AUTOMATION OF CMMC CYBERCURITY IMPLEMENTATION GUIDANCE:

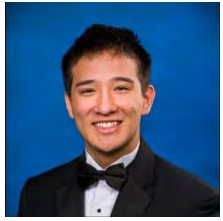
Enhancing Compliance and Efficiency Efforts

CMMC COVA TEAM

Warren Bizub (SIMIS)

Michael Humphrey-Sewell (SIMIS)

Terrance Perry (SIMIS)



Alex Naegele (SIMIS)

Dr. Sachin Shetty (ODU)

Dr. Safdar Bouk (ODU)

Dr. Masud Rana (ODU)

PROJECT OUTLINE

- Motivation Objective
- Project Objective
- Research Questions
- Specific Problems of Practice
  -Enhancing Workforce Development
  -Identifying Barriers and Challenges
  -Assessing the Effectiveness of Experiential Learning
- Approach to Automation
- CMMC Handbook Automation Process Steps
- API Prompt Example
- Outreach
- Outreach Strategies
- Outreach Strategies (Cont.)
- Significance
- Significance (Cont.)
- Questions

MOTIVATION OBJECTIVE

- The objective of this project is to simplify the creation of implementation guidance for the Cybersecurity Maturity Model Certification (CMMC) program.
- The project aims to enhance compliance efforts for CMMC and improve the overall efficiency of cybersecurity implementations in the maritime industry.

PROJECT OBJECTIVE

- The purpose of this project is to contribute to the field of cybersecurity by exploring the benefits and effectiveness of using automation to create more inclusive and experiential focused implementation processes, addressing specific problems of practice, and providing valuable insights for practitioners and policymakers.

- Through research questions and a focus on practical application, the work aims to enhance cybersecurity readiness and cybersecurity skill accessibility, ultimately improving the overall security landscape.

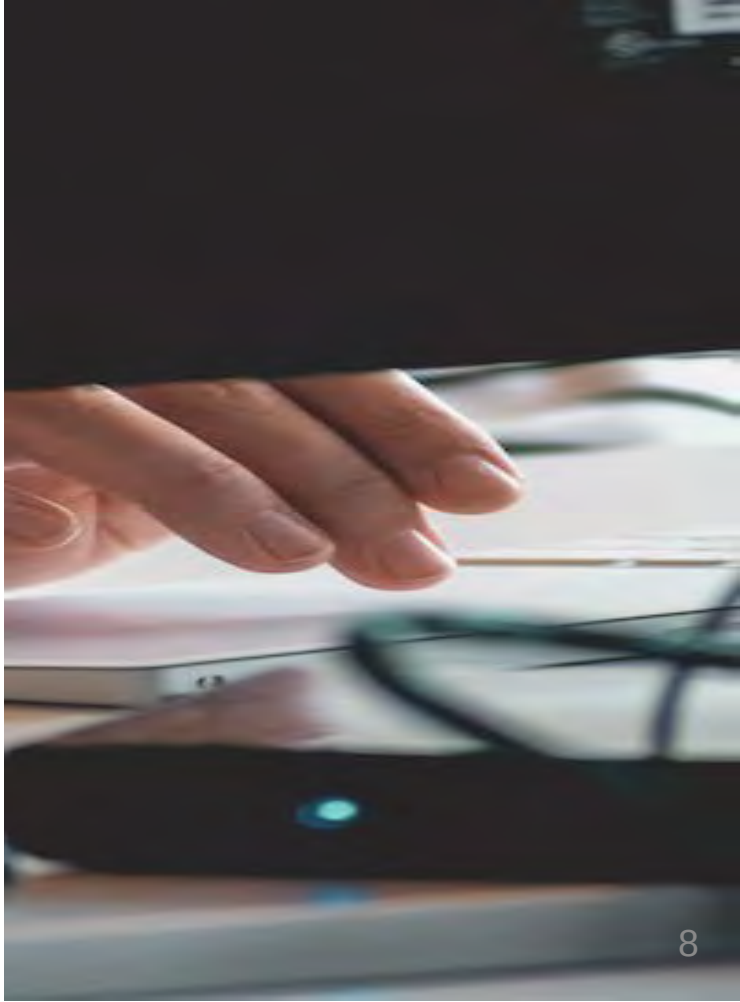
RESEARCH QUESTIONS

- **Question 1:** How can experiential learning opportunities be incorporated into the development of practical cybersecurity implementation guidance?
- **Question 2:** What are the removable barriers faced by non-typical maritime technical professionals participating in cybersecurity teams?
- **Question 3:** How can experiential learning outcomes be measured and assessed in terms of knowledge gain, skill development, and overall impact on cybersecurity practices?

