

政府采购合同

项目名称：广西壮族自治区水运发展中心软硬件运维服务

项目编号：GXZC2026-C3-001837-GXGN

所竞分标：标项二

采购人（甲方）：广西壮族自治区水运发展中心

供应商（乙方）：南宁市微中鑫电子科技有限公司



合同文本

采购计划号: 广西政采[2026]6985号 合同编号: GXZC2026-C3-001837-GXGN-02

采购人(甲方): 广西壮族自治区水运发展中心

供应商(乙方): 南宁市微中鑫电子科技有限公司

项目名称: 广西壮族自治区水运发展中心软硬件运维服务(标项二)

项目编号: GXZC2026-C3-001837-GXGN

签订地点: 南宁市 签订时间: 2026 年 07 月 22 日

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律法规规定,按照竞争性磋商采购文件规定条款和乙方承诺,甲乙双方签订本合同。

第一条 合同标的

1、服务内容一览表

序号	服务内容	数量	单位	单价 (元)	金额 (元)
1	硬件运维服务	1	项	876000.00	876000.00
合同总金额(人民币大写): 捌拾柒万陆仟元整 (¥ 876000.00)					

2、服务时间: 自2026年7月22日起12个月。

3、服务具体内容: 详见响应文件

4、报价应包含但不限于为履行本项目所有服务内容所涉及的知识产权、劳务、运输、旅差、管理、材料、维护、保险、维护期内所有升级、技术支持等相关服务费用,验收专家劳务费、验收会费、利润、税金,政策性文件规定及合同包含的应有风险、责任,招标代理服务等本合同涉及的服务业务及其它所有成本费用的总和,除此之外,甲方不再另行支付任何费用。如竞争性磋商文件对其另有规定的,从其规定。

第二条 质量保证

1、乙方所提供的产品及服务内容、技术规格、技术参数等质量必须与竞争性磋商文件和承诺相一致。

2、乙方所提供的产品及服务各项指标均达到质量要求。

第三条 权利保证

1、乙方应保证所提供产品及服务内容不会侵犯任何第三方的专利权、商标权、工业设计权或其他权利。

2、乙方应按竞争性磋商文件规定的时间向甲方提供有关技术资料。

3、没有甲方事先书面同意,乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、

图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。乙方应对承担维护服务的网络和信息系统履行数据安全保护和保密义务，不得违规将系统数据用于商业用途、向境外提供系统数据。提供维护服务过程中，应注意防止系统数据暴露于无关人员或完全开发的数据共享接口上。本条款为长期有效条款，不因本合同的解除、终止、被撤销、无效等事由而失去效力。

第四条 交付和验收

- 1、交付时间要求：自 2026 年 7 月 22 日起 12 个月。服务地点：广西区内采购人指定地点。
- 2、乙方提供不符合竞争性磋商文件和本合同规定的产品及服务内容，甲方有权拒绝接受。乙方提供的服务承诺、质量保证及其它具体约定事项，详见竞争性磋商文件、响应文件或者双方签订的补充协议。
- 3、当项目完成后，由乙方向甲方提出验收申请，并同时向甲方提交运维报告等验收材料。甲方应当在乙方提交验收申请后20个工作日内进行验收。在验收过程中发现乙方有违约问题，可暂缓资金结算，验收期限也相应顺延，待违约问题解决后，方可办理资金结算事宜。验收合格后由甲乙双方确认的验收代表签署验收单并加盖双方单位公章，甲乙双方各执一份。
- 4、甲方委托采购代理机构组织的验收项目，其验收时间以该项目验收方案确定的验收时间为准，验收结果以该项目验收报告结论为准。
- 5、验收不合格的，甲方在验收后 10 个工作日内以书面形式向乙方提出整改意见，乙方应自收到甲方书面意见后 10 日内及时予以整改。
- 6、验收费用：验收所发生的费用由乙方负责。

第五条 安装和培训

甲方应提供必要安装条件（如场地、电源、水源等），并协调信息系统相关集成商、开发商提供协助以便开展项目实施工作，乙方对安装条件有特殊要求的，应及时向甲方书面提出，否则视为甲方提供的安装条件已符合合同要求。

第六条 质量保证及售后服务

1、乙方应按竞争性磋商文件规定的产品及服务内容、技术要求、质量标准向甲方提供相应服务。产品达不到竞争性磋商文件规定的质量、技术要求者，根据实际情况，经双方协商，可按以下办法处理：

- (1) 重新提供服务：由乙方承担所发生的全部费用。
- (2) 贬值处理：由甲乙双方协议定价。

乙方应按照国家有关法律法规和“三包”规定以及竞争性磋商文件和本合同所附的《售后服务承诺》，为甲方提供售后服务。

2、如在使用过程中发生运维技术问题，乙方在接到甲方通知后，30 分钟内实质响应；最终修复从报修时间算起不能超过 72 小时。如乙方未能按时间要求逾期响应或无法修复的，视为乙方违约，按逾期提供服务确定违约责任和处理措施；乙方逾期响应或拒绝修复的，甲方可聘请第三方修复，由此产生的费用由乙方承担，甲方可直接在履约保证金中扣减，不足部分有权向乙方要求补足。

第七条 合同费用和付款方式

1、本项目合同金额为：人民币大写捌拾柒万陆仟元整，小写¥876000.00元。包括为完成本合同所发生的一切费用（含完成合同项目过程中所需的知识产权、劳务、运输、旅差、管理、材料、维护、保险、维护期内所有升级、技术支持等相关服务费用、验收专家劳务费、验收会务费、利润、税金、政策性文件规定及合同包含的应有风险、责任和招标代理服务费等服务业务及其它所有成本费用等各种费用在内）。

2、资金性质：财政资金。

3、付款方式：

履约保证金：按成交金额的2%收取，即人民币壹万柒仟伍佰贰拾元整（¥17520.00元）。

履约保证金提交方式为，银行转账、支票、汇票、本票或者金融、担保机构出具的保函等非现金方式。待合同履行完毕通过验收后，如无违约问题，甲方在收到乙方退还履约保证金申请后的15个工作日内无息返还。

标项二：合同签订后，甲方支付合同金额的20%（但支付金额不超过14.9万元整），即人民币壹拾肆万玖仟元整（¥149000.00元）；乙方服务期满8个月，经采购人考核服务质量合格后，甲方支付合同金额的70%，即人民币陆拾壹万叁仟贰佰元整（¥613200.00元）；乙方服务期满并经项目验收合格后，甲方支付剩余合同款项，即人民币壹拾壹万叁仟捌佰元整（¥113800.00元）。

满足合同约定支付条件时，应由乙方向甲方提出付款申请，并开具合法足额的完税发票，否则甲方有权暂不付款且不视为甲方违约，甲方在收到付款申请和发票后15个工作日内通过银行转账支付给乙方。

4、银行账户信息

（1）乙方银行账户信息：

开户名称：南宁市微中鑫电子科技有限公司

开户银行：中国建设银行股份有限公司南宁桃源支行

银行账号：4505 0160 4550 0000 0157

（2）甲方收款银行账户信息

开户名称：广西壮族自治区水运发展中心

开户银行：工商银行南宁市枫林路支行

收款账号：2102 1011 0922 1001 515

在合同履行期间，若乙方的开户名称、开户银行、收款账号发生变更的，应当在变更当日书面告知甲方，否则由此产生的损失后果由乙方承担。甲方不接受乙方委托第三方收款。

第八条 税费

本合同执行中相关的一切税费均由乙方负担。

第九条 违约责任

1、乙方所提供的产品及服务内容、技术标准、材料等质量不合格的，或者未按本合同和竞争性磋商采购、响应文件规定的技术要求和承诺提供产品及服务的，应按照甲方规定时限整改，

整改不及时的按逾期交付处罚；对于经乙方三次（含三次）整改仍无法达到甲方要求或通过验收的，乙方应向甲方支付合同金额 5% 违约金并赔偿甲方经济损失，同时甲方有权解除合同并按合同约定总金额的 20%向乙方主张违约金。

2、乙方提供的产品及服务如侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由乙方负责交涉并承担全部责任。如因此产生纠纷且甲方因此产生诉讼费用、执行费用、律师费以及赔偿款的，该费用由乙方承担。

3、乙方无故逾期提供服务的，逾期一方每天向对方偿付合同金额 0.1%违约金，超过 20 天（含 20 天）对方有权解除合同，乙方应按合同约定总金额的 20%支付违约金。

4、乙方未按本合同和竞争性磋商响应文件中规定的服务承诺提供服务的，经 3 次（含 3 次）整改仍无法达到要求的，乙方应按本合同金额 5% 向甲方支付违约金，并承担由此对甲方造成的损失。同时，甲方有权解除本合同，并保留追究乙方其它法律责任的权利。

5、由于乙方提供的产品及服务达不到竞争性磋商文件规定及响应文件提供的服务质量、技术要求，致使验收不合格的，甲方不予验收，后果由乙方负责。

6、乙方不能就所成交的项目进行转包（包括但不限于主体部分分包、肢解分包等变相转包），如发现乙方有转包现象，甲方有权解除本合同，由此造成的损失由乙方负责，同时乙方应按本合同金额 20%向甲方支付违约金。

7、其它违约行为按合同金额 3%收取违约金并赔偿经济损失。

8、因本合同一方违约而产生的一切法律纠纷，守约方为解决纠纷所产生的诉讼费、律师代理费、鉴定费、公证费、合理调查费、保全费、诉讼财产保全保险费及执行费等，均由违约方承担。

9、乙方违反本合同第三条约定的保密义务，甲方有权解除本合同，并要求乙方按合同金额 20%支付违约金，同时甲方由此造成的损失由乙方全额赔偿。

10、甲方依据第九条的约定解除合同的，不再支付剩余合同款项，且有权要求乙方退还已支付的合同款项，同时有权要求乙方支付合同约定总金额的 20%作为违约金。

第十条 不可抗力事件处理

1、在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2、不可抗力事件发生后，受不可抗力事件影响的一方应立即通知对方，并寄送有关权威机构出具的证明。同时应立即尽一切合理努力采取措施，消除影响，减少损失，否则失责而造成损失扩大的一方应对扩大的部分损失承担赔偿责任。

3、不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

4、一方逾期履行合同义务后发生不可抗力的，不适用本合同关于不可抗力的约定及法律规定。

第十一条 合同争议解决

1、因产品质量问题发生争议的，应邀请国家认可的机构对产品质量进行鉴定。产品质量符合标准的，鉴定费由甲方承担；不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商

不能解决，可向甲方住所地有管辖权的人民法院提起诉讼。

3、诉讼期间，本合同中双方无争议的部分继续履行。

第十二条 通知与送达

本合同一方发给对方的文件均以本合同载明的地址、电话等通讯方式为准，若一方变更地址、电话等通讯信息的，应即时以书面形式通知对方，否则，通知人按合同中对方的地址、电话等通讯方式发给对方的文件即视为通知人履行了送达文件的义务。如因合同中一方地址错误或地址变更没有书面通知造成送达不能的，由该方自行承担一切损失和责任。各类书面通知以书面文件为准，接收方签收之时起即为送达。无法直接传送的，市区内自文件邮寄之日起三天后视为已送达，市区外自发送之日起五天后视为已送达。

第十三条 合同生效及其它

1、合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2、合同执行中涉及采购资金和采购内容修改或补充的，须经相关部门审批，并签书面补充协议报相关部门备案，方可作为主合同不可分割的一部分。

3、本合同未尽事宜，双方协商并签订补充协议予以解决。补充协议与本协议不一致的，以补充协议为准。

第十四条 合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第 50 条规定的情形、以及本合同或本项目竞争性磋商文件另有约定外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

2、乙方不得擅自转让（无进口资格的供应商委托进口货物除外）其应履行的合同义务。

第十五条 签订本合同依据

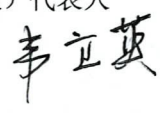
1、政府采购竞争性磋商文件；

2、乙方提供的竞争性磋商响应文件；

3、成交通知书。

第十六条 本合同一式五份，具有同等法律效力，甲乙双方各二份，采购代理机构一份（可根据需要另增加）。

本合同甲乙双方签字盖章后生效，本合同自签订之日起 2 个工作日内，甲方应当将采购合同在广西壮族自治区财政厅指定的媒体上公告。

甲方（章） 广西壮族自治区水运发展中心  2026年7月22日	乙方（章） 南宁市微中鑫电子科技有限公司  2026年7月22日
法定（授权）代表人 （签字）： 	法定（授权）代表人 （签字）： 
单位地址：南宁市青秀区百花岭路6号	单位地址：南宁市西乡塘区衡阳东路51号3栋C单元三层305房
电话：0771-2115330	电话：18077105415
经办人：任苏伟	经办人：韦立英
开户银行：工商银行南宁市枫林路支行	开户银行：中国建设银行股份有限公司南宁桃源支行
账号：2102 1011 0922 1001 515	账号：4505 0160 4550 0000 0157

合同附件

1、项目服务需求内容	
2、磋商报价表	
3、质量保证和服务承诺	
4、成交通知书	
5、履约保证金	
6、营业执照	
7、授权委托书	
甲方（章）： 广西壮族自治区水运发展中心  2026年7月22日	乙方（章）： 南宁市微中鑫电子科技有限公司  2026年7月22日

附件 1 项目服务需求内容

标项二

一、采购内容及技术要求			
序号	标的（服务） 的名称	数量及 单位	技术或服务要求
1	硬件运维服务	1 项	一、船舶吃水自动检测系统运维服务 运维服务分为软件维护、硬件维护、数据维护以及系统服务器运行环境维护四部分，在服务期内，承诺为采购人提供全面和及时的技术支持与服务。 （一）软件维护 1. 系统使用操作指导； 2. 供应商必须管控好系统各类组件账号密码安全，包括但不限于操作系统、数据库、中间件、WEB 系统等，禁止使用弱口令、默认口令、多台设备间使用相同口令； 3. 供应商应做好系统安全管理，系统未经允许禁止直接面向互联网部署，未经允许禁止私自在互联网搭建与我中心有关的测试系统，必须做好开发测试系统各类组件账号密码安全，禁止使用弱口令、默认口令、多台设备间使用相同口令。 4. 供应商必须管控好各类业务系统后台管理功能和页面，非必要禁止面向互联网开放；供应商必须对业务系统检测发现的漏洞进行升级、加固。 5. 日常运行状态监控。每月进行系统运行巡检，巡检软件主要功能是否正常，系统服务器负荷情况、系统内部数据状态，数据库运行状态、数据备份状态、存储空间是否正常。每月巡检后提交 1 次巡检记录（含异常情况处理记录）。 6. 采购方对系统提出的建议进行修改，对影响系统使用的故障，修复时长不超过 24 小时。 （二）硬件维护 1. 按采购人需求，提供三次雇佣蛙人取放水下设备服务。 2. 按采购人需求，对水下设备及线缆进行维修维护。 3. 每月定期对网络专线、网络设备，供电设备等进行巡检维护。发现设备故障需及时处理，提出解决方案。 （三）数据维护 1. 对数据展示模块进行维护；

		2. 每周一次在后台对系统数据进行滚动备份； 3. 因操作失误导致的数据错误修复；每月对数据库进行巡检，并解决数据库运行中出现的各类故障。 4. 按采购人要求将数据推送至中心库。 （四）服务器操作系统运行维护 1. 网络防病毒系统的维护。定期对服务器已有的病毒防护系统进行升级、更新； 2. 定期对服务器进行病毒检测；定期对服务器进行最新的安全漏洞修补； 4. 对发现的漏洞及时进行修复，如：互联网暴露资产、敏感信息泄露情报等。 （五）运维方式 1. 远程维护：系统发生故障时，通过电话、即时通讯工具或远程访问等方式进行系统故障的处理、技术支持、咨询服务等工作。 2. 现场技术服务：即系统软件出现重大故障导致系统业务中止时，供应商收到通知后应立即指派技术人员到达现场对故障进行处理和排除。 （六）服务要求 提供 7*24 小时服务，在接到采购人系统故障报修后，30 分钟内实质响应，4 小时内到达现场，8 小时内确认修复方案，系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题，供应商应向采购人说明并征得采购人同意后，组织技术专家，会同采购人制定技术处理方案，并按方案约定时间要求修复系统故障。 二、广西港航综合指挥中心设备运维服务 （一）维护保障范围 对广西壮族自治区水运发展中心 6 楼广西港航综合指挥中心进行运维服务，包括：1. 会议大屏（主屏+副屏+沙盘大屏）；2. 功放设备；3. 调音台设备；4. 操作台控制电脑；5. 指挥台控制电脑；6. 会议摄像头；7. 会议无线桌面话筒及手持话筒；8. 门禁系统；9. 多媒体发布系统；10. 会议转写系统；11. 机械升降灯光设备；12. 分布式控制系统及配套硬件设备。 （二）定期巡检、故障处理与设备维修 1. 在维保期内每季度对综合指挥中心系统及设备进行现场定期巡检服务，通过巡检，主动检查、发现、修复各种原因引起的系统设备故障、软件故障、应用程序故障，保证系统持续的正常运行。在服务期内，对于重大会议，按采购人要求派遣经验丰富的工程师赶赴现场提供会议保障支持。
--	--	--

