**Project Title: "Secure Software Lifecycle: Identifying and Mitigating Threats through Continuous Integration and Continuous Deployment (CI/CD) Pipelines"**

**Significance/Contribution to the Discipline/Research Problem:** This research project aims to examine how Continuous Integration and Continuous Deployment (CI/CD) pipelines can be leveraged to enhance the security of the software lifecycle. It will contribute to the discipline by identifying and mitigating threats in real-time, ultimately reducing the number of vulnerabilities in software applications and improving overall cybersecurity.

**Research Question:** How can CI/CD pipelines be utilized to identify and mitigate threats within the software lifecycle effectively, thus enhancing the security of software applications?

**Aims and Objectives:**

1. To investigate the role of CI/CD pipelines in the software lifecycle and their potential impact on security.
2. To identify security risks, threats, and vulnerabilities associated with CI/CD pipelines.
3. To explore best practices and tools for integrating security measures within CI/CD pipelines.
4. To develop and evaluate a set of recommendations for implementing security measures in CI/CD pipelines to mitigate threats in the software lifecycle.

**Key Literature Related to the Project:**

1. Humble, J., & Farley, D. (2010). Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation
2. Kim, G., Debois, P., Willis, J., & Humble, J. (2016). The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations
3. OWASP Top Ten Project [Web, Mobile, Api]
4. Cider Security: Top 10 CI/CD Security Risks
5. NIST Special Publication 800-160: Systems Security Engineering

**Methodology/Development Strategy/Research Design:**

1. Conduct a literature review on CI/CD pipelines, their role in the software lifecycle, and their potential impact on security.
2. Analyze existing CI/CD pipeline implementations, identifying common security risks, threats, and vulnerabilities.
3. Investigate best practices and tools for integrating security measures within CI/CD pipelines, through documentation analysis, case studies, and expert interviews.
4. Develop a set of recommendations for implementing security measures in CI/CD pipelines to mitigate threats.
5. Evaluate the effectiveness of the recommendations through real-world case studies and expert feedback.

**Ethical Considerations and Risk Assessment (as part of your ethical approval application):**

1. Ensure the integrity of data collected from open sources and experts during interviews and case studies.
2. Obtain informed consent from participating organizations and individuals, if any.
3. Address potential conflicts of interest arising from collaborations with industry partners or software development tool providers.
4. Consider the broader societal implications of the research, including potential misuse of CI/CD pipeline security measures to exploit vulnerabilities in competing software products.

**Description of Artefact(s) That Will Be Created (if applicable):**

1. A set of recommendations for implementing security measures in CI/CD pipelines to mitigate threats in the software lifecycle.
2. Evaluation results and case studies showcasing the effectiveness of the recommendations.

**Timeline of Proposed Activities:**

**Possible timelines considering this would be a 6-month ranged project.**

1. Month 1-2: Conduct a literature review on CI/CD pipelines and their impact on software security.
2. Month 3: Analyze existing CI/CD pipeline implementations and identify common security risks, threats, and vulnerabilities.
3. Month 4: Investigate best practices and tools for integrating security measures within CI/CD pipelines.
4. Month 4-5: Develop a set of recommendations for implementing security measures in CI/CD pipelines.
5. Month 5: Evaluate the effectiveness of the recommendations through case studies and expert feedback.
6. Month 6: Prepare the final research report and disseminate findings.