**第三章  项目需求和质量标准**

**1、招技术参数要求所有条款均为实质性条款，必须满足或者优于，否则其《响应文件》（竞标）作否决处理。**

**2、投标人所投标货物或服务如国家有强制性要求的按国家规定执行，并提供相关证明材料。若执行标准有修改或更新按最新版本执行。**

**3.本项目预算总金额：80000.00元。**

**一、采购清单、技术规格参数、质量标准和要求**

**（一）采购清单**

|  |  |  |
| --- | --- | --- |
| 序号 | 产品名称 | 数量 |
| 1 | IT资产安全运维服务 | 1项 |

1. **技术规格参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物 | 服务内容要求 | 数量/单位 |
| 1 | IT资产安全运维服务 | **一、互联网攻击模拟风险评估服务**  1.渗透测试服务  1.1服务内容：渗透测试针对业主单位具体某个系统，重点发现技术或业务逻辑层面的漏洞。通过从外部、内部进行渗透测试，从技术、管理、业务逻辑的角度来发现漏洞，充分挖掘业主单位信息泄露的途径，从根源上解决存在的漏洞或问题，减少业主单位信息泄露事件的发生。服务公司使用人工渗透测试技术，对业主单位管辖范围内的某个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及加固方案。  1.2服务方式：本地。  1.3服务范围：业主指定的业务系统 。  1.4服务频率：1次/年。  1.5配备安全设备：渗透测试报告可导入本地服务工具平台实现本地统一展示和漏洞管理。  1.6服务成果：《XX系统渗透测试报告》。  2. 外网资产暴露面检测服务  2.1服务内容：通过多外网云端扫描技术，探测互联网上潜在的未知资产，不必要开放的资产，并自动验证互联网资产是否存在可利用漏洞、弱口令，提供暴露面收敛等相关整改建议，监测数据通过本地平台统一展现和管理。包括但不限于：  互联网资产详情：从基本信息到应用组件、应用指纹、开放端口等。  风险暴露面排查：远程访问端口、VPN入口、后台入口、弱口令、可入侵漏洞等。  未知资产排查：那些被忽略的域名、IP、应用、信息通道等。  生成暴露面监测报告：提供暴露面收敛整改建议，定期更新和审核。  2.2服务方式：本地。  2.3服务范围：互联网出口。  2.4服务频率：每月1次。  2.5配备安全设备：提供服务平台本地化部署实现统一展示和管理，支持在平台首页进行直观展示。  2.6服务成果：《XX攻击面监测报告》。  3.互联网数据泄露监测服务  3.1服务内容：通过各类互联网搜索引擎与第三方信息库，监测业主单位外部信息：企业信息、邮箱信息、敏感代码信息、敏感文档、APP应用程序、微信小程序、微信公众号。  3.2服务方式：本地。  3.3服务范围：业主单位互联网数据。  3.4服务频率：每月1次。  3.5配备安全设备：提供服务平台本地化部署实现统一展示和管理。  3.6服务成果：《外部攻击面信息报表》。  **二、内网资产及漏洞管控服务**  1. 资产梳理服务  1.1服务内容：通过本地化部署平台对业主单位的资产进行梳理，建立业主单位有效安全资产管理，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，包括但不限于：  网站资产梳理服务：对业主单位网站进行梳理服务，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：对业主单位服务器进行梳理服务，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，实现对服务器的运维管理。  终端资产梳理服务：对业主单位终端PC资产梳理服务，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：通过管理业主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。  1.2服务方式：本地。  1.3服务范围：网站、服务器、终端、其他网络资产。  1.4服务频率：每月1次。  1.5配备安全设备：提供服务平台本地化部署实现统一展示和管理，形成资产台账。  