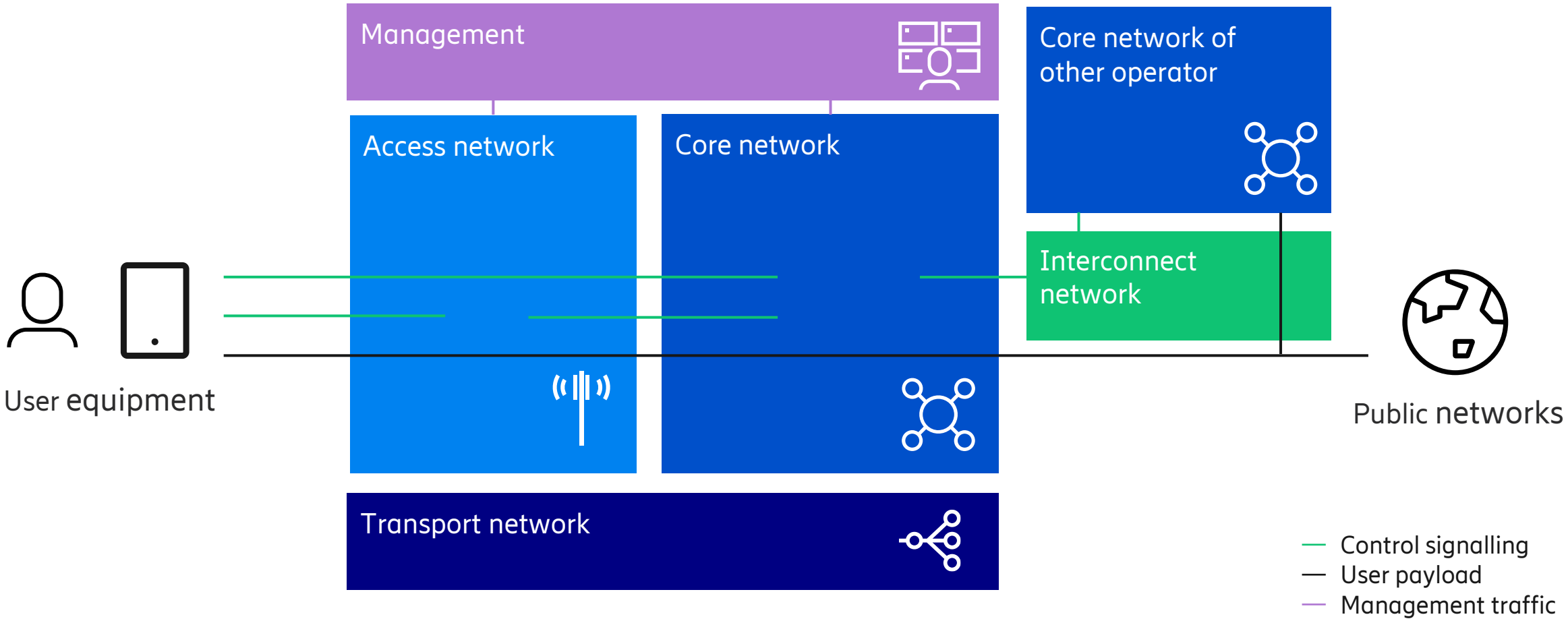
5G RAN - One Software track - security benefits

