IEEE CSR 2022
Cyber Security and Resilience
Virtual Conference | July 27–29, 2022
https://www.ieee-csr.org

2022 IEEE CSR Workshop on Actionable Cyber Threat Intelligence (ACTI)

Call for Papers

Important dates

Workshop papers' deadline:
~~April 22~~ May 20, 2022
Workshop authors' notification:
~~May 13~~ June 10, 2022
Camera-ready submission:
~~May 27~~ June 24, 2022
Early registration deadline:
June 24, 2022
Workshop's date:
July 27–29, 2022

Workshop chairs

Vasilis Katos

Organizing committee

Sotiris Ioannidis
Florent Kirchner
Wim Mees
Costantinos Patsakis
Todor Tagarev
Cagatay Yucel

Publicity chairs

Pavel Varbanov

Contact us

cert@bournemouth.ac.uk

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Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following: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

Supported by

ECHO
CONCORDIA Cyber security cOmpeteNCe fOr Research anD InnovAtion
Cyber Security for Europe
SPARTA

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