Wednesday, January 29, 2025

4:00 PM – 4:20 PM

Risks to AI Adoption for US Sea Services

Parth Vakil

Vice President, Global Field Engineering

HiddenLayer

Abstract:

Artificial Intelligence (AI) is becoming its own "arms" race and for good reason. With the advent of Large Language Models, the applicable use cases for AI technology have exploded and global actors are participating in innovating AI capabilities as well as AI exploitation.

"The United States has been at the forefront of AI innovation... However, China has emerged as a formidable competitor over the past decade. And the narrative that China is merely a "copycat" is false and outdated. China's strong academic institutions and innovative research, particularly from Tsinghua University, has [sic] produced the majority of China's top AI start-ups... China now produces more AI research than the United States, and it is rapidly closing the performance gap with U.S. LLMs..." https://itif.org/publications/2024/08/26/how-innovative-is-china-in-ai/

With the adoption of AI significantly increasing, safeguarding the integrity of our AI assets is mandatory. Not only from China and traditional State actors, but also from non-State threats.

Traditional security solutions are not designed to address adversarial AI attack vectors. Protecting the AI assets we build and trust requires an AI native approach that is rooted in AI security research. With over 30 research blogs, 20+ conference talks, 40+ CVEs, 60+ vulnerabilities and 10+ patents filed, HiddenLayer's SAI Team has set the bar for AI security best practices. In this presentation, we'll provide an overview of what we've learned.