关于网络安全运营服务和HIS,EMR网络安全等级保护测评服务(二级)

询价相关要求及参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **项目名称** | **服务内容要求** | **数量** | **计量单位** |
| 1 | HIS,EMR网络安全等级保护测评服务(二级) | 基于国家标准《CB/T22239-2019网络家全等级保护基本要求》项目清单范围内所有系统的等级保护测评服务，测评内容包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理，在测评过程中应使用符合等级保护相关标准要求的测评方法，并按照等级保护行业主管部门指定的报告模版要求，为每个被测评系统缩制信息系统安全等级保护测评报告。要求采购人使用测评工具至少支持以下功能：支持从网络安全等级保护基本要求的十大层面进行资产管理（网络、安全、服务器系统等）；能够进行漏洞等级通告、支持密码、越权等进行动态展示，支持对于高危风险、脆弱性、Web弱口令等行为进行动态监测展示；支持自定义测评/检查任务并且生成网络安全监督测评/检查表，支持表格的在线填报、佐证材料管理并生成检查任务。提供具有CMA和CNAS标识的第三方检测机构出具的测评工具功能检测报告原件扫描件及授权函并加盖制造商公章予以佐证。注:供应商须在检测报告中检测结果进行标识，未提供或提供不符合要求视为无效响应。 | 1 | 个 |
| 2 | 安全运营服务 | 一、智能威胁监测平台1、网络威胁检测及响应，网络安全状态展示，包括：攻击态势、主机入侵威胁态势等提供持续安全策略优化、AI边缘智能计算、协同防御情报能力，过滤海量安全日志告警噪音。旁路部署模式提供资产管理、威胁检测、脆弱性检查、蜜罐、旁路阻断能力。安全运营中心云端运营年服务授权，提供SaaS化托管威胁检测与响应服务，快速分析研判真实安全事件，保障安全事件的准确性，高效率为用户持续提供预测-防御-检测-响应的全生命周期网络安全服务。安全云运营服务交付物包括周/月度安全运营服务报告、工单、安全事件预警和处置建议（微信、邮件通知、APP）等。2、服务工具可提供全局IP阻断，支持基于源/目IP对监测到的攻击行为进行阻断或封禁，及时对发现的风险进行抑制，降低安全事件带来的损失。3、服务工具可提供DNS防御，支持基于异常DNS发现模型发现C&C通信，并支持基于DNS阻断已失陷资产与攻击者之间的恶意网络通信，避免机器进一步的数据失窃、系统被破坏，或者被勒索加密等安全事故。4、支持基于多源威胁情报，攻击者画像等，对网络环境中存在的各类入侵攻击和对外攻击进行发现，并可进行拦截和阻断。5、安全设备支持将发现的可疑攻击行为形成原始安全日志上传安全运营平台，并通过安全运营平台的关联分析规则对原始安全日志进行归并后，形成安全告警信息，安全运营团队基于告警信息分析研判出真实的安全事件；6、安全运营平台提供支持通过统一的界面查看工单服务情况，包括正在进行、已完成以及待评价的工单情况，并自主创建工单。可以针对已完成的工单详情进行查看，支持通过评星、文字描述等方式对该工单的处理情况进行评价二、安全日志分析服务1、提供持续关联分析策略优化、AI智能分析降噪、统一运营管理能力，大幅去除误报告警噪音，高效率开展异构安全设备告警统一分析研判，实现统一安全运营。三、安全事件处置服务1、快速定位主机的IP、MAC，主机名等相关信息。 对失陷主机快速分析，可以提供相应主机分析。根据安全威胁通告，远程对安全事件进行处置。对内网失陷主机及挖矿主机等提供处置建议2、流量监测工具提供工单管理，提供通过统一的界面查看工单服务情况，包括正在进行、已完成以及待评价的工单情况，并自主创建工单。可以针对已完成的工单详情进行查看，支持通过评星、文字描述等方式对该工单的处理情况进行评价。四、每日安全威胁通告1、对每日外网攻击行为进行分人工分析。分析结果实时汇报给客户。五、每月安全月报1、对每月攻击行为进行统计分析。分析结果及处置建议提供给客户作为参考。六、非法外联阻断服务1、对非法外联（恶意网站和恶意链接）进行检查。发现非法外联行为进行人工干预及拦截阻断服务。七、客户关怀服务1、对客户现有安全设备的使用情况包括：运行情况和运行状态进行完全问题排查，发现安全隐患及时告知客户，并提供相应的解决方案。对服务客户现有环境，提供对环境及现有安全设备的安全规则进行安全问题排查，发现安全隐患提出相关解决方案，配合客户解决安全隐患。八、情报服务1、运营平台推送，近期威胁情报推送服务包括：攻击者、恶意IP、恶意URL等相关信息。九、漏扫服务1、通过工具扫描对系统漏洞进行探测发现，人工排除误报后输出漏洞扫描报告。要求使用具有自主研发的商用安全评估工具进行实施，发现评估对象存在的web应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露等脆弱性问题。2、服务人员应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性。3、服务人员应提交针对性的解决方案，保证漏洞修复可落地。4、交付物：《安全漏洞扫描报告》。 | 1 | 年 |
| 3 | 安全设备维护服务 | 对于医院现有的安全设备，提供免费的版本升级。按客户的实际使用需求进行调试 ，策略优化服务，要求响应积极且熟练掌握设备使用技能。 |