1.6服务成果：《XX网站信息系统资产列表清单（月度）》、《XX服务器信息系统资产列表清单（月度）》、《XX终端信息系统资产列表清单（月度）》。  2. 主机漏洞监测服务  2.1服务内容：对主机进行常态化安全漏洞扫描，提供主机漏洞台账与报告，并根据漏洞风险等级、漏洞被利用可能性、漏洞加固或规避措施等内容，为业主单位进行漏洞处置决策提供参考依据。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。  2.2服务方式：本地。  2.3服务范围：服务器、终端资产。  2.4服务频率：每月1次。  2.5配备安全设备：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安全概况展示和查阅。  2.6服务成果：《XX主机漏洞监测报告及加固建议（月度）》、《XX主机漏洞监测报告及加固建议（紧急）》、《新上线业务系统漏洞扫描及加固建议》  3. 网站安全监测服务  3.1服务内容：对网站的“漏洞、篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持、网站主机环境安全监测”等9个维度开展实时监测，并通过邮件、飞书、钉钉、企业微信等告警形式提供网站风险预警服务，包括但不限于：  网站漏洞监测：对业主单位管辖范围内的Web站点进行扫描，排查WEB站点中的SQL、XSS、敏感信息泄露、文件包含、CSRF、目录遍历、XML注入、备份文件、弱口令等多种web代码层面的漏洞。  黑链/篡改事件监测：高频率监测站点是否存在被黑客植入黑链、篡改的事件，监测频率低至5分钟/次。  敏感词事件监测：自定义敏感词库，支持自定义监控周期，持续对业主单位的网站进行全站页面爬取，发现敏感词字眼。  敏感文件泄露事件监测：对业主单位网站发布的文件中是否含有用户信息等敏感文件进行监测，包括excel、txt、pdf等类型的文件。  网马监测：通过对网页中的恶意脚本的链接进行分析，追查出网页木马传播的病毒、木马程序所在位置，对网络中的有害程序进行准确定位。  域名劫持事件监测：监测站点的DNS解析是否异常，监测频率低至5分钟/次。  可用性异常事件监测：模拟浏览器访问，监测站点的可用性情况，监测频率低至5分钟/次。  网站主机环境安全监测：在服务器部署主机安全监测软件，主动对网站篡改、webshell、后门以及挖矿等主机安全事件与行为进行7\*24实时监测，第一时间对攻击行为进行告警。  3.2服务方式：本地+云端自动化。  3.3服务范围：网站系统。  3.4服务频率：7\*24小时。  3.5配备安全设备：配备平台工具本地化部署，在统一平台进行业务系统安全概况展示和查阅。  3.6服务成果：《xx系统网站安全监测报告（月报）》。  4. 配置合规基线核查服务  4.1服务内容：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。服务业主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。  4.2服务方式：本地。  4.3服务范围：网络设备、主机、操作系统、数据库、中间件。  4.4服务频率：每季度1次。  4.5配备安全设备：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。  4.6服务成果：《信息系统配置核查报告》、《新上线业务系统配置核查报告》。  5.协助安全加固  5.1服务内容：基于攻防视角评估资产漏洞风险，结合内外网资产台账，识别可实际产生风险的漏洞，提供修复的优先级建议，并协助加固。  5.2服务方式：本地。  5.3服务范围：网站系统、服务器、终端资产。  5.4服务频率：每季度1次。  5.5服务成果：《网站系统、服务器、终端资产加固整改报告》。  6.漏洞防护服务  6.1服务内容：通过平台agent帮助业主单位防护多种漏洞，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。  6.2服务方式：本地自动化。  6.3服务范围：网站系统、服务器。  6.4服务频率：7\*24小时。  **三、入侵安全事件监测和响应服务**  1. 全网蜜罐威胁诱捕服务  1.1服务内容：本次服务项目通过部署蜜罐威胁诱捕系统，在不改变业主单位的网络架构前提下（包括：不做镜像流量、不做牵引流量等），通过旁路部署，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，在每个网段部署多个虚拟蜜罐（具体数量根据业主单位实际需求），达到监测内网病毒威胁安全事件，并提前做安全预警。  1.2服务方式：本地。  1.3服务范围：DMZ区、服务器区、终端区等按需。  1.4服务频率：不限数量，按需部署。  1.5配备安全设备：配备蜜罐威胁诱捕系统。  1.6服务成果：《蜜罐威胁诱捕系统监测报告（月报）》。  2. 主机威胁监测服务  2.1服务内容：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，包括但不限于：  恶意文件检测：支持检测“Webshell网马、病毒木马、攻击脚本、宏病毒文件等”。  网站篡改检测：可检测网站文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为。  2.2服务方式：本地自动化。  2.3服务范围：服务器、终端资产。  2.4服务频率：7\*24小时。  2.5配备安全设备：配备平台工具本地化部署，并统一进行主机威胁概况展示和查阅。  2.6服务成果：《主机威胁监测报告（月报）》。  3. 应急响应服务  3.1服务内容：提供7\*24小时全天候6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，包括但不限于：  事件初期：在实施应急响应工作前，服务公司收到业主单位申请应急响应支持，由服务公司技术支持人员和业主单位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，并协助业主单位解决事件。  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，提交给业主单位。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。  3.2服务方式：本地。  3.3服务范围：网站、服务器、终端资产。  3.4服务频率：2次/年。  3.5服务成果：《XXXXX事件应急响应报告》。  **四、其他安全服务**  1. 安全培训服务  1.1服务内容：对技术人员、业主单位职工、管理人员进行周期性的安全意识、安全技术、开发安全、安全管理等内容进行选择性培训，加强整体的安全水平。  1.2服务方式：现场。  1.3服务范围：按需。  1.4服务频率：1次/年。  1.5服务成果：《XX安全意识培训课件》、《XX安全技术培训课件》。  2.现场值守服务  2.1服务内容：攻防演练期间现场蓝队防护：加固、应急、研判、溯源、反制等。  2.2服务方式：现场。  2.3服务范围：网站、服务器、终端资产。  2.4服务频率：1次/年。（每次一周）  2.5服务成果：《攻防演练保障总结报告》。  **五、配套服务工具技术指标**  1. 基本要求  1.1机架式设备，默认配置4个千兆电口，64G内存，2T硬盘存储空间，冗余电源  1.2采用一体化安全运维平台，不接受平台+安全产品组合方式提供。中标后，5个工作日内提供测试样机进行逐项测试。  2 .授权许可  2.1扫描次数授权：无限制；  2.2扫描IP/域名范围授权：无限制；  2.3提供可管理主机资产授权数：无限制；  2.4提供可管理网站资产授权数：1000；  2.5提供仿真业务陷阱授权数：无限制；  2.6提供主机主动监测及漏洞屏蔽授权数：1000；  2.7提供出口流量监测带宽授权：1Gbps；  2.8提供二次开发接口授权；  3.资产测绘和管理功能  3.1暴露面监测  3.1.1暴露面监测：外部信息收集：通过单位全称、关键字、出口IP等信息，收集单位/企业工商注册信息、app程序、微信小程序、微信公众号、邮箱信息泄露、敏感代码泄露、敏感文档泄露等外部/互联网攻击面信息。  3.1.2★二级域名扫描：支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析IP地址；提供由厂商盖章确认的产品界面截图证明。  