PRESS RELEASE

OSCRAT: completato il WP2. Inizia lo sviluppo del tool

OSCRAT: il progetto completa il WP2 e avvia la fase sviluppo del tool che aiuterà le PMI a rafforzare la cybersecurity e garantire conformità al CRA.

OSCRAT: completato il WP2. Inizia lo sviluppo del tool sulla cybersecurity e la conformità al CRA

OSCRAT, il progetto europeo che sviluppa strumenti open source per aiutare le PMI ad adeguarsi al Cyber Resilience Act (CRA), entra in una fase decisiva: il consorzio, infatti, ha appena completato il Work Package 2 (WP2), dedicato alla raccolta e analisi dei requisiti, e si prepara ora alla progettazione e sviluppo vero e proprio della piattaforma.

Perché è nato OSCRAT?

La mancanza di risorse dedicate alla cybersecurity espone le PMI europee a rischi economici e reputazionali significativi. OSCRAT (Open-Source Cyber Resilience Act Tools), finanziato dal programma Europa Digitale dell'Unione Europea, nasce proprio per colmare questo gap, con tre obiettivi di policy di alto livello:

rafforzare la competitività dell'Unione nell'economia globale;
ridurre il divario digitale tra Stati membri;
potenziare la capacità d'intervento dell'UE nelle tecnologie digitali strategiche.

Il cuore del progetto è lo sviluppo di un tool gratuito e open source che permetta alle imprese di:

valutare il proprio sistema di sicurezza informatica;

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.

verificare la conformità ai requisiti del Cyber Resilience Act, il regolamento europeo che definisce gli standard di cybersicurezza per i prodotti con elementi digitali.

OSCRAT si muove in coerenza con altre politiche UE (Mercato Unico Digitale, direttiva RED, AI Act, NIS2, European Green Deal) e persegue cinque obiettivi operativi: accrescere la resilienza delle PMI, facilitare la conformità al CRA, favorire la collaborazione transfrontaliera, contribuire alla sostenibilità ambientale e far rispettare il quadro delle politiche europee sulla cybersicurezza.

Un nuovo traguardo: il completamento del WP2

Il consorzio entra ora in una nuova fase strategica: guidato dal partner Łukasiewicz AI, ha prodotto il deliverable D2.1 – Comprehensive Project Requirements Document. Questo documento raccoglie e organizza in modo sistematico tutti i requisiti che guideranno progettazione, sviluppo e validazione degli strumenti OSCRAT.

Il completamento del WP2 ha permesso inoltre di:

1. Definire lo scopo tecnico degli strumenti OSCRAT

Sono state descritte in dettaglio le funzionalità dei principali moduli:

- Checklist Automation;
- SBOM Management;
- Vulnerability & Incident Handling;
- Centralizzazione della Documentazione.

2. Disegnare workflow conformi al CRA

I partner hanno modellato l'intero processo di compliance, includendo:

- classificazione del prodotto (product classification);
- obblighi pre-market e post-market;
- definizione e verifica dei controlli di cybersicurezza;
- user stories e casi d'uso specifici per ogni tool.

3. Mappare i requisiti del CRA e i requisiti di cybersicurezza

Il consorzio ha condotto una revisione sistematica del regolamento CRA, identificando per ciascuno strumento:

- requisiti CRA applicabili;
- processi obbligatori di valutazione e documentazione;
- elementi essenziali di sicurezza da verificare;

In altre parole, il regolamento è stato "tradotto" in **funzionalità software operative**, condizione necessaria per automatizzare davvero i processi di conformità.

Co-funded by the European Union

Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione europea o del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza. Né l'Unione Europea né l'autorità concedente possono essere ritenute responsabili. - Progetto: 101190180

Il ruolo degli stakeholder e delle PMI

Uno degli elementi chiave del WP2 è stato il coinvolgimento degli stakeholder. L'analisi dei requisiti ha evidenziato:

- le **competenze tecniche** dei partner del consorzio (ricerca, sviluppo software, consulenza cybersecurity, digital innovation hubs);
- due cicli di **Stakeholder Survey**, svolti per comprendere esigenze, aspettative e criticità delle PMI e di altri attori potenziali utilizzatori dei tool di OSCRAT;
- lo stato dell'arte degli strumenti e delle iniziative legate al CRA in Europa.

