# 网络安全服务具体要求

## 1.★服务方式

采用基于实战的一体化网络安全运营服务，服务工具和线下安全专家相结合的服务方式，服务工具具备7\*24小时在线监测和告警能力。

## 2.服务内容：

### 2.1渗透测试服务

渗透测试针对具体某个或几个系统，重点发现技术或业务逻辑层面的漏洞。然而，即使系统内部经过渗透测试，外部仍有可能出现信息泄露等安全事件的风险。因此，希望通过从外部、内部进行渗透测试，从技术、管理、业务逻辑的角度来全面发现漏洞，充分挖掘客户信息泄露的途径（可追溯性），从根源解决存在的漏洞或问题，减少客户信息泄露事件的发生。

服务单位使用人工渗透测试技术，对业主单位管辖范围内的Web站点进行最大限度的挖掘SQL盲注、代码注入、struts2、越权、逻辑错误、存储型跨站脚本、中间件弱口令等使用扫描工具无法排查或挖掘的安全漏洞，并提交漏洞风险报告。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备安全设备 | 服务成果 |
| 远程/现场 | 外网/内网 | 1年/1次 | 渗透测试工具、渗透测试结果可导入服务平台 | 《关键系统渗透测试报告》 |

### 2.2资产梳理服务

通过本地化部署平台对梓潼县妇幼保健院的资产进行梳理，建立梓潼县妇幼保健院有效安全资产管理，能以资产为安全管理单位进行有效的安全运维工作，并通过实时展示资产的安全风险指数。

网站资产梳理服务：对单位网站进行自动化梳理服务，能主动探测互联网上暴露的资产，形成明确的资产清单，发现未知资产，并发现直接对外开放的危险连接方式。

服务器资产梳理服务：对单位服务器进行自动化梳理服务，包括操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本等，实现对服务器的自动化运维管理。

终端资产梳理服务：对单位终端PC资产自动化梳理服务，对识别到的所有IP地址进行有效管理，包括操作系统版本、端口开放情况、协议情况、服务版本、应用程序版本等

资产趋势分析服务：通过管理单位月度资产变化情况，包括IP和端口新增、减少、异常等，横向展示年度资产管理趋势服务。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备服务工具 | 输出报告 |
| 现场服务 | 网站、服务器、终端、其他网络资产 | 常态化动态管理 | 提供平台服务工具本地化部署 | 《网站信息系统资产列表清单》  《服务器信息系统资产列表清单》  《终端信息系统资产列表清单》 |

### 2.3主机脆弱性监测服务

对主机、网络设备、操作系统、数据库、中间件等进行常态化安全漏洞与弱口令扫描，提供漏洞、弱口令台账与报告，结合资产梳理，可快速定位高危组件影响范围。

每次安全漏洞扫描完成后，提交完整的漏洞扫描分析报告，详细说明存在的安全风险，而且对系统以后整改的方向提供适当的解决方案；扫描报告包括综述、主机、漏洞、趋势等信息进行分类，综述中应对漏洞和风险分布进行定量统计分析并展示，主机中应提供漏洞分布、可入侵情况、风险值和风险等级信息。

对服务范围内主机中包含redis、smb、rdp、telnet、ftp、ssh、pop3、smtp、mysql、imap、vnc、snmp、vmauthd、postgres、mssql、oracle、mongodb、onvif等多种服务协议进行弱口令检测，并提供弱口令处置方案。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备服务工具 | 输出报告 |
| 现场服务 | 服务器、终端资产 | 按需、常态化监测管理 | 配备平台工具本地化部署，支持数据安全量化分析，可在统一平台进行漏洞及弱口令安全概况展示和查阅 | 每季度输出一次  《梓潼县妇幼保健院主机漏洞监测报告及加固建议》、《梓潼县妇幼保健院主机弱口令监测报告及加固建议》 |

### 2.4配置核查服务

安全基线是一个信息系统的最小安全保证，即该信息系统需要满足的最基本安全要求。安全基线是实现信息安全风险评估和风险管理的前提和基础，为了满足各业务系统的基本安全需求，就需要充分参考国家及行业标准、规范以及成熟经验，建立并形成一个针对各业务系统的基线安全模型。