3.1.3★IP反查域名监测：输入IP或者网段，通过搜索互联网数据，自动获取到IP对应的域名、url链接、网站标题、返回状态码；提供由厂商盖章确认的产品界面截图证明。  3.1.4★网站资产相关度分析：通过爬取企业单位已知的网站页面，分析网页中是否包含企业单位相关的网站链接，从而发现未知网站；可配置“网段、域名”等命中规则，自动判断是否属于企业单位的网址；提供由厂商盖章确认的产品界面截图证明。  3.2资产深度管理  3.2.1设备类别分析：支持识别“打印机、网络摄像头、安全设备、投影仪、安全设备、路由器”等设备类型，具备4W+指纹特征库，提供由厂商盖章确认的产品界面截图证明。  3.3主机资产台账  3.3.1支持自动扫描IP资产信息，包括：“存活IP、设备厂商、操作系统、端口、应用、数据库、中间件、服务版本”等资产指纹特征，形成主机资产台账。  3.3.2支持通过导入现有资产信息，或在线编辑方式，录入主机资产的管理信息，比如系统所属部门、负责人、联系方式、资产价值、物理位置等。  3.3.3支持对IP、资产组、部门、责任人、应用系统、设备类型、主机名称、操作系统、宿主机ip、资产价值、等级保护等进行精准搜索或模糊搜索  3.3.4可自定义展示列，可排序、选择是否显示。  3.4 网站资产台账  3.4.1支持自动识别网站资产信息，包括：“中间件信息、web框架信息、CMS&OA、程序语言”等指纹信息，支持爬取网站后台、ICP备案编号、网站标题、网站返回码等属性，形成网站资产台账。  3.4.2支持通过导入现有资产信息，或在线编辑方式，录入网站资产的管理信息，比如网站所属部门、负责人、联系方式、资产价值、物理位置等。  3.4.3支持对状态码、IP、资产组、部门、责任人、URL、子域名、易危组件、中间件、ICP备案号、公安备案号、归属地等进行精准搜索或模糊搜索  3.4.4可自定义展示列，可排序、选择是否显示。  3.5 mac地址自动识别:不需要联动第三方设备、不需要在主机中安装任何代理、无需主机开放任意端口，就可支持对跨网段的IP或多个网段对进行MAC地址探测识别，支持识别MAC地址的设备类型包含:“Windos、Linux、国产操作系统、交换机\路由器、安全设备、打印机、物理网设备等”，提供由厂商盖章确认的产品界面截图证明  4.网站风险与威胁监测功能  4.1网站威胁检测  4.1.1web风险监测：对网站的“漏洞、篡改、黑链、敏感文件、敏感词、网马监测、可用性、域名劫持”等8个维度开展实时监测，监测频率低至5分钟/次  4.1.2敏感文件事件泄露监测：可监测发布到网上的pdf、word、excel文件中是否包含“身份证号、邮箱、手机号码、用户名/密码”等敏感信息，可在系统上查看泄露的信息以及敏感文件下载链接。提供由厂商盖章确认的产品界面截图证明。  4.1.3敏感内容审查工具：可上传文件(pdf\word\excel)、或者粘贴内容进行敏感词审查，内置敏感词库10万+，支持人工再确认审查结果，提供由厂商盖章确认的产品界面截图证明。  4.1.4渗透测试台账：支持以excel报表格式导入渗透测试报告，形成渗透测试台账。可在系统查看渗透测试结果，以图表形式可视化展现漏洞风险级别比例、风险应用比例，可对渗透报告中的漏洞进行跟踪确认，处置漏洞状态：未整改、已整改、忽略、未整改。提供由厂商盖章确认的产品界面截图证明。  4.2 漏洞扫描与漏洞管理  4.2.1完善的漏洞库：洞库漏洞信息大于320000+条，集成4000+POC对内网资产进行自动漏洞验证与渗透，提供详细的漏洞描述和对应的解决方案描述，扫描结果需包含漏洞利用证明，包括但不限于攻击Payload、目标响应结果、漏洞利用点、关键参数等内容。提供由厂商盖章确认的产品界面截图证明。  4.2.2漏洞生命周期管理：支持漏洞跟踪管理，能够自动对漏洞状态进行处置，自动识别“新增、已修复、未修复”的漏洞，同时支持人工方式进行漏洞状态处置，以及编写漏洞备注。  4.2.3弱口令扫描研判工具：支持用户针对指定的目标IP与应用，通过在web界面上手工输入“用户名、密码”，系统将返回口令登录后的校验结果，确认弱口令是否真实存在。提供由厂商盖章确认的产品界面截图证明。  