采购需求

态势感知：

指标项	技术参数要求
数量要求	态势感知安全设备，1 台
基本要求	1、2U 机架式设备，接口≥6 个千兆电口+2 个万兆光口，冗余电源，内存≥128G，硬盘≥16TB，支持 raid。 2、数据采集器性能≥20000 条/秒；支持≥10 亿条数据秒级检索响应；支持态势监测、响应处置、分析研判、资产管理、集中管控、安全治理、安全审计、威胁情报等功能模块。 3、含 10 个设备许可数，含三年精准威胁情报、软件升级、硬件质保。
功能要求	1、支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势，支持大屏展示时间设置，支持态势大屏中相关信息下点击跳转到对应的详细页面。 2、支持全网资产概述、风险资产、风险业务系统、漏洞概况、防护设备日志监测概况、告警趋势、攻击趋势、告警统计、最新告警、威胁类型排行等内容的相关展示； 3、支持拖拽方式自定义大屏界面展示顺序，支持不少于多种地图、拓扑展示方式，包括但不限于世界、全国、省份、拓扑、实时数据、历史数据等，支持 logo、版权、大屏超时设置、可视化大屏轮播展示、全网态势、攻击态势、态势三屏的态势单屏专属配置等通用设置（提供产品截图证明）。 4、支持基于场景的安全策略响应编排，支持不少于预案及案例两种场景类型，支持以列表形式展示预案信息，包括预案名称、预案类型、响应动作、关联案例数、来源、创建时间、描述等；支持对预案总数、被引用预案总数、未被引用预案总数等进行统计；支持对案例进行新增、删除、启用、停用等操作，并支持案例批量处理；支持从告警维度查看案例对告警的响应处置详情，支持集中管控执行联动处置动作后下发给安全设备的策略管理（提供产品截图证明）。 5、支持查看、审批、删除等封堵申请报告，支持以报告名称、报告生成时间、提交人、封堵内容、对应日志名称、发生时间等为条件对申请进行检索。支持下载封堵报告，并支持 word 与 PDF 等格式。 6、支持资产外联分析，分析维度包括资产外联热力地图、外联资产排

	名 TOP10、访问目的排名 TOP10、外联趋势、外联事件列表等； 7、支持横向威胁分析，分析维度包括横向威胁的移动轨迹、威胁类型分布、目的端口分布、发起威胁的资产 TOP10、遭受威胁的资产 TOP10 等； 8、支持从日志中发现威胁源，支持以列表形式展示威胁源相关信息，支持威胁加入白名单、关注名单、加入威胁情报库、立即封堵等操作，支持与云端情报进行碰撞。 9、支持对业务系统进行画像、支持以列表形式展示业务系统相关信息，展示信息包括业务系统名称、关注属性、关联资产数/失陷资产数、漏洞、告警、责任人等，支持按照日期、业务系统名称、业务重要性、是否互联网暴露、等保级别、责任人、业务系统类型等进行过滤查询，支持按照 TXT、CSV、EXCEL 等格式进行业务系统信息到处，支持业务系统名称、关联资产数/失陷资产数、告警等字段下钻（提供产品截图证明）。 10、支持内置多种分析模型，包括但不限于失陷状态、FTP 登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等，支持模型新增、编辑、删除、查看、启用、停用等操作（提供产品截图证明）。 11、支持资产探测任务管理，支持任务添加、修改、删除、开始扫描、重新扫描等操作，支持任务列表展示，展示信息包括任务名称、扫描范围、类型、状态、更新时间等 12、支持管控设备概览，支持通过界面快速添加集中管控设备，至少支持与医院现有防火墙、数据库审计等设备的管控与联动处置，支持设备管控情况，包括总数、在线、离线、日志采集、性能监控、策略管控等；支持日志采集趋势展示。(提供产品截图证明)。 13、支持管控拓扑图展示，支持拓扑动态提示管理设备产生的告警，支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息（提供产品截图证明）。 14、支持策略管理，支持策略新建、删除、查看、编辑、下发、下发记录等，支持策略标签管理，策略内容包括名称、设备类型、执行设备、策略标签、策略分类、生效时间（提供产品截图证明）。 15、支持资产性能监测概览，支持监测设备总数、异常数、主机异常数、网络设备异常数、安全设备异常数展示，支持监控资产性能状态占比、性能告警、规则类型事件分布、CPU 使用率、内存使用率、磁盘使用率；

