

**数字化项目可行性研究报告**

项目名称：国网黑龙江电力-2024年基于网格化行为管理的网络安全防护能力提升-业务运营项目

项目申报单位：国网黑龙江省电力有限公司

编制单位：国网黑龙江省电力有限公司电力科学研究院

二〇二四年八月

编 制：

校 核：

审 核：

批 准：

**目 录**

[1 总论 1](#_Toc13253)

[1.1 主要依据 1](#_Toc30266)

[1.2 必要性分析 1](#_Toc17469)

[1.3 效益分析 1](#_Toc4675)

[1.3.1 经济效益 1](#_Toc22388)

[1.3.2 管理效益 2](#_Toc13256)

[1.3.3 社会效益 2](#_Toc11781)

[2 建设现状 3](#_Toc6356)

[2.1 业务职能现状 3](#_Toc30272)

[2.2 信息系统现状 3](#_Toc17699)

[2.2.1 建设历程 3](#_Toc8437)

[2.2.2 应用功能现状 3](#_Toc31293)

[2.2.3 系统关联现状 3](#_Toc5534)

[2.2.4 部署与实施现状 3](#_Toc17788)

[2.2.5 应用成效 3](#_Toc2254)

[3 项目需求分析 4](#_Toc31557)

[3.1 业务功能需求 4](#_Toc3848)

[3.1.1 需求内容 4](#_Toc28919)

[3.1.2 项目类别 4](#_Toc6002)

[3.2 集成需求 4](#_Toc4956)

[3.3 非功能需求 4](#_Toc5374)

[3.3.1 性能与可靠性 4](#_Toc9636)

[3.3.2 信息安全 4](#_Toc4608)

[3.3.3 应用及运行监控 4](#_Toc5423)

[3.3.4 可维护性 4](#_Toc2379)

[3.3.5 易用性 5](#_Toc28849)

[3.3.6 系统灾备要求 5](#_Toc31041)

[4 建设方案 6](#_Toc17785)

[4.1 建设目标 6](#_Toc2185)

[4.2 建设内容 6](#_Toc31710)

[4.3 业务运营范围 6](#_Toc4419)

[4.4 技术方案 6](#_Toc21532)

[4.5 项目管理 6](#_Toc20199)

[4.5.1 项目管理 6](#_Toc28464)

[4.5.2 项目人员 6](#_Toc3139)

[4.5.3 项目进度 6](#_Toc27504)

[4.5.4 项目会议 7](#_Toc23082)

[4.5.5 项目培训 7](#_Toc6890)

[5 硬件设计 8](#_Toc23760)

[5.1 部署方案 8](#_Toc18907)

[5.2 服务器需求测算 8](#_Toc27890)

[5.2.1 设备现状 8](#_Toc32185)

[5.2.2 设备利旧 8](#_Toc29486)

[5.2.3 服务器需求说明 8](#_Toc6562)

[5.2.4 其他说明 8](#_Toc22335)

[5.3 基础环境需求 8](#_Toc31535)

[5.3.1 存储估算 8](#_Toc27129)

[5.3.2 网络接入需求 8](#_Toc31486)

[5.3.3 存储网络接入需求 8](#_Toc10291)

[5.3.4 负载均衡接入需求 8](#_Toc22130)

[5.3.5 安全等级及设备需求 8](#_Toc26122)

[6 主要设备材料清册 9](#_Toc29811)

[6.1 编制说明 9](#_Toc11546)

[6.2 主要设备材料表 9](#_Toc17718)

[7 估算书 10](#_Toc11679)

[7.1 概述 10](#_Toc15709)

[7.2 编制原则和依据 10](#_Toc24999)

[7.3 投资分析 10](#_Toc12008)

[附件1 业务运营工作量明细表 12](#_Toc15029)

# 1 总论

随着信息技术的迅猛发展，网络安全面临着日益复杂和严峻的威胁，尤其是在关键基础设施如电力系统领域，网络攻击的复杂性和潜在破坏力正以前所未有的速度增长。为应对这些挑战，国家发展改革委和国家数据局等部门联合发布的《关于深化智慧城市发展 推进城市全域数字化转型的指导意见》明确指出，必须加强城市数字空间的安全管理，建立健全网络安全监测预警和应急处置机制，并构建全面的城市网络运行安全管理体系。这一指导意见为城市乃至全国的数字化转型提供了关键指导，也为包括电力系统在内的各大基础设施的网络安全建设指明了前进方向。

在这一政策背景下，国网黑龙江省电力有限公司（以下简称国网黑龙江电力）积极响应国家的号召，决定启动“基于网格化行为管理的网络安全防护能力提升”项目。该项目的推出，标志着国网黑龙江电力在应对现代化网络威胁、保障电力系统安全运行方面迈出了重要一步。

