第三章　　采购需求

B包：安全咨询及保障服务

一、安全咨询及保障服务内容

序号	运维对象	备注
1	安全态势预警与通报服务	合并边界实时监测服务、安全事件实时监测服务。系统渗透测试服务及安全态势预警与通报服务要求1名高级安全服务人员。2024年度服务期共计为4个月，本服务按照4人月计算。
2	安全大数据综合服务	安全大数据综合服务要求1名高级安全服务人员。2024年度服务期共计为4个月，本服务按照4人月计算。
3	安全驻场保障服务	安全驻场保障服务要求2名高级安全服务人员进行估算，按8人月计算。2024年度服务期共计为4个月，本服务按照4人月*2计算。
4	安全设备运营服务	安全设备运营要求1名高级安全服务人员。
5	应急演练与攻防演练服务	服务期内开展演练工作，要求1名高级安全服务人员，按4人月计算。2024年度服务期共计为4个月，本服务按照4人月计算。
6	重保服务	重保服务要求1名高级安全服务人员，按4人月计算。2024年度服务期共计为4个月，本服务按照4人月计算。

（一）安全咨询及保障服务方案

海南省医疗保障局于2023年6月采购了安全咨询与保障服务，服务期限为一年。该项服务的主要内容包括对海南省医疗保障信息平台整体网络与安全进行监测监管，以提升医保平台的整体安全性。该项目服务周期将于2024年8月截止。为确保医保局及医保平台的服务质量，本次将采购网络安全服务运维项目，具体服务方案内容如下：

根据《中华人民共和国网络安全法》第十七条中国家推进网络安全社会化服

务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务的要求，从符合性的角度分析出医疗保障信息平台二期信息系统和“村医通”应用系统的技术防护需求，立足海南省医疗保障局的职能定位，围绕“没有网络安全就没有国家安全，没有信息化就没有现代化”的态势，并结合实际情况，在已有信息化建设和网络安全设备的基础上，通过采购网络安全服务，更好地为海南省医疗保障局信息网络安全保障工作、重要信息系统安全防护工作提供全面、及时、准确的情况通报、事件分析报告，特别是在重大活动安保工作中有能力对海南省医疗保障局突发情况进行准确的研判和对重点部位、重要情况进行预警，有必要采购安全监测服务和现场安全运维服务等，提升对网络安全态势的总体掌控能力，同时为信息安全日常工作提供支撑。清单如下：

序号	服务项目	
1	安全态势预警与通报服务	1、通过汇聚互联网全流量测数据及医保系统平台流量数据、日志数据、安全防护设备数据进行网络安全威胁大数据关联分析、交叉验证及人工核验，综合研判网络安全风险隐患并及时进行预警通报。 2、安全态势预警与通报服务能够对业务系统及网络边界提供 7x24 小时持续监测服务，监测对象包括云平台、业务系统，针对网络入侵、异常流量、僵木蠕、系统漏洞、全流量监测及网站监测六个方面进行监测，监测过程发现安全事件实时发出告警，并通过系统页面、邮件或者短信方式通知相应管理员。 3、针对发现的僵尸、木马、蠕虫、DDoS 攻击、域名等安全事件结合威胁情报等数据进行关联分析，验证事件的准确性，并对确定的事件提供研判过程、详情解释、处置建议等。 4、针对平台发现的网站安全漏洞进行漏洞审核或验证，包括但不限于 SQL 注入漏洞、XSS 漏洞、参数污染、JAVA 漏洞、文件包含漏洞等漏洞验证工作，确保漏洞的准确性，对漏洞进行详情解释和处置建议。 5、针对预警通报的安全事件提供整改加固咨询。 6、为满足业务云环境部署条件，服务工具必须满足软硬一体化形态和纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环

		境；服务工具应内置包括规则模型、关联模型、统计模型、情报模型、AI 模型等不少于 5 类安全分析模型； 服务工具应满足安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容； 7、系统渗透测试服务及安全态势预警与通报服务要求 1 名高级人员驻场。
2	安全大数据综合服务	基于互联网全流量监测数据并汇聚医保系统平台流量数据、日志数据及安全防护设备数据进行网络安全威胁大数据关联分析、交叉验证等态势研判，实现从不同视角感知医疗保障信息平台网络安全态势，包括总体态势、威胁态势、攻击态势、隐患态势、事件态势五大视角。 1、网络安全总体态势分析，包括当前数据来源、监管对象统计、监测成果统计、漏洞与隐患详情、隐患、攻击、事件、通报的趋势、系统隐患数量 TOPN、隐患区域 TOPN、事件分布统计、通报处置列表等内容。 2、威胁态势分析。内容包含威胁分类及统计、威胁源分布及统计等。 3、支持隐患态势分析。内容包含隐患分类及统计、隐患区域和行业分布情况等。 4、网络攻击分析，内容包含网络攻击分类及统计、监控总览及分类、最新攻击消息、攻击趋势、受攻击行业分布、攻击类型分布、攻击区域/受攻击区域排名、攻击 IP/受攻击 IP 排名等。 5、安全事件分析，内容包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名等。 6、服务工具应具备全局资产的资产访问图谱可视化模块，支持立体、平面、球面等多种维度的网络实体关系透视。根据资产的风险等级，对资产用不同颜色进行区分，具备访问关系的资产用直线相连，访问关系具体说明，包括但不限于：访问方向、访问类型、累计流量、

