2025年武汉市卫生健康信息中心机房网络安全服务项目采购需求文件

本项目采购预算：人民币117.92万元；最高限价：人民币117.92万元。

第一部分 供应商资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定，即：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

2、应未被列入失信被执行人、重大税收违法案件当事人名单，未被列入政府采购严重违法失信行为记录名单；

3、本项目不接受联合体。

第二部分 技术、服务及商务要求

一、 采购清单

序号	服务分类	服务名称	数量	单位
1	网络安全防护服务	边界安全防护服务	1	年
2		高级威胁防护服务	1	年
3		日志存储服务	1	年
4		VPN 接入服务	1	年
5		主机（服务器和终端）防护服务	1	年
6		漏洞发现服务	1	年
7		数据流转监测服务	1	年
8		网络安全威胁监测管理服务	1	年
9		利旧设备维保及备件服务	1	年
10	网络安全运维保障服务	本日常安全运维服务	1	年
11		重保值守服务	1	年
12		风险评估服务	1	年
13		应急响应与演练服务	1	年

二、 技术、服务要求

2.1、需求概况

武汉市卫生健康信息中心现有的安全保障体系已建设使用多年，大量设备老

旧质保期已过、应对新型攻击手段能力不足，且随着业务的发展和日益增长的安全要求，需持续完善并提升中心本地的网络安全防护能力和高效的安全运维工作。按照统筹规划、整合资源、重点保护、适度安全的原则，结合实际情况，以合适的网络安全防护工具和保障服务，确保相关信息系统免受网络安全威胁，满足网络安全基本属性要求，符合国家法律法规要求，支撑业务安全持续运行管理，数据安全得到有效保护，实现对各类安全告警和事件的快速处置，防范网络安全事件的发生。

1、网络安全防护服务：通过对中心机房现有安全防护设备能力清查评估，以购买服务工具的方式部署高级威胁防护、边界防火墙、安全威胁监测、安全威胁管理平台、日志审计、远程安全接入、主机（服务器和终端）防护、数据安全监测等安全防护设备，完善现有的安全防护体系，提升应对新型安全威胁的防护能力。

2、网络安全运维保障服务：以购买第三方专业安全服务，为中心机房提供网络安全运维保障服务，服务内容包括：本地日常安全运维服务、重保值守服务、风险评估服务、应急响应与演练服务等，确保中心机房的网络安全保障能力始终处于较高水平。

2.2、服务周期

自合同签订之日起，提供 1 年服务。

2.3、网络安全防护服务

2.3.1、边界安全防护服务

2.3.1.1、服务内容

在卫生专网边界处提供冗余的边界防护能力，并对现有安全设备的使用年限、设备性能、防护能力、维保支撑等综合因素，优化现有的安全设备。

2.3.1.2、服务工具

2 台下一代防火墙

序号	指标项	技术要求
1	性能要求	双电源；网络层吞吐率≥10Gbps；最大并发连接数≥350 万； 整机同时具备防火墙、入侵防御、防病毒、应用识别和 web 应用防护（WAF）等功能；
2	安全策略	支持基于域名的安全策略模糊匹配； 支持一体化安全策略，能够基于源/目的安全域、源 IP/MAC 地址、目的 IP 地址、地区、服务、时间、用户/用户组、应用层协议、五元组、内容安全（WAF、IPS、数据过滤、文件过滤、AV、URL 过滤和 APT 防御等）统一界面进行安全策略配置。
3	入侵防御	支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证。
4	入侵防御	支持超过 18000 条以上特征的攻击检测和防御
5	防病毒	可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；防病毒本地库数量 600 万+ 支持发现病毒发送的告警信息，支持用户编辑告警内容；
6	防病毒	支持云端防病毒，为保证检测时效性，特征缓存数至少保证 20 万条且缓存保留时间不应少于 700 分钟
7	WEB 应用防护	支持为 Web 应用提供基于 HTTP 和 HTTPS 的流量防护。对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。
8	WEB 应用防护	支持 SQL 注入、跨站脚本等攻击的防护，支持 CC 攻击防护，可基于检测请求报文头的 X-Forwarded-For 字段，以获取真正的源 IP 地址；

