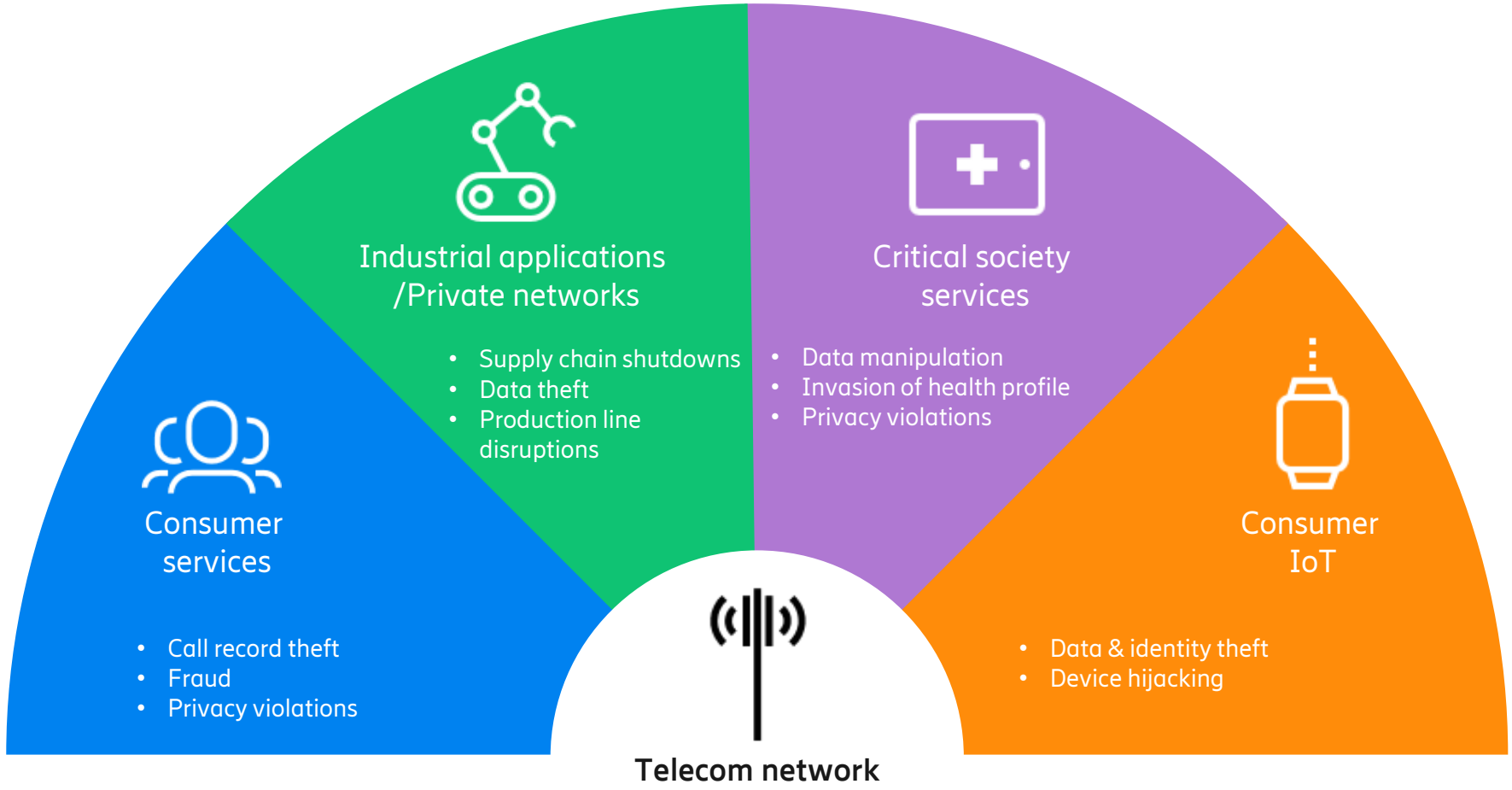
Protecting 5G end-users - a network perspective

Mikko Karikytö

Head of Product Security & CPSO
Ericsson

A telecom network today needs to be secure across multiple contexts and use-cases

