# [Day 4] Unit 4: "Domain Specific LLMs"

**Solving domain Specific Problems using LLMs**

- SecLM: offers solution (ai assist.) @ every layer
- Cyber security pressures: constant emergence of attacks, grunt work (operational toil), talent shortage.
  - * manual tasks can be automated
- Challenges: limited data to train on.

**Creating secLMs**

- Targeted training approach, needs multi-lang cap, cyber sec. training, supervised fine tuning
- Evaluation: compare output to experts answers
  - *human evals play cnt. role.
- in-context learning: app built, train model how to use platform.
- RAG: allows model to get current info
- Flexible & planning framework: planning & exec of complex tasks
- Goal: central platform to transform Cyb. security & save time

**Med LM**

- LLMs can understand & apply med. concepts
- Ways to be used.
  - patients getting tailored responses
  - understanding & categorizing urgency.
  - personalized patient experience.
  - provide real-time feedback.
  - Up to-date knowledge.

**Med PaLM 2**

- Emphasis on safe practices - abs. sure safe & effect.
- first ai to pass med. license exams.
- quantity vs. quality, carefully validated
- Multi-modal generations
- ensemb
- Trained: using med Q&A data
  - few shot, chain of thought, refinement
  - * ensemble refinement: learns from itself, reasoning & answer

**[Codelabs] Fine tuning a custom model**

- Fine tuning can be used from classic NLP to stylized gen.
- Available fine tuning model: Tuned.models.create.
- Download dataset → Prepare data (pre-processing) → apply preprocessing to training & data sets → Sample data → evaluate

The a custom model

- calling fit() specify model training hyperparam.
  - epoch_count: how many times to loop through data
  - batch_size: how many rows to process in a single step
  - learning_rate: defines the scaling factor for updating model weights @ each step.

Google Search Grounding w/ Gemini

- When search grounding is used, model returns extra metadata that includes links & search suggestions.
  Supp. docs & info on how supp. doc was used
- Grounding supports in metadata provide a way to correlate grounding chunks used in the generated output text.
- Search w/ tools

[LinkedIn]

- Effective strategies for specializing LLM's: best method is task to task basis, look @ similar problems
  * experiment!
- Fine-tuning issues: worst case = too far, can only do specific task.
  * important to have thorough eval.
    - does is task in distribution of model?
      - paper: "reversal curse"
- Challenges in SecLM: conflicting methods to approach security, different data sets for tasks which are sensitive.
  * citations provide confidence.

medium: emphasis on governance.

- Tradeoff of fine-tuning: ↑ fine-tune, ↑ chance to lose memory on other tasks.
- In-context learning very effective.
- Retrieval & caching systems in place.
- Reducing token count can reduce token savings

PopQuiz

- C, D, C, B,