上海杨浦

招标文件

项目名称：上海市杨浦区数据局杨数浦“ABCD”安全运营矩阵项目

项目编号：3101100002509221374 91-10275386

采购人：上海市杨浦区数据局（上海市杨浦区信息化委员会、上海市杨浦区政务服务办公室）

集中采购机构：上海市杨浦区政府采购中心

2025年10月22日　　2025年10月22日

目　　录

第一章　　投标邀请

项目概况

上海市杨浦区数据局杨数浦“ABCD”安全运营矩阵项目招标项目的潜在投标人应在上海政府采购网（www.zfcg.sh.gov.cn）获取招标文件，并于 **2025-11-14 09:30:00** （北京时间）前递交投标文件。

一、项目基本情况

项目编号：**310110000250922137491-10275386**

项目名称：**上海市杨浦区数据局杨数浦“ABCD”安全运营矩阵项目**

采购方式：公开招标

预算金额：**15000000.00 元**

最高限价：**包 1-14114000.00 元**

采购需求：**全面建立杨浦区网络安全管理范式，构建网络安全数字底座，具备贯穿信息化项目建设前期规划、项目立项、项目实施、项目运维等全过程的能力，全面落实各项安全防护措施，构建安全生态、创新安全服务，建设完善的安全保障体系。**

合同履行期限：**项目整体建设周期：6 个月，试运行 1 个月（不包含在项目建设周期内）。本项目要求中标单位提供一年整体软件维保服务，从项目验收之日起计算，包括所有定制化开发软件和成品软件及相关配套服务。**

本项目**不允许**接受联合体。

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；

2.落实政府采购政策需满足的资格要求：**本采购项目执行政府采购有关鼓励支持节能产品、环境认证产品、支持中小企业、残疾人福利性单位、监狱企业等的政策规定。**

3.本项目的特定资格要求：

1、符合《中华人民共和国政府采购法》第二十二条的规定；

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、本项目面向大、中、小、微型等各类供应商采购；

4、本项目合同不得转让、不得分包。

5、本项目不接受联合投标。

三、获取招标文件

时间：2025-10-24 至 2025-11-03 （提供期限自本公告发布之日起不得少于 5 个工作日），每天上午 00:00:00~12:00:00，下午 12:00:00~23:59:59（北京时间，法定节假日除外 ）

地点：上海政府采购网（www.zfcg.sh.gov.cn）

方式：网上获取

售价：0 元

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：2025-11-14 09:30:00（北京时间）

投标地点：上海政府采购网（www.zfcg.sh.gov.cn）

开标时间：2025-11-14 09:30:00

开标地点：上海政府采购网（www.zfcg.sh.gov.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

根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目采购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。供应商应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在采购云平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

七、凡对本次采购提出询问，请按以下方式联系。

1.采购人信息

名　　称：上海市杨浦区数据局（上海市杨浦区信息化委员会、上海市杨浦区政务服务办公室）

地　　址：惠民路 800 号

联系方式：021-25031260、18964505975

2.采购代理机构信息

名　　称：　上海市杨浦区政府采购中心

地　　址：　宁国路129号16楼

联系方式：　65550185

3.项目联系方式

项目联系人：　王雄钦

电　　话：　65550160

第二章　　投标人须知

前附（置）表

一、项目情况

项目名称:详见第一章投标邀请

项目编号:详见第一章投标邀请

项目地址：惠民路 800 号

项目内容：全面建立杨浦区网络安全管理范式，构建网络安全数字底座，具备贯穿信息化项目建设前期规划、项目立项、项目实施、项目运维等全过程的能力，全面落实各项安全防护措施，构建安全生态、创新安全服务，建设完善的安全保障体系。

采购预算说明：本项目预算金额 1500 万，最高限价 1411.4 万元，超过最高限价作废标处理。

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

二、招标人

采购人

名称：**上海市杨浦区数据局（上海市杨浦区信息化委员会、上海市杨浦区政务服务办公室）**

邮编：200082

联系人：**刘文婧**

地　　址：**惠民路 800 号**

联系方式：**021-25031260、18964505975**

集中采购机构

名称：上海市杨浦区政府采购中心

地址：宁国路 129 号 16 楼

联系人：详见第一章投标邀请

电话：详见第一章投标邀请

传真：65636267

三、合格供应商条件

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：本采购项目执行政府采购有关鼓励支持节能产品、环境认证产品、支持中小企业、残疾人福利性单位、监狱企业等的政策规定。

3.本项目的特定资格要求：

详见第一章投标邀请

四、招标有关事项

招标答疑会：不召开
踏勘现场：不组织。
投标有效期：90 天
投标保证金：不收取

投标截止时间：详见投标邀请（招标公告）或延期公告（如果有的话）
递交响应文件方式和网址：
响应文件提交方式：由投标人在上海市政府采购云平台（门户网站：上海政府采购网）提交。
响应文件提交网址：http://www.zfcg.sh.gov.cn

开标时间和开标地点网址：
开标时间：同投标截止时间
开标地点网址：上海市政府采购云平台（门户网站：上海政府采购网，网址：http://www.zfcg.sh.gov.cn）

评标委员会的组建：详见第五章
评标方法：详见第五章
中标人推荐办法：详见第五章
中小企业政策：详见第三章

五、其它事项
付款方法：详见第四章《项目招标需求》
履约保证金：无

六、说明

根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目采购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。供应商应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在采购云平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

投标人须知

一、总则

1．概述

1．1 根据《中华人民共和国政府采购法》等有关法律、法规和规章的规定，本采购项目已具备招标条件。

1．2 本招标文件仅适用于《投标邀请》和《投标人须知》前附表中所述采购项目的招标采购。

1．3 招标文件的解释权属于《投标邀请》和《投标人须知》前附表中所述的采购人。

1．4 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

1.5 根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目招投标相关活动在上海市政府采购云平台（门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。

2. 定义

2．1 “采购项目”系指《投标人须知》前附表中所述的采购项目。

2．2 “服务”系指招标文件规定的投标人为完成采购项目所需承担的全部义务。

2．3 “招标人”系指《投标人须知》前附表中所述的组织本次招标的采购人。

2．4 “集中采购机构”系指上海市杨浦区政府采购中心。

2．5 “投标人”系指从招标人处按规定获取招标文件，并按照招标文件向招标人提交投标文件的供应商。

2．6 “中标人”系指中标的投标人。

2．7“甲方”系指采购人。

2．8“乙方”系指中标并向采购人提供服务的投标人。

2．9 招标文件中凡标有“★”的条款均系实质性要求条款。

2.10 “采购云平台”系指上海市政府采购云平台，门户网站为上海政府采购网（www.zfcg.sh.gov.cn），是由市财政局建设和维护。

3. 合格的投标人

3.1 符合《投标邀请》和《投标人须知》前附表中规定的合格投标人所必须具备的资格条件和特定条件。

3.2 《投标邀请》和《投标人须知》前附表规定接受联合体投标的，除应符合本章第3.1项要求外，还应遵守以下规定：

（1）联合体各方应按招标文件提供的格式签订联合体协议书，明确联合体各方权利义务、合同份额；联合体协议书应当明确联合体主办方、由主办方代表联合体参加采购活动；

（2）联合体中有同类资质的供应商按联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级；

（3）招标人根据采购项目的特殊要求规定投标人特定条件的，联合体各方中至少应当有一方符合采购规定的特定条件。

（4）联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政

4. 合格的服务

4.1 投标人所提供的服务应当没有侵犯任何第三方的知识产权、技术秘密等合法权利。

4.2 投标人提供的服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准，均有标准的以高（严格）者为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合采购目的的特定标准确定。

5. 投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用，招标人和集中采购机构在任何情况下均无义务和责任承担这些费用。

6. 信息发布

本采购项目需要公开的有关信息，包括招标公告、招标文件澄清或修改公告、中标公告以及延长投标截止时间等与招标活动有关的通知，集中采购机构均将通过“上海政府采购网”（http://www. zfcg. sh.gov.cn）公开发布。投标人在参与本采购项目招投标活动期间，请及时关注以上媒体上的相关信息，投标人因没有及时关注而未能如期获取相关信息，及因此所产生的一切后果和责任，由投标人自行承担，招标人和集中采购机构在任何情况下均不对此承担任何责任。

7. 询问与质疑

7.1 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.2 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向集中采购机构提出质疑。其中，对招标文件的质疑，应当在其收到招标文件之日（以采购云平台显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。

投标人应当在法定质疑期内一次性提出针对同一采购程序环节的质疑，超过次数的质疑将不予受理。以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

7.3 投标人可以委托代理人进行质疑。代理人提出质疑应当提交投标人签署的授权委托

书，并提供相应的身份证明。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

7.4 投标人提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

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

质疑函应当按照财政部制定的范本填写，范本格式可通过中国政府采购网（http://www.ccgp.gov.cn）右侧的“下载专区”下载。

7.5 投标人提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令第94号）及《上海市政府采购中心供应商询问、质疑处理规程》的规定办理。质疑函或授权委托书的内容不符合《投标人须知》第7.3条和第7.4条规定的，集中采购机构将当场一次性告知投标人需要补正的事项，投标人超过法定质疑期未按要求补正并重新提交的，视为放弃质疑。

质疑函的递交应当采取当面递交或邮寄递交形式。质疑联系部门：上海市杨浦区政府采购中心，联系电话：65550160 详见第一章投标邀请，地址：上海市杨浦区宁国路129号16楼。

7.6 集中采购机构将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人和其他有关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.7 对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的，集中采购机构将通知提出询问或质疑的投标人，并在原招标公告发布媒体上发布变更公告。

8. 公平竞争和诚实信用

8.1 投标人在本招标项目的竞争中应自觉遵循公平竞争和诚实信用原则，不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。“腐败行为”是指提供、给予任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行为；“欺诈行为”是指为了影响采购过程或合同实施过程而提供虚假材料，谎报、隐瞒事实的行为，包括投标人之间串通投标等。

8.2 如果有证据表明投标人在本招标项目的竞争中存在腐败、欺诈或其他严重违背公平

竞争和诚实信用原则、扰乱政府采购正常秩序的行为，招标人将拒绝其投标，并将报告政府采购监管部门查处；中标后发现的，中标人须参照《中华人民共和国消费者权益保护法》第55条之条文描述方式双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

8.3 招标人将在**开标后至评标前**，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。以上信用查询记录，招标人将下载查询结果页面后与其他采购文件一并保存。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

9. 其他

本《投标人须知》的条款如与《投标邀请》、《项目招标需求》和《评标方法》就同一内容的表述不一致的，以《投标邀请》、《项目招标需求》和《评标方法》中规定的内容为准。

二、招标文件

10. 招标文件构成

10.1 招标文件由以下部分组成：

（1）投标邀请（招标公告）；

（2）投标人须知；

（3）政府采购主要政策；

（4）项目招标需求；

（5）评标方法；

（6）投标文件有关格式；

（7）合同书格式和合同条款；

（8）本项目招标文件的澄清、答复、修改、补充内容（如有的话）。

10.2 投标人应仔细阅读招标文件的所有内容，并按照招标文件的要求提交投标文件。如果投标人没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件在各方面作出实质性响应，则投标有可能被认定为无效标，其风险由投标人自行承担。

10.3 投标人应认真了解本次招标的具体工作要求、工作范围以及职责，了解一切可能影响投标报价的资料。一经中标，不得以不完全了解项目要求、项目情况等为借口而提出额外补偿等要求，否则，由此引起的一切后果由中标人负责。

10.4 投标人应按照招标文件规定的日程安排，准时参加项目招投标有关活动。

11. 招标文件的澄清和修改

11.1 任何要求对招标文件进行澄清的投标人，均应在投标截止期15天以前，按《投标邀请》中的地址以书面形式（必须加盖投标人单位公章）通知招标人。

11.2 对在投标截止期15天以前收到的澄清要求，招标人需要对招标文件进行澄清、答复的；或者在投标截止前的任何时候，招标人需要对招标文件进行补充或修改的，集中采购机构将会通过“上海政府采购网”以澄清或修改公告形式发布,并通过采购云平台发送至已下载招标文件的供应商工作区。如果澄清或修改的内容可能影响投标文件编制的，且澄清或修改公告发布时间距投标截止时间不足15天的，则相应延长投标截止时间。延长后的具体投标截止时间以最后发布的澄清或修改公告中的规定为准。

11.3 澄清或修改公告的内容为招标文件的组成部分。当招标文件与澄清或修改公告就同一内容的表述不一致时，以最后发出的文件内容为准。

11.4 招标文件的澄清、答复、修改或补充都应由集中采购机构以澄清或修改公告形式发布和通知，除此以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，招标人和集中采购机构不承担任何责任。

11.5 招标人召开答疑会的，所有投标人应根据招标文件或者招标人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

12. 踏勘现场

12.1 招标人组织踏勘现场的，所有投标人应按《投标人须知》前附表规定的时间、地点前往参加踏勘现场活动。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

12.2 投标人踏勘现场发生的费用由其自理。

12.3 招标人在现场介绍情况时，应当公平、公正、客观，不带任何倾向性或误导性。

12.4 招标人在踏勘现场中口头介绍的情况，除招标人事后形成书面记录，并以澄清或修改公告的形式发布，构成招标文件的组成部分以外，其他内容仅供投标人在编制投标文件时参考，招标人不对投标人据此作出的判断和决策负责。

三、投标文件

13. 投标文件构成

13.1投标文件由商务响应文件（包括相关证明文件）和技术响应文件二部分构成。

13.2商务响应文件（包括相关证明文件）和技术响应文件应包含的内容，以第四章《项目招标需求》规定为准。

14. 投标的语言及计量单位

14.1 投标人提交的投标文件以及投标人与招标人就有关投标事宜的所有来往书面文件均应使用中文。除签名、盖章、专用名称等特殊情形外，以中文以外的文字表述的投标文件视同未提供。

14．2　投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，一律采用中华人民共和国法定计量单位（货币单位：人民币元）。

15. 投标有效期

15.1 投标文件应从开标之日起，在《投标人须知》前附表规定的投标有效期内有效。投标有效期比招标文件规定短的属于非实质性响应，将被认定为无效投标。

15.2 在特殊情况下，在原投标有效期期满之前，招标人可书面征求投标人同意延长投标有效期。同意延长有效期的投标人不能修改投标文件其他内容。

15.3 中标人的投标文件作为项目服务合同的附件，其有效期至中标人全部合同义务履行完毕为止。

16. 商务响应文件

16.1 商务响应文件由以下部分组成：

（1）《投标函》；

（2）《开标一览表》；

（3）《投标报价汇总表》等相关报价表格详见第六章《投标文件有关格式》；

（4）资格条件及实质性要求响应表；

（5）与评标有关的投标文件主要内容索引表；

（6）投标人关于报价等的其他说明（如有的话）。

（7）第四章《招标需求》规定的其他内容；

（8）相关证明文件（投标人应按照《项目招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同）。

17. 投标函

17.1 投标人应按照招标文件中提供的格式完整地填写《投标函》。

17.2 投标人不按照招标文件中提供的格式填写《投标函》，或者填写不完整的，评标时将按照第五章《评标方法》中的相关规定予以扣分。

17.3 投标文件中未提供《投标函》的，为无效投标。

18. 开标一览表

18.1 投标人应按照招标文件的要求和采购云平台提供的投标文件格式完整地填写《开标一览表》、报价明细表和报价构成表等，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

18.2 《开标一览表》是为了便于招标人开标，《开标一览表》内容在开标时将当众公布。开标一览表的内容应与投标报价明细表内容一致，不一致时以开标一览表内容为准。

18.3 投标人未按照招标文件的要求和采购云平台提供的投标文件格式完整地填写《开标一览表》、或者未提供《开标一览表》，导致其开标不成功的，其责任和风险由投标人自行承担。

19. 投标报价

19.1 投标人应当按照国家和上海市有关行业管理服务收费的相关规定，结合自身服务水平和承受能力进行报价。投标报价应是履行合同的最终价格，除《项目招标需求》中另有说明外，投标报价应当是投标人为提供本项目所要求的全部服务所发生的一切成本、税费和利润，包括人工（含工资、社会统筹保险金、加班工资、工作餐、相关福利、关于人员聘用的费用等）、设备、国家规定检测、外发包、材料（含辅材）、管理、税费及利润等。

19.2 报价依据：

（1）本招标文件所要求的服务内容、服务期限、工作范围和要求；

（2）本招标文件明确的服务标准及考核方式；

（3）其他投标人认为应考虑的因素。

19.3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

19.4 除《项目招标需求》中说明并允许外，投标的每一种单项服务的报价以及采购项目的投标总价均只允许有一个报价，投标文件中包含任何有选择的报价，招标人对于其投标均将予以拒绝。

19.5 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均将予以拒绝。

19.6 投标人应按照招标文件第六章提供的格式完整地填写各类报价表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

19.7 投标应以人民币报价。

20. 资格条件响应表及实质性要求响应表

20.1 投标人应当按照招标文件所提供格式，逐项填写并提交《资格条件及实质性要求响应表》，以证明其投标符合招标文件规定的所有合格投标人资格条件及实质性要求。

20.2 投标文件中未提供《资格条件及实质性要求响应表》的，为无效投标。

21．与评标有关的投标文件主要内容索引表

21．1　投标人应按照招标文件提供的格式完整地填写与评标有关的投标文件主要内容索引表。

21．2　与评标有关的投标文件主要内容索引表是为了便于评标。与评标有关的投标文件主要内容索引表与投标文件其他部分就同一内容的表述应当一致，不一致时按照《投标人须知》第 32 条“投标文件内容不一致的修正”规定处理。

22. 技术响应文件

22.1 投标人应按照《招标需求》的要求编制并提交技术响应文件，对招标人的技术需求全面完整地做出响应并编制服务方案，以证明其投标的服务符合招标文件规定。

22.2 技术响应文件可以是文字资料、表格、图纸和数据等各项资料，其内容应包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

23．相关证明文件

23.1　投标人应按照《项目招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同。

24．　投标保证金

不收取。

25．投标文件的编制和签署

25.1 投标人应按照招标文件和采购云平台要求的格式填写相关内容。

25.2 投标文件中凡招标文件要求签署、盖章之处，均应显示投标人的法定代表人或法定代表人正式授权的代表签署字样及投标人的公章。投标人名称及公章应显示全称。如果是由法定代表人授权代表签署投标文件，则应当按招标文件提供的格式出具《法定代表人授权委托书》（如投标人自拟授权书格式，则其授权书内容应当实质性符合招标文件提供的《法定代表人授权委托书》格式之内容）并将其附在投标文件中。投标文件若有修改错漏之处，须在修改错漏之处同样显示出投标人公章或者由法定代表人或法定代表人授权代表签署字样。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

其中对《投标函》《法定代表人授权委托书》《资格条件及实质性要求响应表》《投标诚信承诺书》以及《财务状况及税收、社会保障资金缴纳情况声明函》，投标人未按照上述要求签字和显示公章的，其投标无效。

25.3 投标人应按招标文件和政采云平台规定的内容、格式和顺序编制投标文件。凡招标文件提供有相应格式的，投标文件均应完整的按照招标文件提供的格式打印、填写并按要求在政采云平台上传。投标文件内容不完整、格式不符合导致投标文件被误读、漏读或者查找不到相关内容的，是投标人的责任，投标人需承担其投标在评标时因此被扣分甚至被认定为无效标的风险。

25.4 建设节约型社会是我国落实科学发展观的一项重大决策，也是政府采购应尽的义务和职责，需要政府采购各方当事人在采购活动中共同践行。目前，少数投标人制作的投标文件存在编写繁琐、内容重复的问题，既增加了制作成本，浪费了宝贵的资源，也增加了评审成本，影响了评审效率。为进一步落实建设节约型社会的要求，提请投标人在制作投标文件时注意下列事项：

（1）评标委员会主要是依据投标文件中技术、质量以及售后服务等指标来进行评定。因此，投标文件应根据招标文件的要求进行制作，内容简洁明了，编排合理有序，与招标文件内容无关或不符合招标文件要求的资料不要编入投标文件。

（2）投标文件应规范，应按照规定格式要求规范填写，扫描文件应清晰简洁、上传文件应规范。

四、投标文件的递交

26. 投标文件的递交

26.1 投标人应按照招标文件规定，参考第六章投标文件有关格式，在采购云平台中按照要求填写和上传所有投标内容。投标的有关事项应根据采购云平台规定的要求办理。

26.2 投标文件中含有公章，防伪标志和彩色底纹类文件（如《投标函》、营业执照、身份证、认证证书等）应清晰显示。如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。

招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供，否则投标人须接受可能对其不利的评标结果，并且招标人将对该投标人进行调查，发现有弄虚作假或欺诈行为的按有关规定进行处理。

26.3 投标人应充分考虑到网上投标可能会发生的技术故障、操作失误和相应的风险。对因网上投标的任何技术故障、操作失误造成投标人投标内容缺漏、不一致或投标失败的，招标人和集中采购机构不承担任何责任。

27. 投标截止时间

27.1 投标人必须在《投标邀请（招标公告）》规定的网上投标截止时间前将投标文件在采购云平台中上传并正式投标。

27.2 在招标人按《投标人须知》规定酌情延长投标截止期的情况下，招标人和投标人受投标截止期制约的所有权利和义务均应延长至新的截止时间。

27.3 在投标截止时间后上传的任何投标文件，招标人均将拒绝接收。

28. 投标文件的修改和撤回

在投标截止时间之前，投标人可以对在采购云平台已提交的投标文件进行修改和撤回。有关事项应根据采购云平台规定的要求办理。

五、开标

29. 开标

29.1 集中采购机构将按《投标邀请》或《延期公告》（如果有的话）中规定的时间在采购云平台上组织公开开标。

29.2 开标程序在采购云平台进行，所有上传投标文件的供应商应登录采购云平台参加开标。开标主要流程为签到、解密、唱标和签名，每一步骤均应按照采购云平台的规定进行操作。

29.3 投标截止，采购云平台显示开标后，投标人进行签到操作，投标人签到完成后，由集中采购机构解除采购云平台对投标文件的加密。投标人应在规定时间内使用数字证书对其投标文件解密。签到和解密的操作时长分别为半小时，投标人应在规定时间内完成上述签到或解密操作，逾期未完成签到或解密的投标人，其投标将作无效标处理。有证据能证实是

因系统原因导致投标人无法在上述要求时间内完成签到或解密的除外。

如采购云平台开标程序有变化的，以最新的操作程序为准。

29.4 投标文件解密后，政采云平台根据各投标人填写的《开标一览表》的内容自动汇总生成《开标记录表》。

投标人应及时使用数字证书对《开标记录表》内容进行签名确认，投标人因自身原因未作出确认的视为其确认《开标记录表》内容。

六、评标

30. 评标委员会

30.1 招标人将依法组建评标委员会，评标委员会由采购人代表和上海市政府采购评审专家组成，其中专家的人数不少于评标委员会成员总数的三分之二。

30.2 评标委员会负责对投标文件进行评审和比较，并向招标人推荐中标候选人。

31. 投标文件的资格审查及符合性审查

31.1 开标后，招标人将依据法律法规和招标文件的《投标人须知》、《资格条件及实质性要求响应表》，对投标人进行资格审查。确定符合资格的投标人不少于 3 家的，将组织评标委员会进行评标。

31.2 在详细评标之前，评标委员会要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。评标委员会只根据投标文件本身的内容来判定投标文件的响应性，而不寻求外部的证据。

31.3 符合性审查未通过的投标文件不参加进一步的评审，投标人不得通过修正或撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。

31.4 开标后招标人拒绝投标人主动提交的任何澄清与补正。

31.5 招标人可以接受投标文件中不构成实质性偏差的小的不正规、不一致或不规范的内容。

32. 投标文件内容不一致的修正

32.1 投标文件报价出现前后不一致的，按照下列规定修正：

（1）《开标记录表》报价与投标文件中报价不一致的，以《开标记录表》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《开标记录表》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，按照上述规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

32.2 除《投标人须知》第 33 条规定的澄清、说明或者补正情形之外，《开标记录表》内容与投标文件中相应内容不一致的，以《开标记录表》为准。

33. 投标文件的澄清、说明或者补正

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

33.2 投标人的澄清、说明或者补正应当按照招标人通知的时间和方式以书面形式提交给招标人，并加盖公章，或者由法定代表人或其授权的代表签字。

33.3 投标人的澄清、说明或者补正文件是其投标文件的组成部分。

33.4 投标人的澄清、说明或者补正不得超出投标文件的范围或者改变其投标文件的实质性内容。

34. 投标文件的评价与比较

34.1 评标委员会只对被确定为实质上响应招标文件要求的投标文件进行评价和比较。

34.2 评标委员会根据《评标方法》中规定的方法进行评标，并向招标人提交书面评标报告和推荐中标候选人。

35. 评标的有关要求

35.1 评标委员会应当公平、公正、客观，不带任何倾向性，评标委员会成员及参与评标的有关工作人员不得私下与投标人接触。

35.2 评标过程严格保密。凡是属于审查、澄清、评价和比较有关的资料以及授标建议等，所有知情人均不得向投标人或其他无关的人员透露。

35.3 任何单位和个人都不得干扰、影响评标活动的正常进行。投标人在评标过程中所进行的试图影响评标结果的一切不符合法律或招标规定的活动，都可能导致其投标被拒绝。

35.4 招标人、集中采购机构和评标委员会均无义务向投标人做出有关评标的任何解释。

七、定标

36. 确认中标人

除了《投标人须知》第36条规定的招标失败情况之外，采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

37. 中标公告及中标和未中标通知

37.1 采购人确认中标人后，集中采购机构将在两个工作日内通过“上海政府采购网”发布中标公告，公告期限为一个工作日。

37.2 中标公告发布同时，集中采购机构将向中标人发出《中标通知书》通知中标，向其他未中标人发出《中标结果通知书》。《中标通知书》对招标人和投标人均具有法律约束力。

38. 投标文件的处理

所有在开标会上被接受的投标文件都将作为档案保存,不论中标与否，招标人均不退回投标文件。

39. 招标失败

在投标截止后，参加投标的投标人不足三家；在资格审查时，发现符合资格条件的投标人不足三家的；或者在评标时，发现对招标文件做出实质性响应的投标人不足三家，评标委员会确定为招标失败的，集中采购机构将通过“上海政府采购网”发布招标失败公告。

八、授予合同

40. 合同授予

除了中标人无法履行合同义务之外，招标人将把合同授予根据《投标人须知》第 33 条规定所确定的中标人。

41. 签订合同

41.1 中标人与采购人应当在《中标通知书》发出之日起 30 日内签订政府采购合同。

41．2　中标人应根据合同条款的规定，按照招标文件中提供的履约保证金格式向采购人提交履约保证金。

42. 其他

采购云平台有关操作方法可以参考采购云平台（网址：www.zfcg.sh.gov.cn）中的**“操作须知”**专栏。

第三章 政府采购主要政策

根据政府采购法，政府采购应当有助于实现国家的经济和社会发展政策目标，包括保护环境，扶持不发达地区和少数民族地区，促进中小企业发展等。

列入财政部、发展改革委发布的《节能产品政府采购品目清单》中强制采购类别的产品，按照规定实行强制采购；列入财政部、发展改革委、生态环境部发布的《节能产品政府采购品目清单》和《环境标志产品政府采购品目清单》中优先采购类别的产品，按规定实行优先采购。

中小企业按照《政府采购促进中小企业发展管理办法》享受中小企业扶持政策，对预留份额项目专门面向中小企业采购，对非预留份额采购项目按照规定享受价格扣除 20 %优惠政策。中小企业应提供《中小企业声明函》。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。对于专门面向中小企业采购，则不再执行价格评审优惠的扶持政策。

非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予 20%的扣除，用扣除后的价格参与评审；非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额30%以上的投标人，给予其报价 6%的扣除，用扣除后的价格参与评审。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。组成联合体的大中型企业或者其他自然人、法人或其他组织，与小型、微型企业之间不得存在投资关系。

在政府采购活动中，监狱企业和残疾人福利性单位视同小微企业，监狱企业应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件，残疾人福利性单位应当提供《残疾人福利性单位声明函》。

如果有国家或者上海市规定政府采购应当强制采购或优先采购的其他产品和服务，按照其规定实行强制采购或优先采购。

第四章　项目招标需求

一、项目概述

见附件

二、技术需求

见附件

说明：

为保证招标的合法性、公平性，投标人认为上述技术需求指标存在排他性或歧视性条款，可在收到或下载招标文件之日起七个工作日内提出并附相关证据，招标人将及时进行调查或组织论证，如情况属实，招标人将对上述相关技术需求指标做相应修改。

三、服务标准与履约验收要求

1、投标人提供的服务应符合国家、地方及相关政府管理部门和行业与本项目有关的各项服务标准、规范、规章要求，并满足采购人实际需求，标准、规范等不一致的，以要求高的为准。

2、本项目将按照合同约定的履约验收方案进行验收。

四、付款要求：

付款方法：根据合同的有关规定，按照下列方法和比例付款：

1、中标供应商在签订合同完毕后 30 天内，招标方支付中标供应商合同金额的 50%；主体项目建设内容交付后的 30 天内，支付合同金额的 30% 。达成项目指标要求并完成整体项目验收且合格后的 15 天内，依据《杨浦区时空要素平台（一张图）服务考核暂行办法》对服务进行考核，由财务监理方根据评分结果，出具最终的项目结算审核报告。审核报告出具后在 30 天内支付相应尾款款项。

