六种隐患统计数量、专项隐患情况、各类隐患数据源统计、行政区域隐患统计、行业隐患分布、隐患系统TOP5、最新隐患、隐患趋势等信息。

6）事件态势

事件态势主要汇总网络安全运行平台发现的各类网络安全事件，按照网络攻击事件分类标准对事件进行分类，实时获取不同事件类型及总量，分析事件地域、行业、时间分布，结合网络攻击事件快照抓取技术进行证据留存。可查看最新安全事件发生时间、事件类型，以及所涉重要信息系统IP、所在地区、所属行业、事件截图等信息。

7）预警态势

预警态势主要针对安全事件和威胁风险的预警处置工作进行分析及可视化呈现。针对存在威胁风险隐患，通常进行预警通报，并提供提醒和限期整改两种预警方式。针对已发生的安全事件，可发布安全事件通报，要求相关单位开展应急响应工作。预警处置态势对上述业务过程产生的各类数据进行统计分析，呈现各类业务类型统计、时间趋势分布、区域分布、行业响应处理效率、最新预警处置处理进度等信息，实时把控预警处置工作开展情况。

8）外部攻击态势

外部攻击态势通过分析漏洞、木马、病毒、篡改等不同威胁类型，结合对重要信息系统的监测、第三方威胁情报数据、历史积累数据等多方数据来源，实时获取和分析当前本地区受到的攻击总数、攻击类型情况、受攻击区域分布、攻击来源分布等信息，并借助网络安全杀伤链模型进行威胁分析，将攻击按照侦察、投递、利用、横向渗透、命令控制、内部侦察、获利七个步骤进行归类，实时掌握本地区收到的攻击状况。

9）应用系统态势

应用安全态势提供应用服务的被访问状态和受攻击情况统计，包括网站区域访问量、访问地区排行、访问/攻击IP排行、被攻击网站排行，攻击类型排行，网站访问或攻击变化趋势等。结合柱状图、动态迁徙图对主要攻击类型、攻击源、被攻击目标、访问源、被访问对象分布、排行进行实时动态呈现。

（4）响应中心

响应中心子系统配置将监测到的漏洞隐患或安全事件按照信息系统网络安全事件隐患分级标准进行通报下发、预警提醒或限期整改等功能，被通报的单位反馈处置结果，从而实现通报预警工作流程化管理；支持其他通报方式，包括但不限于短信、邮件、APP等；支持对通报情况和处理情况进行统计展现和提供不同类型的通报报告。

配置将网络安全运行平台下发或本地安全监测、情报中心、等保备案等子系统产生的安全和管理数据进行分级、分类归纳分析等功能，自动形成通报报告，并通过离线方式导出至互联网区的响应中心子系统，并按照不同情况分别通报和进行处置通报反馈的业务流程。同时，支持将本地监测发现的网络安全事件上报。

安全响应流程业务逻辑架构如下：



1）信息公告

信息公告分为发布公告和公告跟进两个功能模块。主要用于发布重大资讯、公告等信息，可跟进下级部门和相关单位消息查阅情况。

a、发布公告

配置发布重大信息、资讯等功能，可批量选择相关接收单位。

b、公告跟进

配置查询相关发布的重大通知公告以及跟进对应接收人查阅情况等功能。

配置公告信息列表查看等功能，字段包括标题、发布时间、查阅进度。

配置跟进公告查询进度等功能，包括已查阅人员和未查阅人员情况。

配置公告信息的查询等功能，查询条件包括发布时间、标题等。

配置公告详情的查看等功能，信息包括标题、内容、图片、接收单位。

配置提醒操作等功能，若相关接收单位未及时查询相关信息公告，可对其进行提醒。

2）任务管理

针对发现的安全隐患、安全事件可通过通报督促相关单位进行整改，除在通报页面直接发起通报外，可实现网络安全运行平台数据无缝对接，网络安全运行平台可接收回复上级通报情况。

创建任务看板功能，实现对通报情况和处理情况进行统计展现，支持图表模式和列表模式。可按照区域或时间进行筛选查询，其中总览情况统计内容主要包括事件通报、限期整改、超时提醒、通知等；同时支持事件通报效率、隐患通报效率统计及区域通报统计（包括事件通报数、限期整改数、提醒数、通知数）。

3）通报管理

配置安全事件、安全隐患和安全情况发起通报等功能，可填写成员单位、单位接收人、选择是否同步给上级主管、选择抄送人、事件备注及附件上传等。

成员单位收到通报后开展处置，将处置结果按时限及时上报。

a、安全事件

配置将用户发送的通报、收到的通报和抄送安全事件通报按照通报流程的生命周期进行汇总统计等功能，可查看通报的事件信息，包括通报的详情（包括发布人、接收人、通报状态等）、事件详情、该次通报的通报记录等信息，实现对整个通报过程进行跟踪记录。通报未完成或未通报的可在网络安全运行平台上进行通报，实现WEB通报和移动端通报的同步。

配置回复通报的信息等功能，支持上传通报报告等附件。

b、风险隐患

将用户发送的通报、收到的通报和抄送安全隐患通报进行统一汇总，可查看通报的隐患信息，包括通报的详情（包括发布人、接收人、通报状态等）、隐患详情、该次通报的通报记录等信息，实现对整个通报过程进行跟踪记录。

配置回复通报的信息等功能，支持上传通报报告等附件。

c、安全情况

汇总分析近期发生的网络安全事件，并发布网络安全事件分析报告。

4）预警管理

当爆发重大漏洞时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。可通过预警详情查看各单位接收阅读情况。

网络安全事件风险预警等级共分为四级：由高到低依次用为红色预警、橙色预警、黄色预警和蓝色预警表示，分别对应表示发生或可能发生特别重大、重大、较大和一般极危、高危、中危和低危网络安全事件风险。

业务流程说明：

网络空间发现风险险情（如新的重大隐患、破坏性严重的木马病毒、针对本区域的网络攻击事件）；

组织涉网监管单位、网络安全专家组、安全企业、技术支撑单位开展分析研判，并在网络安全运行平台汇集研判结果、判断级别及报告；

组织决策是否发起预警；

在平台中筛选匹配资产底数，明确影响范围；

填写预警信息，根据影响范围选择预警接收范围，明确受影响清单的，预警信息附带受影响的资产清单，要求重点处置；

发起专项预警，对其他参与者进行信息抄送；

受影响单位开展专项行动，安全企业、技术支撑单位、专家团队提供技术支持；

反馈处置结果；

完成专项预警响应；

解除预警。

5）通知管理

通过网络安全运行平台完成通知、公告等信息下发，做到信息通报的及时性和线上工作留痕。也可以通过通知管理功能完成信息调查调研等。支持新建通知，包括标题、内容，选择接收单位、接收人（选择本辖区或下辖区域的单位接收人），上传附件，点击发布即可完成发布通知。

信息公告分为发布公告和公告跟进两个功能模块。主要用于发布重大资讯、公告等信息，可跟进下级部门和相关单位消息查阅情况。

a、发布公告

配置发布重大信息、资讯等功能，可批量选择相关接收单位。

b、公告跟进

配置查询相关发布的重大通知公告以及跟进对应接收人查阅情况等功能。

配置公告信息列表查看等功能，字段包括标题、发布时间、查阅进度。

配置跟进公告查询进度等功能，包括已查阅人员和未查阅人员情况。

配置公告信息的查询等功能，查询条件包括发布时间、标题等。

配置公告详情的查看等功能，信息包括标题、内容、图片、接收单位。

配置提醒操作等功能，若相关接收单位未及时查询相关信息公告，对应人员可对其进行提醒。

6）综合报告

网络安全运行平台能提供四种类型的报告包括综合报告、安全通报报告、整改通知书、整改统计报告。支持针对四种报告设置报告模板，包括设置首页LOGO、页眉页脚、具体报告文案等信息。支持用户自主选择报告数据范围，时间范围等；支持查看历史生成的报告。

a、综合报告

可按照区域、时间范围生成综合报告，报告主要描述该区域内的安全风险总体概况、资产分布情况统计、漏洞情况统计及趋势分析、安全事件统计及趋势分析、响应处置情况统计、网络安全运行平台使用情况、APP使用情况等。支持查询及下载历史报告和将报告发送到指定邮箱。

b、安全通报报告

可按照区域、行业、危险等级、具体单位、具体网站等维度生成安全通报报告。以单位或信息系统的角度统计单位或信息系统所面临的漏洞、威胁、攻击事件等情况，并能提供相关整改建议。支持查询及下载历史报告和将报告发送到指定邮箱。

c、整改通知书

可使用设置的整改通知书模板，按照区域、行业、危险等级、单位、网站、限期整改时间等维度生成整改通知书，并提供相关整改建议。支持查询及下载整改通知书和发送到指定邮箱。

d、整改统计报告

可按照区域、时间等维度生成整改统计报告。对未通报事件、已通报事件、整改中事件、整改结束事件和逾期未整改事件进行统计。支持查询及下载整改统计报告和发送到指定邮箱。

e、报告模板设置

配置根据预先设定的模板等功能，生成整改通知书。整改通知书包含区域、行业、网站等级、单位类型、具体单位、具体网站等信息。并支持查看整改统计报告。

7）结果复核

配置相关责任单位提交隐患整改结果或事件处置结果后，可对其反馈结果进行复核操作等功能。

配置待复核任务的展示等功能，展示字段包括任务名称、等级、反馈时间、通报时间、整改截止日期、通报进度、通报反馈状态。

配置待复核任务的筛选等功能，筛选条件包括通报时间、反馈时间整改截止日期、通报反馈状态。

配置单位反馈结果查看等功能，包括隐患整改结果、情况描述、事件处置结果、以及对应上传的附件信息。

配置消息提醒等功能，当责任单位反馈处置结果时，可实时推送单位反馈情况，及时对其进行复核操作。

8）通报方式

网络安全运行平台具备多种通报方式，包括移动端通报浙政钉、钉钉、短信和WEB端通报等方式。移动端通报浙政钉、钉钉，丰富了通报功能的使用场景, 从而实现快速响应通报流程。

用于移动端发布信息安全通报、信息安全通告、政策法规宣传、风险预警等信息，实现方便、快捷、及时通讯等要求， 随时随地查看通报进度，形成监管部门与被监管单位的有效沟通。

通报浙政钉包括监管端和单位端。监管端主要针对监管部门实现通报指令的下发、重大信息的发布等功能进行设计，包括通报发布、通报跟进、信息公告、统计分析等功能模块。单位端主要针对成员单位实现通报结果、处置结果反馈等功能进行设计，包括通报跟进、单位管理等功能模块。

9）移动APP

网络安全运行平台集成移动端通报APP小程序，作为平台的移动端延伸，满足独立性和安全性要求，完全自主可控，不依赖钉钉、微信等第三方平台，为用户提供便捷入口，支持查看平台和操作部分重要业务，主要包括掌上态势、掌上报告、掌上溯源、掌上安保、掌上通报、掌上考核、掌上资产和掌上安全等内容，进而丰富了通报功能的使用场景, 从而实现快速响应流程。

（5）Web端工作台

提供Web端工作台应用，同时提供网络安全运行平台自身的监测管理工作台，从集中监控、安全审计、访问控制、资源控制、运维管控、平台扩展等多个方面全面设计，实现综合安全防护的目的。

1）安全工作台

为运维人员提供安全事件处置工作界面，包括工单总体状态、通报情况、最新安全动态等视图，并提供待办工单状态工作台，帮助运维人员快速处理待办工单。

2）任务管理

实现对流计算任务和定时计算任务的集中管理。

集中监测规则引擎、关联引擎、自定义规则引擎的运行状态与健康度，提供一键重启功能恢复引擎运行。

集中监测定时任务的运行状态，针对定时任务实现任务的启停与编辑。

3）操作审计

大数据操作审计对用户访问、操作大数据平台的行为进行记录审计，为用户画像等功能提供原始分析数据。

对操作用户名、操作者IP、操作信息、操作结果、操作模块、操作类型、操作时间等操作信息进行详细记录。

支持对操作记录信息进行多维度查询。

4）访问控制

通过根管理员帐号对平台用户帐号及相应权限进行统一管理，避免权限过度开放。支持对平台用户角色新增、编辑、删除等管理操作。

设定认证安全策略，避免账号暴破等安全威胁。支持设置连续登录失败X次锁定用户、登录超时时间等。

5）状态监测

对平台整体运行状态进行监测，并可视化呈现，帮助用户及时发现平台异常，保障平台平稳可靠运行。

对平台流量、日志吞吐量进行实时监控，并统计呈现一段时间内的变化趋势。

对平台最新运维告警进行呈现，并支持下钻具体告警信息。

对磁盘容量进行监测，并呈现总容量、剩余容量、存储占比、前一日新增数据量、日志已存储时间、预估剩余可存储时间等信息。

对安全运营、安全监测的基本数据信息进行集中展示，如平台运行时间、告警总数、待办工单、通报数量、管理资产、风险资产等信息。

6）平台运维

提供独立的运维管理功能模块，向系统运维人员集中提供安全运维告警查看、健康检查工具、数据存储管理、组件故障日志，协助用户全面审计大数据系统整体安全状况。

实现系统运维告警的集中查看，包括告警的数量趋势、告警级别与名称、告警总数与各类型告警百分比等，提供运维告警搜索框页面，协助运维人员快速定位告警排查问题。

实现平台系统的一键巡检，针对数据健康、探针健康、大数据集群健康、组件健康、节点健康状态进行一键式排查询价，并针对以上数据异常场景给出可执行的处置建议。

实现随数据存储的集中监控管理，针对磁盘总体使用情况和磁盘空间利用趋势在同一界面进行可视化展示。

实现组件故障日志的集中下载与管理，针对大数据组件的异常信息可以将日志下载到本地进行详细排查。

（6）移动端

处置通报流程和可和浙政钉对接，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。

使用浙政钉进行通报下发或处置流转，对通报过程进行跟踪记录，完整记录任务流转过程详情并同步到Web端平台。

1）安全通报能力建设

浙政钉监管端利用平台选择特定的用户或组织进行下发预警，预制好预警级别、标签等。针对未通报的事件，将根据事件信息，配置好日常通报模板生成通报文件。充分利用数据安全监测、监管溯源、情报信息等模块获取针对数据的违规行为、越权操作、批量操作、高危操作等情况，利用通报系统汇总、分析、研判，并及时将情况上报、通报、下达，进行通报及快速处置。

单位端利用平台提供的全局维度的安全分析通报功能，按照预警名称的维度对公开预警进行查询的功能，并可根据指定的查询条件，快速定位需要重点关注的公开预警，并跟进通报任务情况，包括隐患通报任务和事件通报任务。后续向监管端反馈相关隐患或事件处理情况，内容包括处置方式（处置完成、误报）、情况描述、上传图片及附件。

2）风险预警能力建设

浙政钉监管端针对收集到的有代表性的网络攻击行为、新产生的网络安全威胁情报、网络安全整体分析报告和各部门单位的应急处置状况进行统一发布，提高统一调度和指挥能力。内容包括通报时间、信息标题、通报等级、通报详情、举证信息等。

单位端接收监管方下发的相关通报信息。并针对此类信息进行调查分析，从而确认安全事件的准确性和影响范围。对已经确认的攻击，则通过相应的预警通报机制完成预警通报工作。完成相关应急处置后，反馈相关信息，填写信息包括描述、上传图片、插入表格等。

（7）大数据安全监测

对重要的大数据平台进行统一的监测，摸清全市重点大数据平台数据状况及其使用情况，同时实现对涉大数据平台的单位管理、大数据信息系统管理、大数据平台安全防护情况管理、涉大数据平台或信息系统的人员管理等。

（8）云平台安全监测

网络安全运行平台可对接多种类型云平台，如华为云、阿里云、华三云、青藤云，自动归档、获取到的云实例（ECS、OSS、RDS、SLB）安全问题，包括具有IP 地址的云主机、数据库、存储、负载均衡等实例安全问题，支持对云平台资产进行探测发现、检测状态、追踪变化情况。

配置通过部署流量探针设备，从外部攻击者、CVE漏洞利用成功、勒索病毒、挖矿活动、威胁情报、钓鱼邮件、弱口令等场景分析等功能，支持通过事件名称、攻击者、受害者、目的端口、应用协议、供给链等条件聚合，系统全面地感知云平台安全态势。

（9）资产数据治理

配置通过接入探测设备，基于网络规划的资产主动探测，明确到单位与责任人等功能。针对网络环境包括政务外网，互联网暴露面，兼顾行业专网提供系统可用性和无故障运行时间评估。打造资产普查一体化流程，自动发现、下发确认、信息补全、审核、归档、联动控制，完成政务网的信息资产与安全资产的全面梳理。

1）资产数据摸底

资产数据摸底实现资产检索、探查，支持多种SQL语法组合检索，包括“与”、“或”、“等于”、“存在”、“包含”等语法，且具备语法示例，方便用户快速上手使用。提供资产展示功能，支持资产名称、资产类型、资产大类、资产小类、资产标签、单位名称、所属行业、地理位置、安全等级、事件名称、风险隐患名称、受攻击名称等多个字段展示，并可自定义删减字段。

2）资产数据探测

a、资产探测

域名资产探测：以域名资产为探测条件，对目标域名进行爬取与分析，自动探测该主域名的子域名，并获得所有域名的备案信息和关联IP等指纹信息。同时可定期进行基础数据的收集与持续更新，检查与校验域名解析IP变更和备案信息变更等情况。

0WEB资产探测：通过单位名称关键字，匹配网站备案信息，探测发现相同备案单位名称的WEB资产。通过探测到的域名和子域名资产，验证哪些域名可正常访问，提供WEB服务。

主机资产探测：通过自定义IP段探测功能，对所有IP实施全端口扫描探测，发现开放的端口和提供的服务和协议等，支持端口及IP信息自定义扫描。

资产状态监测：能够通过端口扫描和协议识别的情况，自动分析和统计出资产的新增或减少等变化情况。同时可对资产上线、下线以及服务类型变更、服务指纹变更等进行监测，有助于发现隐蔽风险。

b、探测方式

按行政区划进行搜索：支持按行政区划对区域资产进行探测，支持到区县行政区划。支持按政府、教育、医疗、金融等细分行业进行行业资产探测。

根据域名探测搜索：对暴露在互联网上的网络资产进行探测和分析，通过输入单位主域名可快速探测、识别其相关联的资产数据，包括子域名、二级域名等，支持多个域名作为同时探测。

根据单位名称关键字探测：通过单位名称和重要关键字进行全网探测，以各单位名称作为关键词，对云端数据探测到的资产数据进行关键字匹配，识别筛选出相关联资产，并推送至互联网资产探测服务平台，自动关联至单位组织列表。也可以通过输入业务系统名称、备案信息等关键字对云端扫描的资产进行匹配识别。

根据IP段进行探测：支持对多个IP、IP段内的资产进行探测，发现相关资产信息，包括关联的域名、服务类型、资产指纹、协议类型、开放端口等数据。

资产指纹识别：支持对发现的资产指纹信息识别与维护，主要通过对网站返回的响应头部字段，页面URL特征，页面中的插件特征等进行识别判断，也可以人工维护多类指纹，包括WEB容器指纹、开发语言指纹以及开放端口等信息。

c、探测技术

能够快速并全面的发现单位互联网开放的资产以及资产漏洞、篡改、可用性等安全风险情况。资产探测应采用如下核心技术：

高速网络扫描技术：使用高速的网络扫描技术，在并行化加速方面，资产探测扫描引擎支持多主机分布式扫描。通过对基于素数域原根的扫描地址生成进行分片处理，不同分片的扫描地址集合都是迭代生成的互为不相关的子集，利于地址生成策略的并行化执行，同时其结合了黑名单数据结构、数据包传输机制等其他改进，适应10Gbps环境下更高速的扫描。

网络资产指纹识别技术：支持网络资产指纹识别技术，常见的指纹识别方法主要有常规特征匹配和基于机器学习算法的特征匹配两种。常用的操作系统指纹识别特征有：IP头中的总长度（to-tallength）、标志（ID）、是否分片（DF）、生存时间（TTL）字段等，TCP头中的可选项，TCP头部的窗口大小（wsize）、可选项等，以及ICMP、UDP协议指纹、SYN-ACK包重传时延等。此外，还采用了综合加权匹配的方法，通过指纹评分表对各响应数据项的指纹识别能力进行了量化评分，在计算响应同该条指纹的匹配率时，引入各数据项的评分作为加权，从而进一步提高识别的准确率。