该项目将通过基于机器学习的多源异构网络安全告警日志降噪技术，减少误报率并提高告警分析的准确性；利用生成式大模型进行智能日志分析，提升日志数据的处理效率和攻击响应策略的优化能力；以及通过大模型提升蜜罐的智能交互能力，模拟逼真的网络环境，增强对攻击者行为的捕捉和分析能力。这些措施将为国网黑龙江电力构建一个更加坚固和智能的网络安全防护体系，确保电力系统在复杂多变的网络环境中持续安全稳定运行。

## 1.1 主要依据

（1）《国家电网有限公司企业标准<信息系统非功能性需求规范>》（Q/GDW11212-2018）

（2）《国家电网有限公司关于印发电网数字化项目工作量度量规范及其应用指南》（国家电网互联〔2020〕606号）

（3）《国家电网有限公司电网数字化建设管理办法》（国家电网企管〔2020〕849号）

（4）《国家电网有限公司电网数字化项目可研工作管理办法》（国家电网企管〔2020〕849号）

（5）《国家电网有限公司电网数字化项目竣工验收管理办法》（国家电网企管〔2020〕849号）

（6）《国家电网有限公司关于进一步加强数字化建设统筹工作的通知》（国家电网互联〔2021〕562号）

（7）《国家电网有限公司关于印发〈国家电网有限公司数字化建设统筹管理规范（试行）〉等两项管理规范的通知》（国家电网互联〔2021〕641号）

（8）《国家电网有限公司关于印发〈国家电网有限公司电网数字化项目技术管理办法〉等6项通用制度的通知》（国家电网企管〔2021〕170号）

（9）《国家电网有限公司电网数字化项目分包管理规范（试行）》（国家电网数字〔2024〕81号）

（10）《国家电网有限公司关于推进网络安全态势感知体系建设的工作意见》（国家电网信通〔2023〕102号）

（11）《国家电网有限公司关于深化网络安全技术应用和创新发展的指导意见》（国家电网信通〔2024〕34号）

## 1.2 必要性分析

为落实国家电网公司关于省级能源大数据中心建设运营指导意见，统筹推进省级能源大数据中心建设，推动省地一体化建设运营，同时依据《国家电网有限公司关于推进网络安全态势感知体系建设的工作意见》（国家电网信通〔2023〕102号）和《国家电网有限公司关于深化网络安全技术应用和创新发展的指导意见》（国家电网信通〔2024〕34号），强化各类数据采集汇聚与要素管理，有序拓展能源领域新业务，发挥能源大数据应用价值和服务能力，增强对网络威胁的实时识别和响应能力，从而提升电力系统的整体安全性和运行稳定性。

通过利用基于机器学习的多源异构网络安全告警日志降噪技术，网络安全团队能够更有效地处理来自各种安全工具的日志数据，减少误报率，提高分析效率。同时，借助基于大模型的网络安全日志智能辅助分析，网络安全人员可以更快速地解释日志含义，追踪潜在威胁，优化安全策略。此外，基于大模型的蜜罐智能交互能力提升不仅可以增强蜜罐系统对攻击者的欺骗效果，还能够根据攻击者的动作动态生成响应，提高诱捕成功率。这些技术手段的综合应用有助于网络安全团队更全面、高效地应对复杂的网络安全威胁，提升整体网络安全防护能力，进一步促进网络安全领域的技术创新和发展。通过提高网络安全的自动化预警、分析和响应能力，不仅有助于网络安全团队更全面、高效地应对复杂的网络安全威胁，还能够提升整体网络安全防护能力，进一步推动网络安全领域的技术创新和发展。通过提高网络安全的自动化预警、分析和响应能力，组织可以更快速地检测并应对潜在威胁，降低遭受网络攻击的风险。此外，这些技术的应用还可以增强网络安全团队的工作效率，减少人工干预的需求，从而节省时间和资源。通过优化安全策略和加强网络安全措施，企业和组织可以有效保护重要数据资产，维护业务的连续性和稳定性。

## 1.3 效益分析

**1.3.1 经济效益**

通过提升网络安全告警分析能力、优化攻击响应策略和提升蜜罐智能交互能力，国网黑龙江电力能够显著降低经营成本，提高工作效率，从而增强竞争力和盈利能力。基于大模型的网络安全日志智能辅助分析，不仅有助于提高日志分析效率，快速解释其日志含义，进而辅助优化攻击响应策略，保障国网黑龙江电力的经济利益和资产安全。同时，优化网络安全设备利用率通过升级蜜罐智能交互能力，国网黑龙江电力能够根据各个网格的真实网格结构、关键服务、应用程序等信息模仿各个网络环境的虚拟网络结构和服务配置，降低遭受网络攻击可能带来的损失风险，提高对攻击者的诱捕效果，增强整体网络安全防护力。这不仅有助于降低潜在的法律责任风险和罚金，还能提升生产效率、稳定系统运行，使得网络安全人员能够更有效地应对各种网络安全威胁，全方位促进公司的长远发展和竞争优势。经济效益的提升将直接反映在国网黑龙江电力的盈利状况及可持续发展上，为未来的业务拓展和市场拓展奠定坚实基础。

