My senior design project focuses on developing a comprehensive process protection system for 64-bit Windows applications, coupled with a web-based monitoring interface. This ambitious undertaking represents the culmination of my computer science education at the University of Cincinnati, allowing me to apply the theoretical knowledge and practical skills I've acquired throughout my undergraduate studies to create a sophisticated security solution. The project aims to create a robust anti-cheat system that goes beyond typical gaming applications, offering protection for any user-selected processes running on Windows machines. This system will employ advanced techniques to prevent unauthorized access, including memory protection, code integrity checks, and prevention of DLL injection and remote thread creation. The web-based monitoring component will provide real-time insights into protected processes and alert users to potential threats, adding a layer of transparency and control to the protection mechanism. By tackling this complex project, I'm excited to delve deeper into areas of cybersecurity and system-level programming, contributing meaningfully to the field while expanding my own expertise. This project aligns perfectly with my interests in computer security and presents an opportunity to address real-world challenges in protecting sensitive software from malicious actors. Through this project, I aim to gain valuable experience in developing low-level system software and creating secure, efficient solutions for modern computing environments.

Throughout my college curriculum, I've gained valuable knowledge that will significantly guide the development of this project. Courses such as CS3003: Programming Languages and CS4071: Design & Analysis of Algorithms have provided me with a solid foundation in software design and optimization techniques. EECE3093C Software Engineering taught me crucial project management and team collaboration skills, which will be essential for coordinating our group efforts. Additionally, EECE4029: Operating Systems and Systems Programming has equipped me with the necessary knowledge to develop kernel-level drivers and interact with low-level system components, which is critical for implementing robust process protection mechanisms. These courses have not only honed my technical skills but also instilled in me a systematic approach to problem-solving, which I expect to apply extensively throughout this project. Furthermore, CS4092 Database Design and Development will be instrumental in designing an efficient backend for our web-based monitoring interface, allowing us to store and retrieve real-time data effectively. Lastly, the AI Principles and Applications course has given me insights into machine learning techniques that could potentially enhance our threat detection capabilities. By combining these academic experiences, I'm confident in my ability to contribute meaningfully to all aspects of the project, from low-level system programming to high-level application design.

My co-op experiences have also played a pivotal role in preparing me for this project. As a Software Development Intern at Siemens Digital Industries Software, I've gained invaluable hands-on experience in architecting high-performance modules and designing microservices architecture. These skills will be crucial in developing an efficient and scalable process protection system. My experience with cross-platform application development will be particularly useful when creating the web-based monitoring interface. Furthermore, my involvement in implementing comprehensive unit testing strategies has taught me the importance of thorough testing, which will be vital in ensuring the reliability and effectiveness of our anti-cheat solution. During my time at Siemens, I've worked on projects that required deep integration with Windows systems, giving me practical experience with Windows internals that will be directly applicable to this project. Additionally, my experience in

redesigning critical UI components using .NET C# & WPF will be beneficial when developing the user interface for our protection system. These practical experiences have complemented my academic knowledge, providing me with a well-rounded skill set that I'm eager to apply to this challenging project.

I am deeply motivated to participate in this project due to its potential impact on computer security and its alignment with my personal interests in cybersecurity. The opportunity to create a sophisticated anti-cheat system that goes beyond typical gaming applications excites me, as it presents a chance to contribute meaningfully to the field of computer security. My preliminary approach to designing a solution involves first conducting a thorough analysis of existing anti-cheat systems and identifying their strengths and weaknesses. Then, I plan to focus on developing the core protection mechanisms, starting with memory protection and DLL injection prevention. Following this, I'll work on integrating these protections with the web-based monitoring interface. Throughout the project, I aim to continuously evaluate and refine our solution based on performance metrics and security testing results. To self-evaluate my contributions, I will track my progress against predefined milestones, conduct regular code reviews, and measure the effectiveness of the implemented protection mechanisms against various attack vectors. I'm particularly excited about the challenge of balancing security measures with system performance, as this aligns closely with my experience in optimizing software at Siemens.

Upon completion of this project, I expect to have developed a robust process protection system capable of preventing unauthorized access to protected processes on Windows machines. Our solution should be able to detect and prevent various cheating techniques, including memory manipulation, code editing, and DLL injection. The web-based monitoring interface should provide real-time insights into protected processes and alert users to potential threats. Success will be measured by the system's ability to thwart common cheating methods without significantly impacting the performance of protected processes. Additionally, the ease of use and integration of the web interface will be crucial indicators of success. By the end of this project, I hope to have not only contributed to the advancement of computer security but also further refined my skills in system-level programming, cybersecurity, and web development. This project represents an exciting challenge that I believe will push me to grow both as a developer and as a problem-solver, ultimately enhancing my readiness for future endeavors in the tech industry. Through this capstone project, I aim to demonstrate my ability to tackle complex, real-world problems and deliver a high-quality solution that showcases my skills and knowledge acquired during my time at the University of Cincinnati.