Realizing Our Collective Vision by 2025: Leveraging advances in Artificial Intelligence and Autonomy with Human Systems in Human-Machine Symbiosis to Realize Our Roadmap to the Future … *a Cyber-Security Workforce Use Case*

Dylan Schmorrow, PhD, *Chief Scientist & Executive Vice President*

Denise Nicholson, PhD, *VP of Intelligent Training & Director of "X"*

SOARTECH

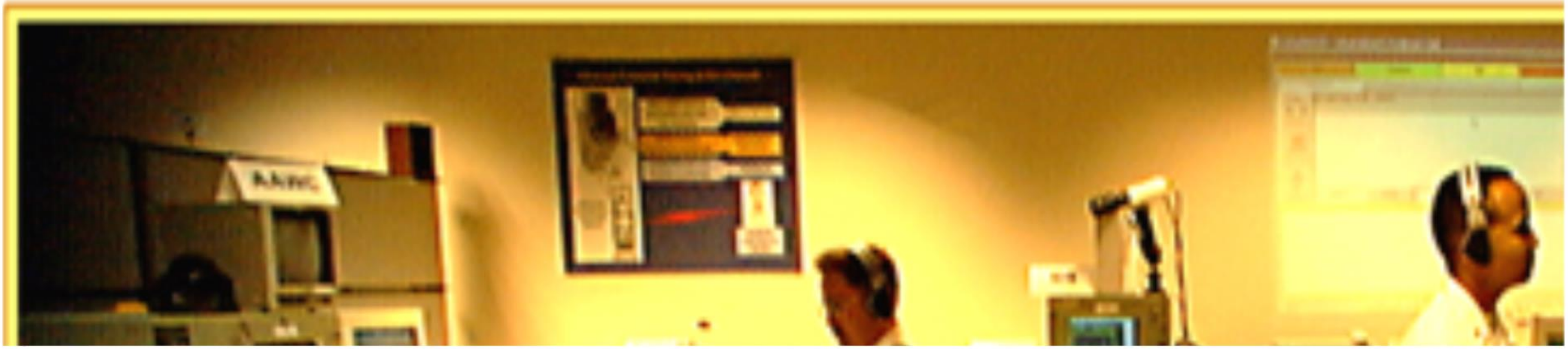
Modeling human reasoning.
Enhancing human performance.

NDIA
Human Systems in Emerging Domains: Autonomy, Human Augmentation and Cyber
01

Outline

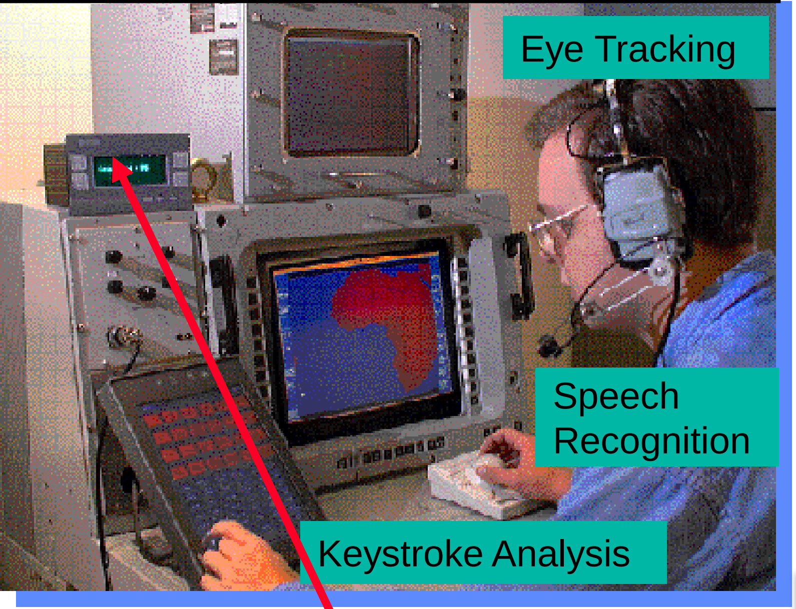
- Where have we come from
  - Early concepts in Advanced Embedded Training
- Where are we going
  - Personalized, Life Long Learning
  - Sailor 2025 – Ready Relevant Learning
- A Use Case in Cyber Workforce Training
  - National Initiative for Cybersecurity Careers and Studies (NICCS) Framework
  - Training Learning Architecture in conjunction with LVC learning experiences
- Challenges for 2025
  - Data Data Data

