**海南省医科大学第二附属医院**

**安全防护服务采购需求书**

# 服务范围及内容

## 服务类别

|  |  |  |
| --- | --- | --- |
| **序号** | **服务类别** | **服务内容** |
| 1 | 安全防护服务 | 根据医院目前信息化安全建设的情况，结合国家政策对信息化安全建设的要求，为了提高信息安全防护水平，向医院提供相应的安全服务，其内容包含服务工具的使用、服务工具规则库的升级以及巡检服务、维护服务等相关配套服务。 |

## 服务要求

### 1.2.1互联网边界安全服务要求

我院90%以上的员工需要每天使用PC终端办公，这些终端是和互联网进行“信息交换”的重要节点。但由于员工安全意识不足、能力水平参差不齐，使我单位的互联网出口安全存在一定隐患。据了解，80%的安全事件来自于终端，终端已经成为黑客的战略攻击点。

由于我单位的员工可以通过PC访问互联网，同时也可以访问数据中心的业务系统，若终端安全得不到保障可能引起对数据中心业务系统的安全威胁。现阶段，黑客攻击的目标是为了获取有价值的“数据”。控制终端以后，可以直接种植如勒索病毒进行敲诈勒索。更严重的是，我单位的存储着重要“数据”的服务器也可能因为终端被控制遭受被影响。受控的终端将成为黑客的跳板，通过失陷主机横向扫描内部网络，发现我单位网络中重要的服务器，从而对这些重要服务器造成威胁。

本次通过互联网边界安全服务需要解决以下几个问题：

（1）失陷主机

本次服务需要防止访问互联网用户被互联网上的不法分子控制的风险；防止被控制的终端电脑被用来向外部发起攻击引起法律纠纷的风险；防止僵尸网络对内部系统造成拒绝服务攻击、对内部系统造成信息泄露等危害的风险。

（2）高级持续威胁

本次服务需要拥有持续性的高级威胁检测能力。高级的攻击往往攻击目标明确、时间周期比较长、采用的攻击方法比较多、而且隐蔽性很好。而研究发现，黑客进行APT攻击最常采用的跳板就是僵尸网络，大量的僵尸主机给了发动APT攻击的黑客很多选择，并且为了达到继续渗透、监视、敏感数据窃取等目的，黑客会让这些僵尸机很好的潜藏起来，减少暴漏的可能。

（3）风险可视化

为了更迅速的闭环网络安全事件，本次服务需要提供感知风险能力、风险可视化能力，威胁影响面分析能力。

### 1.2.2互联网边界上网行为监测与审计服务要求

投标人所提供的互联网边界上网行为监测与审计服务解决以下问题：

1. 应用和内容不可视，存在风险

大量新应用和老应用的新版本，给应用识别与管控以及后续的运维带来巨大的挑战，让网络难管控，难运维。另外，即使是同一个应用也可能具有两面性，他们有“好”的功能，也可能有“坏”的功能，“好”功能具有实用性，而“坏”功能具有风险性，因此，此类应用的管控成了一个两难的问题。

1. 网络流量识不全，控不住

由于流量没有明显的协议特征，再加上其带宽侵蚀性的特性，造成流量的全流量识别困难。

### 1.2.3 服务器边界安全服务要求

本次通过服务器边界安全服务需要解决以下几个问题：

1. 边界防御面临失陷的风险

因为服务器区域面临更高级的安全威胁，有太多的攻击手段可以绕过传统的防御工事，比如各种欺诈、0Day攻击、APT攻击等。而攻击者一旦突破了边界，就会在数据中心内部潜伏下来，通过控制一些主机，进行隐蔽的、慢速的，通过不容易被发现的横向移动的方式持续对数据中心的数据进行持续的窃取。

1. 数据中心业务多，安全管理复杂

IT已经成为提升我单位业务效率必不可少的重要手段，“业务型的IT”使得我单位服务器区域肩负的职能越来越高。自服务器区域建设已来，已上线大量的应用和系统，使得服务器区域业务的复杂度也越来越高。业务的复杂对安全管理提出了更高的挑战，如何应对业务快速上线带来的安全管理的挑战？如何准确的了解数据中心安全态势？如何及时发现数据中心存在的安全隐患？并通过简单有效的手段及时解决问题？成为我单位数据中心安全管理的几个核心问题。

