**采购需求**

为了提高我单位信息安全防护水平，依据《中华人民共和国网络安全法》、上级单位要求，我单位向信息安全服务公司购买网络安全服务工作。

# 服务范围及内容

## 服务类别

|  |  |  |
| --- | --- | --- |
| **序号** | **服务类别** | **服务内容** |
| 1 | 网络安全服务 | 为贯彻落实《中华人民共和国网络安全法》、《网络安全等级保护基本要求》等相关文件的要求，结合医院目前网络安全建设的情况，结合国家政策对网络安全建设的要求，为了提高网络安全防护水平，保证医院网络安全满足《网络安全等级保护基本要求》，提供医院目前缺少的网络安全防护产品（性能必须满足医院业务要求，在服务期内如设备性能无法满足，由服务提供方更换更高性能产品）和对应服务，要求必须提供产品一年的使用、产品规则库的升级以及巡检服务、维护服务等相关配套服务。 |

## 服务内容

本项目中需要投入的服务内容如下

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 数量 | 单位 | 服务内容 |
| 1 | 边界安全防护及保障服务 | 1 | 年 | 为院方提供为期一年的边界防护服务，在提供服务的过程中，由服务方免费提供对应的工具或设备，要求至少针对两个网络边界进行防护及保障，应具备2台边界安全下一代防火墙，并且满足业务性能，在服务期内，服务商确保所提供的工具或设备系统版本为最新版本 |
| 2 | 上网行为分析及管控服务 | 1 | 年 | 为院方提供为期一年的上网行为分析及管控服务，在提供服务的过程中，由服务方免费提供对应的服务设备，要求至少具备1台上网行为管理，并且满足业务性能，在服务期内，服务商免费提供产品的规则库和软件升级，确保规则库为最新版本 |
| 3 | Web安全防护及保障服务 | 1 | 年 | 为院方提供为期一年的Web安全防护及保障服务，在提供服务的过程中，由服务方免费提供对应的服务设备，要求至少具备1台Web安全防护设备，并且满足业务性能，在服务期内，服务商免费提供产品的规则库和软件升级，确保规则库为最新版本 |
| 4 | 全网安全态势分析服务 | 1 | 年 | 为院方提供为期一年的全网安全态势分析服务，在提供服务的过程中，由服务方免费提供对应的服务设备，要求至少具备1套态势感知分析平台+态势感知探针，并且满足业务性能，在服务期内，服务商免费提供产品的规则库和软件升级，确保规则库为最新版本 |
| 6 | 运维安全和综合审计服务 | 1 | 年 | 为院方提供为期一年的运维安全和综合审计服务，在提供服务的过程中，由服务方免费提供对应的服务设备，要求至少具备数据库审计、日志审计、运维安全管理系统（堡垒机）功能的1台设备，并且满足业务性能，在服务期内，服务商免费提供产品的规则库和软件升级，确保规则库为最新版本 |
| 7 | 终端安全保障和恶意代码防范服务 | 1 | 年 | 为院方提供为期一年的终端安全保障和恶意代码防范服务，在提供服务的过程中，由服务方免费提供对应的服务设备，要求至少具备1台终端安全管控设备，根据院方终端数量进行部署和安排，并且不间断提供服务，在服务期内，服务商免费提供产品的规则库和软件升级，确保规则库为最新版本 |
| 8 | 远程网络安全巡检 | 12 | 次 | 每个月完成一次安全巡检，并出具巡检报告 |
| 9 | 漏洞扫描 | 4 | 次 | 每个季度完成一次漏洞扫描，并出具漏洞扫描报告 |
| 10 | 网络安全渗透测试 | 1 | 次 | 针对做过等保备案的业务系统，提供一次渗透测试服务，并出具渗透测试报告。 |
| 11 | 网络安全应急演练 | 1 | 次 | 完成一次网络安全应急演练服务，并提供网络安全应急演练总结报告。 |
| 12 | 网络安全加固 | 1 | 次 | 针对信息系统中存在的网络设备、安全设备、服务器、终端的安全隐患，指导进行安全加固 |
| 13 | 网络安全培训服务 | 2 | 次 | 为信息科提供网络安全相关培训 |
| 14 | 网络安全应急响应服务 | 按需 | 次 | 按需进行服务（发生安全事件），不限次数，响应时间要求7\*24\*365，2小时内抵达现场。 |

