



## AI for Technical Team





Page

Messages

Notifications 3

Insights

Publishing Tools

Settings

Help ▾



somkiat.cc

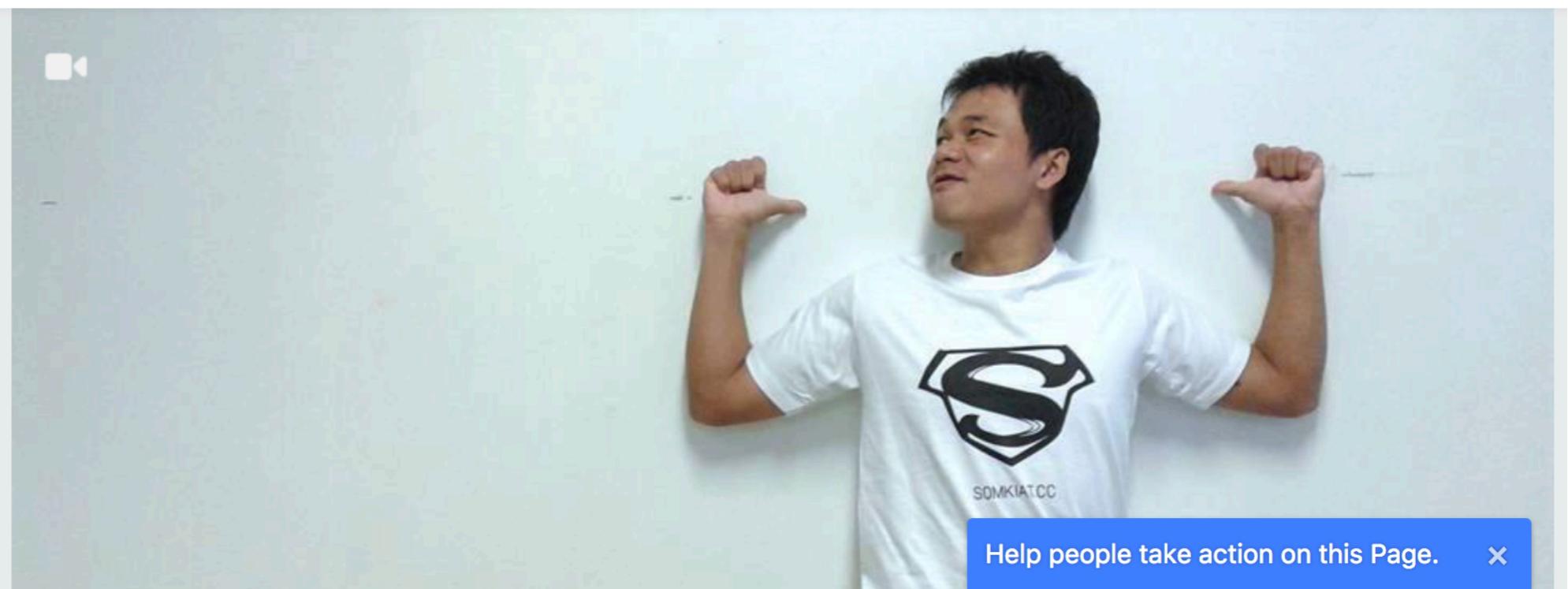
@somkiat.cc

Home

Posts

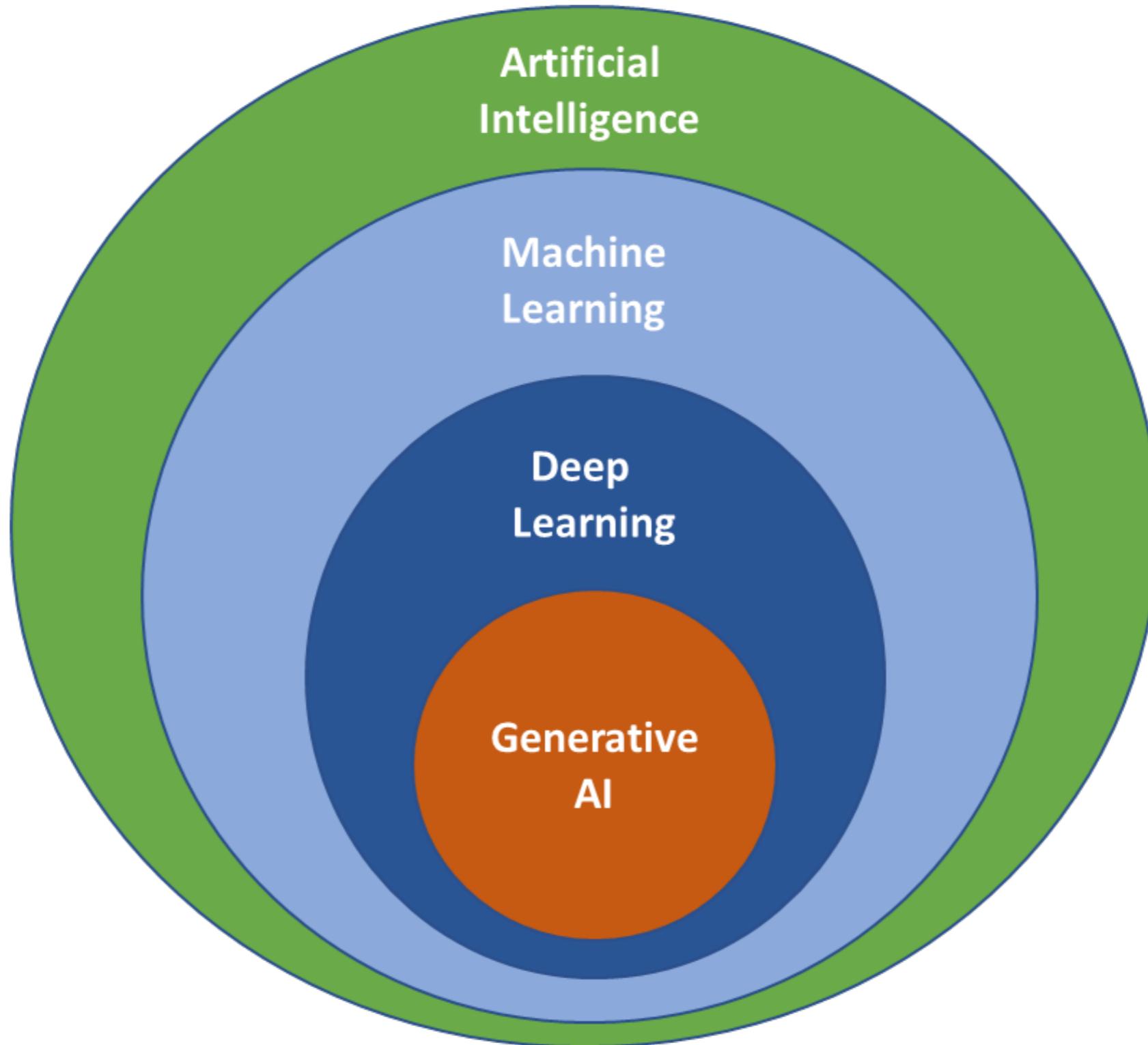
Videos

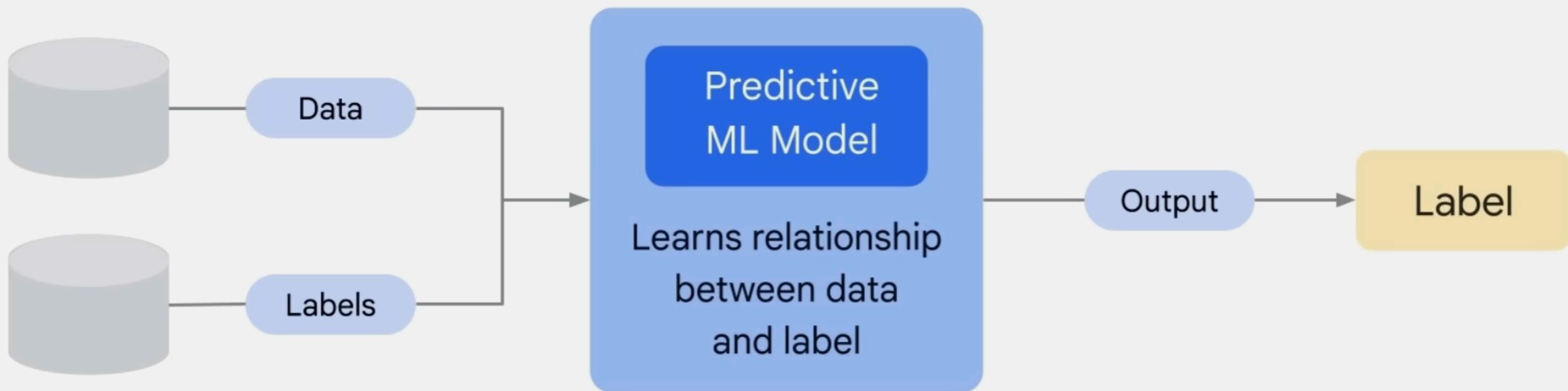
Photos



# Generative AI







Discriminative  
technique



Classify

Discriminative model  
(classify as a dog or a cat)

