合同编号：JSZKY2600179CGN00

# 江苏省农业农村厅2026年度网络与数据安全支撑

# 保障运维服务合同

委托方（甲方）：江苏省农业信息中心

地址：南京市龙江小区月光广场8号

法定代表人/负责人：王平涛

项目联系人：徐月洁、马陈承

联系电话：025-86263604

受托方（乙方）：中国电信股份有限公司江苏分公司

地址：南京市中央路260号

法定代表人/负责人：彭鹏

项目联系人：魏家植

联系电话：15301582498

甲、乙双方根据政府采购编号JSZC-320000-ZCZB-C2026-0003**江苏省农业农村厅2026年度网络与数据安全支撑保障运维**服务竞争性磋商采购的结果，经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下合同，并由双方共同恪守。

第一条 甲方委托乙方进行服务的内容如下：

1.1 服务的目标：江苏省农业农村厅2026年度网络与数据安全支撑保障运维。

1.2 服务的内容：见附件1。

1.3 服务的方式：人员驻场和设备保障服务。

第二条 项目周期和服务地点：

2.1 服务地点：江苏省农业农村厅。

2.2 服务周期：1年，自合同签订之日起计算。

第三条 为保证乙方有效进行服务工作，甲方应当向乙方提供必要的资料及工作

条件。

第四条 甲方向乙方支付服务报酬及支付方式为：

4.1 本合同费用总额（含税价）：人民币大写**壹佰捌拾叁万伍仟**元整，小写**1835000.00**元。

本合同费用总额已包括甲方就乙方履行本合同所应支付的全部报酬、所需的全部费用及税费（包括但不限于营业税、增值税等）。

除另有约定外，甲方无需就本合同项下委托事项向乙方支付上述费用之外的任何其他费用及税费（包括但不限于营业税、增值税等）。

4.2 甲方凭乙方开具的相应金额的、符合国家规定的[增值税专用/增值税普通/营业税/其他]发票支付本合同费用总额，并按以下第2种方式向乙方付款：

（1）一次性支付：[/]。

（2）分期支付：①合同签订后7个工作日内，乙方需向甲方缴纳合同总价10%的资金额度作为该项目的履约保证金（乙方也可按甲方要求提交相关银行出具的针对该项目的同等额度履约保函），甲方在收到乙方缴纳的履约保证金（或提交的履约保函）后7个工作日内，向乙方支付合同总价50%的项目款，作为预付款。②2026年12月底前，经甲方确认乙方无服务质量问题并通过项目阶段性考核后7个工作日内，由甲方视实际情况向乙方支付合同总价的50%。③合同履约结束，经甲方确认乙方无服务质量问题并通过项目验收后7个工作日内，由甲方向乙方退还履约保证金（或协助乙方完成履约保函撤销手续）。

4.3 因乙方未按甲方要求出具相应票据导致的延迟付款，甲方不承担违约责任。若乙方提供发票顺延/遇法定节假日的，则甲方的付款时间相应顺延。

4.4 本项目的付款时间为甲方向政府采购支付部门提出支付申请的时间，不含支付部门审查的时间，乙方应充分理解年初财政预算下达和支付审核所需时间，不因此延迟交付成果和向甲方索赔任何额外费用及追究甲方责任。

4.5 本合同费用总额的所有支付由甲方以银行转账方式（银行转账方式）付至乙方指定的收款银行账户。甲、乙双方指定的收款银行账户信息如下：

| 甲方信息如下： | 乙方信息如下： |
| --- | --- |
| 开户行：南京市工行龙江支行 | 开户行：工商银行城北支行 |
| 户名：江苏省农业信息中心 | 户名：中国电信股份有限公司南京分公司 |
| 账号：4301024109100026043 | 账号：4301010919001154390 |

行号：102301001166　　行号：102301000028

4.6 若根据本合同约定乙方应当支付违约金和/或承担赔偿责任，则甲方有权从上述任何一笔付款中直接扣除相应金额。上述款项不足以支付违约金或赔偿金的，甲方可向乙方另行主张，该违约金或赔偿金包括甲方因乙方的违约行为所支出的律师费、诉讼费、鉴定费、交通费、和解金额或生效法律文书中规定的赔偿金额等合理支出。

第五条 保密

5.1 乙方对甲方所提供的所有资料以及在本合同签订、履行过程中所接触到的甲方及其关联单位的商业秘密、技术资料、客户信息等资料和信息（统称"保密资料"）负有保密义务。未经甲方书面许可，乙方不得向任何第三方披露，不得将保密资料的部分或全部用于本合同约定事项以外的其他用途。乙方有义务对保密资料采取不低于对其本身商业秘密所采取的保护手段予以保护。乙方可仅为本合同目的向其内部有知悉保密资料必要的雇员披露保密资料，但同时须指示其雇员遵守本条规定的保密及不披露义务。

5.2 乙方仅有权为履行本合同之目的对保密资料进行复制。乙方不得以任何方式（如软硬盘、图纸、采样、照片、菲林、光盘等）留存保密资料。乙方应当在完成委托事项或本合同终止或解除时将保密资料原件全部返还甲方，并销毁所有复制件。乙方应当妥善保管保密资料，并对保密资料在乙方期间发生的被盗、泄露或其他有损保密资料保密性的事件承担全部责任，因此造成甲方损失的，乙方应负责赔偿。

