Tuesday, February 10

3:40 PM - 4:00 PM

FortiLayer: AI Security and Assurance platform

Stephen Brennan

Machinie Learning Software Engineer

ObjectSecurity

Abstract:

FortiLayer is an AI security and assurance platform that provides a systematic way to evaluate and improve the models that support naval decision workflows. Instead of relying on surface-level tests, it analyzes how vision models and large language models make decisions, where they may be sensitive to certain patterns or conditions, and how those behaviors align with operational expectations. The platform highlights specific factors that could affect performance, such as adversarial susceptibility, instability across operating ranges, or model components that contribute to unreliable outcomes, and produces clear recommendations for strengthening them. This gives organizations a grounded, evidence-based path to increasing the dependability of their AI systems prior to deployment.