	16、支持新增、删除报告模版，内置报告模版包括但不限于安全告警分析报告、单部门统计报表、部门维度统计报告、资产风险评估报告、全网威胁评估报告、外部威胁评估报告、网络安全综合态势评估报告（提供产品截图证明）。 17、支持等保概览，包括但不限于等保系统级别分布、等保三级系统名称、整体进展、测评结果、待关注业务系统 18、支持等保检查结果记录，包括测评报告及整改报告上传，支持等保检查结果包括测评名称、业务系统名称、测评结论、测评结果、测评单位名称、推荐证书编号、联系方式、通讯地址、审核人、审核日期、完成测评日期、完成整改日期等（提供产品截图证明）。 19、支持威胁情报管理，包括恶意 IP 地址、恶意 URL、恶意样本、恶意域名、垃圾邮件等，支持情报进行分类自定义查询，支持自定义威胁情报信息；
服务要求	提供 3 年技术支持服务、3 年软硬件质保服务。

APT 安全监测

指标项	技术参数要求
数量要求	探针，1 台
基本要求	1、采用国产化 CPU 和操作系统，机架式设备,接口≥6 个千兆电口（含 HA 和管理口）+2 个千兆光口插槽，冗余电源,≥1 个扩展槽位； 2、APT 性能≥1Gbps，探针性能≥2Gbps，并发连接≥20 万，新建连接≥1 万/S，静态检测≥5 万样本/天。 3、含 3 年规则库升级许可，包含但不限于攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库。
功能要求	1、支持威胁监测功能，包括：威胁事件总数、APT 事件、挖矿事件、失陷主机、攻击趋势图、攻击者分布地图等信息。 2、支持攻击者视角分析，按照攻击者、内网、境内、境外、攻击者分布地图、攻击主机 TOPN、归属地、事件描述、受害者、次数、首次发现时间、最近发现时间等条件综合分析攻击者信息，支持攻击者处置功能。 3、支持受害者画像分析，包括：被攻击次数、攻击成功数、是/否失陷、应用协议分布、攻击链、攻击者、事件描述、次数、通联关系图、ATT&CK、被攻击记录等条件综合分析受害者画像信息。(提供截图证明)

	4、支持文件视角分析，按照恶意文件分类、恶意文件传播趋势进行统计分析。记录被检测文件信息，包括：文件名、文件哈希、文件类型、文件大小、事件描述、恶意文件类型、风险等级、应用层协议、首次发现时间、最近发现时间等，支持下钻查看文件详情信息，包括攻击者、受害者、检测引擎、攻击次数等。支持样本下载。(提供截图证明) 5、支持账户安全视角分析，包括：应用类型分布、弱口令排名、受影响资产 TOPN、用户名、服务器地址、服务器端口、应用协议、事件描述、攻击结果、次数、首次发现时间、最近发现时间等条件综合分析账户安全信息，支持事件处置等功能。 6、支持挖矿专题分析，按照挖矿阶段统计、矿池排名、样本排名、币种排名等进行统计分析。记录挖矿主机、事件描述、币种、矿池、挖矿阶段、次数、首次发现时间、最近发现时间等信息综合分析挖矿内容。(提供截图证明) 7、支持资产分析能力，分析内容包含：资产总数、存在风险资产数、威胁事件、业务分布、资产状态、资产类型、指纹信息、端口排名、操作系统分布、文件服务排名、WEB 站点排名等。 8、支持沙箱动态分析，包括：执行流程、风险行为、进程内存、释放文件、提取文件、释放缓冲区、网络分析、页面截图、执行信息等信息。支持反沙箱逃逸检测。(提供截图证明) 9、支持对压缩文件分析，包括：多层压缩文件、压缩文件中衍生文件等，支持≥10 层解压，可对压缩包内的文件进行独立检测。 10、支持多种攻击类型检测，包括：扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、车联网漏洞攻击、物联网漏洞攻击、凭据异常等在内的攻击事件。 11、支持暴力破解检测、支持弱口令检测，能够按照弱口令字典（支持正则、中文)、口令强度（密码长度、类型、用户名子串）等方式进行弱口令检测。 12、支持从外网到内网、外网到外网、内网到外网、内网到内网方向的敏感数据检测。包括身份证、移动电话、固定电话、银行卡、护照、车牌号、邮箱、联系人地址、驾驶证编号、军人证号、增值税注册地址、联系人姓名、客户名称、港澳通行证等。 13、支持 DGA 恶意域名检测、DNS 隧道检测、DNS 投毒检测等；

	14、支持 ARP 投毒检测，支持基于 ARP 请求源 IP 地址无效、ARP 应答源 IP 地址欺骗、ARP 应答目标 IP 地址无效、ARP 请求源 MAC 地址不一致、ARP 应答源 MAC 地址不一致、ARP 应答目标 MAC 地址不一致进行检测。（提供截图证明） 15、支持卸载 SSL，实现对 HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、MQTT、SIPS、XMPPS、SMB、NFS、MYSQL、POSTGRESQL、DB2、REDIS、MONGODB 等多种协议加密流量的分析检测。
服务要求	提供 3 年技术支持服务、软硬件质保服务及相关规则库升级服务。