PIACERE

KER Pitch Deck

Joao Costa, Maitena Ilardia Uribeganecoa, Juncal Alonso

Marketing Materials with Exploitation Insight

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101000162.

PIACERE FULL-STACK

UNIQUE VALUE PROPOSITION

Access an integrated DevSecOps framework to develop, verify, release, configure, provision, and monitor infrastructure as code

PIACERE FULL-STACK

SOLUTION BENEFITS

IAC LANGUAGE INDEPENDENCY

Automatic code generation without the need of having to master the languages and protocols demanded by current solutions; supporting flexibility and reproducibility

AIMS FOR DEPLOYMENT EFFICIENCY

Abstraction of execution environments and infrastructural requirements, allowing for an easy extensibility

OVERALL FOCUS ON SECURITY

Verification of the quality of the models and the generated code to detect errors as soon as possible in the process, with the inclusion of security mechanisms to ensure the trustworthiness of such code in various phases of the IaC life cycle

PIACERE FULL-STACK

INNOVATION SCOPE

INNOVATION

Reduce the complexity in deploying complex software through IaC while using powerful security at desing time and runtime, with an AI engine with features s pecific to PIACERE's self-learning and self-healing needs

PROBLEM

Provide an IaC usage framework for modelling application deployment, support for modelling infrastructure applications and refactoring possibilities

SOLUTION

An integrated DevSecOps framework to develop, verify, release, configure, provision, and monitor infrastructure as code, using a single integrated environment to develop (IDE) infrastructural code will unify the automation of the main DevSecOps activities and will shorten the learning curve for new DevSecOps teams

VALUE

PIACERE is strongly focused on the development, verification, emulation, deployment, orchestration and (partial) reconfiguration of the infrastructure as code that supports applications that need to be deployed on heterogeneous resources and environments, each requiring its own language and protocols

PIACERE FULL-STACK

EARLY ADOPTERS

SMART LOGISTICS

Guarantee of security & privacy when using tools/data in virtualized environments, particularly while running component security inspection

PUBLIC ADMINISTRATION

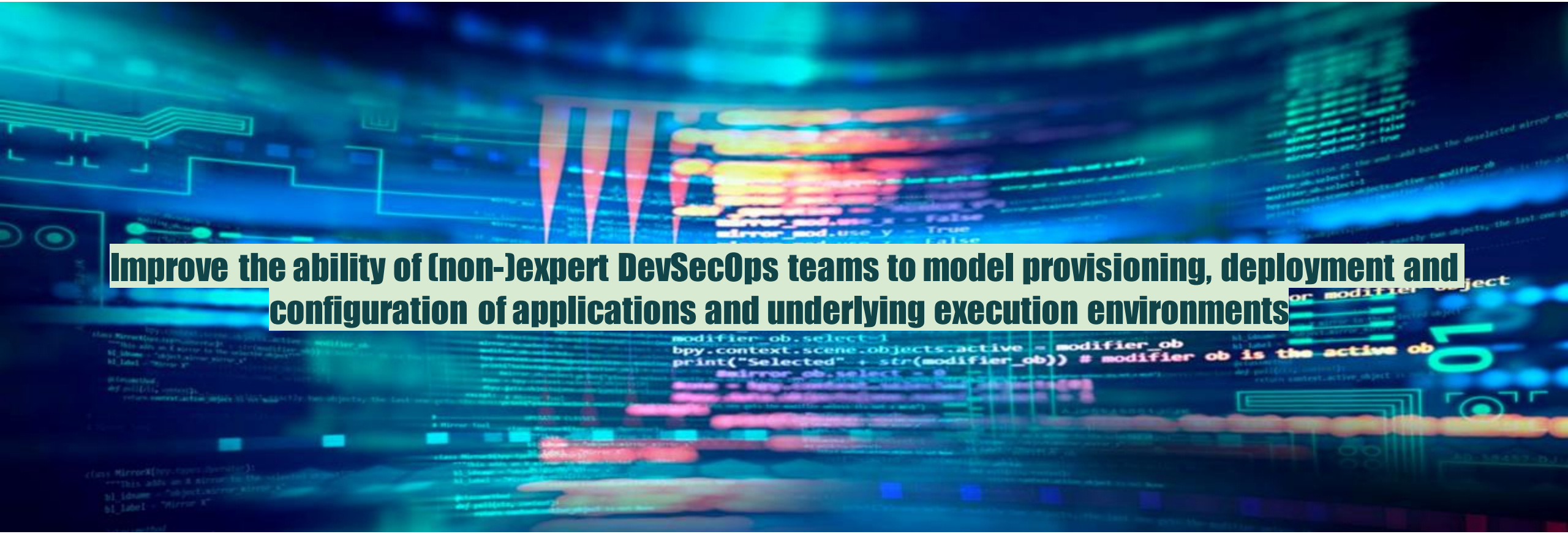
Improved level of information security, with increased number of automated activities, keeping at the same time a higher level of compliance with the security requirements

