OSCRAT
Open-Source Cyber Resilience Act Tools

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

PRESS RELEASE

OSCRAT: an European Project to strengthen the cybersecurity of SMEs and verify compliance with the Cyber Resilience Act.

Introduction

The lack of resources dedicated to cybersecurity can result in serious economic and reputational damage for SMEs in Europe. This has led to the creation of OSCRAT (Open-Source Cyber Resilience Act Tools), a project funded by the European Union's Digital Europe programme, which aims to:

- ✓ improve the Union's competitiveness in the global economy;
- ✓ bridge the digital divide between Member States;
- ✓ promoting the Union's capacity to act in key areas of digital technology.

The programme also provides funding for strategic projects in the following key sectors:

- Cybersecurity;
- Supercomputing;
- Artificial Intelligence (AI);
- Advanced Digital Skills.

Co-funded by the European Union

The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre. Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

What is OSCRAT?

The **OSCRAT** project aims to improve the **cybersecurity** of European SMEs. How? By focusing on a number of European policies, such as the **Digital Single Market** strategy, the EU Radio Equipment Directive (**RED**), the **AI Act**, **NIS2** and the **European Green Deal**.

The project aims to create a **tool that is free and open-source** to help companies evaluate their IT security system, verifying that it complies with the **Cyber Resilience Act** (CRA), whose purpose is to guarantee compliance with cybersecurity quality standards at a European level.

OSCRAT Objectives

The OSCRAT Project has five different objectives:

1. Enhance the cyber resilience of European SMEs

OSCRAT offers open-source tools and resources to enable European SMEs to effectively manage **cyber threats**.

2. Facilitating compliance with the CRA

OSCRAT helps SMEs comply with the **CRA** (Cyber Resilience Act), automating the procedures for producing the necessary documents.

3. Promoting cross-border collaboration

OSCRAT promotes **cooperation across borders** and the sharing of know-how and expertise among SMEs, cybersecurity experts and European institutions, assessing the level of participation in the workshops and events planned for the project on a case-by-case basis.

4. Contributing to environmental sustainability

OSCRAT wants to contribute to the political objective of environmental sustainability, in line with the guidelines of the **European Green Deal**.

5. Promoting consistency with EU policies

OSCRAT's activities are consistent with European cyber security policies.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. - Project: 101190180

What is the 'OSCRAT' tool purpose?

The eponymous **tool** that will be created will improve the cyber resilience of SMEs throughout Europe. Specifically, it will allow companies to:

1. Generating control checklists

The tool will be able to identify the main categories of digital products, generating **checklists**.

2. Managing SBOM manifests

OSCRAT will create the **SBOM** (**Software Bill of Materials**) manifests and the files describing each project with detailed reports compliant with the **SPDX/CycloneDX** standards.

3. Equipping SMEs with a strategic approach

The toolkit provided by OSCRAT will equip SMEs with a **strategic approach** to better manage vulnerabilities, in accordance with **ISO/IEC standards**.

4. Incident Handling process

Once the seriousness of the incidents has been assessed, OSCRAT will report them to the main European cybersecurity organisations, **ENISA** and **CSIRTS**, if significant.

5. Document centralisation

OSCRAT will create a **unique, centralised archive** to facilitate access to information on computer security.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. - Project: 101190180

The OSCRAT consortium

The project consortium is composed by cybersecurity experts and Digital Innovation Hubs, from different European countries:

1. PMF Research (Project coordinator – Italy)

Research and development centre based in **Catania**; it has been working in the field of information and communication technologies (**ICT**) since 2003. The main areas of research are:

- Augmented Reality (**AR**);
- Virtual Reality (**VR**);
- Artificial Intelligence (**AI**);
- Internet of Things (**IoT**);
- **Blockchain**.

The company collaborates with other research centres and **Italian Public Administrations**, participating in many national and European projects.

2. OVES Enterprise (Romania)

Oves Enterprise is based in **Cluj-Napoca**; it is a global software engineering company with experience in **cybersecurity**, **fintech** and **outsourcing services**. In more than 9 years of experience it has trained and recruited the best talents in the aforementioned sectors.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. - Project: 101190180

3. ENERSEC (Romania)

ENERSEC is a **Romanian SME** specialising in technical consultancy and governance for **IT security**, and has been active since **2013**.

4. EDIH Trakia (Bulgaria)

The **EDIH Trakia** consortium brings together **universities**, **SMEs**, **public administrations** and **trade associations** with the aim of bridging the digital divide in Bulgaria. It is a partner of the Enterprise Europe Network (**EEN**) and the European Cybersecurity Corridor.

5. EMAG (Poland)

EMAG, with over **7,000 employees** and **22 research institutes** located in **12 cities in Poland**, is a partner of the Łukasiewicz research network, specialising in applied computer science, information technology and computer security. It excels in the fields of Industry 4.0.

6. Unicis.Tech (Estonia)

Unicis is a start-up that focuses entirely on simplifying and managing privacy and risk. How? By eliminating manual procedures in favour of **compliance procedures**.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. - Project: 101190180

OSCRAT Work Packages

The OSCRAT project is divided into **five** main phases (**work packages**), each led by a partner of the consortium:

1. Project Management (WP1) – PMF Research

PMF Research (a **JO Group** company) and development centre will ensure that the project objectives are achieved within the **budget** and **deadline constraints**. In other words, it will manage all activities related to general management and **coordination**, such as project meetings, financial management and communication tools.

2. Requirements gathering and analysis (WP2) – EMAG

EMAG will collect and analyse the needs of European stakeholders and SMEs to define the scope, functionality and compliance of the tool with the requirements of the **Cyber Resilience Act**.

3. Software Design and Development (WP3) – Oves Enterprise

Based on the results of WP2, **Oves Enterprise** will develop the software: **user-friendly** and in line with **CRA** standards and the needs of **SMEs**.

4. Stakeholder Engagement (WP4) – EDIH Trakia

EDIH Trakia will organise **workshops**, **webinars** and an **international event** to improve the tool with feedback and real use cases.

5. Dissemination & Exploitation (WP5) – PMF Research

PMF Research will develop a **marketing and digital communication** strategy to ensure the visibility of the project, raise awareness of CRA issues and encourage the adoption of the tool even after the end of OSCRAT.

This **roadmap** will ensure a participatory development, oriented towards the needs of European SMEs and aligned with the EU's political objectives in the field of **cybersecurity**.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. - Project: 101190180

Want to get updates on the OSCRAT project?

Cybersecurity is no longer an option and OSCRAT is a unique initiative to **strengthen the cyber resilience of European SMEs**.

If you want to know more about OSCRAT, or are looking for partners for similar projects, please contact us:

- ✓ **Telephone**: 0957225331
- ✓ **e-mail**: projects@jogroup.eu
- ✓ **Website**: oscrat.eu

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. - Project: 101190180