

服务范围及服务要求

1 分标

序号	标的的名称	数量及单位	技术要求
1	网络安全运维服务	1 项	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：渗透测试针对采购人单位具体某个系统，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，充分挖掘采购人单位信息泄漏的途径，从根源上解决存在的漏洞或问题，减少采购人单位信息泄漏事件的发生。供应商需使用人工渗透测试技术，对采购人单位管辖范围内的某个 Web 站点进行挖掘 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：采购人指定的业务系统。 1.4 服务频率：4 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. 互联网数据泄漏监测服务 3.1 服务内容：通过各类互联网搜索引擎与第三方信息库，监测采购人单位外部信息：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：采购人单位互联网数据。 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采购人单位的资产进行梳理，建立采购人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：对采购人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：对采购人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：对采购人单位终端 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：通过管理采购人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，为采购人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：对采购人单位管辖范围内的 Web 站点进行扫描，排查 WEB 站点中的 SQL、XSS、敏感信息泄漏、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，持续对采购人单位的网站进行全站页面爬取，发现敏感词字眼。 敏感文件泄漏事件监测：对采购人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、webshe11、后门以及挖矿等主机安全事件与行为进行 7×24 小时实时监测，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。服务采购人单位使用基线核查工具或人工检查，对采购人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 帮助采购人单位防护多种漏洞，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，在不改变采购人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（具体数量根据采购人单位实际需求），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，供应商收到采购人单位申请应急响应支持，由供应商技术支持人员和采购人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，并协助采购人单位解决事件。 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，提交给采购人单位。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，并结合实际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：《网络安全事件应急响应报告》。 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、采购人单位职工、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的
--	--	---

			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。成交后 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：通过单位全称、关键字、出口 IP 等信息，收集单位/企业信息、邮箱信息、敏感代码、敏感文档、app 程序、微信小程序、微信公众号等外部/互联网攻击面信息，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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；响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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；响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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；响应文件中提供产品界面功能截图证明并加盖供应商公章。 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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲3.2.2 多网卡探测：通过对历史资产探测任务进行二次扫描探
--	--	--	--

		测，发现探测网络上的主机是否存在多网卡，结果信息需包括主机网卡 IP 及多网卡 IP，响应文件中提供产品界面功能截图证明并加盖供应商公章。 3.3 资产台账 3.3.1 支持自动识别 url 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。 3.3.2 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。 3.3.3 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。 3.3.4 支持对已知 url 资产进行深度扫描，进一步发现登录后台和 API 接口，并识别是否暴露外网。 3.3.5 可自定义展示列，可排序、选择是否显示。 3.4 MAC 地址自动识别 ▲3.4.1 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”，响应文件中提供产品界面功能截图证明并加盖供应商公章。 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：本地化提供对网站的“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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲4.1.2 敏感文件事件泄漏监测：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，可在系统上查看泄漏的信息以及敏感文件下载链接，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 4.2 漏洞扫描与漏洞管理 ▲4.2.1 完善的漏洞库：漏洞库漏洞信息大于 340000+条，集成 4500+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。通过 POC 验证过的漏洞，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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 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，对于捕获的流量进行存储、分析，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，精准识别攻击源头，发现不同场景下的已知威胁和未知威胁。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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，包括但不限于非法外联-拦截域名解析的 IP（高风险）、外网恶意攻击（高风险）、利用成功（高风险）、暴力破解（高风险）、外
--	--	--

		网可疑访问（中风险）等标签，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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲5.1.3 实时翻墙上网监测：支持流量加密及非加密场景的翻墙上网行为监测，无需加载证书，可识别主流翻墙工具（如 V2Ray、Surfshark、naiun、clash verge 等）。可关联威胁情报，识别命中非法代理、加密代理节点、订阅链接域名、IP、C2 服务器等违规外联行为。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲5.1.4 提供翻墙行为专属可视化看板，展示翻墙主机 IP，翻墙主机是否暴露在外网、命中规则类型、目标域名或 IP、翻墙工具、首次发现时间、最近活动时间等关键信息。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲5.1.5 支持通过企微、钉钉、飞书、邮箱等方式，自动识别并告警翻墙行为。响应文件中提供产品界面功能截图证明并加盖供应商公章。 6. 内网威胁诱捕扩展能力 6.1 无侵入式全网病毒监测 6.1.1 trunk 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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 6.2.2 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”。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 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程控制程序、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、尝试登录、端口扫描、攻击尝试、强力攻击、异常进程、暴力破解、登录成功、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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 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。响应文件中提供产品界面功能截图证明并加盖供应商公章。
--	--	--	--

			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。 8. 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 webservershell、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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 9.2.2 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。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲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，响应文件中提供产品界面功能截图证明并加盖供应商公章。 11. DeepSeek 模型 AI 智能研判 11.1 本地 AI 模型研判 ▲11.1.1 联动本地 DeepSeek AI 模型，联动分析“流量、蜜罐、主机”三者告警结论，关联“资产+漏洞”信息，辅助输出综合研判结果：1. 给攻击源 IP 定性并打上攻击者标签，如：非法外联、外网恶意攻击、内网恶意攻击、漏洞利用成功等。2. 输出攻击源资产画像，包括网络区域、主机名称、MAC 地址等。响应文件中提供产品界面功能截图证明并加盖供应商公章。 ▲11.1.2 接入 DeepSeek 大模型的云端 AI 智能体，支持深度思考模式：1. 支持对流量、蜜罐、主机等告警事件研判，输出研判过程与研判结论。2. 告警传输前可自动过滤“身份证号”、“手机号”、“邮箱”信息，避免客户数据泄漏。3. 研判结果包括但不限于：分析 payload 中明显攻击特征，分析响应报文并判断是否攻击成功，关联威胁情报输出病毒外联事件关键点。响应文件中提供产品界面功能截图证明并加盖供应商公章。
采购预算：21 万元		
▲一、商务要求		
合同履行期限和地点	1. 合同履行期限：自合同签订之日起为期三年。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。 2. 交付使用期：自合同签订之日起 30 个工作日内，完成调试和集成工作。 3. 地点：梧州市采购人指定地点。	
合同签订时间	自成交通知书发出之日起 25 个日历日内。	
付款条件	完成调试和集成工作并验收合格后，凭双方签署验收合格证，成交供应商开具全额增值税发票给采购人，采购人按维保年度分 3	

	次支付，每次支付合同总额的三分之一。 如验收不合格，采购人有权采取依法解除合同、拒付款、索赔等措施。
报价要求	项目总报价包含各种费用和售后服务、税金、验收检验及其它所有费用的总和。
其他要求	供应商应保证所提供的服务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供应商负责。
验收标准（质量要求）	1. 成交供应商需承担供货时产品质量抽样检测的相关费用以及项目验收时发生的一切费用（如有）；验收标准应符合中国有关的国家、地方、行业标准。 2. 当项目完成调试和集成工作后，由成交供应商向采购人提出项目竣工测试申请，并于验收前向采购人提供一切有关技术文件、资料、图纸和相关记录等竣工材料，并在竣工前 7 个工作日通知采购人及有关部门准备验收。拟竣工项目的实施总体功能、性能符合采购人认可的技术设计方案及合同规定的，予以验收，并作出验收结果报告。供需双方签署项目终验验收证书，并自正式交付使用之日起，整体项目才视为接受，并开始计算质保期。