SZC20230914000066

中共兰州市委网络安全和信息化委员会办公室

网络安全事件监测、处置服务项目（三包）

政府采购合同

兰州市财政局政府采购
合同备案专用章
合同备案号:2023HTBA08169

备案编号：169001JH034-3

项目名称：中共兰州市委网络安全和信息化委员会办公室网络安全事件监测、处置服务项目（三包）

项目编号：169001JH034-3

包　　号：3

甲方（采购人）：中共兰州市委网络安全和信息化委员会办公室

乙方（成交供应商）：奇安信网神信息技术(北京)股份有限公司

2023年9月

中共兰州市委网络安全和信息化委员会办公室网络安全事件监测、处置服务项目（三包）政府采购项目合同

甲方(采购人)：中共兰州市委网络安全和信息化委员会办公室

乙方（中标人）：奇安信网神信息技术(北京)股份有限公司

为了保护甲、乙双方合法权益，根据《中华人民共和国民法典（合同编）》、《中华人民共和国政府采购法》及其他有关法律、法规、规章，双方签订本合同。

一、合同文件

下列文件均为本合同不可分制的组成部分，具有同等法律效力：

1.本合同条款及条款中所包含的附件

2.招标文件澄清及招标文件

3.投标文件澄清及投标文件

4.中标通知书

5.形成合同的其他有关文件，包括甲乙双方就具体单项服务内容签订的合同。

上述文件互为补充和解释，如有不清或相互矛盾之处，以甲方指定的为准，但甲、乙双方有特别约定的除外。

二、合同总价

本合同总价(大写):叁拾柒万捌仟元整，(小写):378000.00元。本合同费用为闭口含税价，已包括但不限于乙方完成全部工作所需的技术服务、图文设计、数据维护、信息发布服务、人工、材料、机械、设备、管理、利润、风险、税费、规费、第三者责任等一切与本合同所涉工作相关的成本、费用及利润。除此之外，甲方无须支付乙方任何费用。

三、付款方式

1.本合同项下所有款项均以人民币支付。

本合同分三次付款，甲方在双方签订合同且收到乙方开具的合格发票后支付合同价款90000（大写：玖万元整），项目运行过半中期验收合格且收到乙方开具的合格发票后支付合同价款的250000（大写：贰拾伍万元整）;余款38000（大写：叁万捌仟元整）作为质量保证金于服务运行满12个月并经甲乙双方复验合格并提供验收材料（包括但不限于图片、音视频和文档等）后付清。

2.服务的完成

乙方的服务应当按时，保质、保量完成，甲方对乙方提供的服务等进行跟踪、检测并及时反馈意见，乙方根据甲方的合理要求要及时调整，以确保网络安全事件监测、处置服务符合采购及合同要求。

3.开具发票

甲方付款前，乙方应按甲方要求开具合同全额发票（其中设备类开具增值税普通发票、服务类开具增值税技术服务费发票）。乙方应开具税务机关认可的合法发票，发票的开出者和收款人必须是乙方本身，服务内容、发票金额需与服务合同一致。乙方出具发票给甲方不视为甲方

已经付款，甲方付款均应以（转账/电汇/汇票）方式支付。如乙方未能开具发票或乙方开具的发票税务部门不予认可，甲方有权不予支付，甲方不承担任何责任。

乙方提交的发票必须真实、合法、有效。若乙方提交虚假发票，乙方必须在甲方规定时限内更换发票。甲方尚未支付款项的，甲方停止支付直至乙方发票符合约定；甲方已支付款项的，乙方应在甲方通知后10日内重新开具，因此产生的一切费用和责任由乙方承担，乙方还应赔偿因此给甲方造成的损失。

4.甲方开票信息

(1)公司(单位)名称：中共兰州市委网络安全和信息化委员会办公室

(2)纳税人识别号：11620100MB0041187G

(3)开户银行：中国建设银行股份有限公司甘肃省分行营业部

(4)账户：62050140000100000701

(5)地址：兰州市城关区临夏路11号金达大厦13楼

(6)联系电话：0931-8463175

5.乙方账户信息

(1)公司名称：奇安信网神信息技术(北京)股份有限公司

(2)纳税人识别号：911101087855446996

(3)开户银行：招商银行北京建国路支行

(4)账号：110902261210404

(5)地址：北京市西城区西直门外南路26号院1号楼2层

(6)联系电话：010-62972893

四、合同履行时间

1年，2023年10月27日至2024年10月26日。

五、服务内容

协助兰州市级单位处置现场发生信息破坏事件（篡改、泄露、窃取、丢失等）、大规模病毒事件、网站漏洞事件等信息安全事件。威胁情报的预警响应服务是基于网络安全威胁情报来监测和管理兰州市级单位互联网资产的安全健康状态，主动给兰州市委网信办提供安全事件预警、分析以及处置解决方案的安全服务。通过已在互联网上暴露的攻击者，利用大数据进行关联分析和行为画像，精确地标签出攻击者威胁情报，主动的为我们的用户提供安全预警通告。可帮助兰州市级单位保持其IT基础设施的更新，让各单位安全专业人员更好地积极阻止安全漏洞，并采取行动来防止数据丢失或系统故障，从而有效地抵御攻击者。

六、合同实施地点

甘肃省兰州市。

七、合同双方的责任与义务

（一）甲方权利

1.甲方有权随时向乙方了解工作并要求乙方提供相关资料。在工作完成后，对产品及服务内容进行验收评估。

2.甲方有权按照合同的约定及有关法律法规和政府管理的相关职能规定，对服务内容和质量进行监督和检查；但甲方并不因行使该等监督和检查权而承担任何责任，也并不因此减轻或免除乙方根据本合同或相关法律法规的要求而应承担的任何义务或责任。

3. 对于乙方提供的服务，甲方有权要求乙方按照甲方的修改意见进行改进。乙方拒绝改进或者多次改进仍然无法达到甲方标准的，甲方有权解除合同。

4. 乙方项目承担的工作成员若在提供服务过程中发生重大事故或不配合甲方工作，影响工作推进的，甲方有权要求更换相应小组成员由此产生的法律责任由乙方自行承担，若对甲方产生连带责任的，由乙方赔偿对甲方造成的损失（包括但不限于差旅费、诉讼费、律师费等）。