Anna Kåhre, Product Security Director – Business Area Networks
Ericsson AB

2023-05-24

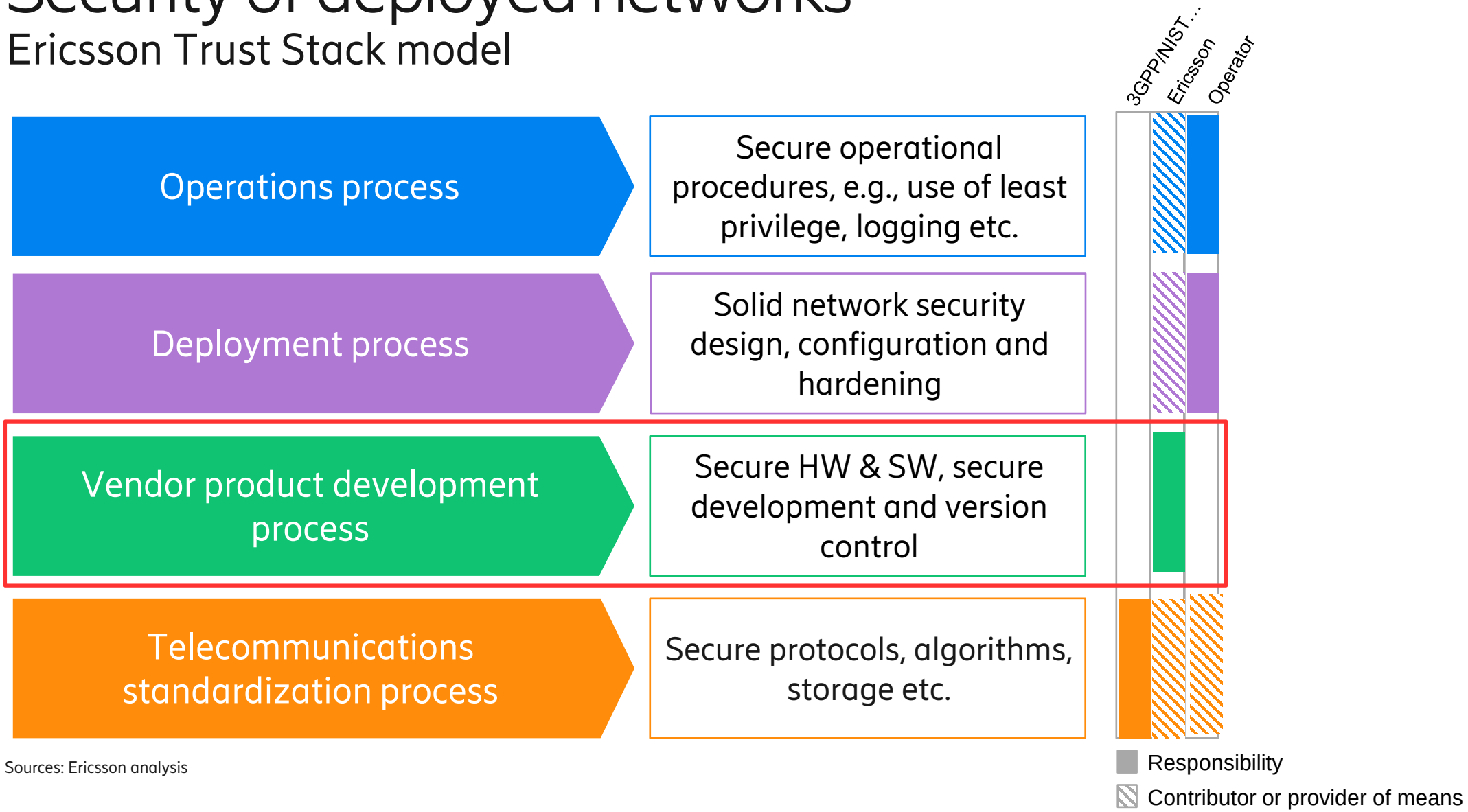
High level mobile network overview

Logical elements and logical planes



Security of deployed networks

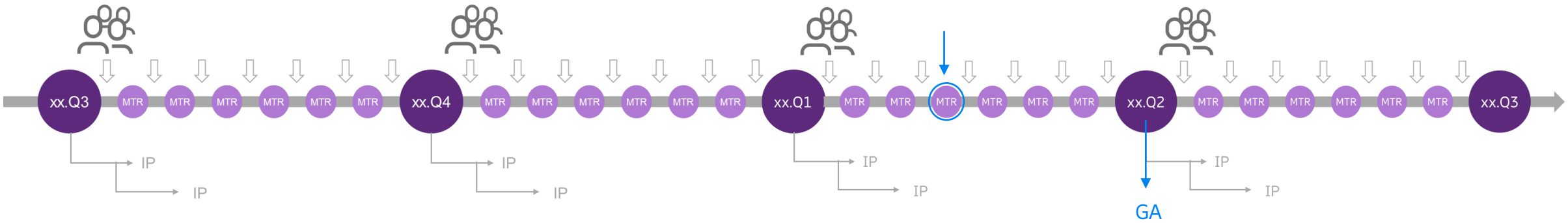
Ericsson Trust Stack model



Sources: Ericsson analysis

One software track for all markets

- One SW (main-track) that serves all markets
- Features and licensing used to meet different markets/customer demands
- Development efficiency
- Bugs, vulnerabilities and fixes handled “once”
- One SBOM facilitates modernization & upgrades of SW components

