

Werkgroep Testen en AI

werkgroepenavond november 2023

Inhoud

Wie zijn wij / Wat hebben we tot nu toe gedaan

Generatieve AI

Vraag en antwoord

Inschatting van ChatGPT versus echte vragen en antwoorden

Wie wij zijn en wat we gedaan hebben

Sinds 2018

[Whitepaper Testen met AI](#) (2019)

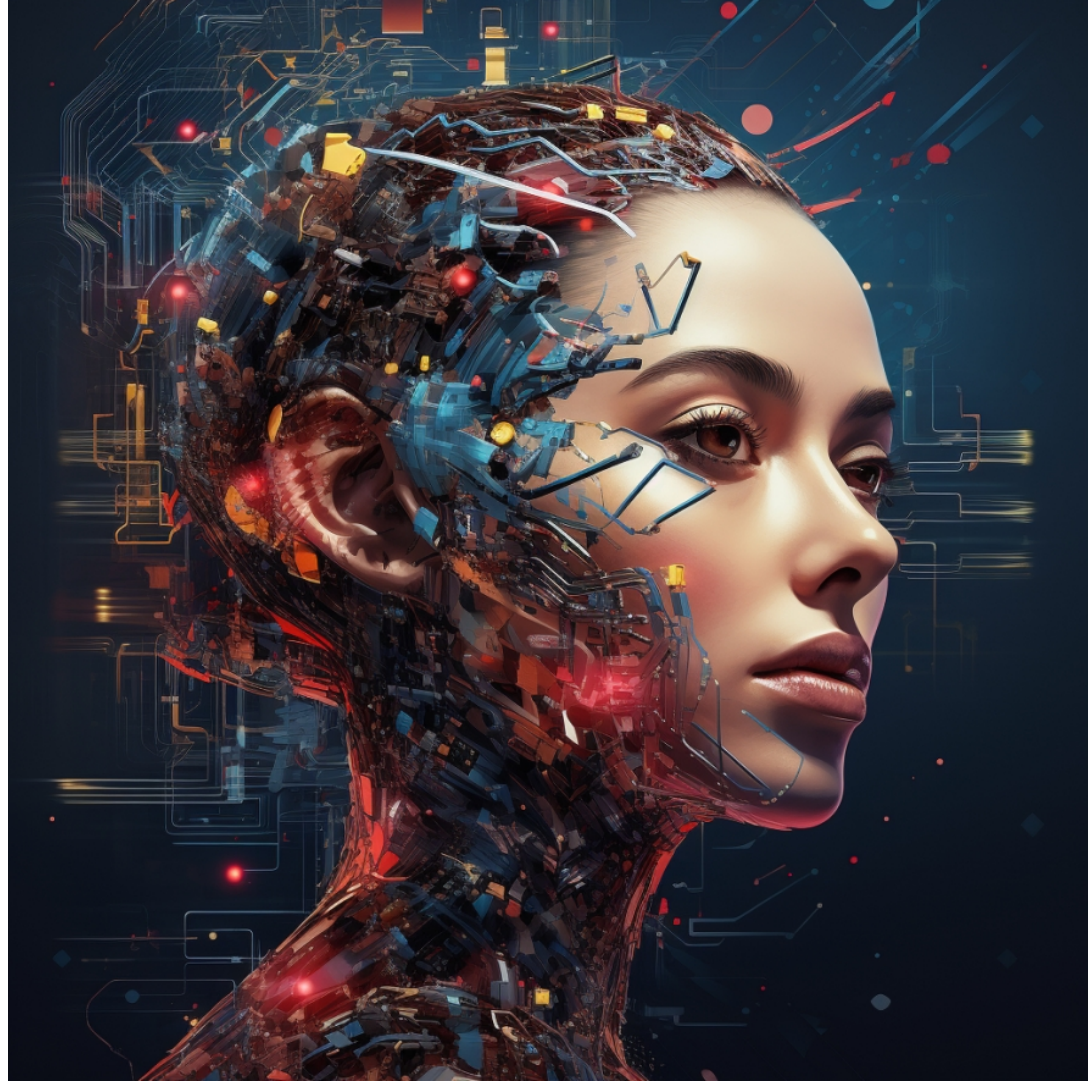
[Whitepaper Testen van AI](#) (2021)

Presentaties bij TestNet en EuroSTAR

Alles staat op de [TestNet site](#)!



Generatieve AI



Generatieve AI

Kwam op toen onze werkgroep begon.

Heeft enorme stappen gemaakt!

