Press Release

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

Bilbao, Spain, April 2022

PIACERE is an H2020 research project funded by the European Commission over a period of three years. PIACERE's main objective is Programming trustworthy Infrastructure As Code in a sEcuRE framework.

The PIACERE consortium, led by TECNALIA, assembles a balanced set of academic and industrial partners, which play key roles in the EU SecDevOps ecosystem, ERICSSON, PRODEVELOP, POLIMI, HPE, XLAB, GOV.SI, 7BULLS.COM and TECNALIA, are from four different countries, representing Northern and Southern Europe. TECNALIA has been entrusted with the leadership of the consortium.

PIACERE aims to increase the productivity of DevOps teams in the development and operation of IaC through the provisioning of an integrated DevSecOps framework. DevOps teams can program IaC as if they were programming any software application.

PIACERE will support the different DevSecOps activities through a single **integrated environment to develop (IDE)** infrastructural code that will unify the automation of the main DevSecOps activities and will shorten the learning curve for new DevSecOps teams. PIACERE will allow DevSecOps teams to model different infrastructure environments, by means of abstractions, through a novel **DevOps Modelling Language (DOML)**, thus hiding the specificities and technicalities of the current solutions and increasing the productivity of these teams. Moreover, PIACERE will also provide an extensible **Infrastructural Code Generator (ICG)**, translating DOML into source files for different existing IaC tools, to reduce the time needed for creating infrastructural code for complex applications. The provided **extensibility mechanisms (DOML-E)** shall ensure the sustainability and longevity of the PIACERE approach and tool-suite (new languages and protocols that can appear in the near future).

Another key innovation of PIACERE is a comprehensive toolkit for verification and trustworthiness. Firstly, a **verification tool (VT)**, that will apply static analysis to both the abstract model and the related infrastructural code, to execute consistency checks and other quality verifications according to identified best practices. Secondly, an **IaC Code Security Inspector** that will offer a form of Static Analysis Security Testing (SAST) by checking the IaC code against the known cybersecurity issues (misconfigurations, use of non-secure libraries, non-secure configuration patterns). Thirdly, a **Component Security Inspector** that by analysing also the IaC code, reports the potential vulnerabilities and proposes potential fixes. Fourth, a **Canary environment** that will allow unit testing of the behaviour of the infrastructural code on an isolated environment, which would enable the simulation of conditions for the production environment and identify some of the most common anti-patterns.

In the Ops part of the DevSecOps lifecycle, PIACERE also presents several key innovations: The **Optimized Platform (IOP)** will present the DevSecOps teams with the most appropriate deployment configurations that best meet their defined constraints out of their catalogue of services, resources and infrastructural elements by means of optimization algorithms. The **Execution Platform** will automatically plan, prepare, and provision the infrastructure and plan, prepare, and install the corresponding software elements needed for the application to seamlessly run. At runtime, PIACERE will continuously **monitor the metrics** associated with the

defined measurable NFRs (e.g. performance, availability, and security through the **runtime security monitoring**) and will be able to **self-learn**, implementing machine-learning algorithms, and realizing an incremental learning strategy by continuously analysing divergences in the decision boundaries and detecting anomalies in the metrics being collected while retaining only the most up to date data to avoid model degradation. Whenever these **self-learning** mechanisms detect an anomaly or a potential SLA violation, an alarm will be triggered, and a self-healing mechanism launched. A **self-healing** mechanism will entail to launch again an optimization algorithm for the actual problem domain and an automatic execution platform, monitoring and so on.

PIACERE approach and toolset will be assessed in three **real use cases**. SI-MPA will deploy an scenario for **The Slovenian Ministry of Public Administration**, Prodevelop will validate it in **Critical Maritime infrastructures Management,** and Ericsson will verify the solution in a **Public Safety on IoT in 5G use case.**

PIACERE will also raise the following expected benefits:

- Making the creation of such infrastructural code more accessible to the DevSecOps teams
- Increasing the quality, security, trustworthiness and evolvability of infrastructural code
- Ensuring business continuity by providing self-healing mechanisms anticipation of failures and violations
- Allowing IaC to self-learn from previous conditions that triggered un-expected situations

In this first year of the project, the work has focused on the definition of the general architecture of PIACERE, as well as on the development of the first version of the integrated framework that will be validated by the use cases.

Breaking news and info available at https://www.piacere-project.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731533

Contact

Maitena Ilardia, Dissemination and Communication Manager in PIACERE. TECNALIA
maitena.ilardia@tecnalia.com
Parque Científico y Tecnológico de Bizkaia, C/Geldo, Edificio 700. E-48160 Derio (Bizkaia)
Tel.: 902.760.000 International calls: (+34) 946.430.850