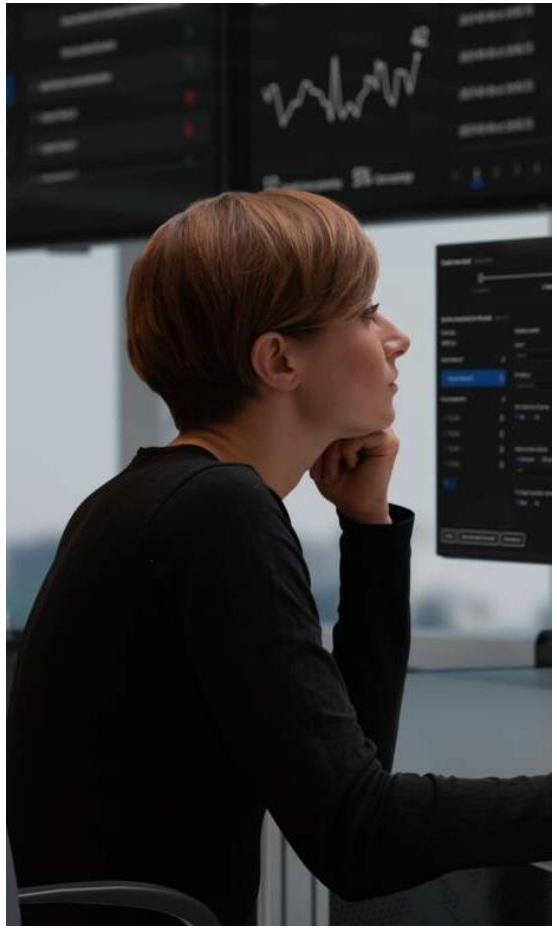
Ericsson Security Presentation US TTI event

7 June 2023
Plano, Texas

Mohammad Khaled
Director of security solutions

Content

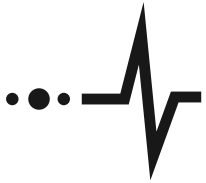


Threat and security landscape

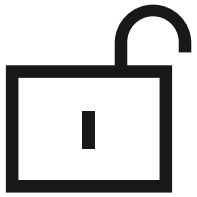
5G Security

Security Culture at Ericsson

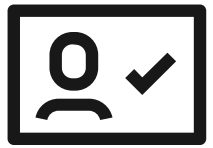
Evolving security and threat landscape



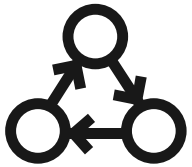
Critical infrastructure
and increased business risks



Constantly evolving
security threats



Increasing regulatory
requirements



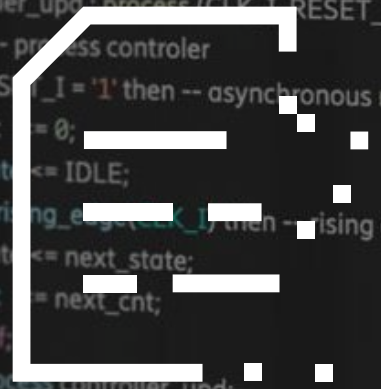
New deployment scenarios
and use-cases

Billions of new devices

5G specific challenges

Motivations for attacks diversify as networks become embedded in critical functions

Money



Information

Service Disruption

Threat actors often leverage vulnerabilities that are avoidable with sound security measures

- Organized cyber criminals
- Politically-motivated actors
- Hacktivists, e.g., “Anonymous”
- Insiders

Security policy not enforced or monitored

Lack of hardening & insecure configuration of the network

Operational procedures prone for mistakes

Lack of visibility, control & continuous monitoring

Increased regulatory demands on networks

"Network and information systems and services play a vital role in society. The **existing capabilities are not sufficient** to ensure a high level of security"

- EU Parliament

"The **private sector**, as owners and operators of the majority of communications infrastructure, is the **primary entity responsible** for protecting sector infrastructure and assets"

- Homeland Security, US

" [5G] will empower a vast array of new and enhanced critical services, from autonomous vehicles and telemedicine, to automated manufacturing and advances to traditional critical infrastructure, such as smart grid electricity distribution. **Given 5G's scope, the stakes for safeguarding these vital networks could not be higher"**

- Cybersecurity & Infrastructure Security Agency, US

Telecom networks used in new contexts and use-cases changes security requirements

Private cellular networks

Enterprises and organizations deploy 5G and cellular networks to connect factories so that connectivity becomes truly critical and security paramount.

Example of attacks and vulnerabilities

- Misconfigured networks and devices could be exposed through fake base stations, connecting the entire campus to a fake network, potentially shutting down the entire factory.
- Device fingerprinting, figuring out which kinds of devices that are connected to the network, could be achieved without proper configuration of the network.

Mission critical use-cases

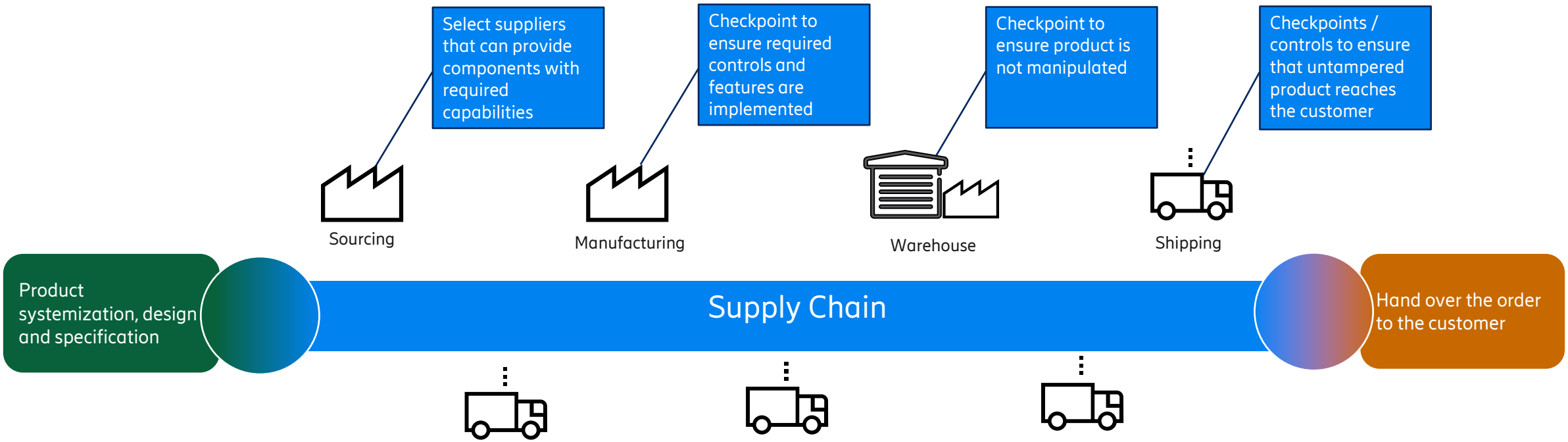
As new kinds of devices connect to service provider networks, new attack vectors and potential vulnerabilities emerge. The broad range of devices, with varying levels of built-in security, are becoming potential points of breaches.

