江苏大学附属医院

服务采购合同

合同编号：JDFY02XX2025000210

招标编号：JSZC-320000-SCZX-G2024-0731

甲　　方：江苏大学附属医院

乙　　方：联通（江苏）产业互联网有限公司

住　所　地：南京市鼓楼区古平岗 4 号 C 座二层

联 系 电 话：15651281395

法定代表人：　曲扬　　职务：　总经理

项目名称：网络安全服务

甲乙双方本着真诚、互惠互利的原则，在平等自愿的基础上，经充分认真协商，根据《中华人民共和国民法典》及相关法律规定，达成如下条款：

一、 工作范围

乙方根据本合同及附件的规定为甲方提供网络安全服务相关服务。根据甲方招标要求及乙方中标承诺，服务范围、服务内容、服务项目见合同附件一。

二、 标准

服务项目需要遵循 HL7 标准，电子病历评审规范，互联互通评审规范，三甲医院评审规范以及满足安全等级保护三级以上标准。

三、 服务方式

1、电话方式：乙方接到甲方技术支持请求或故障报告后，立即以电话方式帮助甲方，指导甲方解决问题，电话支持 7*24 小时服务。需提供乙方具体负责人的联系方式。

2、远程连接服务：乙方技术人员在甲方授权后，可通过远程连接进入甲方系统帮助甲方解决问题。

3、现场服务：乙方通过电话或者远程连接服务无法快速解决问题的情况下，需要对问题作初

夸克扫描王
极速扫描，就是高效

步了解和分析后，派出专业工程师在 2 个工作日内排除故障。如乙方在两个工作日内无法解决，需在两日内向甲方提出详细解决方案及日程安排，交给甲方确认。

4、预防性维护服务：包括现场巡检、调整优化。预防性维护及检测的事件应在不影响甲方软件系统使用的情况下与甲方协商，巡检次数按照每年不少于两次。

5、其他服务方式的具体要求详见附件。

四、 合同价款及支付期限和方式

1、本合同总价款为(大写)：人民币壹佰叁拾壹万捌仟捌佰元圆整(小写)￥1318800.00。每年的服务费是 439600.00 元，前述总价款对应的本服务项目期限为 叁 年。

2、自合同签订之日起，甲方对乙方的服务进行考核(相关内容以及标准等，均由甲方根据实际需要制订和执行)。

3、本合同结算方式：在本合同签署后，甲方按每半年（六个月）对乙方服务行为进行考核，考核合格的，则在此后 3 个月内，向乙方支付当年度总金额 50%，共计（大写）：人民币（小写）￥219800.00；如考核不合格，甲方有权扣除当前半年的服务费用，并有权立即解除本合同。

4、本合同总价款已包含乙方履行本合同全部义务所应获得的价格，乙方在合同规定的服务范围内不得以任何理由要求增加费用，甲方书面同意的除外。

5、除非双方另行约定，本合同总价款已经包含所有完成项目所需要的材料、人工费及销售、使用、服务、增值或类似的税项。

6、甲方支付前述款项的前提至少还包括乙方无任何存量的违约行为。

五、 服务期限

1、乙方提供为期 叁 年的 网络安全 服务和服务质量保证。

2、每天 8 小时（8:00-12:00，13:00-17:00），每周 5 天提供解决一般问题的技术支持，以驻场、电话、电子邮件、传真、远程登录等方式及时做出解答；

3、每天 24 小时，每周 7 天提供业务严重影响的紧急问题的技术支持，以电话、电子邮件、传真、远程登录等方式及时做出解答，在上述方式无法解决问题时，将提供现场支持，协助甲方及时排除故障。

六、 开票约定

1、甲方每次付款前乙方须向甲方出具等额的中华人民共和国法定发票，甲方根据乙方提供的合格发票支付相应款项，如乙方提交的发票不正确，甲方可延迟付款，（但不承担违约责任）。