		在其他时间，提供免费电话技术支持，对于电话解决不了的问题，24 小时内安排工程师到现场配合采购人调试。 2. 供应商在例行巡检发现故障或接到故障处理要求后，须及时组织人员进行故障处理，尽早恢复系统使用，事后通过书面形式将故障处理情况向采购人进行报备，并定期做好故障处理记录汇总。 3. 服务要求 (1) 提供 7*24 小时服务，在接到采购人系统故障报修后，30 分钟内实质响应，4 小时内到达现场，8 小时内确认修复方案，系统故障的最终修复从报修时间算起不能超过 72 小时。 (2) 各类设备硬件损坏的，在保修期内的须在 3 日内完成协调相关厂家更换或返厂维修，跟踪配件更换及修复，按期完成故障修复。不在保修期内的，应在 5 日内提出维修方案及维修报价。 三、会议系统设备运维服务 (一) 维护保障设备范围 宝利通视频会议系统控制单元 MCU 1 台；4 台宝利通视频会议终端；视频会议终端配套摄像机和麦克风。 (二) 定期巡检、故障处理与设备维修 在维保期内每季度对视频会议系统及设备进行现场定期巡检服务，通过巡检，主动检查、发现、修复各种原因引起的系统设备故障、软件故障、应用程序故障，保证系统持续的正常运行。在服务期内，对于重大视频会议，按采购人要求派遣经验丰富的工程师赶赴现场提供会议保障支持。在其他时间，提供免费电话技术支持，对于电话解决不了的问题，24 小时内安排工程师到现场配合采购人调试。 供应商在例行巡检发现故障或接到故障处理要求后，须及时组织人员进行故障处理，尽早恢复系统使用，事后通过书面形式将故障处理情况向采购人进行报备，并定期做好故障处理记录汇总。 (三) 服务要求 1. 提供 7*24 小时服务，在接到采购人系统故障报修后，30 分钟内实质响应，4 小时内到达现场，8 小时内确认修复方案，系统故障的最终修复从报修时间算起不能超过 72 小时。 2. 各类设备硬件损坏的，在保修期内的须在 3 日内完成协调相关厂家更换或返厂维修，跟踪配件更换及修复，按期完成故障修复。不在保修期内的，应在 5 日内提出维修方案及维修报价。 四、通讯机房及网络设备运维服务
--	--	---

		(一) 服务内容 对百花岭路 6 号网络通讯机房和在广西交通运输云数据中心托管的服务器、交换机、存储、安全设备以及其他机房运行所需的配套设备提供技术咨询和维护保障服务，对上述设备在使用过程中出现的故障进行检查、诊断、配置、实施修复操作。对服务器损坏硬盘、故障照明灯具、故障机柜 PDU 进行更换、维修机房精密空调控制电路板和风机故障。协助采购人制定机房信息系统支撑硬件及环境设备的升级改造和备件配备技术方案。对设备维修维护服务及其单项费用按次做好工单记录。按采购人要求，提供设备维修维护所必须的工具及配件。 (二) 服务要求 1. 提供网络及信息系统硬件设备运行监测工具软件。对水运发展中心机房网络设备、服务器设备、安全设备、各楼层交换机进行监控，当发现网络瓶颈或网络安全事件时，协助分析解决；对水运发展中心涉及的各专线进行监控，当发现网络故障时，及时告警并协助分析解决。 2. 提供为履行运维职责所用设施设备、工具等，对百花岭路 6 号机房的设备维护、网络排查等运维工作提供支撑。 3. 必须提供 7*24 小时服务，在接到采购人系统故障报修后，30 分钟内实质响应，4 小时内访问操作服务器和系统，8 小时内确认修复方案，系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题，供应商应向采购人说明并征得采购人同意后，组织技术专家，会同采购人制定技术处理方案，并按方案约定时间要求修复系统故障。 (三) 网络通讯机房消防安全年度检测服务 根据采购人要求，邀请有消防资质的第三方对网络通讯机房进行消防安全检测，并出具检测报告。 (四) 视频管理平台（VMS）运维服务 对采购人指定的视频管理平台进行升级运维服务。 (五) 信息技术服务 购买短信平台、微信开放平台、微信公众平台、DCloud 平台、远程会议平台等第三方平台相关服务供采购人统一使用，在整个运维服务周期内，保障广西数字水运一体化平台手机号登录、密码修改、系统紧急通知推送、微信授权登录，以及广西水运微信公众号、服务号、港航云在线 APP 手机号一键登录等核心业务功能正常可用。 五、网络安全防护攻防演练专项服务 (一) 互联网暴露资产发现服务
--	--	--

		1. 服务描述：针对广西壮族自治区水运发展中心互联网暴露的域名/IP 进行梳理，通过字典穷举、DNS 数据发现、搜索引擎数据挖掘、IP 段扫描、大数据关联等多种方式，全面检测发现当前互联网出口对外开放的已知和未知互联网资产，形成包括域名、IP、服务端口、应用服务等在内的互联网暴露资产信息，并通过与相关部门的核对验证，识别出正常使用资产、违规上线资产、无用僵尸资产、高危风险资产等关键资产信息，协助广西壮族自治区水运发展中心建立完整互联网资产清单，管控外部资产风险，避免被在攻防演练期间被攻击者利用。 2. 服务范围：广西壮族自治区水运发展中心发布在互联网的业务资产发现，识别、统计，服务期内每年提供 1 次服务。 3. 输出成果：《互联网暴露资产》 （二）敏感信息泄露情报服务 1. 服务描述：广西壮族自治区水运发展中心因各种途径散布到互联网上的敏感信息（如项目方案、网络拓扑、系统代码、账号密码等）是黑客实施攻击破坏时的高效助攻信息，黑客可利用此类敏感信息可更高效、更快速实施攻击，达成破坏目的，因此必须对本单位可能散布在互联网上的各类敏感信息周期性开展检查发现工作，以及对敏感信息进行处置，降低本单位网络安全风险。 敏感信息泄露情报服务是以攻击者的视角，通过各种关键字搜索、自动工具探测等手段，对各类互联网平台如搜索引擎、代码托管平台、网盘、文库、社交平台等（不含暗网）开展针对性的检查发现，以检测发现可能存在的敏感信息，并配合用户开展敏感信息处置工作，输出相关敏感信息报告。 2. 服务范围：广西壮族自治区水运发展中心可能散布于互联网平台上的敏感信息材料，服务期内每年提供 1 次服务。 3. 输出成果：《敏感信息泄露情报报告》。 （三）安全漏洞扫描服务 1. 服务描述：依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行安全扫描，对被评估目标进行覆盖面广泛的安全漏洞查找，以真实、全面地反映主机系统、网络设备、应用系统所存在的安全技术漏洞，评估信息基础环境的安全风险；在安全漏洞扫描完成后输出相应的《安全漏洞扫描报告》，其中包括漏洞原理及相关修复建议，并提供相应的技术支持协助客户修复漏洞。 通过常态化的安全漏洞扫描可以及时有效的检测基础环境的安全漏洞
--	--	--

		情况，有助于及时采取修复整改措施，降低安全风险。 2. 服务范围：部署在云上的业务系统涉及的相关主机设备，服务期内提供 1 次服务； 3. 输出成果：《安全漏洞扫描报告》。 （四）安全配置核查服务 1. 服务描述：通过“自动化工具配合人工检查”方式参考安全配置基线进行检查，检查对象包括操作系统、数据库、中间件等安全配置基线，采用主流的安全配置核查系统或检查脚本工具，以远程登录检查的方式工作，完成设备的检查；针对物理隔离或网络隔离的设备使用检查脚本工具来补充完成检查工作，安全基线配置核查工作完成后出具对应的《安全基线核查报告》，其中包括基线检查不合规项及相关修复建议，并提供相应的技术支持协助客户修复漏洞。 2. 服务范围：部署在云上的业务系统相关主机设备，服务期内每半年提供 1 次服务。 3. 输出成果：《安全基线核查报告》。 （五）渗透测试服务 1. 服务描述：渗透测试服务是模拟黑客的思维和攻击手法，采用人工黑盒的方式对授权指定的应用系统进行模拟攻击测试，以真实有效的发现应用系统可能存在的安全漏洞，有效帮助用户识别应用系统安全风险，提高应用系统安全防护能力。渗透测试工作以人工渗透结合工具攻击的方式开展，主要的测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 应用程序测试等，并指导、协助客户修复漏洞，待漏洞修复完成后提供回归性复测。渗透测试服务以用户授权指定的应用系统为测试对象，包含 1 次初测和整改后的复测。 2. 服务范围：部署于云上的 WEB 业务系统，每季度提供 1 次服务。 3. 输出成果：《渗透测试报告》。 （六）安全整改支持及修复确认服务 1. 服务描述：对互联网暴露资产、安全漏洞扫描、基线配置核查、渗透测试等网络安全检测中发现的漏洞和问题，指导、协助广西壮族自治区水运发展中心相关运维、开发人员开展打补丁、安全配置等整改协助工作，并及时跟进整改情况； 2. 服务范围：上述网络安全风险检测工作中发现的中高危安全问题。 3. 输出成果：《安全漏洞清单及加固跟进表》。
--	--	--

		(七) 应急响应服务 1. 服务描述: 项目期内为广西壮族自治区水运发展中心提供 7X24 小时的网络安全事件应急响应处置服务, 由专业二线专家提供网络安全事件应急处置技术支撑保障, 协助广西壮族自治区水运发展中心有效处置各类网络安全相关事件。 承诺提供 7X24 小时的实时响应, 并在发生安全事件后 15 分钟内电话响应, 1 小时内二线专家到达现场协助安全事件处置响应。事件处置完成后 3 天内输出《安全事件应急响应报告》。 2. 服务范围: 广西壮族自治区水运发展中心范围内发生的网络安全事件, 项目服务期内提供不超过 4 次应急处置服务。 3. 输出成果: 《安全事件应急响应报告》。 (八) 攻防演练安全防护服务 1. 服务描述: 为增强和提升自治区水运发展中心应对实战化攻防演练以及常态化外部攻击的能力, 安全服务供应商需要协助自治区水运发展中心采取积极有效的安全布防措施, 从主机安全防护加固、网络安全边界防护、攻击威胁监测分析等方面增强安全防护能力, 提供安全布防建议及协助, 安全服务提供方需自行提供相关服务防护工具协助广西壮族自治区水运发展中心提升纵深安全防护能力。 2. 服务工具: 为满足主机安全防护加固、网络安全边界防护、攻击威胁监测分析的安全布防要求, 安全服务供应商需自行提供相关服务防护工具并满足如下技术要求。 (1) 主机安全防护加固 由供应商为云上不少于 80 台主机提供安全防护服务, 提供包括资产梳理、入侵检测、风险评估、账号风险扫描、漏洞扫描、安全基线、防病毒、Webshell、微隔离、勒索场景化防护、微蜜罐、系统加固、性能监控、主机 IPS、流量转发模块等安全服务能力。服务期内免费提供软件版本、特征库版本升级服务及原厂技术专家远程故障支持服务。 1) 资产梳理能力: 通过自动或任务下发采集资产信息, 并提供账号、端口、计划任务的新增、修改、删除等变更行为的监控能力。 2) 防病毒能力: 提供快速扫描、全盘扫描、自定义扫描等病毒文件查杀能力。支持提供勒索诱饵防护、系统还原点和卷影保护、内核免疫等多种手段增强对勒索病毒的实时防护能力。支持联网进行病毒查杀, 利用云端海量病毒库提升本地病毒检出能力。 3) 漏洞扫描能力: 支持检测的漏洞数量应不低于 4000 个。支持对漏
--	--	---

		洞的快速验证，以检验漏洞是否成功修复。支持对漏洞进行加白。 4) 实体补丁修复：支持对 Windows 服务器漏洞进行补丁修复安装。 5) Webshell 监测能力：支持 Webshell 的实时监测，支持批量开启关闭实时监测。支持通过设置特征关键字定义 Webshell 规则。支持 Webshell 文件的手动、自动隔离，支持 Webshell 隔离区管理，支持批量对隔离区的 Webshell 文件进行恢复、删除等操作。 6) Webshell 增强实时监测能力：支持借助主机 RASP 插件、主机 WAF 插件增强 Webshell 的实时监测能力，支持额外获取 Webshell 植入时的 HTTP 信息，包括方法、user-agent、url、域名等信息。 7) 账号风险扫描能力：支持对常见操作系统、应用的弱口令检测能力。 8) 入侵检测能力：支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表。支持检测恶意扫描、异常登录、暴力破解、反弹 Shell、无文件攻击、RCE 利用、本地提权等功能。 9) 性能监控能力：可根据时间范围以折线图形式展示 CPU 使用率、内存使用率、客户端内存使用率、客户端 CPU 使用率。 10) 微隔离能力：支持五元组防火墙，支持配置源目的 IP、源目的端口、协议、出入站方向、协议等过滤条件灵活开启防火墙功能。支持白名单模式对服务器网络行为进行微隔离访问控制。支持对服务器的一键隔离，应急场景下快速处置服务器网络连接行为。 11) 主机 IPS 能力：IPS 规则库数量不少于 7000 条。支持批量、灵活的 IPS 规则下发能力，细粒度到每条 IPS 规则设置监控、阻断两种模式。 12) 系统加固能力：支持文件监控与防护、注册表监控与防护、操作系统加固、登录控制等功能 13) 防暴力破解能力：支持对 SSH、RDP、GoldenDB、MySQL、Oracle、SQLServer、VsFtpd、PostgreSQL、SMB、Tomcat 等服务进行暴力破解防护。 14) 应用防护能力：支持对一台或一组服务器进行白名单学习策略，并可设置学习时长，学习后可形成应用列表及 HASH 值，对偏离学习列表以外的应用进行告警和拦截。 15) 微蜜罐能力：支持端口蜜罐能力，在配置时可以自定义触发端口后的返回文本信息，可迷惑攻击者提高防护能力以及为取证提供支持。 16) 文件分发能力：支持批量向服务器传输文件并具备一定的自动执行的能力。可通过此功能将需要执行的脚本或补丁快速传输到指定服务器，节省运维成本。
--	--	--

		17) 高级防护：支持对未知威胁识别能力，在不依赖特征库的情况下可以识别出未知 WebShell、未知 SQ 注入漏洞、未知上传漏洞等攻击行为并进行防护。 18) 勒索场景化防护能力：提供纵深防护配置，可结合勒索事件攻击链条依次进行告警查看和安全加固配置：①收敛服务器外网暴露面；②多项风险点排查，提升服务器整体安全性防患于未然 ③勒索病毒实时查杀，对勒索病毒进行实时检测阻断；④勒索病毒专项防护，提供勒索诱饵防护、系统还原点保护、卷影保护能力；⑤系统关键目录加固防护（操作系统加固、用户目录保护、敏感配置文件保护、WEB 目录保护）；⑥勒索病毒应急处置（勒索病毒查杀、一键隔离）。 19) 流量采集转发：根据配置的流量采集转发策略采集主机流量并转发给本项目未知威胁监测与分析系统。支持按全量采集、五元组、自定义采集等采集规则，支持对采集的流量进行 VXLAN 和 GRE 封装转发。 (2) 边界安全防护 服务提供方需配置 2 台防火墙以增强单位网络的网络安全隔离防护能力。要求 1 台防火墙吞吐性能$\geq 3G$，每秒新建连接数≥ 6 万，配置≥ 4 个电口；另 1 台防火墙吞吐性能$\geq 8G$，每秒新建连接数≥ 10 万，配置≥ 8 个电口，≥ 2 个千兆光口，≥ 2 个万兆光口。 防火墙需支持应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能，需保持威胁情报数据、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库为最新版本。 1) 支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。 2) 支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。 3) 支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。 4) 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 5) 支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。 6) 支持灵活的服务链编排功能（服务量管理），支持串接链和旁路链，
--	--	---

		支持网元组的方向和目的位置设置。 7) 支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志，同时支持对 TCP 选项进行时间戳、窗口大小和选择确认进行设置保留、删除和默认三种动作。 8) 支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood、NTP Reply Flood 和 SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）、授权服务器防护（NS 重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 9) 支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。 10) 提供流量解密能力，支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密。同时支持将解密后流量镜像到其他设备进行分析统计；且支持设置是否记录日志。 11) 提供病毒查杀能力，能够对 HTTP（1.x/2）/FTP/POP3/SMTP/IMAP/SMB/NFS/IPTUX 八种协议进行病毒查杀；本地病毒库规模大于 3000 万，支持样本留存。 12) 提供病毒防护能力，可基于严重性、阈值和处置时长进行配置，支持病毒样本上传和页面消息推送功能。 13) 提供漏洞防护能力，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 DOH、FTP、HTTP（1.x/2）、IMAP、NFS、OTHER_APP、POP3、SMB、SMTP、DCERPC、DNS 等应用协议的漏洞防护。 14) 提供漏洞扫描能力，支持 WEB 漏扫、系统漏扫和物联网漏扫三种漏扫类型，可自定 TCP 和 UDP 的端口范围，扫描方式支持手动扫描和定期自动扫描。 15) 提供弱口令检测能力，支持主动检测和被动检测两种检测方式；支持基于网段、协议、用户名字典、弱口令字典进行完整扫描，制行方式包含手动和自动；能够基于数字、字母、数字和字母、自然顺序、键盘顺序、特殊字符、用户名、重复字符进行检测。支持自定义用户名、弱口令字典对象。
--	--	---