序号	指标项	技术要求
		WAF 规则支持用户自定义；
9	WEB 应用防护	支持至少 5000 种独立 Web 特征的攻击检测和防御特征库
10	负载均衡	支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。
11	威胁情报	支持 IP 信誉库、DNS 信誉库、URL 信誉库； 支持挖矿行为检测和勒索病毒检测
12	产品资质	产品必须具有软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；

2.3.2、高级威胁防护服务

2.3.2.1、服务内容

在卫生专网边界处提供冗余的高级威胁防护能力，用于检测并阻止恶意程序，如勒索软件、病毒、僵木蠕、间谍软件、网页木马。拦截间谍软件的回拨企图，阻止间谍软件下载，阻止恶意程序通过即时通信程序进行扩散提供网络威胁防护虚拟补丁能力，发现的主流安全漏洞提供网络层虚拟补丁安全防护，有效防护漏洞利用和 SQL 注入,命令注入，XSS 攻击，CSRF 攻击，Webshell 攻击，阻止应用层攻击和非法获取权限。

2.3.2.2、服务工具

2 台高级威胁防护设备

序号	指标项	技术要求
1	性能要求	网络层吞吐率≥8Gbps；防病毒吞吐率≥2Gbps；双电源； 配置防病毒、IPS（含虚拟补丁）模块、VPN 安全模块授权；
2	防病毒功能	产品具备企业级防病毒，支持双防病毒引擎，包含病毒扫描引擎和高级威胁扫描引擎，并可按照客户具体业务场景进行切换，满足客户针

序号	指标项	技术要求
		对病毒防护与查杀的业务需求。
3		支持快速扫描模式和深度扫描模式，针对不同场景和级别的可疑行为的文件进行安全级别处理措施设置。
4		支持客户自定义防病毒文件扫描大小，可支持 2G 及以上大文件进行扫描，满足客户针对不同文件病毒扫描需求。
5	入侵检测及虚拟补丁	具备服务器及终端虚拟补丁和主动式主机入侵防御系统，可支持在漏洞攻击主机之前予以侦测和拦截。包括但不限于防止漏洞利用和 SQL 注入、命令注入、Webshell 攻击、XSS 攻击，CSRF 攻击
6	仪表盘	能够对威胁进行可视化展示，展示维度至少包括威胁类型统计（至少包含勒索、挖矿、病毒、APT、漏洞利用威胁事件）、近 30 天威胁事件趋势、攻击源 IP TOP5、受影响主机 TOP5、勒索&挖矿事件拦截统计、热门威胁事件 TOP5、自定义黑名单 TOP5 等。
7	产品资质	获得《计算机软件著作权登记证书》和 IPv6 Ready Logo 认证证书，需提供有效证书的复印件；
8		产品具备国家计算机病毒应急处理中心计算机病毒防治产品检验实验室颁发的《网络安全专用产品安全检测证书》需提供有效证书的复印件；

2.3.3、日志存储服务

2.3.3.1、服务内容

部署统一的日志采集、分析、审计系统。集业务访问日志、鉴权日志等核心日志的异构留存；实现对服务器系统的操作日志的异构留存；实现对数据库、网络设备、安全设备的操作记录的异构留存，保障相关日志记录不因为黑客入侵致使日志丢失，提供对业务系统、服务器、数据库、网络设备、安全设备日志的本地存储，保障存储记录完整，且满足《网络安全法》中关于日志留存时效性的要求。