4.3 基线配置核查  4.3.1配置核查支持类型：操作系统，支持Windows 2003/2008/2012/2016/2019/7/8/10/11；支持linux（Centos、Redhat、suse等）；  4.3.2应用服务，支持Linux、Windows下的Apache、Weblogic、TOMCAT、Nginx，以及windows 2003/2008/2012/下IIS 6/7/8；  4.3.3数据库，支持Linux、Windows下Oracle8i/9i/10/11g、Mysql。  4.3.4大数据应用，如Flume、HBase、Hadoop、Spark、Storm、Hadoop、ZooKeeper。提供由厂商盖章确认的产品界面截图证明。  5.边界威胁监测  5.1流量监测  5.1.1流量监测：通过流量镜像对海量流量进行采集，基于80000+威胁特征库，内置多重检测引擎，包含入侵检测、web检测、威胁情报等，结合攻击源、风险等级、地理位置、攻击目标、命中规则数、告警次数等因素综合分析。提供由厂商盖章确认的产品界面截图证明。  5.1.2旁路阻断：不需要设备串联、不需要配置策略路由，就能通过监测中心流量监测告警处，对单个ip进行手工阻断。也可自动关联流量告警，根据智能研判标签，就会自动触发旁路阻断，可灵活针对国内/国外ip进行灵活封禁，可灵活指定封禁时间间隔。提供由厂商盖章确认的产品界面截图证明。  6.内网威胁诱捕扩展能力  6.1无侵入式全网病毒监测  6.1.1trunk部署病毒监测节点：无需在用户服务器上安装agent，可通过trunk方式将诱捕能力发布到全内网各vlan网段，实现在全内网中部署大量高交互病毒监测诱饵，无侵入式部署不影响用户业务运行。  6.1.2病毒诱饵类型：支持高交互病毒监测诱饵，并可同时启用：“samba、ftp、ssh、rdp、telnet、mssql、mysql、mongoDB、postgresql、tomcat、weblogic、jenkins、redis、hadoop、memcache、solr、activeMQ、struts2、wordpress、nginx、jboss、joomla、smtp”等，以上服务须为真实应用服务，能够正常交互，欺骗攻击者。  6.2病毒处置功能  6.2.1失陷主机微隔离：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网络隔离，隔离后失陷主机无法访问同网段以及其它网段IP，提供由厂商盖章确认的产品界面截图证明。  6.1.2取消微隔离：在web管理界面上，支持对已隔离的失陷主机取消微隔离，恢复失陷主机的网络访问权限。  7.互联网威胁诱捕扩展能力  7.1 蜜罐仿真  7.1.1 默认仿真蜜罐：支持至少10种可自定义logo和公司名称的仿真蜜罐，仿真蜜罐类型包括但不限于：“齐治堡垒机、启明堡垒机、深信服VPN、泛微OA、通达OA、u8crm、wiki、mailcow、bbs论坛、订单管理系统”。提供由厂商盖章确认的产品界面截图证明。  7.1.2完全仿真蜜罐：支持通过反向代理的方式，接入用户自身搭建的应用系统，生成完全仿真蜜罐，提供由厂商盖章确认的产品界面截图证明。  7.1.3钓鱼邮件演练：可在平台中统计打开钓鱼邮件的账号、点击连接的账号、提交敏感数据的账号等数据，统计维度包括账号名称、访问ip、提交敏感数据内容、访问时间等。提供由厂商盖章确认的产品界面截图证明。  7.2攻击吸引:引流防御,可将访问真实业务系统的流量引流到仿真蜜罐，使攻击无法命中真实业务系统。提供由厂商盖章确认的产品界面截图证明。  7.3威胁感知  7.3.1入侵攻击链检测：参考MITRE ATT&CK，还原黑客攻击入侵蜜罐的过程，形成黑客攻击链，包含：“针对蜜罐的探测扫描、渗透攻击、攻陷蜜罐、在蜜罐上安装后门远控程序、利用蜜罐进行跳板攻击”等入侵过程。  7.3.2还原攻击数据包：支持还原攻击者的网络数据包，包括icmp、tcp、udp等协议的攻击包，可查看攻击者发起的具体攻击请求数据，比如SQL注入、XSS攻击的http请求头部信息。  7.3.3时间轴告警：支持时间轴告警分析：可根据基于告警时间/攻击类型/地理位置等对攻击行为进行筛查，其中攻击类型可分类为：“可疑访问、尝试登陆、端口扫描、攻击尝试、强力攻击、异常进程、暴力破解、登陆成功、命令执行、可疑文件、恶意文件、跳板攻击”等类型。  