

A large, metallic, robotic wasp with a shiny, chrome-like finish stands on a dense city skyline. The wasp has large, transparent wings, a segmented abdomen, and a head with large, reddish-brown eyes and antennae. It is positioned in the center of the frame, looking down towards the city. In the background, the Golden Gate Bridge is visible, spanning a body of water under a clear blue sky. The city below is filled with various buildings and structures.

# OWASP AI Summit

---

Red Teaming with and to Secure  
LLMs and Generative AI

PANEL SESSION

# Red Teaming with and to Secure LLMs and Generative AI

## PANELISTS



**Ads Dawson**

Core Team, Technical Lead  
and Expert

Cohere



**Jason Ross**

Core Team, Expert

Salesforce



**Ken Huang**

Core Team, Expert

Distributedapps.AI

## MODERATOR



**Scott Clinton**

Core Team, Industry Lead

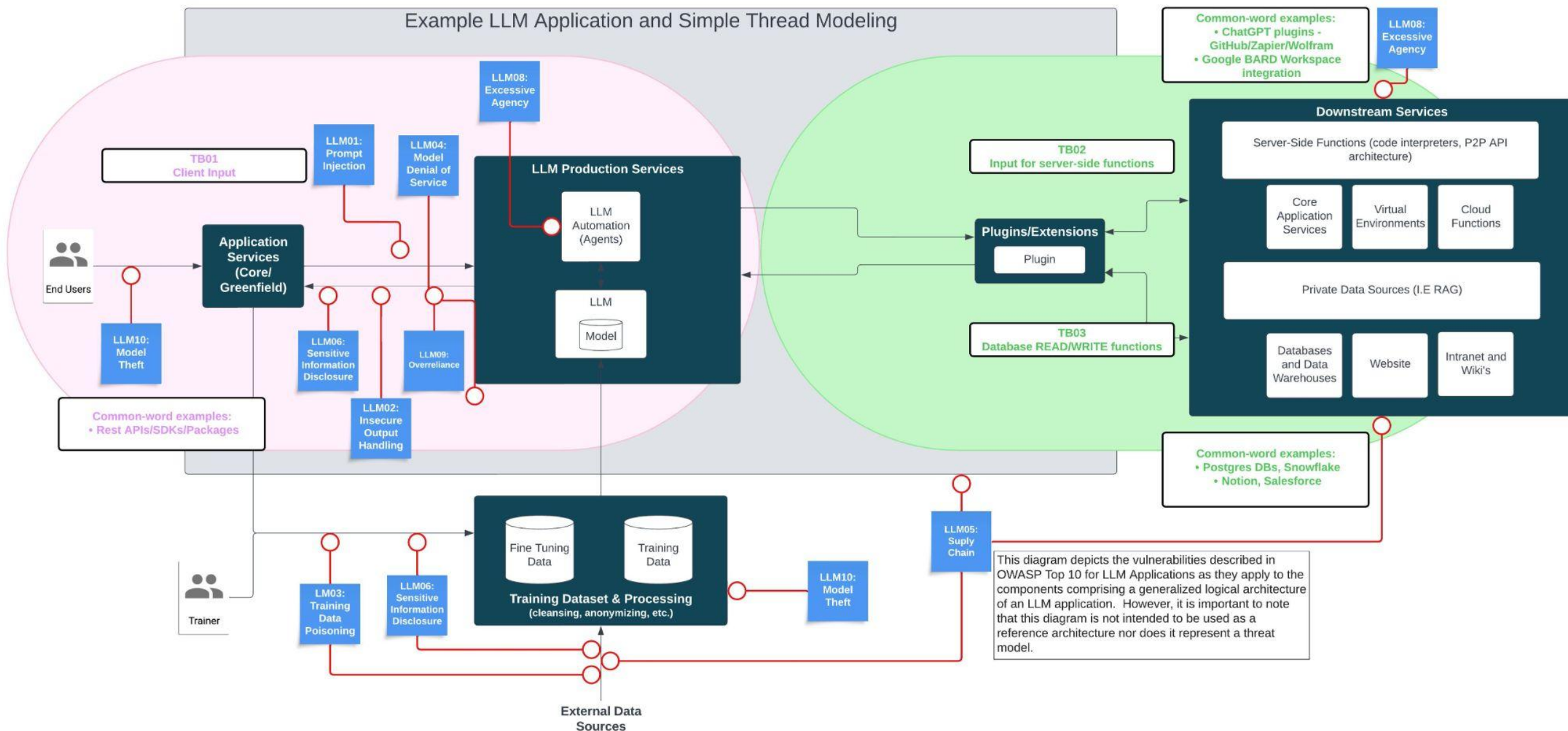
SCVentures



# OWASP Top 10 for LLMs and Gen AI Apps

Credits: Ads Dawson / <https://linkedin.com/in/adamdawson0>

## Example LLM Application and Simple Thread Modeling



# Questions?



**THANK YOU**

---



# OWASP CORE TEAM Q&A



**THANK YOU**

---