2.3.3.2、服务工具

1 台日志审计设备

序号	指标项	技术要求
1	性能要求	授权日志源≥50 个；
2	基础要求	独立完成审计日志采集，不依赖于设备或系统自身的日志系统； 审计工作不影响被审计对象的性能、稳定性或日常管理流程； 审计结果存储于独立存储空间； 自身用户管理与设备或主机的管理、使用、权限无关联； 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件。
3	日志采集	支持 Syslog(UDP、TCP）、目录、远端软件（FTP、SFTP、HDFS、LOCAL）、WMI、SNMP（Trap）、数据库（ORACLE、DB2、MYSQL、SQLITE、POSTGRES、SQLSERVER）协议日志收集。
		1、支持使用代理(Agent)方式提取日志并收集； 2、支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等。
4	日志分析	1、支持对设备日志查询和聚合分析； 2、系统内置常见安全事件关联分析规则； 3、支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警；
5	数据查询	1、支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、地理城市等参数进行过滤查询； 2、支持用任意关键字对所有事件进行高性能全文检索； 3、支持可指定多个查询条件进行组合查询；
6	产品资质	产品具备软件著作权登记证书；

2.3.4、VPN 接入服务

2.3.4.1、服务内容

提供安全高效的远程接入能力、远程运维接入能力、运维行为审计、多因素认证、访问控制细粒度授权与命令控制、支持运维资产和应用工具集中管理、单点登录、操作日志录像关联审计。

2.3.4.2、服务工具

1 台 VPN 和 1 台运维审计

VPN 安全能力

序号	指标项	技术要求
1	性能要求	VPN 接入授权≥50 个；
2	安全策略	支持基于域名的安全策略模糊匹配； 支持一体化安全策略，能够基于源/目的安全域、源 IP/MAC 地址、目的 IP 地址、地区、服务、时间、用户/用户组、应用层协议、五元组、内容安全（WAF、IPS、数据过滤、文件过滤、AV、URL 过滤和 APT 防御等）统一界面进行安全策略配置。
3	VPN	可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。 支持 IPsec VPN 智能选路，根据隧道质量调度流量。
4	产品资质	产品必须具有软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；

运维审计安全能力

序号	指标项	技术要求
1	性能要求	授权资产数≥100 个。
2	部署方式	支持逻辑串联部署、本地 HA 双机部署、异地 HA 双机热备部署、集群部署、多网卡绑定冗余
3	支持协议	各类协议的支持：字符协议支持 SSH、TELNET、RLOGIN； 图形协议支持 RDP、VNC、X11； 文件传输协议支持 FTP、SFTP； 支持通过浏览器页面 H5 方式发起运维操作，无需安装客户端； 支持调用本地数据库客户端工具 Navicat、PLSQL、DM6、DM7 访问数据库资产，支持数据库访问通过本地客户端方式进行单点登录；
4	运维资产	支持 Windows 主机、Unix 主机、Linux 主机、网络设备、安全设备、麒麟、统信；支持 Oracle、SQL Server、MySQL、DB2、Sybase、Informix、DM6、DM7、Kingbase 数据库
5	运维管理	主机访问工具除支持 SecureCRT、Xshell、Putty、WinSCP、FileZilla、MSTSC、RDP 外，还支持 mobaXterm 客户端；
6		支持运维人员发起会话共享，操作者可以邀请其他人员进行协同操作；协同人员支持主动申请操控权，操作者支持在线进行操控权分配，支持实时踢出会话协同人员；
		支持 C/S 架构，在 UOS 操作系统使用单点登录客户端访问；支持在移动端访问，提供 APP 及 H5 的访问，在移动端运维主机资产和实时展现告警消息（要求提供产品证明截图，并加盖公章）
7	资产管理	支持手工、自动方式发现目标资产，自定义配置 IP 地址段及自定义资产协议端口，精确识别是否在系统中存在，支持一键导入；支持手工、

序号	指标项	技术要求
		自动方式采集主机资产上的帐号列表，精确识别是否在系统中存在，支持一键导入；
8		支持资产账号管理，可查看资产账号名、资产名、账号类型、账号登录方式、账号状态等信息；支持自动账号稽核，识别僵尸账号、孤儿账号类型。
9		堡垒机系统系统自身的 IPv4、IPv6 地址配置，同时支持以 IPv4、IPv6、域名方式运维资产；
10	认证管理	支持基于国密资质芯片的手机软令牌双因素认证,芯片卡可作为硬件载体独立接入 4G/5G 网络；
11		应支持用户忘记登录密码时，在登录首页申请密码重置；支持手机短信、令牌口令、邮箱三种方式重置密码；
12	授权管理	支持访问策略的批量导入、导出及批量编辑功能；
13		支持分权分域管理功能，针对多部门实现权限精细划分，各个部门的管理员分别管理本部门的用户、资产及子部门，从而实现各部门之间的权限相互独立；
14	产品资质	产品具备软件著作权登记证书；

