

# 2021 IEEE CSR Workshop on Actionable Cyber Threat Intelligence (ACTI)

## Call for Papers

### Important dates

Workshop papers' deadline:

**April 19, 2021**

Workshop authors' notification:

**May 3, 2021**

Camera-ready submission:

**May 10, 2021**

Early registration deadline:

**May 31, 2021**

Workshop's date:

**July 28, 2021**

Over the past recent years, Cyber Threat Intelligence (CTI) has attracted a considerable attention and investment from the cyber security research community. As such, CTI standards, definitions and practices have reached a notable maturity level; the direction towards standardization of CTI exchange languages such as Structural Threat Information Exchange (STIX), Incident Object Description Exchange Format (IODEF) as well as the efforts for a systematic organization and curation of threats under popular frameworks such as MITRE's ATT&CK matrices, vulnerability databases and enumerations, have set the foundations for reaching a high situational awareness potential.

Actionable CTI is an international workshop aiming to expand and exploit the competencies delivered by the standardization efforts in CTI, by fusing this domain with enabling disciplines such as artificial intelligence and machine learning, risk management approaches, as well as best practices in SecOps and Early Warning System deployments, including reporting and crowdsourcing, in order to make the cyber security information and knowledge actionable and of high subsequent value. We also welcome research on novel designs and design methods to help empowering citizens with tools and literacy and increase their ability in recognizing, reporting and combatting threats.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- › Privacy compliance in CTI exchange
- › CTI in malware and vulnerability analysis
- › Sociotechnical aspects of CTI
- › CTI for smart cities, industrial and cyber physical systems
- › CTI datasets
- › CTI for cyber attribution
- › Data analysis and CTI
- › CTI and situational awareness
- › CTI in early warning systems
- › CTI quality and metrics
- › Psychological and cognitive aspects of CTI
- › Deception systems
- › Reporting and crowdsourcing for CTI
- › Cyber behavior and CTI
- › CTI and threat hunting

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. The workshop's proceedings will be published by IEEE and will be included in IEEE Xplore. Detailed information about the paper submission and guidelines to authors can be found at the workshop's website <https://www.ieee-csr.org/workshops/acti>

### Workshop chair

Vasilis Katos (UK)

### Organizing committee

Sotiris Ioannidis (Greece)

Florent Kirchner (France)

Wim Mees (Belgium)

Costantinos Patsakis (Greece)

Todor Tagarev (Bulgaria)

Cagatay Yucel (UK)

### Program committee

Raian Ali (Qatar)

Saif Al-Kuwari (Qatar)

Louis Galindo Sanchez (ES)

Evaldas Bruze (Lithuania)

Fran Casino (Greece)

Ioannis Chalkias (UK)

Jane Henriksen-Bulmer (UK)

Ahmet Koltuksuz (Turkey)

Theodoros Kostoulas (Greece)

Cornelius Ncube (UAE)

Marcin Niemiec (Poland)

Notis Mengidis (Greece)

Andrii Shalaginov (Norway)

Nikolai Stoianov (Bulgaria)

Theodora Tsikrika (Greece)

Egidija Versinskiene (Lithuania)

Antonis Voulgaridis (Greece)

Stefanos Vrochidis (Greece)

### Publicity chair

Marton Kis (Hungary)

### Contact us

[cert@bournemouth.ac.uk](mailto:cert@bournemouth.ac.uk)

### Supported by

