项目编号：SHXM-13-20231018-1110

宝山区大数据安全运营服务（安全中心）

公开招标文件

采购单位：上海市宝山区大数据中心

集采机构：上海市宝山区政府采购中心

目　　录

第一章　公开招标采购公告

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购货物和服务招标投标管理办法》等规定，现就下列项目进行公开招标采购，欢迎提供本国货物、服务的单位或个人前来投标：

一、项目编号：SHXM-13-20231018-1110

二、公告期限：5 个工作日

三、采购项目内容、数量及预算

包号	包名称	数量	单位	预算金额(元)	简要规格描述或包基本概况介绍	最高限价(元)	备注
1	宝山区大数据安全运营服务（安全中心）	1		5600000.00	宝山区大数据中心网络安全层面提供监测监管、威胁验证、协同处置和持续运营管理的服务支撑工作，	4772000.00	

					具体包括如安全事件感知分析研判、通报预警、安全事件指挥调度与协同处置以及安全应急响应保障等等。		

四、合格投标人的资格要求

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

本项目不接受供应商联合体响应。

五、投标报名：

1、报名时间：2023-10-27 至 2023-11-06 上午 00:00:00~12:00:00；下午 12:00:00~23:59:59（节假日除外）。

2、报名方式：本项目实行网上报名，不接受现场报名。供应商登录上海政府采购网（http://www.zfcg.sh.gov.cn/）进行报名。

3、招标文件售价：0 元，招标文件请至公告附件处下载。

六、投标保证金：

[投标保证金收款账户（金额、开户行、户名、账号等）]

如需缴纳保证金，投标人应于 时前将投标保证金交至上海市宝山区政府采购中心 账户，投标保证金以网银、电汇方式交纳,请将网银电脑打印凭证、电汇底单复印件写上所投项目名称、编号、投标联系人、联系电话，并在开标前在电子招标系统中以 PDF 格式上传。

七、投标截止时间和地点：

1、投标地点：上海市政府采购网http://www.zfcg.sh.gov.cn。

2、投标截止时间：2023-11-17 09:30:00

八、开标时间及地点：

本次招标将于 2023-11-17 09:30:00 时整在**上海政府采购网（http://www.zfcg.sh.gov.cn）**开标，投标人可以派授权代表出席开标会议（授权代表应当是投标人的在职正式职工，并携带身份证及法定代表人授权书有效证明出席）。

开标所需携带其他材料：自行携带无线上网的笔记本电脑、无线网卡、数字证书（CA 证书）。投标人未参加开标会的，视为认同开标结果。

九、联系方式：

上海市宝山区大数据中心

机构管理员

021-56569800

上海市宝山区政府采购中心

侯老师

18121180148

第二章　投标人须知

一、前附表

序号	内　容	要　　求
1	项目名称及数量	详见《公开招标采购公告》二
2	信用记录	根据财库[2016]125号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，**其投标将作无效标处理**。
3	政府采购节能环保产品	财政部、发展改革委、生态环境部、市场监管总局联合发布（财库[2019]9号文），依据品目清单和认证证书实施政府优先采购和强制采购。 投标产品或采购需求中要求提供的产品属于**强制采购节能产品**品目的，投标人须提供该品目产品认证证书，否则其投标将作为无效标处理。 投标产品或采购需求中要求提供的产品属于**优先采购节能产品**或**环境标志产品**品目的，投标人须提供该品目产品认证证书，否则其不享受优先采购政策。
4	小微企业有关政策	1、根据财库〔2020〕46号的相关规定，在评审时对小型和微型企业的投标报价给予10%的扣除，取扣除后的价格作为最终投标报价（此最终投标报价仅作为价格分计算）。属于小型和微型企业的，投标文件中投标人必须提供的《中小企业声明函》。 联合体投标时，联合体各方均为小型、微型企业的，联合体视同为小型、微型企业享受政策;联合体其中一方为小型、微型企业的，联合协议中约定小型、微型企业的协议合同金额占到联合体协议合同总额30%以上的，给予联合体(4-6%)的价格扣除，须同时提供联合体协议约定（包含小型、微型企业的协议合同份额）。 2、根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函（见附件）。 3.根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件（格式自拟）。**（注：未提供以上材料的，均不给予价格扣除）。**

5	答疑与澄清	投标人如对招标文件有异议，应当于公告发布之日起至公告期限满第 7 个工作日内，以书面形式向招标采购单位提出，逾期不予受理。
6	是否允许采购进口产品：	不允许进口产品具体要求详见第六章采购需求各标项的对应内容。
7	是否允许转包与分包	转包：否 分包：否
8	是否接受联合体投标	不允许 接受联合体投标的请提供联合体协议书。
9	是否现场踏勘	不组织现场踏勘 具体要求详见第六章采购需求各标项的对应内容。
10	是否提供演示	不进行演示 系统演示具体要求详见第六章采购需求各标项的对应内容。
11	是否提供样品	不要求提供样品 具体要求详见第六章采购需求各标项的对应内容。
12	最高限价	本项目最高限价为人民币包 1-4772000.00 元元，报价超过的投标将作为无效标处理。
13	中标结果公告	中标供应商确定之日起 2 个工作日内，将在上海市政府采购网(http://www.zfcg.sh.gov.cn/)发布中标公告，公告期限为 1 个工作日。
14	投标保证金	**本项目不收取投标保证金** 交纳：投标保证金应按《招标采购公告》六规定交纳。若一次投多个标项，只需交纳一个标项的投标保证金（按所需保证金最大额的标准交纳为准）。 退还：中标通知书发出之日起5个工作日内，未中标的投标保证金，招标方以电汇或转账等方式退还投标保证金。
15	合同签订时间	中标通知书发出后 30 日内。
16	履约保证金	合同签订时，采购人按《中华人民共和国政府采购法实施条例》有关规定自行收取项目履约保证金。采购人要求中标或者成交供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的10%。
17	付款方式	国库集中支付（采购人自行支付）详见各标项的商务要求表
18	投标文件有效期	90天
19	投标文件的接收	网上投标 投标地点：上海市政府采购网 http://www.zfcg.sh.gov.cn 各供应商在投标（响应）文件加密上传后，应及时查看签收情况，并打印签收回执。未签收的投标（响应）文件视为投标(响应)未完成。

		届时请来现场开标的投标人携带可无线上网并可登录上海市政府采购信息管理平台的笔记本电脑及投标时所使用的CA证书。（集中采购机构可为未带笔记本电脑的投标人免费提供可上网的电脑，但对其稳定性不负责任） 投标截止时间、开标时间、开标地点详见《公开招标采购公告》
20	招标方代理费用	¥0 元
21	解释权	本招标文件的解释权属于上海市宝山区政府采购中心。

二、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《招标公告》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《招标公告》和《投标人须知》前附表中所述的招标人。

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信息管理平台招投标系统正式运行的通知》（沪财采[2014]27号）的规定，本项目招投标相关活动在上海市政府采购信息管理平台（网址：www.zfcg.sh.gov.cn）电子招投标系统进行。

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 “货物”系指供应商按招标文件规定，须向采购人提供的各种形态和种类的物品，包括一切设备、产品、机械、仪器仪表、备品备件、工具、手册等有关技术资料和原材料等。

“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运输、就位、安装、调试、技术协助、校准、培训、技术指导以及其他类似的全部义务。

2.3 “采购人”系指上海市宝山区大数据中心。

2.4 “集中采购机构”系指上海市宝山区政府采购中心。

2.5 “招标人”系指《投标人须知》前附表中所述的组织本次招标的集中采购机构和采购人。

2.6 “投标人”系指按规定获取招标文件，并按照招标文件提交投

标文件的供应商。

2.7 “中标人”系指中标的投标人。

2.8 “甲方”系指采购人。

2.9 “乙方”系指中标并向采购人提供货物和服务的投标人。

2.10 招标文件中凡标有“★”的条款均系实质性要求条款。

2.11 “电子采购平台”系指上海市政府采购信息管理平台的门户网站上海政府采购网（www.zfcg.sh.gov.cn）；由上海市财政局建设和维护。

3. 合格的投标人

3.1 符合《招标公告》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质条件和特定条件。

3.2本次招标不接受联合体。

4. 合格的货物或服务

4. 1投标人对所提供的货物和相应的服务应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

4. 2 投标人提供的货物应当是全新的、未使用过的，货物和相关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。

4. 3投标人应当说明投标货物的来源地（产地），如投标的货物非投标人生产或制造的，则应当按照本次招标采购需求的要求提供其从合法途径获得该货物的相关证明。

5. 投标费用

5.1 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，采购人及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

6.1 本采购项目需要公开的有关信息包括招标公告、招标文件澄清或更正公告、中标结果公示、未中标通知以及延长投标截止时间等与招标活动有关的通知，采购人及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，属于投标人的风险。采购人及集中采购机构对此不承担任何责任。

7. 询问与质疑

7.1 供应商对招标活动事项有疑问的，可以向集中采购机构提出询问。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，采购人及集中采购机构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 供应商认为招标文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以根据中华人民共和国财政部令第94号中相关规定，以书面形式向采购人、集中采购机构一次性针对同一采购程序环节提出质疑。采购人、集中采购机构将拒收未在法定质疑期内发出的质疑函。

7.3 提出质疑的供应商（以下简称质疑供应商）应当是参与所质疑项目采购活动的供应商。对招标文件提出质疑的，应当在获取招标文件或者招标文件公告期限届满之日起7个工作日内提出。对采购过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果以及评标委员会组成人员的质疑，应当在中标公告期限届满之日起七个工作日内提出。

供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（一）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

（三）具体、明确的质疑事项和与质疑事项相关的请求；

（四）事实依据；

（五）必要的法律依据；

（六）提出质疑的日期。

7.4 采购人、集中采购机构应当在收到质疑函后7个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7.5 质疑函的方式：书面形式，质疑函应当使用中文，质疑人提供外文书证或者外国语视听资料的，应当附有中文译本，由翻译机构盖章或者翻译人员签名。

7.6 供应商在全国范围12个月内三次以上投诉查无实据的，由财政部门列入不良行为记录名单。

供应商有下列行为之一的，属于虚假、恶意投诉，由财政部门列入不良行为记录名单，禁止其1至3年内参加政府采购活动：

（一）捏造事实；

（二）提供虚假材料；

（三）以非法手段取得证明材料。证据来源的合法性存在明显疑问，投诉人无法证明其取得方式合法的，视为以非法手段取得证明材料。

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，采购人及集中采购机构将拒绝其投标，并将报告政府采购监管部门查处。

8.3 根据《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库[2016]125号）的有关要求，采购人和集中采购机构将在开标后、评标开始前，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，对被列入“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，以及上述网站查询中其他不符合《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。

8.4(**本项目不适用**)各供应商的信用信息查询记录作为采购文件一并归档。两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

9. 其他

9.1 本《投标人须知》的条款如与《招标公告》、《采购需求》和《评标办法》就同一内容的表述不一致的，以《招标公告》、《采购需求》和《评标方法》中规定的内容为准。本招标文件中出现前后矛盾的，以在招标文件中出现顺序在后的解释为准（有特别说明的除外）。

9.2 本招标文件中的不可抗力是指不能预见、不能避免并不能克服的客观情况。应包括重大自然灾害（如台风、洪水、地震等）、政府行为（如征收、征用）、社会异常事件（如战争、罢工、骚乱）。

9.3本招标文件未尽之处，或者与相关法律、法规、规范性文件要求不一致的，均按相关法律、法规、规范性文件要求执行。

三、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）招标公告（第一章）；

（2）投标人须知及前附表（第二章）；

（4）评标方法及评分标准（第三章）；

（5）政府采购合同主要条款指引（第四章）；

（6）投标文件有关格式（第五章）；

（7）采购需求（第六章）；

（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；投标人自行对招标文件的理解及因此作出的行为负完全责任。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投标，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，并承担由此引起的一切后果和法律责任。

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相关活动，对未按时参加相关活动而造成的后果负责。

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天前，按《招标公告》中的地址以书面形式（必须加盖投标人单位公章）通知集中采购机构。超过时限的，由采购人及集中采购机构需要决定是否对招标文件进行澄清、答复。

11.2对在投标截止期15天以前收到的澄清要求，采购人及集中采购机构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，采购人及采购代理机构需要对招标文件进行补充或修改的，采购人及集中采购机构将会通过“上海政府采购网”以澄清或更正公告形式发布，并通过电子采购平台发送至已下载招标文件的供应商工作区，或者通过电子邮件发送给已下载招标文件的供应商。如果澄清或更正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更正公告中的规定为准。

11.3澄清或更正公告的内容为招标文件的组成部分。当招标文件与澄清或更正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更正公告形式发布，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，采购人及集中采购机构不承担任何责任。

11.5 采购人及集中采购机构召开答疑会的，所有投标人应根据招标文件或者采购人及集中采购机构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，采购人及集中采购机构不承担任何责任。

12. 现场踏勘（本项目不组织）

12.1采购人及集中采购机构组织现场踏勘的，所有投标人应按《投标人须知》前附表规定的时间、地点前往参加现场考察活动。投标人如不参加，其风险由投标人自行承担，采购人及集中采购机构不承担任何责任。采购人及集中采购机构不组织现场考察的，投标人可以自行决定是否现场考察。

12.2 投标人现场踏勘发生的费用由其自理。

12.3采购人及集中采购机构在现场探勘中口头介绍的情况，除采购人及集中采购机构事后形成书面记录、并以澄清或更正公告的形式发布、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，采购人及集中采购机构不对投标人据此作出的判断和决策负责。

四、投标文件

13. 投标的语言及计量单位

13. 1 供应商提交的投标文件以及供应商与采购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。

13. 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）。

14．投标有效期及投标保证金（*本项目不收取投标保证金*）

14．1 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。

14．2 在特殊情况下，在原投标有效期期满之前，采购人可书面延长投标有效期。供应商可拒绝接受延期要求而不会导致投标保证金被没收。同意延长有效期的供应商需要相应延长投标保证金的有效期，但不能修改投标文件。

14．3 中标单位的投标文件作为项目服务合同文本的附件，其有效期至中标单位全部合同义务履行完毕为止。

14.4为了确保招投标工作的顺利进行，应按照前附表要求提交投标保证金，投标保证金作为投标文件的一个组成部分。

本项目投标保证金为人民币0元；应在投标有效期截止日后30天内保持有效；投标人应在网上投标截止时间之前，将投标保证金提交至以下账户。（投标保证金可以是支票、贷记凭证、汇款、银行保函等形式；银行保函必须送至以下单位）

单位名称： 上海市宝山区政府采购中心
账　　号： 03331900040116940
开户银行： 农行上海友谊支行
地　　址： 上海市宝山区友谊支路 238 号

投标保证金的需注意到账时间，到账截止时间应为网上投标截止时间前。

投标人应在提交保证金后，在电子招标投标系统中进行相应环节操作，上传保证金缴纳凭证（PDF格式）（***本项目不收取投标保证金，投标人不需*进行相应环节操作**）。

14.5投标保证金在投标有效期满后30天内保持有效。采购人如按规定延长了投标有效期，则投标保证金的有效期也相应延长。

14.6未中标的供应商的投标保证金将在中标通知书发出后5个工作日无息返还；中标单位的投标保证金在合同签订后5个工作日内无息返还。

14.7如供应商有下列情况之一,将被没收投标保证金:

① 开标后供应商在投标有效期内撤回其投标文件；或

② 作为中标单位未能做到：按本须知规定签订合同。

15. 投标文件构成

15.1供应商应根据网上招标系统的要求填写相关投标信息（表格），根据第五章投标文件有关格式中的规定编制投标文件并上传至网上投标系统并提交，未规定格式的部分由投标人自行设计。

15.2投标文件构成（投标文件应具有但不局限于以下内容）

15.2.1商务响应文件由以下部分组成

（1）投标函；

（2）开标一览表（在电子采购平台填写）；

（3）投标报价明细表等相关报价表格详见第五章《投标文件有关格式》；

（4）资格条件实质性要求响应表；

（5）《法定代表人授权委托书》（含被授权人身份证复印件）；

（6）投标人营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的，仅需提供营业执照）及与本项目相关的资格证书；

（7）没有重大违法记录的声明：

参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明函，截止至解密日成立不足3年的供应商可提供自成立以来无重大违法记录的书面声明；

（8）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、财务状况及税收社会保障资金缴纳情况声明函等（**中标供应商为中小企业、残疾人福利性单位的，其声明函将随中标结果同时公告**）；

（9）第六章《采购需求》规定的其他内容。

15.2.2技术响应文件

（1）投标人对采购项目总体需求的理解、重难点分析及控制措施；

（2）项目服务实施方案（包括但不局限于服务内容、服务响应时间、投标人对拟投入本项目实施人员的管理制度及安全管理培训安排、针对突发事件发生的应急预案。）；

（3）项目服务承诺书（包括但不局限于服务质量标准、惩罚承诺）；

（4）项目团队配置情况，应当包括：

1）项目经理情况表；

2）主要管理人员配备及相关工作经历、职业资格汇总表（需附有效期内的相关服务所需的资质（如有）、专业人员与管理人员职称证书、专业工种持证上岗证书等）；

（5）《投标人近三年以来政府服务项目一览表》：

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、交付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《评分标准》为准；

（6）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。

以上各类响应文件格式详见招标文件第五章《投标文件有关格式》，无格式要求的投标人自拟。

16.上传扫描文件要求

16.1投标人应按照招标文件规定提交彩色扫描文件，并按照规定在电子采购平台网上招投标系统上传其所有资料，文件格式参考第五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）应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。

16.2采购人认为必要时，可以要求投标人提供文件原件进行核对，投标人应按时提供。否则视作投标人放弃中标资格，并且采购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。

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，评标时将按照第三章《评标方法及评分标准》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和电子采购平台电子招投标系统提供的投标文件格式完整地填写《开标一览表》，说明其拟提供货物和相关服务的名称、规格型号、来源地、数量、价格、交付时间、质量保证期等。

18．2 《 开标一览表》是为了便于采购人开标，《开标一览表》内容在开标时将当众公布。

18.3　投标人未按照招标文件和电子采购平台电子招投标系统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　投标报价是履行合同的最终价格，除《采购需求》中另有说明外，投标报价应是投标人为提供本项目所要求的全部服务和相应货物所发生的一切成本、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　除《采购需求》中说明并允许外，投标的每一个货物、服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价，采购人对于其投标均将予以拒绝。

19.3　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，采购人均将予以拒绝。

19. 4 投标人应按照招标文件第五章提供的格式完整地填写各类报价分类明细表。

19. 5 投标应以人民币报价。

20.投标文件的编制和签署

20.1 投标人应按照招标文件和电子采购平台电子招投标系统要求的格式填写相关内容。

20.2 投标文件中凡招标文件要求签署、盖章之处，均应由投标人的法定代表人或法定代表人正式授权的代表签署和加盖公章。投标人应写明全称。如果是由法定代表人授权代表签署投标文件，则必须按招标文件提供的格式出具《法定代表人授权委托书》并将其附在投标文件中。投标文件若有修改错漏之处，须加盖投标人公章或者由法定代表人或法定代表人授权代表签字或盖章。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》、《开标一览表》、《法定代表人授权委托书》，投标人未按照上述要求加盖公章的，其投标无效；加盖公章，但没有法定代表人或法定代表人正式授权的代表签署，或者其他填写不完整的，评标时将按照《评标方法与程序》中的相关规定予以扣分。

