NITRO | Newsletter

Issue 2| February 2025

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

Project Coordinator

Prof. Christos Xenakis

School of Information and Communication Technologies
Department of Digital Systems,
University of Piraeus,
Karaoli and Dimitriou 80,
PC 18534, Piraeus, Greece

Tel: +30 210 4142776

Email: xenakis@ssl-unipi.gr

Project Details

G.A. number: 101145872

Project Website: nitro-project.eu

Project start: 01/01/2024

Duration: 36 Months

Total cost: EUR 1862656

EC Contribution: 101145872

Currently, the NITRO consortium has successfully finalised two deliverables that relate to the core cyber range architecture, testing, and validation plans. These achievements stem from efforts in WP2, titled "Requirements Analysis and Architecture Definition."

The consortium will now focus its attention on accelerating efforts in WP3 ("Cyber Security Training Exercises") and WP4 ("Scoring System and Gamification"). Work on WP2 will continue in parallel, while further dissemination activities will be reported in WP6 ("Dissemination, Communication, and Exploitation of Results").

By the end of Month 18, NITRO will have expanded on designing and implementing the training exercises for 5G-IoT networks and the scoring system that will be employed in connection with them.

CONSORTIUM

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

uni.systems

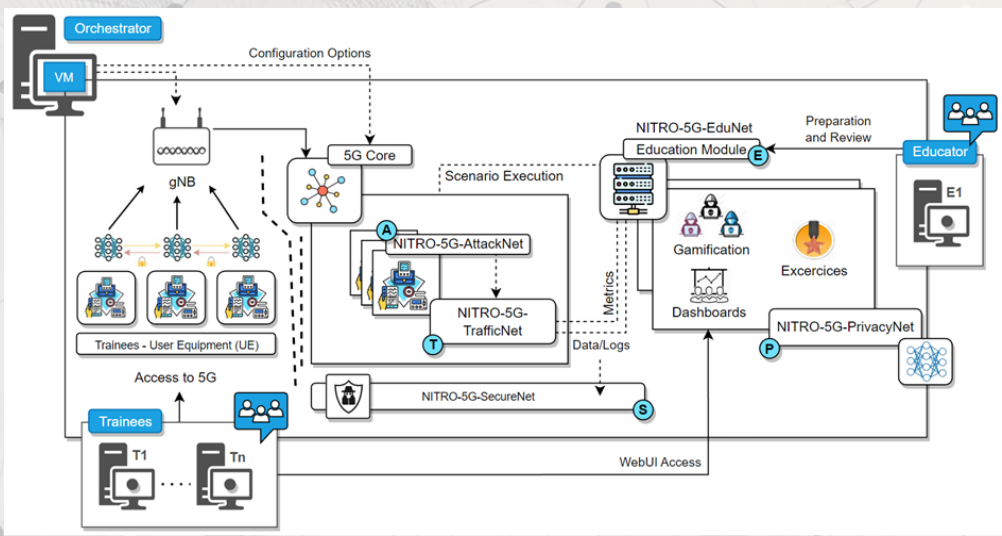
IONIAN UNIVERSITY

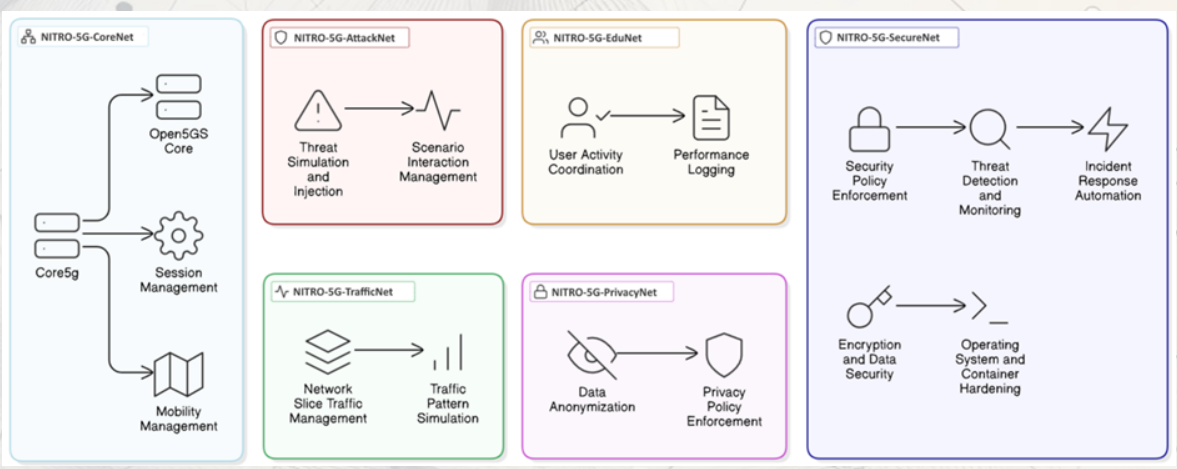
HCSI
HELLENIC CYBERSECURITY INSTITUTE

UBITECH
ubiquitous solutions

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

The NITRO Architecture & respective interfaces

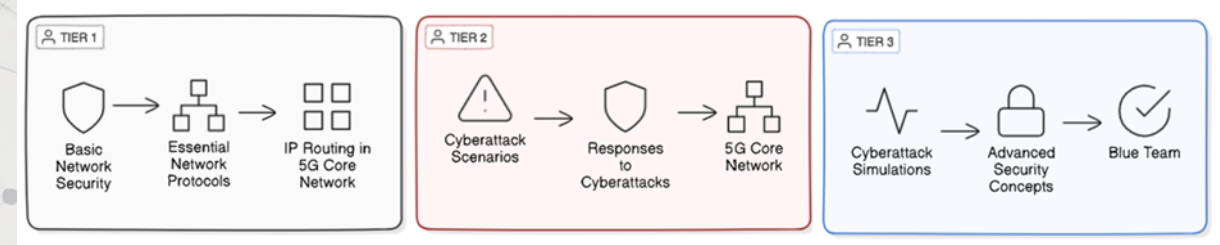




The NITRO architecture is a layered system engineered for interoperability across 5G components within a cyber range, facilitating authentic training and assessment of 5G network capabilities and security. The layers—**CoreNet, AttackNet, TrafficNet, EduNet, PrivacyNet, and SecureNet**—tackle essential functions like core network emulation, threat injection, traffic management, user engagement, data privacy, and security enforcement. Built on Open5GS and UERANSIM, it provides an emulated 5G environment for the examination of protocols and vulnerabilities. The Orchestrator guarantees smooth functionality via automation and Docker containers, while dashboards and data repositories support performance analysis. Incorporating gamification, AI, and Digital Twins, NITRO delivers immersive, secure, and dynamic training for addressing challenges in 5G and Beyond 5G networks.