1998 ACTD
Advanced Embedded Training System



1998 ACTD
Advanced Embedded Training System

Student Model: Measured Operator Actions



Online Feedback

Comparator
Automated
Performance
Assessment
Engine

Expected Operator Actions
Generated By **Expert Models**

Training Mitigation Director
Operator Action Evaluations
Focused on Scenario
Key and Critical Events

Diagnosis of Knowledge
And Skill Deficiencies

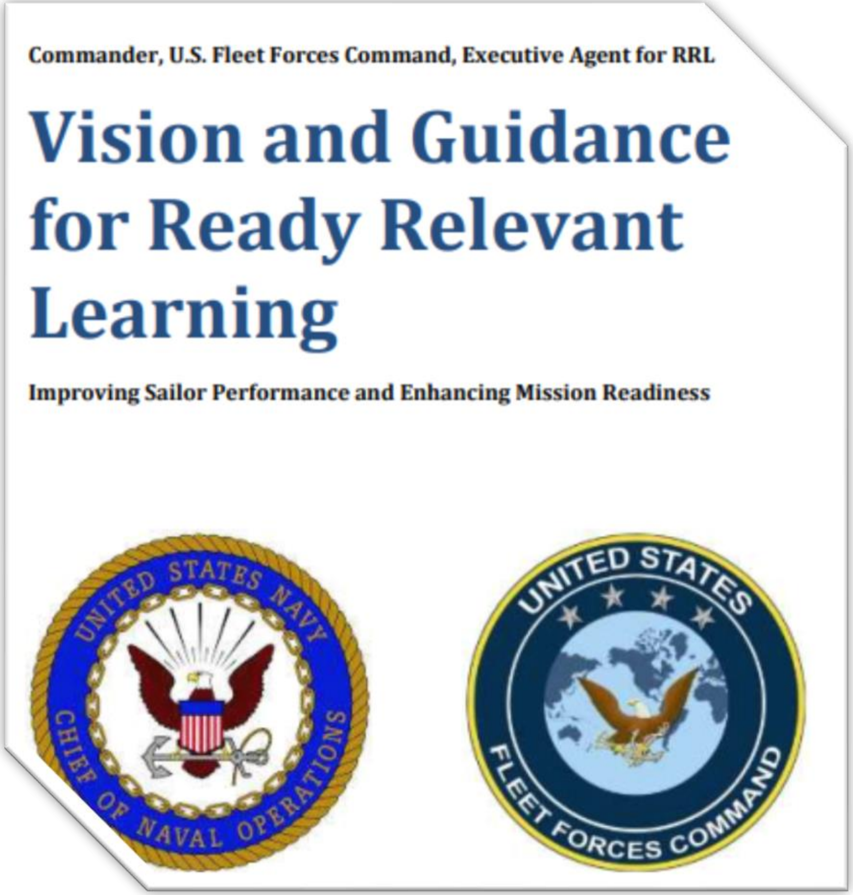
Post-Exercise
Debriefing

Instructor Hand-Held Device
ShipMATE

- 🟩 **Performance Measurement Subsystem – LM ATL & TSD**
- 🟧 **Diagnostic Subsystem – CHI Systems, Aptima & TSD**
- 🟦 **Instructional Subsystem – Sonalysts & TSD**

Sailor 2025 – 3 Key Elements of RRL

1. Career- Long Learning Continuum
2. Modern delivery at the point of need
3. Integrated Content Development
   - Delivery methodologies



