# 项目背景

围绕着网络安全就是国家安全的战略，医疗单位为国家信息安全关键基础设施之一，是国家网络安全的重要组成部分，受到国家高度重视。随着医疗行业信息网络技术的深入应用和“互联网+医疗健康”的不断推进，党中央、国务院及医疗监管部门陆续出台了一系列信息化安全建设与管理的政策法规，并在不断完善医疗行业网络安全体系。

过去十年，我院信息安全建设经历了从“单点”到“体系化”的转变，为满足医院日益增多的业务系统使用需求以及信息安全防护需求，同时满足各项信息化合规要求，通过对医院信息安全防护架构不断优化提升，不断夯实信息安全的基石。

网络和信息安全建设工作是一项系统性工程，需要坚持常态化、长效化机制。结合国家已出台的有关信息安全政策和制度要求，为促进医院高质量发展。结合当下信息安全形势以及各级单位对于信息安全的合规性要求，对照我院目前的信息安全防护体系进行分析，我院的信息安全防护仍存在以下短板：

1. 针对应用安全，根据日常的信息安全事件监视和处置情况，应用安全问题大概占据50%左右，均是由于各类应用源代码设计缺陷或者源代码开源框架存在漏洞导致，在2022年红队攻击检测期间就被攻击者利用，从而被攻击者成功渗透到内网；因此亟需建立漏洞屏蔽机制，规避漏洞被扫描并被利用等风险；

2. 建立安全设备一体化联动机制，实现安全威胁的自动发现以及自动处置，规避人为处置出现的滞后短板；

3. 完善现有的安全服务闭环机制，目前建立了信息安全的“安全检测+通告+处置”的常态化工作机制，但是在最后的处置环节往往无法不够及时，由此导致安全风险增大，因此需要补强机制中的短板；

4. 初步建立数据安全治理手段，保护患者隐私信息，防止核心数据外泄；

5. 完成核心业务系统等级保护2.0测评复评；

6. 优化信息安全运维管理机制等他信息安全工作完善需要；

# 采购需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **技术要求** | **数量** | **推荐品牌** |
| 1 | 等保测评服务 | 详见技术要求章节 | 1套 | 安信检测、安远检测 |
| 2 | 安全服务1 MSS | 详见技术要求章节 | 1套 | 奇安信、深信服、安恒 |
| 3 | 安全服务2 | 详见技术要求章节 | 1套 | 奇安信、深信服、安恒 |
| 4 | 安全服务3 | 详见技术要求章节 | 1套 | 奇安信、深信服、安恒 |
| 5 | 云端威胁分析平台 | 详见技术要求章节 | 1套 | 奇安信、深信服、安恒 |
| 6 | 外网镜像交换机 | 详见技术要求章节 | 1台 | 盛科、数维 |
| 7 | 安全态势运营平台 | 详见技术要求章节 | 1套 | 奇安信、深信服、安恒 |
| 8 | 安全DNS | 详见技术要求章节 | 1套 | 奇安信、zdns |
| 9 | 漏洞屏蔽系统 | 详见技术要求章节 | 1套 | 青藤云、奇安信、安恒 |
| 10 | 云waf | 详见技术要求章节 | 3年 | 安恒 |
| 11 | 安全设备监控系统 | 详见技术要求章节 | 1套 | 云新、华际、 |
| 12 | 集成技术服务 | 详见技术要求章节 | 1套 | / |

# 技术要求

## 等保测评服务

|  |  |
| --- | --- |
| **指标名称** | **指标要求** |
| 等保测评内容 | 包含2个三级、2个二级系统复评 |
| 测评厂商资质要求 | 测评厂商具有信息安全风险评估服务资质证书二级  测评厂商具有信息安全应急处理服务资质证书三级  测评厂商具有源代码备份漏洞利用工具软件著作权证书、源代码安全审计检测系统软件著作权证书、移动安全检测系统著作权证书、验证码安全加固认证系统著作权证书、网站安全扫描工具软件著作权证书  测评厂商连续三年荣获国家信息安全等级保护工作协调小组办公室授予的先进单位且获得全国网络安全等级保护测评机构网络安全攻防大赛获奖证书 |
| 其他要求 | 要求在签订合同后2个月内提供测评报告 |