		访问时间等。服务工具应支持每个用户配置个人专属的统一门户，可配置项包括门户名称、应用名称、应用图标等。服务工具应统一门户，应支持与第三方产品集成，一键跳转至产品功能界面。服务工具应支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录；该服务工具应与安全态势预警通报联动，或整合为统一管理平台。 7、要求 1 名高级人员驻场。
3	安全驻场保障服务	安全驻场保障服务：为保障常态化服务能力，除安全咨询服务内容范围外，提供现场运营、预警、处置、协调人员。应急演练期间现场咨询服务人员 2 人。
4	安全设备运营服务	1、提供具有丰富的设备调试、策略维护的工程师，根据业务需求开展常态化运行过程中所进行的一系列运营维护工作，包括安全产品运行安全监测、策略配置、产品升级设计及策略备份等工作。 2、安全产品运行监测，信息系统运行过程中，可能面临安全产品运行异常、安全事件的发生等情况，为有效应对这些情况的出现需要开展长期的安全产品运行监测工作，以及时发现并按照流程有效处理； 3、安全产品策略配置，安全防护是通过全面落实安全策略、合理配置安全产品防护规则，对来自各网络区域的网络攻击行为进行防护； 4、安全产品升级，安全设备的有效性除了合理配置安全策略，还应该定期对安全设备的软件版本、特征库进行升级，确保安全设备的安全稳定运行的同时，也确保安全设备规则的最新； 5、安全产品策略备份，为确保安全产品在出现异常故障时能够及时恢复，需要定期对安全产品策略进行备份，防止策略意外丢失等情况造成的严重后果； 6、为保障常态化服务能力，提供 1 名信息安全工程师驻场工作。
5	应急演练	根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《中华人民共和国突发事件应对法》《突发事件应急预案管理办法》、

	与攻防演练服务	国家《信息安全技术 网络安全等级保护基本要求》（GB/T 28448-2019）、《海南省信息化条例》和《关于印发海南省党政机关、事业单位和国有企业互联网网站安全专项整治行动方案的通知》等文件对“网络安全事件应急预案、应急演练、应急响应”的相关规定，结合用户信息系统的实际情况，帮助并指导采购人建立健全网络安全事件应急演练工作机制，并对信息系统相关人员进行应急预案、应急技巧及对典型的网络安全事件进行预防等方面的培训，指导和协助其进行 1 次应急演练活动，从而有序地开展，防范并及时、高效处理网络与网络安全突发事件，保障重要信息系统安全、稳定、持续运行，最大限度地减少网络安全突发事件带来的影响，预防造成重大损失和影响。 1、攻防演练宣贯：组织以内容为红蓝对抗模式、攻击方思路、防守方的培训；对抗准备及实施：工具准备及对抗实施； 2、复盘总结：讨论攻防过程中的细节，总结蓝方攻击手段和成果，红队监测和防护成果，结合实际防护情况提出优化建议，固化红蓝对抗成果； 3、报告编写：总结红蓝对抗过程成果，提供安全建议。
6	重保服务	1、协助用户单位做好特殊时期(如春节、国庆、护网等)的信息安全保障工作和值班:服务器、网络、安全等新设备接入网络时进行安全性、可用性检查。特殊情况下,增派资深安全专家并协调相关外部资源。协助用户单位全面构建重保时期的网络安全积极防制体系、从重保单位信息系统的需求、设计、开发、上线和运行等各个阶段，加强信息系统生命周期安全管理、协助被保障单位建立全面的主动安全运备机制、提升被保障单位数据驱动的威胁对抗能力。 2、重大时刻前，要与用户单位的重点保护目标进行确认，确定出需要重点保护的业务系统目标，然后利用风险评估工具对目标系统开展风险评估工作。尽可能最大程度发现目标系统存在的安全漏洞，并配合用户单位及时对漏科进行修复和加固。 3、重大时刻期间，须要派出经验丰富的安全专家对用户单位目标系

		统进行安全值守，对系统的安全状况进行实时监测。当发现异常时，应采取有效有段或工具进行防护，并出具应急响应报告。 4、重大时刻后，安排专家对网络安全保障工作进行总结和汇报。

人员要求：共 7 人。其中安全态势预警与通报服务要求 1 名高级安全服务人员，安全大数据综合服务要求 1 名高级安全服务人员，安全驻场保障服务要求 2 名高级安全服务人员，安全设备运营服务要求 1 名高级安全服务人员，应急演练与攻防演练服务要求 1 名高级安全服务人员，重保服务要求 1 名高级安全服务人员。

该 7 名安全运维人员供医保局综合调配使用，7 名人员的岗位职责安排、值守排班安排、人员上岗面试、人员绩效考核等，均由医保局统筹安排。

该 7 名安全运维人员除负责信息安全服务外，还负责医保局运维中心值守及至片区医院、村卫生室及药店现场处置协调。

该 7 名安全运维人员互为备份，以确保在人力资源有限的情况下，医保信息系统安全的、不间断地运行。

1.1 安全态势预警与通报服务

根据医保局信息系统项目与大数据管理局约定，省网络安全态势感知平台负责对部署在政务云的数据中心 A、B 提供安全态势感知服务，医保局负责对数据中心 A、B 边界监测，及接入近 3000 家医疗单位及医保定点药店对医保二期平台的威胁感知监测、事件预警及通报工作。

根据《海南省电子政务云计算中心管理办法》，省大数据管理局负责对云中心开展实时安全监测，医保局负责对云数据中心 A、B 边界及下属近 3000 家医疗单位及医保定点药店开展安全态势感知工作。

1.1.1 安全态势预警与通报服务

1.1.1.1 服务要求

安全态势预警与通报服务能够对业务系统及网络边界提供 7x24 小时持续监测服务，监测对象包括云平台、业务系统、各医保网络接入单位，针对网络入侵、异常流量、僵木蠕、系统漏洞、全流量监测及网站监测六个方面进行监测，监测过程发现安全事件实时发出告警，并通过系统页面、邮件或者短信方式通知相应

管理员。

1.1.1.2 服务内容

总共提供七个方面服务内容：

（1）网络入侵态势感知服务。针对网络入侵检测设备发现检测到的入侵事件告警，基于攻击链模型，进行事件汇总、分析；支持网络入侵事件监控、同比分析，支持被入侵主机、入侵源的分析。

（2）异常流量态势感知服务。针对异常流量监测系统发现的 DDoS 攻击，进行汇总、分析。支持但不限于流量、攻击类型等方式进行异常流量监控、统计、分析；支持针对不同业务、不同地区、不同类型进行流量统计分析。