夸克扫描王
极速扫描，就是高效

2、根据税法规定，发票必须在真实的业务交易下方能开具，故发票名称必须与合同签订单位一致。

3、发票种类：增值税普通发票。

七、 甲方义务

1、甲方应有专人负责与乙方进行及时的联络并监督、协调软件维护及服务情况。

2、甲方负责人应拥有必要的专业技术知识，定期与乙方代表洽谈、联络、沟通。

3、甲方按时提供有效准确的必要资料，在规定时间内组织各阶段验收，协调甲方内部关系。

4、当系统发生故障时，甲方应及时通知乙方，同时简要说明故障情况。当乙方来人时，甲方给予相关协助，为乙方提供进入现场的便利。

八、 乙方义务

1、乙方在本合同生效之日起，针对本合同产品系统功能范围内的软件程序，提供技术支持服务。

2、乙方工程师或有关人员有义务对甲方工程师和操作人员进行现场操作培训，解答甲方人员提出的问题； 院外培训：双方另行商议。

3、乙方应向甲方提供产品说明书，数据字典，系统修改等说明文档。

4、乙方服务工作需要遵循信息安全原则，规范操作，严格控制对数据库的失误操作，严禁软件留后门，带入病毒等危险行为。严格遵循《中华人民共和国个人信息保护法》的法律法规，如果由于乙方不规范操作导致任何网络信息安全问题和数据泄密事件，乙方应承担相应的责任和处罚。

5、如发生知识产权纠纷，由乙方负责处理并承担相应责任。

6、乙方需在不迟于本合同到期日之前 90 日，正式通知甲方合同到期问题，如因乙方未及时通知而导致甲方未能及时采购相关服务的，由此产生的所有损失及责任由乙方承担。

7、乙方应保证所提供的服务满足安全等级保护三级以上标准及甲方的相关信息安全要求。

九、 保密条款

1、双方应当对本合同的内容、因履行本合同或在本合同期间获得的或收到的对方的商务、财务、技术、产品的信息、用户资料或其他表明保密的文件或信息的内容(简称“保密资料”)保守秘密，除非得到另一方的书面许可，甲乙双方均不得将本合同中的内容及在本合同执行过程中获得的对方的信息向任何第三方泄露。

2、乙方从甲方获得所有保密信息，乙方仅对保密信息具有使用权，而没有所有权、知识产权

夸克扫描王
极速扫描，就是高效

及解释权。

3、甲方所披露的保密信息只能被乙方用于本项目的实施工作，不得将甲方所披露的保密信息用于其它任何目的。

4、乙方有义务妥善保管保密信息。乙方承诺采取合理的措施以保证保密信息不被泄露，此种措施应至少与甲方对自己的保密信息所采取的措施相当。

5、乙方仅能向有知悉必要的乙方人员（包括但不限于雇员或顾问）披露保密信息。一经发现对保密信息的任何未经授权的披露或乙方及其人员违反本协议时，乙方应立即通知甲方，并采取措施防止进一步未经授权而使用保密信息。

6、未经甲方的事先书面批准，乙方不得直接或间接以任何形式或任何方式把保密信息或其中的任何部分，披露、透露给任何第三方或者公开，乙方保证不向任何第三方披露本协议的存在或本协议的任何内容。

7、严禁乙方工作人员利用工作便利以任何途径和方式，为甲方统计医师个人及临床科室有关医药产品用量信息，或为第三方统计提供便利。若工作中发现其他人员有相关违法违纪或泄露相关信息的行为，应立即与甲方或乙方负责人反馈。

8、乙方应当告知并以适当方式要求其参与本项工作之雇员遵守本协议规定，乙方人员向第三方披露保密信息，或依据该等保密信息向第三方做出任何建议，都被视为乙方违反本协议。

