附件 1

佛山市医保局医疗保障专网安全加固服务（2026-2028年）采购需求

一、项目概况

序号	品目名称	项目名称	采购方式	品目预算(元)	服务时限
1	安全集成实施服务	佛山市医保局医疗保障专网安全加固服务	公开招标	2,281,703.00	自合同签订之日起 2 年

服务需求清单

序号	服务需求名称（标的名称）	服务需求名称（标的名称）	数量	单位
1	安全能力服务	SSL VPN 网关能力	1	项
2		SSL VPN 网关配套核心交换能力	1	项
3	安全运营服务	全流量文件监测服务	1	项
4		全流量攻击溯源分析服务	1	项
5		高交互诱捕服务	1	项
6		7×24 小时日常实时安全监控服务	1	项
7		安全规则及功能优化服务	1	项
8		恶意攻击封堵处置服务	1	项
9		重大活动保障专项策略调优及演习协助服务	1	项
10		网络安全态势感知服务	1	项
11		汇聚链路防护服务	1	项

二、主要商务要求

标的提供的时间	自合同签订之日起 2 年。
标的提供的地点	采购人指定地点。
付款方式	1 期：支付比例 40%,在合同签订后，采购人 10 个工作日内支付合同总额的 40%； 2 期：支付比例 30%,运营服务累计满 12 个月后，采购人 10 个工作日内支付合同总额的 30%（如有违约金，违约金在支付款中扣除）； 3 期：支付比例 30%,项目验收后，采购人 10 个工作日内支付合同总额的 30%（如有违约金，违约金在支付款中扣除）。 如项目发生合同融资，采购人需将合同款项支付到合同约定收款账户
验收要求	1 期：验收要求：1.验收主体 验收由采购人组织实施，中标人全程配合；必要时邀请技术专家或第三方机构参与，采购人相关部门全程监督。 2.验收时间 采购人自中标人完成合同履行义务之日起 10 个工作日内组织验收。 3.验收方式 中标人必须按照采购人和相关单位等要求做好验收工作并准备好验收文档

	（包括但不限于安全分析报告、文件分析报告、攻击者诱捕分析报告、应急服务支撑报告、安全事件通报）。 4.验收程序 中标人提交验收申请及全套资料，采购人完成资料初审后组建验收组，开展现场核查与功能测试。 5.验收内容 1）设备硬件按参数部署到位，运行正常。 2）安全能力、安全运营全部服务按要求落地。 3）与省医保安全平台、内部系统对接联动正常。 4）服务台账、日志、报告、证明材料齐全规范。 5）满足考核要求，无安全责任违约事件。 6.验收标准 1）符合政府采购相关法律法规及合同约定。 2）技术参数完全响应采购要求，证明材料真实有效。 3）中标人需无条件配合进行各项验收工作，验收若涉及费用均由中标人负责。
履约保证金	不收取
其他	设备保障:如服务过程中采购人发现中标人所提供的设备无法满足或无法达到服务需要，可要求中标人提供高配置或更换型号，以达到服务要求。中标人须及时响应，并承担相应费用。 付款方式增加：1.合同款项的支付方式：转账结算（银行转账）。 2.付款方：采购人；收款方：中标人。 3.开具发票：中标人收款时必须持有效发票。收款方、出具发票方、合同乙方均必须与中标人名称一致。 4.付款期间如因特殊情况需调整，由双方协商处理。

三、其他商务需求

内容明细	内容说明
报价要求	1.本项目报价为广东省佛山市目的地交付价。 2.投标报价指投标人为完成本项目所收取的全部费用，包含但不限于以下费用：成本费、劳务费、交通费、税金（全额含税发票）、雇员费用以及项目实施过程中其它应预见和不可预见费用等完成本采购项目、达到采购人目的的一切费用及企业利润。3.投标人须考虑本项目在实施期间的一切可能产生的费用。 4.报价不得高于本项目的采购项目预算金额，否则视为无效报价，作无效投标处理。
人员管理	1.本项目需提供至少 3 名技术人员进行远程分析服务，包括全流量攻击威胁分析服务和威胁情报分析服务，同时配备后备服务力量，及时进行远程支持，解决用户的专网安全监控问题，全面保障信息化系统的健康运行。服务团队应具有专业的技术能力，良好的服务态度、爱岗敬业、责任心强、善于与人沟通协调，合作能力强，按照项目技术服务内容和网络安全日常管理开展服务工作。 2.中标人在响应文件中承诺提供的项目组人员必须按要求投入到本项目中，在合同期内不得擅自更换。中标人如因工作安排或其他原因，需要更换项目组人员时，应事前向采购人提出书面申请，未经采购人同意，不得更换人员。 3.采购人有权以书面形式要求中标人更换不能按规定履行合同的人员。即使是采购人要求或同意更换的人员，其代替人员的资质仍应得到采购人的认可，且其资历和经验均不低于被更换人员。由此而产生的费用由中标人承担。 4.如中标人未经采购人书面同意擅自更换项目组人员，采