**1.3.2 管理效益**

提升网络安全告警分析能力，系统能够准确识别安全威胁，减少误报率，从而帮助国网黑龙江电力更高效地应对潜在的网络安全风险，保障网络系统的正常运行。同时，利用基于生成式大模型的智能网络安全增强技术手段，支撑国网黑龙江电力网安人员完成告警分析、网络安全日志智能辅助分析和蜜罐智能交互等工作的开展，有效提升基于网格化行为管理的网络安全防护能力。这一提升有助于安全人员快速追踪安全事件源头，有效阻止攻击行为并减少损失，提高了国网黑龙江电力的安全应急响应能力。另外，通过改进电力系统蜜罐智能交互能力，系统更具交互性和智能性，能够更好地吸引并诱导攻击者，加强电力系统的安全保护。从中获得的管理效益不仅体现在加强了网络安全防护能力，还提升了攻击事件处理的效率，进一步确保了国网黑龙江电力信息安全的稳定性。

**1.3.3 社会效益**

网络安全告警分析能力以及攻击响应策略等独特方法的优化，不仅显著提高了国网黑龙江电力的网络安全水平，还有助于维护互联网的生态稳定和安全，从而增强社会的信息保障机制。同时，采用广泛应用的大型模型技术，推动网络安全技术的不断创新与发展，促进行业技术水准的提高，并突显其对推动行业进步的重要性。此外，持续加强电力系统安全性，能够提升市民对网络安全的信心，增强社会对网络安全的信任，有助于构建更加安全稳定的社会环境，为社会的可持续繁荣做出积极贡献。这种技术方面的创新与应用不仅使公司受益匪浅，而且为整个社会带来了安全稳定的网络环境，展示了科技在推动社会进步与发展方面的关键作用。

# 2 建设现状

## 2.1 业务职能现状

当前，自动化预警系统主要依赖传统的入侵检测系统（IDS）、防火墙和漏洞扫描工具，由于数据来源的多样性和异构性，现有系统在处理大量日志数据时面临挑战，误报率较高，预警系统的准确性和响应速度有待提升。在网络安全日志分析方面，现有的日志管理工具和分析方法依赖传统的手动处理方式，缺乏高效的关联分析能力，这使得日志分析过程费时费力，难以应对复杂的安全事件蜜罐仿真技术虽然能够提供一定的攻击情报，但其交互性和真实感较为有限，不能够有效模拟真实网络环境中的各种复杂场景，影响了对攻击者行为的捕捉和分析整体网络安全体系在应对新型复杂威胁时，缺乏足够的适应性和灵活性，需要进一步优化和提升防护能力。

## 2.2 信息系统现状

本项目首次开展，不涉及以往信息系统现状。

### 2.2.1 建设历程

本项目首次开展，不涉及以往建设历程。

### 2.2.2 应用功能现状

本项目首次开展，不涉及以往应用功能现状。

### 2.2.3 系统关联现状

本项目首次开展，不涉及以往系统关联现状。

### 2.2.4 部署与实施现状

当前，网络安全技术部署依赖于传统工具和系统，这些工具在处理复杂威胁和大规模数据时效率有限。自动化预警系统已在使用中，但数据集成和处理能力不足，导致预警响应时间较长。在网络安全日志分析方面，现有的日志管理工具和分析方法依赖传统的手动处理方式，缺乏高效的关联分析能力，这使得日志分析过程费时费力，难以应对复杂的安全事件蜜罐仿真技术的部署较为基础，缺乏足够的智能性、交互性及动态响应，未能有效模拟真实攻击场景。整体上，现有部署和实施情况需要进一步优化，以提升系统的综合性能和应对能力。

### 2.2.5 应用成效

目前，通过部署传统的网络安全工具和系统，已经在提升基础威胁检测和预警能力方面取得了一定的成效。然而，自动化预警系统在处理多源异构数据时仍存在误报率较高的问题。网络安全日志分析工具已部分部署，但现有工具主要依靠人工分析，处理效率低下，难以快速解析大量日志数据。蜜罐仿真技术的应用提高了对攻击者行为的模拟，但缺乏智能化的交互功能和动态响应能力，无法有效模拟复杂的攻击场景，未能充分发挥其在捕捉攻击行为和提供安全情报方面的潜力。综合来看，虽然取得了一些进展，但各项技术的应用效果仍有进一步优化的空间，以更好地应对日益复杂的网络安全威胁。