9、乙方参加本项目的所有人员必须与乙方签有正式的保密协议，并且该人员在知晓保密信息前应已充分了解本协议的内容。

10、乙方不得全部或部分复制或仿造保密信息。

11、甲方人员不得要求乙方为其统计医师个人及临床科室有关医药产品用量信息，或要求其以任何方式向第三方透露保密信息或其中的任何部分。

12、乙方违反以上任何保密规定，均视为违约。违约方应当对其违约行为给甲方造成的损失承担赔偿责任，并向有关卫生计生行政部门报告。并严格按照相关规定处理。

13、因商业机密泄露造成的损失，由泄露方承担相应的责任。

14、本保密义务应在本协议期满、解除或终止后仍然有效。

十、 违约与赔偿责任

1、如乙方违约，须向甲方承担本合同总价款 10%的违约金。

2、乙方履行任何义务逾期达到 7 日，或存在明显违约且对甲方利益造成影响，或者存在其他违约行为且未能按照甲方要求全部整改完毕，甲方均有权解除本合同。

3、如甲方基于乙方违约而解除合同的，甲方除无需再向乙方支付任何款项之外，乙方还必须

夸克扫描王
极速扫描，就是高效

立即无条件退回从甲方处收到的全部所有款项，并向甲方承担违约金、赔偿损失。

4、如甲方逾期付款且经乙方催要后，仍违约逾期支付，则从收到乙方书面催要通知之次日起，按同期 LPR 的标准向对方承担对应的银行利息损失。

十一、解决合同纠纷的方式

1、就合同条款的解释和执行等发生纠纷，双方应及时协商解决，协商不成时，则由甲方所在地人民法院处理。

2、因一方违约致使对方采取诉讼方式实现债权的，违约方应当承担对方为此支付的诉讼费、律师费、差旅费等实现债权的费用。

十二、其他要求

1、本合同未尽事宜，双方协商并签订补充协议，补充协议与本合同具有同等法律效力。

2、乙方随合同应提供营业执照的复印件（复印件仅供与江苏大学附属医院签订和履行本合同使用，他用无效）并加盖公章。

3、投标文件、项目服务清单及承诺书可作为本合同的附件。附件为本合同的有效组成部分，具有与合同同等的法律效力。甲方的相关制度亦对乙方具备对应的约束力，构成乙方在本合同项下的义务来源并应得到乙方的全面遵守。

4.乙方因签订和履行本合同而涉及的所有安全义务以及对应的费用，均由乙方自行承担，由此产生的所有法律责任(包括民事\行政\甚至刑事)均由乙方承担。

5、本合同载明的乙方住所地以及联系方式，既可作为甲方向乙方送达使用，亦可作为法院向乙方送达使用，且据此所作的前述送达均为有效。

6、本合同所述的各项义务，乙方均应切实履行，即使双方存在付款、开票等争议，乙方亦无权以任何借口或理由拒绝履行。

7、本合同一式四份，甲方执三份，乙方执一份，自双方签章(包括在骑缝处)生效。

8、最终用户：江苏大学附属医院。

甲方：江苏大学附属医院　　**乙方：联通（江苏）产业互联网有限公司**

甲方代表：　　**乙方代表：**

日期： 2025.2.25　　**日期：** 2025.2.25

附件： 附本合同的具体实施条例及售后服务等内容。

夸克扫描王
极速扫描，就是高效

网络安全服务参数

斜体部分为本项目最低实施标准，必须全部满足，否则按无效投标处理。▲部分为需提供证明材料并加盖投标人公章。

一、安全托管服务

技术指标	指标要求
资产数量	*提供3年不少于40个资产IP的7*24小时安全托管服务，围绕着业务资产、漏洞、威胁及事件提供不间断的监测、分析、处置与溯源服务。同时为保障服务的处置效率和效果，并要求每年提供不少于12人天的上门处置服务。*
安全现状评估	应使用安全工具对招标方服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。
	针对服务范围内资产扫描到的高危可利用漏洞，应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失。
安全问题处置	*要求可以对服务范围内发现的每一个高危可利用漏洞提供防护规则，并且承诺防护率达到99%，提供承诺函并加盖服务投标人公章。*
	*具备云端检测和分析平台，通过采集安全设备和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，为招标方提供7*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示。*
服务内容	提供云端服务平台告警审核功能。

夸克扫描王
极速扫描，就是高效

	为了保障服务质量和加强服务方与招标方的沟通，服务方应当承诺为招标方配置一名经验丰富的安全专家作为专属服务经理，并且实时响应服务方咨询的网络安全相关问题；
	*服务方应当为招标方提供 7*24 小时的安全守护，不论是白天、黑夜、节假日服务方都应该能做到 7*24H 在线服务，并且在节假日期间应当每日为招标方提供《节假日值守总结》*
	▲为了降低我院因网络安全事件造成的损失和影响，投标方应当按照以下服务指标和要求为我院提供服务： 1、从安全日志上传分析研判到通告给招标方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于 15 分钟，一般事件的通告时间少于 30 分钟； 2、本次服务人员可通过使用我院现有的防火墙组件和端点防护组件，发生重大威胁与事件的遏制影响完成时间少于 15 分钟，一般威胁与事件的遏制影响完成时间少于 30 分钟； 3、安全事件经过投标方服务人员的确认后，通告给招标方的各类安全事件的准确率不低于 99%（即误报不能超过 1%）；
	▲本次投标方应当给我院承诺：本次服务过程中攻击成功事件 0 漏报，服务人员至少发现攻击链路上的一个攻击行为；我院本次服务范围内的资产安全事件的闭环处置比例达到 100%；投标时提供承诺书并加盖投标人公章。
	应当满足重大事故应启动应急响应机制，工作时间 15 分钟之内云端专家进行响应，非工作时间 30 分钟之内云端专家进行响应，8 小时上门处置。
	云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评。提供证明材料并盖章投标人公章。
	▲云端服务平台应通过国家互联网信息办公室、国家发展和