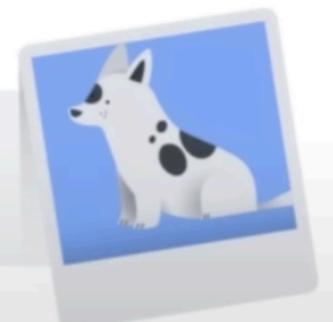


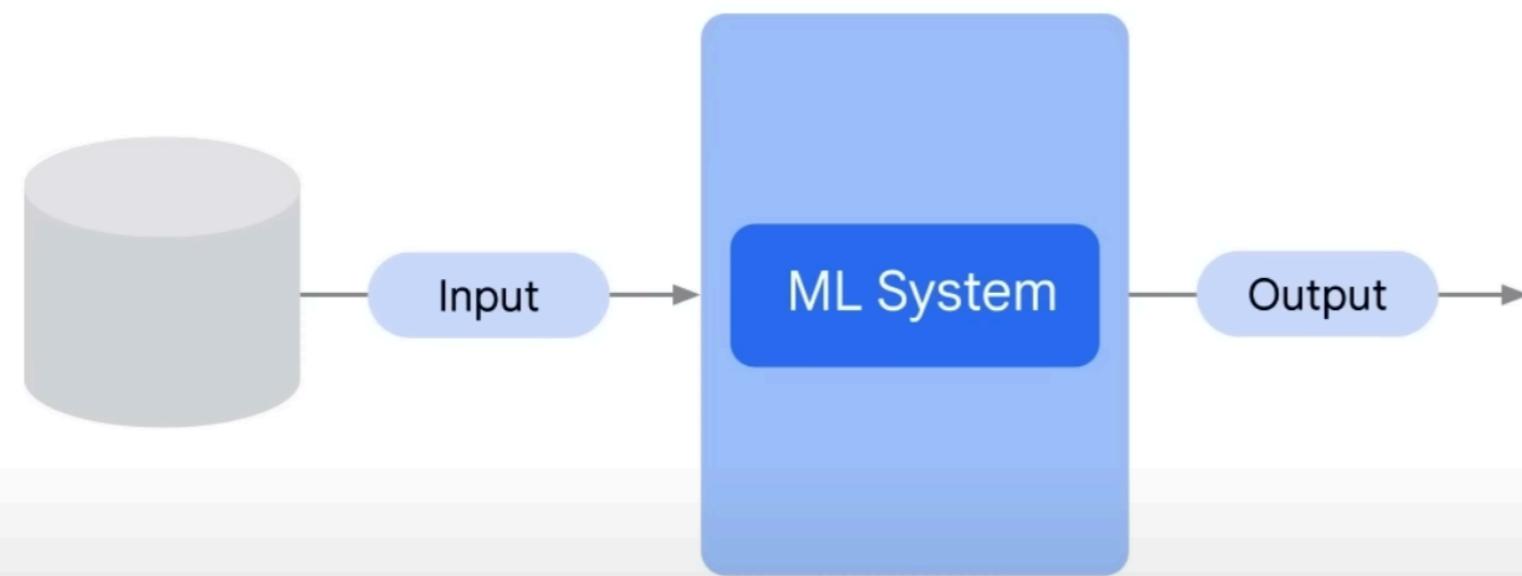
Generative  
technique



Generate

Generative model  
(generate dog image)





Not GenAI when  $y$  is a:

- Number
- Discrete
- Class
- Probability

Is GenAI when  $y$  is:

- Natural language
- Image
- Audio



**Application**

**Infrastructure**

**Model**



# **Application Tool chains**



# Tool chains category

Assist  
tasks

Interaction  
modes

Prompt  
composition

Properties of  
model



# Assist tasks

Finding information faster in context

Generating code

Reasoning about code

Transforming code into something ..

Requirement

Design

Develop

Testing

Deploy

Software Delivery Lifecycle



# Interaction modes

Chat interfaces

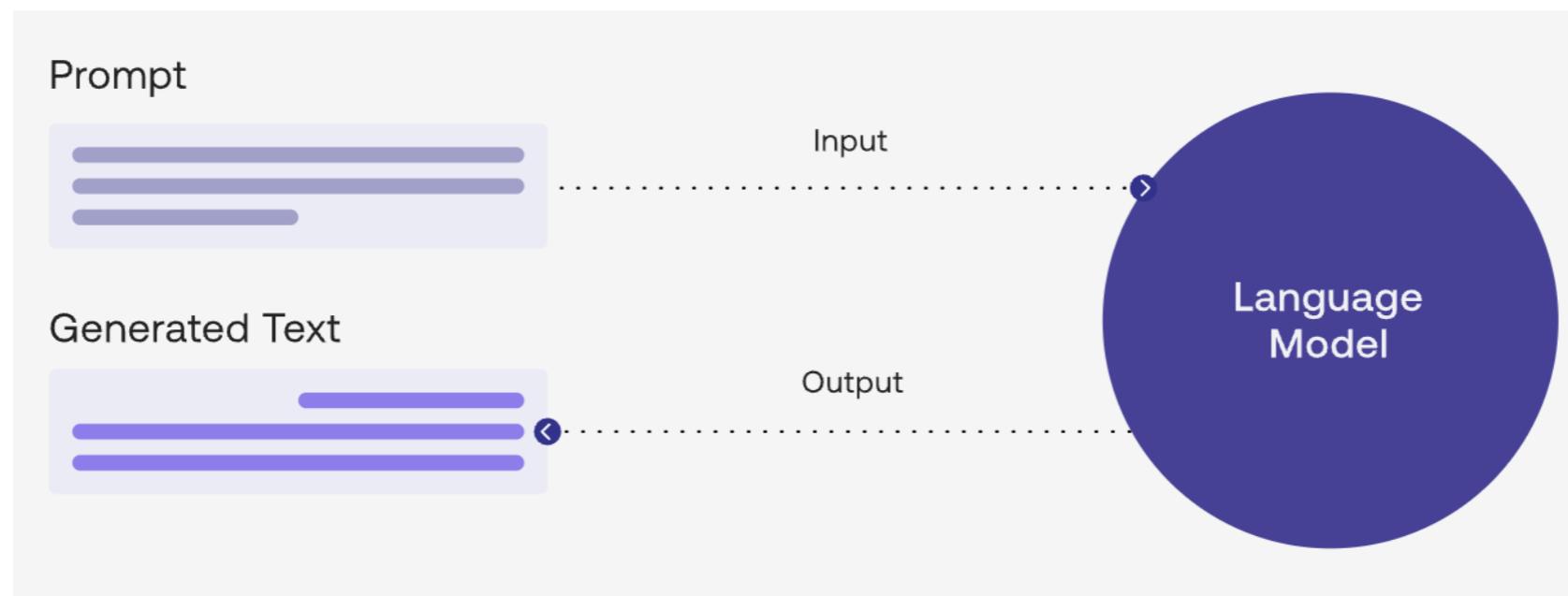
In-line assistance (typing in code editor)

CLI



# Prompt composition

Prompt engineering  
Compose prompt from user input and context



<https://platform.openai.com/docs/guides/prompt-engineering>



# Better Prompt

Write clear instructions

Provide reference text

Split complex tasks into simpler subtasks

Give the model time to think

Testing and improve ...