SPECIFIC PROBLEMS OF PRACTICE

ENHANCING WORKFORCE DEVELOPMENT

- Traditional cybersecurity talent pipelines may not always offer sufficient opportunities to develop the number of cybersecurity professionals needed.
- This project focuses on using pedagogical knowledge to incorporate minimally supervised hands-on activities into cybersecurity implementation to allow non-traditional participants to actively contribute to the cybersecurity field.

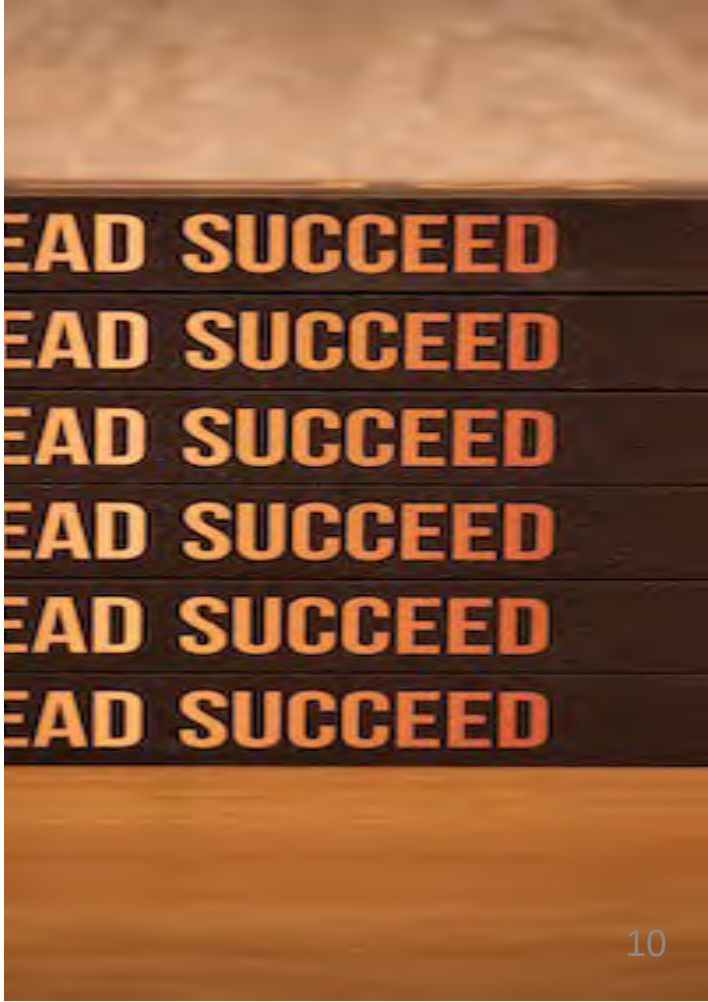


IDENTIFYING BARRIERS AND CHALLENGES

- The authors seek to identify and address the barriers and challenges faced by learners participating in experiential learning activities related to cybersecurity.
- Specifically for learners in the maritime industry but as wide ranging as feasible. By addressing these challenges using systematic semi-automated workflows, the work aims to improve accessibility for non-traditional groups in existing workforce in a rapidly developed and scalable process.

ASSESSING THE EFFECTIVENESS OF EXPERIENTIAL LEARNING

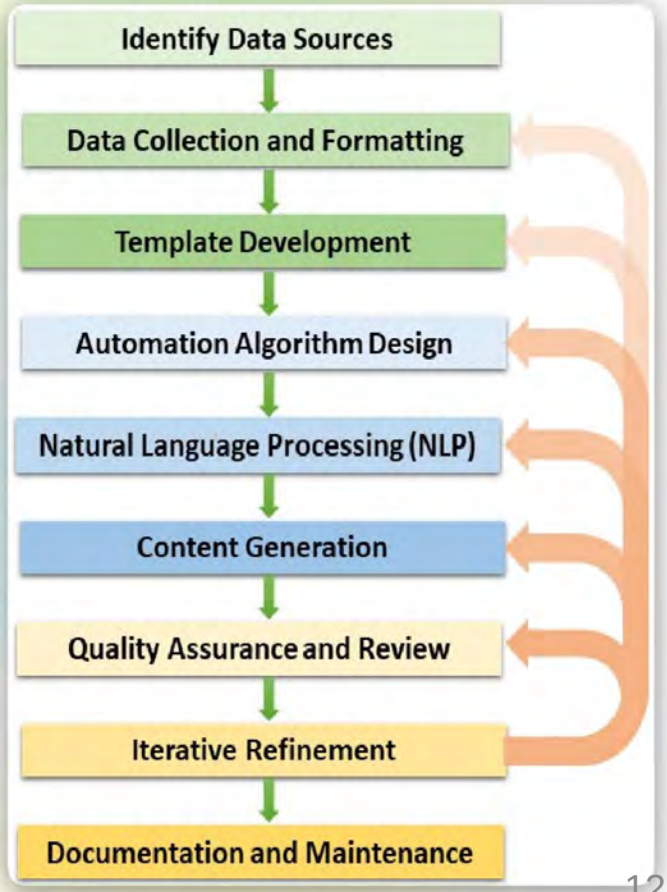
- There is a need to evaluate and measure the effectiveness of programmatically developed experiential learning programs in terms of knowledge gain, skill development, and their impact on cybersecurity practices.
- The work aims to select appropriate assessment methods and metrics to evaluate the outcomes and effectiveness of experiential learning initiatives in both traditional and nontraditional groups (while adhering to experiential learning standards such as xAPI).