服务单位使用基线核查工具或人工检查，对业主单位管辖范围内网络设备、主机、操作系统、数据库、中间件、应用软件、新上线业务系统进行增量基线配置核查及是否满足最小化服务原则进行配置，并提供相对应报告。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备安全设备 | 服务成果 |
| 现场服务 | 服务器、终端资产 | 1年1次 | 配备平台工具本地化部署，并统一进行配置核查概况展示和查阅 | 《信息系统配置核查报告》  《新上线业务系统配置核查报告》 |

### 2.5漏洞屏蔽服务

通过技术手段帮助客户屏蔽各类漏洞，使漏洞扫描器、恶意攻击源无法扫描到主机或web应用系统存在的漏洞，包括可利用漏洞、版本漏洞、web代码层面的漏洞。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备安全设备 | 服务成果 |
| 现场服务 | 服务器 | 常态化 | 配备相关安全工具 | 无法通过未被授权的扫描工具扫描出相关漏洞 |

### 2.6流量入侵检测服务

旁路部署流量检测探针，监测重点区域边界流量，基于威胁感知模型精准识别恶意攻击源IP，可通过旁路阻断技术拦截恶意源IP的访问。

旁路部署流量检测探针：在重点区域边界路由器或交换机上旁路部署流量检测探针，实时监测进出该区域的网络流量，确保对所有流量数据的全面覆盖。

流量特征分析：利用流量检测算法，对监测到的流量数据进行深度分析，提取出包括源IP、目的IP、协议、流量大小等在内的流量特征信息。

威胁感知模型：基于威胁感知模型，综合运用机器学习和深度学习等先进技术，对流量特征信息进行智能分析，精准识别出恶意攻击源IP。

旁路阻断技术：在发现恶意攻击源IP后，通过旁路阻断技术，自动拦截该源IP的访问请求，阻止其进一步对企业网络进行攻击和入侵。

实时告警与日志记录：在检测到恶意攻击源IP时，实时发送告警信息，并生成详细的日志记录，以便后续的调查和追踪。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备安全设备 | 服务成果 |
| 现场服务 | 互联网边界 | 7\*24小时监测 | 配备平台工具本地化部署 | 每季度输出《综合报表》 |

### 2.7★全网攻击诱捕蜜罐服务

本次服务项目旨在通过部署一体化安全服务平台，在不改变单位网络架构的前提下（包括：不做镜像流量、不做牵引流量等），通过旁路部署的方式，在“DMZ区”、“服务器区”、“终端区”分别生成仿真业务系统，与待监测的目标“IP、web”等资产网络可达，通过虚拟出来的蜜罐主机，在每个网段部署虚拟蜜罐，以监测内网病毒威胁和安全事件，并提前做安全预警。通过全网部署蜜罐，基于欺骗防御技术，诱骗攻击者、病毒主机攻击蜜罐陷阱，实时零误报定位攻击威胁，实时通过飞书、钉钉、企业微信等进行预警。

当发现失陷主机时，不需要联动第三方设备、不需要在主机上安装agent脚本，就能对失陷主机进行处置，防止失陷主机继续对东西向主机进行病毒传播、横向攻击等行为；**（提供截图证明材料，加盖供应商鲜章）**

通过自学习的模式对采购方真实业务系统进行遍历访问，形成机器记忆，与真实业务系统一样可进行前后端的数据交互，从而实现包括但不限于以下动态交互类型：“搜索查询、登陆验证、账号注册”等，高迷惑性地吸引攻击者攻击蜜罐，要求拟态仿真蜜罐系统为纯静态系统，无需额外提供蜜罐定制服务；**（提供截图证明材料，加盖供应商鲜章）**

可灵活指定对某个攻击源IP地址发起威慑反制，比如灌输国家网络安全法、告知已获得相关溯源信息，发挥互联网攻击监测诱饵威慑作用，使攻击者放弃后续的攻击行为；**（提供截图证明材料，加盖供应商鲜章）**

