Tailored Cybersecurity Training in LVC Environments

Presented by
Jeremiah Folsom-Kovarik, Ph.D.

On behalf of the co-authors:
Denise Nicholson, Ph.D., Lauren Massey,
Ryan O’Grady and Eric Ortiz

MODSIM WORLD 2016
Empowering User Communities With Modeling and Simulation
Virginia Beach, Virginia • April 26-28, 2016

5 November 2018

SOARTECH

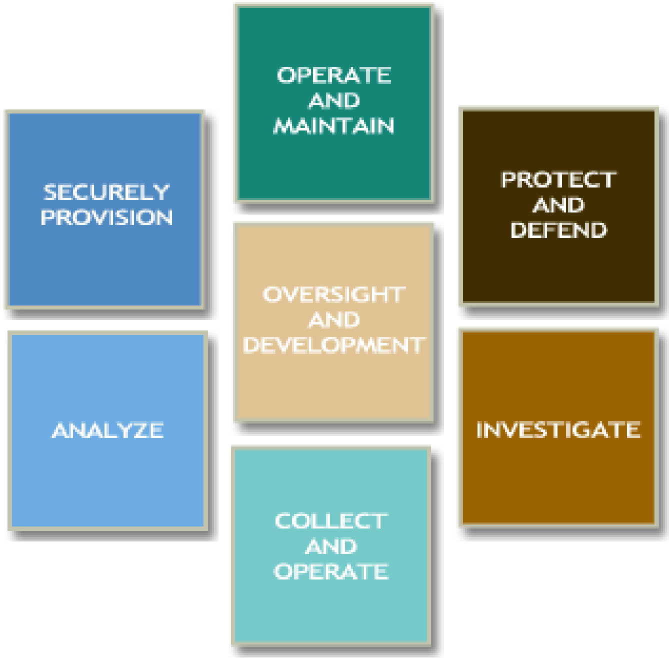
Modeling human reasoning.
Enhancing human performance.

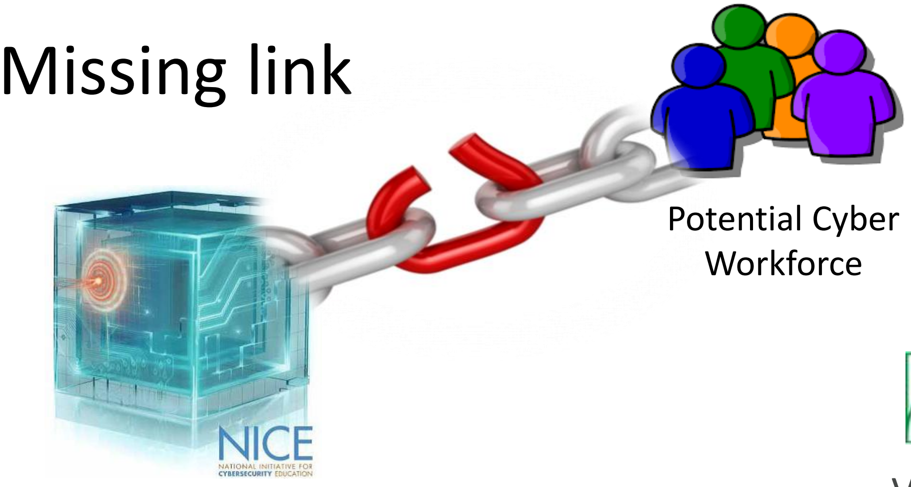
Outline

- What are trying to do:
  - Address the cybersecurity workforce need
- Stakeholders:
  - Homeland security, industry, academia, and government
- What is done today:
  - National Initiative for Cybersecurity Careers and Studies (NICCS) Framework
- What is new:
  - Training Learning Architecture in conjunction with LVC learning experiences
- Use Case

National Initiative for Cybersecurity Careers and Studies (NICCS)

- Shortage in cyber security workforce
- Aid in pinpointing what current and future professionals need to know for a career in the cyber workforce
- Missing link