5.3 当出现下述情况时，本条对保密资料的限制不适用。当保密资料：

（1）并非乙方的过错而已经进入公有领域的。

（2）已通过该方的有关记录证明是由乙方独立开发的。

（3）由乙方从没有违反对甲方的保密义务的人合法取得的。

（4）法律要求乙方披露的，但乙方应在合理的时间提前通知甲方，使其得以采取其认为必要的保护措施。

5.4 如乙方违反本合同关于保密的约定，乙方应赔偿因此而给甲方造成的一切损失。

5.5 本保密条款自保密资料提供或披露之日起至本合同终止或解除后 3 年内持续有效。

第六条 未经甲方事先书面同意，乙方不得将本合同项目部分或全部服务工作转由第三人承担。

第七条 违约责任

7.1 双方确定，任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

7.2 乙方未能按本合同约定按期提供服务的，每逾期 1 日，乙方应当按照本合同费用总额的 1‰向甲方支付违约金。逾期超过 30 日的，甲方有权终止本合同，乙方仍应支付上述违约金、退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息。

7.3 乙方提供服务不符合本合同要求的，乙方应当按照甲方要求更正和修改，并承担由此产生的全部费用。同时，甲方有权终止本合同，乙方应当退还甲方已支付款项并按照同期中国人民银行贷款利率计付利息，并赔偿甲方的相应损失。

第八条 双方确定，在本合同有效期内，甲方指定**徐月洁、马陈承**为甲方项目联系人，乙方指定**魏家植**为乙方项目联系人。一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或，若造成损失的，应承担相应的责任。

第九条 双方确定，出现下列情形之一，致使本合同的履行成为不必要或不可能的，可以解除本合同：

9.1 发生不可抗力。

9.2[政策变化原因]。

第十条 法律适用和争议解决

10.1 本合同适用中华人民共和国法律。

10.2 所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可向甲方所在地有管辖权的人民法院起诉。诉讼进行过程中，双方将继续履行本合同未涉诉讼的其它部分。

第十一条 双方确定，本合同及相关附件中所涉及的有关名词和技术术语，其定义和解释如下：

11.1“不可抗力”：地震、台风、水灾、火灾、战争以及其它本合同各方不能预

见，并且对其发生和后果不能防止或不能避免且不可克服的客观情况。

11.2[/]。

第十二条 双方约定本合同其他相关事项为：

12.1 任何一方未经另一方同意，不得向任何第三方透露本合同的签订及其内容。甲方向其关联单位透露的，不在此限。

12.2 任何与本合同相关但未在本合同中明确规定的事项将由双方另行友好协商解决。对本合同作出的任何修改和补充应为书面形式，由双方签字并加盖单位公章或合同专用章后成为本合同不可分割的部分。本合同与其补充合同或补充协议冲突时，以补充合同或补充协议为准。

12.3 本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、合同和协议。

12.4 甲乙双方因履行本合同或与本合同有关的一切通知都必须按照本合同中的地址，以书面信函形式或双方确认的传真或类似的通讯方式进行。采用信函形式的应使用挂号信或者具有良好信誉的特快专递送达如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。任何一方变更送达地址的，应当立即通知另一方，否则，按照本合同地址送达的视为已送达。

第十三条 本合同自双方法定代表人或授权代表签字并加盖单位公章或合同专用章之日起生效。本合同一式肆份，甲方执贰份，乙方执贰份，具有同等法律效力。

第十四条 附件为本合同不可分割的部分。若附件与合同正文有任何冲突，以合同正文为准。

甲方：江苏省农业信息中心

法定代表人/负责人

或授权代表：（签字）王平涛

2026 年 5 月 29 日

甲方：中国电信股份有限公司江苏分公司

（法定代表人/负责人

或授权代表）（签字）

2026 年 5 月 29 日

附件 1：

# 服务内容

## 一、概况

为全面落实厅党组网络安全工作责任制要求，切实提升厅机关及直属单位网络与数据安全保障能力，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规，进一步提升全厅信息系统、计算机网络与数据安全运行保障能力。本项目将围绕全厅在建在用政务信息系统及相关联网计算机及网络设施资产，通过开展全维度安全检测、风险评估、攻防演练、应急处置、制度建设、安全运维支撑和数据安全检查等系列工作，健全安全管理体系，强化技术防护能力，提升全员安全意识，完善应急响应机制，全面夯实全厅网络与数据安全保障基础，确保政务信息系统和厅计算机网络安全稳定运行。

## 二、内容

1、服务要求

（1）资产管理：全面开展厅机关及直属单位信息化资产全生命周期核查管理工作。采用内部自查与上门清查相结合、人工统计与技术探测相结合的方式，对全厅所有联网信息化资产开展拉网式、全覆盖核查。核查范围覆盖厅机关及所有直属单位，包含但不限于部署于互联网、政务外网、政务云、阿里云等所有非涉密网络环境下的服务器、终端、网络设备、安全设备、业务系统、网站等全类型信息化资产。建立全厅统一的信息化资产台账，实现资产动态更新管理，并严格按照省委网信办相关工作要求，按时保质完成资产普查、信息动态更新及规范上报工作。

（2）制度规范：落实国家、省有关法律法规和政策标准，协助甲方在全面梳理摸排全厅安全管理资产的基础上，研究制定科学合理、具有可操作性的标准规范与管理制度，主要工作内容包括：

