# 题目背景：

当前网络安全运营中面临日常告警日志噪声多、依赖人工分析及专家经验等低效率研判分析难题，随着大模型在各行业领域赋能应用场景愈发显著，期望选手设计网络安全告警日志智能研判流程方法，利用大模型上下文推理能力，综合大小模型实现对网络安全告警日志智能化研判，降低人工分析压力，增强威胁识别准确性，提升安全运营响应效率。

# 题目描述：

需要选手通过在本地部署一定规格的大模型，探索研究大模型在网络安全告警信息上下文推理能力以及结合小模型辅助分析能力，设计对网络安全告警日志智能研判程序，满足对网络安全多种攻击场景告警日志有效研判。

# 考察选手大模型推理应用、告警日志分析能力，挑战内容如下：

1. 通过蒸馏技术将基座大模型的知识迁移至轻量级模型中，生成适用于不同场景的网络安全研判专家模型
2. 基于专家模型构建安全智能体，通过‌模型微调、提示工程、检索增强（RAG）‌等技术优化推理效率，并采用混合专家模型等方式实现多智能体协同研判。
3. 在蒸馏过程中如何平衡模型参数量、精度与性能。
4. 协同研判过程中，如何合理分类资源，提升研判效率。

# 交付件：

1. 大模型选用部署应用说明文档：选用规格、硬件要求、部署实现等描述。
2. 智能研判流程整体说明文档。
3. 智能研判程序源码：大模型推理、小模型辅助等。
4. 测试样例及测试流程说明文档。

# 评价方式：

1、推理资源成本与研判准确度平衡：兼顾本地部署大模型规格下（如7b、13b等）推理资源低成本的同时，网络安全告警日志智能研判有较高的准确度。

2、智能研判流程协同能力及适用性：整体流程能够满足多种攻击场景（web攻击、漏洞攻击、非法外联等）下告警日志研判。

# 咨询邮箱：

zhangnan@topsec.com.cn