		16)提供 SSL 解密能力，支持解密证书自学习，支持透明部署进行 SSL 解密，支持解密 TLS1.3、TLS1.2、TLS1.1、TLS1.0、SSL3.0 协议。 17)支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”、“权重轮询”和“备份”）的方法编排给组内所有网元。 18)支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、启动事件、CPU 温度、CPU 风扇转速、机箱风扇转速、失陷主机告警、并发数告警、NAT 端口池利用率、CPU 利用率、内存利用率、硬盘利用率、接口带宽比等。 19)支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括流量、NAT444、SSL 解密、威胁、域名、URL 过滤、邮件过滤、内容过滤、行为、即时通信、操作、系统等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试等。 (3) 攻击威胁监测分析 配置未知威胁监测与分析系统。以提高港航云上业务系统对未知威胁的监测预警、威胁检测、溯源分析和响应处置能力。要求系统的分析平台最大日志处理速度（日志接入能力）不低于 12000EPS，流量探针对于流量处理性能不低于 6Gbps，服务期内保持未知威胁监测与分析系统的威胁情报更新与规则库为最新版本。 1)支持网络流量还原与深度检测能力，支持接入云上业务南北向、东西向网络流量进行全流量镜像还原与检测，流量实时处理及深度解析能力不低于 6Gbps。 2)提供日志汇聚与智能分析服务能力，实时对接入流量日志、告警日志进行日志关联性分析，日志实时处理吞吐能力不低于 12000EPS。支持以告警字段进行狩猎分析及可视化展示，以攻击链的视角还原告警中的受害主机被攻击的整个过程。 3)▲提供流量威胁检测能力，支持标准模式、精简模式、自定义模式三种检测模式切换；自定义模式下，支持手动配置检测速度、支持手动开启/关闭多种威胁检测引擎、机器学习模型。 4)提供 WEB 攻击检测、WEBSHELL 攻击检测、网络攻击检测、暴力猜解
--	--	--

		检测、加密流量攻击检测、远程工具检测、弱口令检测、挖矿检测、混淆攻击检测等检测能力。 5)提供 AI 检测能力，支持灵活开启机器学习模型，增强检测精度；支持包括：ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测、加密 webshell 检测(http/s)在内的至少 11 种机器学习检测模型，提高威胁行为检出率。 6)提供威胁情报检测能力，支持基于云端威胁情报的威胁检测，威胁情报不低于 800 万，威胁类型包括：APT 事件（定向攻击）、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒等。自定义威胁情报的威胁检测，包括 IP 地址、域名、MD5、URL 等。 7)▲提供威胁情报回溯能力，支持基于增量威胁情报，回溯检测历史原始日志产生威胁情报告警并自动标记告警标签。 8)提供 ATT&CK 分析能力，支持以可视化拓扑结构形式展示告警所命中的 ATT&CK 攻击技术及关联关系。 9)提供 wireshark 分析能力，支持兼容 wireshark 过滤语法关联展示本地 PCAP 会话数据用于告警分析，可以查看会话数量，会话时间、源/目的 IP、协议、会话信息等。 10)▲提供攻击带外分析能力，支持攻击带外检测分析（即检测攻击成功后根据负载信息再次攻击第三方的攻击），支持带外攻击趋势统计。 11)提供勒索专项分析能力，支持对勒索告警进行专项分析，可识别勒索家族包括：Cerber、Tescrypt、Strictor、WannaCry 等；支持威胁统计，包括活跃勒索家族（受害资产数）分布统计、勒索受害资产 Top10、勒索告警趋势图；勒索告警信息包括：最近发生时间、资产 IP、勒索家族、勒索阶段、告警次数、攻击结果、威胁级别、级联单位、资产分组、资产类型、告警来源、告警设备，以及对应的详细告警列表。 12)提供挖矿专项分析能力，支持识别 24+币种，币种类型包括：比特币、比特现金、以太坊、以太经典、莱特币、CKB、渡鸦币、大零币、ZEN、KDA、HNS、德信币、达世币、云储币、尔格币、CFX、MEER、小零币、极特币、XVG、CHI、STC、门罗币、TON 等，支持挖矿病毒威胁情报检测。 13)提供威胁情报专项分析能力，支持专项统计分析告警命中的威胁情报，支持对检索结果进行实时统计，包括威胁事件数量、影响资产数量、威胁类型统计、威胁级别分布等。
--	--	---

		14)提供应用安全专项分析、系统安全专项分析、设备安全专项分析、攻击者视角专项分析、资产视角专项分析、API 风险检测分析、云原生资产视角专项分析等安全能力，专项分析能力均需有单独页面呈现。 15)提供分析溯源能力，包括行为分析、DNS 行为分析、非常规访问行为分析、邮件行为分析、登录行为分析、WEB 服务器行为分析、数据库行为分析、访问行为分析、网络日志检索、告警日志检索、终端日志检索、调查跟踪、威胁狩猎分析等能力。 16)提供告警联动能力，支持基于单条告警或符合告警查询条件多告警的手动，自动处置，处置支持包括 NDR、邮件网关、终端安全、准入、防火墙、服务器安全设备、IPS 等设备。 17)提供态势感知能力，支持以客户端形式 3D 可视化效果呈现威胁态势，统计受攻击资产、攻击者、攻击阶段以及整体流量趋势变化，并支持中国地图下钻。 18)支持对常见网络、数据库、邮件等协议进行识别与还原，生成流量日志，包括但不限于：TCP、UDP、ICMP、HTTP、DNS、DHCP、SMTP、POP3、IMAP、DB2、Oracle、SQL Server、MySQL、MSSQL 、PostgreSQL、Mongo DB、LDAP、Radius、Kerberos 等。 19)支持启用流量过滤，可通过 IP 地址/IP 网段、服务/端口等进行流量过滤。支持通过配置 BPF 语法条件进行流量过滤，可通过 and、or、not 等逻辑运算创建过滤语句。 20)支持对隧道封装流量进行识别，支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测，云场景下支持 GENEVE 协议双层隧道封装流量的解析检测。 21)支持完整还原攻击请求过程，并通过分析响应报文准确判断攻击是否成功。 22)支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。（提供相关功能界面截图） 23)支持告警高亮显示的功能，能在告警中高亮显示规则命中的大概位置。 24)支持工作流程自定义编排，支持联动服务管理，支持 python 语言与 javascript 语言在 web 页面编辑联动服务。（提供相关功能界面截图） 25)支持常见 WEB 攻击行为的检测，包括但不限于：SQL 注入、命令执行、跨站脚本攻击、权限绕过、暴力破解、敏感信息泄露、目录遍历、文
--	--	---

		件包含、任意文件写入/读取/包含、代码执行等。 26)支持网络攻击行为的检测,包括但不限于:溢出漏洞、病毒传播类、其他后门、协议异常、浏览器劫持等。 27)支持 API 风险检测,支持还原 HTTP 完整的会话的请求头、请求体、响应头、响应体。 28)API 检测能力包括但不限于:配置不当、弱认证、未授权访问、敏感信息、数据过度暴露、访问异常、权限绕过、漏洞攻击等。 29)支持加密隐蔽流量攻击检测,包括但不限于:ICMP 隧道、DNS 隧道、HTTP 隧道等协议,支持 JA3 指纹检测。 30)支持灵活开启机器学习模型以增强检测精度,包括但不限于:CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测等。 31)支持导入弱口令字典,支持自定义弱口令规则。可通过正则表达式方式自定义弱口令强度、复杂规则。 32)支持旁路阻断功能,可基于 IP 地址、域名设置旁路阻断策略,支持将 URL 请求进行重定向。旁路阻断策略支持导入、导出,批量启用、停用、删除,支持设置封禁黑白名单。 33)支持 DDOS 攻击检测,包括但不限于 ACK Flood、SYN Flood、UDP Flood 和 Ping Flood、DNS Flood、HTTP Flood 等。 34)支持根据不同的检索条件、列表字段自定义查询告警,支持表头检索。 35)支持内置智能告警降噪规则,对原始告警自动分组归并。 36)支持针对挖矿风险进行专项分析,支持识别多类币种,且支持分析挖矿阶段并告警。 37)支持针对命中的威胁情报告警做专项统计分析,支持对检索结果进行实时统计,包括威胁事件数量、影响资产数量、威胁类型统计、威胁级别分布等。 38)支持从 WEB 应用、数据库、中间件、邮件安全维度做专项分析。支持从暴力破解、弱口令、未授权维度专项分析等系统安全。 39)支持针对 API 资产告警专项统计分析,包括但不限于告警 API 总数、不同威胁级别 API 数量、API 威胁类型分布情况、告警 API 的 Top 排名、告警 API 趋势等。支持基于 PATH、业务应用、HOST、主机 IP、请求方式等统计筛选 API。 40)支持攻击带外检测分析(检测攻击成功后根据负载信息再次攻击第
--	--	--

		三方的攻击), 支持带外攻击趋势统计。 41) 支持对非常规访问的专项分析, 包括但不限于可疑代理, 远程工具, 反弹 SHELL 等。 42) 支持数据库行为的专项分析, 发现数据库协议中的敏感操作或可能存在攻击行为的高危操作。支持对 mysql、mssql、oracle、sybase 等数据库, 支持配置数据库高危行为特征。 43) 支持日志检索, 包括但不限于填充胶囊字段值、lucene 语句搜索、SPL 命令语句搜索模式, 可选择网络日志、告警日志索引类型。 44) 态势大屏支持免密访问登录并展示, 支持轮播、全屏展示等操作。 45) 支持与本项目防火墙进行联动, 发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断 (将策略下发给防火墙, 由防火墙执行阻断) 46) 支持与本项目服务器安全管理系统联动, 支持从服务器安全管理系统采集的流量数据进行检测分析, 支持对服务器安全管理系统联动下发进行扫描弱口令、主动隔离失陷主机等命令。 (九) 代码安全检测服务 1. 服务描述 使用自动化代码检测工具并结合人工专家审计对应用系统进行白盒安全检测, 通过对系统源代码进行深入的安全分析, 充分挖掘当前源代码中存在的缺陷以及规范性缺陷, 从而协助开发人员了解其开发的应用系统可能会面临的威胁, 并指导开发人员正确修复程序缺陷。 2. 服务能力要求 服务提供方需自带代码安全检测服务工具以支持代码检测服务的实施, 自动化代码检测工具满足以下技术要求: (1) ▲支持主流编程语言开发的软件源代码的缺陷检测能力, 包括 C/C++、Objective-C、C#、Java、PHP、Swift、Go、Python、Cobol、Fortran、shell、Kotlin、SQL (Oracle、SQL Server、MySQL、HiveQL 等)、Ruby、Scala、Lua、Shell、Fortran 等。 (2) 支持常见安全缺陷问题的检测能力, 包括代码注入、跨站脚本、输入验证、危险函数、代码质量、API 误用、格式化字符串、资源管理、指针问题、隐私管理、密码管理、硬编码身份证号、硬编码银行卡号、硬编码手机号、异常处理等, 支持二级缺陷类型不低于 2000 个。 (3) 支持在检测时添加函数白名单, 包括 Java、C/C++、ruby、scala、Koltin、C#、python、Php 等开发语言, 检测过程中自动识别白名单函数进
--	--	--

		行路径裁剪，减少误报。 (4) 支持文件/文件夹白名单能力，可以对多个文件或文件夹进行过滤，不统计该文件和文件夹下检测的问题结果，提高系统检测精准性。 (5) 支持根据检测语言类型配置可信数据源，提高检测准确性。可信数据源包括命令行参数、web 表单、json 字符串等，界面可选可信源配置类型应不少于 15 种。 (6) 支持按照缺陷类型和缺陷文件进行分类显示和文件显示两种展示方式，可根据自定义 Top 模版展示用户关注的缺陷类型。 (7) 支持多个批次检测结果去重后的历史缺陷管理，可查看到缺陷首次发现的批次，是否已修复等信息。 (8) 支持自动化审计信息携带，能够将上一次的审计结果携带到下一一次的检测结果中，降低审计成本。 (9) 支持将检测、审计完成后的结果，可以单个或批量提交到 Bugzilla、Jira、TFS、禅道四种缺陷跟踪系统中。 (10) 支持按月、按日进行图形化缺陷趋势统计，统计的内容包括缺陷数、缺陷密度。支持项目经理统计，统计的内容包括项目经理、所属部门、项目数、源代码数、任务数、源代码行数、缺陷总数、缺陷密度、高危缺陷数、中危缺陷数、低危缺陷数、历史缺陷总数、新增缺陷数、未修复缺陷数、已修复缺陷数。 (11) 提供 word、excel、pdf 等多种格式的检测报告输出能力，报告内容可对缺陷等级、缺陷分类、修复建议、跟踪路径、修复建议、提交者信息、审计日志、爆发行代码进行自定义导出条件。 (12) 支持本地直接发起检测任务，也可以从 SVN、GIT、Gerrit、FireFly、StarTeam、TFS、ClearCase 等代码仓库获取代码发起检测任务，同时源代码来源支持 FTP 和共享目录。 (13) 支持构建工具集成能力，包括 Maven，Gradle，支持自动获取被测源代码的第三方依赖进行检测。 (14) 可以从 Visual Studio、Eclipse、intelliJ 直接发起检测任务并查看检测结果，对结果进行审计。支持 Jenkins、TFS 集成检测，可提供插件及操作文档，支持流水线阻断。 六、专项技术服务 供应商须配备不少于 6 名专职工作人员常驻现场开展服务，人员专业能力需匹配本项目运维、技术、项目管理、综合事务等工作需求；驻场人
--	--	--

		员保证工作日正常在岗，服从甲方管理，人员配置稳定，未经甲方同意不得随意更换驻场人员。具体服务内容如下： 1. 符合接入标准的各类感知终端硬件的接入配置工作，平台各子应用的权限管理及问题跟踪，确保各系统稳定正常运转、权限管控合规可控；配合视频会议的保障工作。 2. 综办平台的流程配置工作，配合供应商远程维护人员完成平台本地化配置与日常管理；协助开展来文公文办理相关工作；协助项目事项内部各类流程办理。 3. 跟进系统运维厂商的运维工作，协调解决系统运维过程中出现的各类相关问题；配合完成电子航道图入库审核、发布及替换工作；协同系统供应商开展资源规划、系统 bug 排查与处理，组织供应商实施运维服务、功能更新升级，业务流程处理、数据维护等相关工作；系统资源及网络策略的协调管理。 4. 协调配合中心网络运维、桌面运维及各类硬件设备的日常运维工作；配合网络通讯机房的日常管理工作。 5. 信息化工程项目建设管理相关辅助工作，综合性信息化材料的编写、汇总与整理；配合数字化建设规划计划、数字化建设方案撰写，为部省重大信息化工程提供技术支撑服务；配合组织项目相关验收工作，项目过程资料的整理、归档。 6. 收集、整理科技信息化相关规划、方案、设计、报告等文件的具体需求及技术资料，并进行修改完善；跟踪推进各类系统的实施应用，配合数据整理、分析及报告撰写工作；协助筹备相关会议组织工作，会议文件的准备、整理等辅助工作。
--	--	--

二、商务条款要求

序号	商务条款	商务要求
1	投标报价要求	本项目报价是履行合同的最终价格为总包干价人民币含税价，包含但不限于提供技术服务有关的价格、调试、培训、技术支持、售后服务等费用、必要的保险费用和各项税费、差旅费、项目所需投入的人员、办公设备、会议、印刷、项目评审、采购代理服务、验收、后续服务支持、税费等费用。采购人不再支付任何合同金额以外的费用。
2	合同签订日期	自成交通知书发出之日起 25 日内。
3	服务期限	自 2026 年 7 月 22 日起 12 个月。