网络资产自动分类技术：一方面采用的技术需要可高效、无误差地提取出反映、暗示网站类别或者对网站所属类别有指导性的一些标签内容,需要对网页进行某些标签内容的提取,比如HTML文档的标题提取、META元标签的提取、正文提取等等，并把短文本切分为词的集合。另一方面采用的技术对于目标网页集可对短文本词集合，根据初期提供的文本关键词在每个类别下的分布情况利用特征提取方法进行特征的提取，找出最能代表的网页的类别。进而实现WEB资产自动识别分类，离不开网页特征聚合分类引擎。网页特征聚合是网页分类的重点部分。依托大数据与机器学习算法，结合已知的关键词、特征向量等进行网站页面解析，可实现对网页的特征聚合，而依托大数据分析算法与机器学习，实现新加入网站的页面常见词聚合，拓展新类型的网站分类项。

威胁情报数据：威胁情报作为重要的数据分析资源，威胁情报数据支持导入平台。

d、网站安全监测

安全漏洞检测数据：安全漏洞监测应能发现常见的WEB应用漏洞，支持OWASPTOP10等主流安全漏洞，以及各种挂马方式的网页木马如Iframe、CSS、JS、SWF、ActiveX等。

安全事件监测服务数据：支持对网站进行页面资源与指纹信息的分析，通过监测技术对各类安全事件进行全面分析感知，包括篡改、暗链、黑页、挂马、后门等。

主动探测数据：通过互联网资产探测服务工具主动对网络资产基础数据展开普查性检测与周期性监测，建立与维护行业互联网业务系统资产和硬件设施档案库。

由于全市重点行业资产数量庞大，且安全状态相对于专业入侵者存在不确定性，安全服务厂家监测预警体系中不仅应提供系统自动监测发现的安全问题，为了保障监测的全面性，系统还支持标准化数据接口包括专用数据接口与通用数据API接口，系统支持对接CNVD、GEDB等等第三方漏洞平台。

e、探测周期

具备灵活的资产探测周期设置，可选择“单次探测”、“天”、“周”和“月”等条件进行探测。常态化至少每月执行一次，特殊情况下至少每周执行一次。

f、任务管理

提供资产探测任务管理，包括探查任务新增、执行、停止、编辑、删除等功能。通过资产探测任务管理，针对网络中所有在线设备进行自主网络扫描和深入识别，获取资产的网络地址、系统网络指纹、系统开放端口和服务指纹，并根据积累和运营的指纹库裁定每个资产的类型、操作系统、厂商信息等。

3）资产发现与管理

资产普查主要提供对辖区内开放的各类信息系统进行收录，以实现对网络资产底数的全面探测与管控，采用云端威胁情报资产全面探测与扩散，大面积覆盖网络资产；并依据资产的全生命周期理念，结合单位上报资产，全程管控暴露面资产，能够解决以往资产管控存在的大量短板，例如资产发现不全面，存在监管盲区；新增资产不报备，开设随意不规范；资产下线不彻底，遗留资产有风险等问题。

（10）检查督查

检查督查中心通过从监测中心、等保备案、响应中心等系统中获取的单位系统备案信息、测评信息、威胁隐患、攻击日志等数据建立该单位系统的超级档案，实现对辖区内单位资产的情况摸底，并根据摸底结果筛选出重要单位系统开展针对性的检查工作。同时，系统提供自动分析功能统一分析发现共性问题，替代原有的线下整理，人工通知的繁琐过程，显著提高重点系统的安全防护水平和的工作能力及效率。

检查督查中心主要包括现场检查、安全自查两个部分，通过系统管理检查工作，收集检查数据，评价检查结果。检查调查系统支持与网络安全检查工具箱、工业控制系统安全检查工具箱实现数据对接和业务管理闭环。

检查调查形式包括现场检查和安全自查两种模式。



1）现场检查

现场检查是由组织单位，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shi的情况、检查队伍评价（平均星级排序，平均星级可有半颗星）。

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。

2）安全自查

除了开展现场检查工作外，支持各单位定期自我检查并上报检查结果，统一设计、安排，并经过通知系统下发单位自查通知。

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shi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：系统在单位侧开放自查模块，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。

（11）指挥调度

按照“挂图作战”理念，围绕网络空间测绘与资产分析、地理资源和网络空间数据模型构建，绘制网络空间地理信息图谱，实现平台指挥调度功能。

挂图作战体系利用地理空间理论方法、模型、数据，构建网络空间地理信息图谱。具体做法是基于网络空间安全业务工作场景和能力建设需要，制定网络安全逻辑数据模型，并以此为基础汇聚网络空间安全防护主体的各类信息，包括基础信息、人员情况、物理场所、信息资产、网络安全事件、网络安全监管业务开展情况等要素，从全生命周期、安全生态、业务联动协同三个维度对防护主体数据进行组织和治理，在此基础上制定完善的算法模型和标签体系，全面、精准、透彻、鲜活的刻画防护主体及其关联主体的全息画像，并结合地理空间数据模型叠加后形成重要单位各类要素的结构、分布地图、关系图谱，投射形成网络空间地理测绘系统基础图层，主要包括地理图层、网络图层、行为主体和业务图层，实现网络安全态势地图展示，定标响应网络安全事件，实现网络安全“挂图指挥”。



1）地理图层

打开页面时默认加载GIS地图，支持鼠标拖动地图和地图缩放，可查看街道、3D、楼宇立体展示。支持地图配置和地图2D/3D切换，包括地图模式配置、画质选择、界面配置，并预留后期可供升级的接口。

地理图层支持将单位数据、单位的历史案（事）件、安全漏洞、实时预警等安全监测模块汇集的安全数据，通过地理位置映射直观展示在地图上，清晰的标识管理对象的物理位置以及网络特征。其中，单位数据包含单位名称、单位类型、单位详情等信息。

发生安全事件的单位：地图上标记为红色点，展示单位名称、未处理的事件数量，点击查看单位基本信息及事件列表。

存在隐患的单位：地图上标记为黄色点，展示单位名称、未处理的隐患数量，点击查看单位基本信息及隐患列表。

有资产的单位：地图上标记为蓝色点，展示单位名称及单位下属的系统、设备、云平台、机房、移动应用等资产统计数据，点击查看单位基本信息及相关资产的信息，系统、设备、云平台、机房、移动应用系统等。如果单位坐标重叠，则合并展示，可在窗口中切换单位，如果一个单位有告警、资产、事件则支持分开切换。

支持在地理图层上搜索单位名称，定位单位位置。

2）网络图层

通过对网络资产的动态测绘与嗅探识别，以及重点单位上报的资产信息，实时在地图上展示资产、事件、隐患信息。该图层不仅包括各单位的活跃IP、端口、协议、应用、设备等全资产信息，也包括历史攻击事件、安全漏洞、实时预警等信息。

以系统角度出发，对重点系统的地理位置分布进行展示。支持大屏下钻到系统档案，包括系统基本信息、归属单位、系统相关人员信息、备案信息、实时安全监测信息、所属运营单位、建设单位、设计单位、系统级别、标签等，根据采集的流量/设备日志、网络应用和行为、数据资产等数据，能够通过具体整体系统数据，了解系统整体运行情况。通过多种形式直观统计展示，包括重点系统量、全部系统量、系统风险变化趋势。支持利用列表中的定位图标快速定位出系统所处地理位置。

以设备角度出发，支持设备打点，点击支持查看设备概览信息，支持对设备进行统计展示，包括设备在线情况、安全专项情况。也支持利用列表中的定位图标快速定位出设备所处地理位置。

3）行为主体

以人员角度出发，支持人员打点和对单位负责人、联系人等相关人员分布展示。支持大屏点击查看人员概览信息，下钻到人员档案，包括人员基本信息、人员标签、网络身份、归属单位信息以及所管理到系统风险信息，并支持人员档案下钻到单位档案或系统档案。

配置对人员进行统计展示等功能，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

配置利用列表中的定位图标快速定位出人员所处地理位置等功能。

4）业务图层

基于上述图层，进一步实现业务挂图，依图开展安全运营、预警通报、事件应急处置等一系列流程化、闭环化应用业务。

a、通报预警挂图

以安全事件、威胁风险通报预警处置的角度出发，针对存在威胁风险隐患，进行预警通报；针对已经发生的安全事件，可发布安全事件通报，要求开展应急响应工作。产生的预警处置数据可实时传输到平台，把握预警处置工作开展情况。

b、应急处置挂图

针对已经发生的紧急安全事件（判断事件后果较为严重），可直接在图中发布应急处置任务，指派相关运营人员赶往事发单位或下发至单位进行处置反馈。支持在屏中发起应急处置任务并通过单位为底座，对单位内接收到的应急处置进行展示，从而及时掌握单位应急处置情况；将实时获取的单位处置及反馈情况在地图上通过标注等方式进行展现，通过改变标注的形态直观体现业务情况或结果。

c、指挥调度挂图

在网络空间地图上下发指挥调度指令，以移动APP消息、短信等形式推送，运营人员可通过移动端查看指令内容。

（12）情报中心

情报是一种基于证据的知识，包含了上下文、机制、指示标记、启示和可行的建议。威胁情报描述了现存的或者是即将出现针对网络资产的威胁，并可以用于通知主体针对相关威胁或危险采取某种响应。高级威胁尤其APT攻击手法隐蔽，危害巨大，主要针对掌握有重要数据和信息的特定人群，攻击一经发生就会导致国家重要价值资产的泄密流失，而且后续定位、追查、定性都会遇到技术难度。高级威胁情报可以对APT攻击事件的定位、发现、定性、溯源提供良好的支撑，可以强化用户对各个重点保护单位的监控力度和防护强度。

情报信息中心业务逻辑如下图所示：



威胁情报获取：本功能提供对威胁情报信息的自行添加或通过Restful API请求数据接口的方式从云端接入第三方威胁情报服务商数据的能力。

威胁情报预处理：威胁情报模块可对采集到情报进行统一格式化、标准化、存储、检索、去重等操作。

威胁情报维护：按照不同的情报来源建立网络安全运行平台本地威胁情报数据库，提供定时更新、离线更新和情报模型更新配置功能，情报库更新后相关的情报模型应自动同步最新的情报信息。实时监控各个情报库中有效情报数量、每日更新数量、命中情报数量、情报更新时间和最近更新状态。

威胁情报关联通报：使用威胁情报碰撞关联，将高危信息对相关单位及网络安全运行平台进行通报。

1）情报获取

情报获取支持云端采集、接口采集和本地累计以及离线导入共4种方式进行威胁情报采集和累计。

a、云端采集

以Restful API请求数据接口的方式从云端接入第三方威胁情报服务商的数据。

b、接口同步

提供丰富的云端采集更新接口，支持第三方商用威胁情报库以及开源的威胁情报库，网络威胁情报包含恶意IP、URL、文件HASH 、Domain、Email等。

c、本地积累

威胁情报模块支持将本地发现的安全事件和恶意IP、域名、文件、钓鱼网站、E-MAIL等事件转化为威胁情报，支持后台自动转化和人工判断转化两种方式。

d、离线导入

支持使用离线威胁情报数据包的方式进行更新。

2）情报处理

对采集到情报进行统一格式化、标准化、存储、检索、去重等操作。数据的归一化操作就是在标准数据元、数据项、数据质量等的要求下，进行各类数据的汇聚与管理操作，经过数据归一化处理后，各类不同的数据源将统一为格式标准、内容一致的数据，为下一步的数据碰撞做准备。

同时，实现情报数据的标记功能，以打标签的方式自动对情报数据的来源、厂商、发现时间、命中结果等，打上相关的厂商标签，为情报数据的运营管理、情报追溯、质量评价提供依据。

3）情报检索

提供威胁情报检索功能，可检索IP、域名、HASH值、邮箱、字符串等，可辅助用户对恶意文件进行样本行为分析、样本同源分析、事件回溯分析、IP&域名信誉判断等。

文件HASH值查询：提供可疑文件的动、静态行为分析；提供文件、IP、域名、威胁事件等关联分析；展示文件的基本信息，如：文件原始名字、文件大小、文件 HASH 等。针对Windows 可执行文件，展示可执行文件PE分析结果。支持文件上传检测。

域名查询：提供域名历史解析信息，包含：WHOIS 信息、DNS 信息、安全情报、相关域名、相关样本、可视分析等功能。

IP查询：提供IP查询功能，包括与该IP相关的DNS 信息、安全情报、相关样本、可视分析等。

邮箱查询：提供邮箱查询你，包括注册域名、安全情报、相关样本、可视分析、网络痕迹等。

字符串查询：字符串查询是指通过查找特定字符串，找出所有包含该字符串的样本。如：研究人员通过分析发现Wannacry勒索病毒会包含字符串“Wannacry”，尝试检索该字符串可发现一批Wannacry勒索病毒。

威胁情报查询：提供威胁信息资讯，威胁情报信息来自互联网收集，偏重各种热点事件。

4）情报共享

提供情报订阅和情报接口共享两种方式。

a、情报订阅

提供订阅威胁情报功能，按照行业、IP、域名、区域等订阅内容，并且支持推送告警通知。

b、情报接口共享

提供通过WEB接口、Syslog、API等方式进行情报分发共享。

失陷资产关联

传统的安全设备由于采用了已有攻击签名特征库检测的方式，可发现攻击过程中的情况或者采用远程检测能够检测发现漏洞或安全事件。然而，实际情况是辖区内存在的大量失陷被控的网络资产，缺乏相应的技术手段可以探测感知，任由资产失陷成为僵尸网络或者爆发更大规模安全事件，比如黑客事件，通常是该系统早已遭受入侵失陷，并被植入后门或木马，在需要的时候触发挂上标语。网络安全运行平台结合情报可发现互联网中出现的威胁数据，与网络资产信息进行关联碰撞，从而发现辖区内资产失陷的情况。

5）高级威胁关联

a、高危攻击关联分析

通过威胁情报中的威胁数据，可以感知辖区的重要资产是否遭受了高威胁的攻击，是否需要进行应急处理等。该部分的攻击威胁数据包括：遭受外部攻击的攻击源分析发现其中的高威胁攻击源与黑客组织；遭受的扫描行为分析发现其中的监管机构扫描与违规授权扫描；本区域内存在的攻击源对外发起了攻击需要进行处置；本区域内存在的扫描源是否为备案的扫描机构。

b、0day漏洞预警监测

当互联网发生0day漏洞，通过第三方专家团队会对0day漏洞进行分析，判断其影响的范围，通过云端大数据快速定位到可能受影响的网站和系统，再根据精准的POC策略检测，对用户进行精准的定位是否受0day影响，然后由大数据预警引擎对受影响的用户进行定向通报，以督促受影响单位进行主动防御，摆脱以往的“广播式”预警容易被忽略等困境，实现可落地的预警与风险整改督促。

6）历史攻击回溯

把威胁情报数据的恶意IP与历史流量数据，各类历史日志中的源IP进行比对，发现命中恶意IP而当时未告警的历史数据或虽然告警但未做处理的数据，进行回溯分析源IP行为，判断当时的攻击可能性，必要时进行补救处理。统计恶意IP中在历史流量或日志中经常出现的IP地址，进行重点关注或做黑名单处理。

（13）分析研判

1）订阅规则

通过订阅规则将安全事件通过预警、工单、邮件、短信、钉钉等方式推送给用户，或直接联动防火墙进行威胁阻断，当安全告警满足订阅规则时，自动触发通知或联动，帮助用户实时关注平台告警情况并及时阻断威胁。

对订阅记录进行统一管理，支持多维度记录查询，并支持对订阅规则相关的安全告警进行钻取分析。

2）Sherlock威胁溯源

威胁溯源Sherlock旨在确定攻击事件后，回溯所有攻击相关的网络数据包，对系统近期的所有行为进行串联，确定攻击事件的整个事件周期，展示整个攻击事件的所有攻击路径。以互访流量关系为纽带，将攻击者的所有攻击动作列举出来。通过安全设备的告警日志、系统设备日志与资产画像对比分析，确定遭受攻击的服务器。通过分析这些被攻击的设备的系统日志，挖掘出攻击者的攻击入口。还原出攻击者在不同服务器之间的攻击路径。

Sherlock以资产为核心视角，直观了解自身网络环境中存在风险资产，感知通过攻击链形式展示，剖析从扫描探查阶段到资产破坏阶段资产失陷过程。感知失陷、异常资产，从海量的日志中提取有价值的资产溯源路线。平台简单易用，支持一键全方面钻取，降低运维成本，提高运维效率。根据资产安全告警分析所处安全状态，平台会对资产进行状态标记，帮助用户清晰了解全局资产状态。

3）安全模型自动化编排

基于安全分析能力和应用能力，通过剧本编排，对复杂的分析、处置流程进行集成整合，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。

剧本以原始数据或安全事件作为输入，结合统计模型、情报模型、关联模型、规则模型进行威胁分析，并实现联动阻断、通报预警、人工查验等响应动作。

a、编排要素

数据源：支持将原始日志、异常记录、安全告警作为剧本的数据源输入。

分析组件：支持添加统计指标、统计模型、情报模型、关联模型和规则模型。

处置响应：支持添加联动防火墙及EDR设备，可对分析出的安全威胁直接发布预警或下发通报，此外，支持在必要位置添加人工查验模块，进行人工干预分析，将人添加到整个安全事件处理的闭环中。

b、剧本管理

提供可视化、简单易用的剧本编辑器，并对创建剧本进行统一管理。具体设计包括以下功能。

可视化编排。构建基于WEB的交互式剧本编排图形化可视界面，支持以拖拽方式构建剧本，简化剧本创建流程，提升剧本创建操作的易用性和工作效率。

剧本管理。支持对已创建剧本进行检索，检索条件包括剧本名称、剧本状态、标签等；支持对剧本进行编辑、删除等操作；支持根据剧本执行情况，如误报率或重复告警等，对剧本进行开启和关闭。

c、任务管理

提供任务看板，对执行的自动化任务进行监控。具体设计包含如下功能。

支持执行任务总体情况概览，统计呈现任务总数，并可视化呈现已完成、进行中、已取消的任务占比以及任务变化趋势。

统计呈现任务平均处理时间以及为用户节省的总时间，直观体现SOAR价值。

支持根据剧本名称、任务进度、时间维度等进行任务查询。

支持对剧本各部分执行任务详情进行钻取分析。

（14）安全专项

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安全专项分析，对可能受到影响的受影响的资产、行业、受影响的重要单位进行分析，给各区域监管单位提供相关安全威胁隐患的数据。

1）漏洞预警

对重要产品、软件、系统的安全漏洞进行实时跟踪，经专家分析研判后为客户提供权威、及时、准确漏洞预警。不仅能够快速掌握最新漏洞动态。

2）情报资讯

全网安全动态分析，分析国内外攻防的安全动态资讯：APT攻击、勒索攻击、挖矿、黑灰产、暗链等信息，轻松掌握当下热点技术方向及安全动态。为网用户的络安全规划与建设提供高质量的参考材料。

（15）威胁情报模块

平台具备云端威胁情报订阅模块：内置威胁情报离线库并支持更新。此外平台支持采用情报数据进行实时检测防御。

1）在线查询与溯源

云端提供对IoC威胁类型、多源情报、WHOIS、开放端口、SSL证书等多维度的溯源分析。

2）云端服务

支持订阅高级威胁分析情报，云端提供最新APT入侵、0day漏洞预警、病毒变种情况等分析报告订阅。

（16）重大安保

重大安保中心主要用于在重要会议或重大活动期间，全方位全天候掌握与活动相关的单位、系统和网站安全状况，及时通报预警网络安全隐患，高效处置网络安全事件。实现在安保时期重点对象的监控、安保人员管控、调度指挥、应急处置以及活动情况总结归档。对重大活动期间各职能部门、重要行业部门、技术支持单位进行综合指挥，协同多家技术支撑单位、第三方安全厂商、网络安全专家以及其他职能部门保障重大活动期间的网络安全。



指挥调度中心以大数据基础设施中心、威胁分析研判中心为基础，构建安保指挥业务应用中心，其中大数据基础设施中心完成网络安全运行平台的基础设施、探针设备和大数据的采集接入，威胁分析研判中心主要针对网络威胁通过大数据智能分析加人工专业判别的组合方式完成威胁的定性分析，安保协调指挥业务应用主要实现重大活动网络安全保障协同指挥的相关业务流程能够支持单位部门开展安全风险管理和安保制度、安保值守、安保检查等复杂工作流程。

1）活动管理

安保活动管理是针对多个活动（包含历史活动）的统一管理模块。支持在该模块新建活动、编辑活动摸底、临战、备战、决战阶段的时间进度，支持下钻到具体某个活动，查看活动详情，同时支持结束、归档活动。