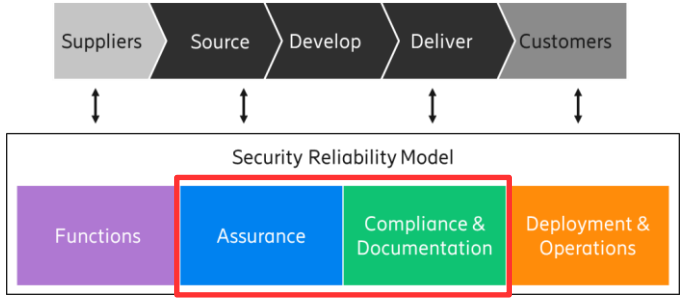


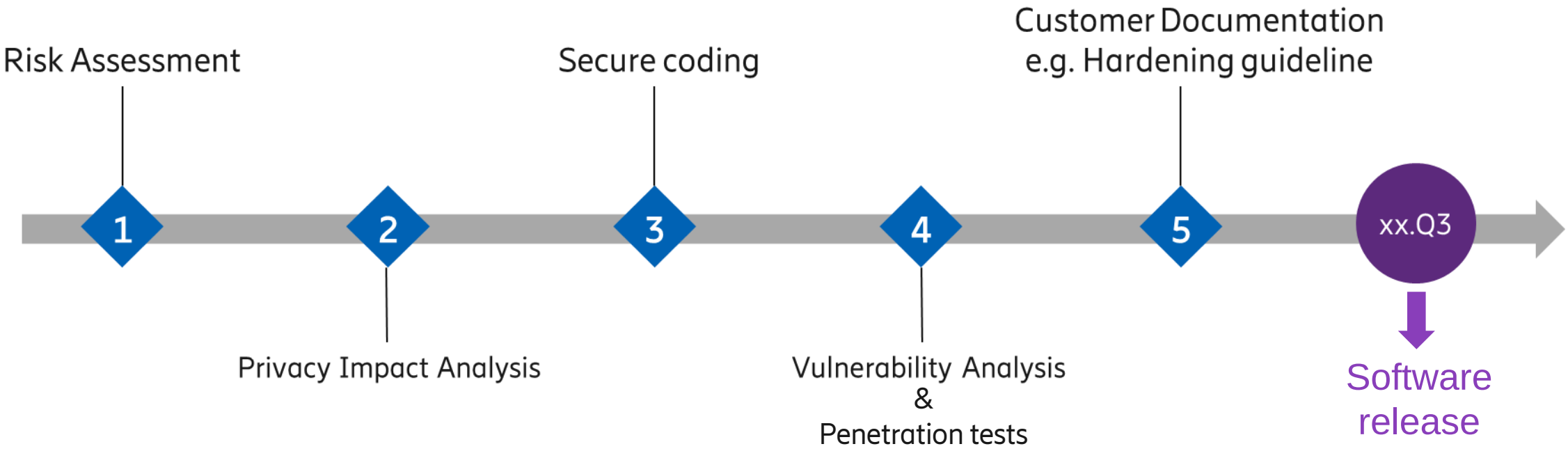
SBOM = Software Bill of Material
MTR = Main Track Release
GA = General Available
IP = Intermediate Package

One SW for all customers => A fix of a fault or vulnerability in the main track means a fix available for all customers

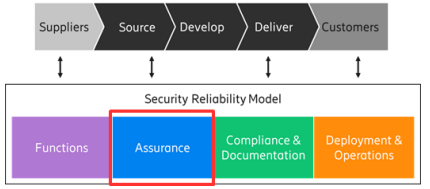
Software Assurance – main activities

- Ericsson (internal) regulation: 'Ericsson Security Reliability Model (SRM)'
  - Assurance, Compliance & Documentation
- Development activities assure strong security posture