A small bird with a black head and wings and features grey wings



256x256
Stage-I GAN
without CA

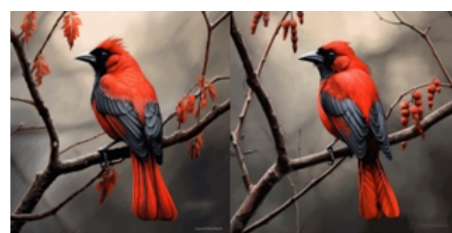
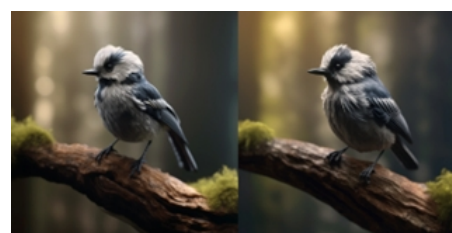
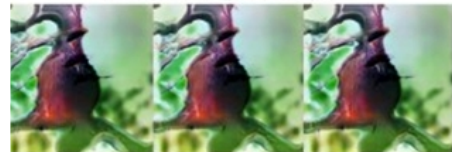
256x256
Stage-I GAN
with CA



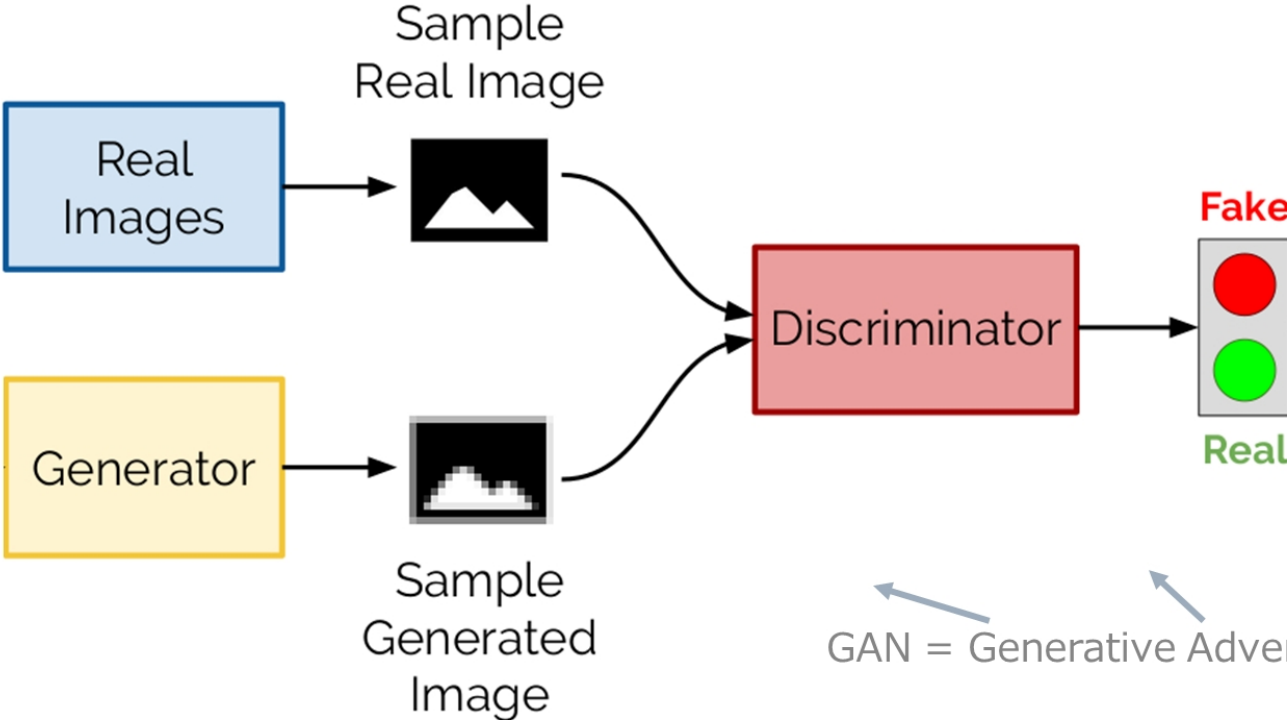
256x256
StackGAN
with CA,
Text twice



This bird is completely red with black wings and pointy beak



Generative Adversarial Networks (GAN)