## 2.3 业务职能功能对应关系

自动化预警系统通过实时监控网络流量和安全日志，识别并分析潜在的安全威胁，尽管在数据处理能力和准确性上仍有提升空间。网络安全日志分析功能负责从各类安全工具中收集日志数据，并进行关联分析，以确定安全事件的性质和严重程度，但目前主要依赖于传统的手动分析，效率较低。蜜罐仿真技术通过模拟真实网络环境，诱捕并记录攻击者行为，提供重要的安全情报，尽管其当前的智能性、交互性和真实性尚未充分达到理想水平。整体网络安全体系建设则通过多层次防护措施，提升系统的综合安全性和应对复杂威胁的能力。

# 3 项目需求分析

## 3.1 业务功能需求

### 3.1.1 需求内容

本项目业务需求主要包括以下三个部分：

**1）**基于机器学习的多源异构网络安全告警日志降噪

在现有网络环境中，主要存在网格区域安全设备种类多，告警日志格式不统一的问题。安全设备包括入侵检测系统、防火墙等，在日常运行过程中，各类安全设备会产生大量的告警日志。告警日志呈现出多源异构的特点，难以统一进行管理和分析。因此，引入基于深度网络等机器学习技术的关联分析方法，支撑对网格区域间不同安全设备所生成的多源异构日志和告警进行解析和关联，减少告警信息中存在的重复和误报，提升网络安全告警分析能力，从而减轻安全运维人员的工作负担，提升告警响应处置的效率。

**2）****基于大模型的网络安全日志智能辅助分析**

在网络安全防护业务运营中，网络安全日志分析面临对日志精确分析的难点。网络安全日志，作为记录网络活动的详尽资料，包含了攻击发生时的关键线索。但在日常运行中，电力系统各安全设备（包括华三防火墙、绿盟IDS设备、南瑞SIEM等）会产生大量日志数据，网络安全人员难以快速分析并进行攻击响应。为有效提升网络安全日志分析能力，优化攻击响应策略，考虑改进网络安全运营方法，即利用基于生成式大模型（千问14B或千问7B）强大的日志数据分析能力，辅助支撑公司网络安全运维人员进行日志数据的分析和追踪，提高工作效率；利用基于生成式大模型千问的辅助工具，精准查询日志管理数据库中各个网格区域内安全工具及系统产生的日志，并快速解释其日志含义，进而辅助攻击响应策略，减轻网络安全服务人员工作负担。

**3）电力系统蜜罐仿真技术性能提升**

蜜罐是一种重要的防御手段，用于在网络安全防护运营过程中模拟关键的资产，吸引并记录攻击者的活动，以便网络安全服务人员分析攻击方法并防范潜在的威胁。在日常运行过程中，常因为蜜罐交互性与正常系统存在差异进而导致被攻击者识破。考虑通过生成式大模型千问，提高蜜罐智能交互能力，从而提升电力系统的网络安全防护能力。利用生成式大模型千问的智能性和交互性，完成电力系统蜜罐仿真交互，使用生成式大模型Agent，根据各个网格的网络结构、关键服务、应用程序等信息，在运行过程中，基于攻击者的动作动态生成交互响应，从而提高蜜罐交互性能，使其能够更逼真地模仿各个网格环境的虚拟网络结构和服务配置，增加蜜罐的吸引力。

### 3.1.2 项目类别

按照《国家电网有限公司电网数字化项目工作量度量规范》及《国家电网有限公司电网数字化项目工作量度量规范应用指南（2020版）》要求，本项目属于“业务运营类”，应按照业务运营类开展相关工作。

|  |  |  |
| --- | --- | --- |
| **序号** | **分类** | **分类描述** |
| 1 | 咨询设计类 | 电网数字化领域的顶层设计、总体设计、专项研究等咨询和设计相关工作，不包括系统开发设计相关工作。 |
| 2 | 系统开发类 | 信息系统功能设计及利用各类编程语言进行开发实现的工作，主要包括需求分析、系统设计和开发等内容 |
| 3 | 集成实施类 | 开发工作完成或购买套装软件的配套安装、配置、调试、培训等工作，一般是以软件功能能够正常使用为主的实施工作。 |
| 4 | 业务运营类 | 以系统运行、业务应用、用户行为等常态统计分析为基础，开展系统优化改造、应用敏捷迭代、内容更新升级、用户产品推广、商务模式拓展、网络安全服务、可研论证、后评估、绩效评估等工作。 |
| 5 | 数据工程类 | 对数据源进行接入整合、加工处理和开发利用，通过数据分析挖掘实现数据价值的相关工作。 |

