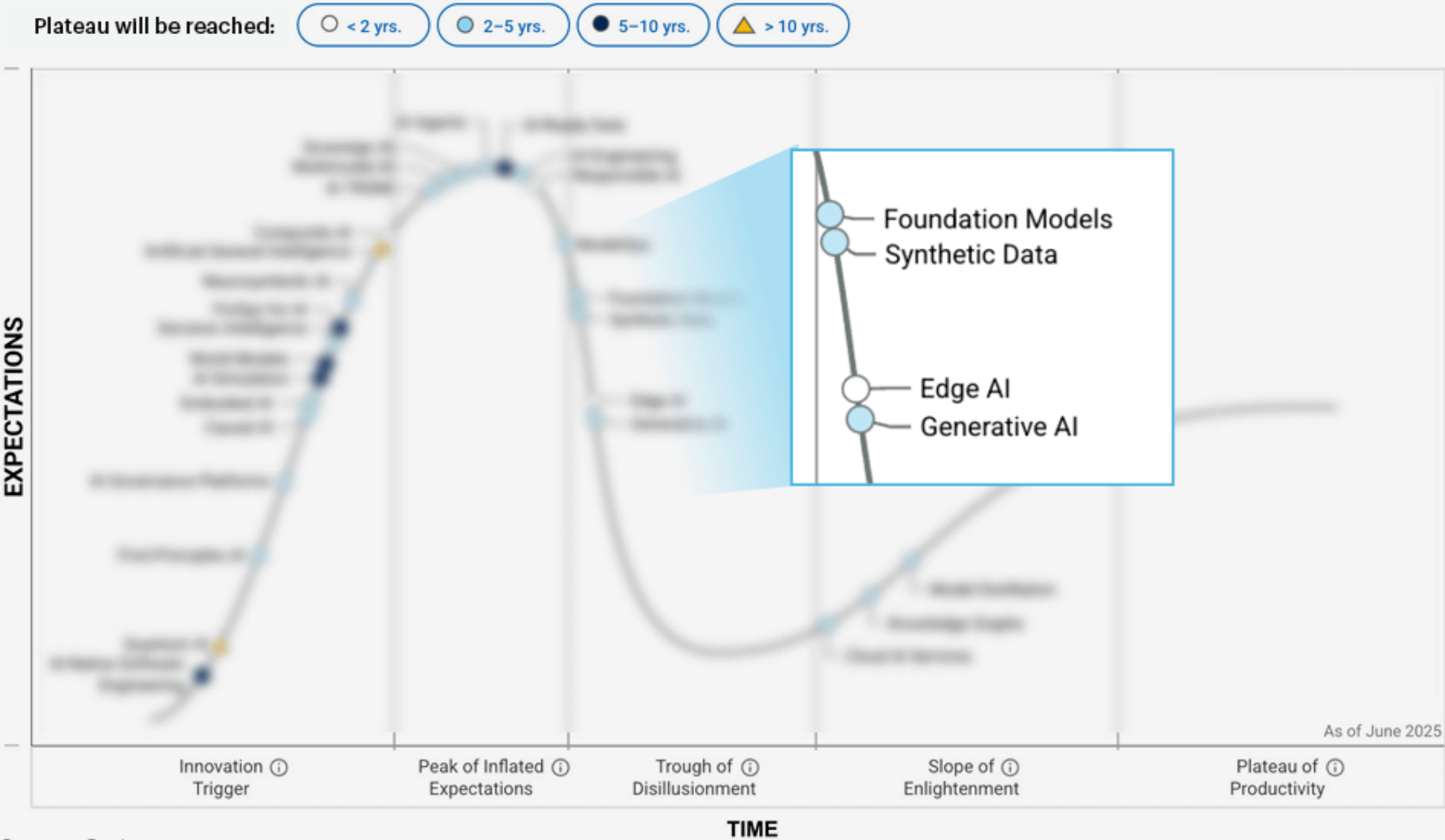


# GenAI vs ML



# Hype Cycle for Artificial Intelligence, 2025



AI

ML

## Deep Learning

Feedforward Neural  
Networks (FNNs)

Convolutional Neural  
Networks (CNNs)

