中大惠亚医院信息化项目技术要求

**用户需求**

**一、采购内容**

| **序号** | **采购项目名称** | **数量** |
| --- | --- | --- |
| 1 | 网络安全系统等级保护升级与服务 | 1项 |

说明： “▲”所标参数为专家进行综合评分的重要参数，但不作为废标条款。

“★”标注项为不可偏离的重要响应内容，否则作无效投标处理。

投标人资格要求

1．投标人应具备《中华人民共和国政府采购法》第二十二条规定的条件；

2．在中国境内注册，在法律上、财务上独立，合法运作并独立于采购人和采购代理机构的法人；

3．经营范围必须满足本次招标范围；

4．投标人应具备网络安全管理技术与服务的能力。

**二、项目背景**

惠州市中大惠亚医院于2013年3月正式开业运行，开业至今逐步建立起了一套服务临床、管理决策的医疗信息系统，随着医院业务不断的发展，对医院IT信息化支撑平台及网络安全提出了更高的要求，近年来，伴随着互联网的高速发展，外部网络环境愈发复杂，网络与信息安全形势严峻。

根据《国家卫生健康办公厅关于2019年卫生健康行业网络安全情况的通报》（国卫办规划函[2020]202号）、《广东省卫生健康委办公室关于“护网行动˙疫情保障”网络攻防演习攻破134家医疗机构网络情况的通报》、《惠州市政务服务数据管理局印发关于加强网络安全防护工作的通知》和《大亚湾区网络安全安全风险范围情况报告》等系列文件要求，医院需夯实网络安全工作基础，严格落实网络安全等级保护制度，加强医院关键信息基础设施安全管理和技术防护，增强身份识别、态势感知、入侵防御、容灾备份等措施，加快完善医院信息应用安全和数据安全技术防护体系。我院医院信息系统作为大亚湾区关键信息基础设施之一，需加强系统安全防护、补齐安全防护短板，完成网络安全等级保护工作。现结合我院网络安全等级保护工作和网络安全整改过程中的实际需求，拟增补一批网络安全设备和系统，以全面提升医院网络信息安全防护能力和水平，切实保障医院网络及信息系统的稳定运行。

**三、技术要求**

**1.系统清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品** | **基本功能** | **数量（台）** |
| 1 | **数据库审计系统** | 实时对国内外主流数据库的全面审计功能，通过对数据库的状态健康、SQL注入检测、弱口令扫描等方式及时发现威胁数据库安全的潜在因素，并及时进行阻断，保障数据库安全运行，并满足《网络安全法》及《信息系统安全等级保护基本要求》中的要求。 | 1 |
| 2 | **网络安全态势感知平台** | 实现对网络安全事件的检测与预警、威胁的检测和感知、事件的深度分析和处理以等多角度网络安全管理，全面掌控网络安全态势，对整体安全形势进行事前预警和事后溯源，以及对事中防护提供重要感知信息。 | 1 |

