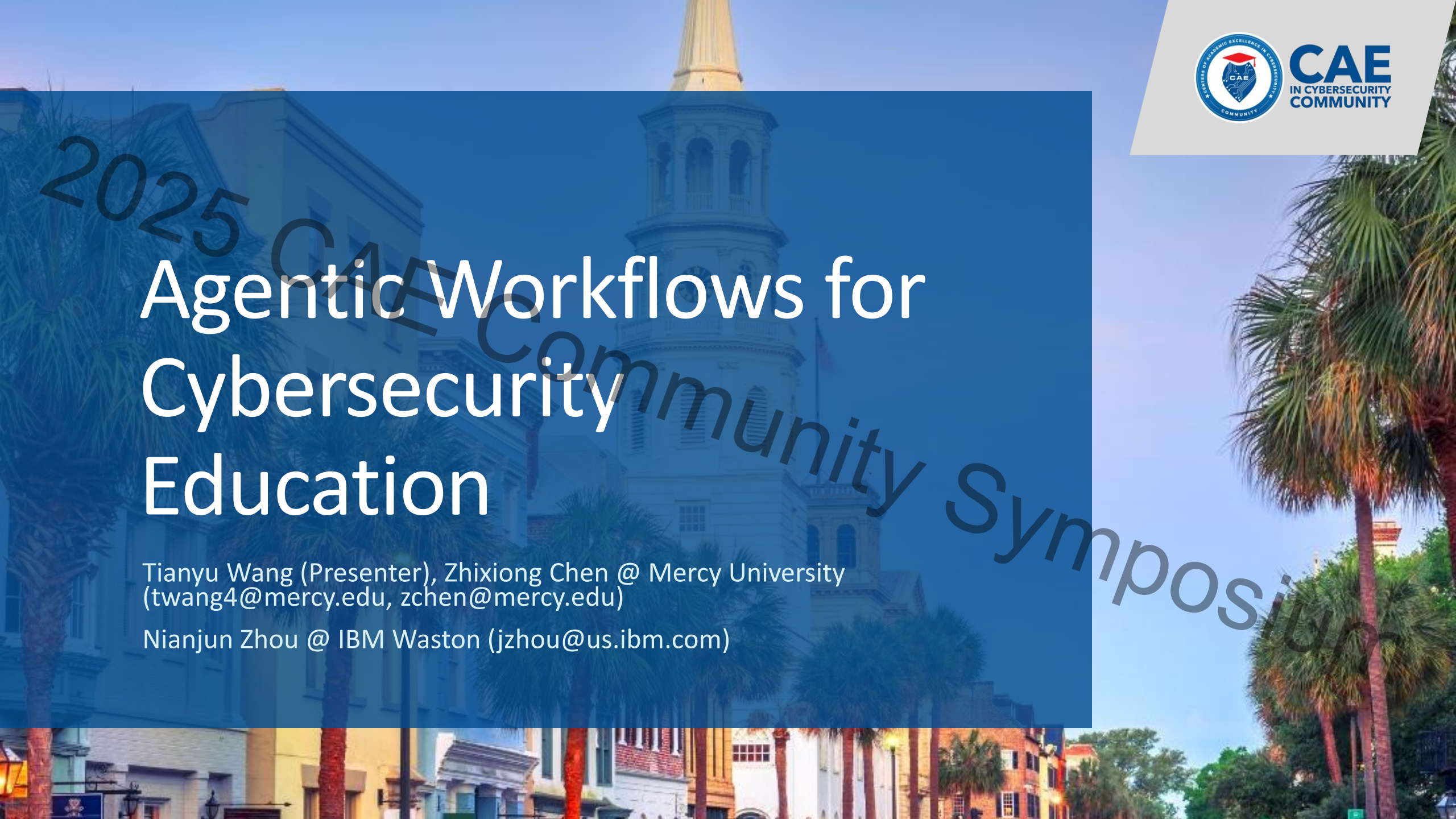


2025 CAE Community Symposium

Agentic Workflows for Cybersecurity Education

Tianyu Wang (Presenter), Zhixiong Chen @ Mercy University (twang4@mercy.edu, zchen@mercy.edu)

Nianjun Zhou @ IBM Waston (jzhou@us.ibm.com)

The Challenge: Cybersecurity Education

- Rapidly Evolving Threat Landscape demands continuous skill updates.
- Need to balance theoretical foundations with practical, industry-relevant skills.
- Keeping curriculum current with cutting-edge technologies is crucial.
- Traditional methods often struggle to personalize learning for diverse needs.

Introducing the Multi-Agent Learning Framework

- **Framework Goal**: To revolutionize cybersecurity education through personalized, adaptive learning.
- **Core Innovation**: Integrates advanced technologies to deliver targeted and effective training.
- **Foundation**: Built upon the robust, peer-reviewed CLARK cybersecurity curriculum.
- **Key Technologies**: Leverages Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG).

Dynamic Content Delivery with LLMs and RAG

Large Language Models (LLMs)

- Enable intelligent content processing and generation.
- Power personalized exercise creation and adaptive guidance.
- Facilitate contextually relevant learning experiences.

RAG

- Dynamically accesses the vast CLARK digital library.
- Ensures content is always up-to-date and relevant.
- Combines retrieval with LLM generation for rich learning materials.