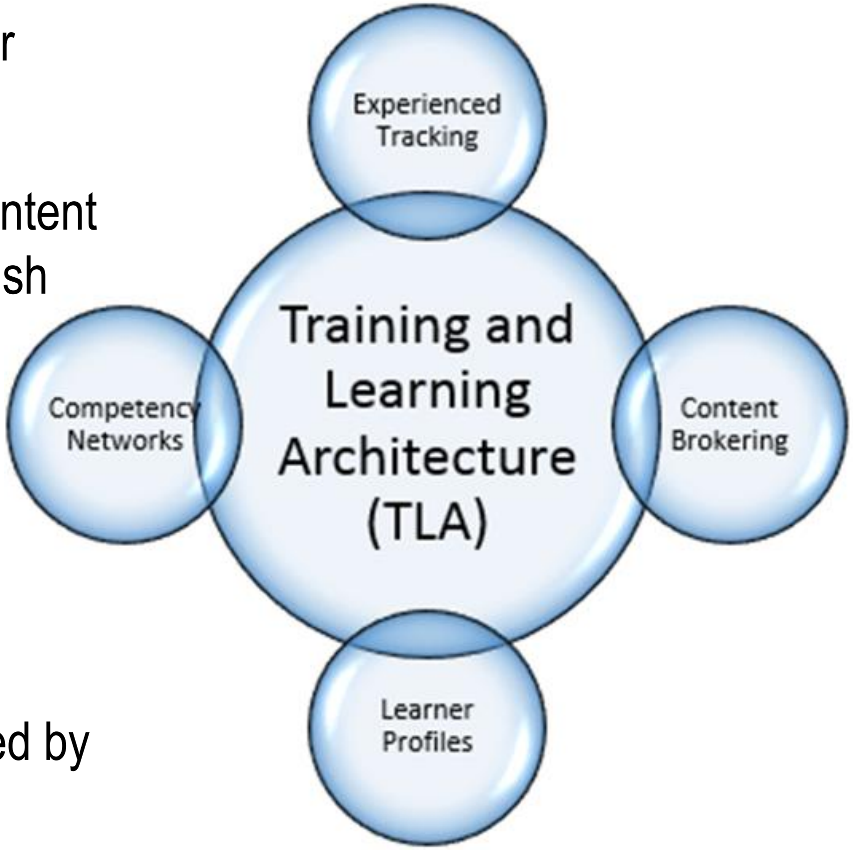

Potential Cyber Workforce
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Development of a Personalized Assistant for Learning (PAL)

- Advance Distributed Learning (ADL) initiative
- Provides life-long, relevant, tailored, timely access to learning content and performance aids
- PAL accomplished through usage a **Training Learning Architecture** (TLA)

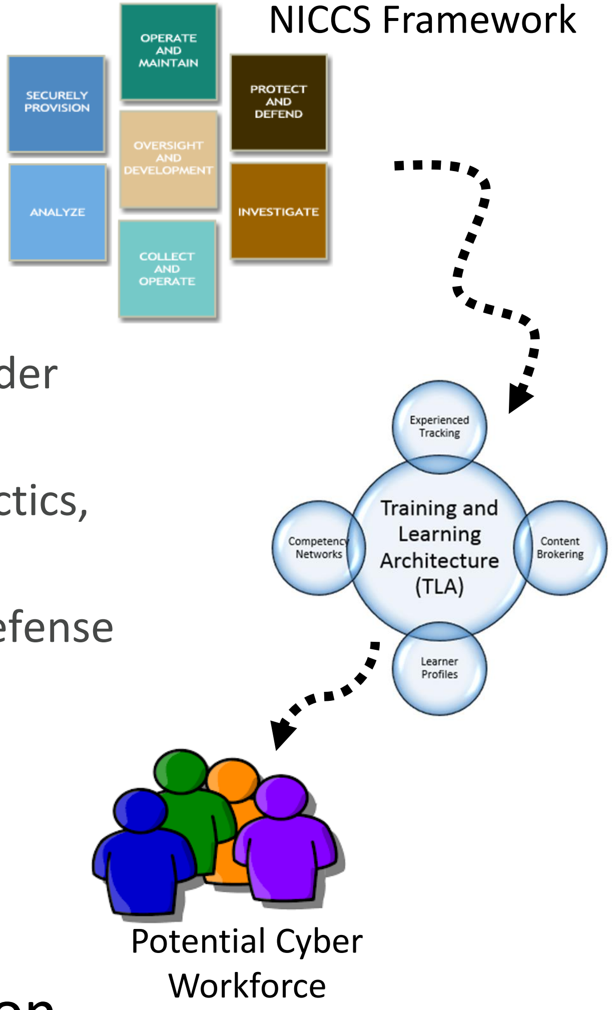
Training and Learning Architecture (TLA)

- Learner Profiles
  - Basic information regarding the user
- Content Brokering
  - Decision making on what type of content the user needs to cover to accomplish their unique goal
- Experience Tracking
  - Learner profiles updated as learner progresses in competency
- Competency Network
  - Library of course content to be pulled by content brokering as needed