2、所有付款支付前，供应商需开具足额对应发票。

五、投标文件的编制要求

投标人应按照第二章《投标人须知》“三、投标文件”中的相关要求编制投标文件，投标文件的商务响应文件（包括相关证明文件）和技术响应文件应当包括（但不限于）下列内容：

1、投标人提交的商务标应由以下部分组成：

（1）投标函

（2）开标一览表（在采购云平台填写）

（3）报价汇总表

（4）资格条件及实质性要求响应表

（5）与评标有关的投标文件主要内容索引表

（6）客观分评审因素响应情况表

（7）法定代表人授权委托书、法人身份证和被授权人身份证；

（8）提供投标人营业执照（或事业单位、社会团体法人证书）；

（9）财务状况及税收、社会保障资金缴纳情况声明函；

（10）享受政府采购优惠政策的相关证明材料，包括：中小企业声明函、监狱企业证明文件、残疾人福利性单位声明函等**（中标人为中小企业、残疾人福利性单位的，其声明函将随中标结果同时公告）**；

（11）投标人基本情况简介；

（12）投标人认为可以证明其能力、业绩、信誉和信用的其他相关材料；

（13）投标人债务纠纷、违法违规记录等方面的情况（如果有的话）；

（14）联合投标时，提供《联合投标协议书》。

（15）提供具有投标人公章、法定代表人和授权代表签字或盖章的《投标诚信承诺书》

（16）投标人与采购项目相关的资质证书（加盖投标人公章）

（17)投标人委托其依法设立的分支机构代表其参加本项目采购活动的，提供《委托书》。

2．技术响应文件由以下部分组成：

（1）投标人对采购项目总体需求的理解以及投标的服务方案。

（2）按照本招标文件要求提供的其他技术性资料以及投标人需要说明的其他事项。

（3）同类及类似项目的业绩（包括类似项目的合同扫描件，合同扫描件中需体现合同的签约主体、项目名称及内容、合同金额、服务日期等合同要素的相关内容，否则不算有效的类似项目业绩。投标人需提供的类似项目数量以《评分细则》为准）。

上传扫描文件要求：

投标人应按照招标文件规定提交彩色扫描文件，并按照规定在政采云平台上传其所有资料，文件格式参考第六章投标文件有关格式。含有公章，防伪标志和彩色底纹类文件（如投标函、营业执照、身份证、认证证书等）必须采用原件彩色扫描以清晰显示。如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。

招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供。否则视作投标人放弃潜在中标资格，并且招标人将对该投标人进行调查，发现有欺诈行为的按有关规定进行处理。

第五章　评标方法与程序

一、资格审查

招标人将依据法律法规和招标文件的《投标人须知》、《资格条件及实质性要求响应表》，对投标人进行资格审查。确定符合资格的投标人不少于3家的，将组织评标委员会进行评标。

二、投标无效情形

1.投标文件不符合《资格条件及实质性要求响应表》所列任何情形之一的，将被认定为无效投标。

2.单位负责人或法定代表人为同一人，或者存在直接控股、管理关系的不同供应商，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效。

3.不同投标人技术方案实质性内容雷同、错漏一致，或投标文件混装等情形的，视为串通投标，相关投标无效。

4.投标人被列入信用中国网站失信被执行人、重大税收违法主体、政府采购严重违法失信名单的，其投标无效。

5.除上述以及政府采购法律法规、规章、《投标人须知》所规定的投标无效情形外，投标文件有其他不符合招标文件要求的均作为评标时的考虑因素，而不导致投标无效。

三、评标方法与程序

1.评标方法

根据《中华人民共和国政府采购法》及政府采购相关规定，结合项目特点，本项目采用“综合评分法”评标，总分为100分。

2.评标委员会

2.1本项目具体评标事务由评标委员会负责，评标委员会由采购人的代表和上海市政府采购评审专家组成。招标人将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家。

2.2评标委员会成员应坚持客观、公正、审慎的原则，依据投标文件对招标文件响应情况、投标文件编制情况等，按照《投标评分细则》逐项进行综合、科学、客观评分。

2.3评标委员会成员应独立评审并签字确认评分结果，对评分畸高畸低（偏离平均值±30%）者需书面说明理由。

3.评标程序

本项目评标工作程序如下：

3.1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。

3.2 澄清有关问题。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，评标委员会应当以书面形式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，并加盖公章，或者由法定代表人或其授权的代表签字，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。

3.3 比较与评分。评标委员会按招标文件规定的《投标评分细则》，对符合性审查合格的投标文件进行评分。

3.4 推荐中标候选供应商名单。各评委按照评标办法对每个投标人进行独立评分，再计算平均分值，评标委员会按照每个投标人最终平均得分的高低依次排名，推荐得分最高者为第一中标候选人，依此类推。如果供应商最终得分相同，则按报价由低到高确定排名顺序，如果报价仍相同，则由评标委员会按照少数服从多数原则投票表决。

4.评分细则

本项目具体评分细则如下：

4.1 投标价格分按照以下方式进行计算：

（1）价格评分：报价分＝价格分值×（评标基准价/评审价）

（2）评标基准价：是经符合性审查合格（技术、商务基本符合要求，无重大缺、漏项）满足招标文件要求且投标价格最低的投标报价。

（3）评审价：投标报价无缺漏项的，投标报价即评审价；投标报价有缺漏项的，按照其他投标人相同项的最高报价计算其缺漏项价格，经过计算的缺漏项价格不超过其投标报价10%的，其投标报价也即评审价，缺漏项的费用视为已包括在其投标报价中，经过计算的缺漏项价格超过其投标报价 10%的，其投标无效。

（4）非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予 20%的扣除，用扣除后的价格参与评审；非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额 30%以上的投标人，给予其报价 6%的扣除，用扣除后的价格参与评审，未提供联合协议或者分包意向协议的，不享受价格扣除优惠政策。以联合体或分包形式参加政府采购活动，联合体各方或分包企业及接受分包企业各方均为中小企业的，联合体或分包企业视同中小企业，其中，联合体各方或分包企业及接受分包企业各方均为小微企业的，联合体或分包企业视同小微企业。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。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。中小企业及联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额 30%以上的联合体、分包企业，应提供《中小企业声明函》。如果本项目专门面向中小企业采购，则不再执行价格评审优惠的扶持政策。

（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，评标委员会应当将其作为无效投标处理。

4.2 投标文件其他评分因素及分值设置等详见《投标评分细则》。

5.评标说明

允许分支机构以自身名义参加政府采购活动的项目，分支机构在投标文件中提供的资格证书、人员、业绩等材料，应当为其自身所有，不得使用其法人、非法人组织（或其他分支机构）的材料。

投标评分细则（100 分）

评分项目	分值区间	类型	评分办法
报价分	0~10	客观分	以满足招标文件要求的所有投标单位报价的最低价作为评标基准价，其价格分为满分。其他投标人的价格分按下列公式计算：投标报价得分=（评标基准价/投标报价）×价格权值×100
项目需求理解	1~3	专家打分	根据投标人项目需求理解的全面性、透彻性、完整性：包括需求理解的准确性，对业务流程的梳理，能做出实质性响应，且能详细描述本项目建设内容，进行综合打分。
重要技术指标分	0~10	客观分	▲条款为重要技术指标，每满足 1 条得 0.5 分，满分 10 分。不提供不得分。▲条款详见招标需求中▲条款列表。▲符号为重要技术指标参数，须提供产品操作界面功能截图证明或三方权威机构的评估报告，证明材料需加盖公章，请对▲条款证明材料进行显著醒目标注。
整体项目技术方案	1~4	专家打分	根据投标人整体项目技术方案的完整性、科学性、可操作性等进行综合评价。
态势感知管理平台	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就态势感知管理平台进行规划设计，方案描述清楚程度、是否完善，相关内容理解深度程度，根据方案设计的完整性、科学性、可操作性等进行综合打分。
网络空间治理平台	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就网络空间治理平台进行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
暴露面风险管理平台	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就暴露面风险管理平台进行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
数据安全管控平台	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就数据安全管控平台进行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
网络空间测绘平台	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就网络空间测绘平台进行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
DNS 安全平台	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就 DNS 安全平台行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
城市网络安全体征监测管理系统	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就城市网络安全体征监测管理系统进行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
城市治理数智化安全能力系统	1~4	专家打分	投标人结合对本项目现状情况的需求分析，就城市治理数智化安全能力系统进行规划设计，根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整

			性、科学性、可操作性等进行综合打分。
城市网络空间安全公共服务系统	1~4	专家打分	投标人结合对本项目现状情况的需求分析,就城市网络空间安全公共服务系统进行规划设计,根据设计方案描述清楚、完善的程度，相关内容理解程度以及方案设计的完整性、科学性、可操作性等进行综合打分。
项目服务方案	1~3	专家打分	根据投标人所提供的项目服务方案的合理性、可操作性和服务内容的完整性，进行综合打分。
项目实施方案	1~3	专家打分	根据投标人提供的项目实施方案，项目进度计划（包括但不限于进度安排时间表、各环节实施周期、进度偏差调整机制等）安排情况的合理性、可行性进行综合打分。
项目验收方案	1~3	专家打分	根据投标人提供的项目验收方案，验收条件的合理性、可行性进行综合打分。
安全保密方案	1~3	专家打分	根据投标人所提供的项目安全保密方案，包括数据安全，人员密保等方案的完整性和可行性，进行综合打分。
项目负责人	0~5	客观分	项目负责人需具备项目管理技能认证中级或以上（1 分）、网络安全技能认证中级或以上（如计算机技术与软件专业技术资格（水平）考试）（1 分）、安全能力类认证（CISP 注册信息安全专业人员证书）（1 分）、数据安全类认证（如中国信息安全测评中心-注册数据安全治理专业人员）（1 分），具有 5 年以上信息化项目且担任项目经理职务的工作经验，需提供工作经验的证明材料,包括但不限于项目验收证明或者甲方开具的工作证明等（1 分），项目负责人须提供半年内任意 1 月社保缴纳记录，提供每项证明得一分，不提供证明材料不得分。
项目服务团队	0~3	客观分	项目服务团队人员具有信息系统项目管理师（高级）证书，有 1 个得 1 分，最多得 3 分；同一人员具有多项证书不重复计分。所有人员提供最近六个月任意一个月依法缴纳社保费的证明，需醒目标注，不提供不得分。
	0~3	客观分	项目服务团队人员具有注册信息安全专业人员证书，有 1 个得 1 分，最多得 3 分；同一人员具有多项证书不重复计分。所有人员提供最近六个月任意一个月依法缴纳社保费的证明，需醒目标注，不提供不得分。
售后服务方案	1~4	专家打分	根据投标人提供的售后服务方案，售后服务方案应完整、合理,承诺具体故障级别采取对应的应急响应,驻场安排，同时需包含培训计划、培训期限、 培训人员、培训等内容进行综合打分。
业绩证明	0~5	客观分	提供近 2022 年 1 月 1 日至投标截止前与本项目招标内容类似项目相关案例，提供一份得 1 分，最高得 5 分，附合同复印件并加盖公章，不提供或提供不满足要求不得分。

企业综合实力	0~5	客观分	投标人提供 1、ISO28000 供应链安全管理体系证书 的证书； 2、信息安全管理体系认证 ISO27001 的证书； 3、CCRC 信息安全服务资质-软件安全开发证书； 4、DSMM 数据安全能力成熟度模型二级及以上认证证书； 5、CCRC 信息安全服务资质-安全集成一级证书； 须提供有效期内的证书，未在有效期内不得分。 每提供一个资质得 1 分，最高得 5 分，不提供或提供不在有效期内不得分。

附：1、上述计算结果四舍五入后保留 2 位有效小数，按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按技术指标优劣顺序排列。

2、最低报价不是被授予合同的保证。

第六章　　投标文件有关格式

一、商务响应文件有关格式

1、投标函格式

致：_____（招标人名称）

根据贵方_____（项目名称、招标编号）采购的招标公告及投标邀请，_____（姓名和职务）被正式授权代表投标人（投标人名称、地址），按照上海市政府采购云平台规定向贵方提交投标文件 1 份。

据此函，投标人兹宣布同意如下：

1.按招标文件规定，我方的投标总价为_____（大写）元人民币。

2.我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

3.投标有效期为自开标之日起 _____日。

4.如我方中标，投标文件将作为本项目合同的组成部分，直至合同履行完毕止均保持有效，我方将按招标文件及政府采购法律、法规的规定，承担完成合同的全部责任和义务。

5.我方同意向贵方提供贵方可能进一步要求的与本投标有关的一切证据或资料。

6.我方完全理解贵方不一定要接受最低报价的投标或其他任何投标。

7.我方已充分考虑到投标期间网上投标可能会发生的技术故障、操作失误和相应的风险，并对因网上投标的任何技术故障、操作失误造成投标内容缺漏、不一致或投标失败的，承担全部责任。

8. 我方同意开标内容以上海市政府采购云平台开标时的《开标记录表》内容为准。我方授权代表将及时使用数字证书对《开标记录表》中与我方有关的内容进行签名确认，授权代表未进行确认的，视为我方对开标记录内容无异议。

9.为便于贵方公正、择优地确定中标人及其投标货物和相关服务，我方就本次投标有关事项郑重声明如下：

（1）我方向贵方提交的所有投标文件、资料都是准确的和真实的。

（2）我方不是采购人的附属机构或与采购存在其他利害关系。

（3）以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

地址：_____

电话、传真：_____

邮政编码：_____

开户银行：_____

银行账号：_____

投标人授权代表签名：_____

投标人名称（公章）：_____

日期：_____年___月___日

2、开标一览表格式

项目名称：

招标编号：

上海市杨浦区数据局杨数浦“ABCD”安全运营矩阵项目包 1

包名称	服务周期（需用文字明确表述：建设期、试运行期和免费运维期）	付款方式是否满足招标文件要求（是/否）	最终报价(总价、元)

说明：(1)“金额（元)”指每一包件投标报价，所有价格均系用人民币表示，单位为元，精确到分。

（2）开标一览表内容与投标文件其它部分内容不一致时以开标一览表内容为准。

（3）投标人应按照《项目招标需求》和《投标人须知》的要求报价。

3、投标报价汇总表格式

项目名称：
招标编号：
包号：

1. 成品软件组成清单：

序号	平台名称	数量	单位
1	态势感知管理平台	1	套
2	网络空间治理平台	1	套
3	暴露面风险管理平台	1	套
4	数据安全管控平台	1	套
5	网络空间测绘平台	1	套
6	DNS 安全平台	1	套

2.定制化开发软件模块清单：

城市网络安全体征监测预警管理系统：

序号	一级功能模块清单	二级功能模块清单	单位	综合单价	小计
1	研判分析子系统	关联组合分析	人月		
		阈值分析	人月		
		序列分析	人月		
		基线分析	人月		
		攻击者分析	人月		
		场景分析	人月		
		实体分析	人月		
		威胁预警分析	人月		
2	安全联动子系统	编排与自动化管理	人月		
		剧本管理	人月		
		应用管理	人月		
		安全告警分诊	人月		
		事件告警关联分析	人月		
		安全事件管理	人月		
3	资产中心	资产目录	人月		
		资产管理	人月		

		资产运营	人月		
		暴露入口管理	人月		
		脆弱性管理	人月		
		漏洞管理	人月		
		弱口令管理	人月		
		基线核查管理	人月		
		WEB 漏洞管理	人月		
		安全隐患管理	人月		
4	外部数据源对接子系统	与运维管理平台对接	人月		
		与统一日志平台对接	人月		
		与云安全管理系统对接	人月		
		与终端安全管理系统对接	人月		
		与云端威胁情报系统对接	人月		
5	体征大屏	体征态势首页	人月		
		资产体征态势	人月		
		全网脆弱性体征态势	人月		
		外部威胁态势	人月		
		内部威胁态势	人月		
6	视图管理	视图自定义	人月		
		视图操作	人月		
7	业务协同	指令接收	人月		
		漏洞协同管理	人月		
		钓鱼情报接收	人月		
		协同监控	人月		
		数据报送	人月		
8	工作指挥	事件管理	人月		
		事件通知	人月		
		工单管理	人月		
		统计报表	人月		
		组织与权限管理	人月		
		风险预警	人月		
		应急指挥	人月		
		预案编排	人月		
9	安全管理	拓扑管理	人月		
		分级管理	人月		

		通报预警	人月		
		设备监控	人月		

城市治理数智化安全能力系统：

序号	一级功能模块清单	二级功能模块清单	单位	综合单价	小计
1	数据资产发现子系统	数据资产识别	人月		
		敏感数据资产	人月		
		存储资产管理	人月		
		应用资产管理	人月		
		账号资产管理	人月		
		数据载体管理	人月		
		数据资产管理	人月		
2	数据分类分级子系统	分类分级模板	人月		
		数据分类分级	人月		
		分类分级版本管理	人月		
		数据资产安全态势	人月		
3	数据流动监测子系统	流动监测视角	人月		
		流动监测过程	人月		
		流动监测内容	人月		
		流动监测图谱	人月		
4	数据安全分析子系统	告警分析	人月		
		数据安全分析规则管理	人月		
		报表管理	人月		
		报告管理	人月		
5	安全响应处置子系统	数据安全事件管理	人月		
		数据安全事件处置	人月		
		数据安全风险管理	人月		
6	数据安全大屏子系统	数据流动态势	人月		
		数据安全态势	人月		
		数据分布态势	人月		
7	数据外发管理子系统	日志外发	人月		
		数据清除	人月		
8	通用管理子系统	用户管理	人月		
		操作日志	人月		
		用户登录	人月		

		系统安全	人月		
		策略配置	人月		

城市网络空间安全公共服务系统

序号	一级功能模块清单	二级功能模块清单	单位	综合单价	小计
1	基础功能	检索方式	人月		
		网站列表页	人月		
		资产详情页	人月		
		企业详情页	人月		
		证书详情页	人月		
		域名详情页	人月		
		导出方式	人月		
		个人中心	人月		
		帮助中心	人月		
		下载中心	人月		
		更新日志	人月		
2	监管功能	测绘数据概览页	人月		
		通用漏洞专题	人月		
		icp 备案专题	人月		
		Database 专题	人月		
		OA 专题	人月		
		Web servers 专题	人月		
		重大漏洞预警专题	人月		
		高危协议专题	人月		
3	网站监测	监测类型	人月		
		DNS 运营分析	人月		
		域名监控	人月		
4	报告中心	周期性报告	人月		
		周期报告任务管理	人月		
		自定义报告	人月		
5	系统配置	监测配置	人月		
		运营配置	人月		

说明：（1）所有价格均系用人民币表示，单位为元/年，精确到分。

（2）投标人应按照《项目招标需求》和《投标人须知》的要求报价。

（3）投标人应根据分类报价费用情况编制明细费用表并随本表一起提供。

（4）分项目明细报价合计应与开标一览表报价相等。

4、资格条件及实质性要求响应表

项目名称：
包号：

项目内容(资格条件、实质性要求)	具备的条件说明（要求）	投标检查项（响应内容说明(是/否)）	详细内容所对应电子投标文件名称	备注
法定基本条件	提供营业执照（或事业单位、社会团体法人证书）符合要求			
法定基本条件	提供财务状况及税收、社会保障资金缴纳情况声明函并加盖公章			
法定基本条件	提供信用查询截图。同时，招标人和评标委员会将通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将拒绝其参与政府采购活动。			
法定代表人授权	在投标文件由法定代表人授权代表签字（或盖章）的情况下，应按招标文件规定格式提供法定代表人授权委托书。			
法定代表人授权	按招标文件要求提供法人身份证和被授权人身份证			
投标诚信承诺书	提供具有投标人公章、法定代表人和授权代表签字或盖章的《投标诚信承诺书》			
联合投标	本项目不接受联合投标			
公平竞争和诚实信用	招标人和评标委员会审查，未发现本项目存在串通投标、违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。评标过程中发现投标人有上述情形的，评标委员会将认定其投标无效，并书面报告本级财政部门。			

投标报价	本项目预算金额 1500 万，最高限价 1411.4 万元，超过最高限价作废标处理。			
投标有效期	投标有效期符合招标文件规定：不少于 90 天。			
付款方式	付款条件满足招标文件要求			
合同转让与分包	本项目合同不得转让、不得分包。			
其他	符合招标文件实质性响应的其它条款			

_____投标人授权代表签字：

_____投标人（公章）：

日期：　　年　　月　　日

5.客观分评审因素响应情况表

序号	名称	是否响应	响应情况	响应材料对应在投标文件中的页码
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
……				

6、与评标有关的投标文件主要内容索引表

项目名称：

包号：

项目内容	具备的条件说明	响应内容说明(是/否)	详细内容所对应电子投标文件名称及页码	备注
1				
2				
3				
4				
……				

说明：上述具体内容要求可以参照本项目评标方法与程序及评分细则。

7、法定代表人授权书格式

致：上海市杨浦区政府采购中心

我_____（姓名）系注册于_____（地址）的_____（投标人名称，以下简称我方）的法定代表人，现代表我方授权委托我方在职职工_____（姓名，职务）以我方的名义参加贵中心_____项目的投标活动，由其代表我方全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务，并签署全部有关的文件、协议及合同。

我方对被授权人的签名事项负全部责任。

在贵中心收到我方撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。

被授权人无转委托权，特此委托。

在此粘贴 法人身份证和被授权人身份证，原件彩色扫描 （复印件须加盖投标人公章）

投标人公章：	受托人（代理人）（签字）：
法定代表人(签字或盖章)：	住所：
邮政编码：	身份证号码：
电话：	邮政编码：
传真：	电话：
日期：	传真：
	日期：

8、投标人基本情况简介格式

（一）基本情况：

1、单位名称：

2、地址：

3：邮编：

4、电话/传真：

5、成立日期或注册日期：

6、行业类型：

（二）基本经济指标（到上年度 12 月 31 日止）：

1、实收资本：

2、资产总额：

3、负债总额：

4、营业收入：

5、净利润：

6、上交税收：

7、从业人数：

（三）其他情况：

1、专业人员分类及人数：

2、企业资质证书情况：

3、其他需要说明的情况：

我方承诺上述情况是真实、准确的，我方同意根据招标人进一步要求出示有关资料予以证实。

投标人授权代表签字：_____

投标人（公章）：_____

日期：_____年_____月_____日

9、中小企业声明函（服务）

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

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

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

……

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：

说明：（1）本声明函所称中小企业，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。事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

（2）本声明函所称服务由中小企业承接，是指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，否则不享受中小企业扶持政策。

（3）采购项目涉及多个采购标的（主要采购标的，不包括配件、辅料等）且由不同供应商承接的，应当逐一填报每个采购标的的承接供应商信息。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。分支机构受委托或被授权参加本项目采购活动的，应当按照设立该分支机构的企业数据进行填报，仅填报分支机构数据的声明函将不被认可。

（4）采购标的对应的中小企业划分标准所属行业，以招标文件第二章《投标人须知》规定为准。

（5）中标人享受中小企业扶持政策的，其在投标客户端中“中小企业声明函”一栏上传的文件将自动随中标结果同时公告。供应商请勿在投标客户端“中小企业声明函”一栏上传投标文件其他内容，否则因自动公告该栏文件导致中标人商业秘密等信息泄露的，招标人不承担任何责任。（实际以采购云平台最新的操作程序为准）

（6）供应商在投标客户端“中小企业声明函”一栏与投标文件中，多处上传本声明函的，以投标客户端“中小企业声明函”一栏上传的作为认定依据。

注：各行业划型标准：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

10、残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位安置残疾人___人，占本单位在职职工人数比例___%，符合残疾人福利性单位条件，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：

说明：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》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：

（1）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）；

（2）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；

（3）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；

（4）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；

（5）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）。

中标人为残疾人福利性单位的，本声明函将随中标结果同时公告。

如投标人不符合残疾人福利性单位条件，无需填写本声明。

11、投标诚信承诺书

本公司郑重承诺:

本公司参加本次政府采购活动前三年内,在经营活动中没有重大违法记录,将遵循公开、公平、公正和诚信守信的原则，参加_____项目的投标。

一、所提供的一切材料都是真实、有效、合法的。

二、不与采购人、其他供应商或者采购机构串通投标，损害国家利益、社会利益和他人的合法权益。

三、不向采购人或评标委员会成员或相关人员行贿，以谋取中标。

四、不以他人名义投标或者其他方式弄虚作假，骗取中标。

五、不接受任何形式的挂靠，不扰乱招投标市场秩序。

六、不在投标中哄抬价格或恶意压价。

七、不在招投标活动中进行虚假、恶意的质疑和投诉。

八、保证所提供的所有货物、服务均无专利权、商标权、著作权或其他知识产权等有侵害他方的行为。

九、保证中标之后，按照投标文件承诺履约、实施项目。

十、本公司若有违反承诺内容的行为，愿意承担相应的法律责任。如已中标的，自动放弃中标资格；给采购人造成损失的，依法承担赔偿责任，

投标供应商全称：_____（盖章）

投标供应商地址：_____

法定代表人（签字或盖章）：_____手机：_____

授权代理人（签字或盖章）：_____手机：_____

年　　月　　日

12. 财务状况及税收、社会保障资金

缴纳情况声明函

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1. 具有健全的财务会计制度；

2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

13.对分支机构的委托书

委托书（如有）

致：上海市杨浦区政府采购中心

（分支机构名称）系我单位依法设立的分支机构，现我单位委托（分支机构名称）作为我单位唯一的受托人，以我单位的名义参加贵中心（项目名称及编号）项目的投标活动，并代表我单位全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务和签署相关文件。

我单位对（分支机构名称）的签章事项及投标活动负全部责任。

在贵中心收到我单位撤销本委托书面通知以前，本委托书一直有效。受托人在本委托书有效期内签署的所有文件不因委托的撤销而失效。

受托人无转委托权，特此委托。

委托人（公章）：

地址：

邮政编码：

电话：

传真：

日期： 年 月 日

受托人（公章）：

地址：

邮政编码：

电话：

传真：

14、《联合投标协议书》格式（如有）

联合投标各方：

甲方：

法定代表人：

住所：

乙方：

法定代表人：

住所：

（如果有的话，可按甲、乙、丙、丁…序列增加）

根据《政府采购法》第二十四条之规定，为响应上海市杨浦区政府采购中心组织实施的项目（项目名称、招标编号）的招标活动，各方经协商，就联合进行投标之事宜，达成如下协议：

一、各方一致决定，以 _____ 为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的合同份额为　　元，乙方承担的合同份额为　　元。

甲方承担的工作和义务为:

乙方承担的工作和义务为：

五、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

六、本协议一式三份，甲、乙双方各持一份，另一份作为投标文件的组成部分提交杨浦区政府采购中心。

甲方（盖章）：　　乙方（盖章）：

法定代表人（签字）：　　法定代表人（签字）：

20　年　月　日　　20　年　月　日

二、技术响应文件有关表格格式

1、项目负责人情况表

项目名称：
招标编号：
包号：

姓名		出生年月		文化程度		毕业时间	
毕业院校和专业			从事本类项目工作年限			联系方式	
职业资格			技术职称			聘任时间	
主要工作经历： 主要管理服务项目： 主要工作特点： 主要工作业绩： 胜任本项目负责人的理由：							

2、主要管理、技术人员配备及相关工作经历、职业资格汇总表

项目名称：

招标编号：

包号：

项目组成员姓名	年龄	在项目组中的岗位	学历和毕业时间	职称及职业资格	进入本单位时间	相关工作经历	联系方式
……							

3、同类或类似项目业绩：投标人近年承接的与本项目类似项目一览表格式

序号	年份	项目名称	项目内容	服务时间	合同金额（万元）	业主情况		
						单位名称	经办人	联系方式
1								
2								
3								
4								

三、各类银行保函格式

1、预付款银行保函格式

致：_____（采购人名称）

鉴于_____（乙方名称）（以下简称“乙方”）根据___年月___日与贵方签订的_____号合同（以下简称“合同”）向贵方提供（服务描述）。

根据贵方在合同中规定，乙方要得到预付款，应向贵方提交由一家信誉良好的银行出具的、金额为_____（以大写和数字表示的保证金金额）的银行保函，以保证其正确和忠实地履行所述的合同条款。

我行_____（银行名称）根据乙方的要求，无条件地和不可撤消地同意作为主要责任人而且不仅仅作为保证人，保证在收到贵方第一次要求就支付给贵方不超过（以大写和数字表示的保证金金额），我行无权反对和不需要先向乙方索赔。

我行进而同意，要履行的合同条件或买卖双方签署的其他合同文件的改变、增加或修改，无论如何均不能免除我行在本保函下的任何责任。我行在此表示不要求接到上述改变、增加或修改的通知。

本保函自收到合同预付款起直至　　年　　月　　日前一直有效。

出证行名称：_____

出证行地址：_____

经正式授权代表本行的代表的姓名和职务（打印和签字）：_____

银行公章：_____

出证日期：_____

说明：1、本保函应由商业银行的总行、**分行或者支行出具，支行**以下机构出具的保函恕不接受。

2、本保函由中标人在合同签订后提交。

第七章　　合同格式

包 1 合同模板：

[合同中心-合同名称]