## 服务要求

### 边界安全防护及保障服务要求

投标人所提供的边界安全防护及保障服务应根据对院内网络架构情况的了解，选取适当的边界位置布置对应的安全设备，从而对边界起到安全防护的效果，在为期一年的服务期内，持续保障院内边界网络的安全性。

通过边界安全防护及保障服务，实现如下层面的服务效果：

**威胁看得到——可视**

通过边界防护服务可以分析出网络中的应用类型、应用内容中的威胁和攻击、威胁带走的数据内容，并能实现报表呈现，实现真正的 L2-7 层统一的安全可视化；

通过主动或者被动流量检测，及时发现业务漏洞，即使没有攻击也能找到业务中潜在的风险；

通过攻击与业务漏洞的关联分析，可以帮助您准确地找到有效攻击，清楚网络和业务运行的安全状况。

**攻击防得住——双向**

通过边界防护服务可以具备 L2-7 层的攻击防护技术，不仅可以防护外部攻击，还能检查服务器/终端外发流量是否有风险，弥补了传统安全设备“只防外、不防内”的不足。

同时，可以检测服务器外发数据是否有泄密或篡改风险，以及内网的终端电脑是否被黑客控制、形成僵尸网络。

### 上网行为分析及管控服务要求

投标人所提供的上网行为分析及管控服务应实现以下要求：

用于提高工作人员工作效率和办公用户体验：通过合理的权限划分，封堵与工作无关的应用和网址，从技术手段上约束工作人员，以此来杜绝上班时间做与工作无关的事情，提高工作人员工作效率。同时，通过限制大量占用带宽的无关应用（ P2P 应用、网络流媒体等），保障带宽不被侵蚀，保证核心业务系统正常运转，提高办公用户的上网体验。

用于规避违法风险，满足合规要求：通过对用户上网行为的监管，记录用户上网痕迹，满足公安部 82 号令的合规要求。一旦出现违法事故，能够快速准确的定位违规终端设备，提取上网记录进行溯源举证。

### Web安全防护及保障服务要求

投标人所提供的Web安全防护及保障服务应针对院内的Web业务系统提供以下几个维度的安全防护。

**基于安全事件周期的设计**

攻击防护不可能做到 100%安全。Web 系统的安全建设必须贯穿到整个 Web 安全事件周期中，从事前、事中、事后三个维度分阶段进行防护。

提供事前策略自检、事中攻击防护、事后防止篡改的整体安全防护。

事前风险自检：在配置完安全策略后，可以提供 Web 漏洞扫描功能，查看系统还存在哪些安全策略漏洞和隐患，也可通过云端安全服务对网站进行持续的监测；

事中攻击防护：2-7 层完整的应用层安全防护，包括：Web 攻击防护、漏洞防护、病毒防护等；

事后快速响应：针对网站黑链，网页篡改，网站植入后门等恶意行为进行主动的探测和处置，云端安全服务保持 7\*24 在线响应。

**基于黑客攻击手段的安全防护**

传统的 Web 安全防护采用的是防火墙+IPS+WAF 割裂式的安全防护体系，针对各类的攻击总是被动的增补相应功能的安全设备。而对于 Web 安全防护不是单一攻击手段的防护，而需要对黑客攻击动机与时机进行分析，基于黑客的攻击过程的每一个环节进行统一防护。

因此本次基于黑客攻击过程的完整Web系统安全防护，针对黑客入侵三步曲即扫描、入侵、破坏进行统一的安全防护：

扫描：提供网站防扫描、口令暴力破解、关键 URL 防护、应用信息隐藏等；

渗透：提供强化的 Web 攻击防护（防 SQL 注入、OS 命令注入、XSS 攻击、CSRF 攻击）、多对象漏洞利用防护等；

破坏：提供 Webshell 后门检测、黑链检测、抗 CC 攻击、恶意脚本上传过滤、僵木蠕检测、异常流量清洗等；

### 全网安全态势分析服务要求

投标人所提供的全网安全态势分析服务应实现以下几个要求：

**资产识别与脆弱性评估**

资产自动发现：以主动+被动的形式相结合，自适应的识别内网网段和外网网段的终端、服务器等。

服务器信息识别：自动识别服务器的资产信息，如操作系统、开放的端口等，可用于发现影子资产，或配合定期巡检，可避免业务频繁更新带来的安全问题（如遗漏、漏配等）。

风险端口/应用：识别服务器资产开放的风险端口及端口被使用情况（如标准端口跑非标准协议），识别因暴露风险应用访问方式（如RDP、SSH、数据库）被非法连入的情况，即使非标准端口亦能识别具体应用。

