# 网络安全服务具体要求

# 采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务内容** | **服务频次** | **计量单位** |
| 1 | 渗透测试服务 | 1 | 次/年 |
| 2 | 网络安全培训服务 | 1 | 次/年 |
| 3 | 应急演练服务 | 1 | 次/年 |
| 4 | 应急响应服务 | 1 | 年 |
| 5 | 漏洞扫描服务 | 2 | 次/年 |
| 6 | 网络安全巡检服务 | 1 | 次/年 |

# 技术服务要求

## ★渗透测试服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术参数 |
| 1 | 服务内容 | 在梓潼县妇幼保健院的授权与监督下，对梓潼县妇幼保健院指定信息系统提供渗透测试服务，模拟黑客使用的漏洞发现技术和攻击手段，对目标网络、系统、主机应用的安全性进行深入探测，发现系统最脆弱环节，出具相应的测试与分析报告，并提出相应的整改建议措施，帮助梓潼县妇幼保健院更直接的了解自己的网络所面临的安全问题，并及时弥补。渗透测试内容至少包括:信息收集类、配置管理类(HTTP方法测试、应用中间件测试、信息泄露、异常错误等)、认证类(用户枚举、密码猜解、密码重置、密码策略测试等)、会话类(cookie测试、session会话测试等)、授权类(越权访问、路径遍历、任意文件下载、逻辑缺陷测试等)、数据验证类(SQL注入、跨站脚本、代码注入、URL跳转、文件上传测试等、输入输出校验绕过、数据篡改)、系统应用漏洞(溢出、0day漏洞等)。 |
| 2 | 服务范围 | 梓潼县妇幼保健院指定的核心业务系统 |
| 3 | 交付成果 | 《渗透测试报告》 |

## ★网络安全培训服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术参数 |
| 1 | 服务内容 | 组织开展梓潼县妇幼保健院核心人员的网络安全培训工作，培训内容包括（不限于）网络安全道德培训、网络安全等级保护要点解读、网络安全法要点解读等，提升职工、信息系统运维人员、系统管理员等相关人员网络安全防护能力，从而提高梓潼县妇幼保健院整体网络安全保障能力和防护水平。 |
| 2 | 服务范围 | 梓潼县妇幼保健院 |
| 3 | 交付成果 | 网络安全培训课件 |

## ★应急演练服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术参数 |
| 1 | 服务内容 | 1、网络安全应急演练：协助梓潼县妇幼保健院制定应急预案演练工作计划，并模拟在网络及重要设备出现故障等紧急情况下，依据前期制定的应急预案进行处理，其中至少包括事件的发现、上报、处理等环节。通过演练，使相关方熟悉应急处理流程，提高对安全事件的响应能力；同时验证预案的正确性和适用性，进行总结分析，并根据需要对应急预案进行修订。 |
| 2 | 服务范围 | 梓潼县妇幼保健院 |
| 3 | 交付成果 | 《网络安全应急演练方案》、《应急预案》 |

## ★应急响应服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术参数 |
| 1 | 服务内容 | 根据安全事件类别，通过远程和现场支持的形式协助采购人进行突发性网络安全事件紧急分析和处理。主要工作内容包括但不限于:突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等。在遭受黑客入侵攻击时，供应商立即安排安全运行保障人员对入侵事件进行分析，并结合应急响应预案，对入侵事件进行检测、抑制、处理，查找入侵来源并恢复系统正常运行。 |
| 2 | 服务要求 | 应急响应服务要求供应商在发生安全事件后，30分钟内响应，2小时内安排专家到达现场进行安全应急，8小时之内对攻击事件进行溯源，并出具应急响应报告;供应商对入侵攻击事件的应急处理，包括但不限于以下内容:  1、判断安全事件类型，查明安全事件原因，确定安全事件的威胁和破坏的严重程度。  2、将受影响的信息系统和业务服务进行隔离。  3、针对发现的安全事件来源，排除潜在的隐患，消除安全威胁，彻底解决安全问题。  4、恢复系统正常操作，使网络系统能在尽可能短的时间内恢复正常的网络服务。  5、对系统中发现的漏洞进行安全加固，消除安全隐患。  6、重新评价系统的安全特性，确保在项目服务期范围内，不发生同类的安全事件。 |
| 3 | 服务范围 | 梓潼县妇幼保健院 |
| 4 | 提供工具 | 供应商提供应急响应服务过程中，应使用专业的安全服务工具，包括网络安全事件应急处置工具、APT攻击分析工具、日志分析工具等，保障服务过程的稳定性和输出的有效性。 |
| 5 | 交付成果 | 《应急响应报告》 |