合同统一编号： [合同中心-合同编码]

项目名称：上海市杨浦区数据局杨数浦“ABCD”安全运营矩阵项目

合同各方：

甲方：**[合同中心-采购单位名称]**

地址：**[合同中心-采购单位所在地]**

电话：**[合同中心-采购单位联系人电话]**

乙方：**[合同中心-供应商名称]**

法定代表人：**[合同中心-供应商法人姓名]**

（**[合同中心-供应商法人性别]**）

地址：**[合同中心-供应商所在地]**

电话：**[合同中心-供应商联系人电话]**

联系人：[合同中心-采购单位联系人]　　联系人：[合同中心-供应商联系人]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1．乙方根据本合同的规定向甲方提供以下服务：

1．1 乙方所提供的服务其来源应符合国家的有关规定，服务的内容、要求、服务质量等详见合同附件。

2. 合同价格、服务地点和服务期限

2．1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 服务地点：详见招标文件要求

2．3 服务期限

本服务的服务期限：[合同中心-合同有效期] 项目整体建设周期：6 个月，试运行 1 个月（不包含在项目建设周期内）。本项目要求中标单位提供一年免费软件维保服务，从项目验收之日起计算，包括所有系统及服务。

3．质量标准和要求

3．1 乙方所提供的服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3．2 乙方所交付的服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保

4．1 乙方保证对其交付的服务享有合法的权利。

4．2 乙方保证在服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4．3 乙方保证其所交付的服务没有侵犯任何第三人的知识产权和商业秘密等权

利。

4．4 如甲方使用该服务构成上述侵权的，则由乙方承担全部责任。

5．验收

5．1 服务根据合同的规定完成后，甲方应及时进行根据合同的规定进行服务验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的10个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至服务完全符合验收标准。

5．3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

5．4 甲方根据合同的规定对服务验收合格后，甲方收取发票并签署验收意见。

6．保密

6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7．付款

7．1 本合同以人民币付款（单位：元）。

7．2 本合同款项按照以下方式支付。

7．2．1 付款内容：（分期付款）

7．2．2 付款条件：

付款方法：根据合同的有关规定，按照下列方法和比例付款：

1、中标供应商在签订合同完毕后30天内，招标方支付中标供应商合同金额的50%；主体项目建设内容交付后的30天内，支付合同金额的30% 。达成项目指标要求并完成整体项目验收且合格后的15天内，依据《“ABCD”安全运营矩阵平台服务考核暂行办法》对服务进行考核，由财务监理方根据评分结果，出具最终的项目结算审核报告。审核报告出具后在30天内支付相应尾款款项。

2、所有付款支付前，供应商需开具足额对应发票。

8．甲方（甲方）的权利义务

8．1、甲方有权在合同规定的范围内享受，对没有达到合同规定的服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的服务内容、或者服务无法达到合同规定的服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供服务，其支付的服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方服务质量或延误服务的原因，使甲方有关或系统损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的服务期限内有义务为乙方创造服务工作便利，并提供适合的工作环境，协助乙方完成服务工作。

8．5 当或系统发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8． 6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同服务范围调整的，应与乙方协商解决。

9．乙方的权利与义务

9．1 乙方根据合同的服务内容和要求及时提供相应的服务，如果甲方在合同服务范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急服务时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成服务延误或不能达到服务质量的，乙方不承担违约责任。

9．4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同系统正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供服务的费用。

9．8 乙方保证在服务中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在服务期限内，如果乙方对提供服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供服务。

11．2 如乙方无正当理由而拖延服务，甲方有权没收乙方提供的履约保证金（如有，以付款方式约定为准），或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

12．误期赔偿

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期服务的服务费用的百分之零点五（0.5%）计收，直至提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13．不可抗力

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．履约保证金（如有）

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为/元人民币的履约保证金(以付款方式为准)。履约保证金应自出具之日起至全部服务按本合同规定验收合格后三十天内有效。在全部服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15．争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同

有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15．3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17．破产终止合同

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章后生效。

19．2 本合同一式叁份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20．合同附件

20．1 本合同附件包括： 招标(采购)文件、投标（响应）文件。

20. 2 本合同附件与合同具有同等效力。

20. 3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21. 合同修改

21. 1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

附件：

履约验收方案

<table>
<tr><td colspan="5">一、验收组织</td></tr>
<tr><td>验收组织方式</td><td colspan="4">☑自行组织/☐委托第三方</td></tr>
<tr><td>验收主体</td><td colspan="4">上海市杨浦区数据局(上海市杨浦区信息化委员会、上海市杨浦区政务服务办公室)</td></tr>
<tr><td colspan="5">二、验收方式与程序</td></tr>
<tr><td>邀请本项目的其他供应商参加验收</td><td colspan="2">☐是/ ☑否</td><td>邀请专家参加验收</td><td>☑是/☐否</td></tr>
<tr><td>邀请服务对象参加验收</td><td colspan="2">☐是/ ☑否</td><td>第三方检测机构参加验收</td><td>☑是/☐否</td></tr>
<tr><td rowspan="2">参加抽查检测</td><td colspan="2">☐是/ ☑否</td><td rowspan="2">存在破坏性检测</td><td colspan="2">☐是/ ☑否</td></tr>
<tr><td>抽查比例</td><td></td><td>被破坏的检测产品处理方式</td><td></td></tr>
<tr><td>履约验收方式</td><td colspan="2">☑一次性验收/☐分期验收</td><td>履约验收时间</td><td colspan="2">供应商提出验收申请之日起 30 日内组织验收</td></tr>
<tr><td>验收程序</td><td colspan="4">自行组织验收</td></tr>
<tr><td colspan="5">三、验收内容与标准</td></tr>
<tr><td>序号</td><td colspan="2">验收环节</td><td>验收内容</td><td>验收标准</td></tr>
<tr><td>1</td><td colspan="2">平台功能验收</td><td>按照投标文件应答的功能点进行逐一验收</td><td>100%覆盖</td></tr>
<tr><td>2</td><td colspan="2">项目指标验收</td><td>参考项目指标进行达成确认</td><td>100%完成</td></tr>
</table>

[合同中心-补充条款列表]

签约各方：

甲方（盖章）：　　乙方（盖章）：

合同签订点:网上签约

附件：

技术需求

项目名称：上海市杨浦区数据局杨数浦“ABCD”安全运营矩阵项目。

预算金额：本项目预算金额 1500 万，最高限价 1411.4 万元，超过最高限价作废标处理。

服务周期：项目整体建设周期：6 个月，试运行 1 个月（不包含在项目建设周期内）。本项目要求中标单位提供一年整体软件维保服务，从项目验收之日起计算，包括所有定制化开发软件和成品软件及相关配套服务。

一、建设目标

（一）项目背景

一是强化“1235”专项行动安全保障，需要构建新一代体系化、数智化安全运营体系。为贯彻杨浦区十一届区委第十次全会中关于“提升韧性安全水平”的工作要求，引用发改数据【2024】660 文件中关于提升城市安全韧性水平的定义：加强城市数字空间安全管理，健全完善网络安全监测预警和应急处置机制，构建城市网络运行安全管理体系；加快推进城市数据安全体系建设，依法依规加强数据收集、存储、使用、加工、传输、提供、公开等全过程

安全监管，落实数据分类分级保护制度，压实数据安全主体责任。

二是杨浦区数智化转型引入大量新兴技术，面临安全保障技术升级的压力。在兼顾传统风险的同时，应针对大模型应用特有的数据泄露、模型攻击、内部滥用等问题，提供针对性的防护体系，涵盖大模型应用的训练、评估、部署、上线和日常运营等各类风险场景。在政务大模应用场景中提供全链条安全技术支撑，为政务大模型安全稳定运行提供可信安全环境。

三是提升“超大城市”数字空间安全韧性。围绕超大城市在人口、城市治理、经济结构等特性，提升全区各委办单位的城市治理业务中网络和数据安全的集约建设、统筹管理能力；增强全区重要企业的营商环境中网络安全服务支撑能力。

四是国家对新时期政务数据安全有序高效共享利用明确了新的、更高的目标要求。基于杨浦区城市治理运行数智化转型过程中的政务数据共享场景，保障政务数据汇聚与流转的政务数据共享安全可靠。

（二）项目目标

本次建设智能公共服务平台，目标是通过深度应用智能技术，构建覆盖服务区各部门及政务服务全场景的智能化支撑体系，实现两大核心目标：

本项目作为立足于杨浦区数智化安全底座统一规划、集约建设的目标，提供杨浦区城市数字空间共性安全能力和服务。构建杨浦区面向全域的“一屏可观”“一屏可管”的综合安全态势能力，面向城市治理运行数智化转型过程中政务数据共享场景提供安全保障能力支撑，面向全区互联网企业、国有企业提供监测预警与通知处置的公共支撑服务。打造安全韧性城市中网络空间内生的、平战结合的、协同的、智慧的数字空间安全底座。

（一）构建超大城市数字空间安全韧性建设方案标杆

通过构建一体化运营中心，提供标准化、可量化安全运营服务，聚焦提升城市治理高效公共服务领域，打造超大城市数字空间安全韧性解决方案。

（二）提升全区营商环境网络空间安全保障，构建全区重点企业的监测预警公共服务能力

通过网络空间测绘、威胁雷达等能力，整体把控全区互联网资产安全风险态势，为全区重要企业、园区等提供风险预警与情报威胁研判等公共服务，为杨浦区营商环境网络空间安全提供全局支撑。

发展数字经济数据创新技术，推进政务数据共享安全体系建设，保障政务数据可信流转。

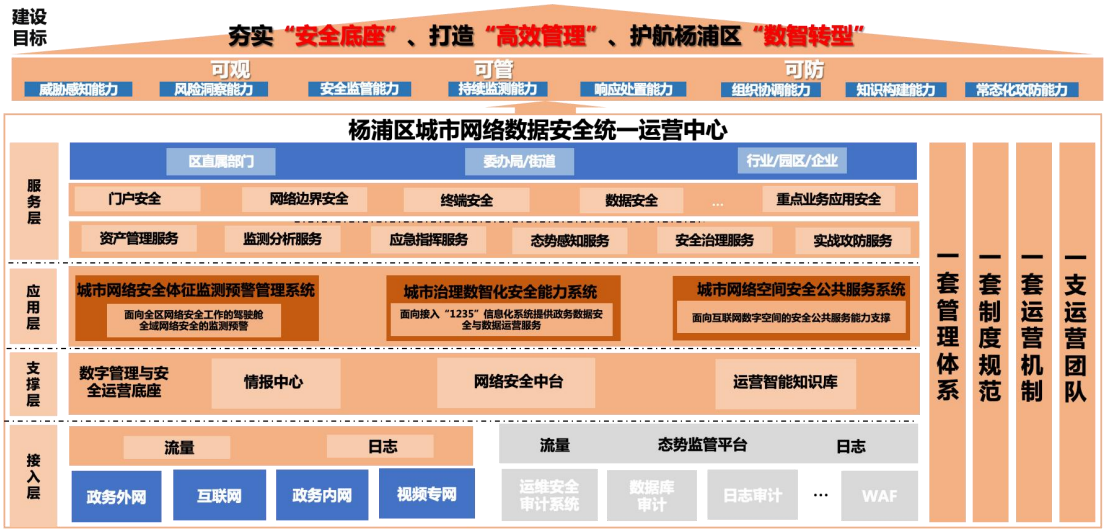
通过构建安全高效稳定运行的政务数据共享体系，对 1235 专项行动政务数据共享过程中的数据流转活动进行全量监测并风险预警，实现数据资产发现、流动监测、安全分析、响应处置等功能。

项目建成后，在不改变原有各委办单位安全责任主体划分的前提下，实现对全区企业互联网暴露资产提供基于网络空间测绘技术的安全预警监测与处置建议等公共支撑服务，全区

接入“1235”专项行动的政务信息化系统实现统一监测预警，并具备通知和协同指挥的能力；实现对以数据局为安全责任主体的政务信息化系统进行监测预警的同时，具备闭环处置能力。

全面建立杨浦区网络安全管理范式，构建网络安全数字底座，具备贯穿信息化项目建设前期规划、项目立项、项目实施、项目运维等全过程的能力，全面落实各项安全防护措施，构建安全生态、创新安全服务，建设完善的安全保障体系。

（三）项目建设内容



蓝色为服务对象与范围
橙色为平台与产品功能
灰色为已有安全设备接入

本项目是杨浦城市治理运行数智化专项行动、打造全国城市网络安全运营样板的前瞻布局，对全区信息安全产业创新发展具有重要推动作用。围绕杨浦区数智城市示范城市和数字政府建设需求，通过引入城市网络安全运营的服务能力，开展城市网络安全体系的规划建设、管理运营、监督治理、创新研究、人才培育和产业促进等工作。

(1)杨浦区城市网络安全体征监测预警管理系统

部署杨浦区城市网络安全体征监测预警管理系统，面向全域网络安全体征监测实现一屏可观、一屏可观的综合能力平台。平台功能定位顺应网络及网络安全技术发展趋势，深入推进网络安全治理，推动并强化各方协同处置，大力促进互联网健康有序发展。

(2)杨浦区城市治理数智化安全能力系统

部署杨浦区城市治理数智化安全能力系统，面向政务数据安全高效有序共享利用过程中，数据流通的安全防护与管控，实现数据使用可控可计量，数据流通可信可追溯；同时基于攻防视角建设政务数据可信空间，支撑数字经济数字创新技术应用。

(3)城市网络空间公共服务平台

部署城市网络空间公共服务平台，以网络空间测绘技术发现资产暴露面，并结合漏洞情报信息形成杨浦区网络空间地图，及时发布存在漏洞风险的空间资产情报，主动通知关联企业；同时面向全区网站提供网站资产安全告警服务，针对违规内容、网站黑链、网站挂马等

威胁隐患及时发现并告知；对于提供授权的企业，可提供通过变更 DNS 指向，向企业提供威胁拦截、自定义资产检测等运营分析能力。

（四）项目数据来源

区电子政务云、电子政务外网按三级等保要求进行建设运营，于重要节点部署了不同功能的安全设备，以保护区政务云、公共数据和政务网络安全。

项目系统需采集现有网络安全产品告警，利用现有设备作为数据来源。项目旨在构建纵深防御体系，整合边界防护、身份认证、数据加密等安全能力，打破云数网设备管理壁垒，实现策略统一配置与威胁联动处置，形成跨域协同防护网络；打造全域态势感知系统，通过区内现有安全设备，如终端行为、安全设备日志等多源数据采集，结合大数据分析实现威胁秒级响应与处置，构建可视化安全大脑；实现数据全生命周期安全管理、威胁感知、风险预警联动，保障跨域数据流通安全，构建"防御-感知-治理"三位一体安全新范式，为数字政府建设提供安全保障。

二、需求依据

（一）国发[2022] 14 号《国务院关于加强数字政府建设的指导意见》

第三章构建数字政府全方位安全保障体系提出“全面强化数字政府安全管理责任，落实安全管理制度，加快关键核心技术攻关，加强关键信息基础设施安全保障，强化安全防护技术应用，切实筑牢数字政府建设安全防线。”1、强化安全管理责任 2、落实安全制度要求 3、提升安全保障能力 4、提高自主可控水平

（二）发改数据[2024] 660 号《深化智慧城市发展推进城市全域数字化转型的指导意见》

是为全面落实 2024 年政府工作报告关于“深入推进数字经济创新发展”“建设智慧城市”要求，将城市作为推进数字中国建设的综合载体，而起草的意见。第二章第十条提升城市安全韧性水平提出：“加强城市数字空间安全管理，健全完善网络安全监测预警和应急处置机制，构建城市网络运行安全管理体系，提升通信网络韧性。加快推进城市数据安全体系建设，依法依规加强数据收集、存储、使用、加工、传输、提供、公开等全过程安全监管，落实数据分类分级保护制度，压实数据安全主体责任。推进建设有韧性的城市数据可信流通体系，健全数据要素流通领域数据安全实时监测预警、数据安全事件通报和应急处理机制。”

（三）《政务数据共享条例》（第六章第三十五条）

提出“政府部门应当建立健全政务数据共享安全管理制度，落实政务数据共享安全管理主体责任和政务数据分类分级管理要求，保障政务数据共享安全。政府部门应当采取技术措施和其他必要措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用。政府部门应当加强政务数据安全风险监测，发生政务数据安全事件时，立即启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。”

（四）2022 年，《关于全面推进上海城市数字化转型的意见》

第四条以数据要素为核心，形成新治理力和生产力中提出“构建具有活力的数据运营服务生态，积极完善数字贸易要素流动机制，探索形成信息便利化体系，引导建立数据治理和安全保障体系”；第八条重构数字时代的社会管理规则中提出“加强数据、系统、网络、产品、安全等标准体系建设。围绕数据安全、网络安全，加快构建与城市数字化转型相适应的大安全格局。”

（五）2022 年，《上海城市数字化转型标准化建设实施方案》

第三章第一条提出“聚焦信息安全、链路安全、数据安全防护，研制实施数据资源全流程监测、生物特征及用户习惯采集和应用管理、数据跨境流通安全评估等标准,以标准化支撑构建城市数字化转型的大安全格局。”

（六）上海市人民代表大会常务委员会公告〔十五届〕第 127 号《上海市促进人工智能产业发展条例》

第五章产业治理与安全第六十四条提出“本市坚持总体国家安全观，统筹人工智能产业发展与安全，保障产业链供应链安全。相关部门应当依法对人工智能应用开展安全检查和监管。”

（七）《关于推进杨浦区城市治理运行数智化工作方案的汇报》

提出“强化安全保障，落实数据分类分级保护、信息安全等级保护和个人信息保护制度，健全安全风险评估、安全责任落实、安全应急处置等相关机制。筑牢安全管理防线，完善安全运营管理机制，明确各部门安全管理责任边界，落实主体责任和监督责任，加强安全事件的协同处置，强化对参与政府信息化建设和运营企业的规范管理。”

三、区内现状

目前全区政务信息化现状共梳理出 141 项信息化系统，涉及 40 余委办单位 1500 台云主机，机关单位、街道在用终端数量约 8500 台，780 余接入点。全区大数据资源平台基本建成，实现国家、市、区三级数据资源一站式检索与共享；一体化三网平台建设效果显现，联动政务办公、城市运行、政务服务。全区基于市区政务云、互联网、物联网边界的防护自 2021 年建成已显成效，现有的运维团队基于边界的日志审计、堡垒机、漏扫等安全产品形成边界防护运维机制。

目前，数智化变革正在全面重塑城市治理模式、发展模式以及生活方式，而网络安全作为城市发展的必要基础，对城市的保护性、关键性作用日益突出。一方面，杨浦区现阶段的数字政府、数智城市建设具有信息和数据高度汇集、高度融合特点，越来越多的数据和不同的系统整合到一个平台运行，同时各个系统的关联度越来越强，承载的业务、终端、受众群体越来越多，越来越多样，与企业生产和民众生活利益息息相关，涉及到企业和民众生活的方方面面；另一方面，大量系统端口延伸到社区和街道等基层网点，面临着网络分区跨度大、业务与数字化挂钩多、网络安全建设分散单一等特点，传统的“见招拆招、头疼医头、脚疼医脚”式传统网络安全防御方式无法应对数智时代新型的挑战，亟须建立新的安全认知及框

架体系。

四、项目需求

（一）成品软件功能需求

1. 态势感知管理平台

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
1	事件管理	字段配置	事件字段配置功能支持列表字段配置、检索字段配置、导出字段配置。列表字段配置功能支持对列表展示的字段进行配置；检索字段配置功能支持对检索的字段进行配置；导出字段配置功能支持对导出事件的字段进行配置。	
2		事件配置	支持事件字段的自定义配置以及事件页面模板的配置；自定义字段支持设置字段的中文名称、中文别名、英文名称、字段类型、输入方式、字段描述、校验规则、规格描述、默认取值，字段是否可检索、是否可编辑；页面模板配置支持配置页面展示的字段以及字段分组，支持每行展示的字段数，支持设置展示的页签；	
3		事件删除	支持安全事件的逻辑删除与物理删除，支持安全事件的单个删除以及批量删除，逻辑删除的事件能够支持恢复操作；	
4	分析引擎管理	▲内置规则（提供相关功能的界面截图并加盖公章）	系统内置 732 条分析规则，涵盖有害程序、攻击利用、信息破坏、拒绝服务、异常活动、信息收集、安全隐患以及后渗透行为；支持按 ATT&CK 进行分类展示，包括资源开发、收集、渗出、防御规避、影响、执行、持久化、发现、侦察、初始访问、凭证访问、命令与控制、提权、横向移动、防御绕过；支持按攻击链进行分类展示，包括侦查追踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成	

			目标；	
5		新建规则	新建分析规则	
6	指令协同	指令管理	支持按照我收到的和我发出的对工单进行管理。支 持工单的创建、下发、工单信息编辑、模版编辑与 工单的跟踪。	
7		消息管理	支持消息下发的创建、下发通道的选择、下发对象 以及相关消息模版的编辑。	
8		协同请求	支持下级和其他协同对象对 YB 的协同请求手段。 包括协同请求执行的内容以及需要协调的对象。	
9		审核人员过滤	创建指令时，审核领导下拉列表仅支持选择当前单位且有审核权限的人，过滤掉其他单位和无审核权限的人员，且支持人员的模糊查询。	
10		发送方式优化	发送方式中，平台为可操作项，不能置灰；其他项置灰，暂不支持。	
11		审批撤回	已提交的审批在已读前可撤回	
12		签收意见设计一致性优化	验证驳回后，签收意见设计与初始签收设计保持一致。	
13		接收方情况概览优化	接收方情况概览页面中，发送者可直接通过页面表单查看反馈内同和附件信息	
14		用户意见录入优化	所有反馈意见、驳回意见等用户意见录入框采用多行文本设计且新增上传附件模块；	
15		审核意见优化	审核意见页面，提供默认审核意见。	
16		新建指令优化	新建时，关联指令下拉项显示格式为“标题名称(指令编号)”；下拉列表支持模糊查询。	

17		接收方支持单位	增加接收方支持选择单位下发指令	
18		岗位配置	增加岗位配置	
19		审核优化	审核操作 1 退回 2 编辑 3 通过 4 再向上级报审。三级审核工作人员、处长、局长三级。	
20		流程信息优化	流程信息优化，建议按照阶段显示，如创建阶段、审核阶段、执行阶段、验证阶段、归档阶段，并显示不同阶段的执行状态；	
21		关联指令优化	关联指令相关逻辑优化；	
22	流程预案	▲流程预案展示（提供相关功能的界面截图并加盖公章）	支持卡片的方式对流程预案进行展示，支持分类分组进行预案的管理。	
23		流程预案新建	支持对流程预案的新建。包括名称、描述、创建 人、创建时间、更新时间、预案类型以及启停状态 等。	
24		流程预案编辑	支持对流程预案的编辑，包括变更分组、重命名 等。每次编辑后形成修订历史记录。	
25		流程预案删除	支持对流程预案的删除，对已经被引用的预案需要 提示流程预案已经被引用，不能删除。	
26		流程预案分组	支持对预案进行自定义的分组管理。支持拖动修改 分组。	
27		流程预案启用停用	支持对预案进行启用、停用。启用的预案才能被业 务流程引用。	
28		流程步骤拖拽编排	支持对管理措施手段以拖拽的方式拖入画布，使用 连线的方式进行时序的连接以及各类网关(分支或 聚合)形成流程预案。	
29		措施手段管理	支持对管理措施的分类管理包括 APP 动作、API、 子流程、人工任务、审批、页面配置措施以及脚本 等手段类型。按照不同的措施类型进行分组的管 理。930 节点重点考虑定期上报事件、零报送手 段。	
30		逻辑运算节点	支持对流程中进行分支和聚合的网关操作。	

31		流程阶段配置	支持对阶段的配置，每个阶段可配置为相应的子流 程预案或执行单个或多个措施手段。	
32		预案管理微改造	重新定义预案管理范围，预案管理包含突发事件应急处置、应急演练 2 类业务涉及的预案，作为流程管理下独立子菜单进行管理展示。	
33		工作方案管理新增	作为流程管理下独立子菜单进行工作方案管理展示，将日常事件通报、重要活动保障、重大风险预警、专项任务 4 类业务涉及的工作方案，统一纳入工作方案管理。	
34		流程配置节点 ID 优化	预案/方案配置简介中【节点 ID】为系统自动带出，作为标签显示,不可编辑。	
35		去掉流程编排右侧冗余的【取消】按钮	去掉流程编排右侧冗余的【取消】按钮；	
36		流程配置简介命名优化	预案/方案配置简介中【XXX 简介】中的 XXX 按照手段、阶段、子流程、逻辑节点 4 类，当选择某一个元件时系统自动生成。	
37		流程阶段属性统一配置优化	预案/方案流程编排时，【阶段】的属性统一在右侧配置简介中进行配置。	
38		预案/方案编排支持子流程	预案/方案支持子流程编排，预案/方案配置简介可选择审批后同类型子流程。	
39		预案/方案子流程在线查看	预案/方案子流程的配置简介中，【去配置】改为【查看子流程】，可查看预案/方案子流程图及子流程各元件配置。	
40		预案/方案编排支持逻辑节点	预案/方案支持【聚合】、【分支】逻辑节点编排，可以对有逻辑分支、逻辑聚合的手段进行编排。	
41		流程编排连线规范	对预案管理和工作方案管理的流程编排元件连线进行初步规范。	
42		元件选中高亮突出显示	支持流程中点击元件，元件高亮突出显示，便于知晓当前选中哪个元件；同时元件拖拽到画布中时，该元件默认被选中。	
43		预案/工作方案管理启停图标更换	更换预案管理和工作方案管理页面的启停图标按钮（比如换成√、×等）	

44		▲流程编排优化（提供相关功能的界面截图并加盖公章）	流程编排优化：1、自有页面手段和人工手段简介配置页面优化（逻辑节点固定条件下拉框选项为“=”，且条件后边值域改为下拉框，选项为 0 和 1）；2、开始、结束不能点击“delete”键删除，且不能往阶段中拖（如果拖动阶段到画布上挡住了开始、结束，开始、结束要自动规避移动位置）；3、支持单个元件从阶段内拖动到画布中任意位置；4、支持按住左键框选流程（开始、结束、连线、手段、阶段及子预案、逻辑节点等），进行画布中拖动、从画布拖到阶段、从阶段拖到画布等拖动场景；5、逻辑节点（分支、聚合）输入参数只有一个，默认将该参数填充显示在下拉框中。	
45		按照不同业务进行手段过滤	通过治理资源中手段配置（选择单个或多个预置标签），区分哪些业务可以使用哪些手段，在流程编排时按照预案/方案类型进行手段过滤展示及使用（业务“6+1”）	
46		流程编排优化	流程编排优化：1、自有页面手段和人工手段简介配置页面优化（逻辑节点固定条件下拉框选项为“=”，且条件后边值域改为下拉框，选项为 0 和 1）；2、开始、结束不能点击“delete”键删除，且不能往阶段中拖（如果拖动阶段到画布上挡住了开始、结束，开始、结束要自动规避移动位置）；3、支持单个元件从阶段内拖动到画布中任意位置；4、支持按住左键框选流程（开始、结束、连线、手段、阶段及子预案、逻辑节点等），进行画布中拖动、从画布拖到阶段、从阶段拖到画布等拖动场景；5、逻辑节点（分支、聚合）输入参数只有一个，默认将该参数填充显示在下拉框中。	

47	重大活动保障	重保工作列表	列表展示当前系统中所有的工作列表（已删除工作除外）列表项支持单项工作执行状态的展示信息，包括重保等级、工作启动事件、预期结束事件、重保对象个数、已处置工作数量等信息。	
48		重保工作检索	支持按重保工作分类、分级条件检索重保工作	
49		重保工作添加	支持创建新的重保工作	
50		重保工作信息编辑	支持对重保工作基础信息进行修改	
51		重保工作删除	支持重保工作删除(需要用户确认)	
52		重保工作复制	基于现有重保工作创建新的重保工作	
53		工作任务界面	基于工作流程编排，按照选择的预案组 装形成工作任务界面，包括阶段导航、 任务导航，阶段导航支持工作时间区间 配置	
54		快捷指令面板	工作任务界面中的浮动指令面板，支持 当前阶段、任务相关的指令列表展示、 列表搜索、指令创建	
55		业务协同	复用指令系统界面(我发出的、我收到 的)，仅展示此任务关联的指令	
56		事件风险管理	复用事件管理界面(实现上报事件的查 询、展示、编辑和删除)	
57		单项重保工作图形化展示	支持对单项重保工作流程中历史执行任 务环节，按时间顺序的图形化展示	
58		工作流程修订	支持业务用户对单项工作流程图形化展 示结果进行修订和持久化保存操作，支 持修订调整预定义工作流	
59		确定重保对象	针对单项重保工作中的被保护目标进行 配置	
60		组建专家队伍	针对单项重保中的技术支持团队进行配置	
61		组建技术支持团队	针对单项重保中的技术支持团队进行配置	
62		零报告管理	查看各重保支撑单位上报的零报告上报 情况	
63		工作总结	实现重保工作总结报告的上传和下载	