（二）甲方义务

1. 甲方应在达到合同约定的付款条件后，按时向乙方支付合作费用。

2. 甲方有义务为乙方的服务提供如下协助：

（1）提供项目服务所需的各种文件、数据和资料等。

（三）乙方权利

1. 乙方达到合同约定的付款条件后，向甲方提出付款申请。

（四）乙方义务

1. 乙方承诺具有从事本合同约定所需的法定资质，并保证资质的真实性、合法性和有效性。

2. 乙方应当接受并配合甲方或甲方组织的对本合同履行情况的监督与检查，对于甲方提出的问题，应及时作出合理解释或予以纠正。

3. 乙方承诺用自己的人员、技术、设备和劳动完成本合同所涉全部工作，不将该工作交付任何第三方；若乙方违反本条约定，未经甲方书面同意，擅自将工作交付第三方完成的，甲方有权解除合同，乙方应当承担违约责任并赔偿甲方一切损失；甲方认可并使用第三方完成的工作成果

的，甲方对第三方不负任何义务，由乙方对第三方承担付款等全部义务并对第三方完成的工作成果承担连带责任保证。

4.乙方保证交付甲方的工作成果内容、形式等符合法律、法规及规范性文件的要求，不存在侵害任何第三方合法权益的情形。乙方交付的工作成果如因违反法律法规或侵害第三方合法权益(如知识产权等）被政府相关部门处罚或任何第三人对此主张权利（包括采用投诉、申告、诉讼或非诉讼等一切方式)，则由乙方承担全部的赔偿、补偿等经济、法律责任，与甲方无关。如甲方因本协议的签订或履行而受到处罚或者被第三人主张权利（包括采用投诉、申告、诉讼或非诉讼等一切方式)，乙方除承担全部赔偿、补偿及其他经济、法律责任外，还应负责赔偿甲方的损失和甲方支付的费用。

5.其他本合同未详细列明事项，但根据甲方签订本合同的目的判断属于乙方服务范围的工作，乙方应尽职尽责完成。

6.在提供服务和项目执行过程中，乙方应遵从相关安全指引，全面履行本服务中的相关安全管理职责，避免发生安全事故。因乙方提供服务发生安全事故的，由乙方承担相应的法律责任。

7.乙方在提供服务过程中不得造成甲方名誉、财产、设施上的损害，不得侵犯他人权利。

8.乙方为本服务项目之外的而依据本合同签订的相关文件应当符合本合同的要求且不得与本合同相抵触。

9.乙方应建立健全服务报告制度，按要求定期向甲方报告服务完成情况、成果总结等材料。

10. 在本次合作的任何环节，在未经甲方书面同意的情况下，乙方不得进行任何业务营销宣传或者以甲方名义进行任何业务营销的宣传行为，否则甲方有权解除合同，并要求乙方向按照合同总价款30%承担违约金，给甲方造成不利社会影响或造成损失的，乙方还应消除不利影响并赔偿甲方的损失（包括但不限于经济损失）。

11. 在签订合同后，如因业务发展需求对本协议现有内容进行补充、变更，由双方或任何一方提出补充、变更的建议和方案，经双方协商并达成统一意见后，以书面形式确定，并由双方签字盖章后补充为本协议的附件，与本协议具有同等法律效力。

12. 合同签订后，乙方严格按照合同要求进行网站安全防护服务，并在合同规定时间内提供技术支持服务。

13. 乙方负责向甲方提供网络安全档案资料整理服务。

14. 甲、乙双方应签订保密协议书，保密协议书作为签订合同的附件。

八、知识产权

1. 甲乙双方确认，乙方向甲方提供服务的相关知识产权（包括但不限于著作权、商标权、专利权等）归乙方所有，但甲方在服务期限内可以无偿使用。提供服务并不视为对该服务相关的知识产权进行转让。合同期间乙方提供的报告类文档其署名权及知识产权归甲方所有。在本合同执行过程中，因使用乙方提供的服务或产品而产生的任何侵权行为与甲方无关。若因乙方上述服务或产品给甲方造成损失的，由乙方负责赔偿甲方的全部损失，该损失包括但不限于甲方缴纳的罚款、对第三方的赔付以及甲方因采取行动减少损失或向乙方追偿而发生的中介费、评估

费、鉴定费、调查取证费、案件受理费、保全费、诉讼财产保全责任保险保费、公告公证费、邮寄送达费、律师代理费等与此相关的成本和费用。

2.甲乙双方在合作过程中知悉的对方一切商业秘密，包括但不限于有关本合同合作双方的公司资料、业务信息、技术资料及本合同项下的服务价格、合作条件等书面或口头信息，双方均承诺严格遵守保密约定。未经对方书面确认许可，任何一方均不得泄露、使用或许可给第三方使用。如侵犯第三方知识产权，责任由乙方承担。

3.本条款的适用不因合同解除或终止而失效。

九、保密条款

1.未经甲方事先书面许可或本协议另有约定，乙方不得向任何第三方（有关法律、法规、政府部门、证券交易所或其它监管机构要求除外）泄露本协议条款的任何内容以及本协议的签订及履行情况，以及通过签订和履行本协议而获知的甲方及甲方关联单位的任何信息，且保证其雇员或委托方也承担相应的义务。但为本协议履行之需任何一方可向其法律、会计、商业及其它顾问、授权雇员（“接收方代表”）披露前述信息，接收方代表应同意承担与本协议中所规定的保密义务相同或更严格的保密义务。信息披露方对因信息泄漏而导致的不利后果，与泄漏方承担连带责任保证。

2.如乙方向任何第三人泄漏或公开本协议内容及本协议的签订及履行情况，以及通过签订和履行本协议而获知的甲方及甲方关联单位的任何信息使甲方遭受损失的，应按照合同总金额的30%向甲方承担违约金，

违约金不足以弥补甲方实际损失的，乙方还应赔偿甲方的全部损失。

3. 在任何情形下，本条所规定的保密义务应永久持续有效。

4. 乙方应与甲方一并签订保密合同或协议，合同或协议附后。

5. 双方应对在合同履行过程中所获得的对方的所有信息承担保密义务。如果乙方违反保密条款约定，甲方有权根据违反的程度以及造成的损害，要求赔偿损失或通过法律手段进行解决。