夸克扫描王
极速扫描，就是高效

	改革委员会、工业和信息化部、财政部四部委联合组织的云计算服务安全评估，入选“通过云计算服务安全评估的云平台”名单，以确保平台的安全性和可控水平。提供证明材料并盖章投标人公章。
	为了保障服务效率和质量，投标方的云端服务平台应当具备一套完善的流程编排引擎，能够为客户灵活编排、定义服务流程，并且定义服务的SLA，将服务过程中的各个关键环节按照一定的顺序和规则进行组织和安排，以达到高效、优质的服务目标；
	云端服务平台应具备智能AI大模型服务工具，支持集成在服务微信群、服务工作台，该工具能力项应支持告警数据包研判、情报查询分析、Payload解码、事件研判定性、自动调用安全设备遏制（IP、域名封堵）、事件调查溯源、运营数据统计（支持在线统计、分析并下载数据）等。提供证明材料。
	*云端服务平台支持与客户现有出口防火墙和服务器终端安全软件对接，实时接收安全设备检测到的安全事件信息、安全日志数据，发生安全事件时服务人员可利用现有安全设备及时处置，提供7*24小时的服务，提供证明材料并盖章投标人公章。*
服务成果可视化	投标方需为我院提供云端服务成果展示门户（或用户Portal），应具备服务质量可视化展示，使我院能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长，以验证投标方所承诺的服务指标。 需提供云端服务成果展示门户中服务质量监控相关的截图证明并加盖投标人公章；

夸克扫描王
极速扫描，就是高效

	投标方需为我院提供移动端服务过程展示门户（移动端Portal），通过清晰可视化的风险消减图和漏洞消减图，让我院清晰了解云端安全托管服务的风险消减机制，直观实时了解当前风险闭环情况，支持直观地查阅服务推送的各种安全事件/威胁的详细专家审核研判过程，需包含安全事件详细的【基本信息】【入侵路径】【影响主机】【主机调查】【数据包分析】等内容。 需提供移动端服务门户中相关的截图证明并加盖投标人公章
服务商资质	▲服务厂商应是国家互联网应急响应中心网络安全应急服务甲级支撑单位，提供证明材料并盖章投标人公章。
	服务厂商为国家信息安全漏洞共享平台(CNVD)技术组成员和用户组成员，提供证明材料并盖章投标人公章。

二、全流量威胁检测服务

技术指标	指标要求
服务设备要求	*吞吐量≥500Mbps，内存大小≥16G，硬盘容量≥128GB MSATA+4TB SATA，接口≥6千兆电口+2万兆光口SFP+，开通第三方应用联动响应软件模块，包含3年的软件升级和规则库升级服务*
服务功能	▲支持资产自动识别和资产扫描功能，支持自动入库、手动入库、设置扫描目标等功能，扫描类型可选择存活性（ARP/TCP/ICMP）、服务/端口（常用/全局）、操作系统、应用识别等。包括逻辑拓扑和物理拓扑识别及可视化展示。（需提供截图证明并加盖投标人公章）
	支持主机类资产识别，能够识别资产数据来源、IP地址、主机名、MAC地址、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组、资产名称、应用、IP类型、识别方式、首次发现时间等。