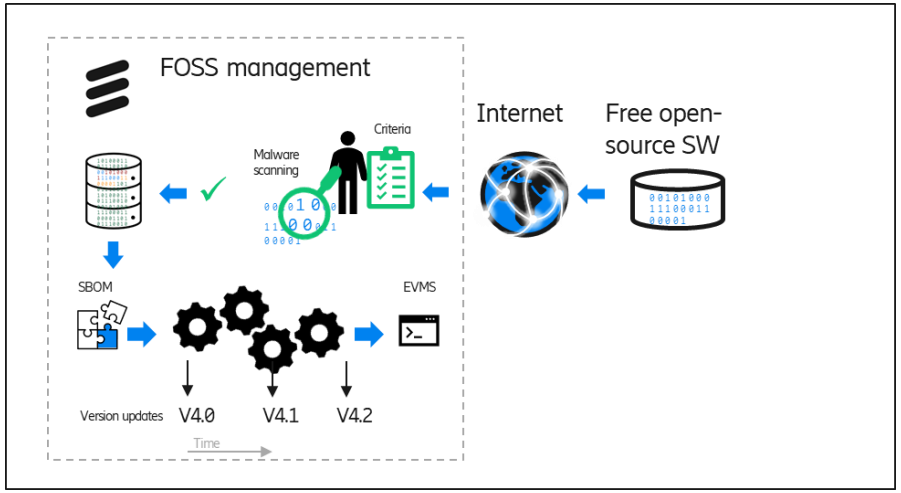


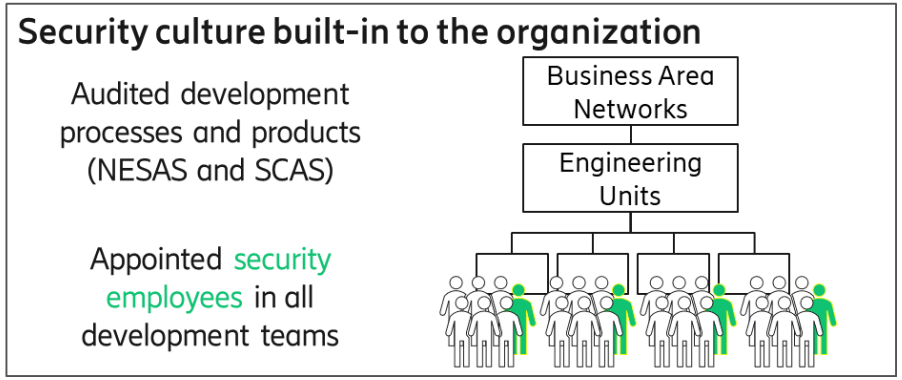
Software assurance



- Vetting of open-source software
- SBOM database mapped to Vulnerability database
- Vulnerability Management
- Code development and code review - "four eyes" principle
- Logging and traceability of code commits
- Test & verification