6. 目标单位提供的相关信息可能涉及敏感信息，仅供委托方内部工作之需，不应复制、传播或向第三方提供。

7. 双方不得向第三方泄露本委托协议的任何内容，以及通过签订和履行本协议过程中所获知的对方及其关联机构的任何信息。

8. 乙方向甲方借阅相关资料必须履行签收手续，在工作完成后，应如数归还，不得泄露或外传。甲方提供的任何资料，未经同意，乙方不得复制。

9. 乙方违反本保密规定使甲方遭受损失的，应按照合同总金额的30%向甲方承担违约金，并赔偿甲方的所有损失（包括但不限于经济损失）。

10. 本协议有效期内及终止后，本保密条款仍具有法律效力。

十、现场安保责任

成交供应商要采取必要措施维护好现场秩序，要制定好应急预案，根据应急预案组织好应急人员，准备好应急物资，履行本合同时，本合同项下的全部安全责任、人身损害责任等全部法律责任均由乙方承担。若因本合同履行，造成甲方损失的，由乙方赔偿，甲方因此承担责任的，甲方有权向乙方追偿。

十一、质量标准

符合国家标准，并与投标时承诺的质量相一致。

1.乙方应提供优质服务，保证服务质量，且不能低于合同规定的范围和种类。甲方将定期或不定期的对乙方提供的服务实行动态跟踪、检查。

2.乙方在收到甲方或使用单位关于服务质量同题，应按照招标文件的要求响应时间迅速查处并对处理结果书面答复。

3.如果乙方在收到通知3天后没有弥补缺陷，甲方自行采取必要的补救措施的，缺陷导致的风险和采取补救措施的全部相关支出由乙方承担。

十二、争议解决方式

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，如果协商不能解决争议，则向兰州仲裁委员会申请仲裁。

十三、质量保修及售后服务

按甲方要求及合同约定进行质量保修和售后服务，乙方所提供的服务应与招标文件规定的技术规格及所附的“技术规格响应表”相一致，不一致的以较高的质量要求为准；若技术性能无特殊说明，则按国家有关部门最新颁布的标准及规范为准。

十四、不可抗力

1.不可抗力是指不能预见、不能避免并不能克服的客观情况。

2.任何一方由于不可抗力而影响本合同义务履行时，可根据不可抗力的影响程度和范围延迟或免除履行部分或全部合同义务。但是受不可

抗力影响的一方应尽量减小不可抗力引起的延误或其他不利影响，并在不可抗力影响消除后，立即通知对方。

对于本条约定的上述情形，乙方应于该情形发生后3日内书面通知甲方并提供相关证明文件，未及时通知或未能按时提供证明文件的，视为上述情况未发生，乙方未能按合同约定向甲方提供服务的，视为乙方违约，甲方有权解除合同并且乙方应当按合同标的额的30%向甲方支付违约赔偿金。

因合同一方延迟履行合同后发生不可抗力的，不能免除延迟履行方的相应责任。

十五、税和关税

1. 对甲方征收的与本合同有关的一切税费均由甲方承担。

2. 对乙方征收的与本合同有关的一切税费均由乙方承担。

十六、违约终止合同

乙方出现下列情况之一的或在甲方认为需要时，甲方随时可向乙方发出书面违约通知书，提出终止部分或全部合同。

1. 如果乙方未能在合同规定的限期或甲方同意延长的期限内按合同约定的质量提供服务。

2. 如果乙方未能履行合同规定的其它任何义务。

3. 如果乙方不能按照合同的约定全面的向甲方提供服务，甲方有权解除或中止合同，并自行购买类似的服务，乙方对购买类似服务全部支出负责，并支付甲方由此遭受的全部损失。上述行为不影响乙方继续执行合同中未解除、未中止的部分。

十七、合同修改

任何对合同条件的变更或修改均须双方签订书面的修改协议。

十八、转让

除甲方书面同意外，乙方不得将自已应履行的全部或部分义务转第三方。

十九、合同的生效

本合同经双方法定代表人或委托代理人签字并加盖单位公章或合同专用章之日起生效。

二十、其他约定

1.本合同一式柒份，甲乙双方各执叁份，代理机构壹份，具有同等法律效应。

2.本合同未尽事宜由双方协商后对本合同进行书面修改或补充，书面修改和补充条款与本合同具有同等法律效应。

3.本合同附件为本合同不可分割的一部分，与本合同具有同等法律效力；如附件内容与本合同冲突的，本合同效力优先。

4.本合同应按照中华人民共和国的现行法律进行解释。

5.本合同签订地：甘肃省兰州市城关区。

6.文书送达地址确认条款

甲乙双方在此确认，本合同中双方各自填写的住所地址是双方指定接收各类法律文书、往来函件、通知的唯一邮寄地址，双方承诺上述住所地址信息均是真实、准确、完整的；且双方同意可采用在本协议中约定的电子邮箱地址进行电子送达的方式。双方约定的接受送达的地址及

接受电子送达的电子邮箱分别为：

甲方：中共兰州市委网络安全和信息化委员会办公室

住所地(接受送达地址)：兰州市城关区临夏路11号金达大厦13层

委托代理人：陈佳

联系电话：13639397775

甲方单位联系电话：0931-8159795

邮政编码：730030

电子邮箱(接受电子送达地址)：wxbaqk@163.com

乙方：奇安信网神信息技术(北京)股份有限公司

住所地(接受送达地址)：兰州市城关区南滨河东路5222号名城广场3号楼811室

法定代表人：冯新戈

委托代理人：宋建平

联系电话：13893300930

乙方联系电话：13893300930

传真：010-62972893

邮政编码：730030

电子邮箱(接受电子送达地址)：songjianping@qianxin.com

附件：1.《分项报价表》

2.《服务方案》

3.《中标通知书》

4.《保密协议》

本页为签署页，无正文

甲方：中共兰州市委网络安全和信息化委员会办公室（签章） 法定代表人 （或委托代理人/经办人）：陈佐 签字日期：2023 年 9 月 13 日	乙方：奇安信网神信息技术（北京）股份有限公司（签章） 法定代表人 （或委托代理人/经办人）： 签字日期：2023 年 9 月 13 日

附件1

分项报价表

服务名称	服务内容	服务数量	投标单价
应急响应服务	应急响应服务范围通常为兰州市级单位现场发生信息破坏事件(篡改、泄露、窃取、丢失等)、大规模病毒事件、网站漏洞事件等信息安全事件时，由中标服务商提供应急响应专家协助处置现场突发安全事件。其中应急响应事件服务范围具体包括以下内容：勒索病毒、挖矿木马、蠕虫病毒、APT事件、网站挂马、网站暗链、网站篡改、漏洞事件、数据泄露以及其他安全事件。	1年	60000
	基于威胁情报的预警响应服务是基于网络安全威胁情报来监测和管理兰州市级单位互联网资产的安全健康状态，主动给兰州市委网信办提供安全事件预警、分析以及处置解决方案的安全服务。通过已在互联网上暴露的攻击者，利用大数据进行关联分析和行为画像，精确地标签出攻击者威胁情报，主动的为我们的用户提供安全预警通告。可帮助兰州市级单位保持其IT基础设施的更新，让各单位安全专业人员更好地积极阻止安全漏洞，并采取行动来防止数据丢失或系统故障，从而有效地抵御攻击者。	1年	90000