夸克扫描王
极速扫描，就是高效

	支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、数据更新、主机资产退库、自定义资产名称等。
	持整体展示服务器脆弱性风险、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web 明文传输、可用性风险）。
	▲支持弱密码主动扫描，支持 SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL 等扫描协议的主动扫描。（需提供第三方检测报告加盖投标人公章）。
	支持镜像流量检测 web 流量中是否存在可截获的口令信息，检测列表包含对应域名/URL、服务器 IP，所属分支和业务，数据包举证等信息，避免因明文传输导致信息泄露的风险。
	支持流量实时识别漏洞分析，支持资产类型和脆弱性等级筛选，支持展示漏洞严重等级分布、影响资产组织 TOP，支持显示漏洞详情，包括主机信息、漏洞信息、风险描述、数据包举证以及防护建议等，并支持导出脆弱性感知报告（所投产品须提供第三方机构关于“漏洞风险识别”功能项的产品检测报告并加盖投标人公章）。
	支持安全检测日志，日志类型包括脆弱性风险、访问风险、服务探测、主机探测、网站攻击、后门通信、暴力破解、攻击利用、邮件攻击、DOS 攻击、黑链、漏洞攻击、黑客工具、数据库攻击利用、访问恶意文件、感染病毒、主机异常、网络行为异常、流量异常、登录异常等。
	▲支持勒索专项检测页面，对勒索主题的安全告警进行展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP 爆破、感染勒索病毒、黑客勒索攻击、勒索 C&C 通信等维度，支持展示受害资产以及受害资产攻击数 Top5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、勒索风险、攻击阶段、威胁等级、受害

夸克扫描王
极速扫描，就是高效

	者 IP、受害者资产类型、攻击者 IP、攻击次数、处置状态等（需提供截图证明并加盖投标人公章）。
	▲支持挖矿专项检测页面，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、挖矿阶段、攻击阶段、威胁等级、受害者 IP、受害者资产类型、攻击者 IP、攻击次数、威胁情报、处置状态等（需提供截图证明并加盖投标人公章）。
	文件威胁分析支持平台内置的恶意脚本分析引擎、webshellkiller 智能引擎、save 智能分析引擎以及云端分析引擎组合进行综合研判，协议类型有 HTTP、FTP、SMB、SMTP、POP3、IMAP 多种类型，支持展示查杀数据统计、受害资产攻击数 TOP5，支持以列表的形式展示文件威胁信息，包括威胁情报、最近发生时间、威胁描述、威胁类型、攻击阶段、威胁等级、受害者 IP、受害者资产类型、攻击者 IP、攻击次数、处置状态等信息。
	支持整体展示服务器脆弱性风险、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web 明文传输、可用性风险）（需提供截图证明并加盖投标人公章）。
	支持综合安全风险报告、主机安全风险报告、处置报告多种方式呈现，可自定义时间范围、资产组、格式、报告名称等信息。
	支持管理员账号的新增、删除、启用、禁用等，支持可信 IP 设置。支持系统管理员、安全保密管理员和安全审计员三个管理员角色。
	支持配置审计白名单，可配置源 IP、源端口、目的 IP、目的端口、及所有审计类型（DNS、SMB、HTTP、邮件、AD 域、FTP、Telnet、数据库、ICMP、RDP），支持导入导出白名单等操作

夸克扫描王
极速扫描，就是高效

	具备安全检测特征识别库、安全知识库、IOC 威胁情报库、热点事件库、文件智能分析模型库检测能力。
	支持与客户现有出口防火墙、服务器终端安全软件进行联动，实现联动封锁、访问控制限制、主机隔离、隔离黑进程、DNS 拦截、下发病毒扫描、IOC 联动溯源五元组举证等（需提供截图证明并加盖投标人公章）
	▲要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务一级资质（一级＞二级＞三级），提供有效证书复印件并加盖投标人公章。
	要求所投产品的生产厂商同时为国家信息安全漏洞共享平台(CNVD)技术组成员和用户组成员，提供有效证书复印件并加盖投标人公章。

三、安全服务

技术指标	指标要求
资产梳理	*要求识别并列出客户单位的所有资产，包括但不限于硬件设备、软件应用、网络基础设施、数据和信息等，确保无遗漏。频率为不少于 4 次/年。*
基线检查	*要求应基于行业标准和最佳实践，基线检查内容包括但不限于账号与权限管理、密码策略、安全审计与日志记录、安全策略与补丁管理。频率不少于 4 次/年。*
漏洞扫描	*要求投标方能够对操作系统（如 Windows、Unix、Linux 等）、数据库（如 Oracle、MS-Sql、MySql 等）、网络设备（如路由器、交换机等）、安全设备（如防火墙、入侵检测系统等）以及特定应用程序等进行全面的漏洞扫描评估。频率为不少于 12 次/年。*
渗透测试	*要求投标方明确渗透测试的具体目标，测试目标应详细列出，包括但不限于 IP 地址、域名、系统类型、应用程序名称等。投标方在渗透测试前应进行充分的信息收集和情报搜集，了解*