Example of attacks and vulnerabilities

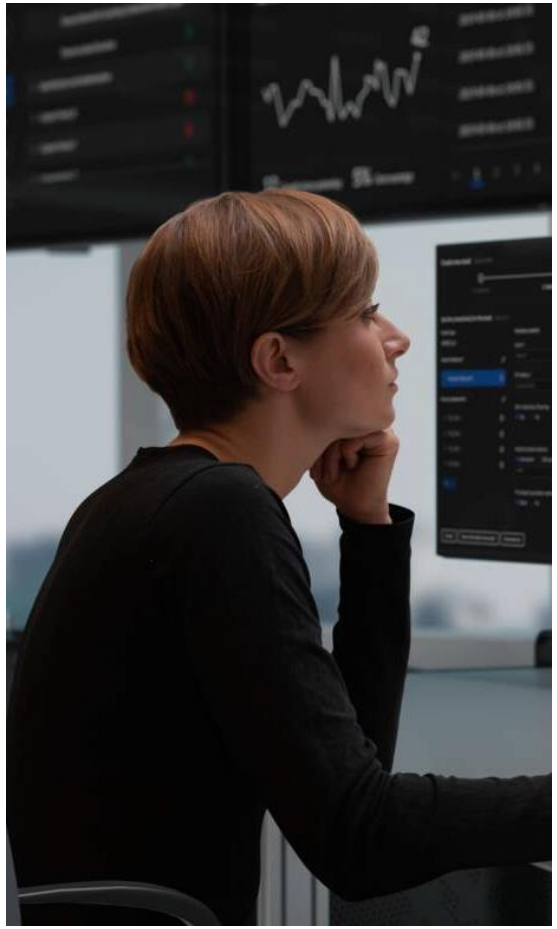
- Lack of security configuration in IoT devices due to lack of capabilities (weak local encryption, hardcoded passwords, lack of transport encryption are some examples that can be found)
- Lack of operational processes such as continuous update of firmware as new threats emerge or weak back-end security for management of IoT devices

Massive IoT networks

Supply Chain landscape



Content

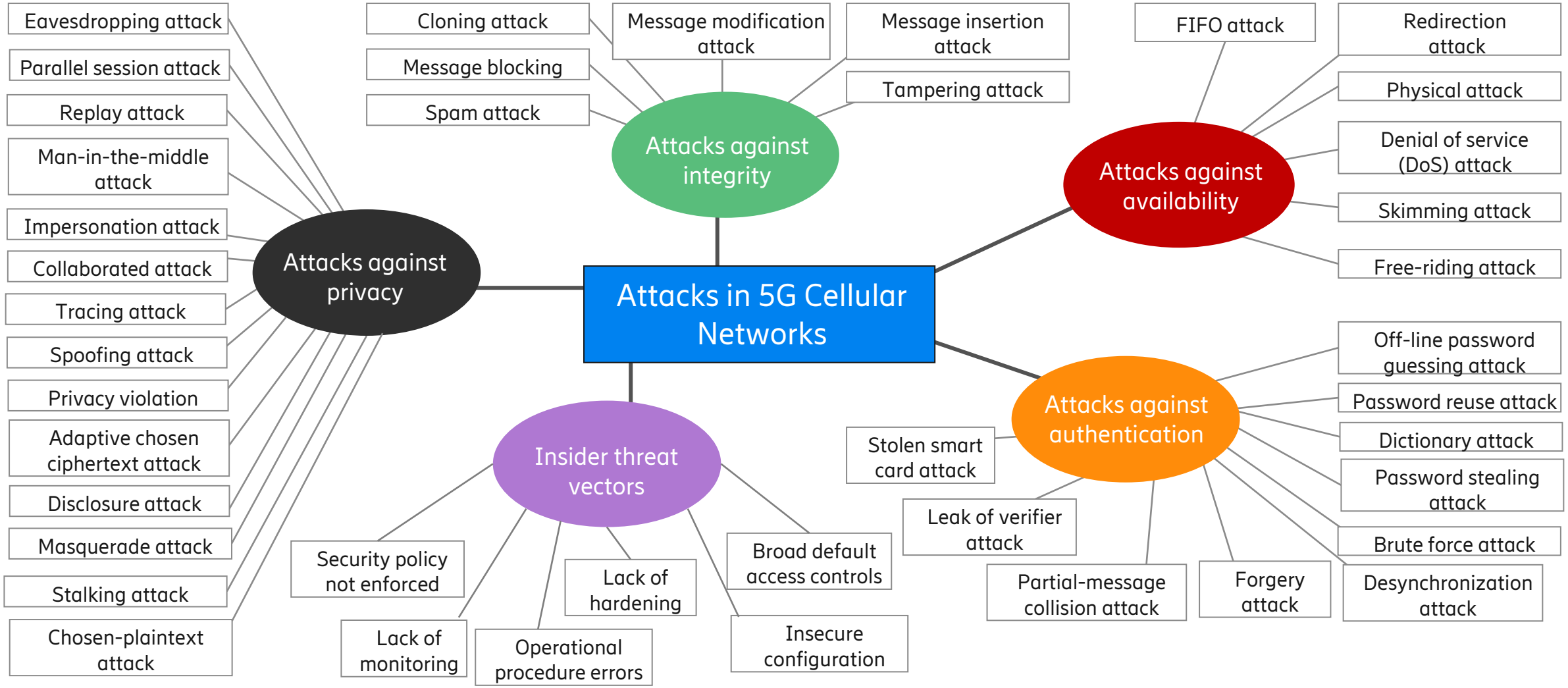


Threat and security landscape

Security culture at Ericsson

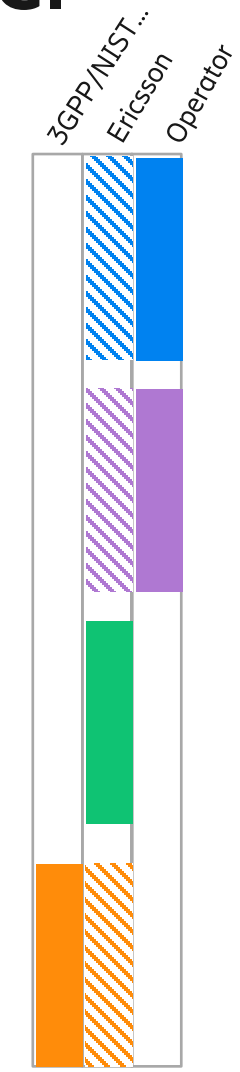
5G Security

5G Diverse network threats



5G Four layer embedded-security model

Security operations	Protect assets Detect threats and vulnerabilities Respond
Security deployment	Security deployment and configuration of security functions
Secure products	Secure product development
Secure approach	3GPP security as foundation



NIST

CIS Center for Internet Security

EU TOOLBOX FOR 5G CYBERSECURITY

enisa

GSMA

NESAS
SCAS

3GPP

Responsibility

Contributor/provider of means and/or services

Sources: Ericsson analysis

Secure approach

I NEED TO BUY A DOOR LOCK FOR MY HOUSE

WHAT ARE THE FUNCTIONS OF DIFFERENT TYPES OF LOCKS?
WHAT ARE THE DIFFERENCES BETWEEN DEADBOLT LOCKS VS MORTISE LOCKS VS KEYLESS LOCKS VS SMART HOME LOCKS?

