Wiem Abbassi

Computer Science Graduate | AI Enthusiast

wiem.abbassi@etudiant-isi.utm.tn +216 20 09 60 70 wiemabbassi wiemabbassi

Experience

Artificial Intelligence Engineer *Feb 2025 – May 2025*
RFC

- Designed and deployed a RAG-based solution integrated with Microsoft Sentinel to automate incident investigation and enrich security alerts using threat intelligence sources (OTX, Maltiverse)
- Evaluated multiple LLMs on a cybersecurity query dataset and selected the optimal model for generating threat analysis and remediation recommendations
- Developed an automated SOAR playbook that orchestrates incident enrichment, analysis, and response workflows, improving investigation efficiency and scalability

Business Intelligence Analyst *Aug 2024 (1 Month)*
MAVISION

- Cleaned and pre-processed raw datasets to ensure data quality, consistency and usability for analysis
- Aggregated key data points and implemented relevant metrics to support business insights and decision-making
- Designed and developed interactive dashboards using Microsoft Power BI to effectively communicate findings

Projects

Threat Hunting Query Generator via AI

- Designed and implemented a multi-platform threat-hunting query generator utilizing local LLMs (Ollama) to translate natural language descriptions into syntactically validated queries for Splunk SPL, Microsoft Sentinel KQL and Elasticsearch DSL
- Developed a deterministic query parsing and post-processing engine that programmatically extracts search parameters, corrects time-window mismatches, and automatically aligns query outputs with specific threat hunts
- Integrated the MITRE ATT&CK framework to map threat scenarios to standardized adversary techniques (TTPs) and built an interactive Streamlit dashboard displaying real-time query generation, validation errors, and performance metrics

AI-Based Data Poisoning Detection

- Contributed to the data poisoning detection module of an open source threat intelligence pipeline for SOC and cyber threat analysis workflows
- Developed anomaly detection mechanisms using IsolationForest and LLM-based semantic validation to identify poisoned or contradictory IOC feed data
- Implemented detection logic for threat intelligence inconsistencies including malware incompatibilities, APT sector mismatches, and implausible IOC combinations
- Improved IOC validation reliability before ingestion into MISP analyst queues through automated AI-driven verification and feedback retraining mechanisms

Tunisian Darija Agricultural AI Assistant

- Build a multimodal AI assistant for olive growers, enabling voice-based question answering in Tunisian Arabic (Darija) using a verified agricultural knowledge base
- Designed a CNN-based olive leaf disease classifier and integrated image-based diagnosis with contextual crop management guidance
- Implemented a RAG pipeline with anti-hallucination safeguards, grounding responses exclusively in trusted agricultural sources (FAO, EPPO, CIHEAM)

OWASP Top 10 for LLM Applications

- Explored the OWASP Top 10 vulnerabilities for LLM applications and analyzed their impact on AI-powered systems
- Used LLMGoat to further investigate LLM security vulnerabilities through practical hands-on testing scenarios
- Hosted Mistral 7B locally and performed adversarial testing, including prompt injection attacks, to evaluate model security risks
- Mitigated identified vulnerabilities by implementing input filters, validation rules, and safer prompt-handling mechanisms

Education

Higher Institue of Computer Science (ISI) *Sept 2022 – June 2025*
Bachelor in Computer Science

Skills

AI & Machine Learning: Machine Learning, Deep Learning, NLP, Computer Vision, Reinforcement Learning, Supervised & Unsupervised Learning, Anomaly Detection, Generative AI

LLMs & GenAI: Large Language Models (LLMs), Prompt Engineering, RAG (Retrieval-Augmented Generation), Fine-Tuning, LangChain, LlamaIndex, AI Agents, Multi-Agent Systems

MLOps & Deployment: REST APIs, HuggingFace, Vector Databases (Pinecone, ChromaDB, FAISS), Model Monitoring, Git/GitHub

Programming & Data: Python, Bash, JSON, Automation Scripting, Data Preprocessing, Feature Engineering, Pandas, NumPy

AI Security & Safety: LLM Security, Prompt Injection Defense, Responsible AI, Bias Detection

Certifications

Building LLM Applications With Prompt Engineering Nvidia, April 2026
Claude code in action Anthropic, March 2026
Azure AI Fundamentals Microsoft, November 2024
Python Kaggle, September 2024

Languages

English: Fluent French: Fluent Arabic: Native