Call for Papers

Important dates

Paper submission deadline:
June 3, 2024 AoE
Authors' notification:
July 3, 2024 AoE
Camera-ready submission:
July 14, 2024 AoE
Early registration deadline:
July 20, 2024 AoE
Workshop dates:
September 2–4, 2024

Workshop chairs

Kostas Lampropoulos (GR)
Vasileios Mavroeidis (NO)

Organizing committee

Fady Copty (IL)
Manos Athanatos (GR)
Mateusz Zych (NO)
Eva Rodriguez Luna (ES)
Jasmin Cosic (DE)
Panagiotis Ilia (CY)

Technical program committee

Aggeliki Aktypi (UK)
Serge Autexier (DE)
Luis Miguel Campos (PT)
Christos Chrysoulas (UK)
Hervé Debar (FR)
Rodrigo Diaz (ES)
Kostas Drakonakis (GR)
Charles Frick (US)
Kostas Fysarakis (CH)
Nenad Gligorić (RS)
Jassim Happa (UK)
Sotiris Ioannidis (GR)
Lucian Itu (RO)
Stylianos Karagiannis (GR)
Odysseas Koufopavlou (GR)
Alexios Lekidis (GR)
Marco Manso (PT)
Eva Marin (ES)
Xavi Masip (ES)
Ciprian Oprisa (RO)
Vassilis Prevelakis (DE)
George Spanoudakis (UK)

Publicity chairs

Diana Guardado (IE)
Ovidiu Mihaila (RO)

Contact us

klamprop@ece.upatras.gr
vasileim@ifi.uio.no

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 (i.e., expanding and complicating their attack surface), thus leaving current Information Technology (IT) and Operation Technology (OT) systems vulnerable to various kinds of cyber-attacks. Motivated by this landscape, 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 is held in conjunction with the IEEE CSR 2024 conference as a **hybrid event**, during September 2–4, 2024. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following: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
- Intrusion detection and prevention
- Secure and resilient software development
- Privacy enabling technologies
- Cybersecurity certification and standardization
- Cyber threat intelligence and collaborative defense
- Advancements in tools, processes, and approaches for security operations centers (SOC)

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
JCOP
CUSTODES
CONSOLE PROJECT
Cybersecurity for Resilient Software Development
Synapse
NGSOC
Next Generation Security Operations Centres

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