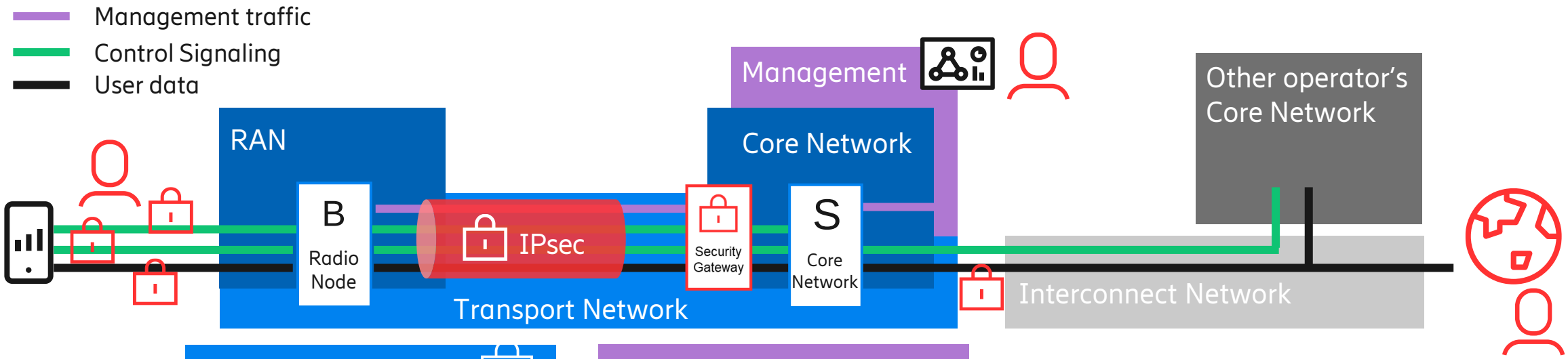
WHAT ARE THE SECURIY FEATURES I NEED IN MY DOOR LOCK?
BUMP RESISTANCE?
KEY CONTROL?
DRILL RESISTANCE?
FORCE RESISTANCE?

Secure products

HOW ARE QUALITY LOCKS MANUFACTURED?

WHAT ARE THE BEST DOOR LOCKS BRANDS? WHY? HOW DO THEY DESIGN THEIR KEYS?

3GPP 5G security standard key features



Improved subscriber authentication

Preventing spoofed phone calls, false billing or eavesdropping

Enhanced subscriber privacy

Preventing IMSI catchers, tracking of subscriber is significantly more difficult

Integrity protection of user plane

The origin and authenticity of data can be cryptographically guaranteed

Interconnect security

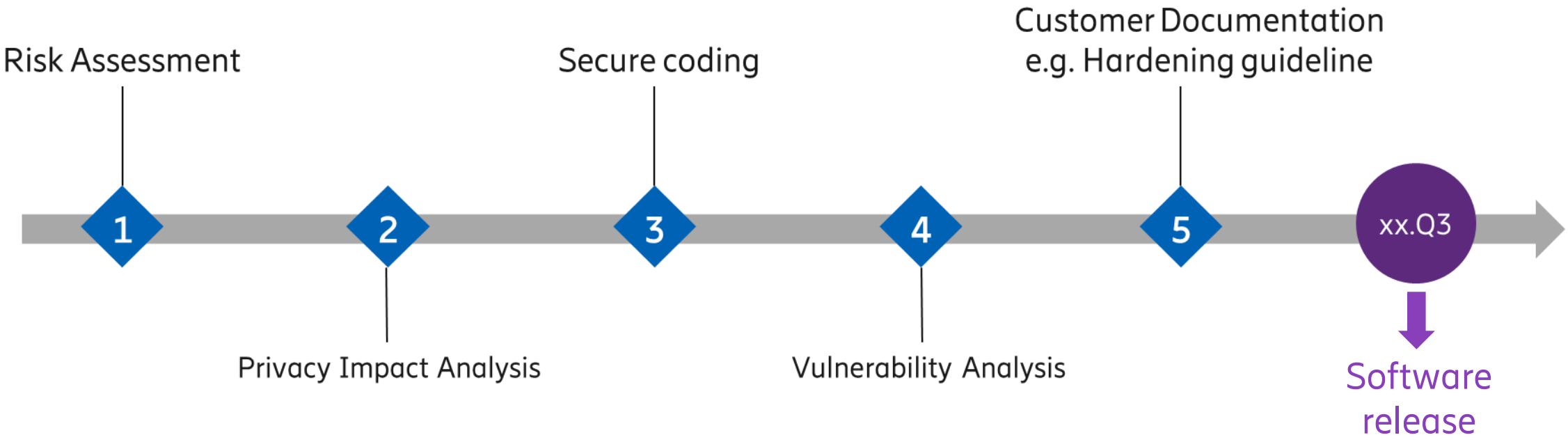
Additional security layer inside and between the core networks

Defense-in-depth for virtual network deployments

Protecting traffic over transport network makes wiretapping more difficult

Secure-by-design

- Ericsson (internal) regulations: 'Ericsson Security Reliability Model (SRM)'
  - Assurance, Compliance & Documentation
- Development activities assure strongest security posture
- Aim → to reduce the number of vulnerabilities



