As a Ph.D. candidate working on distributed threat hunting, I am excited about the opportunity to join Discord's team to help build a secure and private platform for its users. I am passionate about security and privacy and have a deep sense of curiosity and an endless desire to improve. Discord's mission to create space for people to find belonging aligns with my values, and I believe my skills and expertise in cyber threat hunting, and automation can make a significant contribution to the company. I have strong domain knowledge in security, experience in cloud-based environments, and have contributed code to a fast-moving codebase and deployed artifacts to production. Additionally, I have hands-on experience with the MITRE ATT&CK framework, ElasticSearch, and RabbitMQ, making me a perfect fit for the role. Lastly, Discord's comprehensive benefits package, including flexible long-term work options and paid parental leave, demonstrates the company's commitment to its employees' well-being, which is essential for me.

As a Ph.D. candidate at the University of North Carolina at Charlotte, with extensive industry experience in software engineering and team leadership, I have consistently demonstrated excellence in both research and teaching. My research focuses on developing distributed security analytics for distributed threat hunting, and my work has been funded by the Department of Energy and the Office of Naval Research. I have designed and implemented a distributed hierarchical event monitoring system for attack diagnosis through active investigation of attacker activities, reducing attack detection time, communication overhead, and resource usage. I have also developed low-level log collecting agents for Windows systems and detectors to map low-level traces to the MITRE ATT&CK technique and evidential reasoning framework.

My experience with the MITRE ATT&CK framework, ElasticSearch, and RabbitMQ, along with my knowledge of provenance graph analysis, Bayesian network, NLP, and deep learning, have allowed me to develop automated extraction of threat action, observables, and key measurement indicators for each CSC. I have also developed automatic and accurate extraction of threat actions from unstructured text of CTI sources and mapped threat actions to MITRE ATT&CK techniques. I published multiple papers on different well known venue like ACSAC, HoTSOS.

As a teaching assistant, I have designed and prepared graduate courses in Principles of Information Security and Privacy, Network Infrastructure Security, and Data Mining, and I have designed and graded course assignments and exam questions. My knowledge of programming languages such as Python, Java, C++, and Prolog, as well as web development and scripting languages such as Shell Scripting, PHP, JavaScript, and SQL, and frameworks such as Spring, Laravel, and MODX CMS, have enabled me to teach with expertise and authority.

Overall, my extensive experience in the software engineering industry and my exceptional research and teaching skills demonstrate my dedication to excellence in the field of software and information systems. My expertise in cyber threat hunting, malware analysis, the MITRE ATT&CK framework, critical security controls, Bayesian network, and uncertainty reasoning, coupled with my mastery of programming languages and frameworks, make me an exceptional researcher and software developer.

Dear Hiring Manager,

I am writing to express my interest in the Cybersecurity Analyst position advertised on your website. As an experienced cybersecurity professional with a bachelor’s degree in Computer Science and four years of experience in software development in payment industry, I am confident that I have the skills and qualifications necessary to make an immediate and valuable contribution to your team.

In my current position at UNC Charlotte, I have designed and implemented a distributed hierarchical event monitoring system for attack diagnosis through active investigation of attacker activities, reducing attack detection time, communication overhead, and resource usage. I have also developed low-level log collecting agents for Windows systems and detectors to map low-level traces to the MITRE ATT&CK technique and evidential reasoning framework. My experience with Security Information and Event Management (SIEM) has allowed me to triage, mitigate, and escalate issues as needed while capturing essential details and artifacts.

I possess strong knowledge of malware families and network attack vectors, as well as a solid understanding of TCP/IP and internetworking technology including packet analysis, routing, and network security defenses. In addition, I have experience operating and utilizing Security Information and Event Management tools, and I am familiar with common security tools such as SIEM, AV, IDS, Netflow, Packet Analyzer, and Endpoint Detection & Response tools.

My expertise extends to web applications security vulnerabilities, including cross-site scripting, cross-site request forgery, SQL injection, DoS attacks, and API attacks. I have a good understanding of Web Application Security risks and excellent understanding of DDoS techniques and mitigation mechanisms.

I am familiar with incident response methodologies, and I have direct experience in handling cybersecurity incidents and associated incident response tools. I have excellent communication and presentation skills, with proven ability to present analytical data effectively to varied audiences. I am a problem solver with tenacity and resilience to resolve issues, and I possess strong interpersonal and leadership skills to influence and build credibility as a peer.

I am excited about the opportunity to join Visa, a company whose mission is to connect the world through the most innovative, convenient, reliable, and secure payments network. I am confident that my qualifications and experience make me a perfect fit for this position, and I look forward to the opportunity to contribute to the security posture of your enterprise.

Thank you for your consideration.

Sincerely,