**2、技术要求**

**2.1数据库审计系统：**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 规格要求 |
| 1 | 基本要求 | 2U标准机架设备，双电源，至少6个千兆电口，1个接口扩展槽位，储空间不得少于4T，支持RAID1阵列。 |
| 可审计数据库流量500M每秒，事件每秒入库速度至少在25000条/秒以上，日处理事件数15000万条； |
| 2 | 部署和管理 | 旁路部署在服务器区域或运维区域，同时支持旁路和在线两种部署模式； |
| 支持分布式部署，可以通过统一的数据中心采集多个独立引擎的日志。总控制台能够适时监控分布式部署引擎的系统状态、策略和审计事件，审计日志统一存储、查询、分析、统计。 |
| 可HA部署，产品支持主备方式，需提供截图证明； |
| 4 | 数据库审计 | 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用、神通数据库审计，需提供截图证明； |
| 支持对针对数据库的XSS攻击、SQL注入攻击行为进行审计。需提供截图证明。 |
| 支持对超长SQL语句的审计，操作信息的提取审计、支持对数据库绑定变量方式访问的审计。提供国家第三方权威机构颁发的数据库操作的信息提取和审计方法及其装置、系统技术证明文件。 |
| 支持对Oracle数据库状态的自动监控，可监控会话数、连接进程、CPU和内存占用率等信息。需提供截图证明。 |
| 支持双向审计，支持对Select操作返回行数和返回内容的审计。需提供截图证明。 |
| 提供对数据库返回码的知识库和实时说明，帮助管理员快速对返回码进行识别。需提供截图证明； |
| 支持访问数据库的源主机名、源主机用户、SQL操作响应时间、数据库操作成功、失败的审计；  支持数据库操作类、表、视图、索引、触发器、存储过程、游标、事物等各种对象的SQL操作审计； |
| 支持数据库存储过程自动获取及内容审计，需提供截图证明； |
| 5 | 网络协议审计 | 支持Telnet与FTP协议的审计，能够审计用户名、操作命令、命令响应时间、返回码等； |
| 支持审计网络邻居的用户名、读写操作、文件名等； |
| 支持审计NFS协议的用户名、文件名等； |
| 支持审计HTTP/HTTPS协议的URL、访问模式、cookie、页面内容、Post内容；需提供截图证明； |
| 支持IP-MAC绑定变化情况的审计，需提供截图证明； |
| 6 | 业务关联审计 | 支持自动方式建立web访问和SQL访问之间的对应关系，生成访问行为模型库，需提供截图证明。 |
| 支持中间件环境下的SQL语句关联到HTTP操作，HTTP操作关联到HTTP-ID，实现中间件环境下的审计追溯。 |
| 支持实时关联模式，可实时查看关联审计结果，无须事后手工查询。 |
| 7 | 数据库异常行为智能审计 | 支持自动建立数据库操作行为基线。 |
| 数据库操作行为基线包括数据库账号、操作类型（SQL模板）等行为特征，安全威胁检测工鞥呢。提供自主知识产权关于检测数据库是否遭到跨站脚本攻击的方法证明文件。 |
| 对超出数据库操作行为基线的操作可自动识别，并及时告警。 |
| 8 | 审计策略支持 | 系统应自带不少于100个缺省的审计规则库，方便用户选择使用； |
| 用户可自定义审计策略，审计策略支持时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件； |
| 数据库审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件（非正则表达式方式）； |
| 审计策略支持字段名称和字段值作为分项响应条件（非正则表达式方式） |
| 9 | 响应方式 | 支持按照风险级别进行告警，告警方式支持界面告警、Syslog告警、SNMP trap告警、短信告警、邮件告警； |