1） 制定安全运营管理制度，细化网络和数据安全事件监测预警、事件处

置、服务外包管理等工作要求，明确安全事件分类、预警等级、监测手段、监测要求，细化预警流程及责任分工。

2) 协助完善安全事件报告机制，优化完善安全事件处置流程，保障安全事件信息及时准确传递、处置流程标准规范。

3) 修订完善网络和数据安全应急预案，按事件类别等级细化基础设施、通用技术组件、业务应用系统等应急预案。

4) 制定网络和数据安全风险评估工作指南，定期识别、分析和评估网络和数据资产潜在安全风险，提出应对措施，配合修订完善我厅网络和数据安全工作考核办法。

（3）漏洞扫描：建立常态化漏洞全生命周期闭环管控机制，每季度开展 1 次全覆盖漏洞扫描，严格执行初测排查、整改指导、复测验证全流程管理。采用搭载国家级权威安全漏洞知识库的专业工具，对全厅管理终端、服务器、网络设备、网站及业务系统等全资产开展扫描，出具规范漏洞扫描报告。对自主发现的漏洞分级登记，推送责任处室（单位）整改并提供技术指导；对各级主管部门通报的漏洞完成验证、督办，按要求反馈处置结果。同步开展同源漏洞排查，防范同类风险重复出现，对整改结果全面复测，确保漏洞管控闭环、风险有效消除。

（4）应急演练：制定贴合业务实际的实战化应急演练方案，选取 1-2 个核心重要信息系统开展 1 次全流程应急演练，覆盖勒索病毒攻击、数据泄露、网络入侵、拒绝服务攻击等典型高风险场景，规范检测、抑制、根除、恢复、复盘全闭环应急处置环节。演练完成后全面复盘总结，锤炼应急保障队伍实战协同能力，优化应急预案与处置机制，严格落实网络安全责任制要求，出具完整规范的应急演练总结报告。

（5）安全加固和策略分析：制定分级分类安全加固实施方案，全程跟进各

系统加固进度，加固后开展完整性、可用性专项测试，确保不影响业务系统安全稳定运行，为每台加固对象编制专属操作指引与加固报告。全面梳理安全设备访问控制规则，制定标准化访问控制表，打通态势感知与防火墙、入侵防御等设备的数据联动通道。常态化开展访问控制策略合规性检查与管理员操作全流程审计，出具专项检查报告。

（6）重要时期安全值守：组织制定全周期重保专项工作方案，严格执行“零报告”制度，针对护网行动、重大会议活动、法定节假日、国家公祭日等关键时段，组建专项保障团队，派驻资深安全工程师开展7×24小时现场值守。事前完成风险前置排查与专项加固，事中开展全天候安全监测、实时预警与应急处置，事后复盘优化防护策略，全程做好值班值守、事件闭环处置与台账归档，出具重保专项总结报告，确保重保期间网络与业务系统安全稳定运行。

（7）供应链安全性检测：配置专业技术工具和专业安全检测技术人员，通过构建“技术工具扫描+人工专业复核”的双重保障机制，从配置合规性、漏洞风险、应用安全性等多维度进行严格把关，提前发现并消除系统平台存在的安全隐患。主要工作内容包括：

1) 安全基线检查：提取各项配置参数，与预设的安全基线进行自动化比对。重点核查权限设置中是否存在越权配置、账户管理里是否有冗余或弱密码账户、服务与协议配置是否启用了不必要的高危服务或协议。结合工具扫描结果进行人工复核，判断配置是否符合实际业务需求，避免机械套用安全基线导致业务中断。

2) 漏洞检查与修复：运用专业漏洞检查工具，依据最新漏洞库，对系统平台全方位检查，精准定位操作系统、数据库、中间件、应用程序等层面漏洞，提供修复建议并协助完成修复。

3) 应用技术检测：对上线业务应用深度检测，包括渗透测试，挖掘 SQ

L 注入、跨站脚本攻击、敏感信息泄露、身份认证绕过等常见安全漏洞，确保应用安全运行。根据业务流程设计针对性的测试用例，手动验证工具检测出的漏洞，特别是逻辑漏洞和业务相关漏洞。与开发人员紧密协作，共同分析漏洞产生原因，指导开发人员进行代码修复。修复完成后，由开发人员进行单元测试，安全测试人员进行回归测试，确保漏洞修复有效且未引入新的安全问题。

（8）攻防演练：组织开展 1 次实战化红蓝对抗攻防演练，组建不少于 3 家具有网络安全检测能力的单位作为攻击队伍，攻击队伍的检测费用由中标方支付。以不影响业务系统正常运行为前提，采用不限攻击路径与手段的黑盒实战模式，对参演目标系统开展全维度模拟攻击。精准挖掘系统、应用及网络设备等层面潜在安全漏洞，深度还原真实攻击手法与路径，形成攻防演练专项报告与整改方案。通过演练复盘总结，针对性推进安全整改，强化跨部门协同联动，全面提升全厅网络安全防护与应急响应实战能力。通过攻防演练，可以深入了解网络攻击方式和相应的网络安全漏洞，进而有针对性地进行安全整改，提升自身的安全防御能力，促进处室（单位）之间的协作。