夸克扫描王
极速扫描，就是高效

	目标系统的结构、配置和可能存在的漏洞。 要求投标方根据漏洞扫描的结果，尝试利用漏洞进行渗透攻击，验证漏洞的真实性和危害性。 渗透攻击应遵守法律法规和伦理规范，不得对目标系统造成不必要的损害。 渗透测试数量不少于20个系统/年。
应急响应	1）信息安全事件处置：各系统发生安全事件时，要求及时进行应急处置，对信息安全事件的发生、处理办法进行记录，处置完成后提交应急处置报告。 2）信息安全事件汇报：要求将对每次的安全应急情况进行分析，将信息安全事件处理结果和整改建议进行汇报，协助对安全问题进行处置。 服务完成后应提交《应急服务报告》。 应急响应不限次数。
重要时期网络安全加强保障	重大活动期间提供网络安全保障，应对重大活动期间可能发生的大规模网络攻击，确保重要信息系统的安全稳定运行。（例如：国庆、春节、重大发布活动）。重保时期由招标单位指定，次数不限。
安全事件通告预警	应建立明确的预警响应机制，包括预警接收、分析、决策、执行和反馈等环节，确保预警信息能够得到及时有效的处理。安全事件通告预警次数不限。
安全巡检	利用网络中部署的安全审计产品（如日志审计系统、态势感知、防火墙等）对网络、系统、应用的安全日志进行分析，通过收集安全日志，综合分析网络中发生过的事件，寻找事件的来源、发生事件的原因、事件发生可能带来的影响。 频率为不少于每月现场安全巡检1次。
威胁分析服务	要求服务提供商能够全面识别组织面临的各种安全威胁，包括但不限于网络攻击、恶意软件、数据泄露、内部威胁等。对识别的威胁进行深入分析，了解威胁的来源、动机、攻击手段和

夸克扫描王
极速扫描，就是高效

	影响范围。 对识别的威胁进行风险评估，确定威胁的严重程度和可能造成的损失。 威胁分析服务频率为不少于每日 1 次。
安全培训	安全培训内容应涵盖所有关键的安全领域，包括但不限于安全生产法律法规、操作规程、事故案例分析等。培训内容应及时更新，反映最新的安全标准和最佳实践，以确保用户能够了解并掌握最新的安全信息。安全培训不少于 8 学时 1 年。
安全设备巡检与策略调优	网络安全设备、服务器系统、虚拟化系统的安全运行状态进行巡检，查看设备的各项运行指标是否正，设备的软件版本（如操作系统补丁、防病毒系统病毒库等）是否升级。要求投标方对现有的安全策略进行分析，评估其有效性、合理性和安全性。 根据策略分析的结果，对现有的安全策略进行优化，包括调整规则、优化参数、增加新功能等。 频率为不少于 1 年 12 次。
安全咨询	投标方应根据招标方的具体需求，提供针对性的安全解决方案，包括技术解决方案、管理解决方案和流程优化方案等，以帮助招标方提升整体安全水平。安全咨询的次数不限。

四、其他服务要求

1、中标供应商提供 7*24 小时应急响应服务，须确定专人（技术负责人）接受采购人故障申告。接到申告，15 分钟内到达现场，并在到达现场后 2 小时内将故障修复。2 小时内不能修复的，启动备品备件的调用，设备修复后予以恢复。

2、要求中标供应商配合用户根据安全服务要求调整网络配置，并根据用户系统变化情况及时调整优化，对重大的技术问题，供应商应协调组织技术专家小组进行会诊，以确保系统的正常运行。

3、考虑到我院本次项目建设的重要性，要求在项目签订合同前对重要功能参数进行逐条响应并现场演示，如有不满足按照虚假应标处理并取消该代理商在

夸克扫描王
极速扫描，就是高效

本单位的投标资格。本次项目中的安全服务设施在供货时，必须提交生产厂商出具的证明材料，保证该安全系统设施为原厂全新产品且由原厂提供不低于三年的软硬件升级及维修服务。

