Tuesday, June 25, 2024

3:20 PM - 3:40 PM

Decoding the Hype: Practical Applications of Large Language Models in Cybersecurity

Yihua Liao, Ph.D.

Senior Director, AI Labs

Netskope

Abstract:

The current fascination with Large Language Models (LLMs) has ignited both enthusiasm and skepticism in the tech community. While the hype is undeniable, how can cybersecurity professionals actually benefit from these models?

Our team embarked on a journey to answer this question. Utilizing an open-source model named Llama2, we fine-tuned it with a specialized knowledge base to explore a variety of applications within the cybersecurity landscape. The use cases ranged from employing chatbots for automating support queries, to utilizing analytics for a deeper understanding of security stances, to summarizing hefty threat reports into easily consumable information.

So, what worked and what fell short? This session aims to unpack these questions, providing attendees with concrete metrics and methodologies for evaluating the efficacy of LLMs in cybersecurity tasks. We will share the criteria for determining the success or failure of each use case, along with lessons learned from our trials and tribulations. Specifically, the session will cover and demo:

- Chatbots for Product Support: Streamlining issue resolution by automating common queries.

- Interactive Analytics: Leveraging LLMs to gain granular insights into your security posture. - Threat Report Summaries: Condensing complex reports into actionable intelligence.

- Contextualizing Threats and Vulnerabilities: Using LLMs to provide deeper insights into the threat landscape.

- Dynamic Policy Recommendations: Adapting to evolving threats through real-time, data-driven guidelines.

- Documentation Quality Assurance: Employing LLMs to enhance the accuracy and readability of internal documents.

By the end of the session, attendees will have a well-rounded perspective on the opportunities and challenges tied to the implementation of LLMs in cybersecurity. Moreover, the discussion will be geared towards offering actionable takeaways that you can apply in your cybersecurity endeavors. Through this session, we aim to cut through the noise surrounding LLMs and provide a comprehensive guide for cybersecurity professionals looking to harness the power of generative AI. We welcome you to join us in demystifying the buzz and diving deep into the practicalities of LLMs for cybersecurity.