64		重保报送任务列表	展示当前单位需要进行重保报送的任务 卡片，点击任务卡片进入具体重保工作 的信息报送界面	
65		重保报送列表	展示当前单位已报送的零报告列表，包 括上报时间、上报人	
66		重保报送创建	零报告创建表单，用于提交一个零报告， 可选择零报告关联的重保任务	
67	应急指挥	应急管理	从重保管理的事件风险管理中发起应急处置	
68		巡检研判	从事件风险巡检研判中发起应急处置	
69		应急处置	应急处置工作列表展示，包括基于级别、类型、工作状态进行列表筛选	
70		应急处置工作创建	应急处置工作创建	
71		应急处置工作编辑	应急处置工作编辑	
72		应急处置工作删除	应急处置工作删除	
73		应急处置工作基本信息	应急处置工作基本信息展示，包括基本信息、研判信息、审核信息	
74		应急处置工作相关事件列表	应急处置工作相关事件列表展示，事件搜索及事件详情展示	
75		应急处置工作相关报告	应急处置工作相关报告列表展示，报告搜索和下载	
76		应急处置工作评估报告添加	应急处置工作评估报告添加	
77		应急处置工作评估报告编辑	应急处置工作评估报告编辑	
78		应急装备列表	应急装备列表展示，装备搜索和下载	
79		应急装备添加	应急装备添加	
80		应急装备编辑	应急装备编辑	
81		应急处置工作任务	应急处置工作任务根据应急预案自动组装生成	
82		应急处置工作流程动态调整	应急处置工作流程动态调整	
83		应急处置工作流程另存为新流程模板	应急处置工作流程另存为新流程模板	
84		应急处置指令协同	应急处置指令协同功能，包含我发出的和我收到的	
85		应急处置工作相关上报信息展示	应急处置工作相关上报信息展示	
86		应急手段	应急手段：组织专家研判，并录入专家研判结论和建议	

87		应急手段研判审核	应急手段：研判审核，根据事件情况及专家研判信息，提请领导审核确定是否启动应急，并确定响应级别	
88		应急手段启动应急响应	应急手段：启动应急响应，向相关单位发布应急响应指令，通知事件级别和应急响应级别	
89		应急响应级别调整	应急手段：应急响应级别调整，向相关单位发布应急响应级别变更指令，通知更新后的事件级别和应急响应级别	
90		结束应急响应	应急手段：结束应急响应，向相关单位发布应急响应结束指令，通知该项应急响应工作结束	
91		会商记录	会商记录，完成会议时间、参会人员、会议决议的信息记录	
92		信息上报	支持相关单位在应急响应期间的信息上报	
93		评估报告	支持相关单位在应急响应期间的评估报告上传	
94		应急装备上传	支持相关单位在应急响应期间的应急装备上传	
95		应急处置手段：应急值班	应急处置手段：应急值班	
96		应急处置工作流程	应急处置工作流程及工作进展展示	
97	资源治理	单位管理	支持对已创建的单位进行统一管理，列表形式展示每条单位信息；	
98		添加单位	支持添加单位，添加单位基本信息，包括：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。	
99		删除单位	支持删除单个单位列表信息	
100		单位查看/编辑	支持查看/编辑单位详情，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；	
101		单位关系查看	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。	

102		人员管理	支持对已创建的人员进行统一管理，列表形式展示每条人员信息；	
103		添加人员	支持添加人员，添加人员基本信息：人员姓名、所属单位、人员分类、技能标签、职务、出生年月、身份证号、联系电话、收集号码、联系邮箱。	
104		删除人员	支持删除单个人员列表信息	
105		人员查看/编辑	1、支持查看/编辑人员详情，包括：手段基本信息、拥有装备情况、拥有手段情况；	
106		人员类型配置及管理	2、建立“单位-人员-装备-手段”关联关系，支持人员视角查看“所属单位、拥有装备、拥有手段”情况。	
107		标签化类型	1、支持人员类型标签化配置管理；	
108		类型统计	2、添加人员类型，左边树形结构展示各类人员以及统计数量。	
109		人员排序	支持人员优先级排序，置顶和上下移动方式。	
110		关键搜索	支持关键条件搜索，如：人员姓名、所属单位。	
111		装备管理	支持对已创建的装备进行统一管理，列表形式展示每条装备信息；	
112		添加装备	支持添加装备，添加装备基本信息：装备名称、装备分类、所属单位、网站 URL、装备版本、技能标签、装备描述、附件材料；	
113		删除装备	支持删除单个装备信息	
114		装备查看	支持查看/编辑装备详情，包括：装备基本信息、人员信息、拥有手段情况；	
115		装备编辑	建立“装备-单位-人员-手段”关联关系，支持装备视角查看“所属单位、相关人员、拥有手段”情况。	
116		装备类型配置	支持装备类型标签化配置管理	
117		装备类型管理	添加装备类型，左边树形结构展示各类装备以及统计数量。	
118		装备排序	支持装备优先级排序，置顶和上下移动方式。	

119		关键搜索	支持关键条件搜索，如：装备名称、技能标签。	
120		手段管理	支持对已创建的手段进行统一管理，列表形式展示每条手段信息	
121		添加手段	支持添加手段，添加手段基本信息：手段名称、手段模板、手段类型、手段标签、手段描述；	
122		删除手段	支持删除单个手段信息	
123		手段查看	支持查看手段详情，包括手段基本信息、接口信息、人员信息、输入输出情况	
124		手段编辑	建立手段-人员-单位关联关系 支持手段视角查看人员信息、接口信息、输出输入	
125		手段类型配置	支持手段类型标签化配置	
126		手段类型管理	添加手段类型，左侧树形结构展示各类手段以及统计数量	
127		手段排序	支持手段优先级排序，置顶和上下移动方式	
128		关键搜索	支持关键条件搜索。如手段名称、手段标签	
129	报告中心	报告基本查询	支持通过报告名称、报告类型、报告生成时间对报告进行搜索查询	
130		报告预览与下载	支持对指定报告的下载(word、pdf)和预览(pdf)	
131		报告删除	支持单条和批量两种操作方式删除报告	
132		报告分组	支持对报告进行树状的分组管理以及对报告的拖动以改变分组	
133		报告展示	快速报告支持查看系统报告。包括名称、类型、文件大小和生成时间；周期报告查看报告名称、类型以及最近生成时间	
134		快速报告创建	支持通过指定模板快速创建报告	
135		快速报告展示	支持报告列表查看，包括报告名称、创建人、开始时间、结束时间、创建时间、任务状态	
136		快速报告查询	快速报告按照名称进行模糊查询	
137		快速报告操作	支持报告下载（word PDF）、预览、编辑与删除	

138		调度任务创建	支持新增创建调度任务，包括任务名称、模板、周期、开始结束时间。周期支持日报、周报、月报、年报	
139		调度任务展示	支持调度任务列表，包括任务名称、类型、使用模板、更新时间、启停状态、最近执行时间、下次执行时间。	
140		调度任务查询	支持调度任务按照调度任务名称进行模糊搜索	
141		调度任务操作	操作包括任务的禁用、启用、编辑、查看详情、删除操作	
142		周期报告展示	支持报告列表功能，包括报告名称、类型、开始时间、结束时间、生成时间及列表的各字段排序	
143		周期报告操作	支持报告列表的搜索、下载（word）、查看（pdf）和删除功能	
144		数据连接创建	支持添加数据库连接功能，数据库包括 Excel、CSV、ElasticSearch、MySQL、Oracle、PostgreSQL、CK、API 接口	
145		数据连接信息	支持添加数据库连接，包含基本信息：数据链接名称、服务器 IP 和端口号；支持维护、编辑数据连接详情，包括基本信息、表信息；支持查看每个数据连接的操作记录	
146		数据连接操作	支持对数据连接的重命名和删除操作	
147		数据模型创建	支持从已经创建的数据连接中选择连接创建数据模型	
148		数据模型分组	支持创建数据模型文件夹，同时支持重命名和删除操作	
149		数据模型操作	支持对每个数据模型的重命名和删除操作	
150		模版管理列表信息	支持模板列表，包括表项查询和自定义表头。列表包括：模板名称、来源、创建人、创建时间、最后编辑时间及查看详情、编辑模板操作；	
151		模版删除	支持模版的单条删除和批量删除	
152		报告模版预置	支持内置 10 个报告模版	

153		模版创建	支持新建模板，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。	
154		模版新建要素	支持模板编辑中用户自定义展示的图表方式；支持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；支持模板编辑中的最后结果保存、预览和退出；支持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	
155		模版文字要素编辑	支持组件修改标题文字、字体颜色、字体大小、组件背景色等样式；	
156		模版数据源模型	支持图表组件在线选择数据模型，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，支持拖拽选择筛选器，支持通过文本筛选、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；	
157		模版图表管理	支持图表组件切换展示图形类型：饼图、柱图、折线图、表格等；	
158		模版组件管理	支持组件右键编辑图层层级、组件删除、所在报告页位置移动等；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；	
159		模版元素删除	支持模板组件键盘删除事件；	
160		模版画布操作	支持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；	
161		模版预览	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；	
162	攻击链分析	攻击链分析任务管理	支持对攻击链分析任务进行新增，修改，查询，删除，重启和查看。。	

163		攻击链分析任务创建	支持攻击链分析任务创建，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。	
164		攻击链分析任务删除	支持分析任务的删除，确认删除前需要对用户做明显提示。	
165		攻击链分析任务编辑	支持对攻击链分析任务编辑，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。	
166		攻击链分析任务检索	支持攻击链分析任务检索，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。	
167		攻击链分析任务重启	支持对未执行、完成状态的任务进行任务重启操作。	
168		攻击链分析任务查看	支持对完成的分析任务进行分析结果查看。	
169	多维分析	分析任务管理	支持对分析任务使用卡片和列表的方式进行呈现。	
170		分析任务创建	支持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。	
171		分析任务删除	支持分析任务的删除，确认删除前需要对用户做明显提示。	
172		分析任务编辑	支持对分析编辑功能，可以修改任务名称、标签、描述。可对分组进行变更。	
173		分析任务检索	支持对分析任务按照创建时间、关键字以及标签进行检索。	
174		标签管理	支持对分析任务新增、编辑与删除标签。支持对标签的检索。	
175		任务分组	支持在分析任务的分组管理。支持按组对任务进行过滤。	
176		单线索拓线	支持对系统中告警、事件、资产进行检索。	
177		数据查询	底层接口即猛禽提供的似 ES 的 DSL 语句接口。其为对外接口提供告警，事件等流量日志的查询能力	

178		经验模型拓线	支持对已有经验模型：永恒之蓝规则、IP 通联关系模型依赖 ES，IP 资产模型、攻击者画像模型依赖 PG 数据库进行检索	
179		云查	对特定 URL、MD5 查询线索功能和在业务功能模块反查其中 URL、MD5 线索的功能。	
180		线索拓线剪枝	支持对检索结果的线索剪枝	
181		分析任务截图	支持对分析拓线结果进行截图。	
182		清空画布	支持对分析结果一键清空	
183		分析步骤、名称	支持对分析任务按照分析时序进行标号，支持显示分析实体名称	
184		缩略图	支持对系统分析结果全局的缩略图展示与移动	
185		分析布局	支持多种分析布局方式，支持每次检索实体的最大数量限制	
186		全屏显示	支持分析任务全屏和带有组件模式的切换	
187		案例保存	支持对检索过程进行案例的保存。	
188		案例加载	支持对案例载入，载入后可继续进行分析操作。	
189		案例检索	支持对案例名称的模糊搜索。	
190		分析历史快照保存	支持对每一步分析任务的快照保存	
191		分析历史快照恢复	支持恢复到选中的分析历史快照	
192		历史节点列表	支持显示和检索分析历史中的所有节点	
193		历史连线列表	支持显示和检索分析历史中的所有连线关系	
194		分析历史回放	支持对分析任务以时间轴的方式呈现实体的发现过程	
195	资质要求	软著	需提供软件著作权证书	

2. 网络空间治理平台

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
1	部署方式	集群部署	满足软硬一体化形态或纯软件形态部署模式；	
2			支持集群部署，可水平扩展到多台设备集群。	
3	功能支持	功能支持	▲支持监控中心（态势感知、安全概览、仪表	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			板、运维工作台）、分析中心（日志检索、告警分析）、威胁检测（威胁告警、事件管理、模型管理、威胁情报）、响应中心（自动化响应、威胁预警、工单管理）、资产中心（资产管理、脆弱性管理、风险资产）、统计报表、系统管理、威胁情报升级、漏洞知识库等功能，并出厂内置 10 块态势感知大屏，支持接入并解析的数据源数量至少为 50 个。（提供相关功能的界面截图并加盖公章）	
4	国产化适配	国产化适配	X86 架构平台软件支持国产化部署，支持适配海光 CPU、银河麒麟高级服务器操作系统、OpenEuler 操作系统，人大金仓数据库，东方通中间件。	
5	国密改造	国密算法支持	平台系统账户密码存储支持使用国密 SM3 加密;流量传感器数据传输到平台支持使用国密 SM4 加密；日志采集器数据传输到平台支持使用国密 SM4 加密;支持使用国密浏览器访问平台，系统 HTTPS 支持国密 SM3_SM2 加密。	
6	数据采集与存储	数据采集	支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集;支持对日志采集器进行采集配置并下发；提供 Syslog、SNMP Trap、文本格式日志、数据库、WMI、Netflow、HTTP、Script 等采集方式；并支持数据源信息导入、导出、数据源迁移操作。；	
7			预置支持≥700 种设备进行日志解析，支持统计展示已接入设备总数、日志源的总数及其中在线和离线数量;支持实时展示平台整体及各安全设备的日志采集 EPS、处理 EPS 指标变化趋势;支持监控和展示各设备全流程数据处理结果统计（即日志接入、解析、存储、外发、产生告警、事件各环节数据统计）。	
8			▲预置日志解析规则≥2200 条，支持对已适配的第三方日志源自动识别并匹配解析策略，无需手动配置即可自动完成数据解析和接入。（提供相关已支持解析的数据源清单尾页截图并加盖公章）；	
9			支持一键对未能解析日志自动生成解析策略，自动生成的内容包括：解析方式、结构化提取日志字段、各字段的映射方法、解析后字段名称等，帮助客户快速完成全新日志的接入。支持的解析方式至少包括 JSON、正则表达式镪值对、CSV 解析、CEF 解析、Grok 解析、插件解析等。；	
10			预置支持富化规则不少于 190 条;支持通过界面配置操作，实现富化规则构建，包括不限于源字段、表达式、目标字段、参数设置；	
11		数据存储	支持新增日志类型功能，可在线新增字段信	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			息,支持数据存储类型的配置,包括:ES、Hive、Kingbase、mysql，支持存储基础信息的配置:包括数据库名、存储时间、分区方式等基础属性信息，从而达到分类存储日志的目的	
12	资产管理和风险评估	资产管理	支持主机资产管理功能,资产分类至少包括服务器、工作主机、网络设备、安全设备、终端安全管理、数据库、中间件、存储设备、应用服务器、虚拟化设备等类型，支持对 IPV6 资产的管理。	
13			支持资产详情信息的展示，能够展现资产名称、IP 地址、分组、、型号、操作系统、物理地址、责任人、是否外连情况等资产基础信息。	
14			支持从资产分组、组织架构、业务分组、地理位置及网段视角展示主机资产详情信息。	
15			支持资产服务信息管理，支持对服务的 IP 地址、端口号、服务名、服务版本、协议、Banner 等服务属性进行管理。	
16			支持网站资产详情信息的展示,展示内容包括资产名称、URL、责任人、责任部门、网站标题、资产状态、资产分组、技术框架及版本、关联主机等。	
17			支持 DHCP 场景下的资产管理，支持对 DHCP 网段范围、DHCP 租期、资产唯一标识等属性进行配置。支持查看 DHCP 场景下资产 IP 的变更记录。	
18		资产发现	▲支持通过网络流量被动发现资产信息、支持通过脆弱性发现资产信息，资产信息至少包含：IP 地址、服务、服务版本、协议、端口、操作系统、主机名、mac 等。（提供相关功能的界面截图并加盖公章）	
19		资产策略	支持和同品牌的资产探查设备、服务器管理系统、网络流量探针、终端管理系统、网站监测系统、云安全管理平台进行协同对接同步资产信息; 支持对发现资产的方式的优先级、资产更新策略进行配置。	
20		资产风险	支持对资产风险值的自定义计算,计算范围包括威胁告警及脆弱性的危害等级、时间范围、处置状态等纬度。支持对风险计算周期进行配置。	
21	脆弱性管理	脆弱性数据采集	▲支持导入第三方漏洞扫描报告,至少支持绿盟、启明、网神、天融信、Tenable 漏扫报告的解析识别和导入管理;（提供相关功能的界面截图并加盖公章）	
22			支持通过网络数据传感器同步资产信息,通过	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			平台的威胁告警模块同步漏洞，弱口令、网站漏洞信息到资产中心模块	
23		联动扫描	支持对接绿盟、网神、Tenable 中至少 2 款扫描设备，进行漏洞扫描任务调度和弱口令扫描任务调度，支持自动获取扫描器的扫描策略并执行周期性扫描任务和快速扫描任务；支持扫描任务结束通知，通知方式支持邮件、短信、企业微信、消息中心、企业钉钉、蓝信；	
24	威胁情报	本地情报	支持本地威胁情报的检索，检索类型支持域名、URL、IP 地址；威胁情报内容支持 IOC、攻击链阶段、ID、置信度、类型描述、定向攻击、风险等级、恶意家族、发布时间、攻击事件/团伙、影响平台、情报当前状态、威胁描述等；	
25		云端情报	支持云端威胁情报查询，查询结果需包含：IP 主机信息、IP 位置信息、域名流行度、情报 IOC 详情、相关样本、可视化分析、域名解析记录、域名注册信息、关联域名、数字证书等信息；	
26		自定义情报	支持自定义威胁情报，支持类型包含 IP 地址、域名、MD5、域名:URI、IP 地址:URI、域名:端口、IP 地址:端口、域名:端口:URI、IP 地址:端口:URI。支持自定义 IPv6 的威胁情报；	
27		情报能力证明	提供至少 10 份以上公开发布的 APT 报告作为证明。	
28	威胁检测	威胁建模	支持自定义关联规则，支持类 VISIO 的图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式；提供 1100+条预置规则；支持日志关联规则建模，在指定的时间范围内，能够对来自不同数据源的日志进行关联分析，以发现可信度更高的威胁告警；日志关联方式包括不限于：A 事件等于/不等于 B 事件、A 事件包含 B 事件、A 事件大于/小于 B 事件、A 事件开始于/结束于 B 事件等；	
29			支持统计规则建模，在指定的时间范围内，对符合过滤条件的日志中数字类字段进行统计，将其与阈值进行比较以发现异常威胁事件；统计方式包括不限于：计数、求和、平均值、最大值和最小值计算；	
30			支持序列规则建模，在指定的时间范围内，通过对 2 个及 2 个以符合过滤条件的日志发生，以发现复杂场景下的威胁事件；序列方式包括不限于：A 事件后发生 B 事件、A 事件发生 M 次后发生 B 事件等。	
31			支持规则引用规则，以发现深层、复杂威胁事件；	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
32			支持可视化呈现规则间的引用关系,规则被引用的次数。	
33		告警模式	支持配置告警模式，告警模式包括全量告警、精选告警，两种模式。精选告警的配置包括：告警置信度、告警攻击结果、告警危害等级，其中告警置信度包括：高、中、低，告警攻击结果包括：成功、企图、失败，告警危害等级包括：危急、高危、中危、低危。	
34		情报检测引擎	系统内置高级情报检测引擎,支持情报检测规则管理，出厂预置规则支持以 unix 服务器日志、Windows 服务器日志、网络流量传感器流量日志为日志源进行情报碰撞产生告警,支持查看规则名称、日志类型、威胁情报类型、碰撞日志字段、威胁情报数据源、日志计数、情报告警日志计数等。碰撞的失陷情报数据来源可选本地威胁情报库或同品牌威胁情报系统。	
35		关联分析场景	支持预置关联分析场景，包括不限于：攻击利用、恶意软件、拒绝服务、异常事件、内容安全、信息收集、威胁活动、威胁情报命中等不同威胁场景的分析；支持将 VPN、沙箱、流量传感器、Linux、Windows、AD 域、WAF、NIPS、防火墙、HIDS、蜜罐等日志类型定义为标签，支持按照标签一键筛选定位关联规则。	
36		智能分诊规则	提供智能分诊能力,实现对告警的优先级做分类。智能分诊模型支持分诊规则、加白分诊规则两种规则的创建,分诊规则支持配置过滤条件和配置过滤条件组，过滤内容包括：告警名称、首次告警时间、源 IP、目的 IP、源端口、目的端口、通信方向、攻击者等信息 ；智能分诊支持生效时间配置，包括：永久生效和自定义时间	
37		加白过滤	支持加白分诊规则，以避免产生误报。支持对源 IP、目的 IP、数据源 IP、攻击者（IP 类型）、受害者（IP 类型）、域名、文件哈希、URI 资源的类型直接进行全局加白；支持根据单个、多个或者全部检测规则进行加白，如果选择了特定的关联规则,则加白只针对选中规则范围内产生的告警生效,并且支持配置生效时间；	
38			支持对分诊规则配置自动处置,支持开关自动处置、设置自动处置结果，实现对不关注、低关注场景下分诊结果对应的告警的自动处置。	
39		ATT&CK 技战评估	支持展示覆盖 ATT&CK 的矩阵；支持呈现 ATT&CK 知识库跟关联规则的关联关系，支持对告警进行 ATT&CK 攻击战术、攻击技术的标识，并支持通过告警关联到 ATT&CK 知识库。	
40	告警管理	告警管理	告警管理功能至少预置 12 种常见场景的告警	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			快速筛选器，包括今日新增威胁告警、已先陷告警、首次出现告警、IOC 告警、外部攻击告警、横向移动告警、资产外连告警、恶意文件告警、Web 攻击告警、Windows 告警、Linux 告警、自身安全性告警。告警筛选器支持通过安全内容包升级的方式定期自动升级，用户可持续获取到厂家最新的安全经验。	
41		告警归并	支持分析不同、不同种类安全设备上报的告警日志，对其进行威胁分类、危害定级、有效性筛选以及重复告警归并； 支持按照归并条件针对重复告警进行归并，归并条件包括不限于：检测规则 ID、数据源 IP、攻击链阶段、ATT&CK 技术项、失陷状态、攻击结果、攻击者、受害者、CVE 编号、协议、漏洞名称、漏洞描述、漏洞危害、CNNVD 等条件；	
42		告警展示	支持通过智能分诊，对告警进行智能化的归类，协助客户快速分析研判，以可视化的方式呈现归类后告警：重点关注告警、低关注告警、不关注告警、未分诊告警，同时提醒告警的智能分诊率	
43	威胁预警	预警配置	支持对重大网络安全事件（如 Log4j 漏洞）进行威胁预警功能。厂商针对重大网络安全事件生成威胁预警包，通过系统自动升级的方式分发给平台用户。也支持通过导入威胁预警包并启动威胁预警任务，完成网络安全事件的影响面评估和分析。	
44		预警展示	针对重大安全事件，支持统计风险资产数、受攻击资产数、失陷资产数以及资产的日同比及周同比对比情况；	
45			支持按时间范围选择，预警事件影响面的趋势展示，从风险资产数、受攻击资产数和失陷资产数三个维度进行趋势统计分析；	
46			支持预警事件关键里程碑节点展示，支持关键节点配置，预置大面积爆发、有效控制、威胁缓解等节点，支持自定义节点。	
47			支持基于网段的影响面分布，展示不同网段的风险资产数、受攻击资产数、失陷资产数；	
48			支持受攻击资产列表，支持展示受害者 IP、所属网段、资产名、攻击者 IP、失陷状态、告警次数等信息；	
49			支持接入终端安全管理系统数据并分析感染病毒情况，支持展示 IP、所属网段、终端名称、病毒名称等信息；	
50			支持风险资产列表，支持展示 IP、所属网段、端口、软件信息等信息；	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
51			支持关联多个类似告警进行事件创建,事件类型包括：恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、不可抗力事件、其他事件。	
52		事件调查响应	支持事件管理,可查看和调查响应事件详情信息；事件详情包括：事件概览、受影响资产，ATT&CK 战术，攻击技术及攻击者信息列表，攻击痕迹(包括重点关注 IP/域名清单)，事件线索。事件概览支持编辑信息包括:事件名称、事件类型、事件优先级等。事件线索包含事件关联的：告警、资产、其他证据的截图及研判依据信息等，支持移除已添加的告警证据信息，支持在事件线索-告警列表页面进行告警线索搜索过滤，在事件线索-资产列表页面进行资产线索搜索过滤。支持对事件调查详情进行保存、确认、关闭事件、生成报告。	
53			支持以事件维度进行响应，包括：定性和填写事件调查结论,汇总事件关联的所有实体清单并进行一键下发“立即处置”命令，实体对象包括主机、账号、内部 IP、外部 IP、域名、恶意文件、服务端口等，支持显示各实体对象的处置状态。支持一键生成事件报告，报告支持 word、pdf 格式，支持添加展示水印，可以在线查看、下载、重新生成事件报告。	
54		▲告警分析	具备独立的告警分析管理模块,该模块支持基于多视角进行聚合分析,预置分析视角至少包含告警名称分析、攻击者分析(含外部攻击者、内部攻击者)、失陷情报分析、挖矿木马分析、勒索软件分析、ATT&CK 分析。（提供以上 6 个分析视角功能的界面截图并加盖公章）	
55		日志检索	支持通过高级模式构造搜索条件,支持使用多种逻辑运算和关系运算进行复杂搜索语句构造，运算符包含“等于、不等于、属于、不属于、为空、不为空、开始于、结束于、包含、不包含、仅包含、大于、小于、大于等于、小于等于”等。；支持从索引类型和字段列表中快速筛选出日志源和关键字段，形成搜索条件；支持搜索语句保存到收藏夹中，支持快速查看历史搜索结果数据；	
56			支持通过热数据、冷数据方式对存储时间不同的日志进行分类搜索	
57			支持高级模式、Lucene、QAL 三种模式进行搜索。	
58			支持 QAL 语法检索,通过管道符方式拼接搜索语句，支持 10 种搜索命令，80 多种函数。提供语法帮助功能。支持命令联想、常用搜索、	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			如何搜索等指导。	
59			搜索结果支持按照全文或结构化(键/值、JSON串)展示，可筛选展示字段，隐藏不必要字段，支持调整字段展示顺序；	
60			支持搜索内容的高亮显示	
61			支持导出搜索结果，可导出全部字段或展示字段	
62			支持对每个字段进行分组统计，统计结果支持展示和下载；	
63			支持对字段内容进行快速过滤、排除、新建搜索、复制、查询资产、查询情报、解码操作。；	
64			支持对日志内容进行编解码，包含 Unicode、UTF-8、URL、ASCII、Hex、Bse64 六种解码方式；支持对日志内容进行进制转换，包含 2 进制、8 进制、10 进制、16 进制间的互相转换。	
65	响应处置	响应预案	支持对威胁告警和安全事件新增自动化响应策略，支持类 VISO 的图形化连线拖拽交互，通过将数据过滤和联动处置、syslog 外发、通知响应、工单 5 个计算单元进行灵活组合从而对告警实现自动化的、不同方式的响应场景；其中数据过滤计算单元支持引用对象资源、资产信息。支持通过列表的方式管理自动化响应策略，支持对策略进行停用、启用、批量删除等操作。	
66		工单管理	支持通过工单对安全事件进行跟踪处理，工单类型包括：通用、弱口令、告警、配置核查、漏洞、WEB 漏洞。工单流转中支持添加附件，支持 zip,.rar,.pdf,.doc,.docx,.xls,.xlsx,.ppt,.pptx,.txt,.png,.jpeg,.jpg 格式。工单状态包含待下发、待处置、处置中、已处置、已完成、已撤销。	
67			工单支持 SLA 配置，按照工单优先级配置 SLA 时限，分为响应时限和处置时限。响应时限：从工单下发到工单状态变成处置中、处置时限：从工单下发到工单状态变成已完成。	
68			支持集群部署上级组织下发协同工单到下级组织。支持选择下级组织账户作为工单的责任人进行处理工单也可以不指定具体账户作为责任人由下级组织账户进行认领工单。	
69			工单通知方式分为个人和群两种，通知方式（个人）包括：邮件、短信、企业微信、消息中心、企业钉钉、蓝信；通知方式（群）包括：企业钉钉群、企业微信群、蓝信群。	
70	级联管理	级联配置	支持多个平台的级联管理，不限制级联层级。	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
71			支持设置下级平台数据订阅策略，下级平台根据数据订阅策略向上级平台上报数据。数据订阅策略类型包括告警订阅、弱口令订阅、配置核查订阅、漏洞订阅和资产订阅。告警订阅策略包括首次告警时间、危害等级、攻击结果、置信度。弱口令订阅、配置核查订阅、漏洞订阅策略包括最近发现时间和危害等级。	
72			支持上级平台向下级平台下发规则，规则下发支持展示系统版本、关联规则组、下发时间、下发状态、规则运行状态。	
73	态势大屏	▲态势首页（提供相关功能的界面截图并加盖公章）	提供态势感知大屏统一入口，态势首页集中展示至少 10 块态势大屏；支持大屏配置、轮播投放，内置大屏介绍文档，可供用户线上查看和下载；	
74			支持对态势大屏的内网地理位置、重点关注区域进行修改；支持自定义大屏 LOGO；支持设置大屏启停、轮播间隔时间、大屏轮播顺序	
75			态势大屏数量不少于 10 个，维度不限于综合安全态势、安全运营态势、威胁预警态势、外部威胁态势、内网威胁态势、攻击者态势、资产态势、资产风险态势、全网脆弱性态势、告警实时监控大屏	
76		综合安全态势大屏	综合安全态势大屏须至少包含以下展示内容：支持从综合风险值、事件数量、风险资产数量、脆弱性数量、威胁数量、日志数量六个维度以正三角形式展示综合安全态势。支持展示最近 30 天的威胁趋势；支持展示告警类型分布情况；支持展示命中情报 IOC 的告警情况；支持按脆弱性级别分别统计漏洞、配置核查、弱口令数量；支持按资产注册状态统计资产相关脆弱性的数量；支持展示漏洞类型统计情况、配置核查分类统计情况、弱口令服务统计情况。支持展示风险分组列表。	
77		告警实时监控大屏	告警实时监控大屏须至少包含以下展示内容：支持统计告警数量、待处置数量、处置中数量、已处置数量，其中待处置告警应细化展示危急数量、高危数量、中危数量、低危数量；支持展示所选时间周期内的告警变化趋势图，图中可悬浮展示不同告警等级的告警具体数量；支持展示实时告警列表，包含告警时间、告警名称、危害等级、源 ip、目的 ip、处置状态等字段；支持配置大屏名称、告警提醒、告警声音等，支持用户配置监控范围、高风险告警、添加指定关注资产。	
78		安全运营态势大屏	安全运营大屏支持统计服务器、网络设备、数据库服务器、中间件服务器、存储设备、应用服务器的资产和日志接入情况，动态展示被保	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			护 IP 网段情况，安全运营支持统计规则（威胁情报、关联规则、漏洞知识库）运营、威胁检测（威胁、脆弱性）和处置情况，支持统计安全运维人员在平台上的运营情况(处理威胁数量、使用平台时长、常用功能等）；	
79		威胁预警态势大屏	支持通过弦图展示预警事件中攻击者、受害者、既是攻击者也是受害者的 IP 之间关系；支持展示当前威胁预警事件对资产造成的影响趋势，包括风险资产、受攻击资产、失陷资产的影响趋势;支持对预警事件中的关键里程碑节点进行记录、展示；支持展示预警事件中攻击者、受害者的 TOP5 统计。支持展示预警事件中最新的安全事件。	
80		外部威胁态势大屏	支持通过3D地图炮/2D世界地图/2D中国地图展示外部威胁攻击，可以统计外部威胁总数、攻击 IP 数量、受害 IP 数量，TOP5 的受害 IP，支持按威胁级别统计外部威胁分布情况，TOP5 的外部攻击 IP，TOP5 的外部威胁类型，TOP10 的外部威胁来源（国家/地区），统计最近 30 天的外部威胁变化趋势，支持对内网地理位置进行设置，并在地图炮展现该区域。	
81		内部威胁态势大屏	支持可视化呈现内网中是否存在威胁告警，威胁是否在内网网络中蔓延，能够聚焦于核心资产网段，提供对攻击者维度和受害者维度的攻击情况分析，对威胁类型、等级和趋势等进行统计呈现。支持发现内网中的攻击者，以帮助快速定位内网威胁的根源。提供相关统计数据的详情查看能力。支持最近 30 天时间范围内的数据统计。	
82		攻击者态势大屏	支持在 3D 地图/2D 中国地图上展示攻击者来源的分布情况。支持展示攻击者 IP 的相关归属地、攻击手段、攻击链阶段、告警次数、受害者 IP 数、危害等级的明细列表。持统计攻击者 IP 总数，支持统计危急攻击者 IP 的占比。支持展示今日新增攻击者 IP 数；支持统计攻击总数，支持统计攻击结果为成功的攻击占比。支持展示今日新增攻击数量；支持统计受害者 IP 总数，支持已失陷的受害者 IP 的占比。支持展示今日新增受害者 IP 数。	
83		资产态势大屏	支持统计资产发现来源（资产探查、数据同步、脆弱性发现、流量解析、人工方式）的分布情况。支持统计资产总数，以及统计资产注册状态占比情况；支持统计资产上开放的端口情况、服务情况、协议情况。	
84		资产风险态势大屏	支持全局风险态势和每个资产组节点的风险态势计算（包括风险值、资产数量、威胁数量、脆弱性数量）；支持轮播展示资产组的风险情	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			况	
85		全网脆弱性态势大屏	支持统计漏洞数量、配置核查数量和弱口令数量;支持按资产注册状态统计资产相关脆弱性的数量；支持展示漏洞类型统计情况、配置核查影响资产情况、弱口令服务影响资产情况。支持统计展示漏洞利用情况 TOP5 及影响资产情况	
86		▲量化运营态势（提供相关功能的界面截图并加盖公章）	支持针对运营成果进行展示和汇报;支持对威胁和事件的统计至少包括成功发现的威胁的数量，成功阻断的威胁数量，已发生的安全事件数量，已处理的安全事件数量；支持针对安全运营工作的量化包括：安全运营团队人数、团队人员明细信息、团队日均工作量、平均威胁检出时间、平均事件调查时间、平均事件响应时间等信息。支持对运营指标进行修改和拖拽和跳转	
87	统计报表	报表管理	支持快速报表、周期报表功能、自定义模板三种方式	
88			自定义报表模板:支持自定义模板可加入多种统计分析视图(含自定义)和智能备注信息(可根据数据不同展示不同的备注说明)；支持灵活编辑和布局调整以形成整体报表;可添加不限于告警统计、工单统计、异常行为统计、弱口令统计、攻击者统计、日志统计、系统维护、脆弱性统计、调查统计、资产统计、风险统计等;报表模板可被快速报表和周期报表任务引用	
89			快速报表：支持报表名称的自定义；报表模板的引用；水印的展示；自定义报表时间范围；支持 PDF、Word、HTML 三种格式的报表下载；支持通过邮件、短信、企业微信、消息中心、企业钉钉、蓝信通知指定责任人。	
90			周期报告：支持日报、周报、月报季报、年报；支持报表模板的引用；水印的展示；自定义报表时间范围支持 PDF、Word、HTML 三种格式的报表下载；支持通过邮件、短信、企业微信、消息中心、企业钉钉、蓝信通知指定责任人。	
91		统计视图	统计视图支持不限于：列表、指标卡，折线图、面积图、堆积面积图、柱状图、堆积柱状图、条形图、堆积条形图、饼图、玫瑰图、散点图、词云图、双轴图等视图展示。	
92	通报预警	通报管理	支持上级组织自主监管发现或者接收外部监管单位通知下级组织有安全问题，上级组织对下级组织发出正式通报邮件下级组织进行问题处置；支持通报指定组织、相关收件人、抄送人、主题、正文、附件等内容。支持用户自定义新增通报流程。支持对流程内容节点、新	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			增和删除。支持对接节点基本信息、操作、处理人进行修改调整。	
93		预警管理	支持上级组织针对重大安全问题(引用威胁预警)面向下级组织进行事先预警，邮件通知下组织位有序展开自查。支持用户自定义新增预警流程。支持对流程内容节点、新增和删除。支持对接节点基本信息、操作、处理人进行修改调整。	
94	分权分域	分权分域配置	可手动控制分权分域开关;支持根据网段进行数据划分,使得不同的部门或下级单位对应不同的数据域； 可根据角色配置权限，对不同角色从功能权限、日志检索权限、数据权限三个维度进行权限划分;系统管理员可创建分权分域管理员,分权分域管理员账户只有查看及使用本数据域数据的权限,无查看非授权功能及数据域的权限;分权分域管理员可对本数据域内业务数据（日志、告警、资产信息、漏洞信息、风险信息、仪表板、日志搜索等）的分权分域管理。	
95	攻防演练	安全部署	攻防演练监控态势从安全部署和安全威胁监控两个方面进行展示;安全部署方面主要展示值班情况、安全设备部署及响应处置指标三个维度的信息。分别展示值班分组情况、监控日志数、日志类型、日志变化趋势、安全设备总数、监控威胁总数、处置威胁总数及处置威胁趋势；	
96		安全威胁监控	安全威胁监控方面主要展示攻击源监控、威胁监控、资产监控三个维度的信息。攻击源监控展示攻击源 IP 数量、互联网 IP 数量、内网 IP 个数，并按照互联网和内网两个视角分别展示攻击 IP 分布统计表。威胁监控展示 威胁告警数量、攻击成功告警数量、企图攻击告警数量,可从攻击次数最高和攻击成功最多两个视角展示攻击手段 TOP20 统计图或相应趋势图。资产监控展示受攻击资产数量、失陷资产数量、高风险资产数量，还展示单个资产的名称、告警数量、脆弱性数量等信息，点击资产名称能下钻到对应资产详情，相关告警信息、脆弱性信息可继续下钻到告警页面、脆弱性列表页面。	
97		演练配置	支持统计最近 30 秒内发生的危急和高危类型的告警数量,并将两种类型的攻击成功状态的告警数量的统计,将以上统计信息通过底部浮框的方式进行通知。点击通知窗口，可进入告警列表页面查看告警详细情况。还支持开关按钮,可以关闭通知。支持对演练项目进行管理，支持启动、编辑演练项目，支持对演练参与人员、排班表、安全设备部署情况、每日处置数	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
			量等信息的展示、导入和导出，还支持值班班次配置，可手动编辑白班和夜班时间。	
98	设备监控	监控范围	支持监控主机（Unix、Windows、Linux）、网络设备（交换机、路由器）、安全设备（上网行为审计、防火墙、入侵检测、运维审计、漏洞扫描、VPN、网闸、WEB 应用防护、入侵防御、数据库审计、日志审计、防毒墙）、数据库（SqlServer、Oracle、Mysql）、中间件（Tomcat、Weblogic）及邮件、web 等通用服务的运行状态；	
99		监控任务	设备监控任务列表可新增、删除、启用、停用、导入、导出监控任务，也可通过查看、任务详情、编辑等对监控任务进行管理，可查看监控任务的 24 小时、7 天、30 天的可用性和健康状态； 系统预置 200+各种厂商设备的监控模板，支持对监控模板的批量导入；	
100		监控指标	支持自定义监控指标，并能对获取的监控指标进行告警条件和告警等级设置，当指标达到的设置阈值时产生告警，告警通知可启用或不启用，间隔时间可自定义，通知方式支持企业微信、钉钉、蓝信，邮件、短信；监控协议应支持 SNMP V1 、SNMP V2 、SNMP V3、SSH、JDBC、JMX、TCP。	
101	拓扑管理	拓扑绘制	支持拓扑管理功能，提供在线拓扑绘制工具，可手动进行逻辑拓扑的绘制，单个拓扑图支持 300 个设备节点。	
102			支持多级拓扑级联，最多支持 5 级拓扑级联，	
103			支持拓扑图的整体拖拽和缩放操作，支持对单个节点施放操作，支持拓扑画布大小设置	
104			支持导入背景图，支持（PNG、BMP、JPG、JPEG）四种文件格式；	
105			支持鼠标悬停显示拓扑节点资产名称、IP 地址和风险值，支持点击查看节点的资产名称、资产组、责任人、风险值、未处置及风险趋势统计等详细信息；	
106	系统管理	升级管理	支持统一系统软件版本、威胁情报、漏洞知识库、IP 地址定位库、巡检规则包、威胁预警包等数据的升级，支持配置升级地址并展示当前版本和升级相关信息，支持手动/自动升级方式（提供相关功能的界面截图并加盖公章）	
107			提供独立的安全内容包升级，安全内容部包含关联规则、行为基线模型、分诊规则、日志检索预语句、告警筛选器、视图、仪表板、ATT&CK、报表模板。	
108		角色管理	支持用户角色管理， 可以为不同角色赋予不同系统功能模块及数据的读写权限	