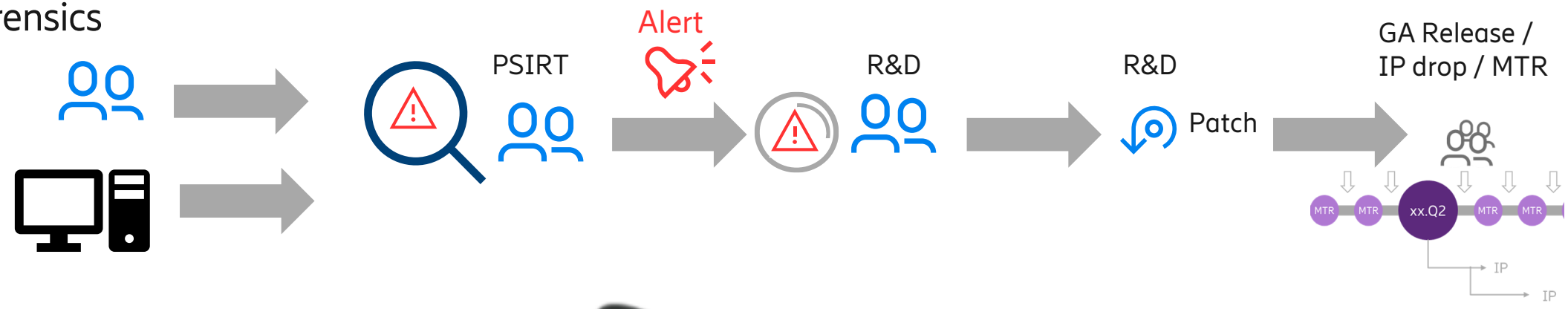
Vulnerability management

PSIRT:
Product Security Incident Report Team

- Vulnerability watch
- Incident handling
- Forensics

Vulnerability watch:

- Ericsson PSIRT tracks new 3rd Party Product vulnerabilities



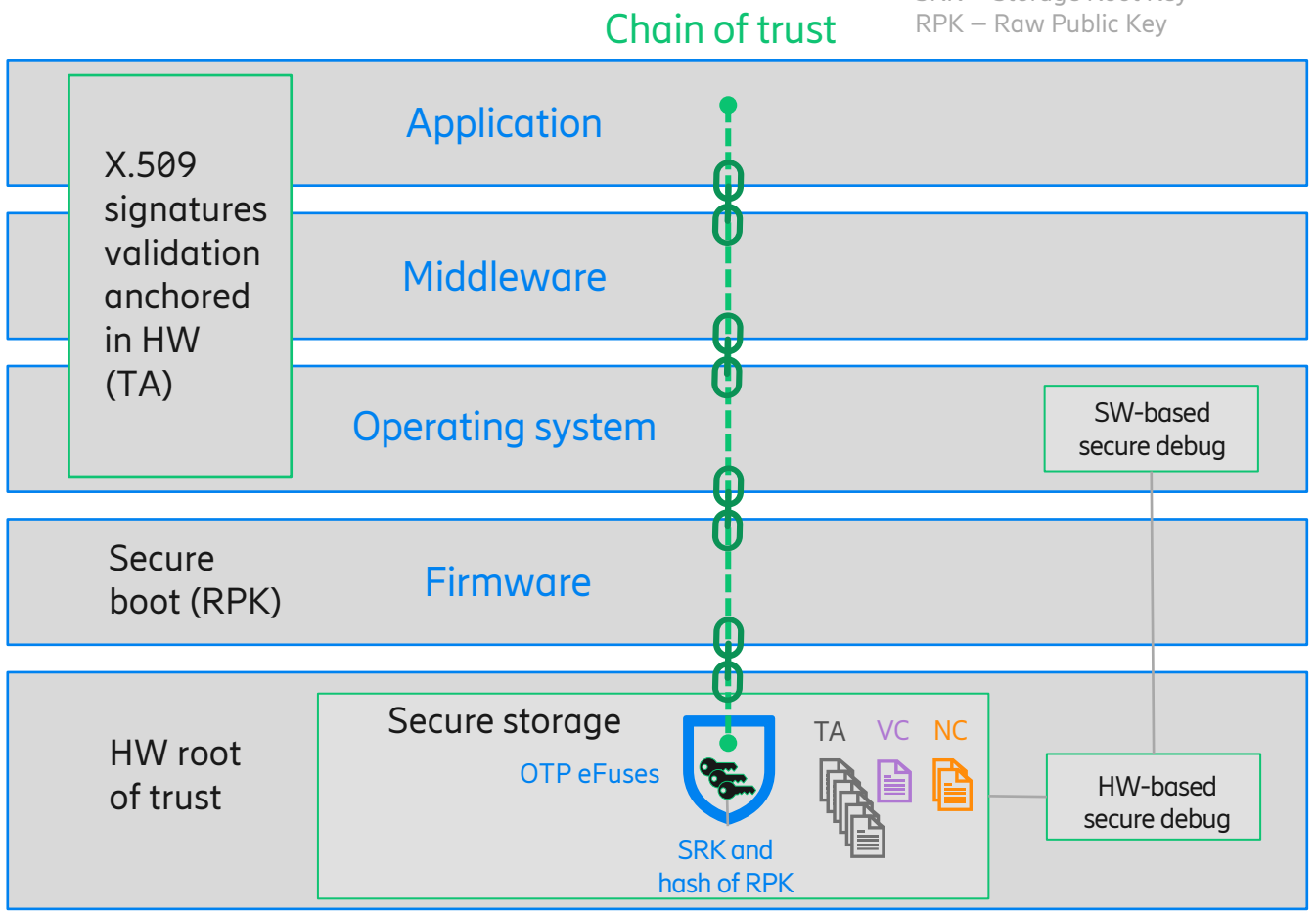
- Ericsson is a member of First

Increased product security

Hardware-rooted in-built security

- Security built into the silicon
- Chain of trust from the hardware all the way to the application layer
- Foundation of all secure operations in the node.
- eFuses to prevent tampering and access
- SRK used to store Ericsson and Operator Keys and credentials
- VC used for Network integration.
- Only Ericsson signed software allowed
  - Prevents manipulation with software and possibility to get hold of keys

NC – Node Credentials (Operator Credentials)
TA – Trust Anchor
VC – Vendor Credentials
OTP – One Time Programmable
SRK – Storage Root Key
RPK – Raw Public Key