2.3.5、主机防护服务

2.3.5.1、服务内容

对信息中心本地服务器和 PC 终端的安全防护和统一纳管，支持对国产服务器和终端的防护。能够提供主机防病毒、防入侵、访问控制等各类安全防护能力。抵御间谍软件、网络钓鱼和其它灰色软件的攻击。同时提供集中的管理、监控、更新和部署等功能。

2.3.5.2、服务工具

1 套主机防护系统

序号	指标项	技术要求
1	性能要求	管理中心支持 CentOS、UOS、银河麒麟等主流操作系统； 客户端支持 Windows Server、Windows7~11、UOS、银河麒麟、中标

序号	指标项	技术要求
		麒麟、CentOS 等主流操作系统。 服务器防护授权数量不少于≥50，服务器需包含防病毒和虚拟补丁模块； 终端防护授权数量≥100，终端需包含防病毒模块。
2	客户端兼容性支持	支持一个管理控制台同时管理 Windows,Linux,信创操作系统，同时支持这些操作系统的服务器版和客户端版本。
3	终端管理	客户端支持多级分组管理，支持多级分组的创建、删除、移动至新分组，支持客户端基于 IP 地址段的自动分组，将满足条件的客户端自动分组。
4		支持以“普通模式”和“调试模式”收集客户端的故障信息，可以将收集的故障信息方便地反馈至安全厂商的服务人员进行故障排查分析。
5		支持客户端的防退出和防卸载功能，避免用户恶意退出或自行卸载，管理员可设置退出密码和卸载密码
6		可设置离线天数后的客户端自动删除，即时回收授权。
7		支持对 windows 客户端的锁屏和屏保进行设置，比如可设置 15 分钟无操作后自动启用屏幕保护。支持上传并设置指定的屏保文件
8	风险展示	支持针对单个终端推荐处置措施，支持以推荐措施的维度，展示针对系统内所有风险的推荐措施，措施信息包括：风险描述、处置措施步骤、受影响终端的统计与信息展示、受影响策略、推荐时间、所属类别
9	系统管理	支持多种更新方式： 1、支持在服务端更新完组件后立即启动客户端组件更新； 2、支持客户端在重新启动并连接到服务端后启动组件更新； 3、支持指定单个或多个客户端做为更新代理，并可指定某特定 IP 地址段的客户端从其他客户端获取更新 4、支持配置外部更新源，离线客户端可直接到外网服务器更新组件版本。
10		支持管理员选择客户端立即更新或回退至上一版本
11	防病毒模块	支持对压缩文件扫描，并可设定最大的压缩层数为 6。可以对超过固定大小文件不予扫描，以减少扫描时间；
12		对于恶意文件处理措施至少支持三种以上，包括厂家推荐措施、统一处理措施、以及针对不同类型病毒/恶意软件提供不同处理措施，同时不同病毒/恶意软件类型不少于 5 种分类
13		处置措施要提供至少两项措施，在首选措施失败的情况下，可以提供第二项措施进行处置；
14		为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时 CPU 占用比例，分高、中、低三个级别。低消耗下 CPU 高于 20%则暂停扫描以保证正常办公要求
15	虚拟补丁模块	支持虚拟补丁功能，通过漏洞防护规则，可在机器不重启，没有补丁

序号	指标项	技术要求
		更新的情况下帮助企业抵御漏洞攻击。
16	产品资质	产品必须具有软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；
17		中国网络安全审查认证和市场监管大数据中心颁发的，符合 GB/T 18336-2015《信息技术安全技术信息技术安全评估准则》和《终端安全管理系统产品安全技术要求》的 IT 产品信息安全认证证书。

