Contribution ID: **131** Type: **Oral Presentation**

(Cancel) Integrating False Positive Reduction and LLM-Based Multi-Agent System into IHEP's SOC to Enhance Network Security Operation Intelligence

Network security operations at the Institute of High Energy Physics (IHEP) face severe challenges, including massive data volumes, high alarm complexity, and low manual processing efficiency. While the current Security Operations Center (SOC) system at IHEP has improved cybersecurity operational efficiency to a certain extent through big data platforms and automated workflows, its intelligence level remains insufficient and requires further enhancement. This work proposes integrating False Positive Reduction (FPR) and Large Language Model (LLM)-based multi-agent technology to upgrade IHEP's existing SOC, endowing it with autonomous decision-making, collaborative reasoning, closed-loop task execution, and accurate false positive filtering capabilities. For FPR, a transfer learning-based false alert filtering method is developed to achieve intelligent discrimination of alert logs using limited labeled samples and a large number of unlabeled samples. For the LLM-based multi-agent system, a collaborative mechanism is designed, integrating key technologies such as Retrieval-Augmented Generation (RAG), Text-to-SQL, Text-to-Command, and Chain-of-Thought (CoT) reasoning. This research provides a scalable and accurate technical pathway for the integration and application of LLMs, multi-agent systems, and transfer learning in the field of network security operations.

Primary authors: WANG, Jiarong (Institute of High Energy Physics); Mr LONG, Futao (IHEP); Mr ZHOU, Jingkai (IHEP); YAN, Tian (IHEP); QI, Fazhi (Institute of High Energy Physics,CAS)

Presenter: WANG, Jiarong (Institute of High Energy Physics)

Session Classification: Networking, Security & Operations - II

Track Classification: Track 7: Network, Security, Infrastructure & Operations