	购人有权扣除中标人一定的违约金。发生本条上述情况累计达 4 次后，采购人有权终止合同，由此引致的经济损失，中标人须全额赔偿，采购人保留追究中标人相关责任的权利。 5.中标人对其雇员的人身安全负全部责任。
保密要求	1.由采购人收集的、开发的、整理的、复制的、研究的和准备的与本合同项下工作有关的所有资料在提供给中标人时，均被视为保密的，不得泄露给除采购人或其指定的代表之外的任何人、企业或公司，不管本合同因何种原因终止，本条款一直约束中标人。 2.中标人在履行合同过程中所获得或接触到的任何内部数据资料，未经采购人同意，不得向第三方透露。 3.中标人实施项目的一切程序都应符合国家安全、保密的有关规定和标准。 4.中标人参加项目的有关人员均需同采购人签订保密协议。 5.由于中标人责任造成的任何损失，中标人及其相关人员均应承担相应的赔偿责任及法律责任。
服务响应	提供 2 年 7×24 小时的远程应急技术支撑服务。
项目相关服务承诺	本项目涉及内容为佛山市医疗保障局重要的信息化资产，是采购人信息化运作的重中之重，为确保本项目合同到期后，采购人安全服务和设备维保升级项目的采购工作以及下一阶段工作顺利展开，供应商需在响应文件中承诺以下内容（包括但不限于）： 1.投标人如获中标，需在服务期内配合采购人开展下一阶段的安全服务和设备维保升级项目的招投标工作。 2.投标人如获中标，需在项目期满后做好各项交底工作，以便下一阶段安全服务和设备维保升级项目的中标服务商顺利开展维护工作。 3.投标人如获中标，需在项目期满后配合下一阶段的安全服务和设备维保升级项目的中标人现场核对、熟悉维护工作内容，现场服务时间不小于 2 天。 4.投标人如获中标，需在项目期满后参加下一阶段的安全服务和设备维保升级项目的启动会议，积极针对新中标人提出的疑问进行解答。 5.投标人需在投标文件中提供加盖投标人公章的《项目相关服务承诺书》，内容包含但不限于以上 4 点内容。

四、技术要求

序号	具体技术(参数)要求
1	**一、安全能力服务** **1.1SSL VPN 网关能力** 1）性能参数：最大理论加密流量（Mbps）≥150，最大理论并发用户数≥600，IPSec 加密最大流量（Mbps）≥150，设备整机理论最大吞吐量≥500Mbps，设备整机理论最大并发会话数≥35w，VPN 接入授权≥300。
2	2）硬件参数：规格≥1U，内存≥2G，硬盘容量≥32GB SSD，电源：单电源，接口：千兆电口≥4。支持国密 SM1、SM2、SM3、SM4 密码算法及其协议，支持多种身份认证方式、含 SSL。
3	**1.2SSL VPN 网关配套核心交换能力** 1）基本要求： a）交换容量：≥4Tbps；包转发率：≥1600Mpps； b）配置端口：≥6 个 QSFP+口，≥2 个 QSFP28 口，≥48 个 SFP Plus 口，≥2 个带外管理以太网口； c）设备包含 24 个 SFP 千兆单模光模块，2 个 SFP+万兆多模光模块，2 个 SFP+万兆单模光模块，4 个 QSFP+40G 多模光模块； d）四个可热插拔风扇模块。
4	2）支持 IRF2 横向虚拟化，IRF3.1 纵向虚拟化。支持 STP、RSTP、MSTP、PVST 及 BPDU

