PIACERE – DevSecOps Automated

Radosław Piliszek
IT Solutions Architect
7bulls.com

2022-07-08
OWASP New Zealand Day 2022

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

PIACERE

Agenda

- DevSecOps – what, why?
- PIACERE – introduction
- PIACERE – architecture overview
- PIACERE deep dive into the bits

PIACERE

DevSecOps – formally

DevSecOps is **the integration of security into emerging agile IT and DevOps development as seamlessly and as transparently as possible**. Ideally, this is done without reducing the agility or speed of developers or requiring them to leave their development toolchain environment.

Source: Gartner IT Glossary: https://www.gartner.com/en/information-technology/glossary/devsecops

PIACERE

DevSecOps – in simple words

DevSecOps is **not forgetting about security when doing DevOps**, ideally without slowing oneself down.

Source: me, myself and I

PIACERE

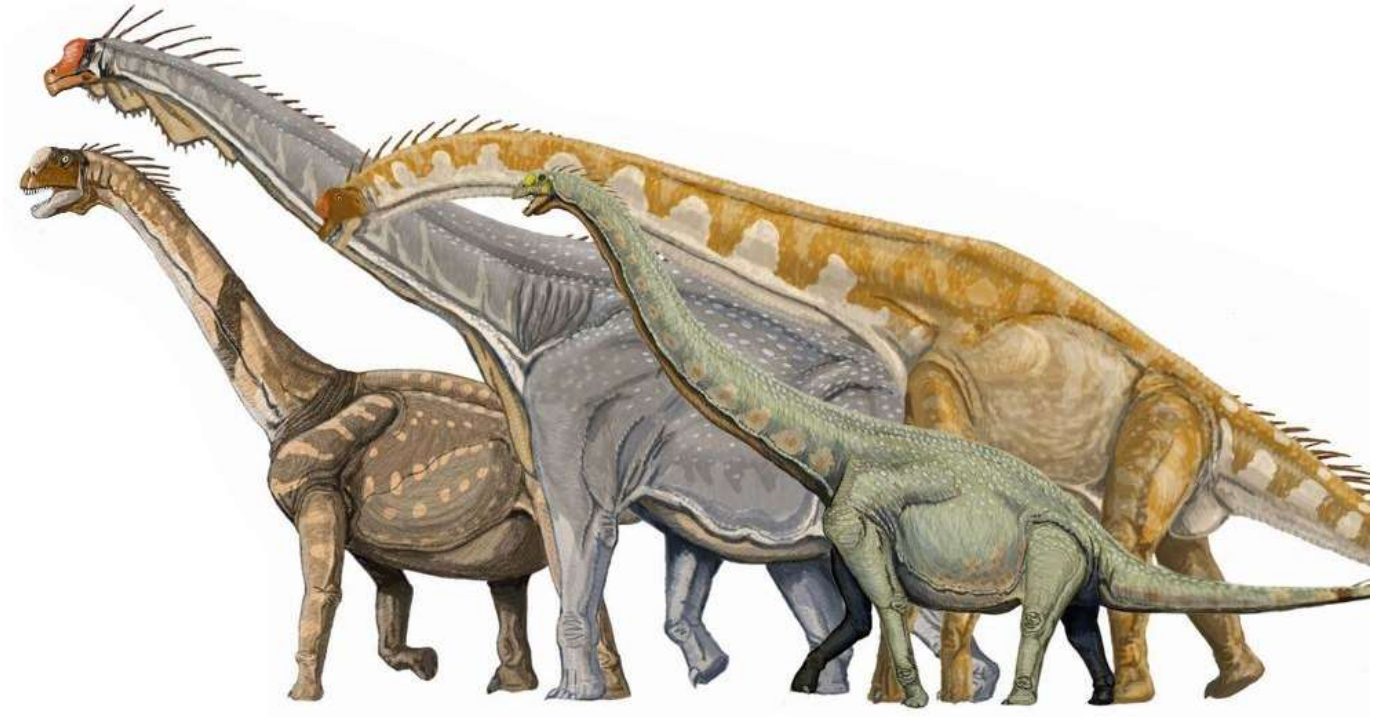
But why DevSecOps?

To consider:

- what was „back then”?
- what happened?

PIACERE

„Back then”



Source:
https://en.wikipedia.org/wiki/File:Macronaria_scrubbed_enh.jpg

PIACERE

„Back then” – silos

Source:
https://upload.wikimedia.org/wikipedia/commons/f/fb/Ralls_Texas_Grain_Silos_2010.jpg

PIACERE

Fast forward – what happened? DevOps happened!