### 1.2.4 DMZ区域Web应用安全防护服务要求

投标人所提供的DMZ区域Web应用安全防护服务需要解决以下几个问题：

1. Web应用安全

Web业务因其运行在互联网常常成为攻击的入口。业务高度集成，逻辑复杂导致安全问题频发。攻击者攻击成功后会修改业务数据，中断业务运行，窃取和加密业务数据，并遥控病毒木马持续横向扩散感染其他业务。因此需要有效的方法来阻断各类Web攻击行为。

1. 网页挂马问题

网页挂马也是利用Web攻击造成的一种网页篡改的安全问题，相对而言这种问题会比较隐蔽，但本质上这种方式也破坏了网页的完整性，用户访问挂马网页就会把木马病毒带入自己的电脑。网页挂马会导致网站的最终用户成为受害者，网站建设方也会因此带来经济信誉损失，还可能因为是攻击者潜在的帮凶问题而承担相应的法律责任。

1. 敏感信息泄露问题

这类安全问题主要是因为Web攻击、系统漏洞攻击等攻击手段操作后台数据库，导致数据库中储存的用户资料、身份证信息、账户信息、信用卡信息、联系方式等敏感信息被攻击者获取。这对于企事业单位而言都是巨大的伤害，可产生巨大的经济损失。

### 1.2.5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需要解决以下几个问题：

1. 业务运维管理风险

信息安全保障的是核心业务和数据资产，如果我们都不清楚被保护的主体包含了哪些系统、哪些资产以及他们之间是如何交互、如何互相访问的，那么就谈不上建立针对性的安全保障体系。越来越多的黑客攻击已经开始基于业务逻辑和业务流开始构建自己的攻击过程，例如著名的孟加拉央行劫案，都不是通用安全防护设备能够应对的；而来自恶意内部员工的窃密和攻击，多数时候甚至都不是严格意义上的网络攻击行为，更加无法依赖标准化交付的安全产品实现。因此，我院目前缺乏有效手段主动识别新增业务、看不清的新增资产产生安全洼地、看不清的业务关系使业务安全防护失效。

1. 难以发现潜伏威胁隐患

近年来，来自外部的攻击手段也变得更高级、更迅速、更隐蔽。我院目前看不见的内部横向攻击、看不见的违规操作、看不见的异常行为。

1. 缺乏整体安全感知能力

安全技术保障体系和安全治理管理体系的脱节，主要是指安全服务工具发现的安全问题缺乏相应的检测分析能力和追溯能力，无法提供有效的事件应对处置闭环；而安全治理所需系统状态、安全态势也缺乏相应的感知和可视手段，无法实现真正的看的到和看的懂。

### 1.2.6等保合规运维审计管理服务要求

投标人所提供的等保合规运维审计管理服务需要解决以下几个问题：

1. 堡垒机运维需求：提供账号管理、授权管理、认证管理、审计管理等功能；
2. 数据库审计需求：数据库审计、数据库行为统计与分析、数据库安全防护等功能；
3. 日志审计需求：日志采集、日志处理与标准化、日志分析与审计等功能；

### 1.2.7终端检测与响应系统服务要求

投标人所提供的终端检测与响应系统服务需要解决以下几个问题：

（1）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。

（2）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。

（3）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，每天都有客户反馈中招。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。

（4）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。

（5）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。

（6）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。

### 1.2.8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，使得客户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，降低安全事件给客户带来的损失和风险。

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

### 1.2.9安全运营服务要求

投标人提供40个资产的安全运营服务，由安全运营中心帮助客户进行7\*24小时持续安全监测，时刻洞悉网络的事件根因，在威胁未发生之前实现最大化精准预警，并进行安全策略调整；对已确定的安全威胁持续监测，并进一步验证策略的有效性；从而实现主动快速响应，精准拦截黑客攻击，保障网络安全的目标，每年四次服务进展汇报。