系统支持全局整体的活动管理能力，同时针对具体的单次活动提供详细的配置管理，包括各个模块可使用的标签、安保值守范围、检查/处置业务审批反馈等。

2）系统配置

为运维管理用户提供安保指挥系统的系统配置页面，包括系统配置、角色管理、系统用户、单位用户、日志审计、许可管理。

当安保管理人员在安保期间，点击进入某个活动时，就可以进入作战台，作战台页面划分为四个模块：信息公开、待办工作/跟进工作、快捷方式、个人信息。通过作战台即可对活动期间的各个活动的阶段的信息公告、组织架构、应急预案、代办工作、安全支撑单位等所有跟安保相关资源和信息，并通过点击对应的按钮处理安保相关工作和跟进未完成的工作，并通过快捷方式快速添加需要直接访问的业务模块并进入该业务模块进行相关安保工作编排。

3）基础信息

基础信息管理是支持安保组维护该次安保活动所需要基础信息的模块，包含安保对象管理（单位、系统）、支撑单位管理、人员管理、小组管理、驻点管理、设备管理、车辆管理等子模块。

安保单位，即安保活动重点保障的单位，系统提供新增、查看、编辑、删除、查询统计功能。

安保系统，即安保活动重点保障的安保系统，如电力、广播等重点行业的系统，系统提供新增、查看、编辑、删除、查询统计功能。

支撑单位管理，即协助安保组完成该次安保活动的单位，系统提供新增、查看、编辑、删除、查询统计功能。

人员管理，安保组线下采集，进行录入，支持指定某人为单位的联系人，该联系人具备新增联系人的权限，新增后需要安保组的人员审批。

小组管理，从安保人员中选择各个人员建立成不同的安保小组，为后续的不同的业务开展服务将各个单位的人员根据岗位、技能等特点划分为不同的小组，安保小组可以通过小组名称、组长姓名、组长联系方式、小组标签、安保人员选择。

可以按照人员姓名、归属单位、人员标签进行查询人员数据。供安保组在安保活动中进行调度，系统提供新增、查看、编辑、删除、查询统计功能。

驻点管理，即在安保活动期间，对于部分十分重要的场所，支持安保组设置驻点，进行全天候值守，对突发事件做应急处置。

设备管理，提供的针对该活动的安保设备的基本运维情况的展示即对该次安保活动使用的设备进行统一管理，在该页面进行包括设备数量、在线离线情况，可以对设备进行新增、导入和删除等操作，每个设备的在线情况，CPU利用率和负债率、内存使用量、磁盘占用率的直观展示统计。

车辆管理，即针对该次安保活动可调度的车辆进行管理、维护，提供了包括新增、查看、编辑、删除、启停用和车辆调配等具体管理项，可操作的字段包括车牌号、颜色、车品牌、车辆类型等具体信息，车辆状态提供可用、停用、使用中具体使用情况标记，当状态为使用中时需要展示是哪个人员在使用。系统具备控制车辆的启用/停用状态，状态为停用时，该车辆无法被调配。

4）安保制度

安保制度是支持安保组维护该次安保活动开展所需制度等信息的模块，包含安保方案、安保制度、组织架构、应急预案、信息公告等子模块。

安保方案支持安保组维护该次活动的安保方案信息同上传方案附件文档的方式进行详细的方案规划。

安保制度，支持安保组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。

组织架构，在安保期间对安保活动的组织架构采用可视化的手段进行展示、维护，支持安保组自定义维护该次安保活动的组织架构信息。

应急预案，具备安保组制定该次安保活动发生各类事件时的应急预案，并在事件发生时启用对应的应急预案，应急预案支持针对预先定义的预案名称、预案等级（1-4类）、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。

信息公告，提供以安保组为单位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。

5）威胁管理

威胁管理子模块直观地展现辖区内单位的安全态势和潜在风险，辅助管理工作人员全面掌控重保期间重保对象的安全动态。

6）通报处置

通报处置是支持安保组在安保活动期间，将发现的各个重点单位的隐患、事件通报给对应的单位联络人，系统提供通报统计、通报发布和通报跟进三个子模块，实现事前预防、事中处置目标的业务模块。

通报处置业务的具体业务流程为，当某单位发生安全隐患、安全事件后，支持安保组在威胁管理发起通报任务，通报给对应的单位；对应的单位联络人接收到通报后，进行处置，处置完成后支持单位联络人在系统中反馈处置情况，经安保组复核完成后，该通报即视为结束。

通报统计以接收的事件、隐患数据为数据源针对事件、隐患和通过业务进行统计展示。

通报发布模块将各个数据来源的数据，统一在该模块进行管理，并在该模块发起通报、处置业务。

通报跟进模块支持用户通过事件管理功能对通报任务进行状态跟进，数据来源于通过事件管理处理的安全事件、隐患和现场建成的结果数据经过威胁分析研判后确认审批后的威胁数据发起的通报业务。

7）安保检查

安保检查提供针对辖区内单位及系统开展安全检查和隐患排查的能力。主要包含检查统计、检查任务管理功能。

检查任务管理支持安保组下发检查任务至安保检查小组，安保检查小组前往现场检查，检查完毕后出具整改通知书并将检查结果填报到网络安全运行平台。待单位完成整改后，安保检查小组接收单位的整改通知书并在网络安全运行平台上完成闭环管理。

检查统计支持统计安保组下发的每一轮检查任务信息，统计每一轮检查中，每家单位/系统的安全隐患数，直观查看每一轮的检查结果，每一轮的检查隐患数量，以及上升下降趋势。

系统为用户提供了直观查看每一轮检查任务的宏观情况，支持查看、导出每个单位、每一轮的检查结果情况。

系统在备战阶段进行安全检查并对检查任务和结果进行统计，统计信息包括数值统计、检查任务趋势统计、隐患趋势统计和每个检查统计的明细信息展示。

8）安保值守

安保值守是在安保活动进入临战阶段后日常的主要工作，安保值守模块可以对安保组在安保期间对各个驻点开展巡检工作，了解各个驻点实时安全情况，提供日历、今日排班情况和今日值守情况便于管理人员对整体安保工作的各组工作情况进行查看和管理的模块，同时安保值守模块提供的全局安保支持统览和针对具体安保活动的巡检工作管理。

安保值守模块区分安保组和安保驻点两个视角。安保驻点端在安保、驻点小组视角，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，并支持安保驻点在活动期间通过移动端（钉钉网络安全运行平台上定制专用功能模块）开展签到/签退、报平安等工作。

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。

9）指挥调度

指挥调度系统基于GIS系统的可视化特性，同业务系统进行数据对接，通过直观图形化点击拖拽等方式支撑安保组在安保活动期间的活动监控和指挥调度两个应用场景。其中活动监控是通过可视化技术直观展示活动的实时情况，包含：当前活动的进度，活动的资源、活动的威胁情况、活动的值守情况、活动的各项业务开展情况等信息。指挥调度将活动要素在地图上展示，在发生突发事件时，支持指挥中心“挂图作战”，依据地图展示的资源来对事件的处置。

10）活动监控

支持用户通过监控大屏了解到整个活动的进度和情况。通过可视化技术将安保指挥调度的相关全部要素以图形可视的方式展现在用户面前，包含当前活动的进度、活动的资源、活动的威胁情况、活动的值守情况、活动的各项业务开展情况等信息的实时数据展示，以及隐患类数据信息、事件类数据信息和攻击类数据信息，并支持近两日相关隐患的变更对比数据等。

安保概况从组织架构、信息公告、安保单位、安保系统、安保支撑单位、安保人员、安保小组、安保驻点、安保设备、安保车辆、安保应急预案、安保制度等统计维度进行全局展示。

值守情况从当天值守情况和整个活动的值守情况两个维度进行展示，当天维度，可以查看当天的驻点排班情况看，当天各个班次的签到、报平安等统计情况展示。

威胁信息从隐患、攻击、事件等角度进行统计分析，支持以累计数量、类型分布、等级分布、今日新增、今日新增趋势、累计趋势、通报状态等维度实现威胁信息的统计展示。

安保检查、通报处置和安保指令支持当日和累计2个维度进行统计展示。

指挥调度将活动要素通过GIS技术的对接在地图上直观展示，在发生突发事件时，支持指挥中心“挂图作战”，依据地图展示的资源来对事件的处置。采用可视化地图技术实现“图上统筹”，将安保活动的举办地采用3D地图的形式展示，并在3D地图上采用直观、区分度强的标记展示不同的单位、系统、小组管理、安保驻点等地图信息。当发生安全事件时，直接在地图上发起通报处置工作，直接通报到对应单位。并支持安保组对直接下发调度指令给安保驻点、小组管理，安保组主动下发调度任务，前线安保小组人员通过移动端APP实时接收指令信息，完成安保组下发的调度任务，完成调度工作主要提供的场景如下。

场景一：

检查视图，查看安保期间单位的检查情况通过在地图上点击重点单位或驻点小组能够快速下发检查任务，在建立检查任务时，支持过滤未检查的单位。

场景二：

通报视图，通过地图上以不同的醒目标识，表达目标状态查看当前的通报情况。

场景三：

值守视图，通过地图上可以查看异常驻点情况，指挥部对应异常驻点下发指令，了解异常情况。

场景四：

当驻点上报事件时，支持指挥部下发调度指令，调度其他驻点协助该上报事件的驻点。

场景五：

调度视图，可以查看当前在执行调度的单位、驻点的基础、检查、威胁、通报、值守的相关信息，在地图上通过发布指令实现指挥调度。

（17）考核评价

考核评价中心协助用户构建常态化网络安全工作情况考核和日常考核的工作机制，针对不同被监管对象建立对应的网络安全检查指标库，实现管理统计、日常考核、综治考核、技术支撑单位考核等功能，并按不同时间周期提供考核报告，达到以查代促、以查促改、以查促管、以查促防，有效推动各重点单位落实网络安全建设工作的目的。

1）管理统计

管理统计对考核评价子系统中整体考核情况进行统计分析，让使用者快速了解当前管理情况，主要包括数据报送情况、综治考核情况、考核报告三个部分。

数据报送情况：数据报送情况是对技术支撑单位提供的数据量、数据质量进行综合统计，数据报送主要类型有资产数据、漏洞数据、事件数据、攻击威胁数据。

综治考核情况：对综治考核情况进行统计，按照被监管单位考核、技术支撑单位考核、下级部门考核三块。考核默认显示最近一次的综治考核结果，如有历年历史数据，则可按年切换查看历史数据。

考核报告：考核报告分为月报、季报、半年报、年报四种类型，分别描述网络安全工作的管理情况，从检查情况、自检情况、安全情况、支撑单位工作情况、数据质量情况等维度由系统根据后台数据自动生成。

2）日常考核

实现网络安全管理工作考核，考评周期可按周、月等，考核内容可动态编辑调整。有别于综治考核，综治考核为一年一次，有严格的计分标准，安全评价中则是常态化的安全监控，主要以发现问题、是否安全为角度出发。日常考核的数据纳入年底综合考核的计算中。

3）综治考核

实现网络安全管理工作的综合考核，每自然年（1月到12月）作为一个评比周期，考核内容可动态编辑调整。

4）考核规则

针对被监管单位、行业主管单位、下级机关的网络安全管理工作制定定制化的考核规则，可从组织管理、安全防护、安全监测、安全成效等维度制定考核规则。

5）支撑单位考核

针对技术支撑单位以及情报数据来源厂商进行考核。考核分为两个部分，一部分是对技术支撑单位工作的支撑情况的考核，另一个部分是对第三方威胁情报厂商提供的情报数据质量的考评。支撑单位的考核按年度统计，每自然年（1月到12月）作为一个评比周期。

a、技术支撑单位考核

通过五星考评机制进行考评，得分在支撑单位考核中直接给出，考核内容包括但不限于：

|  |  |
| --- | --- |
| 考核维度 | 考核内容 |
| 数据支撑 | 每月资产档案新增、补全的数据量，准确率每月安全事件、隐患上报的数据量，准确率每月威胁情报提供的数据量，情报碰撞率 |
| 专家支撑 | 日常分析研判发现的事件个数日常验证的漏洞个数重大活动期间专家的服务时长 |
| 服务支撑 | 资产普查工作服务支持次数检查调查工作服务支持次数 |
| 人才培养 | 每月组织安全课程培训次数每年组织安全攻防演练次数每年发表安全相关研究成果篇数 |

b、数据来源厂商考核

数据质量评分：数据质量评分部分由系统根据后台数据的数据量、数据质量自动计算得出。数据质量从漏洞数据、事件数据、攻击威胁数据、资产数据四个 维度进行评价。

（18）流量监测模块

通过部署流量采集探针，采集核心交换机上的流量进行威胁分析，发现弱点扫描、命令执行、注入攻击、跨站脚本、信息泄露、邮件钓鱼等相关风险行为，并及时做到告警现场相关专家确认后沟通局方人员确认是否要做封堵以及以何种方式去做封堵。

1）资产管理

通过对流量中的协议、应用、IP地址、端口、MAC地址等进行统计分析，对网络资产进行主动发现并快速识别未登记资产，可基于业务服务器、应用软件、资产健康度、资产活跃程度等维度对内部资产进行梳理，检查资产端口暴露情况，支持发现非标端口提供服务的情况，帮助用户全面、精准地梳理出暴露在互联网上的IT资产，可深入查看资产的类别、应用、服务、操作系统等详细情况。此外，平台支持自定义资产分组，可配置多层级资产组织和网段，并对组织和网段打多维度标签，便于用户自定义内部资产属性，同时也支持资产/资产分组的风险告警发现、关联和检索。

2）流量审计

全面审计网络流量协议的访问行为，通过审计信息为网络信息化与安全化管理提供重要依据，产品基于丰富的特征库对全流量行为审计并匹配，包括协议解析、风险行为等，支持全网双向流量行为的审计。

3）协议内容识别

经过数据流特征匹配和应用协议行为构造，对协议内容进行分析。结合数据包字段、时间窗口、协议特征对上下行流量行为匹配，识别URL行为、文件类型、流量大小、构成及流向等，根据匹配度进行流量分类及汇总统计。

4）Web威胁深度检测

通过对Web流量和应用进行深度检测，提供全面的入侵检测能力，能够在攻击到达Web服务器之前进行检测，并进行实时的攻击预警。

解码所有进入的请求，检查这些请求是否合法或合乎规定，仅允许格式正确或遵从RFC的请求通过；已知的恶意请求将被阻断，非法植入到Header、Form和URL中的脚本将被阻止。

执行Web地址翻译、请求限制、URL格式定义及Cookie安全检查。

基于语义语法机器学习，分析流量中的攻击特征，支持业务模块判断，提升语义分析的准确率

对加密报文解密并检测，可发现冰蝎、哥斯拉或其他变种wehshell攻击流量

通过与WAF联动防护已知或未知攻击，阻止跨站点脚本、缓冲区溢出、恶意浏览、SQL注入等攻击。

5）邮件威胁深度检测

对各种基于邮件的APT攻击行为进行检测，支持各种基于Webmail的漏洞攻击检测和基于邮件附件的恶意文件传输行为检测，同时还具备基于邮件头欺骗、发件人欺骗、恶意链接等邮件欺骗行为检测。支持基于链接的钓鱼邮件检测：获取邮件中的链接并通过内置白名单过滤，结合分析邮件头和邮件内容的相关高危特征，生成钓鱼邮件的特征向量，并通过机器学习挖掘特征中的耦合性，检测得到待检测邮件是否为钓鱼邮件，确保发现所有基于邮件的APT攻击行为。

6）病毒木马深度检测

对应用协议解析，在协议中分离文件，通过对病毒木马进行扫描，快速发现各种已知特征的恶意文件攻击行为。

集成了反病毒引擎，可有效发现网络中存在的僵木蠕，识别准确率高达99%，包含各种CVE漏洞利用、病毒感染、恶意代码传播、远控工具和恶意回连行为，分析网络中主机的威胁趋势，感知主机的威胁指数，进一步发现各种恶意样本的传播规律，预警网络安全状况。

7）异常流量深度检测

基于对检测对象的流量特征进行多维度监控统计，依据正常的流量特征建立模型，分析检测对象多个异常参数的关联关系，判断是否有异常行为产生。能够有效检测出DGA域名访问、远程控制行为、挖矿行为、漏洞利用、暴力破解、隐蔽信道传输及弱口令利用等异常流量。

APT攻击通常会结合人工渗透攻击，在人工渗透攻击中经常使用扫描或病毒扩散的过程。这些过程中，通常会产生大量的恶意流量。利用这些恶意流量特征，能检测攻击行为。

目前检测基于以下多个维度：

基于时间检测；

基于IP检测；

基于端口检测；

基于协议检测；

基于DNS异常检测；

基于木马回连行为分析；

基于隧道通信流量检测。

8）自定义检测分析

自定义检测分析模块，可通过用户自定义配置的内容，发现流量中的邮件敏感信息传输、异常登录、违规连接、网络会话异常、周期类异常攻击、特征类异常攻击行为。

邮件敏感信息传输：对流量中的登入位置、通信事件、邮箱账户、关键字等内容进行综合分析，发现邮件内容传递敏感信息、发现异地登录收发邮件、发现特殊时间段收发邮件、发现特殊发件人的邮件，或上述组合特征的邮件投递或接收行为。

异常登录：对流量中的登录协议、账户、服务器、通信时间等内容进行综合分析，发现异地登录、发现特殊时间段的登录、发现特定账号的登录行为、发现特定时间或地理位置登录指定业务服务器，或上述组合特征的登录行为。

违规连接：对流量中的外连位置、通信时间、受控网段等内容进行综合分析，发现与指定地理位置的IP有通信行为、在指定时间段有通信行为，或上述组合特征的流量发现。

网络流量会话异常：对流量中的会话组成和连接状态进行综合分析，发现网络传输异常、拥堵等网络异常状况。

周期类异常攻击：可对流量方向、协议、周期等内容进行自定义配置，发现流量中功能的慢速爆破、分布式拒绝服务器攻击、多频访问IP/域名的异常行为。

特征类异常攻击：可对流量方向、协议、区域、值等内容进行自定义配置，发现流量中的异常行为。

9）智能报表

提供综合威胁分析、主机威胁分析、文件威胁分析、外部威胁分析等多个智能报表，方便快速总览网络威胁情况，提供全方位多视角分析报告，有效替代人工威胁分析。

10）综合分析

综合分析模块基于海量数据，采取多维度关联分析、行为关联分析、日志报表综合分析，提供更全面的分析能力，发现更为隐蔽的APT攻击行为，感知威胁态势。

通过对多个攻击行为的关联分析，分析攻击之间的关联性，还原真实攻击路线，并以直观的形式展示分析。

基于海量数据的分析模型，提取多种类型的攻击行为，挖掘攻击规律。

基于攻击路线的关联分析，可快速识别非持续性的威胁，提取真正的APT攻击。

通过一段时间对访问行为进行统计分析，发现其访问频度的异常行为，如：异常非法访问、通过SQL注入获取数据、扫描、构造各种参数值进行探测等。

基于URL异常、返回码异常、返回数据异常等综合分析访问行为，判断是否存在恶意攻击行为。

通过对请求URL进行统计分析，发现其中的异常，如：没有带referrer的URL进行逆序排列，频繁访问特定页面且时间非常集中。

从攻击者、受害者视角统计数据，通过聚类算法整理数据，使得数据清晰可见。

11）云端高级分析

云端可提供更为深层的威胁分析服务、安全预警服务和情报共享服务，依托于云端的海量数据、高级的机器学习和大数据分析能力，可及时共享最新的安全威胁情报，提供更为精准的威胁分析能力，用户也可直接访问云端，上传、查询和确认样本的分析结果，感知最新的安全态势。