- Silos no more! ~> „No boundaries” as well.
- Developers empowered. They are the controllers of the situation now.
- But who controls the controllers?

Pls can i haz secukitty back?

- Yeas…
- … but at a cost…
  - Abundance of tools
    - And tools for tools
      - And their too… have their config ;-)
  - Tools learning curve
  - Heterogeneity ripple effects
    - Anyone said multicloud? Hybrid cloud?
  - All in all, lack of standardisation ☹

Source: https://commons.wikimedia.org/wiki/File:Tulipflower1.JPG

PIACERE

What do we mean by DevOps?

- Culture (mindset)
- Tooling

PIACERE

Back to basics, aka jailed by the CIA

- `C` – Confidentiality
- `I` – Integrity
- `A` – **Availability**

Introducing PIACERE (PLEASURE)

Programming trustworthy Infrastructure As Code in a sEcuRE framework

PIACERE

- Horizon 2020 project in Software Development call.
- Consortium consists of 12 organizations (academia, business, government).
- Schedule – 01.12.2020 - 30.11.2023
- We (as in: my company) are responsible for integration and Canary Sandbox Environment.

PIACERE

PIACERE – goals

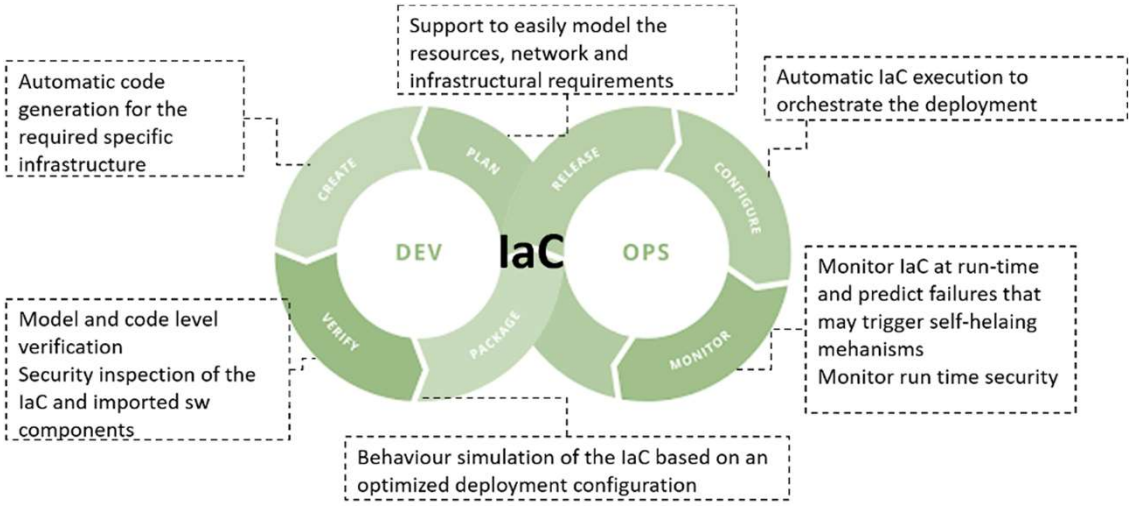
- Infrastructure as Code (IaC) only – avoid snowflakes and related config drifts.
- Deploy infrastructure for applications.
- Manage cloud, hybrid and multi-cloud deployments.
- Optimise usage of resources.
- Enable dynamic testing of IaC.
- Keep the infrastructure churning happily ☺