（9）入侵痕迹检查：每季度开展一次全量入侵痕迹专项检查，覆盖厅机房及政务云所有在用物理服务器与虚拟机。采用多引擎恶意代码检测 + 人工深度溯源模式，精准识别木马、后门等恶意程序，排查异常登录、权限篡改等入侵行为，同步开展主机基础环境安全评估与失陷检测，出具专项检测报告。经运维及开发单位确认后，完成恶意程序清理与风险闭环处置。

（10）“两高一弱”安全检查：利用专业工具检测甲方系统平台存在的高危漏洞、高危端口、弱口令，开展弱口令专项检查，及时清理问题隐患，协助完成整改加固。每次检查后形成检查报告，梳理隐患并提供整改建议，协助完成整改后，通过二次扫描和人工复核验证效果，形成管理闭环。

（11）日常监测预警：根据全厅网络情况，构建威胁感知、响应、处置全链条纵深防御体系，全面夯实精准化威胁监测、全方位态势感知、体系化联动处置的核心能力。以网络和数据安全态势月报为常态化管控核心抓手，加大重要信息系统安全检查力度，按月度完成全厅安全态势汇总分析、风险隐患研判预警、问题整改跟踪督办，并出具监测报告和威胁分析报告，实现安全风险全周期闭环管理。对全厅互联网、政务外网、政务云全场景业务开展统一监测、统一预警，针对网页篡改、安全漏洞等常规安全事件，执行实时响应与闭环处置。

对相关网络安全主管部门和技术平台发现及通报的各层面的系统漏洞、国内外最新网络安全漏洞进行跟踪，持续开展重要漏洞披露平台的跟踪与分析，在发现高危风险后实时向系统责任处室（单位）发送安全预警通告，并由其运维团队通过每月或实时通过书面报告的形式将监测与处理结果进行报告。

监测预警及响应标准：

(一)整体监测要求：对我厅的互联网业务及政务外网业务，提供 7*24 小时不间断监测服务；

(二)针对服务范围内资产扫描到的高危可利用漏洞，提供漏洞修复方案和安全设备防护策略。

(三)对我厅所有互联网资产开展 24 小时的日常监测服务，跟踪和匹配主流漏洞平台发布的漏洞信息，及时进行预警通报。并对突发的安全事件进行响应，开展定位、分析、协调、处理，提交事件调查和处理报告。

(四)对政务云上系统

1)通过采集安全设备和监测工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，提供 7*24 小时持续不间断的安全威

胁分析鉴定。

2)及时发现重大安全漏洞，制定解决方案，通过应急检测服务迅速、精准地梳理出受影响的资产与设备，从而快速进行漏洞修复，缩短漏洞的影响范围。

3)针对我厅突发安全事件，按事件级别及事件影响范围，在规定时间内对突发的重要安全事件进行响应，立即开展定位、分析、协调、处理，提交事件调查和处理报告。

4)可视化展示服务成果，能通过可视化的数据，清晰地了解系统安全状况。

(五)在宁办公区流量监测

1) 为在宁办公区提供专属的网络流量监测服务，提供 7*24 小时全时段流量监测，实现对厅在宁办公区互联网、政务外网出口及内部各网段流量的全量采集、解析与分析。

2) 提供终端安全自动化编排处置，发现告警后能对终端恶意进程进行查杀、对攻击 IP/受害 IP/恶意请求流量进行阻断，实现威胁发现到解决的闭环处置。

3) 监测范围覆盖各办公区互联网、政务外网联网终端、办公设备、内部服务器及网络设备，可识别 HTTP/HTTPS、FTP、SMTP、SSH 等各类网络协议流量。

4) 具备异常流量识别能力，可及时发现大流量下载、恶意外联、网络拥塞、端口扫描、DDoS 攻击前兆等异常流量行为，触发实时告警并推送至安全运维团队。

（12）渗透测试：通过扫描已经发现的安全漏洞，模拟入侵者的攻击方法对互联网系统进行非破坏性质攻击性测试，保证整个渗透测试过程都在可以控

制和调整的范围之内。每季度开展一次渗透测试，通过渗透测试发现系统是否存在被恶意攻击者真实利用的安全漏洞情况、防护情况和数据安全情况，以及可能发生的安全风险事件，并且检测已有安全产品及安全策略是否能够实时防御安全攻击。评估目标系统当前的风险等级和安全防护能力的高低，针对发现的安全风险，提出安全解决方案，完善现有防御体系，优化安全策略。

对渗透测试范围中发现的信息系统资产漏洞、木马、后门等恶意程序，出具渗透测试报告。有新设备或新业务上线时，对业务及设备进行安全扫描检查，并提供结果报告。对于报告中发现的风险，提供切实可行的解决方案。

（13）网络安全运维支撑：针对信息系统在等级保护测评及密码测评过程中发现的不足（中高危漏洞）提供整改咨询与指导，提出整改优化建议，并对整改后的问题进行复测与确认，增强信息系统运维支撑人员的网络安全技能。

（14）数据安全：针对指定的系统开展数据分类分级，并开展数据安全风险评估和数据安全检查。对重要数据平台全链条业务环节进行全面梳理，深入分析数据全生命周期各环节在制度、管理、技术等层面存在的安全风险，从合规和风险管理角度出发，结合重要数据原则、业务结合原则、综合分析原则进行评估，并出具数据安全风险评估报告。在服务过程中协助我厅发现自身数据安全问题和短板，明确数据安全保护需求。数据安全风险评估包括数据资产、数据应用场景、数据威胁、脆弱性、安全措施等要素，需设计相应可实施的评估服务内容。基于评估结果，针对性提出数据安全解决方案和分阶段风险控制安全规划方案。

