成都市第五人民医院

整体安全运维服务市场调研参数

一、项目需求

1、安全运维服务

服务资产数至少200个，提供驻场服务人员2名。

（1）通过对安全工作总体负责人与安全技术人员进行现场访谈调研的形式对安全运营过程中的技术手段与管理流程的现状进行全面摸底，深入了解资产管理、威胁管理、漏洞管理、事件管理等安全运营工作的开展情况，针对具体细节进行适当探讨，必要时需要调阅相关技术报告与制度流程文档验证访谈结果，提升评估的准确性。

（2）需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度（提供漏洞优先级排序截图，展示优先级排序情况）提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，供应商跟进漏洞状态，各个处理进度透明，方便采购人清晰了解当前漏洞的处置状态，将漏洞处理工作可视化。

（3）针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。（提供漏洞修复方案样本，需包含多种修复方案以及修复过程中可能引发的其他问题的解决方案）针对服务平台生成的工单，采购人可按需催单，服务平台采用短信等方式通知安全专家，督促采购人第一时间处理。对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况。

（4）实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件。供应商根据安全事件分析的结果以及处置方式，根据采购人授权情况按需对安全组件上的安全策略进行调整工作基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案。

（5）支持面向采购人的安全状态展示，展示出采购人的业务和用户安全状态信息，使得采购人能直观感受到当前的业务和资产安全状态。支持面向采购人的安全态势展示，展示出当前采购人遭受的威胁事件信息以及脆弱性信息统计，使得采购人能直观感受到当前的风险态势情况。

（6）供应商需为采购人提供服务监控门户，在门户中可查看业务安全状态，处置中的失陷事件以及针对这些事件的处置进度，处置责任人、联系方式等信息，方便采购人实时了解供应商的服务效果。供应商需有可视化的措施监督安全专家的服务水平，从工单的响应、工单的审核以及工单处理等维度判断服务是否出现停滞。

（7）7\*24小时持续专家服务，威胁发现及时响应。对于特别重大安全事件应启动应急响应机制，10分钟之内云端专家进行响应，同城2小时上门处置，同省4小时上门处置。每个月认证工程师上门处置安全风险1次。

2、安全运营服务

（1）依据相关规范，结合采购人现状，开展移动端的安全检测工作。此项服务主要针对采购人拥有的多个移动端（IOS、安卓APP）及H5 等产品，降低移动应用普遍存在的破解、篡改、盗版、钓鱼欺诈、内存调试、数据窃取等各类安全风险；

（2）策略调整：供应商根据安全事件分析的结果以及处置方式，根据采购人授权情况按需对安全组件上的安全策略进行调整工作（需提供截图证明并加盖投标人公章）；

（3）当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题根除、协助业务恢复的服务，能够协助采购人快速止损，最大化降低安全事件带来的影响；

（4）基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况；

（5）实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件（需提供截图证明并加盖供应商公章）；

（6）失陷主机分析：供应商需对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议；

（7）需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度（需提供截图证明并加盖投标人公章）；针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助采购人快速恢复业务，消除或减轻影响

（8）对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得采购人可做到漏洞的可视、可管、可控（需提供截图证明并加盖供应商公章）；新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新；策略定期管理：每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果；需提供漏洞复测措施，及时检验漏洞真实修复情况。复测措施可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围。

3、IT设施运维服务

（1）机房主机设备维护管理：计算机服务器（包括PC服务器及存储服务器）；网络设备（交换设备等）。机房监控设备维护管理：供配电监测系统、温度环境检测系统、门禁设备系统、保安监控设备。

（2）机房空调与配电设备维护管理：空调设备、新风设备、UPS电池、主配电箱。

机房消防设备维护管理：烟感热感探测器、手动报警按钮和报警控制器、灭火器的控制装置。机房供水水路、电路及照明维护管理：水电路管线及接口的检查维护。

（3）机房基础维护管理：机柜线路的整理、标签检查更换、机房除尘清洁、防火地板、墙面、吊顶、门窗及相关配套的维护管理。

4、EDR控制平台升级

（1）Windows Server客户端授权包含智防、智控、智响应模块以及服务端防护（Webshell检测、暴力破解检测、僵尸网络检测、基线合规检查）

（2）PC-Windows客户端-智防模块包括：多维度漏斗型检测框架（包含文件信誉检测引擎，基因特征检测引擎，人工智能检测引擎，行为分析检测引擎，安全云脑检测引擎）威胁自动隔离，安全基线核查，文件实时监控，漏洞补丁，勒索诱饵）

5、网络安全设备特佂库更新

针对采我院现有安全设备：安全感知系统平台、防火墙设备、网闸等过保安全设备提供以下服务：一年特征库及相关规则库升级、一年硬件设备质保、一年软件升级。