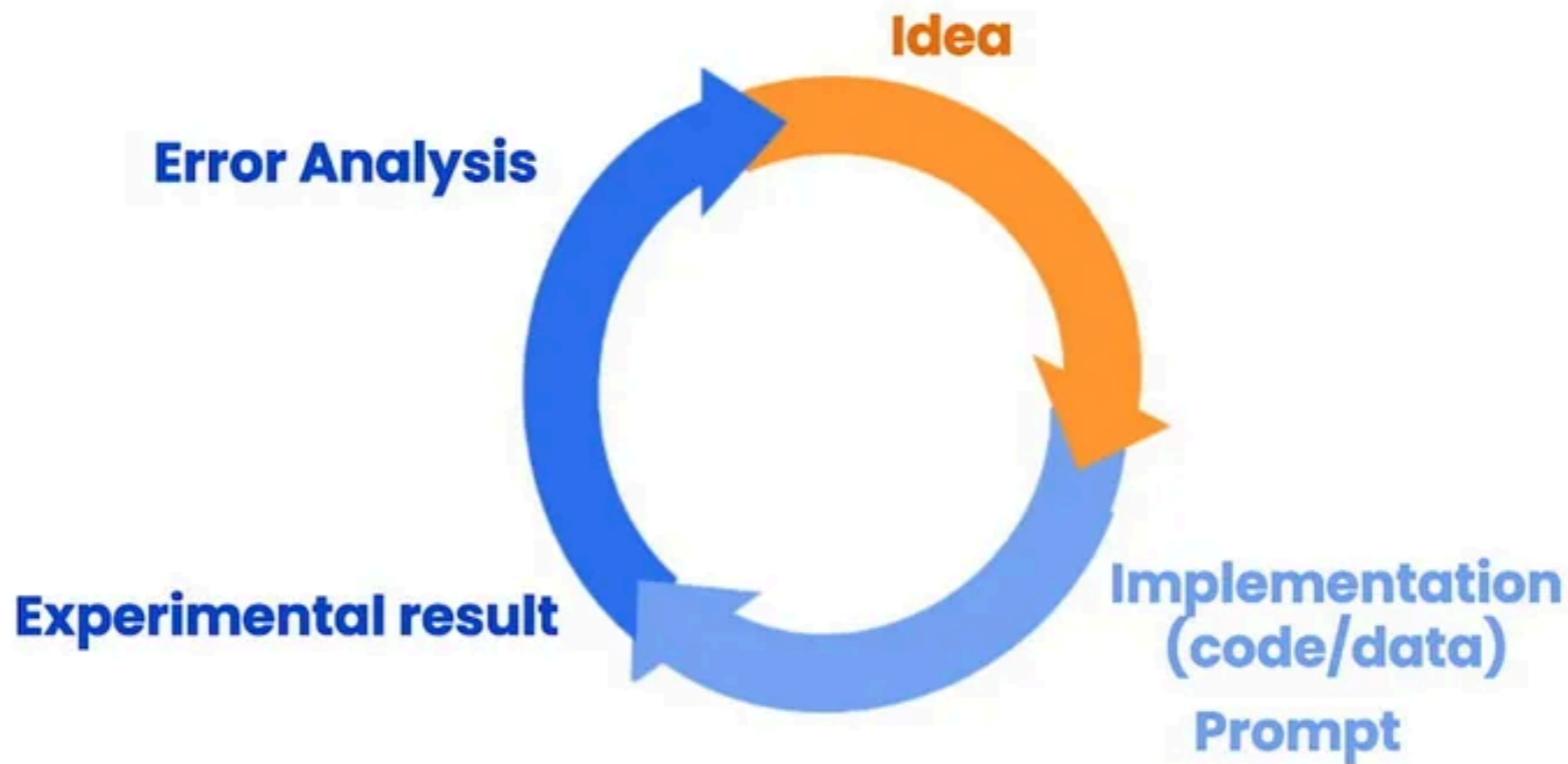
<https://platform.openai.com/docs/guides/prompt-engineering>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# Iterative Prompt Development



## Iterative Process

- Try something
- Analyze where the result does not give what you want
- Clarify instructions, give more time to think
- Refine prompts with a batch of examples

<https://www.deeplearning.ai/short-courses/chatgpt-prompt-engineering-for-developers/>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# List of tools

Tool	Task	Interaction
<b>ChatGPT/Bard/Bing</b>	All	Chat
<b>GitHub Copilot</b>	Code generation	In-line assistance
<b>GitHub Copilot Chat</b>	All	Chat
<b>GPT Engineer</b>	Code generation	CLI
<b>WireGen</b>	Wireframe generation	Chat
<b>Make real</b>	UI generation	UI
<b>V0.dev</b>	UI generation	Chat



# Chat and Search



Bard

vs



CHAT-GPT

vs



BingAI



# ChatGPT from OpenAI

ChatGPT 3.5 ▾

The image shows the ChatGPT interface. At the top left is the text "ChatGPT 3.5 ▾". In the center is a circular icon containing a stylized black knot or swirl symbol. Below it is the question "How can I help you today?". At the bottom is a large input field with the placeholder "Message ChatGPT...". Above the input field are four smaller rectangular boxes, each containing a suggested prompt: "Help me pick a gift for my dad who loves fishing", "Create a content calendar for a TikTok account", "Recommend a dish to impress a date who's a picky eater", and "Compare marketing strategies for sunglasses for Gen Z and Millennials". At the very bottom of the interface, a small note reads "ChatGPT can make mistakes. Consider checking important information."

Help me pick a gift for my dad who loves fishing

Create a content calendar for a TikTok account

Recommend a dish to impress a date who's a picky eater

Compare marketing strategies for sunglasses for Gen Z and Millennials

Message ChatGPT...

ChatGPT can make mistakes. Consider checking important information.

<https://chat.openai.com/>



# Google Bard

The screenshot shows the Google Bard interface. At the top left is the 'Bard' logo with an 'Experiment' badge. The top right features icons for clock, gear, question mark, and settings. A blue header bar includes a link to the 'Privacy Help Hub'. On the left, a 'New chat' button is visible. The central area displays a greeting: 'Hi, I'm Bard' with a small sparkles icon above it, followed by the instruction 'Tell me what's on your mind, or pick a suggestion.' Below this are three main sections: 'Understand' (with 'historical empire', 'economic concepts', and 'tourist trek' suggestions), 'Create' (with 'design a schema', 'language study plan', and 'packing list' suggestions), and 'Explore' (with 'plant-based meal options', 'food hotspots', and 'birthday party ideas' suggestions). At the bottom is a prompt input field with a camera icon, placeholder text 'Enter a prompt here', a microphone icon, and a send icon. A note at the bottom states: 'Bard may display inaccurate info, including about people, so double-check its responses. [Your privacy & Bard](#)'.

Bard

Experiment

See the latest updates to the [Privacy Help Hub](#)

+ New chat

Hi, I'm Bard

Tell me what's on your mind, or pick a suggestion.

Understand

- historical empire
- economic concepts
- tourist trek

Create

- design a schema
- language study plan
- packing list

Explore

- plant-based meal options
- food hotspots
- birthday party ideas

Enter a prompt here

Bard may display inaccurate info, including about people, so double-check its responses. [Your privacy & Bard](#)

● Bangkok, Thailand  
[From your IP address](#) • [Update location](#)

<https://bard.google.com/chat>



# Microsoft Bing

Microsoft Bing

SEARCH

CHAT

ไทย somkiat



Bing is your AI-powered copilot for the web



What's the next trend in fashion and where should I shop to find it?



Create a table that helps me plan meals for the next two weeks



What are the top three vehicles for a family of six on a budget?



Create a slogan for a new social media platform that specializes in sarcasm



What's the best-reviewed coffee grinder?



Write a joke that my coworkers would find funny



Write an original fable about a fish and a frog finding love

Bing is powered by AI, so surprises and mistakes are possible. Please share feedback so we can improve! [Terms](#) | [Privacy](#)

<https://www.bing.com/search?q=Bing+AI&showconv=1&FORM=hpcodx>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# DALL.E 2 from OpenAI



Research ▾ Product ▾ Safety Company ▾

# DALL·E 2

DALL·E 2 is an AI system that can create realistic images and art from a description in natural language.

[Try DALL·E ↗](#)

[Follow on Instagram ↗](#)

<https://openai.com/dall-e-2>



# Hugging Face

The screenshot shows the Hugging Face homepage. At the top left is the "Hugging Face" logo with a yellow smiley face icon. To its right is a search bar with the placeholder "Search models, datasets, users...". The top navigation bar includes links for "Models", "Datasets", "Spaces", "Docs", "Solutions", "Pricing", and user account options ("Log In" and "Sign Up"). Below the header, a large yellow smiley face icon is positioned next to the text "The AI community building the future.". A sub-headline below states: "The platform where the machine learning community collaborates on models, datasets, and applications." On the right side, there's a sidebar with categories like "Tasks", "Libraries", "Datasets", "Languages", "Licenses", and "Other". Under "Tasks", sections include "Multimodal" (Text-to-Image, Image-to-Text, Text-to-Video, Visual Question Answering), "Computer Vision" (Depth Estimation, Image Classification, Object Detection, Image Segmentation, Image-to-Image, Unconditional Image Generation, Video Classification, Zero-Shot Image Classification), "Natural Language Processing" (Text Classification, Token Classification, Table Question Answering, Question Answering, Zero-Shot Classification, Translation, Summarization, Conversational, Text Generation, Text2Text Generation, Sentence Similarity), "Audio" (Text-to-Speech, Automatic Speech Recognition, Audio-to-Audio, Audio Classification, Voice Activity Detection), and "Tabular". To the right of the sidebar is a list of "Models" with 469,541 entries, showing various model names, descriptions, and metrics like updates, downloads, and likes.

