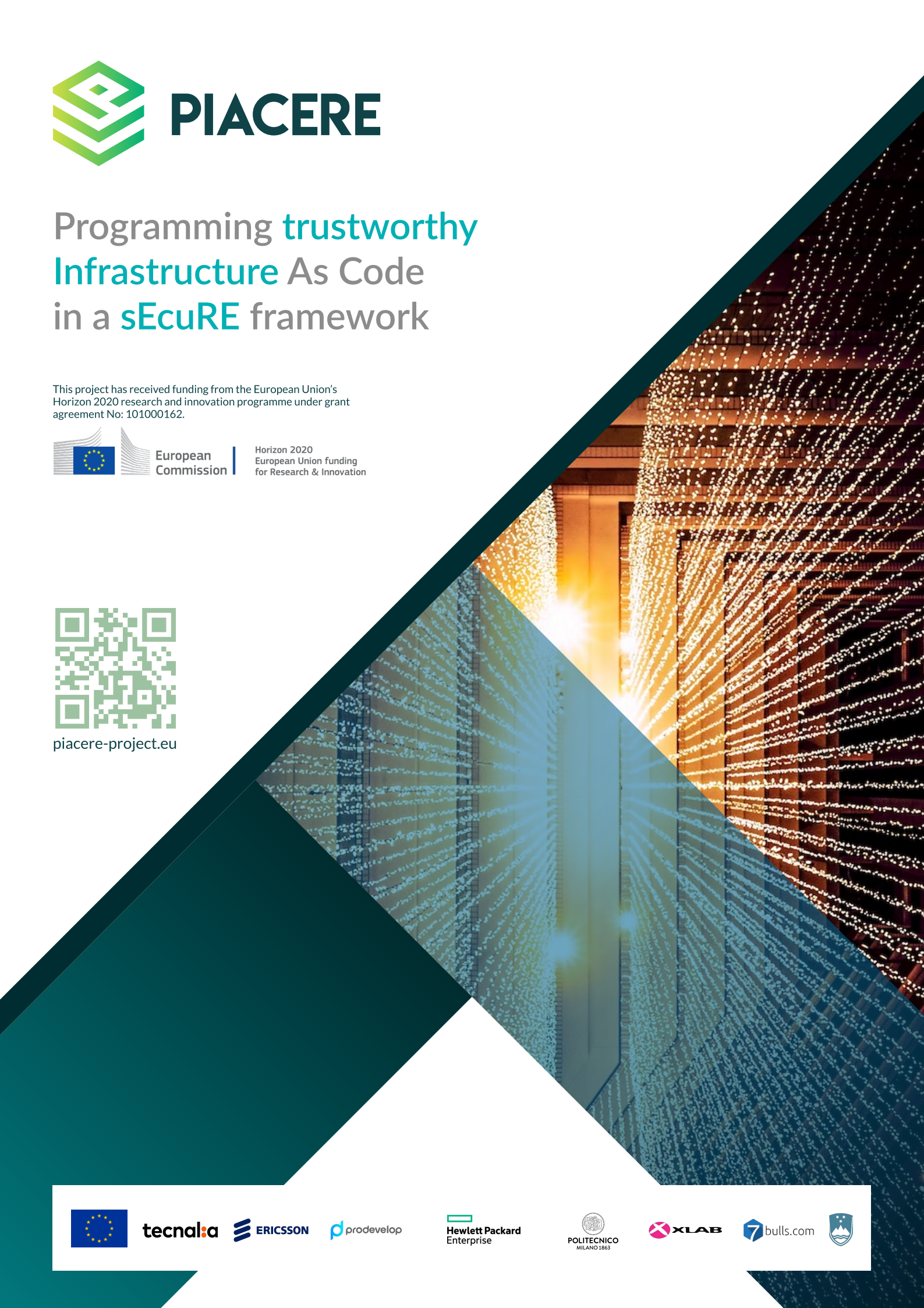
PIACERE

Programming trustworthy Infrastructure As Code in a sEcuRE framework

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

European Commission | Horizon 2020 European Union funding for Research & Innovation

piacere-project.eu



tecnalia ERICSSON prodevelop Hewlett Packard Enterprise POLITECNICO MILANO 1863 XLAB 7bulls.com

PIACERE aims to increase the productivity of DevOps teams in IaC development and operation through the provisioning of an integrated DevSecOps framework.

DevOps teams can program IaC as if they were programming any software application.



