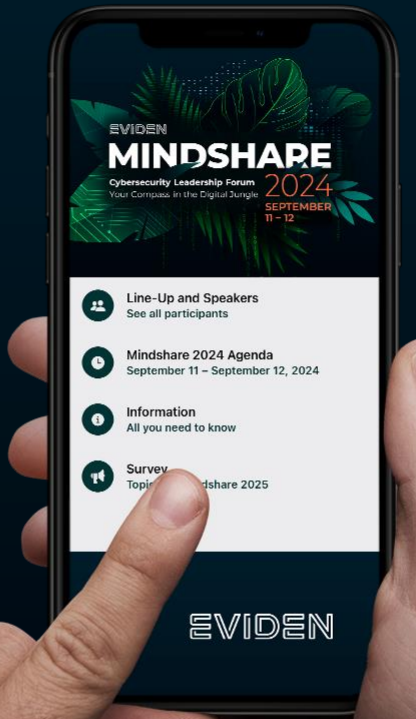
# MINDSHARE 2024 AGENDA

SCAN NOW !



# EU Cyber Resilience Act

## The paradigm shift in the EU market

**Dr. Detlef Houdeau**

## Motivation of the CRA regulation

- Strengthen the protection of **consumers** and **business** who **buy** or **use products** or **software** incorporating **digital components** (HW and SW).
- Improving cybersecurity and cyber resilience in the EU through **common cybersecurity standards**.
- CRA will **close the gap** to other EU regulations,
  - e.g., NLF, NIS, CSA, RED.
- CRA is part of the future **CE-label** and is **mandatory**.
- CRA is a **horizontal regulation**.

# The Scope

- Products must be **designed** and **developed** with security in mind to mitigate known **vulnerabilities** and manage **potential risks**.
- CRA makes **manufactures** responsible for planning, for designing, for developing and for manufacturing their products.
- CRA address **manufactures**, **distributors** and **importers**.

| IoT vertical | End-product | Sub-component in the supply chain, e.g., MCU |
|---|---|---|
| **Health, Medical products** | no | yes |
| **Automotive** | no | yes |
| **Industrial IoT** | yes | yes |
| **Consumer IoT** | yes | yes |

# Out of Scope

– Products, which fall under **other regulation**, e.g.,

**Medical Products**

*EU MDR-2*

**Automotive Products**

*UNECE R 155*

**Defense Products**
**Aviation**
**National Security**

# How the Cyber Resilience Act will work in practice

## 90% of products

**Default category**

Self-assessment

**Criteria:**
n/a

**Examples**


Smart Speakers


Word processing


Photo editing


Games

## 10% of products

**Critical "Class I"**

Application of a standard or third-party assessment

**Critical "Class II"**

Third-party assessment

**Criteria**

- Functionality (e.g. critical software)
- Intended use (e.g. industrial control/NIS2)
- Other criteria (e.g. extent of impact)

**Critical products**

**Examples** (Annex III)


Password managers


Firewalls


**Micro-controllers**

**Examples** (Annex III)

Operating systems


Industrial firewalls


**CPUs**

# Requirements of the CRA guideline

**Prerequisite**

**Security by default**

- Enable adequate security updates
- Protection from unauthorized access
- Confidentiality and integrity of data, commands and programs
- Minimization of data
- Availability of essential functions
- Minimize own negative impact on other devices
- Limit attack surfaces
- Reduce impact of an incident
- Record and monitor security relevant events

≠

**Penalty**

- Up to **15m€** or
- **2,5%** of the global company annual turnover

# Milestones

## Oct/2024

### The Start

The CRA Regulation is published.

## Q3/2026

*+21 months*

### The Amendments

Obligation to **report of vulnerabilities and incidents.**

## Oct/2027

*+36 months*

### The Implementation

The finalization of the regulations and its **entry into force.**

# Lifecycle Management


– Products shall be designed, developed and produced using security by design principles.
– Product need the **CE-label.**

– Products in operation shall remain secure for itself and others.
– Security updates to users for a **minimum of 5 years** (cont.).

## Conformity Test

- Test standard will be developed after the regulation is published.
  - Responsible is CENELEC
- Test catalogue (1st draft) is expected **End of 2025**.
- For 3rd party tests the **CE test labs** are required.
  - The EU manages a public list of the test labs in all member states.

Remark for **Non-Conformity of product:** the product being forcible **withdrawn** from the EU market and product **recall** is possible.

## Requirements on development

- Manufacturers must assess a product's **cybersecurity risks** and **requirements** in detail at all stages of the product development.
- Manufacturers must conduct **regular audits/tests** and **evaluations** to verify the security of the products during the support period.
- Care must be taken to ensure that **3rd parties** (e.g. suppliers) and **open sources do not compromise product security**.
- To track product components and vulnerabilities the CRA requires the manufacturers to create a **software bill of material** (SBOM).

## Requirements on documents – the following information is required:

- **Manufacture** of the product.
- **Central point of contact** for dealing with vulnerabilities.
- Instructions for **installing security updates**
- Instructions for enabling/disabling **automatic security updates.**
- **Intended use** of the product and information on its security properties.
- Known circumstances that could expose the products to cybersecurity risks.
- Duration of the support period.
- Instruction for the **secure commissioning** and use of the product.

## Requirements for reporting vulnerabilities

- Reporting of security-relevant vulnerabilities (events) to the EU central reporting point.
- In (max.) **24 hours** the vulnerability must be reported.
- In (max.) **72 hours** a comprehensive description of the vulnerability (incidents) must be issued.
- In case of hacking (using the vulnerability) in (max.) **14 days** damage limiting measures and a final report are requested.

# Software Vulnerabilities = CVE list

## Common Vulnerabilities and Exposures

- A directory which show **gaps & risks in SW products**
- Since 1999 in use
- Updated daily
- More than 100,000 entries
- Main purpose: **avoid double/multiple reports**
- Scoring of the entries:
  - 0 (no threat) to
  - 10 (critical)

# Questions?

**Dr. Detlef Houdeau**

# TAKE A MINUTE AND GIVE US FEEDBACK …

RATE NOW!