### 1.2.10现场漏洞扫描服务要求

漏洞扫描服务，服务方使用自主知识产权的自动化漏洞扫描工具，对服务范围内的各种软硬件设备进行系统层、网络层、数据库层、应用层的全面的扫描与分析，扫描设备检测规则库及知识库涵盖了CVE、CNCVE、CNVD、CNNVD等标准，全面快速扫描完成后，人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄漏及配置不当等脆弱性问题。最终出具准确有效的扫描报告，并针对扫描结果提供修复建议，协助单位进行修复加固。

### 1.2.11现场渗透测试服务要求

通过红队模拟进攻方式，在不损害单位利益的情况下，根据黑客攻击的思维，参考黑客攻击的手段，指定攻击的路线，尽可能全面发现导致黑客入侵的所有途径；对预审系统资产发现并深入挖掘漏洞，从而实现横向渗透，进而实现整个网络的夺权的思路，达成攻击目标。

### 1.2.12网络应急演练服务要求

应急演练服务根据定制化的演练目的和场景，基于现有应急处置体系，组织开展应急演练工作，进一步提高客户网络安全应急处置能力。主要服务内容包括：制订应急演练方案、准备应急演练环境、实施应急演练、优化应急预案、完善应急处置体系等。

### 1.2.13网络安全加固服务要求

安全加固指导服务针对在安全评估、应急响应、攻防对抗过程中发现的安全风险、不合规项、漏洞扫描报告等提供具体落地的加固方案并指导客户进行加固整改。服务包括安全漏洞漏洞服务与基线安全加固指导服务，指导加固对象包括系统漏洞、中间件、数据库等相关软硬件资产。

### 1.2.14网络安全意识培训服务要求

安全意识培训旨提升公司内部员工安全认知，让员工认识到信息安全意识不足对组织可能造成的危害，传导应正确恪守的行为方式；通过全员安全意识的理论培训和案例分析以及关键行为上的最佳实践指导，让信息安全“人防“保障有效支撑业务高效稳定运行。培训内容包括普通员工的上网安全、邮件安全、通信安全等常见的安全意识内容。

### 1.2.15网络应急响应服务要求

应急响应服务根据应急预案对发生的安全事件快速作出响应，根据安全事件等级，第一时间采用现场或远程的方式对安全事件进行应急处置。安全事件包括：非授权访问、信息泄密、拒绝服务、非法登录、病毒感染，权限篡改等相关攻击行为。

### 1.2.16安全托管式服务

提供一套通过“人机共智”的方式整合技术、专家和流程，帮助用户快速扩展安全能力，实现 7\*24H 持续监测“资产、漏洞、威胁、事件”四个网络安全风险核心要素，主动对发现的风险进行闭环处置，提升安全工作的效率，减轻安全运维工作的压力，帮助用户呈现安全工作价值。

