Dear Hiring Manager,

I am excited to apply for the position Offensive AI Security Engineer – Red Team at Lucid Motors. With my background in Software and Information systems, extensive experience in the software development industry, and academic research, I believe that I possess the skill set and passion to make valuable contributions to your team. My research endeavors have centered on developing a distributed security analytics for distributed threat hunting and automated extraction of measures and metrics for the assessment of the Center for Internet Security's (CIS) critical security control (CSC) enforcement. My work focuses on developing automated measures and metrics generation approach for security controls, and delivering monitoring intrusiveness, reducing communication overhead among agents, and enabling local decision-making while maintaining high accuracy and timely detection of attacks and attack techniques.

While at UNC Charlotte, I was also a core research member in developing specifications to assess CIS CSC enforcement. This project aimed to determine what to measure (observables), how to measure (tools required), and metrics to evaluate the enforcement of CSCs. I used prompt engineering (Zero-shot prompting, Few-shot prompting, Chain-of-Thought, Tree-of-Though) with LLM (ChatGPT, LLaMA) to extract that information from the CIS CSC guidelines. Later, the CIS reviewed and published our proposed approach as guidelines for the industry to assess CSCs. I also published my works at HOTSOS 2018 and ACM SACMAT 2024 as a novel way to develop automated measures and metrics for CIS CSC assessment.

While an independent contributor at Data Annotation Tech, I worked on generating and verifying responses from different LLMs (Gemini, ChatGPT, custom LLM) on the axis of truthfulness, instruction following, and safety guidance compliance. My task is to verify LLM responses by running LLM-generated codes (Python and C++) and fact-checking for truthfulness. Another task I worked on closely was developing different prompt templates for various tasks. One another axis I had to rate across is the harmfulness of the generated code. My task here is to determine whether LLM is generating code containing vulnerability or unsafe in any other way.

During my tenure as a Research Assistant at UNC Charlotte, I was a member of the project TTPdrill, whose goal is to convert threat reports into actionable knowledge. This involved mapping threat actions to adversary TTPs such as those provided by MITRE ATT&CK Framework. To generate the mapping, we used TF-IDF similarity measures. However, before performing similarity measures among CTI reports and adversary TTPs, one has to extract relevant informants from the CTI reports. In this extraction part, I was actively involved in defining the information (threat actor, threat action, threat object, the tools used by the adversary, and the adversary's intent) to extract from the CTI reports using Java, CoreNLP and AllenNLP. Following the extracted TTPs from CTI reports, I started two separate projects about techniques to attack mining pools and detect such attacks by analyzing System Call logs collected through Symbolic Execution of System Calls and developing distributed hierarchical monitoring agent architecture for automated threat hunting. In the monitoring architecture development, I solved the problem of optimal hierarchy generation using approximation algorithms based on monitoring task similarity and end-host locations. Later, I published our work on this topic in ACSACS 2017, SSPREW-8 2018, ESORICS CBT 2018, and Computing 2023.

I am an expert in programming languages like Python, Java, C++. Additionally, I have expertise in relational (MySQL, Oracle Database, Microsoft SQL Server), non-relational (ElasticSearch, MongoDB), and graph (neo4j) databases. I am proficient in using version control tools such as Git. During my research, I extensively used virtualization tools like VirtualBox, VMWare, and Docker. I am familiar with AWS, Azure, and Scrum/Agile development. I am well-versed in TCP/IP networking, OSI models, Cryptography, and CI/CD. I gained experience in machine learning libraries such as CoreNLP, AllenNLP, NLTK, Scikit-learn, Keras, LLM, LangChain, and TensorFlow while evaluating my research on distributed security analytics and doing coursework. I have worked extensively with OpenSSL, MITRE ATT&CK framework, RabbitMQ, IDAPro, Wireshark, Sysmon, OllyDbg, and Splunk.

As a dedicated researcher with experience in software development, my technical skills, research experience, and problem-solving team to drive innovation and create impactful solutions. Thank you for considering my application.

Sincerely,
Mohiuddin Ahmed