COMUNICATO STAMPA

OSCRAT: un progetto europeo per rafforzare la sicurezza informatica delle PMI e verificare la conformità alla legge sulla resilienza informatica.

Introduzione

La mancanza di risorse dedicate alla sicurezza informatica può comportare gravi danni economici e di reputazione per le PMI in Europa. Questo ha portato alla creazione di OSCRAT (Open-Source Cyber Resilience Act Tools), un progetto finanziato dal programma Digital Europe dell'Unione Europea, che si propone di:

- ✓ migliorare la competitività dell'Unione nell'economia globale;
- ✓ colmare il divario digitale tra gli Stati membri;
- ✓ promuovere la capacità di azione dell'Unione nei settori chiave della tecnologia digitale.

Il programma prevede anche il finanziamento di progetti strategici nei seguenti settori chiave:

- Cybersecurity;
- Supercomputing;
- Intelligenza artificiale (AI);
- Competenze digitali avanzate.

Co-funded by the European Union

Il progetto finanziato con l'Accordo di sovvenzione n. 101190180 è sostenuto dal Centro europeo di competenza per la sicurezza informatica.
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 che ha concesso il finanziamento possono essere ritenute responsabili.

Che cos'è OSCRAT?

Il progetto **OSCRAT** mira a migliorare la **sicurezza informatica** delle PMI europee. Come? Concentrandosi su una serie di politiche europee, come la strategia per **il Mercato Unico Digitale**, la Direttiva UE sulle apparecchiature radio (**RED**), l'**AI Act**, **NIS2** e l'**European Green Deal**.

Il progetto mira a creare uno **strumento gratuito e open-source** per aiutare le aziende a valutare il proprio sistema di sicurezza informatica, verificandone la conformità al **Cyber Resilience Act** (CRA), il cui scopo è garantire il rispetto degli standard di qualità della cybersecurity a livello europeo.

Obiettivi dell'OSCRAT

Il progetto OSCRAT ha cinque diversi obiettivi:

1. Migliorare la resilienza informatica delle PMI europee

OSCRAT offre strumenti e risorse open-source per consentire alle PMI europee di gestire efficacemente le **minacce informatiche**.

2. Facilitare la conformità con la CRA

OSCRAT aiuta le PMI a conformarsi al **CRA** (Cyber Resilience Act), automatizzando le procedure per la produzione dei documenti necessari.

3. Promuovere la collaborazione transfrontaliera

L'OSCRAT promuove la **cooperazione transfrontaliera** e la condivisione di know-how e competenze tra PMI, esperti di cybersecurity e istituzioni europee, valutando caso per caso il livello di partecipazione ai workshop e agli eventi previsti dal progetto.

4. Contribuire alla sostenibilità ambientale

L'OSCRAT vuole contribuire all'obiettivo politico della sostenibilità ambientale, in linea con le linee guida del **Green Deal europeo**.

5. Promuovere la coerenza con le politiche dell'UE

Le attività dell'OSCRAT sono coerenti con le politiche europee di sicurezza informatica.

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

Qual è lo scopo dello strumento "OSCRAT"?

L'omonimo **strumento** che verrà creato migliorerà la resilienza informatica delle PMI in tutta Europa. In particolare, consentirà alle aziende di:

1. Generare liste di controllo

Lo strumento sarà in grado di identificare le principali categorie di prodotti digitali, generando **liste di controllo**.

2. Gestione dei manifesti SBOM

OSCRAT creerà i manifesti **SBOM** (**Software Bill of Materials**) e i file che descrivono ogni progetto con rapporti dettagliati conformi agli standard **SPDX/CycloneDX**.

3. Dotare le PMI di un approccio strategico

Il toolkit fornito dall'OSCRAT fornirà alle PMI un **approccio strategico** per gestire al meglio le vulnerabilità, in conformità agli **standard ISO/IEC**.

4. Processo di gestione degli incidenti

Una volta valutata la gravità degli incidenti, l'OSCRAT li segnalerà alle principali organizzazioni europee di cybersecurity, **ENISA** e **CSIRTS**, se significativi.

5. Centralizzazione dei documenti

OSCRAT creerà un **archivio unico e centralizzato** per facilitare l'accesso alle informazioni sulla sicurezza informatica.