	渗透测试服务是通过该项服务需要获得：兰州市级各单位基于Web的应用业务系统是否存在漏洞，漏洞验证服务，提高兰州市级单位处置漏洞修复的效率，攻击者威胁情报，协助兰州市级单位排查安全事件，漏洞二次校验及复测服务，通过资产梳理，准确定位兰州市级单位疑似受害面，针对关键信息业务系统，排查漏洞是否被利用渗透测试服务是通过工具加人工的方式对兰州市级单位互联网资产进行的漏洞检测，在测试实施过程中，测试人员首先使用自动化的安全扫描工具，完成初步的信息收集、服务判断、版本判断、补丁判断等工作。 然后由人工的方式对安全扫描的结果进行人工的确认和分析，并且根据收集的各类信息进行深入渗透测试测试人员在获取到普通权限后，尝试由普通权限提升为管理员权限，获得对系统的完全控制权，此过程将循环进行直到测试完成。测试过程采用交叉测试方式，每次测试至少两名工程师进行同时进行，通过不同角度更为全面的发现系统存在的安全问题。 根据渗透测试工作开展情况，出具详细的测试报告，重点描述测试发现的问题、严重程度，同时在报告中提供对安全漏洞及问题的整改建议，同时配合网信办一起讨论具体加固实施办法，规避安全整改风险，通过安全加固工作修复安全漏洞，降低安全风险。 在兰州市级单位实施完整改工作后，根据渗透测试报告及整改报告进行复测，以确认先前的安全漏洞得要有效的修复，同时没有引入新的安全漏洞，确保整改工作达到预期目标。	1年	138000
	提供一人/年技术支持服务，现场协助兰州市委网信办开展以上相关业务。	1人/年	900000
	大写：　　(人民币)叁拾柒万捌仟元整	合计	378000元

