Cyber Training Research in the Air Force Research Laboratory

Dee H. Andrews, Ph.D.
AFRL 711th Human Performance Wing
Organization
CURRENT RHAS CYBER S&T PROGRAM

Legend:
- SBIR
- EXPECTED SBIR CONTINUATION
- 6.2/6.3
- EXTERNAL FUNDS
- PROPOSED

Network Defense Simulation - CYDEST

Network Defense Game Environment

USAF Cyber Enterprise - Level Work domain analyses

Cyber fratricide workshops

Planning for AOC Defensive Response Against Cyber Attacks and Learning Approaches (DRACALA)

Safe computing enhancement with DoD funding

Cytber Operations Virtual Environment (COVE)

Distributed Training for Cyberspace Operations

DRACALA (FY11-FY15)
CURRENT RHAS CYBER S&T PROGRAM

- **LEGEND**
  - SBIR
  - EXPECTED SBIR CONTINUATION
  - 6.2/6.3 EXTERNAL FUNDS
  - PROPOSED

- **CY06**
- **CY07**
- **CY08**
- **CY09**
  - INSIDER THREAT TRAINING S&T (5 Phase I OSD contracts)
  - TRAINING SIMULATIONS FOR DIGITAL FORENSICS (1 USAF Phase I contract)
  - MICRO-GAMES FOR CYBER THREAT AWARENESS (2 USAF Phase I contracts)
- **CY10**
  - PHASE II INSIDER THREAT TRAINING S&T
  - EXPECTED PHASE II TRAINING SIMULATIONS FOR DIGITAL FORENSICS
- **CY11**
  - EXPECTED PHASE II MICRO GAMES FOR CYBER THREAT AWARENESS

DISTRIBUTED TRAINING FOR CYBERSPACE OPERATIONS
Simulation-Based Learning Environment for Network Defense

Develop a training system to enable CND analysts to learn fundamental concepts and practice their skills in a single platform that offers standard CBT and games and simulations for practical exercises.

Allow students to learn by doing in a safe and efficient practice environment and develop skills as Computer Network Defenders.

Intent is to improve operational decision-making effectiveness, and enhance knowledge retention over traditional learning methods.
XL-CITR - Accelerating Learning for Cyber Insider Threat Reduction

For further information, contact:
Terence Andre, Ph.D., Managing Director
TiER1 Performance Solutions
859-663-2115 x2241
t.andre@tier1performance.com
1. Be proficient in general security awareness
2. Be able to recognize employee predispositions
3. Be able to recognize employee behavioral patterns
4. Be able to manage employee expectations
5. Be proficient in detecting an insider threat
6. Be able to detect individuals who are high risk and have high liability to security
Learner accesses the XL-CITR system via web-based LMS

Learner takes competency-based pretest

After Action Reviews are based on Signal Detection Theory and provide opportunities for the learner to reflect on performance and adjust game play.

YOUR RESPONSE

“No” – Insider Threat
“Yes” – Insider Threat

2 3 4
2 3 4

Correct Rejection
Hit
Miss (relevant)
False Alarm (irrelevant)

Scenario-based games test proficiency on each competency and provide practice in applying knowledge and skills.
Accelerated Learning for Cyber Insider Threat Reduction

3. Personalized, accelerated pathway is generated
4. Post test confirms certification

Content is filtered based on pretest results to accelerate the learning pathway.

Reporting functionality provides summative data on learner’s performance.

Foundational knowledge is presented prior to game play using research-based design principles to accelerate the learning process.

Dynamic remediation is provided as needed when a learner scores poorly on specific learning objectives within game-based scenarios.

COURSE

Learning Objectives 1 2 3 4 5

PRE-TEST

MODULE 1

LESSON 1

LESSON 2

MODULE 1 TEST

MODULE 2

LESSON 1

LESSON 2

LESSON 3

MODULE 2 TEST

If LOs 3, 4, and 5, continue to Course Post-Test
OR
If LOs 4 and 5, but not 3, we recommend you review:
Lesson 1
Then try the scenario again.

TRY AGAIN

COURSE POST-TEST

ROLL UP RULES

MODULE 2 TEST

If LOs 3, 4, and 5, continue to Course Post-Test
OR
If LOs 4 and 5, but not 3, we recommend you review:
Lesson 1
Then try the scenario again.

TRY AGAIN

COURSE POST-TEST

ROLL UP RULES
Role-Play Game Concept

INSIDER THREAT ROLE-PLAY

Click any enabled character to begin a conversation.
RESIST-EM - Resisting Espionage & Sabotage with an Intelligent System for Training Expert Managers

For further information, contact:
Jared Freeman, Ph.D., Sr. VP Research
Aptima, Inc.
202-842-1548 x316 (voice)
freeman@aptima.com

Ó 2009, Aptima, Inc.
What RESIST-EM Trains: Training Objectives

- RESIST-EM training objectives are derived from research & theory
- RESIST-EM assesses & trains
  - Assessment of threat level
  - Attribution of threats to causes
    - Psychosocial factors: Greitzer (in review)
    - Environmental factors: Boye & Jones (1997)
    - Managerial factors: Traub (1996), etc.
    - Organizational policy factors: Cappelli (2006)
  - Actions taken on threats

Ó 2009, Aptima, Inc.
How RESIST-EM Trains: The Game Experience

• Search for clues (email, voicemail, reports…) in an office gamespace
  – Novice scenario – Bold cues
  – Journeyman scenario – Subtle cues
• Issue a report
  – Assess threats
  – Attribute threats to causes
  – Take action
• Review feedback
• Progress to next scenario
  – Training objectives adjusted dynamically based on assessment
  – Scenario generated dynamically

Ó 2009, Aptima, Inc.