4	服务地点或交付地点	广西区内采购人指定地点。
5	付款方式、时间、条件	1. 合同签订后，采购人支付合同金额的 20%（且支付金额不超过 14.9 万元整）； 2. 成交供应商服务期满 8 个月，经采购人考核服务质量合格后，采购人支付合同金额的 70%； 3. 成交供应商服务期满并经项目验收合格后，采购人支付剩余合同款项。上述款项均在成交供应商提供合法有效发票后 15 个工作日内支付。若考核或验收不合格，采购人有权暂缓付款，直至整改合格。
6	服务保障要求	1. 本项目涉及业务敏感数据存储、传输与处理，为保障项目交付质量、信息安全、个人隐私、供应链风险及全流程数据合规管控，要求供应商具备成熟标准化管理能力。项目履约全过程需落实质量管理、供应链安全、信息安全、隐私保护、数据安全成熟度管控，同时需具备专业信息安全技术服务能力，因此供应商需配套具备对应体系管理、安全服务类认证资质。 2. 本项目涵盖机房硬件设备运维、网络信息安全检测、渗透攻防、安全风险处置、运维全周期管理，项目统筹协调难度大、网络安全风险防控标准高，需项目负责人具备成熟项目统筹、信息安全全域管控能力；现场技术团队需具备计算机相关专业基础；专项安全检测工作需资深安全技术人员负责漏洞挖掘、渗透测试等高风险作业，具备渗透测试、安全运维专业能力，相关专业认证作为人员专业能力的评审参考。
7	售后服务要求	成交供应商在服务期内应当为采购人提供以下技术支持和咨询服务： 必须提供 7*24 小时服务，在接到采购人系统故障报修后，30 分钟内实质响应，4 小时内访问操作服务器和信息系统，8 小时内确认修复方案，系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题，供应商应向采购人说明并征得采购人同意后，组织技术专家，会同采购人制定技术处理方案，并按方案约定时间要求修复系统故障。
8	验收方式及标准	1. 验收要求按合同条款执行，未尽事宜按照《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》[桂财采（2015）22 号]以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》[财库（2016）205 号]规定执行。 2. 采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范；多项标准的，按最新标准或较高标准执行。
9	其他要求	1. 知识产权：采购人在中华人民共和国境内使用供应商提供的产品及服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，成交供应商应承担由此而引起的一切法律责任和费用。供应商在响

	应文件中提供承诺或证明材料。 2. 供应商在磋商活动中提供任何虚假材料, 以及响应服务所涉及内容不如实说明, 其响应文件按无效处理, 并报监管部门查处; 3. 未经采购人允许, 不得使用或以其它方式给任何第三方提供本项目的相关信息或数据, 必须对项目实施过程中获取的相关信息保密(相关信息包括但不限于本项目), 如发生失泄密事件即终止合同, 且成交供应商不得参与后续采购人项目投标活动。 4. 供应商须为本项目服务实施投入充足的服务人员, 并确保竞标文件中的人员信息真实、有效。 5. 成交人不得将项目非法分包或转包给任何单位和个人, 否则采购人有权即刻终止合同, 并要求成交人赔偿相应损失。 6. 其他未尽事宜由供需双方在采购合同中详细约定。
--	--

附件 2 磋商报价表

1. 竞标报价表

竞 标 报 价 表

项目名称：广西壮族自治区水运发展中心软硬件运维服务

项目编号: GXZC2026-C3-001837-GXGN

分标（如有）： 标项二

供应商名称: 南宁市微中鑫电子科技有限公司

单位：元

序号	服务名称	①数量	单位	②单价报价	③小计（元） （③=①*②）	注
1	硬件运维服务	1	项	876895.00	876895.00	
合计金额大写：人民币 <u>捌拾柒万陆仟捌佰玖拾伍元整</u> （¥ <u>876895.00 元</u> ）						

注：

1. 供应商的竞标报价表必须加盖电子签章并由法定代表人或者委托代理人签字或者电子签名, 否则其投标作无效标处理。
2. 报价一经涂改, 应在涂改处加盖电子签章或者由法定代表人或者授权委托人签字 (或者电子签名) 或者公章, 否则其投标作无效标处理。
3. 如为联合体投标, “供应商名称”处必须列明联合体各方名称, 并标注联合体牵头人名称, 否则其投标作无效标处理。
4. 如为联合体投标, 盖章处须加盖联合体各方公章, 否则其投标作无效标处理。
5. 如有多分标, 按分标分别提供竞标报价表, 否则投标无效。

法定代表人或者委托代理人（签字或者电子签名）

供应商（电子签章）：南宁市微中鑫电子科技有限公司

日期: 2026 年 7 月 2 日



附件 3 质量保证和服务承诺

7. 技术要求偏离表

技术要求偏离表

(注：按采购需求具体条款修改)

采购项目编号：GXZC2026-C3-001837-GXGN

采购项目名称：广西壮族自治区水运发展中心软硬件运维服务

分标号：标项二

序号	标的名称	磋商文件技术要求	供应商的响应	偏离说明
1	硬件运维服务	一、船舶吃水自动检测系统运维服务 运维服务分为软件维护、硬件维护、数据维护以及系统服务器运行环境维护四部分，在服务期内，承诺为采购人提供全面和及时的技术支持与服务。	一、船舶吃水自动检测系统运维服务 运维服务分为软件维护、硬件维护、数据维护以及系统服务器运行环境维护四部分，在服务期内，承诺为采购人提供全面和及时的技术支持与服务。	无偏离
		(一) 软件维护 1. 系统使用操作指导； 2. 供应商必须管控好系统各类组件账号密码安全,包括但不限于操作系统、数据库、中间件、WEB系统等，禁止使用弱口令、默认口令、多台设备间使用相同口令； 3. 供应商应做好系统安全管理,系统未经允许禁止直接面向互联网部署,未经允许禁止私自在互联网搭建与我中心有关的测试系统,必须做好开发测试系统各类组件账号密码安全,禁止使用弱口令、默认口令、多台设备间使用相同口令。 4. 供应商必须管控好各类业务系统后台管理功能和页面,非必要禁止面向互联网开放;供应商必须对业务系统检测发现的漏洞进行升级、加固。	(一) 软件维护 1. 系统使用操作指导； 2. 供应商必须管控好系统各类组件账号密码安全,包括但不限于操作系统、数据库、中间件、WEB系统等，禁止使用弱口令、默认口令、多台设备间使用相同口令； 3. 供应商应做好系统安全管理,系统未经允许禁止直接面向互联网部署,未经允许禁止私自在互联网搭建与我中心有关的测试系统,必须做好开发测试系统各类组件账号密码安全,禁止使用弱口令、默认口令、多台设备间使用相同口令。 4. 供应商必须管控好各类业务系统后台管理功能和页面,非必要禁止面向互联网开放;供应商必须对业务系统检测发现的漏洞进行升级、加固。	无偏离

	5. 日常运行状态监控。每月进行系统运行巡检,巡检软件主要功能是否正常,系统服务器负荷情况、系统内部数据状态,数据库运行状态、数据备份状态、存储空间是否正常。每月巡检后提交1次巡检记录(含异常情况处理记录)。 6. 采购方对系统提出的建议进行修改,对影响系统使用的故障,修复时长不超过24小时。	5. 日常运行状态监控。每月进行系统运行巡检,巡检软件主要功能是否正常,系统服务器负荷情况、系统内部数据状态,数据库运行状态、数据备份状态、存储空间是否正常。每月巡检后提交1次巡检记录(含异常情况处理记录)。 6. 采购方对系统提出的建议进行修改,对影响系统使用的故障,修复时长不超过24小时。	
	(二) 硬件维护 1. 按采购人需求,提供三次雇佣蛙人取放水下设备服务。 2. 按采购人需求,对水下设备及线缆进行维修维护。 3. 每月定期对网络专线、网络设备,供电设备等进行巡检维护。发现设备故障需及时处理,提出解决方案。	(二) 硬件维护 1. 按采购人需求,提供三次雇佣蛙人取放水下设备服务。 2. 按采购人需求,对水下设备及线缆进行维修维护。 3. 每月定期对网络专线、网络设备,供电设备等进行巡检维护。发现设备故障需及时处理,提出解决方案。	无偏离
	(三) 数据维护 1. 对数据展示模块进行维护; 2. 每周一次在后台对系统数据进行滚动备份; 3. 因操作失误导致的数据错误修复;每月对数据库进行巡检,并解决数据库运行中出现的各类故障。 4. 按采购人要求将数据推送至中心库。	(三) 数据维护 1. 对数据展示模块进行维护; 2. 每周一次在后台对系统数据进行滚动备份; 3. 因操作失误导致的数据错误修复;每月对数据库进行巡检,并解决数据库运行中出现的各类故障。 4. 按采购人要求将数据推送至中心库。	无偏离
	(四) 服务器操作系统运行维护 1. 网络防病毒系统的维护。定期对服务器已有的病毒防护系统进行升级、更新; 2. 定期对服务器进行病毒检测;定期对服务器进行最新的安全漏洞修补; 4. 对发现的漏洞及时进行修复,如:互联网暴露资产、敏感信息泄露情报等。	(四) 服务器操作系统运行维护 1. 网络防病毒系统的维护。定期对服务器已有的病毒防护系统进行升级、更新; 2. 定期对服务器进行病毒检测;定期对服务器进行最新的安全漏洞修补; 4. 对发现的漏洞及时进行修复,如:互联网暴露资产、敏感信息泄露情报等。	无偏离

	(五) 运维方式 1. 远程维护: 系统发生故障时, 通过电话、即时通讯工具或远程访问等方式进行系统故障的处理、技术支持、咨询服务等工作。 2. 现场技术服务: 即系统软件出现重大故障导致系统业务中止时, 供应商收到通知后应立即指派技术人员到达现场对故障进行处理和排除。	(五) 运维方式 1. 远程维护: 系统发生故障时, 通过电话、即时通讯工具或远程访问等方式进行系统故障的处理、技术支持、咨询服务等工作。 2. 现场技术服务: 即系统软件出现重大故障导致系统业务中止时, 供应商收到通知后应立即指派技术人员到达现场对故障进行处理和排除。	无偏离
	(六) 服务要求 提供 7*24 小时服务, 在接到采购人系统故障报修后, 30 分钟内实质响应, 4 小时内到达现场, 8 小时内确认修复方案, 系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题, 供应商应向采购人说明并征得采购人同意后, 组织技术专家, 会同采购人制定技术处理方案, 并按方案约定时间要求修复系统故障。	(六) 服务要求 提供 7*24 小时服务, 在接到采购人系统故障报修后, 30 分钟内实质响应, 4 小时内到达现场, 8 小时内确认修复方案, 系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题, 供应商应向采购人说明并征得采购人同意后, 组织技术专家, 会同采购人制定技术处理方案, 并按方案约定时间要求修复系统故障。	无偏离
	二、广西港航综合指挥中心设备运维服务 (一) 维护保障范围 对广西壮族自治区水运发展中心 6 楼广西港航综合指挥中心进行运维服务, 包括: 1. 会议大屏 (主屏+副屏+沙盘大屏); 2. 功放设备; 3. 调音台设备; 4. 操作台控制电脑; 5. 指挥台控制电脑; 6. 会议摄像头; 7. 会议无线桌面话筒及手持话筒; 8. 门禁系统; 9. 多媒体发布系统; 10. 会议转写系统; 11. 机械升降灯光设备; 12. 分布式控制系统及配套硬件设备。	二、广西港航综合指挥中心设备运维服务 (一) 维护保障范围 对广西壮族自治区水运发展中心 6 楼广西港航综合指挥中心进行运维服务, 包括: 1. 会议大屏 (主屏+副屏+沙盘大屏); 2. 功放设备; 3. 调音台设备; 4. 操作台控制电脑; 5. 指挥台控制电脑; 6. 会议摄像头; 7. 会议无线桌面话筒及手持话筒; 8. 门禁系统; 9. 多媒体发布系统; 10. 会议转写系统; 11. 机械升降灯光设备; 12. 分布式控制系统及配套硬件设备。	无偏离
	(二) 定期巡检、故障处理与设备维修 1. 在维保期内每季度对综合指挥	(二) 定期巡检、故障处理与设备维修 1. 在维保期内每季度对综合指挥	无偏离

	中心系统及设备进行现场定期巡检服务,通过巡检,主动检查、发现、修复各种原因引起的系统设备故障、软件故障、应用程序故障,保证系统持续的正常运行。在服务期内,对于重大会议,按采购人要求派遣经验丰富的工程师赶赴现场提供会议保障支持。在其他时间,提供免费电话技术支持,对于电话解决不了的问题,24小时内安排工程师到现场配合采购人调试。 2. 供应商在例行巡检发现故障或接到故障处理要求后,须及时组织人员进行故障处理,尽早恢复系统使用,事后通过书面形式将故障处理情况向采购人进行报备,并定期做好故障处理记录汇总。 3. 服务要求 (1) 提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内到达现场,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。 (2) 各类设备硬件损坏的,在保修期内的须在 3 日内完成协调相关厂家更换或返厂维修,跟踪配件更换及修复,按期完成故障修复。不在保修期内的,应在 5 日内提出维修方案及维修报价。	中心系统及设备进行现场定期巡检服务,通过巡检,主动检查、发现、修复各种原因引起的系统设备故障、软件故障、应用程序故障,保证系统持续的正常运行。在服务期内,对于重大会议,按采购人要求派遣经验丰富的工程师赶赴现场提供会议保障支持。在其他时间,提供免费电话技术支持,对于电话解决不了的问题,24小时内安排工程师到现场配合采购人调试。 2. 供应商在例行巡检发现故障或接到故障处理要求后,须及时组织人员进行故障处理,尽早恢复系统使用,事后通过书面形式将故障处理情况向采购人进行报备,并定期做好故障处理记录汇总。 3. 服务要求 (1) 提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内到达现场,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。 (2) 各类设备硬件损坏的,在保修期内的须在 3 日内完成协调相关厂家更换或返厂维修,跟踪配件更换及修复,按期完成故障修复。不在保修期内的,应在 5 日内提出维修方案及维修报价。	
	三、会议系统设备运维服务 (一) 维护保障设备范围 宝利通视频会议系统控制单元 MCU 1 台;4 台宝利通视频会议终端;视频会议终端配套摄像机和麦克风。	三、会议系统设备运维服务 (一) 维护保障设备范围 宝利通视频会议系统控制单元 MCU 1 台;4 台宝利通视频会议终端;视频会议终端配套摄像机和麦克风。	无偏离
	(二) 定期巡检、故障处理与设备维修 在维保期内每季度对视频会议系	(二) 定期巡检、故障处理与设备维修 在维保期内每季度对视频会议系	无偏离

	统及设备进行现场定期巡检服务,通过巡检,主动检查、发现、修复各种原因引起的系统设备故障、软件故障、应用程序故障,保证系统持续的正常运行。在服务期内,对于重大视频会议,按采购人要求派遣经验丰富的工程师赶赴现场提供会议保障支持。在其他时间,提供免费电话技术支持,对于电话解决不了的问题,24小时内安排工程师到现场配合采购人调试。 供应商在例行巡检发现故障或接到故障处理要求后,须及时组织人员进行故障处理,尽早恢复系统使用,事后通过书面形式将故障处理情况向采购人进行报备,并定期做好故障处理记录汇总。	统及设备进行现场定期巡检服务,通过巡检,主动检查、发现、修复各种原因引起的系统设备故障、软件故障、应用程序故障,保证系统持续的正常运行。在服务期内,对于重大视频会议,按采购人要求派遣经验丰富的工程师赶赴现场提供会议保障支持。在其他时间,提供免费电话技术支持,对于电话解决不了的问题,24小时内安排工程师到现场配合采购人调试。 供应商在例行巡检发现故障或接到故障处理要求后,须及时组织人员进行故障处理,尽早恢复系统使用,事后通过书面形式将故障处理情况向采购人进行报备,并定期做好故障处理记录汇总。	
	(三) 服务要求 1. 提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内到达现场,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。 2. 各类设备硬件损坏的,在保修期内的,须在 3 日内完成协调相关厂家更换或返厂维修,跟踪配件更换及修复,按期完成故障修复。不在保修期内的,应在 5 日内提出维修方案及维修报价。	(三) 服务要求 1. 提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内到达现场,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。 2. 各类设备硬件损坏的,在保修期内的,须在 3 日内完成协调相关厂家更换或返厂维修,跟踪配件更换及修复,按期完成故障修复。不在保修期内的,应在 5 日内提出维修方案及维修报价。	无偏离
	四、通讯机房及网络设备运维服务 (一) 服务内容 对百花岭路 6 号网络通讯机房和在广西交通运输云数据中心托管的服务器、交换机、存储、安全设备以及其他机房运行所需的配套设备提供技术咨询和维护保障服务,对上述设备在使	四、通讯机房及网络设备运维服务 (一) 服务内容 对百花岭路 6 号网络通讯机房和在广西交通运输云数据中心托管的服务器、交换机、存储、安全设备以及其他机房运行所需的配套设备提供技术咨询和维护保障服务,对上述设备在使	无偏离