Plan and create **infrastructure as code**

Verify the trustworthiness **of Infrastructure as Code**

Package release and configure **Infrastructure as Code**

Monitor plan and self-heal runtime **of Infrastructure as Code**

PIACERE VISION

The **Horizon 2020 PIACERE** project aims to provide means (tools, methods and techniques) to enable most organizations to fully embrace the Infrastructure as Code approach, through the DevSecOps philosophy, by making the creation of such infrastructural code more accessible to designers, developers and operators (DevSecOps teams), increasing the **quality, security, trustworthiness and evolvability of infrastructural code** while ensuring its business continuity by providing self-healing mechanisms, anticipation of failures and violations, allowing the system to self-learn from the conditions that triggered such re-adaptations.

ENGAGE IaC MANAGEMENT WITH PIACERE

IaC code, as any software, can be versioned and can be written by a collaborating team bringing together multiple expertise. In general, any innovative code management applied in traditional software development is applicable in IaC DevSecOps cycle: security by design, automation, testing, reusability, auditability etc. With PIACERE, **DevSecOps team will be able to work with infrastructural code as they do with traditional application code,** starting from the definition of requirements for the infrastructure – such requirements are expressed in terms of technical capabilities the application level should offer – to the design, implementation, verification, deployment, testing, operation and monitoring of such infrastructural code.

PIACERE

Programming trustworthy Infrastructure As Code
in a sEcuRE framework

PIACERE DEVSECOPS APPROACH FOR IaC

DevSecOps teams

Application architects

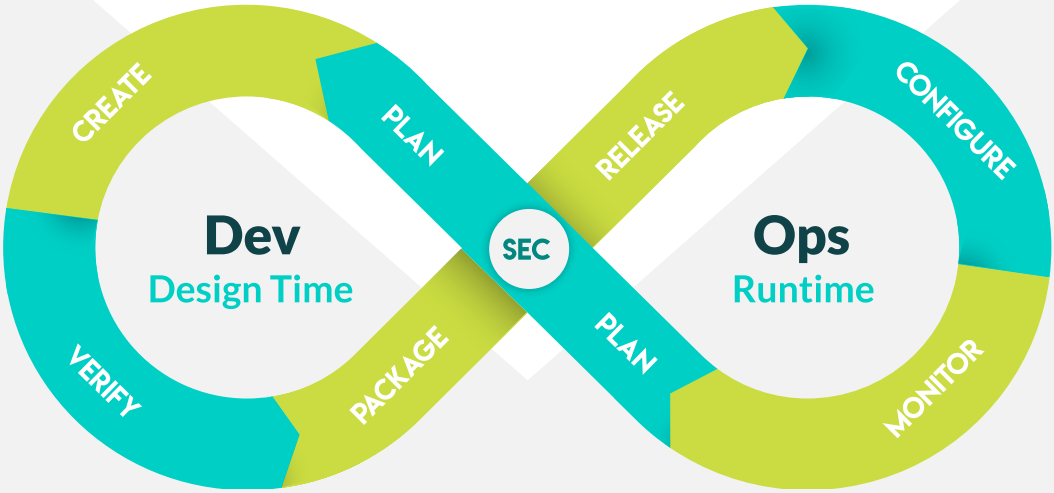
1 Plan, create and package IaC

2 Verify the trustworthiness of IaC

Platform architects

3 Release and configure IaC

4 Monitor, plan and self-heal IaC



BENEFITS

1. Easing the IaC development – from the idea to the living application.
2. Increasing the quality, security, trustworthiness and evolvability of IaC.
3. Ensuring future-proof application life-cycle management by providing self-healing mechanisms to deal with known failures and violations.
4. Allowing the system to self-learn from previous conditions that triggered un-expected situations.

PIACERE

Programming trustworthy Infrastructure As Code
in a sEcuRE framework

FIRST SUCCESS STORIES

SI-MPA

The Slovenian Ministry of Public Administration for hosting information systems on a centralized infrastructure

"With the PIACERE approach and toolset implementation we are moving from traditional to agile way of delivering information systems."

Stjepan Pervan

PRODEVELOP

Critical Maritime Infrastructures for fulfilling the management needs of port authorities



"Automate the creation and configuration of the deployments following IaC approach, making deployments independent of the chosen infrastructure."

Ismael Torres Boigues

ERICSSON

Public Safety on IoT in 5G of both human and IoT devices



"IaC modelling/deployment/configuration in multi-CSP environment, while improving automated security inspection of internal/external components."

Cosimo Zotti

CONTACT INFORMATION

Project Coordinator:
Juncal Alonso Ibarra
Juncal.Alonso@tecnalia.com
+34 664 101 514

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