Navigating the CRA Cyber Resilience Act

Real-World Lessons in Securing Connected Products

1st September 2026

Jonathan Marshall, Founder and Director, SafeShark

SafeShark

Who Are We?

- Founded on a bike ride 10 years ago
- First presented Consumer IoT security in 2017 at IoTSF
- In 2019 we won DCMS funding as part of Secure by Design
- Market leading CRA, RED and PSTI compliance specialists
- We provide straightforward compliance testing process
- Currently working with large CE manufacturers worldwide

Cybersecurity is no longer just a technical feature; it is a fundamental legal requirement for market access.

What is the CRA?

Introducing the Cyber Resilience Act: the EU's new plan to make sure all digital products on the EU market are safe from cyber threats. This important rulebook covers the security of products considering their lifecycle. It requires that devices and software are designed, updated, and maintained to protect users in our increasingly digital world

https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

Components of CRA

The CRA consists of broadly three main elements combining process and testing:

Secure Design & Development

Foundational security practices throughout the product lifecycle.

Deadline: Dec 11, 2027

Essential Requirements Testing

Rigorous testing against mandatory cybersecurity standards.

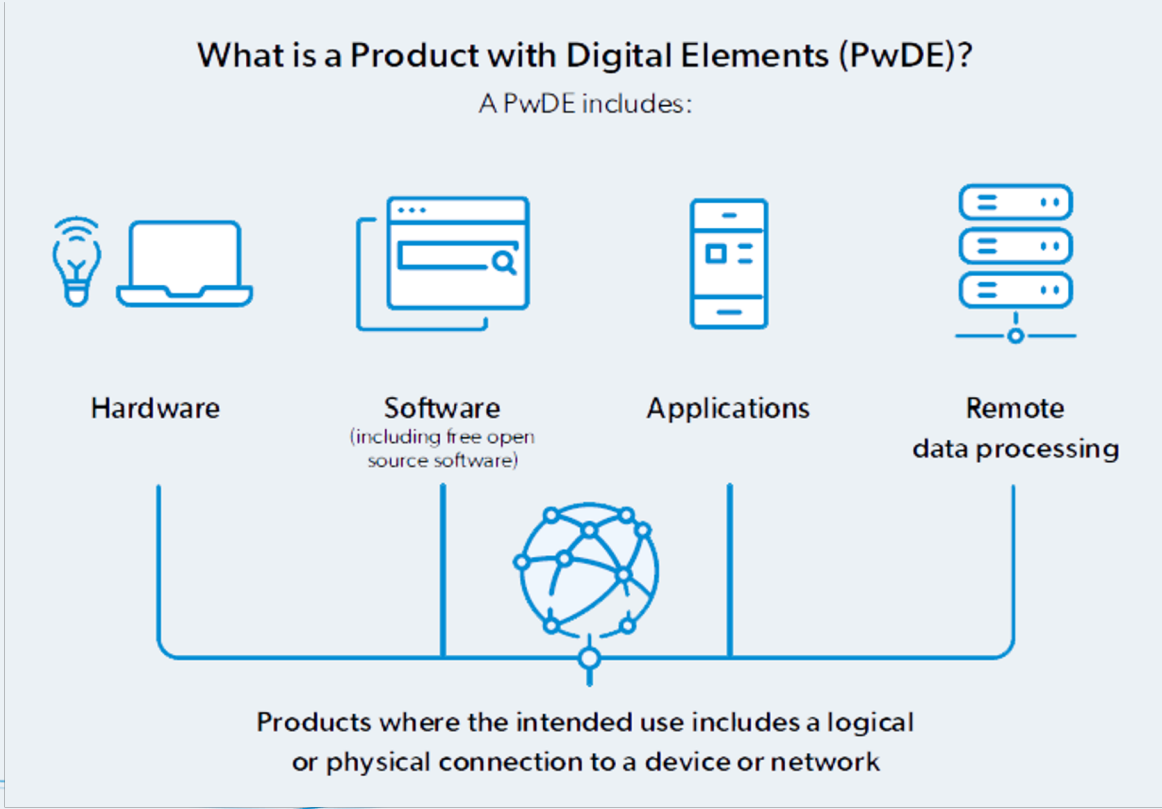
Deadline: Dec 11, 2027

Vulnerability Handling & Reporting

Establishing processes for reporting and addressing security flaws.

Deadline: Sept 11, 2026 (Reporting)

What's in scope of CRA



SafeShark

The CRA product categories

Default category

Low-risk products (90% of market) like TVs, radios, white goods.

Manufacturers can self-assess compliance via horizontal standards.

