云南腾电科技有限公司

曲靖供电局110kV变电站电力监控系统网络安全态势感知系统建设-项目阶段性总结报告（YNTD-ITSS-0904）

编制人：谢广胜　　编制时间：2025.10.30

审核人：赵建中　　编制时间：2025.10.30

批准人：陆涛　　审批时间：2025.10.30

文件编制和变更履历

版本	编制/更改		发布		实施		更改记录
	作者	日期	审核	日期	批准	日期	
V1.0	谢广胜	2025.10.30	赵建中	2025.10.30	陆涛	2025.10.30	首次发布

目录

1. 运维服务概述

自曲靖供电局110kV变电站电力监控系统网络安全态势感知系统（以下简称“系统”）于2025年10月31日完成项目终验并正式交付以来，我方（云南中恒与云南腾电联合服务团队）依据运维服务协议，为该系统提供了为期两个月的首期运维保障服务。

本阶段运维工作的核心目标是：确保系统从“项目交付”向“稳定运营”平稳过渡，保障系统7x24小时稳定运行，有效发挥网络安全监测与预警效能，并初步建立常态化的运维协作机制。本报告旨在对本阶段运维服务工作进行全面回顾、总结与评估。

2. 本阶段主要运维工作内容

2.1. 系统监控与日常巡检

实施情况： 建立了每日、每周两级巡检制度。每日通过平台自监控模块检查核心服务进程、数据采集流量、存储空间及CPU/内存使用率；每周进行深度巡检，包括日志完整性分析、规则库更新状态核查及备份任务验证。

关键数据： 本阶段累计执行日常巡检62次，周度深度巡检9次，生成巡检报告71份。系统核心服务可用性持续保持在99.95% 以上。

2.2. 事件响应与故障处理

实施情况： 提供7x24小时应急响应通道。共接收并处理各类告警及事件单15起，其中：

安全事件告警： 8起（经分析，7起为误报或低风险扫描行为，1起为内部策略违规访问，已协助闭环处置）。

系统性能告警： 5起（主要为特定时段数据峰值导致的分析延迟，通过优化队列策略已解决）。

采集异常： 2起（1起为网络波动导致，1起为探针配置漂移，均已快速恢复）。

关键指标： 所有事件均实现100%响应，严重及以上事件（如有）的解决时间满足SLA要求（<4小时）。平均事件解决时长（MTTR）为 2.1小时。

2.3. 系统维护与优化

实施情况：

规则与模型优化： 根据初期运行产生的告警数据，协同甲方安全分析人员，对3条产生高频误报的检测规则进行了阈值调优，误报率下降约40%。

性能调优： 针对试运行期间发现的特定复杂查询响应较慢的问题，对数据库索引进行了优化，相关场景查询效率提升约60%。

补丁与更新： 在甲方批准的维护窗口内，完成了态势感知平台一次小版本补丁更新，修复了已知的次要缺陷。

2.4. 知识传递与协作

实施情况： 组织了2次专题培训，内容分别为“平台日常运维操作进阶”和“典型安全事件分析案例复盘”。同时，通过日常事件处置的“实战带教”，持续向甲方运维团队传递经验。

协作机制： 建立了“运维协作群”作为日常沟通主渠道，并坚持每周进行一次运维周会，同步状态、对齐问题、规划工作，运行顺畅。

3. 运维成果与成效分析

3.1. 系统稳定性得到验证

经过两个月的连续运行，系统硬件、软件及架构层面均未出现重大故障，高可用机制在计划内重启测试中切换成功，验证了前期建设与扩容成果的可靠性。

3.2. 安全监测价值初步显现

系统累计采集并分析安全日志超千条，初步构建了变电站监控网络的安全基线。成功识别并协助处置1起内部策略违规事件，证明了系统在发现“违规”和“异常”方面的能力，安全价值开始体现。

3.3. 运维流程初步固化

双方团队共同磨合，形成了从“事件发现->通报确认->联合分析->处置闭环->报告归档”的初步协同流程，为后续长期自主运维与托管服务相结合的模式奠定了基础。

4. 遇到的问题与改进措施

序号	问题描述	原因分析	已采取的改进措施	后续建议
1	部分威胁告警规则误报率偏高	初期规则阈值基于通用场景设定，未完全贴合本地网络实际流量模式。	结合本地流量白名单和业务特征，对相关规则进行了参数调优。	建议建立定期的规则评审与优化机制（如每季度一次），持续打磨检测精准度。
2	甲方运维人员对深度分析功能使用不熟练	项目培训偏重基础操作，实战分析经验需积累。	通过案例复盘进行针对性带教，并提供了常见分析场景的“操作手册”。	计划下一阶段开展“威胁狩猎”专项培训，提升主动发现能力。
3	运维数据（如报表）未能完全对接甲方管理需求	初期报表模板为通用格式。	已收集甲方管理层的具体报表需求，正在定制开发2张管理视图。	建议建立常态化的需求反馈渠道，使运维输出更好地服务于管理决策。

5. 下一阶段运维工作计划建议

基于本阶段总结，对下一阶段（2026年第一季度）运维工作提出以下计划建议：

深化主动运维： 从“保障稳定”向“赋能业务”延伸。重点开展资产脆弱性关联分析，将态势感知数据与漏洞扫描结果结合，输出更具针对性的风险修复建议。

开展专项演练：计划在2026年Q1组织一次小范围的网络安全监测与响应桌面推演，检验并优化应急预案和协同流程。

完善知识库： 系统化梳理本阶段遇到的事件及解决方案，初步构建该系统的“本地化知识库”，降低对核心人员的依赖。

性能容量评估： 对系统运行至第一季度的性能与容量数据进行趋势分析，评估现有资源对未来半年业务增长的支撑能力，必要时提前规划调整。

6. 结论

总体而言，本阶段运维服务达成了保障系统平稳过渡、稳定运行的核心目标。系统运行稳定，监测功能有效，初步建立了高效的运维协同机制。我方团队展现出专业的技术能力和积极的协作态度。

对于运行中暴露的误报优化、人员能力深化等预期内的问题，已通过有效协作进行了改进。下一阶段，运维工作重心将从“保稳定”逐步转向“促深化”和“提价值”，以充分发挥系统在曲靖供电局网络安全体系中的核心作用。