

## PRESS RELEASE

---

NEWS

July 22, 2024 || page 1 | 4

---

Fraunhofer AISEC at the it-sa Expo&Congress 2024

### **Knowing where you stand — compliance testing for the Cyber Resilience Act with “Confirmate”**

**With its Cyber Resilience Act (CRA), the EU will in future require manufacturers to guarantee the IT security of products with digital elements. Once the CRA comes into force, which is expected to be in 2024, they will have a maximum of 36 months to demonstrate that their products comply with the new standard. However, due to complex architecture designs and the use of third-party components, assessing the need for action in concrete terms is a challenge.**

**The Fraunhofer Institute for Applied and Integrated Security AISEC is conducting research into automated compliance testing of software components with Confirmate. The tool will help to automatically assess compliance with the CRA and determine the individual need for action. Confirmate compares the security settings with the CRA specifications and helps to quickly identify specific vulnerabilities in the product. The analysis therefore saves valuable time for planning and implementing security measures.**

**Fraunhofer AISEC will be presenting the tool's current range of functions and its application for the first time at this year's it-sa Expo&Congress (Nuremberg, October 22–24, 2024) at the joint Fraunhofer booth in Hall 6, Booth 6-314.**

Garching near Munich, July 22, 2024. Manufacturers of products with digital elements are facing increasingly stringent cybersecurity requirements, primarily due to the imminent Cyber Resilience Act (CRA). This EU regulation requires manufacturers to ensure that fundamental cybersecurity requirements are met, such as ensuring the confidentiality and integrity of data. It also stipulates that manufacturers must maintain the IT security of their products throughout their entire life cycle. As a consequence, manufacturers must demonstrate how they address and rectify vulnerabilities in their products. In future, it will only be possible to place products on the European market with a CE mark if proof of compliance with the CRA is provided.

---

Contact:

Tobias Steinhäuser | Fraunhofer Institute for Applied and Integrated Security AISEC  
Lichtenbergstraße 11 | 85748 Garching near Munich | Phone +49 89 322 9986-170 | [presse@aisec.fraunhofer.de](mailto:presse@aisec.fraunhofer.de)

## **Difficulties in determining individual need for action**

The EU regulation poses new, complex challenges for manufacturers: Following the introduction of the CRA, which is expected to occur sometime in 2024, they will have 36 months to prepare for the new provisions. These will apply to products that are expected to be launched on the market from 2027. However, the complex architecture designs of products with digital elements, consisting of numerous components, including those from third-party providers, make it challenging to clearly identify the individual need for action. The CRA demands a level of security that is proportionate to the risks and explicitly includes the entire product supply chain in the catalog of requirements.

---

NEWS

July 22, 2024 || page 2 | 4

---

## **Finding the starting point on the path to compliance**

This is where Confirmate comes in — a research project launched by Fraunhofer AISEC that supports manufacturers in assessing whether their digital products comply with the CRA. With Confirmate, it will be possible to better understand and document the security requirements for products despite their complex architectures. The tool is designed to show which CRA requirements are being met and where there is still a need for action.

The solution focuses on the source code analysis of the software components integrated in the product and the interfaces provided (e.g., to cloud backends). The company's existing documentation of processes is also reviewed, for example for vulnerability management purposes. Confirmate compares existing security settings with the requirements from the CRA and technical specifications, such as the specifications of the German Federal Office for Information Security (BSI). The program also identifies any third-party software components used and verifies their compliance with the EU regulation using information from databases on known vulnerabilities.

"Confirmate combines static analysis for testing the security properties of program code with automated compliance evaluation. The ability to manually add documents and declarations makes the program a comprehensive monitoring tool that provides a reliable assessment of the compliance status of a digital product," says Christian Banse, Department Head for Service and Application Security at Fraunhofer AISEC. Confirmate provides a detailed and easy-to-interpret overview of which requirements have already been met. This allows manufacturers to quickly identify the status quo of the product in terms of cybersecurity and the need for action with regard to the CRA.

Confirmate's semi-automated analysis process enables continuous evaluation of the program components so that product compliance information is always up-to-date and quickly available. The time saved can be used to design and implement security measures.

Using the results of the Confirmate analysis, experienced cybersecurity experts from Fraunhofer AISEC can support manufacturers of products with digital elements in implementing the necessary security measures in line with the CRA.

### it-sa Expo&Congress: See it in action at Booth 6-314

At this year's it-sa Expo&Congress from October 22–24, manufacturers and operators of products with digital elements will have the opportunity to find out more about the Confirmate tool at the joint Fraunhofer booth in Hall 6, Booth 6-314. The scientists from Fraunhofer AISEC will provide insights into the functionality of the AISEC solution for CRA compliance testing using security-critical sample software that is subject to the Cyber Resilience Act.

---

NEWS

July 22, 2024 || page 3 | 4

---

#### Press photo



With Confirmate, Fraunhofer AISEC is launching a project to develop a software solution that helps manufacturers to check whether their digital products are compliant with the Cyber Resilience Act.

#### **Kurzprofil Fraunhofer AISEC**

The Fraunhofer Institute for Applied and Integrated Security AISEC is considered one of the leading international institutions with regard to applied research in the field of cybersecurity. More than 230 highly qualified employees work to develop customized security concepts and solutions for both commercial businesses and the public sector in order to significantly improve the overall competitiveness of customers and partners. Among these are solutions for greater data security as well as effective cybercrime protection to prevent industrial espionage and sabotage attacks. The range of expertise spans from embedded and hardware security, automotive and mobile security all the way to security solutions for industry and automation. Fraunhofer AISEC also makes it possible to assess the security of networked and embedded systems, hardware and software products as well as web-based systems and cloud services at its modern test labs.

<https://www.aisec.fraunhofer.de/>