Connected 5G-IoT Cyber Range for Training and Secure Operation

NITRO

MISSION

NITRO aims to contribute to and foster the creation of a 5G-IoT cyber range, which refers to a specialized cybersecurity testing and training environment that focuses on simulating and evaluating the security of 5G networks interconnected with Internet of Things (IoT) devices and applications.

RESEARCH OBJECTIVE SCENARIOS

R01 Deliver a novel cybersecurity platform for virtualised 5G-IoT cyber range services.

R02 Create the first common Data Repository for 5G-IoT cyber ranges that will include attacks, threat analysis, scenarios for both 5G and IoT networks.

R03 Offer a powerful training environment for improving the preparedness of professionals (from staff in security operation centres to pen testers) through a variety of exercises.

R04 Deliver the first of its kind cyber range for adversarial AI attack and defence exercises to enable researchers and practitioners to enhance their understanding of adversarial AI techniques and explore strategies for building robust AI systems for 5G-IoT networks.

R05 Expand the access to cyber-range facilities to a broader range of stakeholders.

COMPLIANCE WITH SECURITY STANDARDS

NITRO will provide a platform that will abide by the existing standardisation work, including:

- EU Cybersecurity Act
- General Data Protection Regulation (GDPR)
- NIS2 Directive
- EU AI Act
- EU Cyber Resilience Act

CONSORTIUM

UNIVERSITY OF PIRAEUS · HELLENIC REPUBLIC IONIAN UNIVERSITY 1984 · HCSI HELLENIC CYBERSECURITY INSTITUTE · UBITECH ubiquitous solutions · uni.systems

NITRO project has received funding from the European Union's DIGITAL JU SME Support Actions under the grant agreement No. 101145872

Find us here!

Project Coordinator
Prof. Christos Xenakis
University of Piraeus Research Center
Email: xenakis@ssl-unipi.gr

nitro-project.eu

@nitroEUDEA