**What to do next for Horizon Scanning**

**1. Enhancing LLM Capabilities**

1.1 Fine-tuning LLMs

* + Objective:
* Improve the instruction following and logical reasoning capabilities of current LLMs.
  + Actions:
* Collect specific datasets that mirror the kinds of reasoning and instruction-based tasks you want the LLM to perform.
* Use these datasets to fine-tune models on tasks that are analogous to detecting weak signals and performing complex scenario analysis.

1.2 Ensemble/Merge Different LLMs

* + Objective:
* Leverage strengths from various models to enhance overall performance.
  + Actions:
* Implement ensemble methods where predictions from multiple models are combined to improve accuracy and reduce bias.
* Explore techniques such as stacking or blending where outputs of various models are inputs to a meta-model that provides final predictions.

1.3 Testing Open Source Models

* + Objective:
* Identify the most effective model for your specific needs.
  + Actions:
* Set up a benchmarking framework to evaluate models like Dolphin-Mistral, Mixtral, and others on tasks critical to your project.
* Regularly integrate and test new models from the open-source community to stay at the cutting edge.

**2. Advanced Data Integration Techniques**

* Objective:
* Enhance the data integration capabilities of current CrewAI beyond existing techniques like RAG and GraphRAG.
* Actions:
* Develop or integrate advanced versions of Retrieval-Augmented Generation (RAG) that better handle time-series data and other complex features relevant to cybersecurity.
* Consider integrating other AI techniques such as transformer models that are pre-trained on time-series forecasting for predicting future trends based on historical data.
* Think of solving those issues: messy real world data(text + image), inaccurate retrieval, complex questions …

**3. Implementation of Weak Signal Detection and Amplification**

* Objective:
* Effectively detect and amplify weak signals to forecast and prepare for future cybersecurity challenges.
* Actions:
* Develop algorithms that can identify subtle patterns and anomalies that might indicate emerging threats or opportunities.
* Use techniques from statistical anomaly detection, machine learning models trained on signal recognition, and natural language understanding to improve detection capabilities.

**4. Scenario Planning and Future Prediction**

* Objective:
* Utilize the identified signals to predict and plan for various future scenarios.
* Actions:
* Implement a scenario planning framework within CrewAI that can use the output from signal detection to generate different future scenarios.
* Develop a simulation environment where potential future scenarios can be tested against different responses to evaluate outcomes and prepare strategic responses.

**5. Enhanced Evaluation of LLMs**

* Objective:
* Reduce the incidence of hallucinations in LLM outputs, where the model generates false or misleading information.
* Actions:
* Develop a validation method that cross-references LLM outputs with verified data sources to flag and correct inaccuracies.
* Implement adversarial testing to routinely challenge the LLM with scenarios designed to induce hallucination, helping to identify and mitigate weak spots in the model.

**6. Integration with AI downloader and OpenCTI**

* Objective:
* Ensure the solutions developed are practical and integrate seamlessly with existing systems.
* Actions:
* Develop APIs and interfaces for easy integration of your AI solutions with existing cybersecurity infrastructure.
* Conduct pilot tests with real users to gather feedback and iteratively improve the system based on user interactions and needs.

Reading materials might be helpful:

SPR: <https://youtu.be/awDkuSwfEQA?si=MPN_8ABg8hNWU7Lv>

Horizon Scanning: <https://youtu.be/1Pd0xSsdCAU?si=hN_dpuL5N_wFIfjE>

<https://youtu.be/UX8fXDqqfRw?si=KNNPlEfWPRBHMzrV>

<https://bmjopen.bmj.com/content/13/9/e073730>

<https://www.andrewvorster.com/innovation-toolkit/horizon-scanning-tips-technologies-innovations-patents-and-startups/>

<https://www.dimensions.ai/resources/horizon-scanning-technology-watch-and-technology-foresight/>

<https://www.dowjones.com/professional/resources/blog/horizon-scanning-early-signals-of-the-future>

<https://www.dcipheranalytics.com/solutions/horizon-scanning>

<https://amplyfi.com/2021/06/24/how-to-do-horizon-scanning-effectively/>

<https://www.sciencedirect.com/science/article/pii/S0040162517300707>

<https://www.ncbi.nlm.nih.gov/books/NBK556423/>

<https://samiconsulting.co.uk/techniques-horizon-scanning/>

WSA: <https://www.sciencedirect.com/science/article/pii/S0016328723001064>

Why Horizon Scanning: prepare for the future (scenario planning)

<https://www.jedox.com/en/resources/ebook-power-of-scenario-planning/>

Text Mining: Document Embeddings

<https://youtu.be/XE1_tPgfxoA?si=Paq7iK41Q3djA19j>

Text Clustering:

<https://youtu.be/iZzo9Oxag68?si=26UfceWFiROG-i_C>

For the other materials such as CrewAI, LLMs, RAG …. Please refer to the corresponding documentations.