## 安全服务1 MSS服务

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务内容 | ★本次提供不少于60个资产的云端7\*24小时安全专家服务，提供流量检测服务≥500Mbps，检测服务器数量≥60个，云端威胁情报服务≥1年，移动运营助手服务≥1年，高级漏洞管理功能订阅服务≥1年 |
| 环境要求 | 平台SAAS化形态，无需要在数据中心进行任何下载和安装，通过账号密码在云端获取服务。 |
| 资产识别与梳理 | 需借助安全工具对资产进行识别和梳理，并在后续服务过程中根据识别的资产变化情况触发资产变更等相关服务流程，确保资产信息的准确性和全面性 |
| 安全现状评估 | 对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描 |
| 实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等 |
| 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。 |
| 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 |
| 分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为 |
| 漏洞管理 | 提供客观的漏洞修复优先级排序，排序依据包含资产重要性、漏洞等级以及威胁情报三个维度 |
| ★提供漏洞工单跟踪功能，展示工单跟踪状态，包含漏洞发现、漏洞验证、漏洞处置、漏洞复测等状态，方便清晰了解当前漏洞的处置状态，将漏洞处理工作可视化（提供功能截图证明） |
| 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 |
| ★针对服务平台生成的工单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置（提供功能截图证明） |
| 提供漏洞复测措施，及时检验漏洞真实修复情况，用户可针对指定漏洞进行，降低漏洞复测时的潜在影响范围 |
| 威胁管理 | ★实时监测网络安全状态，对攻击事件自动化生成工单，提供工单跟踪功能，展示工单跟踪状态，包含发现风险、专家审核、跟踪处置等状态（提供功能截图证明） |
| 结合威胁情报，投标方需排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固 |
| 平台展示 | 支持展示出当前遭受的威胁事件信息，提供服务平台漏洞表、事件表统计信息，并支持按照资产类别、威胁类型进行筛选查看。 |
| ★服务平台可生成各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全服务运营月报》、《安全服务运营周报》等。（提供功能截图证明） |
| 服务平台支持导出安全报告，可自定义报告中展示的模块，包括但不限于事件管理、攻击威胁、策略管理、脆弱性管理。 |
| 工单类型 | 平台支持的工单类型应包含内部威胁工单、外部威胁工单、脆弱性工单、应急工单、策略工单、其他工单。 |
| 告警工单管理 | 威胁告警应显示出威胁类型，威胁发生时间，攻击者IP，被攻击者IP，威胁描述，攻击趋势等信息。 |
| 服务质量监督 | 提供服务监控门户，在门户中可查看资产安全状态信息，展示纬度包括服务资产安全评级、服务运营状态及成果、安全风险概览、最新情报等。 |
| ★提供服务质量可视化展示，可以清晰地了解安全专家的服务水平，展示维度包括漏洞闭环率、漏洞平均响应时长、漏洞平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均响应时长、事件平均闭环时长等。（提供功能截图证明） |
| 服务交付物 | 交付物名称：《安全服务运营报告》，报告频率：每周一次 |
| 交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数 |
| 交付物名称：《安全通告》，报告频率：按需触发，不限次数 |
| 交付物名称：《综合分析报告/运营月报》，报告频率：每月一次 |
| 交付物名称：《季度汇报PPT》，报告频率：每季度一次 |
| 交付物名称：《年度汇报PPT》，报告频率：每年一次 |
| 资质要求 | ★为保障安全服务质量和效果，服务厂商安全运营平台的平台能力和人员服务能力需要符合《面向云计算的安全运营中心能力要求》标准，获得云计算开源产业联盟和中国信息通信研究院的认证，提供相关证明材料 |
| 便捷入口 | ★支持快捷入口配置，对关心的模块可标星置顶。实现自定义入口设定。（需提供截图证明） |
| 安全监控 | ★支持首页按日、周、月等时间周期展示风险总览、包括安全事件总览、资产统计、接入设备展示包括不仅限于防火墙、探针、EDR、CWPP，待处置安全事件TOP5、XTH云端威胁狩猎报告总览、攻击面TOP5、脆弱性资产TOP5、风险资产分布及风险资产发生趋势、待处置安全事件分布及安全事件发生趋势。智能对抗统计及对抗场景分析，可展示智能对抗记录，清楚明晰下一步处置方向。（需提供截图证明） |
| ★全网安全能力监控大屏支持展示网端数据源展示，并支持跳转相关日志检索页面。可直观展示日志到告警，告警到事件的消减比例。（需提供截图证明） |
| 数据采集 | 支持对Windows终端采集：进程、网络、注册表、文件、服务、计划任务、账号、WMI、应用漏洞利用探针、API等信息。对Linux终端采集：文件、进程、驱动、系统调用、模块事件等信息。  支持终端防护遥测数据采集：包含传统杀毒类日志、IOA类日志；  Windows系统上支持18种系统事件的遥测数据采集：包含进程销毁、文件创建事件修改、文件重命名、文件删除、远程线程注入、注册表删除、进程调用API、驱动加载、模块加载、WMI Filter创建、WMI Consumer创建、WMI Binding创建、计划任务创建、符号链接创建、命名管道创建、命名管道打开、VolumeSnapshot删除、敏感进程访问。  Linux系统上支持8种系统事件的遥测数据采集：进程创建、文件删除、文件重命名、文件创建、文件修改、DNS请求、网络链接、TCP端口监听。 |
| 威胁检测 | 支持攻击指标检测，对攻击者的攻击手法进行检测，指标覆盖ATT&CK所有阶段攻击手法，以检测攻击准确性为目标，通过采集的网端数据进行研判、挖掘。可以发现高级威胁。  支持自定义IOA规则。  支持终端遥测源对 ATT&CK 框架中各种攻击类型的检测技术覆盖面Windows系统不低于322项，Linux系统不低于127项。（需提供第三方报告证明） |
| ★支持云端专家提供轻量安全服务，进行持续的威胁狩猎，发现潜在威胁；在有攻击事件生成后，进行二次确认，通过Threat Hunting标签进行辨别，对热门威胁进行响应；（需提供截图证明） |
| 检测响应 | ★支持对安全事件推送处置和响应建议，响应建议包括原理介绍、危害影响、处置建议。通过建议描述、业务影响标签和安全效果标签清晰明确指导下一步响应动作，可一键封禁IP、隔离主机等。支持在线实时聊天框或离线留言咨询攻防专家，获取云端专家支持。（需提供截图证明） |
| 支持一键遏制功能，可联动网端防护设备使用端网能力一键处置关键实体，实现外部威胁不入内网，关键数据不出内网，保证内网安全。 |
| ★支持告警智能定性分析，通过分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认、从而确认安全告警的优先级顺序，帮助安全人员高效的完成攻击告警的运营工作，可归类人工渗透攻击，包括定向攻击、攻防演练、内部测试。程序自动化攻击，包括监管通报、病毒、扫描器攻击。业务风险相关，包括脆弱性风险、业务不规范，和其他威胁。（需提供截图证明） |
| 支持配置智能对抗开启及联动范围，页面可展示事件自动遏制率，可查看智能对抗记录及自定义对抗规则。 |
| 资产管理 | 支持展示资产统计、资产来源、资产类型分布、资产防护统计、资产互联网暴、指纹信息、高风险应用统计、特殊账号统计TOP5、端口TOP5统计、应用软件TOP5统计、数据库TOP5统计。 |
| 支持以资产组视角、业务视角的纬度展示资产详细台账，  资产组支持自定义，支持新增、编辑、删除等操作，可配置资产组的基本信息、资产组范围（可自动识别IP属性）和资产责任人。 |
| ★支持通过开放端口、应用软件、数据库、web服务、web框架、web应用、web站点、账号信息、运行进程、运行服务、启动项、计划任务、注册表维度进行资产清点。清点可展示相关资产列表及资产责任人、数据源。（需提供截图证明） |
| 风险管理 | 支持以资产视角，对终端遥测及网络遥测扫描到的资产脆弱性进行展示，可对资产修复优先级、风险类型、风险资产及资产组名、责任人等标签进行筛选，并通过图表进行统计展示资产修复优先级情况、脆弱性统计情况、资产脆弱性TOP5 |
| ★根据资产的维度呈现安全事件、安全告警、攻击面风险等多角度呈现问题，结合ATT&CK矩阵更好发现风险资产已知威胁和潜在风险。展示维度包括ATT&CK攻击图谱命中战术匹配；威胁检测事件告警举证；威胁实体IP、域名、文件、进程提取展示；脆弱性数量及修复优先级展示；潜在风险应用及风险端口展示；风险访问展示、异常信号展示。（需提供截图证明） |
| 支持风险黑客工具和运维工具的检查，至少25种风险应用检测，涵盖主流攻击入侵入口。包括黑客工具：NetworkShare、PsExec、PCHunter、KPortScan、Frp、ProcessHacker、Mimikatz、Nasp、WebBrowserPassView、PowerTool、CobaltStrike、Masscan、Fscan、NLBrute、PortScan、DefenderControl、Gmer、Netpass、DUBrute、Lazykatz。运维工具：ToDesk、向日葵、AnyDesk、Rdp\_Connector、TeamViewer。 |
| 响应策略 | 支持配置规则可按IP/域名/url联动防火墙设备进行封堵，封禁时长可按天/时/分细粒度进行设置。可对封禁对象进行删除、解封、再次封禁等操作（需提供截图证明） |
| 支持拦截域名功能，联动EDR/CWPP进行拦截域名，在拦截域名界面可查看拦截域名信息，并且支持取消拦截。（需提供截图证明） |
| 支持账号管理，展示登录账号信息，可对账号进行开启二次鉴权的动态口令。 |
| 支持角色创建和角色分配，内置包括安全管理员、超级管理员、审计管理员、系统管理员角色，可新建角色及配置相关编辑和查看权限。可对账号和角色进行关联，一个账号可以关联多种权限。（需提供截图证明） |
| ★针对外部威胁防止规模化的数据丢失、泄露、设备被控制，支持账号二次鉴权、设备管理二次鉴权、弱密码二次鉴权（需提供截图证明） |
| APP中心 | 平台支持可视化、免费的钓鱼演练工具。根据钓鱼演练的性质以及组织属性选择合适的钓鱼邮件模版，常见的钓鱼邮件种类可大致分为财务钓鱼、放假通知钓鱼、漏洞自检钓鱼、简历钓鱼等。 |
| 攻防百宝箱 | 支持智能调查功能，通过对威胁情报以及威胁实体IP、域名、MD5的检索，自动进行统计分析，提供全局威胁狩猎，进行快速调查溯源。（需提供截图证明） |
| 服务交付物 | 交付物名称：《安全服务运营报告》，报告频率：每周一次 |
| 交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数 |
| 交付物名称：《安全通告》，报告频率：按需触发，不限次数 |
| 交付物名称：《综合分析报告/运营月报》，报告频率：每月一次 |
| 交付物名称：《季度汇报PPT》，报告频率：每季度一次 |
| 交付物名称：《年度汇报PPT》，报告频率：每年一次 |
| 资质要求 | ★为保障安全服务质量和效果，服务厂商安全运营平台的平台能力和人员服务能力需要符合《面向云计算的安全运营中心能力要求》标准，获得云计算开源产业联盟和中国信息通信研究院的认证，提供相关证明材料 |