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
109		安全性	支持系统账户的安全性验证，包含双因子认证、账户登录设置、可信主机等设置，支持对登录异常账户锁定、密码长度、密码强度、登录会话并发数等进行设置；支持配置可信主机；开启双因子认证，认证方式支持短信、邮件、企业微信、企业钉钉、蓝信。	
110		通知配置	支持通过邮件服务、短信服务、企业微信、钉钉、蓝信方式向个人或群发送系统消息通知。	
111			支持对威胁告警产生的消息通知进行配置模板，模板支持邮件、短信、IM 消息。通知模板支持引用变量作为通知内容。邮件通知模板支持使用富文本编辑通知内容。	
112		对接管理	支持对接第三方设备配置，实现联动处置、免登录认证、资产同步、漏洞同步、日志同步以及情报查询等多种三方联动能力。	
113		知识库	支持知识库管理，内置漏洞知识库、IP 地址定位知识库、ATT&CK 知识库、应用识别知识库、事件日志 ID 知识库。	
114			支持自定义知识库，支持对自定义知识库字段的管理和配置，字段包含文本框、富文本、数值、密码、附件等表现形式，支持自定义知识库的增删改查等基础配置。	
115	仪表板	自定义仪表板	支持自定+B17:D131 义仪表板功能，能够在仪表板内加入多种统计分析视图（含自定义），支持在引用视图时查看视图内容，还支持跳转到视图模块新增视图便于仪表板快速引用。支持选择、拖拽、边框调整等操作，形成账户独有的仪表板展示页面。	
116	资质要求	软著	需提供软件著作权证书	

3. 暴露面风险管理平台

序号	一级功能模块清单	功能需求	备注
1	数据对接	▲支持通过 API 接口对接市场主流资产探测类、主机安全平台、云安全管理平台、终端管理平台、漏洞扫描类、漏洞管理类系统、互联网测绘等第三方数据源获取资产、风险等信息。（提供相关功能的界面截图并加盖公章）	

2		支持对接 CMDB、AD、4A 等系统，获取网段范围、业务系统、物理机房、人员信息相关管理信息。	
3		支持数据源采集适配器进行统一管理，对数据源的连通性状态和配置状态进行监控，提示异常情况。	
4		支持新增数据源设备，并支持设置数据源认证信息、数据采集网段范围且可以控制超出范围是否入库、所属单位和责任人。	
5	数据采集	▲支持通过主动扫描、数据同步、文件导入和人工录入方式，获取资产和风险数据。（提供相关功能的界面截图并加盖公章）	
6		支持针对已对接数据源设置采集策略，按天、按周、按月或自定义时间定期同步或扫描资产及风险数据。	
7		支持跟踪数据采集过程，包括扫描进度、执行状态、执行结果，并可查看每批次采集作业数据处理数量。	
8		支持单个启用或批量启用在停用状态下的数据同步作业。	
9		支持网络隔离或跨网闸环境下，提供分布式数据采集能力。	
10	数据处理	支持查看已接入数据源数据获取的处理过程和状态。包括但不限于处理进度、处理数据类型、数据质量问题等。	
11		支持识别并保存查询原始数据中数据不完整、格式错误等类型数据。	

12		支持对入库数据记录数据来源信息，包括但不限于数据来源、采集方式、采集时间等。	
13		支持自定义属性作为资产归一标识，通过标识对多源资产数据自动归一，并记录归一过程中无法自动归一的冲突数据，由人工确认进行归一。	
14		支持通过原始数据中的姓名、电话、邮箱、员工编号等信息，自动确认资产责任人，并关联人员归属和管理信息。	
15		支持查询数据采集记录，包括数据来源名称、数据源地址、采集方式、调度方式、作业名称、执行人，并可查看采集的原始信息和范化信息。	
16		支持查询管理对象的数据来源，数据源名称、数据源地址、最近发现时间、发现次数。	
17	配置管理	支持自定义配置数据来源映射字段值权重，当针对同一个资产的同一个属性值，不同来源冲突时，采纳权重最高的值，支持保存查看所有数据源的值，并支持人工确认采纳。	
18		支持对网络资产、安全隐患相关对象的属性字段进行管理，可以扩展和删除属性字段，设置属性字段分组、显示名、显隐、排序、检索等参数。	
19		支持导入和导出模型文件，记录最近一次更新时间。	

20	资产管理	支持根据网络范围区分不同网络域的相同 IP 地址。	
21		支持根据数据源接入设置的内外网标识或网段规划设置的内外网信息，自动区分内网和外网 IP 地址、URL 和域名。	
22		支持对网络范围、业务系统、物理机房信息进行导入、导出、编辑、删除。	
23		支持对资产数据高级检索，运算符可选择=、!=、in、not in、is null、is not null 等。	
24		支持对资产数据关联检索，通过资产关联的对象属性信息进行检索过滤，如查询存在某 CVE 漏洞且开放某端口的设备。	
25		支持对常用筛选条件进行保存、删除和重命名。	
26		支持查询资产成分信息，包括资产关联的设备、软件、组件、服务、应用、IP、端口、URL、域名、系统漏洞、系统配置、系统弱口令、应用漏洞、应用弱口令，并支持对资产关联的成分对象检索。	
27		支持查询资产相关安全策略，包括数据源名称、策略类型、策略名称、采集时间、策略内容	
28		支持通过自定义算法计算资产重要程度和风险等级。	

29		支持显示资产的权属信息，包括属主单位、责任人、网络、业务、机房、项目及关联属主单位、内部支撑单位、外部支撑单位、负责人等管理信息。	
30		支持显示资产网络信息，包括 IP 地址、网络归属、最近探活时间、发现次数。	
31		支持显示资产物理信息，包括 MAC 地址、网卡名称、网卡厂商、IPV4、IPV6、子网掩码。	
32		支持记录和查询资产属性值历史变更记录，标记属性值的数据来源、采集方式和采集时间。	
33		支持在资产属性信息发生变化时，提示资产属性值冲突状态。	
34		支持以关系图的方式展示资产构成关系，展示对象包设备、软件、组件、服务、应用、系统账号、应用账号、系统漏洞、系统配置、系统弱口令、应用账号和应用弱口令，并支持查看关联对象详细信息。	
35	隐患管理	支持对多源系统漏洞、系统配置不合规、系统弱口令、应用漏洞、应用弱口令管理，并自动将安全隐患与设备、软件、服务、组件、应用进行关联。	
36		支持通过 CVE 编号、漏洞标题、资产信息等对风险数据自动去重，可以对相同设备不同网卡发现的漏洞进行自动去重。	

37		支持记录数据源名称、数据源 IP、最近发现时间、发现次数。	
38		平台内置资产风险修复优先级、资产风险等级等多种算法，如可按照风险数据结合漏洞 CVSS 评分、风险暴露情况、是否发生在重要资产上等综合因素计算该资产风险的修复优先级分值，并支持自定义配置计算因子的权值和阈值。	
39		支持以关系图的方式展示隐患影响资产的网络层关系，展示对象包括 IP、端口、URL、域名和归属的业务信息，并突出显示存在安全风险的网络对象。	
40		支持安全隐患全生命周期管理，包括状态变更时间、操作人、当前状态、备注、附件。	
41		支持展示不同来源安全隐患信息，包括漏洞名称、漏洞类型、危害等级、漏洞利用条件、检测方法、修复方法、发布时间等。	
42		支持显示安全隐患的权属信息，包括属主单位、责任人、网络、业务、机房、项目及关联属主单位、内部支撑单位、外部支撑单位、负责人等管理信息。	

43		支持对漏洞自动评分和人工评价，评分维度包括攻击复杂度、触发方式、可用性影响、影响范围、机密性影响、完整性影响、用户交互、用户认证。	
44		支持查看漏洞影响资产信息，包括影响的设备、软件、组件、服务、IP、端口，并以网络、业务、机房、组织的维度统计漏洞影响范围。	
45	分析空间	支持以关系图的方式展示物理层、网络层、系统层、服务层、应用层、管理层关联关系，展示对象包括设备、软件、组件、服务、应用、IP、端口、URL、域名、系统漏洞、系统配置、系统弱口令、应用漏洞和应用弱口令、组织、业务、网络、机房、人员。	
46		支持创建 IP、端口、域名相关关系，自定义添加、删除源和目的实体信息，可视化呈现域名解析关系，IP 地址访问关系、IP 映射关系，展示实体类型、实体名称、实体属性、关系类型、关系名称等信息。	
47		支持对关系图谱中的元素删除、缩放、拖拽、分组、选中，并支持以交互式的方式，对实体对象拓展不同类型关联关系，并保存关系图谱。	

48	风险监测	支持通过自定义标签，通过规则自动或人工设置方式，对管理对象打标，可查看标签名称、打标方式、操作方、打标时间	
49		平台内置数据碰撞规则 60+条，自动发现影子资产、无主资产、未按要求安装客户端、失陷等资产安全问题，并支持碰撞规则自定义配置。	
50		支持根据规则生成问题事项，自定义配置事项名称、事项内容、事项命中条件等。	
51		支持根据规则对资产和安全隐患自动打标。	
52		支持对碰撞分析规则启用、停用、编辑、删除。	
53		支持查看问题事项影响对象信息，并以网络、业务、机房、组织的维度统计事项影响范围。	
54	情报管理	支持对接漏洞情报，获取漏洞、补丁、POC 相关安全知识。	
55		支持通过在线或离线升级方式，同步漏洞补丁情报信息。	
56		支持提示漏洞是否存在 POC、EXP、在野利用、0Day。	
57		支持对漏洞、补丁、POC 知识库本地运营，包括漏洞评级、内容编辑、文档上传等。	
58		支持根据漏洞情报中影响资产的 CPE 信息与资产信息碰撞分析，识别存在存在漏洞的资产，生成安全预警。	

59		支持查看预警和补丁影响资产信息，包括影响的设备、软件、组件、服务、IP、端口，并以网络、业务、机房、组织的维度统计预警和补丁影响范围。	
60	任务管理	支持对接第三方工单、邮件、短信、企业微信等通知平台，对异常资产进行整改处置，跟踪处置状态、处置反馈等。	
61		平台内置影子资产派发、资产属性字段补充派发、资产风险处置派发等工单流程，支持跟踪处置状态、处置反馈完成线上闭环。	
62		工单派发支持按角色或自定义选择处置人员。	
63		支持展示与处理人相关的工单任务，包括任务参考信息、任务处理节点信息、任务流程图等。	
64	报告报表	支持自定义配置报表或导入报告模板，报告模板支持编辑文字、柱状图、列表等样式，布局灵活拖动调整，报告导出格式支持 docx、wps。	
65		支持自定义配置统计视图，可支持指标卡、饼图、折线图、条形图等类型，可点击下钻。	
66		支持自定义配置仪表板，仪表板可引用视图，并支持仪表板导入、导出、预览、下钻等操作，导出支持 PDF、图片、CSV、EXCEL 等格式。	

67		支持按账号、用户组授权视图或报告，控制查看、导出权限。	
68	系统管理	支持灵活配置用户菜单权限、功能权限和数据权限，以组织、业务系统、网络范围、机房等多维度进行管理，如一级组织可以看全局资产及风险情况，二级组织只能查看所属组织的资产及相关数据；支持配置功能菜单显隐权限以及查看、删除、编辑、导出等操作权限。	
69		支持单个新增或批量导入用户信息、组织架构信息，导入方式包括 xls、xlsx、csv 等文件格式。	
70		支持设置账号的启用状态、有效期和并行登录个数。	
71		支持首次登录必须修改密码；密码强度要求数字、大写字母、小写字母、特殊字符（除空格）中至少包含 4 种。	
72		支持对用户关键操作记录操作日志，包含 IP、账号信息、操作内容、操作结果等信息。	
73	数据共享	支持提供资产、风险 API 查询接口供第三方系统消费。	
74	其他指标	支持部署在国产化环境，需提供适配证书证明。支持部署硬件环境范围应不少于以下两种：CPU 海光 X86 或鲲鹏 ARM；操作系统至少应支持麒麟 V10。	
75	资质要求	软著	需提供软件著作权证书

4. 数据安全管控平台

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
1	平台架构及部署	平台架构及部署方式	平台具备海量数据采集与快速检索能力；	
2	兼容性	采集器管理	1.支持对接标准数据采集器，可新增流转数据监测系统、数据库审计等采集器，支持设置设备属性。 2.标准流量采集器至少支持HTTP、HTTPS、FTP、TFTP、SMB、邮件（SMTP、IMAP、POP3）和数据库如MySQL、MSSQL、PostgreSQL、DB2、Redis、人大金仓、瀚高、南大通用数据库、优炫、opengauss 、clickhouse等行为的解析。	
3		数据日志处理	▲1.支持展示日志来源，支持根据时间筛选，查询内容包括：日志类型、日志字段内容筛选等内容。（提供相关功能的界面截图并加盖公章）	
4	数据资产梳理	数据资产主动扫描	1.主动扫描：支持对数据库/实例进行自动扫描与解析，自动发现并提取数据库/实例信息、表信息、字段信息、表记录总条数等元数据信息，并识别其中的数据资产； 2.主动扫描：支持对非结构化数据载体进行识别，提取的其中的元数据。 3.支持定期扫描采集任务，灵活设置采样方式、采样数量、匹配规则等，支持扫描任务结果查看。	
5		数据资产动态识别	1.动态识别：对接入日志进行分析处理，发现流动中的敏感数据，并发现相关联的数据库、应用、API、账号信息。	

6		敏感数据资产	▲1.支持从数据标签维度查看敏感数据资产，可查看每种数据标签的敏感数据量、应用数、API数、数据库数、告警数、风险数、事件数，并支持下钻查看；（提供相关功能的界面截图并加盖公章） ▲2.支持从敏感数据的维度查看敏感数据资产，可查看每条敏感数据的发现时间、访问次数，所属的数据库、应用、API，及触发的风险数、事件数； 3.支持查看未打标数据的样本信息及详情，以便安全运营人员进一步优化标签规则。（提供相关功能的界面截图并加盖公章）	
7		数据内容级的识别与打标	对于存储中的静态数据与使用的流动数据，可识别具体的数据内容，并进行一定的敏感数据打标，并针对静态数据和流动数据以全局视图进行展示。提供细粒度到敏感数据内容的全局视图，可直接展示具体的敏感数据内容如手机号“139*****009”、身份证号“2112*********55564”、家庭住址“广州*****港中路”。	
8		存储资产管理	1.支持主动扫描发现网络中的数据库等存储资产； 2.支持手动添加存储资产； 3.支持从接入日志中动态发现存储资产； 4.兼容结构化、非结构化数据载体，进行数据采集和解析，至少包含 PostgreSQL、Mysql、oracle、Gbase8a、Gbase8t、Sqlserver、Cache、OceanBase、DM、KingBase、MariaDB、DB2、Informix、Firebird、HsqlDB、Oscar、Elasticsearch、Hbase、Hive、MongoDB、Kudu、FTP 服务器、HDFS、redis 等； 5.支持查看存储资产列表，并可查看每条存储资产的名称、地址、数据标签、敏感数据访问量、去重访问量、告警数、风险数。	

9		应用资产管理	1.支持从接入日志中，动态发现应用资产及 API 资产； 2.支持查看应用资产列表，并可查看每条应用资产的业务应用、Host、API 数、账号数、应用标签、发现时间、数据标签、敏感数据访问量、去重访问量、告警数、风险数； 3.支持查看 API 资产列表，并可查看每条 API 资产的业务应用、Host、API、发现时间、数据标签、敏感数据访问量、去重访问量、告警数、风险数。	
10		账号资产管理	1.支持从接入日志中，动态发现账号资产； 2.支持查看账号资产列表，并可查看每条账号资产的账号名称、类型（应用或数据库）、业务应用/数据库资产名称、应用 Host/数据库地址、发现时间、数据标签、敏感数据访问量、去重访问量、告警数；	
11		数据载体管理	支持定义并维护应用、数据库等资产信息，包括名称、所属部门等信息。	
12		数据资产管理	1.支持数据资产对象管理，可实现字段级数据资产定义与维护，数据资产记录信息包括元数据信息、数据标签信息及数据分类分级信息等。 2.支持手动维护字段敏感数据标签。	
13	数据分类分级	数据分类分级模版	1.系统内置数据分类分级模板，模板可按照场景需求进行自定义修改，分类分级模版支持多级设置，至少内置个人敏感信息和部分行业模版。 2.自定义安全分级评价要素生成数据安全分级模板，支持弹性定级标准，内置安全等级推荐计算表，通过用户自定义若发生泄露或破坏后分别对国家、公共、组织、个人等利益的影响，从而加权得出一个综合评判的等级。 3.支持自定义数据标签，应用关键字、正则表达式、内置标识符等方式新增数据分类的识别特征。 4.支持多维度的数据资产分类识别，识别纬度包括：列备注、列名称、列内容等。	

