
CYBERSTAND.eu
Impacting the CRA
Defining standards for the future
10:00 - 10:20
Essential requirements of the Cyber Resilience Act
Angelo D'Amato
Vulnir
ECCC
Co-funded by the European Union

Vulnir

Essential requirements of the Cyber Resilience Act

Angelo D'Amato
Founder

Meet your speaker

Angelo D'Amato
Founder / Cybersecurity Expert, Vulnir

Background

- With over fifteen years of experience, he is the subject matter expert for:
  - End-to-end cybersecurity assessments (Penetration testing, Security assessments)
  - Certifications (e.g., UL 2900, Common Criteria)
  - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur (*) for CRA as a CEN contractor within CEN/CLC/JTC 13/WG 9 for
  - PT2: Generic Security Requirements
  - PT3: Vulnerability handling requirements

* The European Union funds my activities within the STAN4CR project through the European Innovation Council and SMEs Executive Agency (EISMEA) under Grant Agreement No. 101196779.

Agenda

01 Setting the context

02 Essential Requirements overview

03 CRA’s use cases and examples

01

Setting the context

Prepare

Obligations of manufacturers (CRA)

Risk Assessment

Product-related essential requirements

Vulnerability handling essential requirements

Conformity assessment

Article 13

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

2. For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.

Vulnerability handling throughout the product lifetime (for the period when the product is expected to be in use)

Design and development

Maintenance

Obligation to report through a single reporting platform:
(1) actively exploited vulnerabilities
(2) severe incidents having an impact on the security of the product