组织结构层级划分：对分支单位等进行多级维度的划分，并可对资产进行划分，自定义设置资产的属性，方便定位资产并进行管理。配置的组织层级情况还与全网安全态势感知展示相结合，展示整体安全情况。

实时漏洞分析：对经过设备的应用流量，对流量进行对应的应用解析，对解析后的应用数据匹配实时漏洞分析识别库，发现服务器存在的操作系统、Web通用软件或框架、Web应用、协议等可能存在的漏洞。同时提供内置和自定义弱密码库，对用户指定的服务器进行弱密码分析，分析服务器是否存在弱密码风险。

资产运行检测：基于SNMP方式对资产、设备进行运行信息和监控，实时展示CPU、内存、磁盘、上下行流量等信息，并形成历史记录。可与历史记录进行对比，供管理员分析设备资源异常情况。

**日志采集与关联分析**

支持对主流的网络设备、安全设备、操作系统、中间件、应用系统等设备的日志进行采集，采集方式支持Webservice、Syslog、WMI、Agent、JDBC、FTP等接入方式，同时平台的日志采集具备良好的可扩展性，可支持自定义正则，快速兼容新的设备类型。

平台接收到日志后，使用与上报日志设备匹配的范式对日志内容提取、整理为统一标准格式，如日志生成时间、IP端口信息、用户信息、协议、日志等级、日志内容等。对标准化后的日志执行清洗无效数据、去除重复数据、按时间维度排序等整理。整理后的日志便于日志分析，提升分析性能和准确性。

平台内置安全规则库、威胁情报、专家经验库、关联分析、自定义关联规则等方式识别日志中各类安全威胁，同时通过大数据和深度挖掘等技术提取有效安全告警，关联生成安全事件，并以可视化形式展示。

1. 内置6大类关联分析规则，涵盖主机可疑行为、账号新增/修改/删除、暴力破解入侵、账号提权、高危操作、网站攻击，识别高危安全告警。
2. 基于行为和状态的机器学习，对IP、用户状态和行为建模，识别用户权限变更、用户越权、非法操作等异常事件。

基于状态、时序、端口、行为活动等关联分析，根据IP、用户在时序上的状态变化、行为操作、开放端口属性变化等关联识别未知异常事件。

**多维度威胁检测**

黑客之所以能入侵企业内网，有时并不是凭借多么高明技巧，相反，对网络安全事件进行复盘总结发现，许多黑客入侵企业内网给企业造成损失，凭借的仅是一些传统的、简单的手段。对于企业的网络安全建设而言，检测技术由简单和复杂之分，但对于检测黑客入侵而言，基础检测能力同样是至关重要的。基础检测能力是指针对那些传统的、常见的异常流量进行检测的能力，主要包括异常会话检测、Web应用安全检测、敏感数据泄密检测。

异常会话检测可实现外联行为分析、间歇会话连接、加密通道分析、异常域名分析、上下行流量分析等在内的多场景网络异常通信行为的分析检测，而Web应用安全检测针对B/S架构应用，应用范围包括ASP、PHP、JSP等主流脚本语言编写的WebShell后门脚本上传，检测SQL注入、XSS、系统命令等注入、CSRF攻击、恶意爬虫攻击、文件包含、目录遍历、信息泄露攻击等攻击，对主流网站内容管理系统CMS进行安全防护。而敏感数据泄密检测能力则是通过对敏感信息的自定义，根据文件类型和敏感关键字进行信息过滤和检测。

