# The 1st Human-Machine Intelligence for Security Analytics (HMI-SA)

(Collocated with IEEE SP 2025)

15 May 2025 @Hyatt Regency San Francisco

-0.1in

## Workshop Focus:

This workshop focuses on the pivotal role of human expertise and its integration with machine intelligence to enhance security analytics in an era of evolving cyber threats. It seeks to explore the synergy between machine intelligence technologies and human intuition within the security domain. The event is tailored to highlight the collaborative efforts between humans and machines, emphasizing the unique contributions of human judgment in conjunction with artificial intelligence-driven insights for cybersecurity. Key areas of discussion will include the development and application of collaborative systems for threat detection and response, the indispensable role of human interpretation in leveraging machine-generated data, and real-world case studies demonstrating successful human-machine integration in security operations.

## Themes of Interest:

- **Human-Centric Design in Security Analytics:**
  - User-centric metrics for measuring user Engagement, Satisfaction, Confidence, and Trust in human-machine collaboration.
  - Human factors impacting efficiency, effectiveness, and trustworthiness in security analysis.
  - Human-Computer Interaction (HCI) for security analysis.
- **Collaborative Security Analytics:**
  - Cognitive models for enhanced human-machine collaboration.
  - Formal methods for verifying consistency and correctness in human-machine collaboration.
  - (Semi-)Automated analytics for critical decision-making harnessing collective human and machine knowledge.
  - Explainable AI to bridge the gap between human understanding and machine decision-making.
  - Human-in-loop security analysis in the era of large language models.
- **Ethical and Social Considerations:**
  - Ethical deployment of human-machine intelligence systems in security analytics.
  - Social implications and acceptance.
- **Sustainable Human-Machine Intelligence for Cybersecurity:**
  - Long-term feedback mechanisms for continuous improvement.
  - Continuous knowledge adaptation to relevant emerging threats.
  - User-centric security awareness training initiatives.

## Tasks of Interest:

- Malware Detection
- Vulnerability Detection and Assessment
- Intrusion Detection
- Anomaly Detection
- Cyber Threat Intelligence Detection and Modeling
- Threat Analysis on AI-Generated Contents (Disinformation, Adversarial Attack)
- Biometric Security and User Authentication Analysis

## Workshop Organizers:

- Elisa Bertino, Purdue University
- Heng Yin, University of California, Riverside
- Kim-Kwang Raymond Choo, University of Texas at San Antonio
- Qian Fu, Commonwealth Scientific and Industrial Research Organisation (CSIRO), Data61
- Reza Ebrahimi, University of South Florida
- Ruitao Feng, Southern Cross University, Gold Coast
- Sin G. Teo, Agency for Science, Technology and Research (A*STAR)
- Xinming (Simon) Ou, University of South Florida
- Yang Liu, Nanyang Technological University
- Yuekang Li, University of New South Wales
- Yulei Sui, University of New South Wales

## Important Dates:

- Call for Proposals: **1 Nov 2024**
- Paper Submissions Due: **31 Jan 2025**
- Acceptance Notice to Authors: **20 Feb 2025**
- Publication-ready Papers Submitted: **1 Mar 2025**

## Workshop Details

For more details, please scan the QR code to visit the workshop webpage.