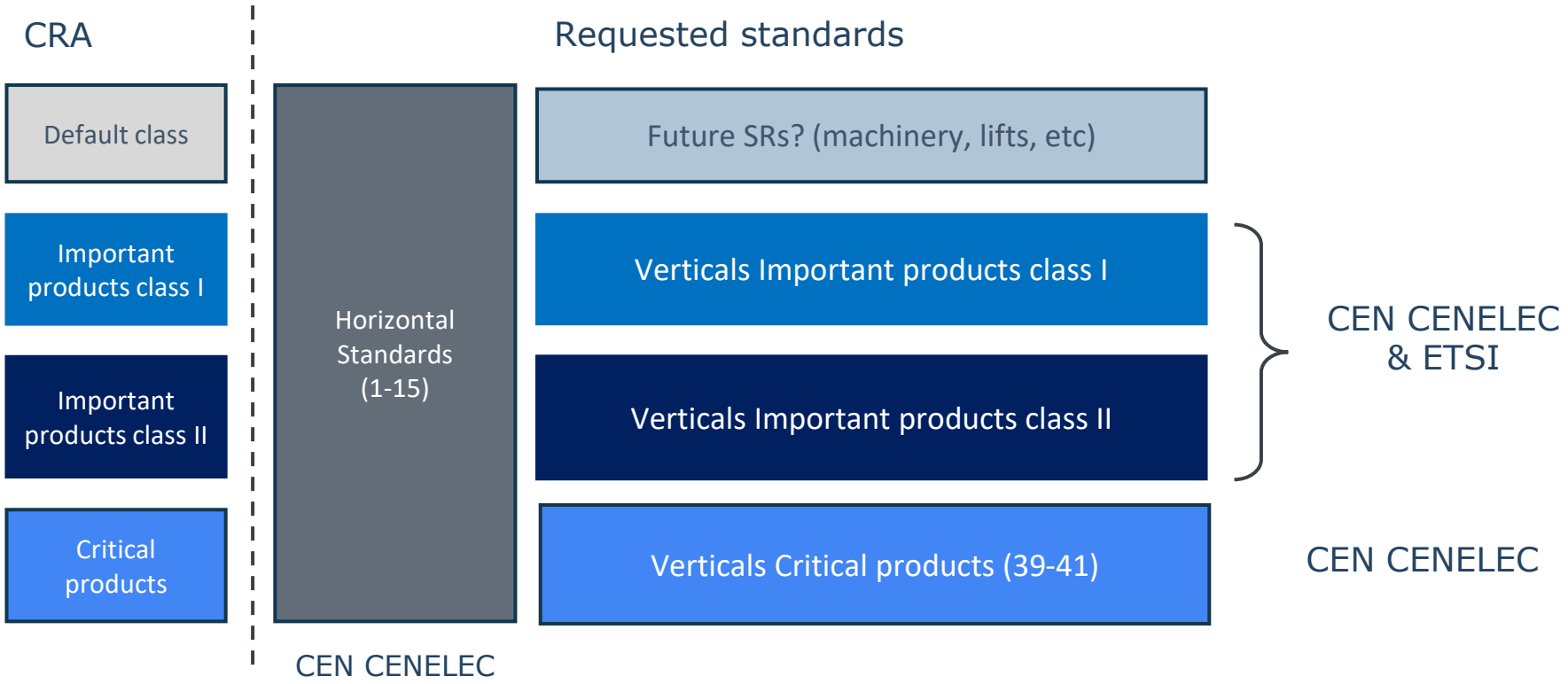
Reporting obligations

European Commission

Vulnir

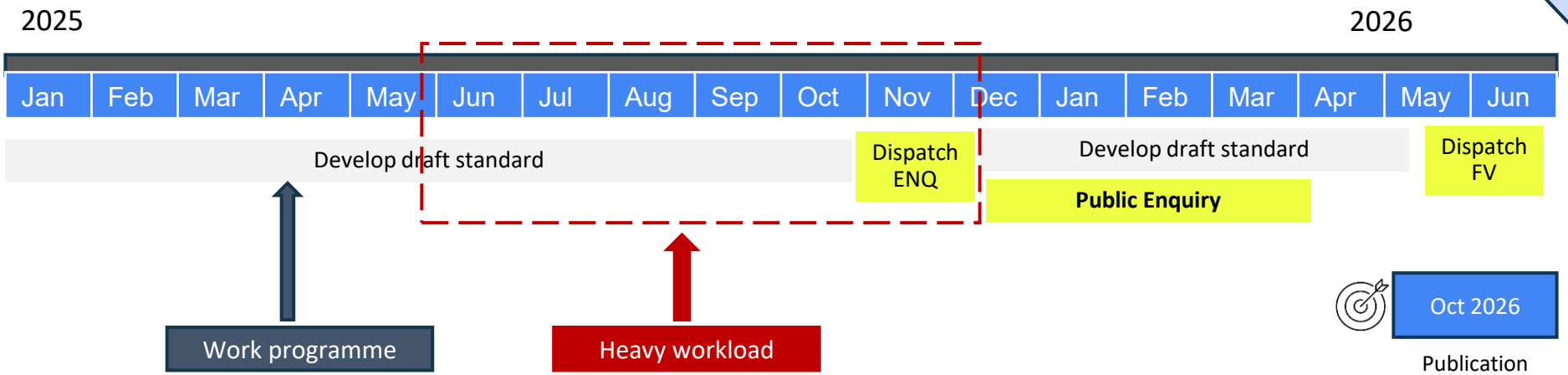
***Source**: CEN/CENELEC Webinar on 10 March 2025 – Standardisation for the Cyber Resilience Act*

Requested standards



High level expected timeline

For discussion purposes only
DRAFT



Oct 2026

Publication by ESOs

(Except PT1 and PT3 deliverables, in August)

How to learn more?

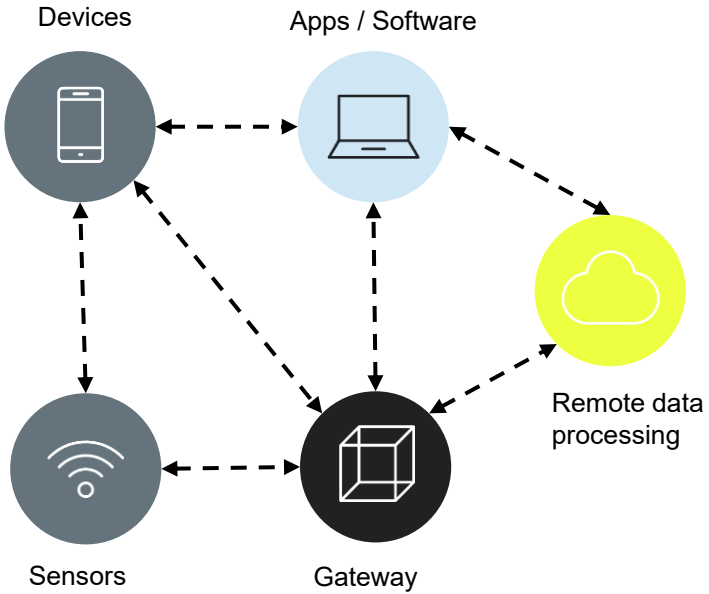
- Cyber Resilience Act: Standardization Request Officially Accepted by CEN, CENELEC, and ETSI
  - Including:
    - CEN, CENELEC and ETSI Work Programme
    - WG9 convener Ben Kokx – Youtube Video)
- **Core knowledge:**
  - Cyber Resilience Act - Legal Text - Regulation (EU) 2024/2847
  - Make sure that you are familiar with the CRA-related C(2025)618 – Standardisation request M/606
- **To have a better understanding and contextualization:**
  - New legislative framework
  - The Blue Guide on the implementation of the product rules 2022
  - Cyber Resilience Act - Impact assessment (REPORT / STUDY Publication 15 September 2022)