12）深度协议解析

平台采集的流量经过流量分析引擎，解析IP报文字段及流特征信息，分析应用层协议，确定流量中存在应用。通过多维度对协议进行协议解析：

a、基于数据包字段解析

源IP地址、目的IP地址、源MAC地址、目的MAC地址、源端口、目的端口、协议号、报文长度、包长度等。

b、基于时间窗口解析

流量最初发生时间和结束时间、流量持续时间。

c、基于协议行为特征解析

根据每种协议自身行为特征和行为为轨迹进行协议解析。

13）基于攻击链的关联分析

通过对多个攻击行为的关联分析，分析攻击之间的关联性，还原真实攻击路线，并以直观的形式展示分析。

基于海量数据的分析模型，提取多种类型的攻击行为，挖掘攻击规律。

基于攻击路线的关联分析，可快速识别非持续性的威胁，提取真正的APT攻击。

通过一段时间对访问行为进行统计分析，发现其访问频度的异常行为，如：异常非法访问、通过SQL注入获取数据、扫描、构造各种参数值进行探测等。

基于URL异常、返回码异常、返回数据异常等综合分析访问行为，判断是否存在恶意攻击行为。

通过对请求URL进行统计分析，发现其中的异常，如：没有带referrer的URL进行逆序排列，频繁访问特定页面且时间非常集中。

（19）硬件支撑配置

网络安全运行平台运行需配置2台平台服务器，用于平台部署。

平台服务器主要技术参数要求如下：

不低于鲲鹏2\*Kunpeng920-24核，内存不少于256G，不少于2块960G SSD固态硬盘（组成Raid 1），其他硬盘不少于48T，网口不少于4个千兆电口，不少于2个GE光接口，不少于2个万兆光接口，不少于1+1热插拔冗余电源，国产化操作系统，具备配置网络安全平台部署所需的一切软件、硬件配件等。

**3.网络安全配套服务**

（1）云端安全实时监测服务

1）服务内容

提供网络信息安全技术专家服务，提供7\*24小时实时威胁检测和响应服务，具备一线安全分析工程师提供实时检测分析、快速响应、事件管理的能力，具备二线安全运营经理提供专业技术支持、过程质量把关、快速审核的能力，具备三线安全专家提供复杂技术研判指导、制定最佳方案、组织事件溯源、复盘工作的能力。

2）服务交付

提供安全监测服务日、周、月报告，季度汇报总结工作报告。

（2）漏洞扫描服务

1）服务内容

现场驻场服务人员或相关技术人员通过定期使用漏洞扫描工具针对业主方指定的主机漏洞、Web应用扫描、指定网站所有的文件进行安全扫描，人工验证扫描结果，扫描内容包括主机层和Web应用层漏洞，涉及对象应包括网络设备、安全设备、系统平台、数据库系统、Web系统等，并在扫描之后，将扫描系统获得的报告汇集成为一个当前网络系统的系统脆弱性报告。

2）服务交付

漏洞检查结束后，相关人员根据检查结果输出《XX年XX月漏洞扫描报告》。

（3）基线检查服务

1）服务内容

针对操作系统、数据库、网络设备等配置合规性进行检查，评估发现潜在风险点。每年提供4次基线检查服务。

2）服务流程

a、Windows操作系统安全配置核查内容

审核Windows类操作系统服务器的补丁情况、帐号和口令管理、共享资源安全、注册表、系统端口、服务安全、审计安全、网络安全、防病毒安全情况。

b、Linux操作系统安全配置核查内容

检查服务器Linux类操作系统的登录要求和帐号口令管理、审计安全检测、文件系统检测、系统服务开发情况、系统信息情况。安全工程师将根据制定的安全基线准则，对审核结果进行分析判断，并给出整改建议。

c、数据库安全配置核查内容

审核数据库的帐号和口令管理、日志审计、权限管理等安全情况。安全工程师将根据制定的安全基线准则，对审核结果进行分析判断，并给出整改建议。

d、网络设备安全策略核查内容

检查网络设备的服务开放情况；我公司的安全工程师将参照安全基线准则，对检查结果进行分析判断，并给出整改建议。

e、安全设备策略核查内容

审核安全设备的登录要求和帐号口令管理策略、管理协议设置和日志审计策略、访问控制策略和其他安全要求。安全工程师将根据制定的安全基线准则，对审核结果进行分析判断，并给出整改建议。

f、应用中间件安全配置核查内容

审核应用中间件的系统安全、帐户和口令管理、审计管理、文件系统权限控制等安全情况。安全工程师将根据制定的安全基线准则，对审核结果进行分析判断，并给出整改建议。

g、制定基线检查策略

针对本次检查具体对象，按版本、类型，形成具体检查策略。调整检查工具内的检查配置基线，约定检查范围及负责复核等工作，形成本次检查的技术规范。

h、实施基线检查

通过离线脚本在被核查主机上运行，得出结果xml文件，导回基线平台分析，得出基线报告。

（4）渗透测shi服务

1）服务内容

渗透测shi是通过模拟黑客攻击的手法对某个特定网络系统进行测shi，以期发现和挖掘网络系统中存在的漏洞。渗透测shi不同于漏洞扫描等安全评估服务，它是遵从黑客通用的攻击流程和路线，利用多种手段对网络系统进行侵略性测shi，而漏洞扫描只会以一种非侵略性的方式，仔细地定位和量化系统的所有漏洞。

每年提供6个系统渗透测shi服务。

2）服务流程

渗透测shi是通过模拟黑客攻击的手法对余姚市电子政务外网网络的信息系统进行测shi，遵从黑客通用的攻击流程和路线，渗透测shi的技术流程如下图所示：



（5）风险隐患与事件通报服务

1）服务内容

常态化提供风险隐患和事件通报服务。

现场驻场服务人员利用网安运营平台能力发现安全风险隐患后，向存在风险隐患的系统责任单位进行安全通报，将安全风险隐患问题进行统一梳理下发，帮助业主方实现安全风险隐患的统一安全管理。

2）服务交付

现场驻场人员定期将风险隐患和事件通报进行整理，最终输出《XX年XX季度安全通报记录》。

（6）安全检查服务

1）服务内容

针对国家、省市下发的相关考核与监督检查要求，提供技术人员配合业主方及相关单位开展自身单位的安全自查工作满足相关考核要求。

在分析阶段完成之后，风险评估项目组将根据风险分析的结果，结合国家有关的法律、法规，总结出当前的安全需求。根据安全需求的轻重缓急以及相关标准和电子政务保障框架，制定出适合的风险处置方案。

2）服务交付

安全检查完成后，相关人员协助业主方及相关单位输出《XX单位安全自查报告》。

（7）安全工作报告

1）服务内容

现场驻场服务人员每月度对发现的安全问题与处置情况进行综合汇总，形成安全态势分析与工作报告。

2）服务交付

现场驻场服务人员输出《XX年XX月安全工作报告》，呈交单位领导后进行汇报。并针对季度的安全情况进行总结形成季度报告，输出《XX年XX季度安全工作报告》。

（8）运营流程优化服务

1）服务内容

针对已有安全运营流程或制度，从可行性、落地性和规范性上进行相应评估，形成余姚市具备特色、具备落地性的安全通报流程和制度。、

2）服务交付

驻场人员协助业主方优化《安全事件处置流程》《安全运营流程》，定期形成相关流程并落实到实际运营流程中。

（9）运营文件编制服务

1）服务内容

常态化安全检查期间，对网络安全专项检查通知文件进行编制，整合、沉淀相应模板文件材料，作为安全监管平台中的知识库，供相关单位或运营人员参考，针对相关检查可以快捷化、规范化下发相关检查材料。

2）服务交付

相关人员配合业主方根据在现有的管理组织架构和安全管理制度要求上进一步确定安全运营内容和职责，输出符合余姚市安全运营体系的网络安全专项检查模板文件和相关规范化材料。

（10）资产梳理服务

1）服务内容

定期提供资产梳理服务，常态化提供资产管理服务，对资产信息库进行常态化管理。

现场驻场服务人员定期针对余姚市政务外网进行定期资产梳理，形成资产信息库，帮助业主方做好政务外网单位资产归属清单，在识别出信息资产后，需要对资产进行风险分析并量化。资产量化分析的过程也就是对资产进行影响性分析的过程。关键资产在遭受泄密、中断、损害等破坏时对系统所承载的业务系统所产生的影响，这一后果可能会危及信息系统并使其丧失机密性、完整性、可用性，最终还会造成其他破坏。

2）服务交付

驻场人员在梳理完成后，输出《电子政务网资产清单》、《余姚市互联网网站资产清单》等。在资产识别的基础上，进一步分析被评估信息系统及其关键资产在遭受泄密、中断、损害等破坏时对系统所承载的业务系统所产生的影响，并进行赋值量化。从而为最后综合风险分析提供参考数据。

（11）策略调优服务

1）服务内容

针对已有网络安全运营平台、智能编排与响应系统、防火墙、流量探针等已有设备以及本期新建设的相关设备进行策略调优，例如进行白名单、黑名单、设备联动、模型优化、规则优化等设备策略的调优，保障相关安全能力有效落地。

2）服务交付

驻场人员在进行设备策略调优后，为保障后续正常运维，需要输出《设备策略调优配置表》。

（12）重要时期安全保障服务

1）服务内容

针对春节、国庆等重要时期提供网络安全高级专家现场保障服务，服务期间保障服务专家利用人工结合工具等方式对指定的单位信息系统、网站、服务器等资产进行实时监测，及时处理发现的系统安全事件。同时对安全威胁及事件进行取证溯源，并对内部安全设备策略进行配置优化，帮助用户建立完善的网络安全保障机制。

协助开展重要时期保障服务，实现：

a、提升安全防护能力

在前期开展安全检查工作，尽可能多的发现高风险、大问题，全面提升安全对抗能力。极大降低安全事件发现的几率。

b、提升安全保障能力

根据业主方需求提供5\*8或7\*24小时的安全专家运维支撑服务，在服务过程中遇到的任何问题。针对后台大量的日志记录，提炼出安全预警、安全漏洞和攻击态势等信息，并对发现的可疑情况和网络攻击行为及时上报，与业主方相关值班人员联系，并协助进行事件处理。

c、保障业务连续性

基于前期的安全检查与协助加固，配合安全防护设备，可全方位的安全防护和网站监控，能有效保障网站的业务连续性，降低了基于各种攻击造成的安全事件导致的服务中断概率，有效提高网站可用性。

2）服务交付

结合业主方现有技术资源及能力输出重要时期安全保障方案，由值守人员配合工具平台整体汇总输出保障期间安全工作情况，重保结束后结合重保期间工作情况进行总结提炼。在重要保障期间输出：《重要时期安全保障方案》、《重要时期安全保障日报》、《重要时期保障总结》。

（13）安全加固服务

1）服务内容

现场驻场服务人员利用网安运营平台能力，对业主方指定的业务系统，针对漏洞扫描、基线核查、安全监管监测、安全运维过程当中发现的安全问题提供处理建议，指导业务系统的漏洞修复，并协助完成服务器、网络设备、安全设备等的安全加固，通过优化安全配置，增强重要信息系统抵抗风险的能力，以提高整个系统安全性。

2）服务交付

汇总输出余姚各单位信息系统安全检查情况，包括漏洞、基线、策略等安全风险情况，并提出安全整改加固建议。并输出《安全监管监测风险整改建议记录》。

（14）宣传教育及培训服务

对业主方工作人员，从数据安全法律法规、政策制度、技术普及、内部管理等视角进行不定期的意识培训服务，提高组织内部整体安全意识及水平。全年开展不少于2次数据安全培训，包括信息安全方面培训、人员安全意识培训、运维操作安全技能等宣传培训活动。

**（三）国产化软件采购**

本项目数据安全服务涉及到的软件拟部署在宁波市政务外网信创云。

由于宁波市信创云是基于国产化环境，但不提供国产化软件，故本项目需新增国产化数据库软件1套、国产化应用中间件1套。国产化操作系统可利旧使用，无需在本项目中进行购置。

**1.国产化服务器操作系统**

国产化服务器操作系统突出高安全性、高可用性、实时性、兼容性等关键应用指标；兼容主流CPU、整机、存储、数据库、中间件等。

**2.国产化数据库软件**

国产数据库软件具备数据存储、访问控制、身份鉴别、安全审计和数据备份恢复等功能。国产数据库部署在服务器，以后台服务形式运行，数据库管理员及用户在管理主机上通过图形化管理工具或命令行工具，可实现对数据对象（表、视图、约束、索引、触发器、存储过程等）的配置管理；开发人员可通过标准化数据库访问接口，开发基于数据库的应用系统和软件产品。

国产数据库主要实现以下功能：

1.实现数据共享：数据共享包含所有用户可同时存取数据库中的数据，也包括用户可以用各种方式通过接口使用数据库，并提供数据共享。

2.减少数据的冗余度：同文件系统相比，由于数据库实现了数据共享，从而避免了用户各自建立应用文件。减少了大量重复数据，减少了数据冗余，维护了数据的一致性。

3.保持数据的独立性：数据的独立性包括逻辑独立性（数据库中数据库的逻辑结构和应用程序相互独立）和物理独立性（数据物理结构的变化不影响数据的逻辑结构）。

4.数据实现集中控制：文件管理方式中，数据处于一种分散的状态，不同的用户或同一用户在不同处理中其文件之间毫无关系。利用数据库可对数据进行集中控制和管理，并通过数据模型表示各种数据的组织以及数据间的联系。

5.数据一致性和可维护性，以确保数据的安全性和可靠性：主要包括：安全性控制、完整性控制、并发控制，使在同一时间周期内，允许对数据实现多路存取，又能防止用户之间的不正常交互作用。

6.故障恢复：由数据库管理系统提供一套方法，可及时发现故障和修复故障，从而防止数据被破坏。数据库系统能尽快恢复数据库系统运行时出现的故障，可能是物理上或是逻辑上的错误。比如对系统的误操作造成的数据错误等。

**3.国产化应用中间件**

国产化应用中间件是位于平台（硬件和操作系统）和应用之间的通用服务，这些服务具有标准的程序接口和协议，目的是为了使用系统软件所提供的基础服务（功能），衔接网络上应用系统的各个部分或不同的应用，能够达到资源共享、功能共享的目的。

国产中间件用于为上层应用提供运行环境，实现对上层应用的部署和动态管理。主要功能包括 Web 容器、EJB 容器、数据源服务、集群管理等。国产中间件部署在服务器，以后台服务形式运行，用户通过管理控制台或者命令行工具完成上层应用的部署、启动、停止等操作。

**（四）数据对接要求**

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》等规范，网络安全管理平台和网络安全运行平台需完成与宁波市级网络安全监管平台对接，逐步建立安全风险报告和情报共享机制等。同时，实现本级平台数据一体化对接，包括：

1. 本级与宁波市级网络安全监管平台的对接；
2. 网络安全管理平台和网络安全运行平台都与本级现有各网络安全产品的对接，包含不限于安恒APT、奇安信天擎、远望边界检测、明御堡垒机、明御日志审计、天融信数据库审计、盈高准入、安恒WAF、网御网闸、绿盟IPS等在用安全设备的数据对接；
3. 与第三方应用系统对接，需根据平台功能需要进行第三方应用的数据对接，为平台功能提供数据支撑。

 上述已在用设备的接口由中标方进行开发设计，并形成安全设备接入接口文档，可以由第三方公司按要求进行开发接入。

**（五）服务要求**

中标方需按用户要求完成各类网络资产调查、梳理工作，并配合用户完成漏洞通报、配置变更、系统暂停服务、风险处置、事件处置等网络安全管理流程的梳理、设计工作。

中标方根据项目实际需求，对所提供的系统保证全面、有效、及时的技术支持和维护服务，服务期为三年。服务范围至少包括运维支持、软件升级、扩容支持、性能调优、技术咨询、各种突发事件的应急策略、数据备份等。

中标方需提出全面的技术服务方案，详细列出技术服务方式，需明确服务提供方名称、服务内容、服务方式、服务人员技术要求以及服务响应时间等。

中标方需提供7\*24 小时的服务响应，保证采购方可以随时找到相应的技术人员，并对用户所反映的故障在15分钟之内响应，必须确保2小时之内赶到现场实地处理（发生灾害性天气时现场维护时限可适当放宽），查找故障原因、提出解决方案，直至故障修复完全恢复正常服务为止。

服务期内对系统进行每3个月定期维护、巡检，及时更新软件产品，并出具巡检报告，提出合理化建议。

未经采购方书面同意，项目所涉信息均不得应用于非本项目的其他用途，严禁向他人出示、泄露。未经许可，不得对项目所涉信息进行复制、传播、销售。否则，所引起的法律后果及损失由泄密方承担。

项目范围内的所有产品，其所有权及使用管理权在服务期第三年开始起归采购方所有。

项目实施完成后，需配置现场驻点人员至少1名，配合业主完成各项网络安全服务内容，驻点年限为3年。

**（六）项目组人员保障能力要求**

为确保项目实施中的人员配备，需提供项目经理1名，技术负责人1名，具有丰富经验的项目实施团队成员不少于4名。

投标方应明确承诺，在投标文件中响应的拟定项目组成员为参加本项目的实际成员，拟定的项目经理为实际参加本项目管理、技术等方面的项目负责人，负责项目协调和调度工作，全程参与本项目，并参与各类项目例会、项目沟通会、项目验收会议等方面工作。在合同签订后的整个项目实施过程中不得更改(用户要求更改的除外)。

**（七）系统测**shi**及验收要求**

1、系统测shi

（1）投标方应提供测shi条件、方法和过程的方案，商谈以后，最终测shi报告由采购方、监理公司、中标方三方共同确认。

（2）系统测shi是在监理公司代表监督下，中标方、采购方督导人员的指导下，由专业厂商技术人员共同进行。

（3）如果系统测shi没有满足测shi方案的要求，要重新整改后再进行系统测shi，直至满足要求。

2、试运行与验收

（1）系统测shi达到测shi方案的要求后，中标方、监理公司、采购方共同整理完成初步验收文件。项目组邀请技术专家对项目进行初步验收，初步验收通过后，中标方、监理公司、采购方三方共同签署项目初验报告，项目进入试运行。

（2）试运行期为3个月，在试运行期内如出现重大问题，试运行期顺延。

（3）试运行顺利完成后，中标方、监理公司、采购方邀请技术专家对项目进行交付验收论证，根据专家意见，三方共同签署项目交付验收报告。

（4）验收和试运行的一切费用由中标方承担。

（5）项目交付验收通过后进入服务期，服务期为三年。

**▲（八）其它要求**

1.采购方仅提供现网在用的安全设备、网络设备和必要的服务器资源，中标价格含所有功能实现所必须的一切软硬件等实施费用。

2.平台开发应基于信创软硬件环境，支持和兼容现有网络和安全产品。

3.平台必须全面支持IPV6，可以运行在IPV6单栈环境下或IPV4/IPV6双栈环境下。

4.投标人需根据本项目所有服务内容，提供详细的投标报价组成明细表。

5.投标人须作出无推诿承诺。即无论由于哪一方产生的问题而使系统发生不正常情况时，在得到采购方通知后，须立即派工程师到场，全力协助采购方和其他相关单位，使系统尽快恢复正常。

6.投标人须作出明确承诺。项目实施过程、服务期间，如有涉及与第三建设方集成工作，投标人应与全力与采购方、系统集成商及其他供应商配合，并提供必要的技术支持，保证系统按时、正常地投入运行。