2.3.6、漏洞发现服务

2.3.6.1、服务内容

提供专业的漏洞扫描能力，对各种主流的操作系统、应用服务、服务器、数据库、网络安全设备、数据库和中间件等进行漏洞扫描。通过漏洞扫描和人工验证，发现高、中、低不同等级的安全漏洞。

2.3.6.2、服务工具

1 台漏洞扫描设备

序号	指标项	技术要求
1	扫描技术	支持智能服务识别、授权登录扫描、多路扫描（可以同时对多个隔离网络进行扫描）等。
		扫描目标支持：IPV4,IPV6,域名同时下发；
2	扫描策略	支持 20 种以上的默认扫描策略，分别针对不同的扫描对象，如 Windows、类 Unix、数据库、WEB 服务、网络设备、云平台、摄像头、大数据、国产化等。
3	口令猜测	单独支持弱口令扫描任务，支持弱口令识别协议数量>30+条。
4	任务管理	任务执行周期支持：立即执行、定时执行、周期执行；
5	漏洞知识库	系统漏洞数量>300000 条； CVE 漏洞数量>28,0000 条； 系统原理扫描漏洞数量>1800 条； 所有的漏洞信息都能够在产品中随机进行浏览和多维度检索。
6	产品资质	产品具备软件著作权登记证书；

2.3.7、数据流转监测服务

2.3.7.1、服务内容

提供数据的共享交互场景的监测能力，对网络流量中的 Http/https 的请求与返回进行解析。针对数据接口中敏感资产传输、异常操作监控，对数据流转过程进行合规监控，并对攻击与风险及时告警与响应。

2.3.7.2、服务工具

1 台数据流转监测设备

序号	指标项	技术要求
1	性能要求	分析流量性能≥2000Mbps；
2	资产发现	支持通过流量解析自动发现应用资产、接口资产、账号资产、敏感数据资产、文件资产和客户端 IP 信息。
3		支持根据应用域名以及应用的业务重合度，深度结合 AI 技术进行资产合并智能推荐，支持应用拆分；
4	API 接口梳理	支持通过导入接口文件的方式进行接口添加，并对未知隐蔽接口进行标识。
5		支持二次封装接口识别和标识，并支持接口封装前后样例对比和查看；
6	资产展示	支持应用列表，展示应用基本信息和访问信息，以及风险和脆弱性标识；并支持列表导出；
7	多维分析	支持对审计日志进行多维条件下钻分析。根据查询条件可自定义选择图表样式，可对分析结果进行可视化查看，也可下载查看；可支持多维分析条件生成自定义报表模板；
8	对比分析	支持基于接口的历史对比分析，分析本周与上周被访问次数、被访问数据量/下载文件数、访问账号数、访问 IP 数、被访问时间段以及访问终端的对比差异。

序号	指标项	技术要求
9	溯源结果分析	支持溯源结果分析，包括溯源内容对应的敏感数据类型，命中的记录数，并图表展示溯源内容在应用、账号、客户端 IP、接口、访问时间等多个维度的访问热度；
10	自身安全	支持系统自身数据安全措施，对审计结果展示内容中包含的敏感数据进行脱敏处理，防止运维过程中的数据泄漏。需通过权限申请，输入密码后查看原始数据，并在查看原始数据时加注网页水印，震慑截图拍照行为。
11	产品资质	产品必须具有软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；
12		中国网络安全审查认证和市场监管大数据中心颁发的《网络关键设备和网络安全专用产品安全认证证书。

2.3.8、网络安全威胁监测管理服务

2.3.8.1、服务内容

通过威胁检测探针采集网络流量，发送至安全威胁管理平台，对信息中心本地卫生专网和互联网的网络流量进行深度分析，发现流量中的恶意攻击，实现统一的安全检测、多维度溯源分析、集中运维管理等核心功能，开展安全可视化管理。