	保护、根保护、环路保护。
5	3）支持基于源 MAC、目的 MAC、源 IP(IPv4/IPv6)地址、目的 IP(IPv4/IPv6)地址、端口、协议、VLAN 的流分类。
6	4）支持 MPLS、MCE，MPLS VPN、MPLS TE。
7	**二、安全运营服务** **2.1 全流量文件监测服务** 利用服务工具进行文件的威胁监测分析服务，监控佛山市医疗保障专网网络传播的新型恶意文件，要求： 1）支持 1G 流量分析。
8	2）支持虚拟化方式部署。
9	3）内置恶意文件静态检测引擎，支持对可执行文件、文档、压缩包和网页脚本进行恶意代码检测和告警。
10	4）支持样本虚拟化执行环境，具备 Windows XP、Windows 7、Windows 10 和 android 执行环境。
11	5）基于虚拟执行的动态检测技术，可以基于软件在虚拟环境的行为及通用漏洞利用特征（进程行为、逃逸行为），分类识别各种加壳病毒及未知恶意代码。
12	6）支持对 office 文档、pdf、压缩文件、flash、pe 等常见 windows 平台文件进行动态检测。
13	7）可记录文件运行期间的注册表行为、文件行为、网络行为等所有行为记录。支持文件检测内容包含恶意文件来源、恶意行为类型、恶意文件进程操作、文件操作、网络操作、注册表操作等可疑行为。
14	8）支持手动导入样本文件进行动态检测。
15	9）详细的文件运行行为以报告形式提供，以便管理人员进行分析。
16	10）支持与本项目中一并提供的全流量攻击溯源流量分析能力进行无缝对接，接收其还原的文件，进行真实模拟分析；并且支持与本项目中一并提供的网络安全态势感知能力进行无缝对接，实时把安全风险发送到其进行联动分析。（投标时提供加盖投标人公章的承诺函作为证明材料，承诺函格式自拟）
17	11）支持与广东省医保专网安全平台无缝对接，同步广东省医保安全平台安全规则信息，实时把安全风险发送到广东省医保安全平台安全进行联动分析。（投标时提供加盖投标人公章的广东省医保专网安全平台上对接成功的截图作为证明材料）
18	**2.2 全流量攻击溯源分析服务** 利用服务工具进行异常流量监测、安全审计网络安全、流量攻击溯源流量分析服务，针对基础攻击威胁进行识别，同时将通过分析解析后的流量元数据，进行溯源分析。 1）支持 1G 流量分析，支持网络入侵分析、网站入侵分析、DPI 拆包解析、全流量存储。
19	2）支持虚拟化方式部署。
20	3）支持接收医保网络镜像，并利用大数据技术进行网络攻击管理分析。
21	4）TCP、UDP、ICMP、SCTP、HTTP、FTP、SMTP、DNS、POP3、LDAP、TELNET、SSL、RDP、SNMP、SSH、VNC、Rlogin、SMB、NFS、DHCP、SIP、TFTP、NNTP、Radius、Kerberos 等常见协议的深度解析和还原。
22	5）支持 VPN 协议的识别，识别的 VPN 类型主要包括：向日葵远控、TeamViewer、PPTP、L2TP、IPSec 等。
23	6）支持对实时流量采集的 pcap 包进行全量存储，供追溯分析和取证使用。
24	7）应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测，攻击特征库数量至少为 14000 种以上。

25	8）支持流量白名单，过滤掉不关注资产流量，白名单类型应包括 IP、端口、邮箱、域名。
26	9）支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、RDP、VNC、POP3S、Telnet）的口令暴力破解检测。
27	10）支持多种抗逃逸攻击检测，检测类型包括：PDF 漏洞利用规避攻击、Adobe PDF JavaScript 文件规避攻击、Metasploit PDF 漏洞利用规避攻击。
28	11）支持针对主流 Web 服务器及插件的已知漏洞攻击检测。Web 服务器应覆盖主流服务器：apache、tomcat、lighttpd、NGINX、IIS 等；插件应覆盖：dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress 等。
29	12）内置基于 webshell 通信特点以及流量特征构建决策模型，支持对 asp 文件、php 文件、jsp 文件和图片码进行检测和告警。
30	13）内置基于统计学特征和操作码序列训练的检测模型，支持对 asp、jsp、php 文件类型进行检测和告警。
31	14）支持对网络中的流量统计，统计类型包括应用流量的构成和占比、协议的构成和占比和 VPN 的构成、接口流量统计和接口流量趋势。
32	15）支持对网络中的威胁进行统计，统计类型包括：威胁事件统计和趋势、攻击者统计和趋势、失陷资产统计和趋势、漏洞统计和趋势。
33	16）支持从攻击者角度进行分析，对攻击者进行画像，攻击者属性包括攻击时间、地理位置、攻击手段、攻击次数、详情等。
34	17）支持从受害者角度进行分析，对受害者进行画像，受害者属性包括资产 IP、资产组、资产类型和风险级别和详情。（投标时提供加盖投标人公章的截图作为证明材料）
35	18）支持从漏洞维度进行分析，识别流量中的漏洞信息，统计漏洞的影响范围。
36	19）支持对采集的全部流量进行存储、检索和下载，检索条件包括源 IP、目的 IP、源端口、目的端口和起止时间。支持将存储的数据包与告警关联并提供下载便于取证。支持将存储的恶意文件与告警关联并提供下载便于取证。
37	20）支持与广东省医保专网安全平台无缝对接，同步广东省医保安全平台安全规则信息，实时把安全风险发送到广东省医保安全平台安全进行联动分析。并且支持与本项目中一并提供的网络安全态势感知能力进行无缝对接，实时把安全风险发送到其进行联动分析。（投标时提供加盖投标人公章的广东省医保专网安全平台上对接成功的截图作为证明材料）
38	21）需提供部署硬件资源，CPU≥40 核，内存≥256G，硬盘≥64T，万兆接口≥2 个，千兆接口≥2 个。
39	**2.3 高交互诱捕服务** 利用服务工具进行高交互诱捕服务，配置高交互诱捕策略诱捕攻击者，并监控诱捕告警进行攻击者溯源和反制。 1）支持专网攻击诱捕分析。
40	2）支持虚拟化方式部署。
41	3）支持仿真高交互操作系统，包括：CentOS、Windows（win7、win2008r2、win2012R2、win10-pro、win2016、win8.1-pro）、Ubuntu、SUSE、RedHat。
42	4）支持仿真高交互数据库服务，包括：Kafka、MySQL、MongoDB、Redis、PostgreSQL、Elasticsearch、memcached、postgresql 等。
43	5）支持仿真 web 应用以及各类 web 服务框架，包括：Drupal、Wordpress、Joomla、jboss、Wiki、Webmin、Weblogic、Jenkins、GitLab、Shiro、tomcat、Dubbo、GlassFish、phpmyadmin、ECShop、Fastjson、6KZZ、Discuz、PHPMyWind、metinfo、Spring、企