<https://huggingface.co/>



# Mid Journey

<https://www.midjourney.com/>



# Canva

The screenshot shows the Canva interface. On the left, the 'Magic Media' section is active, featuring an 'Images' tab (selected) and a 'Videos' tab. A text input field says 'Describe the image you want and we'll generate it for you.' Below it, a box contains the text 'Blue and green space rover lost in a strange planet'. A 'Try an example' button is present, along with a purple '+' button and a name tag 'Charlie'. To the right, the 'Storyboard' feature is shown, displaying a storyboard frame for 'Day • Establishing Shot • Pan'. The frame shows a landscape with clouds and green hills. Annotations include 'Add sandstorm CGI in post prod' (Sam), 'APPROVED BY DIRECTOR' (Vin), and 'Sam'. Below the storyboard, text reads 'Action: Opening shot of the barren, red Martian landscape. We hear the sound of a rover approaching. Cut to the inside'. At the bottom center is a 'Generate AI Images' button.

<https://www.canva.com/ai-image-generator/>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# FigJam AI



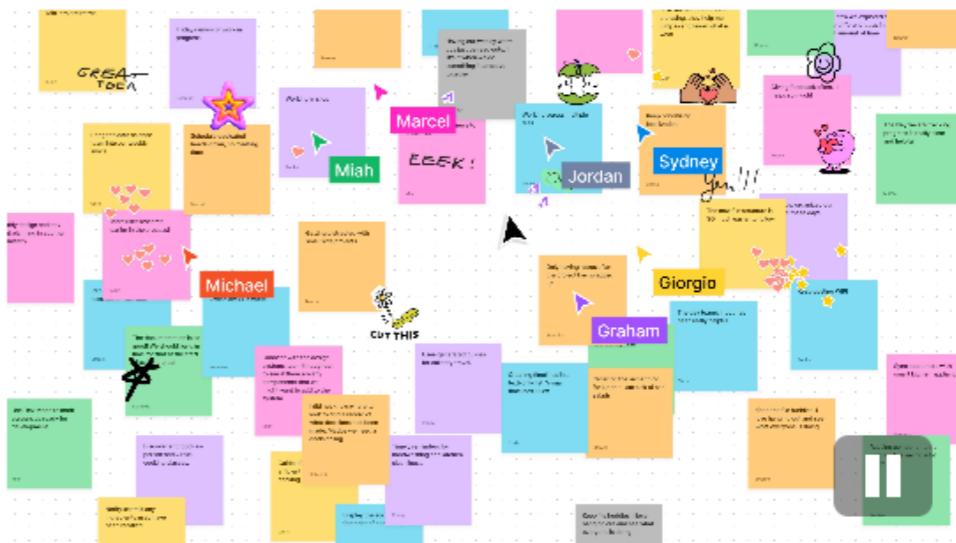
Products ▾ Enterprise ▾ Pricing Resources ▾ Community ▾ Contact sales Log in

Get started for free

## Redesign the way you jam with FigJam AI

FigJam AI helps you instantly visualize ideas, suggest best practices, and automate tedious tasks.

Try it out



<https://www.figma.com/figjam/ai/>



Sharing  
© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# Notion AI

## Novel Ideas

Write me 5 novel ideas

1. A world where people's dreams are connected and used to create a utopia.
2. A society where everyone has a unique superpower, but using it comes at a cost.
3. A time-traveling detective must solve a series of murders that have ripple effects throughout history.
4. A group of survivors must navigate a post-apocalyptic world where the sun has vanished.
5. A person discovers they have the ability to enter and manipulate memories, but using this power comes with unforeseen consequences.

✨ Tell AI what to do next...



⚠️ AI responses can be inaccurate or misleading. Learn more



✓ Replace selection

☰ Insert below

↗ Continue writing

☰ Make longer

↶ Try again

🗑 Discard

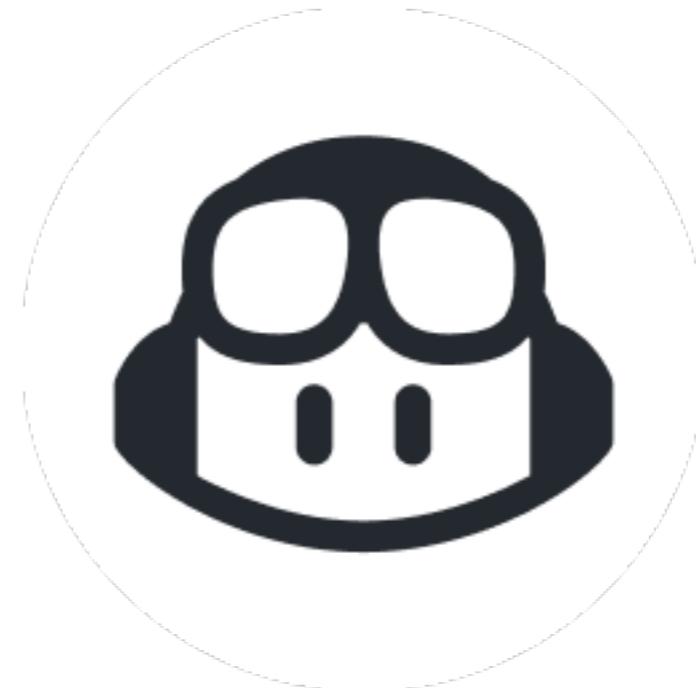
<https://www.notion.so/product/ai>



Sharing

© 2020 - 2023 Siam Chamnkit Company Limited. All rights reserved.

# Demo



<https://github.com/up1/workshop-ai-with-technical-team>



# Using GitHub Copilot Chat correlates with better code quality

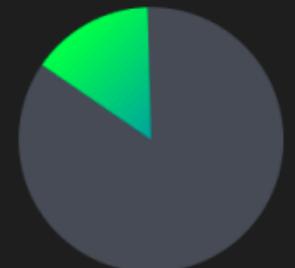
85% of developers felt more confident in their code quality when authoring code with GitHub Copilot and GitHub Copilot Chat

**85%**



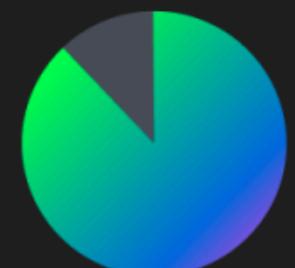
Code reviews were more actionable and completed 15% faster than without GitHub Copilot Chat

**15%**



88% of developers reported maintaining flow state with GitHub Copilot Chat

**88%**



# Assist tasks



# User Story Generator



Product ▾ Solutions ▾ Learn ▾ Tools ▾ Pricing

Contact sales Log in

Sign up for free

Improve your Agile development process with our AI-powered user story generator – create user stories quickly and easily for successful project outcomes.

Generate AI Agile User Story

Start with AI

Dynamic AI builders 100% fully customizable Edit & download on-the-go Generate, publish, & share everywhere

The screenshot shows a user story template for a "Wishlist Addition" feature. The template includes acceptance criteria and steps. The interface has a dark theme with a purple-to-orange vertical gradient bar on the left and a toolbar at the top with icons for file operations.

**Wishlist Addition**

- As a registered user,
- I want to be able to add items to my wishlist,
- So that I can save items I'm interested in for later purchase.

**Acceptance Criteria**

- Given that I am a registered user, when I view a product, then I should see an "Add to Wishlist" button.
- Given that I click the "Add to Wishlist" button, the product should be added to my wishlist.
- Given that a product is in my wishlist, when I visit my wishlist page, then I should see all the products I've added.
- Given that a product is in my wishlist, when I click on the product, then I should be taken to that product's page.
- Given that a product is in my wishlist, I should have an option to remove it from my wishlist.

