**购置网络安全运维服务参数要求**

1. **参数说明：**
2. 参数中加★项为核心指标项，若其中有一项核心指标不满足，则不考虑该服务商。
3. 其他项为一般指标项，若有2项以上（不包含2项）一般指标项不满足，则不考虑该服务商。
4. **服务期限及地点**
5. 服务期限：自合同签订之日起一年。
6. 服务地点：北京市平谷区医院指定地点
7. **服务内容及要求：**

### 服务清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **数量** | **单位** |
| 一、网络安全运维服务 |
| 1 | 安全运营服务 | 1 | 年 |
| 2 | 安全配置核查服务 | 1 | 年 |
| 3 | 应急响应及处置 | 1 | 年 |
| 4 | 日志分析及事件研判服务 | 1 | 年 |
| 5 | 安全加固 | 1 | 年 |
| 6 | 安全风险评估服务 | 1 | 年 |
| 7 | 网络安全值守服务 | 1 | 年 |
| 二、检测服务 |
| 8 | 渗透测试服务 | 1 | 年 |

### 服务内容

#### 1.网络安全运维服务

#### （1）安全运营服务

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 定期对安全服务对象进行巡检，涉及设备自身硬件资源的使用情况、业务应用服务所占用的网络资源情况、端口服务开放情况的变更等内容，主要对网络和重要信息系统安全防护措施是否合规、到位，安全设施是否有效进行检查、验证并提出巡检报告和改进措施，并实施必要的安全维护操作，包括设备CPU、内存状态、开放服务检测，系统故障检查、分析、排除和跟踪。 |
| 2 | 服务工具功能要求 | 1.需展示漏洞的运营状态页面；支持展示未处置、已处置、已标记漏洞数量情况以及最近的漏洞报告导入时间；支持展示近7天和近30天的漏洞数量趋势图、漏洞数量最多的资产排行图、漏洞等级分布图、漏洞类型分布图；支持展示滚动的最近未处置漏洞列表，并可通过点击跳转至漏洞处置页面。要求提供系统证明截图2.需展示资产的运营状态页面；支持展示不同状态资产的数量以及资产中检测到的不同类型告警数量、威胁事件数量、监控状态数量；统计展示风险指数最高的资产/业务系统排行、资产安全趋势图、外连威胁列表；支持展示资产检测到的实时告警列表，并可通过列表内点击跳转至漏洞处置页面。要求提供系统证明截图 |
| 3 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 4 | ★服务频次 | 1年内不限次数 |
| 5 | ★技术能力 | 为保障业务连续性、安全运营：服务商需提供（信息系统安全运维服务资质） |
| 6 | 服务成果 | 《网络安全运营服务报告》 |

#### （2）安全配置核查服务

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 根据定制的设备安全配置基线，以自动化和人工服务相结合的方式对信息系统网络、主机操作系统、数据库、中间件和安全设备配置策略进行核对，并生成初步核查报告，通过人工分析的方式对策略核查结果进行分析和确认，并提出整改建议，针对配置策略设置不合理之处协调相关方实施整改，确保主机操作系统、数据库、中间件、网络、安全等设备的配置策略满足安全基线要求，有效降低信息安全事件的发生。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 1年内不限次数 |
| 4 | ★技术能力 | 为保障信息化系统稳固、安全审计要求：服务商需提供（网络安全审计服务资质） |
| 5 | 服务成果 | 《安全配置核查服务报告》 |

#### （3）应急响应及处置

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 在信息系统发生安全事件时及时响应，执行应急响应流程，通过专家级技术支持和快速响应，及时抑制和消除医院信息系统安全事件，减少损失和负面影响，提高医院信息系统业务连续性。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 1年内不限次数 |
| 4 | ★技术能力 | 为保障安全事件处置及时、后背力量完善：服务商需提供（信息安全应急处理服务资质） |
| 5 | 服务成果 | 《应急响应及处置报告》 |