Commander, U.S. Fleet Forces Command, Executive Agent for RRL

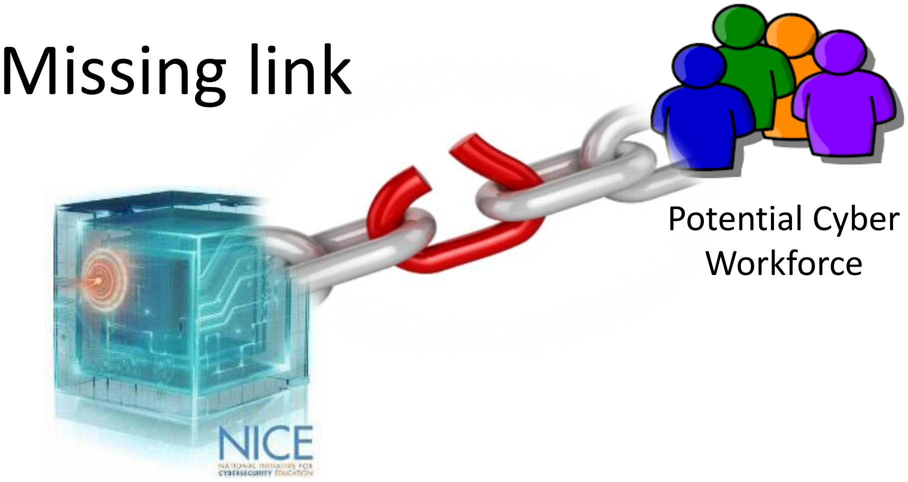
Vision and Guidance for Ready Relevant Learning

Improving Sailor Performance and Enhancing Mission Readiness

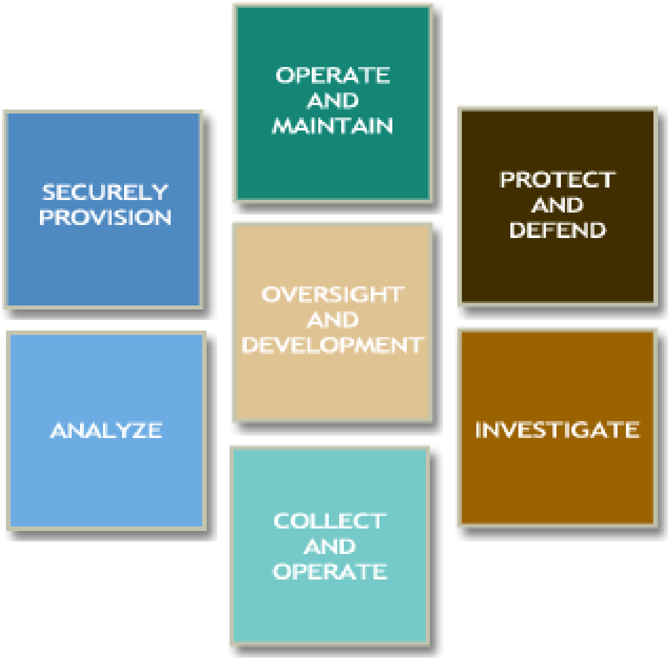
http://www.public.navy.mil/usff/rrl/Documents/PDFs/rrl-vision-and-guidance-final.pdf