## 安全服务2

|  |  |  |
| --- | --- | --- |
| **服务类** | **技术类型** | **指标要求** |
| 渗透测试 | 服务要求 | 1、每年不少于2次，不限制系统数量。 |
| 2、投标方应保证招标方信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助招标方理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全。 |
| 3、投标方应在得到招标方授权后方可开始实施渗透工作。 |
| 4、投标方应确保实施渗透测试的服务人员的工作保密性，签署相关的保密协议，在未经招标方允许的情况下，不得将识别的漏洞外泄、传递。 |
| 4、实施渗透测试服务后，未经招标方同意，禁止在系统留存后门。 |
| 服务内容 | 1、招标方授权后，投标方应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试 |
| 2、渗透测试应至少包括但不限于以下范围的漏洞：   * WEB业务系统 * 微信小程序、微信公众号 * API * C/S架构系统   3、渗透测试内容包括但不限于：   * 信息泄露 * 信息猜解 * 认证信息泄露 * 认证信息猜解 * 认证功能失效 * 认证功能滥用 * 数据猜解 * 专项漏洞 * 综合利用 * 权限篡改 * 权限缺失 * 防护功能滥用 * 防护功能缺失 * 防护功能失效 * 业务逻辑篡改 * 业务功能滥用 * 业务功能失效 |
| 4、投标方渗透测试人员应使用不同技术手段发现不同纬度的漏洞，并进行验证，形成记录和报告。 |
| 5、投标方应编写渗透测试报告并提交给招标方，报告应该阐明招标方业务系统中存在的安全隐患以及专业的漏洞风险处置建议。 |
| 漏洞扫描 | 服务要求 | 1、每年不少于2次。 |
| 2、漏洞扫描应按照以下要求实施：   * 投标方应对漏洞扫描的目标对象进行全面梳理和识别，识别内容包含但不限于资产类型、IP地址、业务部门、责任人、用途、操作系统、数据库、中间件等 * 投标方应提交漏洞扫描工具的情况（包括但不限于：设备厂商、设备型号、漏洞库、销售许可证等）、漏洞扫描工作方案（包括但不限于：目标对象、扫描时间、风险规避措施等）及漏洞扫描申请，招标方授权后，方可进行 * 投标方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 * 投标方应提交针对性的解决方案，保证漏洞修复可落地 |
| 3、漏洞扫描对象范围包括但不限于：   * 网络设备：路由器、交换机等 * 操作系统：windows、linux、UNIX等 * 数据库：Oracle、MS SQL、Mysql等 * 中间件：Apache、Tomcat、IIS、weblogic等 |
| 4、可对WEB漏洞进行扫描检测，包括但不限于：   * 信息泄露 * SQL注入漏洞 * XSS注入漏洞 * 目录遍历漏洞 * 本地文件包含漏洞 |
| 5、可对系统漏洞进行扫描检测，包括但不限于：   * 溢出漏洞 * 拒绝服务攻击漏洞 * 未授权访问漏洞 * 代码执行漏洞 |
| 敏感数据泄露监控服务 | 服务要求 | 提供不少于 1 年敏感数据泄露监控服务 |
| 首次互联网敏感数据泄露历史情况排查 | 投标方根据招标方提供的敏感数据关键字导入到后端的威胁情报信息收集平台，收集相关信息，安全服务专家会对平台发现的相关信息进行过滤和整理，输出针对招标方的定制化互联网敏感数据泄露排查报告。 |
| 实时互联网敏感数据泄露监控 | 投标方每月度根据招标方提供的关键字在互联网进行信息收集与匹配，一旦发现异常的情况会直接通过邮件等方式推送给招标方。 |
| 线上安全服务专家指导答疑 | 投标方需接受招标方对于日常服务中碰到的问题（如报告疑问以及处置建议）的提问并答疑。 |
| 月度报告 | 投标方每个月梳理本月发生的安全事件总结形成报告提供给招标方 |
| 年度报告 | 投标方每年底会形成招标方本年度的互联网敏感数据泄露情况报告 |
| 暗网情报监控 | 支持隐匿暗网平台监控，暗网中文交易市场、茶马古道、自由国度、白宫市场等数十个暗网平台 |
| 支持黑客论坛监控，RaidForums、Rutor、Exploit.in等数十个黑客活跃地区的地下论坛 |
| 支持勒索团伙站点监控，REvil、Avaddon等数十个知名勒索团伙站点 |
| 代码泄露监控 | 支持国外代码托管平台监控，主要包括GitHub、GitLab、Pastebin等主要国外代码托管/共享平台 |
| 支持国内代码托管平台，主要包括码云Gitee等主要国内代码托管平台 |
| 敏感文件监控 | 支持网盘文件监控，包括百度网盘、腾讯微云、115网盘、新浪微盘、蓝奏云、MEGA等 |
| 支持文库文件监控，包括百度文库、道客巴巴、360doc、豆丁网等 |
| 黑产舆情监控 | 支持匿名设计软件监控，Telegram、Potato等黑客常用的即时聊天平台 |
| 资产失陷监控 | 支持风险DNS/URL、IP等海量威胁情报数据 |
| 仿冒网站监控 | 支持仿冒网站、钓鱼网站、域名抢注等网站情况监控 |
| 暗网泄露事件 | ★支持面向招标方检出暗网事件的展示，主要从暗网交易标题、暗网卖家ID、发帖事件、交易链接、交易内容等维度展示出当前招标方泄露的暗网事件信息，使得招标方能直观了解到当前泄露的暗网事件情况。（提供暗网情报监控功能截图） |
| 代码泄露事件 | ★支持面向招标方检出代码泄露事件的展示，主要从代码项目名称、代码链接、命中关键字、关键字代码片段等维度精准定位到当前招标方泄露的代码信息，使得招标方能直观了解到当前泄露的代码事件情况。（提供代码泄露监控功能截图） |
| 文件泄露事件 | ★支持面向招标方检出网盘/文库泄露事件的展示，主要从文件标题、发布时间、文件链接、文件内容等维度精准定位到当前招标方泄露的文件信息，使得招标方能直观了解到当前泄露的文件信息的情况。（提供文件泄露监控功能截图） |
| 黑产舆情事件 | ★支持面向招标方检出黑产舆情事件的展示，主要从黑产论坛网站、涉及舆情群组、发布时间、黑产舆情内容等维度精准定位到当前涉及招标方黑产舆情相关信息，使得招标方能直观了解到当前存在的黑产舆情事件的情况。（提供黑产舆情监控功能截图） |
| 资产失陷事件 | ★支持面向招标方检出资产失陷事件的展示，主要从失陷资产、失陷类型、失陷时间、具体失陷情况等维度精准定位到当前招标方资产失陷的信息，使得招标方能直观了解到当前自身资产的健康情况。（提供资产失陷监控功能截图） |
| 仿冒网站事件 | ★支持面向招标方检出仿冒网站的事件展示，主要通过语义特征和机器视觉等维度精准定位到当前招标方在互联网上被仿冒的信息，使得招标方能直观了解到当前网站在互联网上被仿冒的情况（提供仿冒网站监控功能截图） |
| 交付物 | 交付物名称：《敏感数据监控服务首次排查报告》，报告频率：敏感信息排查服务仅有这个交付报告 |
| 交付物名称：《敏感数据监控服务月度报告》，报告频率：1年12次 |
| 交付物名称：《敏感数据监控服务年度报告》，报告频率：1年1次 |
| 交付物名称：《敏感数据监控服务事件报告》，报告频率：按需触发，不限次数 |
| 知识产权 | ★敏感数据泄露监控平台具备自主知识产权，具备两项在申请中的发明专利： |
| 1、《一种主体识别方法及相关装置》 |
| 2、《一种数据筛选方法及相关装置》 |
| 红队检测 | 服务要求 | 1、每年不少于2 次。 |
| 2、投标方应保证不影响招标方信息系统正常运行前提下，以APT攻击者视角对招标方现有防御体系进行检测，针对目标系统、人员、软硬件设备、基础架构，进行多维度、多手段、对抗性模拟攻击，发现招标方现有防御体系的短板，深入检验网络安全防护能力。 |
| 3、投标方应在得到招标方授权后方可开始实施红队检测工作。 |
| 服务方案 | 1、投标方应根据招标方安全需求及重要业务系统结构，设计针对性的红队检测方案，并提交至招标方进行评审。 |
| 2、投标方应在投标文件技术部分详细说明红队检测的实施流程、红队检测方法、实施过程中用到的工具、实施过程中可供考量的具体工作指标及各阶段输出成果。 |
| 3、投标方提供的红队检测方案必须包括但不限于：   * 红队检测方法和流程 * 红队检测实施方案 * 红队检测须采用专业检测工具如国内外商业检测工具、自有检测工具 * 提供红队检测所面临的主要风险及相应的风险规避措施 |
| 服务内容 | 1、招标方授权后，投标方应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试。 |
| 红队检测的目标范围应包括但不限于：   * Web相关业务系统，包含相同域名或IP下的不同端口的业务系统 * 微信小程序、微信公众号等移动端接入点 * APP服务器（不涉及APP客户端的逆向分析） * 数据库系统（如：Redis、Mysql、Mssql、Oracle等） * 协商的授权范围（如：集团总部、具体二级子公司等） * 其他常见的业务服务（如：邮件系统、RDP、SSH等） |
| 3、红队检测的服务检测内容不仅包括目标系统本身，还会对攻击路径上可能涉及到的系统都进行安全检测，涉及到的测试类别包括但不限于：   * 安全设备类 * 服务器、主机类 * 网络设备类 * 数据库类 * 集权系统类 * 第三方应用类 * Web安全类 |
| 投标方红队检测人员应针对招标方实际情况，使用不同技术手段发现不同纬度的安全风险和隐患，形成记录和报告。 |
| 如有必要，在客户授权下，投标方红队检测可针对员工、高管、供应商等进行远程社工测试。投标方红队检测人员针对招标方员工展开，包括企业的员工以及第三方合作人员，通过获取企业员工敏感信息或者利用员工计算机获得内网的入口并以此为跳板进一步开展内网的渗透测试。 |
| 如有必要，投标方红队检测人员可近在客户授权情况下，红队检测人员会靠近或位于测试目标建筑内部，开展身份识别绕过、本地网络嗅探、硬件系统漏洞利用、树莓派接入评估等安全检测手段，以绕过身份识别、嗅探重要信息、获得系统权限、获得员工信息为目的，揭示如何在真实情景中绕过物理障碍，从而未授权访问导致数据泄露和系统或者网络受损。 |
| 投标方应在完成检测后，编写红队检测报告并提交给招标方，报告应该阐明招标方安全体系中存在的安全隐患以及对应的专业风险处置建议。 |
| 服务交物 | 《红队检测报告》 |
| 《红队检测总结报告》 |
| 外部攻击面管理 | 暴露面检测 | 投标方须识别招标方当前暴露在互联网的资产，动态测绘企业安全的风险边界。对招标方暴露在互联网的web服务/域名/IP进行发现、识别和监测。 |
| 投标方针对招标方在互联网开放的高危资产和端口进行信息收集，通过梳理信息，收敛已知和未知的暴露面，增加攻击者在信息收集时的难度，增加攻击者准备时间，降低单位资产被外部攻击的可能性。 |
| 敏感数据监测 | 投标方根据招标方提供的敏感数据关键字导入到后端的威胁情报信息收集平台，收集相关信息，安全服务专家会对平台发现的相关信息进行过滤和整理，输出针对招标方的定制化互联网敏感数据泄露排查报告 |
| 投标方每个月梳理本月发生的安全事件总结形成报告提供给招标方；每年底会形成招标方本年度的互联网敏感数据泄露情况报告 |
| 支持隐匿暗网平台监控，暗网中文交易市场、茶马古道、自由国度、白宫市场等数十个暗网平台；支持黑客论坛监控，RaidForums、Rutor、Exploit.in等数十个黑客活跃地区的地下论坛；支持勒索团伙站点监控，REvil、Avaddon等数十个知名勒索团伙站点 |
| 支持国外代码托管平台监控，主要包括GitHub、GitLab、Pastebin等主要国外代码托管/共享平台；支持国内代码托管平台，主要包括码云Gitee等主要国内代码托管平台 |
| 支持网盘文件监控，包括百度网盘、腾讯微云、115网盘、新浪微盘、蓝奏云、MEGA等；支持文库文件监控，包括百度文库、道客巴巴、360doc、豆丁网等 |
| 支持匿名设计软件监控，Telegram、Potato等黑客常用的即时聊天平台 |
| 支持风险DNS/URL、IP等海量威胁情报数据 |
| 支持仿冒网站、钓鱼网站、域名抢注等网站情况监控 |
| 攻击面分析 | 投标方外部攻击面管理平台通过主动扫描、被动扫描、数据检测和人工资产管理的方式，将资产数据输入到外部攻击面管理平台，由平台自动进行漏洞扫描和攻击分析。 |
| 投标方根据威胁情报的漏洞等级，对当前外部攻击面的风险进行分类分级，确定关键风险的优先级，并给出关键风险的处置建议。 |
| 投标方攻击面分析范围包括客户所授权的所有网络区域及区域内的安全设备，包含互联网已知和未知资产，内网所有网络区域和安全设备。 |
| 服务频次 | 每年不少于 2 次 |
| 服务交付物 | 1、《XX单位\_暴露面发现结果确认表》 |
| 2、《XX单位-外部攻击面管理服务报告》 |
| 3、《XX单位\_外部攻击面管理服务问题跟踪列表》 |

