SYSC 4907 – Fall 2026/Winter 2027

Supervisor	Jason Jaskolka
Co-supervisor	
Course section	SYSC 4907 H
Project ID	H4
Project title	BEACON: An Explainable Multi-Agent Framework for Intelligent Event-Driven Cyber Defense
Project description	Are you interested in building intelligent, explainable systems that improve cybersecurity decision-making? Join us in developing *BEACON*, an explainable multi-agent cybersecurity framework in which specialized agents collaborate to monitor, analyze, and respond to system activity in support of intelligent cyber defense strategies. Modern cybersecurity systems generate vast volumes of alerts, often with limited prioritization or explanation, making it difficult for analysts and developers to respond effectively. Beyond detecting anomalies, an important challenge lies in accurately assessing threat severity and providing meaningful context to support timely and informed decisions. *BEACON* is a *multi-year project* aimed at addressing this challenge through a modular, agent-based approach to cyber defense. Within the framework, specialized agents work together to provide monitoring, diagnosis, and response capabilities that improve situational awareness and support cyber defense decision-making. Phase 1 of this project focuses on the design and prototyping of an *intelligent threat diagnosis agent*, a core component of the BEACON framework. This agent will analyze system activities and events (e.g., such as login behavior, process execution, and file access patterns) and assign structured threat levels (e.g., *low, medium, high,* and *critical*). By combining reasoning strategies with lightweight machine learning techniques, the agent will produce accurate and explainable threat assessments that can guide downstream response and forensic processes. The threat diagnosis agent will serve as the central intelligence layer within BEACON, receiving input from monitoring components, evaluating threat severity, and generating interpretable assessments that enhance transparency, usability, and trust in cyber defense decisions. 3 **Project Objectives:** The objectives of Phase 1 are to: 1. Model suspicious system behavior by identifying relevant system events and defining features that characterize potential threats, such as repeated failed logins, unusual access patterns, or privilege escalation. 2. Develop an intelligent diagnosis agent that analyzes incoming events and assigns threat scores and classifications using a

	combination of rule-based reasoning and anomaly detection techniques. 3. Enable explainable threat assessment by generating clear, interpretable explanations for why an event has been classified as a threat, improving transparency and decision support. 4. Prototype and evaluate the agent using simulated system activity to assess detection effectiveness, false positives, and the clarity of diagnostic outputs. **Project Expectations:** This project is open to students enrolled in the Software Engineering program. 1. **Application of Software Engineering Principles:** You are required to apply established software engineering methodologies from the initial requirements gathering and analysis, through system architecture and detailed design, to implementation, testing, verification, validation, and maintenance. The project should reflect a systematic and disciplined approach to software development. 2. **Consideration of Constraints:** Your solution must demonstrate thoughtful consideration of relevant constraints, which may include health and safety, environmental impact, societal needs, adherence to standards, and other interdisciplinary factors pertinent to your project context. 3. **Comprehensive Documentation:** You are expected to produce and maintain clear, comprehensive, and well-organized documentation for your software system. This includes, but is not limited to, requirements specifications, design documents, test plans, user manuals, and maintenance guides. The project codebase must be maintained in a structured, version-controlled repository with meaningful commit messages, clear directory organization, and thorough inline code comments. All documentation and code should be prepared with future development in mind, enabling subsequent teams to readily understand, maintain, and extend the platform without reliance on external sources or prior team members. Regular updates to both documentation and the repository are expected throughout the project to ensure accuracy and continuity for future contributors. 4. **Demonstration of Artifacts:** Throughout the project, you will be required to present various software artifacts during team meetings. These may include prototypes, design sketches, test harnesses, infrastructure components, and code repositories. Regular demonstrations will be used to assess progress and provide feedback. Successful completion of this capstone project will require not only technical proficiency but also the ability to integrate engineering principles with real-world constraints, communicate effectively through documentation, and engage in collaborative development practices. These expectations align with professional standards in the software engineering discipline.

	References: References related to anomaly and threat detection and security metrics will be provided. **Prerequisites:** Enrolment in Software Engineering; proficiency in software design and development; familiarity with the software development lifecycle (SDLC); basic knowledge of cybersecurity concepts such as threat detection, system monitoring, and anomaly analysis; experience with version control systems (e.g., Git); teamwork and communication skills; analytical and problem-solving skills. Experience with machine learning, data analysis, or intelligent systems is beneficial but not required.
Program(s)	Software
Maximum number of students	3
Meeting time with supervisor (optional)	Students undertaking this project must be available to meet to discuss project progress, address challenges, and collaborate effectively with team members and the project supervisor. Regular meetings are expected to be primarily in person during regular working hours (Monday-Friday 9:00AM-4:00PM) held every 1-2 weeks for 30-60 minutes.
Do you want the student to contact you before the office assign this project to them ? (Yes/No)	Yes