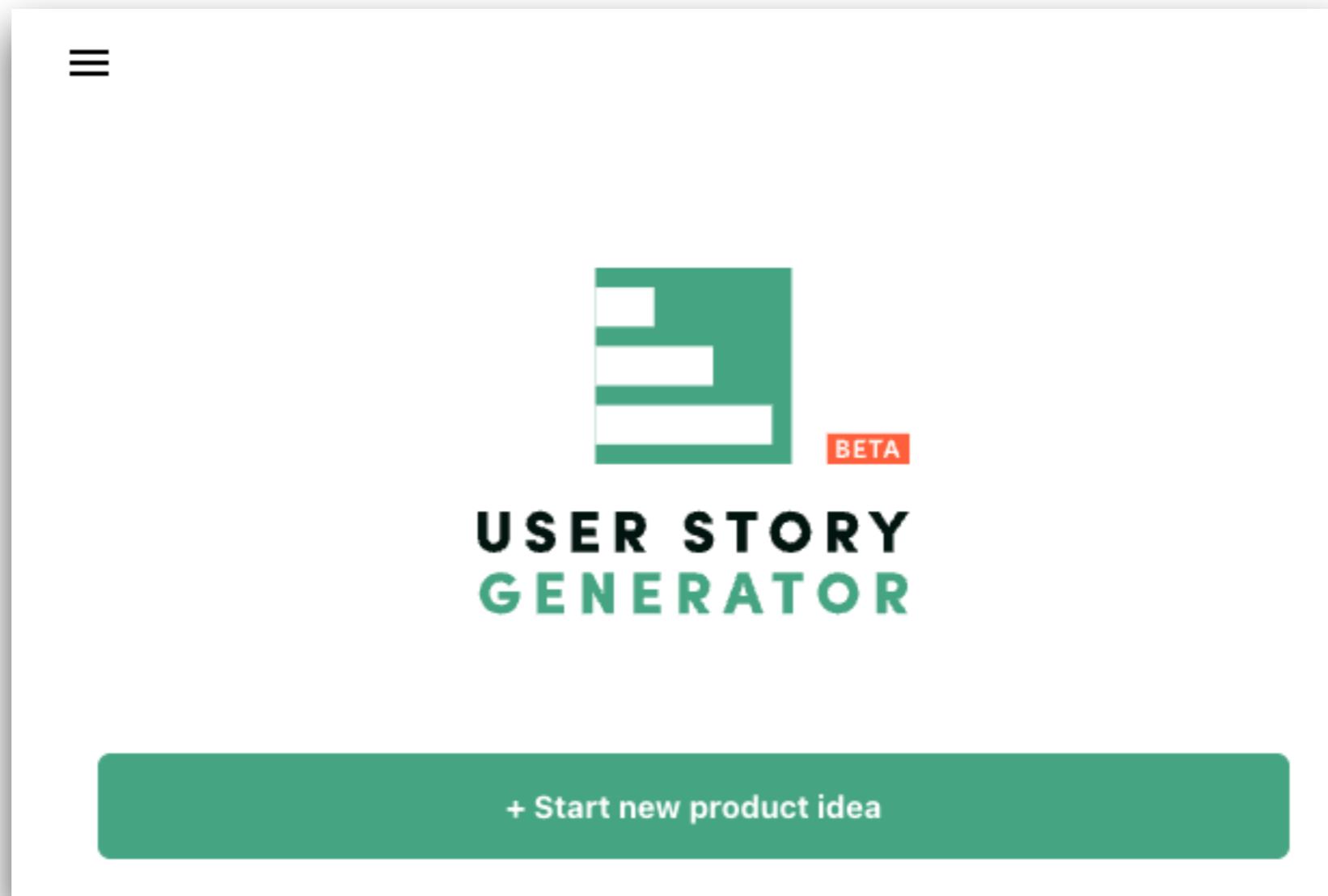
<https://www.taskade.com/generate/project-management/agile-user-story>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

