

Cybersecurity at MIT Sloan

Annual Members Only Conference Agenda

June 3, 2026

Cybersecurity and the Next Wave of AI Systems

Pre-Event Reception: June 2, 2026 – VIP Welcome Reception and Dinner

Location: MIT Samberg Conference Center, 50 Memorial Dr, Cambridge, MA 02142

Floor & Room: Samberg Conference Center, on the 6th floor

- Welcome & Networking & Cocktails
- Dinner & Discussions

Time: 6:00 PM – 8:30 PM

Cybersecurity and the Next Wave of AI Systems June 3, 2026

Location: MIT Samberg Conference Center, 50 Memorial Dr, Cambridge, MA 02142

Floor & Room: Samberg Conference Center, on the 6th floor

Time: 9:00 AM – 5:00 PM

Post-Event Member Networking June 3, 2026

Location: The Locke Bar, 6 Broad Canal Way, Cambridge, MA 02142

Time: Immediately following the conference from 5:00 PM – 6:30 PM

This conference will be available for remote participation via Zoom. In-person attendance is encouraged for the full conference experience.

8:30AM — Registration & Breakfast (30 min)

9:00AM — Conference Overview & Goals: Opening Remarks & Welcome (15 min Opening Remarks) Professor Stuart Madnick & Dr. Michael Siegel (MIT CAMS Directors)

9:15AM — The Escalating Agentic AI Arms Race between the Defenders and Attackers (45 min Academic Talk)

Professor Stuart Madnick, MIT CAMS Founder: "As we know AI can help people accomplish their job, even replace them sometimes. What if the job is to be a cyber defender or cyber attacker? What weapons can AI provide?"

10:00AM — Offensive AI Is Here. What Do We Do About It? (45 min Academic Keynote)

Dr. Yisroel Mirsky, Zuckerman Faculty Scholar, Head of the Offensive AI Lab, Institute of Software, Systems and Security, Ben-Gurion University: "The cybersecurity landscape is

undergoing a fundamental shift as adversaries move from simple scripts to autonomous AI agents."

10:45AM — Morning Break (30 min)

11:15AM — When Cyber Risk Becomes Non-linear, Governance Must Become Adaptive (30 min Academic Talk)

Dr. Sander Zeijlemaker, Research Affiliate, MIT CAMS: *"Through a worse-before-better transition, restoring strategic control"*

11:45AM — Poisoned Intelligence: How LLMs Are Reshaping Software Supply Chain Cybersecurity (60 min Panel)

Moderator: Dr. Ranjan Pal (MIT CAMS) Research Scientist

Panelists: Katrina Hill (Gallagher Re); Kristy Hornland (KPMG); Bridget Quinn Choi (Gallagher); Arjun Ramakrishnan (Mastercard)

12:45PM — Lunch & Member Networking / Poster Session (60 min)

1:45PM — From Tools to Agents: Cybersecurity in an Era of AI-Driven Attacks (45 min Industry Keynote)

Katie Moussouris, Founder & CEO, Luta Security: *"AI has crossed a threshold. It is no longer a behind-the-scenes assistant helping analysts spot threats. It is an active participant in cybersecurity itself, capable of reasoning, planning, and acting on its own, for defenders and attackers alike."*

2:30PM — Student Research Presentations (30 min Student Presentations)

Cynthia Zhang & Lillian Bluestein, MIT CAMS Students

Introduced by Dr. Ranjan Pal

3:00PM — Afternoon Break (30 min)

3:30PM — Securing the Next Generation of Self-Acting Enterprise AI Systems (60 min Panel)

Moderator: Dr. Michael Siegel (MIT CAMS) Director

Panelists: Ilya Kabanov (MIT CAMS); Katie Moussouris (Luta Security); Sandy Pentland (Stanford/MIT); Paul Quinn (Cisco)

4:30PM — Wrap-Up & Next Steps (15 min Closing Remarks)

Professor Stuart Madnick & Dr. Michael Siegel (MIT CAMS Directors)

5:00PM — Drinks & Networking at Locke Bar (90 min Member Networking)