TELECOMMUNICATIONS

Improve automated security inspection of internal/external components, with an extend security by design approach

DevSecOps Modelling Language

UNIQUE VALUE PROPOSITION



Improve the ability of (non-)expert DevSecOps teams to model provisioning, deployment and configuration of applications and underlying execution environments

DevSecOps Modelling Language

SOLUTION BENEFITS

UNIFIED DEPLOYMENT CONFIGURATION

DOML covers all aspects of deployment configuration, from infrastructure deployment to software setup, while the other technologies require the use of multiple languages to achieve the same goals.

LOC REDUCTION

Based on our experiments, DOML is more compact compared to other notations such as Terraform, Ansible and TOSCA

INTERNAL CONSISTENCY AND REQUIREMENTS CHECKING

A DOML model can be checked for internal consistency including the analysis it it fulfils specific user-defined requirements

DevSecOps Modelling Language

INNOVATION SCOPE

INNOVATION

Reduce the complexity in deploying complex software through IaC

PROBLEM

Improve the ability of (non-)expert DevSecOps teams to model provisioning, deployment and configuration needs in complex contexts by providing a set of abstractions of execution environments and composing them into machine-readable representations

SOLUTION

DOML as the end-user language enabling the modelling of deployment and configuration of complex software and infrastructure in a way that can then be transformed by ICG in executable IaC

VALUE

DOML allows DevSecOps teams to select and combine the abstractions with the purpose of creating a correct infrastructure provisioning, configuration management, deployment and self-healing model.

DevSecOps Modelling Language

EARLY ADOPTERS

SMART LOGISTICS

Be able to deploy the same application and related software layers on different infrastructures with limited additional effort

PUBLIC ADMINISTRATION

Configure a complex private cloud infrastructure, deliver services on top of it and enable an agile way of delivering information systems (IS), and use an IaC approach generally with all new IS deployments

TELECOMMUNICATIONS

Automate the configuration of complex networks and support the deployment of a container-based distributed system, being able to take into account non-functional requirements.

Design Time Security

UNIQUE VALUE PROPOSITION

Regain trust in IaC through the DOML verification and the automation of IaC code quality checking for errors and vulnerable dependencies, and thus improving IaC integrity and applicability

Design Time Security

SOLUTION BENEFITS

FASTER MALFUNCTIONING DETECTION

Decrease the time needed to detect IaC malfunctioning or changes in the working conditions of the generated IaC at execution time

DECREASED RESPONSE TIME

Decrease the median time until the relevant stakeholder is notified of infrastructural malfunctions

MINIMIZATION OF DATA LOSS

Level segmentation so to provide the most security to the user, by minimizing data loss and security breaches

Design Time Security

INNOVATION SCOPE

INNOVATION

Security analyser for IaC and application code (when available), using SAST tools, and security analyser and ranker of components (libraries, middleware)

PROBLEM

Lack of tailored solution for checking the integrity and applicability of IaC code to be deployed on an infrastructure provided by the verification tools, leading to a very limited trust in the automated deployment systems

SOLUTION

This tool can check the IaC code for errors and report back to the user with a set of error reports and also recommendations where inefficiencies are in his code

VALUE

Enable users to optimize and reduce the number of errors in their deployment procedure, decreasing the time needed to detect IaC malfunctioning or changes in the working conditions of the generated IaC at execution time