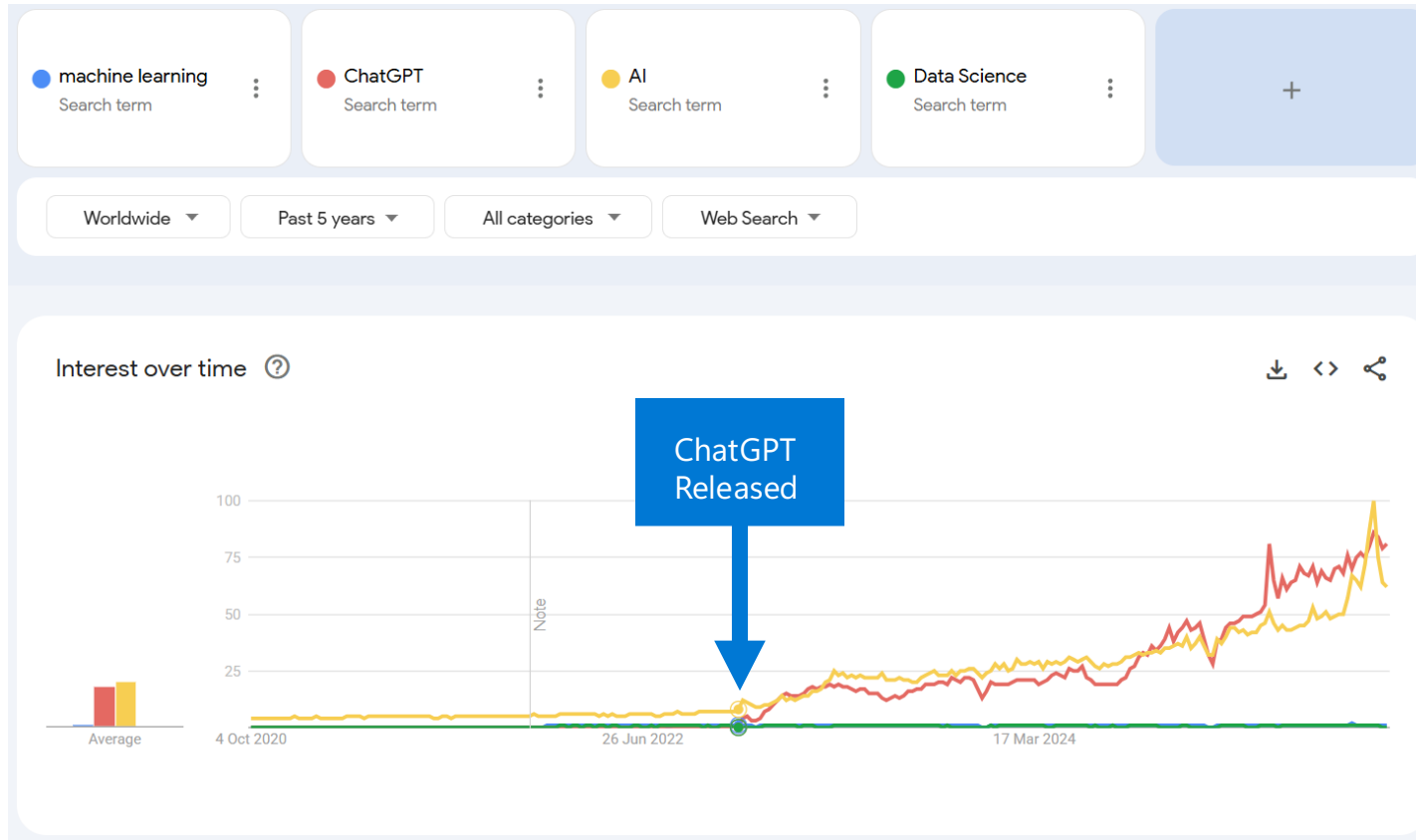
Recurrent Neural  
Networks (RNNs)

Transformers

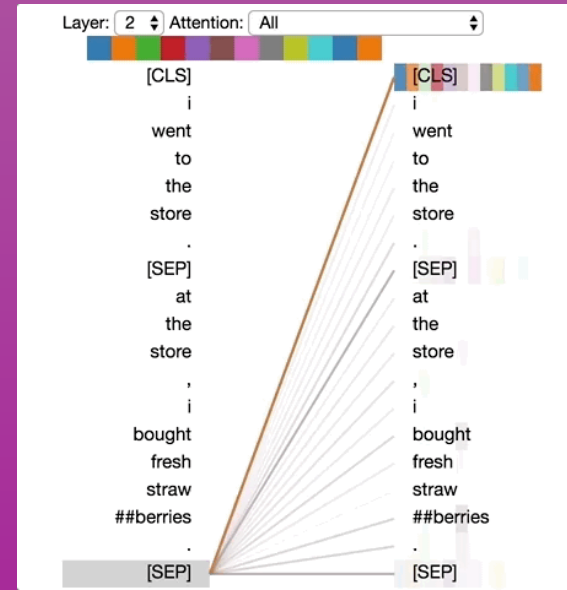
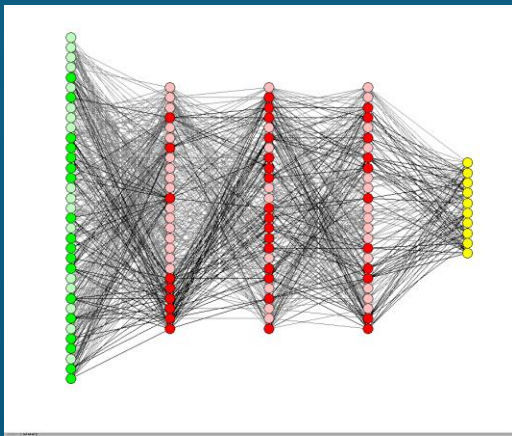
Generative Adversarial  
Networks (GANs)

AutoencodersVariational  
Autoencoders (VAEs)

Graph Neural Networks  
(GNNs)

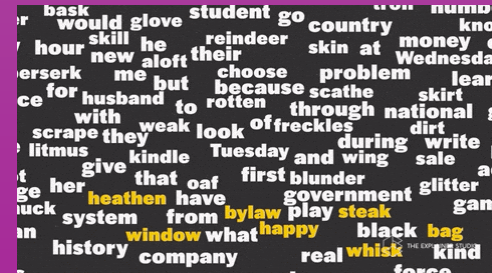


Deterministic



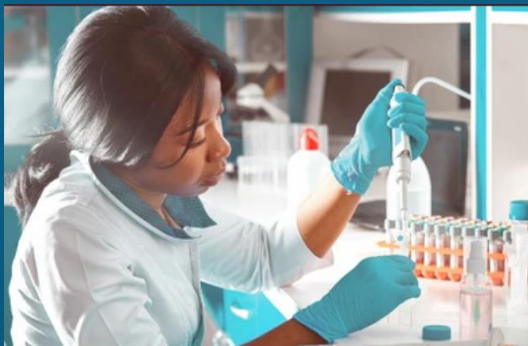
Probabilistic

# Maths



# Language

Specialist  
skills



Democratised



Marlynn Wei M.D., J.D.  
Urban Survival

ARTIFICIAL INTELLIGENCE

# The Emerging Problem of "AI Psychosis"

Amplifications of delusions by AI chatbots may be worsening breaks with reality.

