**宁波市档案馆态势感知一体机设备采购要求**

**一、项目名称：**宁波市档案馆态势感知一体机设备采购项目

**二、项目概况**

宁波市档案馆计划采购态势感知一体机设备，主要包括但不限于设备采购、设备运输、设备的安装、调试服务等。

**三、采购设备清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术参数** | **数量** | **单位** |
| 1 | 态势感知一体机设备 | 基于实时流数据为用户提供安全分析能力和风险告警及多维度可视化展示，提供安全决策依据、提高信息安全的纵深防御能力。  数据采集和处理性能≥12000EPS，每条数据大小>1KB；  10亿数据关键字查询结果响应时间<2秒。  CPU≥24核\*2，内存≥256GB，配置企业级存储磁盘总容量≥48TB；电源规格：冗余电源；网口要求：千兆电口≥4；采用国产化CPU芯片与国产化操作系统  包含以下引擎和模块：  1、智能化威胁检测引擎 2、多维度攻击溯源引擎 3、场景化威胁感知引擎 4、集成化联动响应引擎 5、启发式威胁狩猎引擎 6、安全运营工作台模块 7、可视化模型编排引擎 8、重大活动保障模块 9、资产管理模块。（提供三年系统免费升级服务，以及提供一年网络支撑服务，包含渗透测试、漏洞扫描、安全审计、应急响应等） | 1 | 台 |

**四、技术参数要求**

|  |  |
| --- | --- |
| 指标项 | 技术参数 |
| ★性能要求 | 数据采集和处理性能≥12000EPS，每条数据大小>1KB；  10亿数据关键字查询结果响应时间<2秒。 |
| ★规格要求 | CPU≥24核\*2，内存≥256GB，配置企业级存储磁盘总容量≥48TB；电源规格：冗余电源；网口要求：千兆电口≥4  采用国产化CPU芯片与国产化操作系统 |
| 工作台 | 工作台首页支持自定义个性化配置，支持以拖拽方式进行画布页面设置，页面可选组件包括原始告警、资产管理、组件管理、风险资产、安全事件、安全日志、平台概览、快速搜索、安全设备、SOAR、系统消息、通报预警、工单、告警监控等，可选组件不少于36个，每个组件均支持点击“收藏”按钮进行自定义收藏（需提供截图证明）； |
| AI高级分析 | 平台内置不少于3种机器学习分析场景模型，可Web攻击检测分析、DGA域名检测分析、钓鱼邮件检测分析等特定场景条件下的安全态势异常。 |
| ★通过先进AI人工智能技术，实现自动识别资产，并将相关信息进行分类整理，方便后续的数据分析和决策制定。（提供国家权威机构证明材料） |
| ★支持UEBA、贝叶斯、随机森林等长周期高级机器学习算法；（提供国家权威机构证明材料） |
| 安全态势可视化 | 支持立体、平面、球面等多种维度的网络实体关系透视，点击每个实体可展示资产名称、风险评级、告警TOP3、最近异常发生时间等，点击实体间的访问连线可展示实体间访问方向、访问类型、累计流量、最近访问时间等（需提供截图证明）； |
| 监测中心 | ★支持告警数据自动化归并，并通过告警列表条目颜色区分“已读告警”和“未读告警”；支持查看归并告警基本信息、规则详情、原始告警列表、全部字段、PCAP包详细信息，并支持下载PCAP包；支持在归并告警页面进行告警快速处置，包括忽略告警、误报处置、联动处置、人工处置等（需提供截图证明）； |
| 支持告警展示偏好设置，可配置登录默认筛选告警条件，配置包括攻击结果、告警类型、威胁等级、攻击阶段、攻击方向、处置状态、时间范围等信息；支持告警自动刷新； |
| 分析中心 | 应内置包括规则模型、关联模型、统计模型、情报模型、AI模型等不少于5类安全分析模型，数据配置可选择不同作用域，如全局通用、单选机构，单选机构可选择单独的组织架构； |
| 安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容； |
| ★支持智能检索语句分析，支持检索语句的中文、英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，保留检索语句历史记录；检索语句可直接发布成统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警（需提供截图证明）； |
| ★实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展（需提供截图证明）； |
| 响应中心 | 支持通过单条告警、聚合告警添加白名单，快速过滤误报；白名单配置可自定义过滤条件及作用的组织架构，白名单生效时间设置包括长期生效和定期生效，新建白名单策略可将最近7天告警标记为已处置-误报；支持白名单策略状态的开启、关闭，并统计策略本日匹配次数 |
| 支持钉钉、阿里云、腾讯云等进行消息通知； |
| ★支持将联动设备能力封装到APP，通过导入APP的方式实现和不同产品的联动，支持设置3层递进阻断策略（如第一次阻断10分钟，第二次阻断30分钟，第三次永久阻断），支持选择多台联动设备下发阻断策略；支持查看封禁设备数、封禁IP数、自动封禁IP数、本日解禁IP数、封禁订阅规则数、封禁SOAR剧本数，支持查看最近7天封禁IP趋势及防护设备封禁IP分布；支持封禁策略批量删除、解禁、导出  （需提供截图证明）； |
| 运营中心 | ★平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址（需提供截图证明）； |
| 支持对接威胁情报中心，支持情报离线更新及在线更新，支持查看情报源中有效情报数、最近更新条数、最近更新时间、今日更新情报数、昨日命中情报数等；支持对接第三方威胁情报平台，支持配置外部情报碰撞接口及查询接口，可对接口请求进行限制； |
| ★利用先进的威胁情报提取等主题检测技术，实现从海量数据中准确地识别、分析和检测关键的威胁情报信息。（提供国家权威机构证明材料） |
| 支持重大活动保障功能，重大活动保障任务可分为备战、临战、实战、战后复盘等多阶段，每个阶段均有相应的动作内容；保障监测视角覆盖云、管、端、边界、应用等，保障期间实时展示会战纪实，如纪实名称、状态、相关资产等； |
| 资产中心 | 支持人工录入、流量自动发现、主动扫描、web自动发现、资产同步等不少于5种的资产数据接入方式；流量自动发现方式能自动识别资产类型，如Web服务器、DNS服务器、邮件服务器、FTP文件服务器等多种类型资产，支持web业务系统自动发现；支持批量确认流量发现的资产（需提供截图证明）； |
| 支持私网IP、公网IP、MAC地址、域名、主机名多种类型资产识别方式，IP类资产支持IPv4和IPv6，并支持资产组织架构、责任人、重要程度、资产类型、地理位置属性的批量修改；支持资产信息的增量导入和替换导入； |
| 支持通过流量发现、是否接入日志、PING方式检测资产是否在线； |
| 安全设备资产管理支持一键访问设备的管理界面、大屏投屏演示及设备原始日志，支持查看设备在线状态（需提供截图证明）； |
| ★售后服务 | 提供不少于三年质保服务，包含但不限于硬件保修、系统升级等服务内容； |