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


OPERATE AND MAINTAIN

SECURELY PROVISION

PROTECT AND DEFEND

OVERSIGHT AND DEVELOPMENT

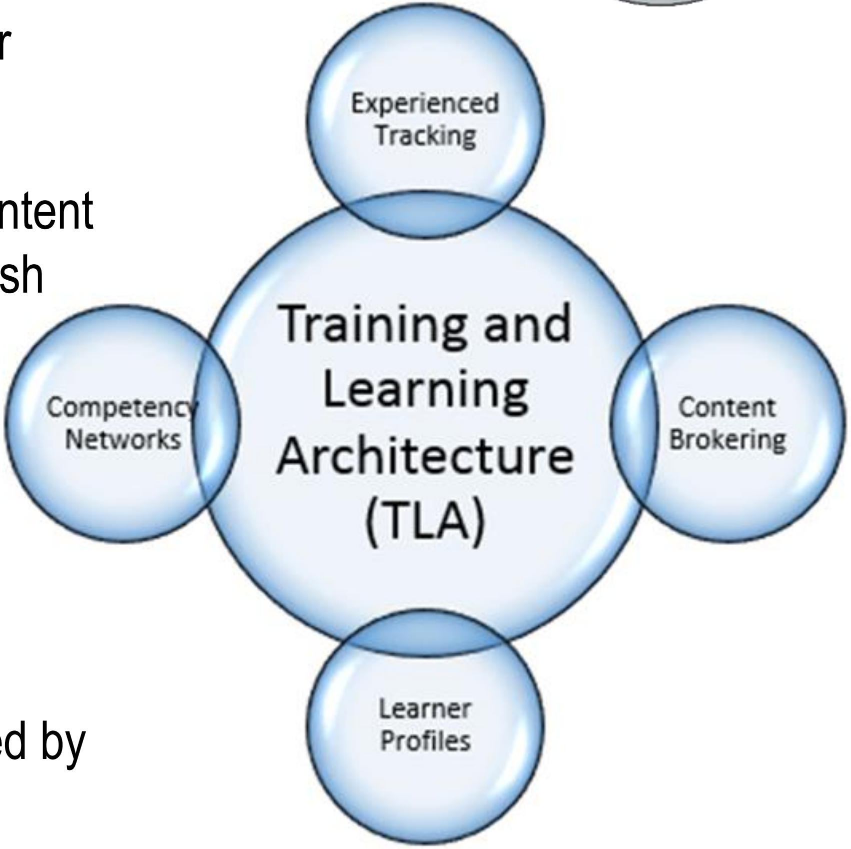
ANALYZE

INVESTIGATE

