Omkar Devalkar

Data Scientist

omkar18devalkar@gmail.com 9082540717

https://github.com/Frag18 www.linkedin.com/in/omkar-devalkar-230335171

Profile

I'm a data scientist with 1.4 year of experience in machine learning, data analysis, and cybersecurity. I specialize in developing baseline models and anomaly detection solutions for SIEM, SOAR, and EDR systems, including signature-less malware detection and process monitoring. Skilled in Python, SQL, Power BI, and Excel, I have also developed production-ready RAG-based LLM chatbots (GPT-3.5 and local OLLAMA/Mistral) for use cases such as alert enrichment, RFP automation, and cybersecurity FAQs. I enjoy uncovering insights from complex datasets and building scalable solutions, and I'm looking for an opportunity to grow and contribute to a team that values data-driven decision-making and innovation in AI-ML field.

Education

BE: Electronic and Tele Communication CGPA 8.59/10
University of Mumbai 07/2020 - 05/2023

Diploma: Information Technology Percentage 84.0/100
Maharashtra State Board of Technical Education 07/2017 - 05/2020

Skills

- **Programming:** Python (Pandas, NumPy, Matplotlib, Scikit-learn)
- **Web Development:** HTML, CSS
- **Data Analysis & ML**: Supervised/Unsupervised Learning, Anomaly Detection, Baseline Modeling, Isolation Forest, DBSCAN, KNN, Autoencoders, LSTM, HMM,PCA
- **Visualization:** Power BI (DAX, Dashboards), Advanced Excel (Pivot, VLOOKUP, HLOOKUP, Conditional Formatting)
- **Databases & Tools:** Elasticsearch, HEDI SQL, Embedded Databases, ChromaDB, GPT-3.5, OLLAMA/Mistral (LLM & RAG Chatbots)

Experience

Velox Solution Pvt Ltd **May 2024 - Present**

Data Scientist – Cyber Security (SIEM / SOAR / EDR / RAG-based AI Chatbot)

- Designed and implemented UEBA (User and Entity Behavior Analytics) baseline models for SIEM and SOAR platforms to detect brute-force, zero-day, and slow attacks using machine learning (Isolation Forest, DBSCAN, KNN, LSTM).
- Built real-time anomaly detection pipelines leveraging Elasticsearch for scalable log ingestion, query optimization, and continuous learning of user behavior patterns.
- Developed signature-less malware detection and process monitoring capabilities for EDR by applying baseline models with Autoencoders, LSTM, HMM and Isolation Forest algorithms on real-time process data.
- Built a correlation-based alerting module that increased detection precision by combining user activity patterns, process behavior, and network telemetry.
- Developed a scalable RAG-based LLM chatbot (Graph-RAG architecture) using ChromaDB as a vector database compatible both with GPT-3.5 and local OLLAMA/Mistral models.
- Implemented multi-schema support and a plug-and-play framework that enables the chatbot to dynamically adapt to multiple cybersecurity use cases (alert enrichment, RFP generation, internal FAQ assistance, and global alert retrospection).
- Integrated the chatbot into the SIEM application to improve analyst productivity by automatically enriching alerts using correlated historical context.

Internship

Clear Secured Services Pvt Ltd

- As a software intern, I contributed to the development of an ATM Security Management System, gaining valuable insights into the intricacies of ATM monitoring.
- My responsibilities included understanding and enhancing the system's functionality, ensuring the secure operation of ATMs. I collaborated with a dynamic team, learning key aspects of ATM security protocols and contributing to the optimization of monitoring processes.
- This internship equipped me with hands-on experience in software development for critical financial infrastructure, enhancing my skills in security-focused programming and systems management.

Exposys Data Labs

- During my internship, I contributed to a project utilizing Python for bulk email automation. The system facilitated efficient communication between senders and subscribers, streamlining the notification process.
- My responsibilities included developing Python scripts, optimizing email transmission, and collaborating on a subscriber notification system.
- This experience enhanced my skills in automation, system optimization, and collaborative development within a practical project context.