Defending the digital future by harnessing novel technologies in critical networks

Mikko Karikytö

Chief Product Security Officer

Ericsson

AI from telecom security perspective

Security for AI

Securing AI integrated in mobile networks from adversarial attempts

AI for security

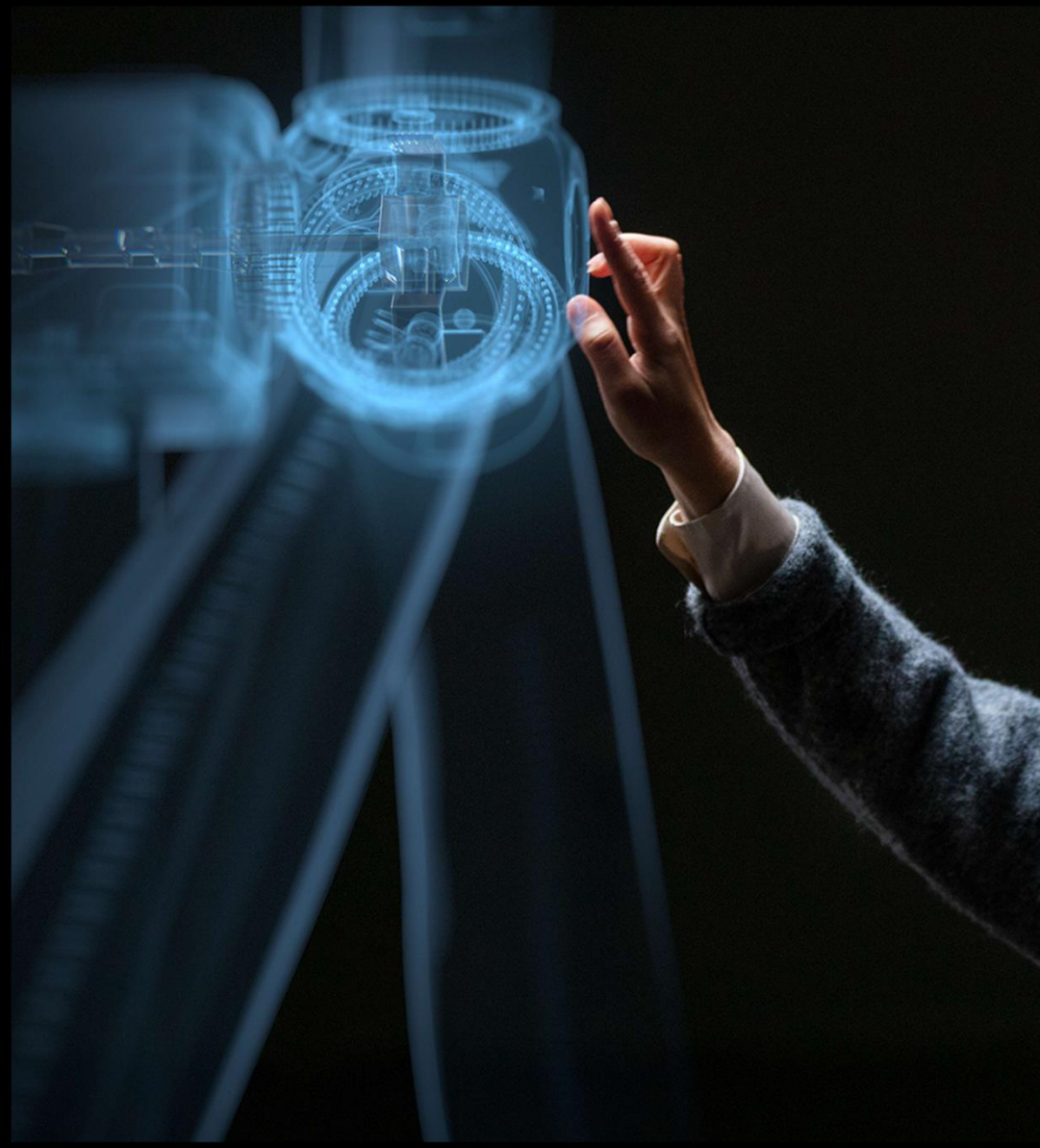
AI as a tool to enhance security of mobile networks

To unlock AI's full potential, the balance between risks and opportunities should be maintained.

