**一、项目背景**

随业务发展，新媒股份业务流量增长快速，导致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。

**二、项目需求**

本次建设包括2个分析平台节点及3台流量探针，平台节点用于扩容现有态势感知分析平台，流量探针部署于数据中心，探针数据回传至平台统一分析。本次项目建设需求清单说明如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **规格要求** | **需求说明** | **数量** |
| 1 | 态势感知分析平台 | 2U机箱；冗余电源；内存≥256GB；硬盘≥960G SSD+12\*4TB SATA；千兆电口≥4个，具备不少于5个扩展槽位。单节点处理性能不低于17000EPS。提供3年软件维保服务、特征库及威胁情报更新服务。 | 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；支持以节点的方式进行扩展。 | 2台 |
| 2 | 态势感知流量采集探针 | 2U机箱；冗余电源；内存≥64GB；硬盘≥4TB SATA；千兆电口≥4个，万兆光口≥2个，具备不少于4个扩展槽位。单探针流量采集能力≥10Gbps。提供3年软件维保服务、特征库及威胁情报更新服务。 | 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。 | 3台 |