

# Press Release



## PIACERE: A DevSecOps framework for secure IaC Development and Operation.

Milano, Italy, April 2022

PIACERE è un progetto di ricerca H2020 finanziato dalla Commissione Europea in un periodo di tre anni. L'obiettivo principale di PIACERE è la programmazione di infrastrutture affidabili mediante *Infrastructure-as-Code* (IaC) in un framework sicuro.

**Il consorzio PIACERE, guidato da TECNALIA, riunisce un insieme equilibrato di partner accademici e industriali, che svolgono ruoli chiave nell'ecosistema SecDevOps dell'UE: ERICSSON, PRODEVELOP, POLIMI, HPE, XLAB, GOV.SI, 7BULLS.COM e TECNALIA** provengono da quattro diversi paesi, che rappresentano l'Europa settentrionale e meridionale. A TECNALIA è affidata la guida del consorzio.

**PIACERE mira ad aumentare la produttività dei team DevOps nello sviluppo e nel funzionamento di IaC attraverso il provisioning di un framework DevSecOps integrato. I team DevOps possono programmare IaC come se stessero programmando qualsiasi applicazione software.**

PIACERE supporterà le diverse attività DevSecOps attraverso un unico ambiente **integrato per lo sviluppo (IDE)** di codice infrastrutturale che unificherà l'automazione delle principali attività DevSecOps e ridurrà la curva di apprendimento per i nuovi team DevSecOps. PIACERE consentirà ai team DevSecOps di modellare diversi ambienti infrastrutturali, per mezzo di astrazioni, attraverso un nuovo **DevOps Modeling Language (DOML)**, nascondendo così le specificità e gli aspetti tecnici delle soluzioni attuali e aumentando la produttività di questi team. Inoltre, PIACERE fornirà anche un generatore di **codice infrastrutturale estensibile (ICG)**, che traduce DOML in file sorgente per diversi strumenti IaC esistenti, per ridurre il tempo necessario per la creazione di codice infrastrutturale per applicazioni complesse. I **meccanismi di estensibilità previsti (DOML-E)** garantiranno la sostenibilità e la longevità dell'approccio PIACERE e della suite di strumenti (nuovi linguaggi e protocolli che possono apparire nel prossimo futuro).

Un'altra innovazione chiave di PIACERE è un toolkit completo per la verifica e l'affidabilità. In primo luogo, uno **strumento di verifica (VT)**, che applicherà l'analisi statica sia al modello astratto che al relativo codice infrastrutturale, per eseguire controlli di coerenza e altre verifiche di qualità secondo le migliori pratiche identificate. In secondo luogo, un IaC Code Security Inspector che offrirà una forma di **Static Analysis Security Testing (SAST)** controllando il codice IaC rispetto ai problemi noti di sicurezza informatica (configurazioni errate, uso di librerie non sicure, modelli di configurazione non sicuri). In terzo luogo, un Component Security Inspector che, analizzando anche il codice IaC, segnala le potenziali vulnerabilità e propone potenziali fix. Quarto, un ambiente *"Canary"* che consentirà di testare in modo unitario il comportamento del codice infrastrutturale in un ambiente isolato, consentendo la simulazione delle condizioni per l'ambiente di produzione e identificando alcuni degli anti-pattern più comuni.

Nella parte Ops del ciclo di vita DevSecOps, PIACERE presenta anche diverse innovazioni chiave: La **piattaforma ottimizzata (IOP)** presenterà ai team DevSecOps le configurazioni di distribuzione più appropriate che soddisfano al meglio i vincoli definiti al di fuori del loro catalogo di servizi, risorse ed elementi infrastrutturali mediante algoritmi di ottimizzazione. La piattaforma di esecuzione pianificherà, preparerà e fornirà automaticamente l'infrastruttura e pianificherà, preparerà e installerà gli elementi software corrispondenti necessari per il corretto funzionamento dell'applicazione. A

runtime, PIACERE monitorerà continuamente le metriche associate agli NFR misurabili definiti (es. performance, disponibilità e sicurezza attraverso il monitoraggio della sicurezza in runtime) e sarà in grado di autoapprendere, implementando algoritmi di machine learning e realizzando una strategia di apprendimento incrementale analizzando continuamente le divergenze nei confini delle decisioni e rilevando le anomalie nelle metriche raccolte, conservando solo i dati più aggiornati per evitare il degrado del modello. Ogni volta che questi meccanismi di autoapprendimento rilevano un'anomalia o una potenziale violazione dello SLA, verrà attivato un allarme e verrà avviato un meccanismo di auto-riparazione. Il meccanismo di auto-riparazione comporterà il riavvio di un algoritmo di ottimizzazione per il dominio del problema effettivo e una piattaforma di esecuzione automatica, monitoraggio e così via.

L'approccio e il set di strumenti PIACERE saranno valutati in tre casi d'uso reali. SI-MPA implementerà uno scenario per il **Ministero della Pubblica Amministrazione sloveno**, Prodevelop lo convaliderà nella **gestione delle infrastrutture marittime critiche ed Ericsson** verificherà la soluzione in un **caso d'uso di pubblica sicurezza su IoT in 5G**.

PIACERE realizzerà inoltre i seguenti benefici attesi:

- Rendere la creazione del codice infrastrutturale più accessibile ai team DevSecOps
- Aumentare la qualità, la sicurezza, l'affidabilità e l'evolubilità del codice infrastrutturale
- Garantire la continuità aziendale fornendo meccanismi di auto-riparazione, anticipando i guasti e le violazioni
- Consentire all'IaC di apprendere da sé dalle condizioni precedenti che hanno innescato situazioni impreviste

In questo primo anno di progetto, il lavoro si è concentrato sulla definizione dell'architettura generale di PIACERE, nonché sullo sviluppo della prima versione del framework integrato che sarà validata dagli use case.

**Ultime notizie e informazioni disponibili su:** <https://www.piacere-project.eu/>

Questo progetto ha ricevuto finanziamenti dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea sull'accordo di sovvenzione n. 101000162

#### **Contatto**

Galia Nedeltcheva, POLIMI  
galia.nedeltcheva@polimi.it  
Piazza Leonardo da Vinci, 32  
20133 Milano