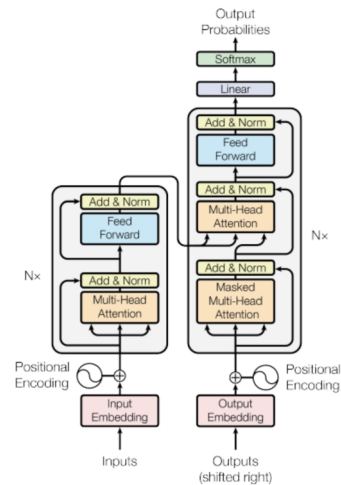
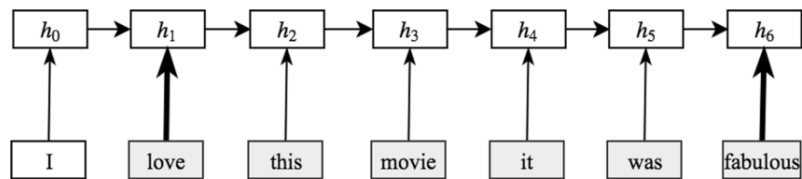


Large Language Models

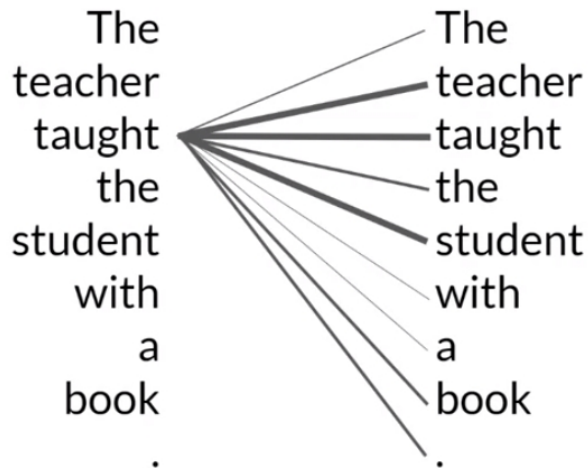
Van Recurrent
Neural Networks (RNN)

naar

Transformers, zoals de
Generative Pretrained
Transformer (GPT)

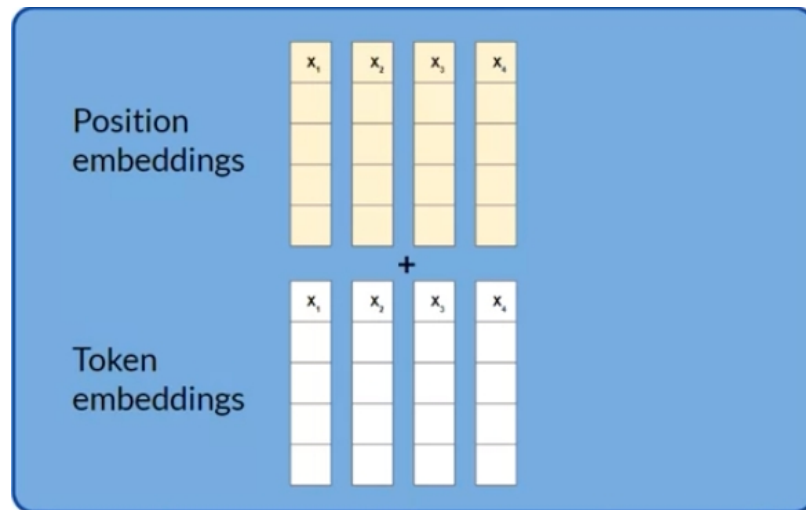


Attentie!



Attention map

Welk woord hoort ná het voorgaande woord?