黑客绕过传统防护措施之后，往往是先选择潜伏和隐藏，比如病毒是黑客入侵内网的常用工具之一，病毒程序进入系统之后一般不会马上发作，而是在几周或者几个月甚至几年内隐藏在合法文件中，对其他系统进行传染且不被发现，大部分病毒的发作是通过HTTP协议访问特定的URL来获取或提交信息来完成的，还有病毒会通过DNS查询出某个域名的IP，然后再与该IP建立连接交互数据。再比如，僵尸网络为了同C&C服务器通信，会通过请求DNS来获取C&C服务器对应的IP，这些URL地址和域名对应IP的主机通常就是为病毒提供交互信息的关键所在，有效识别出这些主机就能够阻断内网病毒和外界的连接。这些攻击方式比传统的攻击方式更加复杂和隐蔽，而深度检测能力就是针对这种具有隐蔽性的恶意行为进行检测。

深度检测能力可提供网络流量的会话级视图，根据网络流量的正常行为轮廓特征建立正常流量模型，判别流量是否出现异常，可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描、端口扫描、ARP欺骗。同时深度检测能力还包含口令暴力破解检测、弱密码扫描检测、黑链检测、终端病毒/恶意软件检测。针对僵尸机、病毒程序的发作需要通过和外界C&C服务器通信来实现发作的特点，深信服安全感知平台独有的融合马尔科夫模型和信息熵的DGA检测算法，利用机器学习的方法识别域名是否由算法生成，根据随机性估计域名信誉值，从而检测出与恶意IP地址相关的流量。

在企业网络环境中，当某员工没有值夜班的情况下，该员工主机在凌晨4点对业务服务器进行访问就属于的访问异常。过去用户业务访问控制和Web业务访问控制主要靠规则实现，但由于个体行为模式存在较大差异，同时黑客的攻击越来越倾向于伪装成正常用户行为从而避开访问规则，因此基于规则的控制策略已经难以有效应对访问异常。而机器学习算法恰恰能够对多样化的用户行为模式和Web访问模式进行建模，从而达到更好的检测效果。

安全感知平台的用户业务访问异常检测基于用户历史行为和用户之间的行为相似性，相似性作统计分析，利用机器学习进行建模，从而对用户和主机等实体进行分析（UEBA）、识别出用户对业务系统的异常访问，进而发现用户凭据被盗、用户主机失陷等潜在威胁。而Web业务访问异常检测使用马尔科夫随机过程和贝叶斯递归估计，结合其它机器学习算法对Web业务的交互行为进行分析和建模，从而检测出Web业务的各类攻击，如数据泄漏、WebShell、内网数据代理转发等高危行为。

**事前事中事后全方位检测**

1. 失陷主机检测

黑客攻入内网之后，会在被攻陷主机上放置木马、后门，从而达到对该主机控制的目的。而在黑客控制大量失陷主机之后，还会对目标主机发起DDOS攻击、扫描暴破等恶意行为。主机失陷是黑客进入内网的第一步，及时发现失陷主机就能够尽早的扼制黑客的进一步行动，从而确保企业网络环境的安全。

目前已知的失陷主机检测算法有20多种，如基于规则、基于库的算法等。安全感知平台内建的算法能够对病毒行为、异常外联行为、黑客常用攻击行为等特征进行分析，该算法融合了fast-flux识别、iForest、主机网络流量模型、协议模型学习，同时结合大数据关联分析引擎提供的联动分析以及DGA域名判别构建融合检测模型，从而及时发现失陷主机。

1. 横向威胁感知

对于大多数用户来说，核心业务系统都会部署大量的安全防护系统和制定详细的管理保障制度，非公众服务的系统甚至根本不会暴露在攻击者直接可访问的视野当中。所以，黑客和攻击者往往难以直接对这些系统进行渗透和攻击，于是就出现了经典的APT“攻击渗透-控制跳板-横向移动-控制目标-窃取破坏”过程，通过攻击和控制防御薄弱的内部非核心资产，以其为跳板进行渗透和攻击。

横向威胁检测将监测分析的对象定位在内部业务和资产的行为逻辑分析上，实时监测系统之间的访问请求、数据包内容和业务逻辑，包括：

* 进行基于特征匹配的攻击检测，即扫描、渗透等传统攻击手段
* 基于白名单策略的违规检测，发现资产行为偏离预设的安全策略
* 基于UEBA技术的行为异常检测，发现资产行为逻辑与自身安全基线或同类资产安全基线验证偏离
* 常见的风险远程登录、数据库请求行为

