

ChatSOC：面向高能所网络安全运营的智能体系统

Monday, 25 August 2025 18:00 (20 minutes)

为抵御大量网络攻击，中国科学院高能物理研究所（IHEP）于 2021 年建成安全运营中心（IHEP SOC）。IHEP SOC 制定了标准化流程，调用多种安全工具执行自动化响应任务。该标准化流程预置固定工具，保障 IHEP SOC 响应时间达分钟级，且误拦率极低，万分之一左右。但工具调用的固定流程更新和管理难度大，通常应对孤立的安全运营任务。针对此问题，本文引入 ChatSOC，这是由大语言模型（LLM）赋能、面向网络安全运营的自主智能体，可完成识别、防护、检测、响应等各类运营任务。在高能物理研究所部署后，ChatSOC 可自动规划并调用不同工具，有效提升安全运营效率。

Summary

Primary author: 王, 佳荣

Presenter: 王, 佳荣

Session Classification: 人工智能与应用

Track Classification: 人工智能与应用