（15）宣传培训：面向厅机关及直属单位全体人员开展网络和数据安全宣传培训工作，全面提升全员安全意识与防护技能。重点做好国家网络和数据安全宣传周活动支撑，定制制作网络安全宣传视频（中标方应保证提供的全部视频素材及内容拥有合法、完整的知识产权，不存在任何版权侵权或权属纠纷。

如因视频内容引发版权争议、法律诉讼及相关损失，均由中标方自行妥善处理，并承担由此产生的一切法律责任与经济损失）。

2、工具要求

提供以下安全技术工具，满足日常政务云和在宁办公区安全检测防护服务需求。

➢ 政务云流量传感器

| 指标项 | | 指标要求 |
|---|---|---|
| 流量采集 | 网络协议 | 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：tcp、udp、icmp、http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、sctp、sybase、smb、sip、ftp、snmp、telnet、nfs、ssl、ssh、ldap、radius、kerberos、netbios、ntp、vnc、ipv6、gtp、tidb、kingbase、mqtt 等。 |
| | 文件协议 | 支持对流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk 等）、压缩格式文件（RAR、ZIP、GZ、7Z 等）、文档类型文件（word、excel、pdf、rtf、ppt 等）。 |
| | 告警过滤 | ▲系统本地需具备攻击告警的过滤能力，能够针对 IP 地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析。（提供产品界面截图，并加盖投标方公章） |
| | 隧道封装 | 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。 |
| 威胁检测 | 威胁情报 | 支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 100+万条。 |
| | 更新规则 | ▲新增加及更新规则，使用标签进行醒目标记展示，新增规则产生的告警在告警详情进行标签标记展示。（提供产品界面截图，并加投标方公章） |
| | 远程工具检测 | 支持包括：向日葵、ToDesk、Sorillus、Stowaway、CcRemote、DWservice 等在内的不低于 6 种远控/远程工具检测 |
| | 检测能力扩展 | ▲系统需具备攻击检测能力的扩展功能，支持自定义漏洞、自定义威胁情报。（提供产品界面截图，并加盖投标方公章） |
| | 暴力破解检测 | 支持 rdp/ftp/telnet/smtp/redis/rlogin/ssh/mysql/mssql/imap/POP3 等在内的网络协议的账号暴力猜解检测；支持撞库、登录页 |

| | | |
|---|---|---|
| | | 面爆破行为检测；支持手动配置暴力猜解告警阈值，减少业务行为误报。 |
| 配套服务 | | 合同有效期内厂家技术支撑及产品升级服务 |

➢ 政务云安全分析平台

| 指标项 | | 指标要求 |
|---|---|---|
| 资产管理 | 资产分组管理 | 支持对资产进行标签化、权重管理，资产分组，地理信息配置功能。 |
| | 资产分析专项 | ▲支持针对资产及资产分组之间互访场景进行专项统计分析，分析信息包括：访问时间、源 IP、源资产组、目的 IP、目的资产组、互访协议、目的端口、互访次数，访问拓扑，访问次数排名。（提供产品界面截图，并加盖厂家公章） |
| 告警分析 | 应用安全分析 | 支持基于 web 应用威胁专项分析，发现攻击应用的攻击者以及使用的 ATT&CK 技术手段，并展示应用 TOP 排名，攻击结果数量，告警类型 TOP 排名的呈现。 |
| | 挖矿专项分析 | ▲支持基于挖矿行为的挖矿阶段分析挖矿告警，可识别 6 个挖矿阶段，包括恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额，支持根据检索结果实时统计，包括挖矿币种分布、挖矿告警趋势，同时支持挖矿态势大屏展示等。（提供产品界面截图，并加盖投标方公章） |
| | 攻击视角专项分析 | ▲支持基于 APT 组织情报及 IP 地理信息检测发现攻击者所属组织、归属国家及地域等信息，基于规则检测发现攻击者所用到的全部攻击手段，用于对攻击者进行画像分析。并展示：攻击 IP，攻击 IP 归属地，受害 IP，攻击类型，资产组，最近攻击时间，攻击次数。（提供产品界面截图，并加盖投标方公章） |
| | 告警研判 | 自动智能分析研判告警，并提供研判依据、研判结果、处置建议；支持配置自动研判开关、自动研判告警范围、自动研判优先级。 |
| 威胁溯源 | 异常登录行为溯源 | 支持检测 SMTP、POP3、SSH、RDP、FTP、MSSQL、MYSQL、REDIS、ES、ORACLE 等协议的异常登录行为；检测类型包括：非正常时间访问，特权帐号登录， 明文密码泄露 |
| | 异常数据库行为溯源 | 支持对 mysql、mssql、oracle、sybase 等常见数据库支持的 SQL 日志中的敏感语句进行检测，支持自定义数据库高危行为特征，可定义数据库类型、高危操作类型，展示源 IP，目的 IP，源地域，源 IP 资产组，目的 IP 地域，数据库类型，数据库用户，高危操作，SQL，发生时间等信息 |
| | 异常访问行为溯源 | 支持资产横向访问分析，能展示源资产 ip、目的资产 ip、端口、协议、banner、时间等详细信息，且能自定义源 ip 白名单。 |
| 配套服务 | | 合同有效期内厂家技术支撑及产品升级服务 |