20.3 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。

五、投标文件的递交

21．投标文件的递交

21．1 投标人应按照招标文件规定，参考《第五章投标文件有关格式》，在电子采购平台电子招投标系统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电子采购平台规定的要求办理。

21．2 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。

采购人认为必要时，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，并且采购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。

21．3 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，采购人不承担任何责任。

21.4各投标人在投标（响应）文件加密上传后，应及时查看签收情况，并打印签收回执。未签收的投标（响应）文件视为投标(响应)未完成。

22．投标截止时间

22.1 投标人必须在《投标人须知》前附表规定的网上投标截止时间前将投标文件在电子采购平台电子招投标系统中上传并正式投标。

22.2 在采购人按《投标人须知》规定酌情延长投标截止期的情况下，采购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。

22.3 在投标截止时间后上传的任何投标文件，采购人均将拒绝接收。

23．投标文件的修改和撤回

23.1在投标截止时间之前，投标人可以对在电子采购平台电子招投标系统已提交的投标文件进行修改和撤回。有关事项应根据电子采购平

台规定的要求办理。

六、开标

24．开标

24．1 采购人将按《投标人须知》或《延期公告》（如果有的话）中规定的时间在电子采购平台上组织公开开标。并邀请所有投标人的法定代表人或其委托代理人准时参加。

24.2采购人将投标人须知前附表规定的时间和地点组织公开开标会议。届时请投标人的法定代表人或其授权的投标人代表持投标时所使用的CA证书出席开标会，出席开标的代表应签到以证明出席。

开标程序在电子采购平台进行，所有上传投标文件的投标人应登录电子采购平台参加开标。开标主要流程为签到、解密、唱标和签名，每一步骤均应按照电子采购平台的规定进行操作。

24．3 投标截止，电子采购平台显示开标后，投标人进行签到操作，投标人签到完成后，由采购人解除电子采购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。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。

如电子采购平台开标程序有变化的，以最新的操作程序为准。

24．4 投标文件解密后，电子采购平台根据投标文件中《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。

24.5 如投标人的法定代表人或其授权的投标人代表未按24.2条规定出席开标会，或未携带24.2条所要求的资料出席开标会的，视同其认可开标结果。

七、评标

25．评标委员会

25．1 采购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。

25．2 评标委员会负责对投标文件进行评审和比较，并向采购人推荐中标候选人。

26．投标文件的初审

26．1 开标后，采购人将对投标文件进行初步审查，检查投标文件内容是否完整、编排是否有序、有无计算上的错误、是否提交了投标保证金、文件签署是否规范以及投标人资格是否符合要求等。

26．2 在详细评标之前，评标委员会要对投标人资格进行审核并审查每份投标文件是否实质性响应了招标文件的要求。实质性响应是指投标文件与招标文件要求的条款、投标人资格、条件和规格相符，没有招标文件所规定的无效投标情形。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。

26．3 没有实质性响应招标文件要求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。

26．4 开标后采购人拒绝投标人主动提交的任何澄清与补正。

26．5 对于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，采购人可以接受，但这种接受不能影响评标时投标人之间的相对排序。

27．投标文件错误的修正

27．1 投标文件中如果有下列计算上或表达上的错误或矛盾，将按以下原则或方法进行修正：

（1）电子采购平台自动汇总生成的《开标记录表》内容与投标文件中的《开标一览表》内容不一致的，以《开标记录表》内容为准；

（2）《开标记录表》内容与《投标报价明细表》及投标文件其它部分内容不一致的，以《开标记录表》内容为准；

（2）投标文件的大写金额和小写金额不一致的，以大写金额为准；

（3）总价与单价和数量的乘积不一致的，以单价计算结果为准，并修正总价；

（4）对投标文件中不同文字文本的解释发生异议的，以中文文本为准。

投标文件中如果同时出现上述两种或两种以上错误或矛盾的，则根据以上排序，按照序号在先的方法进行修正。

27．2 投标文件中如果有其他错误或矛盾，将按不利于出错投标人的原则进行处理，即对于错误或矛盾的内容，评标时按照对出错投标人不利的情形进行评分；如出错投标人中标，签订合同时按照对出错投标人不利、对采购人有利的条件签约。

27．3 上述修正或处理结果对投标人具有约束作用。

28．投标文件的澄清

28．1 为有助于对投标文件审查、评价和比较，评标委员会可分别要求投标人对其投标文件中含义不明确、同类问题表述不一致等有关问题进行澄清。投标人应按照采购人通知的时间和地点委派授权代表向评标委员会作出说明或答复。

28．2 投标人对澄清问题的说明或答复，还应以书面形式提交给采购人，并应由投标人授权代表签字和加盖投标人公章。

28．3 投标人的澄清文件是其投标文件的组成部分。

28．4 投标人的澄清不得改变其投标文件的实质性内容，不得通过澄清而使进行澄清的投标人在评标中更加有利。

29．投标文件的评价与比较

29．1 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。

29．2 评标委员会根据《评标方法与程序》中规定的方法进行评标，

并向采购人提交书面评标报告和推荐中标候选人。

30．评标的有关要求

30．1 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。

30．2 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。

30．3 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。

30．4 采购人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。

八、定标

31．确认中标单位

31.1除了《投标人须知》第34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排名第一的中标候选单位为中标单位。排名第一的中标候选单位放弃中标、因不可抗力提出不能履行合同、招标文件规定应当提交履约保证金而在规定的期限内未提交的，或者存在违法行为被有关部门依法查处，且其违法行为影响中标结果的，采购人可以确定排名第二的中标候选人为中标单位或重新招标。最低投标报价不是被授予合同的必要条件。

32.中标公告及中标和未中标通知

32．1 采购人确认中标单位后，采购人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。

32．2除了因发生有效的质疑或投诉导致中标结果改变以外，中标结果公示的同时，采购人将向中标单位发出《中标通知书》通知中标。《中标通知书》对采购人和投标人均具有法律约束力。

32.3 中标公告同时也是对其他未中标投标人的未中标通知。中标结果公示后，未中标的投标人即可按《投标人须知》的相关规定退还其投标保证金（如有）。

33．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，采购人均不退回投标文件。

34．招标失败

在投标截止后，参加投标的供应商不足三家；或者在评标时，发现符合专业条件的供应商或对招标文件做出实质响应的供应商不足三家；评标委员会确定为招标失败的，采购人将通过“上海政府采购网”发布招标失败公告。

九、授予合同

35.合同授予

除了中标单位无法履行合同义务之外,采购人将把合同授予根据《投标人须知》第31条规定所确定的中标单位。

36.签订合同

中标单位与采购人应当在《中标通知书》发出之日起30日内签订政府采购合同。

中标单位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。（如有）

如果中标单位没有按照上述规定签订合同或提交履约保证金，采购人将取消原中标决定。在此情况下，采购人可将该标授予下一个中标候选人或者重新招标。

37.其他

电子采购平台有关操作方法可以参考电子采购平台（网址：www.zfcg.sh.gov.cn）中的相关专栏。

第三章　评标办法及评分标准

一、资格审查

采购人将依据法律法规和招标文件的《投标人须知》、《资格条件响应表》，对投标人进行资格审查。确定符合资格的供应商不少于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《资格条件响应表》以及超出项目采购预算的投标，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、除上述以及政府采购法律法规、规章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

（一）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。

（二）评标委员会

1、本项目评标工作由评标委员会负责，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，其中采购人代表一名，其余为政府采购评审专家，从上海市政府采购评审专家库中随机抽取；政府采购评审专家的人数不少于评标委员会成员总数的三分之二。

2、中标候选人推荐办法：评标委员会根据综合得分的排序情况，推荐前三名投标人为中标候选人。

3、评委应坚持公平、公正原则，依据投标文件对招标文件响应情况、投标文件编制情况等，按照投标评分标准逐项进行综合、科学、客观评

分。

（三）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，由其授权的代表签字，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，也不得通过澄清而使进行澄清的投标人在评标中更加有利。

3.3比较与评分。评标委员会按招标文件规定的投标评分标准，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。

（四）评分标准

本项目具体评分标准如下：

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）如果本项目非专门面向中小企业采购，对小型和微型企业投标人的投标价格给予本招标文件前附表中规定的比例扣除，用扣除后的价格参与评审。如果本项目非专门面向中小企业采购且接受联合体投标（或参加谈判、报价），联合协议中约定小型或微型企业的协议合同金额占到联合体协议合同总金额30%以上的，给予联合体本招标文件前附表中规定比例的价格扣除，用扣除后的价格参与评审。联合体各方均为小型或微型企业的，联合体视同为小型、微型企业。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。中小企业投标应提供《中小企业声明函》，如为联合投标的，联

合体各方需分别填写《中小企业声明函》。

（3）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

4.2 投标文件其他评分因素及分值设置等详见如下投标评分标准。

综合评分法

宝山区大数据安全运营服务（安全中心）包 1 评分规则：

评分项目	分值区间	评分办法
报价得分	0~10	1）确定评标基准价：经评标委员会甄别确认，满足招标文件要求的合理的最低有效投标报价为评标基准价。 2）确定其他投标报价分：计算公式为投标报价得分=（评标基准价/打分报价单位的投标报价）×10%×100，分值计算保留一位小数。 3）对小型和微型企业投标产品的报价给予

		10%的扣除，用扣除后的价格作为计分依据。其要求标准详见《政府采购促进中小企业发展管理办法》（财库[2020]46 号）中相关规定。 4）投标人报价明显低于通过符合性检查的其他投标人报价的。评标委员会可以要求该投标人作书面说明并提供相关证明材料。投标人不能合理说明或
需求理解	0~10	根据投标方对项目前期情况的了解和现状的需求分析理解全面深刻，重点难点分析透彻，建议有针对性进行综合评审。（10 分）

服务方案	0~30	根据服务要求投标单位提供运营方案、保障体系及措施。对其完整性、合理性、可操作性等综合打分。
安全运营支撑工具	0~30	安全运营支撑工具功能是否符合项目需求，完全符合或优于项目需求得 30 分，核心技术指标（▲项）需根据▲项汇总表应答并提供证明材料，否则视为无效应答，标注“▲”技术参数不响应的每一项扣 1 分，扣完为止。
类似项目经验	0~4	根据投标人类似项目经验进行评审。每提供 1 份有效业绩证明材料扫描件得 1 分，满分 4 分。投标

		人按照评分办法提供相应数量业绩，多提供业绩数量的投标，按投标人编排顺序，以排在顺序在前的为准，其余业绩不纳入评审范围。
项目团队人员	0~7	1、项目经理要求：具备高级职称或以上的得 2 分，具备中级职称得 1 分，否则本项不得分； 2、在项目实施期间，应组建强有力的项目服务团队，其中应包含至少 5 位系统软件原厂工程师，需具备 CISP、CISSP、DJJS、CISAW、CCSK 其中一个，每有一人满足得 1 分，最高得 5 分,一人最多得 1 分。

应急响应服务	0~5	根据投标单位提供的应急响应服务方案的及时性、应急方案的周全程度等综合打分。
企业综合实力	0~2	1、具有增值电信业务许可证的得 2 分（0-2 分）；
响应文件编制质量	0~2	要求：响应文件的完整性、规范性要求，响应文件逻辑清晰，格式规范等 评分标准： 响应文件内容完整、简洁明了、 上传清晰、编排有序、逻辑清晰、格式规范，得 2 分； 响应文件内容较为完整、简洁明了、上传清晰、编排有序、逻辑较清晰、格式规

		范，得 0-1 分。

第四章　政府采购合同主要条款指引

包 1 合同模板：

合同通用条款及专用条款

合同统一编号：［合同中心-合同编码］

甲方：[合同中心-采购单位名称]	乙方：[合同中心-供应商名称]
地址：[合同中心-采购单位所在地]	地址：[合同中心-供应商所在地]
邮政编码：[合同中心-采购人单位邮编]	邮政编码：[合同中心-供应商单位邮编]
电话：[合同中心-采购单位联系人电话]	电话：[合同中心-供应商联系人电话]
传真：[合同中心-采购人单位传真]	传真：[合同中心-供应商单位传真]
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、服务质量等详见本项目[合同中心-项目名称]采购文件。

采购文件是指招标文件、竞争性谈判文件、竞争性磋商文件、询价文件、单一来源谈判文件。

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：详见采购文件《采购需求》

2．3 服务期限：详见采购文件《采购需求》

2．4 合同有效期：[合同中心-合同有效期]

3．质量标准和要求

3.1 乙方所提供的服务标准按照国家标准、行业标准或地方标准确定，均有标准的以高者（严格者）为准。没有国家标准、行业标准或地方标准的，按照通常标准或者符合合同目的的特定标准确定。

3.2 乙方所提供的服务还应符合国家和上海市之有关规定。

3.3 如本项目涉及商品包装和快递包装的，除招标文件或采购文件中的采购需求另有要求外，乙方所提供的货物包装应当参照财政部办公厅、生态环境部办公厅以及国家邮政局办公室联合发布的《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》执行。

4．权利瑕疵担保

4.1 乙方保证对其提供的服务享有合法的权利，甲方接受乙方服务不会因此而侵犯任何人的合法权益。

4.2 乙方保证在提供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。甲方接受乙方服务不会因此而存在合同外义务的负担。

4.3 乙方保证其提供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 如所提供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合同未能通过验收，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合同未能通过验收，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 付款方式：详见采购文件《采购需求》。

7．2．2 付款条件：

付款时间及条件详见采购文件《采购需求》。

8．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，使甲方有关或设备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 当或设备发生故障时，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设备正常工作要求、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，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

14．1 在本合同签署之前，乙方应向甲方提交一笔采购文件规定金额的履约保证金。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，可以向上海市宝山区政府采购中心或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 本合同在满足招标（采购）文件中规定的生效条件或合同各方签字盖章并且甲方收到乙方提供的履约保证金后生效。

19．2 本合同一式份，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：采购（招标)文件、响应（投标）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。

22. 补充条款（如有）

[合同中心-补充条款列表]

签约各方：

甲方（盖章）：	乙方（盖章）：
法定代表人或授权委托人（签章）：	法定代表人或授权委托人（签章）：
日期：**[合同中心-签订时间]**	日期：[合同中心-签订时间_1]

合同签订点:网上签约

第五章　投标文件格式附件

一、商务响应文件有关格式

1、投标函

致：上海市宝山区大数据中心

根据贵方_____（项目名称、招标编号）采购的招标公告及招标公告，_____（姓名和职务）被正式授权代表投标人_____（投标人名称、地址），向贵方在网上投标系统中提交投标文件 1 份　。

据此函，投标人兹宣布同意如下：

1.经慎重考虑，我方的投标总价为_____（大写）元人民币，并谨此无条件承诺按照招标文件要求的服务期限提供合格的服务。

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.如果我方有招标文件规定的不予退还投标保证金的任何行为，我方的投标保证金可被贵方没收。

6.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。

7.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。

8.我方已充分考虑到投标期间网上投标会发生的故障和风险，并对可能发生任何故障和风险造成的投标内容不一致、利益受损或投标失败，承担全部责任。

9.我方同意网上投标内容均以网上投标系统开标时的开标记录表内容为准。我方授权代表将对开标记录进行确认，授权代表不进行确认的，

由我方承担全部责任。

10.为便于贵方公正、择优确定中标单位及其投标货物和服务，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）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、法定代表人授权书

致：上海市宝山区政府采购中心

我_____（姓名）系_____（投标人名称）的法定代表人，现授权委托本单位在职职工　　（姓名，职务）以我方的名义参加贵中心_____项目的投标活动，并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和签署相关文件。

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。除我方书面撤销授权外，本授权书自投标截止之日起直至我方的投标有效期结束前始终有效。

被授权人无转委托权，特此委托。

在此粘贴被授权人身份证正、反面复印件

委托人名称（公章）：　　受托人（签章）：

委托人注册地/营业地：　　住所：

邮政编码：　　身份证号码：

电话：　　电话

传真：　　传真：

日期：　　日期：

3、法定代表人证明

投 标 人：

单位性质：

地　　址：

成立时间：　　年　月　　日

经营期限：

姓名：　　性别：

年龄：　　职务：

系　　（投标人名称）的法定代表人。

特此证明。

法定代表人签字：_____

投标人（公章）：_____

日期：　　年　　月　　日

4、开标一览表

宝山区大数据安全运营服务（安全中心）包 1

供货期/服务项目负责人	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。

（2）投标人应按照《采购需求》和《投标人须知》的要求报价。

（3）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。

投标人授权代表签字：

投标人（公章）：

日期：　　年　　月　　日

5、报价分类明细表格式

5.1、明细报价格式

序号	名称	数量	单位	服务简述	单价	金额（元）
投标总价						
投标总价（大写）						

说明：（1）所有价格均系用人民币表示，单位为元，精确到小数点后两位。

（2）总价是指项目**合同服务时间**所需的所有费用（包括人工费、材料费、差旅费、劳防费用、应急加班费、车辆损耗、燃油费、车辆维修、车辆保险、车辆年检、管理费、规费、利润、税金等一切费用）。采购人支付上述费用为完全的费用，无须支付其他费用。

（3）节能、环境标志产品应本招标文件第五章中的<<节能和环境标志产品认证证书说明表>>中填写，应完整填写认证证书编号并附证书。

（4）本表格可以横置排版。

投标人授权代表签名：

投标人名称（公章）：

日期：　　年　　月　　日

6、资格条件及实质性要求响应表

项目名称：
项目编号：

项目内容	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及页码	备注
资格性检查				
法定基本条件	符合《中华人民共和国政府采购法》第二十二条规定的条件：营业执照（或事业单位、社会团体法人证书）、税务登记证（若为多证合一的，仅需提供营业执照）符合要求			
	财务状况及税收、社会保障资金缴纳情况声明函			
	参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。			
	未被列入“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和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。			
联合响应	本项目不接受供应商联合体响应。			
法定代表人授权	1、在投标文件由法定代表人授权代表签字（或盖章）的情况下，应按采购文件规定格式提供法定代表人授权委托书；2、按采购文件要求提供被授权人身份证。			
资质证书	是否具有招标公告中要求的资质（如有）			
符合性检查				
投标文件内容、密封、签署等要求	1、投标文件按文件要求提供《投标函》、《开标一览表》、；2、投标文件按招标文件要求密封（适用于纸质响应项目），电子响应文件须经电子加密（响应文件上传成功后，系统即自动加密）。			
投标有效期	不少于 90 天。			
投标报价	1、不得进行选择性报价（投标报价应是唯一的，采购文件要求提供备选方案的除外）；2、不得进行可变的或者附有条件的报价；3、报价不得超出采购文件标明的采购最高限价；			
其他	技术要求中★号条款必须满足，否则按无效投标处理;其他违反法律法规规章及相关文件规定的情形			

投标人授权代表签字：

投标人（公章）：

日期：　　年　　月　　日

7、没有重大违法记录的声明

声　明

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。

特此声明。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（盖章）：

日期：

8、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：

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[软件和信息技术服务业] 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，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）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。