	用过程中出现的故障进行检查、诊断、配置、实施修复操作。对服务器损坏硬盘、故障照明灯具、故障机柜 PDU 进行更换、维修机房精密空调控制电路板和风机故障。协助采购人制定机房信息系统支撑硬件及环境设备的升级改造和备件配备技术方案。对设备维修维护服务及其单项费用按次做好工单记录。按采购人要求,提供设备维修维护所必须的工具及配件。	用过程中出现的故障进行检查、诊断、配置、实施修复操作。对服务器损坏硬盘、故障照明灯具、故障机柜 PDU 进行更换、维修机房精密空调控制电路板和风机故障。协助采购人制定机房信息系统支撑硬件及环境设备的升级改造和备件配备技术方案。对设备维修维护服务及其单项费用按次做好工单记录。按采购人要求,提供设备维修维护所必须的工具及配件。	
	(二) 服务要求 1. 提供网络及信息系统硬件设备运行监测工具软件。对水运发展中心机房网络设备、服务器设备、安全设备、各楼层交换机进行监控,当发现网络瓶颈或网络安全事件时,协助分析解决;对水运发展中心涉及各专线进行监控,当发现网络故障时,及时告警并协助分析解决。 2. 提供为履行运维职责所用设施设备、工具等,对百花岭路 6 号机房的设备维护、网络排查等运维工作提供支撑。 3. 必须提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内访问操作服务器和系统,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题,供应商应向采购人说明并征得采购人同意后,组织技术专家,会同采购人制定技术处理方案,并按方案约定时间要求修复系统故障。	(二) 服务要求 1. 提供网络及信息系统硬件设备运行监测工具软件。对水运发展中心机房网络设备、服务器设备、安全设备、各楼层交换机进行监控,当发现网络瓶颈或网络安全事件时,协助分析解决;对水运发展中心涉及各专线进行监控,当发现网络故障时,及时告警并协助分析解决。 2. 提供为履行运维职责所用设施设备、工具等,对百花岭路 6 号机房的设备维护、网络排查等运维工作提供支撑。 3. 必须提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内访问操作服务器和系统,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题,供应商应向采购人说明并征得采购人同意后,组织技术专家,会同采购人制定技术处理方案,并按方案约定时间要求修复系统故障。	无偏离
	(三)网络通讯机房消防安全年度检测服务	(三)网络通讯机房消防安全年度检测服务	无偏离

	根据采购人要求,邀请有消防资质的第三方对网络通讯机房进行消防安全检测,并出具检测报告。	根据采购人要求,邀请有消防资质的第三方对网络通讯机房进行消防安全检测,并出具检测报告。	
	(四) 视频管理平台 (VMS) 运维服务 对采购人指定的视频管理平台进行升级运维服务。	(四) 视频管理平台 (VMS) 运维服务 对采购人指定的视频管理平台进行升级运维服务。	无偏离
	(五) 信息技术服务 购买短信平台、微信开放平台、微信公众平台、DCloud 平台、远程会议平台等第三方平台相关服务供采购人统一使用,在整个运维服务周期内,保障广西数字水运一体化平台手机号登录、密码修改、系统紧急通知推送、微信授权登录,以及广西水运微信公众号、服务号、港航云在线 APP 手机号一键登录等核心业务功能正常可用。	(五) 信息技术服务 购买短信平台、微信开放平台、微信公众平台、DCloud 平台、远程会议平台等第三方平台相关服务供采购人统一使用,在整个运维服务周期内,保障广西数字水运一体化平台手机号登录、密码修改、系统紧急通知推送、微信授权登录,以及广西水运微信公众号、服务号、港航云在线 APP 手机号一键登录等核心业务功能正常可用。	无偏离
	五、网络安全防护攻防演练专项服务 (一) 互联网暴露资产发现服务 1. 服务描述: 针对广西壮族自治区水运发展中心互联网暴露的域名、IP 进行梳理,通过字典穷举、DNS 数据发现、搜索引擎数据挖掘、IP 段扫描、大数据关联等多种方式,全面检测发现当前互联网出口对外开放的已知和未知互联网资产,形成包括域名、IP、服务端口、应用服务等在内的互联网暴露资产信息,并通过与相关部门的核对验证,识别出正常使用资产、违规上线资产、无用僵尸资产、高危风险资产等关键资产信息,协助广西壮族自治区水运发展中心建立完整互联网资产清单,管控外部资产风险,避免被在攻防演练期间被攻击者利用。	五、网络安全防护攻防演练专项服务 (一) 互联网暴露资产发现服务 1. 服务描述: 针对广西壮族自治区水运发展中心互联网暴露的域名/IP 进行梳理,通过字典穷举、DNS 数据发现、搜索引擎数据挖掘、IP 段扫描、大数据关联等多种方式,全面检测发现当前互联网出口对外开放的已知和未知互联网资产,形成包括域名、IP、服务端口、应用服务等在内的互联网暴露资产信息,并通过与相关部门的核对验证,识别出正常使用资产、违规上线资产、无用僵尸资产、高危风险资产等关键资产信息,协助广西壮族自治区水运发展中心建立完整互联网资产清单,管控外部资产风险,避免被在攻防演练期间被攻击者利用。	无偏离

	2. 服务范围:广西壮族自治区水运发展中心发布在互联网的业务资产发现,识别、统计,服务期内每年提供1次服务。 3. 输出成果:《互联网暴露资产》	2. 服务范围:广西壮族自治区水运发展中心发布在互联网的业务资产发现,识别、统计,服务期内每年提供1次服务。 3. 输出成果:《互联网暴露资产》	
	(二) 敏感信息泄露情报服务 1. 服务描述:广西壮族自治区水运发展中心因各种途径散布到互联网上的敏感信息(如项目方案、网络拓扑、系统代码、账号密码等)是黑客实施攻击破坏时的高效助攻信息,黑客可利用此类敏感信息可更高效、更快速实施攻击,达成破坏目的,因此必须对本单位可能散布在互联网上的各类敏感信息周期性开展检查发现工作,以及对敏感信息进行处置,降低本单位网络安全风险。 敏感信息泄露情报服务是以攻击者的视角,通过各种关键字搜索、自动工具探测等手段,对各类互联网平台如搜索引擎、代码托管平台、网盘、文库、社交平台等(不含暗网)开展针对性的检查发现,以检测发现可能存在的敏感信息,并配合用户开展敏感信息处置工作,输出相关敏感信息报告。 2. 服务范围:广西壮族自治区水运发展中心可能散布于互联网平台上的敏感信息材料,服务期内每年提供1次服务。 3. 输出成果:《敏感信息泄露情报报告》。	(二) 敏感信息泄露情报服务 1. 服务描述:广西壮族自治区水运发展中心因各种途径散布到互联网上的敏感信息(如项目方案、网络拓扑、系统代码、账号密码等)是黑客实施攻击破坏时的高效助攻信息,黑客可利用此类敏感信息可更高效、更快速实施攻击,达成破坏目的,因此必须对本单位可能散布在互联网上的各类敏感信息周期性开展检查发现工作,以及对敏感信息进行处置,降低本单位网络安全风险。 敏感信息泄露情报服务是以攻击者的视角,通过各种关键字搜索、自动工具探测等手段,对各类互联网平台如搜索引擎、代码托管平台、网盘、文库、社交平台等(不含暗网)开展针对性的检查发现,以检测发现可能存在的敏感信息,并配合用户开展敏感信息处置工作,输出相关敏感信息报告。 2. 服务范围:广西壮族自治区水运发展中心可能散布于互联网平台上的敏感信息材料,服务期内每年提供1次服务。 3. 输出成果:《敏感信息泄露情报报告》。	无偏离
	(三) 安全漏洞扫描服务 1. 服务描述:依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行安全扫描,对被评估目标进行覆盖	(三) 安全漏洞扫描服务 1. 服务描述:依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行安全扫描,对被评估目标进行覆盖	无偏离

	面广泛的安全漏洞查找，以真实、全面地反映主机系统、网络设备、应用系统所存在的安全技术漏洞，评估信息基础环境的安全风险；在安全漏洞扫描完成后输出相应的《安全漏洞扫描报告》，其中包括漏洞原理及相关修复建议，并提供相应的技术支持协助客户修复漏洞。 通过常态化的安全漏洞扫描可以及时有效的检测基础环境的安全漏洞情况，有助于及时采取修复整改措施，降低安全风险。 2. 服务范围：部署在云上的业务系统涉及的相关主机设备，服务期内提供1次服务； 3. 输出成果：《安全漏洞扫描报告》。	面广泛的安全漏洞查找，以真实、全面地反映主机系统、网络设备、应用系统所存在的安全技术漏洞，评估信息基础环境的安全风险；在安全漏洞扫描完成后输出相应的《安全漏洞扫描报告》，其中包括漏洞原理及相关修复建议，并提供相应的技术支持协助客户修复漏洞。 通过常态化的安全漏洞扫描可以及时有效的检测基础环境的安全漏洞情况，有助于及时采取修复整改措施，降低安全风险。 2. 服务范围：部署在云上的业务系统涉及的相关主机设备，服务期内提供1次服务； 3. 输出成果：《安全漏洞扫描报告》。	
	(四) 安全配置核查服务 1. 服务描述：通过“自动化工具配合人工检查”方式参考安全配置基线进行检查，检查对象包括操作系统、数据库、中间件等安全配置基线，采用主流的安全配置核查系统或检查脚本工具，以远程登录检查的方式工作，完成设备的检查；针对物理隔离或网络隔离的设备使用检查脚本工具来补充完成检查工作，安全基线配置核查工作完成后出具对应的《安全基线核查报告》，其中包括基线检查不合规项及相关修复建议，并提供相应的技术支持协助客户修复漏洞。 2. 服务范围：部署在云上的业务系统相关主机设备，服务期内每半年提供1次服务。 3. 输出成果：《安全基线核查报告》。	(四) 安全配置核查服务 1. 服务描述：通过“自动化工具配合人工检查”方式参考安全配置基线进行检查，检查对象包括操作系统、数据库、中间件等安全配置基线，采用主流的安全配置核查系统或检查脚本工具，以远程登录检查的方式工作，完成设备的检查；针对物理隔离或网络隔离的设备使用检查脚本工具来补充完成检查工作，安全基线配置核查工作完成后出具对应的《安全基线核查报告》，其中包括基线检查不合规项及相关修复建议，并提供相应的技术支持协助客户修复漏洞。 2. 服务范围：部署在云上的业务系统相关主机设备，服务期内每半年提供1次服务。 3. 输出成果：《安全基线核查报告》。	无偏离
	(五) 渗透测试服务	(五) 渗透测试服务	无偏离

	1. 服务描述: 渗透测试服务是模拟黑客的思维和攻击手法, 采用人工黑盒的方式对授权指定的应用系统进行模拟攻击测试, 以真实有效的发现应用系统可能存在的安全漏洞, 有效帮助用户识别应用系统安全风险, 提高应用系统安全防护能力。渗透测试工作以人工渗透结合工具攻击的方式开展, 主要的测试方法包括: 信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 应用程序测试等, 并指导、协助客户修复漏洞, 待漏洞修复完成后提供回归性复测。渗透测试服务以用户授权指定的应用系统为测试对象, 包含 1 次初测和整改后的复测。 2. 服务范围: 部署于云上的 WEB 业务系统, 每季度提供 1 次服务。 3. 输出成果: 《渗透测试报告》。	1. 服务描述: 渗透测试服务是模拟黑客的思维和攻击手法, 采用人工黑盒的方式对授权指定的应用系统进行模拟攻击测试, 以真实有效的发现应用系统可能存在的安全漏洞, 有效帮助用户识别应用系统安全风险, 提高应用系统安全防护能力。渗透测试工作以人工渗透结合工具攻击的方式开展, 主要的测试方法包括: 信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 应用程序测试等, 并指导、协助客户修复漏洞, 待漏洞修复完成后提供回归性复测。渗透测试服务以用户授权指定的应用系统为测试对象, 包含 1 次初测和整改后的复测。 2. 服务范围: 部署于云上的 WEB 业务系统, 每季度提供 1 次服务。 3. 输出成果: 《渗透测试报告》。	
	(六) 安全整改支持及修复确认服务 1. 服务描述: 对互联网暴露资产、安全漏洞扫描、基线配置核查、渗透测试等网络安全检测中发现的漏洞和问题, 指导、协助广西壮族自治区水运发展中心相关运维、开发人员开展打补丁、安全配置等整改协助工作, 并及时跟进整改情况; 2. 服务范围: 上述网络安全风险检测工作中发现的中高危安全问题。 3. 输出成果: 《安全漏洞清单及加固跟进表》。	(六) 安全整改支持及修复确认服务 1. 服务描述: 对互联网暴露资产、安全漏洞扫描、基线配置核查、渗透测试等网络安全检测中发现的漏洞和问题, 指导、协助广西壮族自治区水运发展中心相关运维、开发人员开展打补丁、安全配置等整改协助工作, 并及时跟进整改情况; 2. 服务范围: 上述网络安全风险检测工作中发现的中高危安全问题。 3. 输出成果: 《安全漏洞清单及加固跟进表》。	无偏离
	(七) 应急响应服务 1. 服务描述: 项目期内为广西壮族自治区水运发展中心提供 7X24 小时的	(七) 应急响应服务 1. 服务描述: 项目期内为广西壮族自治区水运发展中心提供 7X24 小时的	无偏离

	网络安全事件应急响应处置服务,由专业二线专家提供网络安全事件应急处置技术支撑保障,协助广西壮族自治区水运发展中心有效处置各类网络安全相关事件。 承诺提供 7X24 小时的实时响应,并在发生安全事件后 15 分钟内电话响应,1 小时内二线专家到达现场协助安全事件处置响应。事件处置完成后 3 天内输出《安全事件应急响应报告》。 2. 服务范围:广西壮族自治区水运发展中心范围内发生的网络安全事件,项目服务期内提供不超过 4 次应急处置服务。 3. 输出成果:《安全事件应急响应报告》。	网络安全事件应急响应处置服务,由专业二线专家提供网络安全事件应急处置技术支撑保障,协助广西壮族自治区水运发展中心有效处置各类网络安全相关事件。 承诺提供 7X24 小时的实时响应,并在发生安全事件后 15 分钟内电话响应,1 小时内二线专家到达现场协助安全事件处置响应。事件处置完成后 3 天内输出《安全事件应急响应报告》。 2. 服务范围:广西壮族自治区水运发展中心范围内发生的网络安全事件,项目服务期内提供不超过 4 次应急处置服务。 3. 输出成果:《安全事件应急响应报告》。	
	(八) 攻防演练安全防护服务 1. 服务描述:为增强和提升自治区水运发展中心应对实战化攻防演练以及常态化外部攻击的能力,安全服务供应商需要协助自治区水运发展中心采取积极有效的安全布防措施,从主机安全防护加固、网络安全边界防护、攻击威胁监测分析等方面增强安全防护能力,提供安全布防建议及协助,安全服务提供方需自行提供相关服务防护工具协助广西壮族自治区水运发展中心提升纵深安全防护能力。	(八) 攻防演练安全防护服务 1. 服务描述:为增强和提升自治区水运发展中心应对实战化攻防演练以及常态化外部攻击的能力,安全服务供应商需要协助自治区水运发展中心采取积极有效的安全布防措施,从主机安全防护加固、网络安全边界防护、攻击威胁监测分析等方面增强安全防护能力,提供安全布防建议及协助,安全服务提供方需自行提供相关服务防护工具协助广西壮族自治区水运发展中心提升纵深安全防护能力。	无偏离
	2. 服务工具:为满足主机安全防护加固、网络安全边界防护、攻击威胁监测分析的安全布防要求,安全服务供应商需自行提供相关服务防护工具并满足如下技术要求。	2. 服务工具:为满足主机安全防护加固、网络安全边界防护、攻击威胁监测分析的安全布防要求,安全服务供应商需自行提供相关服务防护工具并满足如下技术要求。	无偏离
	(1) 主机安全防护加固 由供应商为云上不少于 80 台主机	(1) 主机安全防护加固 由供应商为云上不少于 80 台主机	无偏离

	提供安全防护服务，提供包括资产梳理、入侵检测、风险评估、账号风险扫描、漏洞扫描、安全基线、防病毒、Webshell、微隔离、勒索场景化防护、微蜜罐、系统加固、性能监控、主机IPS、流量转发模块等安全服务能力。 服务期内免费提供软件版本、特征库版本升级服务及原厂技术专家远程故障支持服务。 1) 资产梳理能力：通过自动或任务下发采集资产信息，并提供账号、端口、计划任务的新增、修改、删除等变更行为的监控能力。	提供安全防护服务，提供包括资产梳理、入侵检测、风险评估、账号风险扫描、漏洞扫描、安全基线、防病毒、Webshell、微隔离、勒索场景化防护、微蜜罐、系统加固、性能监控、主机IPS、流量转发模块等安全服务能力。 服务期内免费提供软件版本、特征库版本升级服务及原厂技术专家远程故障支持服务。 1) 资产梳理能力：通过自动或任务下发采集资产信息，并提供账号、端口、计划任务的新增、修改、删除等变更行为的监控能力。	
	2) 防病毒能力：提供快速扫描、全盘扫描、自定义扫描等病毒文件查杀能力。支持提供勒索诱饵防护、系统还原点和卷影保护、内核免疫等多种手段增强对勒索病毒的实时防护能力。支持联网进行病毒查杀，利用云端海量病毒库提升本地病毒检出能力。	2) 防病毒能力：提供快速扫描、全盘扫描、自定义扫描等病毒文件查杀能力。支持提供勒索诱饵防护、系统还原点和卷影保护、内核免疫等多种手段增强对勒索病毒的实时防护能力。支持联网进行病毒查杀，利用云端海量病毒库提升本地病毒检出能力。	无偏离
	3) 漏洞扫描能力：支持检测的漏洞数量应不低于 4000 个。支持对漏洞的快速验证，以检验漏洞是否成功修复。支持对漏洞进行加白。	3) 漏洞扫描能力：支持检测的漏洞数量应不低于 4000 个。支持对漏洞的快速验证，以检验漏洞是否成功修复。支持对漏洞进行加白。	无偏离
	4) 实体补丁修复：支持对 Windows 服务器漏洞进行补丁修复安装。	4) 实体补丁修复：支持对 Windows 服务器漏洞进行补丁修复安装。	无偏离
	5) Webshell 监测能力：支持 Webshell 的实时监测，支持批量开启关闭实时监测。支持通过设置特征关键字定义 Webshell 规则。支持 Webshell 文件的手动、自动隔离，支持 Webshell 隔离区管理，支持批量对隔离区的 Webshell 文件进行恢复、删除等操作。	5) Webshell 监测能力：支持 Webshell 的实时监测，支持批量开启关闭实时监测。支持通过设置特征关键字定义 Webshell 规则。支持 Webshell 文件的手动、自动隔离，支持 Webshell 隔离区管理，支持批量对隔离区的 Webshell 文件进行恢复、删除等操作。	无偏离
	6) Webshell 增强实时监测能力：支持借助主机 RASP 插件、主机 WAF 插	6) Webshell 增强实时监测能力：支持借助主机 RASP 插件、主机 WAF 插	无偏离