**五、投标人能力技术要求**

1.具有网络安全应急服务支撑单位证书（甲级）、信息安全服务资质认证证书（一级信息安全应急处理服务资质）、信息安全服务资质认证证书（一级信息系统安全集成服务资质）等相关资质证书。

2.拟派本项目的实施人员需同时具备信息系统项目管理师、CISP证书、ISO27001主任审核员认证、云计算安全知识认证CCSK证书、CICS国际注册内控师资格认证、等级保护中级及以上测试师等资质证书。

**六、供货要求**

（一）技术要求

1、供应商所投产品须提交详细的技术条款响应表。

2、成交供应商所提供的货物开箱后，如采购人发现有任何问题（如外观有损坏），成交供应商应以同样型号的货物在采购人商定的时间内更换，确保其使用。

3、完成供货设备的安装调试工作。

（二）质量要求

1、应严格按照询价文件的要求，在完全符合国家有关标准、行业规范和相关规定的要求下，提供全新的、未经使用的、原包装未拆封的产品。

2、须保证提供的货物完全与询价文件所述的质量、规格和性能相符，所使用的材料达到优质标准，保证所提供的产品在正确使用和条件下，在规定的使用寿命期内具有合理的性能。

**七、商务部分要求**

**（一）质保及售后服务要求**

1、产品质量保证期

成交供应商提供的所有产品质量保证期不低于3年。

2、售后服务要求

（1）成交供应商应具备完善的售后服务体系，成交供应商在质量保证期内应当为采购人提供以下技术支持和服务：

1）电话咨询

成交供应商应当为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。

2）现场响应

采购人遇到使用及技术问题，电话咨询不能解决的，成交供应商应在24小时内到达现场进行处理；并在48小时内解决相关问题。

**（二）交货及验收要求：**成交供应商负责将所有产品运到采购人指定地点，由成交供应商负责办理运输、装卸等，费用由成交供应商负责，由采购人组织验收，检验不合格或不符合质量要求，成交供应商除无条件退货、返工外，还应承担采购人的一切损失。

**（三）付款方式：**设备交付完成后一次性支付全部合同价款（可根据采购人要求调整）。

**（四）合同期限：**设备交付期限自合同订立日起30天内（具体时间可根据采购人要求调整）。

**八、报价要求**

（一）各供应商报价应包括但不限于产品采购、运输、安装调试、质保、相关售后服务及政策性文件规定等各项应有费用，以及为完成询价文件规定所涉及到的一切相关费用。

（二）各供应商应充分考虑所有可能影响到报价的价格及政策等风险因素，一旦成交，采购清单范围内价格将包定，合同期内一律不予调整；供应商的任何错漏、优惠、竞争性报价不得作为减轻责任、减少服务、增加收费、降低质量的理由。