	业邮件系统、互联网应用平台、Apollo、Druid、Nexus、若依、Solr 等。
44	6）支持仿真企业管理软件，包括 CRM、OA、Zbox、Confluence、jira、Zabbix、堡垒机登录页。
45	7）支持仿真真实漏洞缺陷，包括 Shellshock、Struts2、Eternalblue、反序列化、远程代码执行等。
46	8）支持仿真服务，包括： http_rpc_epmap(udp),instl_bootc(udp),ms_sql_monitor(udp),krb524(udp),sgi_esphttp,palace(udp),wdbrpc,ftp,ssh,telnet,smtp,wins_replication,dns,tftp,http,priv_term_l,kerberos,su_mit_tg,pop3,ntp,RPC,netbios_ns,netbios_dgm,netbios_ssn,imap,snmp,https,samba(445),remote_login,http_rpc_epmap,rsync,instl_bootc,socks,oracle_database_default_listener,mssql,ms_sql_monitor,oracle_database,ctx_bridge,squid_http,netport_id,icpv2,mysql,mcs_mailsvr,rdp,svn,krb524,sip,vnc,redis,irc,weblogic,d_s_n,simplify_media,radan_http,hive_metastore,wap_wsp,git,palace,hive_server,mongodb,hbase_master,hbase_master_info,hbase_regionserver,hbase_regionserver_info。
47	9）支持将诱捕 ip 的攻击转移到远端蜜罐和蜜网中，转发支持 SSL 加密；支持自定义端口转发。
48	10）支持诱捕 IP 分区，可标识区域等级（核心、重要、一般）。
49	11）支持在节点上开启 https 配置，开启后蜜罐同时支持 http 和 https 协议访问。
50	12）支持如下反制场景：IE 反制、VPN 反制、RDP 远控反制、mysql 反制、office 反制、rar 反制、vs 反制、web 应用控件反制。
51	13）支持诱饵类型包括 Linux:hosts、SSH 公钥、SSH_history；windows：RDP 服务连接、HOSTS 映射、XSHELL 应用连接、SECURECRT 应用连接、登录信息文本、桌面文件、域凭据、word 文件、excel 文件；通用诱饵：邮件、web 文件、github 代码。
52	14）支持记录攻击者在攻击过程中产生的所有样本，包括样本 HASH、样本类型、样本大小、最近及最早捕获时间。
53	15）支持对样本进行关联分析，可关联到攻击源、攻击目标以及导入的威胁情报。
54	**2.47×24 小时日常实时安全监控服务** 1）提供 7×24 小时常规化安全监控服务，监控业务可用性和安全告警事件，主动发现佛山市医保保障核心业务骨干网络上攻击威胁，识别骨干网运行系统中潜在的安全威胁。 2）通过中标人提供的安全能力进行威胁检测、可疑事件监测等多种方法对威胁进行安全风险检测，并在此基础上进行威胁分析（包括安全威胁分析、安全隐患分析、重要信息系统安全状况分析等），通过威胁源攻击能力、威胁源攻击动机、威胁发生频率及影响程度等因素，确定威胁值，形成威胁分析报告，并协助佛山市医保安全运维人员进行整改，具体工作： （1）结合采购人的业务及防护设备情况进行风险分析、不限于热点事件预防，防护设备自定义规则防护编写、风险分析模型输入等，要求在热点事件发布后 24 小时之内完成防护策略的建议。 （2）关联常态化的攻击威胁进行关联分析，针对持续的高级风险进行分析运营，在攻击者找到攻陷方法或路径之前，针对访问源进行拦截，破坏自动化攻击行为，达到比设备自动拦截和防护威胁行为更好的效果，针对高危访问源的封杀可以有效提升攻击者的时间成本、技术成本迫使对方放弃攻击。 （3）匹配高危访问源，尤其在历史重保活动中有“案底”的高危访问源，即在攻击发

