https://sand5g-project.eu/

SAND5G -Security Assessments for Networks anD services in 5G

Paris Kitsos, University of Patras

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

This article describes work undertaken in the context of the SAND5G project, “Security Assessments for Networks anD services in 5G” which has received funding from the European Union’s Digital Europe programme under grant agreement No 101127979 and is supported by European Cybersecurity Competence Center. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

SAND5G General Information

Project number	**101127979**
Project name	Security Assessments for Networks anD services in 5G
Project acronym	SAND5G
Call	DIGITAL-ECCC*-2022-CYBER-03
Topic	DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE
Type of action	DIGITAL-JU-SIMPLE
Service	CNECT/H/01
Starting date	1 January 2024
Duration	36 months

ECCC: European Cybersecurity Competence Center

Consortium

No.	Participant	Type	Country
1	Sphynx	SME	Switzerland-Greece
2	OQ Technology	SME	Luxemburg-Greece
3	Wings ICT	SME	Greece
4	University of Patras	Academic	Greece
5	P-NET	5G Competence Center	Greece
6	Hellenic Authority for Communication Security and Privacy (ADAE)	Authority	Greece
7	National Cyber Security Authority	Authority	Greece

Project summary

- 5G -and beyond- networks provide a strong foundation for EU's digital transformation
- Since 5G (and its future evolutions, 6G etc.) offers the fabric that connects EU systems and services, critical infrastructures, economy, etc., it is imperative to focus on the security, privacy, and trust challenges
- Securing 5G networks and the services running on top of them requires high quality technical security solutions and strong collaboration at the operational level
- All stakeholders (operators, vertical infrastructures, national authorities and public bodies, security experts, research community, etc.) must work together to build robust defenses and establish cooperation channels and practices for preparedness, incident handling, response and mitigation actions

Challenges

- **Challenge 1**: The EU and its Member States must adopt a comprehensive cybersecurity strategy.
  SAND5G will deliver a platform for 5G security assessment, active monitoring, and risk awareness for regulators and authorities.

- **Challenge 2:** Strengthening overall resilience, beyond cyber supply chain attacks, is essential.
  SAND5G will create a risk platform integrating data from assets, architecture, and physical components.

- **Challenge 3**: Member States should avoid strategic external dependencies and vendor lock-in in ICT services.
  SAND5G introduces a model-driven approach enabling flexible component replacement without redesigning security.

- **Challenge 4**: Highlights the strategic and operational importance of the European Cybersecurity Competence Centre and the National Coordination Centers.
  SAND5G will boost knowledge and capacity by linking 5G stakeholders, national authorities, and security providers.

Project objectives

- The primary goal of SAND5G is to provide a platform for risk and impact assessment tailored for 5G

- This platform aims to assist

  a) 5G stakeholders in enhancing the security of their systems and services

  b) National Authorities and Member States' Regulators in monitoring the security status and measures implemented to align with their respective national cybersecurity strategies and legislation, as well as European 5G cybersecurity policies and the proposed EU toolbox for 5G security