## 3.2 集成需求

不涉及。

## 3.3 非功能需求

### 3.3.1 性能与可靠性

不涉及。

### 3.3.2 信息安全

本项目信息系统，其安全防护依据《国家电网有限公司网络与信息系统安全管理办法》（国网（信息/2）401-2020）要求，坚持“同步规划、同步建设、同步使用”的理念，遵循“管业务必须管安全”的原则，严格落实网络安全管理责任，建立网络安全保障体系和监督体系。

### 3.3.3 应用及运行监控

不涉及。

### 3.3.4 可维护性

不涉及。

### 3.3.5 易用性

不涉及。

### 3.3.6 系统灾备要求

不涉及。

# 4 建设方案

## 4.1 建设目标

1. 通过基于深度网络等机器学习技术，实现网格区域内网络设备多源异构日志记录的关联分析，提升网络安全告警分析能力。
2. 通过开展基于生成式大模型的网络安全日志智能辅助分析，支撑公司网络安全人员进行日志数据的分析和追踪，提高网安人员分析日志的效率。
3. 通过基于生成式大模型的深度学习技术，增强普通蜜罐系统的交互性和智能程度，使其能够模仿各个网格环境的虚拟网络结构和服务配置，以延长攻击者的停留时间并获取更多有价值的攻击数据。

## 4.2 建设内容

本项目不对现有系统功能模块进行调整，不新增任何系统功能模块。

通过基于机器学习的多源异构网络安全告警日志降噪、基于大模型的网络安全日志智能辅助分析和基于大模型的蜜罐智能交互能力提升等手段，有效提升基于网格化行为管理的网络安全防护能力，具体包括：

1. 基于机器学习的多源异构网络安全告警日志降噪。针对网格区域内的安全工具（如入侵检测系统、防火墙）产生的多源异构日志和数据，通过基于大模型等神经网络技术的关联分析，识别并判断出网格之间的安全威胁，减少误报率，提升网络安全自动化预警能力。

2. 基于大模型的网络安全日志智能辅助分析。利用基于生成式大模型千问强大的日志数据分析能力，支撑公司网络安全人员进行日志数据的分析和追踪，提高日志分析效率。利用基于生成式大模型千问的辅助查询工具查询日志管理数据库中各个网格区域中安全工具及系统（包括华三防火墙、绿盟IDS设备、南瑞SIEM等）产生的日志数据，并快速解释其日志含义，进而辅助优化攻击响应策略。

3. 基于大模型的蜜罐智能交互能力提升。利用生成式大模型千问的智能性和交互性，完成高交互性的电力系统蜜罐仿真交互，根据各个网格的真实网络结构、关键服务、应用程序等信息构建生成式大模型agent，使其能够模仿各个网格环境的虚拟网络结构和服务配置，同时基于生成式大模型可以根据攻击者的动作动态生成响应，提高诱捕过程的交互性。

| **序号** | **工作任务** | **工作内容** | **成果物** |
| --- | --- | --- | --- |
| **1** | 基于机器学习的多源异构网络安全告警日志降噪 |  |  |
| 1.1 | 多源异构数据的采集 | 从网格区域间安全设备（如入侵检测系统、防火墙等）中提取告警数据。 | 数据处理与验证报告 |
| 1.2 | 智能关联分析与告警优先级分类 | 对不同来源的日志和告警数据进行解析和分析，识别潜在的安全威胁。同时，根据威胁的严重程度自动分配优先级，确保高危告警能够优先得到响应。 | 威胁分析报告 |
| 1.3 | 重复告警的自动去重过滤 | 自动识别并对重复的告警信息进行分组。通过智能分析技术，识别不同来源但本质相同的安全事件，将其合并过滤，减少告警数量。 | 告警去重报告 |
| **2** | **基于大模型的网络安全日志智能辅助分析** |  |  |
| 2.1 | 日志数据收集与整合 | 确保所需网络设备（如服务器、防火墙、路由器等）的日志的获取，明确其字段信息。 | 用于生成式大模型分析的日志数据获取文档和字段文档 |
| 2.2 | 基于生成式大模型算法应用进行辅助日志查询 | 通过生成式大模型算法及应用辅助查询设备日志，形成生成式大模型辅助日志分析流程和手册，协助运维人员有效使用模型对日志进行快速查询。 | 基于生成式大模型的日志查询流程文档和帮助手册 |
| 2.3 | 基于生成式大模型算法应用进行辅助日志分析 | 通过生成式大模型算法及应用，对安全设备日志进行分析，形成生成式大模型辅助日志分析流程和手册，协助运维人员有效使用模型开展日志分析。 | 基于生成式大模型的日志分析流程文档和帮助手册 |
| 2.4 | 基于生成式大模型辅助攻击响应 | 通过生成式大模型算法及应用辅助攻击响应，，完成生成式大模型辅助攻击溯源方法，协助运维人员快速对网络安全攻击进行定位、处置及溯源。 | 生成式大模型辅助攻击响应方法文档 |
| 2.5 | 攻击响应策略优化 | 通过生成式大模型算法及应用辅助优化攻击响应策略，形成生成式大模型攻击响应策略优化经验文档，协助运维人员优化防护策略。 | 生成式大模型攻击响应策略优化经验文档 |
| **3** | **基于大模型的蜜罐智能交互能力提升** |  |  |
| 3.1 | 现有蜜罐交互协议需求收集 | 收集现有蜜罐的系统所需的交互协议信息，为生成式大模型算法及应用提供基础协议数据。 | 形成所需协议信息描述文档 |
| 3.2 | 蜜罐系统所需信息收集 | 分析现有应用系统、网络结构、关键服务和应用程序，梳理特征文件，完善蜜罐中特征文件交互部分，为大数据模型提供改造依据。 | 形成网络结构、关键服务和应用程序特征文档，描述需实施蜜罐的交互部分 |
| 3.3 | 基于生成式大模型进行蜜罐能力改造 | 通过生成式大模型，对旧版蜜罐交互后端进行升级改造，进而使大模型能够接管交互行为，提升蜜罐吸引和诱捕能力。 | 蜜罐改造方法和工具 |
| 3.4 | 基于生成式大模型的高交互性蜜罐试验 | 对改造后的高交互性蜜罐进行实施试验，为试验成效评估提供试验数据支撑。 | 高交互蜜罐试验文档 |
| 3.5 | 蜜罐数据分析 | 对实施后的蜜罐运行数据进行分析，评估蜜罐效果。 | 高交互蜜罐测试分析文档 |