## ★漏洞扫描服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术参数 |
| 1 | 服务内容 | 采用具有销售许可证或软件著作权证书的专业漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的全面扫描与分析，扫描设备检测规则库及知识库应涵盖CVE、CNCVE、CNVD、CNNVD等标准。扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供修复建议。 |
| 2 | 服务范围 | 梓潼县妇幼保健院核心业务系统 |
| 3 | 服务方式 | 供应商安排工程师，采用现场的方式，对单位信息系统、主机、数据库、应用层面进行漏洞扫描工作。 |
| 4 | 交付成果 | 《漏洞扫描报告》 |

## ★网络安全巡检服务

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术参数 |
| 1 | 服务内容 | 定期对梓潼县妇幼保健院信息系统和单位网络安全设备开展安全巡检工作，通过工具和人员，对单位网络设备、服务器、操作系统、应用系统进行周期性的状态检查、安全扫描、日志分析，补丁管理并提交巡检报告及安全建议，以持续提升安全运行和防护能力。 |
| 2 | 服务范围 | 梓潼县妇幼保健院 |
| 3 | 交付成果 | 《安全巡检报告》 |

# 服务工具指标要求

1、漏洞扫描工具：漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容；

2、▲漏洞扫描工具：具备检测数据库内核入侵行为，同时能够探测出黑客创建的一些隐藏对象能力；（提供国家认可的第三方检测机构或单位出具的证书或检验检测报告并加盖供应商鲜章）

3、漏洞扫描工具：具备弱口令扫描能力，支持弱口令扫描协议数量不低于22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3等常见协议，主流数据库协议和WEB协议等进行弱口令扫描，允许用户自定义用户、密码字典；

日志分析工具：支持收集分析网络安全设备、交换设备、路由设备、操作系统、应用系统等日志，至少支持Syslog、SNMPTrap、HTTP、ODBC/JDBC、WMI、FTP、SFTP等协议日志的收集；

4、▲日志分析工具：在安全事件发生后，支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件；（提供国家认可的第三方检测机构或单位出具的证书或检验检测报告并加盖供应商鲜章）

5、日志分析工具：具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件；

6、▲信息安全等级保护检查工具：提供安全巡检服务的过程中，供应商需利用公安部认可的“信息安全等级保护检查工具”针对服务范围内的信息系统进行全面的安全检查，通过工具提供专业检查知识和检查方法，提高服务的规范化水平；（提供公安部认可的盖章证明文件并加盖供应商公章）

7、信息安全等级保护检查工具：工具内置等保2.0检查指标标准，支持一键检查调用可用待查的检查工具进行检查；

8、▲网络安全事件应急处置工具：提供应急响应服务过程中，使用的网络安全事件应急处置工具应支持一键提取安全事件相关信息，包括系统配置信息、使用痕迹信息、运行状态信息、恶意代码情况等；（提供工具功能界面截图证明并加盖供应商鲜章）

9、▲网络安全事件应急处置工具：具备多维度网络安全事件分级能力；（提供国家认可的第三方检测机构或单位出具的证书或检验检测报告并加盖供应商鲜章）

10、APT攻击分析工具：具备文件攻击检测、WEB攻击检测、Mail攻击检测、失陷主机检测、内部渗透检测、异常流量检测、资产管理等能力；

11、▲APT攻击分析工具：工具应支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现；（提供国家认可的第三方检测机构或单位出具的证书或检验检测报告并加盖供应商鲜章）

12、▲APT攻击分析工具：工具应支持对网页进行恶意代码检测，特别针对JavaScript类别的恶意代码进行安全检测；（提供国家认可的第三方检测机构或单位出具的证书或检验检测报告并加盖供应商鲜章）

# 服务工具清单

为保障项目服务质量，确保服务实施工作中的安全性、专业性，在各项服务实施过程，供应商应使用以下专业安全服务工具以支撑网络安全服务交付：

|  |  |  |
| --- | --- | --- |
| **序号** | **工具名称** | **数量** |
|  | 漏洞扫描工具（含系统扫描、WEB扫描、数据库扫描、基线扫描能力） | 1套 |
|  | 日志分析工具 | 1套 |
|  | 信息安全等级保护检查工具 | 1套 |
|  | APT攻击分析工具 | 1套 |
|  | 网络安全事件应急处置专用工具 | 1套 |

注：以上工具需在服务过程中全部提供使用，服务工具不单独进行报价，供应商应充分考虑服务工具的成本等因素，将报价包含在服务项目中，响应文件中应对拟采用的服务工具进行介绍（至少包括服务工具的制造厂商、版本型号），为避免法律纠纷，如供应商使用的工具非本单位自主研发，供应商需提供承诺函，承诺服务过程中向采购人提供与投标响应一致的所有工具，并提供服务工具制造厂商授权使用证明材料。