# 第三部分 投标资料表

本部分关于本次招标项目的具体要求是对 “投标人须知”和“合同格式”的相关条款的补充和修改，如有矛盾，应以此为准。

| 条款号 | **条款内容** |
| --- | --- |
| 1.1 | 采购人名称： 余姚市大数据发展管理局地 址：余姚市梨洲街道谭家岭东路2号邮 编：315400电 话：0574--89553573 联 系 人：沈老师  |
| 采购代理机构名称：宁波国咨工程造价咨询有限公司地 址： 宁波市鄞州区和源路510号宁兴国贸大厦21楼2102室邮 编： 315040电 话： 0574-87312175电子邮件： 625740900@qq.com联 系 人： 戴佳颖、黄一达、唐权勇、李莺 |
| 项目名称：余姚市电子政务外网网络安全服务集成项目（本次采购为非专门面向中小企业） |
| 3.1 | 招标范围：详见招标文件第二部分“招标项目需求”。 |
| **★**4.1 | **合格投标人的资格要求（本项目采用资格后审）：**1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。2.落实政府采购政策需满足的资格要求：无。3.本项目的特定资格要求：无。 |
| 8.1 | 现场考察：不组织答疑会：不组织 |
| **★**9.1 | 投标文件组成：**1.商务技术文件，含：**(1)投标函；(2)单位负责人授权书或单位负责人身份证明；(3)投标单位情况一览表（若联合体投标的，联合体各方均须提供）；(4)技术条款偏离表；(5)商务条款偏离表；(6)第五部分“评标办法”中“评分标准”要求提供的资料（如有需提供）；以上条款请按本招标文件第七部分“附件（投标文件格式）”编制。**2.资格证明文件，含：**(1)资格条件自查表；(2)投标声明书（若联合体投标的，联合体各方均须提供）；(3)有效的“多证合一”的营业执照（未办理多证合一的提供营业执照、税务登记证、组织机构代码证）副本复印件。投标人如果有名称变更的，应提供由行政主管部门出具的变更证明文件（若联合体投标的，联合体各方均须提供）；(4) 关于资格的承诺函（若联合体投标的，联合体各方均须提供）；(5)投标人的特定条件的证明文件（如有）；(6)联合体协议书（如需联合体时提供）。**3．报价文件，含：**(1)开标一览表；(2)投标报价组成明细表；(3)中小企业声明函（如有需提供）；(4)残疾人福利性单位声明函（如有需提供）；(5)监狱企业声明函（如有需提供）。**供应商应对投标文件编制目录和评分索引表以方便查询。** |
| **★**10.1 | 本项目采用**固定总价方式。**投标报价的组成：本项目投标报价应为承包完成本次投标需完成全部工作所发生的所有费用，并承担一切风险责任，包括但不限于实施过程中涉及的专用工具、辅材、安装、调试、检验、培训、技术服务、运杂、保险费、税金、验收检定、软件升级以及其他费用，凡影响报价的所有相关费用均应列入。供应商自行应承担其编制响应文件与递交投标文件及参与本次招标活动所涉及的一切费用。投标人应承担其参加本招标活动自身所发生的费用。项目实施过程中可能发生的风险和费用均由中标人承担。 |
| **★**10.5 | **本项目采用最高投标限价，超过最高限价的投标将被判定为无效投标。****本项目最高限价为419.38万元。** |
| 11.4 | **投标文件数量要求：**本项目实行网上投标，供应商应准备以下投标文件：**★**（1）上传到政府采购云平台的电子投标文件（含资格证明文件、商务和技术文件、报价文件）1份。（2）以U盘或光盘存储的电子备份投标文件（含资格证明文件、商务和技术文件、报价文件）1份。**注意事项** **（1）电子投标文件中所须加盖公章部分均采用 CA 签章。** **（2）电子备份投标文件不作实质性要求，是否提交由供应商自行决定。** |
| 12.1 | **投标有效期**： 90 天。 |
| 13.1 | **投标保证金金额：无** |
| 15.1 | 投标截止时间：2024年2月21日14点00分（北京时间）。 |
| 28.1 | 1. 根据宁波市中介超市网上本项目的中选公告，采购代理单位向中标单位收取人民币 32000元整的代理服务费。
2. 中标人负责承担中标服务费，并应在采购代理机构发出中标通知书5个工作日内向采购代理机构支付中标服务费。

3.中标服务费只收电汇款。4.代理服务费收款账户信息：开户银行：建行宁波分行营业部；户名：宁波国咨工程造价咨询有限公司；账号：33101983679050502597。 |
| 29 | 发布本项目招标公告、中标结果公告的媒体：浙江政府采购网https://zfcg.czt.zj.gov.cn/宁波政府采购网[www.nbzf](http://www.nbzfcg.cn)[c](http://www.nbzfcg.cn)[g.cn](http://www.nbzfcg.cn) |

# 第四部分投标人须知

**A 总则**

1. **适用范围**

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

**2. 定义**

**2.1** “采购人”、“采购代理机构”和“项目名称”：见“投标资料表”。

**2.2** “投标人”系指向采购人提交投标文件的单位或个人。

**2.3** “产品”系指投标人按招标文件规定，须向采购人提供的一切设备、保险、税金、备品备件、工具、手册及其它有关技术资料和材料。

**2.4** “服务”系指招标文件规定投标人须承担的安装、调试、运维、技术协助、校准、培训、技术指导以及其它类似的义务。

**2.5** “项目”系指投标人按招标文件规定向采购人提供的货物或服务。

**2.6** “书面形式”包括信函、传真、邮件等。

**2.7** “★”系指实质性要求条款。投标文件对这些条款的任何负偏离将导致投标无效。

**3. 招标范围**

**3.1** 招标范围：见“投标资料表”。

**3.2** 本项目不得转包。

**4. 合格的投标人**

**4.1** 合格的投标人应该是：

具有提供本次招标服务内容能力，具有合法营销资格，并独立于采购人和采购代理机构的中国境内企业、其它组织或者自然人。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可以投标，但需依法办理工商、税务和社保登记手续，并获得总机构授权或者能够提供房产权证或其他有效财产证明材料，证明其具备实际承担责任的能力和法定的缔结合同能力。

单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加该采购项目的其他采购活动。

投标人应遵守国家有关的法律、法规、规章等相关文件的规定，具有健全的财务会计制度、依法缴纳税收和社会保障资金、参加本次采购活动之前的三年内，在经营活动中无重大违法记录，在招标投标活动中无欺诈和腐败行为。

**根据政府采购相关法律、法规、规章、文件规定并满足招标文件规定资格条件的区域性分支机构、个人独资企业、合伙企业参加本项目投标并由单位负责人签署的相关投标资料与本招标文件规定由法定代表人签署的文件材料具有同等效力。**

**4.2** 符合本招标文件载明的对上述**4.1**条的例外的规定或对投标人资格的其他补充要求：详见招标公告。

**5. 投标人代表**

**5.1** 投标人代表须持有“单位负责人授权书”。单位负责人是指单位法定代表人或者法律、行政法规规定代表单位行使职权的主要负责人（下同）。

**5.2** 若投标人代表是单位负责人的，则须符合本须知第**9.1**条的要求。

**6. 投标费用**

**6.1** 不论招标的结果如何，投标人自行承担其参加本次投标有关的全部费用。

**B 招标文件**

**7. 招标文件的构成**

**7.1** 招标文件共有七部分。内容如下：

第一部分 采购公告

第二部分 招标项目需求

第三部分 投标资料表

第四部分 投标人须知

第五部分 评标办法

第六部分 合同格式

第七部分 附件（投标文件格式）

**投标人应详细阅读招标文件的全部内容和要求，不按招标文件的要求提供投标文件和资料导致的风险由投标人承担。**

**8. 招标文件的澄清和修改**

**8.1** 采购人或者采购代理机构可以在招标文件提供期限截止后，组织已获取招标文件的潜在投标人现场考察或者召开开标前答疑会。组织现场考察或者召开答疑会的在招标文件“投标资料表”中载明，或者在招标文件提供期限截止后以书面形式通知所有获取招标文件的潜在投标人。

**8.2** 若潜在投标人对招标文件有疑点，要求采购人澄清的，应以书面形式通知采购代理机构，要求澄清的截止时间同有效质疑的截止时间。

**8.3** 采购人或者采购代理机构可以对已发出的招标文件进行必要的澄清或者修改，但不得改变采购标的和资格条件。澄清或者修改在原公告发布媒体上发布澄清公告。澄清或者修改的内容为招标文件的组成部分。

**8.4** 澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构在投标截止时间至少15日前，以书面形式（纸质、传真或电子邮件形式）通知所有获取招标文件的潜在投标人；不足15日的，采购人或者采购代理机构顺延提交投标文件的截止时间。

**8.5** 潜在投标人收到招标文件澄清或修改通知，或推迟截标和开标时间通知后，应在通知单回执上明示意见、盖上投标人单位公章，以书面形式（纸质、传真或电子邮件形式）回复采购代理机构。

**C 投标文件**

**9. 投标文件的组成**

**9.1** 投标文件组成在本招标文件“投标资料表”中做出规定。

**9.2** 组成投标文件的各项资料中本招标书的有规定格式的，应统一按本招标书的规定格式填写。未有规定格式的资料，投标人应自行编制，但至少要包含组成投标文件要求的内容。

**10. 投标报价**

**10.1** 本次招标对投标报价组成的具体要求在招标文件“投标资料表”中做出规定。

**10.2** 投标人要按照招标文件中的“开标一览表”格式和内容完整填写投标总价及其他事项。

**10.3** 除非招标文件另有备选投标方案的规定，投标应该只有一个投标报价。

**10.4** 开标后以及在评标及中标后的合同执行过程中，投标人不得以任何理由变更投标价格。**若投标人在中标以后做出任何改变投标价格的决定，将被视作撤标而失去中标资格。**

**10.5 本项目采用最高投标限价，超过最高限价的投标文件无效。**

**10.6** 本项目的投标货币为人民币。

**11. 投标文件的形式和效力**

**11.1** 投标文件分为电子投标文件以及备份投标文件，备份投标文件为以U盘或光盘存储的电子备份投标文件。

**11.2** 电子投标文件，按“项目采购-电子招投标操作指南”及本招标文件要求制作，并加密。

**11.3** 以U盘或光盘存储的电子备份投标文件，按“项目采购-电子招投标操作指南”制作的电子备份文件。

**11.4** 投标文件填写字迹必须清楚、工整，对不同文字文本投标文件的解释发生异议的，以中文文本为准。

**11.5** 投标文件的效力

投标文件的启用，按先后顺位分别为电子投标文件、以U盘或光盘存储的电子备份投标文件。在下一顺位的投标文件启用时，前一顺位的投标文件自动失效。

电子投标文件未能按时解密，供应商提供了电子备份投标文件的，以电子备份投标文件作为依据，否则视为投标文件撤回。电子投标文件已按时解密的，电子备份投标文件自动失效。

**12. 投标有效期**

**12.1** 投标有效期在本招标文件“投标资料表”中做出规定。投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期。

**12.2** 在特殊情况下，在原投标有效期截止之前，应采购人要求，采购代理机构可要求投标人延长投标有效期，这种要求的提出和投标人的答复都应以书面形式进行。

**12.3** 供应商可拒绝接受延期要求。同意延长有效期的供应商不能修改投标文件。

**13. 投标保证金**

**13.1**  投标保证金金额在本招标文件“投标资料表”中做出规定。

**13.2** 投标保证金递交时间和形式在本招标文件“投标资料表”中做出规定。

**13.3** 投标人在投标截止时间前撤回已提交的投标文件的，采购人或者采购代理机构自收到投标人书面撤回通知之日起5个工作日内，退还已收取的投标保证金，但因投标人自身原因导致无法及时退还的除外。

**13.4** 采购人或者采购代理机构自中标通知书发出之日起5个工作日内退还未中标人的投标保证金，自采购合同签订之日起5个工作日内退还中标人的投标保证金或者转为中标人的履约保证金。

**13.5** 采购人或者采购代理机构逾期退还投标保证金的，除退还投标保证金本金外，还应按中国人民银行同期贷款基准利率上浮20%后的利率支付超期资金占用费，但因投标人自身原因导致无法及时退还的除外。

**13.6** 投标人有下列情形之一的，投标保证金将不予退还：

（1）投标人在投标有效期内撤销投标文件；

（2）中标人无正当理由不与采购人订立合同；

（3）中标人不按招标文件要求提交履约保证金；

（4）投标人串通投标、提供虚假材料投标。

**14. 投标文件的组成和份数**

**14.1 投标文件的组成：**

投标文件组成在本招标文件“投标资料表”中做出规定。

组成投标文件的各项资料中本招标书的有规定格式的，应统一按本招标书的规定格式填写。未有规定格式的资料，投标人应自行编制，但至少要包含组成投标文件要求的内容。

**14.2 投标文件制作：**

（1）应按照本项目招标文件和政府采购云平台的要求编制、加密并递交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政府采购云平台技术支持热线咨询，联系方式：95763。制作电子投标文件的系统配置要求：请使用windows7及以上64位操作系统，不适用于mac或linux桌面系统。

（2）供应商通过政府采购云平台电子投标工具制作投标文件。电子投标工具请供应商自行前往浙江政府采购网下载并安装（zfcg.czt.zj.gov.cn/bidClientTemplate/2019-05-27/12946.html）。

供应商投标文件制作及电子交易操作指南详见：

①政府采购项目电子交易管理操作指南（视频）：

[service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/7GyLXW0BXgMSmLUuYuPM](https://service.zcygov.cn/%22%20%5Cl%20%22/knowledges/CW1EtGwBFdiHxlNd6I3m/7GyLXW0BXgMSmLUuYuPM)（电脑登录账号观看）；

②政府采购项目电子交易管理操作指南（文本）：

service.zcygov.cn/#/knowledges/CW1EtGwBFdiHxlNd6I3m/6IMVAG0BFdiHxlNdQ8Na（电脑登录账号浏览）。

（3）以U盘或光盘存储的电子备份投标文件1份，即按“项目采购-电子招投标操作指南”制作的电子备份文件，以用于异常情况处理。

（4）开标前准备：各供应商应在投标截止时间前确保成为浙江政府采购网正式注册入库供应商，并完成CA数字证书办理。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。供应商CA申领操作指南（help.zcygov.cn/web/site\_2/2018/11-29/2452.html），完成CA数字证书办理预计一周左右，请供应商自行把握时间。

**15. 投标文件的签署盖章**

**15.1** 招标文件第七部分“附件”中标明加盖公章或签字的，加盖公章部分采用CA签章，签字部分由法定代表人或授权代表签字后扫描上传。授权代表签字的，还应附法定代表人签署的法定代表人授权书。

**15.2** 投标文件须由供应商在规定位置盖章并由法定代表人或法定代表人的授权委托人签署，供应商应写全称。如为联合体投标，除联合体协议及联合体各成员单位提供的本单位证明材料外，响应文件由联合体牵头人按上述规定加盖联合体牵头人单位公章。

**D 投标文件的递交**

**16. 投标文件的密封和标记**

**16.1** 电子投标文件：供应商应根据“项目采购-电子招投标操作指南”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。

**16.2** 以U盘或光盘存储的电子备份投标文件用封袋密封后递交。

**16.3** 电子备份投标文件须在封袋上分别注明：

（1）注明：“电子备份投标文件”；

（2）项目编号：NBGZZB123150

（3）项目名称：余姚市电子政务外网网络安全服务集成项目；

（4）所投标项（如有多个标项须填写）：

（5）在年月日（规定的开标日期和时间）前不准启封；

（6）供应商的名称：。

供应商须在包封上加盖供应商公章或由其法定代表人（或授权代表）签字。

供应商未按上述要求标记的，采购人（代理机构）不承担错放或提前开封的责任。

**17. 投标递交**

**17.1** 投标文件递交的具体要求：

（1）供应商应于提交投标文件截止时间前将电子投标文件上传到政府采购云平台（[www.zcygov.cn](http://www.zcygov.cn)），并应于提交投标文件截止时间前，将以U盘或光盘存储的电子备份投标文件密封后按以下方式送达。

方式一：现场递交方式，请供应商在投标截止时间前将电子备份投标文件余姚市公共资源交易中心（余姚市谭家岭东路2号，南雷大厦附楼4楼，详见开评标场所安排），投标文件递交时须同时递交供应商的法定代表人（或其授权代表）联系方式，并保证开标期间联系方式畅通。

方式二：邮寄送达。供应商可以通过邮寄送达电子备份投标文件，送达地址宁波国咨工程造价咨询有限公司（宁波市鄞州区和源路510号宁兴国贸大厦2102室），联系方式：0574-87312175。供应商邮寄后须将邮件单号发送至代理机构电子邮箱（电子邮箱：625740900@qq.com），并致电采购代理机构，以便采购代理机构查询物流记录。各供应商应当确保投标文件的密封包装在邮寄过程保持完好，并在邮寄包裹上注明项目名称，因邮寄造成投标文件密封破损而不符合招标文件对投标文件的密封要求、或邮寄过程中导致投标文件未按时送达的，代理机构将拒绝其投标文件。各供应商自行考虑邮寄在途时间，投标文件送达时间以采购代理机构工作人员实际签收时间为准。电子备份投标文件邮寄送达截止时间为投标截止时间前一天17时00分。

**17.2** 供应商未按上述要求密封的电子备份投标文件，代理机构不予受理。

**17.3** 逾期送达的或者未送达指定地点的，代理机构不予受理。

**18. 投标文件的补充、修改**

投标截止时间前，供应商可以对递交的投标文件进行补充、修改，补充、修改电子投标文件的，应当先行撤回原文件，补充、修改后重新上传，电子备份投标文件也应重新制作。在投标截止时间之后，供应商不得对其投标文件进行补充、修改。投标截止时间之后供应商要求撤销投标文件的，应向采购人提交正式文件。

**E 开标**

**19**. **开标**

**19.1** 代理机构在招标文件规定的时间和地点公开开标，请供应商在投标截止时间前将电子备份投标文件送至余姚市公共资源交易中心（余姚市谭家岭东路2号，南雷大厦附楼4楼，详见开评标场所安排），在完成电子备份投标文件和人员登记后立即离开。电子备份投标文件递交时须同时递交供应商的法定代表人（或其授权代表）联系方式，并保证开标期间联系方式畅通。

**19.2** 电子投标开标及评审程序：

（1）宣布开标；

（2）本项目实行网上投标，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。投标截止时间后，供应商登录政府采购云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密，在线解密电子投标文件时间为开标时间后半小时内。供应商按时在线解密投标文件的，以在线解密的投标文件作为评审依据，若供应商在规定时间内无法解密或解密失败，则以备份电子投标文件作为评审依据（若备份电子投标文件与政采云平台上传的投标文件被识别为不一致，仍以备份电子投标文件作为评审依据）。无论是否启用备份电子投标文件，备份电子投标文件均不退还供应商。若供应商在规定时间内无法解密或解密失败且未提供备份电子投标文件或所提供的备份电子投标文件无法读取的，视为投标文件撤回。

（3）介绍开标现场的人员情况；

（4）宣读递交投标文件的供应商名单、开标纪律、应当回避的情形等注意事项；

（5）供应商签署不存在影响公平竞争的《政府采购活动现场确认声明书》；

（6）在政府采购云平台开启已解密供应商的“资格证明文件、商务和技术文件、报价文件”，并做开标记录；

（7）在政府采购云平台宣告评审无效供应商名单及理由；

（8）在政府采购云平台公布评审结果；

（9）开标会议结束。

**19.3** 特别说明：政府采购云平台如对电子化开标及评审程序有调整的，按调整后的程序操作。

本项目原则上采用政采云电子投标开标及评审程序，但有下情形之一的，按以下情况处理：

（1）若供应商在规定时间内无法解密或解密失败，代理机构将开启上述供应商递交的以U盘或光盘存储的电子备份投标文件，上传至政采云平台项目采购模块，以完成开标，电子投标文件自动失效。

（2）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，采购人（或代理机构）可中止电子交易活动：

2.1 电子交易平台发生故障而无法登录访问的；

2.2 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；

2.3 电子交易平台发现严重安全漏洞，有潜在泄密危险的；

2.4 病毒发作导致不能进行正常操作的；

2.5 其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购人（或代理机构）可以待上述情形消除后继续组织电子交易活动。

**F 评标和定标**

**20. 评标委员会及评标**

**20.1** 受采购人的委托，采购代理机构依据《中华人民共和国政府采购法》、《中华人民共和国政府采购实施条例》等有关规定组建评标委员会，并主持评标活动。评标委员会由采购人代表和政府采购云平台随机抽取的技术、经济专家组成。**评标委员会成员名单在招标结果确定之前依法保密**。

**20.2**  评标委员会将遵循公平、公正、科学、廉洁的原则和法定的程序进行评标，并且只依据招标文件要求和投标文件的响应情况进行评审，不依据任何来自开标后的补充声明、修正方案。

**20.3** 评标委员会根据本须知的规定、招标文件的“评标标准”和“招标项目要求”中所列的具体标准，对投标文件进行评审和比较。

**21. 投标的澄清**

**21.1** 评标委员会在对投标文件的有效性、完整性和响应程度进行审查时，可以要求供应商对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等做出必要的澄清。供应商的澄清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。

**21.2** 政采云具体操作如下：

在评审过程中，如评标委员会对投标文件有疑问，由评标委员会组长将问题汇总后发函，或由采购代理机构代替发起。供应商在截止时间前，予以回复。此回复将作为投标文件内容的一部分，具有相应的法律效力。

路径：用户中心—项目采购—询标澄清

（1）政采云平台通过待办事项和短信提醒供应商在截止时间前完成澄清。

（2）供应商在“询标澄清-待办理”标签页下选择状态为“待澄清”的项目，点击操作栏【澄清】。

（3）查看函内容，在澄清截止时间前上传澄清文件并对澄清文件进行签章。（注：澄清文件必须以PDF格式上传，文件大小：50M）

（4）签章完成，文件名称处显示“已签章”，供应商可“撤回签章”修改澄清函和“查看文件”。

（5）确认澄清文件内容后，点击右上角【提交】；（注：供应商未对澄清文件签章，提交时，弹框提醒“澄清文件未签章，请进行签章操作”，如遇CA突发情况无法签章，供应商可点击【放弃签章并提交】提交澄清文件；反之则签章后再提交。）