Use Case: Usage of PAL

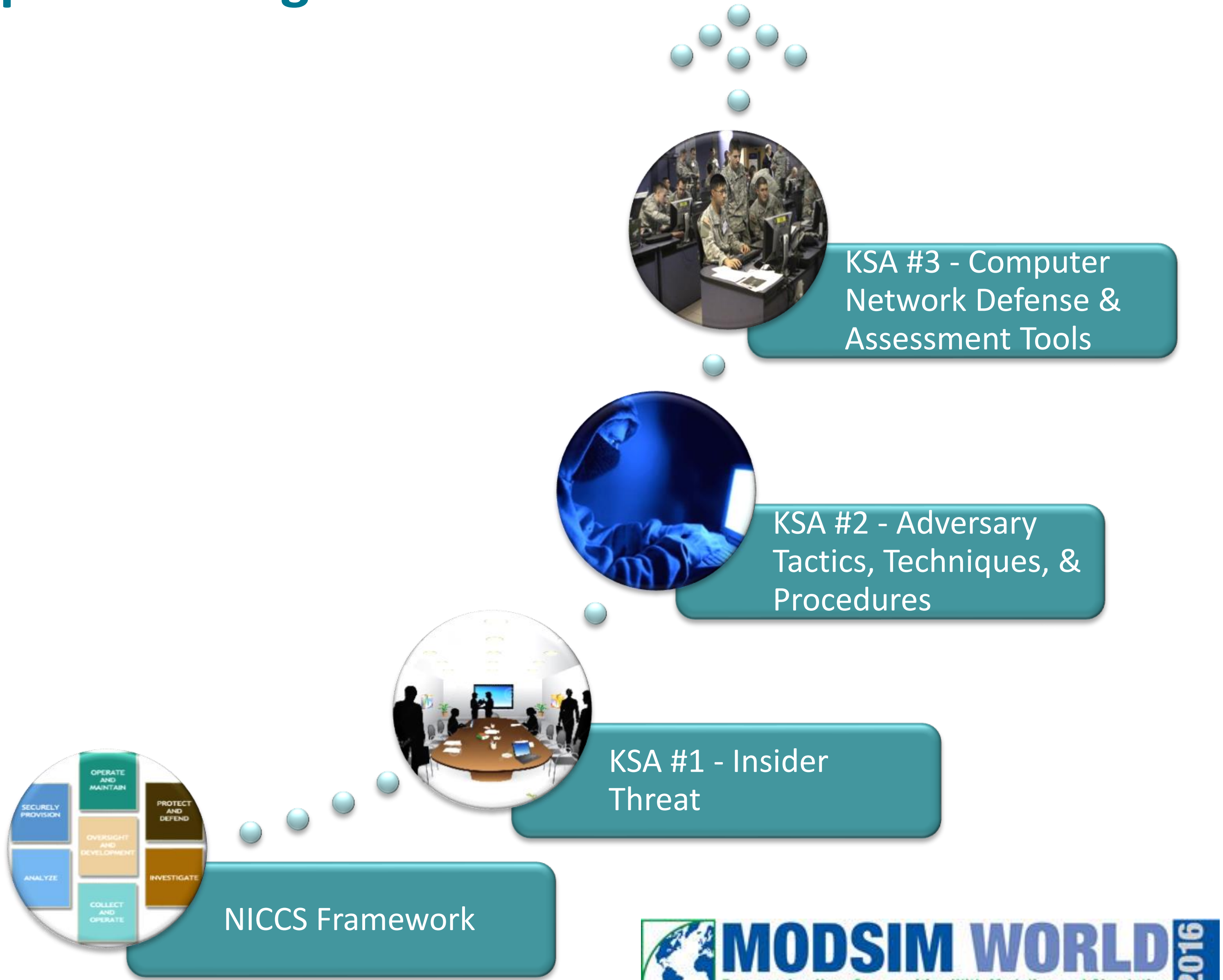
- User
  - Advancement of career
  - Interest in Computer Network Defense
    - Knowledge, Skills, and Abilities (KSAs)
      1. Knowledge of and experience in Insider Threats
      2. Knowledge of common adversary tactics, techniques, and procedures
      3. Knowledge of Computer Network Defense and vulnerability assessment tools



- The needed KSAs are linked to PAL and the TLA would manage, track, and monitor their progression thru a selection of learning experiences