## 服务组件

### 服务组件清单要求：

|  |  |  |
| --- | --- | --- |
| 序号 | 服务名称 | 服务要求 |
| 1 | 互联网边界安全服务 | 本项服务需提供互联网边界安全服务工具，服务期限1年，工具具体要求如下：  1、性能指标：网络层吞吐量≥40Gbps，IPS吞吐量≥3.5bps，全威胁吞吐量≥2bps,并发连接数≥420万，每秒新建连接数≥19万；  2、硬件指标：内存≥16G，硬盘≥256G SSD，接口≥16个千兆电口，≥6万兆光口；  3、该服务工具支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等；  4、该服务工具支持对应用的识别和控制；  5、该服务工具支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  6、该服务工具支持僵尸主机检测功能，该服务工具内置僵尸网络特征库，可识别主机的异常外联行为；  7、该服务工具内置漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  8、产品支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型；  9、该服务工具内置WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护； |
| 2 | 服务器边界安全服务 | 本项服务需提供一台下服务器边界安全服务工具，服务期限1年，工具具体要求如下：  1、性能指标：网络层吞吐量≥50Gbps，IPS吞吐量≥6bps，全威胁吞吐量≥3.5Gbps,并发连接数≥800万，每秒新建连接数≥35万；  2、硬件指标：内存≥32G，硬盘≥128G SSD+480G SSD，接口≥16个千兆电口，≥6万兆光口；  3、该服务工具支持对应用的识别和控制，应用类型包括数据库、远程登录、木马控制、FTP、代理工具等类型应用进行检测与控制；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  4、该服务工具支持僵尸主机检测功能，服务工具内置僵尸网络特征库，可识别主机的异常外联行为；  5、该服务工具内置漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  6、 支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  7、该服务工具内置WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护； |
| 3 | 互联网边界上网行为监测与审计服务 | 本项服务需提供互联网边界上网行为监测与审计服务工具，服务期限1年，工具具体要求如下：  1、性能指标：网络层吞吐量≥5.8Gbps，并发连接数≥50W，新建连接数≥10000，支持用户数≥4000；  2、硬件指标：1U规格；存储≥128G SSD+960G SSD；单电源；标配≥6个千兆电口，≥2个万兆光口；  3、该服务工具支持两台及两台以上设备同时做主机的部署模式；  4、该服务工具支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  5、针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  6、该服务工具支持通过OAuth认证协议对接，支持企业微信第三方账号授权认证；同时支持企业微信平台支持同步组织结构，用户通过企业微信认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  7、该服务工具支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  8、该服务工具支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为（包括包括钓鱼及恶意网站、漏洞利用、挖矿页面、恶意跳转、跨站脚本攻击和病毒文件等），避免用户网页资源被滥用，支持实时阻断和告警；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章） |
| 4 | DMZ区域Web应用安全服务 | 本项服务需提供一台DMZ区域Web应用安全服务工具，服务期限1年，工具具体要求如下：  1、该服务工具网络层吞吐量≥20G，HTTP应用层吞吐量≥800M，HTTP新建连接数≥10万，HTTP并发连接数≥350万。  2、该服务工具内存大小≥8G，硬盘容量≥128G SSD，单电源，接口≥8千兆电口+2万兆光口SFP+。  3、该服务工具支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  4、该服务工具支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上；  5、该服务工具支持Cookie攻击防护功能，并通过日志记录Cookie被篡改；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  6、该服务工具内置应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护； |
| 5 | 态势感知探针服务 | 本项服务需提供态势感知探针服务工具，服务期限1年，工具具体要求如下：  1、工具吞吐量≥1Gbps,标准1U，硬盘容量≥128GB SSD，标配≥6个千兆电口，2个千兆光口，配置单电源；  2、为了保证服务工具的兼容性和稳定性，态势感知探针服务工具需与本项目中“态势感知分析平台服务工具”为同一品牌；  3、该服务工具支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用，针对命令注入检测、SQL注入检测等类型支持自定义高检出、低误报模式；  4、该服务工具支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Media漏洞攻击、Network Device、Shellcode漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击、IPS云防护等服务漏洞攻击检测；  5、该服务工具支持5种场景的日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章） |
