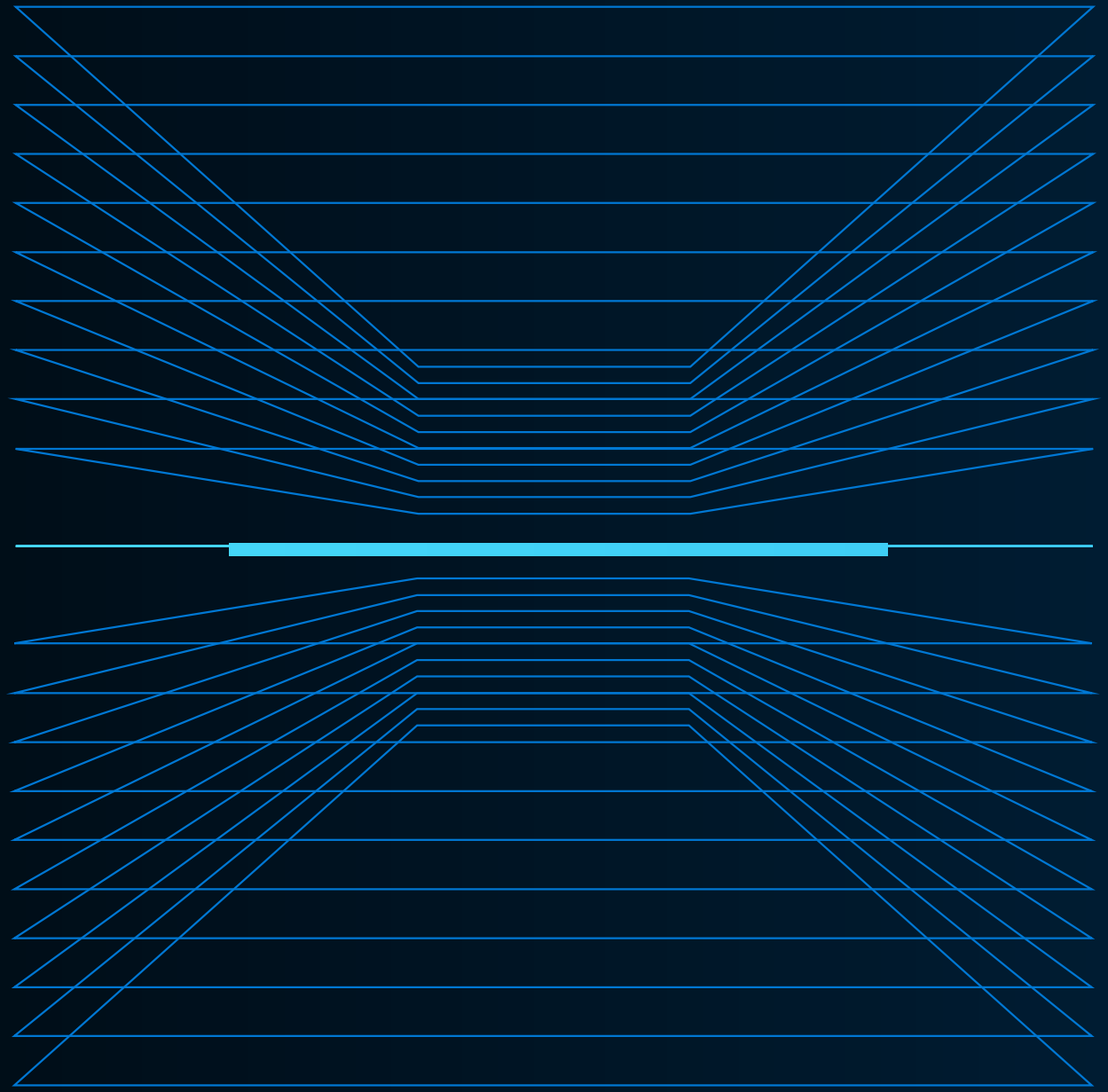
Microsoft

Microsoft + OpenAI

책임있는 AI를 구축하기 위한 Microsoft AI 소개

김형석
Microsoft Data&AI Lead



Microsoft의 Azure OpenAI – ChatGPT (생성형 AI)

Azure

ChatGPT 활용예시) 챗봇, 아바타, 컨택센터 댓글

GPT-3

대형 언어 모델을 기반으로
분류 /생성 / 대화 / 변환 / 요약측면 등의
텍스트와 관련된 기능을 제공합니다.

Codex

코드에 특화된 모델을 기반으로
자연어 기반 코드 생성기능을 제공합니다.
활용 방식은 로우코드 앱 활용지원,
주석의 코드전환, 자연어검색에 대해 SQL
쿼리 작성 등이 있을수있습니다.

DALL·E 2 (Preview)

자연어 기반 이미지 생성 및 제공된
이미지 외의 OutPainting,
inpainting, Styletransfer 기능을
제공합니다.