## 安全服务3

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 重要时期现场保障服务 | 1、在重大节日及庆祝活动保障期间，根据实际情况进行现场安全值守，提供安全应急响应的技术支持，提出安全建议，判断事件类型，处理安全事件，降低安全风险和影响，并每日提交日报。  2、提供一名安全服务专家现场驻场服务。  3、服务周期：一年，至少提供2次。  4、为保证服务质量和水平，要求提供服务的原厂商为CNCERT应急服务支撑单位(APT监测分析)，提供证书复印件。 |
| 应急响应服务 | 1、提供应急响应处置服务，应对突发/重大安全事件第一时间响应、第一时间协助处置。实施安全事件检测、安全事件抑制、安全事件根除、安全事件恢复、安全事件总结，增强应急技术能力，健全应急响应机制。安全事件处置完成，系统得到恢复，提供安全事件应急响应报告。  2、服务周期：一年，按需提供；  3、为保证服务质量和水平，提供服务的原厂商为CNCERT网络安全应急服务支撑单位（国家级）和具备通信网络安全服务能力评定证书-应急响应（二级）资质；（提供证书复印件）。 |
| 安全巡检服务 | 1、提供安全巡检服务，对部署的各类安全设备提供设备运行状态、检测规则升级、安全日志等进行巡检，发现异常及时上报，并提供安全巡检报告。  2、服务周期：一年，至少1季度/次。  3、提供服务的原厂商具备信息通信行业企业信用等级评价—运维服务领域（AAA级别），提供证书复印件。 |
| 天眼平台报告服务 | 1、提供远程天眼平台安全分析服务，对天眼平台上相关告警及进行分析研判，包括病毒木马攻击行为分析、爆破行为分析、web攻击行为分析、数据库攻击行为分析、恶意邮件行为分析等，及时发现潜在或正在攻击的安全风险及事件，提出对应整改建议，并输出报告。  2、服务周期：一年，至少1月/次。  3、提供服务的原厂商为CNCERT应急服务支撑单位(APT监测分析)，提供证书复印件； |

## 云端威胁分析平台

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 性能指标 | 吞吐性能≥1Gbps |
| 硬件指标 | 规格1U，内存≥8GB，硬盘≥128GB minisata SSD，单电源，接口≥6个千兆电口+2个千兆光口 |
| 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响 |
| 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录。 |
| WEB智能检测 | ★支持命令注入检测、PHP代码检测、XSS攻击检测、Webshell上传检测、SQL注入检测、XXE攻击检测、JAVA代码检测、SQL非注入型检测、MYSQL解析增强、php反序列化检测等自定义配置启用、高检出、低误报模式。（提供功能截图证明） |
| 敏感信息检测 | 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤。 |
| 高级检测 | ★支持5种类型日志传输模式，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求（提供功能截图证明） |
| 支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。 |
| 支持传输访问检测日志，包括正常访问、风险访问、违规访问。 |
| ★支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域协议审计日志、WEB登录审计日志、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志。（提供功能截图证明） |
| 违规访问检测 | 支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式 |
| 沙盒对接 | 支持将流量还原的文件发送至沙盒分析，可支持第三方沙盒对接 |
| 特征库 | 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。 |
| 抓包分析 | ★支持流量抓包分析，基于五元组灵活抓取数据包，可定义配置源IP、源端口、目的IP和目的端口、传输层协议以及标签类型（vlan、vxlan、mpls）选择添加抓包任务，接口额外提供标签选项，帮助安全工程师高效分析威胁。（提供功能截图证明） |
| 接入要求 | ★要求该探针支持接入SaaS-XDR平台，上传安全日志和解析数据，在平台上展示来自探针的数据来源（提供功能截图证明） |
| 质保服务 | 提供探针特征库软件升级不少于5年，产品质保不少于5年，软件升级不少于5年 |

## 外网镜像交换机

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 国产化 | 必须基于ASIC架构，核心转发芯片必须是国产 |
| 硬件形态 | 要求产品为标准1U机架设备，支持固定单电源、冗余风扇  支持至少2G 内存, 8G Flash  支持至少9M包缓存  支持设备前面板上有USB接口、Console口、以太网管理口  支持至少8个10G SFP+光口  支持至少24个10/100/1000M RJ45电口 |
| 端口聚合 | 端口聚合组数量最少16组，每个端口聚合组支持的成员端口数最少可以到64个 |
| 性能 | 支持208Gbps线速转发能力 |
| 接口 | 支持链路震荡检测（link-flap）,检测到链路频繁UP/Down震荡后可以自动把接口shutdown，允许定时恢复 |
| 支持interface range，可以批量操作多个接口 |
| 管理 | 支持Syslog，snmp, telnet, ssh, web, radius, tacacs+, tftp, ftp，ntp |
| 支持异常用户锁定 |
| ACL过滤Telnet/SSH的登录接入 |
| 支持目录和文件管理 |
| 可以安装多个软件image，选择其中一个启动，以便于做备份 |
| 流量统计 | 支持SFlow  支持IPFIX |
| 可编程 | 支持开放的RPC API |
| 去重 | 支持去重 |
| 报文复制 | N个端口进来的报文转发到M个端口，N>=1, M>=1 |
| N个端口进来的报文转发到一个负载均衡组，选择一个出口出去。支持同源同宿负载均衡 |
| 可以对报文根据2-4层字段进行过滤，有条件的进行转发 |
| 可以在入方向和出方向分别进行过滤 |
| 支持将报文从入端口转发出去 |
| 负载均衡 | 支持Hash和轮询的负载分担方式 |
| 支持crc和xor两种Hash算法，用户可配 |
| 这些字段可以参与Hash计算：源Mac，目的Mac,源IP,目的IP, Protocol，L4源端口，L4目的端口，VxLAN VNI, GRE Key， GRE VSI。 如果是tunnel报文，则报文内层的源Mac，目的Mac,源IP,目的IP, Protocol，L4源端口，L4目的端口都可以参与。 |
| 报文匹配过滤 | 可以基于匹配的报文字段进行分发和过滤，包括以下字段：   1. 支持匹配IPv4目的IP， IPv4源IP， IPv6目的IP， IPv6源IP 2. 支持匹配TCP/UDP目的端口（支持范围匹配），TCP/UDP源端口（支持范围匹配）,DSCP, 4层protocol字段， TCP选项（ack | fin | psh | rst | syn | urg）, Ip-precedenc, 是否分片，是否首分片，是否小分片,是否携带IP Option 3. 支持匹配EtherType, 目的Mac，源Mac, Vlan, Cos 4. 支持匹配双层vlan TAG的内外层vlanId和内外层Cos 5. 支持匹配nvgre tunnel/vsid, VxLan Tunnel/VNI, ERSPAN Key, 6. 支持至少可以匹配4 层 MPLS label 7. 支持匹配PPPOE的PPP Type 8. 支持匹配用户自定义字段 |
| 单通 | 可以支持端口单收以及单发，光模块只插单纤端口也能UP。 |
| 去重 | 支持报文去重 |
| 报文编辑 | 支持修改报文的源Mac,目的Mac,源IPv4/IPv6, 目的IPv4/IPv6 |
| 支持去掉1层或者2层Vlan TAG |
| 支持增加和修改Vlan TAG |
| 支持将转发出去的报文打上时间戳，可根据本地或者NTP作为时间源 |
| 支持将VxLAN/GRE/IPinIP头剥掉，内层报文转发出去 |
| 支持将进来的报文加上vxlan header或者L2GRE header或者L3GRE header送出去 |
| 支持将MPLS头剥掉，内层报文转发出去 |
| 支持将ERSPAN的头剥掉，内层报文转发出去 |
| 可以将转发出去的报文截短，截短的长度全局指定，可以基于端口或者基于流来enable/disable该功能 |
| 规格大小 | 支持至少512个TAP group  支持至少1800条入方向过滤规则  支持至少250条出方向过滤规则 |
| 售后服务 | 提供原厂商三年保修服务，投标时提供原厂商售后服务承诺函 |