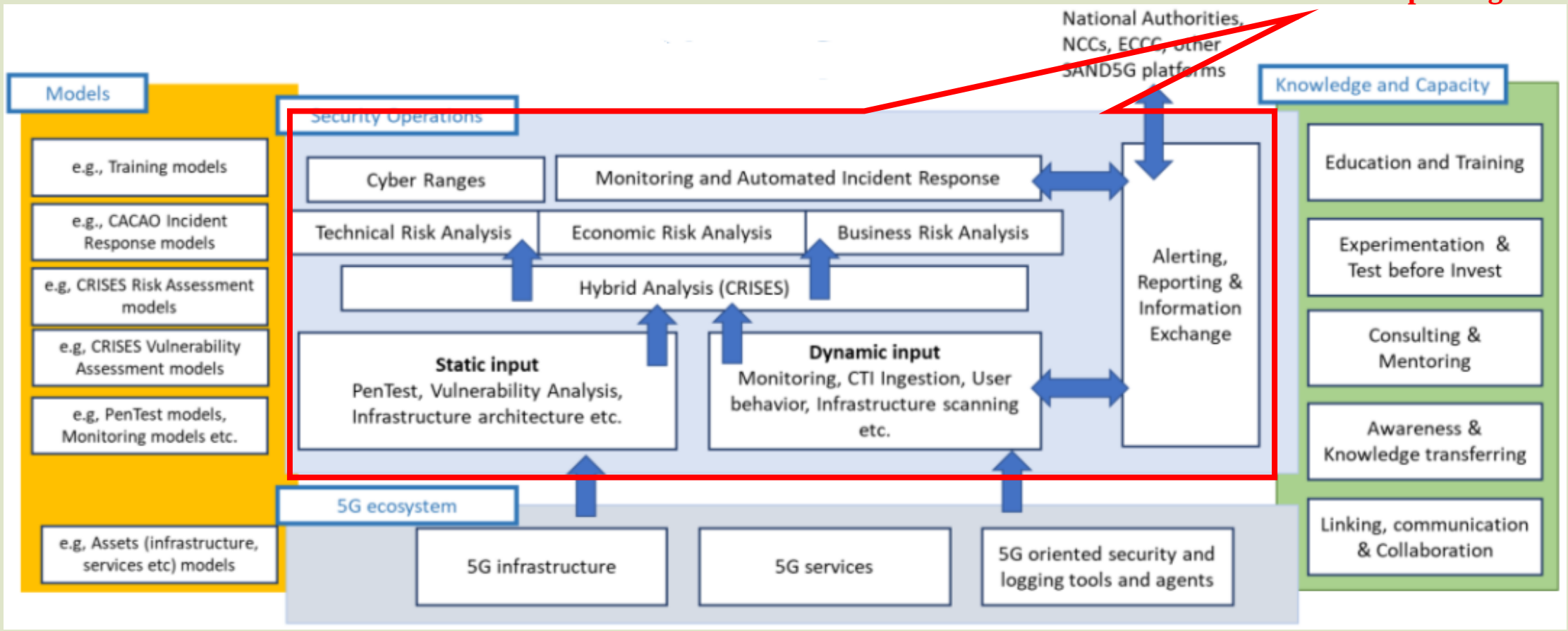
Architecture

- SAND5G project aims to develop a platform that can generate both technical and financial risk evaluations for stakeholders involved in 5G
  - Ensuring the security and compliance of their infrastructures and offerings with national cybersecurity strategies and telecommunications security frameworks
  - This platform will provide ongoing monitoring of 5G systems and incorporate automated Incident Response (SOAR - Security Operations and Automated Response) features for proactive defense

Architecture

Offers the proposed security functionalities

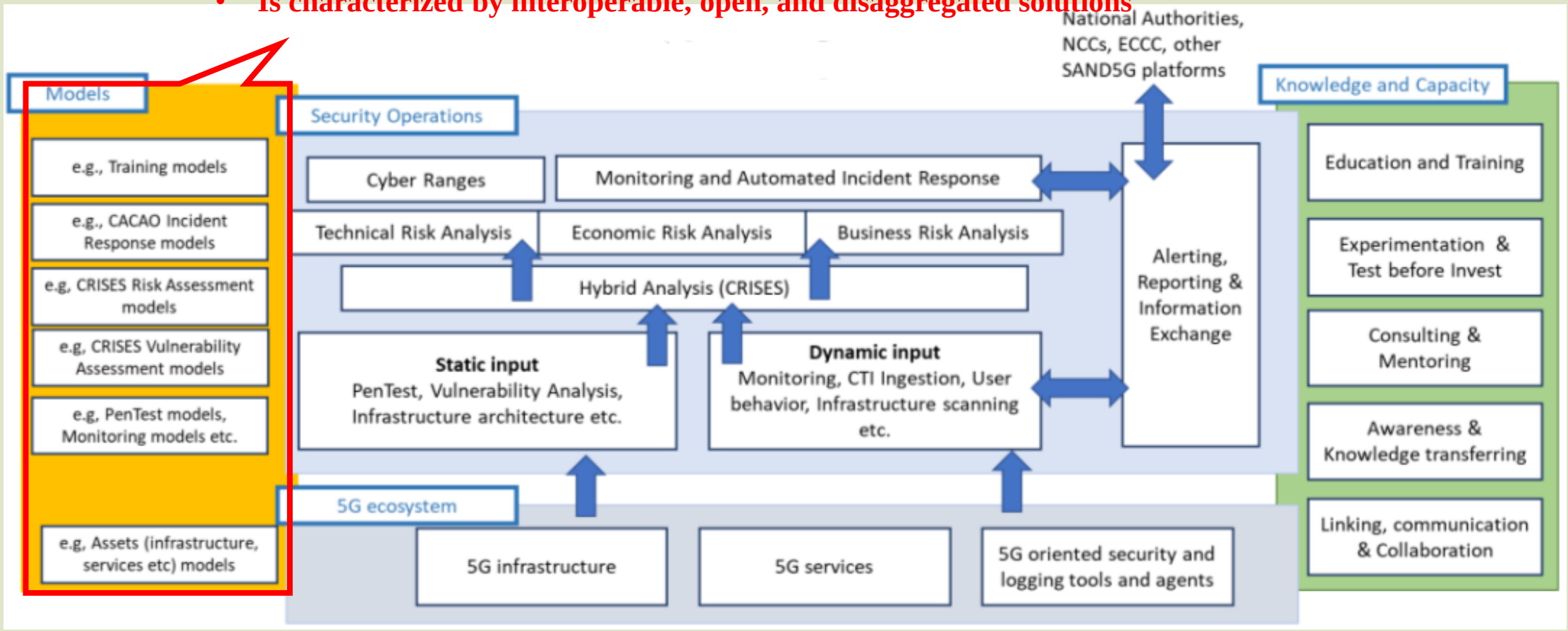
- **Protects the targeted 5G system**
- **Conducts real-time technical and financial risk assessments and reporting**



