第二部分 技术要求

序号	名称	规格	数量	单位
1	数据安全风险监督检查工具箱	防护箱要求：箱体应配备拉杆、滑轮和密码锁。 工具箱性能要求：1、镜像流量处理速率≥300Mbps;2、系统扫描，最大可扫描 IP 或域名数≥512；3、扫描任务并发≥5，扫描 IP 并发≥50；4、最大可扫描网站数≥50；5、自带 3 年资产脆弱性特征库；cpu:主频：≥2.9GHz，最高睿频≥4.8GHz，三级缓存≥16MB，物理核数≥8，线程数≥16；内存：大小≥32GB DDR4，最大内存容量≥128GB，I/O 接口：千兆网口≥2，USB3.2(Type A)接口≥2，电源接口≥1；外设规格：配备键盘、鼠标等；存储：固态存储容量≥1TB SSD；屏幕为≤14 英寸，显存≥64G，支持国产操作系统。 工具箱功能要求： *1、实现对核心资产设备的一站式台账管理，包括边界资产、视频资产、文件服务资产、WEB 资产、服务器资产，支持查看所有被监管的设备资产信息，支持通过设备类型、所属区域、设备年限、IP 地址等检索条件进行查询和筛选。（提供经 CMA/CNAS 认可的第三方检测报告证明并加盖原厂公章） *2、具备各种核心资产的发现能力，支持通过发包探测、端口扫描、WEB 扫描和镜像流量方式，获取核心资产的品牌型号、端口和服务列表、设备类型（包括网闸、单向光闸、数据交换系统、代理服务器、NAT 网关、可信认证接入网关、视频交换系统等不少于 50 种设备资产类型）；（提供经 CMA/CNAS 认可的第三方检测报告证明并加盖原厂公章） *3、支持部署在 IPV4、IPV6 环境下，且系统扫描、Web 扫描、数据库扫描、弱口令扫描、基线配置核查等各类型任务均支持添加 IPv6 扫描目标。（提供经 CMA/CNAS 认可的第三方检测报告证明并加盖原厂公章） 4、支持针对指定 IP 段，同时一键下发系统扫描、Web 扫描、弱口令扫描任务，其中 Web 扫描能够自动发现该网段内的在线网站并开展扫描；弱口令扫描能自动发现该网段 IP 开放服务并自动开展弱口令扫描。 5、支持按照固定格式，对检查结果进行汇聚、融合，生成符合要求的正式文档，支持导出、打印检	1	台

		查结果、检查报告等内容。 6、支持开展数据资产排查梳理，可显示数据资产排查梳理完成度，采用探针技术识别发现数据资产及其分类分级，具备数据资产目录和检索能力。 *7、支持检测的系统漏洞数≥17 万，覆盖 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq 多种漏洞标准。（提供经 CMA/CNAS 认可的第三方检测报告证明并加盖原厂公章） 8、默认内置多种不同的检测模式，包含但不限于标准扫描、快速扫描、完全扫描、深度扫描，不同检测模式默认对应不同的扫描任务策略及配置。 9、支持对网络资产识别和风险检测，对目标域中业务系统（包括应用、数据库、文件、数据服务、前置机等）的服务器、主机系统常见漏洞和弱口令进行检测，发现数据安全风险隐患。 10、支持自定义基线核查规则，可基于系统内置的检查规则快速修改基线值或参数，以满足特定配置核查要求。 11、基于数据内容检测，对敏感数据是否脱敏，个人信息是否匿名化处理进行检测，发现数据安全风险隐患。 12、基于网络流量检测，对敏感数据的明文传输情况进行检测，发现敏感数据保密性、完整性隐患。 *13、支持多种探测模型，包括文件泄露风险、cookie 中包含密码信息、单次返回数据量过大、数据库查询 API、未鉴权访问、api 参数可遍历、弱口令、明文传输密码、命令执行 API、数据出境风险；（提供经 CMA/CNAS 认可的第三方检测报告证明并加盖原厂公章） 14、厂家提供数据检测报告		

2	安全事件应急处置工具箱	1、应急处置终端 cpu 处理器：≥英特尔® 酷睿 I7 系列；内存：≥16G；硬盘容量：固态存储容量≥256GB SSD，机械存储容量≥1TB 机械硬盘；屏幕规格：≥14 英寸；包含病毒检查工具、木马检查工具、取证工具、移动硬盘、winPE 工具、webshell 检查工具、日志提取工具、防震箱。 2、支持设置线索，发现关键可疑行为，包括 IP 线索、关键词线索、文件名线索、时间线索的设置； 3、支持根据所提供的线索自动发现关键可疑行为并进行标记； 4、支持根据勒索文件后缀查找对应解密工具，提供解密工具的下载、使用介绍等； 5、支持按照分区、磁盘、内存进行证据固定生成固定镜像文件； 6、支持一键提取安全事件相关信息，包括系统配置信息、使用痕迹信息、运行状态信息、恶意代码情况等； 7、支持自动搜索功能，可以自动搜索出某一网段或指定 IP 范围内（端口号可默认或指定范围）的活动数据库，获得数据库的基本信息（包括 IP、数据库类型、服务名、端口号、数据库版本等）； 8、支持针对数据库每张表每个字段的内容进行敏感数据探测； 9、支持主动扫描、被动扫描两种模式的深度扫描；支持多域名批量扫描； 10、支持设置跳过主机发现进行扫描； 11、支持资产管理并从资产管理中导入资产记录进行扫描； 12、支持扫描原始数据、测试数据的查看与浏览器回放显示； 13、支持自动提取使用痕迹相关文件； 14、厂家提供数据检测报告 以上功能需提供证明截图并加盖原厂公章	1	台

备注：售后服务要求

1、系统或设备出现故障时，立即安排人员进行抢修、维护，并确保在 8 小时内解决问题，如需替换不在备品备件库中的设备，承诺立即协调，免费提供。

2、提供三年售后质保，在质保期内免费提供硬件维修、更换，软件升级维护服务。

3、数据安全检查供应商须按照采购人工作需要，定期配合采购人开展安全检查。

4、供应商应针对设备使用和日常维护开展专项培训，使用户达到独立管理使用的目标。

5、供应商须第一时间响应采购人在网络安全案事件中的支援需求，在网络安全案事件的应急处置中及时全面地提供技术支撑。