

AGENDA

Securing AI Applications: Understanding the New Attack Surface

Executive Dinner

[Click Here to Register](#)

SECURING AI APPLICATIONS: UNDERSTANDING THE NEW ATTACK SURFACE



September 24, 2026

6:00 PM-9:30 PM

Central European Time

AI hasn't just changed how we build, it's fundamentally reshaped the attack surface. Today's AI applications are dynamic, interconnected systems spanning models, data pipelines, agents, and cloud infrastructure—introducing new and often invisible paths for risk. In this session, we'll break down where risk actually exists across modern AI applications and why traditional security approaches fall short. You'll learn how leading teams are evolving their approach to gain end-to-end visibility, prioritise real risk, and protect AI systems across code, cloud, and runtime. We'll also explore how to move beyond fragmented tooling to better understand attack paths, reduce noise, and secure AI at the speed it's built.