（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）中标人为中小企业的，本声明函将随中标结果同时公告。

（6）投标人未按照上述格式正确填写《中小企业声明函》的，视为未提供《中小企业声明函》，不享受中小企业扶持政策。

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，本声明函将随成交结果同时公告。

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、技术响应文件有关表格格式

1.项目经理情况表

项目名称：
项目编号：
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： 胜任本项目经理的理由：							

备注：投标人应分别提供项目经理情况表、主要设计师情况表。

2.主要管理人员配备及相关工作经历职业资格汇总表

项目名称：
项目编号：
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.投标人近三年以来类似项目一览表

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

说明：（1）近三年指：从解密之日起倒推三年以内正在进行或已完成的项目；

（2）需提供类似项目的合同扫描件、用户评价情况等，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、交付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。供应商需提供的类似项目数量以《评分标准》为准。

4.技术规格参数偏离表

序号	品名	采购规格	投标规格	偏离	说明

声明：除本规格、技术偏离表所列的偏离指标外，其它所有规格、技术参数均完全投标“招标文件”中的要求。

法人代表或其正式授权人签字 并 公章：_____

二、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_____（投标人名称）根据　　年　月　日与贵方签订的_____合同（以下简称“合同”）向贵方提供_____（货物和相关服务描述）。

根据贵方在合同中规定，_____（投标人名称）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_____（投标人名称）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_____（投标人名称）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或者分行出具，分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生效前提交。

2、履约保证金（银行保函）格式

致：_____（采购人名称）

鉴于_____（投标人名称）根据　　年　月　日与贵方签订的_____合同（以下简称“合同”）向贵方提供_____（货物和相关服务描述）。

根据贵方在合同中规定，_____（投标人名称）应向贵方提交由一家信誉良好的银行出具的、合同规定金额的银行保函，作为其履行合同义务并按照合同规定提供给贵方

货物的履约保证金。

我行同意为_____（投标人名称）出具此保函。

我行特此承诺，我行作为保证人并以（投标人名称）的名义不可撤销地向贵方出具总额为_____（以大写和数字表示的保证金金额）元人民币的保函。我行及其继承人和受让人在收到贵方第一次书面宣布_____（投标人名称）违反了合同规定后，就立即无条件、无追索权地向贵方支付保函限额之内的一笔或数笔款项，而贵方无须证明或说明要求的原因和理由。

本保函自出具之日起至全部合同货物按合同规定验收合格后三十天内完全有效。

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或者分行出具，分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生效前提交。

采购需求

1 项目内容

本项目服务内容主要为宝山区大数据中心网络安全层面提供监测监管、威胁验证、协同处置和持续运营管理的服务支撑工作，具体包括如安全事件感知分析研判、通报预警、安全事件指挥调度与协同处置以及安全应急响应保障等等。结合宝山区大数

据中心实际业务现状，对标市级安全建设及安全保障运营的经验，并依据相关政务服务的政策法规，及网络安全等级保护的要求，进行宝山区大数据中心的“云”、“网”、“数”、“端”四个类别的安全状况进行综合监测与持续运营管理的服务支撑工作，其中“云”是指“政务云、城运云、信创云”，“网”是指“政务外网”，“数”是指“各类政务应用系统本身数据及大数据资源平台的汇聚融合的数据”，“端”是指“与政务外网接入的各类物联感知终端，非桌面终端”。

1.1 付款方式

合同签订后按季度支付，每季度支付项目 25%合同款。

1.2 服务期限

服务期限：1 年。

1.3 项目最高限价

本项目最高限价：477.2 万元

2 服务要求

2.1 风险主动识别服务

对涉及近 50 个核心互联网应用（每季度进行一次渗透工作，重大活动保障之前在做一次）系统开展渗透测试工作，包括前期信息收集、漏洞探测、钓鱼攻击和后渗透测试，验证当前的攻击防御能力、威胁分析能力、应急响应能力、业务恢复能力及员工的安全意识，发现安全管理的漏洞，补全安全建设的短板，明确后续安全建设的重心。

代码审计能力要求不低于每 5 工作日审计 10 万行。

2.2 防御验证服务

防御验证服务根据实际业务情况要求每年进行一次红蓝对抗工作。

2.3 威胁狩猎服务

威胁狩猎服务过程中，需要构建基于日志关联分析、失陷主机监测及深度 APT 威胁监测来发现和阻止恶意的并且极难检测的攻击行为。威胁狩猎是一个持续的过程，也是一个闭环。威胁狩猎服务每月进行 1 次，每次时间不得低于 5 天。

2.4 应急运营服务

建立应急响应体系，根据业务场景设计和常态化演练应急处置预案,发生安全事件后，按标准流程进行评估和分级分类处置，及时止损，控制影响，开展反制，查找原因，消除隐患，恢复生产。

➢应急演练服务

提供一年一次的应急演练服务。

➢应急处置服务

针对安全突发事件的特点和造成的危害，进行协同指挥、协助应急处置。

➢应急预案服务

提供应急预案剧本编写及优化服务，包含根据应急演练的结果对应急预案进行优化调整。

2.5 安全运营管理服务

序号	服务说明		服务简述	工作开展要求
1	安全高阶能力培训		提供 13 人/天安全高阶能力培训如：攻防技术培训、代码安全培训等	每年
2	日常	资产管理	持续跟踪资产发现、资产变更收集、资产登记信息核查、资产登记、资产漏洞信息管理等工作	每周 1 次

3	安全监测服务	漏洞扫描	利用扫描器对待上线系统进行安全检查	每季度1次
4		安全基线核查	必要安全设备、核心业务相关安全基线情况核查，避免漏查造成的脆弱性	每季度1次
5		病毒免疫能力检测	定制化模拟勒索病毒脚本，以检测疫苗形式，验证勒索病毒防御能力，检测报告及整改建议。	每年1次
6		安全数据上报服务	按照市大数据中心的要求，完成每日数据上报。上报数据内容包括但不限于：系统级联认证、系统运行状态、告警、安全事件、统计、预警通报共六大类	每月1次
7		情报检测与分析及预警	利用高可信威胁情报关联安全日志和流量，实时检测出恶意攻击，并根据情报的威胁分值设定相应的威胁等级，提供至安全人员进行处置	提供现场7*24小时服务
8		网络安全行为分析及预警	网络安全行为分析基于网络流量，整合和优化用户行为数据，监控业务访问的整体情况，同时基于大数据分析平台和高级分析算法，有效发现内部人员的恶意或异常的行为，进行风险预警，及时发现问题	提供现场7*24小时服务
9		态势感知监测分析及通报预警	根据部署的安全运营平台上联动的所有安全设备接入日志及流量进行综合统筹分析，对发现的攻击行为、攻击特征进行捕获和研判，并详细记录攻击相关数据为后续处置和溯源以及安全策略优化工作开展提供信息并通报安全事件。	提供现场7*24小时服务
10		安全攻击溯源分析	找到攻击源头。攻击溯源的手段，包括但不限于：IP定位技术、ID追踪技术、攻击路径分析等手段。	每年4次现场
11		督促整改及威胁协同处置	1、与业务部门、运维部门进行联合评判，根据事件影响以及业务属性制定对应的应急处置方案；2、督促、跟进相关服务商完成整改，协助安全加固	每年4次现场
12		安全辅助决策服务	通过安全运营平台对各类事件进行聚合分析，形成动态实时的态势展示，为基层员工研判处置，中层干部管理落地、高层领导辅助决策，提供依据	每年4次现场
13		基础安全培训	提供7人/天基础安全培训，例如：人员意识培训、内部安全宣贯等	每年
14		重保值守服务	国庆10人/天、两会25人/天、进博会等重要时期安全保障30人/天	重保总工时65人/天（可按照实际重保需求动态调整人/天资源）
15		安全汇报	通过安全运营平台输出安全报告，配合其他安全工作的相关信息，形成汇报材料向业主安全负责人进行工作汇报	每周1次（含汇报材料撰写）
16	等级保护预测评		邀请具有测评资质的第三方机构对安全防护能力进行评估、测试	3个系统

17	安全管理制度		1、建立、新增、完善、优化安全运营管理流程与安全运营管理制度； 2、安全体系类、系统化的安全规划； 3、宝山多安全厂商及服务商之间的安全应急流程设计； 4、安全服务商评估体系设计	新建/修订安全管理制度共计115个管理制度
18	特色场景运营服务	数据安全运营	数据安全告警策略定制化	每月1次，每次3天
19			数据安全态势分析	
20			数据安全场景化预警模型定制	
21			数据威胁研判分析及威胁协同处置	

3 服务工具要求

本项目服务支撑工具包括：安全运营平台、流量探针（APT威胁检测系统）、资产威胁与漏洞管理平台、数据安全管理系统等。在服务期限内，服务支撑工具的版本、引擎库等能及时更新。

服务支撑工具参数指标

3.1 安全运营平台

序号	指标项	子模块	指标项描述
1	工作台	日常运营工作台	支持开箱即用的个人工作台界面。 支持默认展示工单、安全事件、合并告警、脆弱性、预案、风险资产概况，支持展示报告生成情况。 所有安全信息支持点击下钻，展现进一步信息。 支持自定义工作台内容、内容分组。
2	态势感知	内置标配大屏	系统内置9张大屏，包括威胁攻击态势、资产安全态势、安全事件态势、安全成果态势、综合安全态势、威胁情报态势、运行监控态势、大数据中心态势、XDR运行态势
3		大屏自定义	态势感知大屏元素支持自定义，选择经过仪表盘定义的图例替换原有大屏元素
4		大屏轮播	支持大屏轮播，支持自定义参与轮播的大屏，轮播间隔时间、轮播大屏顺序。

5		仪表盘	支持自定义仪表盘配置，根据需要添加不同的监控组件，自定义选择过滤条件和过滤条件组的监控组件添加、修改和删除。 支持同时组合多种展示图形，如柱形图、堆积柱形图、折线图、分组折线图、面积图、饼图、环形图、表格、统计值、玫瑰图、气泡图、热力图、复合计算统计、上传图片、外部图片、外部网页等，可配置排序方法、TOP 数量、数据时间跨度。 仪表盘的图形位置和大小支持自由拖拽，所见即所得。 支持设置常用仪表盘，通过拖拽调整仪表盘的顺序，将选定的仪表盘设为首页，登录系统后将直接展示对应的仪表盘的内容。
6			支持从仪表盘下钻至具体事件、告警、资产等并且可直接配置下钻选项，支持跳转到自定义的其它仪表盘，实现仪表的嵌套来满足分析需要。支持仪表直接调用 SOAR 预案来快速处置，支持仪表的内容通过点击快速变为过滤条件。
7		报告报表	支持从原始日志与流量、安全设备告警、平台关联告警以及安全事件输出多个层面自动呈现统计数据。支持对概况、事件、IP 地址、端口、服务、事件严重程度、攻击种类、用户等数据进行统计。报表内容支持自定义编辑，直接引用图标、文本、链接、图片、宏变量、嵌套报表、外部网页等元素。
8			报告中数据支持统计查询与过滤条件满足与、或、非、In、Not In、exist、like 字符串匹配、rlike 正则匹配等基础组合。支持报表图形化结果展示包括但不限于柱状图、饼图、面积图、趋势图、表格、统计、同比、环比、百分比、复合统计等。
9			支持周期性（每日、每周、每月）自动生成报表并通过邮件发送、下载、导出等方式获取。支持导出 WORD/HTML/EXCEL/PPT 等格式，报告可指定人员进行分享。
10	分析中心	场景化检索	支持对日志、告警进行场景化检索。 支持针对日志\告警内容的不同场景，自动化推荐检索字段、列表字段进行检索
11		综合检索	支持对日志、告警、事件、漏洞、资产、风险、预案进行检索分析。 支持添加结构化语言过滤条件和过滤条件组对内容进行查询，支持查询条件支持 and、or、not 等多重逻辑操作组合，支持等于、不等于、大于、小于、存在、不存在、属于（内置安全信息）、网段包含、字符串匹配、正则表达式匹配等多种操作符。
12			支持研判分析过程中在线解码，无需使用其他工具即可实现 BASE64\HEX\URL\JSON 等常见编码和解码转换功能，提高分析效率。
13			支持对结果数据任意字段添加过滤条件，仅展示相同值或者不同值。 支持对结果中的资产、IP、域名、URL 等对象直接联动 SOAR 预案进行自动化响应处置。
14			▲针对原始日志检索结果，支持一键跳转原始日志相关的威胁告警、安全事件。
15		高级检索	支持单一界面统一检索日志、告警、事件、资产、脆弱性、安全风险、安全预案执行情况等多类型数据。
16			支持在主查询语句中嵌套子查询语句，多查询语句的管道连接，以支持复杂场景。管道支持任意级别。

17			支持对字符串、数字、时间等类型的参数进行常见函数调用，支持平均值、计数、去重计数、最大值、最小值、差值、求和等统计聚合函数；支持 search、where、eval、bucket、stats、sort、join、fields、head、top、format、append 等搜索命令
18		可视化分析	三种检索方式均支持检索一键切换 BI 可视化分析，通过可视化 BI 图表自定义展示与分析，图表展示包括柱形图、堆积柱形图、折线图、分组折线图、面积图、饼图、环形图、表格、统计值、玫瑰图、气泡图、热力图等 24 种类型，多维度快速展现数据的价值，在分析过程中支持设定周期自动刷新。 支持样式配置，实现不同的展现形式，如小标题、数值单位、横坐标标签样式、是否显示统计值、图例布局等。 支持图表直接发布到既有仪表盘或新增仪表盘中。 支持仪表盘和报表模板对 BI 分析结果的直接引用，BI 分析所用的查询条件和 BI 图例一起保存和发布。
19		威胁图谱	支持实体分析入口页，可对外网 IP、内网 IP、样本 Hash、账号、域名、主机等 6 类实体进行统一检索，跳转到对应详情页； 入口页支持外网 IP、内网 IP、样本 Hash、账号、域名、主机等 6 类实体的总数、24 小时活跃数、24 小时产生告警数的统计展示，并能够跳转到对应的实体列表页查看该类实体更详细的信息。
20			支持对外网 IP、内网 IP、样本 Hash、账号、域名、主机等 6 类实体实体的网络连接关系进行图谱绘制，以拓线图谱的方式展示本实体与其他内外网实体之间的关联互访关系，标记出各实体的类型与风险等级，通过图谱快捷交互可以展示关联实体的概要信息并跳转至详情页进行查看。 对图谱的手动操作包含删除、返回、前进、居中显示、固定显示等操作，对实体的分析操作包含按关系分类拓线、复制、固定节点、删除、预案执行、多源查询等操作。
21			支持外网 IP 类实体的画像分析与展示，支持展示情报匹配详情、关联威胁告警数量、关联安全事件总数、被实体访问数、主动访问实体数、关联账号数、传输文件数、可交互威胁拓线图谱、基础信息、访问关系、行为、操作历史、实体相关预案概览等。
22			支持域名类实体的画像分析与展示，支持展示情报匹配详情、关联威胁告警数量、关联安全事件总数、被实体访问数、关联账号数、传输文件数、域名绑定 IP 数、可交互威胁拓线图谱、基础信息、访问关系、行为、操作历史、实体相关预案概览等。
23			支持 Hash 类实体的画像分析与展示，支持展示情报匹配详情、关联威胁告警数量、关联安全事件总数、关联实体总数、可交互威胁拓线图谱、基础信息、访问关系、行为、操作历史、实体相关预案概览等。
24			支持内网 IP 类实体的画像分析与展示，展示内容包括本实体关联的资产基础信息、实体上的脆弱性数量与等级分布、关联威胁告警数量与等级分布、关联安全事件数量与等级分布。页面集成内网 IP 实体的威胁图谱，并能汇总呈现与本实体相关的威胁告警/安全事件详情、关联资产信息详情、内外网实体访问关系详情、账号登录操作交互详情、实体信息操作变更历史详情、实体关联处置预案信息等。

25			支持主机类实体的画像分析与展示，展示内容包括本实体关联的资产基础信息、实体上的脆弱性数量与等级分布、关联威胁告警数量与等级分布、关联安全事件数量与等级分布。页面集成主机类实体的威胁图谱，并能够汇总呈现与本实体相关的威胁告警/安全事件详情、关联资产信息详情、内外网实体访问关系详情、主机操作行为、主机进程树详情、账号登录操作交互详情、实体信息操作变更历史详情、实体关联处置预案信息等。
26			支持账号类实体的画像分析与展示，概览展示内容包括本实体关联的威胁告警数量与等级分布、关联安全事件数量与等级分布、账号登录过的内网主机数量、账号触发的用户异常行为数量。页面集成账号类实体的威胁图谱，并能够汇总呈现与本实体相关的威胁告警/安全事件详情、账号登录主机详情、实体信息操作变更历史详情、实体关联处置预案信息等。
27		威胁告警	支持查看威胁告警概览信息，包含开始时间、结束时间、告警阶段、告警次数、数据源、责任人等信息，且能进行下钻查看原始日志和原始告警详情、执行 SOAR 预案、发起工单、处置、一键加白等操作；
28			支持查看告警基础信息，包含相关资产、外网 IP、威胁特征、告警内容、请求、响应流量等信息，重点分析字段用图标进行标记，流量类告警相关字段高亮显示且支持下载 pcap 包分析； 涉及进程异常的告警类型详情中支持进程树的绘制； 告警详情中支持提取相关实体，并能跳转到实体详情进行分析。
29			▲在联网场景中，非威胁情报类型的告警详情中管理的外网 IP 支持情报富化，如命中可展示地理位置、运营商、AS、ASN、网络类型、匿踪类型、情报风险等级、情报风险类型、威胁类型、置信度、阻断系数、处置建议等信息。
30			支持查看同类告警，可以参考历史研判经验，或者进行批量处置响应。
31		关联分析规则	支持不少于 800 条规则的安全检测分析场景的开箱即用； 场景包括：扫描探测、主机异常、异常通信、漏洞攻击、运维监控、Web 攻击、账号异常、网络攻击、威胁情报、恶意程序、邮件攻击、多维关联、内容安全
32			支持原始告警关联、威胁情报关联、终端行为关联、网络行为关联、资产关联、漏洞关联、技战术关联等多种维度的多字段关联。
33			去重统计关联：在一段时间内，多个事件中某属性值不同的次数满足条件即触发统计类告警。
34			不去重统计关联：在一段时间内，某事件发生的次数满足条件即触发统计类告警。
35			分组后的某个数值进行累加统计关联：在一段时间内，多个事件中某个属性值的和满足条件即触发统计类告警
36			支持 A 事件后发生 B 事件，事件 A 发生后关联产生 B 事件，如检测到 webshell 连接后疑似通过 mysql 提权。事件前置条件是 webshell 连接成功，连接成功后通过 mysql 有提权操作，这两件事 30 分钟内先后发生。
37			支持至少 M 次 A 事件之后发生了 B 事件，事件 B 的发生是因为事件 A 导致（事件 A 不限数量），如特定账号 5 分钟内进行暴力破解的次数大于或等于 10 次后，登录成功。