Architecture

Enables a customizable security platform capable of supporting 5G and future networks

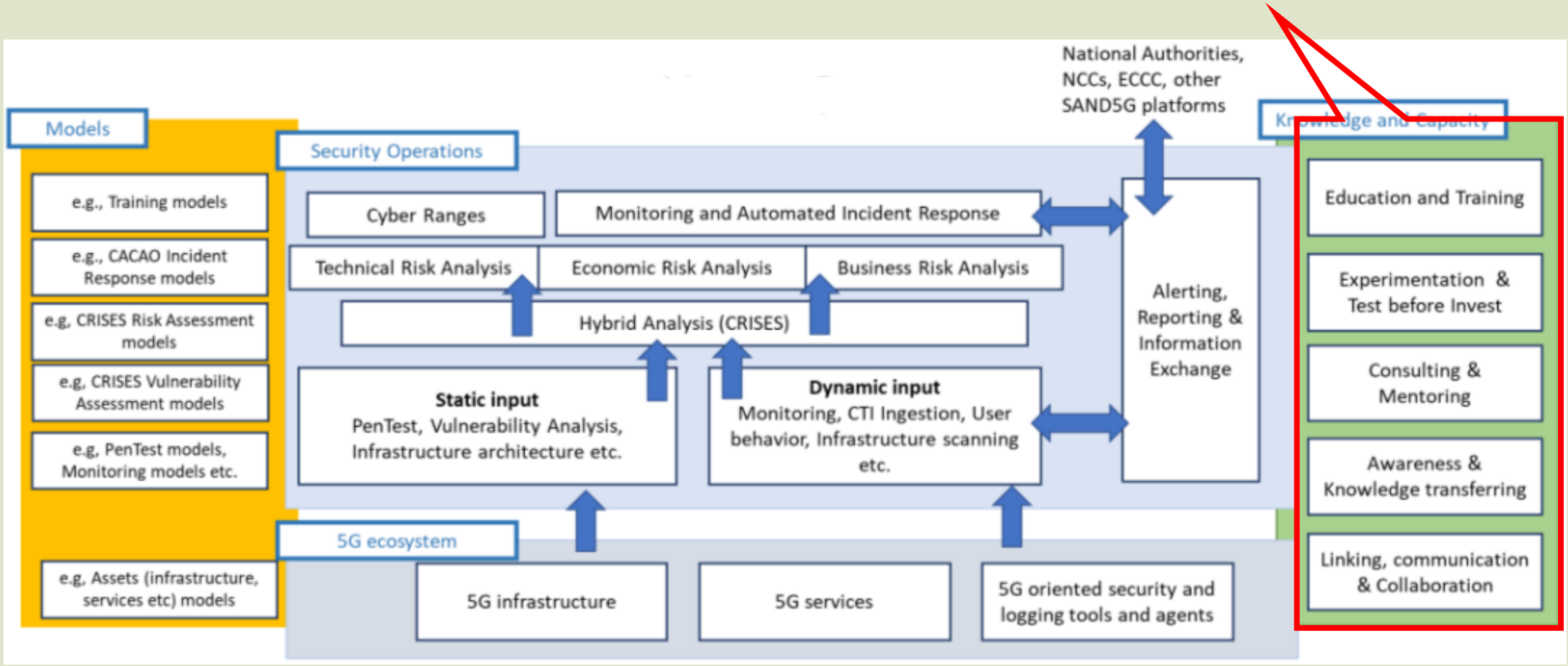
- **Is characterized by interoperable, open, and disaggregated solutions**