通过监测中心可统一展现蜜罐告警事件、边界威胁监测告警，事件及告警结果自动刷新。支持蜜罐、与拓展边界威胁告警的关联分析，提升告警可信度。支持根据攻击行为自动研判，对攻击IP进行自动分类并打上对应的攻击者标签；**（提供截图证明材料，加盖供应商鲜章）**

漏洞无效化：联动部署的蜜罐，自动精准检测恶意攻击源、扫描源，并可基于告警风险值、或者定向源进行处置，使漏洞扫描器、恶意攻击源无法扫描到主机存在的漏洞，包括可利用漏洞、版本漏洞；**（提供截图证明材料，加盖供应商鲜章）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备安全设备 | 服务成果 |
| 现场服务 | 全网段 | 7\*24小时监测 | 配备平台工具本地化部署 | 每季度输出《综合报表》 |

### 2.8主机威胁监测

在重要系统服务器部署主机安全监测软件，可主动监测恶意文件（webshell、病毒木马）、挖矿进程与病毒检测、网站篡改检测等，发现可疑的入侵事件，并实时将告警同步到资产安全运维平台服务平台，第一时间对攻击行为进行告警。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备安全设备 | 服务成果 |
| 现场服务 | 重点服务器 | 7\*24小时监测 | 配备平台工具本地化部署 | 每季度输出《综合报表》 |

### 2.9安全加固咨询服务

根据每次安全扫描结果进行分析，提供分析报告和安全加固方案，组织并监控梓潼县妇幼保健院各驻点运维部门实施服务器操作系统、中间件、网络、安全设备等层面的安全加固、威胁加固，并提供加固报告。

|  |  |  |  |
| --- | --- | --- | --- |
| 服务内容 | 服务内容 | 服务频率 | 服务成果 |
| 系统漏洞加固咨询 | 根据主机扫描结果，针对不同版本的应用系统及操作系统进行安全漏洞加固咨询。 | 每季度一次 | 《安全加固咨询服务记录表》 |
| 安全配置加固咨询 | 根据配置核查结果，针对不同版本的应用系统及操作系统进行安全配置加固咨询 |
| 加固追踪 | 每季度提供主机漏洞、业务系统漏洞、配置加固等方面的安全加固情况，跟踪加固进度，通过平台展示安全加固率，便于监测安全加固工作情况与效率，推动安全加固工作的开展。 | 每季度一次 | 《安全加固追踪报告》 |

### 2.10应急演练服务

应急演练服务协助梓潼县妇幼保健院定期组织各部门进行应急演练，其内容包括但不仅限于：网页挂马、网页篡改、病毒感染、邮件钓鱼等。

另外，提供咨询和指导服务，确保各部门能根据不同的应急恢复内容，确定演练的内容，并具备独立开展应急演练的能力。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备服务工具 | 输出报告 |
| 现场服务 | 网站、服务器、终端资产 | 每年一次 | 配备平台工具本地化部署，通过平台开展应急演练 | 《梓潼县妇幼保健院XXX事件应急演练方案》 |

### 2.11安全应急响应

提供7\*24小时全天候、2小时到达现场，每次提供相应的响应报告，找出根源并提供可行解决方案。安全事件应急处理流程应包含三个阶段，包括事件初期、应急响应实施及输出报告与汇报：

事件初期：在实施应急响应工作前，客户经理或项目经理收到客户申请应急响应支持，由客户经理或项目经理协调内部技术支持人员和客户技术人员第一时间取得联系，了解事件发生情况。技术人员判断事件类型，是否需要启用应急响应服务。

应急响应实施：在判断事件类型可能为安全事件，启用应急响应后，技术人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处理建议，并协助客户解决事件。

输出报告与汇报：待事件处理结束后，技术人员整理事件分析、事件处理的过程记录和相关资料，撰写应急响应服务记录报告，提交给客户。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作。

安全事件应急处理过程中，应关联失陷主机发现过程，并结合实现主机分析报告进行处置汇报。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备服务工具 | 输出报告 |
| 现场服务 | 网站、服务器、终端资产 | 按需 | 配备平台工具本地化部署 | 《梓潼县妇幼保健院XXX事件应急响应报告》 |