件增强 Webshell 的实时监测能力，支持额外获取 Webshell 植入时的 HTTP 信息，包括方法、user-agent、url、域名等信息。	件增强 Webshell 的实时监测能力，支持额外获取 Webshell 植入时的 HTTP 信息，包括方法、user-agent、url、域名等信息。	
7) 账号风险扫描能力：支持对常见操作系统、应用的弱口令检测能力。	7) 账号风险扫描能力：支持对常见操作系统、应用的弱口令检测能力。	无偏离
8) 入侵检测能力：支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表。支持检测恶意扫描、异常登录、暴力破解、反弹 Shell、无文件攻击、RCE 利用、本地提权等功能。	8) 入侵检测能力：支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表。支持检测恶意扫描、异常登录、暴力破解、反弹 Shell、无文件攻击、RCE 利用、本地提权等功能。	无偏离
9) 性能监控能力：可根据时间范围以折线图形式展示 CPU 使用率、内存使用率、客户端内存使用率、客户端 CPU 使用率。	9) 性能监控能力：可根据时间范围以折线图形式展示 CPU 使用率、内存使用率、客户端内存使用率、客户端 CPU 使用率。	无偏离
10) 微隔离能力：支持五元组防火墙，支持配置源目的 IP、源目的端口、协议、出入站方向、协议等过滤条件灵活开启防火墙功能。支持白名单模式对服务器网络行为进行微隔离访问控制。支持对服务器的一键隔离，应急场景下快速处置服务器网络连接行为。	10) 微隔离能力：支持五元组防火墙，支持配置源目的 IP、源目的端口、协议、出入站方向、协议等过滤条件灵活开启防火墙功能。支持白名单模式对服务器网络行为进行微隔离访问控制。支持对服务器的一键隔离，应急场景下快速处置服务器网络连接行为。	无偏离
11) 主机 IPS 能力：IPS 规则库数量不少于 7000 条。支持批量、灵活的 IPS 规则下发能力，细粒度到每条 IPS 规则设置监控、阻断两种模式。	11) 主机 IPS 能力：IPS 规则库数量不少于 7000 条。支持批量、灵活的 IPS 规则下发能力，细粒度到每条 IPS 规则设置监控、阻断两种模式。	无偏离
12) 系统加固能力：支持文件监控与防护、注册表监控与防护、操作系统加固、登录控制等功能	12) 系统加固能力：支持文件监控与防护、注册表监控与防护、操作系统加固、登录控制等功能	无偏离
13) 防暴力破解能力：支持对 SSH、RDP、GoldenDB、MySQL、Oracle、SQLServer、VsFtpd、PostgreSQL、SMB、Tomcat 等	13) 防暴力破解能力：支持对 SSH、RDP、GoldenDB、MySQL、Oracle、SQLServer、VsFtpd、PostgreSQL、SMB、Tomcat 等	无偏离

	服务进行暴力破解防护。	服务进行暴力破解防护。	
	14) 应用防护能力: 支持对一台或一组服务器进行白名单学习策略, 并可设置学习时长, 学习后可形成应用列表及 HASH 值, 对偏离学习列表以外的应用进行告警和拦截。	14) 应用防护能力: 支持对一台或一组服务器进行白名单学习策略, 并可设置学习时长, 学习后可形成应用列表及 HASH 值, 对偏离学习列表以外的应用进行告警和拦截。	无偏离
	15) 微蜜罐能力: 支持端口蜜罐能力, 在配置时可以自定义触发端口后的返回文本信息, 可迷惑攻击者提高防护能力以及为取证提供支持。	15) 微蜜罐能力: 支持端口蜜罐能力, 在配置时可以自定义触发端口后的返回文本信息, 可迷惑攻击者提高防护能力以及为取证提供支持。	无偏离
	16) 文件分发能力: 支持批量向服务器传输文件并具备一定的自动执行的能力。可通过此功能将需要执行的脚本或补丁快速传输到指定服务器, 节省运维成本。	16) 文件分发能力: 支持批量向服务器传输文件并具备一定的自动执行的能力。可通过此功能将需要执行的脚本或补丁快速传输到指定服务器, 节省运维成本。	无偏离
	17) 高级防护: 支持对未知威胁识别能力, 在不依赖特征库的情况下可以识别出未知 WebShell、未知 SQL 注入漏洞、未知上传漏洞等攻击行为并进行防护。	17) 高级防护: 支持对未知威胁识别能力, 在不依赖特征库的情况下可以识别出未知 WebShell、未知 SQL 注入漏洞、未知上传漏洞等攻击行为并进行防护。	无偏离
	18) 勒索场景化防护能力: 提供纵深防护配置, 可结合勒索事件攻击链条依次进行告警查看和安全加固配置: ①收敛服务器外网暴露面; ②多项风险点排查, 提升服务器整体安全性防患于未然; ③勒索病毒实时查杀, 对勒索病毒进行实时检测阻断; ④勒索病毒专项防护, 提供勒索诱饵防护、系统还原点保护、卷影保护能力; ⑤系统关键目录加固防护 (操作系统加固、用户目录保护、敏感配置文件保护、WEB 目录保护); ⑥勒索病毒应急处置 (勒索病毒查杀、一键隔离)。	18) 勒索场景化防护能力: 提供纵深防护配置, 可结合勒索事件攻击链条依次进行告警查看和安全加固配置: ①收敛服务器外网暴露面; ②多项风险点排查, 提升服务器整体安全性防患于未然; ③勒索病毒实时查杀, 对勒索病毒进行实时检测阻断; ④勒索病毒专项防护, 提供勒索诱饵防护、系统还原点保护、卷影保护能力; ⑤系统关键目录加固防护 (操作系统加固、用户目录保护、敏感配置文件保护、WEB 目录保护); ⑥勒索病毒应急处置 (勒索病毒查杀、一键隔离)。	无偏离
	19) 流量采集转发: 根据配置的流量采集转发策略采集主机流量并转发给本	19) 流量采集转发: 根据配置的流量采集转发策略采集主机流量并转发给本	无偏离

	项目未知威胁监测与分析系统。支持按全量采集、五元组、自定义采集等采集规则，支持对采集的流量进行 VXLAN 和 GRE 封装转发。	项目未知威胁监测与分析系统。支持按全量采集、五元组、自定义采集等采集规则，支持对采集的流量进行 VXLAN 和 GRE 封装转发。	
	(2) 边界安全防护 服务提供方需配置 2 台防火墙以增强单位网络的网络安全隔离防护能力。要求 1 台防火墙吞吐性能$\geq 3G$，每秒新建连接数≥ 6 万，配置≥ 4 个电口；另 1 台防火墙吞吐性能$\geq 8G$，每秒新建连接数≥ 10 万，配置≥ 8 个电口，≥ 2 个千兆光口，≥ 2 个万兆光口。 防火墙需支持应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能，需保持威胁情报数据、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库为最新版本。 1) 支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。	(2) 边界安全防护 服务提供方需配置 2 台防火墙以增强单位网络的网络安全隔离防护能力。要求 1 台防火墙吞吐性能$\geq 3G$，每秒新建连接数≥ 6 万，配置≥ 4 个电口；另 1 台防火墙吞吐性能$\geq 8G$，每秒新建连接数≥ 10 万，配置≥ 8 个电口，≥ 2 个千兆光口，≥ 2 个万兆光口。 防火墙需支持应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能，需保持威胁情报数据、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库为最新版本。 1) 支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。	无偏离
	2) 支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。	2) 支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。	无偏离
	3) 支持 DDNS 功能，支持 Oray 向日葵、Pobyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。	3) 支持 DDNS 功能，支持 Oray 向日葵、Pobyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。	无偏离
	4) 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复	4) 支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复	无偏离

	策略的检查。	策略的检查。	
	5) 支持共享上网检测功能,可以通过设置管控地址和例外地址优化管控功能,同时支持阻断或告警动作。	5) 支持共享上网检测功能,可以通过设置管控地址和例外地址优化管控功能,同时支持阻断或告警动作。	无偏离
	6) 支持灵活的服务链编排功能(服务量管理),支持串接链和旁路链,支持网元组的方向和目的位置设置。	6) 支持灵活的服务链编排功能(服务量管理),支持串接链和旁路链,支持网元组的方向和目的位置设置。	无偏离
	7) 支持灵活的细粒度引流策略,可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向(内网到外网/外网到内网)的引流策略,并详细记录日志,同时支持对 TCP 选项进行时间戳、窗口大小和选择确认进行设置保留、删除和默认三种动作。	7) 支持灵活的细粒度引流策略,可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向(内网到外网/外网到内网)的引流策略,并详细记录日志,同时支持对 TCP 选项进行时间戳、窗口大小和选择确认进行设置保留、删除和默认三种动作。	无偏离
	8) 支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood、NTP Reply Flood 和 SIP Flood 攻击,并支持警告、丢弃、普通防护(首包丢弃)、增强防护(TC 反弹技术)、授权服务器防护(NS 重定向)、普通防护(自动重定向)、增强防护(手工确认)等多种防护措施。	8) 支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood、NTP Reply Flood 和 SIP Flood 攻击,并支持警告、丢弃、普通防护(首包丢弃)、增强防护(TC 反弹技术)、授权服务器防护(NS 重定向)、普通防护(自动重定向)、增强防护(手工确认)等多种防护措施。	无偏离
	9) 支持 DHCP 协议防护;支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。	9) 支持 DHCP 协议防护;支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。	无偏离
	10) 提供流量解密能力,支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密,支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略,动作可以设置解密或不解密。同时支持将解密后流量镜像到其他设备进行分析统计;且支持设置是否记录日志。	10) 提供流量解密能力,支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密,支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略,动作可以设置解密或不解密。同时支持将解密后流量镜像到其他设备进行分析统计;且支持设置是否记录日志。	无偏离

11) 提供病毒查杀能力, 能够对 HTTP (1. X/2) /FTP/POP3/SMTP/IMAP/SMB/NFS/IPTUX 八种协议进行病毒查杀; 本地病毒库规模大于 3000 万, 支持样本留存。	11) 提供病毒查杀能力, 能够对 HTTP (1. X/2) /FTP/POP3/SMTP/IMAP/SMB/NFS/IPTUX 八种协议进行病毒查杀; 本地病毒库规模大于 3000 万, 支持样本留存。	无偏离
12) 提供病毒防护能力, 可基于严重性、阈值和处置时长进行配置, 支持病毒样本上传和页面消息推送功能。	12) 提供病毒防护能力, 可基于严重性、阈值和处置时长进行配置, 支持病毒样本上传和页面消息推送功能。	无偏离
13) 提供漏洞防护能力, 同时将漏洞防护特征库分类, 至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类; 漏洞防护支持日志、阻断、放行、重置等执行动作, 可批量设置针对某一分类或全部攻击签名的执行动作; 支持基于 DOH、FTP、HTTP (1. x/2)、IMAP、NFS、OTHER_APP、POP3、SMB、SMTP、DCERPC、DNS 等应用协议的漏洞防护。	13) 提供漏洞防护能力, 同时将漏洞防护特征库分类, 至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类; 漏洞防护支持日志、阻断、放行、重置等执行动作, 可批量设置针对某一分类或全部攻击签名的执行动作; 支持基于 DOH、FTP、HTTP (1. x/2)、IMAP、NFS、OTHER_APP、POP3、SMB、SMTP、DCERPC、DNS 等应用协议的漏洞防护。	无偏离
14) 提供漏洞扫描能力, 支持 WEB 漏扫、系统漏扫和物联网漏扫三种漏扫类型, 可自定 TCP 和 UDP 的端口范围, 扫描方式支持手动扫描和定期自动扫描。	14) 提供漏洞扫描能力, 支持 WEB 漏扫、系统漏扫和物联网漏扫三种漏扫类型, 可自定 TCP 和 UDP 的端口范围, 扫描方式支持手动扫描和定期自动扫描。	无偏离
15) 提供弱口令检测能力, 支持主动检测和被动检测两种检测方式; 支持基于网段、协议、用户名字典、弱口令字典进行完整扫描, 制行方式包含手动和自动; 能够基于数字、字母、数字和字母、自然顺序、键盘顺序、特殊字符、用户名、重复字符进行检测。支持自定义用户名、弱口令字典对象。	15) 提供弱口令检测能力, 支持主动检测和被动检测两种检测方式; 支持基于网段、协议、用户名字典、弱口令字典进行完整扫描, 制行方式包含手动和自动; 能够基于数字、字母、数字和字母、自然顺序、键盘顺序、特殊字符、用户名、重复字符进行检测。支持自定义用户名、弱口令字典对象。	无偏离
16) 提供 SSL 解密能力, 支持解密证书自学习, 支持透明部署进行 SSL 解密, 支持解密 TLS1.3、TLS1.2、TLS1.1、TLS1.0、SSL3.0 协议。	16) 提供 SSL 解密能力, 支持解密证书自学习, 支持透明部署进行 SSL 解密, 支持解密 TLS1.3、TLS1.2、TLS1.1、TLS1.0、SSL3.0 协议。	无偏离

	17) 支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”、“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”、“权重轮询”和“备份”）的方法编排给组内所有网元。	17) 支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”、“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”、“权重轮询”和“备份”）的方法编排给组内所有网元。	无偏离
	18) 支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、启动事件、CPU 温度、CPU 风扇转速、机箱风扇转速、失陷主机告警、并发数告警、NAT 端口池利用率、CPU 利用率、内存利用率、硬盘利用率、接口带宽比等。	18) 支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、启动事件、CPU 温度、CPU 风扇转速、机箱风扇转速、失陷主机告警、并发数告警、NAT 端口池利用率、CPU 利用率、内存利用率、硬盘利用率、接口带宽比等。	无偏离
	19) 支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括流量、NAT444、SSL 解密、威胁、域名、URL 过滤、邮件过滤、内容过滤、行为、即时通信、操作、系统等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试等。	19) 支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括流量、NAT444、SSL 解密、威胁、域名、URL 过滤、邮件过滤、内容过滤、行为、即时通信、操作、系统等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试等。	无偏离
	(3) 攻击威胁监测分析 配置未知威胁监测与分析系统。以提高港航云上业务系统对未知威胁的监测预警、威胁检测、溯源分析和响应处置能力。要求系统的分析平台最大日志处理速度（日志接入能力）不低于 12000EPS，流量探针流量处理性能不低于 6Gbps，服务期内保持未知威胁监	(3) 攻击威胁监测分析 配置未知威胁监测与分析系统。以提高港航云上业务系统对未知威胁的监测预警、威胁检测、溯源分析和响应处置能力。要求系统的分析平台最大日志处理速度（日志接入能力）不低于 12000EPS，流量探针流量处理性能不低于 6Gbps，服务期内保持未知威胁监	无偏离