## 安全态势运营平台

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 硬件配置 | 2U标准上架设备，含滑轨；CPU: 2颗12核 主频2.2 GHZ ；内存： 256G（总容量）DDR4；硬盘1：2块960G SSD固态硬盘组成Raid 1；硬盘2：12\*4TB企业级SATA 3.5寸硬盘，总容量48T；电源：冗余双电源；网口：4\*GE管理电口、2\*SPF+插槽（含两个多模光模块）；其他接口：3\*USB3.0接口;1\*DB9 Console接口；提供五年产品标准维保服务（含硬盘保留服务），自签收之日起开始计算。 |
| 部署方式 | 支持单台服务器部署和集群部署，为灵活适应现场环境，须满足软硬一体化形态和纯软件形态部署模式。 |
| 数据采集与存储 | 支持接入并管理日志采集器、流量采集器，可支持第三方采集器接入；  支持对网络设备、安全设备、服务器、应用等日志进行解析、范式化、预处理；  支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、agent等采集方式；  支持文件导入的方式导入日志数据，支持的文件类型至少包含csv、.log、txt； |
| ★日志接入支持界面交互式配置，通过图形化界面配置日志解析条件，利用正则表达式、分隔符、Key-Value、JSON等方法定义解析规则，系统自动生成解析规则，无需通过代码编写解析规则（提供相关功能的界面截图）； |
| 支持自定义日志类型功能，支持对日志类型名称、存储方式、存储时间、分区方式、重要度等基础属性信息进行配置，达到分类存储日志的目的； |
| ★支持与现网两台流量探针进行对接，可作为平台的流量探针来使用，流量探针将全流量网络日志数据和告警日志数据推动至平台进行综合分析。（提供功能截图，并提供原厂承诺函加盖公章） |
| ★威胁情报 | 支持本地威胁情报的检索，检索类型支持域名、IP地址、文件MD5值；威胁情报内容支持IOC、攻击链阶段、置信度、类型描述、威胁家族、攻击事件/团伙、影响平台、情报状态、威胁描述等；  支持云端威胁情报查询，查询结果需包含：IP主机信息、IP位置信息、域名流行度、情报IOC详情、相关样本、可视化分析、域名解析记录、域名注册信息、关联域名、数字证书等信息；  支持自定义威胁情报，支持类型包含IP地址、域名、MD5、域名:URI、IP地址:URI、域名:端口、IP地址:端口、域名:端口:URI、IP地址:端口:URI。支持自定义IPv6的威胁情报。  提供原厂商至少10份以上公开发布的APT报告作为证明；（提供APT报告与官网截图） |
| 资产管理 | 支持主机资产和网站资产管理功能，并分别提供不同管理模块，支持主机资产和网站资产的关联管理。主机资产的类型包括但不限于IOT设备、服务器、工作主机、网络设备、安全设备、终端安全管理、数据库服务器、中间件服务器、存储设备、应用服务器、安全域、虚拟化设备。  支持对主机资产的服务信息进行管理，服务信息应包括：IP地址、端口、协议、服务名、服务版本和Banner；支持对IPV6资产的管理，支持对资产分类、资产属性进行自定义扩展。 |
| 支持DHCP场景下的资产管理，支持对DHCP网段范围、DHCP租期等属性进行配置。支持查看DHCP场景下资产IP的变更记录。 |
| ★支持与现网的服务器安全加固系统、终端管理系统进行协同对接，同步资产信息，支持对发现资产的方式的优先级、资产更新策略进行配置。（提供相关功能的界面截图） |
| 威胁预警 | 支持对重大网络安全事件（如永恒之蓝）进行威胁预警，通过厂商对重大网络安全事件的追踪生成预警包，通过预警包导入完成网络安全事件的影响面评估，并持续的跟进事态的发展，快速完成重大网络安全事件的预警及处置。  针对此类风险支持统计潜在风险资产数、受攻击资产数、失陷资产数以支持对重大网络安全事件进行威胁预警。  针对此类风险支持统计潜在风险资产数、受攻击资产数、失陷资产数以及资产的日同比及周同比对比。支持影响面趋势视图统计分析。支持基于网段潜在风险资产数、受攻击资产数、失陷资产数责任人等影响面分布。  支持根据风险资产数量统计自定义关键点节点条件，比如大面积爆发、有效控制、威胁缓解等。支持事态扩散过程发展趋势图的展示及详细告警列表及告警信息展示。 |
| ★脆弱性管理 | 系统至少支持绿盟、启明、网神、天融信、Tenable五款漏扫报告的解析识别和导入管理，支持人工漏洞报告导入，使用模板进行漏洞信息的导入；（提供相关功能的界面截图）  支持对绿盟、启明、网神、Tenable中至少两款主流扫描设备进行漏洞扫描任务调度和弱口令扫描任务调度，支持对绿盟、启明、网神、盛华安至少三款第三方配置核查扫描报告及人工配置核查报告的的解析识别和导入管理； |
| 支持通过网络流量同步漏洞、弱口令信息；支持和现网的服务器加固系统、终端管理系统协同对接，同步漏洞信息；支持直接同步绿盟漏扫设备的漏扫任务及扫描结果；支持直接同步盛华安配置核查系统的配置核查扫描任务和扫描结果。（提供相关功能的界面截图）  漏洞信息、弱口令、配置核查可直接调用工单系统，漏洞信息可直接添加到调查任务，支持添加到已有任务或创建新的调查任务； |
| 威胁检测 | 支持分析不同厂商、不同种类安全设备上报的告警日志，对其进行威胁分类、危害定级、有效性筛选以及重复告警归并；支持分析AD域、服务器、VPN、网站等系统的日志，对账号攻击事件、失陷事件、违规事件、可疑事件进行监测；支持分析Windows、Linux服务器的日志，对服务器失陷事件、违规事件、可疑事件进行监测，ATT&CK技术项覆盖率达到44%；支持分析网络流量，对网络入侵事件、恶意软件事件、威胁情报事件进行监测；支持分析阿里云平台各安全设备的告警日志，对其中的安全、违规、可疑事件进行监测。  支持自定义关联规则，支持类VISIO的图形化连线拖拽的交互配置方式而非编辑逻辑语法树配置方式，支持对日志配置基本的、复杂的数理统计\数值比较分析模型、时序分析模型、多源关联分析模型；支持通过日志命中对自定义关联规则的有效性进行验证，并对产生的告警支持删除或转为威胁告警；支持将日志同资产信息、漏洞信息、威胁情报信息进行关联分析；支持定义数值、IP、字符、端口类黑\白名单，并在分析模型中直接使用；支持通过配置模型自动输出黑/白名单数据。（提供相关功能的界面截图）  支持分析数据库访问日志、Web访问日志、邮件传输日志、Windows/Linux服务器、AD域日志、VPN日志等；支持9大类行为异常场景：Web应用异常、进程异常、数据库应用异常、用户操作数据库异常、用户传输文件异常、用户登录行为异常、用户访问应用系统异常、用户收发邮件异常、账号异常。  支持对不同类型实体的个体、群体进行行为画像；支持个体同个体、个体同群体、群体同群体的异常行为分析；支持对数值类、时间类、字符类异常特征进行分析；支持人工/自动对学习的行为基线结果进行修正。  支持对威胁告警和异常行为告警配置加白策略和响应策略；支持类VISO的图形化连线拖拽交互，通过将数据过滤、加白响应、联动处置、syslog外发、通知响应、工单5个计算单元进行灵活组合从而对告警实现自动化的、不同方式的响应场景。 |
| 场景分析 | 具备失陷情报分析、热点恶意软件分析、账号安全分析、邮件安全分析场景；  账号安全分析场景应包含异地账号登陆、暴力破解、弱口令检测、明文密码泄露、VPN账号登录行为统计场景；邮件安全分析场景包含邮件威胁分析、敏感关键词邮件列表、敏感后缀邮件列表； |
| 事件调查 | 支持通过创建事件调查任务对威胁事件和可疑事件进行调查分析，调查任务中可添加的证据数据包括：日志、告警、漏洞、弱口令、配置核查、文本；支持对以攻击者和受害者情况视角对调查任务中的数据做统计分析；支持调查结果的图形化展示； |
| 实体分析 | 支持以IP地址、域名作为实体的快速分析能力：对于外部IP分析，支持集中展示该IP相关的威胁趋势、攻击阶段、威胁分类、威胁关联情况等数据以及该IP对资产的登录分析等；对于内部IP分析，支持集中展示该IP相关的威胁信息、脆弱性信息、暴露面、登录分析、外连分析数据等；对于域名分析，支持集中展示该域名相关的鉴定结果、威胁情报信息、访问源统计、解析结果、首次出现时间、访问趋势等。（提供相关功能的界面截图） |
| ★自动化响应 | 支持类VISIO的图形化连线拖拽交互，灵活组合告警响应动作策略中的计算单元（包括6类计算单元：数据过滤、加白响应、联动处置、syslog外发、通知响应、工单、安全编排）以应对不同告警响应的场景。数据过滤计算单元支持引用对象资源、资产信息；（提供相关功能的界面截图）  支持通过告警响应策略，对告警自动创建工单任务，及时通知到工单责任人处理告警。  支持下发安全编排剧本对告警进行自动响应，支持配置剧本以及剧本的执行周期。  支持基于告警进行自动化联动处置的配置，能够自动下发联动处置命令；支持的联动处置设备包括：同品牌上网行为管理、防火墙等。 |
| 工单处置 | 支持通过工单形式通知告警、漏洞、弱口令及配置核查，通知方式包括邮件、短信、企业微信、钉钉、蓝信；工单包含待下发、待处置、处置中、已处置、已完成、已撤销状态吗，支持对工单状态的跟踪；支持对工单SLA要求进行设置，SLA超期支持通知提醒；支持多人协同的工单跟踪处理方式；工单流转中支持添加附件。 |
| ★联动处置 | 支持与现网内的防火墙、终端安全管理进行联动处置，当发现威胁事件后，可以及时给联动设备下发阻断或告警的安全防护策略动作；支持对终端安全管理软件联动设备下发的联动处置命令，包含：全网终端隔离特定文件，特定终端隔离特定文件等；（提供相关功能的界面截图） |
| 支持与现网内服务器安全加固系统进行联动处置，下发的联动处置措施包括：禁止失陷主机访问其他主机、禁止其他服务器访问失陷主机、隔离指定主机、隔离指定主机恶意文件以及隔离全网主机恶意文件等。 （提供相关功能的界面截图） |
| 态势大屏展示 | 支持态势大屏展示，至少包括资产风险态势、全网脆弱性态势、外部威胁态势、内网威胁态势、安全运营态势、威胁预警态势、综合安全态势、攻击者态势、资产态势；  资产态势支持统计展示全网资产分布情况，并且支持按照资产分组展示对应的资产数量、风险值和风险等级的明细列表；支持统计资产总数，以及统计资产注册状态占比情况；支持统计资产上开放的端口情况、服务情况、协议情况；支持统计资产发现来源（资产探查、数据同步、脆弱性发现、流量解析、人工方式）的分布情况；支持按照资产发现来源（资产探查、数据同步、脆弱性发现、流量解析、人工方式）统计最近30天资产发现的趋势。 |
| 系统管理 | 支持用户角色管理， 可以为不同角色赋予不同系统功能模块及数据的读写权限 |
| ★支持硬盘减震技术，投标时提供信息产业信息安全测评中心、公安部计算机信息系统安全产品质量监督检验中心或国家知识产权局第三方权威机构出具的检测报告或证明文件复印件（检测报告或证明文件须具有“硬盘减震”等字样来明确体现支持该技术）； |
| 支持通过企业微信、钉钉、蓝信方式向个人或群发送系统消息通知 |
| 支持对接威胁情报平台，实现对可疑IP、域名、URL的情报鉴定。 |
| 可对平台日志采集发送速率、平台数据处理速率、ES入库速率、HIVE入库速率、流量采集器发送速率、平台接收速率等维度进行最近5分钟、最近24小时、最近7天维度的监控； |
| ★支持对日志的高性能处理和存储技术，投标时提供信息产业信息安全测评中心、公安部计算机信息系统安全产品质量监督检验中心或国家知识产权局第三方权威机构出具的检测报告或证明文件复印件（检测报告或证明文件中须具有 “高性能的Syslog日志处理和存储”等关键字样来明确体现支持该技术） |
| 市场排名 | 提供第三方市场调查机构出具的产品市场排名前三或解决方案排名前三的证明报告，仅限IDC、赛迪顾问（CCID）、数世咨询三家大型咨询机构报告。（提供报告或数据引用证明） |
| 产品资质（提供证书复印件） | 具备公安部销售许可证（安全管理平台品类） |
| 具备IPV6 ready资质 |
| 具备“国家信息安全测评信息技术产品安全测评证书”（级别：EAL3+）资质 |
| 厂商资质（提供证书复印件） | 厂商为CNCERT反网络诈骗领域应急服务支撑单位 |
| 厂商具备信息通信行业企业信用等级评价—系统集成领域（AAA级别） |
| 厂商具备ITSS运行维护符合性证书（二级） |
| 其他 | 中标三个工作日内提供原厂商出具的五年原厂商质保服务承诺函。中标后将对上述功能要求进行逐一测试验证，测试中发现虚假应标的行为将予以废标处理并保留追究相关责任的权利。 |