- Security professionals





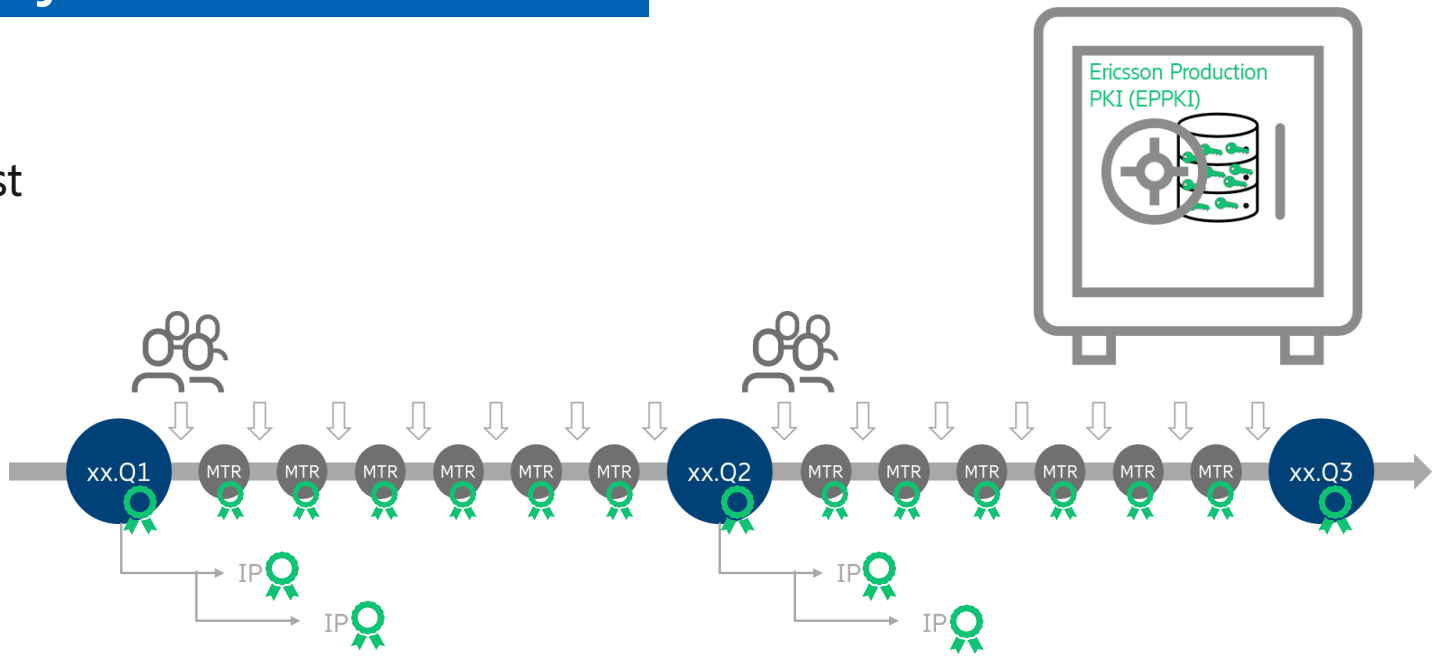
FOSS = Free Open-Source SW
SBOM = Software Bill of Material
EVMS = Ericsson Vulnerability Management Service
NESAS = Network Equipment Security Assurance Scheme
SCAS = Security Assurance Specifications