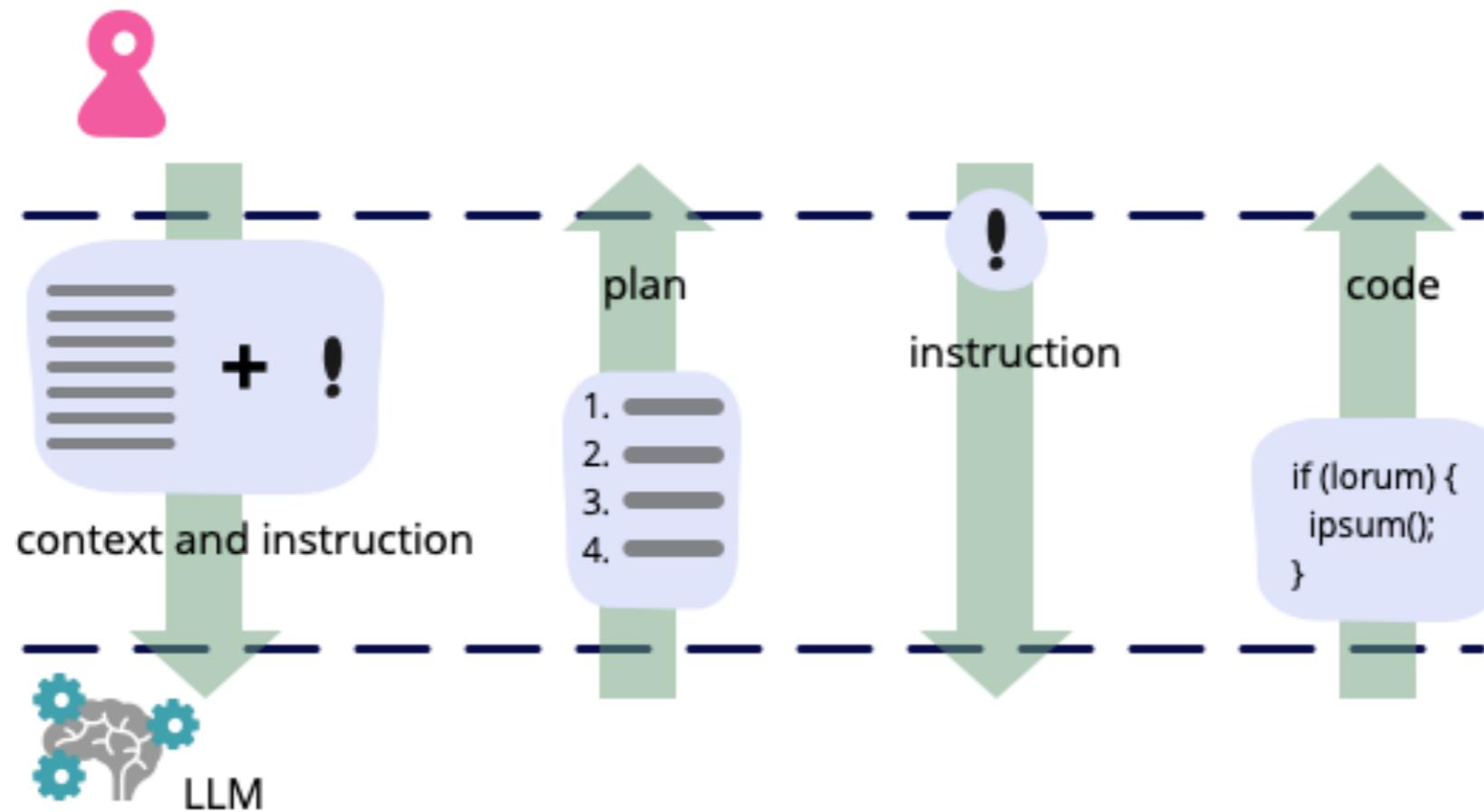
# User Story Generator



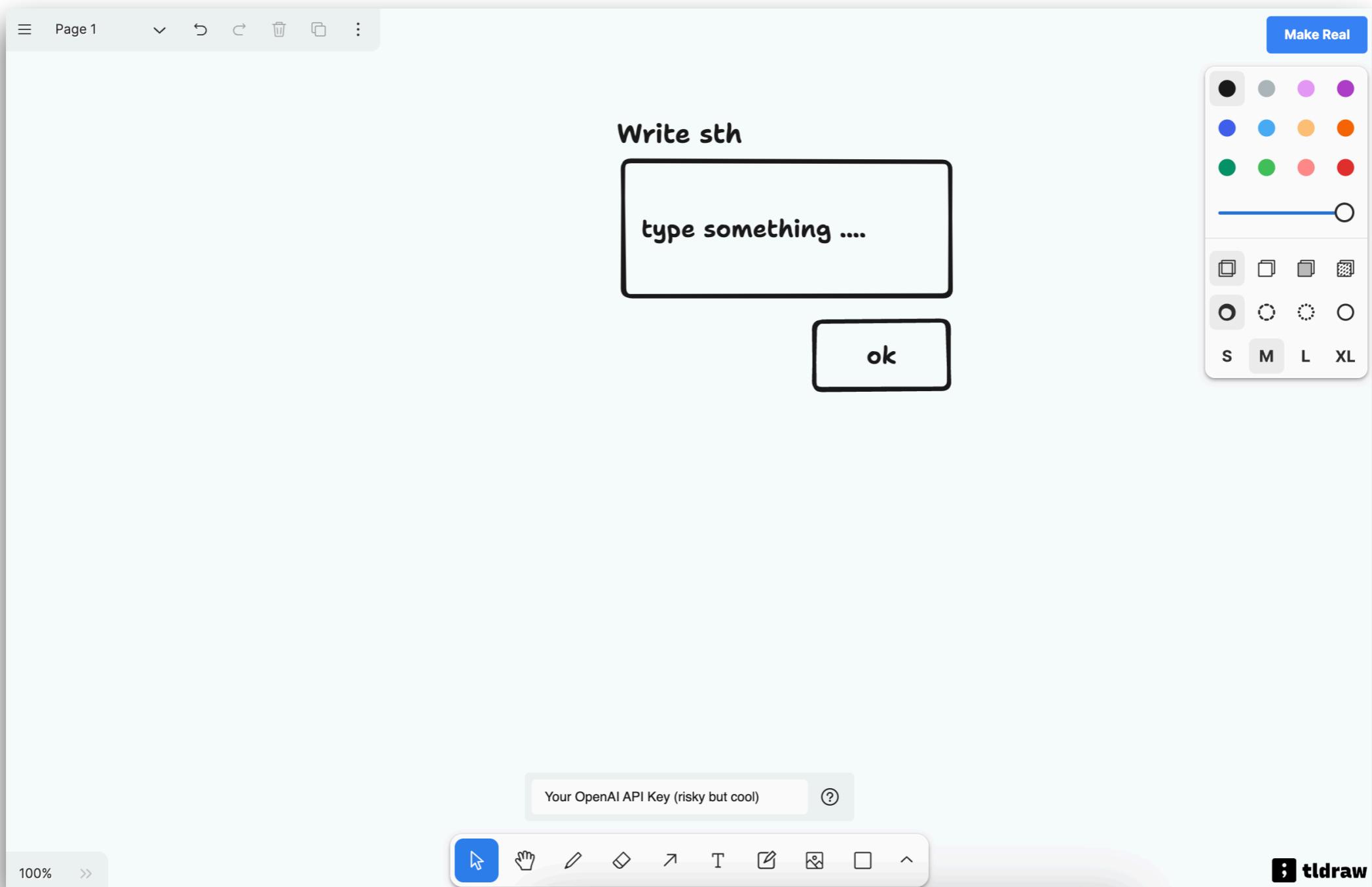
<https://userstorygenerator.ai/>



# Development



# Make Real



<https://github.com/tldraw/make-real>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# v0.dev

The screenshot displays the v0.dev platform, which offers a variety of website templates and design features. At the top, there's a navigation bar with a logo, a "Private Beta" button, and a search bar containing the placeholder "A 'report an issue' modal". Below the search bar are four circular buttons labeled "Product categories ↗", "Hero section ↗", "Contact form ↗", and "Ecommerce dashboard ↗". The main content area shows several website wireframes:

- A wireframe for a "Soccer Game" page with two teams and player profiles.
- A "Hero section" for "Enhance Your Education Journey" with a search bar and "Learn More" button.
- A "Monochromatic Site" wireframe with a sidebar and a main content area showing "User Data" for three items.
- A "product tour like appcues" wireframe with a "Welcome to the Product Tour" message and a "Next" button.
- A wireframe for a "Chats" section with a search bar and a user profile.
- A "Products" section wireframe showing a table with columns for Image, Name, Status, Inventory, Vendor, and Actions.
- A "School Dashboard" wireframe with sections for Credit Hours, Payments, and Courses.

Annotations from users are overlaid on the wireframes:

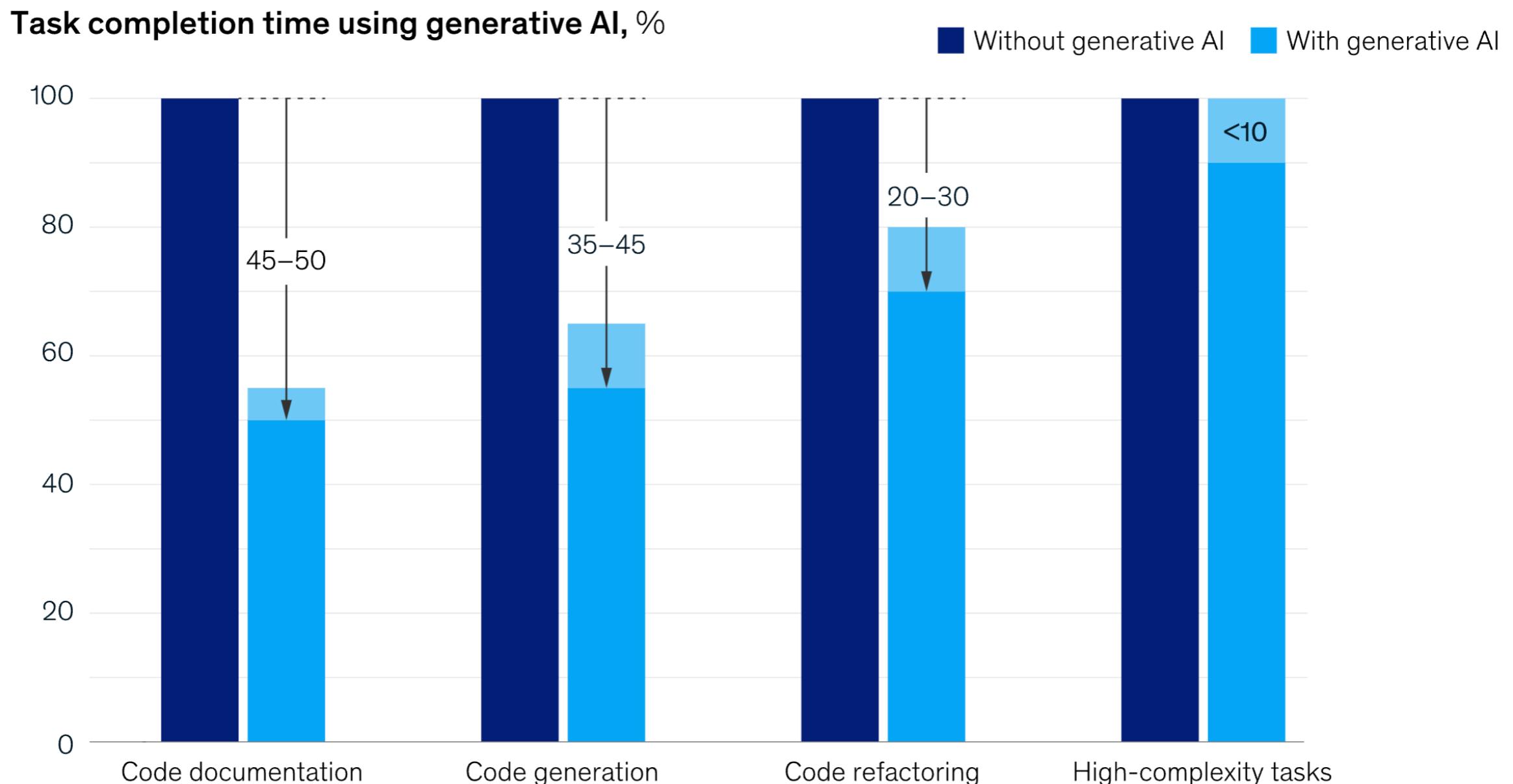
- "page for a soccer game,..." (next to the Soccer Game wireframe)
- "A hero section for a..." (next to the Hero section wireframe)
- "A website in a black and..." (next to the Monochromatic Site wireframe)
- "product tour like appcues" (next to the product tour wireframe)