2.3.8.2、服务工具

2 台威胁检测探针、1 套安全威胁管理平台

威胁检测探针安全能力

序号	指标项	技术要求
1	性能要求	监测能力≥2Gbps，
2	威胁检测能力	挖矿检测能力：提供多样性的挖矿检测手段，矿池协议告警须提供虚拟币家族、类型等信息。
3		分析监测类别：支持恶意文件侦测、恶意行为分析侦测、应用程序侦测、常见漏洞检测、WebShell 工具检测、黑客工具检测。

序号	指标项	技术要求
4	威胁分析能力	告警一键降噪：能够使用统计模型对产生的告警日志进行噪声分析。用户在分析日志时，可以根据噪声级别对日志进行实时过滤。支持对历史数据进行噪声标记。分析模型支持在线更新。
5		告警多维度筛选分析：支持在安全告警筛选与分析层面，能够提供超过 60 个维度的告警筛选，包括但不限于：攻击方法、攻击结果、威胁描述、攻击阶段、攻击方向、文件 SHA1、http 返回码、攻击评分、威胁特征、威胁标签、传输协议、应用协议等维度的筛选与展示。
6		监测探针内置自动研判功能，能够对攻击方向、攻击结果进行自动判定，并在告警中展示攻击结果。对于聚合后的告警，能展示不同攻击结果的次数。
7	威胁情报	自定义威胁情报：支持网络威胁自定义与威胁情报自定义，网络威胁能自主添加规则名称，规则等级与规则类型，语法兼容业界最常用的 snort 规则的写法。威胁情报自定义包括 IP、URL、DOMAIN、文件 HASH 四种类型，可以根据具体的使用场景进行选择。威胁情报自定义的规则可以支持多个同类对象的集合，比如对多个 IP 同时进行监控。
8		产品厂商能在全国范围内收集恶意域名，具备通信管理局部颁发的全国范围互联网域名解析服务业务经营许可证。
9	威胁溯源能力	恶意文件流转溯源：能够以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载。
10		威胁流量数据下载：支持威胁流量的自动存储，及威胁流量 PCAP 文件格式下载
11		流量抓包：能够配置灵活的抓包策略，支持设定抓包的 IP 地址范围、协议等条件，可设定抓包文件大小。
12		流量包回放：支持 pcap 回放功能，对导入的 pcap 进行回放并进行威胁检测，回放产生的告警必须和生产网络流量的告警分页面展示，避免干扰正常安全运营。
13	产品资质	产品必须具有软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；
14		产品具备中国网络安全审查技术与认证中心颁发的符合 GB/T 18336-2015《信息技术安全技术信息技术安全评估准则》、《APT 安全监测产品安全技术要求》的 IT 产品信息安全认证证书；

安全威胁管理平台安全能力

序号	指标项	技术要求
1	性能要求	支持接入≥2Gbps 的镜像流量；支持接入≥50 台服务器和 100 个终端资产；
2	态势感知大屏	支持安全态势的可视化呈现，以大屏的方式从全网已发现威胁、已拦截威胁、潜在威胁、热门威胁的统计数据等多个维度进行可视化展示，并提供对整体网络安全级别的评估。
3		支持勒索治理场景化大屏，支持从六个攻击阶段展示勒索入侵全流程

序号	指标项	技术要求
		的相关安全告警，实现了攻击进程可视化。并通过勒索大屏展示了勒索告警趋势。
4	统一管理	支持通过态势感知平台对流量检测设备、主机加固系统、终端安全管理系统等进行统一的管理和单点登入。
5		支持通过平台对接入的流量检测设备、主机加固系统、终端安全管理系统等进行系统升级，升级包支持在线更新和本地上传的方式实现。
6	终端管理	平台支持对同品牌的终端安全管理软件进行统一管理，方便查找、过滤和了解终端安全情况。
7	威胁情报管理	支持手动自定义添加本地威胁情报，威胁情报的类型至少包括文件名称的 SHA-1、IP 地址、URL、域名等类型。
8		支持云端威胁情报和本地威胁情报，本地威胁情报支持手工添加和批量导入。
9		本地威胁情报源支持同步威胁分析设备和沙箱设备的情报；支持对接上级/下级单位态势感知中心的威胁情报库。
10	系统管理	系统支持维护功能，能直观的显示系统的 CPU、内存、磁盘和日志存储的使用情况；
11	安全告警	支持告警规则的自定义，能够选择风险类型、告警阀值进行设置，达到阀值之后对选择指定负责人进行邮件告警。为避免重复告警，支持在告警通知中取消重复告警。
12	产品资质	产品具备软件著作权登记证书；

