GitOps: l’approccio open source integrato per la resilienza, automazione e sicurezza dei workload
Business objectives
The Tree of Taste company

- Reduce the Time to Market
- Support the business dynamically and proactively during peak seasons
- Security as an essential element to win customers’ trust and protect the brand

Journey to modernization - 1st phase
- Legacy Application Modernization
- Break down the Monolith
- Converge to PaaS and Cloud Services models

Journey to modernization - 2nd phase
- Integrated approach to application and infrastructural resilience through the use of multi-cluster solutions
- Focus on application automation to speed up release process
- Focus on a pervasive security model from application development, release and deployment process
Adopting a Cloud Native Approach

Top Objectives

- **Speed**: Increase developer productivity and ship quality applications faster
- **Security**: Application and supply chain security from start to production
- **Scale**: Automate and scale application delivery on hybrid cloud infrastructure

DevOps
DevSecOps
GitOps
Continuous Integration (CI) & Continuous Delivery (CD)

A key DevOps principle for automation, consistency and reliability

DevOps is the key to meet the insatiable demand for delivering quality applications rapidly
Kubernetes is the standard for application innovation...

...and Kubernetes-native security is increasingly critical

- Microservices architecture
- Declarative definition
- Immutable infrastructure

- Secure supply chain
- Secure infrastructure
- Secure workloads

**Zero trust** is an approach to designing security architectures based on the premise that every interaction begins in an untrusted state.
GitOps Workflow
a declarative approach to application delivery

What you want (desired state)
What you have (current state)

Scope: Automate a Continuous Delivery chain
Adoption of DevSecOps and GitOps practices

OpenShift Pipelines

Kubernetes-native on-demand delivery drive all the pipeline

Build → Test → Security Checks → Release → Deploy Stage → Deploy Prod

Shift Left

OpenShift Build
Automate building container images using Kubernetes tools

Red Hat Advanced Cluster Security for Kubernetes

OpenShift GitOps
Declarative GitOps for multi-cluster continuous delivery

Ecosystem Integrations
GitHub, GitLab, Azure DevOps, Travis CI
The first cluster is the **Cluster Hub** and contains all the tools and capabilities to drive the pipeline in a DevSecOps approach.

The other **two managed clusters** were already deployed on Cloud and represent development and stage environments.
Hands-on Environment
Technical Preview Features

Pipelines as Code and Tekton Chains

- Task `git-clone`
- Task `build-container`
- Task `sign-image`

Container Registry
Hands-on
Pipeline as code
Recap and Benefits

- E2E automation in supply chain from development, to build and to deploy
- DevOps and Security teams can use a common language and source of truth
- Diversify infrastructure in order to reduce costs, avoid vendor lock-in and increase agility
- Adherence to corporate compliance through centralized governance over distributed environments
- Control and reduce the risk of drift between the desired and current state of infrastructures and / or applications