As telecom networks have new, more demanding use cases, **attack motivations increase**, **attack vectors multiply** and the need to **protect the network grows exponentially**



Increased value at stake decreased-risk tolerance

5G
Game Changer

Enabler for new industrial use cases

Digitalization

Every company will become a digital company

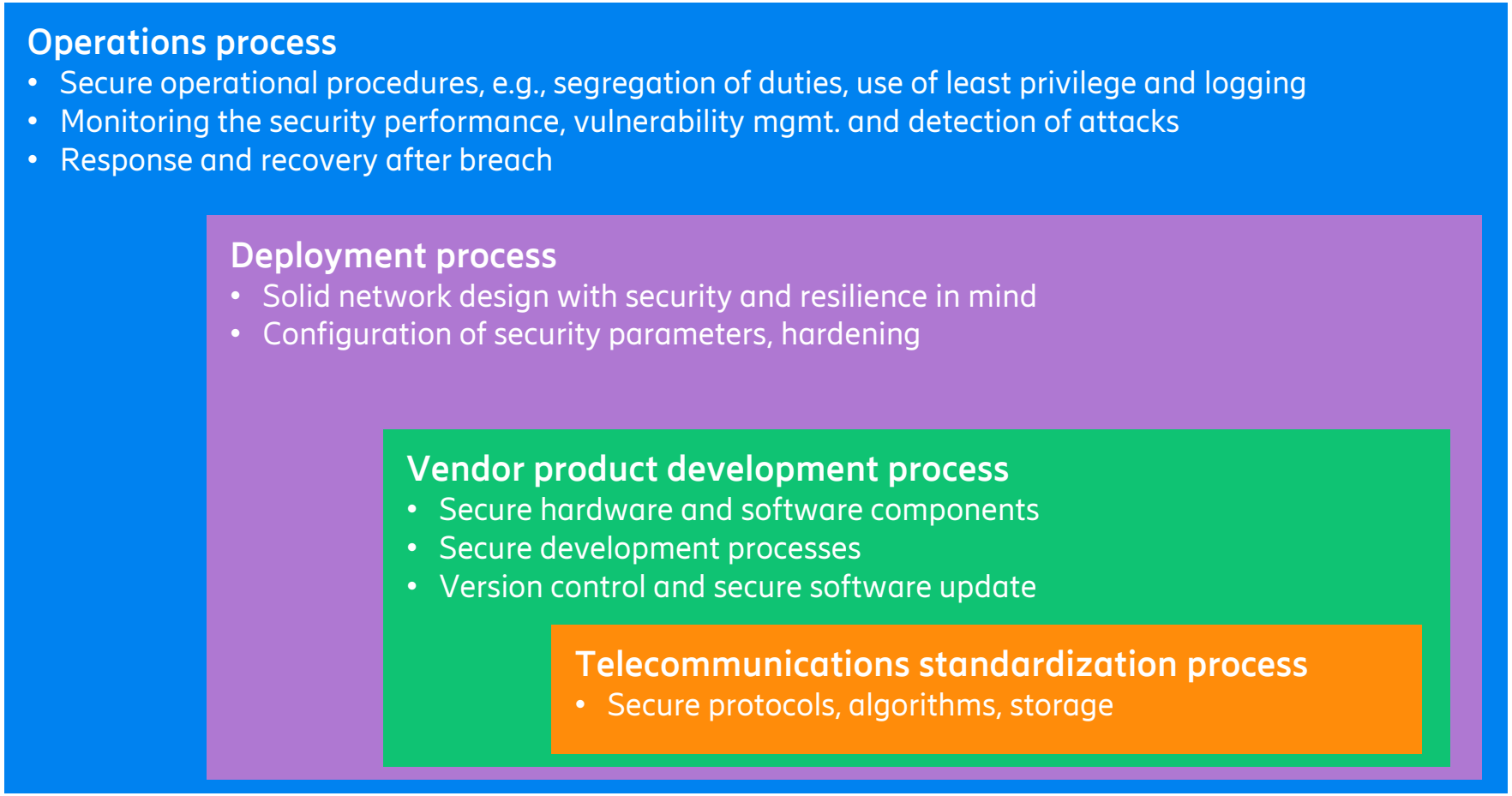
Systems
GO Mobile

New attack vectors emerge – IOT