## 安全DNS

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 解析能力 | 支持信风114运营商级解析能力，解析稳定性更高，延时更低。 |
| 解析稳定性高，累计域名解析量120亿+，拦截恶意域名26W+。 |
| ★威胁情报能力 | 威胁情报库ioc数量1.4亿+，订阅一年服务。 |
| 威胁情报服务器200W+活跃情报，每小时更新。 |
| 威胁分析能力基于威胁情报中心商业威胁情报，能够对APT攻击、勒索软件、窃密木马、远控木马、僵尸网络等几十种网络威胁请求进行有效检测和拦截。 |
| 具备网络入侵行为检测分析能力（提供网络入侵行为检测系统及检测方法自主知识产权证明或第三方权威机构的检测报告） |
| 威胁情报能力成熟度高，得到市场检验和认可，在近三年内（自2021年开始算）IDC安全分析和情报市场领域排名前三名。（提供IDC证明材料） |
| ★域名监控 | 支持客户自定义域名监控任务，实时统计监控域名访问情况与告警情况，通过邮件策略配置，及时将告警信息传递给客户，方便客户快速定位问题并处理。（提供功能截图） |
| 平台部署 | SaaS平台，秒级部署，无需本地硬件，无需网络改造。本项目提供1年使用服务期。 |
| 数据可视化 | 支持查看域名解析/拦截趋势，实时全局掌控解析态势。 |
| 支持以域名解析维度，查看自定义时间内域名解析日志。 |
| 支持以告警事件维度，查看自定义时间内的事件分析日志。 |
| 支持查看请求类型分布、威胁类型统计、资产IP解析域名信息。 |
| 资产管理 | 支持告警事件邮件通知，方便客户快速定位问题并处理。 |
| 支持自定义监控资产IP任务，实时监控资产IP解析域名情况并对威胁进行告警，方便及时了解内部资产威胁情况。 |
| 日志审计 | 支持记录用户后台操作行为，便于查看历史操作记录。 |
| 厂家资质（提供证书复印件） | 厂商具备ITSS云计算服务能力标准符合性证书（SaaS服务）二级； |
| 厂商具备信息通信行业企业信用等级评价--网络安全领域（AAA级别） |

