2025年都匀供电局网络防护能力提升与高级威胁应对服务建设技术规范

项目名称：2025年都匀供电局网络防护能力提升与高级威胁应对服务建设

编制人签字（项目负责人）：

审核人签字（部门专业技术主管或专责）：

审批人签字（部门领导）：

都匀供电局信息中心

2025年10月

2025年都匀供电局网络防护能力提升与高级威胁应对服务建设技术方案

1. 项目背景

随着都匀供电局数字化转型的深入，业务发展对信息网络的依赖性日益增强，电力系统与信息网络的融合日益紧密，面临的网络安全威胁也日趋复杂和隐蔽，网络安全已成为电网安全稳定运行的生命线。为应对日益严峻的高级持续性威胁、勒索软件、数据泄露等网络安全风险，保障核心业务系统的连续性和数据安全，提升整体网络安全防护、监测、响应和恢复能力，特启动本项目。

2. 项目目标

本项目旨在通过引入专业化的网络安全技术服务，全面提升都匀供电局的网络安全综合防护水平，确保在网络攻击发生时能够快速响应、有效遏制和快速恢复，将安全事件带来的影响降至最低。具体目标包括：

能力提升：显著提升网络安全技术团队的攻防对抗、威胁狩猎、应急响应和漏洞管理能力。

体系完善：构建常态化、智能化的威胁监测与情报驱动防御体系，实现对高级威胁的快速发现和精准响应。

风险可控：全面梳理信息资产安全状况，及时发现并闭环整改高危安全漏洞，降低被攻击利用的风险。

赋能培训：通过体系化的培训和实战演练，为都匀供电局培养一支技术过硬、反应迅速的内部网络安全核心队伍。

3. 服务范围

本项目为服务类采购，要求投标人提供为期30天的专业技术服务，服务内容包括但不限于：

高级威胁监测与分析

网络安全态势感知与通报

攻击模拟与漏洞评估

安全事件应急响应与处置

威胁情报的整合与应用

安全培训与能力转移

4. 投标人资格要求

（1）具有独立法人资格且为中华人民共和国境内注册的法人，持有合法有效的企业法人营业执照；事业单位、高校或科研机构投标的，持有事业单位法人证书。

（2）其他不得存在的情形：南方电网公司供应链管理部门暂停或取消其投标资格，且未解除的。处于南方电网公司供应商黑名单预警名单中“不接受投标”、“市场禁入”情形的。

5. 技术服务要求

5.1 高级威胁监测与狩猎

投标人应利用其威胁情报分析能力、大数据分析能力和网络安全专家经验，基于我单位提供的网络流量、终端日志、安全设备日志等数据，进行深度挖掘和关联分析。

应具备在无明确告警的情况下，主动发现潜伏性威胁、未知恶意软件和内部异常行为的能力，描述分析过程、发现结果和提供处置建议。

5.2 安全事件应急响应

提供 7x24 小时网络安全事件应急响应热线与服务窗口。在发生安全事件时，需在 30 分钟内首次响应，2 小时内提供初步分析报告和遏制方案，并根据事件级别提供远程或现场支持。事件处理后，需提供应急响应报告，包括事件根因分析、处置过程、损失评估及后续加固建议。

5.3 漏洞评估

对我单位网络现状进行漏洞评估，提供漏洞评估报告及处置建议。

5.4 威胁情报服务

提供威胁情报订阅服务，情报需与我单位行业相关。情报应整合到监测与分析流程中，用于更新检测规则和狩猎假设。定期提供威胁情报，解读最新威胁趋势、攻击团伙活动及应对策略。

在互联网收集“都匀供电局”名称、logo 等敏感信息，提供收集报告及搜集方法。

5.5 安全培训与赋能

至少为我单位安全团队及 IT 相关人员提供 1 次专项安全技术培训。培训内容应围绕网络安全事件分析、应急响应、取证分析、攻防技巧等实战技能。在重大应急响应事件后，应进行案例复盘培训，提升我方人员自主能力。

5.6 安全保密设备技术服务

对我单位安全保密设备提供相应安全技术服务，配置相关策略，对主机监控与审计、终端外设和端口管控、违规外联探测告警、终端接入控制、终端密码策略、客户端统一纳管等方面提供技术服务。

6. 项目管理与团队要求

6.1 项目团队

中标人必须组建一支不少于 3 人的项目团队，并指定一名项目经理全程负责。团队核心人员（项目经理、安全分析师、渗透测试工程师）需具备相关领域经验，并在投标文件中提供人员简历。未经招标方书面同意，不得随意更换核心成员。

6.2 服务方式

采用“远程+现场”相结合的服务模式。常态化监测、情报推送等以远程为主；应急响应、重要培训等提供现场服务。

6.3 沟通机制

建立定期沟通机制，每周至少向招标方汇报一次项目进展。建立专用沟通渠道（如工作群、专用电话），确保信息畅通。

7. 服务交付物要求

中标人需按服务周期提交以下交付物（包括但不限于）：

1. 《安全事件分析报告》（每次事件）
2. 《应急响应报告》（每次事件）
3. 《威胁情报收集报告》
4. 《漏洞评估报告》
5. 《培训总结报告》及培训材料