	生之前曾经对其他主机或系统采取攻击行为的高危访问源。 （4）识别扫描探测类的高危访问源，通过威胁分析平台对访问流量和日志分析，可精确识别各类有扫描行为和探测行为的访问源。 （5）识别具有攻陷意图的高危访问源，精确识别攻击者攻击的步骤和环节，从而识别具有攻陷意图的高危访问源。 （6）日常实时监控承载业务的可用性和告警事件，主动发现佛山市医保保障核心业务骨干网络上攻击威胁。
55	**2.5 安全规则及功能优化服务** 1）提供安全规则/功能优化服务，通过审核调整业务安全防护模型，减少业务流量误阻断的风险并根据新的攻击威胁实时更新安全防护规则和系统功能，提升攻击防护能力。 2）借助骨干网的安全能力，从网络会话、业务应用等层级基于特征规则匹配进行统一分析，实时进行威胁检测数据采集分析，实现已知威胁检测。同时，鉴于威胁分析的结果，远程安全运营人员定期针对安全能力的策略配置巡检及优化，配置适用于骨干网安全运行的防护策略，全面提升边界、网络、应用安全防护强度，进一步保障业务安全稳定运行。
56	**2.6 恶意攻击封堵处置服务** 1）提供一键封堵服务，结合现网安全能力、网络设备的能力梳理应急处置规则，接到告警后 5 分钟内完成封堵，并输出封堵处置报告。 2）结合现网安全设备、网络设备的能力，针对网页篡改应急、入侵事件应急、恶意程序应急提供分钟级的重大活动保障预演。 3）发现网页篡改攻击时，快速阻断用户通过访问医保平台的能力，阻断方式不限于防火墙、路由器、安全设备封堵等。 4）发现入侵攻击告警时，快速对攻击源 IP 进行封堵，封堵方式不限于防火墙、安全设备策略等。 5）发现恶意程序告警时，实现恶意程序地址封堵、内容过滤等。
57	**2.7 重大活动保障专项策略调优及演习协助服务** 1）重保专项策略调整，在重大活动【包括但不限于全国两会、五四运动、建党节、博鳌亚洲论坛、年度网络安全周、国庆节、澳门回归、公安部攻击预演行动、公安厅攻击预演行动、临时安排的保障等】前期进行保障预演习，并针对期间出现的高级风险进行分析，调整安全能力的策略调整优化。 2）在重大活动前进行攻击保障预演，包括但不限于业务破坏类（主要以影响业务的正常开展为攻击目标）预演及业务入侵类（主要以非法渗透到服务器为主要目标，并展开黑客攻击）的预演。 3）在重大活动保障前，模拟检测机构及攻击者通过重大活动保障预演服务，完善应急保障体系，以实战的形式检验重大活动保障流程和保障方法的可用性、有效性。 4）提供一种接近真实环境的安全攻防预演，进行真实的安全攻防来达到真实预演的效果。并指定运维人员会根据应急预案的要求进行应急工作的开展，以实现应急预演人员的在其中对应急过程、防御过程的实践操作。同时对应急预案进行实践预演，确定应急预案的可行性及有效性。 5）在预演中，为了保障效果，需在真实环境中进行。为了避免应急预演中存在的网络攻击影响正常业务，同时考虑到应急预演效果，需在应急预演之前制定出切实可行的方案。并且需根据真实环境现状，确定方案的可行性。
58	**2.8 网络安全态势感知服务**

	利用服务工具进行专网的网络安全态势感知服务，监控佛山市医疗保障专网网络整体网络安全态势情况，要求： 1）支持网络安全态势感知分析。
59	2）支持界面化配置规范化规则，采集第三方日志实现异构日志格式归一化。解析规则支持正则表达式等前置过滤方式及 JSON、Key-value、csv、正则表达式、扁平化 JSON 类型的解析规则，支持界面划取字段配置、多级解析提取嵌套字段、配置规范化规则对解析提取的字段进行字段类型、名称、取值规范化。
60	3）支持以地图、指数、雷达图、柱状图、趋势图等形式展示监测网络安全的整体安全态势，可投放大屏，兼容分辨率要求，易于操作，可动态提醒当前网络最新的安全威胁态势。
61	4）综合态势支持从网络风险状况及健康状态维度对网络的综合风险态势进行量化评估感知及可视化呈现，包括但不限于网络风险综合评分及评分指数、网络健康状态评分，以及日志、漏洞、资产、设备接入数、攻击链威胁分布、专项整治分类统计、资产脆弱性统计和影响资产漏洞 TOP、最近重点事件等。支持手动配置威胁指数、脆弱性指数、网络健康评分。
62	5）支持可视化大屏的自定义编排，包括但不限于：扩展响应态势自定义编排、威胁态势统计项自定义以及新增基于内置接口统计项的自定义大屏。
63	6）支持安全治理能力，能够结合环境数据自动化评估安全治理等级和评分，安全治理等级应包括优、良、待改进三级，总评分应充分结合建设情况指标、运行能力指标、安全态势指标、合规指标等加权计算得到。（投标时提供加盖投标人公章的截图作为证明材料）
64	7）支持最近 1 小时、24 小时、8 天的全局运维事件统计与监控并可按需自定义仪表盘，监控内容包括但不限于各类统计数据如事件、失陷资产、日志、攻击源、情报等，支持重点事件、风险处置监控、攻击源、事件类型、外发事件类型 TOP 等统计监控，支持资产威胁类型、资产发现、高危资产、资产脆弱性 TOP 等统计监控。
65	8）支持对关注的 IP 从攻击者或受害者资产两种维度进行跟踪监控，监控该目标最近的攻击行为，如发生的攻击事件、日志，并支持基于相关数据进行目标分析。
66	9）支持简易模式的自定义规则，可支持用户在选择日志类型、设置常见日志类型字段过滤条件之后，即可新建或编辑规则，从而生成事件。支持配置过滤型模板，可基于响应码，源/目的 IP，源/目的资产（是否命中目的资产），源/目的区域（国家，省份，城市），日志内容（log_message），域名，URL，发生次数等字段进行规则定义。
67	10）支持专家模式的自定义规则，可按需自定义生成的规则描述、规则模板，如普通模板、时序模板等；可按需引用事件模板；可按需选择日志源，并基于可视化方式编辑过滤条件、关联条件；可按需绑定 ATT&CK 战术等。（投标时提供加盖投标人公章的截图作为证明材料）
68	11）支持失陷资产检测，可对失陷资产进行判定并提供失陷资产的判定依据，包括但不限于失陷资产概要信息、攻击结果、攻击链分布阶段、失陷资产的攻击过程及过程判定依据，如攻击特征、流量上下文、关联的告警日志及流量日志，以及 pcap 包下载；并可快速扩展该失陷资产的全部攻击事件，以及该失陷资产攻击者发起的攻击、该失陷资产的同类型威胁事件。
69	12）支持提供威胁事件统一运维入口，并支持运维人员自定义威胁运维页签，实现关注 IP、资产、攻击类型、攻击结果、来源设备、置信度等多维度自定义的运维事件。
70	13）支持对各类运维事件常见属性，如资产名称、IP、端口、载荷关键字、攻击链、攻击结果、来源设备、规则 ID、情报 IoC、来源设备、关联漏洞等的按需检索；支持

