



OSCRAT
Open-Source Cyber Resilience Act Tools



As Cyber Resilience Act reporting obligations take effect, OSCRAT launches state-of-the-art, free, open-source platform for European SMEs

Launched on 11 September 2026 — the day new Cyber Resilience Act (CRA) reporting obligations begin to apply — the Open-Source Cyber Resilience Act Tools (OSCRAT) platform gives European Small and Medium Sized Enterprises (SMEs) an accessible state-of-the-art environment for managing CRA assessment, cybersecurity risk, Software Bill of Materials (SBOMs), vulnerabilities, incidents and compliance documentation.



The OSCRAT platform was officially launched during the project's online Final Event on 11 September 2026, as the first Cyber Resilience Act reporting obligations entered into application.

FOR IMMEDIATE RELEASE | 11 September 2026

The OSCRAT project consortium officially launched the **OSCRAT platform**, a free, state-of-the-art open-source solution designed to help European small and medium-sized enterprises (SMEs) translate the requirements of the **Cyber Resilience Act (CRA)** into structured cybersecurity and compliance processes.

The launch comes on a significant date for European cybersecurity regulation. **From 11 September 2026, manufacturers must report actively exploited vulnerabilities and severe incidents affecting the security of products with digital elements.** The CRA requires an early warning within 24 hours of becoming aware of such an event, followed by a more detailed

notification within 72 hours. While most other CRA provisions will apply from 11 December 2027, these reporting requirements bring the regulation into practical application for businesses today.

Against this backdrop, OSCRAT addresses one of the major challenges facing European SMEs: **how to turn increasingly complex cybersecurity obligations into manageable day-to-day processes without the resources available to larger organisations.**

The platform was presented during the **OSCRAT Final Event**, held online on 11 September 2026, bringing together cybersecurity experts, European stakeholders, digital innovation actors and organisations preparing for the implementation of the CRA.

Turning CRA requirements into practical workflows

The Cyber Resilience Act is changing the way products with digital elements must be designed, developed, maintained and secured throughout their lifecycle. For SMEs in particular, meeting these requirements can involve considerable technical expertise, organisational change and documentation.

OSCRAT has therefore been designed to bring key cybersecurity and compliance activities together within a single environment. **The state-of the art OSCRAT platform provides full versioning life-cycle for products with digital elements to meet European CRA requirements. Its functionalities include:**

CRA applicability and compliance assessment, helping organisations understand which requirements may apply to their products and structure the related compliance work;

Software Bill of Materials (SBOM) management and security scanning, improving visibility over software components and potential vulnerabilities;

Vulnerability and incident management, supporting the recording, assessment and follow-up of security issues and corrective actions;

Cybersecurity risk assessment and risk-treatment workflows, helping organisations identify and manage product-related security risks;

Configuration management and compliance task management, supporting the organisation and traceability of security activities;

Technical documentation and Declaration of Conformity workflows, helping organisations organise the evidence and documentation needed throughout the compliance process;

Audit logging and traceability, providing a record of activities performed within the platform.

The platform also incorporates security-awareness and training-related activities.

By connecting regulatory requirements with concrete workflows, OSCRAT aims to make cybersecurity compliance **more understandable, structured and accessible for SMEs**, while helping organisations embed cybersecurity into their broader product-development and risk-management processes.

The OSCRAT platform presented live

During the Final Event, the consortium presented the development journey and main achievements of the OSCRAT project alongside an overview of the CRA and its practical implications for European companies. A live demonstration showcased the final OSCRAT platform and representative workflows, illustrating how organisations can move from assessing CRA applicability and compliance requirements to managing products, vulnerabilities, incidents, risks, SBOMs, tasks and technical documentation.

The programme also brought OSCRAT into dialogue with other European initiatives working on CRA implementation, cybersecurity standards and digital-product security, highlighting the importance of collaboration as Europe moves from regulatory preparation towards practical implementation.

Making cybersecurity compliance more accessible

OSCRAT has been developed primarily with **European SMEs and manufacturers of products with digital elements** in mind, while also serving as a resource for Digital Innovation Hubs, cybersecurity professionals, industry associations, policymakers and other organisations supporting businesses through the changing European cybersecurity landscape.

Its **free and open-source model** is central to this ambition. By lowering financial and technical barriers to accessing cybersecurity and compliance tools, OSCRAT seeks to support broader participation in Europe's transition towards more secure digital products.

Open-source availability also promotes transparency, collaboration and continued technical development, enabling organisations and cybersecurity communities to use, adapt and contribute to the platform beyond the lifetime of the project.

About OSCRAT

OSCRAT – Open-Source Cyber Resilience Act Tools is a European project dedicated to strengthening the cyber resilience of European SMEs by developing free, open-source tools that support activities related to compliance with the Cyber Resilience Act.

The project brings together expertise in **cybersecurity, software development, regulatory requirements, stakeholder engagement and digital innovation**, with the objective of translating CRA requirements into practical and accessible tools for European businesses.

OSCRAT is co-funded by the European Union under **Grant Agreement No. 101190180** and supported by the **European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)**.

Further information: [Project website](#) | [OSCRAT platform](#) | [Contact](#)

Media contact:

PMF Research, projects@jogroup.eu