## 漏洞屏蔽系统

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 部署架构 | ★软硬件一体化部署交付，采用旁路镜像流量模式部署，无需更改业务逻辑 |
| 漏洞智能分析 | ★支持导入多种外部漏洞设备扫描数据，可按模板批量导入漏洞信息进行分析处理 |
| 支持自动学习网络流量，快速识别待防护目标主机，也可自定义添加防护目标主机 |
| 展示被屏蔽漏洞的详细信息，包含漏洞名称、CVSS评分、漏洞编号、说明、参考链接、可利用评估等多项信息 |
| ★支持对导入的漏洞信息进行智能分析，生成漏洞分析结果和屏蔽建议 |
| 漏洞防护 | 支持对网络流量中包括远程命令执行漏洞、反序列化漏洞、任意文件上传漏洞、未授权访问漏洞、sql注入漏洞、模板注入漏洞、任意文件读取漏洞、目录遍历漏洞、文件包含漏洞、远程代码执行漏洞、信息泄露漏洞、硬编码漏洞、XXE漏洞等漏洞攻击等漏洞利用行为进行防护 |
| ★支持一键开启漏洞屏蔽策略，支持针对不同主机范围应用不同的屏蔽策略，并支持灵活调整屏蔽的策略，设置是否拦截漏洞攻击，也可对应设置屏蔽白名单，放行正常业务。 |
| 支持对当前漏洞的屏蔽的情况进行统计分析，方便用户快速知晓当前环境的漏洞屏蔽概况，可快捷调整屏蔽策略 |
| ★针对漏洞拦截期间内，若受攻击主机存在主动外连行为，支持自动进行封禁，避免主机遭受反弹攻击 |
| 可实时展示拦截的漏洞攻击告警，告警信息支持一键设置屏蔽和忽略告警的操作 |
| 屏蔽增强 | ★对漏洞攻击行为进行扩展检测，并进行相应屏蔽和告警，支持阻断模式和仅告警模式两种 |
| 支持白名单配置，屏蔽增强只对白名单以外的主机生效，白名单内主机的漏洞防护功能不受影响 |
| ★屏蔽增强支持对指定范围内的主机生效 |
| 告警列表导出 | 支持一键导出告警列表信息 |
| 配置向导 | 设备初次登录，支持通过配置向导功能引导客户完成管理接口IP配置、业务接口配置、系统时间等。 |
| 网络配置 | 网络配置支持对某一接口进行编辑配置，同时在网卡状态能够直观的展示网卡的UP和Down |
| 系统管理 | 支持系统平台和引擎本地更新，漏洞规则可联网自动更新，并可查看历史更新的记录 |
| 展示当前系统的概览信息，包含软件信息、硬件信息以及服务流量信息，支持下载系统日志，以便排查系统故障 |
| ★支持开启OTP二次验证，账号登录需进行二次验证后方可登录 |
| 支持通过输入qtreset命令，恢复设备到出厂默认配置 |
| 系统初次登录强制要求修改web和SSH密码 |
| 售后服务 | 提供三年特征库更新以及三年保修服务； |

## 云waf

|  |
| --- |
| 总体要求 |
| 针对现有云waf(玄武盾)的订阅服务，三年；针对门户网站持续提供web防护； |

## 安全设备监控系统

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 基本要求 | ★国产自主 | 产品必须为国产、独立自主研发的品牌，不接受国外品牌、合资类品牌、使用开源软件开发的产品。 |
| ★数据采集 | 基于设备独立的带外管理口直接对设备硬件运行情况进行监控，不依赖操作系统，不能在被监控设备上安装任何代理、客户端或插件，需提供原厂承诺函。 |
| ★系统访问分析 | 可对平台各项功能的使用频度及实时在线人数进行统计分析。 |
| 安全验证 | 支持多因子登录验证（登录密码、程序随机码、短信验证码），加强对系统登录的安全性管理。 |
| ★操作系统用户管理 | 支持根据Agent或账号认证的方式对用户进行管理，包括修改密码，新增用户、分组等。  支持批量或定时修改操作系统密码，可自定义设置执行周期、频率和时间范围。 |
| ★设备安全控制 | 支持对设备在指定时间段的安全操作，包括：关机\重启，远程控制，重启带外等；  支持设备操作的申请和审批，包括操作的行为，具体操作时间、设备范围、审批人等；  支持对设备安全控制策略进行配置，根据下发策略信息在特定时间范围可对设备进行控制操作。 |
| 部署要求 | Linux系统 | 应用系统支持部署在开源的Linux操作系统上，保证监控平台的稳定性和安全性；  应用系统部署需支持开源数据库，不得采用国外品牌商业版数据库；  要求支持Linux平台开源的中间件。 |
| 国产环境适配 | 应用系统要求部署适配在麒麟、统信、中兴新支点、中科方德等国产化操作系统上；  应用系统要求部署适配在达梦、优炫、巨杉、TiDB、GoldenDB、海量等国产数据库环境；  应用系统要求部署适配在东方通、中创的中间件。  以上提供兼容性证书并加盖公章 |
| 数据展现 | 个人工作台 | 自定义展现：提供自主设定工作台展现内容的能力，通过图表综合展示资源运行情况、性能状况、各类指标TOPN分析等内容。 |
| ★大屏展现 | 大屏展现：支持从综合、监测、机房、机柜、资产、业务和能耗等多个角度展现数据中心IT基础设施运行情况，可定制大屏视图，要求至少提供10张标准化大屏视图。 |
| 监测管理 | ★信创生态支持 | 国产服务器：支持华为、曙光、浪潮、中兴、联想、五舟、长城、宁畅、烽火等服务器的适配支持，需提供适配兼容性证书；  国产存储：支持柏科、宏杉、浪潮、中兴、联想、曙光、华为、联创信安、同有、海康威视、紫光西部、群晖等存储监控；  网络及安全设备：支持华为、华三、中兴、启明星辰、深信服、山石网科、网御、360、信安世纪、烽火、迈普、神州数码、锐捷、天融信、迪普等网络设备监控；  云服务：支持ZStack、华为云等云计算服务监控。 |
| 支持IPv6 | 需同时支持纳管IPv4和IPv6地址的设备。 |
| 密码算法 | 支持国密算法加密系统密码信息。 |
| ★适配要求 | 支持以下设备类型及品牌的监控，以实现有效替代人工机房巡检，实时掌握硬件工作状态信息：   1. 操作系统：支持Windows、Linux、Unix（HP-Unix、AIX、FreeBSD）、AS400、OpenVMS； 2. 数据库：支持对MySQL、SQL Server、Oracle（含RAC）、Sybase、Informix、DBCaché、mongodb等数据库的深度监控； 3. 应用服务：Tomcat、kafka、Apache、HACMP、PowerHA、RHCS、ActiveMQ、IBM MQ、MSMQ、WebLogic、IIs、Nginx、Resin、SharePoint、Skype、Jboss、memcached、Redis、ZooKeeper等监控； 4. 云计算：支持VMWare、Amazon、Aliyun、青云、docker、Redhat、FusionInsight、FusionCompute、kubernetes等监控； 5. X86服务器：支持IBM、HP、DELL、Fujitsu、宝德、安擎、新华三、百信等品牌； 6. 刀箱&刀片：支持IBM、HP、DELL、Cisco等品牌； 7. 小机：支持IBM、HP、Oracle、Sun、KunLun 、富士通等品牌； 8. 存储&磁带库：支持IBM、HP、EMC、DELL、HDS、Sun、NetApp、昆腾等品牌，支持对高端存储和虚拟化存储的监测，如：IBM V7000系列、IBM DS8000系列、EMC DMX系列、EMC VMAX系列等监测； 9. 光纤交换机：支持Brocade、Cisco等品牌； 10. 网络安全设备：支持启明星辰、深信服、信安世纪、烽火、锐捷、天融信等品牌； 11. 动环设备：支持温湿度传感器、PDU、UPS、空调等动环设备监控。 |
| ★MIB浏览器 | 提供MIB浏览器，支持OID解析、MIB文件导入功能，提供更清晰地MIB库展示的能力。 |
| ★配置备份 | 可对网络设备的配置进行备份，提供手动和自动备份两种形式，配置变更后可进行告警通知。 |
| ★系统崩溃截图 | 支持系统崩溃时页面抓图与屏幕录像功能，辅助故障诊断，并保存最近3次宕机的截图，查看故障时间和导出图片保存。 |
| 在线数据查询 | 支持在系统页面上直接执行SQL语句进行数据查询，无需登陆后台数据库。 |
| 网络资源管理 | 支持对IP地址、网段进行统一管理，包括地址规划、管理域管理、定时刷新等功能； 支持自动检测IP是否已占用或空闲；  支持自动或手动获取存储，SAN交换机，服务器之间关联关系；  支持查看设备详细ARP、FDB、LLDP、路由表信息，同时支持表数据刷新和导出。 |
| ★网络流量分析 | 支持通过应用、端口、协议对网络流量数据进行采集和分析。 |
| ★开关机重启记录 | 支持统计服务器在一段时间内的开关机、重启信息。 |
| ★场景提测 | 支持模拟场景操作自动监测系统页面是否异常，支持对录制文件、场景列表进行统一管理；  支持按照业务角度查看场景数据，包括正常、异常、平均时耗、页面健康度等信息；  支持查看系统当天的WEB性能数据。 |
| ★自定义监测 | 新增自定义监测器的批量管理，可提供脚本、SNMP、JDBC运行的功能，实现针对定制化的应用软件、网络设备、数据库的自定义监控。 |
| ★暂时忽略 | 支持对同一指标集合下指标项的告警进行暂时忽略操作。 |
| 一键巡检功能 | ★一键巡检 | 支持设置巡检任务“一键巡检”“定时巡检”，支持选择巡检指标项、巡检设备。巡检结果可以自动通知相应的值班人员； 支持查询巡检历史，页面展示巡检结果一览。 |
| 拓扑管理功能 | 网络拓扑 | 支持自动发现和手动拓扑添加两种模式，支持生成LAN网络拓扑以及SAN网络拓扑；  支持拓扑图的拖拉拽设置，可自主设置拓扑图形状；  当设备及网络链路出现异常时，例如：负载过高、流量过大等，平台会以颜色直观的提示相关人员；  支持多层次显示网络拓扑结构视图，支持展开和折叠不同层次的节点和连接关系。 |
| SAN拓扑 | 支持自动发现存储-光纤交换机-服务器拓扑，直观呈现SAN拓扑中节点和网络故障。 |
| VM拓扑 | 支持自动生成虚拟化平台资源拓扑，直观呈现平台内资源告警情况。 |
| 告警管理 | 告警展现 | 支持监控告警功能：提供统一告警平台，以不同颜色表示不同类型的事件及严重程度。 |
| 通知规则 | 支持告警过滤、告警合并、告警压缩、告警升级等功能，并且可以对各设备设置差异化告警策略，对管理人员进行不同设备的告警订阅。 |
| ★告警方式 | 支持微信公众号、短信、电话、邮件、钉钉、飞书、第三方告警平台对接等告警方式。 |
| ★日志分析 | 支持收集服务器设备，网络设备等硬件的日志信息；  支持查看日志信息的详细页面，支持批量删除和下载；  支持对H3C、华为X86服务器日志的深入分析，自动关联告警信息并给出故障处理建议。 |
| ★预警功能 | 支持部件预警、能耗预警、空间预警等功能； 支持部件预警指标，包含：设备厂商、磁盘预警、电源预警、内存预警、CPU预警、网卡预警等。 |
| 资产管理 | 资产管理 | 支持按照多种不同角度统计展现设备资产、备件、网络资源（交换机端口、IP）等资产信息； 支持远程资产信息自动采集，包括（CPU、内存、磁盘、电源、风扇、阵列卡、网卡等），达到资产管理和配置信息自动更新的目的，提高设备信息维护的效率。 |
| 备件信息 | 支持对设备备件进行统一管理，支持单个或批量入库。支持库存备件进行模糊或精确查询； 支持保存入库和出库记录；  支持在设备部件故障时，快速自动匹配备件库的所需备件，包括部件类型、部件数量、存放位置等信息，缩短维修时间。 |
| ★保修管理 | 支持保修管理功能：支持实现对设备过保时间的提醒和信息管理功能。可根据已过保的设备、将过保的设备、正常设备等不同维度进行数据筛选和显示； 支持通过客户端及Web两种方式查询IBM、HP、Dell、华为、浪潮等x86服务器的过保时间； 支持手工批量导入设备维保信息； 支持续保管理，支持数据导出成Excel或PDF。 |
| 变更管理 | 支持对设备的变更信息进行统一管理，包括：部件变更、位置变更、网络配置变更、信息变更、维保变更、序列号变更等； 支持模糊或多个条件组合精确搜索设备变更信息。 |
| 现场维护 | 系统支持批量生成资产二维码，通过配套APP扫码的方式进行现场资产维护。 |
| 部件信息 | 支持对部件信息进行统计展示和集中管理，支持导入导出操作；  支持一键获取所有设备的RAID配置信息。清晰展示阵列卡、物理磁盘、逻辑磁盘的关系。 |
| ★采购与验收 | 支持对采购订单和合同信息进行统一管理，包括：新增、删除、搜索、导出等功能； 支持对X86服务器进行到货验收核对部件信息，自动确认设备和采购订单部件规格型号是否相符；支持对验收成功和不成功的设备生成报告。 |
| ★预上架 | 支持以图形化方式统计展现数据中心、机房的机柜空间、能耗承重等信息；  支持按照数据中心、机房的角度进行预上架；  支持对预上架条件进行配置，如设备规格、数量、机柜空间等，并自动推荐合适的上架位置。 |
| 数据分析 | 数据报表 | 报表类型管理：系统内置多种报表类型，包括：资产类、监测类；  报表模板管理：用户可以基于报表类型，自定义报表模板。自定义内容包括：统计周期（日报、周报、月报、季报和年报）、报表数据项、统计方式、过滤条件、发送规则等；  支持手工报表和定时报表，支持自定义报表发送规则。支持报表共享，或通过邮箱发送；  统计对象集合管理：可以按资源视图、业务视图或机房视图进行分组管理；  支持在线预览报表和导出报表。 |
| 移动运维 | ★手机APP | 提供移动端运维APP，满足移动资产维护和监测运维需求，需支持Android和iOS方式。 |
| 售后服务 | | 配置200个许可授权以及五年原厂技术支持服务；投标时提供原厂售后服务承诺函； |
| 其他 | | ★招标人保留对第一中标候选人提供的产品进行功能测试的权利（按招标技术要求），测试过程中发现虚假应标的行为将予以废标处理，并保留对该原厂追究相关责任的权利。 |