Example Learning Path

Career Goals



NICCS Framework

KSA #1 - Insider Threat

KSA #2 - Adversary Tactics, Techniques, & Procedures

KSA #3 - Computer Network Defense & Assessment Tools

KSA #1:
Knowledge of and experience in Insider Threat

- Insider Threat
  - Individuals that have the ability to or at one time had permissions to access an organization’s data and network structures
  - Insider advantages:
    - Knowing where critical data exists
    - Ability to access restricted areas

Suggested Activity - LVC for Insider Threat

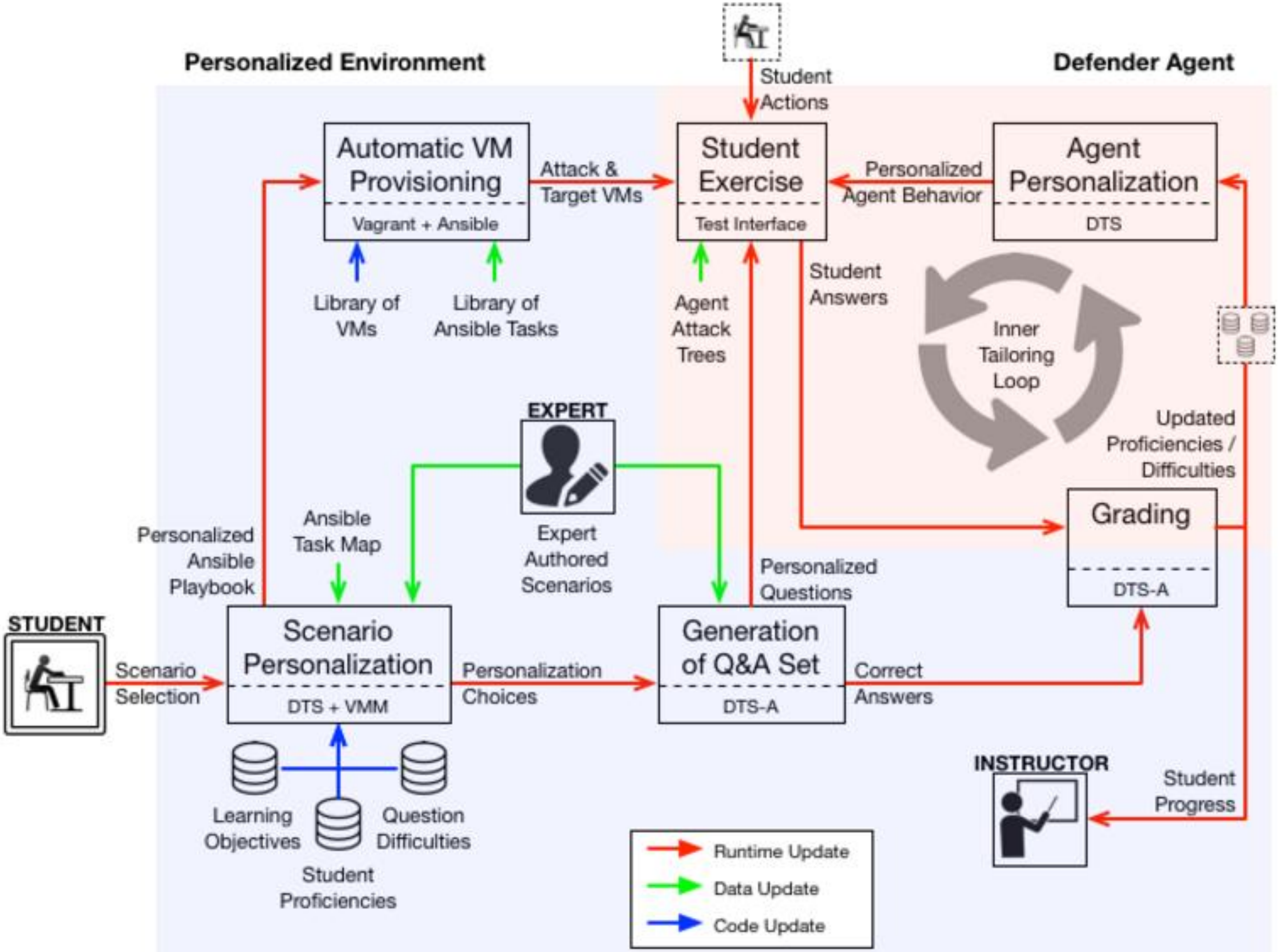
- Serious games environment offer an interactive training method to engage participants
- Allows for high level of engagement that can present logically control, difficult, dangerous, or complicated situations in practical and safe environments