## 4.3 业务运营范围

在国网黑龙江省电力有限公司完成本项目的业务运营工作。

## 4.4 技术方案

在处理多源告警数据的过程中，首先将来自不同来源的告警数据进行汇集，确保所有数据能够集中处理。针对这些告警数据，要进行告警文本的预处理。预处理过程中，利用专业的告警词汇库、数据字典以及人工标注信息，对告警全文本进行清理，剔除无用的文本信息，并提取出关键的词汇，以便于后续分析。在告警文本聚类阶段，采用多种不同的聚类技术进行分析。如MinJoin聚类算法，通过最小化局部哈希值来计算文本编辑距离，从而进行聚类分析。基于向量相似度的聚类方法，对告警文本进行分词处理，然后利用特征工程将其向量化表示，最后基于向量之间的相似度（例如余弦相似度）来进行聚类，同时通过机器学习、NLP算法，可自动学习告警之间的关联或相似关系进行合并，达到智能降噪的效果。

利用生成式大模型千问及相关应用工具，通过其强大的日志数据分析能力，协助公司网络安全运维人员，对安全设备（包括华三防火墙、绿盟IDS设备、南瑞SIEM等）的日志数据进行搜索、分析和追踪，提高日志分析过程的工作效率。利用基于生成式大模型工具的辅助查询工具，对日志管理数据库中各个网格区域间安全工具及系统产生的日志数据进行查询，并由应用工具辅助快速解释其日志含义，进而优化攻击响应策略。

利用生成式大模型千问，对电力系统蜜罐智能交互能力提高，将各个网格的真实网络结构、关键服务、应用程序等特征信息，输入生成式大模型Agent工具，令Agent工具进行蜜罐交互模拟，使其能够模仿各个网格环境的虚拟网络结构和服务配置，并根据攻击者的动作行为动态生成响应，提高诱捕过程的交互性。

## 4.5 项目管理

### 4.5.1 项目管理

在公司数字化领导小组领导下，由省公司成立项目指导小组。项目管理采取分层管理方式，主要分为高级管理层和项目管理层两个层次，项目管理层结合具体工程项目情况又可分为多个职责明确的工作组，对项目组织结构及相关各工作组的岗位设置、岗位职责及人员安排做了细致的安排，以便做到责权明确，科学管理，确保项目顺利完成。

### 4.5.2 分包管理

本项目不具备专业分包条件。

### 4.5.3 项目人员

| **序号** | **岗位** | **职责** | **人员数量** |
| --- | --- | --- | --- |
| 1 | 项目管理 | 负责项目实施进度管控、工作协调、人员调配、项目文档编写、横纵向沟通等工作。 | 6 |
| 2 | 业务运营 | 收集业务需求、数据需求，通过需求整理和分析，编制需求方案。提供门户应用产品及数据共享服务的宣传推广，提高平台行业关注度和热度。 | 13 |
| **合计** | | | **19** |