Signing of Software & Firmware

✓ Minimum amount of exploitable Vulnerabilities

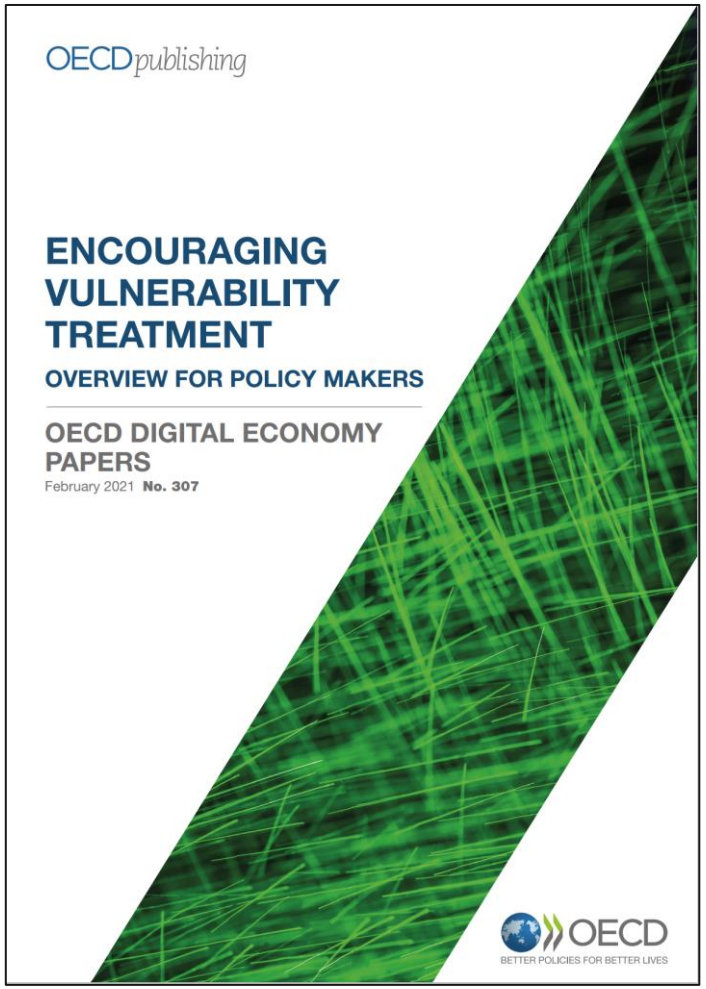
✓ Minimized risk of malware injection

- The SW is signed after assurance activities (test and verification)
- The UP (Upgrade Package) contains X.509 signatures
- The firmware is signed
- Software is made available in SW GW



OECD Vulnerability recommendations

Risk-based approach : 1) Mitigating measures 2) exploitability 3) feasibility

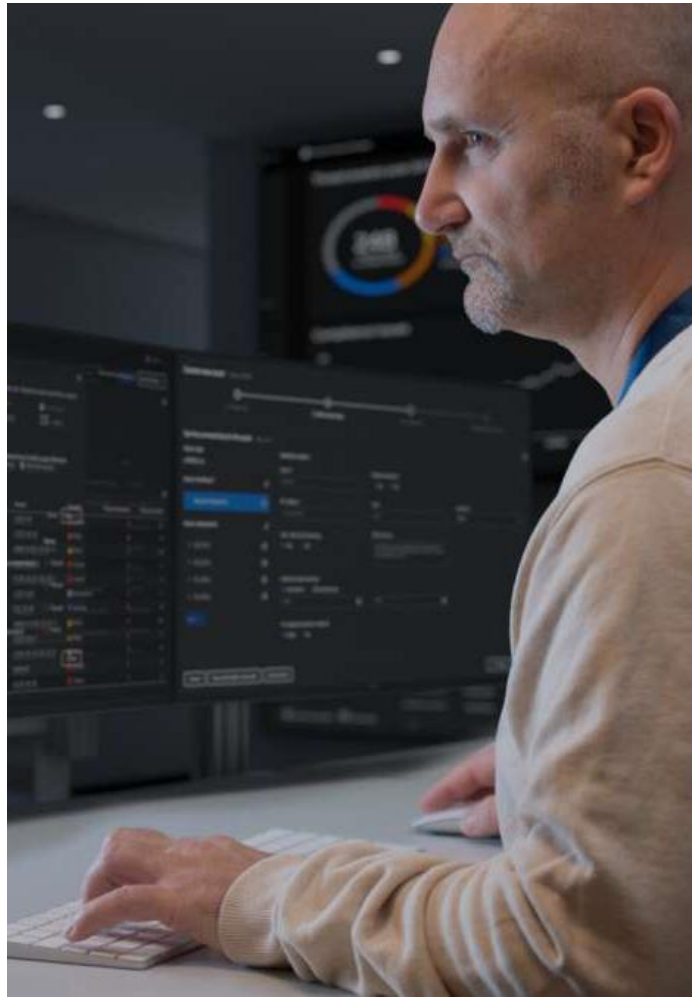


- **To reduce the risk, it is possible to apply a mitigation measure ("mitigation").** For *code vulnerabilities*, a mitigation called a "patch" modifies the code to fix the vulnerability. Patches need to be implemented on each software instance through a security update, broader update or new release (e.g. upgrades in mobile apps). However, it is not always possible to develop a patch, for example, when the product is no longer supported, does not have update capabilities, or would have to be redesigned to fix the vulnerability. In such cases, a set of instructions, configuration requirements or documentation can reduce the risk without necessarily eliminating it. In some smart products, such as certain low-cost IoT devices, the code cannot be updated. For *system vulnerabilities*, mitigations consist in actions that system owners can take, e.g. changing configuration settings or applying an existing patch previously set aside.
- **However, there is no way to eliminate all vulnerabilities.** While addressing vulnerabilities is essential, fixing *all* vulnerabilities would not be a realistic objective, for many reasons including cost and technical feasibility. Furthermore, many code vulnerabilities will never be exploited, and some system owners may not apply a patch because it would disrupt operations, create compatibility issues or introduce additional risk. Moreover, vulnerabilities may be discovered in products that are still in use but no longer supported and will never be corrected. In absence of a code mitigation, or when a patch cannot be applied, a workaround may exist, such as a configuration change in a firewall.
- **Risk management, which enables discernment and flexibility, is the cornerstone of vulnerability treatment.** The overarching objective of vulnerability treatment is to make products and information systems "secure enough" rather than absolutely secure, in order to sufficiently reduce, rather than entirely eliminate, security risk for users and third parties. Mitigation development is primarily a matter of prioritisation based on risk assessment.