#### （4）日志分析及事件研判服务

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 依托专业团队与先进工具，全方位、多维度地深度收集信息系统服务器操作系统、数据库、中间件、网络及安全设备等核心组件产生的海量日志信息，确保数据无遗漏、无失真。运用智能工具与资深专家经验相结合的分析模式，对收集到的日志进行深度剖析与精准审查，不仅能快速定位现有安全漏洞、性能瓶颈及异常操作等显性问题，更能凭借敏锐洞察力与前瞻性思维，从繁杂数据中挖掘潜在风险趋势，提前预警可能出现的系统故障、安全威胁等重大隐患。同时，基于分析结果，为客户量身定制详细、专业且具有高度可操作性的分析报告，为客户的信息安全防护、系统性能优化及业务稳定运行提供坚实有力的决策依据，全方位保护客户核心资产安全。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 1年内不限次数 |
| 4 | 服务成果 | 《日志分析及事件研判服务报告》 |

#### （5）安全加固

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 根据渗透测试等工作结果，结合用户信息系统业务需求，通过技术手段对信息系统相关的操作系统、数据库、中间件、网络与安全设备进行安全策略加强、调优，包含网络结构优化调整、系统设备脆弱性加固、加固效果跟踪评价等，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 1年内不限次数 |
| 4 | 服务成果 | 《安全加固报告》 |

#### （6）安全风险评估服务

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 基于医院信息系统及其所依托的基础网络的安全状况，参照国家信息安全风险评估规范、等级保护政策和技术要求等，从技术、管理和人员等多个方面，包括网络安全技术架构、网络/安全设备性能和策略、主机（包括操作系统和数据库）安全策略、信息系统安全机制和策略以及安全管理制度方面，查找受保护的信息系统和关键资产存在的脆弱性，分析其面临的威胁和安全措施的有效性，明确保护重点。从资产重要性、脆弱性严重程度和威胁发生频率等方面分析信息系统面临的风险，为后续信息系统安全加固以及整改提供客观数据，为建立信息安全保障体系提供决策依据。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 1年内不限次数 |
| 4 | ★技术能力 | 为保障核心系统及业务数据安全可控：服务商需提供（信息安全风险评估服务资质） |
| 5 | 服务成果 | 《安全风险评估服务报告》 |

#### （7）网络安全值守服务

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 基于医院信息系统及其所依托的基础网络的安全状况，参照国家信息安全风险评估规范、等级保护政策和技术要求等，从技术、管理和人员等多个方面，包括网络安全技术架构、网络/安全设备性能和策略、主机（包括操作系统和数据库）安全策略、信息系统安全机制和策略以及安全管理制度方面，查找受保护的信息系统和关键资产存在的脆弱性，分析其面临的威胁和安全措施的有效性，明确保护重点。从资产重要性、脆弱性严重程度和威胁发生频率等方面分析信息系统面临的风险，为后续信息系统安全加固以及整改提供客观数据，为建立信息安全保障体系提供决策依据。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 1年，5\*8小时现场服务 |
| 4 | 服务成果 | 《网络安全值守服务报告》 |

#### 2.检测服务

#### （1）渗透测试服务

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 服务内容 | 通过模拟黑客对目标系统进行渗透测试，对系统的任何弱点、技术缺陷或漏洞进行主动分析，并且以有利于攻击为目的而对漏洞加以利用，以发现并验证其存在跨站脚本漏洞、主机远程安全、残留信息、SQL注入漏洞、系统信息泄露、弱口令等安全隐患，评估系统抗攻击能力，全面了解和掌握应用系统所面临的安全威胁和存在的风险。 |
| 2 | 服务范围 | 针对北京市平谷区医院指定信息系统 |
| 3 | ★服务频次 | 所有系统 |
| 4 | 服务成果 | 《渗透测试服务报告》 |

### （二）服务要求

投标人须为本项目组建稳定的、专业的、独立的安全服务团队，专门负责本项目运维工作。包括项目经理1名，项目驻场人员1名，项目组其他技术人员不少于4名，确保人力、物力的投入，项目组成员必须稳定，项目组成员在项目终验前如果人员退出或更换，需要征得采购方同意。

项目经理需具备以下资质：

项目经理：具有ITIL证书、信息系统项目管理师证书、专业职务任职资格评审委员会颁发的高级工程师（信息安全专业）资格证书、

★驻场人员：具有CISP证书、且有丰富的网络安全项目维护经验，驻场人员须为投标公司正式员工，且工作年限不少于5年，并提供证明材料。