	测与分析系统的威胁情报更新与规则库为最新版本。 1) 支持网络流量还原与深度检测能力, 支持接入云上业务南北向、东西向网络流量进行全流量镜像还原与检测, 流量实时处理及深度解析能力不低于 6Gbps。	测与分析系统的威胁情报更新与规则库为最新版本。 1) 支持网络流量还原与深度检测能力, 支持接入云上业务南北向、东西向网络流量进行全流量镜像还原与检测, 流量实时处理及深度解析能力不低于 6Gbps。	
	2) 提供日志汇聚与智能分析服务能力, 实时对接入流量日志、告警日志进行日志关联性分析, 日志实时处理吞吐能力不低于 12000EPS。支持以告警字段进行狩猎分析及可视化展示, 以攻击链的视角还原告警中的受害主机被攻击的整个过程。	2) 提供日志汇聚与智能分析服务能力, 实时对接入流量日志、告警日志进行日志关联性分析, 日志实时处理吞吐能力不低于 12000EPS。支持以告警字段进行狩猎分析及可视化展示, 以攻击链的视角还原告警中的受害主机被攻击的整个过程。	无偏离
	3) ▲提供流量威胁检测能力, 支持标准模式、精简模式、自定义模式三种检测模式切换; 自定义模式下, 支持手动配置检测速度、支持手动开启/关闭多种威胁检测引擎、机器学习模型。	3) ▲提供流量威胁检测能力, 支持标准模式、精简模式、自定义模式三种检测模式切换; 自定义模式下, 支持手动配置检测速度、支持手动开启/关闭多种威胁检测引擎、机器学习模型。	无偏离
	4) 提供 WEB 攻击检测、WEBSHELL 攻击检测、网络攻击检测、暴力猜解检测、加密流量攻击检测、远程工具检测、弱口令检测、挖矿检测、混淆攻击检测等检测能力。	4) 提供 WEB 攻击检测、WEBSHELL 攻击检测、网络攻击检测、暴力猜解检测、加密流量攻击检测、远程工具检测、弱口令检测、挖矿检测、混淆攻击检测等检测能力。	无偏离
	5) 提供 AI 检测能力, 支持灵活开启机器学习模型, 增强检测精度; 支持包括: ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测、加密 webshell 检测 (http/s) 在内的至少 11 种机器学习检测模型, 提高威胁行为检出率。	5) 提供 AI 检测能力, 支持灵活开启机器学习模型, 增强检测精度; 支持包括: ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测、加密 webshell 检测 (http/s) 在内的至少 11 种机器学习检测模型, 提高威胁行为检出率。	无偏离
	6) 提供威胁情报检测能力, 支持基于云端威胁情报的威胁检测, 威胁情报	6) 提供威胁情报检测能力, 支持基于云端威胁情报的威胁检测, 威胁情报	无偏离

	不低于 800 万，威胁类型包括：APT 事件（定向攻击）、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒等。自定义威胁情报的威胁检测，包括 IP 地址、域名、MD5、URL 等。	不低于 800 万，威胁类型包括：APT 事件（定向攻击）、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒等。自定义威胁情报的威胁检测，包括 IP 地址、域名、MD5、URL 等。	
	7) ▲提供威胁情报回溯能力，支持基于增量威胁情报，回溯检测历史原始日志产生威胁情报告警并自动标记告警标签。	7) ▲提供威胁情报回溯能力，支持基于增量威胁情报，回溯检测历史原始日志产生威胁情报告警并自动标记告警标签。	无偏离
	8) 提供 ATT&CK 分析能力，支持以可视化拓扑结构形式展示告警所命中的 ATT&CK 攻击技术及关联关系。	8) 提供 ATT&CK 分析能力，支持以可视化拓扑结构形式展示告警所命中的 ATT&CK 攻击技术及关联关系。	无偏离
	9) 提供 wireshark 分析能力，支持兼容 wireshark 过滤语法关联展示本地 PCAP 会话数据用于告警分析，可以查看会话数量，会话时间、源/目的 IP、协议、会话信息等。	9) 提供 wireshark 分析能力，支持兼容 wireshark 过滤语法关联展示本地 PCAP 会话数据用于告警分析，可以查看会话数量，会话时间、源/目的 IP、协议、会话信息等。	无偏离
	10) ▲提供攻击带外分析能力，支持攻击带外检测分析(即检测攻击成功后根据负载信息再次攻击第三方的攻击)，支持带外攻击趋势统计。	10) ▲提供攻击带外分析能力，支持攻击带外检测分析(即检测攻击成功后根据负载信息再次攻击第三方的攻击)，支持带外攻击趋势统计。	无偏离
	11) 提供勒索专项分析能力，支持对勒索告警进行专项分析，可识别勒索家族包括：Cerber、Tescrypt、Strictor、WannaCry 等；支持威胁统计，包括活跃勒索家族（受害资产数）分布统计、勒索受害资产 Top10、勒索告警趋势图；勒索告警信息包括：最近发生时间、资产 IP、勒索家族、勒索阶段、告警次数、攻击结果、威胁级别、级联单位、资产分组、资产类型、告警来源、告警设备，以及对应的详细告警列表。	11) 提供勒索专项分析能力，支持对勒索告警进行专项分析，可识别勒索家族包括：Cerber、Tescrypt、Strictor、WannaCry 等；支持威胁统计，包括活跃勒索家族（受害资产数）分布统计、勒索受害资产 Top10、勒索告警趋势图；勒索告警信息包括：最近发生时间、资产 IP、勒索家族、勒索阶段、告警次数、攻击结果、威胁级别、级联单位、资产分组、资产类型、告警来源、告警设备，以及对应的详细告警列表。	无偏离

	12)提供挖矿专项分析能力,支持识别24+币种,币种类型包括:比特币、比特现金、以太坊、以太经典、莱特币、CKB、渡鸦币、大零币、ZEN、KDA、HNS、德信币、达世币、云储币、尔格币、CFX、MEER、小零币、极特币、XVG、CHI、STC、门罗币、TON等,支持挖矿病毒威胁情报检测。	12)提供挖矿专项分析能力,支持识别24+币种,币种类型包括:比特币、比特现金、以太坊、以太经典、莱特币、CKB、渡鸦币、大零币、ZEN、KDA、HNS、德信币、达世币、云储币、尔格币、CFX、MEER、小零币、极特币、XVG、CHI、STC、门罗币、TON等,支持挖矿病毒威胁情报检测。	无偏离
	13)提供威胁情报专项分析能力,支持专项统计分析告警命中的威胁情报,支持对检索结果进行实时统计,包括威胁事件数量、影响资产数量、威胁类型统计、威胁级别分布等。	13)提供威胁情报专项分析能力,支持专项统计分析告警命中的威胁情报,支持对检索结果进行实时统计,包括威胁事件数量、影响资产数量、威胁类型统计、威胁级别分布等。	无偏离
	14)提供应用安全专项分析、系统安全专项分析、设备安全专项分析、攻击者视角专项分析、资产视角专项分析、API风险检测分析、云原生资产视角专项分析等安全能力,专项分析能力均需有单独页面呈现。	14)提供应用安全专项分析、系统安全专项分析、设备安全专项分析、攻击者视角专项分析、资产视角专项分析、API风险检测分析、云原生资产视角专项分析等安全能力,专项分析能力均需有单独页面呈现。	无偏离
	15)提供分析溯源能力,包括行为分析、DNS行为分析、非常规访问行为分析、邮件行为分析、登录行为分析、WEB服务器行为分析、数据库行为分析、访问行为分析、网络日志检索、告警日志检索、终端日志检索、调查跟踪、威胁狩猎分析等能力。	15)提供分析溯源能力,包括行为分析、DNS行为分析、非常规访问行为分析、邮件行为分析、登录行为分析、WEB服务器行为分析、数据库行为分析、访问行为分析、网络日志检索、告警日志检索、终端日志检索、调查跟踪、威胁狩猎分析等能力。	无偏离
	16)提供告警联动能力,支持基于单条告警或符合告警查询条件多告警的手动,自动处置,处置支持包括NDR、邮件网关、终端安全、准入、防火墙、服务器安全设备、IPS等设备。	16)提供告警联动能力,支持基于单条告警或符合告警查询条件多告警的手动,自动处置,处置支持包括NDR、邮件网关、终端安全、准入、防火墙、服务器安全设备、IPS等设备。	无偏离
	17)提供态势感知能力,支持以客户端形式3D可视化效果呈现威胁态势,统计受攻击资产、攻击者、攻击阶段以及整体流量趋势变化,并支持中国地图下	17)提供态势感知能力,支持以客户端形式3D可视化效果呈现威胁态势,统计受攻击资产、攻击者、攻击阶段以及整体流量趋势变化,并支持中国地图下	无偏离

钻。	钻。	
18) 支持对常见网络、数据库、邮件等协议进行识别与还原,生成流量日志,包括但不限于: TCP、UDP、ICMP、HTTP、DNS、DHCP、SMTP、POP3、IMAP、DB2、Oracle、SQL Server、MySQL、MSSQL、PostgreSQL、Mongo DB、LDAP、Radius、Kerberos 等。	18) 支持对常见网络、数据库、邮件等协议进行识别与还原,生成流量日志,包括但不限于: TCP、UDP、ICMP、HTTP、DNS、DHCP、SMTP、POP3、IMAP、DB2、Oracle、SQL Server、MySQL、MSSQL、PostgreSQL、Mongo DB、LDAP、Radius、Kerberos 等。	无偏离
19) 支持启用流量过滤,可通过 IP 地址/IP 网段、服务/端口等进行流量过滤。支持通过配置 BPF 语法条件进行流量过滤,可通过 and、or、not 等逻辑运算创建过滤语句。	19) 支持启用流量过滤,可通过 IP 地址/IP 网段、服务/端口等进行流量过滤。支持通过配置 BPF 语法条件进行流量过滤,可通过 and、or、not 等逻辑运算创建过滤语句。	无偏离
20) 支持对隧道封装流量进行识别,支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测,云场景下支持 GENEVE 协议双层隧道封装流量的解析检测。	20) 支持对隧道封装流量进行识别,支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测,云场景下支持 GENEVE 协议双层隧道封装流量的解析检测。	无偏离
21) 支持完整还原攻击请求过程,并通过分析响应报文准确判断攻击是否成功。	21) 支持完整还原攻击请求过程,并通过分析响应报文准确判断攻击是否成功。	无偏离
22) 支持与云端威胁情报中心联动,可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索,查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。(提供相关功能界面截图)	22) 支持与云端威胁情报中心联动,可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索,查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。(提供相关功能界面截图)	无偏离
23) 支持告警高亮显示的功能,能在告警中高亮显示规则命中的大概位置。	23) 支持告警高亮显示的功能,能在告警中高亮显示规则命中的大概位置。	无偏离
24) 支持工作流程自定义编排,支持联动服务管理,支持 python 语言与 javascript 语言在 web 页面编辑联动服务。(提供相关功能界面截图)	24) 支持工作流程自定义编排,支持联动服务管理,支持 python 语言与 javascript 语言在 web 页面编辑联动服务。(提供相关功能界面截图)	无偏离
25) 支持常见 WEB 攻击行为的检测,包括但不限于: SQL 注入、命令执	25) 支持常见 WEB 攻击行为的检测,包括但不限于: SQL 注入、命令执	无偏离

行、跨站脚本攻击、权限绕过、暴力破解、敏感信息泄露、目录遍历、文件包含、任意文件写入/读取/包含、代码执行等。	行、跨站脚本攻击、权限绕过、暴力破解、敏感信息泄露、目录遍历、文件包含、任意文件写入/读取/包含、代码执行等。	
26)支持网络攻击行为的检测,包括但不限于:溢出漏洞、病毒传播类、其他后门、协议异常、浏览器劫持等。	26)支持网络攻击行为的检测,包括但不限于:溢出漏洞、病毒传播类、其他后门、协议异常、浏览器劫持等。	无偏离
27)支持 API 风险检测,支持还原 HTTP 完整的会话的请求头、请求体、响应头、响应体。	27)支持 API 风险检测,支持还原 HTTP 完整的会话的请求头、请求体、响应头、响应体。	无偏离
28)API 检测能力包括但不限于:配置不当、弱认证、未授权访问、敏感信息、数据过度暴露、访问异常、权限绕过、漏洞攻击等。	28)API 检测能力包括但不限于:配置不当、弱认证、未授权访问、敏感信息、数据过度暴露、访问异常、权限绕过、漏洞攻击等。	无偏离
29)支持加密隐蔽流量攻击检测,包括但不限于:ICMP 隧道、DNS 隧道、HTTP 隧道等协议,支持 JA3 指纹检测。	29)支持加密隐蔽流量攻击检测,包括但不限于:ICMP 隧道、DNS 隧道、HTTP 隧道等协议,支持 JA3 指纹检测。	无偏离
30)支持灵活开启机器学习模型以增强检测精度,包括但不限于:CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测等。	30)支持灵活开启机器学习模型以增强检测精度,包括但不限于:CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测等。	无偏离
31)支持导入弱口令字典,支持自定义弱口令规则。可通过正则表达式方式自定义弱口令强度、复杂规则。	31)支持导入弱口令字典,支持自定义弱口令规则。可通过正则表达式方式自定义弱口令强度、复杂规则。	无偏离
32)支持旁路阻断功能,可基于 IP 地址、域名设置旁路阻断策略,支持将 URL 请求进行重定向。旁路阻断策略支持导入、导出,批量启用、停用、删除,支持设置封禁黑白名单。	32)支持旁路阻断功能,可基于 IP 地址、域名设置旁路阻断策略,支持将 URL 请求进行重定向。旁路阻断策略支持导入、导出,批量启用、停用、删除,支持设置封禁黑白名单。	无偏离
33)支持 DDOS 攻击检测,包括但不限于 ACK Flood、SYN Flood、UDP Flood 和 Ping Flood、DNS Flood、HTTP Flood 等。	33)支持 DDOS 攻击检测,包括但不限于 ACK Flood、SYN Flood、UDP Flood 和 Ping Flood、DNS Flood、HTTP Flood 等。	无偏离
34)支持根据不同的检索条件、列	34)支持根据不同的检索条件、列	无偏离

表字段自定义查询告警，支持表头检索。	表字段自定义查询告警，支持表头检索。	
35) 支持内置智能告警降噪规则，对原始告警自动分组归并。	35) 支持内置智能告警降噪规则，对原始告警自动分组归并。	无偏离
36) 支持针对挖矿风险进行专项分析，支持识别多类币种，且支持分析挖矿阶段并告警。	36) 支持针对挖矿风险进行专项分析，支持识别多类币种，且支持分析挖矿阶段并告警。	无偏离
37) 支持针对命中的威胁情报告警做专项统计分析，支持对检索结果进行实时统计，包括威胁事件数量、影响资产数量、威胁类型统计、威胁级别分布等。	37) 支持针对命中的威胁情报告警做专项统计分析，支持对检索结果进行实时统计，包括威胁事件数量、影响资产数量、威胁类型统计、威胁级别分布等。	无偏离
38) 支持从 WEB 应用、数据库、中间件、邮件安全维度做专项分析。支持从暴力破解、弱口令、未授权维度专项分析等系统安全。	38) 支持从 WEB 应用、数据库、中间件、邮件安全维度做专项分析。支持从暴力破解、弱口令、未授权维度专项分析等系统安全。	无偏离
39) 支持针对 API 资产告警专项统计分析，包括但不限于告警 API 总数、不同威胁级别 API 数量、API 威胁类型分布情况、告警 API 的 Top 排名、告警 API 趋势等。支持基于 PATH、业务应用、HOST、主机 IP、请求方式等统计筛选 API。	39) 支持针对 API 资产告警专项统计分析，包括但不限于告警 API 总数、不同威胁级别 API 数量、API 威胁类型分布情况、告警 API 的 Top 排名、告警 API 趋势等。支持基于 PATH、业务应用、HOST、主机 IP、请求方式等统计筛选 API。	无偏离
40) 支持攻击带外检测分析（检测攻击成功后根据负载信息再次攻击第三方的攻击），支持带外攻击趋势统计。	40) 支持攻击带外检测分析（检测攻击成功后根据负载信息再次攻击第三方的攻击），支持带外攻击趋势统计。	无偏离
41) 支持对非常规访问的专项分析，包括但不限于可疑代理，远程工具，反弹 SHELL 等。	41) 支持对非常规访问的专项分析，包括但不限于可疑代理，远程工具，反弹 SHELL 等。	无偏离
42) 支持数据库行为的专项分析，发现数据库协议中的敏感操作或可能存在攻击行为的高危操作。支持对 mysql、mssql、oracle、sybase 等数据库，支持配置数据库高危行为特征。	42) 支持数据库行为的专项分析，发现数据库协议中的敏感操作或可能存在攻击行为的高危操作。支持对 mysql、mssql、oracle、sybase 等数据库，支持配置数据库高危行为特征。	无偏离
43) 支持日志检索，包括但不限于填充胶囊字段值、lucene 语句搜索、SPL	43) 支持日志检索，包括但不限于填充胶囊字段值、lucene 语句搜索、SPL	无偏离