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

NITRO's Trainee Groups



One of NITRO's primary goals is to offer customised cybersecurity training through exercises that develop practical knowledge of 5G and IoT security. The training groups within the cyber range are divided into three main categories: beginner, intermediate, and advanced. **Beginner trainees** concentrate on fundamental principles, including 5G architecture, network slicing, and basic IP routing inside Open5GS, as well as an overview of authentication, encryption, and access control. **Intermediate trainees** participate in simulations of actual assaults, such as replay, denial-of-service, data flooding, and eavesdropping, aimed at essential 5G components like the AMF and UPF, focusing on effect analysis and the implementation of mitigation mechanisms. **Advanced trainees** engage in vulnerability assessments, incident response methods, and adversarial AI methodologies, concentrating on the identification of system vulnerabilities, the management of security breaches, and the defense against assaults on AI-driven intrusion detection systems. NITRO, with the support of academic institutions, business partners, government agencies, and training organizations, ensures that these exercises are connected with industry needs, regulatory standards, and best practices, supporting overall skill development across all trainee levels.

NITRO News & Events

NITRO 5G-IoT Cyber Range Presentation at Ionian University during the Hellenic University Hack 2024

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

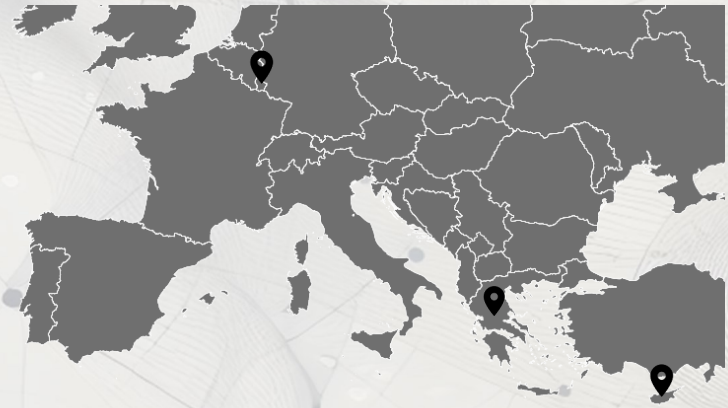
Hellenic University Hack 2024: NITRO 5G-IoT Cyber Range Featured at the University of Piraeus

Upcoming Deliverables and Future Activities

NITRO researchers are working on deliverables and tasks in order to fulfill all the main objectives where will lead toward the completion of the project.

In the next months, researchers will work *on the following deliverables*:

- **D1.3:** Project management report—first version
- **D3.1:** NITRO security training exercises design and development—first version
- **D4.1:** NITRO scoring and gamification system—first version
- **D6.2:** NITRO dissemination, communication and exploitation activity—second version



Find us here!

Website: nitro-project.eu

@nitroEUDEA

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