（3）系统漏洞态势感知服务。对系统漏洞扫描产生的系统漏洞日志进行汇总、分析。 支持对系统新增、已修复漏洞进行统计分析、支持系统漏洞总数、漏洞类型、漏洞 TOPN 的监控分析。

（4）网站安全态势感知服务。对网站安全监测系统、网站脆弱性监测系统、网站安全管理系统产生的监测日志进行汇总、分析。

（5）僵木蠕态势感知服务。对网络入侵检测系统产生的僵尸、木马、蠕虫及恶意文件告警进行汇总、分析。支持对上述事件的下钻分析，实现影响主机 IP 分析、影响主机数分析、攻击次数分析；支持对上述事件类型的 TOP N 分析。

（6）提供全流量威胁分析服务。针对 UTS 探针上报的告警信息和流量元数据信息，利用规则检测和机器学习引擎能力，及时发现网络安全事件线索，及时检测病毒木马、网络攻击等安全事件情况。实现流量数据的采集和解析工作，可以对流量数据进行逐层解码，将解析后的流量元数据上传至大数据平台，将原始流量 pcap 数据留存在本地硬盘；提供 HTTP 协议、DNS 协议、邮件协议、FTP 协议、TELNET、数据库操作、SSL/TLS 协商记录、登录记录、认证记录、ICMP 协议、TCP 会话、UDP 会话等元数据提取。

（7）态势感知情报分析服务。支持针对资产、地域、IP 进行攻击过程分析，将攻击过程进行可视化呈现，并且支持下钻分析，对各个攻击过程上的安全事件进行详细呈现。能大屏展示出最新攻击源（IP）的分布情况，可通过点击具体 IP 快速获取该 IP 的地理位置、攻击类型、恶意历史记录等信息。输入漏洞的编号或关键字，可进行精确或模糊搜索，能查询出该漏洞的名称、编号、热度、影

响范围、解决方案等信息，并能基于厂商、产品类型、风险等级、热度、是否有POC等角度对搜索结果做筛选。

1.1.1.3 服务工具要求

（1）为满足业务云环境部署条件，服务工具必须满足软硬一体化形态和纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环境；

（2）服务工具应内置包括规则模型、关联模型、统计模型、情报模型、AI模型等不少于5类安全分析模型；

（3）服务工具应满足安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容；

（4）服务工具应支持对安全日志里200个以上字段进行任意形式的逻辑与或非形式组合建模，运算方式包括但不限于等于、不等于、大于、小于、大于等于、小于等于、属于、不属于、存在、不存在，并能根据组合方式自动生成运算表达式，字段包括但不限于应用协议、目的IP、目的主机名、目的端口、目的用户名、数据流方向、情报IOC等；

（5）服务工具应内置不少于4种机器学习分析场景模型，可检测发现流量异常、网络会话数异常、网址访问失败异常、域名请求数异常等特定场景条件下的安全态势异常；

（6）服务工具应支持自定义部署AI机器学习模型，允许用户选用的高级机器学习算法不少于4种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。

1.1.1.4 服务人员要求

安全态势预警与通报服务驻场服务由1名高级安全服务人员提供支撑。

1.1.1.5 服务频率

服务期内提供7x24小时不间断服务。

1.1.1.6 服务成果

输出各种安全态势报告，包括电子政务网边界安全态势感知报告、僵木蠕毒安全态势报告、系统主机漏洞报告。交付物包含但不限于以下内容：

《电子政务网态势感知月度安全态势报告》

《僵木蠕病毒安全态势报告》

《系统主机漏洞报告》

《全流量威胁分析》

1.1.2 安全事件实时监测服务

1.1.2.1 服务要求

安全事件实时监测服务对所要求的监测对象进行 7x24 小时监测，监测到安全事件实时报警，不能出现漏报、误报；监测告警频率能够根据实际需要进行调整，告警的方式可以通过邮件、短信等方式发送；整个服务过程自动化，无人工参与。

1.1.2.2 服务内容

对安全事件进行汇总统计，动态梳理当前热点安全场景，如外部攻击者、漏洞利用成功、弱口令、勒索病毒等，帮助海南省医疗保障局聚焦热点安全问题，并对热点场景类型进行重点监测。

安全事件实时监测服务帮助将海量告警汇聚聚合为安全事件，帮助海南省医疗保障局抓住关注重点，减轻海南省医疗保障局分析负担，以安全事件为切入点，以威胁对象为聚合条件，梳理当前告警数据，变海量告警为几十条甚至十几条事件。

以资产为核心视角，直观了解自身网络环境中存在风险资产。结合攻击链进行分析展示，剖析从侦查阶段到获利阶段的资产失陷过程。感知失陷、异常资产，从海量的日志中提取有价值的资产溯源路线。从以下方面进行功能设计。

风险资产视角。通过资产被攻击严重程度展示网络环境中资产安全风险，包括已失陷、高风险、低风险三个维度，并可进一步对各维度资产情况进行钻取分析。安全域风险视角。以资产所属安全域为维度展示网络环境资产安全风险，并可根据安全域进行钻取分析。风险资产列表。为海南省医疗保障局列出当前存在风险的资产列表，方便海南省医疗保障局进行快速处置分析，并支持资产详情钻取分析。

以业务资产为视角，辅助海南省医疗保障局以资产为核心构建面向业务部门和管理层的业务资产管理模型。业务建模重点管理海南省医疗保障局的业务支撑系统，实现业务资产拓扑和资产安全等级评价等，为海南省医疗保障局提供业务

实时监控能力，保障海南省医疗保障局业务可持续平稳运行。主要设计包括以下功能。支持资产自动发现，也可从海南省医疗保障局现有资产平台进行资产信息同步，帮助海南省医疗保障局及时发现环境中资产，避免非法资产入网。支持对资产进行管理，包括修改、删除等管理操作，并根据海南省医疗保障局资产用途和网站结构划分，将资产至少分为内部资产、互联网资产和重点安全资产。

