Secure AI with Local LLM’s

Out of the hot tub and into the deep end.

Stephen Nelson 4/5/2024

README.MD

pinpoint01:~ snelson$ whoami

- Technology Enthusiast
- Security Professional (CISSP/GSEC/GPEN/yada/yada)
- Well traveled homebody
- Football (soccer) fan
- Entrepreneur (https://www.pinpointsecurity.io/)

Shall we play a game?

A
14
15
16
17

Introduction to LLM

Definitions

- IBM
- Wikipedia
- Nvidia

Large language models (LLMs) — are a category of foundation models trained on immense amounts of data making them capable of ***understanding*** and ***generating*** natural language and other types of content to perform a wide range of tasks.

A large language model (LLM) — is a language model notable for its ability to achieve general-purpose language *generation* and other natural language processing tasks such as *classification*.

Large language models (LLMs) — are deep learning algorithms that can ***recognize***, ***summarize***, translate, predict, and ***generate*** content using very ***large datasets***.

B

Popular Examples

- ChatGPT
- Google Gemini
- Copilot

C

Benefits

- NLU - Natural Language Understanding
- NLG - Natural Language Generation
- Text Analysis and Processing

D

Security Concerns

- Data Privacy
- Model Bias and Fairness
- Model Opacity
- Provider Dependency/Censorship

What about Local LLM’s?

How is it even possible?

- Continued investment/increased power of GPU/Specialized silicon
- Big tech making models freely available
- Mobile use cases continue to drive innovation
- Data privacy and security benefits

E

What we are going to do?

Run a local LLM with RAG - Retrieval Augmented Generation

- Platforms
  - LMStudio with AnythingLLM
  - PrivateGPT with Ollama
- Models
  - Mistral
  - Llama2
  - WhiteRabbitNeo

F

SETUP TIME

NO WHAMIES, NO WHAMIES

Use Cases

- Report Analysis
- **Report Generation
- **Phishing Email Analysis
- What script do we want it to write?

DEMO TIME

NO WHAMMIES, NO WHAMMIES

FIN QA

- stephen@pinpointsecurity.io
- https://www.pinpointsecurity.io/
- https://www.linkedin.com/in/stephen-nelson-pinpoint/
- https://github.com/sdanelson/BSidesOK2024

Sources and Shout Outs

- Private AI - Network Chuck - YT - @NetworkChuck
  - https://www.youtube.com/watch?v=WxYC9-hBM_g
- Run local AI Chatbot - Hanselman - YT @shanselman
  - https://www.youtube.com/watch?v=_AxXtXwdZmY
- LMStudio and AnythingLLM - Tim Carambat - YT @TimCarambat
  - https://www.youtube.com/watch?v=-Rs8-M-xBFI
- Installing PrivateGPT on WSL with GPU support - Emilien Lancelot
  - https://dev.to/docteurrs/installing-privategpt-on-wsl-with-gpu-support-1m2a