

Florida Center for Cybersecurity

(FC2)

University of South Florida

(USF)

Adaptive Immersion Technologies

(AIT)



Unique Capabilities:

FC2:

- Access to researchers across 12 Florida State University System Institutions
- Academic and Research Outreach across Florida
- Top Secret Facility Clearance

USF:

- Cyber intelligence – collection and analysis of information concerning the intentions, capabilities, activities of adversaries and competitors in the cyber domain
- Combining information analytics and structured intelligence analytic techniques to develop operationally insider threat actor profiles (e.g., categories, databases)
- Discerning attack/activity trends within an industry or sector to develop probabilistic risk/threat assessments (e.g., targets, tactics)
- Integrating collection and knowledge management technologies to improve the efficiency of intrusion detection systems

AIT:

- Novel machine learning applications to complex human performance prediction problems
- Computational modeling of human performance with potential applications to insider threat modeling
- Technology-enabled performance assessment and diagnosis
- Algorithm development, optimization, and benchmarking for real time, simulation-based assessment
- Automated, generative simulation applications for personnel assessment, selection, training, and screening.

Open to further research in areas mentioned, to include:

- Cyber Intelligence
- Human Sensors
- Machine Learning
- Computational Modeling of Human Performance

Research areas of Interest:

- Development of novel methodologies for the measurement of insider threat behavioral signatures, network activity profiles, cognitive and conative attributes within specific organizational contexts
- Development of insider threat detection applications based on a process model that contextualizes insider cognition, intention, and behavior
- Pattern recognition of complex or covert activities within distributed, networked environments for insider threat detection
- Evolution and application of machine learning algorithms for complex pattern recognition and anomaly detection
- Development of insider threat actor profiles and categories based on psychological states and traits, capabilities, intentions, targets, activities
- Creation of complementary, integrated solutions for addressing insider threats that combine multiple pre-emptive and reactive components (assess, select, screen, detect)

Phillip M. Mangos, Ph.D.
President and Chief Scientist
Adaptive Immersion Technologies
Phillip.mangos@adaptiveimmersion.com
(813) 815 – 1999