注：报价包含完成本项目所发生的所有费用。

合计总金额(大写)：叁拾柒万捌仟元整

附件2

服务方案

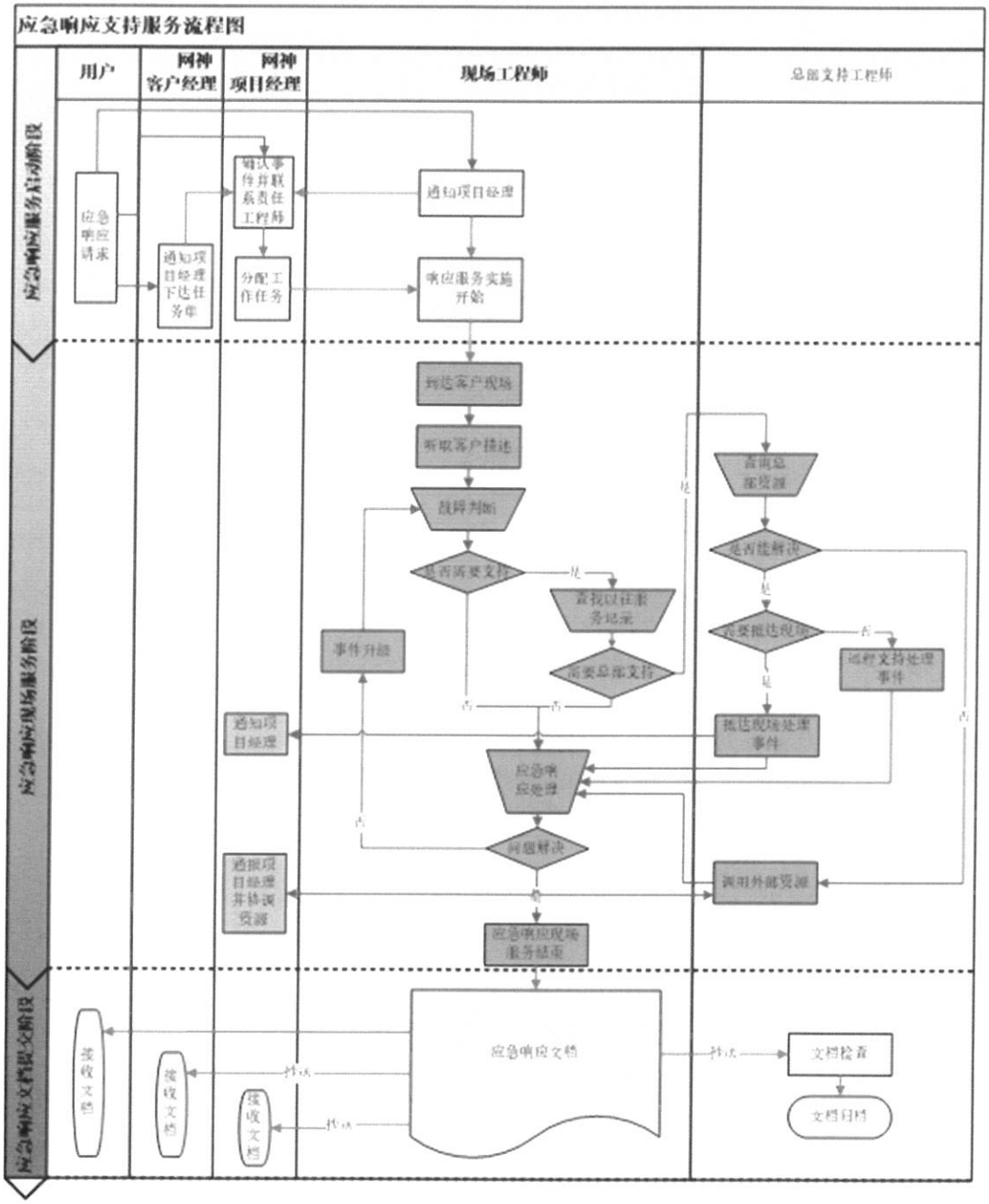
1. 应急响应服务

1.1 服务内容

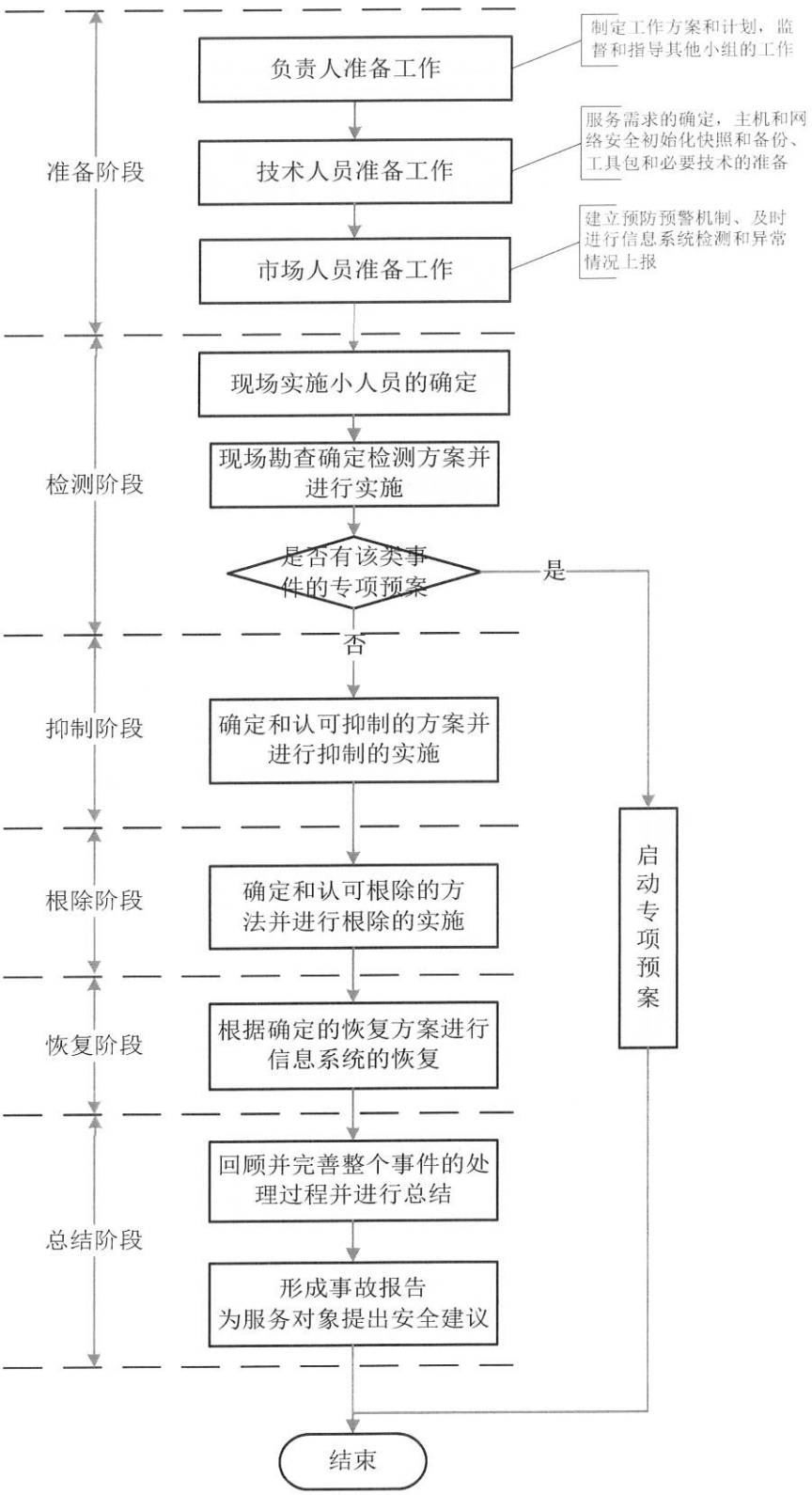
在项目服务期间，为兰州市委网信办提供应急响应服务，当出现安全事件时，网神工程师会第一时间进行协助处理，完成安全事件的应急响应工作。

1.1.1 工作流程

根据我公司长期的项目和工作积累，在开展应急响应工作中需要采用如下工作流程，确保能够取得可控的工作成果，具体如下图所示：


应急响应支持服务流程图
用户
网神客户经理
网神项目经理
现场工程师
总部支持工程师
应急响应服务启动阶段
应急响应现场服务阶段
应急响应文档提交阶段
应急响应请求
通知项目经理下达任务单
确认事件并联系责任工程师
分配工作任务
通知项目经理
响应服务实施开始
抵达客户现场
听取客户描述
故障判断
是否需要支持
查找以往服务记录
需要总部支持
事件升级
通知项目经理
查询总部资源
是否能解决
需要抵达现场
远程支持处理事件
抵达现场处理事件
应急响应处理
问题解决
通报项目经理并协调资源
调用外部资源
应急响应现场服务结束
应急响应文档
文档检查
文档归档
接收文档
接收文档
接收文档
是
否

现场处理流程如下：



应急响应处理流程主要分为六个阶段，包括响应阶段、检查阶段、抑制阶段、根除阶段、恢复阶段和总结阶段：

- 响应阶段

在实施应急响应工作前，客户经理或项目经理收到客户申请应急响应支持，由客户经理或项目经理协调相关技术支持人员和客户技术人员第一时间取得联系，了解事件发生情况。

技术人员判断事件类型，并与客户确认是否需要启用应急响应服务。

- 检测阶段

启用应急响应服务后，应急响应实施人员通过现场或非现场等方式进行信息收集，使用检测搜集流量信息、检测搜集系统信息及主机检测等多种技术手段对事件进行详细分析，并查找入侵痕迹。

最后确定安全事件类型，评估安全事件的影响。

- 抑制阶段

应急响应实施人员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，同时要与相关系统负责人沟通，确保抑制方法对涉及相关业务影响最小。

抑制阶段通常采用的技术手段如下：

1）确定受害系统的范围后，将被害系统和正常的系统进行隔离，断开或暂时关闭被攻击的系统，使攻击先彻底停止；

2）持续监视系统和网络活动，记录异常流量的远程IP、域名、端口；

3）停止或删除系统非正常帐号，隐藏帐号，更改口令，加强口令的安全级别；

4）挂起或结束未被授权的、可疑的应用程序和进程；

5）关闭存在的非法服务和不必要的服务；

6）使用反病毒软件或其他安全工具检查文件，扫描硬盘上所有的文件，隔离或清除病毒、木马、蠕虫、后门等可疑文件；

- 根除阶段

应急响应实施人员协助客户检查所有受影响的系统，在准确判断安全事件原因的基础上，提出基于安全事件整体安全解决方案，排除系统安全风险。

- 恢复阶段

应急响应实施人员协助客户恢复安全事件所涉及到的系统，并还原到正常状态，使业务能够正常进行，恢复工作应避免出现误操作导致数据的丢失。

- 总结阶段

在本阶段，所有参与应急的人员回顾并完善应急过程，完成记录表单填写并按流程提交至指定人员，并最终形成应急报告。

1.1.1.工作重点

应急响应工作需要重点做好如下内容：

做好安全事件的分类：由于安全事件种类繁多，对信息系统及用户使用的影响也不尽相同，如果对于安全事件产生不加以区别对待的话，将会造成资源过度投入或者不足，因此，我公司根据长期项目经验，为用户预拟定了安全事件级别分类和响应方式，能够快速准确保障响应服务的到位。