38			支持 A 事件和 B 事件均发生但无时间先后，如服务器 webshell 行为检测，服务器进程创建的路径是可疑路径并且进程创建的当前目录是某应用所在目录，这两件事只要在 10 秒内发生即可。
39			支持多件事（事件数量大于等于 2）同时发生（无前后顺序），多个事件同时产生没有数量限制。
40			支持 A 之后一定不发生 B 事件，如在 WAF 的日志中访问 www.test.com 以外网站数据的源地址一定没出现在 WAF 的告警日志中。证明了该攻击事件绕过了 WAF。
41			支持 B 事件发生之前一定没发生 A 事件，如在管理员未登录时主机上创建异常定时任务， 说明可能是非人工创建或存在登录绕过风险，主机行为非常可疑。
42			支持指定时限内特定事件未发生，例如心跳周期内未发生心跳连接
43			支持同比分析算子，根据历史的同周期数据进行对比并判定偏差度来发现异常线索。支持通过同比昨天、上周、上个月及自定义周期的方式来计算，根据统计变化率（如同比增长 10%，增长 20%-40%等）或变化的绝对值（如登录次数同比增长 5 次）来进行同比分析。
44			支持基线分析算子，根据历史数据生成基线并判定偏离度来发现因为变化难以直接给定阈值的异常行为。支持配置以小时、天为单位生成基线的周期，同时指定周期内取样的颗粒度（如分钟、小时和天），基于以上配置生成基准线。在基线的基础上支持配置偏离度，偏离度的数值是大于、小于、在某两个值区间等。
45		关联分析规则管理	关联分析系统的模型配置支持图形化配置和管理，有助于根据场景运营，支持修改所有预置关联分析规则，支持通过 WEB 界面 新建、编辑关联分析规则
46			支持关联规则在配置时评估该策略运行所使用的资源情况，在线显示该规则的性能指标，分为优、良、差多个级别。
47			支持把前一个关联分析结果作为内部事件为作为后一个关联规则的输入进行多级（数量无限制）关联分析的嵌套，以支持复杂的关联分析。
48			▲支持关联规则根据数据标准进行规则编写的自动化推荐，系统根据事件类型自动推荐其所属的对象，并且会自动判断规则内容是否与该对象匹配。
49			关联分析规则支持通过配置调用 SOAR 预案形成自动触发场景，支持触发周期、责任人的配置。支持指定告警阶段、告警级别和该告警使用的 ATT&CK 技战术。
50		XDR 分析规则	内置 10 种神经元的 600+条分析规则；覆盖 10+类安全场景。
51			支持查看 XDR 规则对应的典型攻击场景，理解典型的攻击过程，辅助告警分析研判
52		XDR 分析规则管理	支持查看 XDR 模型规则，启停 XDR 模型； 支持配置 XDR 规则的合并告警规则、响应预案； 支持查看神经元激活分析模型数量。直观了解不同神经元对安全分析的贡献。
53		告警调整规则	支持配置告警调整规则，使用资产、漏洞、情报等信息对告警级别进行调整； 支持在告警调整规则中配置适用该规则的威胁分析规则，支持通过类 sql 语法过滤适用该规则的告警；

			支持设置直接调整，脆弱性匹配调整，条件字段匹配调整三种告警级别调整方式，支持对告警级别上升、下降 1-3 级。
54			支持在告警界面查看告警级别调整记录，查看初始告警级别，命中告警调整规则名称、级别变化，最终告警级别； 支持在威胁分析规则界面查看所有可能会影响当前威胁分析规则触发告警的最终级别的告警调整规则。
55			支持告警调整规则管理，包括新建、删除、编辑、导入导出等； 出厂预制不少于 5 条告警调整规则。
56		告警合并规则	支持配置告警合并规则，聚合告警，生成合并告警； 支持告警合并规则管理，包括新建、删除、编辑、导入导出； 支持配置合并告警名称、规则描述、合并策略。
57			支持引用告警的任意字段、字段组合生成合并策略，引用相同合并告警规则且合并策略内容相同的告警会聚合为一条合并告警
58		静态安全信息	支持关联分析过程中随时调用静态对象来快速完成分析模型的构建，避免频繁修改模型内容。 支持内置包括 IP 类、时间类、数字类和字符类的不低于 100 种常用的安全信息，如办公区 IP、工作时间段、黑名单 IP、常见服务端口、cmd 进程白名单、可疑进程列表等。 静态信息组的管理支持包括新建、删除、编辑、导入、导出、检索，并以树形结构进行分类管理。
59			支持键值对类型信息组，支持日志中的 2 个字段与信息组内容进行匹配。 例如：设置服务器进程黑|白名单信息组，支持根据服务器 IP 设置不同的进程黑|白名单；支持日志中 IP、进程名均命中信息组告警，或 IP 命中、进程不命中告警。
60		动态安全信息	动态信息组的管理，支持包括新建、删除、编辑、导入、导出动态信息，数据类型包含 IP、数字、字符串，支持将命中规则事件的中任意字段自动添加、删除到动态信息组。
61			动态信息组支持定义数据过期时间，包含不过期、根据数据创建时间计算和根据数据更新时间计算，指定数据保留所需的秒、分钟、小时、天和周等时间段。
62		告警加白	支持对产生的告警进行统一过滤降噪，命中告警过滤规则的告警讲不会被展示。 支持告警过滤维度包含关联分析规则名称、攻击者 IP、受害者 IP、URL、域名、样本 MD5、客户端标识。 支持使用类 SQL 语法进行规则配置，使用任意字段、and|or|not 逻辑关系进行告警过滤 支持设定规则生效时长，1 天、7 天、30 天、永久。 支持从告警界面一键创建告警过滤规则，自动代填告警中出现的信息。
63		云端情报	支持连接云端，获取不低于 2000W IOC 情报
64		本地情报	支持本地化的情报管理，支持情报类型包括：IP、IP:PORT、DOMAIN、URL。支持本地情报的新建、删除、修改、查询、导入、导出
65		安全事件	支持查看安全事件详情，包括不限于：概览、威胁图谱、告警、相关证据、影响面、处置信息。

66			展示安全事件概览信息，包括不限于：数据源，攻击阶段统计，告警总量，待处置告警数据，影响面实体数量，其他实体数量，证据数据等。 支持将安全事件中所有告警的攻击技战术，以矩阵形式展示。 支持根据告警先后顺序，以及告警的攻击者、受害者所处安全域绘制杀伤链。
67			支持将安全事件中所有涉及到的实体、实体之间的关系进行可视化呈现，支持通过和实体交互执行流量分析、进程树查看，SOAR 预案调用等分析、响应动作， 支持实体上下文信息自动化补全，上下文信息包括不限于攻击者情报、历史攻击行为，受害者资产信息等，支持直接下钻到实体画像和情报详情查阅； 支持点击回放，按照时间顺序回放攻击过程。
68			支持以时间轴方式展示安全事件中的所有核心告警、非核心告警、日志信息，支持点击时间轴快速定位相应的告警、日志； 支持以卡片或者列表模式展示安全事件中的告警；卡片模式支持展示告警名称、级别、告警类型、攻击者、受害者、攻击阶段信息；列表模式支持用户自定义表头； 支持展示告警的关联条件以便于理解告警合入安全事件的原因；
69			▲支持抽取安全事件中支撑分析研判的证据进行集中展示； 支持证据跳转相应的告警查看完整上下文； 支持的证据类型包括不限于：威胁情报、恶意样本鉴定结果、威胁特征。
70			支持抽取安全事件中涉及到的内部实体（内网 IP、主机、账号）进行统一展示，支持查看实体名称、风险等级等信息，支持跳转相应的告警。
71			支持安全事件将所有相关告警的处置建议进行统一汇总和展示，对每个告警有对应的分析内容和处置建议，提供兼容 ATT&CK 并且新增扩展的缓解建议和检测建议。
72			支持研判分析过程中直接添加新的日志和告警信息进安全事件。
73		安全事件模型	▲支持自动化威胁猎捕模型，可在线编写脚本语言算法模型模拟分析人员溯源取证的过程，基于告警事件为入口触发条件的威胁场景自动溯源分析，向前、向后自动抽取若干分钟、小时和天为单位的数据，结合时间、过滤条件关联，多层逻辑嵌套、自动聚合分析包括日志、流量、告警等内容，聚合跨阶段展示整个威胁事件。
74			支持将告警按照整个事件的攻击链、攻击方向聚合及攻击时间轴排序，整合为一个事件的完整攻击链阶段。 并根据聚合事件的安全评分模型化动态评估严重等级，模型维度包括不限于告警数量、告警等级、攻击阶段、威胁情报。
75			内置不低于 15 种聚合事件威胁场景，如 Tomcat 遭受暴力破解攻击后被上传 webshell，并发起了 445 端口扫描、FTP 账号被暴力破解成功后数据遭到窃取、内网主机遭受远程漏洞攻击后连接矿池、UAC 提权并驻留并发现 Powershell 系列攻击等。
76			系统模块内置信息统计聚合模型，通过聚合主机访问行为、命令执行安全告警、服务器短时间内频繁执行信息收集命令告警、运行代理工具告警等多源数据进行自动化提取和校验，检测出主机遭受 ssh 暴力破解后主机层面出现异常命令操作行为，爆破成功并驻留。

77			系统模块内置横向移动聚合模型，通过以进程执行哈希传递攻击告警、黑客脚本工具 invoke_Psexec 行为和哈希传递登录行为为入口，自动化溯源聚合多源告警和行为的关联关系，检测出哈希传递技术手段的 Windows 登录事件突破边界横向移动并还原攻击者上下文操作的安全事件。
78			系统模块内置权限维持聚合模型，以 webshell 执行可疑命令的告警为入口，从网络行为日志中提取入口告警前 30 分钟的告警，从主机行为日志中提取入口告警向后 30 分钟的进程行为，系统自动校验多源数据还原主机在被植入 Webshell 后,攻击者执行的上下文操作,,包含 webshell 如何植入,以及植入 webshell 后攻击者又执行了哪些操作。
79			▲系统模块内置病毒扩散聚合模型，以内网主机发起特定端口扫描后并对该端口进行攻击的告警为切入点，聚合向前 10 小时向后 2 小时的威胁情报的告警、向前 3 小时向后 2 小时的基于漏洞的告警、向前 3 小时向后 2 小时的主机网络连接行为，系统自动对以上多源信息进行校验和聚合，生成外网利用漏洞攻陷内网主机后进行蠕虫传播的安全事件。
80		攻击者分析	支持从所有产生的告警中，提炼出外网攻击者的 IP 列表和 Domain 列表，从而方便快速针对具体攻击者做分析研判。 支持通过攻击者 IP\域名、受害主机 IP、告警处置状态、对攻击者进行检索 支持查看高频攻击者 top5、攻击阶段等统计信息 支持通过攻击阶段、合并告警数量、最近攻击时间等进行攻击者排序
81			支持自动分析攻击者威胁等级，支持手动修改威胁等级。 支持一键跳转威胁情报。 支持调用 SOAR 预案 支持分 tab 显示攻击者基础信息、关联网络\行为，分析处置历史。 攻击者基础信息包括不限于：攻击者告警类型分布、告警趋势、杀伤链；威胁情报详情；相关告警列表；相关安全事件列表 关联网络\行为 内容包括不限于：传输样本列表，相关网络访问统计、相关域名信息统计。 分析处置处置内容包括不限于：威胁级别变化历史，响应预案执行历史。
82		风险资产分析	所有产生的告警中，提炼出遭受到攻击的内网资产信息，从而方便快速排查具体内网资产的风险情况。 支持通过资产名称、资产 IP、资产标签、是否存在漏洞、是否失陷等条件对风险资产进行检索。 支持通过风险等级、最近受攻击时间等维度进行风险资产排序。
83			支持自动分析资产风险等级、失陷状态，支持手动修改威胁等级、失陷状态。 支持调用 SOAR 预案 支持分 tab 显示资产相关威胁详情、资产详情、关联网络\行为，分析处置历史。 威胁详情包括不限于：攻击者 top5、告警类型分布，告警趋势；资产失陷外联告警、横向移动攻击告警、受攻击告警；相关安全事件 资产详情包括不限于：资产管理信息，资产脆弱性信息、相关服务信息、相关网站信息等

			关联网络\行为 内容包括不限于：资产相关文件信息，内部\外部访问关系、登陆信息。 分析处置处置内容包括不限于：风险级别\失陷状态变化历史，响应预案执行历史。
84		历史回溯分析	支持使用关联分析规则、安全事件模型对历史数据进行回溯，排查历史上的攻击行为。
85			支持使用 AI 算法对历史数据进行检索、分析，； 支持算法包括个人动态基线算法-Prophet 模型部门基线算法 - 自编码器模型、部门基线算法 - 时序特征的孤立森林模型；
86			▲支持使用系统内置情报或手动上传的情报包对历史数据进行回扫，排查历史攻击行为； 支持手动创建回扫任务或者配置自动回扫任务； 支持设置回扫威胁情报类型、回扫情报严重级别，回扫时间范围，回扫任务开始时间； 支持查看回扫任务结果，包括不限于回扫 IOC 数量，回扫命中 IOC 数量、回扫告警数量、回扫受害者数量，支持查看回扫告警详情。
87		专项场景	针对高危、高频出现的攻击场景，支持针对性的场景化分析、展示。 支持根据不同安全场景，预制不同的检索字段，统计字段，列表字段；支持不同场景下的不同的合并告警二次聚合，以提高分析处置效率；支持在场景化分析界面调用处置预案进行快速处置。 支持安全场景包括不限于：Webshell、通用 web 攻击、漏洞利用、弱口令、爆破攻击、邮件威胁、隐蔽隧道、威胁情报、挖矿木马、异常登录、
88	处置中心	自动化动作	支持机器动作、人工动作和子预案嵌套的分类，机器动作为设备可自动化执行的行为，人工动作为人工干预判定的行为，预案嵌套为前一个已定义好的预案作为动作为下一个预案调用。
89			支持集成对接框架，外部设备或系统可通过统一定义的接口供自动化动作调用，结构包括不限于包括 REST API 接口、SSH 接口。 支持通过 Python 自主定制动作脚本，提供可视化的脚本助手来协助动作编写。
90		可视化编排	支持 SOAR 预案可视化编排，根据不同安全策略的需求，通过拖拽预案动作的方式自定义安全预案，实现安全流程的自动化处置。 支持多级子预案嵌套形成复杂的预案，并且预案可以复用。
91			支持对自动化动作以及人工动作的逻辑编排，支持顺序执行、判断分叉执行实现 or、and、if else 等自动判断逻辑。每种动作都可单独设置责任人，人工动作支持判断型、确认型和信息收集型 3 种满足不同场景需求。
92		预案执行	支持对责任人、标签、预案名称、任务状态等进行过滤后查看、删除预案的执行情况，点击详情后通过图形化流程图来查看预案运行的细节，包含执行结果、自己关联的任务。支持按照账号\预案分配执行权限，避免高危预案误执行。
93			支持预案自动执行、手动执行、定时执行三种执行方式，自动执行支持告警/安全事件自动触发预案，手动执行支持任意分析界面通过手动触发，定时执行支持单次、每日、每周、每月等绝对时

			间和每隔 X 分、小时、日等周期的相对时间，单个预案可以编排多条不同时间安排策略。
94		预案审计	支持对预案执行情况进行审计。支持通过任务名称、执行参数、应用实例、执行状态、审计结果、任务执行人等维度进行检索审计记录。
95		封禁 IP	支持根据调用预案进行封禁、解封动作的执行情况，记录 IP、Domain 的当前封禁状态； 支持手动新建记录，标识或者变更 IP、Domain 的封禁状态； 支持查询 IP、Domain 的历史封禁、解封记录
96		工单内容	支持设置工单标题，优先级，截止时间，受理人，是否需要审批，审批人，工单内容、工单附件； 工单内容支持在线富文本编辑，包括文字、表格、图表等； 工单附件支持文件类型包括：rar、zip、gz、doc、docx、pdf、txt、ppt、pptx、xlsx、xls、csv、jpg、jpeg、png； 支持保存工单至草稿箱，便于后续编辑。
97		工单调用	系统支持四种类型的工单：合并告警工单、安全事件工单、脆弱性工单、通用工单； 支持在合并告警、安全事件、脆弱性界面一键发起对应类型的工单，并根据所选择的合并告警、安全事件、脆弱性内容，自动设置工单标题、优先级、自动填入工单内容；支持选择多个合并告警、安全事件、脆弱性发起批量工单； 支持通过响应预案模块自动化发起工单； 支持手动发起通用工单。
98		工单通知	支持工单配置系统通知、邮件通知。
99		攻防知识图谱	支持知识图谱技战术热力图，支持通过颜色深浅来代表该技术的攻击强度。 支持点击攻击技术，查看详情，包括不限于子技术、技术描述，相关安全事件等。
100			▲支持 Mitre ATT&CK 之外扩展出具备中国特有的技战术总结。
101		案例库	支持从安全事件管理直接自动生成案例和通过手动方式新建案例，包括案例名称、分类、描述、解决办法； 支持从案例库直接下钻到原始的事件详情进行复盘分析
102	资产中心	资产信息管理	支持资产信息管理，按资产组分视图展示。 支持资产数据导入导出。 支持资产属性字段自定义扩展。
103		资产组管理	支持多层级资产组划分资产，提供自定义资产组功能；支持调整子级分组的上下排序；支持设置资产组的责任人信息包括姓名、手机号、邮箱等。 支持多个视角的资产视图查看，包括普通分组、安全域、业务系统、物理位置及未分组资产，支持将未分组资产默认加入“未分组资产”。
104		网段管理	支持对客户资产 IP 信息进行统一集中管理，支持网段信息展示、检索、新建、导入导出、详情、编辑、删除等功能。 支持以 IP 值、IP 区间、子网掩码、IPv6 值、IPv6 区间及 IPv6 前缀 6 种模式录入网段信息。 支持网段信息关联所属组织机构、安全域信息。

