IEEE CSR 2025
Cyber Security and Resilience

Chania, Crete, Greece | August 4–6, 2025

https://www.ieee-csr.org

2025 IEEE CSR Workshop on Information and Operational Technology Security (IOSEC)

Call for Papers

Important dates

Paper submission deadline:
April 14, 2025
Authors' notification:
May 5, 2025
Camera-ready submission:
May 26, 2025
Registration deadline (authors):
May 26, 2025
Workshop dates:
August 4–6, 2025

Workshop chairs

Kostas Lampropoulos (GR)
Ciprian Oprisa (RO)

Organizing committee

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

Technical program committee

Aggeliki Aktypi (UK)
Serge Autexier (DE)
Christos Chrysoulas (UK)
Fady Copty (IL)
Rodrigo Diaz (ES)
Kostas Drakonakis (GR)
Charles Frick (US)
Kostas Fysarakis (CH)
Panagiotis Ilia (CY)
Sotiris Ioannidis (GR)
Lucian Itu (RO)
Stylianos Karagiannis (GR)
Odysseas Koufopavlou (GR)
Xavi Masip (ES)
Vassilis Prevelakis (DE)
Mateusz Zych (NO)

Publicity chairs

Ovidiu Mihaila (RO)

Contact us

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

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 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 2025 conference as a **physical event**, during August 4–6, 2025. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- 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 and 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 workshop will accept high-quality 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) 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

PHOENIIX
CyberSecDome
CUSTODES
SAND5G
NATWORK
CONSOLE PROJECT
Cybersecurity for Resilient Software Development
NGSOC
Next Generation Security Operations Centres
CONSENTIS
SecOPERA

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