2.3.9、利旧设备维保及备件服务

2.3.9.1、服务内容

7 台老旧设备维保及备件服务：

序号	设备名称	生产厂家
1	上网行为管理	天融信
2	防火墙	华为
3	数据库审计	安恒
4	IPS	网御星云
5	IPS	网御星云
6	网闸	网神
7	网闸	网神

2.3.10、网络安全防护服务交付

交付成果（包括但不限于）：

- 《本地机房安全防护服务月度巡检分析报告》（按照使用情况，内容包括工具情况、记录、监测告警、处理等）
- 《漏洞扫描季度分析报告》

服务提供工具：

- 2 台边界安全设备
- 2 台高级威胁防护设备
- 1 台日志审计设备
- 1 台 VPN 和 1 台运维审计设备
- 1 套主机加固软件
- 1 台漏洞扫描设备
- 1 台数据流转监测设备
- 2 台威胁检测探针和 1 套威胁管理平台

2.4、网络安全运维保障服务

2.4.1、本地日常安全运维服务

2.4.1.1、服务内容

以 5*8 小时的现场服务，派遣 1 名技术人员提供驻场服务（具体工作时间以中心工作时间为准），负责中心本地机房的网络安全进行管理。驻场人员需具备 CISP 资质，针对机房网络、主机、数据库、中间件、网络设备、安全设备、应用系统等重要信息资产，持续开展安全风险监测，动态跟踪，研判风险态势并及时处置，对漏洞与威胁处置进行持续跟踪，每月对安全设备进行安全巡检，并提供协助迎检服务等。配备二线、三线技术专家适时按需提供支撑，需具备 CISAW 或 CISSP 及以上资质。工作内容包括但不限于：

1、数据流异常分析和黑客入侵监控；

2、重要服务器系统信息监控、服务器重要文件监控、重要服务器网络连接和系统进程监控；

3、对核心数据库异常操作进行监控，并对监控、性能数据进行统计分析；

4、配置信息监控、故障监控、性能监控；

5、核心网络设备的日志告警信息和设备运行状况监控；

6、重要安全设备的安全事件、入侵报警等信息和设备运行状况监控；对关键应用的进程监控、应用的异常监控、应用的网络连接监控；

7、每月对本地安全设备（如防火墙、入侵防御、日志审计等）进行安全巡检，设备运行状态、安全策略的配置检查等，对发现的问题及时进行处置；

8、对漏洞与威胁处置进行持续跟踪。漏洞检测、分析与验证、漏洞修复跟

踪、威胁监测预警处置跟踪；

9、根据不同类型的检查要求（风险排查及评估、等保及商用密码测评、责任及制度执行、漏洞整改等），调整协助迎检服务内容（自查自评、完善政策、技术防护、应急演练、编写文档及整理等）。

2.4.1.2、服务交付

交付成果报告（包括但不限于）如下：

- 《安全运维周报》
- 《安全运维月报》（包括安全设备巡检内容）
- 《安全事件处置报告》
- 《资产台账》
- 《漏洞管理台账》
- 《迎检服务报告》

2.4.2、重保值守服务

2.4.2.1、服务内容

提供不少于40天的重保服务（包括但不限于春节、国庆、两会、护网等，具体保障时段以中心要求为准）。期间进行相关网站、重要业务系统、网络进行安全检测、监测及安全值守工作。

1、建立值班表，保证24小时电话畅通。现场人员在保障期间不得离汉，远程人员随时可使用互联网进行工作；重要服务器系统信息监控、服务器重要文件监控、重要服务器网络连接和系统进程监控；