通过这些资产的行为特征判断其是否出现被黑客控制并成为内部攻击跳板。由于攻击渗透和控制跳板的过程多数情况下总是基于0Day和未知威胁的新型攻击手段，但内部横向移动的过程必然伴随受控资产的访问请求、数据包内容和行为逻辑异常，可以作为有效的APT攻击检测手段，通过在横向移动阶段检测和阻断攻击，可以有效防止核心业务失陷和敏感信息失泄密。

1. 外联威胁感知

传统的网络安全设备和解决方案只注重功能，即便是专业的安全运维人员也难以实时了解整个网络的安全状态。医院需要的不只是安全的网络环境，还需要以简单、直观的方式了解网络环境的安全状态，比如对于事后检测而言，医院关心的重点是其核心业务服务器是否已经失陷，医院的业务系统是否存在外连情况、与哪些国家和省份外连、外连访问存在什么风险和态势、如何解决等等。

从业务服务器的外发流量进行检测是判断该服务器安全状况的一个有效手段。失陷的服务器一般会表现得与正常运行时不一样。通过分析服务器外连的行为，建立服务器正常运行的模型，以此为基准检测服务器的异常运行情况。可视化平台将医院的业务系统外连情况进行可视，让管理员直观感知业务系统动态，形成完整的“外连态势觉察、外连态势理解、外连态势预测以及外连风险解决”的闭环，在交互体验上，几乎零操作零学习成本，结合大屏幕投放，清晰而直观的做到“安全态势可感知、安全价值可呈现”。

1. 成功的事中攻击

典型的APT攻击过程，攻击者往往不会止步于控制目标主机或系统，而是会通过该系统作为媒介，实施进一步的攻击和渗透。所以，在进行安全事件的分析和研判过程中，就不仅仅需要对攻击的来源和方式进行分析，从而确定当前的应急处置方案和事后的安全加固策略，还需要对其可能的影响面和攻击手段进行跟踪和分析，确保这一成功的事中攻击尚未对其他更多的资产造成实际影响，或者如果造成影响了，进一步确认危害和启动相应的处置流程。

1. 外部风险访问

对于多数单位来说，来自外部的攻击者依然是其面临的主要威胁主体，所以对来自互联网或分支机构等不可信/相对不可控网络的数据进行深度分析和检测，关联其直接访问逻辑、访问请求和行为特征，对目录遍历、ftp爆破、知名漏洞利用攻击、远程文件包含、SQL注入、网站登录爆破、 WebShell文件上传等多种主流的高风险渗透攻击进行全面检测。

### 运维安全和综合审计服务要求

投标人所提供的运维安全和综合审计服务应实现以下效果：

通过集中化运维管控、统一运维管理、身份认证与权限控制、运维访问合规性控制、运维过程实时监看、自定义应用发布等功能，为数据中心运维构建一套完善的事前预防、事中监控、事后审计的安全管理体系。通过建立面向用户集中、主动的运维安全管控模式，从而达到降低人为安全风险，满足合规要求，保障单位效益的目的。

数据库安全审计实现全程记录网络中一切对数据库的访问行为。实时监控数据库用户的访问行为，通过对用户访问数据库行为进行记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，并可以根据用户设置等信息有效的评估数据库潜在风险，加强内外部网络行为记录，提高数据资产安全管控能力。

主机安全审计实现能够对计算机进行全面的监控，包括对文件操作行为、外接设备挂载及卸载行为、打印刻录行为以及网络访问行为等进行实时监控，做到事中监控、事后审计，全方位帮助单位加强计算机的安全防护及管理，有效防止泄密事件的发生。

### 终端安全保障和恶意代码防范服务要求

投标人所提供的终端安全保障和恶意代码防范服务应实现以下效果：

**终端资产的全面管理**

全网终端资产的全面盘点，包含业务服务器的终端和用户 PC 的终端。盘点每台终端设备的名称、IP 地址、MAC 地址、所属组织、责任人、资产编号、资产位置等。每一台的终端上的资产信息清晰，每一个安全事件责任到人，使得安全管理能落实到位。

