|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术指标** | **单位** | **数量** | **备注** |
|  | 安全运维服务 | 1.服务内容：派遣安全技术人员在现场协助医院开展日常安全运维，提供全方位的运维服务和技术支持，针对相关安全设备开展日常巡检、日常告警处置、定期统计报告、流量分析、安全规则调优等工作，协助做好信息系统的安全运行，为核心业务提供日常安全维护和技术保障，保障信息系统可靠、高效、持续及安全地运行，及时发现并处理网络安全事件，提高网络的整体安全防护能力。  2.基于医院的已有的网络现状，综合医院的业务需求以及监管要求，协助医院对安全设备进行配置及更改、调整设备策略。  3.监测到医院网络安全存在潜在问题或已经发生故障时，通过现场支持和远程支持相结合的方式尽快处理故障。  4.服务频率：常态化驻场运维，安全工程师现场安全运维服务一周至少3个工作日以上  5.服务期限：1年  6.输出内容：《安全运维季度总结报告》 | 项 | 1 |  |
|  | 安全咨询服务 | 1.服务内容：根据医院信息系统等级保护的要求，进行差距分析，在定级、评估、整改、运维方面提供支持。  2.根据医院的需求和风险评估结果，制定全面的安全策略，包括不限于网络安全策略、访问控制策略、应急响应策略等，明确安全目标、安全原则和安全措施。  3.参照等级保护要求，制定信息系统安全建设目标与安全规划方案，建立信息安全保障体系框架。  4.服务频率：每年一次  5.服务期限：1年  6.输出内容：《相关文件档案（测评所需）》 | 项 | 1 |  |
|  | 安全培训服务 | 1.服务内容：针对医院相关的运维人员、技术人员，开展安全能力培训，以提升信息安全认知和技术能力以及管理能力；针对工作人员，组织开展信息安全意识提高培训。培训内容包括但不限于网络安全意识、网络安全基础知识、安全配置、安全升级、安全政策、Web安全培训、攻防演练培训等内容。  2.信息安全意识培训：网络安全相关安全事件提高人员安全意识，恪守安全红线。网络安全相关法律（网络安全法、数据安全法、密码法、关键信息基础设置条例）的立法背景以及解读，网络安全相关法律的案例剖析，网络安全常见问题应对方法。  3.信息安全运维培训：计算机网络基础、网络规划与设计、网络资源设备分析、网络安全技术、计算机网络概论、数据通信基础、广域通信网、局域网与城域网、网络互连与互联网、网络安全、网络操作系统与服务器、组网技术、网络管理、网络规划与设计、系统开发与运行、计算机组成及结构、操作系统基础。  4.信息安全攻防培训：以网络与信息安全为主线分别介绍黑客攻击及防范技术、文档安全管理及实现、网络安全架构设计及网络安全设备实施部署、加密技术在网络安全中的应用、实现主机操作系统及应用服务器安全加固、风险评估、病毒防范、数据恢复及网络诊断与故障排除等内容。  5.信息安全管理培训：针对信息安全管理人员介绍如何对内部的信息安全进行监督和管理，分别为信息安全内部人员管理、信息安全制度落实情况管理、管理制度修订和评审、应急演练等内容。  6.服务频率：每年两次  7.服务期限：1年  8.输出内容：《网络安全培训课件》 | 项 | 1 |  |
|  | 安全评估服务 | 1.服务内容：针对医院相关信息系统的资产，包括物理环境、网络资产、设备资产、主机资产、应用资产、管理制度资产等，开展资产评估、脆弱性评估、威胁评估，并根据评估结果进行风险计算，对发现的安全问题或风险，提供解决方案和建议，指导后续制定其安全发展战略和目标，建立或完善安全防护和管理体系，提升整体的安全防护能力和防护级别。  2.管理层面风险评估：对医院的安全管理机构、安全管理制度、人员安全管理、系统安全建设管理、系统安全运维管理等维度的管理层内容进行风险评估，输出安全管理建议。  3.技术层面风险评估：对医院的物理安全、网络安全、主机安全、应用安全、数据备份与恢复安全等维度的技术层内容进行风险评估，输出安全技术建议。  4.服务频率：每年一次  5.服务期限：1年  6.输出内容：《安全风险评估报告》 | 项 | 1 |  |