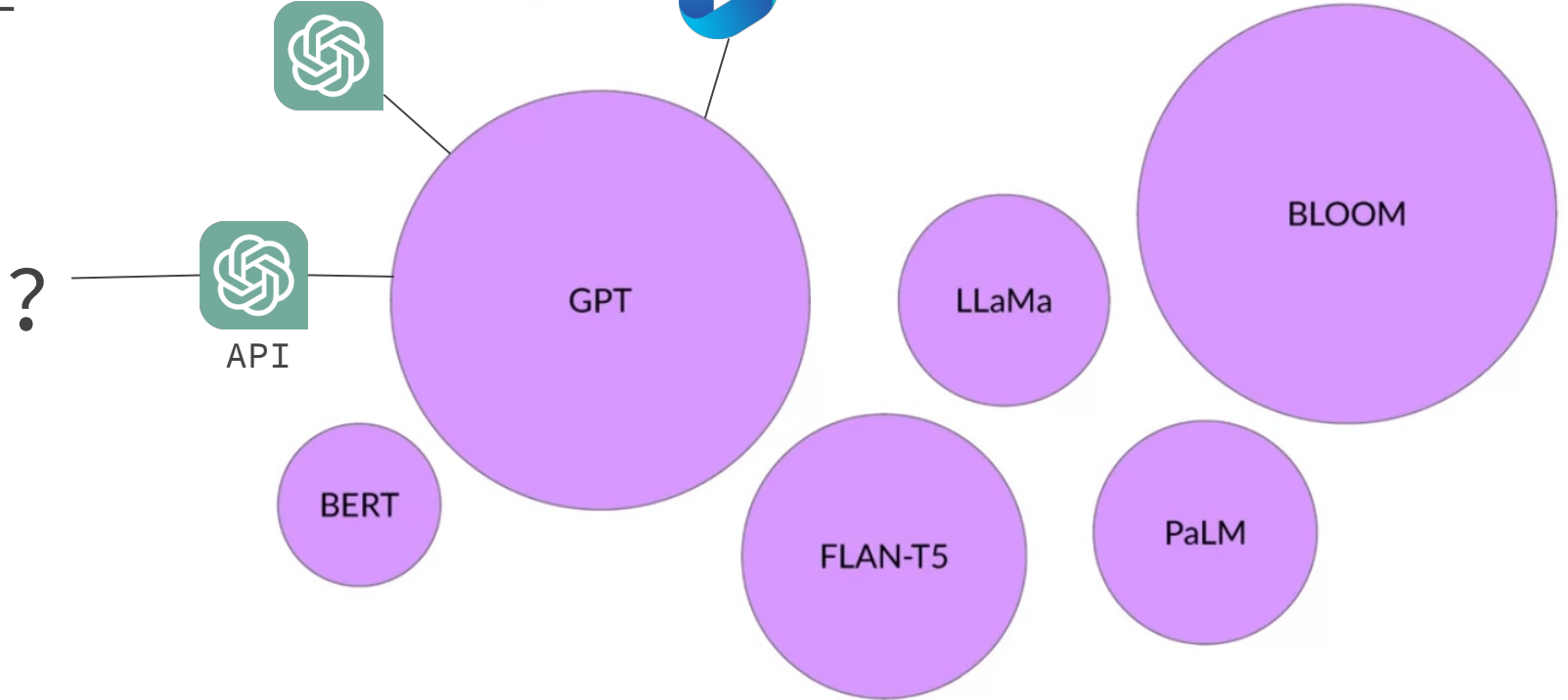


Welk woord is inhoudelijk verbonden met alle eerdere woorden? Qua onderwerp, taal, klank, enzovoort.

Genereren

En zo genereert het de tekst. Woord voor woord.

Large Language Models



Large Language Models

Prompt: de ingevoerde opdracht in een LLM

Inference: het genereren van uitvoer door een LLM

Context window: de meegenomen gegevens voor de inferentie

Completion: de uitvoer uit een LLM

Tokens: (delen van) woorden omzetten naar token-cijfers

Zero-shot, one-shot, few-shot: aantal voorbeelden in prompt

Multi-modal: tekst, beeld, video, geluid, aansturing robots

Bias



MidJourney 5.2



Nurses

Dall-E 3



Builders



Wat kun je zoal ermee doen

Notuleren (live tijdens je gesprek)

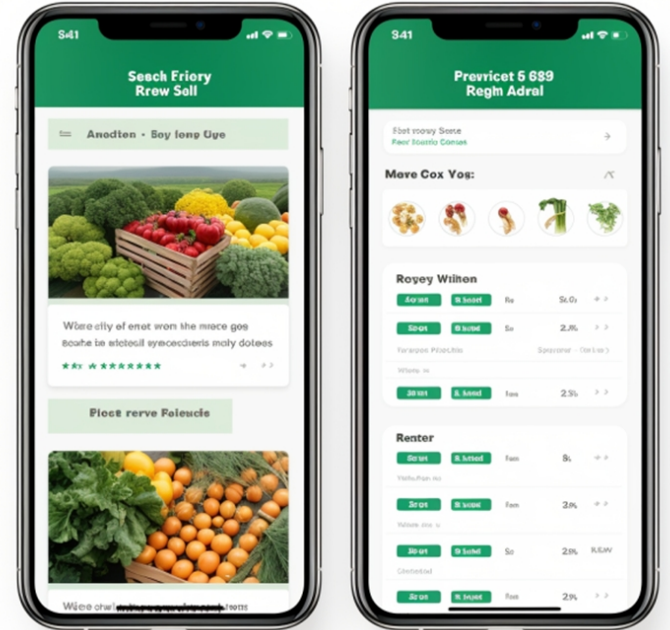
Samenvatten (ook van meerdere teksten)