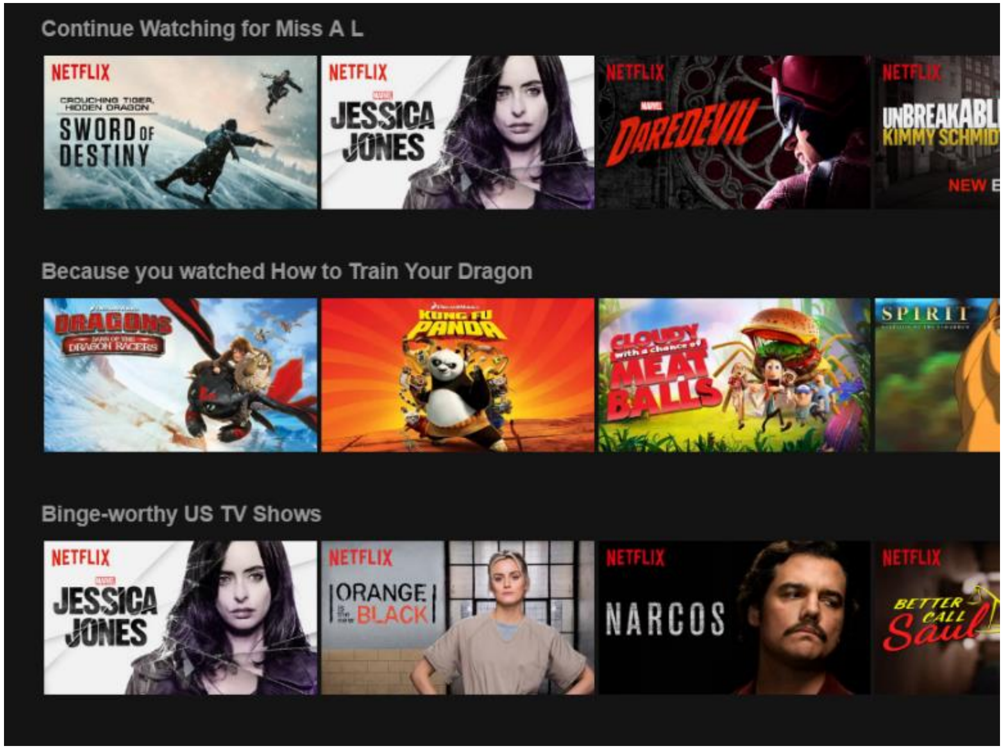
COLLECT AND OPERATE

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



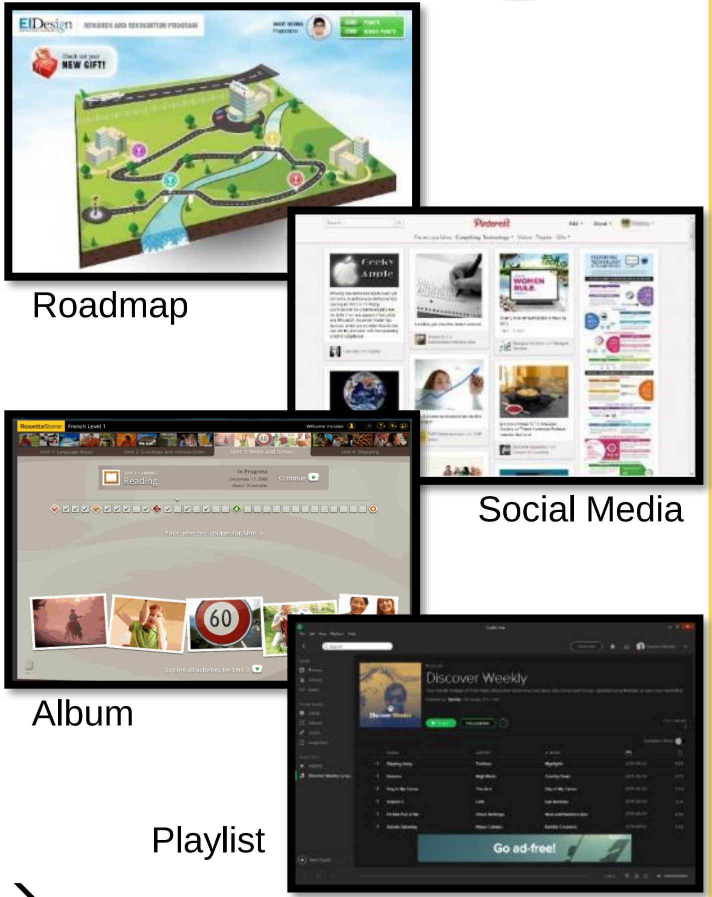
Recommender UI
Our metaphor: multiple offerings and rationales