7.4 攻击溯源  7.4.1攻击者社交信息溯源：支持记录攻击者的“黑客社交画像”信息，包括社交账号、昵称、头像等信息，比如溯源百度等不同类型的社交账号。提供由厂商盖章确认的产品界面截图证明。  7.4.2 攻击者指纹溯源：设备指纹溯源至少包括：操作系统信息、浏览器指纹、浏览器类型、mac地址、设备厂商、屏幕分辨率，浏览器历史记录、计算机名、显卡成像参数、CPU等硬件信息。  位置信息溯源至少包括：真实攻击IP（攻击者拨VPN也可获得真实攻击IP）、代理转发前的IP地址、IP地理位置、经纬度。  7.5 攻击反制  7.5.1威慑反制：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。提供由厂商盖章确认的产品界面截图证明。  7.5.2拒绝服务反制：可使攻击者浏览器拒绝服务，可灵活指定对某个攻击源IP地址发起拒绝服务反制。  7.5.3木马诱骗反制：可使攻击者下载某个文件时，替换成木马文件，诱骗攻击者下载安装；可在web管理界面上灵活指定对某个攻击源IP地址发起木马远控反制。  7.5.4漏洞攻击反制：支持一键扫描攻击源IP地址，探测攻击者主机的开放端口信息、弱口令、漏洞等。   1. 服务器主动监测扩展能力   8.1 服务器威胁监测要求  8.1.1主动威胁监测：在用户的服务器、业务系统上安装安全监控软件，主动监测webshell、暴力破解、异常登录成功、反弹shell、挖矿检测等，发现可疑的入侵事件，并实时将告警同步到服务平台，提供由厂商盖章确认的产品界面截图证明。  8.1.2 Web日志分析：可输入最新的web日志文件以及对应web端口号，后续会自动跟踪相同目录下的web日志，发现各类web入侵攻击，包括但不限于目录穿越、SQL注入、XSS跨站脚本攻击、web路径遍历漏洞攻击，高亮显示攻击特征。提供由厂商盖章确认的产品界面截图证明。  8.1.3文件篡改检测：可检测文件的篡改行为，包括：“创建、写入、修改权限、重命名、删除”等篡改行为。提供由厂商盖章确认的产品界面截图证明。  8.2 漏洞攻击屏蔽：精准检测恶意攻击源、扫描源，并可基于告警风险值、或者定向源进行屏蔽，使漏洞扫描器、恶意攻击源无法扫描到主机存在的漏洞。提供由厂商盖章确认的产品界面截图证明。  8.3资产识别:可识别精细化识别主机的硬件信息（包括cpu、线程、内存、磁盘等使用率信息），网卡信息，运行进程、自启动服务、安装软件等。  9.风险统计  9.1 报表管理  9.1.1站点报表：支持生成excel、word格式的综合报表、外部攻击面报表、内部攻击面报表、安全事件报表等报表类型，每月、每周、每季度生成运营报表，也可以单独导出资产报表、主机风险报表、网站风险报表、攻击事件报表等，可基于资产范围、位置、责任人、部门、时间、模块等条件筛选范围生成报表。  9.2 监测中心  9.2.1监测中心：通过监测中心可统一展现蜜罐告警事件、主机威胁事件、流量检测告警，事件及告警结果自动刷新。支持蜜罐、主机威胁与流量告警的关联分析，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。提供由厂商盖章确认的产品界面截图证明。  9.1.2大屏展示：支持大屏展示功能，可视化呈现监测中心的数据，包括主机资产监测概况、攻击监测诱饵监测概况，大屏界面能够自动刷新监测数据，实时展示最新监测结果。  10.其他功能  10.1多级用户管理  10.1.2二级用户关联资产运维：一级用户可创建与管理二级用户，并可给二级用户关联资产。  10.1.3多级用户管理，一级用户可查看与管理二级用户所有资产风险信息，二级用户只能查看与管理自身的资产风险信息。提供由厂商盖章确认的产品界面截图证明。  10.2告警:多样化告警方式,支持将平台监测事件，通过企业微信、钉钉、飞书通知管理员及时处置，支持邮件告警，可自定义告警邮箱，提供由厂商盖章确认的产品界面截图证明。  11.产品资质:产品需为国内自主研发，提供软件著作权证书。  六、服务期限：自合同签订之日起为期一年。在服务期限内，设备不得拆除撤回。服务期满后，须彻底清除设备内所有数据，方可进行设备拆除撤回。 | 1年 |