做好安全事件的快速发现：传统的安全事件响应方式都是被动响应，既不利于处理时间，也不利于影响控制。网神公司集团通过为

客户提供安全预警服务，能够有效帮助用户主动快速发现安全隐患，实现安全响应的防患于未然。

安全事件溯源：通过工具的海量、高质量数据，利用先进的人工智能模型，高精度的识别结果，和定制化的大数据存储与处理技术，在保障期间对重大的安全事件进行追踪及溯源。

1.1.2.交付成果

交付物资料包括不限于如下内容：

《安全事件应急响应报告》

1.1. 威胁情报预警响应服务

1.1.1.服务目的

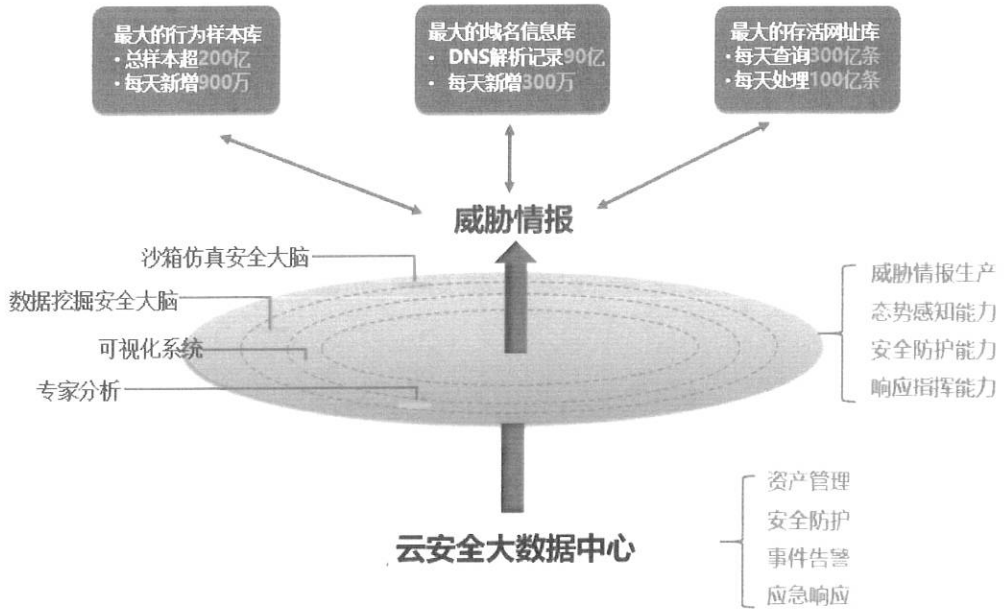
基于网络安全威胁情报来监测和管理兰州市级单位互联网资产的安全健康状态，主动给兰州市委网信办提供安全事件预警、分析以及处置解决方案。

1.1.2.工作说明

通过已在互联网上暴露的攻击者，利用大数据进行关联分析和行为画像，精确地标签出攻击者威胁情报，提供安全预警通告。

1.1.3.服务内容

依托自身威胁情报平台，多维度多方位提供威胁情报预警服务。



1.1.4.交付成果

交付物资料包括不限于如下内容：

《威胁情报预警信息》

1.2. 渗透测试服务

1.2.1.服务目的

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

1.2.2.服务内容

1、系统层安全渗透测试

系统安全脆弱点测试包括但不限于如下内容：

- 口令猜解

针对操作系统、数据库等应用的口令登录安全进行测试，利用自动化工具，并通过使用密码字典文件，大量尝试登录单位内部的系统，进而找出存在空口令、弱口令的系统账号。该测试存在一定的安全风险，因为当系统设备启用密码登录安全策略时，大量的尝试会造成账号锁定，导致拒绝服务攻击发生，故执行相关操作时需特别当心。

- 溢出测试

当无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统从新启动并开启原有服务即可。

- 敏感信息泄露

敏感信息的泄露会使系统存在于风险当中，如开启了不需要的服务、服务端口不恰当的对非授权区域开放、DNS区域传送机制未合理配置、特定系统服务（如Telnet、SSH、FTP等）旗标未修改屏蔽等，此类敏感信息的不合理控制，会给攻击者的信息收集以及系统攻击工作带来极大便利，因此，在本服务测试中将对此类信息进行重点排查。

- 系统安全管理

严格管理系统账户、有效控制系统服务，优化系统的安全配置，启用系统必要的安全控制措施，避免系统发生故障或遭受攻击。

- 系统漏洞

针对业务系统所需要的系统服务进行优化管理和配置。

- 系统访问控制和审计

对系统进行有效访问控制和日志审计。

2、Web 中间件渗透测试

针对Web常见的软件，例如Apache、IIS、Tomcat中间件等各类应用软件中常用到的软件，自身存在一些由于版本较低或配置不当所造成的安全隐患和漏洞，作为渗透测试的一些主要内容和方向。

- 缓冲区溢出

由于应用服务版本过低所造成的应用自身的安全漏洞。

- 路径和参数安全

由于对应用配置不足够所造成的路径和参数泄露。

- 测试和帮助页面

由于应用配置不足所造成的测试和帮助页面显示。

- 账号和口令

由于应用配置和测试导致无用账号或口令简单。

3、Web 应用渗透测试

针对Web常见的应用，重点是由于应用软件在设计和开发的过程中，由于安全设计不足和开发不规范所造成的隐患和漏洞，主要包括如下几类：

信息收集：

- 域名及 IP 信息收集

收集被测试网站的域名、二级域名、IP地址、对应的C段IP地址等信息。

- 系统信息收集

Web运行平台的操作系统信息、数据库信息。

- 中间件信息收集

Web应用的中间件信息，如Apache、Tomcat、Weblogic等。

- 信息系统开发框架信息

收集Web应用开发框架的信息，如Struts2。

- CMS 信息收集

探测并收集Web应用的应用类型、版本等。

- 其他信息

其他必要的渗透测试信息，如第三方组件等。

身份验证：

- 在未加密的网络链接上传递身份验证凭据或身份验证 cookie，这会引起凭据捕获或会话攻击；
- 利用弱密码和账户策略，这会引起未经授权的访问；
- 将个性化与身份验证混合起来。