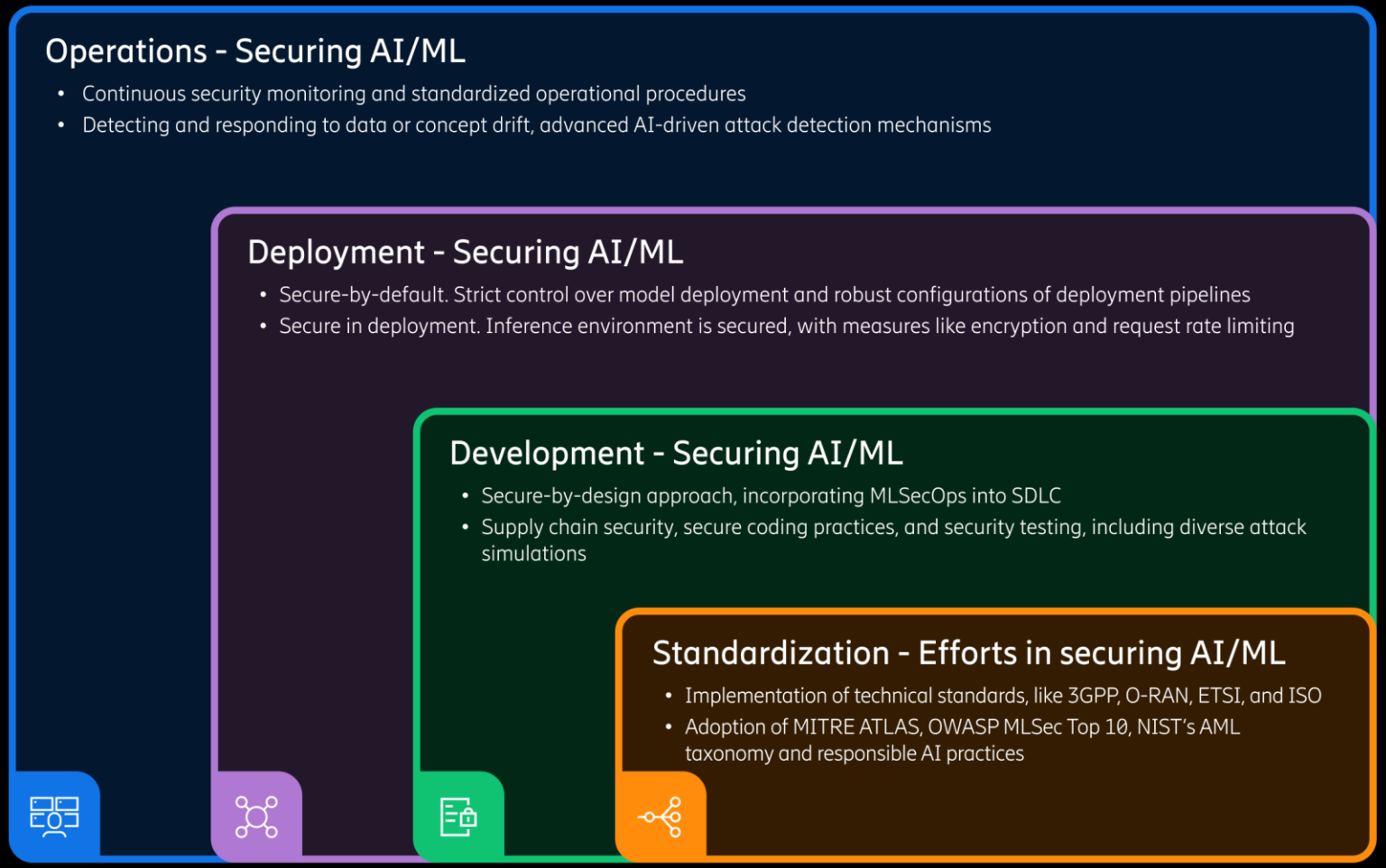
Increased awareness and diverse skill sets are required.

Collaborative efforts across organizations in academia, industry, standards organizations, and regulators to address AI´s unique security challenges are required.

A holistic approach to AI security is required, taking into account the four processes: standardization, development, network deployments and network operation.