105		资产拓扑管理	支持定义拓扑图并标注资产、资产组对应的位置，大屏展示时支持下钻查看局部风险评估同时支持拓扑定义的配置导入、导出。
106		资产被动发现	支持通过网络流量被动发现资产信息。 支持对被动发现的资产分析是否未纳管资产，如未纳管支持补全信息添加至正式资产列表。
107	安全大数据	采集方式	支持业内通用标准数据获取方式，获取方式不少于 15 种，包括 TCP|UDP-Syslog、SFTP、文件、Kafka、HDFS、主机终端(win/linux)Agent、DB2、Mysql、Oracle、Sqlserver、Postgrel、SNMP、Netflow、WMI、ES、AWS 等。 可接入各类设备和应用系统，包含但不限于主机、服务器、防火墙、IPS/IDS、WAF、其他网络设备、其他安全设备、数据库、应用系统、中间件、存储设备、虚拟化设备、机房设备、云平台(AWS)。
108		采集监控	支持监控数据源的采集情况，监控维度包括不限于解析链耗时、解析链解析日志平均字段数、解析链核心字段解析情况、解析失败趋势，采集数据量，日志采集延时等。
109		采集异常告警	支持针对采集异常进行告警，支持客户选择需要告警的异常维度，并设置异常阈值，支持异常告警维度包括不限于解析过慢、解析字段数异常、解析失败、采集数据量异常、日志采集延时异常。
110		数据连接器接入	针对常见的三方设备，支持提供数据连接器接入模式，仅需配置设备 IP、日志采集端口等基础环境信息，无需配置任何数据采集、数据解析参数，即可完成数据接入。
111		神经元统一管理	支持在对系统接入的自有神经元进行统一管理。 支持监控神经元数据上报情况；支持对神经元进行 SSO。
112		神经元统一接入	支持在单一界面进行自有神经元数据接入、联动响应对接。 支持对接神经元类型包括：NDR、EDR|EPP、浏览器、资漏管理、浏览器、沙箱等
113		数据接入概览	支持展示接入 XDR 探针|三方数据源概况，包括总量、异常数量、正常数量，DR 探针|三方数据源列表； 支持用户配置重点 XDR 探针|三方数据源，支持展示重点 XDR 探针|三方数据源状态； 支持展示系统采集节点概况，包括在线状况，工作负载等。
114		数据解析	支持图形化在线配置数据解析规则； 支持规则嵌套和逻辑组合方式，能够对一组事件进行多层规则解析处理； 支持添加、删除、重命名、合并、拆分与裁剪现有字段，对范式化后字段再解析处理； 支持多种数据解析，包含精准匹配、包含再解析、正则匹配后从数据头、尾进行二次解析等处理 。
115			支持数据删除配置，包括删除字段、字段裁剪、删除整条数据、json 字段提取、格式化成 json 对象或数组、字段拆分等过滤方法。
116			支持日志解析包括正则表达式、Grok 表达式、键值对、分隔符、CEF、XML、JSON、脚本、不解析等
117			针对正则表达式解析方式，支持选中日志中任意字符串，自动生成正则解析语句，减少人为错误并提升解析速度。
118			针对 JSON 解析，支持自动校验 JSON 格式正确性，并返回 JSON 格式异常原因
119			支持解析字段可以通过映射关系进行别名显示，映射方式有：文本、时间、URI 解码、IP 解码、重定义、正则、映射表等。

120			支持对字段进行加密，无对应权限的用户无法查看字段值。
121			支持统一的映射表管理，支持新建、编辑、导入、导出映射表。
122			▲支持字段解析的自动化智能推荐，根据该日志数据的特点自动推荐匹配优先的对象类型，同时在字段映射时自动推荐靠前的字段类型。系统用不同的颜色提示推荐字段的匹配程度，减少人为选择的错误并提高效率。
123			支持解析规则在线验证，支持客户输入日志样例，在线预览解析结果内容。
124			同时支持向导式简单解析、一站式高级解析模式，支持简单解析模式的规则一键转换为复杂解析模式。
125		内置解析规则	系统需要预置 1000 条以上范式化解析规则，支持解析规则的导入导出。所有解析操作支持可视化的配置界面。
126		标准丰富化	支持针对日志中的源地址、目的地址、主机 IP、日志来源地址这四个字段，匹配系统中存储的资产信息、地理信息（GEO）、网段信息，补全资产、GEO、网段数据至日志、告警中； 支持根据日志中的源地址、目的地址补全二元组信息； 支持根据日志中的源地址、目的地址、源端口、目的端口、传输层协议补全五元组信息。
127		自定义丰富化	支持配置自定义丰富化策略，指定日志中的任意字段，上传映射表，富化出任意字段。
128		地理位置管理	支持配置 IP 的地理位置已覆盖内置的标准地理信息库信息。
129		数据标准	支持属性、对象、事件|设备 3 层结构进行数据标准化。 属性为最底层字段标准；一组拥有相关性的属性构成对象；一组相关性的对象构成事件和设备。 属性、对象、事件|设备均支持客户自定义配置。
130			支持属性配置，系统内置不低于 1000 余种属性满足绝大多数场景需要，例如威胁类型、DOS 攻击、威胁特征、登录类型。同时可以在线配置扩展新的属性字段形成新的标准，包括 IP 型、整型、长整型、浮点数、时间、字符和枚举等类型。
131			支持对象配置，系统内置各类对象，包括：日志对象（威胁、事件等）、计算机对象（主机、流量、文件、进程、驱动、登录等）、安全设备对象（防火墙、沙箱、蜜罐、情报等）、协议对象（TCP、SMB、DHCP、FTP、HTTP、DNS 等）； 系统模块支持数据标准的管理维护功能，包含新建、编辑、删除、导入、导出等操作
132			支持事件配置，系统内置 80+事件，支持配置事件的必选属性、必选属性值
133		数据存储	支持双栈式存储引擎，同时支持高速索引 ES 存储架构、普通索引 Hadoop 存储架构
134			支持基于 Hadoop 分布式文件系统(HDFS)的自研存储引擎，支持 PB 级数据存储； 支持高压缩比存储，压缩比高达 10:1； 支持实时在系统界面查看当前真实的数据压缩比
135		存储管理	支持数据存储高速索引、普通索引分区，并可分别配置高速索引、普通索引存储时间，提高数据查询性能。

136		系统监控	支持监测各节点运行状态，包括节点部署模块情况运行情况，支持点击下钻查看详情包括 CPU、内存、网络、磁盘使用情况； 支持检测各业务模块运营状态，包括所属节点，运行状态，并支持根据业务组件展示核心业务指标，支持点击下钻查看详情，包括更详细的业务指标、节点运行指标。
137		系统监控告警	支持单一界面查看所有系统监控告警； 支持配置系统监控告警项，支持设定是否告警、是否通知。
138	系统设置	云服务更新	支持展示情报订阅、互联网测绘服务订阅、云查杀服务订阅、全景攻防知识库-安全运营库订阅、全景攻防知识库-评估用例库订阅等服务的描述、订阅与否、当前版本、到期时间等信息。
139		云服务配置	支持情报云、TIP 对接配置管理，同时支持资产情报配置展示。
140		审计日志	支持基于每个账户的用户登录、操作动作描述、操作状态、操作结果等行为进行审计。
141		补丁管理	支持手动、自动记录系统补丁记录，支持查看历史补丁记录。
142		通知配置	支持配置邮件、短信、阿里云短信，企业微信，钉钉，webhook 的通知方式
143		用户管理	支持管理本地用户： 支持图形化配置方式与 LDAP 进行集成，同步用户信息；
144		功能分权	支持根据账号角色，配置所有功能界面权限； 权限类型包括：不可见、只读、可编辑
145		数据分权	支持根据账号所属的组织机构配置数据权限； 支持配置任意字段、字段组合进行数据分权； 支持修改用户数据权限并对历史数据生效； 支持针对日志、告警、安全事件、资产脆弱性、UEBA 使用不同的分权条件。
146		登陆管理	支持双因子登录，认证码通过邮件发送，提高账号访问安全性。
147		数据外发	支持配置数据外发,支持使用 syslog_tcp 或 syslog_udp 外发 告警、审计日志
148	产品资质		提供《计算机信息系统安全专用产品销售许可证》资质证书
149			提供《计算机软件著作权登记证书》认证证书
150			提供 IT 产品信息安全认证证书评估保障级（EAL）认证证书
151			提供信息技术产品安全测试证书
152			提供 IPv6 Ready Logo 认证证书
153			提供 2021 至 2022 年连续入选 Forrester 证明材料
154			▲提供入选 Gartner 中国安全运营标杆厂商证明材料
155			▲支持信创环境，并提供鲲鹏-互认证书

3.2 流量探针（APT 威胁检测系统）

序号	主模块	指标项	指标描述

1	产品架构（安装部署）	硬件服务器配置要求	2U 硬件，2 *16 核心 32 线程 CPU，256G 内存，1 * 500G SSD 系统盘+3 * 4T HDD RAID0 数据盘，2 集成千兆电口（管理口）+4 独立千兆电口（业务口）+2 独立万兆光口（业务口），冗余电源。网络吞吐量：应用层 5Gbps；静态文件检测：400 万个/天，动态文件检测：16000/6400 个/天
2	资质要求	销售许可证	要求产品具备销售许可证书，需提供证书电子扫描件。
3		软件著作权	要求产品具备计算机软件著作权证书，需提供证书电子扫描件。
4	产品检测规则	规则库数量	▲至少包括 12 万条黑 DNS 检测规则、2800 条黑 URL 检测规则、1000 条动态域名检测规则、1.4 万条流量检测规则、攻击确认规则覆盖全部告警信息。
5		威胁情报数量	至少包括 300 万条本地威胁情报数据，并支持扩展至 1000 万条以上。
6		黑/白文件 HASH 数	至少包括 200 万本地黑文件 HASH 和 40 万条白文件 HASH，用于快速进行文件检测。
7		动态沙箱行为数据	至少包括 1000 条动态行为规则数，用于沙箱动态文件检测。
8	流量数据采集	网络协议还原	至少支持 31 种网络协议采集和协议还原，包括 ICMP、UDP、TCP、DNS、HTTP、HTTP PROXY、FTP、SMTP、POP3、IMAP、SMB、TLS、SSH、DCERPC、MODBUS、ENIP、DNP3、NFS、NTP、IKEV2、KRB5、DHCP、TFTP、IPV4、IPV6、SNMP、SIP、RDP、TELNET、RIP、NETBIOS。
9		行为数据还原	至少支持对 8 种网络协议进行深度解析，抽取其中重要字段内容，并外发到第三方平台中进行深度分析和溯源取证，协议包括：dns、ftp、http、imap、pop3、smtp、tcp、telnet。 支持设置行为数据请求和响应长度，避免长度过长占用网络带宽。
10		文件还原类型	支持至少 72 种文件类型还原和识别，包括：jse、vbe、ace、hta、sct、xlsm、eml、apk、jar、dps、et、ett、wpt、docm、wps、psl、elf、tgz、gz、htm、html、bin、msi、com、ocx、dll、ppsx、pptx、xlsb、xlsx、mid、wav、iso、tbz2、tar、7z、zip、rar、chm、js、mht、bmp、ico、gif、png、jpg、cmd、sh、py、vbs、bat、sys、exe、rtf、vsd、vsdx、ppt、xls、doc、docx、swf、pdf、wpd、lnk、u3d、class、ttf、mid、wmf、tiff、cab、mst；并且支持自定义扩展文件类型。
11		文件还原协议及方式	支持通过 http、ftp、smb、pop3、imap、smtp 等网络协议还原文件或者邮件附件。 支持对文件进行前置过滤，降低文件还原压力。
12	网络威胁检测	威胁检测分类	支持 11 种威胁事件的一级分类和 118 种威胁事件二级子类，一级分类包括扫描探测、远程控制、拒绝服务、恶意文件、WEB 攻击、APT 攻击、应用程序通信、欺骗攻击、可疑网络行为、威胁情报、漏洞利用；威胁事件二级子类包括挖矿木马、僵尸网络、蠕虫、木马后门、病毒程序、勒索软件、后门程序、病毒程序、SQL 注入、信息泄露、命令代码执行、权限绕过、文件包含、脚本攻击、APT 活动行为、代理软件、网络钓鱼、隐蔽信道、网络设备攻击、移动端设备攻击、弱口令、口令爆破、云端漏洞攻击、可疑 SSL

			等事件类型。
13		告警降噪	支持将流量威胁事件、文件检测事件、威胁情报事件按照源 IP、目的 IP、目的端口、告警规则、威胁情报、时间等维度进行告警聚合，以实现告警降噪。 告警聚合后的降噪率原则上低于原事件总数的 30%
14		分析研判	支持对攻击事件进行自动威胁等级判定，并对其攻击阶段进行判定。
15			提供对攻击事件的详细信息，包括但不限于：五元组（源 IP、目的 IP、源端口、目的端口、协议）、事件类型、攻击阶段、威胁等级、国家、检测信息、漏洞信息、威胁标签、攻击结果、事件次数、网站 IP 地址、响应码、HOST、URL、XFF、XRI、文件名、文件类型、文件来源、文件 MD5、HASH 检测结果、内容分析结果、行为分析结果、YARA 检测结果、机器学习检测结果、关键行为信息等。
16			支持提供威胁事件相关的详细知识库信息，包括但不限于威胁类型、安全分类、威胁描述、影响范围、漏洞说明、漏洞建议等。
17			支持对威胁事件添加研判标签，默认包括研判、误报，或者用户自定义输入值。
18			支持存储威胁事件关联的原始 pcap 信息，并支持在线 pcap 预览，支持 ASCII 和 HEX 方式预览 payload 内容，并支持展示 MAC 地址等信息。
19			▲提供相关攻击手段样例 payload 截图，辅助进行研判。
20			提供解码小工具，能够对 base64、urlencode、hex、unicode 等多种编码进行编码和解码。
21		攻击确认	▲支持通过上下文内容关联分析，对失陷主机、漏洞攻击、WEB 攻击、可疑流量、文件检测的攻击结果进行判定，攻击结果包括但不限于：成功、失败、企图、失陷、失陷+失败通信、失陷+解析失败、失陷+解析成功、失陷+成功通信、可疑、可疑+成功通信、可疑+解析成功、可疑+失败通信、可疑+解析失败等。
22		情报检测	▲支持通过域名、URL、IP 进行威胁情报检测，本地威胁情报的数据不少于 300 万条，支持扩展到 1000 万条。 威胁情报类型包含 APT 攻击、勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件、僵尸网络、常规木马、其他远控等。 威胁情报知识库涵盖情报 IOC 情报状态、恶意家族、攻击团伙、远控类型、解决方案等数据。
23		威胁展示	支持提供可视化界面对网络威胁告警进行展示。 支持对网络告警相关的 payload 进行留存。 提供二进制分析能力和解码工具，支持 HEX 十六进制展示。
24		威胁情报升级	威胁情报可支持在线和离线升级两种方式。
25		WEB 攻击检测	支持 WEB 漏洞检测，包括但不限于：反序列化攻击、SQL 注入、信息泄露、脚本攻击、文件上传、文件读取、权限绕过、目录遍历、命令代码执行、文件包含、目录穿越、SSRF 攻击、CSRF 攻击等。

26		APT 攻击检测	▲支持 20 种以上 APT 特种木马家族的通信特征指令检测，包括攻击目标为中国的组织例如美人鱼、验证器、海莲花、摩诃草、蔓灵花、奇幻熊等。
27		代理软件检测	支持 40+代理软件通信行为的检测，支持 FRP、ngrok、EarWorm、Termite、Dnscat、reGeorg、tunna、reduh 等。
28		远控应用检测	支持 10+常见远控办公应用软件的通信行为监测，包括不限于 todesk、向日葵、teamviewer、RDP 远程桌面、VNC 服务等。
29		端口反弹检测	支持 10+端口反弹攻击行为检测，包括 lcx、NC、rtcp、netcat、socat、portmap、netsh 等黑客工具的端口反弹通信行为。
30		shell 反弹检测	支持 10+各类 shell 反弹行为的检测，包括 BASH shell、telnet shell 反弹、nc shell 反弹、python shell 反弹、perl shell 反弹、ruby shell 反弹、php shell 反弹、socat shell 反弹、curl shell 反弹、powercat shell 反弹、Reverse UDP shell 反弹等通信检测。
31		挖矿活动检测	支持挖矿活动生命周期各个阶段的检测，在侦察阶段，支持对资产探测、端口扫描行为的检测；在投放植入阶段，支持漏洞植入利用行为检测，支持文件传递虚拟沙箱动静态行为预警；在控制阶段，支持僵尸网络、P2P 网络等通信控制行为的检测；在挖矿运行阶段，支持挖矿通信、矿池连接通信行为的检测；在横向移动阶段，支持内网横向漏洞攻击、端口扫描、暴力破解等横向攻击拓展行为的检测。 支持 40+挖矿家族通信特征的告警行为，包括 Blouiroet、xMRig、WMAMiner、CoinMiner、GhostMiner、520Miner 等。 支持多种挖矿通信协议检测，挖矿特征覆盖 Stratum、Getblocktemplate、JSONRPC、ETH_JSONRPC 等协议。 支持 10+种虚拟货币的识别，支持检出的虚拟货币币种包括不限于比特币、门罗币、莱特币、狗狗币、以太坊、达世币、大零币、小零币、奇亚 chia、涡轮币(THP)、云储币等
32		勒索软件检测	支持对勒索软件 IOC 检测，包括程序下载地址、关联域名、IP、URL 等。 通过沙箱支持 100+勒索软件家族的检测。 支持利用诱饵文件技术精准检测勒索软件，支持包括但不限于删除卷影、修改文件后缀、修改桌面背景、加密文件、删除系统日志等 5 种以上恶意文件行为识别。
33		AD 域攻击检测	支持基于域渗透攻击检测，支持 Kerberoasting 票据降级攻击，Kerberos 用户名枚举攻击，dcshadow，dcsync 域敏感信息泄露攻击，smbexec、psexec、wmiexec 远程命令执行攻击，schtasks、AT 远程任务计划访问检测。
34		WEBSHELL 攻击检测	支持 50+常见加密和非加密 Webshell 检测，包括但不限于冰蝎、哥斯拉、蚁剑、中国菜刀、小马上传工具等。
35		敏感信息泄露及未授权页面检测	支持针对个人账号密码、银行卡账号、手机号等明文传输行为的检测。 支持 20+未授权页面接口访问，包括不限于 NPS、Apache Kylin、Zabbix、通达 OA、spring boot、RabbitMQ、Redis、Elasticsearch、Confluence 等未授权页面。

36		僵木蠕类通信特征检测	支持至少 100 种木马家族通信指令特征特征检测，木马家族包括 BrushaLoader、新型 Loader：Buer 恶意软件、Bitter RAT 、Bladabindi aka nJrat、WARZONE RAT、AZORult 窃密木马、Bandook 恶意软件、BetaBot 木马、Avemaria 等。 支持至少 15 种以上僵尸家族的通信指令特征检测，僵尸网络家族信息包括 Avzhan DDoS Bot、Cutwail、Andromeda、Dorkbot、Travnet、PointOfSales、Eclipse DDOSBot、Blue Bot DDoS、Neutrino、Mirai、Muhstik、Tsunami 等。 支持至少 10 以上蠕虫家族的通信特征检测，包括 Conficker、Phatbot、Otwycal、Sohanad、Ngrbot、TheMoon、BlackEnergy 等。
37		暴力破解	支持 30+暴力破解行为监测，包括不限于 SSH 暴力破解、mongodb 认证暴力破解、SMB 暴力破解、sqlserver 认证暴力破解、RDP 口令暴力破解等。
38	恶意文件检测	文件上传	提供标准 API 接口用于上传文件进行检测，支持人工通过 web 批量提交和从网络下载样本检测。
39		邮件附件提取	支持 EML 格式文件检测，能自动提取附件并进行检测，能为每一条文件检测事件提供详细的知识库说明；
40		加密压缩包破解	支持对加密的压缩包进行破解检测，支持用户自定义字典对压缩包解密；
41		压缩包类型数量	支持对常见 9 种压缩包（gz、cab、rar、zip、7z、tar、tbz2、iso、ace）解压检测，支持最多 5 层解压，多层嵌套压缩包解压、可对压缩包内的子文件进行独立检测、对压缩包内存在依赖关系文件进行激活检测；
42		偏移值配置	支持对文件检测特征配置偏移值进行特征匹配；
43		内容检测	支持 AV 检测引擎检测恶意样本文件，支持对 Office 文件、PE 文件等文件内容进行检测，发现漏洞利用、木马、蠕虫、病毒、黑客工具等恶意代码；
44		检测引擎	具备 HASH 检测，杀软检测、CVE 检测、动态行为检测、YARA 检测、机器学习检测、机器学习分类等检测引擎，且每种检测引擎可独立输出检测结果。
45		文件 HASH 检测引擎	具备独立的文件 HASH 库（文件信誉库）检测引擎，支持对文件的 MD5 HASH 进行检测，发现已知的恶意文件，同时文件 HASH 库支持 200+万个以上活跃已知恶意文件 MD5 特征；
46		白文件 HASH 快速过滤	支持内置 30 万以上白文件 HASH 用于快速过滤安全文件，降低性能资源损耗；
47		自定义 HASH	支持自定义黑白 HASH，扩展检测能力；
48		CVE 漏洞检测	支持通过 AV 及动态行为规则检测已知 CVE 漏洞，并输出 CVE 漏洞编号；
49		静态信息提取	支持提取 OFFICE 类文档支持提取宏代码、内嵌超链接并展示；
50			支持 swf 文件提取内嵌 Actionscript 字节码。
51			支持对 PE 文件提取 PE 信息、字符串信息，展示导入 DLL 列表详细函数等信息、资源列表信息、节信息、时间戳；