|  | 安全通告服务 | 1.服务内容：针对医院相关信息系统，提供最新安全漏洞、威胁（0day、系统漏洞、网络攻击）的解决办法、安全问题描述和相应的处理意见。安全通告的范围主要有：常见厂商的软、硬件网络设备，常见厂商的操作系统，常见厂商的数据库软件，常见厂商的Web软件。  安全通告内容组成包括不限于以下模块：  ① 公告ID：CVE编号；  ② 公告标题：漏洞名称；  ③ 厂商：漏洞涉及的厂商；  ④ 发布时间：漏洞发布时间；  ⑤ 受影响软件及系统：漏洞影响的软件及系统；  ⑥ 综述分析：对漏洞进行描述,同时分析其造成影响的原因；  ⑦ 解决方法：厂商补丁发布的链接；若厂商还未发布相应的补丁，根据安全问题的实际情况,提供暂时的解决方案。  2.服务频率：每月一次  3.服务期限：1年  4.输出内容：《安全通告》 | 项 | 1 |  |
|  | 弱口令扫描服务 | 1.服务内容：收集医院相关信息系统现有服务器、网络设备、数据库、WEB应用等资产，通过常用弱口令字典，使用专业工具进行口令验证与暴力破解，通过渗透测试人员人工对WEB应用系统进行弱口令检测、暴力破解、MD5密码碰撞等方式，纠察脆弱账号口令，防范因弱口令带来的安全威胁。  2.服务频率：每季度一次  3.服务期限：1年  4.输出内容：《弱口令检查报告》 | 项 | 1 |  |
|  | 漏洞扫描服务 | 1.服务内容：针对医院相关信息系统的服务器、数据库、WEB应用和网络设备等，通过具备自主知识产权的漏洞扫描工具以及综合安全评估工具，以本地扫描或远程扫描的方式进行安全扫描，从内网和外网两个角度查找安全对象目标存在的安全风险、漏洞和威胁。  2.因漏洞扫描涉及业务系统账号和口令，为保障漏洞扫描工具的安全性，产品后台所采用数据库需为国产数据库，且符合国家对软件可控的要求，需提供数据库的《信息技术产品自主原创性测评证书》。**（提供国产数据库国家网络与信息系统安全产品质量监督检验中心颁发的测评证书复印件并加盖供应商公章）**  3.由于医院资产数量较多、且业务连续性要求高、为降低扫描对业务的影响、需在短暂的时间内完成扫描，扫描工具后台国产数据库需支持分布式大规模并行处理集群150个节点以上。**（提供第三方机构出具的带CNAS或CMA标识的检验或检测报告复印件，并加盖供应商公章）**  4.为保障漏洞扫描工具数据存储的安全性，漏洞扫描工具所使用的后台数据库需为国产数据库，后台国产数据库支持AES、DES等国密SM算法等、保障漏扫数据的安全。**（提供第三方机构出具的带CNAS或CMA标识的测试报告复印件，并加盖供应商公章）**  5.服务频率：每季度一次  6.服务期限：1年  7.输出内容：《漏洞扫描报告及整改建议》 | 项 | 1 |  |
|  | 渗透测试服务 | 1.服务内容：针对医院相关的信息系统，使用多种渗透技术和方法进行模拟黑客攻击的渗透性测试，检查系统安全性，验证当前的安全防护措施，及时发现其存在安全漏洞，避免应用系统被攻击、控制，并提供有价值的安全建议。  2.WEB网站渗透：对WEB网站进行渗透攻击，获取或篡改关键信息，据此形成专业的渗透测试报告。  3.应用服务渗透：对专用应用服务，进行渗透攻击，获取或篡改关键信息，最大程度提升权限，据此形成专业的渗透测试报告。  4.数据库渗透：对专用数据库，如SQL、Oracle、Sybase、DB2等进行渗透攻击，获取或篡改关键信息，最大程度提升权限，据此形成专业的渗透测试报告。  5.渗透测试完成后，将协助医院对已发现的安全隐患进行修复。修复完成后，渗透测试工程师对修复的成果再次进行远程测试复查，确保修复结果的有效性。  6.服务频率：每半年一次  7.服务期限：1年  8.输出内容：《渗透测试报告》 | 项 | 1 |  |
|  | 配置核查服务 | 1.服务内容：严格参照等保、医院的各种设备安全配置规范要求，对医院全局网络和信息系统的总体安全架构进行风险分析，深入了解各系统的业务状况下。  2.定期对医院网络设备、安全设备、业务系统、中间件、数据库、操作系统等进行基线配置核查，对核查结果进行分析，识别出现有安全配置与基线标准之间的差距，确定存在的安全风险和隐患。  3.根据差距分析结果，结合医院业务特点，提供有针对性的安全修补建议，如修改配置、加强管理、升级软件等，并提供安全基线配置核查报告。  4.服务频率：每季度一次  5.服务期限：1年  6.输出内容：《配置核查报告》 | 项 | 1 |  |
|  | 安全措施有效性核查 | 1.服务内容：针对医院的防火墙、入侵检测设备、防病毒网关、web 应用防火墙等安全设备，进行安全策略稽核，确认安全设备的部署位置及配置的安全策略已发挥安全作用。  2.对核查过程中发现的问题进行分析，提供改进建议和解决方案，协助医院进行整改。  3.服务频率：每季度一次  4.服务期限：1年  5.输出内容：《安全措施有效性核查报告》 | 项 | 1 |  |