Design Time Security

EARLY ADOPTERS

SMART LOGISTICS

Guarantee of security & privacy when using tools/data in virtualized environments, particularly while running component security inspection

PUBLIC ADMINISTRATION

Improved level of information security, with increased number of automated activities, keeping at the same time a higher level of compliance with the security requirements

TELECOMMUNICATIONS

Improve automated security inspection of internal/external components, with an extend security by design approach

KER 3: IaC Execution Manager

SOLUTION BENEFITS

EFFICIENT PROVIDER-SPECIFIC IaC WRITEUP

Decrease the time needed to create an IaC, to describe infrastructure using provider-specific IaC, and to translate IaC between providers, regarding multiple environment deployments and multiple cloud providers

BETTER DEPLOYMENT AGILITY

Increase deployment agility in terms of unexpected complications, efficiency, and predictability, while decreasing the time for self-healing re-configuration and partial re-deployments of Infrastructural code

WORKFLOW AUTOMATION

Reduce overhead through workflow automation, and the cost of deploying IT solutions on various infrastructure platforms

IaC Execution Manager

UNIQUE VALUE PROPOSITION

Avoid vendor lock-in and time consuming manual processes in infrastructure management, while increasing resilience and supporting self-healing

IaC Execution Manager

INNOVATION SCOPE

INNOVATION

Based on already existing open source technologies in the field of IaC. It streamlines the application life cycle, and with a common interface for the deployment of software components

PROBLEM

Develop and maintain infrastructure as code for heterogeneous infrastructures and different phases (configure, provision, deploy, orchestrate), supporting multilingualism with one tool

SOLUTION

Platform to automatically plan, prepare, and provision the infrastructure and plan, prepare, and install the software elements needed for the application to seamlessly run

VALUE

Automatic, parametrizable, and therefore faster and easier execution, orchestration and deployment of IaC code on heterogeneous vendor providers, with no need to utilize different languages for the different providers, and it facilitates the exploitation of the project with independence to the provider

IaC Execution Manager

EARLY ADOPTERS

SMART LOGISTICS

Flexible, hybrid deployment of applications by seamless mixing of on-device and cloud services and SW, ensuring reproducible timing performance from a user perspective

PUBLIC ADMINISTRATION

Reduced time consuming activities, allowing to increase the quality, efficiency, performance of the deployed IaC code

TELECOMMUNICATIONS

IaC modelling/ deployment/ configuration in multi-CSP environment, allowing to improve the capacity to validate at a very early stage the correctness of the platform and infrastructure deployment

IaC Optimized Platform

UNIQUE VALUE PROPOSITION

Perform the most appropriate deployment configurations that best meet your defined constraints out of DevSecOps catalogue of services, resources and infrastructural elements by means of optimization algorithms.

IaC Optimized Platform

SOLUTION BENEFITS

COST, PERFORMANCE AND AVAILABILITY OPTIMIZATION

The user can easily find combination of infrastructure elements that optimize objectives such as cost, performance or availability

TAKES IN CONSIDERATION USER REQUIREMENTS

The technology contemplates some requirements useful for the user, such as a maximum cost, a minimum availability, the elements to optimize or the region of the elements chosen

FLEXIBILITY TO ADDITIONAL OBJECTIVES & REQUESTS

The tool is flexible enough to contemplate additional objectives and requirements, using two evolutionary algorithms for conducting the optimization: NSGA-II and NSGA-III, but it is flexible enough to easily use other methods, such as SMPSO or MO-Cell

KER 4: IaC Optimized Platform

EARLY ADOPTERS

SMART LOGISTICS

Ensure a platform optimized for the specific environment, with reduction of infrastructure migration time and better adjust the cost of infrastructures

PUBLIC ADMINISTRATION

Optimized repeatability of the deployment configuration of the IaC with our infrastructural elements, with reduced management overhead

TELECOMMUNICATIONS

Adopting automated tools allows to speed up the Infrastructure deployment for applications running in distributed environment independent from adopted IaC framework.