### 4.5.4 项目进度

国网黑龙江电力-基于网格化行为管理的网络安全防护能力提升-业务运营项目，投入19个人，总工期为2.5个月。具体项目进度及提交成果如下：

* 业务运营部分：

| **序号** | **阶段** | **工期** | **提交成果** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 项目启动 | 0.25个月 | 详细工作计划 |  |
| 2 | 业务运营 | 2个月 | 数据处理与验证报告；威胁分析报告；告警去重报告；用于生成式大模型分析的日志数据获取文档和字段文档；基于生成式大模型的日志分析流程文档和帮助手册；基于生成式大模型的日志查询流程文档和帮助手册；生成式大模型辅助攻击响应方法文档生成式大模型攻击响应策略优化经验文档；形成所需协议信息描述文档；形成网络结构、关键服务和应用程序特征文档，描述需实施蜜罐的部分；蜜罐改造方法和工具；高交互蜜罐试验文档；高交互蜜罐测试分析文档。 |  |
| 3 | 项目验收 | 0.25个月 | 项目验收文档 |  |

### 4.5.5 项目会议

* 业务运营部分：

| **序号** | **项目** | **内容** | **项目要求** |
| --- | --- | --- | --- |
| 1 | 项目启动会 | 项目启动 | 人×天：1人×1天 |
| 2 | 项目成果评审会 | 成果评审 | 人×天：1人×1天 |
| 3 | 项目竣工验收 | 项目竣工验收 | 人×天：1人×1天 |

### 4.5.6 项目培训

不涉及。

# 5 硬件设计

## 5.1 部署方案

不涉及。

## 5.2 服务器需求测算

### 5.2.1 设备现状

不涉及。

### 5.2.2 设备利旧

不涉及。

### 5.2.3 服务器需求说明

不涉及。

### 5.2.4 其他说明

不涉及。

## 5.3 基础环境需求

### 5.3.1 存储估算

不涉及。

### 5.3.2 网络接入需求

不涉及。

### 5.3.3 存储网络接入需求

不涉及。

### 5.3.4 负载均衡接入需求

不涉及。

### 5.3.5 安全等级及设备需求

不涉及。

# 6 主要设备材料清册

## 6.1 编制说明

不涉及。

## 6.2 主要设备材料表

不涉及。

# 7 估算书

## 7.1 概述

针对上述内容，按照有关要求，对项目建设过程中的相关费用进行估算。国网黑龙江电力-基于网格化行为管理的网络安全防护能力提升-业务运营项目,预投入19名相关人员,项目费用预估151.35万元，无其它费用，合计151.35万元。

## 7.2 编制原则和依据

（1）项目划分和项目工作量度量方法、过程及原则参照《国家电网有限公司电网数字化项目工作量度量规范》（以下简称《规范》）及《国家电网有限公司电网数字化项目工作量度量规范应用指南（2020版）》（以下简称《应用指南》）测算。

（2）按照《规范》、《应用指南》规定，咨询设计类人工费率为2500元/人天，开发类人工费率为2100元/人天，集成实施类、业务运营类人工费率为1500元/人天，数据工程类 人工费率分为三档，其中，数据接入、上传、下发及数据产品（应用）实施参照集成实施人工费率标准执行（1500元/人天），数据产品（应用）研发工作参考系统开发人工费率标准执行（2100元/人天），数据标准化、资源目录、治理等其它工作参考软件行业协会基准费率执行（1800元/人天）。

（3）本报告中人工费率即为综合人工单价，包括直接人力成本、直接非人力成本、间接人力成本、间接非人力成本及合理利润，但不包括购置类费用。

（4）本期不计取价差预备费及建设期贷款利息。

（5）工作量依据可研设计提资。

## 7.3 投资分析

项目预估总投资为**151.35**万元，各项费用如下表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | | **工作量**  **（人天）** | **人工费率**  **（万元/人天）** | **金额**  **（万元）** |
| 一 | 咨询设计费 | | - |  |  |
| 二 | 系统开发费 | 系统功能开发 | - |  |  |
| 系统集成开发 | - |  |  |
| 三 | 集成实施费 | 系统实施 |  |  |  |
| 系统集成实施费 |  |  |  |
| 四 | 业务运营费 | | 1009 | 0.15 | 151.35 |
| 五 | 数据工程费 | 数据产品（应用）研发 |  |  |  |
| 数据标准化、盘点、目录构建、数据治理等 |  |  |  |
| 数据接入、上传、下发、数据产品（应用）实施 |  |  |  |
| 六 | 其它费用 | | - | - |  |
| **总 计** | | | | | 151.35 |