|  | 安全策略优化服务 | 1.服务内容：针对医院的安全设备、服务器等设备的策略进行策略优化，增加整体网络的安全性，减少网络安全隐患。  2.为保障安全策略优化的有效性，进行服务器安全策略优化加固时需采用“人工+工具”优化方式实现。  3.工具支持对操作系统安全基线进行检测、加固、恢复，满足操作系统安全防护基线要求。**（提供工具功能截图并加盖供应商公章）**  4.工具支持应用程序白名单，只有属于白名单列表的可执行程序可以运行，不在列表中的所有可执行程序都不能执行。**（提供工具功能截图并加盖供应商公章）**  5.工具支持进程保护，可以保护指定进程，如系统进程、应用进程，防止进程被非法终止等操作。**（提供工具功能截图并加盖供应商公章）**  6.工具支持文件的强访问控制权限：可以细化和严格定义用户对文件的访问权限（剥离超级用户权限），也可以结合强访问控制模型定义用户对文件的访问权限。**（提供工具功能截图并加盖供应商公章）**  7.工具支持微隔离策略配置，微隔离支持标签和标签、标签和主机、主机和主机之间的隔离策略配置。**（提供工具功能截图并加盖供应商公章）**  8.服务频率：每季度一次  9.服务期限：1年  10.输出内容：《安全策略优化报告》 | 项 | 1 |  |
|  | 应急响应服务 | 1.服务内容：针对医院相关信息系统突发的网络安全事件，以现场、远程、电话等多种服务方式提供7×24小时应急响应服务，对于突发的安全事件在最短时间内做到应急响应，了解安全事件的基本现象，判断安全事件的原因，进行故障和事件的处理。  2.事件发生后，迅速采取措施和行动，以最快速的方式阻止安全事件的损害扩大，同时降低安全事件带来的影响，恢复业务到正常服务状态，调查安全事件发生的原因，进行整改加固，避免同类安全事件再次发生。  3.服务频率：按需服务，第一时间（五分钟内）远程响应，确定事件性质，如需到场，30分钟内到场。  4.服务期限：1年  5.输出内容：《应急响应报告》 | 项 | 1 |  |
|  | 应急演练服务 | 1.服务内容：针对医院相关信息系统，开展包括但不限于内容安全事件、网络攻击或病毒事件等场景的模拟演练。回溯、重现黑客攻击、安全人员防御、修复加固的过程，制定网络安全应急演练预案，制定演练的计划，以及进行演练总结。  2.检验预案：通过开展应急演练，查找已经编制的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。  3.完善准备：通过开展应急演练，检查应对突发事件所需应急队伍、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。  4.锻炼队伍：通过开展应急演练，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，提高其应急处置能力。  5.磨合机制：通过开展应急演练，进一步明确相关单位和人员的职责任务，理顺工作关系，完善应急机制。  6.宣传教育：通过在开展应急演练，普及应急知识，提高工作人员风险防范意识和应对能力。  7.服务频率：每年一次  8.服务期限：1年  9.输出内容：《应急演练报告》 | 项 | 1 |  |
|  | 信息安全迎检保障服务 | 1.服务内容：协助医院做好信息自查和准备工作，满足上级单位对信息安全要求各类指标，包括安全整改、配置加固、资料准备等。  2.协助医院配合检查人员的工作，解答检查人员的疑问，确保检查工作的顺利进行。  3.对检查过程中发现的问题及时进行记录和分析，为后续的整改工作提供依据。  4.服务频率：按需服务  5.服务期限：1年  6.输出内容：《迎检所需相关材料》 | 项 | 1 |  |
|  | 硬件支持服务 | 1.服务内容：针对医院网络设备、服务器、机房设备等提供硬件支持服务，在出现硬件故障时，第一时间进行支持处理（1000元以内由服务商负责解决）。  2.服务频率：按需服务  3.服务期限：1年  4.输出内容：《硬件支持服务报告》 | 项 | 1 |  |
|  | 突发事件协助处理服务 | 1.服务内容：医院因紧急业务需求或其他突发事件需要提供技术或协助服务时，服务商及时进行应急响应并协调资源配合医院处理相关突发事件。若相关服务涉及第三方费用，由医院与服务商另行友好协商。  2.服务频率：按需服务  3.服务期限：1年  4.输出内容：《突发事件协助处理记录》 | 项 | 1 |  |