IaC Optimized Platform

INNOVATION SCOPE

INNOVATION

The solutions are provided to the user in a ranked way, in order him/her can choose that one that fits better user needs

PROBLEM

The main problem is to develop a tool flexible enough to be able to meet the different heterogeneous needs of the users. Each user has his/her own needs, and the IOP should provide solutions adapted to these needs

SOLUTION

Optimize deployments based on his/her needs. The IOP is flexible enough to allow the user to define which objectives should be optimized (such as the cost and the performance), and which are the main requirements that should be met (such as a minimum availability or the use of the resources of a certain provider)

VALUE

The IOP is an optimization tool which is capable of model and solve single-objective, multi-objective and many-objective optimization problems depending on the user need. Also, the user is able to introduce non-functional requirements, requiring to the algorithm to build the optimization search space accordingly

Canary Sandbox

UNIQUE VALUE PROPOSITION

PIACERE

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

Canary Sandbox

SOLUTION BENEFITS

EASE OF PREPARATION AND DEPLOYMENT OF ENVIRONMENT

The user is no longer concerned with preparing and deploying testing environments by themselves

CUSTOMISATION OF TESTING ENVIRONMENTS

The user can customise the testing environment to their needs so that it matches their needs and capabilities, avoiding cloud-related costs when testing cloud-focused IaC

EARLY IDENTIFICATION OF ISSUES ON IAC

The user can catch issues with IaC execution earlier than usually, well before IaC reaches the production environment

Canary Sandbox

INNOVATION SCOPE

INNOVATION

Currently, the only option is to deploy directly to the cloud, without any ability and verification that it is a similar environment to the production one

PROBLEM

Currently there is no out of the box solution to make a test deployment, with real infrastructure deployment, but in the sandbox (controlled) environment

SOLUTION

Canary Environment provides a controlled environment based on Open Stack which allows deploying a real application in a controlled way to make all of the tests (functional, security, performance, etc) in this environment before deploying to production

VALUE

Canary Environment allows making controlled deployment and tests before deployment to the production environment, which will minimize the negative impact on production in case of bugs or misconfiguration.

Canary Sandbox

EARLY ADOPTERS

SMART LOGISTICS

Ensure a safe environment for risk-free testing that best fits real-world conditions, with improvements in the testing phase of the infrastructure by testing it under real conditions

PUBLIC ADMINISTRATION

Isolated environment for execution, testing and simulating the conditions of the production environment, with stable and consistent environment for faster iterations

TELECOMMUNICATIONS

Facilitate the transition from the DevOps to the DevSecOps approach

Runtime Security Monitoring

UNIQUE VALUE PROPOSITION

Ensure that the conditions of the QoS are met at all times and that a failure or non-compliance of NFRs is not likely to occur, with verified security violations at runtime

Runtime Security Monitoring

SOLUTION BENEFITS

DEPLOY SECURITY AGENTS AUTOMATICALLY

Automatically deploy security monitoring agents, integrated into the monitoring mechanisms at runtime

COMPREHENSIVE KNOWLEDGE ON THREATS

Notify about security threats according to the policies, defined in the NFRs

DYNAMIC SECURITY MONITORING

Tackle unexpected situations that may affect the correct performance of IaC and its underlying environment (i.e. infrastructure failures, deterioration in the response time, etc.)

Runtime Security Monitoring

INNOVATION SCOPE

INNOVATION

Using a powerful trust and incident management, adapted to new functionalities, and an AI engine with features specific to PIACERE's self-learning and self-healing needs

PROBLEM

Need for monitoring stack for the run-time conditions so that the self- learning and self-healing mechanisms can be fed

SOLUTION

Monitoring system capable of detecting security-related events and incidents in the deployed application's environment. It is (to the extent possible) deployable automatically and notifies users about security alerts

VALUE

This monitoring system allows to create informative metrics/variables with significant discriminative power

Runtime Security Monitoring

EARLY ADOPTERS

SMART LOGISTICS

Ensure security and compliance with non-functional requirements defined with customers, achieving greater customer satisfaction by ensuring QoS.

PUBLIC ADMINISTRATION

Continuous runtime verification for any security violation, recognizing violations of defined security policies and eliminate threats

TELECOMMUNICATIONS

Improve security at runtime while supporting different multiple infrastructure, reducing time and costs.

PIACERE

www.piacere-project.eu // Contact: juncal.alonso@tecnalia.com