



2026 IEEE CSR Workshop on Information & Operational Technology security (IOSEC)

Call for Papers

Important dates

Paper submission deadline:
April 13, 2026
Authors' notification:
May 4, 2026
Camera-ready submission:
May 25, 2026
Registration deadline (authors):
May 25, 2026
Workshop dates:
August 3–5, 2026

The recent advancements in Information and Communication Technologies (ICT) have given the opportunity to private and public entities, including Critical Infrastructures and other Operators of Essential Services (OES), to offer new and innovative services while lowering their operational costs. These advancements however, are often hastily adopted without proper evaluation of their impact on security, leaving current Information Technology (IT) and Operation Technology (OT) systems vulnerable to various kinds of cyber-attacks. The CSR IOSEC Workshop aims to bring together viewpoints from diverse areas to explore the commonalities of security problems and solutions for advancing the collective science and practice of IT and OT security.

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 Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

Workshop chairs

Kostas Lampropoulos, (GR)
Ciprian Oprisa (RO)

Organizing committee

Manos Athanatos (GR)
Eva Rodriguez Luna (ES)
Vasileios Mavroeidis (NO)
Jasmin Cosic (DE)
Mays Al-Naday (UK)

Technical program committee

Aggeliki Aktypi (CY)
Serge Autexier (DE)
Mateusz Zych (NO)
Christos Chrysoulas (UK)
Rodrigo Diaz (ES)
Charles Frick (US)
Habtamu Abie (NO)
Fady Coptly (US)
Kostas Fysarakis (CY)
Sotiris Ioannidis (GR)
Lucian Itu (RO)
Frank Fransen (NL)
Reinder Wolthuis (NL)
Xavi Masip (ES)
Panagiotis Iliia (CY)

- Security architectures and frameworks for enterprises, SMEs, public administration, or critical infrastructures
- Threat modeling, detection, analysis, classification and profiling
- Artificial intelligence (AI)/machine learning (ML) and generative AI in cybersecurity
- Vulnerability risk assessment and management
- Secure and resilient software development
- Identity Management & Privacy enabling technologies
- Cybersecurity certification
- Cyber threat intelligence and collaborative defense
- Advancements in tools, processes, and approaches for security operations centers (SOC)
- Intrusion detection and prevention

The CSR IOSEC 2026 workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cybersecurity 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) 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/iosec>.

Supported by



Publicity chairs

Ovidiu Mihaila (RO)

Contact us

klamprop@ce.upatras.gr
ciprian.oprisa@cs.utcluj.ro