**一、项目背景**

随业务发展，现有态势感知平台性能瓶颈，重点业务流量分析不全，存在网络安全监测盲区。为此，需提升流量监测覆盖面，并对现有态势感知平台进行扩容，拟采购1个分析平台节点及1台流量探针。

**二、需求说明**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **详细要求** |
| 1 | 态势感知分析平台 | 1个 | 软硬件一体设备，平台节点支持分布式部署，以节点的方式进行扩展，能够统一纳入平台管理。具备高级威胁监测、异常行为检测、告警处置等功能；支持对告警进行深度分析；支持日志关联性分析产生告警；支持威胁情报；  要求最大日志处理速度≥17000EPS，≥2U设备，千兆电口≥4个，SSD硬盘≥960G，SATA硬盘≥48TB，扩展槽位≥1个，冗余电源。 |
| 2 | 态势感知流量探针 | 1台 | 软硬一体设备，对网络流量的镜像流量进行采集并还原，还原后的流量日志加密传输给分析平台；拥有威胁情报实时匹配能力，能发现恶意软件、APT事件等威胁。  要求单探针流量采集能力≥10Gbps（实际处理不低于8Gbps）。≥2U设备，千兆电口≥4个，万兆光口≥4个（满配光模），扩展槽位≥1个，SATA硬盘≥8TB，冗余电源，提供高级旁路阻断功能模块。 |
| 3 | 软硬件维保服务、特征库及威胁情报更新授权 | 3年 | 对本项目采购的软硬件设备（即上述的分析平台节点及流量探针），提供3年的原厂软硬件维保服务、特征规则库及威胁情报授权服务。 |

**三、报价要求**

注：按照下列格式提供报价内容，不得修改表格，如有其他说明请在备注提出。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **需求内容** | **数量** | **单位** | **单价（元）** | **小计（元）** | **备注** |
| 1 | 态势感知分析平台 | 1 | 个 |  |  |  |
| 2 | 态势感知流量探针 | 1 | 台 |  |  |  |
| 3 | 软硬件维保服务、特征库及威胁情报更新授权 | 3 | 年 |  |  |  |
| **合计:** | | | | |  |  |