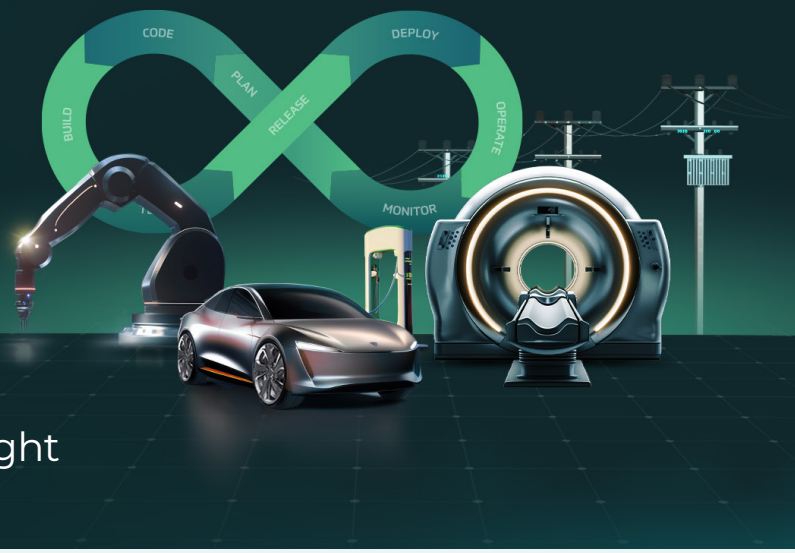
C2A security

Cyber Resilience Act (CRA)

Product Security Regulation Spotlight



Cyber Resilience Act (CRA) Snapshot

EU-wide legislation introducing common cybersecurity rules for manufacturers & developers of products with digital elements.

Secure and resilient digital environment, by establishing a baseline for product security regulations across the supply chain, throughout the product lifecycle.

- Industrial and Manufacturing
- Consumer Electronics
- Consumer Appliances
- Information Technology

March 12th, 2024
Legislation approved ✓

October 10th, 2024
Current status
The Council adopted the CRA, and it will be published in the coming weeks

20th day following its publication
Once adopted: the CRA will enter into force

36 months / 21-month Upon entry into force
36 months for adaption limited 21-month grace period

Essential Requirements

- ✓ Dynamic Risk Management & Assessments
- ✓ Security and Operations by Design (SDLC)
- ✓ Continuous Vulnerability Updates & Reporting
- ✓ Prompt Response & Mitigation
- ✓ On-demand Documentation, Reports, and Analytics for Cybersecurity Risks, Business Impacts and more

Violations & Fines

Violations of the CRA	* Up to 15,000,000 EUR / 2.5%
Non-compliance with other Obligations	* Up to 10,000,000 EUR / 2%
Supply of Incorrect, Incomplete or Misleading Information	* Up to 5,000,000 EUR / 1%

* Of the total worldwide annual turnover of the preceding fiscal year – whichever is higher

Driving Innovation with

DAIMLER TRUCK · BMW · APTIV · inCSS · SIEMENS · Valeo · NTTGroup · MARELLI

Unmasking the CRA Requirements

Breaking down the Essential Requirements into Common Security Practices Covered by our Product Security Platform

Risk Management

- Manage cybersecurity events based on risk
- Protect the availability of essential functions
- Minimize the negative impact on your business
- Limit the attack surface of your entire supply chain
- Securely manage and distribute software patches and updates

Vulnerability Management

- Delivered without any known exploitable vulnerabilities
- Use appropriate mitigation mechanisms
- Address vulnerabilities through updates and notifications to users
- Address and remediate vulnerabilities with minimal delay
- Enforce a policy on coordinated vulnerability disclosure
- Facilitate sharing of information about potential vulnerabilities
- Delivered with a secure by default configuration

SDLC & Reporting

- Deploy appropriate access control mechanisms
- Protect the confidentiality and integrity of data
- Record and/or monitor relevant internal activity
- SBOM covering the top-level dependencies of the product
- Regularly test and review the security of the product
- Publicly disclose information about fixed vulnerabilities

Holistic Coverage of CRA Requirements

C2A Security's Risk Management & Automation Product Security Platform

Dynamic Risk Management

Centralized Risk Platform ensures threat analysis, risk assessment, and management throughout the product lifecycle with all product security data layers (BOM, threats, etc.).

Security and Operations by Design

Agile Product Security Development and Operations. That optimizes the needed security controls for development teams and enriches operations with product security data for faster incident response.

Context-based SBOM and Vulnerability Management

Risk-Driven Approach for Automated SBOM and Vulnerability Management, prioritizing true impact on the product and optimizing mitigation based on cost and time.

Supply Chain and Team Collaboration

Manage Internal Teams and the Supply Chain utilizing centralized real-time sharing and collaboration of systems, joint work at scale, and full visibility into the supply chain and internal teams.

On-Demand Analytics, Dashboards, and Reports

On-Demand Analytics, Dashboards, and Reports. Compliance workflows, reports, and analytics that allow data-driven decision-making for engineers and management based on risk, supply chain behavior, business impact, and more.

Ensure Automated Compliance with the CRA

Streamline Security and Data Flow

Set a New Standard for Product Security