**终端安全的合规检查**

每一个组织都有自己的终端安全合规要求，特别是等级保护的合规要求，对主机的安全要求。终端安全合规审查依据等级保护的主机安全要求进行设计，对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等策略进行合规性审查，满足企业建设等级保护系统的主机安全要求。

**勒索病毒的实时防御**

勒索病毒通过加密文件的方式，要求中招者支持一定数额的赎金。这种攻击方式越来越流行，国内几乎每天都有发生。非常精准的识别不同的勒索软件家族，并通过专业分析识别出种种勒索病毒感染行为和加密特征，对最新的勒索软件进行有效的查杀，防止用户感染最新的勒索软件。

**无文件攻击的高级防护**

无文件攻击方式利用PowerShell的命令加载恶意代码，利用无文件落地方式绕过传统杀软的检测与防护，该方式快速且具有隐秘性，不易被察觉，被广泛利用于挖矿，窃密等非法行为上。准确拦截PowerShell的对恶意代码的执行，实现实时准确阻断，防止用户主机被利用破坏。

**入侵攻击的主动检测**

终端主机被入侵攻击，导致感染勒索病毒或者挖矿病毒，其中大部分攻击是通过暴力破解的弱口令攻击产生的。主动检测暴力破解行为，并对发现攻击行为的 IP 进行封堵响应。针对 Web 安全攻击行为，则主动检测 Web 后门的文件。针对僵尸网络的攻击，则根据僵尸网络的活跃行为，快速定位僵尸网络文件，并进行一键查杀。

**访问关系的策略控制**

当前各种感染性病毒大部分都是通过网络进行传播，从而导致大范围内的终端中招，影响范围较广。微隔离支持网络访问关系策略的配置，可以实现业务域之间或者终端之间的网络隔离，从源头上杜绝病毒的传播，减少用户的损失，进一步保证终端的安全。

**文档宏病毒的精准检测**

宏病毒经常通过各式各样的文档进行传播，具有破坏文档、损害系统等严重危害。基于对大量宏病毒的研究，构建了强大的宏病毒检测规则，能够更加精准的识别隐藏于文档中的宏病毒。并通过高效的手段去除这些恶意宏，达到修复文档的目的，保护文档和主机安全。

### 远程网络安全巡检服务要求

投标人所提供的远程网络安全巡检服务应依据《信息安全技术信息系统安全等级保护基本要求》，结合院内的实际安全需求，进行定期或不定期的多种工具的交叉远程网络安全巡检，了解系统及服务器存在的安全隐患，建立安全可靠的WEB应用服务，改善并提升应用系统抗各类WEB应用攻击的能力(如：注入攻击、跨站脚本、钓鱼攻击、信息泄漏、恶意编码、表单绕过、缓冲区溢出等)；提供详细的安全评估报告，包括扫描的漏洞详细信息、安全加固建议等，对所有漏洞弱点的相关背景提供详细描述、引用，以及相应的修复和改进建议。

通过主动防御，及时发现信息系统存在的安全隐患以及发生的安全事件，使得管理员可以更及时快速地处理安全事件，制定相应的预防措施，防患于未然。

提前消除安全事件带来的影响，降低安全事件给医院带来的损失和风险。

周期性的远程网络安全巡检分析报告，提供专家建议，为医院提供信息系统安全整体风险状况以及安全发展趋势。

### 漏洞扫描服务

投标人所提供的漏洞扫描服务应结合院方的实际安全需求，通过定期开展信息系统漏洞扫描服务，及时发现存在的安全问题和薄弱环节，分析面临的安全威胁和风险，并对发现的安全隐患提供改善建议，协助指导院方落实防范对策和改进措施，以加强网络与信息系统安全管理和技术防护，促进安全防护能力和水平提升，预防和减少重大信息安全事件的发生。漏洞扫描服务对象范围应涵盖网络设备、安全设备、主机操作系统、数据库系统、应用系统等信息系统元素。