| 支持数据库操作的命令级阻断，可阻断单个操作，但会话保持。具备数据库操作响应时间测算技术能力，提供国家第三方权威机构颁发的技术证明文件。 |
| 10 | 日志查询统计 | 支持按时间、级别、源\目的IP、源\目的MAC、协议名、源\目的端口为条件进行查询 |
| 支持查询、统计的条件模板编辑与应用，需提供截图证明； |
| 支持多个查询、统计任务同时进行； |
| 数据库访问日志，支持按数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、SQL语句关键字、数据库返回码、SQL响应时间、数据库返回行数作为查询和统计条件 |
| web访问日志，支持按URL、访问模式、cookie、页面内容、Post内容等作为查询和统计条件，需提供截图证明； |
| 支持查询统计条件之间的与、或、非逻辑组合； |
| 提供缺省的报表模板库，包括SOX报表、PCI报表等模板，供用户选择使用； |
| 支持自定义报表模板，包括统计日志周期、过滤条件、图标样式等； |
| 支持按每天、每周、每月、时刻生成报表，支持邮件方式定期自动发送报表； |
| 具备数据库安全保护方法技术能力，提供国家第三方权威机构颁发的技术证明文件 |
| 11 | 自身管理 | 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能 |
| 管理员登陆支持静态口令认证，支持密码的复杂性管理，比如大小写、数字、特殊字符、长度等； |
| 能够对连续失败登陆进行自动锁定，锁定时间可设置； |
| 提供审计数据管理功能，能够实现对审计日志、审计报告的自动备份； |
| 提供系统升级功能，能够通过升级包的方式实现升级； |
| 提供磁盘存储容量不足、磁盘Raid故障等自动邮件报警； |
| 提供CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能； |
| 12 | 联动功能 | 与WAF支持联动，可对WAF上报的应用系统攻击实现场景还原展示。需提供截图证明； |
| 支持与APT检测产品的联动，对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件。需提供截图证明。 |
| 13 | 第三方接口 | 支持SNMP方式，提供系统运行状态给第三方网管系统； |
| 支持Syslog、SNMP方式向外发送审计日志； |
| 支持连接外置存储，以扩展日志存储能力； |
| 支持NTP时间同步； |
| 14 | 数据库攻击检测 | 支持对针对数据库的SQL注入、XSS攻击行为进行检测。需提供截图证明。 |
| 15 | IPV6支持 | 支持IPV6环境下数据库的审计，需提供截图证明； |
| 16 | 质量保障 | 为确保项目质量，所投产品是主流厂商产品，并且近三年(2016年或2017年或2018年市场占有率前三，提供权威机构盖章的数据引用证明文件（如：IDC、CCID、Frost & Sullivan等权威机构）。 |
| 16 | 资质要求 | 产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（增强级）；需提供证书复印件； |
| 产品具有中国信息安全认证中心颁发的强制认证证书（增强级）；需提供证书复印件； |
| 产品具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》，需提供证书复印件； |
| 产品具备网络关键设备和网络安全专用产品安全认证证书；需提供有效资质证明复印件。 |
| 产品具有IPv6 Ready logo Phrase 2认证，并提供证书复印件； |
| 17 | 厂商资质 | 必须是CNCERT网络安全应急服务国家级支撑单位； |
| CVE等漏洞挖掘能力，挖掘漏洞数量不少于400个，提供漏洞列表。 |
| 产品生产厂商应具备安全服务和应急响应支撑能力，必须具备信息安全服务资质证书（安全工程类三级），并提供证书复印件。 |