OpenAI

Azure OpenAI Service

Microsoft

- Azure **구독 내에 배포**하여,준비된 데이터세트 및 앱에 연결
- 새로운 시나리오를 창조할 수 있는 **미리 훈련된 대규모 AI 모델**
- 준비된 데이터 및 hyperparameter로 **fine-tuning된 맞춤형 AI 모델**
- 유해한 사용을 감지하고 완화하는 **책임 있는 AI 내장**
- **RBAC(역할 기반 액세스 제어) , 고객키기반 암호화** 및 사설 네트워크를 통한 **Enterprise급 보안**

Announcement
$10B investment

Microsoft Responsible AI

Microsoft principles

Fairness
AI systems should treat all people fairly

Inclusiveness
AI systems should empower everyone and engage people

Reliability & Safety
AI systems should perform reliably and safely

Transparency
AI systems should be understandable

Privacy & Security
AI systems should be secure and respect privacy

Accountability
People should be accountable for AI systems

Responsible AI Framework

모델의 공정성 보장 | 데이터 보호 | 투명성 제공

모델 해석 가능성 | 인공지능 모델의 공정성 검증

위험최소화

제한적 ACCESS

- 책임감 있는 사용을 촉진
- 예기치 않은 비정상 동작 방지
- 고위험 사용 부정 영향 차단

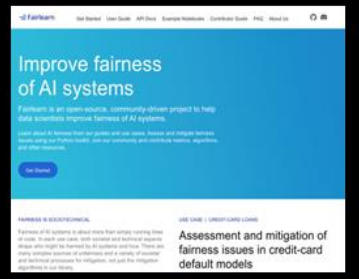
Microsoft Responsible AI

Example

lifecycle Resources

	Guideline	Management Tool	Technology Tool
Responsible assessment	HAX Workbook	AI Fairness Check List	Fairlearn InterpretML Error Analysis Counterfit
Responsible development	Human AI Interaction Guidelines HAX Design Patterns AI Security Guidance Inclusive Design Guidelines Conversational AI guidelines	HAX Playbook	SmartNoise Presidio
Responsible deployment		Dataset Documentation	Confidential computing for ML SEAL Homomorphic Encryption
Toolkits			Responsible AI Toolbox Human AI eXperience (HAX) Toolkit

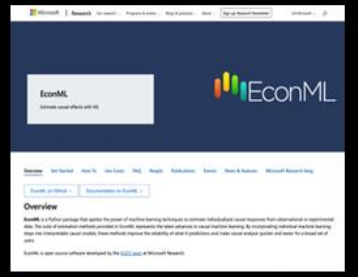
Tools



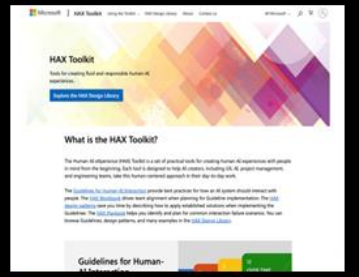
Fairlearn

InterpretML

Error Analysis



EconML



HAX Toolkit

Counterfit

1 사업주관 부서 선정

2 Governance 체계 수립 및 통제

3 비용 및 표준 아키텍처 설계

Example

AI Task

1

External

Call Center고도화 사업 / AICC

Conversational Devices

Internal

Internal Knowledge Chatbot

Responsible AI Controller

2

AI설계 가이드 및 제도수립

사회적 책임 통제

학습 데이터 셋 거버넌스 & 가이드

모니터링

기술 협업

3

Microsoft Azure Consumption Contract

Azure

Microsoft Engineering Support

Microsoft Responsible AI Framework

Legal Consent / Agreement on Investment

생성형 AI에 대한 우려

❑ 생성 AI의 Hallucination 제거 및 답변의 일관성 보장

- ✓ 검색증강생성형모델 (RAG)
- ✓ Prompt Engineering
- ✓ Temperature를 0으로 설정

❑ 안정적인 보안 제공

- ✓ 데이터 Opt Out
- ✓ ExpressRoute를 이용한 Direct 통신
- ✓ Private Endpoint 사용

❑ Enterprise Performance

- ✓ Vector Search를 이용한 검색 성능 향상
- ✓ Vector DB를 Azure상에 구축

Microsoft Cloud
Runs on trust

기업의 데이터는 고객별로 관리	Data is stored encrypted in your Azure subscription
Fine tuning 데이터는 기본 **AI** 모델을 학습하는 데 사용되지 않음	Azure OpenAI Service provisioned in your Azure subscription Model fine tuning stays in your Azure subscription and never moves into the foundation AI models
데이터는 가장 포괄적인 엔터프라이즈 규정 준수 및 보안 제어로 보호	Encrypted with Customer Managed Keys Private Virtual Networks, Role Based Access Control Soc2, ISO, HIPPA, CSA STAR Compliant

ChatGPT를 OpenAI 사용과 Azure 사용의 차이점

Example

Feature	OpenAI	Azure OpenAI
Security & Data Privacy	Basic Security	Enterprise Security, RBAC, Customer-Managed Keys
Compliance	None	SOC2, ISO, HIPAA, CSA STAR
Reliability	No SLA (yet)	Azure SLA, Dedicated Capacity Option (soon)
Responsible AI	Separate Safety Classifier (adds latency)	Built-in, enterprise-grade, low latency moderation and harm prevention
Holistic Solution	Advanced LLM & Image Generation, Basic Speech	OpenAI Models, Complete AI Solution, and a Complete PaaS
Monitoring	None	Azure Monitor, Dashboard, Alert

감사합니다. Q&A