Emergono anche due messaggi forti:

- le PMI attribuiscono grande valore agli strumenti di automazione della compliance, che riducono oneri interni, costi e necessità di competenze altamente specialistiche;
- vi è una disponibilità concreta a partecipare ai test, aspetto che sarà fondamentale nella fase di validazione degli strumenti.

Questi input sono stati incorporati nei flussi dei tool e nelle priorità di sviluppo, assicurando che OSCRAT non sia un esercizio teorico, ma una **piattaforma progettata "a partire dalla realtà"** delle PMI europee.

Cosa succede adesso?

Con il completamento del WP2, OSCRAT può avviare il **Work Package 3 – Software Design and Development**, coordinato dal partner Oves Enterprise.

Le prossime attività previste includono:

1. Progettazione architetturale della piattaforma

Definizione dell'architettura software, dei moduli, delle interfacce e delle integrazioni tra i vari strumenti (checklist, SBOM, gestione incidenti, repository documentale).

2. Sviluppo e integrazione delle funzionalità CRA

Implementazione delle feature mappate durante il WP2, con particolare attenzione all'usabilità per le PMI e all'allineamento puntuale ai requisiti CRA.

3. Validazione tramite casi d'uso reali

Test del sistema attraverso scenari concreti, in collaborazione con PMI e stakeholder che hanno già manifestato interesse e disponibilità a partecipare.

4. Workshop

Organizzazione di attività formative e dimostrative per facilitare l'adozione degli strumenti, per accrescere la consapevolezza sui temi del CRA e della cybersecurity.

Co-funded by the European Union

Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione europea o del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza. Né l'Unione Europea né l'autorità concedente possono essere ritenute responsabili. - Progetto: 101190180

Impatto atteso: una piattaforma open source sulla cybersecurity al servizio delle PMI europee

Guardando al quadro complessivo, OSCRAT si configura come una piattaforma:

- **open source e gratuita**, quindi accessibile anche alle realtà con budget limitati;
- **orientata alle PMI**, che spesso non dispongono di gruppi di lavoro dedicati alla compliance;
- **allineata al quadro normativo UE**, non solo CRA, ma anche alle strategie digitali più ampie;
- **costruita in modo collaborativo**, grazie al coinvolgimento di più partner da Italia, Romania, Bulgaria, Polonia, Estonia e di altri stakeholder;
- **sostenibile**, ovvero in sintonia con gli obiettivi dell'European Green Deal e con l'idea di una trasformazione digitale responsabile.

Il completamento del WP2 rappresenta molto più di una semplice tappa amministrativa: è il passaggio che trasforma la visione iniziale (**raccontata qui**) in una roadmap tecnica concreta per gli sviluppatori e per tutto il consorzio.

Nei prossimi mesi, con l'avanzamento del **WP3** e delle attività di **test e formazione**, OSCRAT mostrerà come tradurre il progetto in risultati concreti, capaci di aiutare davvero le PMI a **"fare sul serio" con la cybersecurity** e a farsi trovare pronte di fronte al **nuovo quadro normativo** delineato dal Cyber Resilience Act.

Contattaci per partecipare a progetti simili

Se vuoi saperne di più su **OSCRAT** o cerchi partner per progetti simili, puoi contattarci:

- chiamando al numero di telefono **0950936053;**
- scrivendo all'indirizzo e-mail **projects@jogroup.eu;**
- compilando il **contact form** in fondo alla pagina.

Co-funded by the European Union

Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione europea o del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza. Né l'Unione Europea né l'autorità concedente possono essere ritenute responsabili. - Progetto: 101190180