* 通过持续化的检查，及时发现信息系统存在的安全漏洞、安全隐患以及可能发生的安全事件，可以快速地进行修补改进，防患于未然；
* 可以更为全面的掌握信息系统的安全状况与安全发展态势；
* 提前消除安全事件带来的影响，降低安全事件给医院带来的损失和风险；
* 帮助用户顺利开展安全运维工作，排除技术障碍；
* 周期性的安全分析报告，提供专家建议。

### 网络安全渗透测试服务要求

投标人所提供的网络安全渗透测试应为通过模拟黑客可能使用的攻击方式和漏洞挖掘行为，对目标信息系统的安全进行深入安全检测的一种评估方法。通过渗透测试，直观的让单位信息系统管理人员了解自身信息系统所面临的安全问题，看到对这些漏洞的利用或攻击可以产生什么样的破坏及影响。同时，为我单位信息系统管理人员提供安全加固建议，及时采取必要的安全防范措施，帮助其更好的保护信息系统，保证信息系统安全、稳定运行。

### 网络安全应急演练服务要求

投标人所提供的网络安全应急演练服务应根据《中华人民共和国网络安全法》的要求，每年都至少要针对自己所负责的信息系统进行一次网络安全应急演练工作。通过网络安全应急演练查找应急预案中存在的问题，进而完善应急预案，提高应急预案的实用性和可操作性；通过网络安全应急演练，检查应对网络安全事件所需应急队伍、物资、装备、技术等方面的准备情况，发现不足及时予以调整补充，做好应急准备工作；增强演练组织单位、参与单位和人员等对应急预案的熟悉程序，加强配合，提高其应急处置能力；通过开展攻防演练，普及网络安全知识，不断增强网络安全管理的专业化程度，提高全员网络安全风险防范意识

网络安全应急演练服务，针对信息系统环境在运行过程中或者操作过程中可能出现的紧急问题，建立健全网络与信息安全运行应急预案工作机制、模拟布置出一套或多套安全威胁场景，考验单位相关部门和人员的应急处置能力和应急管理能力，其目的是验证相关组织和人员应对网络和信息安全突发事件的组织指挥能力和应急处置能力，保证各项应急指挥调度工作迅速、高效、有序地进行，满足突发情况下网络与信息系统运行保障和故障恢复的需要，确保信息系统安全畅通、缩短系统中断时间、减少业务损失风险

### 网络安全加固服务

投标人所提供的网络安全加固服务应根据院方需求，对院方所备案的信息系统，根据网络安全等级保护测评的合规性要求，对系统所涉及的网络设备、安全设备、服务器操作系统、终端等的配置进行最大程度的配置整改，以便于关于配置方面的测评要求可以最大程度满足要求，同时提升网络自身的安全性。

### 网络安全培训服务要求

投标人所提供的网络安全培训服务应根据院方需求，结合信息化发展的攻防形势，采用演讲、实战演示等方式对人员进行培训。培训课程的内容、时间、地点将最大限度地根据甲方要求而设定。

### 网络安全应急响应服务要求

投标人所提供的网络安全应急响应服务应当信息系统安全事件发生时，指导院方进行信息安全事件应急响应服务，参与现场应急响应支持工作，通过应急响应对安全事件发生的信息系统进行安全事故分析，以及时解决安全故障、修复系统，最大限度的保护服务器和数据，最快的速度恢复访问和网络畅通，使信息系统恢复正常工作，尽可能挽回或减少损失。

# 工期及服务地点

服务工期：自院方通知进场并开始服务之日起一年内。

项目地点：海南省海口市。

# 付款方式

本项目采取按服务季度进行付款，每个服务季度完成合同约定的相关服务并提交服务文档，经医院信息科确认后，凭据服务提供方（乙方）提供有效发票进行支付该服务季度的服务费（合同总金额1/4）。

# 项目验收标准

针对本项目1.2章节的“服务内容”，至少出具以下交付成果：

1. 按1.3章节的“服务要求”，完成全部工作内容并出具相应的服务报告；
2. 12份远程安全巡检报告及相应过程文档；
3. 4份漏洞扫描报告及相应过程文档；
4. 1份渗透测试报告及相应过程文档；
5. 1份网络安全应急演练总结报告及相应过程文档；

6、1份网络安全加固报告及相应过程文档。