船舶工业软件日志审计测试工具-技术需求

该工具以面向船舶工业软件为主要场景，交付物产品需要适配船舶工业软件的应用场景。

序号	货物（服务）名称	数量	单位	性能参数及技术指标（服务要求）
1	工业软件日志审计测试工具	1	套	1. 全城日志归集，统一管控； 2. 多源道配：持工控协议(Modbus、OPCUA 等)、操作系统、数据库、应用系统等各类日志接入、覆盖 IT/OT 全域设备； 3. 集中存储：分布式部署+中心化管理，解决工业现场设备分散、日志孤岛问题，保障数提完整性与可追溯性； 4. 实时同步：毫秒级日志采集，避免因延迟导致的取证缺失； 5. 智能解析与关联分析； 6. 语义化翻译：将原始日志转化为易读的事件描述（如“某账号登录失败”），降低人工解读门槛； 7. 行为基线建模：基于机器学习建立正常操作基准线，自动标记异常行为（如非工作时间方问、高频次错误尝试）； 8. 跨日志关联：串联用户操作、设备状态、网络流里等多维度日志，还原完整攻击链或事故过程； 9. 可视化与报表赋能； 10. 交互式仪表盘：直观展示日志总量、高危事件趋势、TOP 风险资产排行，辅助决策层掌握全局态势； 11. 一键生成报告：预置《网络安全法》《等保 2.0》等合规模板，自动输出审计周报/月报，简化迎检工作； 12. 钻取式查询：从宏观统计到微观日志条目，逐层深入定位问题根源； 13. 支持通过 REDIS、HTTP 方式进行数据外发； 14. 支持监控模板配置，系统预制包括监控模板 200+，系统支持对单个资产以监控任务的形式进行监控，支持单个任务的启停，监控时间间隔配置； 15. 支持 3D 模型导入，支持资产或资产组可配

				置到模型节点； 16. 日志解析配置智能体，日志解析配置智能体可以简化日志解析模板配置过程，用户使用智能配置可完成对新接入日志的解析规则方式选择和映射配置选择，简化配置的过程，减少配置的时间。