Security deployment

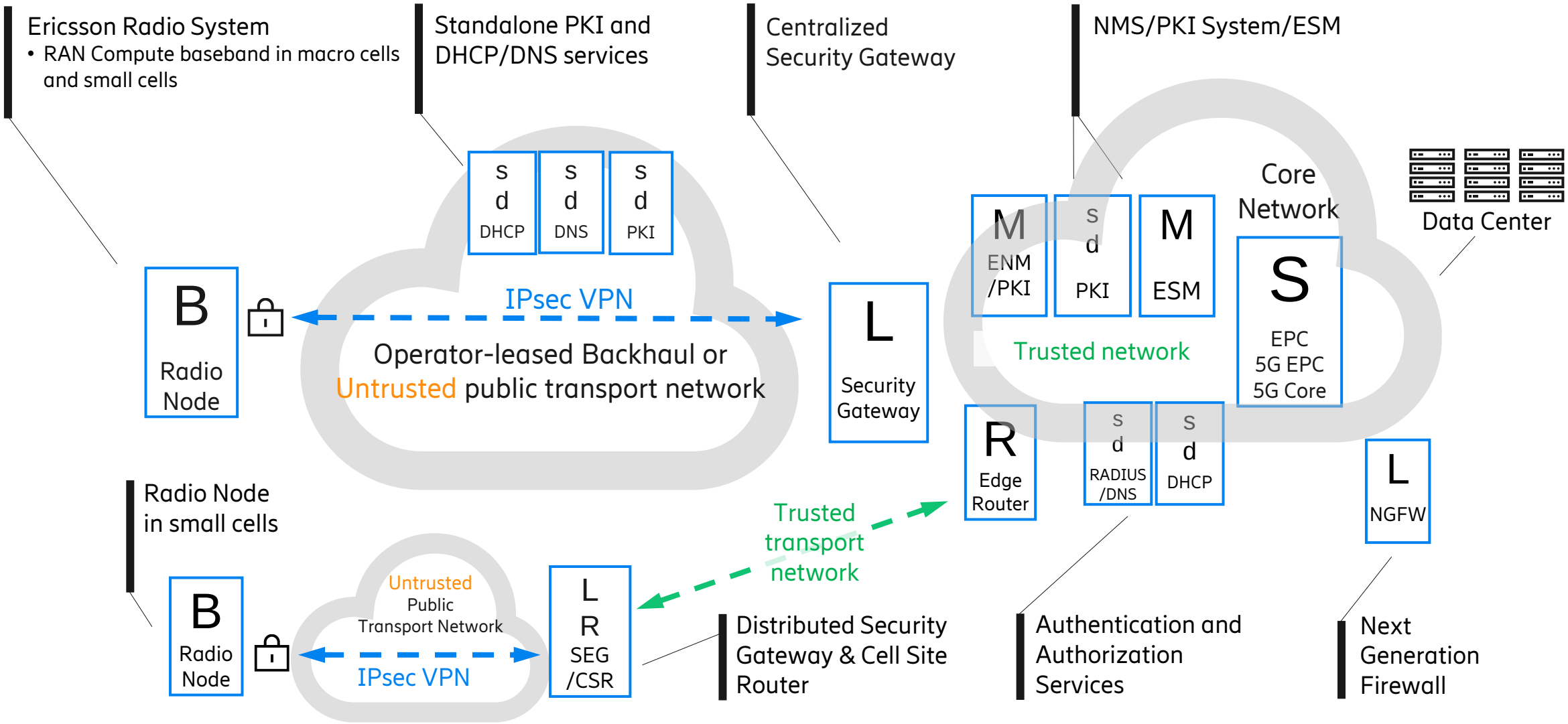
INSTALL IT RIGHT!

MAKE SURE ALL OF YOUR DOORS HAVE LOCKS.

KEEP THE KEYS WITH YOU!

USE THE HELP OF PROFESSIONAL LOCKSMITHS FOR THE BEST SECURITY!

Secure mobile networks deployment



Security operations

DID I LOCK THE DOOR BEFORE I WENT TO BED? LET ME DOUBLE CHECK!

WHERE ARE MY KEYS?

I LEFT MY DOOR UNLOCKED

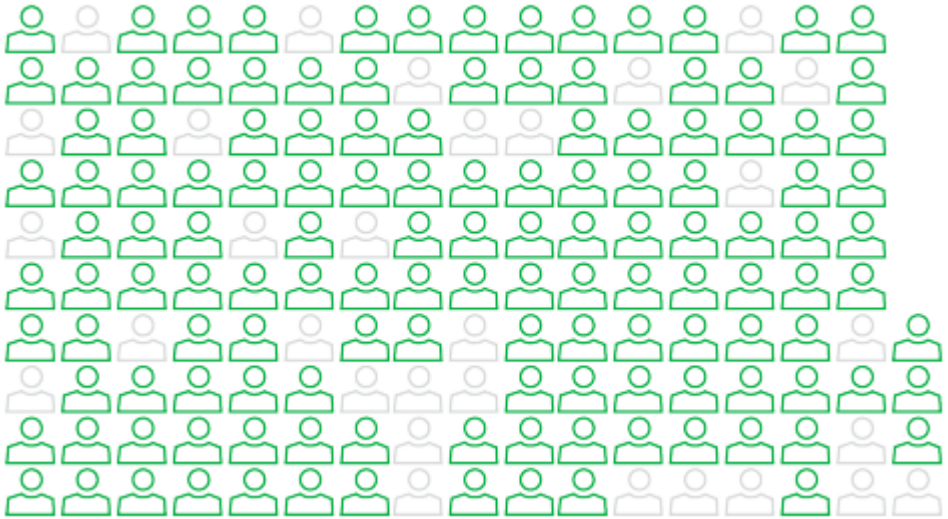
YOUR NEIGHBOR IS CALLING: SOMEONE IS TRYING TO OPEN YOUR DOOR, CALL THE POLICE PLZ.

Secure operations

- Secure communication between network management systems and the network Nodes
- Authentication and authorization with possibility of Multi-factor Authentication
  - Certificate-based authentication
  - Role-based Access Control
  - Target-based Access Control
- Security Logging
- Back-up of logs, configuration and SW
- Security training of staff

82%

of breaches involved the Human Element, including Social Attacks, Errors and Misuse.



"The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike."

Source: Data Breach Investigations Report 2022, Verizon

Improving network security posture

3GPP networks offer in-built security protections

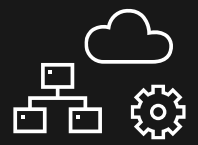
So, what makes networks vulnerable?