	提供多种运营场景的检索条件，支持运营场景条件的自定义、导入导出和过滤查询；支持运维事件自定义检索条件，可按需扩展检索条件。
71	14）支持直观展示待运维事件的核心信息，并自定义按需扩展待运维事件的展示内容，如运维事件类型、攻击结果、载荷、等级、攻击方向、攻击次数、运维对象、规则 ID、原目的 IP、端口等。
72	15）支持可视化展示运维事件详情，包括但不限于：事件关键属性，如攻击结果、响应码、事件描述处置建议、攻击类型、原目的 IP 端口等；攻击长镜头、攻击关联漏洞、关联资产、攻击时序过程及攻击载荷、流量上下文、告警日志、关联的会话日志、流量日志、情报命中信息以及可快捷扩展调查同类型或者同 IP 或同资产的相关运维事件；事件关联资产详情列表；攻击者使用的 ATT&CK 中定义的战术及技术；处置历史及处置建议等。支持攻击证据，如攻击载荷、流量取证 PCAP 包导出，并支持运维事件详情报告的导出下载。
73	16）提供攻击者画像威胁分析功能，支持以列表形式展示攻击者 IP、最近攻击时间、攻击持续时间、攻击组织、攻击者来源、攻击手段、ATT&CK 攻击技术、画像指纹信息、攻击资产信息、风险等级等信息，支持通过时间范围、IP、地域、情报信息、画像关键字符串、风险等级、ATT&CK 攻击技术对攻击者进行检索过滤；支持在攻击者列表中对攻击者进行一键响应的快捷操作。
74	17）支持解码助手功能，提供 Base64、URL、Unicode、ASCII、UTF-9 解码转换功能，提供 AES 解密功能。
75	18）对存储的流量日志进行回溯查询，包括 TCP/UDP 会话日志、DNS 解析日志、Web 访问日志、邮件日志、文件传输日志、SSL/TLS 协商日志、数据库操作日志、社会账号日志、登录日志、认证日志、ICMP 日志，回溯时间可以自定义。
76	19）提供流量取证功能，支持接入还原的流量包数据，并在关联的流量日志查询页面提供下载，可以查看历史的流量取证列表。
77	20）支持统一白名单配置，基于源目的 IP、源目的端口、规则 ID、URL/域名、x-forwarded-for、全局 IP 等维度的白名单的按需定义。支持配置白名单的生效时间范围、支持配置白名单生效功能范围，至少包括事件研判、异常资产分析和一键响应。
78	**2.9 汇聚链路防护服务** 1）吞吐量可达 1.3G，能高效应对大规模数据传输需求；同时支持 100 万并发连接数，确保多用户同时在线时的稳定运行，每秒新建连接数可达 2 万，可快速响应大量设备的接入请求。在 VPN 服务方面，该网关支持 SSL VPN、IPSec VPN、GRE VPN 和 L2TP VPN 四种 VPN 类型，每种类型均支持 750 个并发连接，且自带 40 个 SSL VPN 用户授权，能满足中小型企业的远程办公需求。此外，网关还支持 3000 条域间策略/安全策略、1000 个 VRF 和 1024 个安全域，带机量（DPI）可达 1000 台，可灵活构建复杂的网络安全架构并支持大规模设备接入。
79	2）安全网关在硬件配置上采用 1U 高度设计，便于在标准机柜中安装部署。接口方面，配备 8 个 GE 电口和 2 个千兆 combo 口，可满足多种网络接入需求，暂不支持 10GE 接口，扩展槽配置未明确标注。安全防护接口方面，设有 2 个 bypass 口，在设备故障时可自动切换网络链路，保障网络不中断。存储配置上，支持 1 个硬盘插槽，标配 480G 硬盘，可满足日志存储和系统运行需求。电源配置采用单电源设计，能为设备稳定供电。整体硬件设计兼顾了实用性和稳定性。
80	3）具备安全态势感知的能力，在同一个平台下既能提供安全防护状态的态感大屏，也能提供对网络流量审计分析的态势大屏，支持通过动态大屏实时展示攻击态势，查看境内、境外攻击趋势、应用流量占比、访问域名 TOP，包括失陷资产趋势、威胁类型分