# 综合评分明细表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评审项目及权重 | 分值 | 详细描述 | 备注 |
| 1 | 价格部分  15% | 15分 | 以本次最低有效投标报价为评标基准价，其他供应商的价格分统一按照下列公式计算：投标报价得分=（评标基准价/有效投标）×15分 | 评分的取值按四舍五入法，保留小数点后两位 |
| 2 | 技术服务要求  26% | 26分 | 本项满分26分，全部满足“工具指标要求”得26分，不满足要求按照以下扣分细则扣分，扣完为止。  标“▲”为重要参数项（共7条），一项不满足或不完全满足扣3分，非“▲”项为一般参数（共5条），一项不满足或不完全满足扣1分，直至本项分值扣完为止。（以序号1、2、3等为一条参数） |  |
| 3 | 供应商服务能力  18% | 18分 | 1、供应商具备信息安全管理体系认证证书、信息安全服务资质认证证书（信息系统安全运维）、信息安全服务资质认证证书（信息安全风险评估）的得3分，具备任意一个得1分，不提供或没有不得分；（有效期证书复印件并加盖供应商公章）  2、供应商具备网络安全服务工具类软件著作权（如漏洞扫描系统、端口扫描系统、运维管理系统等），具备任意1个得1分，最多得3分，不提供或没有不得分；（提供软件著作权证明材料并盖供应商公章）  3、供应商应为本项目配置1名项目经理，项目经理具备注册信息安全工程师认证证书、信息安全保障人员认证证书（安全运维专业级）、信息安全保障人员认证证书（风险管理专业级）、项目管理专业人士资格认证（PMP）证书中任意一个得1分，本项最多得4分，不提供或没有不得分；（提供人员身份证复印件、有效的相关证书复印件、在职证明并加盖供应商公章）  4、除项目经理外，供应商本项目拟派人员中每有1位具有注册信息安全专业人员（CISP）或信息安全保障人员认证证书的得1分，本项最多得4分。（项目团队成员（不含项目经理）如具有多个证书的只计一次分，提供人员身份证复印件、有效的相关证书复印件、在职证明并加盖供应商公章）  5、供应商自2021年1月1日（含）起至投标截止时间止，具有类似项目业绩的，每提供1个得1分，满分4分；（提供完整合同复印件或中标/成交通知书并加盖供应商公章）  注：类似业绩是指网络安全服务类项目业绩。 | 未提供不得分。 |
| 4 | 履约能力  18% | 18分 | 1.供应商所使用的服务工具制造厂商具有中国信息安全测评中心颁发的信息安全服务资质证书安全工程类，三级得3分，二级得2分，一级得1分，不满足的不得分；(提供有效期内证书复印件并加盖供应商公章)  2.供应商所使用的服务工具制造厂商（具有强大网络安全漏洞收集能力，拥有基于互联网公开的漏洞响应平台,满足得3分，不满足的不得分；（提供漏洞响应平台计算机软件著作权证书复印件,网站带URL截图）  3.供应商所使用的服务工具制造厂商具备知识产权管理体系认证证书（国家知识产权局授权认证机构颁发）得3分，不满足的不得分；(提供有效期内证书复印件并加盖供应商公章)  4.供应商所使用的服务工具制造厂商具备较强的漏洞发现及支撑能力，近3年（2021年、2022年、2023年）任意一年获评国家信息安全漏洞库（CNNVD）年度特殊贡献奖得3分，不提供或没有不得分;（提供国家信息安全漏洞库（CNNVD）评奖结果公告官网截图及证书证明材料并加盖供应商单位公章）  5.供应商使用的漏洞扫描工具具备国家信息安全漏洞库兼容性资质证书得3分，不满足的不得分；（提供有效期内证书复印件并加盖供应商公章）  6.供应商使用的APT攻击分析工具达到《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》认证标准 增强级的得3分，不提供或没有不得分；（提供有效期证书复印件并加盖供应商公章） | 未提供不得分。 |
| 5 | 服务方案  24% | 24分 | 根据供应商提供的方案进行综合评分，方案包括：（1）渗透测试方案、（2）安全培训服务方案、（3）应急演练方案、（4）应急响应方案、（5）漏洞扫描方案、（6）安全巡检方案，以上六项内容每有一项完全符合项目实际需求及项目情况的该项得24分，每缺少一项扣4分，每有一项内容存在缺陷的扣2分。本项目最多得24分。  注：“内容存在缺陷”是指：方案项目名称、项目编号与本项目要求不一致，或套用其他项目方案，或对采购需求理解缺位混乱，或前后内容互相矛盾，或存在与本项目无关的内容。 |  |