Important Class I*

High-risk products like smart home assistants and locks.

Requires testing against specific vertical standards.

Important Class II* + Critical**

Highest risk: firewalls, smart meter gateways.

Typically requires mandatory third-party assessments for compliance.

What’s out of scope of CRA

Medical devices

Motor vehicles

Civil aviation

Marine equipment

National defence and security

SafeShark

What’s out of scope of CRA

Exemption considerations for:

- Free and open-source software provided outside commercial activity
- Products for internal use only
- **Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS)***

**Cloud services fall in scope if they are required for the functionality of the product and are under the responsibility of the manufacturer*

Vulnerability reporting requirements

The full requirements for CRA vulnerability reporting are in Article 14 of the CRA (coming into force 11th Sept 2026).

Manufacturers must report to their CSIRT and ENISA via the single reporting platform:

Severe incidents

Exploited vulnerabilities

Reporting Timelines & User Obligations:

Early Warning

An early warning within 24 hours

Notification

A notification within 72 hours

Final Report

14 days after corrective measure or 1 month after notification

User Info

Inform users of risk mitigation and corrective measures

Reminder: The manufacturer is responsible for open source software integrated into the product

Single Reporting Platform (SRP)

Reports of exploited vulnerabilities or severe incidents need to be submitted to **ENISA**. ENISA is developing the SRP to centralize and streamline this process.

Centralized Reporting

A single point of entry for all CRA-mandated vulnerability and incident reports.

Official Resource

Learn more at the ENISA project page:

enisa.europa.eu/srp

Placing on the market

Once the requirements have been met, technical documentation must be in place, CE marking applied, and the product managed for its lifecycle.

Technical Documentation

Requirements are outlined in Annex VII of CRA.

New: SBOM included.

CE Marking

The CE marking must be applied once conformity is established.

Lifecycle Management

The product must be managed effectively throughout its entire lifecycle.

Key timelines

The Cyber Resilience Act (CRA) comes into force in stages, beginning in 2026 and becoming fully applicable by late 2027.

Sept 11th 2026

Reporting Requirements

Manufacturers must report exploited vulnerabilities or severe incidents to ENISA/CSIRTs.

Dec 11th 2027

Full CRA Application

- Secure development lifecycle
- Essential requirements testing
- Vulnerability handling

The Cost of Non-Compliance

€15M

Or 2.5% of Global Revenue

Severe Financial & Market Risk

Failing to meet essential cybersecurity requirements triggers massive fines. Secondary violations can cost up to €10M (or 2%), while providing misleading data can cost €5M (or 1%).

Beyond fines, market surveillance authorities can mandate product withdrawals, expensive recalls, and outright bans from the European market.

The Cost of Delay

- **Documentation fixes can take days, but according to our experience fixing cryptographic issues can take months.**
- **When an emerging threat compromises a static key, how fast can you respond?**
  - Our data shows the answer is not fast enough. A long fix time reveals that many manufacturers lack the architectural resilience to push secure, unique cryptographic updates efficiently.

The sel4 Advantage

- The EU Cyber Resilience Act (CRA) mandates that connected software and hardware products enforce security-by-design, minimize attack surfaces, and prevent unauthorized access or data modification.
- seL4 serves as a structural enabler for meeting these regulatory requirements:
  - **Provable Vulnerability Elimination**:
  - **Fault Containment and Isolation**:
  - **Streamlined Compliance**:

Provable Vulnerability Elimination

- The CRA emphasizes the reduction of exploitable flaws and a shift toward memory-safe environments.
- seL4's formal verification mathematically proves the kernel's integrity and confidentiality, inherently satisfying CRA mandates by definitively eliminating memory-safety vulnerabilities at the system's most privileged level

Fault Containment and Isolation

- The CRA requires systems to limit the impact of compromised components.
- seL4's architecture guarantees strong spatial and temporal isolation. If an application or network driver is compromised, the hardware-enforced capability model prevents the attacker from escalating privileges or accessing critical system operations.

Streamlined Compliance

- Formal verification is actively being integrated into cyber resiliency standards for operating systems.
- By building on a mathematically proven core, manufacturers drastically reduce their Trusted Computing Base (TCB), making it significantly easier to document, audit, and prove CRA compliance for products in critical infrastructure, IoT, and defense.

Final Takeaway

Although seL4 does not require CRA compliance, commercial manufacturers need seL4 so they can easily prove to regulators that the foundational layer of their commercial product is secure by design.

Thank you

Q&A

Want to discuss one to one?
Scan the QR code to get in touch
jonm@safeshark.co.uk