PIACERE

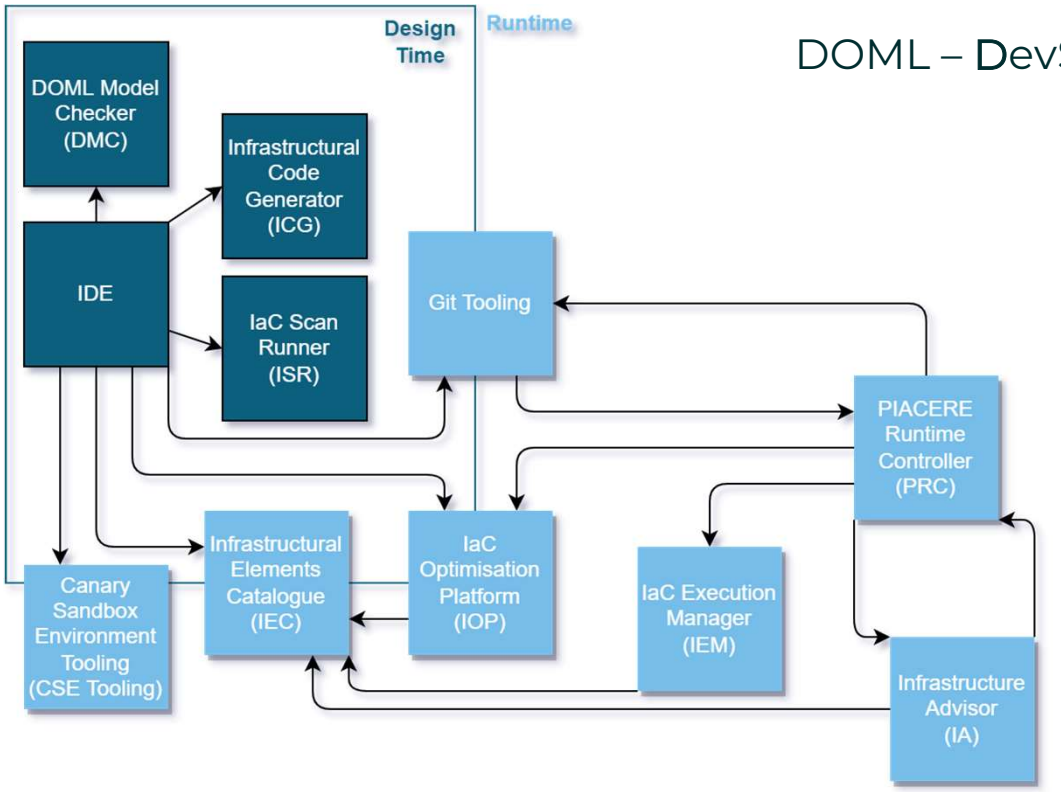
PIACERE – key features

- **GitOps**, single source of truth, access control and accountability.
- **Integrated security principles and tooling** into the DevOps operations.
- **Sandboxing guide** to test the dynamic properties of to-be-deployed infrastructure.
- **Cloud-agnostic, multi-cloud-capable**.
- Automatic **healing and optimisation**.
- Reusing and enhancing Open Source.

PIACERE continuum



PIACERE – architecture



DOML – DevSecOps Modelling Language

PIACERE

DOML

DOML – **D**evSec**O**ps **M**odelling **L**anguage

- **Cloud-agnostic-able.**
- **Multiple layers** of modelling.
- **Application modelling**: components, connections, security, etc.
- **Infrastructure modelling**: abstract (environment-agnostic) and concrete (environment-dependent).
- Target IaC generation possible to multiple languages thanks to the ICG.
- Modelling toolbox available in Eclipse IDE.

DOML Model Checker & IaC Scan Runner

- **Static analysis** of properties of DOML and the generated IaC.
- Verifies **correctness** according to select criteria.
- Ensures the IaC and used components are **free of known vulnerabilities** and follow **best security practices**.

PIACERE

PIACERE Runtime Controller

- **One ~~ring~~ source** to rule them all (deployments).
- **Single-flow** operations: push to the repository and get your deployment updated.
- **Single source of truth** – everything your infrastructure needs in one place.
- Simplified and **streamlined access control** – control access via repository permissions.
- Based on BPMN (Business Process Model and Notation) – an **extensible** vernacular.
- Feedback loop with the Infrastructure Advisor, control loop with the Git tooling.

Infrastructure Advisor

- Collects and analyses **metrics and events** related to **performance** (Telegraf-based) and **security** (Wazuh-based).
- Infrastructure-side deployed during IEM run.
- **Self-learning and self-healing** included.
- Metrics and events are saved into the Infrastructural Elements Catalogue.

IaC Optimisation Platform & Infrastructural Elements Catalogue

- **Optimisation of the infrastructure** based on collected metrics.
- Optimises the trade-off of **cost, performance and availability**.
- Machine-learning-based optimization algorithms.

PIACERE

IaC Execution Manager

- **Executes IaC** against chosen Canary Sandbox or Production Environment.
- **Understands** the deployed infrastructure.
- Supports **redeployment** (including scaling).
- **Secure** use of credentials to the target environments.

PIACERE

Canary Sandbox Environment tooling

- Two main tools:
  - **Provisioner** – deployment of selected environments (OpenStack, Kubernetes) in an opinionated way.
  - **Mocklord** – mocked APIs of selected cloud providers.
- Ability to test dynamic aspects of the deployment in a **controlled, sandbox environment**.
- Avoids the steep learning curve of BYOI deployments and costs of public cloud providers.

Thank you very much!
Stay in touch with us

www.piacere-project.eu

Get more info from our social media