Security policy not enforced or monitored

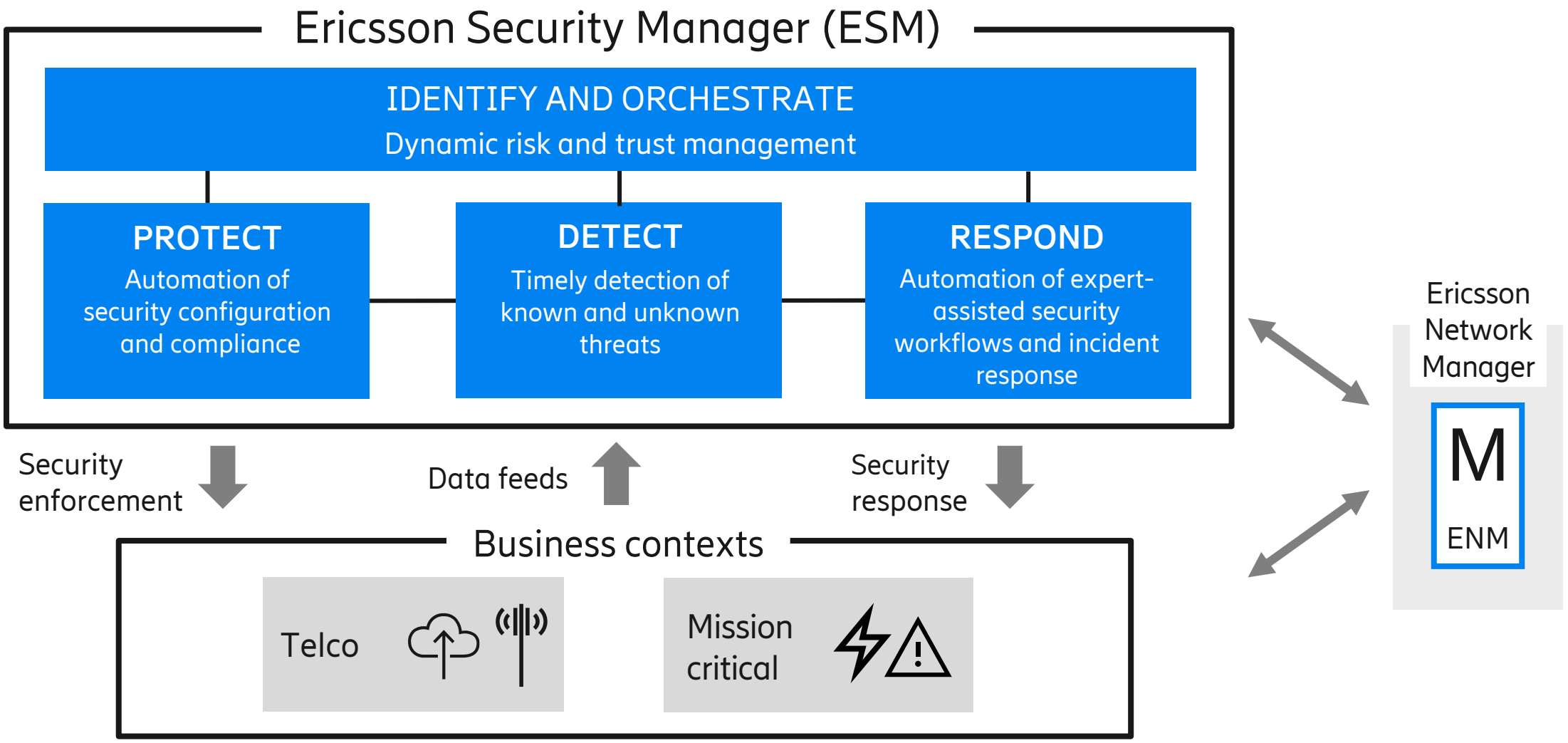
Operational procedures prone to mistakes

Limited visibility, control and continuous monitoring

Lack of hardening and insecure network configuration



Intelligent security management



5G deployments require ZTA

Zero Trust Architecture	
NIST SP 800-207	CISA
Perimeter-less Security	Assume the adversary is already inside the network
There is no implicit trust granted to an asset based upon ownership, physical location, or network location	Perimeter defenses are no longer sufficient to secure a network, and there should always be an assumption that a threat actor has established a foothold in the network

Alignment of 5G Security to NIST 7 Tenets of ZTA

T1. All data sources and computing services are considered resources

- The end-to-end 5G network, including UEs, RAN, Transport, Core, Applications, and Services are assets and data sources
- In the 5G SBA, NFs are identified as consumers and producers

T2. All communication is secured regardless of network location

- Subscriber identity privacy using SUCI
- TLS to provide confidentiality and integrity protection across the SBI
- IPsec and DTLS to protect control messaging and user data in transport
- Full-rate User Plane Integrity protection
- Stronger False Base Station (FBS) protection

T3. Access to individual resources is granted on a per-session basis

- UE access is granted using 5G-AKA, EAP-AKA', and EAP-TLS
- Authentication and authorization between NFs over SBI in the 5GC is provided with certificate-based mutual authentication using TLS
- Home Control of authentication is provided for roaming devices
- RAN Slicing supports slice-specific mutual authentication for devices using the NSSAA

T4. Access to resources is determined by dynamic policy

- The PCF feeds the AMF with access and mobility policies that affect UE authorization to access 5G network resources
- Unified 5G policy allows for creating security policies for security use cases and user plane security enforcement within the session management and established security policies

T5. The operator monitors and measures the integrity and security posture of all owned and associated assets

- 5G is re-defining security monitoring from physical probes and cables to software and virtual links. New software-based solutions include monitoring of East/West and North/South directions
- NWDAF defined in 3GPP TS 29.520 incorporates standard interfaces from the service-based architecture to collect data and evaluate systems in terms of compliance with security policy rules

T6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed

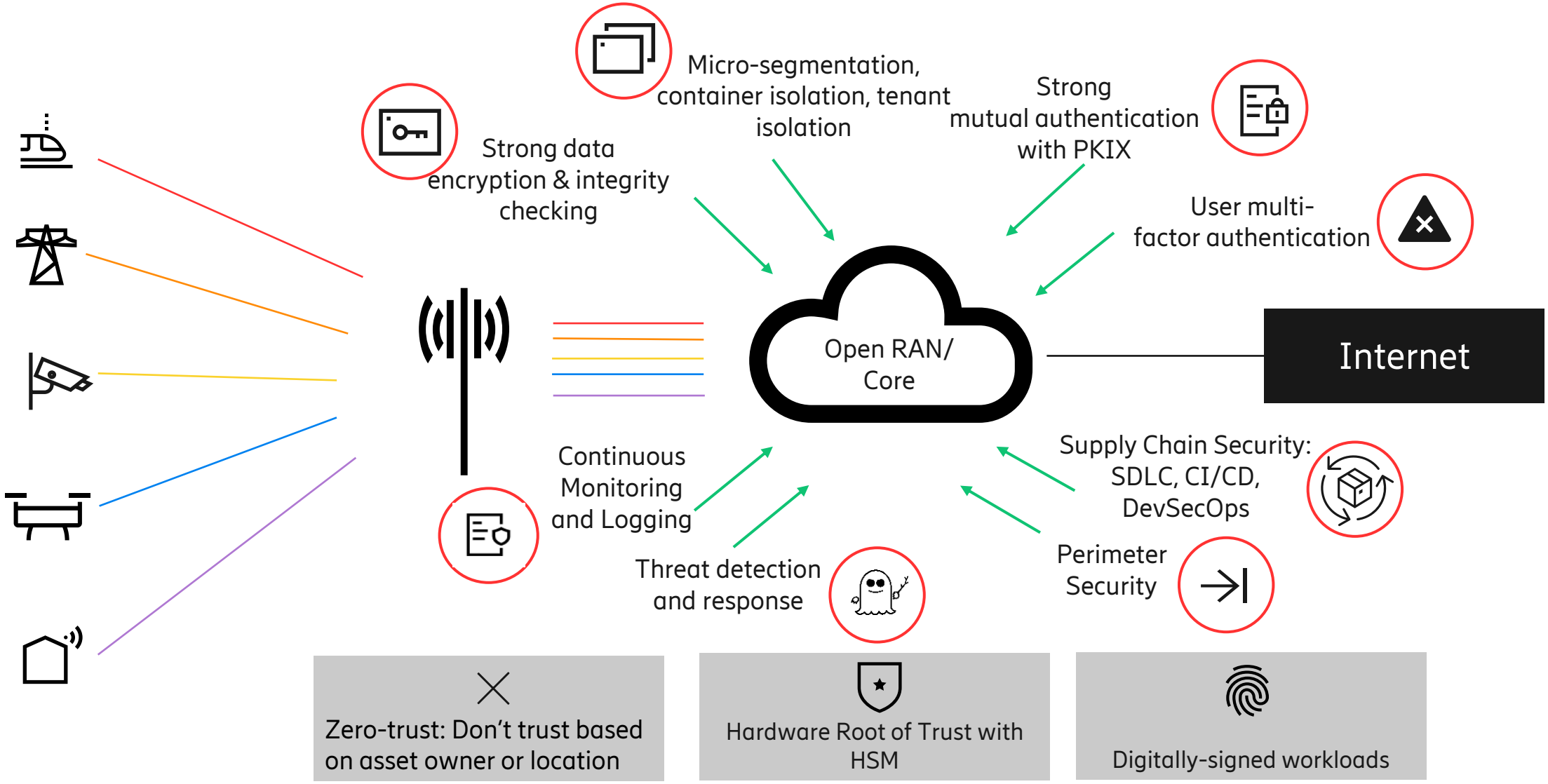
- The SBA uses OAuth 2.0 token-based authorization for any NF that wants to communicate with another NF
- Mutual authentication enables the device to authenticate the network using the AUTH (Authentication Token) returned by the network
- Shared Key using Security Anchor Function (SEAF) and AUthentication Security Function (AUSF).

