

AIXCC STAGE SCHEDULE

SUBJECT TO CHANGE

Friday, August 8th

- 12:30 PM

AI in OT Should be Cheaper Than in IT
Daryl Haegley, Technical Director, Air Force & Space Force Control Systems Cyber Resiliency
- 1:30 PM

Driving Tech Forward: A Fireside Chat with Perri Adams and Alexei Bulazel
Alexei Bulazel, Special Assistant to the President and National Security Council Senior Director for Cyber;
Perri Adams, Fellow, Institute for Security, Technology, and Society at Dartmouth College
- 2:05 PM

The Path Towards Self-Defending Systems
Heather Adkins, Google
- 2:40 PM

From Data Security to Discovery: How ARPA-H is Using AI to Transform Health Care in America
Jennifer Roberts, Ph.D., Resilient Systems Mission Office Director; Andy Kilianski, Ph.D., Program Manager and acting Health Science Futures Mission Office Deputy Director; Ross Uhrich, DMD, MBA, Program Manager; Andrew Carney, AIXCC Program Manager (moderator)
- 3:25 PM

Autonomous System Demo
Mike Walker, Senior Director at Microsoft Research
- 3:45 PM

An update from the LLM scaling laws frontier
Jason Clinton, CISO, Anthropic
- 4:20 PM

Orchestrating the Reasoners
Ken Harding, Competitor Interface Lead, Kudu Dynamics LLC; Jeff Casavant, Maintainer Interface Lead, Kudu Dynamics LLC; Scott Lee, Scoring & Challenge Research Lead, Kudu Dynamics LLC; Jon Silliman, Researcher Interfaces Lead, Kudu Dynamics LLC; Isaac Goldthwaite, Challenge Design Lead, Kudu Dynamics LLC; Nicholas Vidovich (moderator)
- 5:00 PM

Challenges and Lessons from the AIXCC Journey: A Perspective from 42-b3yond-6ug
Xinyu Xing, professor/President, Northwestern University / B3YOND
- 5:30 PM

“Robo Duck” Architecture
Tyler Nighswander, Theori

Saturday, August 9th

- 10:30 AM

Applying DevSecOps Lessons to MLSecOps
Christopher Robinson, Chief Security Architect, OpenSSF; Sarah Evans, Security Research Program Lead, Dell Technologies; Eoin Wickens, Director of Threat Intelligence, HiddenLayer; Jeff Diecks, Technical Project Manager, OpenSSF (moderator)
- 11:30 AM

Impossible Until It Isn’t: DARPA, Disruption, and the Future of Cyber
DARPA Director Stephen Winchell, I2O Director Kathleen Fisher, I2O Deputy Director Matt Turek; I2O PM Allison Kline
- 12:10 PM

The CMS.gov OSPO One Year Later: Launching the Agency’s First Bug Bounty!
Remy DeCausemaker, Open Source Program Office Lead, Digital Service at CMS.gov; Keith Busby, CISO, Office of Information Technology at CMS.gov; Patrick Newbold, CIO, CMS.gov
- 1:00 PM

ARTIPHISHELL Intelligence
Wil Gibbs and Lukas Dresel, Shellphish
- 1:40 PM

All You Need Is a Fuzzing Brain: A Retrospective
Jeff Huang, Professor, Texas A&M University; Ze Sheng, Graduate student, Texas A&M University; Qingxiao Xu, Graduate student, Texas A&M University; Matthew Woodcock, Undergraduate student, Texas A&M University
- 2:20 PM

Testing 1, 2, 3 Testing: Automatically Finding and Fixing Software Vulnerabilities at Scale and Speed
Dr. David Musliner, Staff, SIFT & Dr. Matt McLure, Researcher, SIFT
- 3:00 PM

Security Research: OpenAI's reflections and direction
Ian Breilinsky, Program Staff, OpenAI; Matt Knight, Vice President, OpenAI; Dave Aitel, Technical Staff, OpenAI
- 4:00 PM

Buckle Up, Buttercup - Our Experience Competing in AIXCC
Michael D. Brown, Principal Security Engineer and Head of AI/ML Security Research, Trail of Bits
- 4:40 PM

State of the Evals: Lessons from U.S. CAISI's Evaluations of Cyber Capabilities and Security in AI Models
Maia Hamin, Member of Technical Staff, U.S. Center for AI Standards and Innovation (CAISI)
- 5:15 PM

Team Atlanta’s Takeaways from DARPA's AIXCC
Taesoo Kim, VP at Samsung Research and Professor at Georgia Tech

Sunday, August 10th

- 10:30 AM

The Challenge with Designing Challenging Challenges
David Brumley, Scoring Advisor / CEO, Mayhem Security; Isaac Goldthwaite, Challenge Design Lead, Kudu Dynamics LLC; Tim Allison, Challenge Author & OSS Maintainer, Rhapsode Consulting; Chris Connelly, Challenge Author, MIT-LL; Sierra Haex, Challenge Author, Cromulence; Matt Turek, Deputy Director, DARPA's Information Innovation Office (moderator)
- 11:30 AM

The Human's Guide to Understanding AIXCC
Mark Griffin, Founder, Undaunted Development LLC