CAREER: Understanding the Cognitive Processes of Computer Network Defense

SJSU SAN JOSÉ STATE UNIVERSITY

Challenges:

- Effective decision making by defenders remains a critical security layer.
- The NICE Framework defines knowledge and skills for cybersecurity defenders, but how human cognition supports defender knowledge and skills is poorly understood.
- A workforce shortage persists.

Solution:

- Use interviews of defenders from industry to understand expert and novice cognitive processes
- Observe defender cognition in a simulated incident response task
- Create new assessments of cognitive skills for defenders

Interview cybersecurity professionals to understand cognitive processes

⬇

Develop a method to observe cognition and performance in simulation

⬇

Develop training and assessments of cognition and decision making
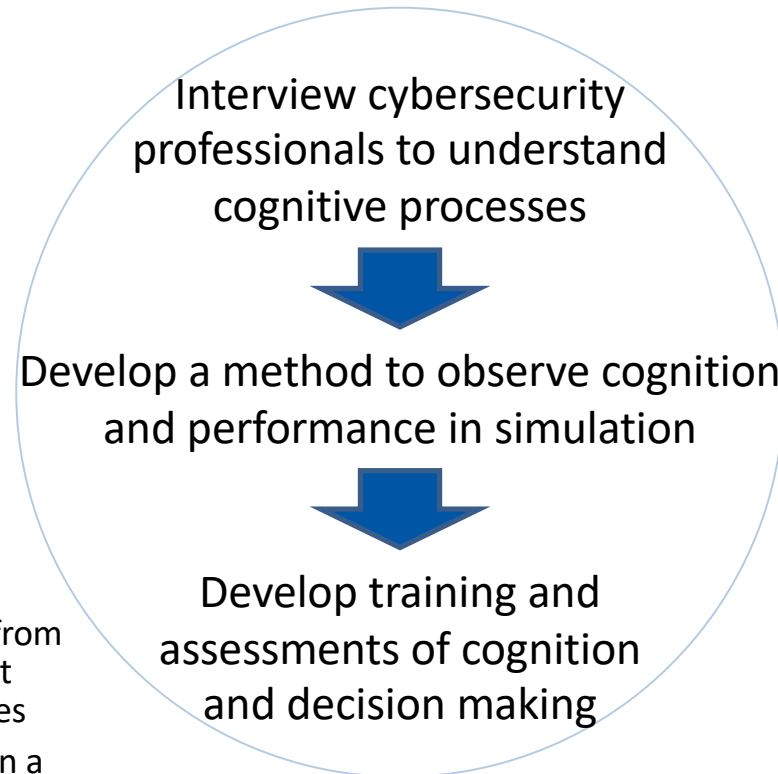
Scientific Impact:

- Knowledge of how expert defenders think can improve training, recruitment, and selection of novice defenders
- Low-cost simulation method facilitates observations of defender cognition
- Measures of cognition for cybersecurity defenders can be used to diagnose performance

Broader Impact and Broader Participation:

- Broaden recruitment, training, and participation of people in cybersecurity careers by matching relevant cognitive skills to job roles
- Improve human decision making to allow the cyber workforce to better adapt to evolving threats
- Inform the development of emerging automation to capitalize on human cognition

vectrlab.net