https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en

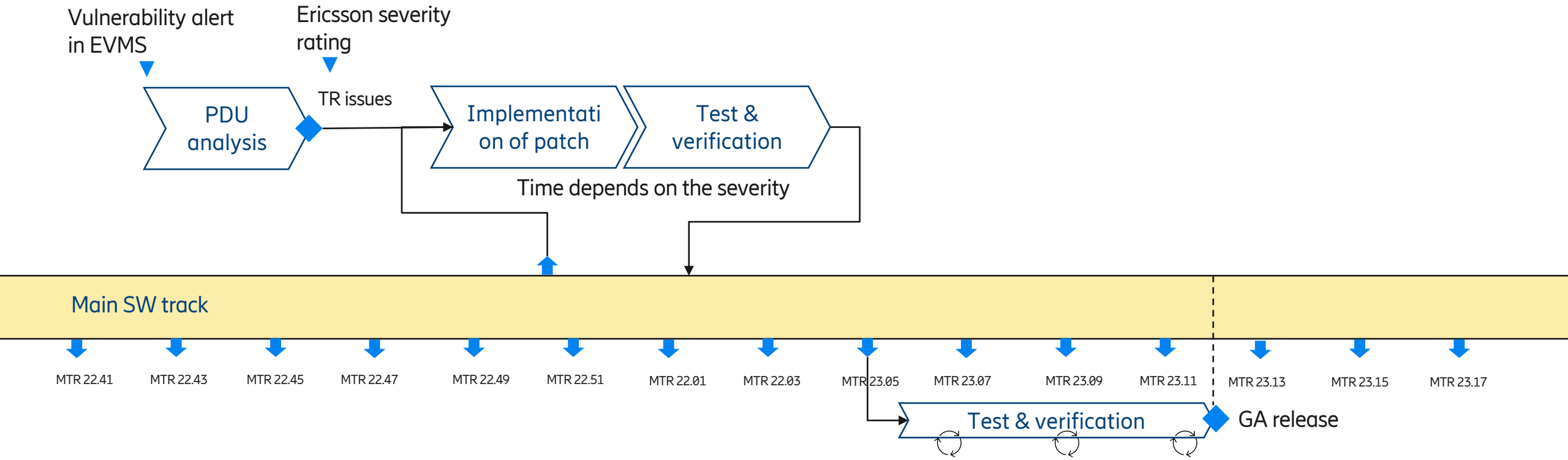
Not all vulnerabilities are equal!

- To help identify the severity of a vulnerability, **a globally recognized standard** exists.
  - **CVSS – Common Vulnerability Scoring System**,
- **The base** CVSS score (as often discussed in the media) only considers the vulnerability in isolation.
- In reality, systems and telecom networks are implemented in a **security context**
  - layers of protective measures
- **This security context is captured in the CVSS by the environmental and temporal security relevant criteria**.

