Call for Papers

Important dates

Paper submission deadline:
April 6, 2026
Authors' notification:
May 4, 2026
Camera-ready submission:
May 25, 2026
Registration deadline (authors):
May 25, 2026
Workshop dates:
August 3–5, 2026

Workshop chairs

General chairs

Fabio Martinelli (Italy)
Javier Lopez (Spain)

Program chairs

Sokratis Katsikas (Norway)
Cristina Alcaraz (Spain)

Technical program committee

- P. Bountakas (Switzerland)
- A. Cardenas (USA)
- M. Conti (Italy)
- R. Di Pietro (Saudi Arabia)
- V. Gkioulos (Norway)
- D. Gollmann (Germany)
- X. Huang (China)
- S. Ioannidis (Greece)
- N. Kaloudi (Norway)
- G. Kavallieratos (Norway)
- N. Kolokotronis (Greece)
- T. Kyriakakis (Greece)
- W. Meng (UK)
- O. Orta (Spain)
- A. Rashid (UK)
- R. Setola (Italy)
- K. Waedt (Germany)
- C. Xenakis (Greece)
- J. Zhou (Singapore)

Publicity chairs

Wenjuan Li (China)

Contact us

alcaraz@uma.es (C. Alcaraz)

CSAIP 2026 is the first workshop focusing on addressing the main challenges of proactivity and active defense. Its scope includes, among other things, the discovery, analysis, and mitigation of potential threats and vulnerabilities, complementing the approach with the principles of eradication and recovery as part of resilience. To fully embrace the concept of CSAIP, the event focuses on the protection and defense of large-scale hyperconnected networks. These include from large corporate networks to complex cyber-physical systems and the industrial Internet of Things, whose resources and services are essential to the proper functioning of industry and the social well-being.

Among the most representative and specialized areas of the event, we highlight those related to preparedness, situational awareness, information sharing, cyber intelligence, threat hunting, and advanced response and recovery. In all these cases, the time factor, efficiency, and quality of actions are essential to guarantee the overall effectiveness of defending high-reach networks with an impact on business continuity and productivity. This also means that new technological trends, such as artificial intelligence (AI) and its derivatives (e.g., Machine Learning (ML), Deep Learning (DL), Large Language Models (LLM), or Generative AI (GenAI)); software agents supported by the notion of AI agentic; simulation, including digital twins and Cyber Ranges; blockchain; supercomputing or hybrid computing; among others, can become drivers for the proactivity and defense expected in large-scale hyperconnected networks.

The workshop will be held in conjunction with the IEEE CSR 2026 conference as a **physical event**, during August 3–5, 2026. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Governance, regulated management, and dynamic risk management
- Adversarial offense, modeling, and demonstrations
- Green proactivity through lightweight AI-enhanced approaches for CSAIP
- Advanced discovery, prediction and detection of threats and vulnerabilities
- Advanced attack response, playbooks, mitigation, eradication, and recovery
- Threat hunting through situational awareness, traceability, and feedback
- Cyber threat intelligence and coordination
- Sharing data, trust management and privacy issues
- Human-centered preparedness under dynamic approaches and simulation
- Auditing and accountability for situational awareness
- Practical use cases with useful demonstrations for hyperconnected networks deployed in Security Operations Centers (SOCs), operational networks, and strategic sectors such as energy, healthcare, transportation, manufacturing, etc.

The CSAIP 2026 workshop will accept **high-quality original research papers** presenting strong theoretical contributions; applied research and innovation results obtained from funded cyber-security and resilience projects; and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed **6 pages** (plus 2 extra pages, being subject to overlength page charges) in high-quality English and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore, subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website **`https://www.ieee-csr.org/CDR2026`**

Supported by

- **SYNAPSE, European project,** https://www.synapse-project.eu

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
SMC Homeland Security Technical Committee
LOGOS RI RESEARCH&INNOVATION