| 6 | 态势感知分析服务 | 本项服务需提供态势感知分析服务工具，服务期限1年，工具具体要求如下：  1、该服务工具采用外观≥2U的机架式服务器，配置8\*4TB 企业级硬盘、1块240G SSD系统盘，标配≥4个千兆电口，配置冗余电源；  2、该服务工具支持支持基于规则检测引擎、情报检测引擎、文件分析引擎、攻击行为分析引擎以及异常行为引擎查看攻击技术分布，支持针对具体攻击技术展示检测能力图谱以及受影响的风险资产（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）；  3、弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web空密码等（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）；  4、该服务工具支持web登录结果自定义，可根据登录行为检测是否登录成功，支持基于响应状态码、响应内容格式、URL、关键字、服务器IP地址、所属资产组等信息判定成功或失败的通用规则设置，支持机器学习引擎持续学习用户登录行为，生成登录成功规则模型。；  5、该服务工具支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，支持通过首页搜索框输入IP/域名/URL/端口/通信对进行搜索，同时支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员及时了解威胁的影响，并找到攻击入口点（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）；  6、该服务工具支持对服务器、客户端的各种应用发起的漏洞攻击进行检测；  7、该服务工具支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认、从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它4个维度对告警进行分类，帮助安全人员快速处置高危告警（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）；  8、该服务工具支持勒索专项检测页面，对勒索主题的安全告警进行展示和管理，支持以勒索病毒的感染途径/方式为维度进行分类，包括勒索常用端口、勒索常用漏洞、RDP爆破、感染勒索病毒、黑客勒索攻击、勒索C&C通信等维度，支持展示受害资产以及受害资产攻击数Top5，支持以列表的形式展示勒索事件，包括最近发生时间、威胁描述、威胁定性、勒索风险、威胁等级、受害者IP、攻击次数等信息（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）；  9、该服务工具支持挖矿专项检测页面，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者IP、攻击次数、威胁情报等信息（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）；  10、该服务工具支持与本次项目互联网边界安全服务工具、互联网边界上网行为监测与审计服务工具联动，包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章） |
| 7 | 等保合规运维审计管理服务 | 本项服务需提供等保合规运维审计管理服务工具，服务期限1年，工具具体要求如下：  等保一体机硬件平台：  1、规格：2U的机架式服务器，可以放入42U标准机柜；  2、处理器：配置≥2颗16核CPU，主频≥2.4GHZ；  3、内存：配置≥128GB内存；  4、硬盘：配置≥2块4T SATA数据盘、≥1块240G SSD系统盘（不占用前置硬盘槽）、≥1块480G SSD缓存盘；  5、为了提供更好的排障手段，该服务工具支持在平台内节点抓包分析分析功能，能够设置抓包的网口、过滤条件、文件大小等参数；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  6、业务、用户风险界面，支持针对业务、用户的风险事件进行分类，至少包含已经明确失陷的业务以及业务的威胁、脆弱性分析，同时能够针对已经实现、具备威胁与脆弱性不同阶段的安全事件进行等级描述、定位事件从何种安全组件上报，是否处理以及安全事件详情；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  **运维安全管理系统软件：**  1、性能指标：运维授权数≥300；  2、该服务工具支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入；  3、该服务工具内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  4、该服务工具支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  5、该服务工具支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人；  **数据库安全审计系统**  1、性能指标：数据库流量比≥300Mb/s；  2、该服务工具支持精细化日志秒级查询，通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  3、该服务工具支持TB级日志秒级查询、支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多SQL语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  4、该服务工具内置大量SQL安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等；  5、该服务工具支持数据库威胁分析：可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助企业快速溯源；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  **日志审计系统：**  1、主机审计许可证书数量≥300；  2、该服务工具支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析；  3、该服务工具支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用；  4、该服务工具支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  5、该服务工具支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章） |
| 8 | 终端检测与响应服务 | 本项服务需提供终端检测与响应作为服务期间的服务工具，服务期限1年，工具具体要求如下：  1、PC软件授权数量≥3500，服务器防病毒软件授权数量≥200；  2、该服务工具提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  3、该服务工具支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户；  4、针对Windows系统，该服务工具支持开发环境智能识别和调整，动态识别开发环境，安全的开发编译软件所使用的文件产生的风险支持设置成仅告警、不处置、不弹窗，规避开发场景编译软件拉取文件和代码卡顿、延时过久的问题；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  5、该服务工具支持客户端的错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴；  6、通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整客户端的资源占用（CPU、IO等），为业务让出资源，不卡业务，对业务零摩擦；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  7、该服务工具支持勒索可疑行为检测，通过行为AI能力对勒索信、命令行、修改文件等多种躲避式投放勒索病毒的高危高频场景进行精准告警和自动拦截；  8、该服务工具支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章） |