2、每日撰写保障日报，提供二线专家团队支撑；

3、风险暴露面排查：针对互联网暴露的域名/IP 进行梳理，充分识别出对外开放的已知的和未知的互联网资产；

4、日志分析服务：对安全设备的告警日志信息进行人工分析，并协助进行策略加固；

5、严格按照安全保障工作要求每日多时段进行零报告，不得迟报、漏报和瞒报；

6、应急处置：重保期间，对异常情况、突发安全事件及时上报并处置，查明原因出具相关报告；

7、重保结束提交《重要时期安全保障总结报告》。

2.4.2.2、服务交付

交付成果报告（包括但不限于）如下：

- 《风险排查报告》
- 《重保监测日报》
- 《攻击事件分析处置报告（重保期间）》
- 《重保总结报告》

2.4.3、风险评估服务

2.4.3.1、服务内容

每半年开展一次风险评估。对信息中心本地信息系统进行物理环境评估、网络结构分析、安全基线检查、渗透测试工作。

2.4.3.2、服务交付

交付成果报告（包括但不限于）如下：

- 《渗透测试报告》
- 《风险评估报告》

2.4.4、应急响应与演练服务

2.4.4.1、服务内容

1、应急响应：为中心提供7×24小时应急支持服务，事先建立完备的应急响应预案。当发生重大安全事故时，响应时间少于5分钟，到达现场时间不超过1小时，协助进行系统恢复、网络恢复、保存痕迹等工作，并配合执法部门完成调查取证。事后输出《应急响应报告》。

2、应急演练：每年开展2次。制定以主要网络攻击场景的应急演练方案，内容涵盖处理过程、各环节的处理内容以及应急机制等；完成演练后，输出应急演练总结报告，并完善《应急预案》。

2.4.4.2、服务交付

交付成果报告（包括但不限于）如下：

- 《应急预案》
- 《应急响应报告》
- 《演练实施方案》
- 《应急演练总结报告》

三、 商务要求

序号	商务条款	内容
1	服务期	合同签订后 1 年
2	地点	甲方指定地点
3	报价要求	投标人报价应包含为完成本招标文件提出的货物或服务等全部相关工作所有可能发生的费用，即投标总报价为“交钥匙”价。对在合同实施过程中可能发生的其他费用，采购人概不负责。 对本文件未列明，而投标人认为必需的费用也需列入投标总报价。在合同实施时，采购人将不予支付中标人没有列入的项目费用，并认为此项目的费用已包含在投标总报价中。
4	售后服务	针对突发安全应急事件，在收到应急响应服务请求，提供半小时内远程响应，以远程的方式协助查明安全事件原因，确定事件的威胁和破坏的严重程度，安全资深专家 1 个小时内到达现场，立即对事件进行分析、检测完成后给出应急响应报告。
5	培训	按照采购人要求提供培训服务
6	验收标准与方式	验收标准：甲方根据合同条款、服务要求、相关报告完备合格对乙方服务进行验收。 验收方式：甲方组织相关专家验收，确认达到各项服务标准要求后，完成验收。
7	付款方式	首付款：合同签订后，乙方向甲方提供相应金额发票，甲方在 10 个工作日内向乙方支付本合同总价的 30%，用于服务启动（服务工具租赁及服务人员）。 第二次付款：安全运维服务期满三个月，相关技术档案完备、合格，且无重大安全事故，乙方向甲方提供相应金额发票，甲方在 10 个工作日内向乙方支付本合同总款额的 20%。 第三次付款：安全运维服务期满九个月，相关技术档案完备、合格，且无重大安全事故，乙方向甲方提供相应金额发票，甲方在 10 个工作日内向乙方支付本合同总款额的 30%。 尾款：项目服务期结束，经验收合格，10 个工作日内，乙方向甲方提供相应金额发票，甲方在 10 个工作日内向乙方支付本合同总款额的 20%。
8	保密	未经采购人书面许可，中标人及其工作人员不得擅自对相关数据和信息进行复制、备份或留底。