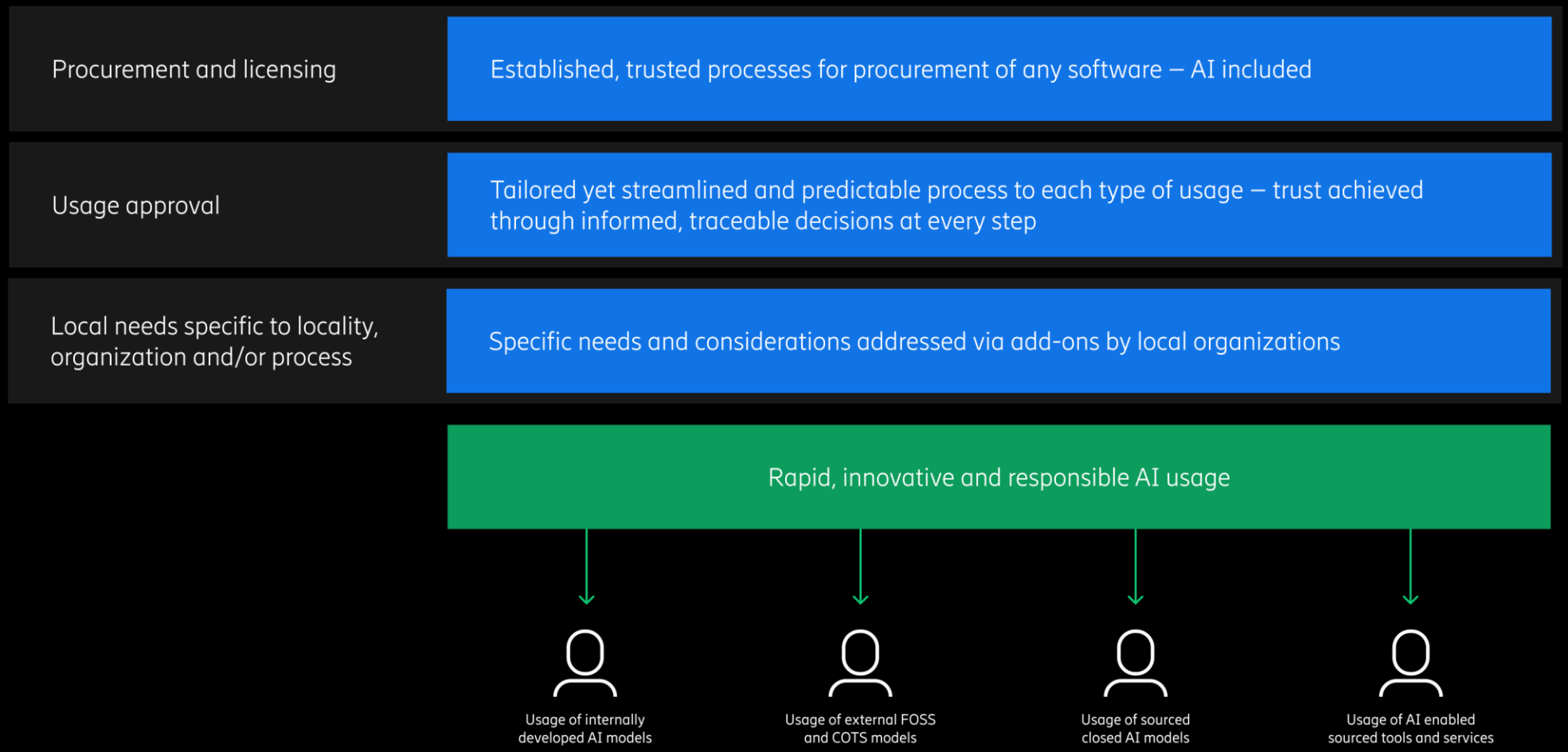


Securing AI using a holistic approach



- End users' experience of network security is determined by deployed networks.
- Security status of deployed networks depends on four inter dependent levels.
- Holistic approach to security includes all four levels.
- Operators are in control of operations, deployment and integrator and vendor selection.
- Vendors are in control of their product development and sourcing decisions (component suppliers).
- Standards are set in a multi stakeholder fashion.

Responsible AI overview



Responsible AI benefits

- Unlocking the innovation of the workforce ensuring responsible AI usage bringing faster and better AI features to customers
- A tailored yet consistent approach to varying types of AI usage, from internal to external, from Ericsson developed AI to sourced
- Designed to be future-proof, with agentic AI in mind
- End-to-end bidirectional traceability of which AI models were used where, by whom and how risk have been addressed


ERICSSON
www.ericsson.com/security