APPROACH TO AUTOMATION

- The main objective is to automate the CMMC handbook development process because this automation will bring efficient, scalable, reliable, real-time updatable, data-driven, optimized guidance to the certification process.
- Each domain handbook will provide summary, tasking, and implementation guidance for the 15 domains and is written in language suitable for maritime staff with technical level implementation knowledge.

CMMC HANDBOOK AUTOMATION PROCESS STEPS (1 – 9)



API PROMPT EXAMPLE

OUTREACH

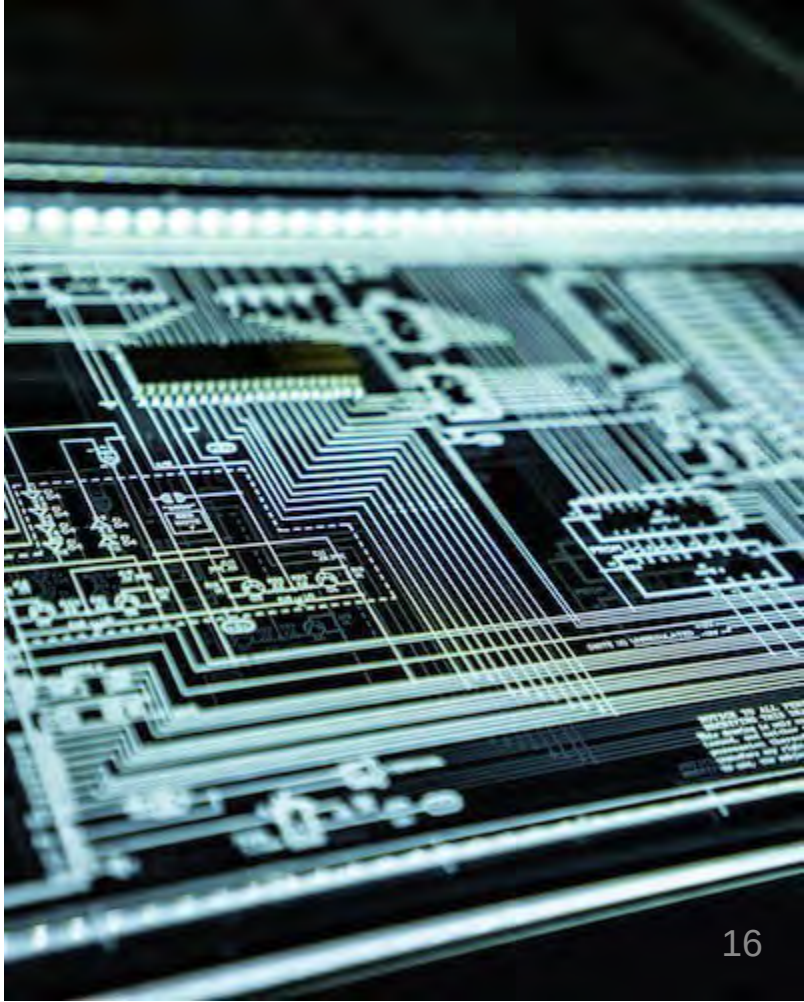
- Our goal is to engage and educate individuals and groups in the maritime industry who have an interest in cybersecurity, face barriers to obtaining necessary experience via traditional methods, and working in workplaces that need to implement CMMC.
- **Target Audience:** We seek to reach those non-cybersecurity technical professionals already working in the maritime industry at organizations implementing CMMC. The aim is to attract individuals at various stages of their educational or professional journeys, from beginners to more experienced 4 practitioners.