**（1）咨询设计费**

不涉及。

**（2）系统开发费**

不涉及。

**（3）集成实施费**

不涉及。

**（4）业务运营费**

本次业务运营工作包括基于机器学习的多源异构网络安全告警日志降噪、基于大模型的网络安全日志智能辅助分析、基于大模型的蜜罐智能交互能力提升等3个子项工作，预估需要1009人天,费用合计151.35万元。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **业务运营工作项名称** | **工作量（人天）** | **费用（万元）** |
| 1 | 基于机器学习的多源异构网络安全告警日志降噪 | 300 | 45 |
| 2 | 基于大模型的网络安全日志智能辅助分析 | 405 | 60.75 |
| 3 | 基于大模型的蜜罐智能交互能力提升 | 304 | 45.6 |
| **合计** | | 1009 | 151.35 |

**（5）数据工程费**

不涉及。

**（6）其它费用**

不涉及。

附件1 业务运营工作量明细表

**国网黑龙江电力-2024年基于网格化行为管理的网络安全防护能力提升-业务运营项目**

**业务运营工作量明细表**

单位：人天

| **序号** | **工作任务** | **工作内容** | **合计工作量（人天）** |
| --- | --- | --- | --- |
| **1** | **基于机器学习的多源异构网络安全告警日志降噪** |  | **300** | |
| 1.1 | 多源异构数据的采集 | 从网格区域间安全设备（如入侵检测系统、防火墙等）中提取告警数据。该工作计划投入10人，工作时长9天。 | 90 | |
| 1.2 | 智能关联分析与告警优先级分类 | 对不同来源的日志和告警数据进行解析和分析，识别潜在的安全威胁。同时，根据威胁的严重程度自动分配优先级，确保高危告警能够优先得到响应。该工作计划投入10人，工作时长11天。 | 110 | |
| 1.3 | 重复告警的自动去重过滤 | 自动识别并对重复的告警信息进行分组。通过智能分析技术，识别不同来源但本质相同的安全事件，将其合并过滤，减少告警数量。 工该工作计划投入10人，工作时长10天。 | 100 | |
| **2** | **基于大模型的网络安全日志智能辅助分析** |  | **405** | |
| 2.1 | 日志数据收集与整合 | 确保所需网络设备（如服务器、防火墙、路由器等）的日志的获取，明确其字段信息。该工作计划投入8人，工作时长10天。 | 80 | |
| 2.2 | 基于生成式大模型算法应用进行辅助日志查询 | 通过生成式大模型算法及应用辅助查询设备日志，形成生成式大模型辅助日志分析流程和手册，协助运维人员有效使用模型对日志进行快速查询。该工作计划投入9人，工作时长10天。 | 90 | |
| 2.3 | 基于生成式大模型算法应用进行辅助日志分析 | 通过生成式大模型算法及应用，对安全设备日志进行分析，形成生成式大模型辅助日志分析流程和手册，协助运维人员有效使用模型开展日志分析。该工作计划投入10人，工作时长10天。 | 100 | |
| 2.4 | 基于生成式大模型辅助攻击响应 | 通过生成式大模型算法及应用辅助攻击响应，，完成生成式大模型辅助攻击溯源方法，协助运维人员快速对网络安全攻击进行定位、处置及溯源。该工作计划投入10人，工作时长9天。 | 90 | |
| 2.5 | 攻击响应策略优化 | 通过生成式大模型算法及应用辅助优化攻击响应策略，形成生成式大模型攻击响应策略优化经验文档，协助运维人员优化防护策略。该工作计划投入9人，工作时长5天。 | 45 | |
| **3** | **基于大模型的蜜罐智能交互能力提升** |  | **304** | |
| 3.1 | 现有蜜罐交互协议需求收集 | 收集现有蜜罐的系统所需的交互协议信息，为生成式大模型算法及应用提供基础协议数据。该工作计划投入11人，工作时长4天。 | 44 | |
| 3.2 | 蜜罐系统所需信息收集 | 分析现有应用系统、网络结构、关键服务和应用程序，梳理特征文件，完善蜜罐中特征文件交互部分，为大数据模型提供改造依据。该工作计划投入10人，工作时长5天。 | 50 | |
| 3.3 | 基于生成式大模型进行蜜罐能力改造 | 通过生成式大模型，对旧版蜜罐交互后端进行升级改造，进而使大模型能够接管交互行为，提升蜜罐吸引和诱捕能力。该工作计划投入11人，工作时长7天。 | 77 | |
| 3.4 | 基于生成式大模型的高交互性蜜罐试验 | 对改造后的高交互性蜜罐进行实施试验，为试验成效评估提供试验数据支撑。该工作计划投入7人，工作时长10天。 | 70 | |
| 3.5 | 蜜罐数据分析 | 对实施后的蜜罐运行数据进行分析，评估蜜罐效果。该工作计划投入10人，工作时长6天。 | 60 | |