

Comunicato stampa

MEDINA implementa una certificazione continua ai fornitori di servizi cloud. Una certificazione ad alta affidabilità e basata su evidenze digitali

Milano, Italy, 8 April 2022

Nonostante gli evidenti benefici del cloud computing, la sua adozione è ancora limitata, in parte a causa della mancanza di sicurezza e trasparenza percepita dagli utenti europei. I fornitori di servizi cloud (CSP) di solito si affidano alle certificazioni di sicurezza come mezzo per migliorare la trasparenza e l'affidabilità, tuttavia i CSP europei devono ancora affrontare molteplici sfide per certificare i loro servizi (ad esempio, la frammentazione del mercato della certificazione e la mancanza di un riconoscimento reciproco).

In questo contesto, il nuovo EU Cybersecurity Act (EU CSA) propone di migliorare la fiducia dei clienti nel mercato europeo dell'ICT, attraverso uno schema Europeo di certificazione di sicurezza informatica per i servizi cloud (EUCS). Questo schema di certificazione porta ad affrontare nuove sfide tecnologiche, a causa della presenza di 'livelli di garanzia' che devono essere soddisfatti al fine di portare tutti i benefici attesi dell'EU CSA ai fornitori di servizi cloud dell'UE e ai clienti.

MEDINA è una 'Research and Innovation Action' finanziata dal programma europeo H2020, con l'obiettivo di creare un sistema sicuro per ottenere una certificazione continua, basata su audit, per i CSP. Il sistema si basa sullo schema di certificazione di sicurezza informatica dell'UE per i servizi cloud. A questo scopo, MEDINA affronterà sfide in aree come validazione/test di sicurezza, i linguaggi di certificazione interpretabili da un calcolatore, prestazioni di sicurezza del cloud e fornitura/gestione delle prove di audit.

- Guida all'implementazione dei controlli EUCS, comprese le misure da applicare e le prove da raccogliere, riducendo così il tempo del processo di certificazione;
- Supporto per le verifiche automatiche di conformità dei controlli nei principali schemi di certificazione della sicurezza del cloud, riducendo l'impegno umano, i costi e i rischi per ottenere e mantenere una certificazione;
- Snellimento per la raccolta e valutazione delle evidenze digitali;
- Assicurazione di un audit trail delle evidenze, per garantire che nessuno le abbia manomesse durante il periodo di validità della certificazione.

Il consorzio MEDINA, guidato da TECNALIA, consiste in un insieme ben equilibrato di partner accademici e industriali, che svolgono ruoli chiave nell'ecosistema della certificazione della sicurezza cloud dell'UE. Il consorzio comprende centri di ricerca ([TECNALIA](#), [Consiglio Nazionale delle Ricerche](#), [Fraunhofer](#)), fornitori di cloud ([Bosch](#), [Fabasoft](#)), fornitori di tecnologia ([Hewlett Packard Enterprise](#), [XLAB](#)) e auditing ([Nixu](#)).

La metodologia di MEDINA sarà valutata in **due casi d'uso reali che coprono i tre modelli di servizio cloud (IaaS, PaaS e SaaS).** Da un lato, Bosch implementerà uno scenario per la **certificazione europea di backend multi-cloud per soluzioni IoT**, e dall'altro, Fabasoft convaliderà **un audit continuo di soluzioni SaaS per il settore pubblico.**

MEDINA aumenterà anche la consapevolezza sui benefici del progetto nel contesto del Cybersecurity Act, portando avanti attività di training e di standardizzazione (ad esempio, ENISA EUCS).

In sintesi, MEDINA contribuisce alla politica europea di certificazione della sicurezza del cloud, migliora l'affidabilità dei servizi cloud grazie alla conformità con gli schemi di certificazione di sicurezza, collabora con le parti interessate, e aiuta l'Europa a prepararsi per le sfide di sicurezza del cloud di domani.

MEDINA ha completato la metà del percorso (la durata complessiva è pari a 36 mesi) e sta progredendo rapidamente verso il raggiungimento delle prossime tappe. Finora, il lavoro si è concentrato sulla definizione dell'architettura generale di MEDINA, delle sue componenti e della loro integrazione. Il tutto sarà convalidato dai casi d'uso di Bosch e Fabasoft. Tra gli strumenti sviluppati possiamo evidenziare il servizio di gestione del rischio e il catalogo dei requisiti e delle metriche di sicurezza, entrambi essenziali per un monitoraggio continuo (e automatico), come richiesto da EUCS e da altri schemi di certificazione.

Breaking news and info available at <https://medina-project.eu>