### 1.3.2 安全服务内容清单（服务期限：1年）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务描述** | **交付物** | **单位** |
| 1 | 漏洞扫描 | 漏洞扫描服务，服务方使用自主知识产权的自动化漏洞扫描工具，对服务范围内的各种软硬件设备进行系统层、网络层、数据库层、应用层的全面的扫描与分析，扫描设备检测规则库及知识库涵盖了CVE、CNCVE、CNVD、CNNVD等标准，全面快速扫描完成后，人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄漏及配置不当等脆弱性问题。最终出具准确有效的扫描报告，并针对扫描结果提供修复建议，协助单位进行修复加固。 | 《 漏洞扫描报告》 《人员保密协议》 | 4次 |
| 2 | 渗透测试 | 通过红队模拟进攻方式，在不损害单位利益的情况下，根据黑客攻击的思维，参考黑客攻击的手段，指定攻击的路线，尽可能全面发现导致黑客入侵的所有途径；对预审系统资产发现并深入挖掘漏洞，从而实现横向渗透，进而实现整个网络的夺权的思路，达成攻击目标。 | 《渗透测试报告》 《渗透测试授权书》 《渗透测试复测报告》 《人员保密协议》 | 1次 |
| 3 | 应急演练 | 应急演练服务根据定制化的演练目的和场景，基于现有应急处置体系，组织开展应急演练工作，进一步提高客户网络安全应急处置能力。主要服务内容包括：制订应急演练方案、准备应急演练环境、实施应急演练、优化应急预案、完善应急处置体系等。 | 《应急演练预案》 《应急演练总结报告》 | 1次 |
| 4 | 安全加固 | 安全加固指导服务针对在安全评估、应急响应、攻防对抗过程中发现的安全风险、不合规项、漏洞扫描报告等提供具体落地的加固方案并指导客户进行加固整改。服务包括安全漏洞漏洞服务与基线安全加固指导服务，指导加固对象包括系统漏洞、中间件、数据库等相关软硬件资产。 | 《安全加固计划》 《安全加固进度跟踪表》 《系统加固报告》 | 1次 |
| 5 | 安全意识培训 | 安全意识培训旨提升医院内部员工安全认知，让员工认识到信息安全意识不足对组织可能造成的危害，传导应正确恪守的行为方式；通过全员安全意识的理论培训和案例分析以及关键行为上的最佳实践指导，让信息安全“人防“保障有效支撑业务高效稳定运行。培训内容包括普通员工的上网安全、邮件安全、通信安全等常见的安全意识内容。 | 《培训人员签到表》 《培训课件》 《培训现场照片文件》 | 2次 |
| 6 | 应急响应 | 应急响应服务根据应急预案对发生的安全事件快速作出响应，根据安全事件等级，第一时间采用现场或远程的方式对安全事件进行应急处置。安全事件包括：非授权访问、信息泄密、拒绝服务、非法登录、病毒感染，权限篡改等相关攻击行为。 | 《检测结果记录》 《抑制处理记录表》 《根除处理记录表》 《恢复处理记录表》 《应急响应报告表》 | 按需 |
| 7 | ▲安全托管服务 | 1、服务资产（IP）数量≥40个；  2、暴露面梳理：对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；  3、针对服务范围内资产扫描到的高危可利用漏洞，做好每一个高危可利用漏洞的防护工作，包括但不限于提供漏洞修复方案和安全设备防护策略，以及帮助配置防护规则，保证不因此出现重大事件和损失，并且支持对扫描到的高危可利用漏洞能够自动匹配漏洞防护规则；（需提供的相关功能认证证书复印件或服务工具操作界面截图并加盖投标人公章）  4、应当具备检测和分析平台，通过采集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，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；分析研判包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容，并支持根据情况提供备注；  5、提供定期的勒索病毒入侵风险专项排查，应按照勒索预防Checklist开展勒索风险评估，勒索预防Checklist应当包含勒索高危利用漏洞、端口、安全策略、勒索攻击行为几个纬度。  6、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，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）；  7、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》；  8、服务平台应当支持对接该项目服务工具，支持实时接收服务工具检测到的安全事件信息、安全日志数据提供7\*24小时的服务；  9、为了保障服务效率和质量，服务平台应当具备一套完善的流程编排引擎，能够灵活编排、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； | 《项目启动会PPT》 《首次安全风险分析报告》 《漏洞举证报告》 《漏洞清单》 《应急响应报告》 《威胁情报》 《暴露面梳理清单》 《威胁狩猎报告》 《安全运营周报》 《安全运营月报》 《半年度总结汇报》 《年度总结汇报》 | 1年 |

# 工期及服务地点

服务工期：自用户通知进场起一年内。

项目地点：海南省海口市。

# 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份现场安全巡检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份攻防演练报告及相应过程文档。