提供业务监控视图，支持根据网络架构自定义资产拓扑，同时也支持拓扑模板导入和拓扑文件导出。支持资产组织聚合，在上层资产模型中，对二级资产模型进行聚合，为运维人员查看提供便利。支持根据具体业务流程自定义构建业务视图，并支持业务模型修改、删除等管理操作。

以 IP 为视角，以互访流量关系为纽带，聚合呈现信息系统内部的所有资产。结合资产安全状态的综合打分评价结果，透视资产自身状态为高危/中危/低危/安全，以及资产间互相访问关系的正常或异常。主要设计包括如下功能。

资产健康状态评价：根据资产安全告警分析所处安全状态，对资产进行状态标记，帮助海南省医疗保障局清晰了解全局资产状态。资产互访关系透视：全局化呈现基于流量梳理发现的所有资产互访关系，访问类型包括正常访问和异常访问，并统计访问次数，访问方向包括访问内网、来源内网、访问互联网、来源互联网，帮助区分外部攻击和横向威胁。此外，支持一键关系拓展，可视化呈现访问关系，帮助海南省医疗保障局清晰查看威胁扩散情况。资产威胁深度追溯：实现对透视页面独立资产的深度追溯，以攻击者视角对资产进行攻击链阶段定位，并对资产相关告警进行聚合呈现，帮助海南省医疗保障局简化海量告警。资产指纹刻画：结合漏洞管理、终端风险管理等刻画资产详细指纹信息，包括资产自身属性信息、流量管控情况、设备安全信息等。

1.1.2.3 服务频率

服务期内提供 7x24 小时不间断服务。

1.1.2.4 服务成果

《安全事件实时监测报告》

1.1.3 边界实时监测服务

1.1.3.1 服务要求

边界安全事件实时监测服务对网络边界进行 7x24 小时监测，监测到安全事

件实时报警，不能出现漏报、误报；监测告警频率能够根据实际需要进行调整，告警的方式可以通过邮件、短信等方式发送；整个服务过程自动化，无人工参与。

1.1.3.2 服务内容

对医保局网络边界进行安全实时监测，对发现的安全事件进行实时告警，定期提供监测报告；提供数据管理、资产管理服务。提供多合一硬件探针、支持服务。多合一硬件探针提供僵木蠕毒分析、入侵事件检测、APT 事件检测服务。提供基于信誉的僵尸网络检测能力，具备可以持续升级的信誉库，IDS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的检测动作；提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等）；提供覆盖广泛的攻击特征库，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和阻断，攻击特征库数量至少为 6000 种以上。

1.1.3.3 服务频率

服务期内提供 7x24 小时不间断服务。

1.1.3.4 服务成果

《边界安全态势报告》

1.2 安全大数据综合服务

（1）服务要求

基于互联网全流量监测数据并汇聚医保系统平台流量数据、日志数据及安全防护设备数据进行网络安全威胁大数据关联分析、交叉验证等态势研判，实现从不同视角感知医疗保障信息平台网络安全态势，包括总体态势、威胁态势、攻击态势、隐患态势、事件态势五大视角。

①网络安全总体态势分析，包括当前数据来源、监管对象统计、监测成果统计、漏洞与隐患详情、隐患、攻击、事件、通报的趋势、系统隐患数量 TOPN、隐患区域 TOPN、事件分布统计、通报处置列表等内容。

②支持威胁态势分析。内容包含威胁分类及统计、威胁源分布及统计等。

③支持隐患态势分析。内容包含隐患分类及统计、隐患区域和行业分布情况等。

④支持网络攻击分析，内容包含网络攻击分类及统计、监控总览及分类、最

新攻击消息、攻击趋势、受攻击行业分布、攻击类型分布、攻击区域/受攻击区域排名、攻击 IP/受攻击 IP 排名等。

⑤支持安全事件分析，内容包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名等。

（2）人员要求

要求 1 名高级安全服务人员。

（3）服务工具

服务工具应具备全局资产的资产访问图谱可视化模块，支持立体、平面、球面等多种维度的网络实体关系透视。根据资产的风险等级，对资产用不同颜色进行区分，具备访问关系的资产用直线相连，访问关系具体说明，包括但不限于：访问方向、访问类型、累计流量、访问时间等。服务工具应支持每个用户配置个人专属的统一门户，可配置项包括门户名称、应用名称、应用图标等。服务工具应统一门户应支持与第三方产品集成，一键跳转至产品功能界面。服务工具应支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录；该服务工具应与安全态势预警通报联动，或整合为统一管理平台。

（4）服务频率

服务期内提供 7x24 小时不间断服务。

（5）服务成果

《安全大数据综合展示报告》

1.2.1 安全驻场保障服务

1.2.1.1 安全事件处置服务

（1）服务要求

针对市级部门网站、各区（市）县等单位门户网站及重要信息系统提供应急响应及演练服务；对信息安全领域疑似非法攻击事件进行处置，包括突发安全事件远程技术支持；突发安全事件现场技术支持；安全事件溯源及调查取证；保障业务连续性；安全事态控制。事件处置过程对客户公开，并严格遵循信息安全突发事件处置流程（准备－－检测－－抑制－－根除－－恢复－－总结）。本项服务包含在安全驻场保障服务内。

（2）服务内容

通过人工现场供应方式提供重大安全事件应急响应服务。包括：编制应急响应预案服务、应急预案演练服务、安全事件分析服务、安全事件溯源服务、安全取证支持服务、安全事件处置服务、重要活动、会议保障服务、事件通告服务、安全预警服务、经验教训总结服务等。

建立应急响应体系，包括：编制应急响应工作预案和流程，并在重大信息安全事件发生时严格按照预案组织实施。分析信息安全事件的类型及产生的原因，进行应急处置，排除隐患，恢复系统正常操作，获取并保存相关证据。信息安全事件处置完毕后 3 个工作日内提交详细的应急工作报告，并提出整改方案和建议。建立应急响应组织，建立完善预防预警机制，建立安全事件分级管理体系，建立应急响应保障措施，进行应急预案的定期测试和演练。

