IEEE CSR 2025
Cyber Security and Resilience
Chania, Crete, Greece | August 4–6, 2025
https://www.ieee-csr.org

2025 IEEE CSR Workshop on Generative AI Applications to Security of Cyber-Physical Assets (GAIA-SEC)

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

Fiammetta Marulli (IT)
Francesco Mercaldo (IT)
Alessandra De Benedictis (IT)

Organizing committee

Antonio Balzanella (IT)
Marianna Bifulco (IT)
Lelio Campanile (IT)
Emanuele Damiano (IT)
Maria Stella De Biase (IT)
Michele Mastroianni (IT)
Muddassar Naeem (IT)
Giovanni Paragliola (IT)
Vincenzo Reccia (IT)
Paolo Valletta (IT)

Technical program committee

Lelio Campanile (IT)
Maria Stella De Biase (IT)
Gladys Diaz (FR)
Cristian Martin Fernandez (ES)
Peter Kieseberg (AT)
Michele Mastroianni (IT)
Muddassar Naeem (IT)
Torsten Priebe (AT)
Ricardo J Rodiguez (ES)

Publicity chairs

Fiammetta Marulli (IT)

Contact us

fiammetta.marulli@unicampania.it
francesco.mercaldo@unimol.it
alessandra.debenedictis@unina.it

The workshop focuses on research advances and industrial applications of Generative Artificial Intelligence (AI) models and techniques in cybersecurity, investigating and obtaining an effective landscape of the current opportunities provided by meshing generative AI and cybersecurity to enhance defense strategies and systems and to observe novel threats and malicious opportunities raised by this combining Gen-AI and security.

Generative AI holds the potential to enhance cybersecurity by improving threat detection, but complete automation is not expected soon. Malicious actors are also investigating how generative AI can assist in cyberattacks by developing evolving malware. In today's landscape, both cybersecurity consumers and service providers have opportunities to leverage this new technology while ensuring their protection. Following the launch of ChatGPT and other products utilizing large language models (LLMs), the cybersecurity sector is strategizing to integrate generative AI as a crucial tool. Despite the initial challenge generative AI faces in cybersecurity due to the sensitive and isolated nature of security data, which hinders the acquisition of high-quality, comprehensive datasets required for training and updating LLM models. Currently, the primary focus lies in threat identification, where Generative AI is already contributing to the expedited detection of attacks and providing a more comprehensive assessment of their scale and potential impact. For instance, it aids analysts in more efficiently filtering out false positives from incident alerts. The capabilities of generative AI in threat detection and analysis are expected to become increasingly dynamic and automated.

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:

- Generative AI for intrusion detection and response
- Generative AI for malware analysis and prevention
- Generative AI for security testing and red teaming
- Generative AI for secure software development
- Generative AI for physical security
- Generative AI for privacy-preserving data analysis
- Generative AI for ethical hacking and cybersecurity education
- Generative AI for secure IoT device development
- Generative AI for supply chain security
- Generative AI for enhancing human–AI collaboration in cybersecurity
- Generative AI for adversarial machine learning in cybersecurity
- Generative AI for cybersecurity policy and regulation

The CSR GAIA-SEC 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/gaia-sec.