**附件：态势感知系统技术需求表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备**  **名称** | **技术需求** | **单价**  **（万元）** | **数量**  **（套）** | **总价**  **（万元）** |
| 1 | 态势感知系统 | 机架式设备、配备冗余电源；  ▲必须能支持内外网两个独立网段  ▲CPU数量≥2个，内存≥128G；存储≥16TB；  接口：千兆电口≥4个，万兆光口（监听口）≥2个；  ▲设备性能：并发连接数：≥100万个；每秒新建会话≥1万个；流量吞吐≥1Gbps；最大日志处理速度≥1000eps  网络协议：能识别常见协议并还原网络流量，可用于取证分析、威胁发现；支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，文件类型包括可执行文件、压缩格式文件、文档类型文件  威胁情报：支持基于流量实时IOC匹配功能  动态监测：支持动态行为监控功能可监控文件、进程、网络、注册表等操作相关的系统和内核调用接口，能识别堆喷射、异常控制流跳转等漏洞利用攻击过程，支持未知威胁检测，支持敏感操作识别，可识别动态释放文件、动态启动进程、远程线程注入、文件自删除等操作，并能提取和还原相应参数。  Web攻击检测：支持检测针对WEB应用的攻击  威胁分析：应用安全的细分维度包括：WEB安全、数据库安全、邮件安全、中间件安全，统安全的细分维度包括：主机爆破、弱口令、未授权行为、挖矿行为，以攻击者的维度进行分析，可对攻击者进行画像  威胁溯源：支持检索异常报文、域名解析、文件传输、FTP控制通道、LDAP行为、登录动作、邮件行为、MQ流量、网络阻断、数据库操作、SSL加密协商、TCP流量、Telnet行为、UDP流量、WEB访问等网络流量日志，并可基于时间、IP、端口、协议、上下行负载等多重字段组合记录日志  资产管理：支持展示自动发现、终端管理系统获取和人工录入的资产信息，信息包括：资产IP、资产名称、分类、设备型号、操作系统、物理地址、网关标识、厂家  攻击源IP预警：支持多种攻击源IP的情报标签、自定义IP标签显示。 | **35** | **1** | **35** |

一、服务要求

文档交付：须提交完整可行的技术方案、实施方案、测试报告、验收文档等。

技术支持：须提供7X24小时技术咨询服务，接到电话后2小时响应，24小时内到达现场。

安装调试：要求提供原厂上门安装调试服务，服务包括但不限于硬件上架安装和配置、软件的安装和配置优化、业务相关参数配置、对产品功能进行测试。

培训服务：提供现场培训服务,提供培训资料。

▲售后服务：要求提供不低于三年原厂免费硬件保修服务，提供三年软件（包括但不限于应用特征库，防病毒库等）免费升级服务。

二、技术能力要求

态势感知系统制造厂商要具备中国信息安全测评中心颁发的安全开发类（一级及以上）和安全运营类（一级及以上），提供相关证明文件复印件或网页面截图，投标时要求提供生产厂商售后服务承诺函。