（6）完成状态：供应商澄清文件提交成功后，在“询标澄清-全部”标签页下显示状态为“已澄清”。

**21.3** 澄清文件应当由供应商的法定代表人或授权代表签字或者加盖供应商公章。澄清文件将作为投标文件内容的一部分，具有相应的法律效力。

**21.4** 供应商未在截止时间前完成澄清，将被视作自动放弃。

**22. 评标办法：**评标采用综合评分法。**本项目招标采用的评标方法载明在招标文件第五部分“评标办法”中。**

**23. 评标程序和原则**

**23.1** 评标程序：遵循资格审查、符合性审查、澄清有关问题、比较与评价、推荐中标供应商（或中标候选人）的程序依次进行。

**23.2** 资格审查：公开招标采购项目开标结束后，采购人或者采购代理机构应当依法对投标人的资格进行审查。详见招标文件第五部分“评标办法”。

**23.3** 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。详见招标文件第五部分“评标办法”。

**23.4** 澄清有关问题：按第**21**条规定进行。

**23.5** 综合比较与评价：评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

**23.5.1** 商务评价：按照招标文件的要求和“评标标准”对照投标文件的响应进行商务评价，并对其偏差计算相应的商务评分分值。

**23.5.2** 技术评价：按照招标文件的要求和“评标标准”对照投标文件的响应进行技术评价，评定其偏差程度，并计算其相应的技术评分分值。

**23.5.3** 综合评价：对经过商务评价、技术评价的投标，按“评标标准”规定的评价办法进行综合评价，做出评标结果排序。

**23.6 评标过程处理原则**

**23.6.1** 通过资格审查的投标人不足3家的，不得评标。

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

（1）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；

（2）大写金额和小写金额不一致的，以大写金额为准；

（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；

（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。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照投标文件招标文件的规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

**23.6.3** 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，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

**23.6.4** 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。

**23.6.5**  采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一标项投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定，其他投标无效。

使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一标项项投标的，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，由采购人或者采购人委托评标委员会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。

非单一产品采购项目，招标文件中应载明核心产品，多家投标人提供的核心产品品牌均相同的，按上述规定处理。

**23.6.6** 有下列情形之一的，视为投标人串通投标，其投标无效：

（1）不同投标人的投标文件由同一单位或者个人编制；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（5）不同投标人的投标文件相互混装；

（6）不同投标人的投标保证金从同一单位或者个人的账户转出。

**23.6.7** 投标人存在下列情况之一的，投标无效：

（1）未按照招标文件的规定提交投标保证金的；

（2）投标文件未按招标文件要求签署、盖章的；

（3）不具备招标文件中规定的资格要求的；

（4）报价超过招标文件中规定的预算金额或者最高限价的；

（5）投标文件含有采购人不能接受的附加条件的；

（6）法律、法规和招标文件规定的其他无效情形。

**23.6.8** 评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

（1）分值汇总计算错误的;

（2）分项评分超出评分标准范围的;

（3）评标委员会成员对客观评审因素评分不一致的;

（4）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者采购代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审，重新评审改变评标结果的，书面报告本级财政部门。

投标人对本条第一款情形提出质疑的，采购人或者采购代理机构可以组织原评标委员会进行重新评审，重新评审改变评标结果的，应当书面报告本级财政部门。

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

**24. 推荐中标候选人**

**24.1** 评标委员会按照招标文件第五部分“评标标准”推荐中标候选人。

**25. 定标**

**25.1** 确定中标人。本项目由评标委员会推荐中标候选人，采购人不得在评标委员会推荐的中标候选人以外确定中标候选人。

**25.2** 采购代理机构在评标结束后2个工作日内将评标报告交采购人确认，采购人在收到评标报告之日起5个工作日内在评标报告确定的中标候选人中按顺序确定中标人，采购人在收到评标报告之日起5个工作日内未按评标报告推荐的中标候选人排序确定中标人，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标人。

**25.3** 采购代理机构自中标人确定之日起2个工作日内，在发布招标公告的网站上对中标结果进行公示，中标结果公告期限为1个工作日。

**G 授予合同**

**26. 中标通知**

**26.1**  在公告中标结果的同时，采购代理机构应当向中标人发出中标通知书。

**26.2** 中标通知书发出后，采购人不得违法改变中标结果，中标人无正当理由不得放弃中标。

**27. 签订合同**

**27.1** 中标人应在采购代理机构发出中标通知书的30日内，应与采购人签订合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

**27.2** 除中标通知书外，招标文件、中标人的投标文件及评标过程中有关的澄清文件也均应作为合同附件。

**27.3** 中标人拒绝与采购人签订合同的，采购人可以按照评标报告推荐的中标候选人名单排序，确定下一候选人为中标人，也可以重新开展政府采购活动。

**28. 履约保证金**

**28.1** 招标文件若有规定，在签订合同后，采购人按合同支付定金的同时，中标人应向采购人提供履约保证金。

**28.2** 若中标人不按上述第28.1条要求提供，采购代理机构和采购人有权按前述第13.6条规定处理并撤销其中标资格。在这种情况下，采购代理机构和采购人可按本须知第27.3条规定另选中标人。

**29. 履约验收**

 采购人负责对中标人的履约行为进行验收，验收符合相关政策法规和地方标准。

**H 采购代理机构服务费**

**30. 采购代理机构服务费**

**30.1** 中标人应在中标结果公示结束后向采购代理机构支付采购代理机构服务费。

**Ⅰ 信息发布媒体**

**31. 有关发布项目招标公告、中标结果公告的媒体：**

浙江政府采购网https://zfcg.czt.zj.gov.cn/

宁波政府采购网[www.nbzfcg.cn](http://www.nbzfcg.cn)

**J 其他规定**

**32. 其他规定**

**32.1** 自购买招标文件之日起，投标人应保证其提供的联系方式(电话、传真、电子邮件)一直有效，以保证往来函件(招标文件的澄清、修改等)能及时通知投标人，并能及时反馈信息，否则采购人不承担由此引起的一切后果。

**32.2** 知识产权

**32.2.1** 投标人应保证提交的全部文件不会侵犯其他任何人的知识产权或专有技术或商业秘密。投标人应保证，如果投标文件使用他人的知识产权或专有技术或商业秘密，投标人已获得了适当授权。投标人应进一步保证，采购人使用其成果不会侵犯他人的知识产权或专有技术或商业秘密，并应当使采购人免于因被指控侵犯上述权利产生的任何责任，若采购人使用其成果被指控侵犯上述权利，投标人应赔偿采购人由此而产生的费用和损失。

**32.2.2** 投标人中标后参与本项目研究的资料、成果等知识产权归采购人，有关的信息未经采购人同意不得向第三方泄露。

**32.2.3** 采购人在招商引资、产权转让的商业活动中，所使用本项目有关的任何成果，无需征得中标供应商同意，中标供应商应积极配合提供相关资料和成果；中标供应商有责任对涉及项目的重要信息进行保密；中标供应商如因为项目的开展需要向第三方提供资料,必须提前得到采购人批准。

**33. 政府采购活动中有关中小企业的相关规定（采购进口产品项目不适用）**

**33.1**  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。

**33.2**  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，享受本办法规定的中小企业扶持政策：

（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，不享受本办法规定的中小企业扶持政策。

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。

**33.3** 中小企业参加政府采购活动，应当出具《中小企业声明函》（格式见附件），否则不得享受相关中小企业扶持政策。

**33.4** 对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，采购人、采购代理机构应当对符合本办法规定的小微企业报价给予10%—20%（工程项目为3%—5%）的扣除，用扣除后的价格参加评审。

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采购项目，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，采购人、采购代理机构应当对联合体或者大中型企业的报价给予4%-6%（工程项目为1%—2%）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。

价格扣除比例对小型企业和微型企业同等对待，不作区分。具体采购项目的价格扣除比例，由采购人根据采购标的相关行业平均利润率、市场竞争状况等，在招标文件内确定。

**33.5** 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。

**33.6** 执行财政部、司法部《关于政府采购支持监狱企业发展有关问题的通知》。监狱企业（监狱和戒毒企业）提供自己企业的产品（服务）参加投标视同小型、微型企业，享受评审中价格扣除等政府采购促进中小企业发展的政府采购政策，监狱企业参加政府采购活动时，必须提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件，未能提供上述证明文件的不予认可。

**33.7** 根据《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，残疾人福利性单位视同小型、微型企业。符合条件的残疾人福利性单位在参加政府采购活动时，应当在投标文件中提供通知规定的《残疾人福利性单位声明函》（格式详见该通知附件），并对声明的真实性负责,未能提供上述证明文件的不予认可。

**33.8** 执行财政部、国家环保总局《关于环境标志产品政府采购实施的意见》，政府采购优先采购环境标志产品，本项目将对环境标志产品给予一定幅度的价格扣除或技术加分，具体见 “评标标准”说明。

**33.9** 执行财政部、国家发展改革委员会《节能产品政府采购实施意见》，政府采购优先采购节能产品，本项目将对节能产品给予一定幅度的价格扣除或技术加分，具体见招标文件“评标标准”说明。

**33.10** 进口产品采购需符合“财政部关于印发《政府采购进口产品管理办法》的通知（财库[2007]119号）”第四、八、九、十、十一条的规定。

**34. 招标文件对投标人质疑的相关规定**

**34.1** 供应商应当自知道或者应当知道其合法权益受到损害之日起7个工作日内提出质疑。提出质疑的有效期计算，依照下列规定：

（1）对采购信息公告提出质疑的，应当在采购信息公告发布之日起7个工作日内提出。

（2）对招标文件提出质疑的，应当在获取招标文件或者招标文件公告期限届满之日起7个工作日内提出。

（3）对采购过程提出质疑的，应当在招标文件接收、开标、评标工作、宣布评标结果等环节结束之日起7个工作日内提出。

（4）对采购结果提出质疑的，应当在采购结果公告期限届满或书面通知（书面通知可以采用电子邮件、传真方式）采购结果之日起7个工作日内提出，未按规定在发布采购结果公告同时书面通知采购结果的，以供应商实际知道采购结果之日起计算。

**34.2** 对采购信息公告内容提出质疑的，不限制质疑主体。未依法获取招标文件的，不得就招标文件提出质疑；未提交投标文件的供应商，视为与采购结果没有利害关系，不得就采购响应截止时间后的采购过程、采购结果提出质疑。

**34.3** 供应商提出质疑应当提交质疑函和必要的证明材料，质疑函应当面以书面形式提出，质疑函格式和内容须符合财政部《质疑函范本》要求，供应商可到中国政府采购网自行下载财政部《质疑函范本》。

**34.4** 接收书面质疑函的方式：质疑人可通过送达、邮寄、传真、邮件的形式提交书面质疑函，通过邮寄方式提交的书面质疑函以被质疑人签收邮件之日为收到书面质疑文件之日，通过传真或邮件方式提交的书面质疑函以被质疑人收到书面质疑文件原件之日为收到书面质疑文件之日。采购人和采购代理机构接收质疑函的联系方式：见本招标文件第一章有关联系方式。

**34.5** 供应商对采购人或采购代理机构的质疑答复不满意或者采购人或采购代理机构未在规定时间内作出答复的，可以在答复期满后十五个工作日内向同级采购监管部门投诉。

**35. 联合体规定**

**35.1** 两个及以上的自然人、法人或者其他组织可以组成一个联合体，以一个供应商的身份共同参加政府采购。**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具备本法第二十二条规定的条件，并应当向采购人提交联合协议，载明联合体各方承担的工作和义务。**联合体各方应当共同与采购人签订采购合同，就采购合同约定的事项对采购人承担连带责任。本项目接受联合体投标。组成联合体的成员数量不得超过2个。

**35.2** 联合体中有同类资质的投标人按照联合体分工承担相同工作的，按照资质等级较低的投标人认定资质等级。

**35.3**  **以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他投标人另外组成联合体参加同一标项号的政府采购活动。**

**35.4 联合体协议中仅约定由联合体主办单位或成员单位中某一方与采购人签订合同的，或联合体协议中仅约定由联合体主办单位或成员单位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，该联合体的投标文件将被作无效处理。**

# 第五部分 评标办法

**一、总则：**

1．本办法严格遵照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》（87号令），结合项目所在地有关政府采购的规定和项目的实际情况制定。本评标标准是对“投标人须知”相关条款的具体表述或补充，如有矛盾，应以本办法为准。

2．本项目评标采用综合评分法。

3．本次采购为非专门面向中小企业，本次评标将对《中小企业声明函》满足招标文件要求的小微企业的价格按本办法中规定的比例进行扣除，用扣除后的价格参与评审。价格扣除只用于评审过程，如中标，中标价格仍按照其投标价格进行公示。

**二、评标组织**

评标委员会：采购人和采购代理机构根据采购项目的内容和特点，按国家相关规定组建评标委员会。评标委员会由采购人代表和政府采购云平台随机抽取的技术、经济方面专家等人员组成。

**三、评标程序**

**1．资格审查**：由采购人或代理机构对投标人的资格进行审查。

| 审查类别 | 审查项目 | 审查内容 |
| --- | --- | --- |
| 资格条件审查 | 1. 符合《中华人民共和国政府采购法》第二十二条的要求：1.1具有独立承担民事责任的能力；1.2具有良好的商业信誉和健全的财务会计制度；1.3具有履行合同所必需的设备和专业技术能力；1.4有依法缴纳税收和社会保障资金的良好记录；1.5参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；1.6法律、行政法规规定的其他条件。 | (1)资格条件自查表；(2)投标声明书；(3)有效的“多证合一”的营业执照（未办理多证合一的提供营业执照、税务登记证、组织机构代码证）副本复印件。投标人如果有名称变更的，应提供由行政主管部门出具的变更证明文件；(4) 关于资格的承诺函；(5) 投标人的特定条件的证明文件（如有）。 |
| 2.未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。 | 根据财库【2016】125号文要求，采购人或采购代理机构对投标人的信用记录进行查询并甄别：（1）信用信息查询的截止时点：投标截止时间；（2）查询渠道：“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）；（3）信用信息查询记录和证据留存具体方式：打印查询网页并与其他采购文件一并保存；（4）信用信息的使用规则：投标人存在不良信用记录的，其投标将被作为无效投标处理。不良信用记录指：被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。若在开标当天因不可抗力事件导致无法查询且一时无法恢复查询的，可在发布中标结果公告之前对中标候选人进行事后查询。中标候选人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的，采购人将依法取消其中标资格。 |
| 3.落实政府采购政策需满足的资格要求： | / |
| 4. 本项目的特定资格要求： | / |
| 1. 本项目接受联合体投标。
 | 若为联合体投标时须提供联合体协议书 |
| 资格审查结论 |  |

**2．符合性检查**：评标委员会应当对符合资格审查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。

|  |  |  |
| --- | --- | --- |
| **序号** | **要求说明** | **审查要求** |
| 1 | 投标有效期：符合第三部分“投标资料表”12.1条的要求。 | 提供“投标函”。 |
| 2 | 单位负责人授权书或单位负责人身份证明。 | （1）投标文件由法定代表人签字的，提供“单位负责人身份证明”。（2）投标文件由授权代表签字的，提供“单位负责人授权书”。 |
| 3 | 符合第三章“投标须知”第15条的要求。 | 投标文件的签署盖章符合所述要求。 |
| 4 | 标项以赠送方式投标的，对一个标项提供两个投标方案的。 | 是否有两个投标方案。 |
| 5 | 供应商不得在投标活动中提供任何虚假材料或从事其他违法活动的。 | 不得提供任何虚假材料或从事其他违法活动。 |
| 6 | 违反公平竞争的原则或恶意串通或妨碍其他投标人的竞争行为或损害采购人或者其他投标人的合法权益的； | 不得有所述情形。 |
| 7 | 不允许含有采购人不能接受的附加条件的； | 不得有所述情形。 |
| 8 | 不允许出现与招标文件有重大偏离的投标文件。 | 不得有所述情形。 |
| 9 | 评标委员会经过审查，认定供应商虚假应标、串通投标的，有下列情形之一的，视为供应商串通投标：（1）不同供应商的投标文件由同一单位或者个人编制；（2）不同供应商委托同一单位或者个人办理投标事宜；（3）不同供应商的投标文件载明的项目管理成员或者联系人员为同一人；（4）不同供应商的投标文件异常一致或者投标报价呈规律性差异；（5）不同供应商的投标文件相互混装； | 不得有所述情形。 |
| 10 | 符合法律、法规和招标文件中规定的其他实质性要求（实质性要求招标文件中“**★**”标记） | 符合所述要求。 |
| 11 | 本项目公开招标设有最高限价**419.38万元。** | 提供“开标一览表”。 |
| 12 | 投标文件报价出现前后不一致，经按招标文件规定修正后，投标人对修正后的报价不确认的； | 不得有所述情形。 |
| 13 | 评标委员会认为供应商的报价明显低于其他通过初步审查的供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。 | 符合所述要求。 |
| 符合性审查结论 |  |

3．比较与评价：评标委员会对资格审查、符合性审查合格的投标文件，依照本办法“七、评分标准”对投标文件作进一步评审、比较，判定其偏差性质和程度。评标委员会成员经过阅标、审标和询标，对各投标人进行打分。

4．最终得分及排序：评标委员会成员独立按照评分标准（兼评委打分表）规定的内容和分值设置，对各投标文件分别打分汇总后计算平均分（小数点后保留两位数），即为各投标人的综合得分。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并列，采取随机抽签的方式确定排序。

5．推荐中标候选人原则：投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

6．确定中标人：采购代理机构在评标结束后2个工作日内将评标报告交采购人确认，采购人在收到评标报告之日起5个工作日内在评标报告确定的中标候选人中按顺序确定中标人，采购人在收到评标报告之日起5个工作日内未按评标报告推荐的中标候选人排序确定中标人。中标人因不可抗力或者自身原因不能履行政府采购合同的，采购人可以按照评标报告推荐的下一中标候选人为中标人或重新招标。

**四、澄清问题的形式**

对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会可要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权代表签字或盖章确认，并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。

**五、错误修正**

投标文件报价出现前后不一致的，按照下列规定修正：

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

2. 大写金额和小写金额不一致的，以大写金额为准；

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；

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。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照招标文件的规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

**六、其它投标无效的情形**

1．未提供或未如实提供投标货物的技术参数，或者投标文件标明的响应或偏离与事实不符或虚假投标的；

2．投标技术方案不明确，存在一个或一个以上备选（替代）投标方案的；

3．未采用投标文件要求的报价形式报价的；

4．投标报价具有选择性；

5．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，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的；

6．两家或两家以上供应商提供的投标文件出自同一终端设备的，或在相同Internet主机分配地址（相同IP地址）获取招标文件或网上投标的，且经询标澄清供应商无令人信服的理由和可靠证据证明其合理性的。