	命令语句搜索模式，可选择网络日志、告警日志索引类型。	命令语句搜索模式，可选择网络日志、告警日志索引类型。	
	44) 态势大屏支持免密访问登录并展示，支持轮播、全屏展示等操作。	44) 态势大屏支持免密访问登录并展示，支持轮播、全屏展示等操作。	无偏离
	45) 支持与本项目防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）	45) 支持与本项目防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）	无偏离
	46) 支持与本项目服务器安全管理系统联动，支持从服务器安全管理系统采集的流量数据进行检测分析，支持对服务器安全管理系统联动下发进行扫描弱口令、主动隔离失陷主机等命令。	46) 支持与本项目服务器安全管理系统联动，支持从服务器安全管理系统采集的流量数据进行检测分析，支持对服务器安全管理系统联动下发进行扫描弱口令、主动隔离失陷主机等命令。	无偏离
	（九）代码安全检测服务 1. 服务描述 使用自动化代码检测工具并结合人工专家审计对应用系统进行白盒安全检测，通过对系统源代码进行深入的安全分析，充分挖掘当前源代码中存在的安全缺陷以及规范性缺陷，从而协助开发人员了解其开发的应用系统可能会面临的威胁，并指导开发人员正确修复程序缺陷。 2. 服务能力要求 服务提供方需自带代码安全检测服务工具以支持代码检测服务的实施，自动化代码检测工具满足以下技术要求： （1）▲支持主流编程语言开发的软件源代码的缺陷检测能力，包括 C/C++、Objective-C、C#、Java、PHP、Swift、Go、Python、Cobol、Fortran、shell、Kotlin、SQL（Oracle、SQL Server、MySQL、HiveQL 等）、Ruby、	（九）代码安全检测服务 1. 服务描述 使用自动化代码检测工具并结合人工专家审计对应用系统进行白盒安全检测，通过对系统源代码进行深入的安全分析，充分挖掘当前源代码中存在的安全缺陷以及规范性缺陷，从而协助开发人员了解其开发的应用系统可能会面临的威胁，并指导开发人员正确修复程序缺陷。 2. 服务能力要求 服务提供方需自带代码安全检测服务工具以支持代码检测服务的实施，自动化代码检测工具满足以下技术要求： （1）▲支持主流编程语言开发的软件源代码的缺陷检测能力，包括 C/C++、Objective-C、C#、Java、PHP、Swift、Go、Python、Cobol、Fortran、shell、Kotlin、SQL（Oracle、SQL Server、MySQL、HiveQL 等）、Ruby、	无偏离

	Scala、Lua、Shell、Fortran 等。	Scala、Lua、Shell、Fortran 等。	
	(2) 支持常见安全缺陷问题的检测能力,包括代码注入、跨站脚本、输入验证、危险函数、代码质量、API 误用、格式化字符串、资源管理、指针问题、隐私管理、密码管理、硬编码身份证号、硬编码银行卡号、硬编码手机号、异常处理等,支持二级缺陷类型不低于 2000 个。	(2) 支持常见安全缺陷问题的检测能力,包括代码注入、跨站脚本、输入验证、危险函数、代码质量、API 误用、格式化字符串、资源管理、指针问题、隐私管理、密码管理、硬编码身份证号、硬编码银行卡号、硬编码手机号、异常处理等,支持二级缺陷类型不低于 2000 个。	无偏离
	(3) 支持在检测时添加函数白名单,包括 Java、C/C++、ruby、scala、Kotlin、C#、python、Php 等开发语言,检测过程中自动识别白名单函数进行路径裁剪,减少误报。	(3) 支持在检测时添加函数白名单,包括 Java、C/C++、ruby、scala、Kotlin、C#、python、Php 等开发语言,检测过程中自动识别白名单函数进行路径裁剪,减少误报。	无偏离
	(4) 支持文件/文件夹白名单能力,可以对多个文件或文件夹进行过滤,不统计该文件和文件夹下检测的问题结果,提高系统检测精准性。	(4) 支持文件/文件夹白名单能力,可以对多个文件或文件夹进行过滤,不统计该文件和文件夹下检测的问题结果,提高系统检测精准性。	无偏离
	(5) 支持根据检测语言类型配置可信数据源,提高检测准确性。可信数据源包括命令行参数、web 表单、json 字符串等,界面可选可信源配置类型应不少于 15 种。	(5) 支持根据检测语言类型配置可信数据源,提高检测准确性。可信数据源包括命令行参数、web 表单、json 字符串等,界面可选可信源配置类型应不少于 15 种。	无偏离
	(6) 支持按照缺陷类型和缺陷文件进行分类显示和文件显示两种展示方式,可根据自定义 Top 模版展示用户关注的缺陷类型。	(6) 支持按照缺陷类型和缺陷文件进行分类显示和文件显示两种展示方式,可根据自定义 Top 模版展示用户关注的缺陷类型。	无偏离
	(7) 支持多个批次检测结果去重后的历史缺陷管理,可查看到缺陷首次发现的批次,是否已修复等信息。	(7) 支持多个批次检测结果去重后的历史缺陷管理,可查看到缺陷首次发现的批次,是否已修复等信息。	无偏离
	(8) 支持自动化审计信息携带,能够将上一次的审计结果携带到下一一次的检测结果中,降低审计成本。	(8) 支持自动化审计信息携带,能够将上一次的审计结果携带到下一一次的检测结果中,降低审计成本。	无偏离
	(9) 支持将检测、审计完成后的结果,可以单个或批量提交到 Bugzilla、	(9) 支持将检测、审计完成后的结果,可以单个或批量提交到 Bugzilla、	无偏离

Jira、TFS、禅道四种缺陷跟踪系统中。	Jira、TFS、禅道四种缺陷跟踪系统中。	
(10) 支持按月、按日进行图形化缺陷趋势统计,统计的内容包括缺陷数、缺陷密度。支持项目经理统计,统计的内容包括项目经理、所属部门、项目数、源代码数、任务数、源代码行数、缺陷总数、缺陷密度、高危缺陷数、中危缺陷数、低危缺陷数、历史缺陷总数、新增缺陷数、未修复缺陷数、已修复缺陷数。	(10) 支持按月、按日进行图形化缺陷趋势统计,统计的内容包括缺陷数、缺陷密度。支持项目经理统计,统计的内容包括项目经理、所属部门、项目数、源代码数、任务数、源代码行数、缺陷总数、缺陷密度、高危缺陷数、中危缺陷数、低危缺陷数、历史缺陷总数、新增缺陷数、未修复缺陷数、已修复缺陷数。	无偏离
(11) 提供 word、excel、pdf 等多种格式的检测报告输出能力,报告内容可对缺陷等级、缺陷分类、修复建议、跟踪路径、修复建议、提交者信息、审计日志、爆发行代码进行自定义导出条件。	(11) 提供 word、excel、pdf 等多种格式的检测报告输出能力,报告内容可对缺陷等级、缺陷分类、修复建议、跟踪路径、修复建议、提交者信息、审计日志、爆发行代码进行自定义导出条件。	无偏离
(12) 支持本地直接发起检测任务,也可以从 SVN、GIT、Gerrit、FireFly、StarTeam、TFS、ClearCase 等代码仓库获取代码发起检测任务,同时源代码来源支持 FTP 和共享目录。	(12) 支持本地直接发起检测任务,也可以从 SVN、GIT、Gerrit、FireFly、StarTeam、TFS、ClearCase 等代码仓库获取代码发起检测任务,同时源代码来源支持 FTP 和共享目录。	无偏离
(13) 支持构建工具集成能力,包括 Maven、Gradle,支持自动获取被测源代码的第三方依赖进行检测。	(13) 支持构建工具集成能力,包括 Maven、Gradle,支持自动获取被测源代码的第三方依赖进行检测。	无偏离
(14) 可以从 Visual Studio、Eclipse、intelliJ 直接发起检测任务并查看检测结果,对结果进行审计。支持 Jenkins、TFS 集成检测,可提供插件及操作文档,支持流水线阻断。	(14) 可以从 Visual Studio、Eclipse、intelliJ 直接发起检测任务并查看检测结果,对结果进行审计。支持 Jenkins、TFS 集成检测,可提供插件及操作文档,支持流水线阻断。	无偏离
六、专项技术服务 供应商须配备不少于 6 名专职工作人员常驻现场开展服务,人员专业能力需匹配本项目运维、技术、项目管理、综合事务等工作需求;驻场人员保证工作日正常在岗,服从甲方管理,人员配	六、专项技术服务 供应商须配备不少于 6 名专职工作人员常驻现场开展服务,人员专业能力需匹配本项目运维、技术、项目管理、综合事务等工作需求;驻场人员保证工作日正常在岗,服从甲方管理,人员配	无偏离

	置稳定,未经甲方同意不得随意更换驻场人员。具体服务内容如下: 1. 符合接入标准的各类感知终端硬件的接入配置工作,平台各子应用的权限管理及问题跟踪,确保各系统稳定正常运转、权限管控合规可控;配合视频会议的保障工作。 2. 综办平台的流程配置工作,配合供应商远程维护人员完成平台本地化配置与日常管理;协助开展来文公文办理相关工作;协助项目事项内部各类流程办理。 3. 跟进系统运维厂商的运维工作,协调解决系统运维过程中出现的各类相关问题;配合完成电子航道图入库审核、发布及替换工作;协同系统供应商开展资源规划、系统 bug 排查与处理,组织供应商实施运维服务、功能更新升级,业务流程处理、数据维护等相关工作;系统资源及网络策略的协调管理。 4. 协调配合中心网络运维、桌面运维及各类硬件设备的日常运维工作;配合网络通讯机房的日常管理工作。 5. 信息化工程项目建设管理相关辅助工作,综合性信息化材料的编写、汇总与整理;配合数字化建设规划计划、数字化建设方案撰写,为部省重大信息化工程提供技术支撑服务;配合组织项目相关验收工作,项目过程资料的整理、归档。 6. 收集、整理科技信息化相关规划、方案、设计、报告等文件的具体需求及技术资料,并进行修改完善;跟踪推进各类系统的实施应用,配合数据整理、分析及报告撰写工作;协助筹备相关会议	置稳定,未经甲方同意不得随意更换驻场人员。具体服务内容如下: 1. 符合接入标准的各类感知终端硬件的接入配置工作,平台各子应用的权限管理及问题跟踪,确保各系统稳定正常运转、权限管控合规可控;配合视频会议的保障工作。 2. 综办平台的流程配置工作,配合供应商远程维护人员完成平台本地化配置与日常管理;协助开展来文公文办理相关工作;协助项目事项内部各类流程办理。 3. 跟进系统运维厂商的运维工作,协调解决系统运维过程中出现的各类相关问题;配合完成电子航道图入库审核、发布及替换工作;协同系统供应商开展资源规划、系统 bug 排查与处理,组织供应商实施运维服务、功能更新升级,业务流程处理、数据维护等相关工作;系统资源及网络策略的协调管理。 4. 协调配合中心网络运维、桌面运维及各类硬件设备的日常运维工作;配合网络通讯机房的日常管理工作。 5. 信息化工程项目建设管理相关辅助工作,综合性信息化材料的编写、汇总与整理;配合数字化建设规划计划、数字化建设方案撰写,为部省重大信息化工程提供技术支撑服务;配合组织项目相关验收工作,项目过程资料的整理、归档。 6. 收集、整理科技信息化相关规划、方案、设计、报告等文件的具体需求及技术资料,并进行修改完善;跟踪推进各类系统的实施应用,配合数据整理、分析及报告撰写工作;协助筹备相关会议	
--	--	--	--

		组织工作，会议文件的准备、整理等辅助工作。	组织工作，会议文件的准备、整理等辅助工作。	
--	--	-----------------------	-----------------------	--

注：

1. 说明：应对照磋商文件“第三章 采购需求”中的技术要求逐条作出明确响应，并作出偏离说明。
2. 供应商应根据自身的承诺，对照磋商文件要求，在“偏离说明”中注明“正偏离”、“负偏离”或者“无偏离”。既不属于“正偏离”也不属于“负偏离”即为“无偏离”。

法定代表人或者委托代理人（签字或者电子签名）

供应商（电子签章）：南宁市微中子科技有限公司

日期：2026 年 7 月



4.项目质量控制措施方案

4.1 运维服务承诺书

运维服务承诺书

致:广西壮族自治区水运发展中心

我方作为投标人已熟知并愿意参加广西壮族自治区水运发展中心软硬件运维服务项目的投标。如果我方有幸中标,十分感谢评委及招标单位的信任,并对售后服务作出如下承诺:

1、我司书面承诺,运维服务期自合同生效之日起 12 个月。

2、提供 7*24 小时服务,在接到采购人系统故障报修后,30 分钟内实质响应,4 小时内到达现场,8 小时内确认修复方案,系统故障的最终修复从报修时间算起不能超过 72 小时。如遇较复杂问题,供应商应向采购人说明并征得采购人同意后,组织技术专家,会同采购人制定技术处理方案,并按方案约定时间要求修复系统故障。

3、为确保所有用户的问题得到及时反馈和解决,需要进行定期巡检,具体包括:软件运行巡检、数据库巡检、软件支撑环境巡检、主机资源性能巡检、项目设备硬件巡检等。

4、在运维期内服务响应不及时给招标人造成的损失,我司负责由此产生的一切后果,并进行经济赔偿。

5、我司承诺与本项目相关的集成商的友好合作。

供应商(电子签章): 南宁市微中鑫电子科技有限公司

日期: 2026 年 7 月 2 日



附件 4 成交通知书

中标(成交)通知书

南宁市微中鑫电子科技有限公司：

广西冠宇工程咨询有限公司受广西壮族自治区水运发展中心委托，就广西壮族自治区水运发展中心软硬件运维服务，项目编号:GXZC2026-C3-001837-GXGN采用竞争性磋商方式进行采购，按规定程序进行了开标、评标，经磋商小组评审，采购单位确认，贵公司为本项目标项二的成交人，成交金额:人民币捌拾柒万陆仟元整(¥876000.00元)。

请贵公司接此通知书后在25日历日内与采购单位签订合同，并按采购文件要求和响应文件的承诺履行完合同。

特此通知。

采购单位联系人：陆文 联系方式：0771-2115672

采购代理机构联系人：阮学燕 联系方式：0771-3940928



附件 5 履约保证金

中国建设银行网上银行电子回执							
币别：人民币元		日期：20260717		凭证号：108520888172			
				账户明细编号-交易流水号：1506-450604550F2D0MIV4FJ			
付款人	全 称 南宁市微中鑫电子科技有限公司			收款人	全 称 广西壮族自治区水运发展中心		
	账 号 45050160455000000157				账 号 2102101109221001515		
	开户行 中国建设银行股份有限公司南宁桃源支行				开户行 中国工商银行股份有限公司南宁分行		
大写金额	壹万柒仟伍佰贰拾元整			小写金额	17,520.00		
用 途	履约保证金			钞汇标志	钞		
摘 要	电子转账						



广西壮族自治区水运发展中心
业务专用章
3508025872587

附件 6 营业执照

1. 供应商为法人或者其他组织的提供其营业执照等证明文件

统一社会信用代码
91450107MA5L7AEL1Q (1-1)

营业执照
(副本)

扫描二维码
“国家企业信用信息公示系统”
了解更多登记、备案、许可、监管信息。

名称 南宁市微中鑫电子科技有限公司

类型 有限责任公司(自然人独资)

法定代表人 韦立英

经营范围 计算机软硬件技术开发、技术咨询、技术转让、技术服务、农业、林业的技术开发、计算机网络综合布线、网页设计(除经营互联网互联网信息服务); 图文设计、文化艺术交流活动策划、企业营销策划(以上三项除国家有专项规定外); 设计、制作、代理、发布国内各类广告; 计算机软硬件维修维护服务、通讯设备安装(除国家专控产品); 销售:计算机软硬件及配件、电子产品、通讯产品、安防产品(以上三项除国家专控产品); 办公设备、照明设备、家居用品、家具、化工产品(除危险化学品)、家用电器、五金交电、农副产品产品(仅限初级农产品)、日用百货、服装鞋帽、机电设备、化妆品、工艺品、建筑装饰材料(除危险化学品及木材)、货物仓储(仅限分支机构经营); (依法须经批准的项目, 经相关部门批准后方可开展经营活动。)

注册资本 伍佰万圆整

成立日期 2017年06月15日

住所 南宁市西乡塘区衡阳东路51号3栋C单元三层305号房

登记机关
2024
12
年 月 日

国家企业信用信息公示系统网址:
<http://www.gsxt.gov.cn>

国家市场监督管理总局监制

附件 7 授权委托书

2. 法定代表人身份证明书及法定代表人有效身份证正反面复印件

法定代表人证明书

供应商名称: 南宁市微中鑫电子科技有限公司
地 址: 南宁市西乡塘区衡阳东路 51 号 3 栋 C 单元三层 305 房
姓 名: 韦立英 性 别: 女
年 龄: 35 职 务: 总经理
身份证号码: 452132199109101220

系南宁市微中鑫电子科技有限公司（供应商名称）的法定代表人。

特此证明。

附件：法定代表人有效身份证正反面复印件



供应商（电子签章）：南宁市微中鑫电子科技有限公司

日期：2026 年 月 日



注：自然人竞标的无需提供，联合体竞标的只需牵头人出具。

3. 授权委托书及委托代理人有效身份证正反面复印件

答：投标人为法定代表人，无需授权委托书。

供应商（电子签章）：南京市微中鑫电子科技有限公司

日期：2026 年 7 月 2 日



注：1. 法定代表人必须在授权委托书上签字或者盖章或者电子签名，委托代理人必须在授权委托书上签字或者电子签名，否则其响应文件按无效响应处理。

2. 法人、其他组织竞标时“我方”是指“我单位”，自然人竞标时“我方”是指“本人”。