14		数据自动分类分级	▲1.支持对结构化数据进行自动分类分级，支持对非结构化数据进行自动分类分级。（提供相关功能的界面截图并加盖公章） 2.支持基于数据安全分级模板构建数据资产安全分级引擎，自动分析形成数据资产分类分级推荐结果； 3.针对系统推荐的安全定级结果，支持对级别、数据标签进行手工修正； 4.支持分类分级结果的导入导出。 5.支持对相似字段进行统一归并分析，便于管理员批量调整打标。	
15		数据分类分级版本	1.支持数据资产安全分级结果的发布，对历次发布的版本进行快照保存； 2.支持查看每个版本的分类分级统计，包括各级数据资产的数量分布及与资产总量情况。 3.支持多个版本间变迁对比及版本查阅，支持对不同版本的结果差异进行统计展示，包括敏感数据总量变迁、近期新增类别等。	
16		数据资产态势	▲1.支持大屏可视化展示数据资产态势，包括数据资产类型分布、数据资产等级分布、新增数据类型、数据源分布等信息（提供相关功能的界面截图并加盖公章）	
17	数据流动监测	数据流动监测	1.数据流动监测可从运营人员最关注的信息开始，逐步增加筛选条件，缩小范围，查看数据流动日志。 2.每条数据访问日志均可查看其源 IP、目标类型（应用、数据库）、IP 地址、数据标签、敏感数据去重访问量、访问时间等信息，并可查看该访问日志的数据流转图。 3.支持以链路的形式展示一段时间内的源 IP 通过应用访问数据库或者直接访问到数据库的行为，可以查看数据流转的节点、数据泄露的路径、访问者的源 IP、访问时间和访问的数据内容等信息。	

18		数据内容级的监测与分析	对于存储中的静态数据与使用的流动数据，可识别具体的数据内容，并基于数据内容进行行为监测	
19	数据安全风险分析	数据安全告警配置	1.支持基于监测分析规则进行威胁告警，支持用户自定义告警列表的展示字段，包括名称、类型、基本信息等，支持告警信息字段灵活扩充； * 2.支持数据安全告警的统一、集中展示，实时获取、展示数据安全告警总体情况； 3.支持告警信息钻取，支持根据不同的时间期限进行展示； 4.支持告警降噪，支持根据告警的类型、等级等配置告警归并规则，支持基于告警信息配置后置过滤规则，增强告警信息的可读性，避免告警数据过多，运营人员精力过渡分散。*	
20		数据安全告警分析	1.支持查看告警详情，包括告警描述、研判处置、关联敏感数据信息、关联身份信息、关联应用信息、关联数据库信息、关联文件信息； 2.支持把告警研判为风险或事件，支持人工研判及自动研判。	
21		数据安全分析规则	1.支持通过对多源日志关联分析发现数据安全事件； 2.支持通过特征建模及历史数据分析建立基线模型，以发现数据安全事件； 3.支持通过统计规则建模，在指定的条件范围内发现数据安全事件； 4.支持图形化交互配置方式，灵活组合规则建模中的计算单元；	

22		数据安全分析策略	1.支持告警穿透、单表过滤、单表统计、关联统计、序列、基线等 10 种引擎规则模板，针对特定场景，方便分析师快速定义流式规则； 2.支持图形化交互配置方式，灵活组合规则建模中的计算单元； 3.支持自定义场景，可灵活的将关心的多个分析规则放到同一个场景中组合显示； 4.支持通过人工自建、配置分析脚本的方式生成分析规则。 5.支持资源管理和过滤器配置，通过引用过滤器和提前配置好的资源快速生成策略，以便提高策略配置效率。	
23		场景化风险分析	支持通过自学习和用户自定义规则/场景，对流量、日志进行实时统计和分析。内置规则包括：数据源安全、数据操作异常、数据流动异常、账号使用异常等大类。	
24		数据资产安全评估报告	1.系统提供数据安全评估报告模板管理功能，预置至少 5 种不同内容框架如组织架构、制度保障、数据风险、权限管理、安全审计等的报告模板，支持自定义数据安全评估报告的内容框架、样式格式，并建立评估报告的分类体系； 2.至少包含告警、事件、态势等评价要素，支持根据不同的评价要素中的指标项组合自定义评估模型，支持自定义分数范围，各评价要素报告方式支持编辑，提供文本、表格、选项、文件上传等反馈方式； 3.支持自定义整改建议模板，包含整改建议和安全事件的关系、整改建议的展现样式等内容 4.支持根据数据资产安全评估模型生成安全评估报告；支持根据评估过程中产生的各种指标和最终结论，针对相应的薄弱环节提出安全整改建议； 5.支持 PDF、Word、HTML 三种格式的报表生成与下载。	

25		数据资产统计分析报表	1.报表生成配置要素支持根据项目需求扩展； 2.支持 PDF、图片、csv 和 excel 等格式的报表生成与下载； 3.支持报表模板管理，可自定义报表内容，支持灵活编辑和布局调整以形成整体报表，包括选择展示数据内容、图表类型等，系统预置 5 种以上报表模板；	
26		数据安全事件管理	1.支持数据安全事件的统一、集中展示，实时获取、展示数据安全事件总体情况、发展趋势； 2.支持事件关联日志信息钻取，支持根据不同的时间期限进行展示； 3.展示和过滤字段等支持灵活设定。	
27	数据安全响应处置	数据安全事件溯源	1.支持基于告警信息自动生成数据安全事件； 2.支持人工研判方式生成数据安全事件，支持根据事件信息字段关联告警或日志； 3.支持从安全事件入口，溯源展示关联身份信息、关联敏感数据信息、原始日志信息：支持在已知泄漏数据或数据片段情况下，将其作为线索进行溯源； 4.输入检索条件后针对出现的多个可疑来源 IP 进行集中度聚合统计分析，如目的 IP 出现占比、资产名称出现比例等，从而方便运营人员去快速分析研判。 5.支持数据安全事件查询与展示，展示内容包括事件统一编号、事件名称、事件等级、事件描述和事件危害等。	
28		数据安全事件处置	1.支持数据安全事件与处置方案库的匹配，针对数据安全事件，自动检索处置方案库，确定事件处置方案；对于处置方案库没有的场景，支持人员补充更新处置方案； 2.支持邮件事件通知，事件通知支持自定义模板； 3.支持事件处置跟踪记录。	

29		数据安全风险溯源	1.支持人工研判方式生成数据安全风险，支持根据风险信息字段关联告警或日志； 2.支持从风险入口，溯源展示风险资产名称、资产类型、资产地址、原始日志信息； 3.支持数据安全风险查询与展示，展示内容包括风险统一编号、风险名称、风险等级、风险描述和处置建议等。	
30		数据安全风险处置	1.支持邮件风险通知，风险通知支持自定义模板； 2.支持风险处置跟踪记录。	
31		数据安全联动处置	1.支持联动同品牌数据安全设备： API 防护系统：对涉事 API 进行限流处置； 特权账号管理系统（PAM）：禁用资产相关的 PAM 用户，暗资产信息发送给 PAM 进行纳管。 2.支持单点登录至同品牌其他低位安全组件（至少应包含流转数据监测系统、API 安全监测系统、数据库审计监测系统、零信任控制系统、API 安全网关、跨境数据监测系统、堡垒机、应用访问监测系统、应用安全网关、PAM、智能身份分析系统等），支持对其他低位安全组件进行状态监测。 3、对接同品牌跨境数据监测系统，完成对告警日志的接入及分析。	
32	数据安全态势	数据流动态势	通过图形化的方式展示企业内敏感数据的流动情况，包括敏感数据的来源、去向、趋势等；可直观展示敏感数据流出趋势、敏感数据流出 TOP5、敏感数据访问量 TOP5、涉敏资产统计及敏感数据流动实时监测；帮助企业更好地了解敏感数据的流动趋势和热点情况。	
33		数据安全态势	通过图形化的方式展示企业中的风险和事件，以及他们的分布情况。包括最新风险、最新事件、事件类型分布、风险类型分布、危险趋势、资产风险等。通过图形化展示方式，帮助企业更好地了解风险和事件的分布情况。	

34		数据分布态势	通过图形化的方式展示企业内的数据分布情况，包含敏感数据的数据源和敏感数据的维度展示数据源的分布情况、敏感数据的类型、级别、新发现的包含敏感数据的库表等	
35	系统自身安全	系统自身安全	1.用户的统一管理，支持角色定义与系统自身操作权限设置，支持灵活细致的权限设置 2.支持对系统自身所有操作生成日志信息，支持对操作日志的查询检索，支持备份系统日志，系统支持日志保存期限不少于180天； 3.支持对用户登录进行统一认证和鉴权，具备登录失败处理功能，具体参数可以由管理员设置；	
36	资质要求	资质要求	《计算机软件著作权登记证书》、《网络关键设备和网络安全产品证书》、《国家信息安全漏洞库（CNNVD）兼容性资质证书》具备信通院颁发的《分类分级能力检验（基础级、进阶级）》数据安全产品检验证书、《数据异常行为监测（基础级、进阶级）》数据安全产品检验证书、《数据安全管控平台（基础级）》数据安全产品检验证书	

5. 网络空间测绘平台

序号	一级功能模块清单	二级功能模块清单	功能需求	备注
1	探活任务调度	▲基于伪随机序列生成算法的任务调度策略，支撑全球IPv4地址空间探活任务高效随机化调度。（提供相关功能的界面截图并加盖公章）	350M IPv4地址，200端口，每2000个任务批量请求的情况下，每台扫描节点约占用2.6Kbps带宽 国内约3.5亿IPv4地址，800个高频端口的扫描场景下，在满足NIST 16种伪随机检验标准的前提下，1台4核心/8G内存/20Mbps上行带宽的机器配置，可支持30台4核心/8G内存/100Mbps上行带宽的机器集群的探活任务调度	

2	IP 与端口探活	IP 与端口探活功能完成 TCP 协议端口探活、UDP 协议 IP 探活工作，基本探活过程是以半连接方式（发 SYN 包收 ACK）完成的。	扫描目标：国内 3.3 亿 IP，国外 33 亿 IP 支持虚拟化环境，包括但不限于 KVM(Virtio Linux Bridge),KVM(Virtio DPDK),VMware(VMXNet3) 4C/8G 单机可在 75 小时完成国内高频端口探活 4C/8G 单机可在 31 天完成国外高频端口探活 全端口覆盖	
3	协议识别	协议识别依赖协议指纹，协议指纹通常包含两部分：协议发包 payload、网络回包 banner 匹配规则。在协议指纹的基础上，结合一套基于统计的协议识别发包策略，完成协议的识别工作	1. 国内 IP 800 高频端口探活性能 2.. 协议总数：大于 1000 3. 支持协议清单详见“协议” sheet 页	
4	网络爬虫	针对 web 资产需要使用网络爬虫技术，对网站进行爬取，以获取更多的资产信息，在此基础上对网站进行指纹识别。并结合使用无头浏览器技术，对部分需要动态渲染的网站资产进行爬取。	1. 4C/8G 单机 1000 万网页爬取任务大约需要 80 小时完成 2. 4C/8G 单机 1 小时能够爬取大约 12.5 万网页 3. 支持 JS 渲染，页面缓存，静态资源缓存，重定向识别记录，url 级别流量重定向(Socks5)等 4. 每个页面平均 1MB 大小，4C/8G 单机需 280Mbps	
5	IP 地理位置标定	通过对 IP 地址的地理化标定，能够有效的将虚拟的网络空间资产进行地域化设定，从而实现虚拟到现实的过程，明确虚拟空间的归属区域、管理区域。	1. 支持城市级属性标定，包括但不限于国家、省、市、邮编等信息 2. 支持 AS 相关信息标定，包括 AS 号、AS 名称、AS 注册机构等信息	
6	备案信息关联	通过将测绘网站资产与 ICP 备案信息关联，测绘平台能够快速定位网站资产的主体单位，获取单位名称、单位性质等信息，协助个人、企业、监管单位明确网站责任归属，梳理网站暴露面。	1. 支持网站备案信息关联，包括企业备案名称、备案号、备案类型等。	
7	指纹识别	指纹数据主要由规则、分类、标签等信息构成，在数据融合阶段，通过指纹规则与资产的回包 banner、响应等数据进	1. 指纹数量大于 80 万 2. 支持厂商、版本等信息识别	

		行碰撞，从而识别资产的指纹信息。		
8	操作系统识别	操作系统是服务器、计算机、终端、网络设备的运行基础，操作系统识别是指纹识别的重要组成部分，能够对网络测绘资产属性进行补充。	1. 支持 16 种操作系统识别，包括 Windows、Ubuntu、Debian、Linux、Centos、RHEL Linux (Red Hat)、FreeBSD、FreeboxOS、Fedora、VMware Photon OS、SUSE Linux、MacOS、Gentoo、SunOS、netBSD、Dopra	
9	资产标签	资产标签着眼于资产应用，通过对探测获取的高层级的应用信息进行维度分析，实现对网络资产的应用标记，帮助用户挖掘数据的应用业务价值。	1. 标签数量 202 种，包括不限于党政事业单位、登录页面、OA、监控系统、主机面板等	
10	IP 标签	IP 标签注重网络层面的技术数据价值，通过对探测获取的资产网络属性表现进行聚合或特征分析，实现对探测资产的网络技术标记，帮助用户挖掘数据的网络技术价值。	1. 标签数量 3 种，包括蜜罐、CDN、云厂商	
11	相似 ICON	网站 favicon 是 web 资产的一个重要特征，对海量 web 资产 favicon 数据，通过机器学习的方法，进行模型训练，将海量 favicon 数据按相似度进行聚类，用户可找出与目标 favicon 具有相似 favicon 的资产。	1. 超过 20 万聚类分组，准确率 90%以上	
12	相似网站	相似网站功能从网站结构角度，进行特征向量分析、建模，找出海量 web 资产网页结构维度具有相似度的资产。	1. 超过 3 万聚类分组，准确率 80%以上	
13	语法查询	支持用户输入满足平台语法规则的查询语法，查询对应的数据。用户可以在首页点击【查询语法】，或在【帮助中心-基础语法】了解平台的语法分类。 在输入语法的过程中平台会自动提示语法与说明，同时平台兼容了友商的语法，致力于提升	1. ip 语法，查询时间 610ms，聚合时间 600ms 2. ip.port 语法，查询时间 790ms，聚合时间 820ms 3. domain 语法，查询时间 810ms，聚合时间 810ms 4. protocol 语法，查询时间 1.1s，聚合时间 2.2s 5. protocol.banner 语法，查询时间 1.3s，聚合时间 1.8s	

		用户检索效率，降低用户学习语法成本。	6. web.title 语法，查询时间 790ms，聚合时间 950ms 7. web.body 语法，查询时间 890ms，聚合时间 1.1s 8. web.tag 语法，查询时间 810ms，聚合时间 3.2s 9. app 语法，查询时间 1s，聚合时间 1.4s 10. cert 语法，查询时间 520ms，聚合时间 1s	
14	ICON 查询	平台支持用户上传 icon 来查询资产，解决了用户在已知资产特征较少的情况下，可以通过 icon 检索资产。	1. web.icon 语法，查询时间 700ms，聚合时间 750ms 2. 图片格式支持但不限于 jpg、png 等	
15	相似 ICON 查询	平台引擎结合了机器学习，能够根据用户上传的 icon,提取特征聚类，推荐“图形相同大小不同”或“图形相似”的 icon 所命中的资产。	1. web.similar_icon 语法，查询时间 750ms，聚合时间 1.2s 2. 相似 ICON 聚类分组准确率 90%以上	
16	相似网站查询	相似网站功能从网站结构角度，进行特征向量分析、建模，找出海量 web 资产网页结构维度具有相似度的资产。	1. web.similar 语法，查询时间 750ms，聚合时间 950ms 2. 相似网站聚类分组准确率 90%以上	
17	批量查询	支持用户通过上传文件、或批量检索 ip/域名/网段，快速查询资产	1. text/file(10 条 IP 批量查询)语法，查询时间 1.2s，聚合时间 1s 2. 支持 IP/域名/IP 段混合批量查询	
18	数据检索与处理	资产列表	根据用户的检索语法，系统将展示匹配的资产数据。资产列表页左侧的统计数据基于用户检索结果聚合而来，默认展示最近 1 年的数据、以及国家排行、开放端口排行、使用组件/协议排行。	
		IP 详情	IP 详情页从 IP 的视角出发，展示当前 IP 的基础信息，以及在最近 1 年内开放的端口，关联的域名；点击域名，可在右侧查看该域名所属 ICP 企业，以及端口响应，html 等信息。	
		企业详情	企业详情页从企业的视角出发，展示企业基本信息、企业资产概况、备案概况、域名概况、网站概况、资产标签、IP 概况、证书概况、IP 地理位置等信息。	

		证书详情	证书详情页从证书的视角出发，展示当前选中资产、证书链、证书基础信息（包括证书信息、使用者信息、颁发者信息）、使用者可选名称、域名解析 IP 等信息。	
		域名详情	域名详情页从域名视角出发，展示域名的 whois 相关信息、ICP 备案信息、域名解析记录、证书概况等信息。	
		API 功能	平台提供 Open API，支持获取条件检索结果详情、获取条件检所结果聚合值等。 查询接口支持上传文件或语法来检索，输出内容包括但不限于 ip、端口、协议、域名、url、地区等；支持运算符、翻页条查询；支持每次查询返回记录数；支持查询参数可选等。	
		导出功能	平台提供导出功能，支持运营、安服人员在 HW/攻防期间，为企业提供资产清单的需求，格式支持 csv。 资产清单内容包括但不限于：url、IP、端口、网站标题、域名、协议、状态码、应用组件、操作系统、备案单位、备案号、国家、省市区等。	
		区域测绘专题	区域测绘专题是专门针对区域的数据在监管场景下预制的进行多维度的专题分析，包括但不限于区域资产数量、漏洞暴露面、icp 备案率统计、应用组件专题等维度。 区域测绘专题以城市为单位进行授权，购买区域测绘专题的客户，可对所购买城市下的数据进行浏览以及全量导出。	
		漏洞专题	漏洞专题页汇总统计了全国存在风险的资产数量，以及受严重与高危漏洞影响的资产分布及地区排名。同时根据地理位置查看区域内热门漏洞 Top20，支持检索单条漏洞所关联的资产分布情况及修复状态。	
		ICP 备案专题	ICP 备案专题页汇总统计了全国网络资产的备案情况，对区域备案情况进行排序、未备案率进行统计并对未备案资产	

			进行导出。	
		数据库专题	数据库专题整合了市面上广泛使用的数据库品牌在互联网的暴露情况，帮助用户快速了解常见数据库的品牌分布、区域分布、历史数据趋势信息。	
		OA 专题	OA 专题整合了市面上广泛使用的 OA 品牌在互联网的暴露情况，帮助用户快速了解常见 OA 的品牌分布、区域分布、历史数据趋势信息。	
		Web Servers 专题	Web Servers 专题整合了市面上广泛使用的 Web Servers 品牌在互联网的暴露情况，帮助用户快速了解常见 Web Servers 的品牌分布、区域分布、历史数据趋势信息。	
		重大漏洞预警专题	重大漏洞预警专题，主要应对互联网漏洞刚披露时快速对于辖区资产影响面的预警分析。利用全球鹰网络空间测绘系统暴露面资产数据，可实现重大漏洞披露后 2 小时获取全国各省市地域分布情况。	

6. DNS 安全平台

序号	一级功能模块清单	功能需求	备注
1	解析能力	解析能力必须具备运营商级别解析能力，解析稳定性更高，延时更低。	
2		▲解析稳定性高，累计域名解析量 120 亿+。（提供相关功能的界面截图并加盖公章）	
3	威胁情报能力	威胁情报库 ioc 数量 1.4 亿+。	
4		安全 DNS 威胁情报数据服务 200W+活跃情报，情报数据每小时更新。	
5		安全 DNS 威胁分析能力，能够对 APT 攻击、勒索软件、窃密木马、远控木马、僵尸网络等几十种网络威胁请求进行有效检测和拦截。	
6	▲域名监控	支持客户自定义域名监控任务，实时统计监控域名访问情况与告警情况，通过邮件策略配置，及时将告警信息传递给客户，方便客户快速定位问题并处理。（提供相关功能的界面截图并加盖公章）	
7	部署便捷性	SaaS 平台，秒级部署，无需本地硬件，无需网络改造。	
8	数据可视化	支持查看域名解析/拦截趋势，实时全局掌控解析态势。	
9		支持以域名解析维度，查看自定义时间内域名解析日志。	

10		支持以告警事件维度，查看自定义时间内的事件分析日志。	
11		支持查看请求类型分布、威胁类型统计、资产 IP 解析域名信息。	
12	资产管理	支持告警事件邮件通知，方便客户快速定位问题并处理。	
13		支持自定义监控资产 IP 任务，实时监控资产 IP 解析域名情况并对威胁进行告警，方便及时了解内部资产威胁情况。	
14	日志审计	支持记录用户后台操作行为，便于查看历史操作记录。	

（二）定制化开发软件功能需求

1. 城市网络安全体征预警平台

序号	一级功能模块清单	二级功能模块清单	备注
1	研判分析子系统	关联组合分析	
		阈值分析	
		序列分析	
		基线分析	
		攻击者分析	
		场景分析	
		实体分析	
		威胁预警分析	
2	安全联动子系统	编排与自动化管理	
		剧本管理	
		应用管理	
		安全告警分诊	
		事件告警关联分析	
		安全事件管理	
3	资产中心	资产目录	
		资产管理	
		资产运营	
		暴露入口管理	
		脆弱性管理	
		漏洞管理	
		弱口令管理	
		基线核查管理	
		WEB 漏洞管理	
		安全隐患管理	
4	外部数据源对接子系统	与运维管理平台对接	
		与统一日志平台对接	

		与云安全管理系统对接	
		与终端安全管理系统对接	
		与云端威胁情报系统对接	
5	体征大屏	体征态势首页	
		资产体征态势	
		全网脆弱性体征态势	
		外部威胁态势	
		内部威胁态势	
6	视图管理	视图自定义	
		视图操作	
7	业务协同	指令接收	
		漏洞协同管理	
		钓鱼情报接收	
		协同监控	
		数据报送	
8	工作指挥	事件管理	
		事件通知	
		工单管理	
		统计报表	
		组织与权限管理	
		风险预警	
		应急指挥	
		预案编排	
9	安全管理	拓扑管理	
		分级管理	
		通报预警	
		设备监控	

1.1 研判分析子系统

定制适用于杨浦区全业务需求的研判分析系统，利用安全分析技术，对接入的杨浦区安全数据进行统计、分析、规律性探索及预测等，支撑安全应用业务场景复杂、多变的需求。包括关联组合分析、阈值分析、序列分析、基线分析等分析方法，以及场景分析、实体分析、攻击者分析、威胁预警分析等分析工具。

- 关联组合分析

由于单一安全设备的分析无法发现类似 APT 的持续复杂攻击行为，在系统已经采集的海量安全日志基础上，通过将不同数据资源的两个或多个要素相关联，发现满足多个条件的关

联线索，触发响应，生成关联组合分析结果。海量的大数据关联分析需要高性能的关联分析引擎。通过关联分析引擎实现在大数据量级下，对数据进行实时关联分析，发现更复杂的、更具价值的威胁事件，并将威胁事件规模控制在可人工处理的数量级。

能够接入各种类型数据，包括但不限于：设备日志、网络流量、失陷类威胁情报数据、资产数据、漏洞数据等类型数据进行关联分析。能够实现各种威胁检测规则建模，包括统计模型、关联模型、序列模型等典型威胁场景模型。能够设置各种模型参数和规则条件，包括：支持多条规则与或、非逻辑关系运算，支持规则的多级嵌套，支持对规则分析输出字段的自定义。

建模过程和实现方式尽量可视化，降低操作难度，避免负责的配置过程甚至是类代码的编写过程。例如安全人员通过 web 图形化配置界面完成对应的威胁建模配置后，关联分析的引擎应能根据 web 界面的配置输入，自动进行词语法解析、规则分析、规则编译、代码生成，进而生成该建模规则的代码层面计算任务。系统内置的关联分析引擎则将按照该计算任务，对其所接收到的实时数据流进行关联分析计算，最终产生符合该威胁建模规则的告警事件同时，考虑到未来整个系统的信息量会持续增长，需要整个关联分析系统基于大数据架构设计和实现，支持集群部署，可根据业务和数据量将分析系统水平扩展至多台计算节点的集群以提升处理性能。

- 阈值分析

基于统计规则的建模，在指定的时间范围内，对符合过滤条件的日志出现的次数进行计数，以发现统计类场景下的威胁事件。例如，能够对暴力破解场景下，登录日志中账号登录失败的次数进行统计以触发告警。

通过统计规则建模，在指定的时间范围内对符合过滤条件的日志中数字类字段进行求和、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事件。例如，发现当前 1 小时内的 TCP 平均流量超过一周时间内 TCP 平均流量的 40%，触发一条威胁告警。

- 序列分析

支持序列规则建模，在指定的时间范围内，对多种安全事件（即日志）发生的顺序进行判断，以发现复杂场景下的威胁事件。例如，对“永恒之蓝”勒索病毒攻击的一系列先后发生的事件进行判断，触发威胁告警。

- 基线分析

能够对历史及实时日志数据进行基线学习，生成基线数据，通过动态基线计算、对比和深度分析，检测发现严重偏离基线的异常事件。主要能力包括：

日志行为模型建模：对实时日志进行检测，发现实时日志中的行为不符合基线。如检测受 WEB 应用受访来源异常，模型会学习访问 web 应用的源 IP 空间，实时日志中的源 IP 不在基线空间这种，则产生一条异常行为。

统计行为模型建模：对实时日志的统计结果进行检测，发现统计行为不符合基线。如检测工作时间 WEB 应用访问频次异常，统计工作时间内，8 小时的访问次数超过基线，则产生一条异常。

基线分析结果管理：可以对系统自动生成的基线结果进行人工编辑，修改。并将修改后的人工基线与系统自动生成的基线进行对比，方便实现持续优化。

能够对基线分析下发现的异常行为进行打分量化：实现例如统计查看前 TOP20 的异常行为得分，能够快速了解哪个异常行为得分最高；异常行为得分的时间分布，能够快速了解哪个时间点异常最严重；查看前 TOP20 的异常对象得分，能够快速了解哪个异常对象的异常行为最严重。

异常行为分析结果能够体现的信息维度包括：异常名称、异常对象、分组条件、异常得分、异常描述、异常时间、模型类型、检测模型、关联资产、置信度、检测特征、异常值、正常基线。

- 攻击者分析

基于攻击者视角对告警进行归纳分析，能够提供更直观、目的性更强的告警信息，可快速定位攻击者 IP、攻击类型、攻击链阶段、危害等级、IP 归属地、IP 来源、威胁告警数、首次攻击时间、最新一次攻击时间。受害者情况等。同时能够通过攻击者详情查看攻击行为、受害者影响范围情况，快速定位问题，进行联动处置，例如联动边界安全设备实现快速封堵，或者告警信息通知等等。事件调查分析

系统提供对威胁事件的调查分析能力，安全运营人员可以对需要调查的威胁事件创建任务，将所有与调查问题相关的告警、日志、漏洞、弱口令、配置弱点、文本和图片信息都添加至任务中，从而将多种告警、日志、孤立的线下事件等信息重新按照攻击链模型等类似攻击全流程视角进行所有安全信息的重新排序，梳理出各安全告警等信息对应的不同阶段，例如侦查跟踪、武器构建、载荷投递、突防利用、安装植入、通信控制、达成目标等。最终以时间维度串联成完整事件，通过时间线展示、标注等功能回溯并记录威胁事件的发展过程和相关影响。

在调查任务中还需能够对任务进行级别标注、备注说明、历史操作记录，以便于分析，弥补对事件调查分析的不足。调查分析需要能够针对任何需要调查的安全问题创建实例（case），将所有与要调查的问题相关的告警、日志，甚至其他文本、图片信息都录入 case 中，然后通过时间趋势展示、标注等功能可以回溯并记录问题的发展过程和相关影响，再通过搜索等功能不断的扩展其他的日志线索，丰富该问题的相关证据。最后在有支撑的情况下形成调查结论。

- 场景分析

系统提供场景化的威胁分析能力，包括失陷情报、热点恶意软件、邮件安全、账号安全、异常访问 5 大类分析场景，从多维度多视角进行分析并采用可视化技术进行展现，安全运营人员经过简单分析后即可判断异常事件中包含潜在威胁。其中：

失陷情报分析场景：结合强大的威胁情报能力，可快速获取全局下的安全状况和特定情报下的安全状况；

热点恶意软件分析场景：对当前流行的挖矿木马、勒索软件、网络蠕虫、僵尸网络类的威胁事件进行分析，可快速了解全网受害情况、扩展趋势和最早在网内出现等信息；

邮件安全分析场景：从邮件附件是否为恶意文件、敏感后缀，邮件中是否包含恶意链接、敏感关键词等多个维度进行分析；

账号安全分析场景：包含暴力破解、明文密码传输、账号异地登录、VPN 账号安全等多个维度进行分析；

异常访问安全场景：包含 DGA 域名检测、业务资产主动外连、http 代理、DNS 隧道等场景的检测与分析。

- 实体分析

由于安全运营中心建成后已能够收集到各种不同维度的安全信息，而安全运营人员在实际分析安全事件的过程中，需要频繁地结合各个多维的安全信息对某个具体的对象（即实体）进行综合性判断，因此平台通过提供高聚合、便捷的实体分析能力，能够帮助安全运营人员提升安全分析效率、节约分析时间、避免遗漏关键信息。