Continue Watching for Miss A L

Because you watched How to Train Your Dragon

Binge-worthy US TV Shows



Roadmap

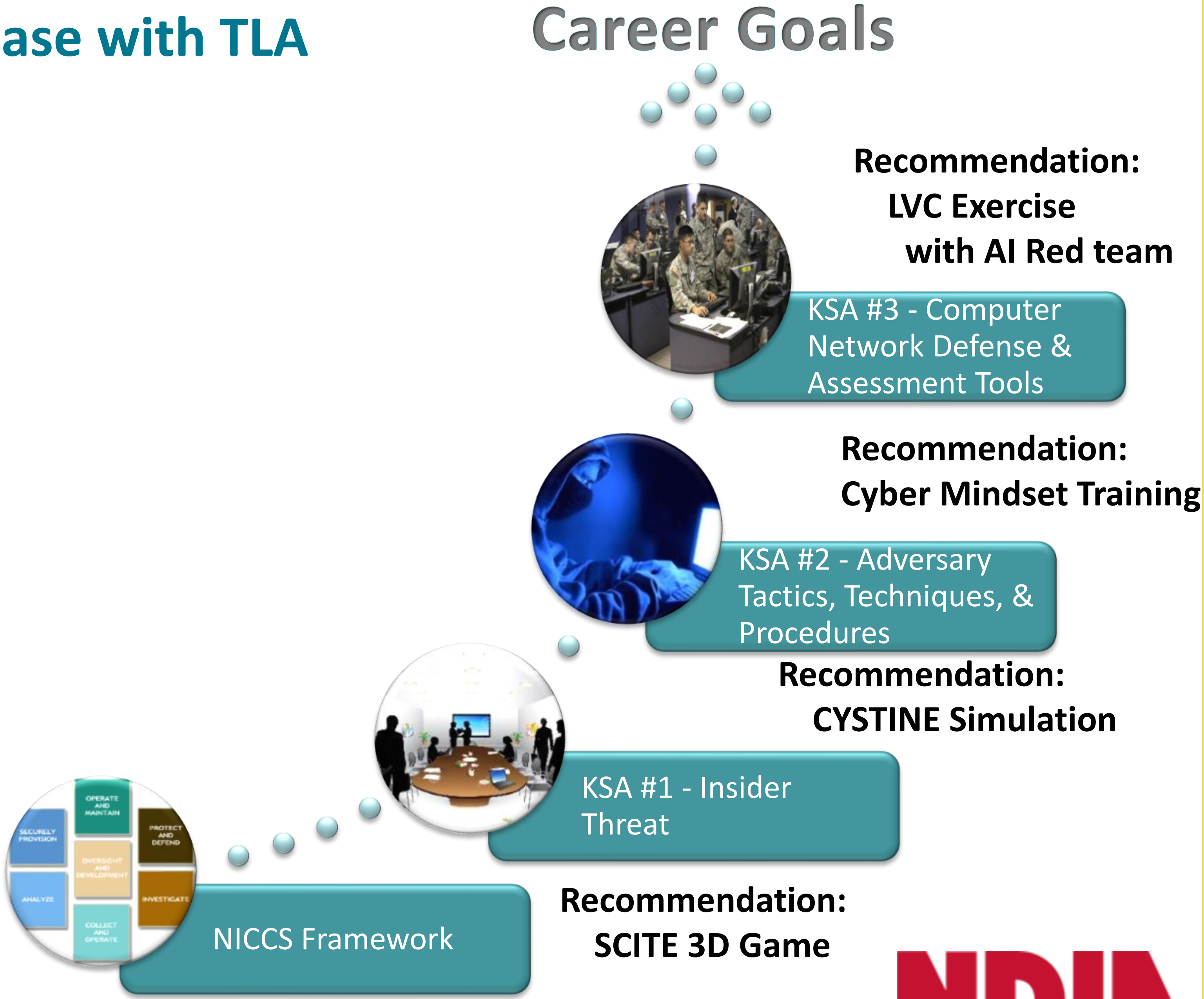
Social Media

Album

Playlist

Alternate / future UIs →

Use Case with TLA



NICCS Framework

Recommendation:
SCITE 3D Game

KSA #1 - Insider Threat

Recommendation:
CYSTINE Simulation

KSA #2 - Adversary Tactics, Techniques, & Procedures

Recommendation:
Cyber Mindset Training

KSA #3 - Computer Network Defense & Assessment Tools

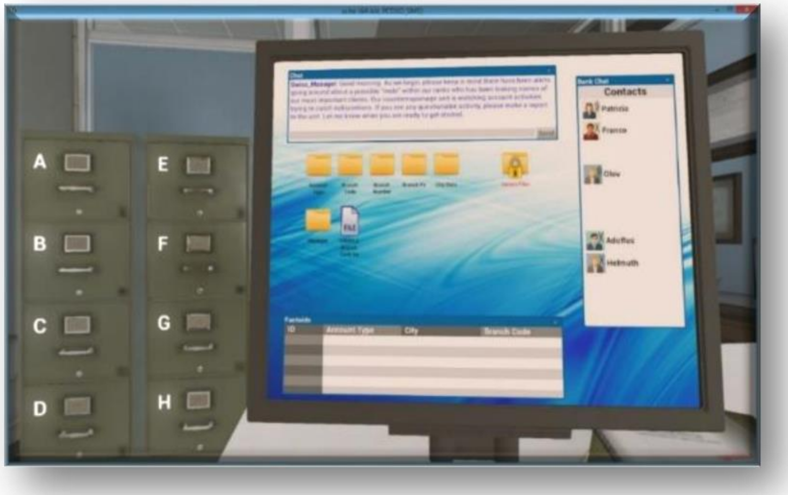
Recommendation:
LVC Exercise
with AI Red team

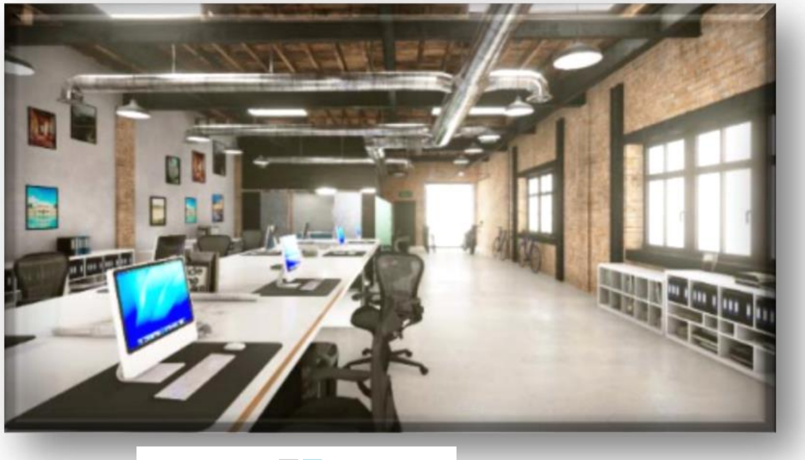
Career Goals

KSA #1: Knowledge of and experience in Insider Threat

Recommended Activity: 3D Insider Threat Game

- Scenario based gaming environment to experience insider threats
- Occurs within an office space and designed to replicate the exploitation of computer systems by employees to gain access to financial information without permission