**2.2网络安全态势感知平台**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 规格要求 |
| 1 | 部署方式 | 软件系统，系统内置管理分析中心和内置FLOW采集器，镜像采集器，无需安装任何其他软件和组件。支持镜像，分光，FLOW等多种数据采集方式，配置至少100节点的基线（资产基线，流量基线，服务基线）建模对象授权。 |
| 支持按照源区域，目的区域， 源端口，目的端口，应用协议来来配置报文过滤规则，实现镜像流的采集过滤。 |
| 支持镜像包采样配置，支持FLOW采集的流采样配置；支持路由器的配置管理，路由流量上下行方向的设定。提供界面截图证明。 |
| 2 | 外部威胁感知 | 检测高风险流量：境外/区域外通信流量：对境外连接、省际连接、区域外连接进行全面监控，生成地图；检测网络中不安全的TELNET通信流量；发现隐藏恶意行为的SMB流量； |
| DNS异常分析：通过内置机器学习算法发现DNS隧道，实现DNS异常行为分析 |
| 威胁情报：从恶意DN，URL，EMAIL，IP 威胁情报信息来进行威胁预警，给出疑似恶意域名预警，疑似恶意IP预警，疑似恶意EMAIL预警，疑似恶意URL预警，情报来源包括开源情报，内部情报等 |
| 支持检测阈值自学习，支持检测插件的检测模式（仅包数检测，仅字节数检测，包数和字节数同时满足，包数或字节数任意满足）配置，提供界面截图证明 |
| DDOS 攻击发现：基于特征的，基于时间窗口基线的，基于周期性基线算法实现DDOS攻击检测：支持syn flood ,ack flood ,icmp flood ,udp flood 等网络层DDOS攻击以及http get flood,dns query flood,dns response flood dns 随机域名攻击，dns 投毒检测等应用层DDOS攻击；支持网络误用攻击，支持ip黑名单，ip白名单，私有IP的配置；支持检测群组的设置 |
| 支持DDOS攻击的异常缓解，将异常流量牵引到清洗设备上进行异常流量清洗，支持与同品牌的流量清洗guard设备进行联动，提供界面截图证明 |
| 3 | 潜伏威胁感知 | 支持内网中失陷主机分析与取证。  支持失陷主机列表分析，列表字段包括问题设备，区域，攻击方式，确定度指标，威胁度指标，处理状态和详情：。  支持支持主机失陷状态迁移图查看以及失陷主机的资产详情：资产详情包括所属区域，主机名称，设备类型，所属区域等。 |
| 支持潜伏威胁安全事件分析，包括嗅探行为监测，入侵行为监测，C&C控制行为监测，威胁横向扩散以及可疑数据的外发监测。 |
| 支持对失陷主机的取证，根据安全事件类型对失陷主机给出处置建议，提供界面截图证明。 |
| 利用行为监测：支持入侵利用事件统计与列表，安全事件包括外连SMB会话：.暴力登陆（FTP暴力破解，WEB 暴力破解，MYSQL暴力破解等），扫描后建立双向会话的行为。 |
| 嗅探行为监测：支持扫描事件的统计与列表展示，安全事件包括基于tcp/udp 端口扫描，基于tcp/udp的主机扫描告警，ping扫描，stealth主机扫描，提供界面截图证明。 |
| C&C命令控制行为监测：支持C&C安全事件统计和列表，安全事件包括僵尸命令&控制服务器会话连接，僵尸主机尝试CC活动，僵尸感染主机成功完成CC通信行为，可疑的轻量长连接，提供界面截图证明。 |
| 威胁横向扩散行为监测：支持拓扑展示威胁在内网的扩散情况，包括蠕虫传播，蠕虫活动，提供界面截图证明。 |
| 可疑数据外传监测：支持可疑数据外传的安全事件统计与外传事件列表，包括Icmp隧道，可疑数据囤积，DNS隧道，数据外发事件。 |
| 4 | 网络感知功能 | 流量基线自学习，当访问流量与与学习到的基线模型存在偏差，则对偏离基线的资产进行预警：资产的流量基线，服务基线，访问关系基线来感知网络，建立相应的用户网络基线，并对偏离基线的资产进行预警。  1资产服务基线学习与变化预警  1)未知服务发现  2)流氓服务：非标准端口上开启的服务发现，隐藏应用的发现  2资产访问关系基线学习以及变化预警：在设定的学习周期内，计算主机的连接的IP数，连接的IP网段/区域，连接的地理范围  3资产流量峰值与均值学习以及变化预警：计算bps,pps,sps的峰值与均值，  4关键服务器梳理与私建服务器发现  1）FTP服务器梳理与私建FTP服务器发现  2）DNS服务器梳理与私建DNS服务器发现；  3）WEB 服务器梳理与私建WEB网站发现；  4）NAT设备发现：发现边界的NAT设备，以及NAT设备后挂接的私网设备数目，提供界面截图证明。 |
| 5 | 流量分析功能 | 支持从全网到关键业务区域到特定业务主机逐层细粒度精细化流量分析，对于监控的目标（路由器，路由器组，路由器接口组，服务器,业务场景，协议，应用，对比分析）,可以根据总流量、路由设备、 TOP地址、TOP应用、TOP协议、TOP自治域等角度进行分析展现；可按照时间范围进行查询，展现内容至少包括平滑流量、上行流量、下行流量，实际流量上行流量、下行流量，展示维度为bps，pps，sps；支持按业务场景进行流量分析，可自定义业务场景，支持业务场景对比分析，提供界面截图证明。 |
| 发现带宽占用症结：占用网络带宽的TOP地址、TOP应用，可定位到具体的时间，具体区域，具体IP，具体使用责任人。 |