当发现外部可疑攻击者时，通过实体分析功能可快速获取可疑攻击者相关的威胁、脆弱性、登录访问关系、威胁情报等上下文信息，例如一键对于外部 IP 进行实体分析，集中展示该 IP 相关的威胁信息、登录内部网络资产的情况、威胁情报鉴定信息和在网络中最早出现的时间等，并从多维度进行可视化展示与分析；

当发现疑似受攻击资产时，通过实体分析功能可快速获取疑似受攻击资产相关的威胁、脆弱性、登录访问情况、资产非法外连、资产暴露面等上下文信息，例如一键对内部 IP 进行实体分析，集中展示该 IP 相关的资产信息、服务/端口暴露情况、威胁告警信息、漏洞/配置核查/弱口令等脆弱性信息、被登录访问情况、主动外连行为等，并从多维度进行可视化展示与分析。

- 威胁预警分析

为提高内部网络应对重大网络安全事件的能力，系统提供威胁预警分析能力，通过基于业界厂商发布的重大事件威胁预警规则等信息，快速完成内部网络安全影响面评估，并持续跟进事态的发展，快速完成重大网络安全事件的预警分析。需要威胁预警系统能自动化实现的能力包括：

1）受该事件影响的风险资产数、受攻击资产数、失陷资产数以及数量变化趋势监控。

2）该事件发展过程节点监控和展示，如首次出现、大面积爆发、有效控制、威胁缓解等，支持自定义里程碑节点。

3）此事件在内部网络的扩散过程发展趋势监控和展示，可以直观呈现被攻击及失陷资产出现的前后顺序、扩散关系，以及关联的告警记录详情。

4）此事件关联的终端信息，包括如资产 IP 地址、所属网段、终端名称、病毒名称等；

系统还需要能够实现灵活的自定义预警监测规则的能力，以方便用户按实际情况（如攻防演练）实现快速的个性化预警监测诉求。

1.2 安全联动子系统

定制安全联动系统，将安全运营相关的团队、工具和流程通过编排和自动化技术整合在一起的，有序处理多源数据，持续进行安全告警分诊与调查、威胁猎捕、案件处置、事件响应，并最终实现高效、有效安全运营的智能协作系统，是智能化协作运营系统，关键功能包括，安全告警分诊与调查、威胁猎捕、安全事件处理、安全事件响应等。

- 编排与自动化管理

编排与自动化是整个系统的核心功能，实现了运营流程的剧本化和安全应用的编排化，并通过编排器实现了剧本和应用的自动化执行。安全运营人员通过剧本库对所有剧本进行统一管理，支持剧本的增删改查、导入导出。系统内置基本的剧本，包括基本的调查类剧本和响应类剧本。

- 剧本管理

系统具备完善的剧本管理功能，包括剧本库管理和可视化剧本编辑器。安全运营人员通过剧本库对所有剧本进行统一管理，支持剧本的增删改查、导入导出。系统内置基本的剧本，包括基本的调查类剧本和响应类剧本。

系统内置可视化剧本编辑器，允许剧本设计师方便地进行剧本创作。在编写剧本的时候，可以选择的元素包括应用动作、API、人工任务、审批、自定义变量、脚本、子剧本、条件分支，等等。管理员可以将这些元素通过鼠标拖拽的方式加入编辑器中，构成一个图形化的剧本图。针对每个元素，管理员都可以进行详细的设置。

- 应用管理

应用管理实现了对内外部应用及其动作和实例的统一化管理，借助系统内置的应用管理功能，可以将所有与外部安全设施和运营相关的各种系统和功能映射为内部可识别的应用，每个应用都是特定安全能力的服务化封装。应用是安全能力集成的基础，是编排化安全剧本的基本元素。

- 安全告警分诊

系统基于预定义的合并策略自动化的聚合告警信息，减少管理员需要查看的告警数量，同时还能自动地计算告警的处置优先级。安全运营人员可以修订告警的状态，针对具体的告警信息产生工单，或者添加到安全事件中去。在将告警信息添加到案件的时候，可以指明将告警的哪些属性值作为痕迹加入该案件中。

- 事件告警关联分析

针对每条告警，可以进入告警调查页面，对告警信息进行全面呈现和调查分析。在告警调查过程中，可以对告警信息进行追溯，可以调用剧本和应用动作，并查看执行结果。系统通过列表方式，按照告警所处的不同状态显示所有告警信息，以及每种状态的告警数量。安全运营人员可以对告警信息进行检索查询，可以以时间线的方式显示不同时间切片下不同等级告警的数量信息，并可以自定义各种告警统计图表，能够以曲线图、面积图、柱状图、饼图等形式可视化呈现统计结果。

安全运营人员可以修订告警的状态，可以针对具体的告警信息产生工单，或者添加到案件中去。在将告警信息添加到案件的时候，可以指明将告警的哪些属性值作为痕迹加入该案件中。

- 安全事件管理

安全事件管理用于帮助安全运营人员对一组相关的告警进行流程化、持续化、协作化、全周期的调查分析与响应处置。系统提供痕迹管理、标注管理和附件管理功能，相关安全运营人员可以往案件里面添加痕迹信息、进行标准、上传附件，从而不断积累该案件相关的痕迹物证（IOC）和攻击者的战技过程指标信息（TTP），并记录案情进展。

安全运营人员可以查看事件相关的事告警信息，并能够对聚合告警进行追溯。系统提供关系图等可视化调查分析的手段，以帮助用户拓展相关案件的痕迹信息。对于事件中的每个痕迹，可以激活预置的响应动作，所有动作的执行操作及其结果都会自动记录，作为该案件

的活动记录。安全运营人员也可以针对事件激活预置的编排剧本，并将相关操作和结果记录到活动记录中。所有事件相关的活动记录都可以被查阅和审计。

1.3 资产中心

定制开发资产中心实现对了资产的关键实体、属性以及关联关系的资产逻辑数据模型（LDM）的定义，形成统一、准确、实时的资产信息图谱，从而构建以单位、系统、网站、计算设备、软件、服务、机房、云平台、网络、数据库等为主体的网络资产库，实现资产、漏洞、威胁的原生关联，为资产管理、分析、评估提供数据支撑。
同时资产中心实现资产纳管能力，通过资产归属自动运营，实现并解决资产更新、冲突、合并等运营工作复杂的问题，将原始发现的资产通过运营规则进行自动纳管，包括内置的归属规则、运营规则和忽略规则。同时能够根据不同的资产数据的数据源配置不同的置信度，从而当不同数据源的数据发生冲突时，自动采纳高优先级的数据源或推荐保留数据，提升资产管理工作的效率。

- 资产目录

资产目录展示纳管资产的整体统计信息，包括单位、系统、服务、设备、网站、机房和软件的数量统计，以及资产运营统计、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、资产单位分布和行业资产分布等。根据不同纳管资产的检索需要，系统支持对所有纳管资产的统一检索。系统支持根据不同的检索条件进行查询，可支持快捷模式和高级模式两种查询模式。检索的结果可以按照不同的资产类型（单位、设备、软件、服务、系统、网站、机房、云平台、网络、数据库等）进行分类。

- 资产管理

实现不同类型资产（单位、设备、软件、服务、系统、网站、机房、云平台、网络、数据库等）进行统一管理，包括新增、编辑、删除、导入、建立关联关系等操作。

- 资产运营

资产运营实现对资产发现后无归属单位或系统的无主资产，或在资产运营中出现归属冲突的资产进行归属管理。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的规则自动将原始发现资产通过归属规则、运营规则和忽略规则，自动解决运营中的冲突处理，将资产进行纳管；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将资产纳管。资产运营的主要功能包括：规则管理、资产归属管理、发现资产审核。

- 暴露入口管理
- 脆弱性管理

脆弱性管理实现了对资产脆弱性的管理和运营闭环，通过已纳管的资产、漏洞扫描告警数据和漏洞知识库进行关联分析，实现对不同视角查看脆弱性的情况，包括主机漏洞、WEB漏洞、弱口令、配置核查等专项管理。

- 漏洞管理

漏洞管理提供漏洞知识库的管理功能，包括漏洞库统计、公共漏洞库和我的漏洞库。其中漏洞知识库提供了漏洞查看和漏洞影响面功能，我的漏洞知识库提供了对自身维护的漏洞知识库的管理功能。

- 弱口令管理

系统支持对于弱口令漏洞进行管理，包括主机 IP、主机名称、应用层协议、服务名称、服务端口号、用户名、密码、危害等级最近发现来源、发现次数、最近发现时间、修复状态等。系统支持针对弱口令转指令处理，包括创建处置指令和添加到处置指令。

- 基线核查管理

系统基于模型学习行为基线，实时发现偏离基线的行为，产生行为异常事件。行为异常事件可关联资产进行风险评估和风险统计。用户可查看发生异常行为的实体对象，根据发生异常的实体对象进行处置。

- WEB 漏洞管理

系统支持对于 WEB 漏洞进行管理，包括网站地址、网站名称、最近发现来源、漏洞名称、漏洞类型、漏洞危害等级、漏洞描述、发现次数、首次发现时间、最近发现时间、修复

状态等。

- 安全隐患管理

能够持续监控内部漏洞、弱口令和配置弱点情况，展现内网脆弱性分布、趋势、被攻击者利用的情况，有效地管理安全隐患

1.4 外部数据源对接子系统

外部数据源对接子系统通过资产测绘、流量发现、人工报送、第三方平台对接等方式接入各类资产数据，同时通过资产探测、流量探针、第三方漏扫设备等收集资产脆弱性相关数据。

外部数据源对接子系统将为其他系统提供基础数据源：

为威胁中心告警管理、事件管理提供数据源；

为分析中心多维分析提供资产关系数据源；

为指挥中心的通报、重保、应急等业务提供对象数据源；

为评估中心提供业务的数据源；

为报表中心提供分析数据源；

为态势感知提供资产相关的分析数据源。

1.5 体征大屏

定制适用于杨浦区网络安全整体展示与指挥协同的体征监测大屏，体征监测系统内置不同分析组件，可针对大数据平台的数据情况，进行不同维度的分析呈现，便于安全运营管理者在宏观角度上了解全区网络安全情况。所有分析组件组成的不同分析维度场景均可保存为模板或存为默认首页，并能够关联到不同用户。有效提升不同用户、不同场景下安全态势感知平台分析效率和结果呈现。

体征大屏服务于平台各个模块子系统，通过选择需要展示的子系统数据来源，并设置数据的可视化展示样式等，实现个性化的展示需求。本子系统包含以下几个模块：可视化大屏管理，自定义组件，数据源设置，可视化展示层次配置，数据交互配置。

(1)可视化大屏管理

系统能够对于构建的大屏及组件进行系统的管理。可以对于大屏进行新增、修改、删除、复制、预览等功能，并能够定义不同的应用场景进行分组管理。

(2)自定义组件样式

系统能够组件样式，应用拖拽、缩放、配置等方式，对于大屏的图形， 布局进行调整。主要包括：

页面配置：对当前大屏的页面进行配置。

屏幕大小设置：对当前大屏的页面大小进行设置，如：1920px * 1080px。

主题设置：对当前大屏的主题进行统一设置。

背景颜色设置：对当前大屏的背景颜色进行设置。

背景图设置：对当前大屏的背景图进行设置。

页面缩放方式设置：对当前大屏的缩放方式进行设置，包括等比缩放宽度铺满、等比缩放高度铺满、全屏铺满三种方式。

栅格间距设置：是在缩放拖拽组件时可以缩放拖拽的最小像素值。

(3)数据源设置

系统能够支持针对不同类型的数据源的数据进行可视化分析展示的功能。数据源主要包括，文件（JSON 格式），数据库 API 接口，数据模型（选择平台已经连接的数据库中的数据模型）等。

根据数据源的不同，可以选择不同类型的组件进行可视化展示，包括但不限于文字，表格，柱状图，饼图，百分比图，时间轴图，进度条图或地图等各种可视化展示方式。

(4)可视化展示层次配置

对于不同数据展示的效果，可以进行不同展示层次的设置，包括置顶、置底、上移一层、

下移一层等内容， 以丰富可视化大屏展示的效果。
(5)数据交互配置
系统可以对于不同的分析图进行配置，实现下钻分析、组件联动分析、多屏联动分析等数据关联展示方式，直接将数据的结构，层次和关联展示通过配置实现。

1.6 视图管理

- 视图自定义

支持根据分析需求构建视图，能够实现视图的统一管理，包括名称、图表类型、创建者更新时间等。支持新建目录、新建视图、复制视图、批量移动、编辑、删除重命名等操作。支持构建交叉表、明细表、分组表、以及饼图、柱图、条形图、双轴图、指标卡、矩形树图、词云图等 20 类以上可视化分析。

- 视图操作

支持视图复制和编辑功能，通过拖拽方式配置视图数据。能够对数据排序、显示格式配置，同时支持如下计算模式：

（1）支持对数据进行同环比、百分比、累计值的计算，如去年同比、上月同比、上周同比、环比等。

（2）支持对字段进行聚合运算，包括求和、最大值、最小值、平均值、计数、计数（去重）等。

（3）支持在编辑视图维度或度量的计算字段，支持函数表达式进行计算字段的公式编写。支持指标设置参考线，包括最大值、最小值、平均值、指定值等。

1.7 业务协同

定制开发业务协同系统，实现完整的数据交互体系，通过业务数据和指令的跨平台工作流转，可以更好地整合和利用监管资源解决跨部门、跨行业的监管难题，从而提升监管水平，更有效地监督和管理网络空间安全治理工作。

- 指令接收

上级指令接收实现省（区、市）机关、重要央企、网络安全研究机构、大型互联网企业、网络安全骨干企业等单位的接收上级平台指令信息，实现同上级平台进行指令信息交互能力。

- 漏洞协同管理

漏洞协同管理汇聚下级单位或其他平台报送的漏洞信息，从而整体提升网络安全协调能力和漏洞响应能力，包括通用型漏洞和事件性漏洞的管理。

- 钓鱼情报接收

钓鱼情报接收支持及时、高效的管理钓鱼情报信息，向上级平台报送钓鱼情报信息，从而满足数据报送的需求，降低潜在危害。钓鱼情报接收，主要包括钓鱼情报名称、样本编号、行为类型、运行环境、发现时间、报送时间、数据来源等内容进行列表管理，并支持对钓鱼情报信息进行新增、编辑、查询、删除等操作。

- 协同监控

协同监控实现对于数据报送等协同任务情况的监控，包括任务名称、任务类型、任务状态、开始时间、发送方、接收方、接口调用时长等。

- 数据报送

数据报送依据国家统一要求和数据报送标准和接口，实现向上级平台手动报送数据能力，包括网络资产信息、网络安全事件信息、恶意代码信息和漏洞信息等。

1.8 工作指挥

定制开发工作指挥系统，实现平台整体协同指挥的能力，构建运营中心协同其他部门、各政企单位共同健全完善网络安全协作机制，实现网络空间安全治理工作的可视、可管、可控。在日常工作中，通过实时威胁监测、风险预警、安全分析等机制，解决常态化工作问题，形成针对网络安全威胁、异常行为的监测能力体系，及时发现重点目标网络安全事件和威胁来源，形成统一的安全管理体系，加强网络安全整体防御能力，减少重大网络安全事件发生概率，减少或避免重大网络安全事件所造成的经济损失，为网络安全监管工作提供有力支撑。同时，通过重要活动保障、应急处置、可编排可执行的预案能力，高效调度各方面安全力量和资源形成合力，齐抓共管，将重大网络安全威胁化解于苗头阶段。通过及时监测、处置网络安全重大风险隐患和威胁，针对网络安全情报、安全预警等信息，支撑研判、决策、管理、协调、整合相关资源进行快速响应。最大程度降低、消除安全事件引起的负面影响，保障网络安全和业务系统的顺利的运行。

工作指挥系统基于资源库、主题库和业务库，实现重要活动保障、应急处置、通报预警等一系列协同指挥能力。

- 事件管理

网络安全事件管理功能旨在为企业和组织提供一套全面、高效的网络安全事件管理解决方案。该功能通过实时监控、预警分析、事件响应及事后总结等流程，实现对网络安全事件的快速发现、准确评估、有效处置及持续改进，从而保障网络空间信息系统的安全稳定运行。

- 事件通知

事件通知作为一种业务指令，统一由基础的指令协同应用支持底层的流程运转，支持通过图形化方式呈现指令的整体流程，使用不同状态进行标识事件通报流程中的执行完的环节、正在执行中的环节和未执行的环节。有效的对未进行进行签收、执行反馈等处置节点操作的执行人进行预警和催办。

- 工单管理

工单管理主流程为提交通报、通报审核、通报执行方进行签收，选择是否进行转发、通报处置方进行处置后进入初核及复核，核实通过后通报进行归档。启动事件通报的指令事件状态会有待处置变为处置中，支持完成归档后事件状态从处置中变为已处置。

- 统计报表

系统通过配置功能和图形化的操作界面，帮助用户轻松制定专业水准的数据报告，通过所见即所得式操作引导用户像搭建乐高积木一样来快速组装不同需求场景下的数据报告。

支持以表格、饼图、柱状图、趋势图等方式进行数据可视化展示，支持对视图的统计维度、度量、过滤条件、下钻逻辑等进行配置。

针对仪表板进行管理，支持新建仪表板、授权、导出、导入、删除、查看、编辑、引用关系、下线等操作。支持对视图的新建、复用，支持对视图的自定义大小和布局。

- 组织与权限管理

建立平台的账号体系和权限体系，支持对用户账号和组织机构的统一管理，实现用户角色的具体功能权限和数据权限的配置。同时针对用户登录的认证方式、密码策略和第三方组件的权限集成进行设置和管理。

- 风险预警

风险预警将安全监测中监测分析产生的网站漏洞、风险和事件及手工导入的外部获取的安全事件等数据，通过事件通报、风险通报和风险预警等方式，及时通报涉事的单位，协调联动涉事单位进行快速处置，确保问题得到及时整改、反馈、核实、归档，从而实现完整业务流程的闭环，并向其他单位或者公众网络发布预警。

- 应急指挥

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，结合事前应急演练，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，对各类资源的统筹调度、情报共享、协同联动，对不同类型的安全事件定义个性化监控指标和视图，对事态发展进行实时监控，提高在重大网络安全事件期间的应急响应能力。

- 预案编排

预案编排具体包括预案管理和预案试运行。支持对原子手段的编排形成预案，解决当前业务工作由于流程不同，需要多个业务功能应对，并且在业务变更或新的场景新增时，需要定制或者新增业务功能时模式固化、缺乏灵活性的问题。如日常事件通报、重要活动保障等

业务，都离不开流程管理的支撑，都要用到流程管理中的预案或方案资源。因此流程管理是重要的业务基础支撑。

1.9 安全管理

- 拓扑管理

系统支持对拓扑的统一管理，支持针对不同的安全设备、服务设备、网络设备、终端设备和其他构建拓扑图，能够通过拖拽的方式可视化的进行拓扑图的绘制，在绘制拓扑时可以关联资产。

- 分级管理

支持组织架构进行分级管理，能够在组织架构树中选中需要查看组织，能够查看子分支信息和分支成员信息。支持子分支和分支成员的创建、删除和移动等功能。

- 通报预警

系统预置一套通报流程和一套预警流程。流程分为发送工作流和接收工作流。通报和预警按照系统预置的工作流进行流转。通报预警模板内容支持富文本编辑。支持设置字体大小、加粗、下划线、斜体、字体颜色、项目符号、编号、对齐方式。

- 设备监控

支持对服务器主机(windows、linux、unix)、网络设备（交换机、路由器）、安全设备(防火墙、入侵检测、入侵防御、运维审计、上网行为审计、漏洞扫描、防毒墙、VPN、网闸、等)、数据库（Mysql、Oracle、SQL Server）、中间件（Tomcat、WebLogic）通用服务端口等对象的运行状态进行监控。

2. 城市治理数智化安全能力系统

序号	一级功能模块清单	二级功能模块清单	备注
1	数据资产发现子系统	数据资产识别	
		敏感数据资产	
		存储资产管理	
		应用资产管理	
		账号资产管理	
		数据载体管理	
		数据资产管理	
2	数据分类分级子系统	分类分级模板	
		数据分类分级	
		分类分级版本管理	
		数据资产安全态势	
3	数据流动监测子系统	流动监测视角	
		流动监测过程	
		流动监测内容	
		流动监测图谱	
4	数据安全分析子系统	告警分析	
		数据安全分析规则管理	

		报表管理	
		报告管理	
5	安全响应处置子系统	数据安全事件管理	
		数据安全事件处置	
		数据安全风险管理	
6	数据安全大屏子系统	数据流动态势	
		数据安全态势	
		数据分布态势	
7	数据外发管理子系统	日志外发	
		数据清除	
8	通用管理子系统	用户管理	
		操作日志	
		用户登录	
		系统安全	
		策略配置	

2.1 数据资产发现子系统

以数据资源检测能力，识别重要业务和关键场景为基础，定制开发实现对关键场景数据安全风险的评估，采集和识别数据资产、信息、事件等要素，对现有数据资产进行分类分级，对现有安全管理措施进行梳理，对业务及数据流程进行流向整理，开展数据安全制度建设。

- 数据资产识别
- 敏感数据资产数据

实施数据安全建设，在深入到具体的数据内容之前，首先应理解目标业务应用，梳理业务流程和敏感数据资产，识别重要业务集。围绕重要数据资产集合，发现关键的数据访问业务场景，识别数据存在哪，谁在使用，如何使用，绘制业务流等。

- 存储资产管理

支持主动扫描发现网络中的数据库等存储资产，手动添加、批量导入存储资产。支持从接入日志中动态发现存储资产。支持查看存储资产列表，并可查看每条存储资产的名称、IP地址、数据标签、数据类别、数据级别、敏感数据访问量、去重访问量、告警信息、风险信息且支持对列表栏字段进行排序。

- 应用资产管理

支持从接入日志中，动态发现应用资产及 API 资产；支持手动添加、批量导入应用资产。支持查看应用资产列表，并可查看每条应用资产的业务应用、Host、API 数、IP、账号数、应用标签、发现时间、数据标签、数据类别、数据级别、敏感数据访问量、去重访问量、告警信息、风险信息且支持对列表栏字段进行排序。

- 账号资产管理

支持从接入日志中，动态发现账号资产。支持查看账号资产列表，并可查看每条账号资产的账号名称、类型（应用或数据库）、业务应用/数据库资产名称、应用 Host/数据库地址、账号数、应用标签、发现时间、数据标签、数据类别、数据级别、敏感数据访问量、去重访问量、告警信息、风险信息。

- 数据载体管理

支持对非结构化数据载体进行识别，提取其中的元数据。

- 数据资产管理

针对数据库资产以及数据库账户、权限情况进行梳理清查，同时针对重要数据库进行敏感数据分布梳理、敏感数据访问操作汇总，通过对数据资产的摸底，形成数据资产清单，全局掌握数据资产情况。

业务数据流梳理：面向线上线下的业务应用，针对重要的业务数据梳理相关业务数据流向，各业务组件之间的逻辑关系，掌握数据的传播路径和访问关系全景，为后续的风险分析奠定基础。

2.2 数据分类分级子系统

- 分类分级模板

系统内置数据分类分级模板，模板可按照项目要求进行修改。系统内置数据分类分级模型，内置安全分级要素，支持弹性定级标准，支持数据标签自定义。

- 数据分类分级

结合杨浦区政务数据分级标准，定制开发基于分类分级模板，并以此模板开发数据资产安全分级引擎。针对数据资产进行分类分级的标准制定和级别打标，为后续的分级策略制定提供依据。

- 分类分级版本管理

支持数据资产安全分类分级结果的发布，定义生效周期，支持逐级钻取明细信息。支持安全分级模板、安全分级结果的版本管理，对历次审批发布的版本进行快照保存。多个版本间变迁对比及版本查阅，支持对不同版本中各级数据资产的数量分布及与资产总量情况进行统计展示。

- 数据资产安全态势

从全局出发，实施体系化的数据安全能力评估。根据实际信息化场景，从管理、技术、运营多维度开展数据安全合规性评估、数据全生命周期成熟度评估、业务场景风险评估，发现组织数据安全差距和风险，为数据安全保护和检测能力建设提供参考依据。

2.3 数据流动监测子系统

- 流动监测视角

对杨浦区存储在不同载体上的政务数据情况进行综合安全监测，实现数据分布风险监测能力，及时检测数据的驻留风险。如数据库存储了超过本身允许存储的最高等级重要数据、重要数据缺失、同一个数据源存储了大量的重要数据、同一个数据源包含多种重要数据、重要数据没有做对应的安全防护策略等。防止数据分布风险容易被利用，进而产生更大的数据安全事件。数据分布风险监测对产生异常的数据源进行提示和告警，帮助用户快速发现数据分布的风险。

- 流动监测过程

在不改造现有网络架构和业务系统的情况下，通过对网络流量的还原分析，梳理敏感数据相关应用、接口账号，记敏感数据的流动状况。通过数据流动监测，动态掌控数据安全状态，构建一幅连接“数据资产、业务、主体”的数据流动业务视图。使管理者能够从全局视角掌握应用数据的访问和使用情况。

- 流动监测内容

（1）数据库监测

通过对数据库网络流量的采集，基于数据库协议解析与还原技术实现对数据库所有访问行为的监控和审计、对其中的危险操作进行多种方式的告警、对数据库访问行为进行多维度的统计并进行图形化展现。

（2）API 漏洞攻击检测

针对事件型漏洞：应依据已知的 API 事件型漏洞的原理和攻击特征检测网络中利用已知

API 事件型漏洞的攻击行为。并支持攻击结果的研判,结果包括失败、尝试、成功和失陷。
针对通用型漏洞：应依据典型的漏洞原理及攻击特征检测网络中的漏洞攻击行为，包括但不限于命令执行、SQL 注入、跨站攻击(XSS)等。并支持攻击结果的研判,结果包括失败、尝试、成功和失陷。

针对授权类漏洞:应依据漏洞的产生原理及其特征检测网络中的授权类漏洞攻击行为，包括但不限于弱口令,后门账户等。并支持攻击结果的研判,结果包括失败、尝试和成功。
针对配置异常问题:应依据配置异常所产生的数据特征检测 API 配置异常的接口,包括但不限于配置异常所导致的敏感信息泄露、接口滥用等。该类型问题出现告警时,结果为成功。

（3）API 逻辑异常攻击检测

针对流程绕过行为：通过访问日志训练用户访问行为基线,并检测用户绕过流程的行为,包括但不限于登录流程绕过,验证码流程绕过等。并支持攻击结果的研判,结果包括失败、尝试和成功。

针对未授权访问行为:基于凭证识别、用户访问行为基线技术,检测网络中已知或未知的未授权访问行为。并支持攻击结果的研判,结果包括失败、尝试和成功。

（4）API 逻辑异常行为检测

根据单个用户及用户群体日常访问物理地点、日常访问时间、IP 范围建立基线的能力，并具备在此基线的基础上发现特定用户访问地址变化或者访问群体出现访问地点离群值的情况，同时产生相应的异常告警。并具备对于同一会话期间访问物理地址发生跳变的异常行为的检测能力，并产生相应的异常告警。
对于撞库、密码暴破、用户名暴破、验证码暴破、跨因子认证、批量注册等登录认证/注册功能异常访问行为的检测能力，同时产生相应的异常告警。针对于特定接口的访问速率建立基线的能力，并具备在此基线的基础上发现高频率异常访问行为的能力，并产生相应告警。

- 流动监测图谱

建设数据安全风险综合分析能力，基于数据活动日志和风险情报，结合大数据分析、机器学习等先进技术，加强数据安全风险分析、预测、评估。风险识别应从身份账号、访问行为、资产类型、活动环境等多个视角关联分析，能够智能化发现隐蔽性高的违规行为和未知威胁。当发现可能导致较大危害事件的风险时及时发布预警信息，提出防范应对措施，指导、监督数据处理者做好数据安全保护工作。建立基于场景的风险统计和风险分析能力，基于组织单位数据安全不同场景，建立数据安全风险分析规则和基线模型，根据不同的场景进行风险总体监控、事件风险分析和用户风险分析，对于重点可疑用户，建立用户的风险画像能力。

2.4 数据安全分析子系统

定制开发数据风险分析组件，内置多种常见异常类型的分析模型，便于快速制定异常分析规则。系统支持针对日志中的字符串、数字、IP、时间等字段和频率统计结果的丰富处理规则，提供可自定义的异常事件分析策略配置功能。系统支持基线分析模型，即通过观察一段时间内用户或用户所在群组的行为进行统计分析，找出用户或群组的行为固有基线，当发现用户行为与个人基线或群组基线发生较大偏离时，即判断为一次可疑的异常事件。系统支持多种机器学习算法建立高级分析模型。