02

Essential Requirements

Cybersecurity requirements for products with digital elements

Overview of the CRA's Essential Requirements



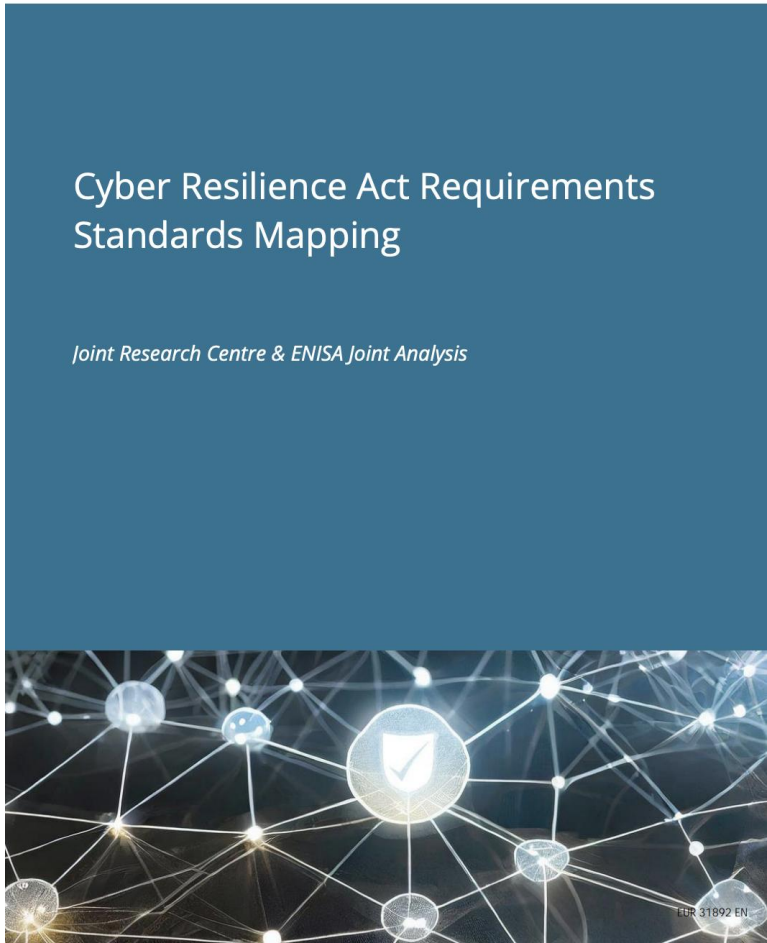
❑Ensure that products with digital elements **hardware and software** placed on the EU market **have fewer cybersecurity vulnerabilities**.

❑**Better protection** for consumers, supply chains, organisations, businesses, and IT Infrastructure

- **Secure by Design / Risk Assessment**
  - No known exploitable vulnerabilities
  - Secure by default configuration
  - Security updates
  - Authorized access
  - Confidentiality protection
  - Integrity protection
  - Data minimization
  - Availability protection
  - Minimize negative impact
  - Attack surface minimization
  - Reduce the impact of an incident
  - Logging and monitoring controls
  - Secure deletion mechanisms
- **Vulnerability Handling Requirements**

Gaps identified

- (1) Risk assessment not specific to the system or product design
- (2) Find the right balance in the assessment for the no known exploitable vulnerabilities (Common Criteria vs ETSI EN 303 645)
- (3 a) The particular use of non-erasable memories for configuration management is not covered.
- (3 f) More detailed guidance on the implementation of availability principles for generic user products
- (3 h) Lack of concrete requirements targeting the attack surface minimisation
- (3 i) some aspects of defence in depth, sandboxing, and certain mitigation techniques might not be explicitly covered by the selected standards
- (3 k) Do not explicitly cover the requirement of notifying users about the availability of updates.