UCF

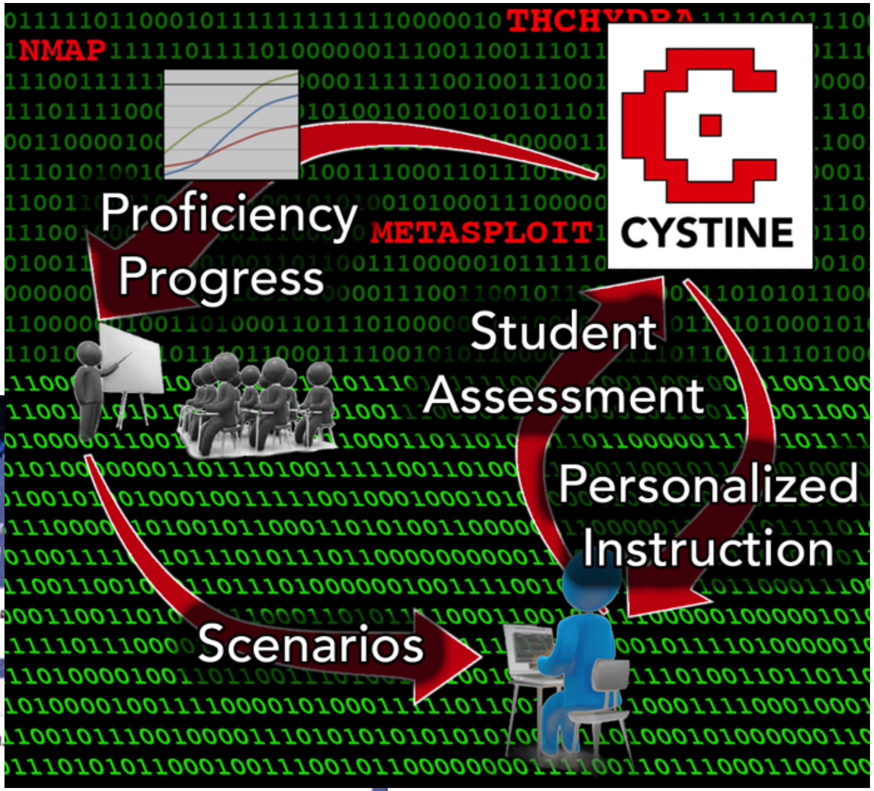
SOARTECH
Modeling human reasoning.
Enhancing human performance.

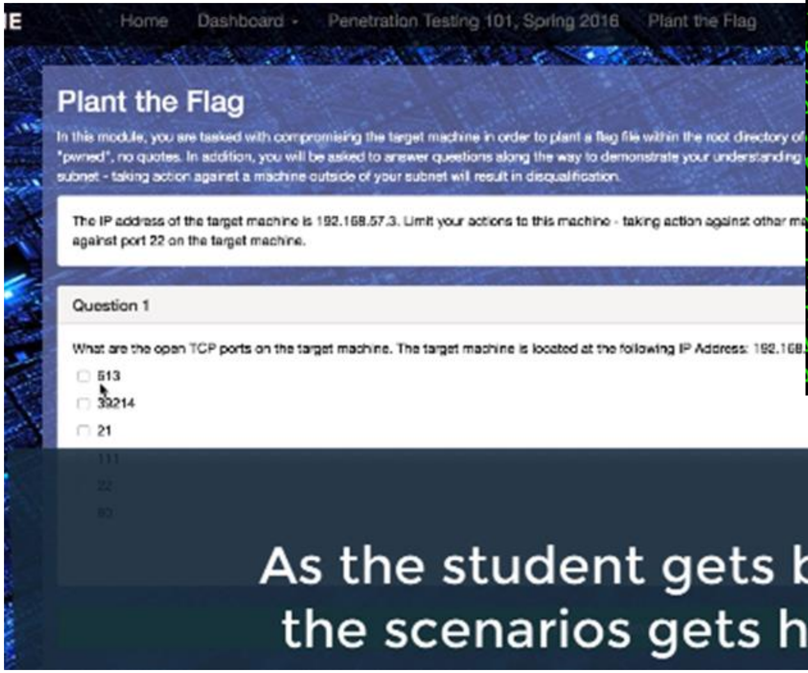
NDIA
HUMAN SYSTEMS

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

Recommend: Cyber Security Environment (CYSTINE)

- Dynamic training scenario that adapts to the skill of the trainee
- Cyber defender cognitive agents, provide dynamic, cognitively realistic adversaries





Plant the Flag

In this module, you are tasked with compromising the target machine in order to plant a flag file within the root directory of
"pwned", no quotes. In addition, you will be asked to answer questions along the way to demonstrate your understanding
subnet - taking action against a machine outside of your subnet will result in disqualification.