### 2.12重保远程值守服务

做好重要时期（两会、国庆等时期）用户网络安全保障工作，提前开展安全自查，安全加固，消除安全隐患。重保期间做好远程安全值守，保障业务稳定，网络安全，保障单位利益。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备服务工具 | 输出报告 |
| 远程服务 | 按需 | 按需 | 配备平台工具本地化部署 | 《重保值守报告》 |

### 2.13安全培训服务

面向梓潼县妇幼保健院全员，通过网上视频学习和线下专题培训两种方式进行有效的安全意识灌输，针对目前主流的网上诈骗、个人信息泄露、办公安全意识等进行全面的讲解。需要配套相应的安全攻击过程演示等，保证培训过程中的生动性，确保学员的培训效果。

针对信息安全技术人员，提供安全技术应用经验培训，加强对安全技术手段在本单位的应用能力，提高整体业务技术能力。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务方式 | 服务范围 | 服务频率 | 配备服务工具 | 输出报告 |
| 现场服务 | 管理人员、信息技术人员 | 1年/1次 | 无 | 《梓潼县妇幼保健院安全培训课件》 |

### 2.14★服务工具要求

为保障安全服务效果，供应商需提供一体化运维服务平台工具。工具规格要求如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 指标 | 规格参数 |
| 1 | 基本要求 | 1.服务工具采用B/S设计架构，无须安装客户端，可通过浏览器远程对产品进行管理；  2.机架式设备，配置≥4个千兆电口；CPU：≥24核心48线程；内存：≥64G内存；硬盘≥1T\*2硬盘存储空间，冗余电源（≥2个电源）；  3.为简化运维，提高效率，节约机柜空间，不接受多平台或多产品组合方式提供。 |
| 2 | 授权及许可 | 1.扫描次数授权：无限制；  2.扫描IP/域名范围授权：无限制；  3.提供仿真业务陷阱授权数：无限制；  4.提供可监测网站授权数：无限制；  5.提供主动监测及漏洞屏蔽授权数：无限制；  6.提供互联网出口数据监测带宽：≥1G  7.提供二次开发接口授权； |

## 3.其他技术、服务等要求

1.服务质量保障：供应商应按照项目工作特点为项目服务人员提供必要的工作设备。工作设备在现场服务需要接入网络应遵守采购人的安全要求。供应商对参与的服务人员进行安全管理，服务人员安全管理不到位由供应商承担经济和法律责任，触犯法律的依法追究相关人员的法律责任。

2.应急响应要求：服务期内，当全国或采购人出现高危漏洞或突发重要网络安全事件以及暗网内出现有与采购人有关联的高危漏洞时，提供相应的紧急安全事件通告。采购人提出技术支持请求后，项目服务团队须在0.5小时内响应；当发生硬件故障时，在0.5小时内响应，并快速恢复系统正常运行；当硬件故障不能解决时，应在故障发生24小时内提供同档次或更高配置的设备对故障设备进行替换，完成配置，保证业务正常运转，直至故障设备修复后重新部署回原节点。供应商如未能在上述规定时间内解决故障并恢复系统运行，采购人有权请其他专业公司进行维修，所有费用由供应商支付。

3.网络安全与保密要求：供应商需提供安全保密承诺书，并与采购人签订供应链保密协议（适用于单位）、安全保密责任书（适用于单位）、个人保密协议（适用于个人）、安全保密责任书（适用于个人），承诺在服务期限内，遵守采购人的安全保密规定，保护采购人的系统、数据、信息的安全，保密期限自服务开始日始至本项目约定的信息全部成为公开信息止。由于供应商违反保密规定而导致的泄密或破坏，由供应商负全责，并由供应商赔偿采购人所有损失。违反保密规定的，采购人有权终止合同，并有权要求供应商向采购人支付合同金额20%的违约金，对由于供应商泄密给采购人造成的经济及声誉损失，采购人有权依照合同和相关保密法律法规追究供应商的法律责任。