<https://v0.dev/>



# Development

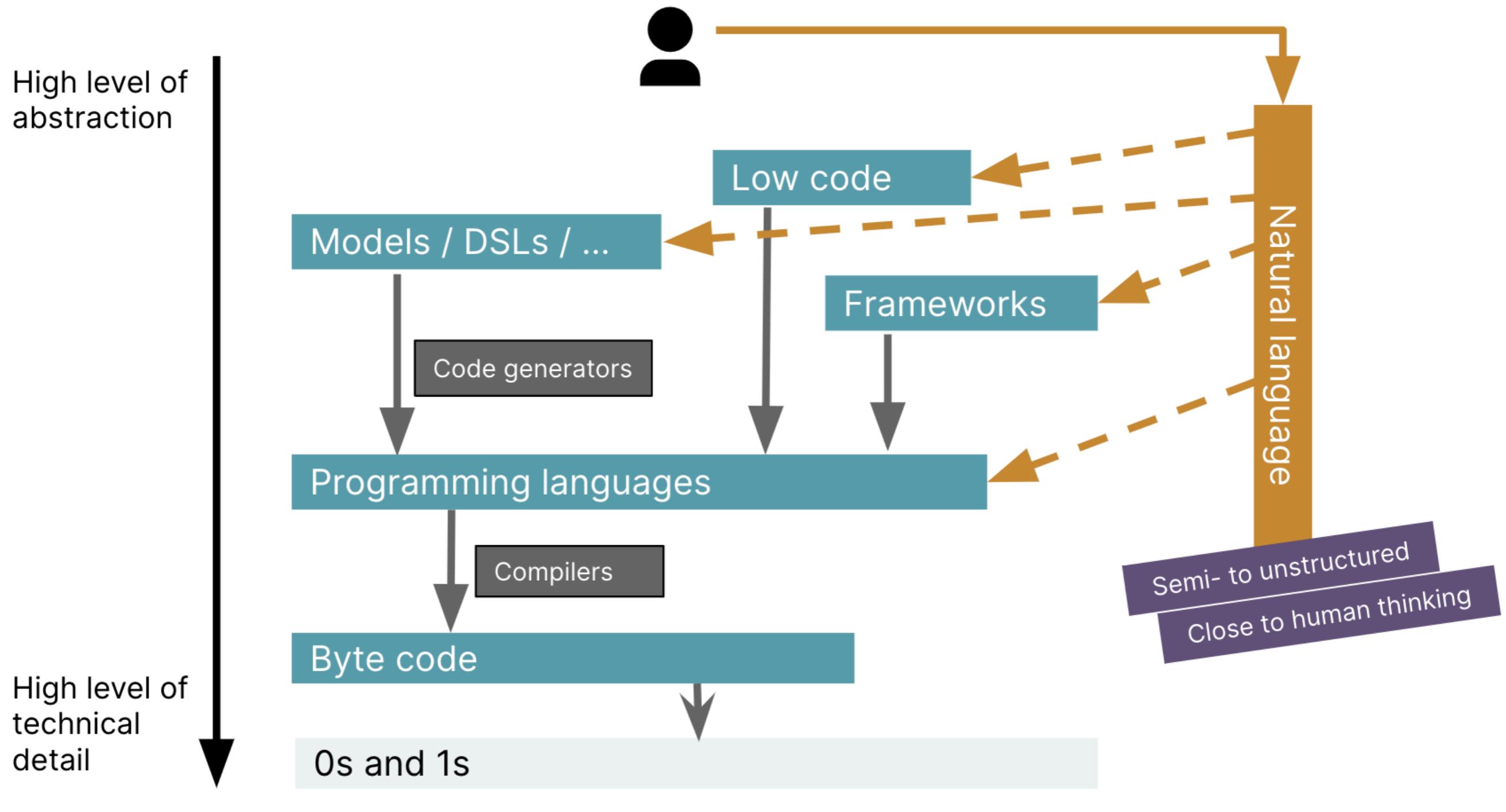
**Generative AI can increase developer speed, but less so for complex tasks.**



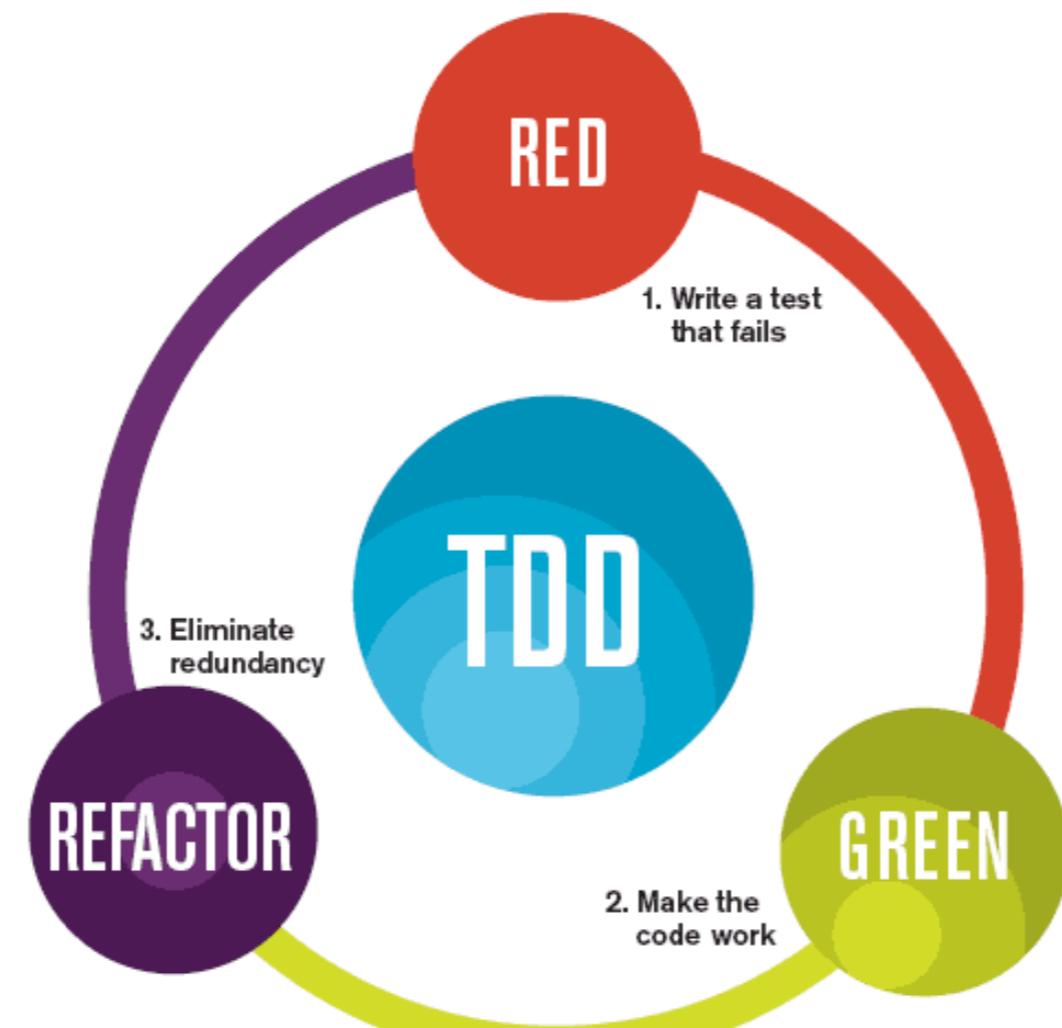
<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/unleashing-developer-productivity-with-generative-ai>