➢ 政务云服务器防护

| 指标项 | | 指标要求 |
|---|---|---|
| 风险发现 | 风险总览 | 支持统计总风险及各类风险数量，展示影响服务器信息。通过各类图表展示安全评分趋势、风险项趋势、账户风险类型分布、口令风险应用排行 Top5/Top10、漏洞风险项数量 Top5/Top10、配置风险排行 Top5/Top10 等相关统计信息。 |
| | RCE 利用风险监测 | 支持监控和分析目标主机的网络流量和应用程序行为，以防范远程命令执行（RCE）攻击。通过深入分析对外服务进程的执行命令行参数、网络连接以及其他相关数据，能够发现并记录异常的远程命令执行活动，一旦发现潜在的 RCE 利用行为，将立即产生告警。同时支持追溯攻击路径，显示每个命令的执行调用链。 |
| | 无文件攻击检测 | 基于九种关键行为进行检测，包括命令执行、文件下载、脚本执行、文件创建、数据执行以及敏感调用等。通过实时监控和特征比对，能够发现服务器上的无文件攻击事件。 |
| | 恶意扫描风险检测 | 支持对攻击者发起的恶意扫描行为进行识别，可防护端口扫描和扫描器扫描行为，以攻击和受害两种视角展示扫描信息包括：发生时间、受害 IP、攻击 IP、攻击类型、扫描端口、扫描次数、在威胁情报中是否为黑 IP 等信息。 |
| 系统防护 | 注册表监控与防护 | 支持监控和保护指定的注册表项、键值。 设置可信进程和可信注册表项/值允许操作。 |
| | 虚拟补丁 | ▲支持主机虚拟补丁功能，灵活对服务器批量开启、关闭该功能。（提供产品界面截图，并加盖投标方公章） |
| 应用防护 | 口令复用防护 | ▲支持对不同账号使用同一密码的口令复用行为进行检测，支持统计相同密码的账户数量、账户所在服务器、账户名称、账户状态等信息，并支持导出。（提供产品界面截图，并加盖投标方公章） |
| | 主机微隔离 | ▲支持一键全部启用以及全部停用微隔离策略，灵活设置微隔离规则，支持直接引用对象、设置主机共享规则、同时支持对单台主机个性化的规则策略制定。（提供产品界面截图，并加盖投标方公章） |
| | 后门程序防护 | 支持展示后门文件的发现时间、后门名称、后门类型、风险等级、来源、命中规则、文件类型、文件路径、文件大小、文件访问权限、文件所属用户、文件所属用户组、文件 MD5、文件创建时间、文件修改时间、文件最近访问时间等信息。 |
| 配套服务 | | 合同有效期内厂家技术支撑及产品升级服务 |

➢ 在宁办公区政务外网流量监测

| 指标项 | 指标要求 |
|---|---|

| | |
|---|---|
| 终端威胁 | 支持以受害资产维度进行告警分析，包括资产安全状态分布、风险资产 TOP10、资产告警详情，详情包括：资产名称、风险值、登录资产 IP、资产组、漏洞数、告警事件数、失陷状态。 |
| | 支持以主机资产维度进行告警分析，包括资产威胁级别统计、攻击维度统计、重点资产统计、失陷资产分布、告警资产趋势图。 |
| 邮件行为分析 | 支持邮件行为分析，包括邮件异常类型分布、邮件异常类型统计、邮件日志详情。 |
| 访问行为分析 | 支持外部访问分析，包括访问地域分布、被访问 IP 资产 TOP10、外部访问日志详情。 |
| 响应处置 | 可与用户已部署网络安全产品进行适配，形成安全联动机制，包括防火墙处置工作流，上网行为管理处置工作流，终端杀毒处置工作流。 |
| 资产感知 | 支持自动从流量中识别资产信息包含：IP、端口、服务、操作系统、MAC，支持对资产进行分组管理及对应内网网段的录入。 |
| | 支持展示资产漏洞信息，信息包括：资产 IP、资产名称、资产组、漏洞名称、最近发现时间、威胁级别、漏洞来源、漏洞披露时间、CVE 编号、CNNVD 编号。 |
| | ▲支持通过主机资产详情查看全部关联告警，同时针对单个资产也支持检索场景配置，关联告警支持按照 IP 归并，支持多维统计，包括但不限于：告警资产数量，不同攻击结果/攻击维度的资产数量，失陷资产组分布，未处置告警/全部告警、不同攻击结果/攻击维度告警数量、告警类型分布情况、攻击阶段分布情况、告警趋势图。（提供产品界面截图，并加盖投标方公章） |
| 配套服务 | 合同有效期内厂家技术支撑及产品升级服务 |

