Contribution ID: **10** Type: **Oral Presentation**

(REMOTE) ChatSOC: A Large Language Model Powered Autonomous Agent for Security Operations Center

Wednesday, 19 March 2025 14:40 (20 minutes)

Network security operations depends on many kings of network security tools to deal with the monitoring, detecting, and responding for security incidents, threats, and vulnerabilities across the organization's infrastructure. However, despite the evolving power of these tools, they are relatively cumbersome to use and often require interaction through specific interfaces, which increases the difficulty and professional requirements for the security operation personnel to understand and combine their inputs and outputs. Therefore, the integration of a complex set of network security tools to enhance interoperability is a critical concern for network security operations. Recent advancements in large language models (LLMs) have showcased their exceptional capabilities in natural language processing and comprehension, offering a novel approach to interfacing with network security tools. This paper introduces ChatSOC, an autonomous agent for network security operations empowered by a large language model, which is effectively capable of managing five types of operations: identify, policy, protection, detection, response. ChatSOC streamlines different operations by effectively task planning, and task execution when instructed by the security operation personnel. Our work is an innovative approach to achieve the easy to use and understanding for the network security tools. Through comprehensive experimental evaluations, ChatSOC has demonstrated the high accuracy in network security operations task planning and execution in five types of operational scenarios.

Primary authors: WANG, Jiarong (Institute of High Energy Physics); Dr ZHOU, Caiqiu; Mr YI, Yang; Mr SUN, Qianran; Dr YAN, Tian; Prof. QI, Fazhi

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

Session Classification: Network, Security, Infrastructure & Operations I

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