KSA #2: Familiarization with Common Adversary Tactics, Techniques, and Procedures

Suggested Activity:

- Cyber Security Environment (CYSTINE)
  - Training system to create a dynamic training scenario that responds to the training skill of the trainee
  - Cyber defender cognitive agents, Soar agents, provide dynamic, cognitively realistic adversaries
    - Defenders that offer active opposition to the student
  - The simulation – based training system adapts and learns with the students without placing an unreasonable burden on instructors

CYSTINE Architecture



KSA #3:
Knowledge of Computer Network Defense and Vulnerability Assessment Tools in a Live Simulation Exercise

- Although knowledge of computer network defense system can be provided through traditional methods , there is a lack of real world dynamics
  - Traditional methods: classroom training with static vulnerabilities
- Current cyber simulations and tools lack the element of active opposition
  - Trains cyber operators to behave as though opponents do not have a tangible existence or do not have higher level goals

Activity: Red on Blue Cyber Exercises

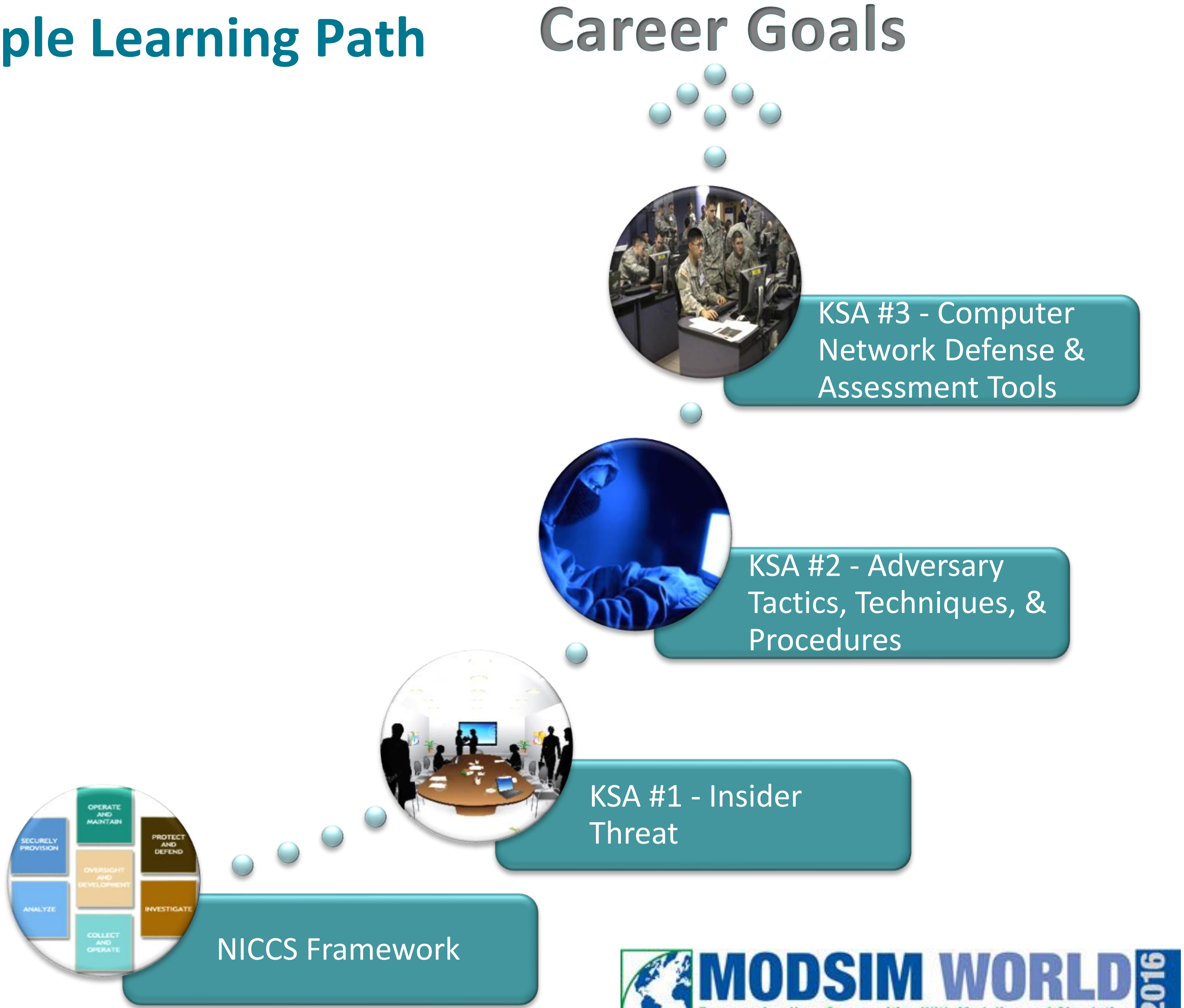
- The military academies participate in a yearly competition to attack and defend their systems in a four day competition.
  - Issues:
    - The exercise is a large scale competition with highly trained cadets which makes reproduction on a smaller scale difficult
    - Not feasible for emerging professionals to receive this scale of training because of lack of readily available trained personnel