提供远程应急处置协助，包括热线支持、远程支持、现场支持等服务手段。

（3）服务频率

每日响应用户需求，按次数提供安全事件处置服务。

（4）服务成果

交付物包含但不限于以下内容：

提供安全事件分析报告、安全事件紧急通报、安全取证支持服务报告、运维值守报告。

1.2.1.2 安全咨询服务

（1）服务要求

通过提供专业人士所储备的知识经验和通过对各种信息资料的综合加工而进行的综合性研究开发，针对环境内存在的各种网络安全问题，专业人士从管理、技术、体制、机制等各方面提出解决方案，融合发现问题、分析问题、解决问题。通过建立安全管理制度和安全考核体系给出有效的解决方案，从而持续地保证业务的安全运行。本项服务包含在安全驻场保障服务内。

（2）服务内容

参照国家等级保护标准 GB/T22239、GB/T22240 及行业等级保护标准要求，提供重要信息系统信息安全等级保护合规建设过程的专业咨询服务，建立健全的网络安全责任制，完善网络安全规章制度、操作规程、台账、档案、记录等，帮助用户确定网络安全方针和目标。

（3）人员要求

团队成员至少一人同时具备的资质包括 CISP（注册信息安全专业人员）和 CISSP（信息系统安全专业认证）。

（4）服务频率

根据用户需求，根据实际情况提供咨询解决方案。建立安全管理制度，并不断进行完善。

（5）服务成果

- 《咨询解决方案》
- 《安全管理制度》
- 《安全考核制度》

1.2.1.3 安全培训服务

（1）服务要求

管理类培训：对从业人员开展信息安全管理类培训，提供丰富先进的专业知识，有效提高参与培训人员的技术和管理水平，增强参与培训人员的安全意识和技能，提供培训报告。

认证类培训：对从业人员进行人员资质认证培训，提供国家信息安全权威测评机构的授权认证， 并确保参与培训的相关人员在培训考试后取得符合国家标准的资质证书。

实践类培训：对从业人员开展信息安全实践类培训，提供丰富先进的实践、演练服务，在线教育培训与靶场对抗，提供实时在线、同步、异步学习、学习评价、对抗演练与模拟仿真环境，提供培训报告，提升技术人员的实操技能。

本项服务包含在安全驻场保障服务内。

（2）服务内容

管理类培训服务包括的服务内容有：（a）IT 战略规划与项目实施高级课程：IT 战略规划，完整 IT 战略规划过程与案例分析，企事业 IT 架构规划，IT 项目管理。（b）IT 治理体系规划与实施高级课程： IT 治理三大支柱，IT 治理核心，IT 决策治理，IT 激励与 IT 控制， IT 治理体系规划与实施。（c）IT 服务管理课程： 服务战略，服务设计，服务转换，服务运营，持续服务改进。

认证类培训服务包括的服务内容有为注册信息安全专业人员系列认证：（a）

国家注册信息安全员、（b）国家注册信息安全管理人员、（c）国家注册信息安全工程师、（d）国家注册信息安全审计人员、（e）国家注册信息安全开发人员等。

实践类培训服务包括的服务内容有：（a）网络渗透与深度防御课程：搭建拟真攻防对抗环境，动手演练黑客入侵步骤，针对性进行主动全面防御部署分析，在短暂时间内提高实践动手能力和综合防御能力。（b）网络渗透测试能力实践课程：安全攻防基本原理与流程，渗透测试技能，恶意代码，脚本木马，客户端安全（c）网络攻防技术实践培训课程：网络攻防技术概述，网络信息收集技术，网络嗅探与协议分析，TCP/IP 网络协议攻击，网络安全防范技术，Windows 操作系统安全攻防，Linux 操作系统安全攻防，恶意代码安全攻防，软件安全攻防——缓冲区溢出和 Shellcode，Web 应用程序安全攻防。

定制类培训服务根据用户的实际需求提供基于政策解读、行业解读、岗位解读等安全专业技术服务。

（3）服务频率

认证培训根据认证机构的开班时间而定，其他部分根据用户培训类型、相关要求以及规模进行。

（4）服务成果

帮助培训对象提高管理层的管理能力，提升全员的安全意识水平，提升技术人员的实操技能，提高单位整体信息安全保障能力，提供培训报告。

交付物包含但不限于以下内容：

《安全教育服务实施报告》《安全教育服务反馈调查》《培训计划安排》、培训资料、信息安全人员资质权威认证证书。

1.2.1.4 驻场人员分工

配合各类应急演练要求，根据在演练期间，按照医保局要求派驻 2 名高级安全服务人员；主要任务如下：

（1）负责通过运维平台远程监测安全设备、安全软件的运行状态，配合安全态势预警、通报的即时信息，根据医保局授权进行响应，并根据医保局要求形成响应及处置需求，提交安全服务处置人员进行处置，对处置结果编写报告，提交医保局信息办备案；

（2）编制对大数据局安全服务及医保局安全设备、安全软件的运维方案及

计划，并填报运营日志。

（3）编制安全设备、安全软件策略规划及配置手册，并以此为基础对驻场运维人员进行培训、指导演练，以达到所有驻场人员均可以根据常态化保障要求或应急情况调度值守。

（4）按照各级医疗机构、定点药店等，按照海口、三亚、儋州三个片区进行分工。主要负责对三个片区下的接入机构进行联网安全监测、监管，接收安全设备、安全软件、安全服务发送的接入单位告警、预警信息，进行协调、协助处置、编制运维日志、编制处置报告；并协调医保局工作人员或受医保局授权委托，对接入医保网的医院、药店、村医室等进行现场安全核查，以确保接入医保网的终端设备、终端设备中的软件、各客户端软件、插件控件等应装尽装，并进行合规性检测和评估，直到符合接入要求。驻场人员负责医保局运维中心值守及至片区医院、村卫生室及药店现场处置协调。

1.2.2 安全设备运营服务

（1）服务要求

运用先进可靠的信息安全技术，提供 1 名高级安全服务人员开展安全设备运营服务，驻场人员服从甲方工作安排，按照甲方相关工作要求协调各相关安全设备运维单位开展具体工作。