<table>
<tr><td></td><td>布及最新攻击事件等内容，支持自定义大屏名称的个性化设置。</td></tr>
<tr><td>81</td><td>4）具备 AI 智能运营的能力，提供 AI 大模型智能辅助运营的能力，覆盖场景不应少于 4 个，不限于安全通用知识咨询风险洞察、资产处置等安全运营场景，提供 NLP 交互界面，自然语言查询响应时间≤3 秒，风险预测准确率≥90%，误报率≤5%，满足 web 端及移动端均能使用。</td></tr>
<tr><td>82</td><td>5）具备互联网暴漏面监测与发现，提供基于公网地址实现互联网资产探测的能力，支持对互联网资产测绘（IP、服务、域名）与高危暴露风险的识别，可结合互联网访问情况检测恶意外联风险，提供全方位互联网资产风险监测服务，并提供监测服务报告。</td></tr>
<tr><td>83</td><td>6）具备威胁处置联动能力，提供多层级防护能力的联动响应，支持对风险主机一键下发病毒查杀和网络隔离等操作，封堵攻击路径，实现网络攻击的闭环处置。</td></tr>
<tr><td>84</td><td>7）具备内网资产漏扫能力，提供对内网资产的全面漏洞探测扫描能力，支持基于漏洞库匹配的主动探测技术，可精准识别内网资产中存在的高危漏洞、高危端口开放情况及弱口令，同时支持对扫描结果进行风险等级评估，自动生成漏洞扫描报告。</td></tr>
<tr><td>85</td><td>8）具备 DDoS 流量监测能力，提供运营商大网 DDoS 流量监测能力，展示出入流量速率统计、出入数据包速率统计、协议流量趋势分析、端口流量趋势分析等多维度信息展示，并提供告警通知。</td></tr>
<tr><td>86</td><td>9）具备移动端运营能力，提供 Web 端和移动端多种运营访问方式，支持通过移动端小程序查看安全防护概况、安全报告、告警消息等内容，可实时查看安全防护状态。</td></tr>
<tr><td>87</td><td>三、服务可用性扩展需求
1.安全链路服务：提供一条 100M 数据传输专用线路，互联佛山市医疗保障专网汇聚节点与佛山市政务外网。【投标时提供：①服务承诺函（承诺函格式自拟）②《基础电信业务经营许可证》资质证书扫描件或与具备前述资质的单位签订的网络服务租赁意向书扫描件作为证明材料】</td></tr>
<tr><td>88</td><td>2.可扩展抗 DDoS 能力：为保障链路服务可用性，需按需抵御 DDoS 攻击。
（1）整网 DDoS 防护能力不少于 25Tbps，全球清洗节点数不少于 80 个。（投标时提供第三方检测机构出具的检测报告扫描件作为证明材料）</td></tr>
<tr><td>89</td><td>（2)为线路安全所提供的 DDoS 攻击 SAAS 防护产品,符合 EAL3 增强级(增强:AVA VAN.3)的检测要求。（投标时提供第三方检测机构出具的检测报告扫描件作为证明材料）</td></tr>
<tr><td>90</td><td>（3）产品通过 AI 云上抗 DDoS 安全能力评估，支持实时流量分析与异常检测、自适应学习与智能响应。（投标时提供第三方检测机构出具的检测报告扫描件作为证明材料）</td></tr>
<tr><td>91</td><td>（4）产品基于端侧、城域网、骨干网多级联动流量牵引。（投标时提供第三方检测机构出具的检测报告扫描件作为证明材料）</td></tr>
<tr><td>92</td><td>（5）产品需依据相关标准评估，具备：1）安全审计；2）用户数据保护；3）标识和鉴别；4）安全管理；5）TSF 保护；6）具备可信路径保护功能。（投标时提供第三方检测机构出具的检测报告扫描件作为证明材料）</td></tr>
<tr><td>93</td><td>四、服务考核要求
本项目根据项目执行结合考核情况支付合同款项，按要求时限和质量完成相关工作，若考核分数低于 60 分，采购人有权解除合约，并要求中标人赔偿相应的损失。此外，若由于中标人未提前发现并通报佛山市医疗保障专网安全事件，每出现一次按本项目合同金额的千分之五向采购人支付违约金。
具体考核要求以采购人颁布的最新要求为准，中标人应无条件接受并遵照执行。
<table>
<tr><td colspan="6">考核表</td></tr>
<tr><td>考核项</td><td>考核</td><td>分</td><td>评分标准</td><td>扣分</td><td>单项</td></tr>
</table>
</td></tr>
</table>