Ideeën genereren (beeld en tekst)

Log-analyses

Bevindingen uitwerken

Testgevallen genereren



Generatieve AI

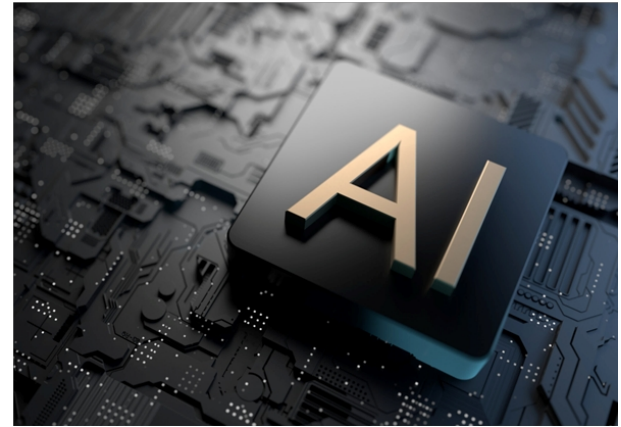
We kregen machines, ...



... we kregen digitalisering ...



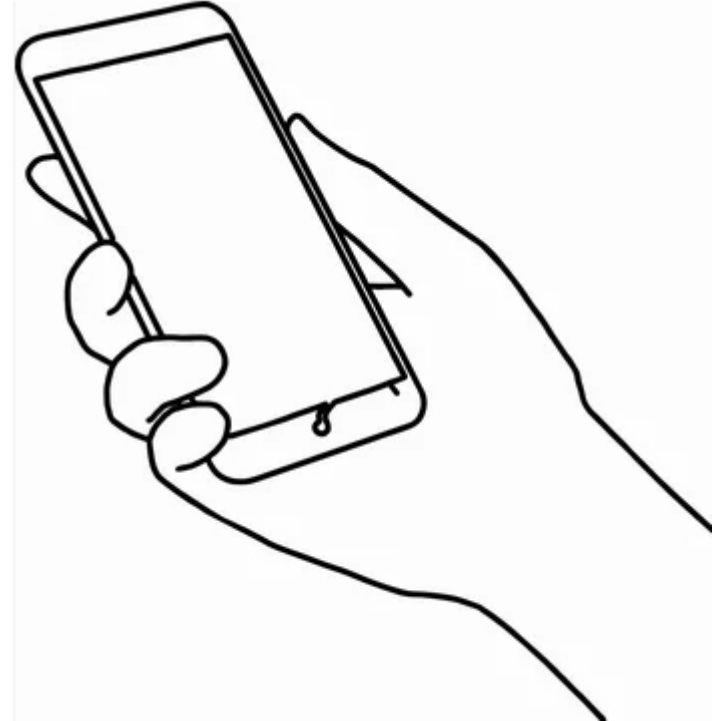
... en nu krijgen we AI.



Vraag maar raak

website: <https://www.mentimeter.com>

code:



Vraag aan ChatGPT (GPT 3.5)

Er gaat een presentatie over generatieve ai gegeven worden aan software te

Er zal veel ruimte zijn om vragen te stellen.

Welke vragen zullen deze software testers gaan stellen over generatieve ai?

Kun je de 10 belangrijkste vragen opschrijven?



Antwoord

1. Hoe werkt generatieve AI in eenvoudige bewoordingen?
2. Wat zijn enkele populaire generatieve AI-modellen en frameworks?
3. Hoe kunnen generatieve AI-modellen worden getraind en geëvalueerd?
4. Wat zijn de mogelijke toepassingen van generatieve AI in softwareontwikkeling en -testen?
5. Wat zijn de uitdagingen en beperkingen van generatieve AI?
6. Hoe kunnen we de kwaliteit en betrouwbaarheid van generatieve AI-modellen verifiëren?
7. Zijn er ethische overwegingen bij het gebruik van generatieve AI in softwaretesten?
8. Hoe kunnen software testers samenwerken met ontwikkelaars bij het gebruik van generatieve AI?
9. Welke specifieke use-cases zijn er voor generatieve AI in testautomatisering?
10. Wat zijn enkele best practices bij het implementeren van generatieve AI in testprocessen?