（2）服务内容

为了保证网络安全服务质量，在相关实施方提供安全服务期间，实施方应满足以下安全设备运营服务要求：

①安全设备运行监测，对于安全设备运行过程中可能发生的异常故障等情况开展长期运行监测工作，以及时发现并按照相应流程处置；

②安全设备策略配置，对于安全设备的网络策略及防护规则进行审核，策略或规则变更（新增、停用等）应经审核并报用户单位同意后落实，以有效应对来自不同网络区域的网络攻击行为；

③安全设备升级，为保障安全设备有效性，合理配置安全策略，定期对安全设备的软件版本、特征库、规则库进行升级，确保安全设备稳定运行并具备最新安全防护能力；

④安全设备备份，为保障安全产品在出现异常故障或其他不可控因素时能够

及时恢复，定期对安全设备策略及配置进行备份，防止因故障导致防护缺失等严重后果；

⑤其他工作，驻场期间用户分配的其他保障任务。

（3）服务方式

①远程支持

②现场支持

③E－MAIL 支持服务

④电话支持

（4）服务频率

①现场安全运维值守服务 5*8 小时开展安全值守工作。

②设备调试、策略维护、策略配置、设备升级、备份按照用户需求和实际情况。

（5）服务成果

交付物包括但不限于：《安全设备巡检报告》、《安全设备策略规则配置情况报告》、《安全设备升级情况报告》、《安全设备策略备份报告》。

1.2.3 应急演练与攻防演练服务

1.2.3.1 服务概述

在万物互联时代背景下，“没有网络安全，就没有国家安全”，没有网络安全，就没有网络空间中人的安全。网络安全的本质是攻防两端能力的较量，网络安全应急演练与攻防演练是检验用户整体网络安全真实防护能力的最佳实践之一。根据网络安全等级保护的安全防护要求，提供安全应急演练与攻防演练服务，旨在帮助用户检验网络安全实战防御能力，提高用户对网络安全事件应急响应的理解与掌握，提高网络安全应急处突能力，从而有序地开展防范并及时、高效处理网络安全突发事件，保障重要系统安全、稳定、持续运行，最大限度地减少网络安全突发事件带来的影响，预防造成重大损失和恶劣影响。

1.2.3.2 服务内容

安全应急演练与攻防演练，是针对信息系统在运行过程中或者操作过程中可能出现的紧急安全问题，进行次模拟应急演练。其目的是加强自有业务安全管理，梳理和完善自有业务系统遇到突发事件后应急处理流程，缩短系统中断时间，全

力保障业务系统安全。本次演练方案为业务平台网页被篡改事件处理专题预案,其目的是为进一步规范网页被篡改事件的处理方法和处理程序,提高对自有业务系统网页被篡改事件的反应速度。

演练事件：

海南省医疗保障局受到恶意人员的网络攻击或病毒木马等,导致业务系统功能异常、非法恶意信息传播或网站被恶意挂马等,对单位造成极大的负面影响和损失等情况。

服务内容:安全意识防护培训、应急预案编制、演练页面准备、演练方案、流程梳理、脚本准备、现场环境准备、现场演练彩排、现场演练环节及总结，服务完成后出具《应急演练与攻防演练报告》。

将通过各层面的攻击渗透及社会工程学攻击渗透的实战攻击手段，对防守单位开展实战攻击，检验相关单位网络安全防护能力，提升网络安全应急处置能力，避免发生重大网络安全事件，保障重要信息系统安全、稳定、持续运行。实战演练结束后，针对本次攻防演练发现的问题，组织相关单位人员，提供配套的安全培训，提出整改意见。服务内容主要包括实战攻击、过程展示与风险控制、实战演练培训及总结三大部分。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	应急演练与攻防演练服务	1.网站恶意篡改事件 2.上传 webshell 木马事件 3.病毒攻击事件 4.拒绝服务攻击事件。	用户单位	《网络安全应急演练与攻防演练报告总结报告》《整改建议》、培训课件和培训文稿等	服务期内根据医保局要求开展演练服务	远程服务、现场服务

1.2.3.3 服务成果

通过应急演练服务，输出《网络安全应急演练与攻防演练报告总结报告总结报告》《整改建议》、培训课件和培训文稿等。

1.2.3.4 服务收益

（1）落实网络安全法，贯彻法律法规要求；

（2）以攻代检，检验实战防御能力；

（3）实战促防，提升意识提升，促成应急处置能力提升。

（二）重保服务

1、重保服务的主要工作就是在重要会议或重大活动期间从网络层面、服务器层面、数据层面为用户构建全方面的重要敏感时期的安全保障服务。保障网络基础设施、重点网站和业务系统安全，提供全方位的安全防守构建咨询以及事前、事中、事后的全面安全建设托管服务，确保企业客户的业务系统能够在重大活动期间安全平稳运行。