7．招标文件规定的其他无效情形。

**七、评分标准（兼评委打分表）**

|  |
| --- |
| 评分项及分值 |
| 商务技术分（75分） | 技术部分（62分） | 项目需求分析（6分） | 根据投标人对本项目及运维对象现状情况的分析，以及运维的重点、难点和服务要求理解程度进行评议，本项最高得6分，未提供不得分。（1）投标人提供的重点、难点分析方案，方案内容阐述详实全面，合理，思路清晰的，措施针对性较强的得6分；（2）投标人提供的重点、难点分析方案，方案内容阐述较为全面、具体详细， 较为合理、有一定针对性、操作性一般的得3分；（3）投标人提供的重点、难点分析方案，方案内容阐述说明内容简单、缺乏针对性、操作性差的得1分。 |
| 技术参数响应情况（29分） | 根据投标人提供平台功能和技术参数进行打分，技术参数完全符合招标要求没有负偏离的得29分，带▲的参数为重要指标，负偏离每项扣1分，其他负偏离每项减0.5分，扣分大于29分的作无效标处理。 |
| 技术方案（6分） | 根据投标人提供的网络安全平台维护方案进行评议，未提供不得分。（1）维护服务方案全面合理，服务流程及内容具体，响应时间迅速，服务人员齐备，得3分；（2）维护服务方案较全面，有基本服务流程及内容，响应时间较为迅速，服务人员匹配基本满足需求，得2分；（3）维护服务方案较片面，服务流程及内容空洞或欠缺，响应时间缓慢，服务人员匹配欠缺，得1分。 |
| 根据供应商提供的应急预案评分，需能根据不同场景（包括软件系统故障、硬件系统故障、网络故障、服务器故障、网络攻击事件、信息破坏事件、信息内容安全事件、灾难性事件，根据实际项目不同选择不同场景）、不同等级故障（包括一般事件、较大事件、重大事件、特大事件）出具相应的应急措施、服务响应及应急保障。1. 应急预案细化全面，应急措施科学合理，服务响应及时高效，应急保障人力及物资安排合理，得3分；
2. 应急预案较全面，应急措施恰当，服务响应较及时，具有基本的应急保障人力及物资安排，得1分；
3. 应急预案不全，应急措施混乱，服务响应时间滞后，未考虑人力及物资安排或安排不合理，得2分；
4. 未提供应急预案或预案与项目严重不符，本项得0分。
 |
| 日常运维（6分） | 根据投标人提供的日常运维方案（运维内容、时间安排等）合理性且能落实到实处。要求日常运维方案全面完整、流程合理规范、文档齐全详细、管理制度完善、运维人员配置合理进行评议，本项最高得6分，未提供不得分。（1）投标人提供的日常运维方案，方案内容阐述详实全面、合理，思路清晰的，针对性强的，得6分；（2）投标人提供的日常运维方案，方案内容阐述较为详实全面，较为科学合理，思路较清晰的，针对性较强的，得3分；（3）投标人提供的日常运维方案，方案内容阐述空泛，思路模糊的，有明显漏洞的，得1分。 |
| 安全服务（6分） | 根据投标人提供的安全服务方案（保障技术、保障措施、保障人员、保障安排等）合理性且能落实到实处。要求技术方案全面完整、流程合理规范、文档齐全详细、管理制度完善、技术人员配置合理，本项最高得6分，未提供不得分。（1）投标人提供的安全服务方案，方案内容阐述详实全面、合理，思路清晰的，针对性强的，得6分；（2）投标人提供的安全服务方案，方案内容阐述较为详实全面，较为科学合理，思路较清晰的，针对性较强的，得3分；（3）投标人提供的安全服务方案，方案内容阐述空泛，思路模糊的，有明显漏洞的，得1分。 |
| 重大活动保障方案（6分） | 根据投标人提供的重大活动保障方案（保障时间、人员配备、保障措施流程、保障制度等）合理性且能落实到实处。要求保障人员配备齐全、保障时间满足要求、保障流程和措施合理规范、保障制度完善，本项最高得6分，未提供不得分。（1）投标人提供的重大活动保障方案，方案内容阐述详实全面、合理，思路清晰的，针对性强的，得6分；（2）投标人提供的重大活动保障方案，方案内容阐述较为详实全面，较为科学合理，思路较清晰的，针对性较强的，得3分；（3）投标人提供的重大活动保障方案，方案内容阐述空泛，思路模糊的，有明显漏洞的，得1分。 |
| 培训方案（3分） | 根据投标人提供的培训方案、计划的可行性及合理性。要求方案内容包含但不限于培训师资、培训课程、培训时间、培训方式等内容，本项最高得3分，未提供不得分。（1）培训方案全面合理有效，具有详细的培训计划、培训师资力量、培训内容，得3分。（2）培训方案不够全面，有效性欠缺，培训计划、培训师资力量、培训内容不够详细，得2分。培训方案片面，（3）不具有执行有效性，培训计划、培训师资力量、培训内容不详细，得1分。 |
| 商务部分（13分） | 团队配置（7分） | （1）项目经理具有信息系统项目管理师的得1分，具有注册信息安全专业人员证书（CISP证书）的得1分，具有网络规划设计师的得1分，本项最高得3分。（2）技术负责人具有注册信息安全专业人员证书（CISP证书）的得2分，最高得2分。（3）根据项目组其他成员（除项目经理、技术负责人）具有网络工程师、信息安全保障人员认证（CISAW）的，每项证书得1分，最高得2分。同一位组员有多本证的只计一本；单本证书不重复得分。注：须提供有效期内证书复印件和投标截止日前半年内任意二个月的社保缴费证明复印件并加盖公章或提供项目团队为投标人本单位人员的承诺函原件，否则不得分。 |
| 综合实力(4分） | 投标人具有有效的ISO27001信息安全管理体系认证的得2分；具有有效的信息技术服务ITSS证书的得2分。注：须提供有效期内证书复印件加盖公章，否则不得分。 |
| 业绩（2分） | 自 2020年 1 月 1 日（以合同签订日期为准）以来，投标人具有类似运维服务项目案例的，每提供1个得1分，最高得2分。 |
| 报价分（满分25分） | 评标基准价指的是满足招标文件要求且最低的参与评审的价格。参与评审的价格=投标报价-小微企业价格扣除优惠值（如有）。参与评审的价格为评标基准价的其价格得分得满分25分。其他供应商价格得分按照下列公式计算：价格得分=（评标基准价/各供应商参与评审的价格）×25。注：1、投标报价超过对应最高限价的作无效标处理。2、价格得分小数点后保留2位小数，第3位小数四舍五入。3、根据《政府采购促进中小企业发展管理办法》（财库[2020]46号）、《财政部关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号），对符合规定的小微企业报价给予20%的扣除，用扣除后的价格参加评审。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采购项目，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，采购人、采购代理机构应当对联合体或者大中型企业的报价给予6%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。 |

注：表内要求提供的资料，未按要求提供的均不得分。

**第六章 采购合同**

**余姚市电子政务外网网络安全服务集成采购项目**

合 同

甲方： 余姚市大数据发展管理局

乙方： XXXX公司

签订地点: **余姚**

签订时间: 20 **年 月 日**

根据“余姚市电子政务外网网络安全服务集成采购”项目（招标编号为 XXXX ）公开招标的结果，甲、乙双方协定签订以下协议内容：

**1、项目概况**

1.1 项目名称：余姚市电子政务外网网络安全服务集成采购项目

1.2 实施地点：余姚市

**2、项目服务内容**

余姚市电子政务外网网络安全服务集成采购项目，包括数据安全服务和网络安全服务购置，年限为三年。

服务期内每年提供的服务内容和成果资料：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 服务成果资料 | 备注 |
| 1 | 业务需求收集和实施 | 实施记录 | 根据业务动态变化，进行需求收集和过程协调，并单位及时有效实施 |
| 2 | 数据健康状态监控 | 数据安全报告 | 数据异常捕获、预警及处置 |
| 3 | 网络健康状态监控 | 网络安全报告 | 网络异常捕获、预警及处置 |
| 4 | 月度巡检 | 月度巡检报告 | 每月一份 |
| 5 | 季度巡检 | 季度巡检报告 | 每季度一份 |
| 6 | 年度巡检 | 年度巡检报告 | 每年度一份 |
| 7 | 日常运行维护 | 运行维护报告 | 日常运行管理，运行情况记录，运行情况检查与评价 |
| 8 | 数据安全服务制定一系列数据管理制度规范 |  | 每年度一份 |
| 9 | 数据安全培训 | 培训记录及报告 | 每年2次 |
| 10 | 数据安全应急演练 | 记录及报告 | 每年2次 |
| 11 | 数据安全相关检查工作 | 记录及报告 | 根据业务和用户需求，每年提供服务 |
| 12 | 数据资产发现工作 | 数据资产发现报告 | 每季度一次 |
| 13 | 数据资产分类分级工作 | 数据资产分类分级报告 | 每季度一次 |
| 14 | 数据源详情展示工作 | 数据源详情展示报告 | 每季度一次 |
| 15 | 安全事件的深度分析 | 重点高危事件分析报告 | 每年4次 |
| 16 | 事件跟踪管理服务 | 工作周报 | 每周 |
| 17 | 主动分析服务 | 运营月度报告 | 每月 |
| 18 | 漏洞扫描服务 | XX年XX月漏洞扫描报告 | 每季度一次 |
| 19 | 基线检查服务 | XX年XX月基线检查报告 | 每季度一次 |
| 20 | 渗透测shi服务 | XX系统渗透测shi报告 | 每年6个系统 |
| 21 | 安全检查服务 | 安全检查服务报告 | 每年4次 |
| 22 | 安全工作报告服务 | 安全态势分析与工作报告，《XX年XX月安全工作报告》 | 每月 |
| 23 | 运营流程优化服务 | 全通报流程和制度 | 一次性 |
| 24 | 运营文件编制服务 | 对文档资料进行编制、整合、沉淀，形成知识库 | 每年一次 |
| 25 | 资产梳理服务 | 《电子政务网资产清单》、《余姚市互联网网站资产清单》 | 每年2次 |
| 26 | 策略调优服务 | 输出所有安全设备、安全系统调优服务报告 | 每年2次 |
| 27 | 重要时期安全保障服务 | 重要时段服务报告 | 按需 |
| 28 | 宣传教育及培训服务 | 培训记录及报告 | 每年2次 |
|  | ...... |  |  |

**3、项目实施期限**

3.1余姚市电子政务外网网络安全服务集成采购项目工期自合同签订之日起XX内完成实施并进入试运行，试运行时间为3个月。

3.2项目服务期由项目通过交付验收之日起计算，服务期限叁年。

**4、合同文件使用语言文字和适用法律、标准及规范**

4.1 适用法律和法规：国家有关法律、法规和浙江省法规、规范及规范性文件均对本合同有约束力。

 4.2 适用标准、规范：除合同另有规定外，按国际、国家、行业和浙江省现行质量评定标准和技术验收规范执行。

**5、监理单位委派的工程师**

按甲方委托的监理公司（待定）签订的《余姚市电子政务外网网络安全服务集成采购项目委托监理合同》规定执行。

**6、甲方主要义务**

6.1负责合同签订后项目实施的工作（如与乙方的具体联系和衔接，现场安装调试时配备人员进行监管控制）；

6.2 负责提供设备和项目安装调试所必须的场地和环境；

6.3 负责组织成立验收小组对设备和项目进行验收并签署验收报告。

**7、乙方主要义务**

7.1 按规定办理项目实施过程中所需的一切手续并承担相应费用；

 7.2在甲方规定的时间安排施工并完成所有工程，完成工程所需的费用（如人工、材料费等）由乙方承担，并保证符合招标文件规定。维修人员在收到故障报告后保证2小时内到达现场；乙方每3个月对设备进行定期保养（或维护、巡检）；

7.3遵守甲方现场关于安全文明施工、后勤卫生、环保、消防、保卫等方面的管理规定；

7.4 配合所有现场施工单位的进度及工作；

 7.5定期参加施工现场由甲方召开的相关工种协调会，服从并按期执行协调会所作的一切决定；

 7.6负责按政府、行业的有关规定和要求搜集本工程的档案资料。

**8、进度计划**

 乙方负责编制项目的实施计划，经甲方和监理公司审定后由乙方组织实施。

**9、项目实施期限延误**

9.1 因甲方原因影响本工程施工，经监理公司审核后，由甲方确定延期时间。

 9.2 如因工程量临时增加（非甲方因素），工期不得顺延。

 9.3 因不可抗力而使工程处于停工或缓建时，工期另议。

 9.4 对以下造成交付日期推迟的延误，经甲方确认工期相应顺延。

 ⑴由于不可抗力影响施工正常进行（不可抗力以政府部门发布为准）；

 ⑵合同中约定或甲方同意给予顺延的其他情况。

 在上述情况发生48小时内，乙方就延误内容和因此产生的经济支出，向甲方提出书面报告。甲方在收到报告后48小时内就工期延长给予书面答复。但工期之延长不附带经济赔偿，除非为顺利实施工程，甲方自愿给予乙方经济之赔偿。非上述原因，工程不能按合同工期完工，乙方承担违约责任。

**10、工程质量**

10.1 在施工过程中，因乙方达不到工程要求及标准的部分，甲方一经发现，可要求乙方返工，乙方应尽快按甲方要求返工，直到符合约定条件，并承担返工费用，工期不予顺延。

10.2 乙方应保证货物是全新、未使用过的，并完全符合合同约定的质量、规格和性能的要求。甲方（或监理方）先查看包装是否完好，封印是否清晰完整，确认是否为厂家的“原装货”，然后再打开包装，查看合格证及设备上的生产日期标志和条形码，有无涂改、改动迹象，打厂家免费电话查询确认。乙方应保证所提供的货物经准确安装、正常运转和保证在其使用寿命期内应具有的性能。在货物质量保证期限内，乙方应对提供的货物由于设计、工艺或材料的质量缺陷而发生的任何不足或故障负责。

10.3 乙方交付的货物不符合约定的，甲方（或监理方）应在约定的时限内以书面形式通知乙方，由乙方承担继续履行、采取补救措施或赔偿损失等违约责任。

10.4 乙方在收到通知后15天内应免费维修或更换有缺陷的货物或部件。如果乙方在收到通知后15天内未弥补缺陷，甲方可采取必要的补救措施，但费用由乙方承担。

**11、验收及标准**

11.1项目验收：乙方负责设备安装和调试，完工后，甲方、监理方测shi是否合格并满足技术要求。

11.2试运行验收：系统测shi达到测shi文件的要求后，甲方、监理公司、乙方共同整理完成测shi报告和验收文件。上述工作全部完成后，项目组邀请技术专家对项目进行初步验收，初步验收通过后，甲方、监理公司、乙方共同签署系统初验报告，项目进入试运行；项目正常试运行达到3个月后，由乙方申请，甲方组织交付验收。

11.3甲方在验收时，如发现有工程施工与设计方案有不合格之处，乙方应在甲方指定期限内修改完善，待修改完善后再报请复验，复验合格后方可视为通过，复检费由乙方承担，造成的工期延误由乙方承担。

11.4本工程验收或施工期间的检查及抽验所需的人工、设备，均应由乙方无偿提供，费用由乙方承担。

11.5在本项目交付验收合格后，进入正式服务期。服务期内，乙方按照双方共同确认的服务方案进行运维服务，并按月、季度、年度及时提供运维报告。

**12、履约保证金**

12.1履约保证金金额：合同金额的1%，即 元；

12.2履约保证金形式： ；

12.3担保收件人： ；

12.4提交时间： ；

12.5履约保证金的退还： 。

**13、合同总价及付款方式**

13.1合同总价：大写 （小写： ）。合同总价包含项目达到预期使用效果所需的一切费用，甲方不再另行付费。但按实际结算后服务费总额少于合同总价的，则双方按实结算。

13.2付款方式：

13.2.1（1）合同生效后7个工作日内支付合同总价的30%（中标人为非中小微企业）；（2）合同生效后7个工作日内支付合同总价的40%（中标人为中小微企业）；

13.2.2（1）第二年服务期结束前两个月，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的35%（如有违约金，在扣除第一年度违约金后支付）（中标人为非中小微企业）；（2）第二年服务期结束前两个月，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的30%（如有违约金，在扣除第一年度违约金后支付）（中标人为中小微企业）；

13.2.3（1）第三年服务期开始并完成资产移交后，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的35%（如有违约金，在扣除第二年度违约金后支付）（中标人为非中小微企业）；（2）第三年服务期开始并完成资产移交后，甲方收到乙方开具的税务发票确认无误后30个工作日内支付合同总价的30%（如有违约金，在扣除第二年度违约金后支付）（中标人为中小微企业）。

注：约定的支付时间以政府财政性资金支付要求为准，如因财政等原因导致支付延迟，甲方不承担相应责任。

**14、违约责任**

 合同自甲乙双方盖章签字后，即具有法律效力，任何一方不得擅自修改或拒绝执行合同内任何条款（除本合同特殊说明外）。

14.1因乙方原因导致工期延误，工程建设期限延误1-10天，扣违约金5000元每天，工程期限期延误10天以上，第11天开始扣违约金10000元每天；延误超过30天的，甲方有权单方面解除本合同，乙方投入的所有设备归甲方所有，乙方支付甲方合同总价30%的违约金，并赔偿甲方所有损失。

　　14.2因乙方原因合同提前终止，则本工程中乙方投入的所有设备无条件归甲方所有，乙方支付甲方合同总价30%的违约金，并赔偿因此而造成的其它损失；因甲方原因合同提前终止，甲方应承担损失。

14.3每发生一次重大故障的赔偿金额10000元，不可抗力引起的重大故障除外。一年度内出现重大故障五次以上的，甲方有权单方面终止合同，乙方投入的所有设备归甲方所有，乙方支付甲方合同总价30%的违约金，并赔偿由此带来的损失。

14.4乙方擅自更换派驻人员的，处违约金50000元/次，且甲方有权拒绝接受其擅自更换的派驻人员。

14.5 乙方未按月、年度及时提供各类运维报告的，处违约金200元/次。

14.6 因乙方运维人员原因发生网络安全、数据安全事件的，处违约金5000元/次，造成重大影响或被上级部门通报的，加倍扣款。

14.7 本项目内相关设备/软件产品未定期维护保养和除尘清洁的，处违约金200元/处。

14.8服务期内发现问题，乙方整改不及时、不全面、不彻底、乱汇报，再次检查发现问题仍未处理的，处违约金2000元/次。

14.9乙方在投标文件中响应的拟定项目组成员为参加本项目的实际成员，拟定的项目经理为实际参加本项目管理、技术等方面的项目经理，负责项目协调和调度工作，全程参与本项目，并参与各类项目例会、项目沟通会、项目验收会议等方面工作。在合同签订后的整个项目实施过程中不得更改(用户要求更改的除外)，乙方不得擅自更改项目经理，乙方书面申请，经甲方同意后，每更换一人次，处违约金10000元/次，更换次数达3次及以上或者乙方擅自更换项目经理，甲方有权终止合同，且乙方已投入的所有软硬件产品归甲方所有。项目经理如缺席会议、项目重要环节工作的，每缺席一次，处违约金5000元/次，缺席次数达3次及以上，甲方有权终止合同，且乙方已投入的所有软硬件产品归甲方所有。

14.10 以上违约金在年度服务费中予以扣除，服务费不足以扣的，从待支付的年度服务费和履约保证金中扣除，履约保证金不足以扣的，甲乙双方另行协商。

**15、安全、网络安全、数据安全管理**

15.1 乙方应按照有关安全规范施工及提供一切所需安全设备和措施，因乙方违反安全管理的规定而造成的事故，或由于乙方原因造成人员伤亡或其它物品的破坏，责任由乙方承担。

15.2 如发生任何伤亡事故，乙方应按有关规定立即报告有关部门并通知甲方，甲方协助抢救伤员，由于非甲方原因发生伤亡事故的费用均由乙方承担。

15.3 运维期间必须严格按照《中华人民共和国网络安全法》《中华人民共和国保守国家秘密法》《网络安全法》等法律法规标准执行，并应按照甲方的运维机制和考核办法开展服务工作。甲方对乙方在服务期间的网络安全、监管制度、保密制度、技术防范、信用情况、数据安全等进行考核。

15.4 乙方运维人员做好操作账号管理，设置相应的操作权限，严禁多名运维人员共用一个操作账号。所有操作行为日志必须符合《网络安全法》规定留存6个月以上。

15.5乙方不得收集与其提供的服务无关的信息，不得泄露、篡改或者毁损信息，不得违反法律、法规的规定收集、使用和向第三方提供信息。

15.6 乙方应配合甲方定期组织开展应急演练，及时有效处置网络安全、数据安全事件。

15.7 乙方应加强乙方人员管理，落实安全背景审查，与其签署保密等协议。乙方应建立健全人员离职（调离）管理制度，做好工作交接，回收系统账号，与其签订离岗保密协议提交甲方备案。

**16、工程停建及缓建**

16.1 由于不可抗力的原因导致工程停建或缓建，使合同不能继续履行，乙方应妥善做好已完成工程和材料、设备的保护和移交工作，甲方应为乙方撤出提供必要条件。

16.2 由于甲、乙任何一方不能按所签合同履约，导致工程停建或缓建，造成的损失由责任方承担。

**17、争议及解决**

17.1 在解释或者执行本合同的过程中出现疑问或发生争议时，双方应通过协商方式解决。

 17.2 经协商不能解决的争议，向余姚市人民法院起诉。

 17.3 除有争议或正在诉讼的部分外，本合同其他部分仍应按合同条款继续履行。

17.4 如果产生争议或正在诉讼时，乙方未经甲方同意不得擅自停止施工，如果影响施工进度按本合同规定执行。

**18、设备采购与产权**

18.1 本项目中由乙方投入设备的所有权及使用管理权在服务期第三年开始起归甲方所有，按照固定资产管理要求，乙方必须提供所有设备的购置发票给甲方，并在第三年服务期开始后的10个工作日内完成资产移交，并无条件配合甲方完成固定资产登记工作。服务期内设备的更换和维修由乙方负责，相关费用由乙方承担。