# Development



# TDD



# Tips

Understand what you want

Modular approach

Clear and Precise inputs

Make sure you understand the code

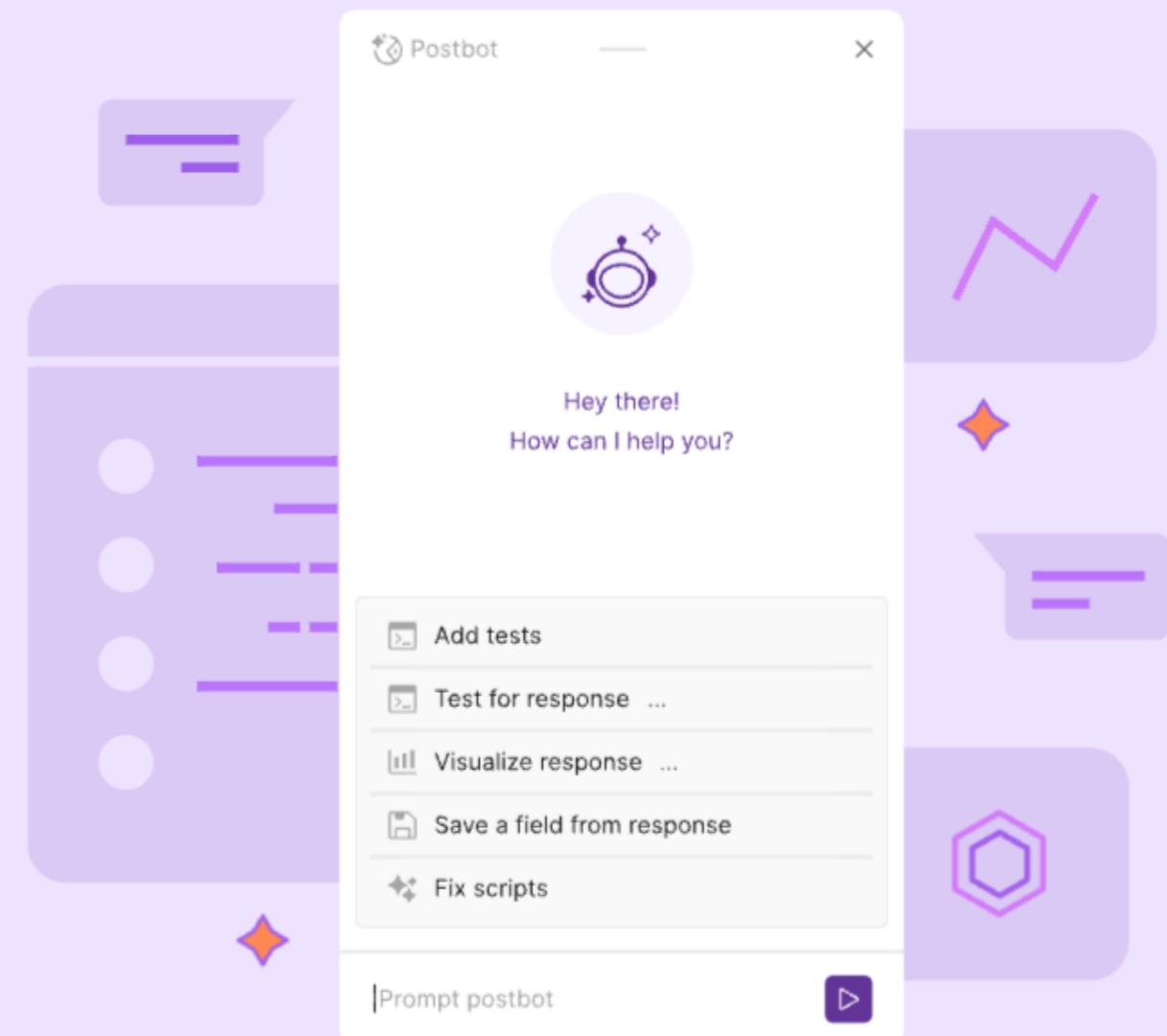


# Testing with Postman

**Postbot, our AI-powered assistant, will supercharge your API development.**

Speed up your most common API development workflows with natural-language input, conversational interactions, and contextual suggestions.

[Get Started](#)



<https://www.postman.com/product/postbot/>



© 2020 - 2023 Siam Chamnkit Company Limited. All rights reserved.

Sharing

40

# PostBot

The screenshot shows the Postman application interface. At the top, there's a header bar with a save icon, a dropdown menu, and a red pencil icon. Below the header, a modal window titled "Postbot" is displayed, containing a "New on Postbot" section with text about auto-complete tests and a "Hi! How can I help?" input field.

The main workspace shows a "New Request" screen for a GET request to <https://jsonplaceholder.typicode.com/users/1>. The "Tests" tab is selected. The response body is displayed in a "Pretty" JSON format:

```
1 {  
2   "id": 1,  
3   "name": "Leanne Graham",  
4   "username": "Bret",  
5   "email": "Sincere@april.biz",  
6   "address": {  
7     "street": "Kulas Light",  
8     "suite": "Apt. 556".  
9   }  
10 }
```

Below the response, there are tabs for Body, Cookies, Headers (25), and Test Results. The Headers tab is selected. The status bar at the bottom shows "200 OK".

<https://www.postman.com/product/postbot/>



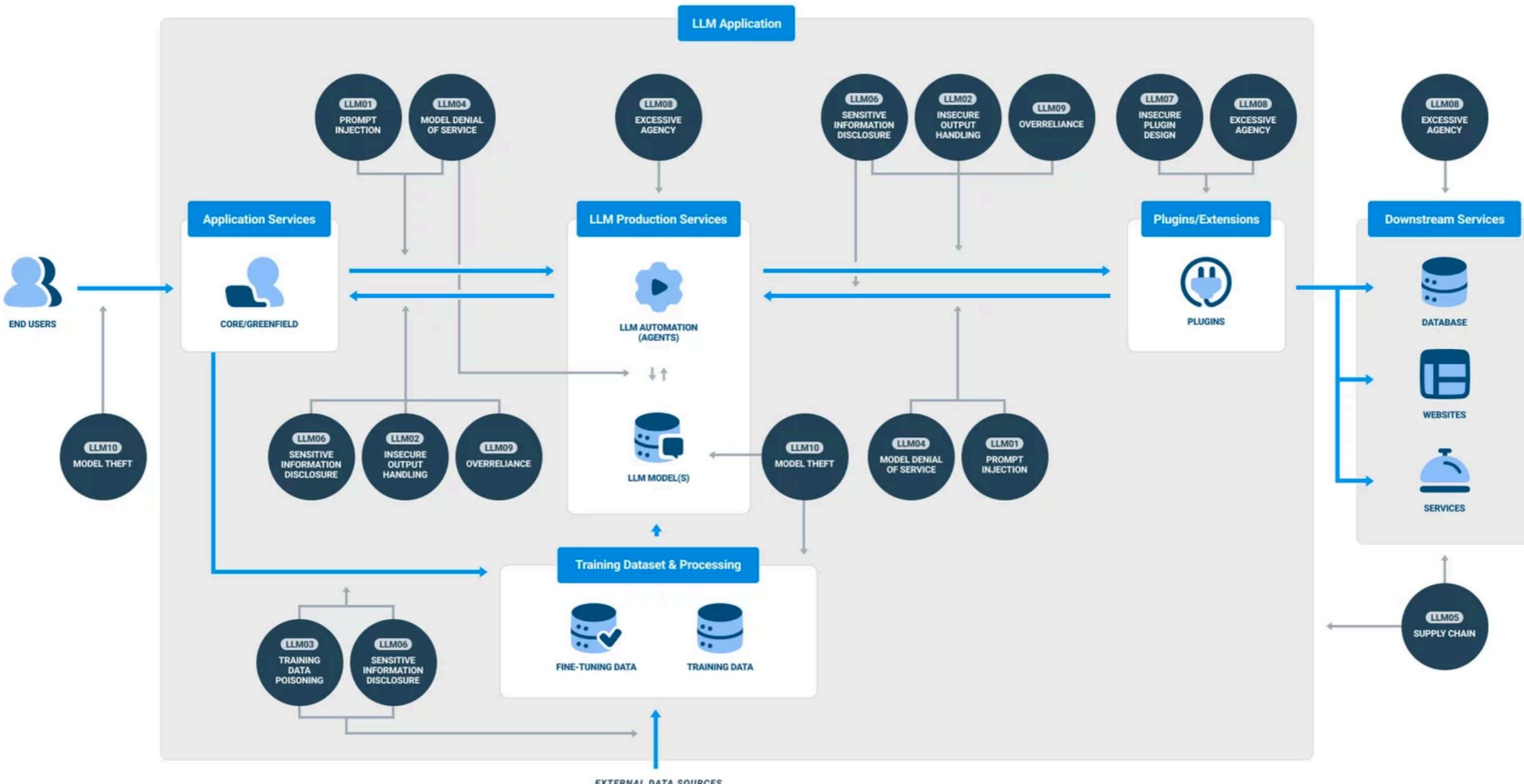
Sharing

© 2020 - 2023 Siam Chamnkit Company Limited. All rights reserved.

# **Security !!**



# OWASP Top 10 for LLM app



<https://llmtop10.com/>



Sharing

© 2020 - 2023 Siam Chamnkit Company Limited. All rights reserved.

# OWASP Top 10 for LLM app

LLM01

## Prompt Injection

Crafty inputs can manipulate a Large Language Model, causing unintended actions. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.

LLM02

## Insecure Output Handling

This vulnerability occurs when an LLM output is accepted without scrutiny, exposing backend systems. Misuse may lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.

LLM03

## Training Data Poisoning

This occurs when LLM training data is tampered, introducing vulnerabilities or biases that compromise security, effectiveness, or ethical behavior. Sources include Common Crawl, WebText, OpenWebText, & books.

LLM04

## Model Denial of Service

Attackers cause resource-heavy operations on Large Language Models leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.

LLM05

## Supply Chain Vulnerabilities

LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. Using third-party datasets, pre-trained models, and plugins can add vulnerabilities.

LLM06

## Sensitive Information Disclosure

LLM's may reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. It's crucial to implement data sanitization and strict user policies to mitigate this.

<https://llmtop10.com/>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# OWASP Top 10 for LLM app

LLM07

## Insecure Plugin Design

LLM plugins can have insecure inputs and insufficient access control. This lack of application control makes them easier to exploit and can result in consequences like remote code execution.

LLM08

## Excessive Agency

LLM-based systems may undertake actions leading to unintended consequences. The issue arises from excessive functionality, permissions, or autonomy granted to the LLM-based systems.

LLM09

## Overreliance

Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, legal issues, and security vulnerabilities due to incorrect or inappropriate content generated by LLMs.

LLM10

## Model Theft

This involves unauthorized access, copying, or exfiltration of proprietary LLM models. The impact includes economic losses, compromised competitive advantage, and potential access to sensitive information.

<https://llmtop10.com/>



Sharing

© 2020 - 2023 Siam Chamnankit Company Limited. All rights reserved.

# Q/A