2、重保服务人员需具备 CISP（注册信息安全专业人员）资质。

3、重保服务工作内容：

3.1 网站安全综合监控：对网站可用性、黑链、暗链、篡改、挂马等进行监测。

3.2 扫描与评估服务：利用专业安全扫描工具对网站进行脆弱性扫描，人工评估漏洞。

3.3 渗透测试服务：白帽子团队对网站进行人工渗透测试。

3.4 整改与复检：针对漏扫和渗透结果，协助整改，并对整改后的站点进行复检。

3.5 主机加固与检测：利用专业主机安全加固与检测响应工具，防止黑客埋雷。

3.6 高危事件应急演练：协助设计重保期间，高危应急演练场景，并完成演练。

3.7 模拟攻防演练：指导业主方完成攻守演练，发现应急处置的设计缺陷。

3.8 重保期间服务：计划设计保障计划、通报流程、协作机制、处置规范及注意事项等。

3.9 现场值守服务：

（1）重保期间 7*24 小时安全监控与值守，针对网站可用性、黑链、暗链、篡改、挂马及其他安全事件进行分析和处置。

（2）同步外部威胁情况，提前添加 IP 黑名单和设置安全策略。

（3）每小时专属群汇报，每日提供日报，每周提供周报。

（4）远程人工日志分析，每日分析当天 web 全流量、各类告警、安全设备等日志。

3.10 安全通告与预警：重保期间，发生的重大外部安保事件、高危漏洞威胁，第一时间通报预警，并协助修复。

3.11 入侵审计服务：专家级入侵取证人员现场入驻，分析入侵路径和手段，攻击溯源。

3.12 重保工作总结：对保障工作情况进行总结，提交报告。

3.13 交付成果物:《重要时期安全保障工作方案》、《重要时期安全保障值守报告》、《重要时期安全保障工作总结报告》等。

（三）网络安全运营方案

随着各类安全手段逐步到位，用的不多、效果不好的问题凸显，网络安全工作没有发出与其关系海南省医疗保障局及下属单位重要性、与运维工作不可分割的特殊性、工作量巨大和超越部门支撑全网的重大作用相一致的声音，也极大地削弱了网络维护部门在网络安全工作领域的领导作用，并进一步导致人员配备不足、进入恶性循环，最终影响网络安全保障能力。

为此，本文进一步明确网络安全运营体系内涵，明确各类人员安全工作职责，希望借此强化责任意识、主动意识，结合海南省医疗保障局及下属单位的考核体系，加快建立专业网络安全运营团队、面向全网重要系统、 IDC 以及其他部门互联网应用开展 7*24 小时集中化安全运营。

1、设计基本原则

1.1 网络安全运营体系以管控互联网安全风险和业务系统安全风险为核心。

1.2 网络安全运营体系是网络维护体系的有机组成部分， 需要与日常网络运维工作密切配合，实现安全运营和网络运维一体化。

1.3 各省网络安全运营体系需要与总部远程安全检查、安全培训、安全事件监测通报、互联网安全治理、两部委考核专项工作、定期生产分析和信息通报等进行衔接，实现海南省医疗保障局及下属单位安全运营一体化。

1.4 通过安全技术手段的建设和应用，不断提高自动化水平。

1.5 不断壮大安全人员队伍和提升安全技能，不断提高专业化水平。

2、主要内容

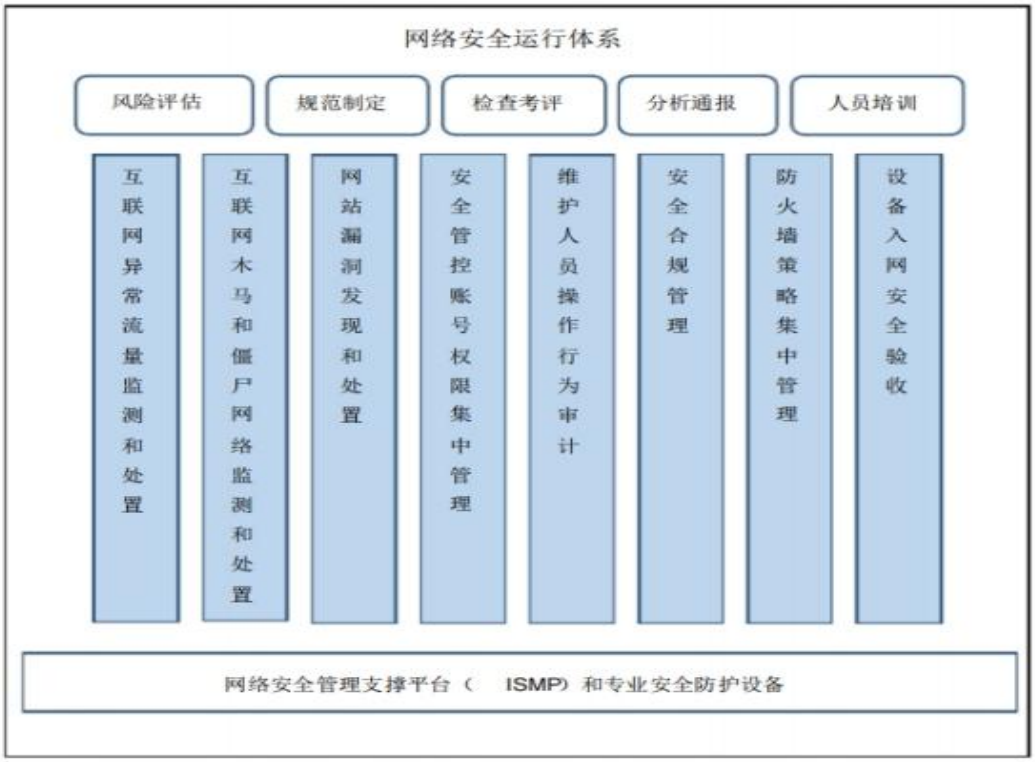
网络安全运营体系包含以下三方面具体内容：

2.1 由安全专职人员主导各专业配合的横向内容：风险评估、规范制定、检查考

评、分析通报、人员培训。

2.2 按照“谁维护，谁负责”的原则，由各专业作为主体进行落实执行的纵向内容：与安全专职人员配合开展互联网异常流量监测和处置、按照安全专职人员监测结果进行互联网木马和僵尸网络处置、网站漏洞发现和处置、基于安全管控平台的网元账号权限集中管理、维护人员操作行为审计、安全合规检查加固、防火墙策略集中管理和核查、设备入网安全验收。

2.3 安全专职人员负责网络安全运行体系的支撑手段，包括网络安全管理支撑平台（ISMP ）以及底层专业安全防护设备的运营工作，各类安全专业防护设备，如互联网异常流量监测和处置、互联网木马和僵尸网络监测运营工作。