T7. The operator collects information about the current state of assets, network infrastructure and communications and uses it to improve its security posture

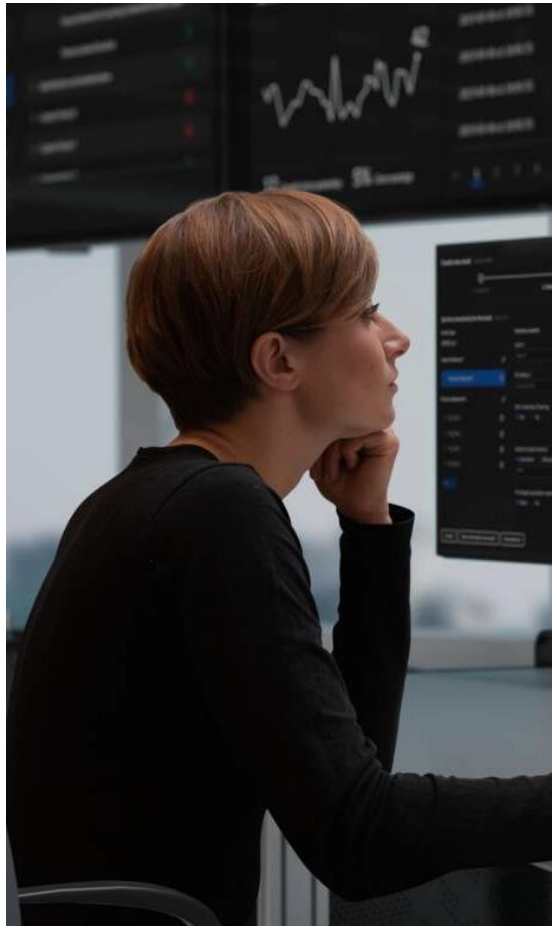
The operator should leverage solutions that align with the continuous diagnostic and mitigation (CDM) systems as defined by NIST in Special Publication 800-207

The operator should have a mature supply chain risk management (SCRM) to ensure 5G network functions to be compliant with GSMA NESAS.

Security features to enable a zero-trust architecture for a secure 5G cloud deployment



Content

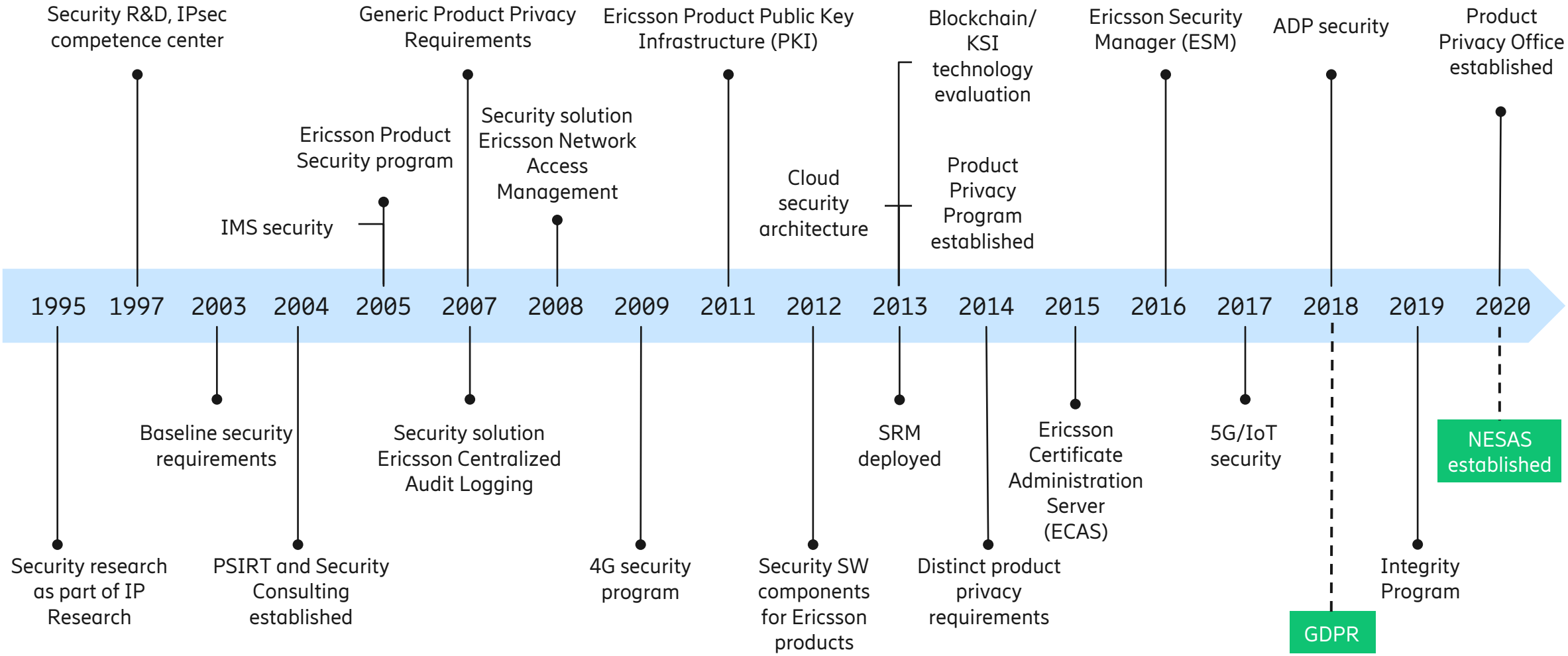


Threat and security landscape

5G Security

Security culture at Ericsson

A pioneer in building secure foundations in the 21st century



Key standardization, certifications and compliance addressed or contributed by Ericsson