| 6 | 资产感知功能 | 资产发现，建立资产基线，具备资产发现功能，资产IP库自学习与变化预警：在设置资产IP基线学习周期内，全面监控管理区域的在线设备，形成用户正常业务周期内的资产库白名单。 |
| 支持资产列表，字段包括IP地址，区域，主机名称，资产类型，厂商，型号，版本，联系人，购置日期，质保日期，最近出现时间，当前流速，总流量。  具备资产自学习功能，支持资产类型管理：工控设备，网络设备，安全设备，数据库，中间件，存储设备，应用系统，虚拟化，机房设备等，支持通过资产列表查看查看资产活跃状态，最近出现时间，当前总流速，总流量，会话流量桑基图，会话列表，提供界面截图证明。 |
| 支持主机画像功能：可刻画主机的告警，流量基线，访问端口，访问关系(进出），开放服务端口，提供界面截图证明。 |
| 支持行为拓扑监控视图：以拓扑视图的方式可视化整网或指定区域的数据行为的合规，违规关系：点击区域，则下钻到区域内部IP之间的连接行为关系和此区域内部IP和其他区域的连接关系。将鼠标的焦点放在节点之间的连线上，可以查看数据总流量，流速，网络协议，应用协议，提供界面截图证明。 |
| 拓扑可支持时间轴方式查看历史拓扑，时间轴的粒度为当天24小时，一周，一个月，二个月，半年，自定义。当天24小时可查看每小时的拓扑行为视图；周月年的时间粒度，可以查看每天的拓扑行为视图。也可以查看任意时间段（最小粒度为小时）的行为拓扑，提供界面截图证明。 |
| 7 | 协议解析 | 支持HTTP/HTTPS/DNS/FTP/SMTP/POP3/IMAP/LDAP/SMB/MYSQL/TELNET/TDS/等应用层协议的深层解析； |
| 流量信息包括五元组，应用层协议，发送流量，接收流量，发送包数，接收包数，发/收（字节）比率，发/收（数据包）比率，开始时间，持续时间，结束时间，源MAC，目的MAC，TCPFlags，请求内容，响应，解析内容，Title，Tos，总包数，功能码，发送者地址，接收地址，文件名，下一跳，采集器IP地址等30个流量字段。同时还包括事件分类，解析内容，请求内容，设备名称，业务场景，日志类型等多个流量相关的空间，时间维度信息，提供界面截图证明。 |
| 8 | 调查取证功能 | 支持取证功能：支持规则触发告警的追溯取证，可下载到原始pcap包，提供界面截图证明。 |
| 支持安全事件的调查分析功能：支持安全事件的危害说明与安全处置建议，提供界面截图证明。 |
| 9 | 综合态势大屏 | 支持自学习策略：包括基于基线建模的20多种异常检测算法：智能检测基于自适应自学习基线算法，包括周期性基线同比分析或时间窗口基线的环比分析，从而发现Ddos攻击，网络误用，流量超常（bps超常，pps超常，会话连接数超常等），协议比例异常（tcp比例异常，udp比例异常，icmp比例异常，igmp比例异常等），流量分布异常（源地址分散度异常，目的地址分散度异常，端口分酸度异常等），支持检测群组的设置，可根据不同的检测群组设定不同的字节阈值和包数阈值，提供界面截图证明。 |
| 支持基于特征检测的蠕虫事件：Code Red，硬盘杀手，冲击波，SQL Slammer,震荡波，UDP Fragment Flood，私有IP异常，DarkIP 异常等 |
| 支持违规行为策略：支持链路层（源目的MAC 地址），网络层（五元组，发送流量，接收流量，发收比率，Tos等)，传输层（源目的端口，协议），应用协议（DNS 域名，HTTP 协议的请求内容，解析内容，响应，MAIL 的发送方，接收方，邮件主题等字段）设置关联分析，支持逻辑关联，统计关联，多事件关联。 |
| 支持流秩序，网络感知，潜伏威胁感知，外部威胁感知4个大屏展示页面，提供界面截图证明。 |
| 从网络态势感知需要”知己”的角度来呈现用户网络中已知资产与未知设备接入情况，关键业务系统的服务开启以及使用状况，不同区域、部门间流量访问情况。业务访问合规审计与告警，基于行为基线的偏离度告警。 |
| 10 | 报表报告 | 支持报表报告的导出，导出的格式支持EXCEL、PDF、WORD、PNG、HTML、RTF等，支持Office 2007格式； |
| 流量统计报表支持：TOP10\_L4协议统计报表，TOP10\_L7协议统计报表，TOP10地址统计报表，TOP10自治域统计报表 |
| 支持流量趋势报表： L7协议趋势报表，流量趋势报表，地址趋势报表，自治域趋势报表。 |
| 11 | 系统 | 支持数据代理接口：syslog或SNMP TRAP转发告警日志，系统日志。 |
| 支持多种系统资源：地址资源，端口资源，时间资源，指令功能码，自定义资源，提供界面截图证明。 |
| 支持存储策略配置：支持全流量存储，支持根据IP，端口信息条件设定存储原始报文。 |
| 支持多种诊断工具：PING，SNMP，抓包分析。 |
| 12 | 产品资质要求 | 产品须获得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； |
| 产品须具有《计算机软件著作权登记证书》； |
| 产品须具有中国信息安全测评中心《信息技术产品安全测评证书》EAL3级； |
| 产品须获得中国信息安全认证中心《IT产品信息安全认证》； |
| 产品须具有《军用信息安全产品认证证书》。 |