4、中标供应商提供的服务设施必须为全新生产，系统设施到货后，用户方将与供应商及生产厂商代表三方共同对系统设施进行非破坏性拆解验收，如发现系统设施内部有长时间使用、维修痕迹以及主要零部件生产日期过久等异常现象而供应商对此不能做出合理解释的话，则用户方将终止合同、并报政府采购监督管理相关部门进行处理， 供应商应承担相应违约法律责任。

5、中标供应商应按要求提供完整的服务项目建设档案，包括施工方案、竣工和技术文档、使用说明等。

6、在法定节假日（元旦、春节、五一、十一等）期间、重大活动（由采购人指定并提前告知）前及其举行期间，根据采购人的具体要求对相关系统进行额外的安全巡检服务，确保设备及系统在此时期的正常工作，必要时派专业技术人员在现场保障服务根据采购人要求。

7. 中标供应商交付物要求：

交付物名称：《安全服务运营报告》，报告频率：每周一次

交付物名称：《首次威胁分析与处置报告》，报告频率：一次

交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数

交付物名称：《安全通告》，报告频率：按需触发，不限次数

交付物名称：《综合分析报告》，报告频率：每月一次

交付物名称：《季度汇报 PPT》，报告频率：每季度一次

交付物名称：《年度汇报 PPT》，报告频率：每年一次

8、中标供应商承诺在中标后签订合同前提供加盖所投服务厂商公章的针对技术参数的证明材料（提供承诺函并加盖投标人公章），若供应商与投标文件中提供的技术偏离表不一致，不予验收，用户方有权追究其责任。

9、保密要求

（1）安全服务人员在工作现场未经采购人工作人员允许，不得接触涉密信息和敏感信息；不得私自进入服务器等设施设备存放场所。在工作过程中因需要，确需接触涉密信息或敏感信息和进入上述场所的，应在取得采购人管理人员同意后进行操作。

夸克扫描王
极速扫描，就是高效

（2）安全服务人员在工作过程中，不得以任何形式私自外传、记录、下载和存储本系统中的任何信息和数据；不得使用未经采购人许可的计算机和存储设备对上述信息和数据进行运行和操作。

（3）安全服务人员未经采购人管理人员许可，不得将本系统中的任何信息和数据以任何形式在任何网络和媒体上发布和传播。

（4）安全服务工作人员因工作失当违反本要求的，未造成严重后果或用户方信息泄密的，经用户方批评教育后，按罚则条款相关规定进行处罚；安全服务工作人员三次及以上违反本要求或者造成用户信息系统破坏和数据泄密等严重后果的，采购人将即时终止合同更改维护单位，并依据《中华人民共和国网络安全法》及其实施办法严格追究相关责任人的法律责任。中标供应商须加强安全服务人员的保密培训，进场开展安全服务前须与采购人签署保密协议。

10、服务质量保证（含罚则条款）

（1）服务响应时间：未在规定时间内响应的或未在规定时间内修复故障按5000元/次扣除合同款。

（2）未按合同要求保质保量完成安全服务工作的，按2000元/次扣除合同款。

（3）未在规定时间内提交相关书面材料的，按2000元/次扣除合同款。巡检质量不符合要求，对于网络安全隐患应该发现，却未能发现的，造成网络安全事件，按5000元/次扣除合同款。网络安全事件包括，但不限于公安、网信系统的整改函、通报函、整改通知书等。

（4）服务质量严重不到位的，采购人将对中标供应商处以整改通知书，中标供应商收到整改通知书后应于一周内向采购人提交整改报告。若逾期不提交整改报告或一年之内被二次处以整改通知书的，采购人有权中止合同并采取相应措施保障设备正常运行，期间产生的费用由中标供应商承担。

11、验收标准和方法

（1）中标供应商提交验收汇报材料，主要包括工作量统计、服务响应情况、全年系统运行是否正常、维保服务方工程师服务质量是否符合采购人要求等。

（2）采购人组织专家验收，对服务质量和效果进行评审，形成专家验收意见并确认签字。

夸克扫描王
极速扫描，就是高效