Mission Critical
ICT Infrastructure

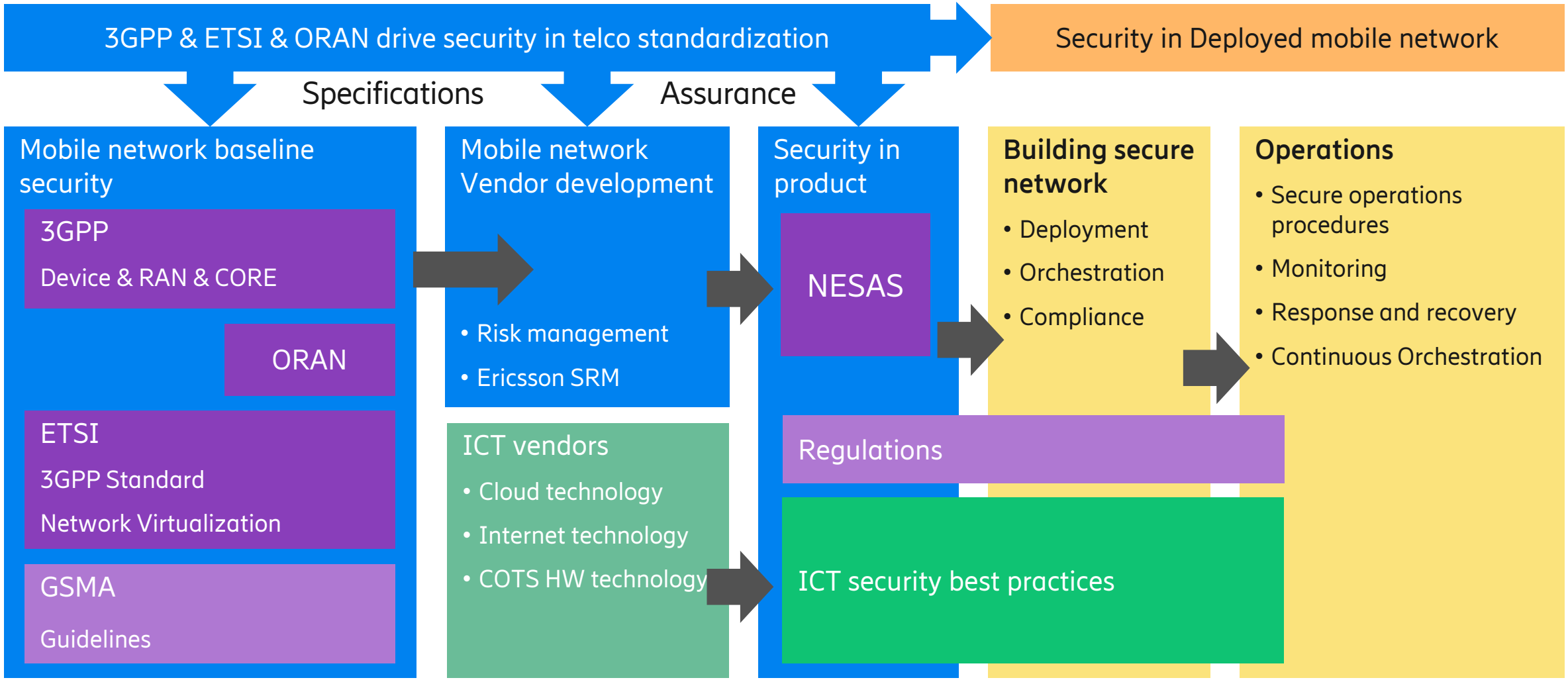
More value, concentrated more attacks

Ensuring security in deployed networks requires mitigation strategy on four levels



- End users' experience of network security is determined by deployed networks.
- Security status of deployed networks depends on four interdependent layers.
- 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.