18.2 乙方不得将本项目相关设备的全部或部分用于其它业务使用。

18.3 乙方未按本合同第18.1条办理资产移交手续的，则应向甲方支付合同总价30%的违约金。

**19、本合同的制定、效力、解释、履行和争议的解决均适用中华人民共和国法律。**

**20、合同份数**

 本合同一式陆份，甲乙双方各叁份，具同等法律效力。

**21、补充条款**

21.1 乙方应严格履行其本工程投标文件中的承诺（包括运行维护、技术支持与保证措施、技术培训等承诺）。

21.2 乙方投标文件中承诺视为本合同一部分。合同期内因双方工作需要，发生机房搬迁等问题由乙方负责实施并承担全部费用。

21.3乙方在叁年合同期内免费提供XX名专业对口的，具有一年以上安全运维工作经验的人员常驻甲方单位；被派遣人员的工作地点、工作岗位、岗位职责，由甲方决定，乙方有义务教育、督促被派遣人员遵守国家法律、法规、保守国家秘密以及工作、商业秘密，乙方应教育被派遣人员遵守甲方依法制定的各项内部规章制度；被派遣人员在甲方工作期间，乙方对被派遣人员的工资、福利、补贴及值班费等待遇不得少于乙方单位同等相关人员，同等条件下，优先考虑提升、晋升机会；在派遣用工期内，因派遣人员工作原因，甲方有权退还或者退换被派遣人员，乙方不得随意撤回或者撤换被派遣人员。

**22、本合同未尽事宜，将由双方通过协商另行签订补充协议。但不能违背招标文件的实质性内容。**

**23、合同文件**

下列文件构成本合同的组成部分：

1、招标文件；

2、中标人（乙方）的投标文件及其澄清文件；

3、招标人发出的中标通知书；

4、采购内容及技术要求（招标文件）；

5、投标报价明细表（投标文件）；

6、技术响应表 （投标文件）；

7、合同补充条款或说明（包括出卖人出具的承诺书、投标文件中的各类承诺）；

各构成本合同的组成部分的条款与本合同正文有不符的，以本合同正文为准。项目具体技术需求及采购人地址等详见招标文件、投标文件以及询标记录。合同总价包含项目达到预期使用效果所需的一切费用。

**24、合同的生效**

本合同经双方法定代表人（企业负责人）或其委托代理人签字盖章后生效。

甲 方： 乙 方：

名称（公章）： 名称（公章）：

法定代表人（签章）： 法定代表人（签章）：

或其委托代理人： 或其委托代理人：

# 第七部分 附件（投标文件格式）

## 商务技术文件

封面

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目

**投 标 文 件**

招标编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

标项：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

投标文件名称： **商务技术文件**

投标人： （盖章）

日 期： 年 月 日

1．商务技术文件，含：

(1)投标函

(2)单位负责人授权书或单位负责人身份证明；

(3)投标单位情况一览表（若联合体投标的，联合体各方均须提供）；

(4)技术条款偏离表；

(5)商务条款偏离表；

(6)第五部分“评标办法”中“评分标准”要求提供的资料（如有需提供）；

以上条款请按本招标文件第七部分“附件（投标文件格式）”编制。

**（一）投 标 函**

致： （采购人、采购代理机构）

我方确认收到贵方关于 的招标文件（项目编号： ），法定代表人（或《单位负责人授权书》中的授权代表） 作为我方代表，在此声明并同意：

1.愿意遵守招标文件的各项规定，自愿参加投标，并已清楚招标文件的要求及有关文件规定，并严格按照招标文件的规定履行全部责任和义务。

2.同意本投标文件的投标有效期从提交投标文件的截止之日起 日历天内有效。如果我方的投标被接受，则直至合同生效时止，本投标始终有效并不撤回已提交的投标文件。

3.我方已详细审查并理解全部招标文件，包括修改文件（如有）以及全部参考资料和有关附件，已经了解我方对于采购文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及进行询问、质疑、投诉的相关渠道、要求。我们同意放弃对招标文件提出不明或误解的一切权力。

4.我方同意提供采购人或采购代理机构与评标委员会要求的有关投标的一切数据或资料。

5.我们理解采购人或采购代理机构与评标委员会并无义务必须接受最低报价的投标或其它任何投标。

6.如果我方未对招标文件全部要求作出实质性响应，则完全同意并接受按无效投标处理。

7.我方证明提交的一切文件，无论是原件还是复印件均为准确、真实、有效、完整的，绝无任何虚假、伪造或者夸大。我们在此郑重承诺：在本次招标采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我方承担。

8.如果我们提供的声明或承诺不真实，则完全同意认定为我方提供虚假材料，并同意作相应处理。

9.如我方中标，承诺按照招标文件规定的金额、时间和方式支付采购代理服务费。因我方违约致使采购代理机构采取诉讼或仲裁等方式实现债权，为此支付的律师费、差旅费、执行费、评估费及其他实现债权的一切费用由我方承担。

10.所有有关本次投标的函电请寄：

地址： 邮编： 电话：

传真： 电子邮箱：

投标人：\_填写全称并加盖公章

法定代表人或授权代表签名： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日 期：

## （二）单位负责人授权书

（单位负责人来投标的，此表不用）

 致 （*采购代理机构*） ：

 （*投标人全称*） 单位负责人 *（姓名、职务）* 授权 （*被授权代表姓名、职务*） 为本公司合法代理人，参加贵采购代理机构组织的 *（招标编号）* (*项目名称*) 项目的招标投标活动，代表本公司处理招标投标活动中的一切事宜。

 本授权书于 年 月 日签字生效,特此声明。

 单位负责人（签字或印章）：

 投标人单位全称（公章）：

 日 期：

附：

 被授权代表姓名：（印刷体）

 职 务：

被授权代表签字：

 详细通讯地址：

 邮 政 编 码：

 传 真：

 电 话：

**附：单位负责人及被授权人身份证复印件**

## 单位负责人身份证明

（单位负责人不来投标的，此表不用）

投标人名称：

单位性质：

地址：

成立时间： 年 月 日

经营期限：

姓名： 性别： 年龄： 周岁 职务： \_

身份证号码：

系 （投标人名称）的法定代表人（或单位负责人）。

特此证明。

投标人： （盖单位公章）

 年 月 日

**附单位负责人身份证复印件（正反面）：**

## （三）投标单位情况一览表

|  |  |
| --- | --- |
| 投标人名称 |  |
| 注册地址 |  | 邮政编码 |  |
| 联系方式 | 联系人 |  | 电话 |  |
| 传真 |  | 电子邮址 |  |
| 法定代表人 | 姓名 |  | 技术职称 |  | 电话 |  |
| 技术负责人 | 姓名 |  | 技术职称 |  | 电话 |  |
| 成立时间 |  | 员工总人数： |
| 资质资格与业务范围 |  | 其中 | 高级职称 |  |
| 中级职称 |  |
| 营业执照号 |  | 各类注册人员 |  |
| 注册资金 |  |
| 基本账户开户银行 |  |
| 基本账户账号 |  |
| 经营范围 |  |
| 备注 |  |

投标人（公章）：

投标人代表（签字或印章）：

日期：

**注：（若联合体投标的，联合体各方均须提供）**

## （四）技术条款偏离表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件技术要求 | 投标文件对应规格 | 说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：1.须与招标文件第二部分“招标项目需求”中“技术要求”逐项比较填写。

2.如有偏离的，须在本表中列明，并提供详细的偏离说明。如投标人未在本表中列出偏离说明，即使其在投标文件的其他部分说明与招标文件要求有所不同或回避不答，亦视为完全符合招标文件中所要求的最佳值并写入合同。若中标人在定标及合同签订前，以上述事项为借口而不履行合同签订手续及执行合同，则视作其放弃中标资格。

投标人（公章）：

投标人代表（签字或印章）：

日期：

## （五）商务条款偏离表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 招标文件的商务条款 | 投标文件的商务条款 | 说明 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：1.须与招标文件第二部分“招标项目需求”中“商务要求”逐项比较填写。

2.如有偏离的，须在本表中列明，并提供详细的偏离说明。如投标人未在本表中列出偏离说明，即使其在投标文件的其他部分说明与招标文件要求有所不同或回避不答，亦视为完全符合招标文件中所要求的最佳值并写入合同。若中标人在定标及合同签订前，以上述事项为借口而不履行合同签订手续及执行合同，则视作其放弃中标资格。

投标人（公章）：

投标人代表（签字或印章）：

日期：

## 第五部分“评标办法”中“评分标准”要求提供的资料（如有需提供）

主要内容详见第五部分的评分标准中内容。

**供应商技术商务分自评表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分项目 | 评分标准 | 分值 | 自评分 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 合计 |  |  |

注：上表评标项目、评分标准、分值，供应商可对应招标文件中的评标办法，并提供相应资料。

供应商（盖章）：

法定代表人或授权代表(签字或盖章)：

日 期：

**1.1拟委任的项目组成员汇总表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 姓名 | 年龄 | 拟在本项目中担任的职务 | 职称 | 执业资格 | 工作年限 | 类似项目经验年限 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

注：须提供有效期内证书复印件和投标截止日前半年内任意二个月的社保缴费证明复印件并加盖公章或提供项目团队为投标人本单位人员的承诺函原件，否则不得分。

投标人（公章）：

投标人代表（签字或印章）：

日期：

**1.2投标人自*2020年1月1日*以来项目汇总表**

|  |  |  |  |
| --- | --- | --- | --- |
| 项目序号 | 项目名称 | 委托人名称 | 服务开始和完成日期 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：表后附合同复印件加盖公章，时间以合同签订时间为准。

投标人（公章）：

投标人代表（签字或印章）：

日期：

**资格证明文件**

封面

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_项目

**投 标 文 件**

招标编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

标项：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

投标文件名称： **资格证明文件**

投标人： （盖章）

日 期： 年 月 日

2.资格证明文件，含：

(1)资格条件自查表；

(2)投标声明书（若联合体投标的，联合体各方均须提供）；

(3)有效的“多证合一”的营业执照（未办理多证合一的提供营业执照、税务登记证、组织机构代码证）副本复印件。投标人如果有名称变更的，应提供由行政主管部门出具的变更证明文件（若联合体投标的，联合体各方均须提供）；

(4) 关于资格的承诺函（若联合体投标的，联合体各方均须提供）；

(5)投标人的特定条件的证明文件（如有）；

(6)联合体协议书（如需联合体时提供）。

**（一）资格条件自查表**

|  |  |  |  |
| --- | --- | --- | --- |
| **评审内容** | **招标文件要求** | **自查结论** | **证明资料** |
| **资****格****性****审****查** | 1.投标人具备《政府采购法》第二十二条所规定的条件： | □通过 □不通过 | 第（ ）页-（ ）页 |
| 1.1有效的“多证合一”的营业执照（未办理多证合一的提供营业执照、税务登记证、组织机构代码证）副本复印件。投标人如果有名称变更的，应提供由行政主管部门出具的变更证明文件； | 第（ ）页 |
| 1.2 关于资格的承诺函； | 第（ ）页 |
| 2.未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。 |  |  |
| 3.落实政府采购政策需满足的资格要求：（如有） | □通过 □不通过 | 第（ ）页-（ ）页 |
| 4.本项目的特定资格要求：4.1本项目接受联合体投标。 | □通过□不通过 |  |

**备注：**

**1.投标人自查表将作为投标人有效性审查的重要内容之一，投标人必须严格按照其内容及序列要求在投标文件中对应如实提供，对资格证明文件的任何缺漏和不符合项将会直接导致投标无效！**

### （二）投标声明书

（*采购代理机构*）**：**

关于贵司年　　月　　日发布XXXXXXXXXXXXXXXX项目（项目编号：　　　）的招标公告，本单位愿意参加投标，并声明：

我单位具备《中华人民共和国政府采购法》第二十二条资格条件，并已清楚招标文件的要求及有关文件规定。

我单位的单位负责人或单位负责人与所参投的本采购项目的其他投标人的单位负责人或单位负责人不为同一人且与其他投标人之间不存在直接控股、管理关系。

根据《中华人民共和国政府采购法实施条例》的规定，本单位如为本采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加该采购项目的其他采购活动。否则，由此所造成的损失、不良后果及法律责任，一律由我单位承担。

我单位未被信用中国网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法件当事人名单，未被中国政府采购网（www.ccgp.gov.cn）列入政府采购严重违法失信行为记录名单。

本次招标采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我单位承担。

特此声明！

投标人（公章）：

投标人代表（签字或印章）：

年 月 日

**注：若联合体投标的，联合体各方均须提供。**

### （三）有效的“多证合一”的营业执照（未办理多证合一的提供营业执照、税务登记证、组织机构代码证）副本复印件。投标人如果有名称变更的，应提供由行政主管部门出具的变更证明文件；

（复印件并加盖公章）

**注：若联合体投标的，联合体各方均须提供。**

### （四）关于资格的承诺函

致：采购人

我单位承诺：

我单位满足《中华人民共和国政府采购法》第二十二条 供应商参加政府采购活动应当具备的下列条件：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）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；

（六）法律、行政法规规定的其他条件。

特此承诺。

投标人（公章）：

投标人代表（签字或印章）：

年月日

**注：若联合体投标的，联合体各方均须提供。**

### （六）投标人的特定条件的证明文件（如有）

**（七）联合体协议书（如需联合体时提供）**

 （所有成员单位名称）自愿组成 （联合体名称），共同参加 （项目名称）。现就联合体投标事宜订立如下协议。

1． （某成员单位名称）为 （联合体名称）牵头人。

2．联合体各成员授权牵头人代表联合体参加投标活动，签署文件，提交和接收相关的资料、信息及指示，进行合同谈判活动，负责合同实施阶段的组织和协调工作，以及处理与本项目有关的一切事宜。

3．联合体牵头人在本项目中签署的一切文件和处理的一切事宜，联合体各成员均予以承认。联合体各成员将严格按照招标文件、投标文件和合同的要求全面履行义务，并向采购人承担连带责任。

4．联合体各成员单位内部的职责分工如下：

（1）由联合体牵头人承担 工作（占合同总金额 %）；

（2）由联合体成员承担 工作（占合同总金额 %）。

5．投标工作和联合体在中标后实施过程中的有关费用按各自承担的工作量分摊。

6．本协议书自所有成员单位法定代表人签字或盖章并加盖单位章之日起生效，合同履行完毕后自动失效。

7．本协议书一式 份，联合体成员和采购人各执一份。

联合体牵头人名称： （盖单位章）

法定代表人： （签字或盖章）

联合体成员名称： （盖单位章）

法定代表人： （签字或盖章）

 年 月 日

**注：采用联合体形式投标的供应商必须提供联合体协议。**

**报价文件**

封面

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_项目

**投 标 文 件**

招标编号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_

标项：\_\_\_\_\_\_\_\_\_\_\_\_

投标文件名称： **报价文件**

投标人： （盖章）

日 期： 年 月 日

3.报价文件，含：

(1)开标一览表；

(2)投标报价组成明细表；

(3)中小企业声明函（如有需提供）；

(4)残疾人福利性单位声明函（如有需提供）；

(5)监狱企业声明函（如有需提供）；

## （一）开标一览表

项目名称： 招标编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目内容 | 最高限价（元） | 投标报价（单位：元） | 工期 | 投标声明 |
| 1 |  |  |  |  |  |
| 投标报价（元） | 大写：小写：¥ |

投标人（公章）：

投标人代表（签字或印章）：

日期：

## （二）投标报价组成明细表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 技术参数 | 单位 | 数量 | 单价 | 合价 | 品牌 | 备注 |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| ... | ... |  |  |  |  |  |  |  |
| 投标价合计（元） |  |

**注：1、供应商应详细列出招标文件规定的所有费用的明细表，本表“投标价合计”应与“开标一览表”中的“投标报价”保持一致。**

1. **本表需根据采购文件第二部分 招标项目需求的所有内容进行分别报价。**
2. **此表在不改变表式的情况下，可自行制作扩展。**

供应商（盖章）：

法定代表人或授权代表(签字或盖章)：

日 期：

**（三）中小企业声明函**

（如非中小微企业，可不提供此声明函）

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

1.**（余姚市电子政务外网网络安全服务集成项目）**，属于**（软件和信息技术服务业）**；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，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：

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

2、本项目所属行业见前附表。

**3、中小企业划型标准规定（工信部联企业[2011]300号）附后。**

**中小微行业划型标准规定**（根据工信部联企业〔2011〕300号制定）

|  |  |  |  |
| --- | --- | --- | --- |
| **行业** | **中型企业** | **小型企业** | **微型企业** |
| 从业人员X（人） | 营业收入 Y（万元） | 资产总额 Z（万元） | 从业人员X（人） | 营业收入Y（万元） | 资产总额Z（万元） | 从业人员X（人） | 营业收入Y（万元） | 资产总额Z（万元） |
|  1、农林牧渔业 |  |  500≤Y＜20000 |  |  |  50≤Y＜500 |  |  | Y＜50 |  |
|  2、工业 | 300≤X＜1000 | 2000≤Y＜40000 |  | 20≤X＜300 | 300≤Y＜2000 |  | X＜20 | Y＜300 |  |
|  3、建筑业 |  | 6000≤Y＜80000 | 5000≤Z＜80000 |  | 300≤Y＜6000 |  300≤Z＜5000 |  | Y＜300 | Z＜300 |
|  4、批发业 |  20≤X＜200 | 5000≤Y＜40000 |  |  5≤X＜20 | 1000≤Y＜5000 |  | X＜5 | Y＜1000 |  |
|  5、零售业 |  50≤X＜300 |  500≤Y＜20000 |  | 10≤X＜50 | 100≤Y＜500 |  | X＜10 | Y＜100 |  |
|  6、交通运输业 | 300≤X＜1000 | 3000≤Y＜30000 |  | 20≤X＜300 | 200≤Y＜3000 |  | X＜20 | V＜200 |  |
|  7、仓储业 | 100≤X＜200 | 1000≤Y＜30000 |  | 20≤X＜100 | 100≤Y＜1000 |  | X＜20 | Y＜100 |  |
|  8、邮政业 | 300≤X＜1000 | 2000≤Y＜30000 |  | 20≤X＜300 | 100≤Y＜2000 |  | X＜20 | Y＜100 |  |
|  9、住宿业 | 100≤X＜300 | 2000≤Y＜10000 |  | 10≤X＜100 | 100≤Y＜2000 |  | X＜10 | Y＜100 |  |
| 10、餐饮业 | 100≤X＜300 | 2000≤Y＜10000 |  | 10≤X＜100 | 100≤Y＜2000 |  | X＜10 | V＜100 |  |
| 11、信息传输业 | 100≤X＜2000 | 1000≤Y＜100000 |  | 10≤X＜100 | 100≤Y＜1000 |  | X＜10 | Y＜100 |  |
| 12、软件和信息技术服务业 | 100≤X＜300 | 1000≤Y＜10000 |  | 10≤X＜100 |  50≤Y＜1000 |  | X＜10 | Y＜50 |  |
| 13、房地产开发经营 |  | 1000≤Y＜200000 | 5000≤Z＜10000 |  | 100≤Y＜1000 | 2000≤Z＜5000 |  | Y＜100 | Z＜2000 |
| 14、物业管理 | 300≤X＜1000 | 1000≤Y＜5000 |  | 100≤X＜300 | 500≤Y＜1000 |  | X＜100 | Y＜500 |  |
| 15、租赁和商务服务业 | 100≤X＜300 |  | 8000≤Z＜120000 | 10≤X＜100 |  |  100≤Z＜8000 | X＜10 |  | Z＜100 |
| 16、其他未列明行业 | 100≤X＜300 |  |  | 10≤X＜100 |  |  | X＜10 |  |  |

说明　1.企业类型的划分以统计部门的统计数据为依据。2.个体工商户和本规定以外的行业，参照本规定进行划型。3.本规定的中型企业标准上限即为大型企业标准的下限。

## （五）残疾人福利性单位声明函（如有需提供）

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（盖章）：

 日 期：

**注：**

**享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：**

**（一）安置的残疾人占本单位在职职工人数的比例不低于25%（含25%），并且安置的残疾人人数不少于10人（含10人）；**

**（二）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；**

**（三）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；**

**（四）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；**

**（五）提供本单位制造的货物、承担的工程或者服务（以下简称产品），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）。**

**前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1至8级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或者服务协议的雇员人数。**

**（六）监狱企业声明函（如有需提供）**

监狱企业参加政府采购活动时，应当提供由省级以上监狱管理本企业郑重声明，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，本企业为监狱企业。

根据上述标准，我企业属于监狱企业的理由为：。

本企业为参加（项目名称： ）（项目编号： ）采购活动提供本企业的产品。

本企业对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标单位名称（盖章）：

日期： 年 月 日

供应商为监狱企业的提供此函。

监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

监狱企业：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。