授权：

- 使用越权角色和账户；
- 没有提供足够的角色粒度；
- 没有将系统资源限制于特定的应用程序身份。

输入和数据验证：

- 完全依赖于客户端验证；
- 使用 deny 方法而非 allow 来筛选输入；
- 将未经验证的数据写出到 Web 页；
- 利用未经验证的输入来生成 SQL 查询；
- 使用不安全的数据访问编码技术，这可能增加 SQL 注入引起的威胁；
- 使用输入文件名、URL 或用户名进行安全决策。

配置管理：

- 以明文存储配置机密信息，例如，连接字符串和服务帐户证书；

- 没有保护应用程序配置管理的外观，包括管理界面；
- 使用越权进程帐户和服务帐户。

敏感数据：

- 在不需要存储机密信息时保存它们；
- 在代码中存储机密信息；
- 以明文形式存储机密信息；
- 在网络上以明文形式传递敏感数据。

会话管理：

- 在未加密信道上传递会话标识符；
- 延长会话的生存期；
- 不安全的会话状态存储；
- 会话标识符位于查询字符串中。

加密：

- 使用自定义加密方法；
- 使用错误的算法或者长度太短的密钥；
- 没有保护密钥；
- 对于延长的时间周期使用同一个密钥。

参数管理：

- 没有验证所有的输入参数这使系统的应用程序容易受到拒绝服务攻击和代码注入攻击，包括 SQL 注入和 XSS；
- 未加密的 cookie 中包含敏感数据。攻击者可以在客户端更改 cookie 数据，或者当它在网络上传递时进行捕获和更改；
- 查询字符串和表单域中包含敏感数据。很容易在客户端更改查询字符串和表单域。

异常管理：

- 没有验证所有的输入参数；
- 显示给客户端的信息太多。

审核与记录：

- 没有审核失败的登录；
- 没有保护审核文件。

4、漏洞扫描

对网站或Web应用系统进行漏洞检测、漏洞验证、提出漏洞处置建议、安全加固方案、验证处置结果等工作。

漏洞来源包括漏洞扫描工具检测结果，CNVD 等实时发布的通用型漏洞。新系统的安全扫描主要包括对应用的所有配套设施的扫描检查和评估，包括新系统的运行操作系统、数据库系统、WEB 中间件和应用系统自身的扫描。具体的检查点包括：

设备/系统类型	子类型	说明
主机	端口扫描	主流端口的扫描/识别，例如HTTP、FTP、Telnet、VNC、Teamview等等
	操作系统漏洞	可以覆盖主流的操作系统，包括：Windows系列，Linux系列，Unix系统、Soliar系统等
	弱口令	
数据库系统	数据库系统漏洞	可以覆盖主流的结构化数据库，包括：SQL Server，My SQL，DB2、Oracle、PostGresql、Sybase等。
	数据库系统的弱口令	
中间件	中间件系统的漏洞	可以覆盖主流的Web中间件，例如Apache、Tomcat、Weblogic等
应用漏洞	注入漏洞	包括：命令注入、XML注入、SQL注入、Xpath注入等
	跨站脚本漏洞	包括存储型XSS、反射型XSS、跨站请求伪造等
	输入验证漏洞	包括缓冲区溢出、HTTP变量欺骗测试、HTTP参数污染测试等

	错误配置	敏感信息的文件扩展名处理测试、HTTP严格传输安全测试和RIA跨域策略测试等
	不良实现	完整性校验、处理时间限制、请求次数的限制等
	敏感信息泄露	信息外泄的问题
	未授权访问漏洞	授权绕过、URL未认证等
	其他漏洞	根据最新OWASP更新的Top10漏洞