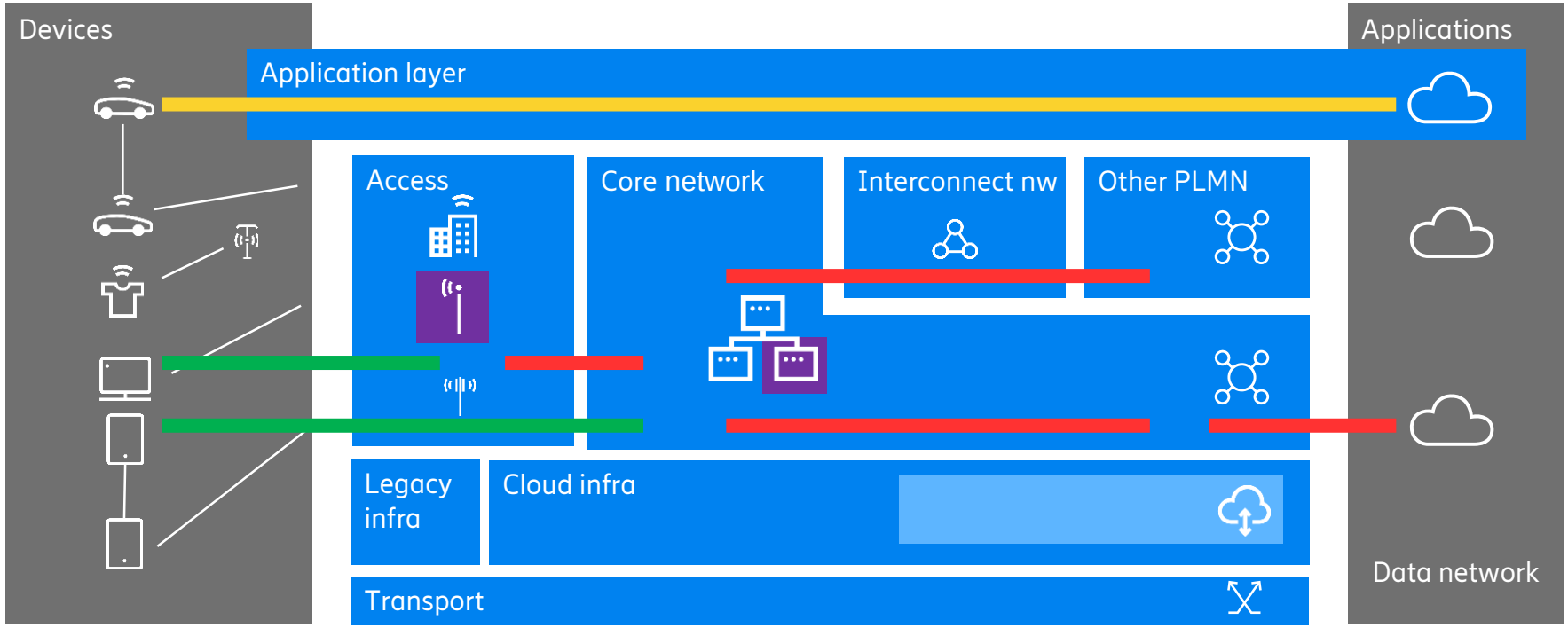
From security in standards to security in deployed networks



3GPP security area

In principle, all work in 3GPP SA3 can be divided into the following areas

- Application security
- UE to network access security
- Network to network security
- Security assurance
- Virtualization security*



Rel(ease)-15 created the foundation of security for the 3GPP 5G system.

Later releases have added enhancements to the system security and added security for features to enable new use cases.

Security Reliability Model (SRM) - Ericsson's risk management framework

Product value flow: The controls in SRM applies across the flow from component intake to operations in customer networks

Security Reliability Model

Functions	Assurance	Compliance & Documentation	Deployment & Operations
Functions implemented in products and solutions	Activities in the value flow that ensure that product security and privacy has been addressed throughout	Key documentation that supports the product and shows compliance	Activities in the value flow that ensure that the product is deployed and operated in a secure way and with compliance to privacy