系统基于场景的风险统计和风险分析，场景代表某种业务风险的集合，由具有同一属性的风险分类及其对应的权重构成，如账号风险、应用访问风险、数据库访问风险、用户异常行为风险、DLP 违规分析等。管理员可以根据不同的场景进行风险分析、事件分析。

- 告警分析

支持数据安全告警的统一、集中展示，实时获取、展示数据安全告警总体情况。 支持告警归并，避免告警数据过多，运营人员精力过度分散。告警详情，包括告警描述、研判处置、关联敏感数据信息、关联身份信息、关联应用信息、关联数据库信息、关联文件信息、数据类别、数据级别。在监控过程中，若出现与已知安全的白名单元素相关的网络流量或事件，系统将自动跳过进一步的分析和处理，从而避免误报的产生。

- 数据安全分析规则管理

支持通过对多源日志关联分析、行为链分析、特征建模及历史数据分析建立基线模型、数据时间分布异常、内容分布异常等发现数据安全事件。可灵活地将关心的多个分析规则放

到同一个场景中组合显示。

- 报表管理

支持快速报表生成，报表生成配置要素支持灵活调整。可自定义报表内容，支持灵活编辑和布局调整以形成整体报表，系统预置 5 种以上报表模板。

- 报告管理

系统提供数据安全评估报告模板管理功能，预置至少 5 种不同内容框架的报告模板，支持自定义数据安全评估报告的内容框架、样式格式，并建立评估报告的分类体系。可自定义整改建议模板，包含整改建议和安全事件的关系、整改建议的展现样式等内容。系统提供数据安全分析报告管理及模版管理功能，支持自定义数据安全分析报告的内容框架，支持导出 POC 报告，包含资产发现、数据流动概览及详情、安全分析等内容。

2.5 安全响应处置子系统

- 数据安全事件管理

面向安全事件管理构建可视化数据安全事件溯源能力，提供主体溯源和线索溯源等溯源场景。在发生数据泄漏、数据滥用或其他异常事件时，安全运营人员可以对搜集到的所有线索同时进行交互式的深入分析溯源，完成还原数据访问链路，定位事件或风险源头。首先，基于多种类型的日志，支持多种条件（用户、应用、接口、数据等）的统计查询功能，便于管理者从海量日志中精准查询到事件相关日志。其次，系统基于大数据架构，支持使用线索关键字进行快速检索，支持深入挖掘日志，用于在安全事件发生后，迅速定位溯源。最后，系统支持对查询检索的结果进行统计分析，并支持用户进行统计模板定义，提升分析溯源效率。

- 数据安全事件处置

定制开发数据安全的统一审计与告警处置能力平台，对数据安全日志进行汇聚，接入多源日志，实现数据安全的场景化审计能力的联防联控。建立全网动态监测系统，通过审计设备合理采集重要数据处理活动日志，监测数据产生采集、传输、存储、分析使用、共享发布、销毁的各个活动阶段，提供可视化的检索查询和统计分析平台，为审查、取证、风险评测提供必要技术能力。建立集中风险与告处置平台，实现告警的集中研判、分析、处置，为数据安全的运营工作提供依赖。

- 数据安全风险管理

基于大数据技术完成海量数据的存储、处理、分析和检索，综合多源日志进行关联分析，全方位感知数据流动过程中面临的风险。基于多种风险异常分析能力，结合基线分析、行为链分析、频率分析等分析策略，发现隐蔽的数据安全风险。接入多场景监测日志，进行场景化的数据安全风险分析，如账号风险、数据访问风险、API 风险等。并基于自身场景，设置场景关联分析规则，发现关注的数据安全风险。同时对数据风险事件和用户异常行为事件告警功能，一旦发生风险事件，将告警发送给指定人员，便于进行后续的快速处置。基于数据安全风险的运营情况、数据安全管理落实情况、数据安全审计检测覆盖情况，提取关键指标，并结合制度要求，进行数据安全水平的评估，生成评估分数和评估报表。

2.5 数据安全大屏子系统

基于资产管理中心提供的数据资产目录，通过对指定时间段内的数据资产分布、敏感数据量、敏感数据类型等指标进行统计分析与趋势预测，自动生成敏感数据分布态势图；基于策略协同中心提供的安全业务视图和动态监测中心提供的数据业务视图，通过对安全策略变更和数据库、应用、API 等涉敏对象的敏感数据量、敏感数据类型等指标进行统计分析与趋势预测，自动生成敏感数据流动态势图；基于风险管理中心提供的数据，对分布在不同位置、不同时间、不同类别、不同级别的数据资产的安全告警、事件处置等指标进行统计分析与趋势预测，自动生成数据安全风险态势图。三大安全态势围绕数据从分布、流动、风险三个维度为运营人员构建了清晰的宏观视图。

➢ 数据流动态势

通过图形化的方式展示企业内敏感数据的流动情况，包括敏感数据的来源、去向、趋势等；可直观展示敏感数据流出趋势、敏感数据流出 TOP5、敏感数据访问量 TOP5、涉敏资产统计及敏感数据流动实时监测；帮助企业更好地了解敏感数据的流动趋势和热点情况，从而采取相应的安全措施，保护企业的敏感数据安全。

➢ 数据安全态势

通过图形化的方式展示企业中的风险和事件，以及他们的分布情况。包括最新风险、最新事件、事件类型分布、风险类型分布、危险趋势、资产风险等。通过图形化展示方式，帮助企业更好地了解风险和事件的分布情况，从而采取相应的安全措施，降低企业的风险。

➢ 数据分布态势

通过图形化的方式展示企业内的数据分布情况，包含敏感数据的数据源和敏感数据的维度展示数据源的分布情况、敏感数据的类型、级别、新发现的包含敏感数据的库表等

3. 城市网络空间公共服务平台

序号	一级功能模块清单	二级功能模块清单	备注
1	基础功能	检索方式	
		网站列表页	
		资产详情页	
		企业详情页	
		证书详情页	
		域名详情页	
		导出方式	
		个人中心	
		帮助中心	
		下载中心	
		更新日志	
2	监管功能	测绘数据概览页	
		通用漏洞专题	
		icp 备案专题	
		Database 专题	
		OA 专题	
		Web servers 专题	
		重大漏洞预警专题	
		高危协议专题	
3	网站监测	监测类型	
		DNS 运营分析	
		域名监控	
4	报告中心	周期性报告	

		周期报告任务管理	
		自定义报告	
5	系统配置	监测配置	
		运营配置	

3.1 基础功能

- 检索方式

平台提供了 3 种查询方式，分别是：语法查询、icon 查询、批量查询。该功能解决了用户在渗透前期搜集资产，或 HW 前期梳理暴露面情况的需求。

- 网站列表页

提供资产类型、资产总数、IP 总数、年份、国家/地区、端口、组件、icon、域名的聚合项进行聚合统计，资产列表包括：IP:PORT:DOMAIN、server、title、icon、icp 备案名称、所属地区、发现时间等信息。支持通过发现时间、资产类型、状态码、资产标签的筛选条件，和 IP 标签过滤器等筛选项

- 资产详情页

提供 IP 的基础信息，例如开放端口数、ASN、AS_ORG、ISP 等。通过 IP:PORT:DOMAIN，展示 banner、html、app、cert、vul、tls-jarm 等信息

- 企业详情页

企业详情页从企业的视角出发，展示企业基本信息、企业资产概况、备案概况、域名概况、网站概况、资产标签、IP 概况、证书概况、IP 地理位置等信息。

- 证书详情页

证书详情页从证书的视角出发，展示当前选中资产、证书链、证书基础信息（包括证书信息、使用者信息、颁发者信息）、使用者可选名称、域名解析 IP 等信息。

- 域名详情页

域名详情页从域名视角出发，展示当前选中域名 whois 相关信息、ICP 备案信息、域名 DNS 解析记录（包括 A 记录、CNAME、MX）。

- 导出方式

提供导出功能，支持运营、安服人员在 HW/攻防期间，为企业提供资产清单的需求，格式支持 csv。资产清单内容包括但不限于：url、IP、端口、网站标题、域名、协议、状态码、应用组件、操作系统、备案单位、备案号、国家、省市区等。

- 个人中心

展示账号的基础信息，账号收藏的语法，例如语法名称、语法内容、创建时间、修改时间等。

- 帮助中心

产品介绍、新手入门、账号问题、数据问题、API 说明文档、服务条款等

- 下载中心

展示下载文件名称、下载文件所用的语法、文件生成状态、文件包含的资产条数、剩余导出时间、文件剩余有效期、创建时间等

- 更新日志

展示版本迭代的时间、内容、版本号

3.2 监管功能

➢ 测绘数据概览页

区域测绘是专门针对区域的数据在监管场景下预制的进行多维度的专题分析，包括但不限于区域资产数量、漏洞暴露面、icp 备案率统计、应用组件专题等维度。区域测绘专题以杨浦区为单位进行授权，购买区域测绘专题的客户，可对辖区的数据进行浏览以及全量导出。

➢ 通用漏洞专题

漏洞专题页汇总统计了全国存在风险的资产数量，以及受严重与高危漏洞影响的资产分布及地区排名。同时根据地理位置查看区域内热门漏洞 Top20，支持检索单条漏洞所关联的资产分布情况及修复状态。

➢ ICP 备案专题

ICP 备案专题页汇总统计了全国网络资产的备案情况，对区域备案情况进行排序、未备案率进行统计。

➢ Database 专题

数据库专题整合了市面上广泛使用的数据库品牌在互联网的暴露情况，帮助用户快速了解常见数据库的品牌分布、区域分布、历史数据趋势信息。

Database 专题页汇总统计单一数据库类型在全国互联网侧暴露的情况，并对各省、市、区地区的暴露情况进行排名，同时支持查看应用分布情况。帮助监管单位对辖区内互联网应用暴露面情况有宏观的了解。

➢ OA 专题

OA 专题整合了市面上广泛使用的 OA 品牌在互联网的暴露情况，帮助用户快速了解常见数据库的品牌分布、区域分布、历史数据趋势信息。

OA 专题页汇总统计单一 OA 品牌类型在全国互联网侧暴露的情况，并对各省、市、区地区的暴露情况进行排名，同时支持查看应用分布情况。帮助监管单位对辖区内互联网应用暴露面情况有宏观的了解。

➢ Web Servers 专题

Web Servers 专题整合了市面上广泛使用的 Web Servers 品牌在互联网的暴露情况，帮助用户快速了解常见数据库的品牌分布、区域分布、历史数据趋势信息。

Web Servers 专题页汇总统计单一 Web Servers 品牌类型在全国互联网侧暴露的情况，并对各省、市、区地区的暴露情况进行排名，同时支持查看应用分布情况。帮助监管单位对辖区内互联网应用暴露面情况有宏观的了解。

➢ 重大漏洞预警专题

重大漏洞预警专题，主要应对互联网漏洞刚披露时快速对于辖区资产影响面的预警分析。利用全球鹰网络空间测绘系统暴露面资产数据，可实现重大漏洞披露后 2 小时获取全国各省、市、区地域分布情况

➢ 高危协议专题

展示杨浦区关联 IP 数量、非 web 资产数、高危协议端口开放数、高危端口开放率，高危协议端口开放率排名，高危协议端口开放分布情况，根据数量多少分 3-5 级分布。

3.3. 网站监测

➢ 监测类型

（1）可用性监测提供了 http、https、dns 等可用性监控方式，每个资产具有独立的可用性监控配置及灵活的告警策略。

（2）漏洞监测提供深度专业的漏洞扫描，可以扫描以下漏洞：认证和授权类、命令执行类、注入攻击类、服务端攻击类、信息泄漏类、版本漏洞及其他类型漏洞。漏洞扫描为全站扫描，支持附件检测。并且配置 7X24 小时人工运营验证。

网站黑链检测采用专用爬虫进行全站监测，用户可以自定义黑词，配置 7X24 小时人工运营验证。

（3）违规内容检测基于海量样本数据和先进的人工智能技术，精准高效识别违禁内容。可支持自定义敏感词检测，提前防御网站内容风险。支持附件检测，配置 7X24 小时人工运营验证。

（4）内容变更检测采用网页指纹技术，即对每一个爬取的网页进行指纹提取，如果发

现网页指纹与之前备份的不同，则可断定该网页内容发生了变更。支持首页及自定义重点页面监测，可定位至内容变更具体位置。

（5）网站挂马监测采用特征分析技术对网站进行木马检测分析，实现快速、准确的发现和定位网页木马，确保用户在第一时间发现感染的木马并及时消除。对木马威胁进行报警、通知、处置管理

- DNS 运营分析

包含域名解析分析/日志，和告警事件分析/日志两部分内容。域名解析分析页主要展示解析趋势以及部分解析事件概览。告警事件分析主要展示 威胁解析趋势以及威胁分类概览。

- 域名监控

包含域名解析分析/日志，和告警事件分析/日志两部分内容。域名解析分析页主要展示解析趋势以及部分解析事件概览。告警事件分析主要展示 威胁解析趋势以及威胁分类概览。

3.4 报告中心

- 周期性报告

日报/周报/月报/季报的生成及导出，按平台报告模板生成

- 周期报告任务管理

周期性报告任务可以进行新增/删除/编辑操作，任务可以暂停继续

- 自定义报告

自定义生成报告的时间范围（最大范围为最近半年）、告警类型、告警威胁等级、资产对象等，生成报告及导出

3.5 系统配置

- 监测配置

查看各个监测类型默认监测策略，用户可以根据实际业务需要添加自定义监测策略（可配置项参照平台）

- 运营配置

对告警可以配置白名单/自动通知/忽略告警操作

五、项目服务要求

（一）服务要求

提供自项目竣工验收之日起 1 年配套运营服务，自项目竣工验收之日起 1 年配套运营服务，包括：持续平台运行保障，支持 7x24 小时平台连续运行，平台可用性≥99%；平台软件升级、性能监控等日常保障服务等。

（二）社会面网络应用系统监管服务

包含重要信息系统更新服务、安全检查服务预警通报服务，重要信息系统风险发现服务每月对重要信息系统进行安全扫描。本项目监管的网络应用系统主要包括区内互联网侧重要信息基础设施和重要单位、互联网企业 和国有企业、医院、学校等重要网站、平台、业务系统。

（三）一网统管安全监管服务

包含针对一网统管系统的信息安全检查、风险通报及处置服务、一网统管专网网络安全监管服务、一网统管专网设备上线监管服务、一网统管专网设备退出监管服务、一网统管专网数据安全监管服务、一网统管专网应用安全监管服务、一网统管专网系统安全监管服务、一网统管专网密码安全监管服务、一网统管专网机房环境安全监督服务、一网统管专网应急响应监管服务、应急响应和重要任务保障服务、测评协助、应急演练、安全培训服务。服务期间需安排不少于五名信息安全技术服务人员及一名项目经理专职常驻现场，本服务驻场人数总共不少于六人，招标方有权要求投标方安排必要的加班、值班时间。 招标方将对驻场人员进行日常考勤、考核。

（三）政务云安全管理服务

包含杨浦区云上实际应用系统提供基于网络安全等级保护和应用实际需要的安全服务，包括漏洞扫描服务、在线防护 waf 服务、虚拟主机安全防护服务、用户身份认证服务等相关安全服务内容，支撑杨浦区实际云上应用安全，降低网络及应用安全风险，满足电子政务应用系统的安全保障。

（四）响应程度要求

提供 5x8 技术咨询，提供客户在使用产品和产品逻辑方面的问题响应和受理。

故障响应提供 7x24 小时支持服务。提供对产品故障、宕机等情况的电话人工支持服务。

六、项目保障要求

（一）服务能力要求

为了更好的为客户提供支持服务，投标人必须有服务能力和技术服务团队，能快速响应采购方的服务要求，突发情况下可以快速到达客户现场。

（二）项目人员配备要求

投标人具备承担软件开发项目的研发能力，具有一定的技术服务管理体系，能保障系统总体设计方案的先进性、科学性、可落地性。为保证本项目平台功能深化过程中，沟通和协调的便利，中标方必须指定一名项目总协调人。项目平台功能深化及运营服务过程中一旦出现重大问题，项目总协调人应该能及时赶到现场。

中标单位须按照本系统平台功能深化要求，组建由资深项目经理带领、具备丰富经验与较强开发能力的项目团队，在系统调研、分析设计、开发测试及培训实施等各阶段保障团队稳定性，若需变更团队成员须事先征得项目采购单位同意，未经同意不得擅自变更，同时须单独组建实施团队（不含项目经理）并明确设置项目经理，项目实施团队总人数不少于 12 人，且须配备项目经理、技术负责人、安全负责人、培训讲师等关键岗位人员；项目进入运维阶段后，须组织专业运营团队提供运营保障服务，该团队人数不得少于 8 人，驻场人数不得少于 5 人。

七、项目文档要求

（一）文档内容要求

系统开发应严格遵照国家软件项目规范进行，须提供产品用户手册和测试报告等过程文档。

未经采购人认可的情况下，所有的技术文件必须用中文书写或有完整的中文注释。

（二）文档管理要求

本项目所有文档最终必须向采购人提供纸质和电子文档各一套。中标人必须设置专人在项目平台功能深化及运营服务期间对文档进行检查和管理，项目最终验收后全部移交采购人。

（三）项目管理要求

投标人在合同签定后应向采购人补充提交投标文件的电子版。

投标人应按照项目定制化开发和成品软件实施进度依次向采购人提交项目的技术文件和管理文件。

投标文件中应包括投标人用于本项目的项目管理机制、团队组成、主要管理和技术负责人员的资质与经验说明。在项目实施过程中，如果投标人要变更主要管理和技术负责人员，须给出充分理由并取得采购人的同意。

投标人应按采购人要求派主要项目管理人员和有关技术人员定期参加该包件的项目管理例会；投标人给出的项目管理基本制度和实施总计划在得到采购人认同后，应该被所有包件投标人遵守。投标人有责任按采购人要求派合适人员参加所有包件的项目管理例会，并按采购人的要求协调有关各方。

投标人在定制化软件需求的功能深化中可以针对部分目标的实现或全部主要目标的实现提出部分试运行申请或系统试运行申请。提出试运行申请时投标人同时提交试运行方案。用户批准系统试运行之日，该包件即进入免费维护期，用户明确要求的特别维护期除外。

投标人应该针给出对应的开发或集成工作的项目管理方案。

投标人应该给出本期项目平台功能的深化内容一年免费维护期的维护责任和维护办法。

投标人应对采用非自行开发、未包含在投标报价内而需要采购人另外购买的商品软件给予说明。特别要说明采用该软件的理由和该软件使用环境要求。如果有条件，还应说明其市场参考价格与服务内容。

与某包件或整个项目有关的性能维护、故障排除、设备保修等事宜发生时，有关的包件投标人应该无推委地响应用户现场服务要求，并承诺与其他有关方合作，尽快解决用户面临的有关软件、硬件、网络和系统问题。

投标人完成规定工作所需要的通用性软、硬件工具，原则上由投标人自行准备。

投标人应详细说明贵公司的售后服务体系和运作方式。

八、培训要求

中标单位必须向采购方提供培训服务，培训方式应包括管理培训、理论培训和现场培训。中标单位须针对不同的培训对象，包括对区领导、管理者、各级最终用户和系统管理员等相关技术人员，在投标文件中提出全面、详细的培训计划，包括且不限于培训内容、培训时间、

地点、授课老师等，并提供课程体系、培训方法和考核方法等，培训讲师费用由中标人负责。

中标单位派出的培训教员应具备丰富的相同课程教学经验，所有的培训教员必须中文授课，中标单位具备为所有被培训人员提供培训用文字资料和讲义等相关用品。

中标单位按招标方约定合理地安排培训时间。

中标单位需在投标书中说明培训的计划、内容和深度，原则上要求招标方的相关人员要完全学会系统的知识技能。

九、安全保密要求

本项目要求投标人在实施方案中针对本项目平台功能的深化内容制定保密措施和安全防护措施并在项目实施过程中严格执行，以保证项目的成功实施。投标人必须提供对本项目的保密承诺及人员保密承诺书和人员稳定承诺书（如有变更，需经过采购人确认同意才能更换）。投标单位需提供数据安全的防护方案。

十、项目验收要求

项目完成应用软件定制开发工作后，进行试运行、培训和配合第三方测评单位完成测评后并获取通过后的测试报告，可提出验收申请，由采购人组织验收评审。

十一、项目工期要求

根据项目分期实施的建议，制定详细的项目实施工作计划，以满足项目工期的要求。服务周期：项目整体建设周期：6 个月，试运行期为 1 个月（不包含在项目建设周期内），具体实施验收进度将根据项目落地实际情况作动态调整。本项目要求中标单位提供一年免费运营，从通过整体验收之日起计算，包括所有系统及服务。

十二、项目权益

本项目涉及成品软件部分，采用永久授权许可模式，采购人应合法免费享有软件的完整使用权。本项目涉及定制化开发软件部分，采购人应享有软件著作权等。

项目工程进度经采购人确认和同意后，投标人不得随意变更其进度安排，如需变更，应经采购人确认和同意。

十三、售后服务要求

（1）投标单位必须明确提出维护期内软件的升级、维修、维护内容及服务方式、范围，并在投标文件中提供将来需要升级时的升级方案。必须具备专业的售后服务团队，能保证提供不间断的售后服务。遇有重大活动需要确保系统正常运作的，中标单位在接到通知后，应当在活动期间提供人员现场保障。

（2）项目验收时中标单位应递交完整的文档。

（3）产品优化与咨询服务。中标单位必须明确可以根据应用的使用情况和用户反馈，提供平台技术优化和使用咨询服务。

（4）应急故障维护。对平台运行出现故障或意外情况导致系统不能正常运行，中标方需提供进行 7x24 小时的问题的响应和处理服务。同时，针对重大影响的应急问题，须提供

2 小时以内的响应时间，一般影响的问题，提供 12 小时内的响应时间。

（5）提供平台使用者培训服务，投标单位应明确可以提供上门培训服务。

（6）数据安全服务。中标单位应保证数据安全，提供定时备份数据、恢复数据服务。

（7）文档服务。中标单位需提供平台完善的文档记录服务。

（8）应用软件服务

缺陷管理：针对平台功能中存在的 bug、缺陷，提供持续提供修正与消缺服务，并提供必要的补丁版本的升级服务。

运行支持：对平台运行过程中管理员的问题提供解答和问题解决跟踪，对于关键业务点的上线推广与运行提供保障。

十四、应急预案要求

（1）覆盖核心应急场景：需明确应对系统突发故障、数据安全事件、网络异常等关键场景，确保覆盖软件运行中可能导致业务停滞的主要风险。

（2）明确响应处置流程：设定故障分级标准，对应明确响应时效；明确基本处置步骤，包括故障上报路径、临时替代方案、恢复验证标准。

（3）保障基础支撑能力：确保 7×24 小时响应，具备必要技术储备，包括关键数据定时备份机制、基础应急工具。

十五、项目绩效考核要求

依据项目合同绩效考核方案相关要求和内容（绩效考核方案作为合同附件）对项目绩效进行最终考核，由财务监理方根据评分结果，出具最终的项目结算审核报告。审核报告出具后在 30 天内支付相应尾款款项。

最终绩效指标和考核方案以本项目合同附件对应项目绩效考核方案为准。

杨树浦“ABCD”安全运营矩阵质量由采购人委托的工程监理单位按采购人要求进行考核，考核依照《“ABCD”安全运营矩阵平台服务考核暂行办法》，从产出目标、质量目标响等相关指标维度对中标供应商进行考核。考核结果作为项目验收的依据。

十六、付款方式

付款方法：根据合同的有关规定，按照下列方法和比例付款：

1、中标供应商在签订合同完毕后 30 天内，招标方支付中标供应商合同金额的 50%；主体项目建设内容交付后的 30 天内，支付合同金额的 40% 。达成项目指标要求并完成整体项目验收且合格后的 15 天内，由财务监理方根据评估结果，出具最终的项目结算审核报告。审核报告出具后在 30 天内支付相应尾款款项。

2、所有付款支付前，供应商需开具足额对应发票。

附件：《杨树浦“ABCD”安全运营矩阵平台服务考核暂行办法》

说明：1、依据本项目应实现的目标或工作计划，对照已完成的情况，进行评分。

2、等级说明：评分合计 80≤X≤100 为优秀，70≤X≤80 分为良好，60≤X≤70 分为合格，X≤60 分为不合格。

3、产出目标、质量目标可根据实际工作情况以及上级单位考核内容同步进行增加或修改相应指标。

序号	指标类别	指标名称	分值	考核标准	考核办法	得分	扣分依据
1	服务人员管理	人员配备	25	提供 4 人专业安全技术人员 5*8 小时驻场服务，7*24 小时响应。其中项目经理 1 名，项目经理资质符合要求(PMP、CISP)，并保持人员相对稳定，未经甲方允许全年更换人员人次数不超过 2 次。	项目经理资质缺失 1 项，扣 1 分； 人员要求未达标扣 1 分/人次； 无故更换项目经理扣 5 分/次； 驻场人员数量不足 4 人，每次扣 2 分； 15 分钟内未响应，每次扣 2 分		
2				所有人员均需提供真实简历	提供虚假简历扣 5 分/人次		
3				所有人员需安全可靠，不得有黑客、黑产、失信等记录	黑客、黑产、失信等情况扣 5 分/人次		
4		日常管理		遵守甲方日常管理制度	旷工扣 1 分/人次；迟到早退扣 1 分/人次； 现场服务人员违反甲方办公室管理制度，导致影响工作环境的，扣 1 分/次		
5		保密管理		遵守保密协议要求，履行保密责任	违反保密规定 1 次扣 5 分		
6	服务交付管理	服务交付情况	25	根据服务台账提交服务清单要求的服务交付成果物，如网络安全检查、安全分析、专项整治等报告和方案； 每月 10 日前及时提交服务台账，并进行运营总结	服务成果物每缺失 1 项扣 1 分； 成果物内容不达标每次扣 1 分； 未及时提交服务台账或运营总结汇报，每次扣 1 分； 未提交服务台账或运营总结汇报每次扣 2 分		
7				网络安全应急演练服务：制定应急演练方案，开展应急演练培训，并协助预案演练，出具应急演练报告。每年应急演练 1 次	未编制应急演练方案扣 2 分，未完成应急演练培训扣 2 分，未提交应急演练报告扣 2 分，应急预案存在明显不足扣 3 分。未按照方案完成演练扣 5 分		
8				重保服务：制定重保服务方案，并协助完成重保工作，确保重保时期“零事故”	未编制重保方案扣 2 分，未完成重保工作 1 次扣 5 分，确保重保期间不因乙方原因导致网络安全事故，每出现一次扣 5 分		
9				培训服务：实战型攻防技能培训服务不低于 10 人的培训 1 次、安全运营技术培训服务 10 人的培训 1 次、网络安全意识培训 20 人的培训 2 次等	未完成培训扣 2 分/次。每年培训人次每少于 10 人口 2 分		
10		通知情况	5	针对杨浦区数据局负主体安全责任的应用系统存在的网络安全隐患（漏洞）被相关部门提前发现并通报情况	由于运营商原因，因安全问题导致被国家相关部委通报的，每次扣 5 分，被上海市相关部门通报的，每次扣 3 分，被其他部门通报的，每次扣 2 分。加分项不得与该项扣分相抵消。针对先于相关部门发现并采取了整改措施或因特殊原因无法彻底根除的网络安全隐患(漏洞)，被相关部门通报的不扣分。		
11				政务网络及其他接入 1235 的政务	由于运营服务商原因，因安全问题		

				云上的应用系统存在的网络安全隐患（漏洞）被相关部门提前发现并通报，给甲方造成不利影响的	导致被相关部门通报并给甲方造成不利影响的，每次扣 2 分。加分项不得与该项扣分相抵消。针对先于相关部门发现并采取了整改措施或因特殊原因无法彻底根除的网络安全隐患(漏洞)，被相关部门通报的不扣分。		
12	系统损失管理	特别严重的系统损失	30	确保服务周期内不出现因服务交付不当导致的特别严重系统损失，详情请见备注中的“特别严重的系统损失”说明	出现 1 次特别严重系统损失，该考核周期不合格；事件级别由杨浦区数据局根据《国家网络安全事件应急预案》认定		
13		严重的系统损失		确保服务周期内不出现因服务交付不当导致的严重系统损失，详情请见备注中的“严重的系统损失”说明	出现 1 次（含）严重系统损失，该考核周期不合格；事件级别由杨浦区数据局根据《国家网络安全事件应急预案》认定		
14		较大的系统损失		详情请见备注中“较大的系统损失”说明	每出现 1 次较大的系统损失，服务期指标扣 5 分；事件级别由杨浦区数据局根据《国家网络安全事件应急预案》认定		
15		较小的系统损失		详情请见备注中“较小的系统损失”说明	每出现 1 次较小的系统损失，服务期指标扣 2 分；事件级别由杨浦区数据局根据《国家网络安全事件应急预案》认定		
16	满意度评价	服务满意度	15	按照工作配合情况、投诉情况进行评分	由杨浦区数据局根据整体服务满意度情况进行评价		
	总分						
	备注： 特别严重的系统损失： 造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的： 严重的系统损失： 造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大但对于事发组织是可承受的； 较大的系统损失： 造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的： 较小的系统损失： 造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性受到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小						