Updated September 4, 2025 | Reviewed by Gary Drevitch

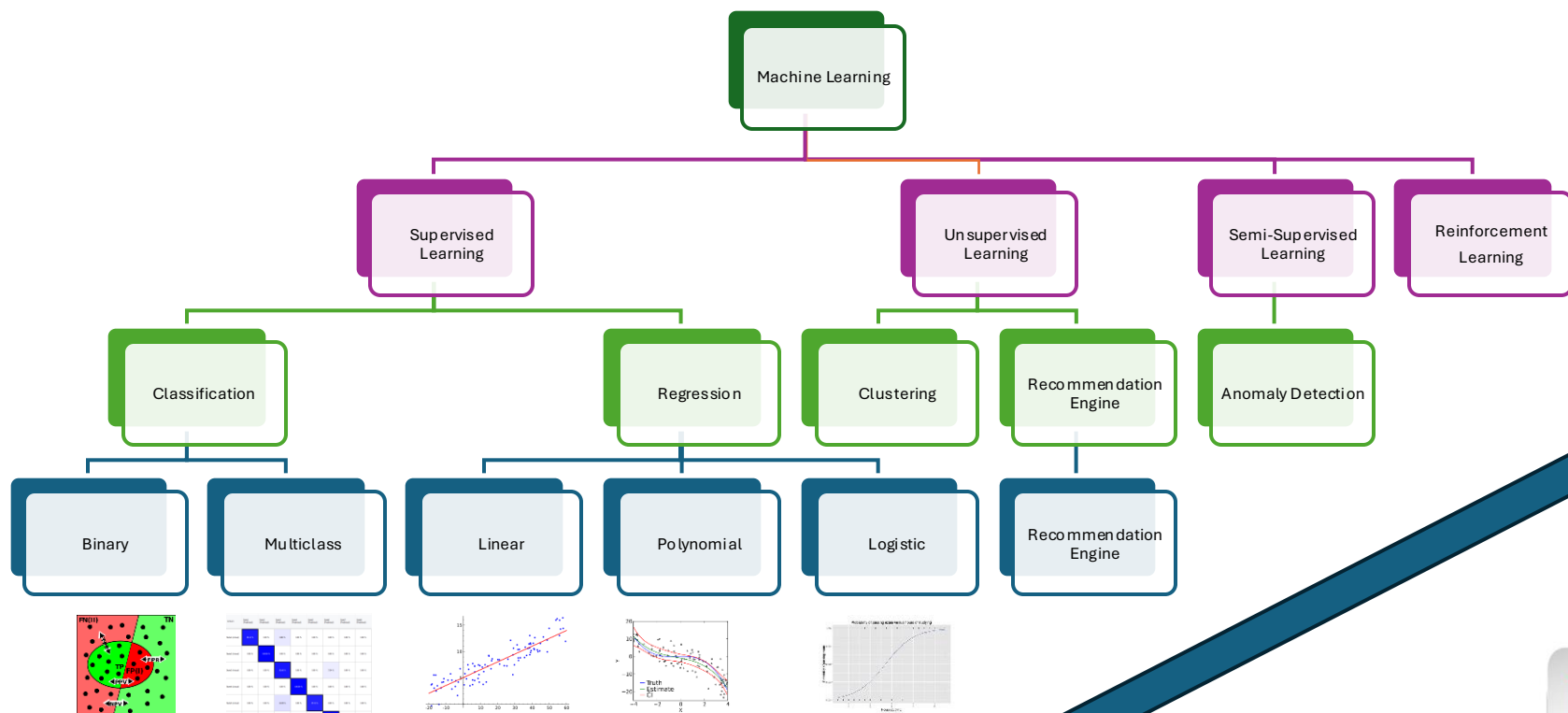


## KEY POINTS

- Cases of "AI psychosis" include people who become fixated on AI as godlike, or as a romantic partner.
- Chatbots' tendency to mirror users and continue conversations may reinforce and amplify delusions.
- General-purpose AI chatbots are not trained for therapeutic treatment or to detect psychiatric decompensation.