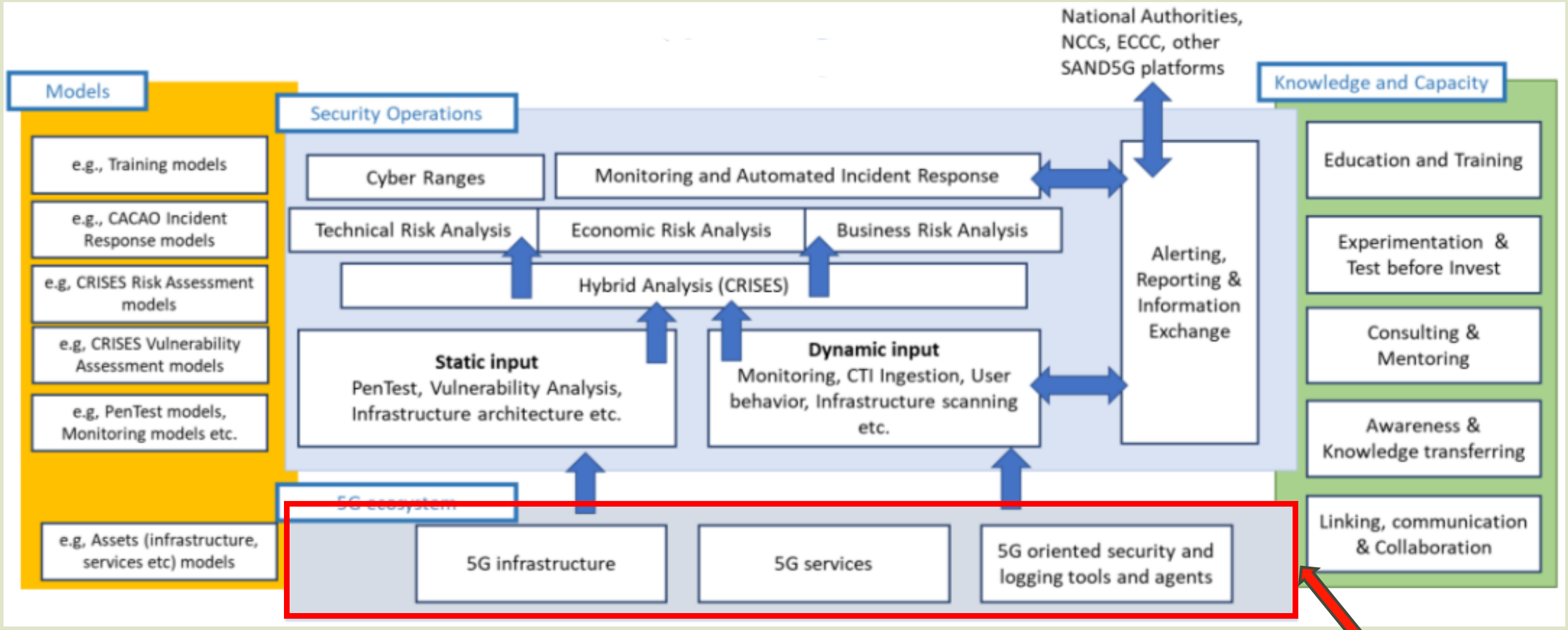
SAND5G

Architecture

Offers supportive services that go beyond the boundaries of a single 5G system or infrastructure



Architecture



Targets at improving the skills, awareness, collaboration etc. of the overall EU 5G ecosystem

SAND5G

Piloting - Validation

SAND5G will conduct some pilots to validate the proposed system

- Operators
  - This pilot focuses on aligning infrastructure with national policies and regulations while testing the security implications of new components in 5G systems
- Vertical providers
  - Two pilots aim to assess the security impact of integrating 5G technologies into their infrastructures and services
  - They will also develop models, playbooks, and training aligned with national and European cybersecurity policies
- Member States' Regulators and National Authorities
  - This pilot enables oversight of security measures at various levels (infrastructure, supply chains, nationwide) by regulatory bodies and national authorities

Thank you for your attention

SAND5G