1. **项目产品基本要求**

1、以上产品必须是具备合法资质的制造商生产的**全新正品**，并满足招标采购文件的要求，若产品在运输或安装过程中损坏或擦伤须无偿调换相同产品。

2、投标人所投产品参数应同等或优于以上各项参数要求，产品、辅材及生产工艺符合国家相关规范。

3、投标人应保证所提供的货物或其任何一部分均不会侵犯任何第三方的专利权、商标权等，如在使用过程中出现的一切经济和法律责任均由投标人负责。

4、投标总价必须包含货物及货物运抵指定交货地点的各种费用和安装调校、售后服务、税金、验收检验及其它所有费用的总和，如另有要求请在投标文件中注明。

5、投标人在竞价文件中必须提交设备配置清单，如设备有配套耗材及定期更换的配件请投标时与设备一起报价。

6、投标人所投产品必须提供产品“三包”服务；定期安排相关人员回访进行质量跟踪；保证提供临床应用和售后技术服务支持方式；保修期后提供终身维修服务及配件供应；其他售后服务按厂家承诺实行。

**（四）商务要求**

**1、投标人资格要求**

1）竞争性谈判供应商应为满足《中华人民共和国政府采购法（中华人民共和国主席令第八十六号）》第二十二条规定各项标准的法人、其他组织或者自然人。

2）被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将被拒绝其参与本次招投标活动（在“信用中国”网站（www.creditchina.gov.cn）或“中国政府采购网”（www.ccgp.gov.cn）查询相关供应商主体信用记录。）

3）被列入我院投标人黑名单（在我院招投标活动中存在2次违规行为）未满3年的投标人将被拒绝其参与本次招投标活动。

4）本项目不接收联合体投标。

**5)是否专门面向“中小企业”开放竞标： 是**

**6）**是否接受进口产品： 是

**2、投标产品资格要求**

1）本项目支持创新产品、节能优化产品、环境标识产品、中小企业发展等政府采购政策。

2）投标人所投产品要求包含以下相关证件：软件著作权证书。

**3、售后服务和资质**

1）售后资质要求：厂家须设有24小时免费服务电话，成交供应商应提供维保人员名单、联系电话等。

2）维修备件必须是原厂备件。

3）质保期：设备安装完毕通过验收投入使用之日起不少于 1 年。

4）故障处理：质保期内，在使用过程中发现质量问题或故障时，须接到通知后24小时内派工程师到达用户现场及提供常用备件，按国家及行业标准对故障进行及时处理或更换，以保证采购单位的正常使用，所发生的一切费用由成交供应商负责。

5）签订合同后，30天内仪器设备安装调试结束并交付使用。投标人予以特别注意：如出现未能到期供货的情况，采购人有权单方终止合同的执行，所有的经济损失由逾期供货商单方承担。

6）交货地点为：广西壮族自治区桂东人民医院

**7）**付款条件（进度和方式）

（1）分期付款：签订合同后，全部货物到达指定地点、安装调试并验收合格后，凭双方签署验收合格书，甲方按照政府规定时间内支付，第一期：甲方支付合同总金额的90% ；第二期：交付后十二个月，经乙方书面申请，甲方支付合同总金额的 10%（不计利息）。

**二、合同签订**

招标人和中标人应当自公示结束后25日内签订采购合同。

**三、其他**

**四、特别说明**

如果招标文件中对部分采购设备技术参数要求不详细，请各投标人在投标时补充说明。如投标人不作补充说明，广西壮族自治区桂东人民医院招标管理办公室将从有利于招标人的角度出发，认定其所报配置为可能存在情况的最高标准。

**第四章  评标方法与评分标准**

**一、评标方法与定标原则**

评委会将对确定为实质性响应招标文件要求的投标文件进行评价和比较，评标方法采用 **最低评标价法** 确定中标候选人。