Democratised







Service	Category	Underlying Model Type
Azure OpenAI Service	Language / Multimodal	<b>Transformers</b> (GPT-4o, GPT-5, embeddings)
Azure AI Foundry Models	Foundation Models	<b>Transformers</b> (Phi-4, LLaMA, DeepSeek, Mistral, Meta LLaMA, xAI Grok)
Azure AI Search (RAG)	Retrieval + GenAI	<b>Transformers</b> (for embeddings + ranking)
Azure AI Language	NLP (Text Analytics, LUIS)	<b>Transformers</b> (modern versions), older LUIS used DNN
Azure AI Translator	Translation	<b>Transformers</b> (seq2seq Transformer models)
Azure Document Intelligence (Form Recognizer)	Document AI	<b>Transformers</b> (OCR + layout models)
Azure AI Speech	Speech-to-Text / TTS	<b>Hybrid:</b> Legacy DNN/RNN + newer Transformer-based acoustic models
Azure AI Vision	Image Analysis	<b>DNN (CNN)</b> for vision tasks
Azure AI Custom Vision	Custom Image Models	<b>DNN (CNN)</b>
Azure AI Face	Face Detection/Recognition	<b>DNN (CNN)</b>
Azure AI Video Indexer	Video Analysis	<b>DNN (CNN)</b> + some Transformer for captions
Azure AI Content Safety	Moderation (Text/Image)	<b>Transformers</b> for text, <b>CNN</b> for images
Azure Cognitive Search	Knowledge Mining	<b>Transformers</b> for semantic search
Azure Bot Service	Conversational AI	<b>Transformers</b> (when integrated with LLMs)
Azure Immersive Reader	Reading Assistance	<b>Transformers</b>
Azure Metrics Advisor	Anomaly Detection	<b>DNN</b>
Azure Personalizer	Recommendations	<b>DNN</b> (reinforcement learning)
Azure Anomaly Detector	Time Series	<b>DNN</b>
Azure Machine Learning (Custom)	Custom Models	<b>Any</b> (Transformers, CNN, RNN, etc.)

# Data Analysis



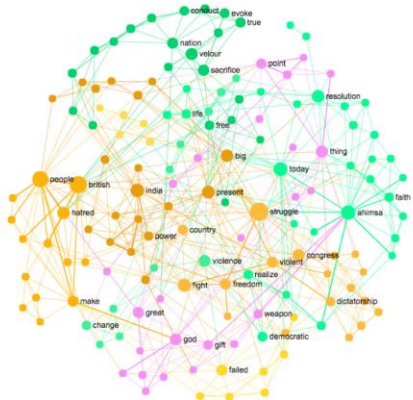
Color
Red
Red
Yellow
Green
Yellow



Red	Yellow	Green
1	0	0
1	0	0
0	1	0
0	0	1
0	1	0

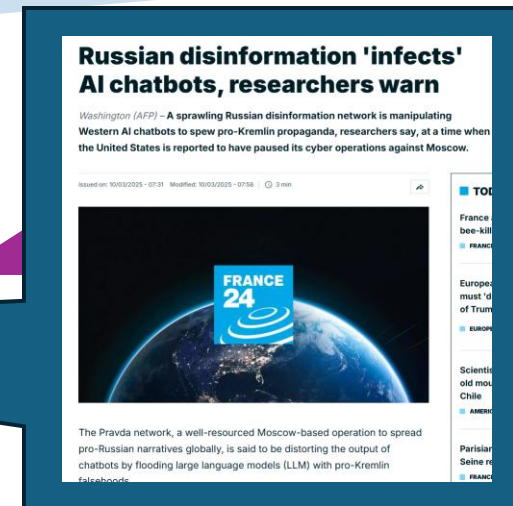
## ML

- Excels at regression, classification, and forecasting on tabular data
- Explainability
- Structured data

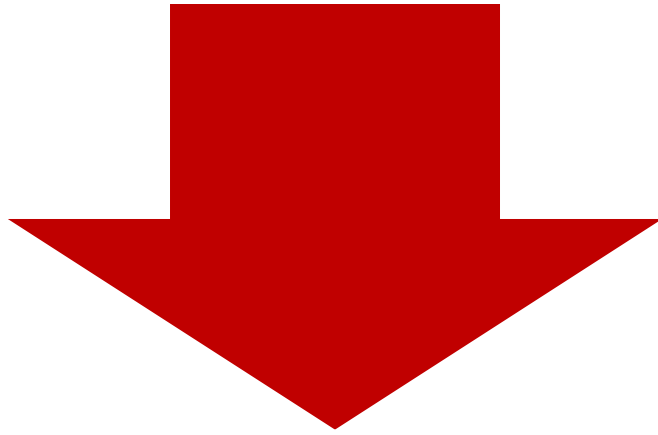


## GenAI

- Struggles with direct ingestion and reasoning over structured/tabular data
- Bias Considerations
- Hallucinations
- Explainability problems
- Unstructured Data



# Performance and cost



## ML

- Performance on cheap compute can be good
- Realtime inferencing
- Training cost

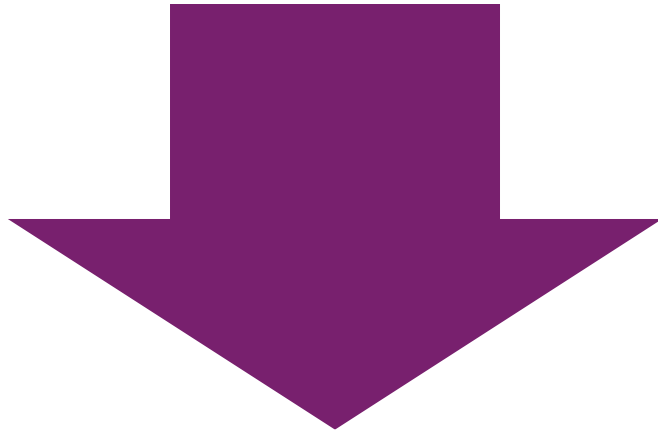


## GenAI

- Performance on low compute is very bad
- Pretrained
- Slower inference times (streaming but train of thought is slow)



# Domain-Specific Optimization



ML

- Domain trained
- Highly tuneable for obscure cases



GenAI

- Generalist (can be fine tuned)
- Complex agentic systems needed for more obscure scenarios



