NSF Program: CICI

Program Area: SSC   **Award Number:** 1917117

PI: Hsinchun Chen

co-PIs: Sagar Samtani, Mark Patton, Peter Troch, Edwin Skidmore

Project Title: CICI: SSC: Proactive Cyber Threat Intelligence and Comprehensive Network Monitoring for Scientific Cyberinfrastructure

Hsinchun Chen
Regents Professor
AI Lab, U. of Arizona
hchen@eller.arizona.edu

Sagar Samtani
Assistant Professor
U. of South Florida
ssamtani@usf.edu

Mark Patton
Lecturer
U. of Arizona
mpatton@email.arizona.edu

Peter Troch
Professor
LEO, U. of Arizona
patroch@hwr.arizona.edu

Edwin Skidmore
Director of Infrastructure
CyVerse, U. of Arizona
edwin@cyverse.org

Quad Chart for: *CICI: SSC: Proactive Cyber Threat Intelligence and Comprehensive Network Monitoring for Scientific Cyberinfrastructure*

Challenge Project Seeks to Address:

- Modern computing technologies, scientific instruments have accelerated the rate of paradigm shifting scientific discoveries.
- Proprietary and custom software, applications, with unknown vulnerabilities.
- The risks to scientific facilities and how they can be attacked have not been properly mapped.

Scientific Impact:

- Advancements of cybersecurity data science capabilities
- Prioritized links will be disseminated at operational intelligence workshops and relevant conferences.
- Synergy with NSF funded SaTC and SFS programs.
- Integration into emerging and top-ranked MS in cybersecurity programs.
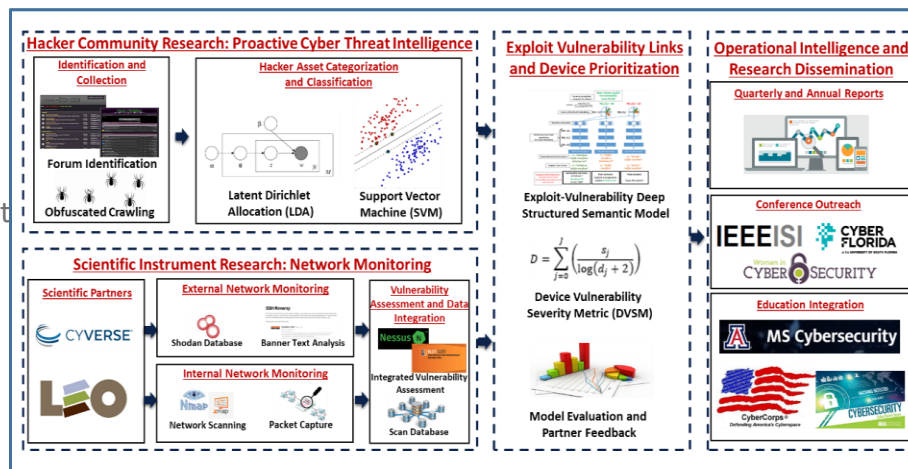
Solution(s):

- Partner with NSF funded interdisciplinary Earth sciences (LEO) and life sciences (CyVerse).
- Collect, categorize, and analyze a millions of hacker forum exploits.
- Comprehensively scan CyVerse/LEO internal/external networks for vulnerabilities
- Automatically link exploits and vulnerabilities via deep learning-based methods

Metadata tag:

- *Project starting up!*
- *Gathering data!*
- *Growing our dataset!*
- *Seeking collaborators!*