# 服务内容与要求

## 资产梳理：

每次梳理后提交《资产梳理报告》。（提供资产梳理报告样本，并加盖投标人公章）

★投标人需提供的资产梳理工具，资产梳理工具具体要求详见《资产梳理漏洞扫描服务工具要求》。

## 渗透测试服务：

配合医院处理相关漏洞问题，完成整改后进行复扫，服务后提交《渗透测试授权书》《渗透测试方案》《渗透测试报告》《整改建议书》《渗透测试复测报告》等。

投标人应采用多样化的技术手段针对web安全漏洞、安全功能缺失漏洞、业务逻辑漏洞、中间件漏洞等进行检测，并针对系统层面与网络层面开展安全测试。

## 漏洞扫描服务：

通过技术人员定期漏洞扫描，对存在的各种安全漏洞、隐患，以及系统运行状态，提供检测报告及系统加固意见和相关处置措施，协助完成漏洞修补和安全整改后进行复扫；每次服务后提供《漏洞扫描报告》和漏洞解决方案。

★投标人需提供的漏洞扫描工具，漏洞扫描工具具体要求详见《资产梳理漏洞扫描服务要求》。

## 安全基线评估服务：

根据采购人要求每次服务后提交《系统网络安全基线检查报告》《系统基线检测复查报告》。

★投标人需提供的基线检查工具，基线检查工具具体要求详见《资产梳理漏洞扫描服务工具要求》。

## 攻防、应急演练、安全培训服务：

中标人在服务前后需提交《攻防应急演练方案》《攻防应急总结评估分析报告》以及《突发网络安全事件应急预案》。

须提供至少一场全院网络安全现场培训，培训内容涵盖安全意识、安全技能等，提高医院网络安全建设和运维水平。

## 重要时期安全保障服务：

提供至少3人/天（8小时）,1人/天(24小时)驻场服务。

投标人在服务前后须提交《重要时期安全保障服务方案》《重要时期安全保障服务工作总结》

## 日常运维及监测服务：

投标人每次巡检服务后提交《网络安全巡检报告》《网络安全监测报告》；每次对处理的安全事件提交《安全事件处置报告》

★提供的安全运营服务相关工具能够充分利用现有网络安全设备，实时监测网络安全状态，支持安全态势（威胁情报、漏洞等）展示，对攻击事件能够及时进行分析与实时告警，并能在紧急响应和处置。

★投标人需提供服务质量可视化监控平台，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、安全事件闭环率、安全事件平均闭环时长。