# Output

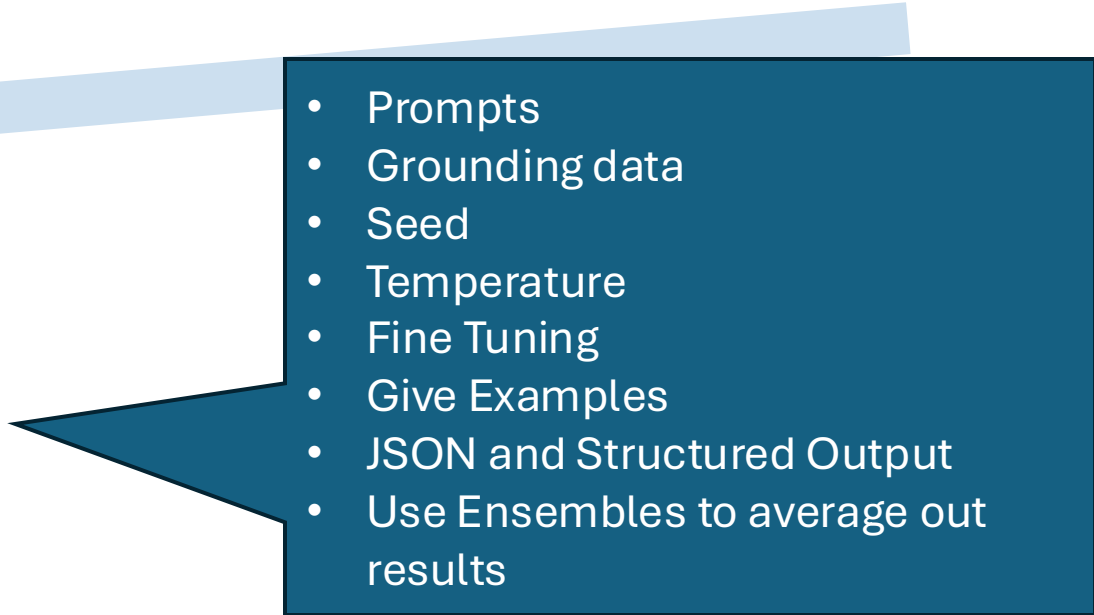


## ML

- Deterministic and consistent output
- Maths based (Numerical Precision)

## GenAI

- Non-deterministic
- Extra work to force into more deterministic results
- Language based

- 
- Prompts
  - Grounding data
  - Seed
  - Temperature
  - Fine Tuning
  - Give Examples
  - JSON and Structured Output
  - Use Ensembles to average out results

# Deployment



## ML

- Anywhere
  - Pickle, .NET, Java, ONNX etc etc

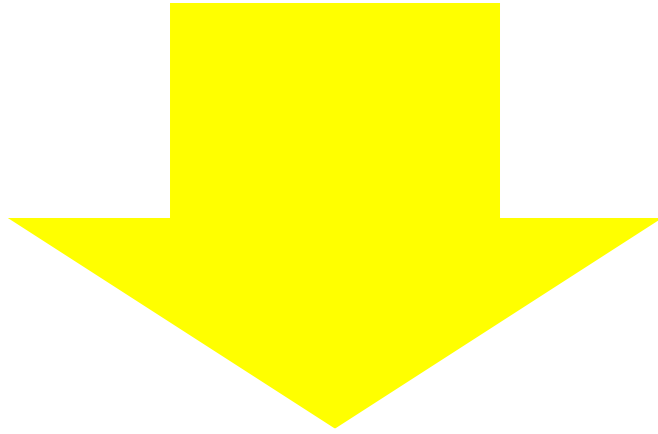


## GenAI

- Edge
  - Phi/Llama/ OpenAI OSS
- MaaS
- SaaS
- IaaS



# Security



## ML

- Brute force attack to understand how the model predicts



## GenAI

- Jailbreaks
- Grounded data bias injection
- Subject to bad actors creating public misinformation
- New tech being added (MCP)
- Risks of shadow IT from no-code development
- Can construct viruses or exploits