Ericsson strongly and actively supports both 3GPP and GSMA's initiatives for standardization

3GPP and SA3 Standardization

Long-term commitment	SA3 Working Group	Technology leadership

ISO/IEC Standardization

ISO/IEC 27001:2013 certified

NESAS Assurance Scheme

Fully compliant with NESAS standards

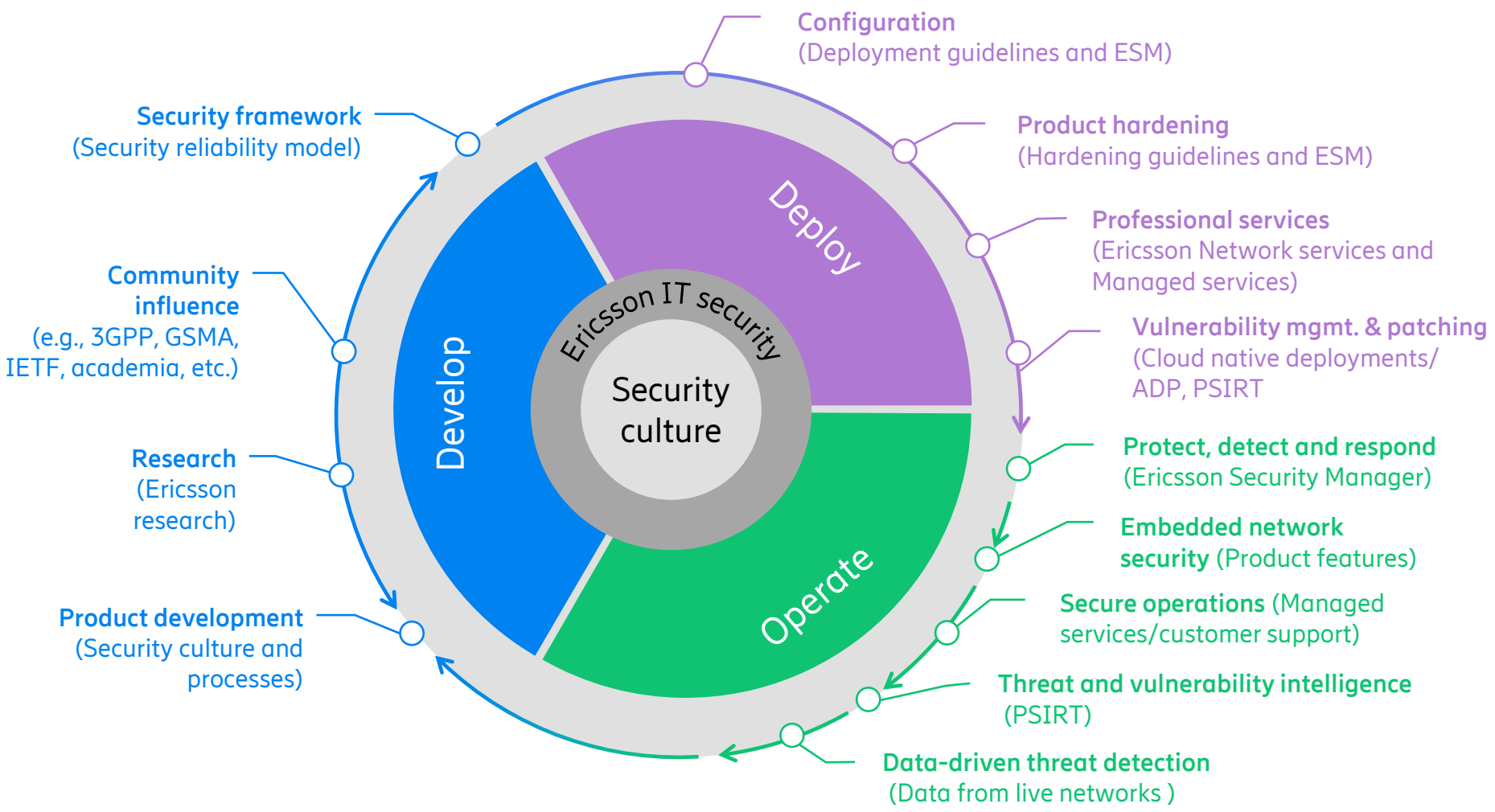
IETF

ETSI

NIST

GSMA

Security Assurance @ Ericsson - Three dimensions of security, working together holistically



Ericsson's range of security capabilities work in tandem to ensure secure and resilient networks.

We **develop** products in a secure way, ensuring security from supply to production and coding.

We **deploy** products and solutions securely in customers' networks and in **operations** our embedded features, security management solutions and incident response team maintain security over time.

Key conclusions:
5G Security is National Security

Industry organizations

Key conclusions

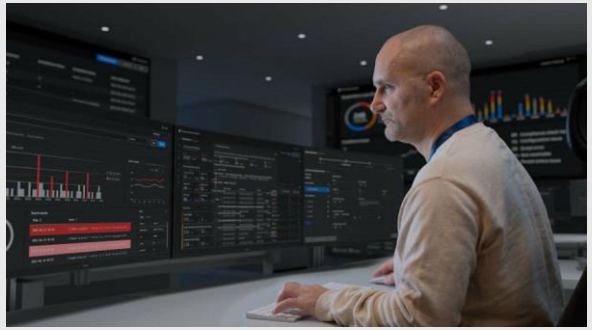
Defense-in-depth

to meet common threats

- Secure-by-design
- Ericsson offers in-built security controls on all levels

Network security

depends on operator policy and configuration



- IPsec/Security Gateways and NW/node configuration
- Unique users with fewest privileges
- Staff education

Strengthen safeguards

with intelligent security management

- Maintained hardening
- Security policy management
- Quick discovery and recovery in case of an intrusion or attack

https://www.ericsson.com/en/5g

https://www.ericsson.com/en/security