Ericsson works with multiple perspectives to ensure secure networks

Develop

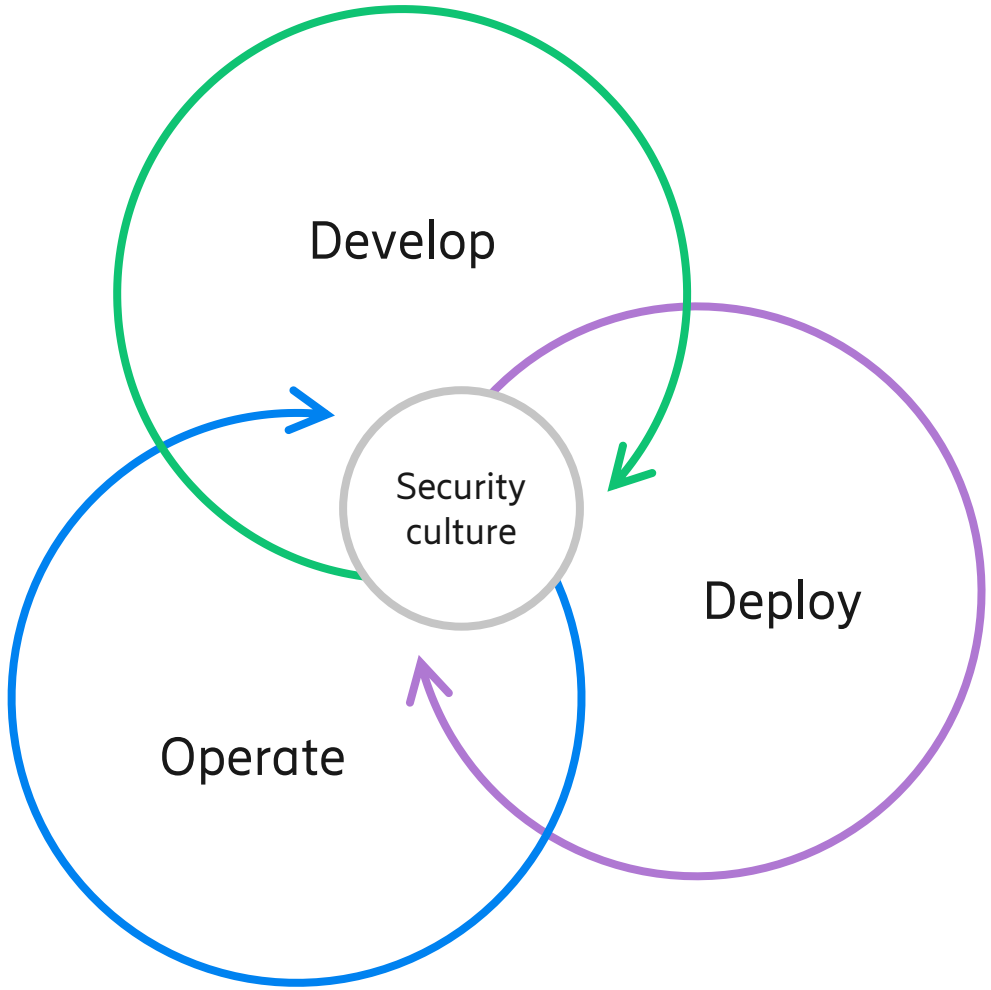
Ericsson develops secure products and solutions, built on the strong foundation of 3GPP, with a strong and rigorous security perspective, including a controlled supply chain, deep knowledge of existing and emergent threats, and the contexts where our products will be used.

Deploy

Ericsson works together with our customers to ensure solid deployments of our products and networks, with clear guidelines for secure configurations, handover and hardening of the network. We also work with our customers on to create an overarching secure architecture of the networks we build.

Operate

Ericsson works together with communication service providers in ensuring the security of networks in operations. Features in our products mitigate the risk of successful attacks; security solutions help CSPs detect, mitigate and respond to threats; and 24/7 incident response team captures and patches vulnerabilities in networks.