**2.3信息安全服务**

**2.3.1服务范围**

本次网络安全服务针对医院信息系统整体安全的现状，提供专业化安全管理和技术服务，安全管理和技术服务的范围涉及到以下内容:

（1）医院核心网络，包括医院内网和外网；

（2）医院现有安全设备，包括边界类设备、摆渡类设备、终端设备、旁路设备等；

（3）医院现有运行系统（HIS、PACS、LIS、EMR等）后台支撑系统和软件（如操作系统、数据库、中间件等）；

（4）机房内物理安全，包括机房监控、机房灾难预防设备、机房管理设备；

▲（5）配合医院完成医院网络安全管理制度的建设和运维。

▲（6）配合完成医院信息安全等级保护工作相关整改需求。

（7）本次信息安全服务服务期为壹年。

**2.3.2安全维护服务内容**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **形成文档** |
| 1 | 现有安全设备整合 | 上网行为管理、应用防火墙、漏洞扫描系统、日志审计系统、网闸、入侵检测、审计设备、企业版杀毒软件、终端准入控制系统等安全设施的安全规则设计和实施任务的差距分析 |  |
| 2 | 定期安全检查 | 每季度一次，分析现网络的安全风险，发现潜在的系统漏洞，排查网络中潜伏的未知风险和威胁。 | 巡检报告 |
| 3 | 安全风险评估 | 在网络架构的改动、新系统上线、配置变更的时候，对变动带来的风险进行识别和评估，提出风险预防和必要的整改措施。 | 风险评估报告 |
| 4 | 安全事件紧急响应 | 在出现安全事故、数据泄密、网络入侵等安全事件的时候，紧急响应，快速定位和查找问题，制定出解决方案。 | 事件分析处理报告 |
| 5 | 渗透测试服务 | 半年一次渗透测试，通过渗透测试和工具扫描等方式在客户的授权和监督下对客户的系统和网络进行非破坏性质的测试。 | 测试报告 |
| 6 | 安全设备日志分析 | 每个季度对安全设备进行一次安全日志分析，对防火墙、IDS告警、防病毒服务器、应用服务器日志的安全分析，发现和挖掘潜在的网络层面、主机层面安全威胁，形成日志分析报告，预防安全事件发生。 | 日志分析报告 |
| 7 | 信息安全审计服务 | 每半年一次对本地安全评估中位于物理层、网络层、主机层、数据层和用户层的所有安全对象目标进行最有效和最完整的安全评估，建立了详细有效的本地控制台审计CheckList，并提供最合理和最及时的安全建议。 | 解决建议 |
| 8 | 系统漏洞修复 | 每季度一次，通过安全检查、漏洞扫描等方式发现操作系统、数据库、中间件等通用软件的潜在高危安全漏洞时，配合医院维护人员进行系统漏洞修复工作，该工作需要评估修复带来的潜在风险和保障修复后系统正常稳定运行。 |  |
| 9 | 安全加固指导服务 | 一年一次，结合等保初次测评结果，指导用户对操作系统和应用系统进行修补、加固和优化。包括针对全网信息平台各种设备、多种操作系统、多项应用的打补丁、停止不必要的服务、升级或更换程序、除去后门程序、修改配置及权限以及针对复杂问题的专门解决方案等服务。 |  |
| 10 | 安全培训服务 | 根据医院需要不定期培训，针对网络安全环境、医院人员现状进行针对性的安全培训工作，培训具体内容可与医院商议后制定。 |  |

