

April 25, 2023

Dear Hiring Manager,

I am excited to apply for the position of Senior Security Engineer, Detection and Response at Coalition. With my Ph.D. in Software and Information Systems and industry experience, I have honed my Cyber Threat Hunting, Malware Analysis, and Machine Learning skills. I am a Graduate Assistant at the University of North Carolina at Charlotte, developing a distributed security analytics system for distributed threat hunting. My research has been funded by DOE and ONR. My work aims to deliver monitoring intrusiveness, reduce communication overhead among agents, and enable local decision-making while maintaining attacks and attack techniques detection accuracy high and in time.

As a Teaching Assistant, I teach, design, and prepare graduate courses in Principles of Information Security and Privacy, Network Infrastructure Security, and Data Mining. Before joining UNC Charlotte as a Ph.D. student, I worked as a Software Engineer and Team Lead at Kona Software Lab Ltd., Dhaka, Bangladesh, developing middleware libraries for PKI and CA systems. I also led a team of three software developers to design and develop NFC-based smart card authentication for Windows OS.

I am well-versed in programming languages like Python, Java, C++, C, and Prolog. Additionally, I have expertise in web development and scripting with Shell Scripting, PHP, JavaScript, HTML5, and SQL. I am proficient in using visualization tools such as UML, Weka, and Gephi and version control tools such as Git. I have experience with virtualization tools like VirtualBox, VMWare, Kubernetes, and Docker, and I am familiar with Scrum/Agile development. I am well-versed in TCP/IP networking, OSI models, CI/CD, OOD, and SOA. I have experience with machine learning libraries such as Stanford CoreNLP, AllenNLP, NLTK, Scikit-learn, Keras, and TensorFlow. I have worked extensively with cryptography, OpenSSL, MITRE ATT&CK framework, TCP/IP, Elasticsearch, RabbitMQ, IDAPro, Sysmon, OllyDbg, and Splunk.

Several research and project experiences make me a strong candidate for this position. I am currently working on AUTO-Hunter, a Distributed Hierarchical Event Monitoring System for Attack Diagnosis through Active Investigation of Attacker Activities. I designed and implemented this system to reduce attack detection time, communication overhead, and resource usage. I also developed low-level log collecting agents for the Windows system (ETW, event logs, Syslog, NetFlow) and detectors to map low-level traces to the MITRE ATT&CK technique and evidential reasoning framework. I have also worked on the Critical Security Control (CSC) Validation project, which involved automated extraction of threat action, observables, and development of key measurement indicators (KMI) and metrics for the KMI of each CSC. Additionally, I worked on TTPDrill, which was an Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources and mapping of threat actions to MITRE ATT&CK techniques. Finally, I developed PKI-Middleware, a PKCS#11 dynamic library that complies with KISA and FIPS standards.

I am excited to bring my skills and experience to your team. I appreciate your consideration.

Sincerely,

Mohiuddin Ahmed

Ph.D. Candidate, Department of Software and Information Systems

UNC Charlotte, NC

(Phone No) +19802670371