OUTREACH STRATEGIES

- **Online Platforms:** To reach the target audience effectively, we plan to leverage various online platforms. We will utilize social media channels such as LinkedIn and cybersecurity-focused forums to promote the more inclusive guidance. By engaging with relevant communities and sharing compelling content, we aim to generate interest and attract potential individuals.
- **Educational Programs:** We plan to collaborate with universities, colleges, and educational bodies to spread awareness about the CMMC handbooks. We will reach out to faculty members, career centers, and student organizations involved in cybersecurity education to distribute information and encourage awareness. Guest lectures, workshops, or presentations at these institutions may also be arranged to showcase the organizational benefits of inclusive implementation.

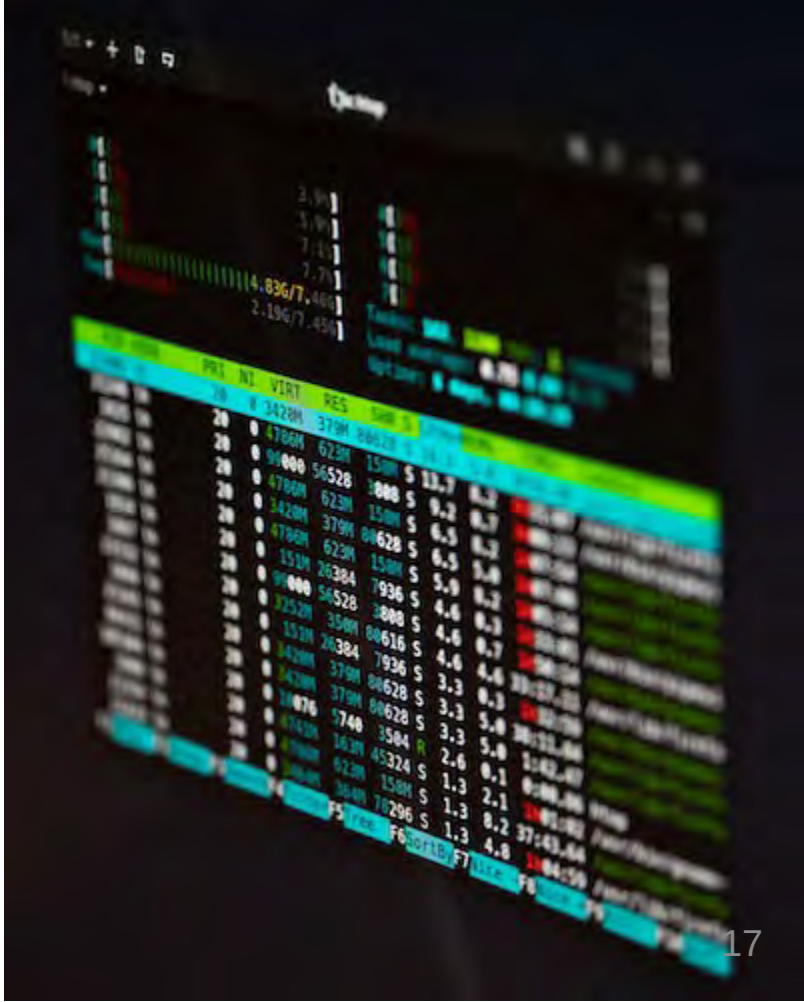
OUTREACH STRATEGIES (Cont.)

- **Professional Networks**: We plan to tap into professional networks and industry associations related to cybersecurity and the maritime industry. We will also connect with cybersecurity organizations, attending events, conferences, and webinars to establish relationships with professionals in the field. By presenting the benefits at these gatherings, we aim to reach fellow cybersecurity practitioners who might be interested in mentoring or collaborating.
- **Partnerships:** To maximize outreach, we plan to seek partnerships with organizations or individuals already active in the cybersecurity community. Collaboration with cybersecurity companies or prominent professionals allows for increased exposure and credibility.



SIGNIFICANCE

- **Accuracy and Resource Efficiency:** Automation can greatly reduce human errors when creating CMMC implementation requirements. Limited cybersecurity expertise can be more efficiently focused on quality assurance of automatically created guidance versus content creation duties or lengthy manual update processes.
- **Automation of Enhanced Accessibility Workflows:** Automation of content generation allows for consistent and standardized application of algorithms designed to create more inclusive guidance for technical processes. By refinement of complex processes which leverage AI/ML to expand skill development accessibility, organizations gain a wider talent pool to implement policy from. These same techniques might also be applied to other fields in the future.



SIGNIFICANCE (Cont.)

- **Maritime Workforce Development:** Specific to the maritime industry, the existing workforce can be more easily leveraged to fill cybersecurity needs in cases when traditional pipelines might not be able.
- **Speed of Adoption:** Automation provides rapid scalable and agile products to meet the needs of changing cybersecurity requirements. As needs evolve over time, automated systems can be updated and adjusted more easily, ensuring organizations receive and implement guidance faster.


QUESTIONS?