**四、商务要求**

**1．供货要求：**

（1）投标人必须承诺提供生产厂商原装、全新的、符合国家及用户提出的有关质量标准的产品，并按招标文件要求附带相关的合法生产厂商证明文件。

（2）投标人必须承诺所提供产品符合国家或行业标准，以及用户提出的有关应用需求，且不存在第三方侵权行为。

（3）投标人应具备本项目的服务能力，投入具备相应资质、经验的技术服务团队和服务工程师；

（4）投标人应为本项目提供专业的系统检测技术工具，并对功能要求一一响应；

（5）投标人应具备信息化建设项目同类经验，需提供不少于3个2017年至今信息化建设项目案例业绩证明文件。

**2．工期要求：**

合同签订之日起60个工作日内完成硬件设备的供货、布线、安装与调试、软件系统功能升级并完成对使用单位相关人员的操作与使用培训，并开展相应的信息安全服务，服务期限为壹年。

**3．交货地点：**采购人指定地点。

**4．验收要求：**

（1）项目设备与系统安装调试完工后试用30个工作日，采购人应组织验收工作。

（2）所有设备、器材在开箱时必须完好，无破损，配置与装箱单相符，数量、质量及性能不低于招标要求。

（3）拆箱后，中标供应商应对其全部产品、零件、配件、用户许可证书、资料、介质造册登记，登记册作为验收文档之一；

（4）中标供应商应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档汇集成册交付设备使用单位。

（5）信息安全服务到期后，需将风险评估报告、日志分析报告、巡检报告等文档形成信息安全服务报告。

**5．响应时间：**提供7×24小时电话技术支持，软硬件设备故障报修的响应时间：1小时，若电话中无法解决，4小时内到达现场进行维护。除特殊情况外，故障排除时间不超过24小时。

**6．售后服务要求：**

（1）质保期：硬件设备免费质保期为验收之日起3年。

（2）质保期自双方代表在软件及设备安装调试后的验收证明文件上签字之日起计算，保修费用已计入总价，并以书面形式承诺。成交人提供免费部件、人力。

（3）质保期内，由供应商免费提供备品备件及服务，保修期后，供应商只收取配件费。无论何时，因货物质量缺陷造成采购方损失，供应商应予以赔偿。

（4）质保期内，所有设备保修、保养、维修服务均为上门服务，由此产生的费用均不再收取。

（5）要求投标人具有快速到达现场维护、应急抢修的能力，以及在医院设立售后服务机构点，应对现场维护、应急抢修措施等情况。

**7．培训要求：**

（1）制定详细的培训方案，提供技术培训、操作培训和现场指导，完成对系统集成、开发技术及工具等在内的全部免费培训。培训方案要详细描述每次培训的具体内容、深度和时间安排。

（2）培训方式应包括技术讲课、操作示范、参观学习和其它必须的业务指导和技术咨询，确保培训人员对系统基本原理、技术特性、操作规范、运行规程、管理维护等方面获得全面了解和掌握。

**8．报价要求：**

（1）投标人报价中必须包括项目全部内容的费用（包括安装配件、安装组件、吊装、配送、安装调试、培训、相关法律规定的必须的检验、验收、税金等），费用不管是否在投标人报价书中单列，均视为投标总价中已包括该费用。

（2）若投标人所投报价比本项目最高限价低25%（含25%）以上的，投标人应对其报价是否低于成本价进行说明，并提供相关证明材料，若投标人未提供证明材料进行说明或提供的证明材料不能充分说明其报价不低于成本价的,或有可能影响产品质量或者不能诚信履约的，评标委员会有权否决其投标。

**9．付款方式：**

（1）合同签订后，10个工作日内，采购人向中标人支付合同价的40%；

（2）软硬件到货、签收、安装、调试完毕，试运行、经验收合格后10个工作日内，采购人向中标人支付合同价的60%；

（3）合同签订后，5个工作日内中标人向采购人支付合同总价的5%作为履约保证金， 1年安全服务期结束后凭信息安全服务维护报告无息退还。