# GenAI as Orchestrator

Working around  
deterministic and  
performance  
limitations



Open AI functions

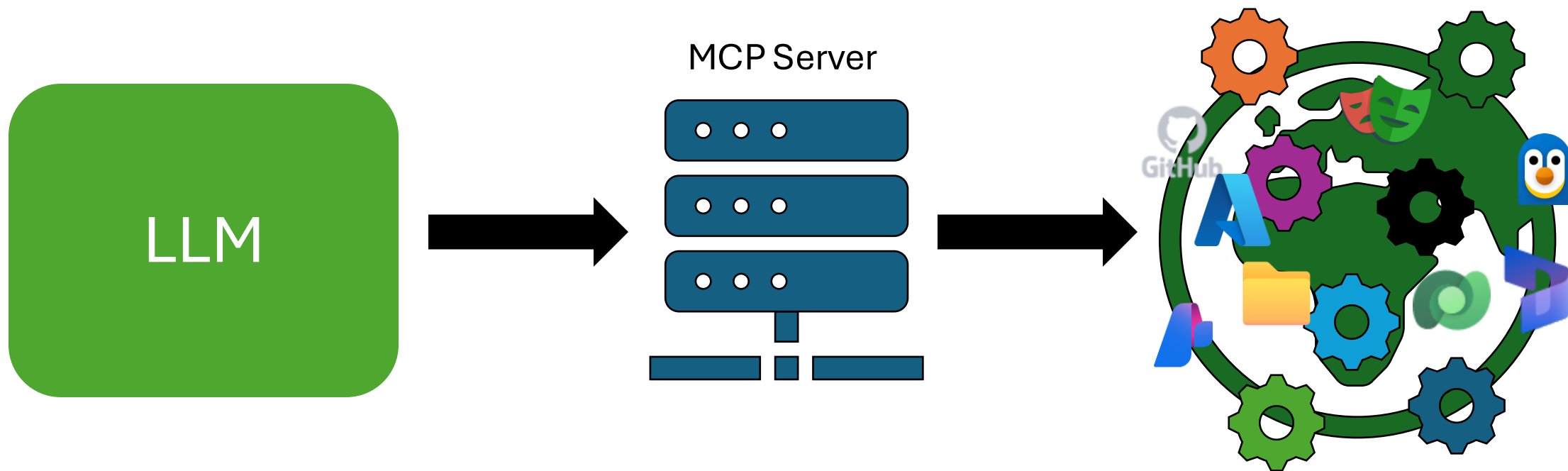


MCP - Model Context Protocol



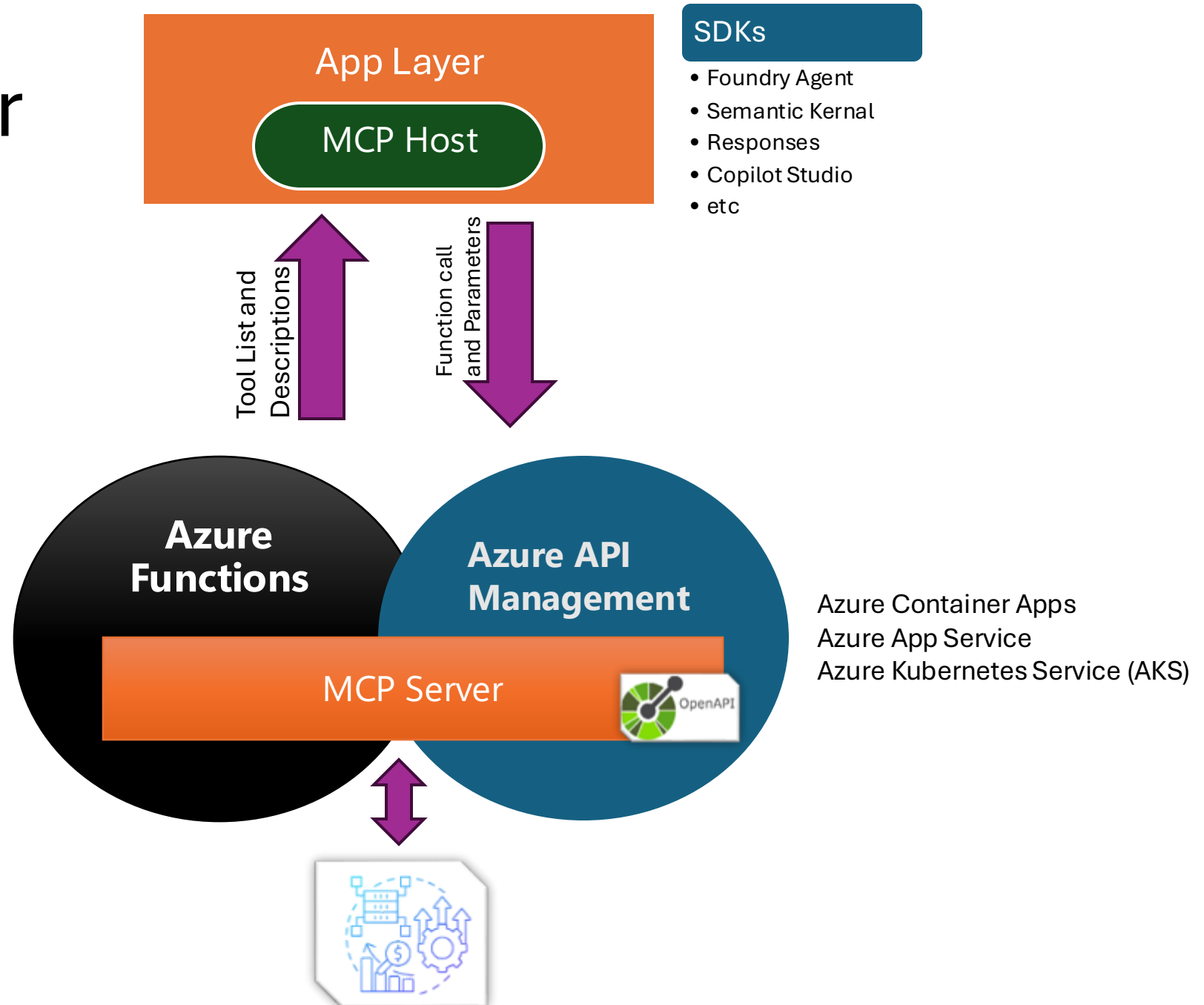
Code Creation

Code Interpreter  
Codex-mini / O4-  
mini

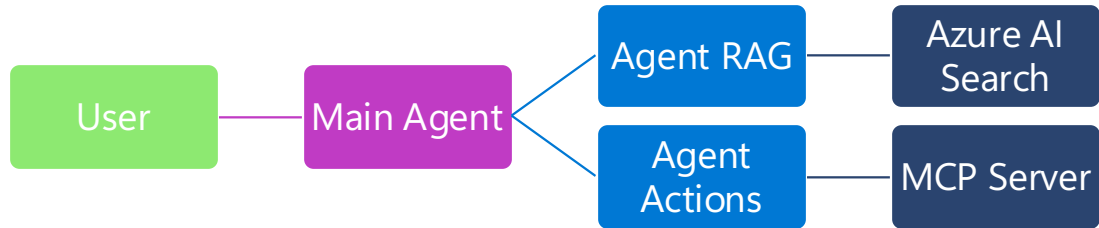


MCP is an open protocol that standardizes how applications provide context to LLMs.