CLARK: A Curated and Modular Cybersecurity Curriculum

- Leverages the established and peer-reviewed CLARK digital library.
- Provides a modular structure for flexible curriculum design.
- Access to diverse learning resources: slides, quizzes, labs, videos, and more.
- Ensures content relevancy and comprehensive coverage of cybersecurity domains.

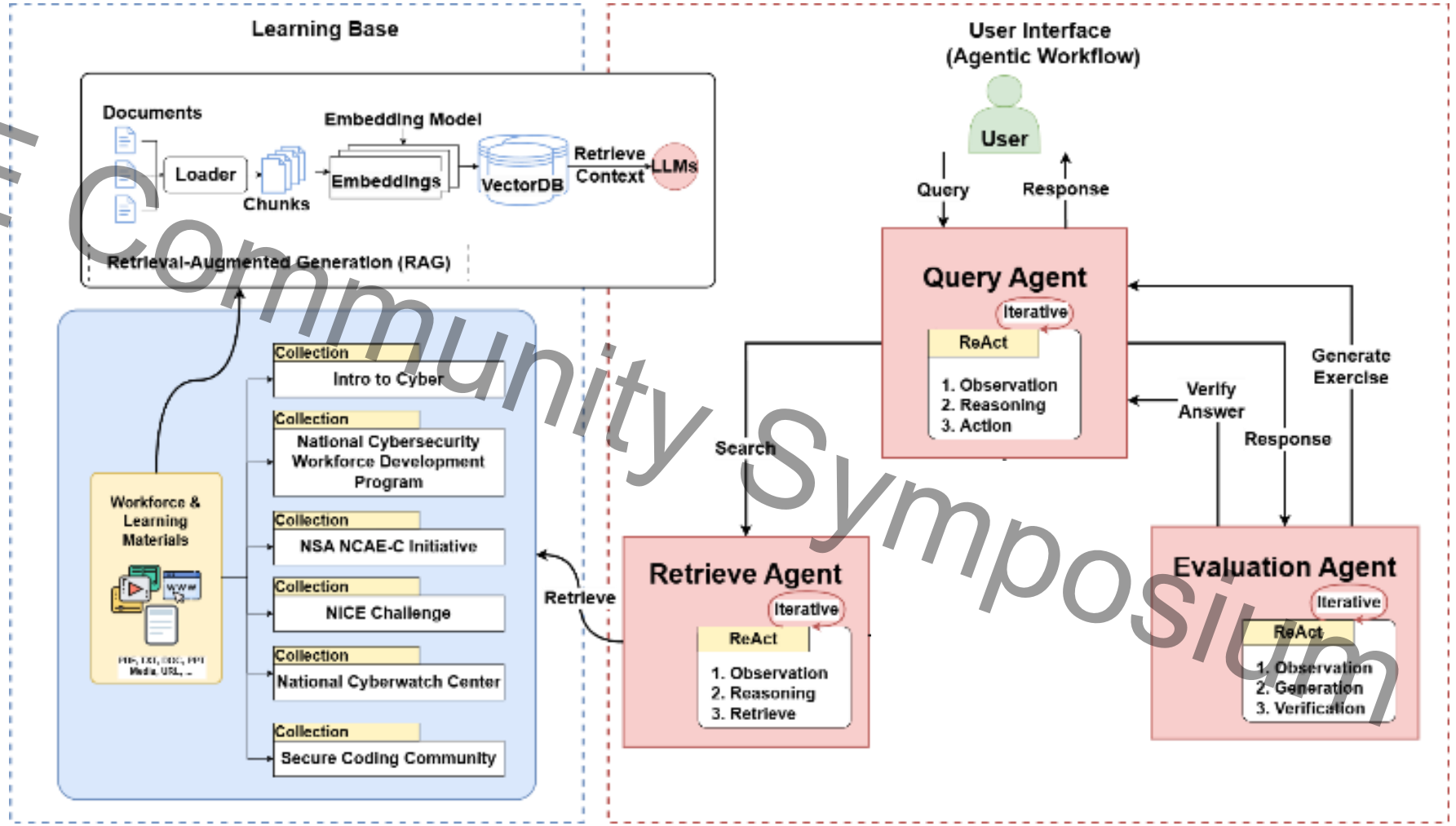
Personalized Learning Experiences: Contextual Practice

- Generates personalized and contextually relevant practice exercises.
- Adapts to individual learner's progress and knowledge gaps.
- Enhances engagement and knowledge retention through targeted practice.
- Moves beyond generic, one-size-fits-all exercises.

From Theory to Practice: Active Learning and Skill-Based Education

- Integrates active learning strategies to promote deeper understanding.
- Explicitly maps content to key cybersecurity skillsets and career pathways.
- Focuses on developing practical skills needed in the cybersecurity workforce.
- Bridges the gap between academic education and industry readiness.

Proposed Framework



2025 CAE Community Symposium

Demo

Impact & Future Directions: Shaping the Future of Cybersecurity Education

- **Enhanced Learning Outcomes**: Personalized and adaptive approach leads to deeper understanding and better skill acquisition.
- **Improved Industry Readiness**: Focus on practical skills and career pathways prepares graduates for the workforce.
- **Scalable and Sustainable**: Leverages existing resources (CLARK) and advanced technologies for efficient delivery.
- **Continuous Improvement**: Framework designed for ongoing refinement and adaptation based on learner data and evolving cybersecurity landscape.

Thank You!

Q&A