ChatGPT (GPT 4) Wat zouden softwaretesters willen weten over generatieve AI.

1. Hoe test je de betrouwbaarheid van AI-modellen?
2. Hoe identificeer en mitigeer je bias in AI?
3. Welke kwaliteitsmetrics gebruik je voor generatieve AI?
4. Hoe test je AI in combinatie met traditionele software?
5. Hoe test je AI performance en schaalbaarheid?
6. Hoe waarborg je de veiligheid van generatieve AI?
7. Welke tools automatiseren AI-testen?
8. Hoe test je systemen die continu leren?
9. Hoe verzamel en beheer je AI-testdata?
10. Welke wetgeving beïnvloedt het testen van AI?

Tot ziens

Contact:

ai@testnet.org



Bijlage vragen en antwoorden

1. Hoe werkt generatieve AI in eenvoudige bewoordingen?

Generatieve AI is een vorm van kunstmatige intelligentie die in staat is om nieuwe content, zoals tekst, afbeeldingen of geluid, te genereren op basis van patronen en gegevens die het heeft geleerd. Het maakt gebruik van neurale netwerken en algoritmes om creatief nieuwe informatie te produceren.

2. Wat zijn enkele populaire generatieve AI-modellen en frameworks?

Populaire generatieve AI-modellen en frameworks zijn onder andere GPT-3, GPT-4, OpenAI's DALL-E, Google's BERT, en Tensorflow.

3. Hoe kunnen generatieve AI-modellen worden getraind en geëvalueerd?

Generatieve AI-modellen worden getraind door grote hoeveelheden tekst- of mediagegevens te gebruiken en het model aan te passen om te voorspellen welke informatie er vervolgens moet worden gegenereerd. Evaluatie omvat het meten van de kwaliteit van de gegenereerde resultaten, zoals nauwkeurigheid en cohesie.

Bijlage vragen en antwoorden

4. Wat zijn de mogelijke toepassingen van generatieve AI in softwareontwikkeling en -testen?

Generatieve AI kan worden toegepast in softwareontwikkeling en -testen voor het automatiseren van testcases, genereren van testdata, en het versnellen van het ontwikkelproces door het aanbieden van ontwerpsuggesties en het identificeren van fouten in de code.

5. Wat zijn de uitdagingen en beperkingen van generatieve AI?

Uitdagingen en beperkingen van generatieve AI zijn onder meer het genereren van onjuiste of misleidende informatie, gevoeligheid voor de kwaliteit van de trainingsdata, en de neiging tot het reproduceren van vooroordelen die in de data aanwezig zijn.

6. Hoe kunnen we de kwaliteit en betrouwbaarheid van generatieve AI-modellen verifiëren?

De kwaliteit en betrouwbaarheid van generatieve AI-modellen kunnen worden geverifieerd door middel van evaluatiecriteria zoals nauwkeurigheid, cohesie, en relevantie van gegenereerde inhoud. Ook kunnen menselijke beoordelaars worden ingezet om de kwaliteit te beoordelen.

Bijlage vragen en antwoorden

— — —

7. Zijn er ethische overwegingen bij het gebruik van generatieve AI in softwaretesten?

Ja, er zijn ethische overwegingen bij het gebruik van generatieve AI. Dit omvat zorgen over privacy, de mogelijkheid van bias in gegenereerde content, en de verantwoorde toepassing van de technologie om misbruik te voorkomen.

8. Hoe kunnen software testers samenwerken met ontwikkelaars bij het gebruik van generatieve AI?

Software testers kunnen samenwerken met ontwikkelaars bij het gebruik van generatieve AI door te communiceren over testvereisten, het identificeren van geschikte gebruiksscenario's, en het helpen bij het evalueren en fine-tunen van de AI-modellen voor specifieke testdoeleinden.

9. Welke specifieke use-cases zijn er voor generatieve AI in testautomatisering?

Voorbeelden van use-cases voor generatieve AI in testautomatisering zijn onder andere het automatisch genereren van testdata, het aanmaken van testscripts, het simuleren van randgevallen en het testen van gebruikersinterfaces met automatisch gegenereerde input.

10. Wat zijn enkele best practices bij het implementeren van generatieve AI in testprocessen?

Best practices bij het implementeren van generatieve AI in testprocessen omvatten het definiëren van duidelijke doelen voor automatisering, het zorgvuldig evalueren van de kwaliteit van gegenereerde content, het monitoren van ethische overwegingen, en het regelmatig herzien en bijwerken van de AI-modellen om te blijven voldoen aan de testbehoeften.