52		沙箱引擎	沙箱引擎的虚拟机系统支持 Windows XP、Windows 7 操作系统模板，分析环境内置办公软件（office）、PDF 阅读器、浏览器（ IE）、压缩工具（7Z、zip）等常用软件，且支持在不重启系统情况下的实时切换沙箱模版；
53		用户交互行为检测	支持在沙箱中模拟用户交互行为，支持鼠标点击动作，支持应用程序的安装点击操作、应用程序打开运行操作；
54		样本激活方式	支持样本激活方式，其中涵盖：自启动项激活、鼠标模拟点击激活、runonce 自启动项激活、CPI 文件激活、普通类压缩包解压激活、压缩包内存在依赖关系的压缩包解压激活、普通 dll 类加载激活、ServiceMain 类 dll 加载激活、模拟网络激活、html 文件激活；
55		特种木马检测	支持反病毒检测功能，针对特种木马的反病毒检测技术进行检测和处理；
56		勒索软件检测	支持利用诱饵文件识别已知勒索软件样本行为及其家族信息和未知勒索软件样本行为信息。
57		样本行为检测	支持 1000+恶意行为特征其中涵盖：API 规则、进程规则、文件规则、网络规则、IOC 规则、PE 异常规则、其他杂项规则；
58			支持捕获样本的文件操作、进程操作、注册表操作、网络通信、API 调用等详细行为；
59		原始日志提取	支持捕获样本所有原始网络流量并存储为 PCAP 包，支持在线查看 PCAP 包分析取证，至少包括源 IP、源端口、目的 IP、目的端口、16 进制和 ASCII 格式数据包内容；
60		shellcode 提取	支持自动提取样本所释放的衍生文件并进行检测;支持 shellcode 提取，能将 shellcode 反汇编成汇编代码；
61		样本通信行为检测	支持对样本产生的联网行为进行威胁情报检测，发现黑 IP、黑域名、黑 URL 请求行为及记录。
62		YARA 检测	支持用户自己编写 YARA 规则，扩展检测能力；
63		行为分析报告	输出详细的检测报告和原始报告，报告至少包含样本的进程树、样本的屏幕截图、样本的文件行为、进程行为、网络行为、注册表行为、API 调用；
64		逃逸手段对抗	▲支持 100+种以上反逃逸欺骗对抗手段，能够针对特种木马等恶意代码反虚拟机检测技术进行规避，避免恶意代码绕过；如：检测在注册表中搜索 VMware 等字符串的行为、压缩样本“睡眠”时间 等反逃逸欺骗对抗手段。
65		机器学习检测模型	支持至少 5 种及以上机器学习模型，检测 PE、office、PDF 等格式文件；
66		机器学习分类模型	支持通过机器算法对恶意样本分类，分类方式至少包含病木马、后门、蠕虫、广告等 5 种及以上；
67	异常行为检测	隐蔽信道检测	支持发现利用网络合法通信数据包作为载体构建隐蔽通道的数据传输行为，以发现潜在的数据窃密、特种木马控制行为。 支持 HTTP、ICMP、DNS 等 3 种协议隐蔽信道检测，检测模型总数不低于 10 个，包括 DNS 协议 TXT 字段、DNS 域名 Label 长度内容、DNS 协议非法字符、HTTP 中的 Cookie 数据传输 、ICMP 流负载等。 支持受害者 IP、通信协议、隧道服务端、响应信息、通信负载数据、通信时间、检测结果等详细字段展示。

68		动态域名检测	支持通过动态域名规则对互联网中的动态域名请求信息进行记录，以发现潜在未知木马通信行为。 支持动态域名规则总数不少于 1000 个，支持 dnslog、花生壳、洋葱路由 onion、No-IP 等主流动态域名提供商。 支持 DNS 请求发起者 IP、请求 DNS 内容、返回的查询结果 IP 列表以及对应的国家、查询总次数进行记录。
69		DGA 检测	支持通过 DGA 算法生成的 C&C 域名的上线行为的检测。 支持 130W+DGA 域名库的静态检测。 支持基于 LSTM 算法的机器学习 DGA 域名检测。 支持源地址、源端口、目的地址、请求域名、响应结果等事件字段的展示。
70		异常协议检测	支持通过畸形报文，或者利用常用端口传输非常用端口对应的协议等异常流量，以发现潜在代理通道或木马控制行为。 支持 HTTP、DNS 2 种异常协议的检测。 支持源地址、源端口、目的地址、目的端口、PCAP 报文、负载数据、告警信息等详情的展示。
71		异常心跳	支持检测流量中与大量木马心跳行为相似的心跳行为事件，结合威胁情报、业务特性来发现潜在的木马心跳行为。 支持源地址、源端口、目的地址、目的端口、心跳周期、请求域名、参考信息等详情的展示。
72	场景化分析	常见服务登录口令审计	支持对 imap、pop3、smtp、telnet、ftp 等 5 种常见网络登录口令进行审计记录，并根据算法模型判断口令是否为弱口令。 支持判断登录状态，包括成功、失败。 密码信息默认经过敏感信息处理，支持通过二次验证的方式授权查看明文密码信息。
73		访问关系审计	支持审计记录所有网络中的访问请求，并根据方向判断为内对内、内对外、外对内的请求，方便进行快速溯源分析。 支持通过源 IP、目的 IP、访问方向进行聚合，降低审计日志总量，便于分析，并支持查看原始关联的访问请求信息，包括五元组信息、流量大小等。
74		基线检测	支持以时间、IP 地址、端口等维度设置网络中合法的网络互访范围，以便于识别非合规的访问请求。 支持通过源 IP、目的 IP、访问方向进行聚合，降低非合规访问产生的日志数量。 支持查看原始关联的访问请求信息，包括五元组信息、流量大小等。
75		异常访问告警	支持策略事件告警，以时间、策略名称、源地址、源端口、目的地址、目的端口等信息展示。 支持对异常邮箱登录行为、异常 web 访问行为、异常 web 登录、异常文件传输行为和其它异常访问行为配置异常访问策略并告警。
76		邮件内容检测	支持针对邮件正文内容系统内置/用户自定义关键词匹配，以期能够发现钓鱼邮件攻击行为。 支持事件 IP、端口、协议、发件人邮箱、收件人邮箱、抄送地址、时间、告警信息等字段的展示。
77		邮件发件人检测	支持用户自定义恶意发件人邮箱的配置，以期发现钓鱼邮件。 支持事件 IP、端口、协议、发件人邮箱、收件人邮箱、抄送地址、时间、告警信息等字段的展示。

78		邮件附件检测	支持基于邮件附件的检测，包括静态 hash、AV 引擎、动态行为的检测，样本运行产生情报 IOC 匹配，以期发现钓鱼邮件。 支持 IP 协议五元组、收发件人邮箱地址、抄送账户、国家、时间等字段的展示。
79		eml 留存和预览	支持留存原始 eml 格式邮件信息，并提供在线预览功能查看邮件内容。
80		邮件附件解密	▲支持内置引擎对邮件正文、标题中的密码进行识别，并用于邮件附件的解密，提升邮件附件检测率。
81	取证分析	时间序列分析	支持按照时间维度对系统产生的攻击事件和可疑行为进行可视化分析，还原攻击链。 支持对指定的 IP 进行时间维度分析，并支持多重过滤条件，如攻击者、攻击者国家、检测信息、威胁等级、事件类型等 支持下钻指定的事件的详情信息进行研判分析。
82		攻击阶段分析	支持按照攻击阶段（KILLCHAIN）维度对系统产生的攻击事件和可疑行为进行可视化分析，还原攻击链。 支持对指定的 IP 进行时间维度分析，并支持多重过滤条件，如攻击者、攻击者国家、检测信息、威胁等级、事件类型等。 支持下钻指定的事件的详情信息进行研判分析。
83		安全知识库	提供安全知识库功能，能够对网络攻击行为、恶意代码、漏洞等进行详细说明，包括描述、威胁类型、运行平台、来源、参考地址等。
84		实时全流量存储	支持实时全流量存储，并根据指定策略过滤掉不必要流量。 支持 IP、端口、协议、时长、数据包大小等方式对流量存储策略进行设定。 支持对存储的全流量 pcap 文件进行管理，包括下载、删除等。
85		离线 pcap 取证分析	支持本地离线导入 PCAP 文件到系统中进行分析，最大文件大小为 500M。
86	联动处置	syslog 转发	支持通过 syslog 方式上传告警信息、审计信息和系统性能日志信息到外部服务器中。 支持对告警信息进行策略设置，包括事件类型、威胁等级。 支持设置多个转发地址，支持 TCP、UDP 协议通信方式，可指定转发端口。 支持断点重发功能，在异常通信断开之后，再次连接发送上一次的事件。
87		kafka 转发	支持通过 kafka 方式+json 数据格式上传告警信息、审计信息和系统性能日志信息到外部 kafka 集群中。 支持对告警信息进行策略设置，包括事件类型、威胁等级。 支持设置告警长度信息，默认为 2KB。 支持加密通信，支持 AES、SM4 算法加密。 支持断点重发功能，在异常通信断开之后，再次连接发送上一次的事件。
88		元数据转发	支持通过 kafka 方式+json 数据格式外发重要协议字段到第三方平台中，以方便溯源分析和二次检测分析。 支持协议包括：dns、ftp、http、imap、pop3、smtp、tcp、telnet。 支持设置行为数据请求和响应长度，避免长度过长占用网络带宽。

89		snmp 功能	支持通过 snmp 和 snmp trap 方式获取系统基本状态信息，包括 CPU、磁盘、内存、风扇、流量大小、引擎状态、告警总量等信息。 支持 snmp v1、v2、v3 版本。 snmp trap 支持配置多个 snmp 服务器地址。
90	资产管理	被动资产识别	支持被动资产识别功能，能够从流量中识别指定的内网资产，并对资产关联的服务进行识别和记录。
91		业务系统管理	支持设置资产归属的业务系统进行管理，包括新增、删除、修改等。
92		资产管理	支持对自识别资产和手工添加的资产进行管理，包括新增、删除、修改等。 支持批量导入资产信息，支持 CSV 格式导入，资产信息包括资产名、IP、资产类型、操作系统、所属区域、资产登记、归属业务系统、MAC 地址、归属人等。
93	态势分析	威胁态势监控	支持全局威胁态势监控，通过可视化图表的方式展示系统当前的威胁状态，包括威胁总数统计、威胁趋势统计、攻击者 TOP 5、攻击者国家 TOP 5、被攻击者 TOP 5、检测信息 TOP 5、文件 MD5 TOP 5、发件人 TOP 5、收件人 TOP 5、文件来源 TOP 5、XFF TOP 5、被攻击网站 TOP 5、威胁情报 TOP 5。 支持设置统计时间范围，默认为当天。 支持自动刷新，并可设置刷新时间。 支持按照时间维度进行实时告警。
94		重点资产监控	支持对资产进行重点监控，查看指定资产的风险等级。
95		全局态势感知	提供可视化的方式查看全局网络安全态势情况，包括实时攻击路径、威胁总数、威胁事件统计、攻击阶段分布、攻击者 TOP 5、攻击者国家 TOP 5、攻击手段 TOP 5、实时告警等信息。 支持设置统计时间范围，默认为当天。
96	统计分析	安全报告	支持自动化生成安全报告功能，能够根据指定的策略动态生成全网网络安全报告，包括全网态势、总结建议等信息。 支持在线预览报告，以及提供 word 格式报告下载。
97		统计报表	支持自定义时间和类型统计报表查询，能够对指定时间段内，当前系统的所有事件以及指定分类（文件检测、失陷主机、远程漏洞攻击、WEB 攻击检测、异常行为）进行统计分析，并支持在线可视化预览和 pdf 格式文档下载。 支持以邮件形式自动发送报表到指定邮箱中。 支持按照指定周期定时导出统计报表，并支持对导出的统计报表进行管理。
98	配置管理	系统规则管理	支持对系统内置检测规则进行管理，包括规则信息查看（规则 ID、规则名、规则标签、威胁等级）、规则启用/禁用。
99			▲支持对系统内置规则威胁等级进行自定义调整，降低误报。
100		文件检测配置	支持对文件检测进行配置，包括基础配置、检测类型设置、检测特征设置、自定义 YARA 规则配置、压缩包口令破解设置。
101			支持基础设置功能，包括文件检测大小、虚拟执行策略、机器学习结果处理、虚拟机环境切换、虚拟机内网络配置，以及样本下载口令设置等。
102			支持设置待检文件类型，包括是否开启检测、以及是否进入到沙箱动态检测。
103			支持自定义增加文件特征信息，增加文件类型的识别率。
104			支持自定义增加 yara 规则，提升动态沙箱检出率。支持规则管理，包括下载、查看和删除。

105			支持设置加密压缩包口令字典，对加密压缩包进行自动破解。
106		自定义规则	支持用户设置自定义规则，类型包括黑 IP、黑域名、黑 URL、黑流量特征、黑文件 HASH、恶意邮件内容、恶意发件人 黑流量特征支持填写多段特征，并支持设置匹配模式、协议类型、作用域和威胁等级。
107		白名单	支持设置系统全局白名单，类型包括白 IP、白域名、白文件 HASH、白发件箱。
108			支持系统规则白名单，能对指定规则告警进行过滤。
109			支持告警事件白名单，能够对流量检测事件（WEB 攻击检测、失陷主机、远程漏洞检测、可疑流量事件）全字段进行过滤。 支持非操作(NOT)语法，能够对 IP、端口等条件进行排除。
110		邮件告警	支持通过邮件的方式对指定安全事件进行告警，策略包括：事件类型、威胁等级、指定资产。
111		协议还原设置	支持设置文件还原的协议，包括 HTTP、FTP、IMAP、POP3、SMTP、SMB。 支持设置单条流大小，最大 50M。
112		SSL 解密	支持通过上传私钥信息，对 HTTPS 流量进行解密（仅支持 AES 一类加密算法）。 支持设置解密策略，包括域名/IP、网站端口等。
113		检测功能开关	支持对系统内置每个检测功能模块进行启用、停用管理，提升系统性能。
114		产品更新	支持通过离线升级包的方式对系统核心组件进行升级，并记录升级信息。
115		规则库更新	支持通过在线升级和离线方式对系统规则、威胁情报进行升级，支持定时自动在线升级。 支持记录升级信息，包括版本信息、升级方式、升级状态和时间。
116		网络基本配置	支持配置系统管理口网络地址信息，包括手工配置和自动获取。 支持对每个网络接口状态进行查看，包括接口名、状态、当前实时流量、MAC 地址、网口类型和型号，并支持启用/禁用操作。 提供网络诊断功能，判断指定主机的存活情况。
117		可信主机登录	支持可信主机登录控制功能，限制只有可信 IP 才能访问系统 WEB 服务。
118		SSH 服务开关	支持 SSH 登录服务开关功能，可以根据需要开启或关闭 SSH 服务，以及设置 SSH 端口号。
119		网络代理配置	支持 HTTP PROXY 和 SOCKS5 代理方式，实现系统版本和规则库升级，以及文件检测中远程文件下载。
120		内网配置	支持设置内网 IP/IP 段，用于内网地址判定。
121		用户管理	支持对系统用户进行管理，包括增删改查、解锁用户、重置用户密码等。
122		三权分立	支持三权分立管理，用户角色包括操作员、审计员/审计管理员、管理员。
123		密码规范修改	支持设置用户密码规范，可以设定用户密码策略，包括复杂度、最小长度、最大长度、密码有效率、自动锁定次数、锁定时间。
124		时间与日期	支持设置手工设置和 NTP 同步系统时间。
125	系统管理	系统状态	支持对系统状态进行查看和管理，包括实时镜像流量图、CPU/内存/磁盘状态信息、系统各个引擎状态。 支持对系统进行关机和重启操作，支持对各个系统引擎进行关闭和重启。

126		日志审计	支持对系统重要操作进行审计，并记录审计日志。 支持设置系统审计日志策略，能够设置最大审计日志条数，超过最大条数后进行删除。
127		系统备份	支持自动备份和手动备份系统检测相关数据，并提供备份文件管理。
128		系统清理	支持自动和手动方式清理系统中存储的文件、pcap 等数据。 支持磁盘告警设置，可设置告警事件、清理阈值、自定义时间类型。
129		系统还原	支持对导出的备份文件进行数据还原。 支持恢复到系统初始化状态。
130		系统授权	支持查看系统版本信息以及授权情况，并支持更新授权。

3.3 资产威胁与漏洞管理平台

序号	主模块	子模块	指标项	指标描述
1	资产	IT 资产测绘	IP 存活探测功能	支持内外网 IPv4 和 IPv6 探测，并可自动标记内外网，自动识别 IP 的类型（IPv4/IPv6）
2				支持 TCP、UDP、ICMP 等多种探测方式，支持 TCP 响应超时自动重发、速率自适应动态调整等。
3			域名解析 IP 探测功能	▲支持对近 3 年内主域名所关联的全部子域名解析 IP 结果的收集，提供解析 IP 的首末次解析时间，支持子域名的检出率达到 97%以上
4				支持对域名的状态标记，可以标记域名已停用、使用中的状态。
5				支持通过 A 记录/AAAA 记录解析 ipv4/ipv6 地址。
6				支持针对域名解析结果进行泛解析清洗，支持通过已知的泛解析后缀和域名解析特征识别泛解析数据，并自动过滤泛解析数据。
7				支持基于 CDN 情报库识别 CDN 地址，可标识出是 CDN 的解析记录，CDN 情报库数量≥45 万。
8			开放端口探测功能	支持对 TCP、UDP 协议端口开放性探测，支持对比端口历史开放情况自动调整重探策略提升端口探测稳定性。
9				支持指定端口范围探测，包括常用端口、全量端口探测，并支持常规端口的预置模板。
10				支持探测扫描速度配置，可以选择配置端口扫描策略，并且支持自定义设置扫描并发数。
11				支持全量端口开放探测准确率不低于 95%。
12			网站资产探测功能	支持 dig、ping、curl 等多种方式探测网站可用性。
13				▲支持网站子 URL 的爬取，并形成网站地图。支持标记来源，来源至少包括爬虫、被动流量、情报等。支持限制爬取的目录层数（不低于 5 级）、单个路径下文件数量（不少于 50 个文件）、爬取 URL 总数（不少于 3000）、能够过滤特定类型的 URL（如图片、样式表、字体等），支持对网站地图中爬取到的特殊 URL 进行自动化标记，至少包括 API 和管理后台标记。
14			协议识别功	支持识别协议和服务的名称、版本等信息。