## 集成技术服务

1.上线前用户将会对相关系统功能要求进行逐一测试验证，测试中发现虚假应标的行为将予以废标处理并保留追究相关责任的权利。

2.提供详细的实施方案，若在实施过程中造成医院业务非计划性停机或者数据丢失，由中标方负全部责任并赔偿院方因此造成的全部损失。

3.投标人需充分考虑医院现有的软、硬件的利旧方案，并免费提供设备搬迁服务、机柜搬移服务和数据迁移服务，所产生的第三方费用由中标方承担。

4.投标供应商须具备全专业技术团队服务能力并针对本项目组建专门的实施团队，且实施团队不少于5人，其中须由具有CCRC信息安全认证的人员担任本次项目经理，负责本次项目实施工作的整体管理和协调工作，其余成员要求不少于一名oracle ocm工程师、一名VCP工程师、一名RHCE工程师、一名CISP工程师、一名HCNP工程师，要求投标时提供相关工程师社保证明以及证书原件，后续实施的工程师必须与投标文件中的工程师一一对应，进场施工时须核对工程师相关证件及专业证书；

5.投标单位在标书中确认的项目经理和主要技术人员，必须参与项目施工，未经用户同意不允许变更，在实施时用户有权验证实施工程师身份和认证证书原件。

6.投标单位须提供7\*24小时技术支持，全年不少于40个工作日的现场技术支持。

7.投标单位须提供不少于四次/年的巡检服务，巡检对象须包括医院现有的核心网络安全设备的巡检服务。

8.投标单位须提供现场技术保障服务，协调原厂人员实行网络安全检查和加固，并向用户汇报各项工作情况。

9.要求供应商具备服务质量管理系统并提供账号供用户使用，用户可通过该系统对服务方的售后服务进行监督和管理。投标时提供该系统登录网址，并且该系统功能要求如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 功能要求 | 功能描述 |
| 1 | 总体要求 | 1.为确保用户能够对各项服务进行审计和审查，要求投标供应商具备服务质量管理系统并向用户开放系统使用权限，使得用户能够通过系统来管理服务商。在签订合同前须提供系统测试地址和账号。 |
| 2 | 系统部署模式 | 1.系统支持SAAS模式部署和本地部署模式，本次项目采用saas模式交付。 |
| 3 | 功能要求 | 1.系统支持管理员模式和用户模式，支持通过不同登录界面区分。 |
| 4 | 账号体系 | 1.支持管理员账号体系以及客户账号体系，客户账号体系面向客户，客户可通过账号登录系统查看与之关联的合同执行情况。 |
| 5 | 客户管理功能 | 1.支持客户管理功能，可为每个客户创建独立账号，每个客户即独立租户，数据相互不可见，同时可设置客户归属信息等，支持修改、锁定、删除、重置密码等功能。在签订合同前须提供系统测试地址和账号，若不满足要求，按虚假应标处理，中标方承担一切后果。 |
| 6 | 合同管理功能 | 1.支持合同管理功能，并与客户、销售及项目经理关联，支持合同上传等功能；在签订合同前须提供系统测试地址和账号，若不满足要求，按虚假应标处理，中标方承担一切后果。 |
| 7 | 工单管理 | 1.支持工单管理功能，能够区分合同内以及合同外的工单，并支持关联合同，根据合同签订时间自动提醒工单指定干系人实行巡检等工作。在签订合同前须提供系统测试地址和账号。 |
| 8 | 服务总结 | 1.支持服务总结功能，可针对每个合同录入服务总结，与合同关联的客户可通过系统查看服务总结。在签订合同前须提供系统测试地址和账号。 |
| 9 | 文档查询 | 1.支持文档查询功能，可通过文档查询功能查询所有工单执行过程中记录的文档。在签订合同前须提供系统测试地址和账号。 |
| 10 | 服务管理 | 1.支持服务管理功能；  2.支持自定义服务类别；  3.新建服务项目支持与服务类别进行绑定；  4.支持绑定工单以及要求必须提供相关的交付物；  5.支持与合同绑定；  以上功能在签订合同前须提供系统测试地址和账号。 |
| 11 | 系统管理 | 1.支持人员管理功能；  2.支持角色管理功能；  3.支持系统管理功能，可设置邮件、短信  以上功能在签订合同前须提供系统测试地址和账号。 |