achelos

Cyber Resilience Act (CRA)
Cyber security for digital products

Enhanced cybersecurity for products with digital elements

Today, an increasing number of products are incorporating digital components to meet the rising demands for connectivity and functionality. However, many products still suffer from inadequate cybersecurity, leaving users unsure about which products are truly cyber secure.

The EU Cyber Resilience Act (CRA) aims to protect consumers and businesses that purchase or use products or software with a digital component. The regulation requires manufacturers to implement comprehensive cyber security measures throughout the entire product lifecycle – from development and placing on the market to updates and vulnerability handling.

The CRA applies to products, software and hardware with digital elements and therefore affects a wide range of industries – from connected devices and embedded systems to software products, cloud services and sector-specific solutions.

The CRA entered into force on 11 December 2024 and will be implemented in phases. By the end of 2027, all new products must comply with the CRA requirements.

Our security engineering services

Introduction to the EU Cyber Resilience Act (CRA) – workshop

- Cybersecurity risks for manufacturers
- Understanding the law on cyber resilience
- Resulting cybersecurity requirements for companies and their processes
- Resulting cybersecurity requirements for products with digital elements

achelos

Assessment and analysis of CRA gap

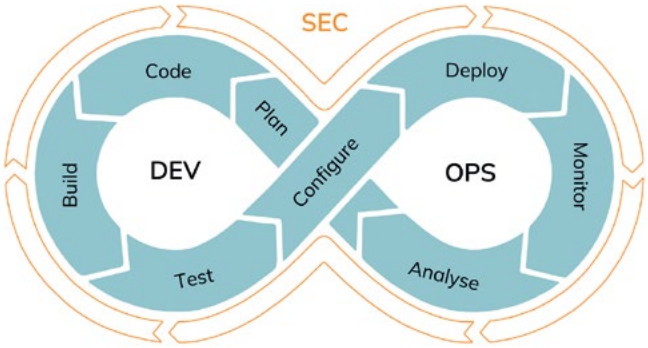
- Analysis of selected products in the customer portfolio
- Getting to know the product to be analysed and identifying the relevant requirements of the Cyber Resilience Act
- Analysis of the current status with regard to the CRA
- Identifying gaps compared to the CRA
- Drafting an action plan

Threat Analysis and Risk Assessment (TARA) – workshops

- Analysis of selected products in the customer portfolio
- Workshop on product consolidation and identification of product assets
- Threat Analysis and Risk Assessment (TARA) by experienced security consultants
- Workshop on risk minimisation
- Detailed TARA report

Further services in the Secure Development Lifecycle (SDL):

- Security concept development and security architecture
- Secure product development
- Hardening of software and system components
- Consultancy on security engineering tools
- Testing of security functions
- Vulnerability assessments and penetration testing
- Support with conformity assessment



Cybersecurity built in from the start

achelos supports you in achieving CRA compliance efficiently and with confidence. Our security engineers work alongside your teams throughout the development lifecycle, embedding cybersecurity into your products from day one – practical, standards-driven and aligned with regulatory requirements.
Make your development ready for tomorrow – contact us today.

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Allianz für Cyber-Sicherheit Teilnehmer