The IP address of the target machine is 192.168.57.3. Limit your actions to this machine - taking action against other m
against port 22 on the target machine.

Question 1

What are the open TCP ports on the target machine. The target machine is located at the following IP Address: 192.168

- □ 513
- □ 39214
- □ 21
- 111
- 22
- 80

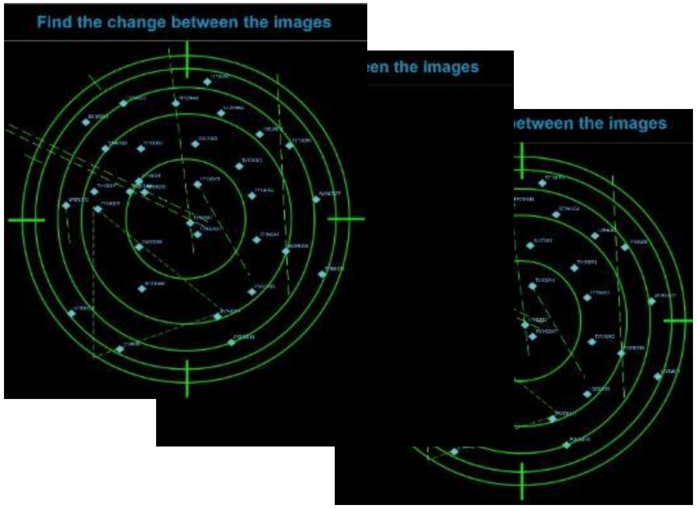
As the student gets better, the scenarios gets harder

KSA #3: Knowledge of Computer Network Defense Recommendation - Cyber Mindset Training

Cyber basics: Prepare non-cyber personnel to participate in largescale synthetic cyber training

- **Interactive instruction on how to minimize cognitive bias interference**
  - **Challenge assumptions** about immunity to, e.g.,
    - Attentional tunneling
    - In-attentional blindness
    - Confirmation bias
- **Game-based event recognition practice**
  - Develop **perceptual sensitivity**
  - Gain appreciation for importance of maintaining **system awareness**

In-attentional Blindness Exercise:



KSA #3: Knowledge of Computer Network Defense and Vulnerability Assessment Tools Recommend – LVC Exercise with AI Red Team

Simulated Cognitive Cyber Red-team Attack Model SC2RAM allows training exercises to be implemented on a scale that adaptable to the emerging professionals

NDIA HUMAN SYSTEMS

Future Challenges – Data, Data, Data …..

Data

- About the activities/training
  - –Learner progress thru the activity
- About existing content – reuse

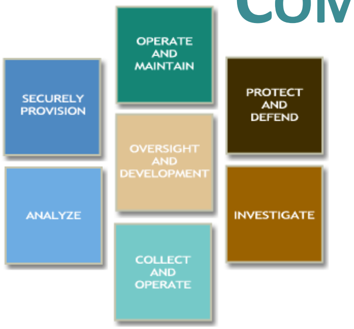
Data

- Competencies
  - – Personal Qualification Standards
- Learner models
  - –thru the activity not just complete

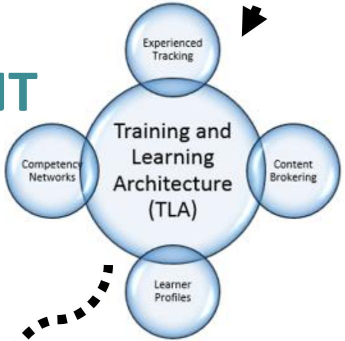
Data

- Security & IA
  - – Readiness, Personal data protection

COMPETENCIES



CONTENT



SECURITY

QUESTIONS and DISCUSSION

Dylan Schmorrow

dylan.schmorrow@soartech.com

Denise Nicholson

denise.Nicholson@soartech.com