3、职责分工

为了更好地推动网络安全运营体系的建立，各省必须逐一细化明确各相关专业的职责分工、具体流程、工作内容、周期要求等，以下内容是对各类人员落实安全职责的基本要求：

3.1 管理层（网络运维部门领导）工作要求：

序号	内容	要求	评价标准
1	明确职责分工	对网络安全运营体系的九项重要工作内容明确安全专职人员和相关系	有明确的部门发文

		统维护人员的职责界面，协调公司相关部门落实安全专职人员配备要求。	
2	听取生产分析	至少每季度听取一次网络安全运营体系生产情况分析报告。	每季度一次生产分析会材料，并提供部门生产分析会纪要。
3	对网络安全运营体系重大事项进行决策	对网络安全运营体系存在的问题、重大事件进行决策，审定需要通报的内容和范围，并督导落实。	部门生产分析会或者专题工作汇报纪要
4	向省局主管领导进行汇报	每年至少一次汇报网络安全工作内容、整体情况、问题和需要省局领导给予资源支持的决策事项，做到各级人员对网络安全工作特点、内涵、现状、方向的认识完全一致	汇报材料、纪要

3.2 安全专职人员工作要求

序号	内容	要求	评价标准
1	风险评估	定期组织对网络和业务系统的安全 风险评估	1、风险评估的频次不低于等级保护的相应要求，即 3 级及 3 级以上系统每年至少开展 1 次以上等保测评等安全服务，其他系统至少两年开展 1 次评估； 2、评估内容侧重安全渗透； 3、有完善的评估报告和闭环整改证明文档
2	生产分析	定期（月度、季度）对网络安全运营体系的主要工作的执行情况和重大安全事件、问题	生产分析的频次和各项指标的完整度。

		进行分析	
3	安全通报	对网络安全运营体系的执行情况进行通报。	1、通报的频次和通报问题的整改率。 2、至少每 3 个月通报一次。通报内容应全面涵盖文件要求的八个方面的工作内容。 3、通报涉及的系统范围应包括所有与互联网有连接关系的系统，设备范围应包含终端之外的所有主要设备。 4、分析内容应包含多个维度，至少包括：纵向（整改情况）、横向（部门、系统间）、重大或者共性问题专题等。 基于各类自动化安全管理、核查、 漏洞扫描工具，以及数据基本真实准确的安全设备告警（如防病毒、 DDOS 、 WEB 防攻击、僵木蠕）和人工处理内容等。
4	检查考评	制定具体的考评指标，并开展检查 和考评工作。	各类事项的检查频率和覆盖范围不低于集团的要求，即合规、弱口令、防火墙策略核查不低于一季度一次，安全域划分情况核查不低于每半年一次，管控平台接入情况核查不低于每半年一次。
5	闭环管理	对集团公司发现问题、省公司检查发现问题、	及时整改率

		工单要求、预警公告等的落实情况，在明确的处置时间内进行及时复查，全面掌握，直至全 部解决	
6	手段建设	组织规划、需求整理、方案制定、配合建设、协调施工等一系列工作	集团要求的手段建设项目进展顺畅，准确了解进度、问题、未完成任务等
7	手段运营	安全手段策略（如管控平台用户主账号与手机号的对应关系、访问网元使用的账号密码的有效性等）运营，关键数据的定期备份、利用安全手段进行安全核查、扫描等工作，宣传、推动系统维护人员等使用与系统维护职责中安全内容有关的手段。 注：系统主机维护、数据备份可以纳入 IT 维护专业统一管理	集团公司使用省公司管控平台正常 省公司安全手段使用情况

3.3 系统维护人员工作要求

序号	内容	要求	评价标准
1	互联网异常流量监测和处置	确定本系统的流量基线和清洗策略	DDOS 事件发现能力和处理能力
2	互联网木马和	负责处置本系统相关的互联网木马	互联网木马和僵

	僵尸网络监测和处置	和僵尸网络监测事件	尸网络事件处置及时率
3	网站漏洞发现和处置	负责对本系统含有的网站进行扫描自查，对自查或者通报的问题进行整改。	网站漏洞处置及时率
4	补丁管理	按照预警公告加载安全补丁，及时升级存在高危漏洞的操作系统、中间件、上层应用和数据库	补丁加载、软件升级及时率
5	账号集中管理	负责对访问本系统的人员账号进行授权、负责本系统资源同步接入和绕行控制配置工作。	口令自动修改率；资源接入率
6	操作行为审计	负责确认对本系统的敏感可疑操作进行审计。对审计判定和实际存在出入的情况，要提出相应证明材料。	违规操作比率；审计事件响应及时率。
7	合规检查	负责对本系统的安全配置和口令复杂度进行自查，并整改不合规项。	每设备弱口令数；设备配置合规率
8	防火墙策略核查	负责配置本系统的防火墙策略，并对防火墙策略定期审核，并过期策略	防火墙违规策略比率。
9	网络安全管控平台的使用	在管控平台正常运行期间，要使用管控平台完成日常操作维护。	管控平台使用率。

二、商务要求

1、服务期限：2024 年 8 月 31 日至 2024 年 12 月 31 日。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、项目的实施要求

5、测评项目实施过程中，投标人应遵循国家标准、行业标准。在项目实施中投标方必须做到:

（1）提供项目实施组织架构；

（2）提供详细的项目实施方案和计划进度说明书；

（3）对于采购人的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在 2 小时内到达采购人现场；

（4）严格按照双方确定的计划进度保质保量完成工作；

（5）规范项目实施过程中的文档管理；

（6）项目实施中要引入风险管理、质量管理、成本管理；

（7）签署《保密协议》。中标单位(含项目组所有成员)必须对项目技术文件以及由招标人提供的所有内部资料、技术文档、数据和信息予以保密。中标单位必须与招标人签订保密协议并严格遵守，未经招标人书面许可，中标单位不得以任何形式向第三方透露本项目标书以及本项目的任何内容。

6、采购资金的支付方式、时间、条件：本项目经费采用两次付款支付方式。

6.1 合同签订生效后，甲方凭乙方提供的正式有效等额发票，在 10 个工作日内向乙方支付合同总价的 60%。

6.2 乙方完成项目服务内容，并提交《安全咨询及保障服务项目自评报告》及阶段性工作成果报告且通过甲方组织的验收后，甲方凭乙方提供的正式有效等额发票，在 10 个工作日内向乙方支付合同总价的 40%。

7、验收要求：按标书服务要求和国家行业标准进行验收。