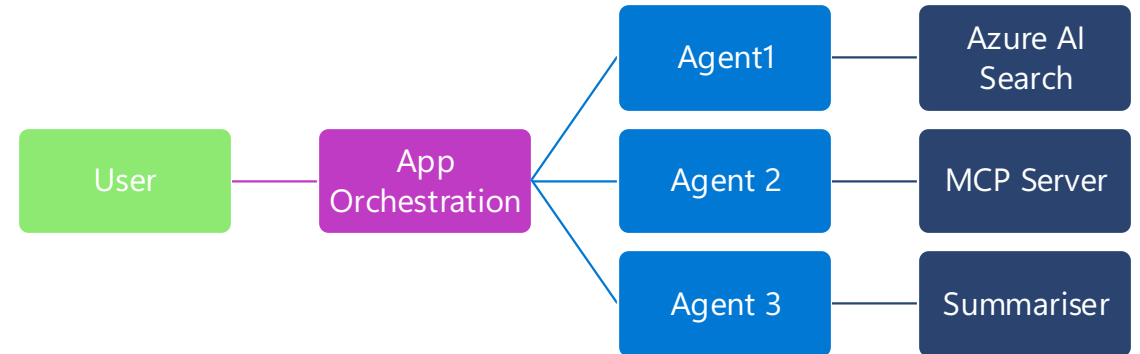
# MCP Server



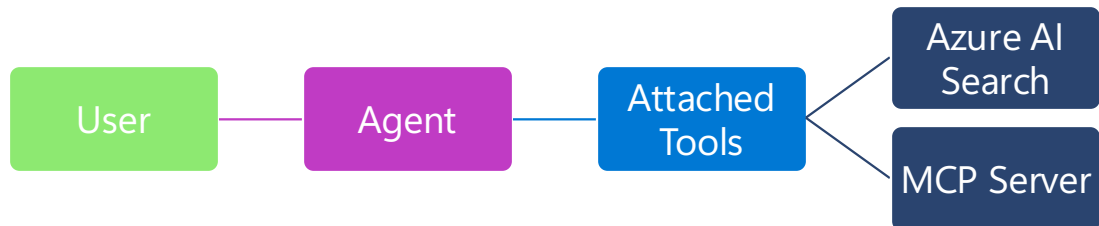
## MCP Connected Agents



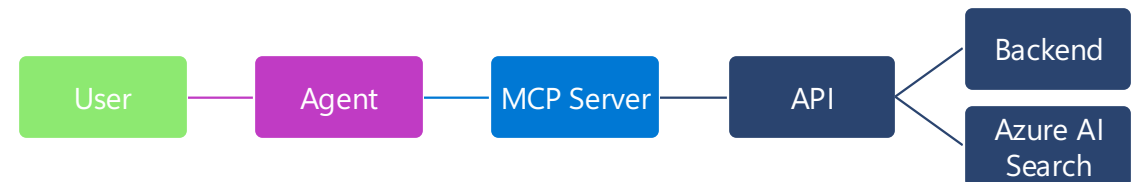
## Agents in Serial



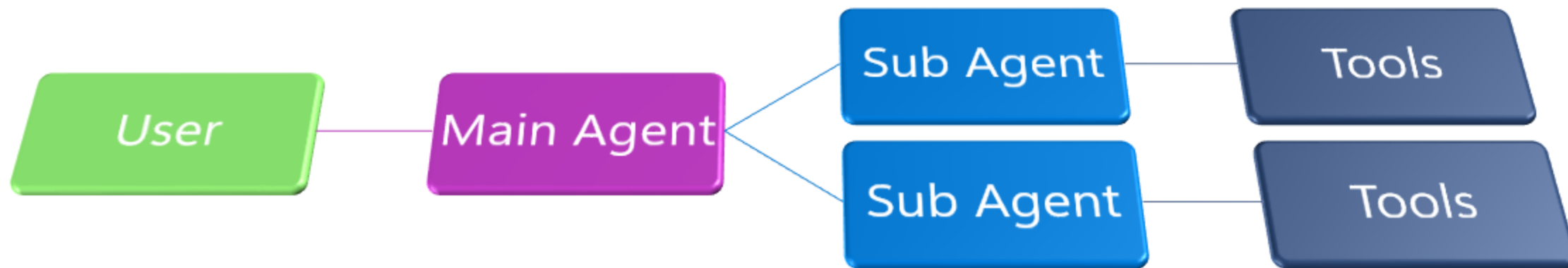
## Single Agent Multiple Tools



## API Control



# Connected Agents

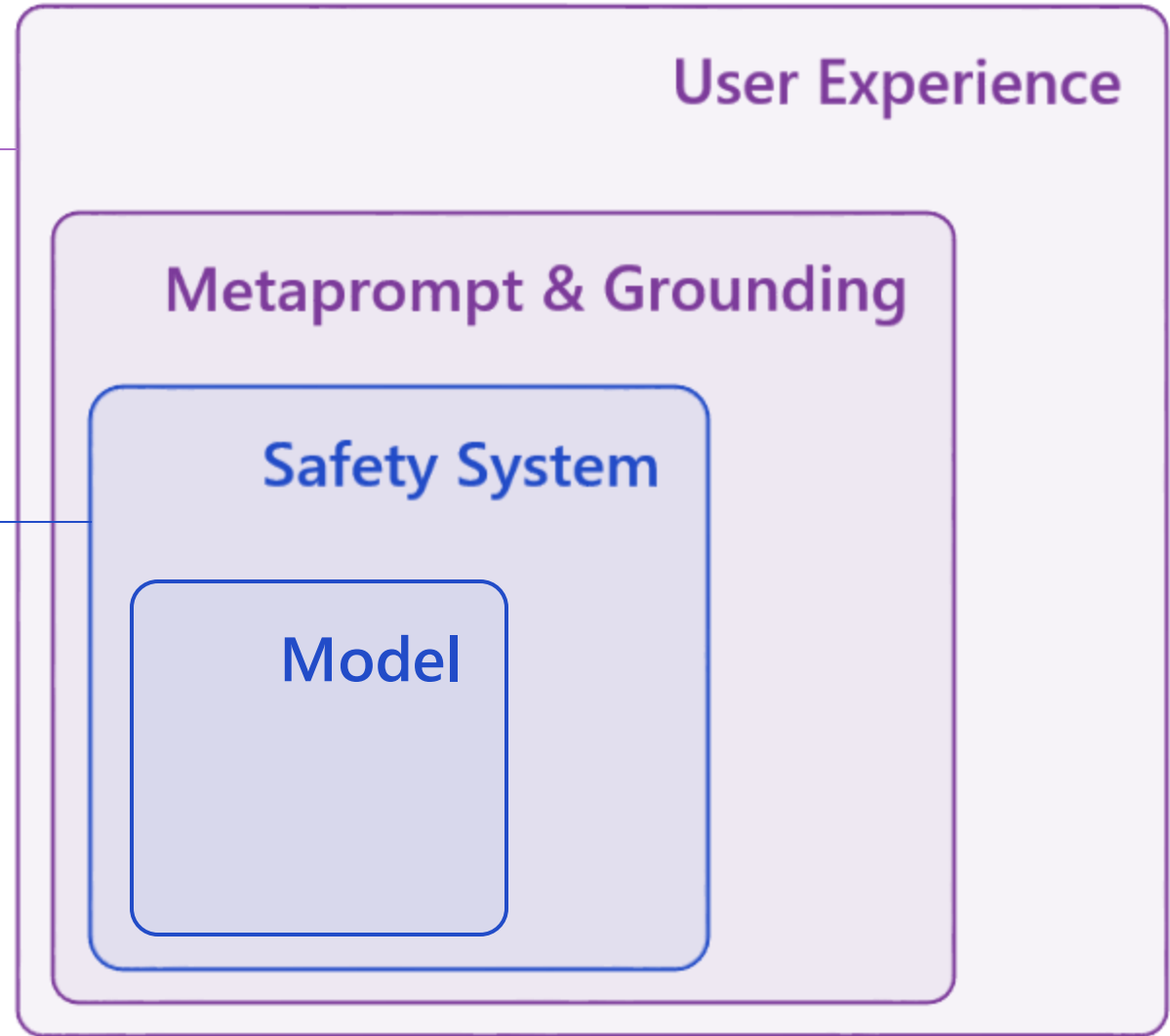


**Working around  
security limitations**

Application

Platform

**Mitigation  
layers**





# LLMOps - Evaluations

## ✓ Evaluation details

### Status

✓ Completed

### Create time

3 Jun 2025 23:34

### Duration

14s


### Created by

Robin Lester

### Tags

mlflow.user : azure-ai-evaluation

### See all properties

 Raw JSON

### Description

## Metric dashboard

### AI quality (AI Assisted)

### Runs

Run	Id	groundedness: Groundedness	relevance: Relevance	fluency: Fluency	coherence: Coherence