15			能	支持探测过程多步交互，支持探测 SOCKS4、SOCKS5、HTTP 代理等代理服务。
16				支持不少于 10 种物联网协议，至少包括 AMQP、MQTT、STOMP、XMPP、JMS、DDS、COAP、REST 等
17				支持不少于 30 种金融行业专有协议，至少包括：探测通达信、同花顺、易盛极星等。
18				支持不少于 10 种国产信创协议识别，至少包括：达梦、人大金仓、神通等。
19				支持不少于 1000 种应用及服务类协议探测识别，至少包括：HTTP、HTTPS、FTP、TFTP、LDAP、SMTP、UPnP、IMAP、POP3、MYQSL 等。
20				支持不少于 30 种工控协议探测识别，至少包括：BACnet、CoDeSys、DNP3、Siemens S7、IEC-60870-5-104 等。
21				网络资产协议识别支持特殊处理机制，具有超时处理机制、数据增量更新机制增强协议识别能力。
22			资产指纹识别功能	支持识别资产的名称、厂商、版本等信息。
23				支持通过回包信息指纹比对方式实现设备类资产准确识别，至少包含基于报文信息（TCP、ICMP、HTTP 等）指纹比对、基于 banner 信息指纹比对、基于交互信息指纹比对的方式进行识别。
24				支持 40000+种应用及设备指纹特征（同一设备不同版本记为 1 种指纹），其中： 1）路由交换指纹≥1000 种；打印机指纹≥300 种；摄像头指纹≥200 种；网络存储≥120 种，工控设备≥100 种，挖矿应用≥20 种，CDN≥50 种。 2）编程语言指纹≥20 种；JavaScript 库≥1500 种；开发框架 指纹≥150 种；应用服务指纹≥10000 种。 3）重点行业指纹≥5000 种。
25				指纹涵盖对象类型≥80 大类。包括但不限于网络设备、安全设备、工业控制设备、网络打印机、网络投影仪、网络摄像头、邮件服务器、认证服务器、数据中心、数据库服务器、云服务资源、操作系统类、网页技术类、应用服务类、中间件类等。
26				支持按照应用层、支撑层、服务层、系统层、硬件层五个层级来划分指纹识别的资产信息。
27				▲支持国产化设备的指纹特征识别，支持 3000+种国产化指纹，其中包括： 1）达梦、人大金仓等国产数据库的指纹≥10 种； 2）东方通等中间件的指纹≥10 种； 3）华为、海康威视等国产监控设备≥200 种； 4）金蝶 OA、致远 OA 等国产业务系统指纹≥500 种； 5）360 天擎、天融信防火墙、启明 IDS 等国产安全设备指纹≥500 种；
28				能够识别的行业种类：≥30 种，至少包括交通、证券、银行、电信、电力等业务网络的识别能力；
29				识别设备的类型、厂家、品牌、型号的准确率≥85%；识别软件的类型、版本、开放服务的准确率≥85%；
30			操作系统识别功能	支持识别 Windows、Linux 、Unix、MacOS 等通用操作系统，网络操作系统、嵌入式操作系统等≥50 种操作系统能力。

31				支持识别国产信创操作系统识别≥20 种，包括但不限于：中标麒麟、统信 UOS、银河麒麟、中科红旗等。
32		IT 资产管理	资产变更监测	▲支持动态资产变更检测，可识别新增 IP、新增端口、新增 URL、组件变更、资产存活性变更。
33			资产变更自动确认	支持基于规则的新增资产自动确认，支持通过资产来源、内外网、情报信息、网站 title、端口号、地理位置的资产信息设置自动确认条件，支持同时设置至少 10 个自动确认条件。
34			资产分组分类	支持多层级资产组划分资产，至少支持 10 层资产组的设置与管理。
35				支持以业务系统划分资产，支持重要资产标记。
36			资产智能增删	支持资产的一键智能增删，可以通过配置资产范围智能判断需要保留、新增、删除的资产，并全量替换系统内管理的资产。
37			资产标签	▲支持基于资产指纹为资产自动添加标签，包括但不限于：云主机、防火墙、管理后台、API 等，支持自定义配置新增资产标签自动识别的规则。
38			资产关联	支持内外网资产关联、ip 与网站关联、ip 与业务系统关联、网站与业务系统关联，并可基于内网 ip/外网 ip/未关联 ip 的维度查看资产关联情况。
39			高危端口服务识别	支持高危服务协议与高危端口识别，在系统中重点标注，并支持自定义配置高危服务和高危组件。（需区分内外网）。
40			自定义拓展字段	支持 ip 资产的自定义拓展字段，可以自定义字段名称至少可自定义拓展 10 个字段。
41				支持网站资产的自定义拓展字段，可以自定义字段名称至少可自定义拓展 10 个字段。
42			资产自定义导出	支持 IP、端口、url、域名的自定义字段导出，IP 和 url 还可支持拓展字段的自定义导出。
43			IP 资产变更记录	支持记录 IP 资产变更信息，通过变更内容（包括但不限于端口 up、down）和变更时间形成 IP 资产变更时间线。
44			资产数据权限控制	支持设置用户可以管理的资产范围，能够限制用户只能管理资产范围内的资产和这些资产对应的威胁。
45		移动资产测绘	公众号发现	支持根据企业关键词发现企业相关微信公众号的基本信息，需包括但不限于公众号名称、状态、类型、绑定微信号、认证主体、统一社会信用代码、服务提供商、公众号简介、最后更新时间、功能菜单名称、功能菜单状态、功能菜单链接和功能菜单类型。
46			小程序发现	▲支持根据企业关键词发现企业相关小程序的基本信息，需包括但不限于小程序名称、状态、小程序 ID、APPID、认证主体、统一社会信用代码、服务提供商、小程序简介、最后更新时间和业务域名清单。
47		数据泄露监测	网盘监测	支持基于关键词监测百度网盘、新浪微盘、微云网盘等至少 6 个不同网盘来源的数据信息，信息内容需包括但不限于文件名称、来源、关键词、上传者、上传时间、文件大小、链接地址、提取码、简介、标记。
48			文库监测	支持基于关键词监测百度文库、csdn、oschina 等至少 45 个不同文库来源的数据信息，信息内容需包括但不限于文件名称、来源、关键词、上传者、上传时间、链接地址、简介、标记。

49			代码托管平台监测	支持基于关键词监测 GitHub、码云的相关数据信息，信息内容包含但不限于仓库名称、仓库简介、作者、语言、关键词、状态、最后更新时间、来源、标记、泄露文件内容。
50			暗网监测	▲支持基于关键词监测暗网中的相关数据信息，信息内容包含但不限于主题、帖子详情、作者、创建时间、发现时间、匹配关键词、链接地址、标记，且支持提供暗网交易快照的查看。
51		供应商管理	内置供应商库	支持内置供应商识别，提供≥10000 内置供应商库信息，需包括供应商的名称、是否信创厂商、是否国内厂商等信息。
52			资产自动关联	支持通过指纹识别结果自动关联资产与供应商之间的关系，并能在供应商中查看资产关联。
53			供应商管理	支持按照设备、组件、业务系统、操作系统 4 个维度查看供应商关联信息，并可基于供应商数据统计关基业务系统的资产国产化率。
54	威胁	威胁检测	漏洞检测	支持对 IPv4/IPv6/网站资产的脆弱性探测识别能力，支持对资产进行系统漏洞与应用漏洞的探测。
55				支持根据 CVE 漏洞编号、Bugtraq 漏洞编号、CNVD 漏洞编号、CNNVD 漏洞编号、国内外主流扫描器漏洞编号、漏洞名称以及威胁等级进行查询，系统收录的漏洞库融合后总数≥20 万条。
56				支持对 1day 漏洞进行 POC 检测，系统提供 POC 数量≥5000，其中： 1）高危漏洞插件≥1000 个，其中命令及代码执行漏洞≥400 个，SQL 注入漏洞≥500 个。 2）插件应覆盖常见应用，其中办公系统漏洞插件不少 400 个，安全设备漏洞插件不少于 300 个。
57				POC 插件需至少支持国产信创应用漏洞检测，国产信创应用漏洞≥500 个。
58			弱口令检测	支持对资产进行弱口令检测，可以自定义配置弱口令字典，可检测的资产类型≥50 种包括： 1）常规的协议，至少包括:FTP、SSH、TELNET 等 2）数据库，至少包括：mysql、oracle、mssql 等 3）常规应用，至少包括：Apache Tomcat、weblogic 等 4）web 应用，至少包括：zabbix、路由器 web 管理等
59		漏洞情报	1day 漏洞情报推送	▲支持在 1day 漏洞爆发的 24 小时内进行漏洞情报实时推送（需联网），且能针对新披露的高危 1day 漏洞自动匹配预估受影响资产数据，明确受影响范围。
60		威胁管理	漏洞闭环管理	支持将漏洞指派给系统用户，用户能录后能够查看分配给自己的漏洞并能进行二次分配。能够设置漏洞的过期时间，并在漏洞过期加以标记。
61				支持漏洞全生命周期管理，对漏洞状态和处置流程进行跟踪，如新增、遗留、减少、已加固、误报、待复测等，并能对漏洞状态分布、业务分布等进行统计，掌握信息系统漏洞整体状况。
62			白名单管理	支持漏洞白名单功能，加入白名单后所有页面统计实时生效过滤白名单漏洞。
63				支持基于规则的漏洞自动白名单，支持通过漏洞名称、漏洞等级、关联 IP、关联网站等规则设置自动白名单条件，支持同时设置至少 10 个自动确认条件。

64			告警管理	支持告警线设置，根据资产范围、事件类型、威胁级别自定义告警线。
65				支持在新增高危漏洞、高危漏洞超过阈值、弱口令数量超过阈值、漏洞情报有关联资产时进行告警。
66				支持通过邮件发送告警信息。
67	可视化	大屏可视化		支持大屏可视化展现关基业务信息，需要有关基设备统计、关基资产风险数量统计、关基资产走势统计、关基业务的风险统计、关基业务（供应商、设备、操作系统）的国产化率统计、关基设备的操作系统统计、关基资产的数据库统计以及供应商统计。
68		历史数据对比		支持端口、漏洞检测数据和历史数据比对，判断是否为新增端口/漏洞。
69		内置安全场景视图		▲支持多维度分析，提供自定义安全场景视图。视图种类不少于 25 种，支持视图自定义拼接。
70	任务	智能任务模式		支持智能任务模式，智能任务模式可以自动根据当前系统内资产与威胁的情况智能编排测绘与威胁检测涉及到的所有任务的执行步骤与顺序。
71		任务风险控制		支持自定义设置任务禁止检测时间，在禁止检测时间内所有任务不执行检测。
72				支持自定义配置检测白名单，检测白名单内的资产将不会进行扫描。
73				支持自定义扫描强度配置，支持轻量、常规、深度扫描强度的配置。
74				支持自定义扫描任务并发数，支持自定义配置任务并发数的最大阈值。
75		任务管理		支持通过单个资产、业务系统、应用组件、负责人等多种方式过滤资产范围并下发漏洞检测任务，提高任务检测灵活性。
76				支持任务的暂停、恢复、强制结束，并支持查看运行中任务的任务进度。
77				支持单次或周期性检测任务，能够按月、周、日、时、分灵活组合配置任务检测周期 。
78	报表	自动报表		支持资产威胁变更日报，并能根据设置自动发送至相应用户邮箱。
79				支持按周期（周和月）自动生成 Word 格式资产威胁态势报告。
80		自定义报表		支持根据一个月以内的资产数据生成 word 格式的报表。
81	国产化适配			支持 ARM 架构下的鲲鹏、飞腾 CPU 的适配。
82				支持统信 UOS、银河麒麟的国产化操作系统的适配，需提供适配证书。
83				支持东方通的国产化中间件适配。
84	资质要求	软件著作权	软件著作权	提供《计算机软件著作权登记证书》
85		销售许可证书	销售许可证书	提供《计算机信息系统安全专用产品销售许可证》资质证书
86		CNNVD 兼容认证	CNNVD 兼容认证	▲提供中国信息信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）兼容性资质证书》。

87		国产化兼容认证	鲲鹏	▲提供华为云计算技术有限公司颁发的产品兼容性证书。

3.4 数据安全管理系统

序号	主模块	指标项	指标项描述
1	数据态势	数据资产态势	支持针对数据资产发现，能够支持 18 种以上常见数据存储类型,例如:MongoDB、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、Redis、ElasticSearch、DB2、Clickhouse、Hive、GreenPlum、MariaDB、Informix、Oracle、SQL-Server、Opengauss、Kafka 等
2			支持从数据库审计流量中发现数据库资产，包括：资产类型、数据库 IP、数据库端口
3			支持数据资产管理，资产组可以根据:安全域、业务系统、物理位置、组织机构等其它自定义类型进行划分，并且指定资产组责任人.
4			支持数据资产维护属性有:数据库 IP、数据资产类型、版本号、用户名、密码、负责人、负责人电话、部门、机房属性，并可进行连通性测试.
5			支持数据资产脆弱性评估,包括：脆弱性名称、漏洞类型、处置状态、资产 IP、端口、威胁等级、最新发现时间
6			资产生命周期，包括：资产变更类型统计、资产敏感程度统计、添加时间等
7		分类分级态势	▲支持三种数据源类型按行业分类分级运行，包括针对数据库、API、文件 3 大类;
8			支持内置行业分类分级标准，并配套行业分类分级规则，并支持自定义分类与分级；并能够切换系统当前生效行业标准
9			支持分类分级文件类型包括: 支持常见文件 28 种:txt，html ，doc，docx，docm，dotx，dotm，xls，xlsx，xlsm，xlt，xltx，xltm，ppt，pptx，ppsx，ppam，potm，ppsm，pptm，pdf，csv，wps，wpt，et，ett，dps，dpt 支持源文件类型 7 种：java，cpp，c，sh，sql，xml，py 支持压缩文件 6 种：7z，zip，tar，gz，bz2，xz 支持图片类型 4 种：jpg，png，bmp，tif 支持音视频文件 3 种：Mp3，flac，wma
10			支持按行业进行分级名称定义，例如:1-5 级分别定义为:一级、二级、三级、四级、五级别名显示，并可新增级别
11			支持按行业分类进行配置规则，规则支持按数据库、API 接口、文件类型进行区分，并可配置生效时间、失效时间、
12			支持按逻辑表达式定义分类分级规则，例如:>、<、>=、<=、==、!=、contains、not contains、memerOf、not memberOf、matches、not matches、()括号等达式进行逻辑条件进行运算，并且支持界面自动生成逻辑表达式语法结构.

13			▲支持即时调度与周期性调度，包括：调期性调度包括：每小时、每天、每周、每月，并可指定开始调度时间；所有调度任务把分类分级结果自动合并到统一库中，可以按:数据库、API、文件(图片)对象进行分类结果分析
14			针对数据库分类分级结果结构化查看，可以按数据资产、库、表、列维度进行查看，可以直观看出数据库、表的敏感分类与级别、敏感数据数量，并且可以看到所在库和资产的敏感级别
15			支持快速手工修正分类分级结果，调整分类时自动带出分级．并进行自动打上确认标志
16			▲支持针对分类分级的结果生成数据DNA功能，把手工分类后的数据进行数据基因保存
17			支持针对分类分级的结果生成数据DNA功能，把手工分类后的数据进行数据基因保存;支持数据 DNA 文件管理，针对 DNA 中的数据进行复核、确认、生效,以及重新导到新版数据 DNA
18			支持云端按行业自动下载数据 DNA 文件,获得最新的 DNA 基因数据
19		数据流转态势	数据流转过程：关联数据库访问与业务系统访问行为，展示从用户到应用到数据库的完整流转过程
20			终端文件流转：关联终端文件流转过程，包括文件来源、终端用户、文件分享操作方式
21			支持流转统计：数据库访问次数排行、数据库脱敏次数排行、数据库操作类型排行、应用访问次数、流动数据类型分布、终端用户违规外发方式、用户文件终端操作
22			数据流向分析，包括：支持从数据库、敏感数据、数据库用户、终端用户等角度，查看数据流向。
23			支持从数据资产的角度，追查相关的可疑人员，查看数据资产在一段时间内曾经有多少人做过风险操作、对哪些数据表做了操作，列出相关日志证据。
24			支持从数据库用户、终端用户的角度，查看用户访问过哪些资产，操作了哪些敏感数据，以及攻击者的影响范围。
25			支持数据库脱敏分析，包括：源数据库 IP、目标数据库 IP、脱敏算法、启动时间、运行时间；例如，在“从正式库导出数据到测试库，供开发人员测试”的场景下，企业用户可以查看一段时间内，数据库间进行过几次导出，每次导出是否做了脱敏，以免开发人员直接将敏感数据偷走。
26		数据风险态势	支持安全事件，并对安全事件的分析、处置状况进行管理。对每个安全事件进行跟踪分析，查看原始日志、相关资产的画像、攻击链路的分析，根据研判结果进行及时处置，填报处置措施和结果。
27			支持合并告警，满足检索条件的所有合并告警进行实时统计，包括不限于，合并告警级别、数据、趋势、受害主机 top、 攻击源 top、攻击类型 top 等，并可下载符合条件的告警。
28			支持数据风险场景，包括:账号爆破、弱口令、邮件威胁、IP 威胁情报等数据安全威胁场景
29			支持针对攻击者分析，包括:高频攻击源、攻击者地理位置、攻击阶段统计等

30			支持风险资产分析，包括:高风险资产、告警影响、风险资产数、已失陷资产数、主动攻击资产数
31		终端数据态势	▲支持泄密文件溯源，包括：终端 ID、设备名称、设备 MAC、文件名称、文件 MD5、违规操作次数
32			▲支持终端违规外发，支持按内容、文件名称、时间段进行搜索、统计违规外发方式、违规外发次数
33			支持终端文件操作，包括：本地文件操作、网络文件操作、外设文件操作三大类
34			支持终端打印告警，包括：设备名、设备 MAC、文件名、文件路径、违规类型、风险级别、风险时间
35			▲支持对敏感文件的使用和流转过程进行追溯，查看哪些人对该文件做过违规编辑、改名、违规外发（QQ、微信、移动存储设备、蓝牙、FTP、Http/Https、SMTP 等）、违规打印等操作
36		数据合规态势	呈现企业合规工作的整体态势，进行多部门合规建设工作的协调管理。
37			支持合规概况跟踪与统计：展示待整改系统数量、合规要求满足度、现存漏洞数、已评测系统数、即将到期排行、待整整项数量、各法规满足度排行、责任人待整改排名
38			支持法规有:等保一二三四级、数据安全法、个人信息保护法、网安法、电信互联网数量安全相关法规
39			支持业务系统与合规标准、资产对象、责任人进行关联，并可以设置完成时间以限定完成日期
40			针对每个评测项目可以批量编辑完成状态、原因、上传合规附件、按分类统计完成数量、导出报告等操作
41		综合态势大屏	支持 7 个以上的态势大屏，包括数据综合态势大屏、威胁攻击态势大屏、资产安全态势大屏、安全事件态势大屏、安全成果态势大屏、威胁情报态势大屏、运行监控态势大屏
42	大数据平台	数据采集&解析	支持本地文件、目录、Syslog、SNMP-TRAP、Netflow、数据库、Kafka、HDFS、ElasticSearch、SFTP、WMI、SNMP 协议格式
43			支持数据标准的属性配置，系统内置不低于 1000 余种属性满足绝大多数场景需要，例如威胁类型、DOS 攻击、 威胁特征、登录类型。同时可以在线配置扩展新的属性字段形成新的标准，包括 IP 型、整型、长整型、浮点数、 时间、字符和枚举等类型。
44			支持通过选择映射的方式由定义的属性字段组成生成各种对象来归类管理，避免手动直接编辑导致的错误配 置，满足各种分析层面的需要，包括日志对象(威胁、事件等)、计算机对象(主机、流量、文件、进程、驱 动、登录等)、安全设备对象(防火墙、沙箱、蜜罐、情报等)、协议对象(TCP、SMB、DHCP、FTP、 HTTP、DNS 等)
45			对解析标准化后的数据进行信息的丰富化，包括:二元组、五元组、资产、经纬度信息
46		大数据平台存储	支持 ElasticSearch、Kafka、网络转发、数据转发、CCS、HDFS、本地文件方式
47			支持数据存储温、热分区，并可分别配置冷、热存储时间，提高数据查询性能。