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

Il consorzio OSCRAT

Il consorzio del progetto è composto da esperti di cybersecurity e Digital Innovation Hubs, provenienti da diversi Paesi europei:

1. PMF Research (Coordinatore del progetto - Italia)

Centro di **ricerca e sviluppo** con sede a **Catania**, opera dal 2003 nel campo delle tecnologie dell'informazione e della comunicazione (**ICT**). Le principali aree di ricerca sono:

- Realtà aumentata (**AR**);
- Realtà virtuale (**VR**);
- Intelligenza artificiale (**AI**);
- Internet degli oggetti (**IoT**);
- **Blockchain**.

L'azienda collabora con altri centri di ricerca e con le **Pubbliche Amministrazioni italiane**, partecipando a numerosi progetti nazionali ed europei.

2. Impresa OVES (Romania)

Oves Enterprise, con sede a **Cluj-Napoca**, è un'azienda globale di ingegneria del software con esperienza nei settori della **cybersecurity**, del **fintech** e dei **servizi di outsourcing**. In oltre 9 anni di esperienza ha formato e reclutato i migliori talenti nei settori citati.

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

3. ENERSEC (Romania)

ENERSEC è una **PMI rumena** specializzata in consulenza tecnica e governance per la **sicurezza informatica**, attiva dal **2013**.

4. EDIH Trakia (Bulgaria)

Il consorzio **EDIH Trakia** riunisce **università**, **PMI**, **amministrazioni pubbliche** e **associazioni di categoria** con l'obiettivo di colmare il divario digitale in Bulgaria. È partner della rete Enterprise Europe Network (**EEN**) e del Corridoio europeo di sicurezza informatica.

5. EMAG (Polonia)

EMAG, con oltre **7.000 dipendenti** e **22 istituti di ricerca** situati in **12 città della Polonia**, è partner della rete di ricerca Łukasiewicz, specializzata in informatica applicata, tecnologia dell'informazione e sicurezza informatica. Eccelle nei campi dell'Industria 4.0.

6. Unicis.Tech (Estonia)

Unicis è una start-up che si concentra interamente sulla semplificazione e sulla gestione della privacy e dei rischi. Come? Eliminando le procedure manuali a favore di quelle **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

Pacchetti di lavoro OSCRAT

Il progetto OSCRAT è suddiviso in **cinque** fasi principali (**pacchetti di lavoro**), ciascuna guidata da un partner del consorzio:

1. Gestione del progetto (WP1) – PMF Research

PMF Research (società del **Gruppo JO**) e il centro di sviluppo garantiranno il raggiungimento degli obiettivi del progetto nel rispetto dei **vincoli di budget** e di **scadenza**. In altre parole, gestirà tutte le attività relative alla gestione e al **coordinamento** generale, come le riunioni di progetto, la gestione finanziaria e gli strumenti di comunicazione.

2. Raccolta e analisi dei requisiti (WP2) - EMAG

L'EMAG raccoglierà e analizzerà le esigenze degli stakeholder e delle PMI europee per definire l'ambito, le funzionalità e la conformità dello strumento ai requisiti del **Cyber Resilience Act**.

3. Progettazione e sviluppo del software (WP3) - Oves Enterprise

Sulla base dei risultati del WP2, **Oves Enterprise** svilupperà il software: **facile da usare** e in linea con gli standard **CRA** e le esigenze delle **PMI**.

4. Coinvolgimento delle parti interessate (WP4) - EDIH Trakia

EDIH Trakia organizzerà **workshop**, **webinar** e un **evento internazionale** per migliorare lo strumento con feedback e casi d'uso reali.

5. Divulgazione e valorizzazione (WP5) – PMF Research

PMF Research svilupperà una strategia **di marketing e di comunicazione digitale** per garantire la visibilità del progetto, sensibilizzare l'opinione pubblica sui temi del CRA e incoraggiare l'adozione dello strumento anche dopo la fine di OSCRAT.

Questa **tabella di marcia** garantirà uno sviluppo partecipativo, orientato alle esigenze delle PMI europee e allineato agli obiettivi politici dell'UE nel campo della **sicurezza informatica**.

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

Vuoi ricevere aggiornamenti sul progetto OSCRAT?

La sicurezza informatica non è più un'opzione e OSCRAT è un'iniziativa unica per **rafforzare la resilienza informatica delle PMI europee**

Se volete saperne di più su OSCRAT o cercate partner per progetti simili, contattateci:

- ✓ **Telefono**: 0957225331
- ✓ **e-mail**: projects@jogroup.eu
- ✓ **Sito web**: oscrat.eu

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