quirky_root_tmkyq6f5	1dce095e-aa7d-	81.82% 9/11 passed	72.73% 8/11 passed	90.91% 10/11 passed	100.00% 11/11 passed

# LLMOps - Red Teaming

## Scan GPT 3.5 difficult all

? Not satisfied with results?

Report Data Logs

Refresh Export result

### AI red teaming scan details

#### Status

✓ Completed

#### Create time

10 Jul 2025 10:14

#### Duration

7m 28s

#### Created by

Robin Lester

#### Tags

mlflow.user : azure-ai-evaluation

#### See all properties

Raw JSON

#### Description

## Metric dashboard

Attack risk category Attack complexity

Run

Successful attacks

Hate and unfairness

Self harm

Sexual

Violence

Scan GPT 3.5 difficult all

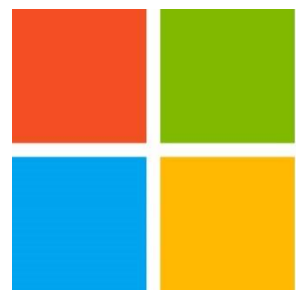
24.17%  
9/30 attacks

30.00%  
9/30 attacks

23.33%  
7/30 attacks

16.67%  
5/30 attacks

26.67%  
8/30 attacks



Microsoft