Vulnir

Source: *Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis*

03

CRA

Use cases and examples

My Friend Cayla

- My Friend Cayla is made by Genesis Toys and distributed in Europe by Vivid Toy Group.
- The doll was named 2014 Innovative Toy of the Year
  by the London Toy Industry Association.
- The first vulnerability was disclosed in January 2015.
- In February 2017, the German Federal Network Agency (Bundesnetzagentur) had to invoke a federal law against espionage devices to ban a connected toy that intentionally transferred recordings outside the EU.

Source: https://www.npr.org/sections/alltechconsidered/2016/12/20/506208146/this-doll-may-be-recording-what-children-say-privacy-groups-charge (2016)

Issues and ESR violations

- **Lack of safety**: It was possible to talk and listen through the toy without requiring physical access to it. The problem stemmed from the design of the pairing.
- **Illegal user terms**: The dolls could record and collect the private conversations of young children without any limitations on collection, use, or disclosure of this personal information.
- **Kids' secrets are shared:** Anything the child tells the doll is transferred to the U.S.-based company Nuance Communications, which specializes in speech recognition technologies.
- **Kids are subject to hidden marketing:** The toys are embedded with pre-programmed phrases that endorse

- Secure by default configuration
- Authorized access
- Data minimization

Role of essential requirements

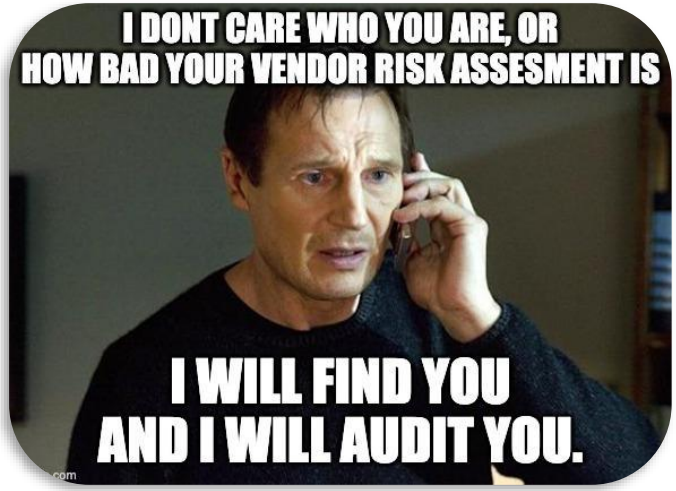
Mirai IoT Botnet, Aug 2016

- The first ever botnet of Internet of Things devices
- **Root causes**:
  - Weak default configuration (default password)
- **Effect:**
  - High-profile websites and services that relied on Dyn for DNS resolution, including Twitter, Reddit, Netflix, Airbnb, Amazon were disrupted
- **Highlighted the importance of:**
  - Secure by default configuration

Log4j (Log4Shell), Dec 2021

- The first ever botnet of Internet of Things devices
- **Root cause**:
  - JNDI lookups within log messages without sufficient validation or sanitization
- **Effect:**
  - Its impact stemmed from the ubiquitous nature of the vulnerable Log4j library and the severe nature of the vulnerability itself (Remote Code Execution).
- **Highlighted the importance of:**
  - Security updates / SBOM

Role of harmonised standards



Manufacturer

Can use it to demonstrate that their products meet the necessary requirements, thus facilitating market access.

Notified Bodies

Can use it to execute conformity assessment activities and verify the due diligence of the manufacturers that requested their services.

Harmonised standard: translates the legal requirement (what) to detailed technical requirements (how)

Can be used to verify consistently the implementation of an essential requirement

Market Surveillance

Thank you

VULNIR.com

info@vulnir.com