- **An opportunity to replicate such environments for emerging cyber professionals with a training against dynamic, automated adversaries**

SC2RAM - Cognitive Agent in Cyber Defense Training

- The cognitive simulation provides:
  - Adaptive, goal –oriented aggressors/defenders
  - Ability to learn and adjust strategies and tactics at the cognitive time scale
  - Real – time, cognitive scale situation understanding and decision making
- Cognitive simulation can be used to substitute human counterparts.
- This allows training exercises like the CDX to be implemented on a scale that adaptable to the emerging professionals.

Example Learning Path



Career Goals

KSA #3 - Computer Network Defense & Assessment Tools

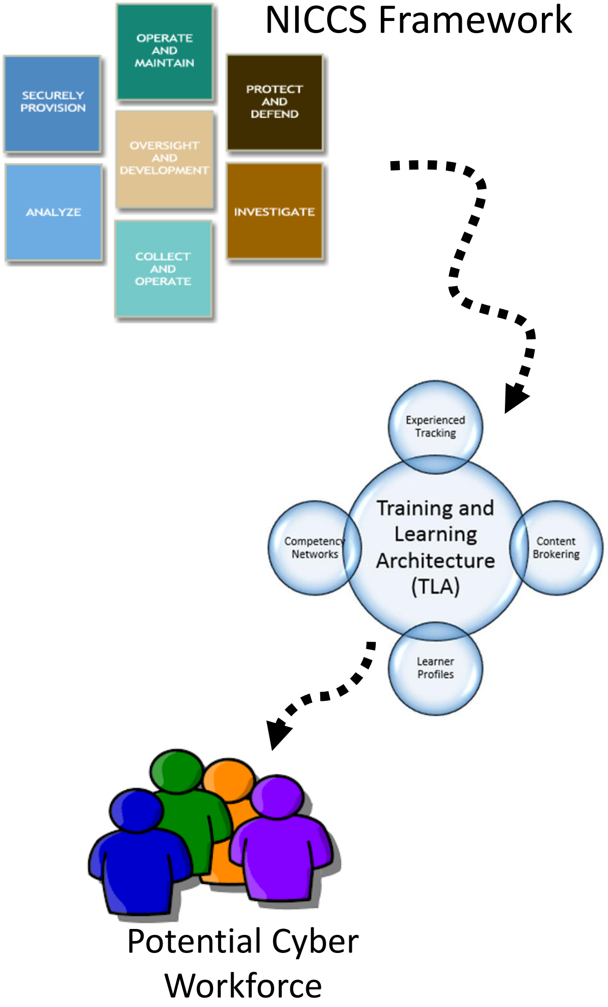
KSA #2 - Adversary Tactics, Techniques, & Procedures

KSA #1 - Insider Threat

NICCS Framework

Next Steps

- Implementation of the TLA and development of LVC activity learning experiences
- Exploration of making LVC Cyber Learning Activities TLA compatible
- Iterative future testing and experimentation



NICCS Framework

OPERATE AND MAINTAIN

SECURELY PROVISION

PROTECT AND DEFEND

OVERSIGHT AND DEVELOPMENT

ANALYZE

INVESTIGATE

COLLECT AND OPERATE

Experienced Tracking

Competency Networks

Training and Learning Architecture (TLA)

Content Brokering

Learner Profiles

Potential Cyber Workforce

QUESTIONS and DISCUSSION

- **For more information**

  Denise Nicholson, Ph.D.

  denise.nicholson@soartech.com

- **Acknowledgement**

This material is based upon work supported by the Advanced Distributed Learning (ADL) Initiative under Contract No. W911QY-16-C-0019. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Advanced Distributed Learning (ADL) Initiative.