		细项	值			得分
	项目服务内容	网络安全能力建设	3	安全设备服务可用性不低于 99.95%，已申报的变更时间之外，安全平台可用性低于 99.95%一次扣 1 分。		
			3	安全业务开通：收到工单后 2 个工作日内完成数据配置。2 个工作日未完成扣 1 分，5 个工作日未完成扣 2 分。		
			8	应用中断恢复时间：由安全平台故障导致的业务应用的单次非计划内服务中断时间，一级业务恢复时间≤120 分钟/每次。一级业务未在要求时间内恢复，一次扣 8 分。		
			5	应用中断恢复时间：由安全平台故障导致的业务应用的单次非计划内服务中断时间，二级业务恢复时间≤240 分钟/每次。二级业务未在要求时间内恢复，一次扣 5 分。		
			3	应用中断恢复时间：由安全平台故障导致的业务应用的单次非计划内服务中断时间，三级业务恢复时间≤24 小时/每次。三级业务未在要求时间内恢复，一次扣 3 分。		
			8	指对系统业务运行有重大影响的故障，如导致系统整体或核心业务中断。未按照故障处理原则（为第一时间响应、先抢通、再抢修）进行响应，一次扣 8 分。		
			5	指对系统业务运行有重大影响，但不属于 A 类的故障，如严重影响系统功能、某一核心功能模块无法使用等。未按照故障处理原则（为第一时间响应、先抢通、再抢修）进行响应，一次扣 5 分。		
			3	指对系统业务运行有一定影响，但不属于 A、B 类的故障，如系统功能、流程不正常、系统运行质量劣化等。未按照故障处理原则（为第一时间响应、先抢通、再抢修）进行响应，一次扣 3 分。		
		安全运营服务	9	被省级通报佛山市医疗保障专网安全问题，每次扣 9 分，上不封顶。		
			2	委派不少于 2 人的运维人员提供远程运维服务。不足 2 人扣 1 分，无远程运维服务扣 2 分。		
			3	对设备远程操作可做到：安全业务开通和调测、安全平台故障处理、软件升级和平台优化等工作。无法通过远程操作完成工作时不积极寻找解决方法扣 1 分。		
			3	配合安全业务开通及调整，无视安全业务开通及调整需求一次扣 1 分。		
			3	配合运维系统故障工单受理，无视运维系统故		

				障工单一次扣 2 分。		
			4	不回应咨询扣 1 分，投诉咨询回复不理想，一次扣 2 分。		
			3	安全平台日常维护操作（资源查询、日志收集、查询分析），维护操作结果不理想扣 1 分。		
			4	安全平台主机性能监控（物理、虚拟资源监控，出现告警情况联系租户进行沟通），缺少实时监控或出现告警不主动联系扣 1 分。		
			4	安全平台服务监控（监控安全平台的运行状态、服务响应时延、吞吐量、成功率的趋势等指标），缺少监控手段扣 1 分。		
			4	提供 7×24 小时客户服务渠道，客户投诉服务渠道不通畅一次扣 1 分。		
			3	日常巡检报告、故障处理报告、故障分析工作延迟、信息收集与分析不完全等，每次扣 1 分。		
			4	巡检结束后准时提交巡检报告，应急响应结束后提供故障处理报告。否则，每次扣 1 分。		
			2	根据巡检发现的安全平台运维问题及部署问题，提出优化解决建议，并进行方案实施后的效果评估。否则，每次扣 1 分。		
			4	服务人员办事认真、严谨，不能弄虚作假；服务人员积极配合沟通，及时完成相关工作任务。服务人员无被评定为合理的投诉，每被投诉一次扣 1 分。		
			4	严格遵守国家相关法律法规，严格按照甲方网络安全规范进行相关的维护工作，不得擅自改变安全设备服务进程、账号、密码，每违反一次扣 1 分。		
			3	严格遵守通信行业的相关规程和规范，每违反一次扣 1 分。		
			3	严格按照甲方的操作维护技术规范进行相关的维护工作，每违反一次扣 1 分。		
		加分项	3	在服务期间提前发现本项目平台安全的业务机制或业务逻辑安全隐患漏洞，经过确认的，每次加 3 分。		
			2	对安全平台服务工作提出合理可实施的建议，经过确认的，每次加 2 分。		
			2	专题分析报告效果突出，质量优异，具有创新性成果，经过确认的，每次加 2 分。		
	总分			100		