➢ 在宁办公区互联网流量监测

| 指标项 | 指标要求 |
|---|---|
| 工作台 | 支持自定义个性化配置，支持以拖拽组件的方式进行画布页面设置 |
| 态势可视 | 支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测等多个维度进行可视化展示，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序 |
| 监测中心 | 告警监控支持查看告警的基本信息、受害者、攻击者、处置响应、举证全文信息，其中受害者和攻击者支持查看响应 ATT&CK 矩阵视图 |
| 分析中心 | ▲可对所有安全模型进行管理，具体可进行新增、删除、启用、告警等具体操作，创建定义模型，包含规则模型、统计模型、情报模型、AI 模型、关联模型。（提供第三方权威机 |

| | |
|---|---|
| | 构检测报告并加盖厂家公章） |
| | 支持输入 IP、域名、文件 HASH、URL、邮箱信息进行本地情报碰撞查询，可展示情报标签、情报类型、危险等级、运营商、家族信息等内容 |
| | ▲满足用户对告警级别的调整，通过自定义配置过滤条件对告警级别进行调整，并支持选择适用不同的组织架构；告警级别支持相对级别的升降和绝对级别的高、中、低，规则可选择长期生效或定期生效（提供产品界面截图并加盖厂家公章） |
| | 支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；支持将检索语句一键翻译为中文，提高可读性；保留搜索语句历史记录 |
| | 实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过一键溯源进行威胁关系的自动拓展 |
| 响应中心 | 支持前端拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于数据源、分析组件、处置响应等，可自动判断策略编排是否合理并弹窗提示 |
| | ▲支持将联动设备能力封装，实现和不同产品的联动，支持设置 3 层递进阻断策略（如第一次阻断 10 分钟，第二次阻断 30 分钟，第三次永久阻断）；支持查看封禁设备数、封禁 IP 数、自动封禁 IP 数、本日解禁 IP 数、封禁订阅规则数、封禁 SOAR 剧本数，支持查看最近 7 天封禁 IP 趋势及防护设备封禁 IP 分布；支持封禁策略批量删除、解禁、导出（提供产品界面截图并加盖厂家公章） |
| 运营中心 | 情报源管理支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等 |
| | 内置运营简报、安全分析运营、风险资产等多种报告模板，支持手动生成报告或以订阅方式自动生成报告，报告订阅可设定报告发送周期和报告生成时间，并可支持选择相应组织架构，通过邮件方式发送一位或多位收件人 |
| | 支持预警、通报、工单功能，工单详情与备注支持多种内容格式，包括但不限于文字、图片、超链接、表格、代码片段、附件等类型；支持将预警信息直接转为内部通报，通报可直接派发工单 |
| | ▲通过工单处理情况、总资产数、风险资产数、风险概率等信息，对总部及分部的工作行为及取得的工作业绩进行评估，并运用评估结果对总部及分部的工作行为和业绩产生正面的引导（提供第三方权威机构检测报告并加盖厂家公章） |
| 资产中心 | 支持任意两天的历史风险资产对比，对比风险资产评级变 |

| | |
|---|---|
| | 化、资产评分变化，历史风险资产对比数据，包括：新增、变动、修复、不变、风险上升、风险下降，以及维持不变 |
| | ▲对资产的概况信息进行展示,具有资产概况、访问关系、行为画像、服务端口、访问端口、脆弱性等功能（提供第三方权威机构检测报告并加盖厂家公章） |
| 运维管理 | 支持一键巡检功能，检查项包含但不限于数据健康、探针健康检查、大数据集群健康、实时流计算引擎健康、管理服务健康、服务器节点健康等多种维度检查，提供巡检处置建议，并能将巡检结果导出 PDF 格式分析 |
| 配套服务 | 合同有效期内厂家技术支撑及产品升级服务 |

➢ 数据分类分级

| 指标项 | 指标要求 |
|---|---|
| 数据源资产管理 | 支持数据库类型包括但不限于 MySQL、Oracle、PostgreSQL、UXDB、MSSQL、MariaDB、Informix、Sysbase、DM、DB2、GBase、CacheDB、KingBase、Oscar、Oceanbase、GoldenDB、TiDB、MyCat、DBLE、DRDS、Hive、Inceptor、Impala、MongoDB 等 |
| | 支持通过 FTP/SFTP/LOCAL 文件协议对 csv、txt 等文件进行分类分级 |
| | ▲支持对于数据源中所包含的数据质量进行评估，评估指标包含：字段总数、字段注释存在数、有含义的字段注释数、有含义的字段注释去重数、表总数、表注释存在数、有含义的表注释数、有含义的表注释去重数（提供产品界面截图并加盖厂家公章） |
| | 支持以库、表、列方式对于数据资产目录进行可视化展示，数据表资产信息包含：数据源、主机、库名、Schema、行业模版、分类、分级、是否梳理、业务系统、部门、责任人、最后梳理时间、字段数、敏感字段数、已梳理占比，数据字段资产信息包含：字段名、字段注释、类型、规则名称、分类、分级、是否敏感、是否梳理、最后梳理时间、查看样本数据 |
| 分类分级管理 | 支持对于结构化分类分级任务进行管理，包含任务创建、编辑、开始执行、批量执行、批量调度等功能 |
| | 可对于结构化分类分级任务进行相关配置，包括：抽样策略、执行逻辑、分类预选、字段含义识别、数据表筛选，其中执行逻辑中包含分类分级规则匹配规则、小模型分析、大模型分析 |
| | 支持对于非结构化文件进行分类分级，可支持的文件类型包括：doxc/doc/txt/pdf/dcm，且支持非结构化分类分级模版的维护 |
| | 支持数据分类分级的标准化项目管理流程，涵盖任务分配、数据打标、结果审核、结果验收、结果发布等环节 |
| | 支持数据分类分级模版管理，且内置金融、政府、运营商、 |