4.★成交供应商在合同签订前须提供服务支撑工具的演示，在采购方确认满足服务所需要求后方可签订服务合同（需提供承诺函，格式自拟）。

5.★供应商需承诺在服务过程中，未经采购方书面同意，不得更换服务人员（需提供承诺函，格式自拟）。

# 二、评分标准

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评分项目 | 分值 | 评分依据 |
| 1 | 报价 | 10 | 以评标委员会认定的有效供应商的有效投标文件中的最低报价为基准价，其价格为满分。投标报价得分为(基准价／投标报价)×10。  根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）第九条和《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）的规定，本项目执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（10%）。  在磋商过程中，磋商小组认为供应商报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在合理的时间内进行书面说明，必要时提交相关证明材料。供应商提交的书面说明，应当加盖供应商公章，在磋商小组要求的时间内提交，否则视为不能证明其响应报价合理性。供应商不能证明其响应报价合理性的，磋商小组应当将其响应文件作为无效处理。（注：供应商报价低于最高限价50%或者低于其他有效供应商报价算术平均价40%的，磋商小组可以认为该供应商“报价明显低于其他实质性响应的供应商报价”。） |
| 2 | 类似业绩 | 15 | 供应商提供近三年以来的类似业绩，每提供1个得3分，最多得15分。 |
| 3 | 履约能力 | 43 | 1.供应商具有中国网络安全审查技术与认证中心的《信息安全风险评估服务资质》、《信息系统安全集成服务资质》、《信息系统安全运维服务资质》和《信息安全应急处理》，每具备1个服务资质得3分，最多得12分；（提供证明材料，加盖供应商鲜章） |
| 2.供应商具有质量管理体系认证证书（认证范围含网络安全技术服务）、环境管理体系认证证书（认证范围含网络安全技术服务）、职业健康安全管理体系认证证书（认证范围含网络安全技术服务）、信息安全管理体系认证证书（认证范围含网络安全技术服务）和信息技术服务管理体系认证证书（认证范围含计算机软硬件运维服务方向），每具备1个认证证书得3分，最多得15分；（提供证明材料，加盖供应商鲜章） |
| 3.供应商具有近三年来，具有地（市州）级及以上攻防演练经验，每具有一次攻防演练经验得3分，最多得12分；（提供证明材料，加盖供应商鲜章）  4.供应商近3年参与过重大活动网络安全保障任务，参与过以下任意1次重大活动网络安全保障任务(重大活动网络安全保障任务如冬季奥林匹克运动会、世界大学生运动会、亚洲运动会、G20金融峰会、一带一路国际合作高峰论坛等）得4分，不满足不得分。（提供证明材料，加盖供应商鲜章） |
| 4 | 服务团队 | 26 | 1.供应商拟派驻本项目的项目经理（1人），具有信息系统项目管理师（软考高级）认证证书、网络工程师（软考中级）认证证书、信息安全保障人员认证证书(CISAW）风险管理和注册信息安全管理人员（CISO）认证证书，每提供一个认证证书得2分，最多得8分；（提供证明材料，加盖供应商鲜章） |
| 2.供应商拟派驻本项目的技术负责人（1人），具有信息安全保障人员认证证书(CISAW安全运维）、信息安全保障人员认证证书(CISAW风险管理）、注册信息安全管理人员认证证书（CISO）、注册渗透测试工程师认证证书(CISP-PTE)和信息安全工程师（软考中级）认证证书，每提供一个认证证书得2分，最多得10分；（提供证明材料，加盖供应商鲜章） |
| 3.供应商拟派驻本项目的服务团队人员（项目经理和技术负责人除外），具有注册信息安全管理人员认证证书（CISO）、注册信息安全工程师认证证书（CISE）、注册渗透测试工程师认证证书(CISP-PTE)和注册数据安全治理专业人员认证证书（CISP-DSG），每提供一个认证证书得2分，最多得8分；（提供证明材料，加盖供应商鲜章。同一人员具有多个认证证书，按一个认证证书认定） |
| 注：人员须提供在职证明材料，加盖供应商鲜章。 |
| 5 | 服务方案 | 6 | 根据供应商提供的服务方案进行评分，包括但不限于①服务内容、②服务流程、③服务交付物、④服务计划、⑤服务工具、⑥服务承诺，全部内容完整有效的得6分，每有一项缺失扣1分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣0.5分，扣完为止。 |