Call for Papers

Important dates

Paper submission deadline:
April 13, 2026
Authors' notification:
May 4, 2026
Camera-ready submission:
May 25, 2026
Registration deadline (authors):
May 25, 2026
Workshop dates:
August 3–5, 2026

Workshop chairs

Prof. Liqun Chen (UK)
Asst. Prof. Konstantinos Maliatsos (Greece)
Edgardo Montes de Oca (France)
Dr. Ahmed Walid Amro (Norway)

Organizing committee

Dr. Davide Ariu (Italy)
Dr. Evangelos Kafantaris (Greece)
Dr. Sophia Karagiorgou (Greece)
Ioannis Ledakis (Greece)
Prof. Fabio Roli (Italy)

Technical program committee

Dr. Aida Akbarzadeh (Norway)
Theodora Anastasiou (Cyprus)
Dr. Athanassios Giannetsos (Greece)
Dr. Evangelos Kafantaris (Greece)
Dr. Sophia Karagiorgou (Greece)
Dr. Georgios Kavallieratos (Norway)
Ioannis Ledakis (Greece)
Nikolaos Maragkos (Greece)
Dr. Sofianna Menesidou (Greece)
Ioannis Pastellas (Cyprus)
Katerina Samari(Greece)
Dr. Sarang Shaikh (Norway)

The CyberShield workshop focuses on showcasing cutting-edge innovations and methodologies developed through prominent EU-funded and National projects such as CyberSuite, APPtake, PROTEAS, NERO, TRITON, MIMESIS, SONIC, RHOE, DETANGLE, CertifAI, CYRUS, SEC4AI4SEC and CASTOR. These projects collectively address critical challenges in cybersecurity automation, trusted computing, resilience and defense and discusses how the integration of such operational assurance extensions can safeguard today's computing infrastructure. Especially considering the emergence of a new threat landscape characterized by both SW- and HW-level vulnerabilities that can bypass conventional protections and compromise the entire network. It, therefore, becomes a necessity to not only bootstrap trust for a system but been able to also equip it with runtime defense mechanisms (converging next-generation AI, confidential computing and formal trust assessment methods) to ensure its sustainable security: Elevating also the device-level trust quantification to Compute-Continuum-wide trust assessment by introducing adaptive-to-changes mechanisms for reacting to devices (HW and SW) trust score fluctuation (the Below-Zero-Trust paradigm).

The workshop will create a collaborative ecosystem to explore pioneering approaches in Security-as-a-Service (SECaaS), AI-driven threat and vulnerability detection, automated pentesting and ethical hacking, blockchain integration and abundant traceability, adversarial robustness, cybersecurity compliance and awareness training, collective threat intelligence, and incident response. The endmost goal is to spwan scientific debates on mission-aligned security and resilience solutions and the steps that we need to take –as a community- for rolling next-generation secure networks in the standards.

The scope spans applied research, mature technologies, and practical solutions—including tailored cybersecurity tools, methods for AI in cybersecurity and cybersecurity in AI, policy-driven security enforcement, proactive threat mitigation strategies and trusted path routing. Participants will gain valuable insights into how the research community and these projects collaborate to deliver comprehensive cybersecurity methodologies and frameworks, seamlessly integrating R&D outcomes with real-world applications.

This workshop aligns seamlessly with the IEEE Cyber Security and Resilience (CSR) conference themes, particularly by exploring cybersecurity resilience and compliance—a core pillar of the event. While the conference emphasizes theoretical advancements, CyberShield complements it through practical implementations, applied solutions, and real-world use cases.

The inclusion of EU-funded projects enriches the conference by:

1. **Widening at EU-level Specialized Cybersecurity Focus:** Spotlighting collaborative European initiatives that innovate in cybersecurity, addressing the unique needs of SMEs often overlooked in wider forums.
2. **Application-Oriented Insights:** Delivering hands-on demonstrations and case studies that bridge research and industry best practices.
3. **Collaborative Synergies:** Creating an interdisciplinary space to explore converging technologies like blockchain, AI and Generative AI (GenAI), pentesting automation, and cybersecurity analytics, sparking cross-sector partnerships.

This workshop serves as a dynamic addition to the IEEE CSR conference, advancing its mission to drive resilience, compliance and innovation in cybersecurity.

Publicity chairs

Dr. Sophia Karagiorgou (Greece)
Georgia Protogerou (Greece)

Contact us

gprotogerou@ubitech.eu

The workshop will be held in conjunction with the IEEE CSR 2026 conference as a **physical event**, during August 3–5, 2026. 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-as-a-Service (SECaaS) for SMEs
- AI-Driven Cyber Threat Detection
- Blockchain-Based Cybersecurity
- Cyber Resilience for SMEs
- Collective Threat Intelligence and Information Sharing
- Policy-driven Cybersecurity Deployments
- Proactive and Automated Pentesting and Ethical Hacking
- Next-generation trustworthy computing security solutions (e.g., TPMs, TEEs, RISC-V) and attacks
- Trusted Path Routing
- Social Engineering, Cybersecurity Awareness and Training
- Secure Integration of Digital Technologies
- Incident Response and Recovery
- Cyber Risk Assessment and Management
- Cybersecurity Metrics and Analytics
- Compliance and Legal Assessment and Mitigation Strategies in Cybersecurity
- Holistic Cybersecurity Lifecycle empowering Resilient Defense Methods
- Arms races and trade-offs in cyber-security vs. trust; vs. usability
- Trust management and reputation
- Secure communication protocols

The **CyberShield** 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/cybershield`.

Supported by

https://cybersuiteproject.eu/

https://www.apptake.eu/

https://edfproteas.eu/

https://certifai.info/

https://triton-edf.eu/

https://cyrus-project.eu/

https://www.sec4ai4sec-project.eu/

https://castorhorizon.eu/

https://nerocybersecurity.eu/

DETANGLE (TBA)

SONIC (TBA)

RHOE (TBA)

MIMESIS (TBA)