| | |
|---|---|
| | 医疗、教育等行业通用模版及个人信息安全规范模版，其中个人信息相关识别规则不少于200条 |
| | ▲支持对于分类分级框架进行自动化校验，校验错误包含：精炼性检测失败、业务含义明确性检测失败、分类间唯一性检测失败，且支持人工根据检测结果进行调整（提供产品界面截图并加盖厂家公章） |
| | 支持用户自定义分类分级规则，规则判断主体包含字段内容、字段名、字段注释、表名、表注释等，匹配方式包括正则匹配、字典匹配，且支持通过AND和OR进行多个规则的组合 |
| | ▲支持有监督学习模型的训练，模型算法包括传统集成学习、快速神经网络、深度神经网络等至少3种类型，传统集成学习支持分类器数量配置，快速神经网络支持训练轮数、学习率、最小词频、n-gram配置，深度神经网络支持训练轮数、学习率、批处理大小、滤波器数量配置，以便满足不同场景的学习训练要求（提供产品界面截图并加盖原厂公章） |
| | 系统具备多租户管理能力，系统管理员可对于租户进行新建、编辑、删除、启用、停用等操作。租户之间数据相互隔离不可见、不可管理，并具备独立且完整的分类分级相关功能及配置 |
| | 支持对于结构化分类分级任务进行管理，包含任务创建、编辑、开始执行、批量执行、批量调度等功能 |
| 系统安全管理 | 系统本身安全至少包括但不限于：强密码校验、密码尝试次数、密码锁定时长、密码有效期、页面超时时长等 |
| | 系统本身需支持“三权分立”功能，至少包含系统管理员、安全管理员、审计管理员、权限管理员 |
| 配套服务 | 合同有效期内厂家技术支撑及产品升级服务 |

3、人员要求

本服务拟投入项目组成员不得少于4名，设置项目经理1名、技术负责人1名、网络安全负责人1名、保障安全运维工程师2名，所有人员资质证书复印件须加盖供应商公章，未按要求提供的不予认可。各岗位具体要求如下：

（1）项目经理1名，总体负责本次安全运维项目全流程统筹管理工作。要求项目经理具有本科及以上学历，五年以上同类型政务网络与数据安全运维项目管理工作经验，熟悉国家网络安全等级保护、商用密码应用安全性评估、数据安全管理等法律法规及技术标准，具备扎实的网络安全技术能力与全流程项

目管控能力。须具备与信息化相关专业的高级工程师证书，同时具备计算机技术与软件专业技术资格高级（系统规划与管理师）证书、信息安全保障人员认证证书（CISAW）、ITSS IT 服务项目经理证书 。

（2）技术负责人 1 名，全面负责项目技术方案落地、技术攻坚、安全技术验证与全流程技术质量管理工作。要求具备三年以上政务网络安全项目技术管理经验，精通网络安全攻防、漏洞挖掘与修复、数据安全防护、渗透测试等核心技术，具备丰富的政务信息系统安全防护项目实操经验。须具备高级网络信息安全工程师证书、注册信息安全专业人员证书（CISP）、网络安全能力认证证书（CCSC）。

（3）网络安全负责人 1 名，专项负责项目安全运营体系建设、风险管控、应急处置、安全制度规范落地与重保工作统筹。要求具备三年以上政务行业网络与数据安全运营相关工作经验，熟悉政务信息系统安全防护要求、应急处置流程与网络安全责任制相关规定。须具备注册信息安全工程师证书（CISP）、信息安全保障人员认证证书（CISAW）、计算机技术与软件专业技术资格高级（信息系统项目管理师）证书。

（4）安全运维工程师 2 名，负责日常安全运维、7×24 小时监测预警、现场值守、漏洞整改指导、安全事件应急处置等一线执行工作。要求具有两年及以上同类型项目安全运维工作经验，具备扎实的安全运维实操能力，熟悉政务网络环境与常见安全设备、系统的运维操作。每名工程师须至少具备信息安全保障人员认证证书（CISAW）或信息安全工程师证书。

4、运维计划要求

本次安全保障运维服务期为 1 年，本次服务开展分为四个阶段，分别为准备阶段、实施方案阶段、现场实施阶段，总结验收阶段。需提供服务实施方案，明确各阶段工作内容与交付。

5、项目保密要求

必须严格规范项目组成员的行为，执行各项保密制度，合同签订完成后签订保密协议，对在项目实施过程中接触的各类信息进行保密管理，杜绝敏感信息泄露事件的发生。

6、项目验收要求

必须严格规范项目组成员的行为，执行各项保密制度，合同签订完成后签订保密协议，对在项目实施过程中接触的各类信息进行保密管理，杜绝敏感信息泄露事件的发生。

7、供应商要求

至少具备 1 种资质证书，证书类别包含 ISO27001《信息安全管理体系认证证书》、国家信息安全测评信息安全服务资质证书（安全运营类一级及以上）、国家信息安全测评信息安全服务资质证书（风险评估或安全运维一级及以上）、中国网络安全审查技术与认证中心信息安全服务资质证书（信息系统网络安全审计）、中国国家信息安全漏洞库（CNNVD）技术支撑单位、检验检测机构资质认定证书（CMA）。