★以上投标人需要提供的服务工具要求详见《流量探针服务工具要求》《安全感知服务工具要求》

## 应急响应服务

每次对处理的安全事件提交《安全事件应急响应报告》《应急响应服务确认单》；每季度提交《安全运营报告》，年度汇总形成《年度网络安全综合报告》。

供应商有提供安全事件闭环能力，要求供应商具有CISP、高级网络信息安全工程师\数据库系统工程师、信息系统运维管理工程师等相关的工程师及其证书。

## MSS安全托管服务

|  |  |
| --- | --- |
| **类型** | **内容及要求** |
| 资产数量 | ▲本次服务共10个信息系统资产，需提供7\*24小时安全服务，对目标范围内的信息系统服务资产，持续开展资产安全、脆弱性、威胁、安全事件管理服务。 |
| 首次安全评估 | 暴露面梳理：投标方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。 |
| ★投标方应具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标方举证，及对应暴露资产存在的漏洞**【**提供服务工具具备以上暴露面梳理能力的证明截图**】** |
| 威胁管理 | **7\*24小时威胁鉴定：**投标方应当具备云端检测和分析平台，通过采集招标方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； |
| **个性化的检测规则定制：**为了保证安全监测的准确率和服务质量，投标方应当支持为招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求； |
| **受影响资产排查与加固：**安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。**【**提供一个威胁情报的安全通报工单，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况**】** |
| **★安全策略检查：**投标方安全专家每月对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标方云端服务平台应当具备丰富的策略检查工具（要求不少于40种策略检查的工具），支持排查安全设备防护策略配置的合理性。**【**提供投标方云端服务平台策略检查工具的截图证明，证明具备上述能力**】** |
| 7\*24H的服务团队 | 为了保障服务质量和加强投标方与招标方的沟通，投标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，并且实时响应投标方咨询的网络安全相关问题； |
| 投标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、节假日投标方都应该能做到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》。 |
| 服务指标要求 | ★为了降低招标方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招标方提供服务：  (1)分析研判通知时效MTTA：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)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%）； (3)投标方应当承诺攻击成功事件0漏报，服务人员至少发现攻击链路上的一个攻击行为。 (4)投标方应当承诺，服务范围内的所有安全事件的闭环处置比例达到100%。 (5)投标方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，省会2小时上门处置，省内8小时上门处置。  (6)事件闭环时间MTTR：经招标方授权后，投标方服务人员协助进行安全事件的闭环，一般安全事件的闭环完成时间少于8小时，重大事件的闭环完成时间少于24小时；  **【**要求投标方对标以上服务指标可否满足进行应答，需提供服务承诺函**】** |
| 服务成果可视化（用户portal页面） | ★服务质量监控：投标方需为招标方提供的服务成果展示门户（或用户Portal）应具备服务质量可视化展示，投标方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（或称为服务SLA）。**【**提供服务成果展示门户中服务质量监控相关的截图证明**】** |
| 服务交付物管理：投标方需为招标方提供的服务成果展示门户（或用户Portal），可以直观的管理服务过程中生产的服务报告和交付物，包括但不限于《准备阶段文件》、《特殊时期值守报告》、《运营周报》、《运营月报》、《运营季报》、《威胁情报》、《年度汇报》、《事件总结报告》； |
| 服务过程与成果可视化（移动端助手） | 服务过程透明化可视化：投标方需为招标方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，让招标方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。 |
| ★投标方需为招标方提供移动端服务过程展示门户（移动端Portal），支持实时直观地查阅服务的每日运营动态。运营动态需包括【事件通告】【威胁通告】【威胁情报】【服务报告】【夜间值守快报】等，并支持自定义进行筛选和管理。【提供移动端服务过程展示门户中支持查阅每日运营动态的截图证明】 |
| 投标方需为招标方提供移动端服务过程展示门户（移动端Portal），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。 |
| 云平台服务 | 投标方应当具备云端7\*24小时运行的服务平台，并具备以下能力为招标方提供专属的安全托管服务： |
| ★**安全设备对接与数据采集:**投标方云端服务平台应当支持对接招标方网络中已部署的主要安全设备：安全态势感知，支持实时接收安全设备检测到的安全事件信息、安全日志数据提供7\*24小时的安全托管服务；【提供云端服务平台支持对接的上述安全设备的能力证明，展示详细的对接步骤】 |
| **平安合规性要求：**  投标方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](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E6%8A%80%E6%9C%AF%E2%80%94%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E7%AD%89%E7%BA%A7%E4%BF%9D%E6%8A%A4%E5%9F%BA%E6%9C%AC%E8%A6%81%E6%B1%82/53703710?fromModule=lemma_inlink" \t "/Users/duan/Documents\x/_blank)》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；【投标方应当提供云端服务平台等级保护三级测评通过证明，提供报告首页、基本信息表、等级测评结论首页，以上内容中必须明确指出该平台用于为用户提供7\*24小时的安全托管服务；（敏感内容投标方可脱敏展示）】  投标方云端服务平台应通过国家互联网信息办公室、国家发展和改革委员会、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；【提需供中央网络安全和信息化委员会办公室、国家互联网信息办公室官方网站发布的《通过云计算服务安全评估的云平台》入选名单作为证明（名单截图），需明确写明为安全托管服务运营平台。】 |
| **服务流程引擎：**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；  【投标方应当提供云端服务平台具备上述流程编排能力的证明】 |
| **GPT能力：**投标方托管服务平台应具备GPT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。提供安全托服务平台GPT能力项的证明截图。 |
| 资质项 | （1）所投厂商具备国家信息安全服务（安全运营类二级）资质，需提供有效证明材料。  （2）投标方的安全运营平台的平台能力和人员服务能力需要符合《面向云计算的安全运营中心能力要求》 标准，获得权威机构认证，提供证明材料。  （3）市场能力：所投厂商的远程托管安全服务连续3年在中国区IDC中国远程托管安全服务市场占有率排名前三，要求提供证明材料。  （4）所投厂商是国家互联网应急响应中心网络安全应急服务国家级支撑单位，需提供有效证明材料； |

# 服务工具技术要求

## 服务工具清单

★投标人需为本项目提供不低于如下工具数量及参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序列 | 名称 | 参数要求 | 数量 | 单位 |
| 1 | 资产梳理漏洞扫描服务工具 | 详见后续 | 1 | 套 |

## 资产梳理漏洞扫描服务工具要求

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 系统要求 | 采用有自主知识产权的安全操作系统，采用B/S设计架构，并采用SSL加密通信方式，无须安装客户端，用户可通过浏览器远程方便的对产品进行管理。 |
| 产品性能 | 支持≥100个扫描IP授权（可扩展）、≥20个WEB漏洞扫描URL授权（可扩展）。其中系统漏洞扫描，基线配置核查，弱口令扫描受授权IP数限制，资产发现不限制IP数量。 |
| 支持同时开启全插件系统漏洞扫描、WEB漏洞扫描、弱口令扫描、基线配置核查，扫描速度不低于1000ip/h。 |
| 风险统计服务 | ★支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。（需提供产品功能截图证明） |
| 支持从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，支持以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情。 |
| 任务类型 | ★支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。（需提供产品功能截图证明） |
| 系统漏洞扫描服务 | 支持认证管理功能，对系统登录信息进行统一管理和配置，提供登录信息的新增、删除和批量导入功能，在系统漏洞扫描和基线核查登录扫描时，可从认证管理中批量导入登录信息。 |
| 内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息。 |
| WEB漏洞扫描服务 | 支持行业通用标准OWASP，支持通用WEB漏洞检测，如：SQL注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等。 |
| 支持信息泄漏类漏洞检测，如：mail地址、敏感目录暴露、内部ip地址、会话令牌、源码、数据库备份文件、SVN文件、系统重要配置、日志文件向外网泄漏等。 |
| 弱口令扫描服务 | 产品内置常用字典和精简字典两种弱口令扫描模板，常用字典包含常见的用户名及TOP160密码，精简密码适用于爆破速度快的密码猜解场景，支持自定义新增密码字典功能。 |
| 合规自检平台服务 | ★按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。（需提供产品功能截图证明） |
| 报告管理服务 | ★产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。（需提供产品功能截图证明） |
| 服务资质 | 所投产品应具有国家信息安全漏洞库（CNNVD）兼容性资质证书，需提供有效证书复印件。 |
| 服务厂商资质 | 厂商应具备三年以上漏洞研究经验和独立漏洞发掘能力，自主发现的CNVD原创漏洞不少于24个，需提供相关证明材料。 |
| 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资质，需提供有效证书复印件。 |