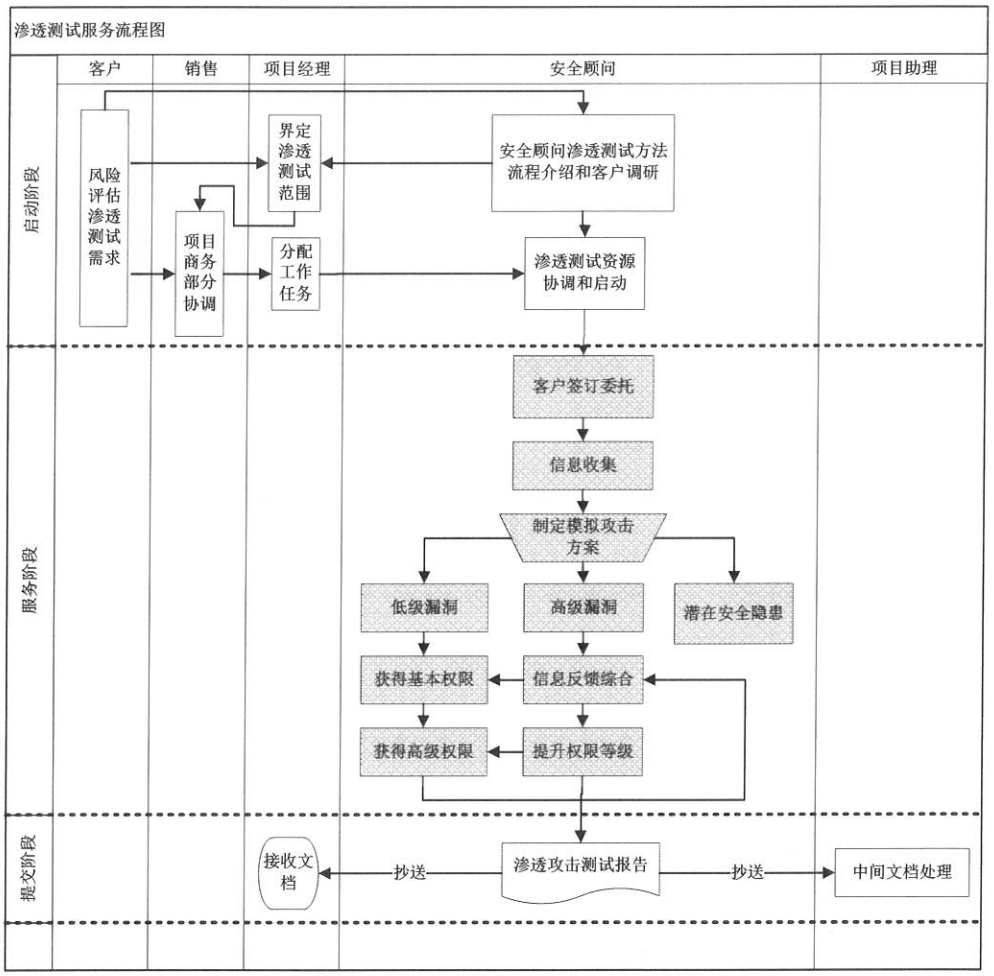
5、整改建议和复测

根据渗透测试工作开展情况，出具详细的《信息系统渗透测试报告》，重点描述测试发现的问题、严重程度，同时在报告中提供对安全漏洞及问题的整改建议，同时配合用户单位或者第三方公司一起讨论具体加固实施办法，规避安全整改风险，通过安全加固工作修复安全漏洞，降低安全风险。

在实施完整改工作后，根据《信息系统渗透测试报告》及整改情况进行复测（回归测试），以确认先前的安全漏洞得要有效的修复，同时没有引入新的安全漏洞，确保整改工作达到预期目标，并输出《信息系统渗透测试复测报告》

1.2.3.服务流程

服务工作的流程如下：



1.2.4.风险及规避

对于Web进行渗透测试常用的手法不会对服务器造成较大影响，对某些诸如超长字符串类溢出测试可能会导致服务停止。

建议尽量在测试环境内完成渗透测试；对于无法搭建测试环境的应用，我们将在进行可能引起服务器异常的操作时，首先通告客户，并在获得批准后进行实施。

1.2.5.交付成果

交付物资料包括不限于如下内容：

《信息系统渗透测试及复测报告》

1.3. 技术支持服务

1.3.1.服务目的

网神提供一人/年技术支持服务，现场协助兰州市委网信办威胁情报预警响应、渗透测试、应急响应等业务的开展。

1.3.2.工作说明

在项目服务期间，技术服务人员协助兰州市委网信办开展威胁情报预警响应、渗透测试、应急响应等工作。

威胁情报预警响应，依托自身威胁情报平台，多维度多方位提供威胁情报预警服务，周期性进行安全预警推送，并提供安全加固建议。

渗透测试，通过网神自研工具，依托网神内部武器库系统，针对兰州市级单位互联网资产进行渗透测试工作，更加快速的发现互联网资产的脆弱性，并提供修复方案。

应急响应，依托网神自研日志分析系统，通过分析 windows，linux 操作系统日志，安全日志，web 访问日志，各类中间件日志，进行应急溯源处置，按照网神积累的大量应急经验，标准化流程化的处理安全事件。

1.3.3.交付成果

交付物资料包括不限于如下内容：

《威胁情报预警信息》

《信息系统渗透测试报告》

《安全事件应急响应报告》

附件3

中标通知书

中 标 通 知 书

169001JH034

甘肃铠聚项目管理有限公司 受 中共兰州市委网络安全和信息化委员会办公室 的委托，对 中共兰州市委网络安全和信息化委员会办公室网络安全事件监测、处置服务项目 政府采购项目以公开招标方式进行采购，按照该项目招标文件规定，已于 2023年09月07日 进行了开、评标。最终确定该项目 第二包 中标供应商： 奇安信网神信息技术（北京）股份有限公司，中标金额：叁拾柒万捌仟元整(378000.0元)

中标通知书对采购人和中标供应商均具有法律效力，一式四份，涂改无效。请采购人与中标供应商在中标通知书发出之日起30日内据此办理有关手续。

甘肃铠聚项目管理有限公司

2023 年 09 月 07 日

兰州市公共资源交易中心

2023 年 09 月 08 日

附件4

保密协议

甲方：中共兰州市委网络安全和信息化委员会办公室

乙方：奇安信网神信息技术(北京)股份有限公司

根据甲方相关保密制度和规定，为明确双方在业务合作中的保密责任和义务，经共同商定，签署此《保密协议》。

第一条 定义

保密信息：指甲方向乙方提供的，属于甲方原有的下列资料及原有在信息载体上明确标示“密级”的材料和信息。网络扑拓图、网络资源规划图及各种方案、员工、领导的姓名及电话号码、网络设备的配置、服务器布署情况等非公开的、保密的或专业的信息和数据。

第二条 乙方在接受保密信息后，必须承担以下义务：

1、对保密信息谨慎、妥善持有，并严格保密，没有甲方事先书面同意，不得向任何第三方泄露；

2、乙方仅可为双方合作业务之必需时，才能将保密信息披露给其直接或间接参与合作事项的管理人员、职员、顾问和其他雇员（统称“有关人员”），但应保证该类有关人员对保密信息严格保密；

3、若具有权力的法庭或其他司法、行政、立法机构要求乙方披露保密信息，乙方应立即通知甲方此类要求；

4、若乙方或有关人员违反本协议的保密义务，乙方须承担相应责任，并赔偿甲方由此造成的损失。

5、乙方向甲方借阅相关资料必须履行签收手续，在工作完成后，应如数归还，不得泄露或外传。甲方提供的任何资料，未经甲方同意，乙方不得复制。

6、凡与工作事项无关的内容，乙方不得询问、记录。

7、未经甲方书面同意，乙方不得将其在本协议书项下的权利和义务转让给第三方。

8、服务完成后，乙方应将涉密系统资料全部移交给甲方，不得私自留存或擅自处理。

第三条 乙方违反以上条款，致使甲方在相关考核中被扣分或罚款处理，由此造成的经济损失由应由乙方承担。如泄漏甲方保密事项，给国家或者甲方造成危害，甲方将依据有关法律规定，追究乙方责任。

第四条 因执行本协议而发生纠纷，可以由双方协商解决或者共同委托双方信任的第三方调解。协商、调解不成或者一方不愿意协商、调解的，任何一方都有权向向兰州仲裁委员会申请仲裁。

本协议一式柒份，甲乙双方各执叁份，代理机构壹份，双方签字盖章后即可生效。

甲方：中共兰州市委网络安全和信息化委员会办公室（签章）

法定代表人(或委托代理人)（签字）：

2023年9月13日

乙方：奇安信网神信息技术(北京)股份有限公司（签章）

法定代表人(或委托代理人)（签字）：

2023年9月13日