48	安全运营策略	规则关联分析	支持单一关联:基于日志、告警、资产、情报、漏洞等范式化后的单个事件的单一字段(如事件名称或某个特定字段)进行关联，触发产生告警
49			支持复合关联:复合关联分析是指关联单个事件的多个字段形成 更加准确的告警，支持对日志、告警、漏洞、情 报等规范化后的基础字段、富化属性及标签，进 行 2 个以上字段的多条件关联。
50			支持统计关联:统计关联是对日志、告警、漏洞、情报等规范化 后的基础字段、富化属性及标签进行统计计数， 在时间阈值内符合某种统计特征形成分析结果。 如一分钟内登录 3 次。
51			支持时序关联:时序关联是存在时序先后关系攻击行为进行多事 件关联分析，支持日志、告警、漏洞、情报等规 范化后的基础字段、富化属性及标签进行 XDR 复杂关联分析，实现复杂安全事件在逻辑层面的自动化检测分析。
52			支持时序关联:非时序关联是对没有强时序关系但具备某种相同特征的行为进行关联，支持日志、告警、漏洞、情报等规范化后的基础字段、富化属性及标签进行关联分析。
53			支持互拆关联:互斥关联是 A、B 两件事是不可能同时发生的情 况进行关联，一般用于对串行设备行为的判定， 支持日志、告警、漏洞、情报等规范化后的基础 字段、富化属性及标签进行关联分析。
54			支持反向关联:反向关联指对限定时间内，特定事件未发生的情况进行关联分析
55		事件聚合	支持自动化威胁猎捕模型，可在线编写脚本语言算法模型模拟分析人员溯源取证的过程，基于告警事件为入口触发条件的威胁场景自动溯源分析，向前、向后自动抽取若干分钟、小时和天为单位的数据，结合时间、过滤条件关联，多层逻辑嵌套、自动聚合分析包括日志、流量、告警等内容，聚合跨阶段展示整个威胁事件。
56			支持将告警按照整个事件的攻击链、攻击方向聚合及攻击时间轴排序，整合为一个事件的完整攻击链阶段。并根据聚合事件的安全评分模型化动态评估威胁数值，模型维度包括不限于告警数量、告警等级、攻击阶段、威胁情报。
57			支持威胁的持续性评估，随攻击发展持续聚合相关告警，动态调整威胁数值。
58			支持新增模型后，可对已有历史数据进行规则验证或利用规则针对历史数据进行威胁追踪发现。通过场景任务编排可以实现历史数据的回扫，用新的线索挖掘风险。支持历史时间跨度选择、过滤条件配置、验证任务的启停等。
59	日志与告警	智能日志检索	支持三种检索模式, 分别是: 场景化检索、综合检索、高级检索
60			支持单一界面统一检索日志、告警、事件、资产、脆弱性、安全风险、安全预案执行情况等多类型数据。
61			支持在主查询语句中嵌套子查询语句
62			多查询语句的管道连接，以支持复杂场景。管道支持任意级别
63			支持 1000 个以上函数调用, 包括对字符串、数字、时间等类型的参数进行常见函数调用

64			支持数值计算，包括：平均值、计数、去重计数、最大值、最小值、差值、求和等统计聚合函数
65			支持 search、where、eval、bucket、stats、sort、join、fields、head、top、format、append 等搜索命令进行各种统计操作
66			▲支持 API 接口调用这些查询、统计操作指令，以提供给其它产品的数据接入能力.
67		合并告警	支持通过 key-value 模式或类 SQL 模式进行合并告警检索。
68			支持对满足检索条件的所有合并告警进行实时统计，包括不限于，合并告警级别、数据、趋势、受害主机 top、 攻击源 top、攻击类型 top 等，并可下载符合条件的告警。
69			支持查看合并告警详情:包括不限于合并告警基础信息、攻击者详情、受害者详情、原始告警。
70			支持查看未处置的同类告警，便于批量处置。
71			支持查看已处置的同类告警历史经验，可以参考或者进行重新研判，支持展示历史处置记录，已提供分析、处置参考。
72	威胁情报	威胁情报	可以开通云端情报更新模块，自动同步云端情报信息
73			本地安全事件可以关联事情中恶意 IP、域名等情报信息
74	展示及报表	仪表盘	支持自定义各类图表并进行权限控制，支持公开、不公开。
75			支持自定义仪表盘配置，根据需要添加不同的监控组件，自定义选择过滤条件和过滤条件组的监控组件添加、 修改和删除。
76			支持同时组合多种展示图形，如柱状图、饼图、面积图、趋势图、表格、统计、同比、环比、百 分比、复合计算统计、上传图片、外部图片、外部网页等，可配置排序方法、TOP 数量、数据时间跨度。仪表盘的图形位置和大小支持自由拖拽，所见即所得。
77			支持从仪表盘下钻至具体事件、告警、资产等并且可直接配置下钻选项，支持跳转到自定义的其它仪表盘，实 现仪表的嵌套来满足分析需要。
78			支持仪表直接调用 SOAR 预案来快速处置，支持仪表的内容通过点击快速变为过 滤条件。
79		攻击热力图	▲支持知识图谱技战术热力图，展示 360 全景攻防知识图谱，包括:侦察、资源部署、初始访问、执行、持久化、权限升级、防御逃逸、凭据访问、发现、横向移动、采集、命令与控制、数据渗漏、恶劣影响等阶段，进行关联威胁事情发生位置与数量
80			▲支持点击攻击技术，查看详情，包括不限于子技术、技术描述，相关安全事件等
81			▲支持 Mitre ATT&CK 之外扩展出具备中国特有的技战术总结。
82		智能报表	持报表和报表模板管理，可自定义报表和报表模板，区分不同类别报表。
83			支持从原始日志与流量、安全设备告警、平台关联告警以及安全事件输出多个层面自动呈现统计数据。

84			支持对概况、事件、IP 地址、端口、服务、事件严重程度、攻击种类、用户等数据进行统计。
85			报表内容支持自定义编辑，直接引用图标、文本、链接、图片、宏变量、嵌套报表、外部网页等元素。
86			报告中数据支持统计查询与过滤条件满足与、或、非、In、Not In、exist、like 字符串匹配、rlike 正则匹配等基 础组合。
87			支持报表图形化结果展示包括但不限于柱状图、饼图、面积图、趋势图、表格、统计、同比、环比、 百分比、复合统计等。
88			支持周期性(每日、每周、每月)自动生成报表并通过邮件发送、下载、导出等方式获取。
89			支持导出 WORD/PDF/HTML/EXCEL 等格式，报告可指定人员进行分享。
90	产品资质	销售许可证	提供《计算机信息系统安全专用产品销售许可证》资质证书
91		软件著作权	提供《计算机软件著作权登记证书》

▲项汇总表

序号	具体指标
安全运营平台	
1	▲针对原始日志检索结果，支持一键跳转原始日志相关的威胁告警、安全事件。
2	▲在联网场景中，非威胁情报类型的告警详情中管理的外网 IP 支持情报富化，如命中可展示地理位置、运营商、AS、ASN、网络类型、匿踪类型、情报风险等级、情报风险类型、威胁类型、置信度、阻断系数、处置建议等信息
3	▲支持关联规则根据数据标准进行规则编写的自动化推荐，系统根据事件类型自动推荐其所属的对象，并且会自动判断规则内容是否与该对象匹配。
4	▲支持抽取安全事件中支撑分析研判的证据进行集中展示； 支持证据跳转相应的告警查看完整上下文； 支持的证据类型包括不限于：威胁情报、恶意样本鉴定结果、威胁特征。
5	▲支持自动化威胁猎捕模型，可在线编写脚本语言算法模型模拟分析人员溯源取证的过程，基于告警事件为入口触发条件的威胁场景自动溯源分析，向前、向后自动抽取若干分钟、小时和天为单位的数据，结合时间、过滤条件关联，多层逻辑嵌套、自动聚合分析包括日志、流量、告警等内容，聚合跨阶段展示整个威胁事件。
6	▲系统模块内置病毒扩散聚合模型，以内网主机发起特定端口扫描后并对该端口进行攻击的告警为切入点，聚合向前 10 小时向后 2 小时的威胁情报的告警、向前 3 小时向后 2 小时的基于漏洞的告警、向前 3 小时向后 2 小时的主机网络连接行为，系统自动对以上多源信息进行校验和聚合，生成外网利用漏洞攻陷内网主机后进行蠕虫传播的安全事件。

7	▲支持使用系统内置情报或手动上传的情报包对历史数据进行回扫，排查历史攻击行为； 支持手动创建回扫任务或者配置自动回扫任务； 支持设置回扫威胁情报类型、回扫情报严重级别，回扫时间范围，回扫任务开始时间； 支持查看回扫任务结果，包括不限于回扫 IOC 数量，回扫命中 IOC 数量、回扫告警数量、回扫受害者数量，支持查看回扫告警详情。
8	▲支持 Mitre ATT&CK 之外扩展出具备中国特有的技战术总结。
9	▲支持字段解析的自动化智能推荐，根据该日志数据的特点自动推荐匹配优先的对象类型，同时在字段映射时自动推荐靠前的字段类型。系统用不同的颜色提示推荐字段的匹配程度，减少人为选择的错误并提高效率。
10	▲提供入选 Gartner 中国安全运营标杆厂商证明材料
11	▲支持信创环境，并提供鲲鹏-互认证书
流量探针（APT 威胁检测系统）	
1	▲至少包括 12 万条黑 DNS 检测规则、2800 条黑 URL 检测规则、1000 条动态域名检测规则、1.4 万条流量检测规则、攻击确认规则覆盖全部告警信息。
2	▲提供相关攻击手段样例 payload 截图，辅助进行研判。
3	▲支持通过上下文内容关联分析，对失陷主机、漏洞攻击、WEB 攻击、可疑流量、文件检测的攻击结果进行判定，攻击结果包括但不限于：成功、失败、企图、失陷、失陷+失败通信、失陷+解析失败、失陷+解析成功、失陷+成功通信、可疑、可疑+成功通信、可疑+解析成功、可疑+失败通信、可疑+解析失败等。
4	▲支持通过域名、URL、IP 进行威胁情报检测，本地威胁情报的数据不少于 300 万条，支持扩展到 1000 万条。 威胁情报类型包含 APT 攻击、勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件、僵尸网络、常规木马、其他远控等。威胁情报知识库涵盖情报 IOC 情报状态、恶意家族、攻击团伙、远控类型、解决方案等数据。
5	▲支持 20 种以上 APT 特种木马家族的通信特征指令检测，包括攻击目标为中国的组织例如美人鱼、验证器、海莲花、摩诃草、蔓灵花、奇幻熊等。
6	▲支持 100+种以上反逃逸欺骗对抗手段，能够针对特种木马等恶意代码反虚拟机检测技术进行规避，避免恶意代码绕过；如：检测在注册表中搜索 VMware 等字符串的行为、压缩样本“睡眠”时间 等反逃逸欺骗对抗手段。
7	▲支持内置引擎对邮件正文、标题中的密码进行识别，并用于邮件附件的解密，提升邮件附件检测率。
8	▲支持对系统内置规则威胁等级进行自定义调整，降低误报。
资产威胁与漏洞管理平台	
1	▲支持对近 3 年内主域名所关联的全部子域名解析 IP 结果的收集，提供解析 IP 的首末次解析时间，支持子域名的检出率达到 97%以上
2	▲支持网站子 URL 的爬取，并形成网站地图。支持标记来源，来源至少包括爬虫、被动流量、情报等。支持限制爬取的目录层数（不低于 5 级）、单个路径下文件数量（不少于 50 个文件）、爬取 URL 总数（不少于 3000）、能够过滤特定类型的 URL（如图片、样式表、字体等），支持对网站地图中爬取到的特殊 URL 进行自动化标记，至少包括 API 和管理后台标记。
3	▲支持国产化设备的指纹特征识别，支持 3000+种国产化指纹，其中包括： 1）达梦、人大金仓等国产数据库的指纹≥10 种； 2）东方通等中间件的指纹≥10 种； 3）华为、海康威视等国产监控设备≥200 种； 4）金蝶 OA、致远 OA 等国产业务系统指纹≥500 种； 5）360 天擎、天融信防火墙、启明 IDS 等国产安全设备指纹≥500 种；

4	▲支持动态资产变更检测，可识别新增 IP、新增端口、新增 URL、组件变更、资产存活性变更。
5	▲支持基于资产指纹为资产自动添加标签，包括但不限于：云主机、防火墙、管理后台、API 等，支持自定义配置新增资产标签自动识别的规则。
6	▲支持根据企业关键词发现企业相关小程序的基本信息，需包括但不限于小程序名称、状态、小程序 ID、APPID、认证主体、统一社会信用代码、服务提供商、小程序简介、最后更新时间和业务域名清单。
7	▲支持基于关键词监测暗网中的相关数据信息，信息内容包含但不限于主题、帖子详情、作者、创建时间、发现时间、匹配关键词、链接地址、标记，且支持提供暗网交易快照的查看。
8	▲支持在 1day 漏洞爆发的 24 小时内进行漏洞情报实时推送（需联网），且能针对新披露的高危 1day 漏洞自动匹配预估受影响资产数据，明确受影响范围。
9	▲支持多维度分析，提供自定义安全场景视图。视图种类不少于 25 种，支持视图自定义拼接。
10	▲提供中国信息信息安全测评中心颁发的《国家信息安全漏洞库（CNNVD）兼容性资质证书》。
11	▲提供华为云计算技术有限公司颁发的鲲鹏产品兼容性证书。
数据安全管理系统	
1	▲支持三种数据源类型按行业分类分级运行，包括针对数据库、API、文件 3 大类;
2	▲支持即时调度与周期性调度，包括：调期性调度包括：每小时、每天、每周、每月，并可指定开始调度时间；所有调度任务把分类分级结果自动合并到统一库中，可以按:数据库、API、文件(图片)对象进行分类结果分析
3	▲支持针对分类分级的结果生成数据 DNA 功能，把手工分类后的数据进行数据基因保存
4	▲支持泄密文件溯源，包括：终端 ID、设备名称、设备 MAC、文件名称、文件 MD5、违规操作次数
5	▲支持终端违规外发，支持按内容、文件名称、时间段进行搜索、统计违规外发方式、违规外发次数
6	▲支持对敏感文件的使用和流转过程进行追溯，查看哪些人对该文件做过违规编辑、改名、违规外发（QQ、微信、移动存储设备、蓝牙、FTP、Http/Https、SMTP 等）、违规打印等操作
7	▲支持 API 接口调用这些查询、统计操作指令，以提供给其它产品的数据接入能力.
8	▲支持知识图谱技战术热力图，展示 360 全景攻防知识图谱，包括:侦察、资源部署、初始访问、执行、持久化、权限升级、防御逃逸、凭据访问、发现、横向移动、采集、命令与控制、数据渗漏、恶劣影响等阶段，进行关联威胁事情发生位置与数量
9	▲支持点击攻击技术，查看详情，包括不限于子技术、技术描述，相关安全事件等
10	▲支持 Mitre ATT&CK 之外扩展出具备中国特有的技战术总结。

注：

1.以上工具打“▲”为工具自身的主要功能需求，应提供实现功能的证明截图，不得以厂商承诺书进行替代。

2.核心技术指标（▲项）需根据▲项汇总表应答并提供证明材料，否则视为无效应答，标注“▲”技术参数不响应的每一项扣 1 分，扣完为止。

4 驻场人员要求

在服务期限内，投标方团队成员应保持稳定，以保证服务工作的正常运行。投标方提供的驻场人员需满足招标方需求，由招标方对投标方人员进行考核。

投标方应在中标后遵照招标单位的管理要求，履行对现场服务人员管理责任，确保驻场人员在招标方的驻场办公地点工作期间严格遵守招标方的出入管理、行为规范、出勤管理、保密等相关规定。

驻场服务人员提供 7*24 小时服务。白天工作时间内提供 4 人现场驻场服务，非工作时间提供 2 人，节假日期间提供 2 人。

服务期：1 年。

5 运营清单

序号	名称	单位	数量
1	风险主动识别服务		
1.1	渗透测试	项	1
1.2	代码审计	项	1
2	防御验证服务		
2.1	红蓝对抗服务	项	1
2.2	威胁狩猎服务	项	1
3	应急运营服务		
3.1	应急预案服务	项	1
3.2	应急演练服务	项	1
3.3	应急响应服务	项	1
4	安全运营管理服务		
4.1	安全高阶能力培训	项	1
5	日常安全监测服务		
5.1	资产管理	项	1
5.2	漏洞扫描	项	1
5.3	安全基线核查	项	1
5.4	病毒免疫能力检测	项	1
5.5	安全数据上报服务	项	1

5.6	情报检测与分析及预警	项	1
5.7	网络安全行为分析及预警	项	1
5.8	态势感知监测分析及通报预警	项	1
5.9	安全攻击溯源分析	项	1
5.10	督促整改及威胁协同处置	项	1
5.11	安全辅助决策服务	项	1
5.12	基础安全培训	项	1
5.13	重保值守服务	项	1
5.14	安全汇报	项	1
5.15	等级保护预测评	项	1
5.16	安全管理制度	项	1
6	特色场景运营服务		
6.1	数据安全运营		
6.1.1	数据安全告警策略定制化	项	1
6.1.2	数据安全态势分析	项	1
6.1.3	数据安全场景化预警模型定制	项	1
6.1.4	数据威胁研判分析及威胁协同处置	项	1
6.2	数据脱敏服务	项	1
6.3	数据加密服务	项	1
6.4	数据水印服务	项	1
6.5	数据安全审计服务	项	1
7	客户需求定制化服务		
7.1	运营管理平台定制化服务（工单系统）	项	1
7.2	安全可视化定制服务	项	1
7.3	数据共享与协同定制化服务	项	1

6 本项目面向大、中、小企业采购。