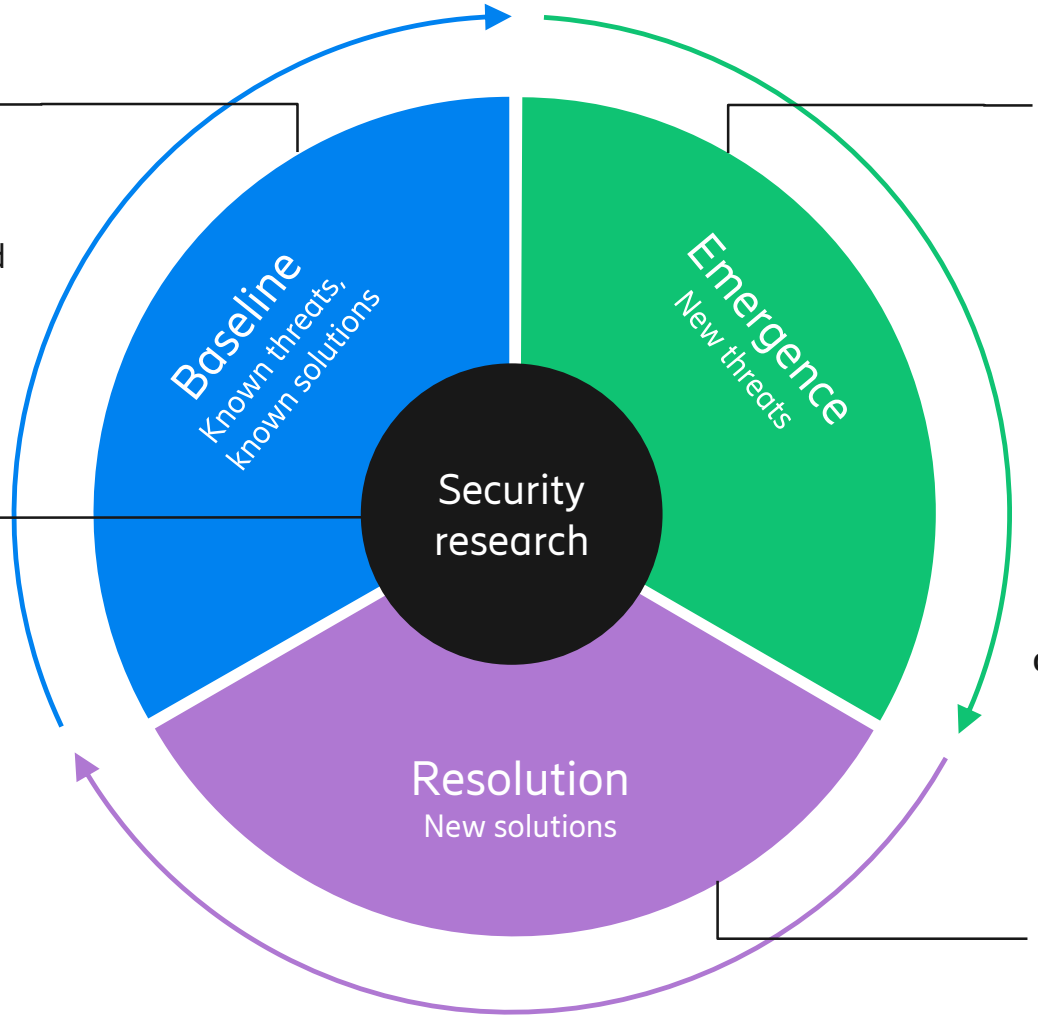


Strong security is built as a continuous process of learning by doing

Twenty years delivering security competence, new solutions, and technical proof points in:

- **Standardization of security for mobile networks -** 3GPP, IETF, GSMA, ETSI
- **Collaboration with business areas** and other parts of Ericsson
- **External collaborations:** EU-CONCORDIA, Hexa-X, UC Berkeley, RISELab, Concordia University, RISE Sweden

Ericsson Security Reliability Model
Embodies security practices and is continuously updated over time



PSIRT
Ericsson Product Security Incident Response Team tracks emergence of new vulnerabilities and threats that feed into new product development

Data-driven development and CI/CD
Developing solutions based on data from live networks and PSIRT, that are then continuously integrated and deployed in customers networks.

Key conclusions

- Increased value at stake – from personal information to mission critical
- Protecting end-users is about securing deployed networks in the field that render end-user services
- Holistic approach to protect end-user is necessary
  - Secure operations*
  - Deployment – architecture and configuration*
  - Vendor product security**
  - Global standards ***
- Mind the interdependencies between layers, avoid false sense of security
- No silver bullets, security is a continuous process

*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.

https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security