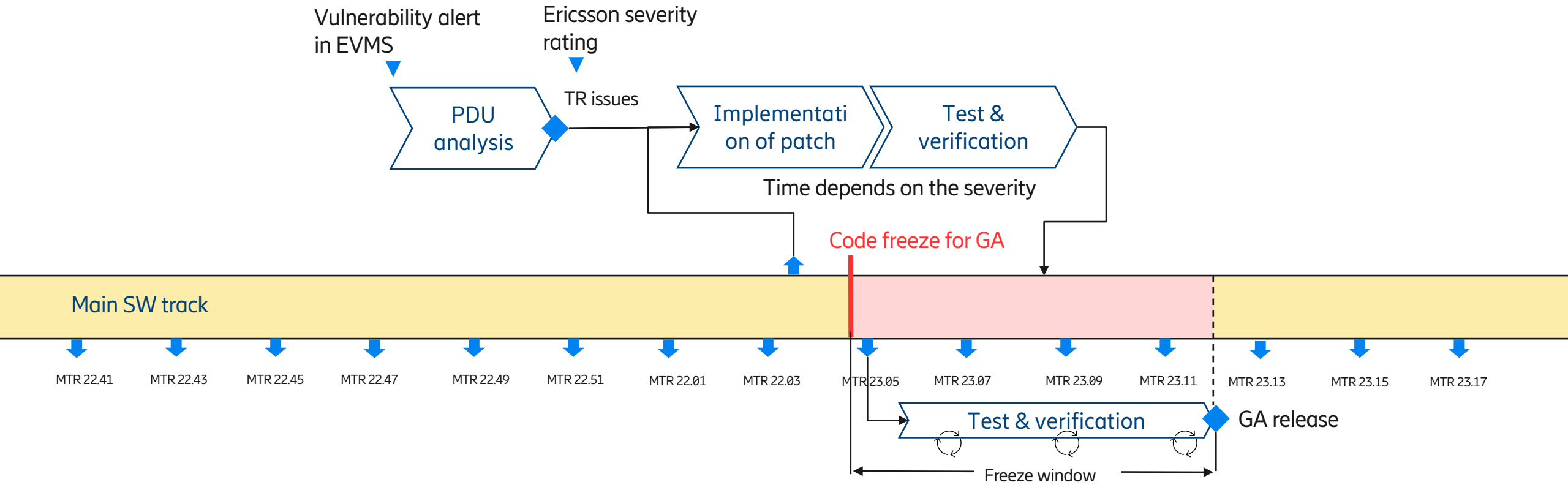


Source: https://www.first.org/cvss/

Example of vulnerability handling



Example of vulnerability handling



Which vulnerabilities matters for ensuring resilience ?

Cyber Resilience Act

ANNEX I
ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

Products with digital elements shall be delivered without any known **critical or high severity exploitable vulnerabilities**.

OECD Vulnerability recommendations

Risk-based approach : 1) Mitigating measures 2) exploitability 3) feasibility

- **To reduce the risk, it is possible to apply a mitigation measure ("mitigation").** For *code vulnerabilities*, a mitigation called a "patch" modifies the code to fix the vulnerability. Patches need to be implemented on each software instance through a security update, broader update or new release (e.g. upgrades in mobile apps). However, it is not always possible to develop a patch, for example, when the product is no longer supported, does not have update capabilities, or would have to be redesigned to fix the vulnerability. In such cases, a set of instructions, configuration requirements or documentation can reduce the risk without necessarily eliminating it. In some smart products, such as certain low-cost IoT devices, the code cannot be updated. For *system vulnerabilities*, mitigations consist in actions that system owners can take, e.g. changing configuration settings or applying an existing patch previously set aside.
- **However, there is no way to eliminate all vulnerabilities.** While addressing vulnerabilities is essential, fixing *all* vulnerabilities would not be a realistic objective, for many reasons including cost and technical feasibility. Furthermore, many code vulnerabilities will never be exploited, and some system owners may not apply a patch because it would disrupt operations, create compatibility issues or introduce additional risk. Moreover, vulnerabilities may be discovered in products that are still in use but no longer supported and will never be corrected. In absence of a code mitigation, or when a patch cannot be applied, a workaround may exist, such as a configuration change in a firewall.
- **Risk management, which enables discernment and flexibility, is the cornerstone of vulnerability treatment.** The overarching objective of vulnerability treatment is to make products and information systems "secure enough" rather than absolutely secure, in order to sufficiently reduce, rather than entirely eliminate, security risk for users and third parties. Mitigation development is primarily a matter of prioritisation based on risk assessment.

https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en

Summary

- Security of deployed networks is determined by standards, vendor development processes, configuration and operations.
- One software track benefits our customers and ensures efficiency and hence affordability of products and services
- Software assurance throughout the development process increase security
- The main consideration in CRA should be to minimize the risk of cyber incidents as opposed to minimizing the mere presence of any kind of vulnerability

https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security?video-dialog=1_kw4tjgm6