GenAI-Powered Security Operations Center (GSOC)

M. Alsahly, H. Farooq, N. Alali, A. Alkhoraidly, Saudi Aramco

Objectives/Scope: The aim of this proposal is to explore and explain the integration of GenAI models into Energy related Security Operations Center (SOC) workflows, detection of cyber security threats, threat intelligence synthesis, automated threat investigation, alert triage and adversary simulation.

Methods, Procedures, Process: In this proposal, we proposed and evaluated the use of Meta's Llama Guard models in order to enhance the analysis of large-scale enterprise security data to demonstrate a Gen-AI powered SOC (a.k.a GSOC). We first built a lab environment to build a POC framework, where raw security logs were forward to a centralized ingestion platform (with Llama Guard deployed). Later, we leveraged Llama Guard's reasoning capabilities to generate GenAI-based alerts, which were reviewed by the SOC Analysts during the routine incident response.

Results, Observations, Conclusions: Our results highlighted achieving nearly 90% threat detection accuracy while using advanced generative models (Meta Llama Guard 3 and 4) for cybersecurity threat detection, therefore reinforcing the importance of ongoing tuning and contextualization.In summary, the integration of Generative AI into Security Operations Centers (GSOC) offered a glimpse to the incoming technological shift about how organizations shall defend themselves against increasingly complex and high-volume cyber threats. Based on our evaluations, Llama Guard Morels are definitely an effective tool and massively enhances SOC operations by accelerating anomaly and threat detection through contextual analysis. The synergy between human analysts and intelligent systems will be essential in building the next generation of defense operations—ones that can not only keep pace with cyber adversaries but stay ahead of them.

Novel/Additive Information: GenAI models are generally used for Chat Competitions, Assistive Agents and for building Agentic platforms. Utilization of GenAI models to augment threat detection in energy sector and assist SOC Analysts is something very new and an massively emerging trend in the global Cyber Security industry.