雲原生架構下的安全應用部署並實現安全左移

DevSecOps & CICD Integration

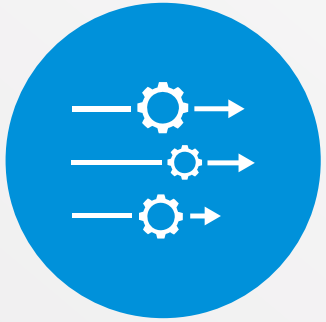
Brandon Chen
Consulting Architect / PSO Taiwan

2022-10-19

Tanzu Application Platform

企業級雲原生應用服務架構的 CI/CD 平台

開發者能很快速藉由平台快速部署與測試

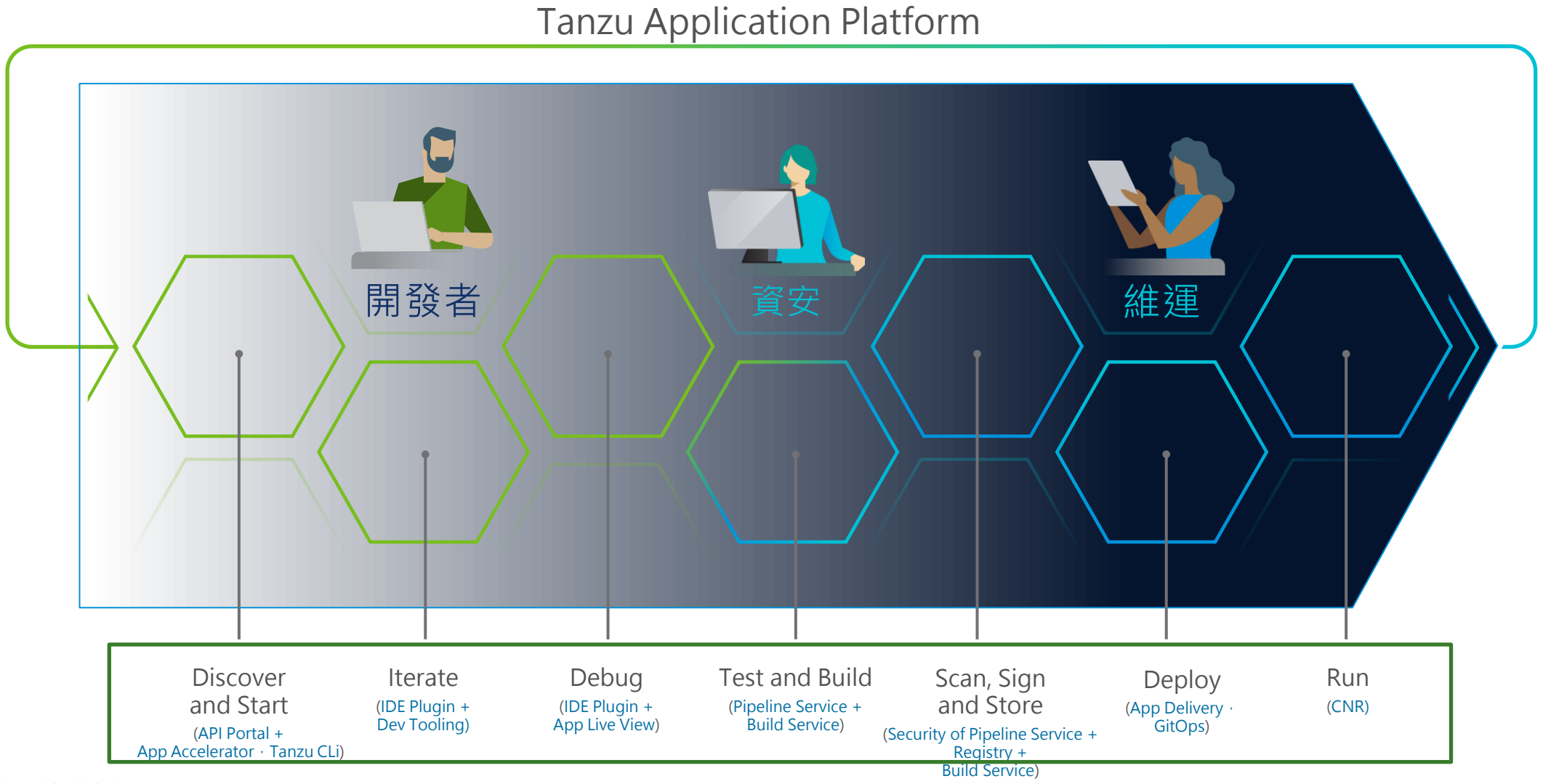


透過Supply Chain機制快速達成上線之路

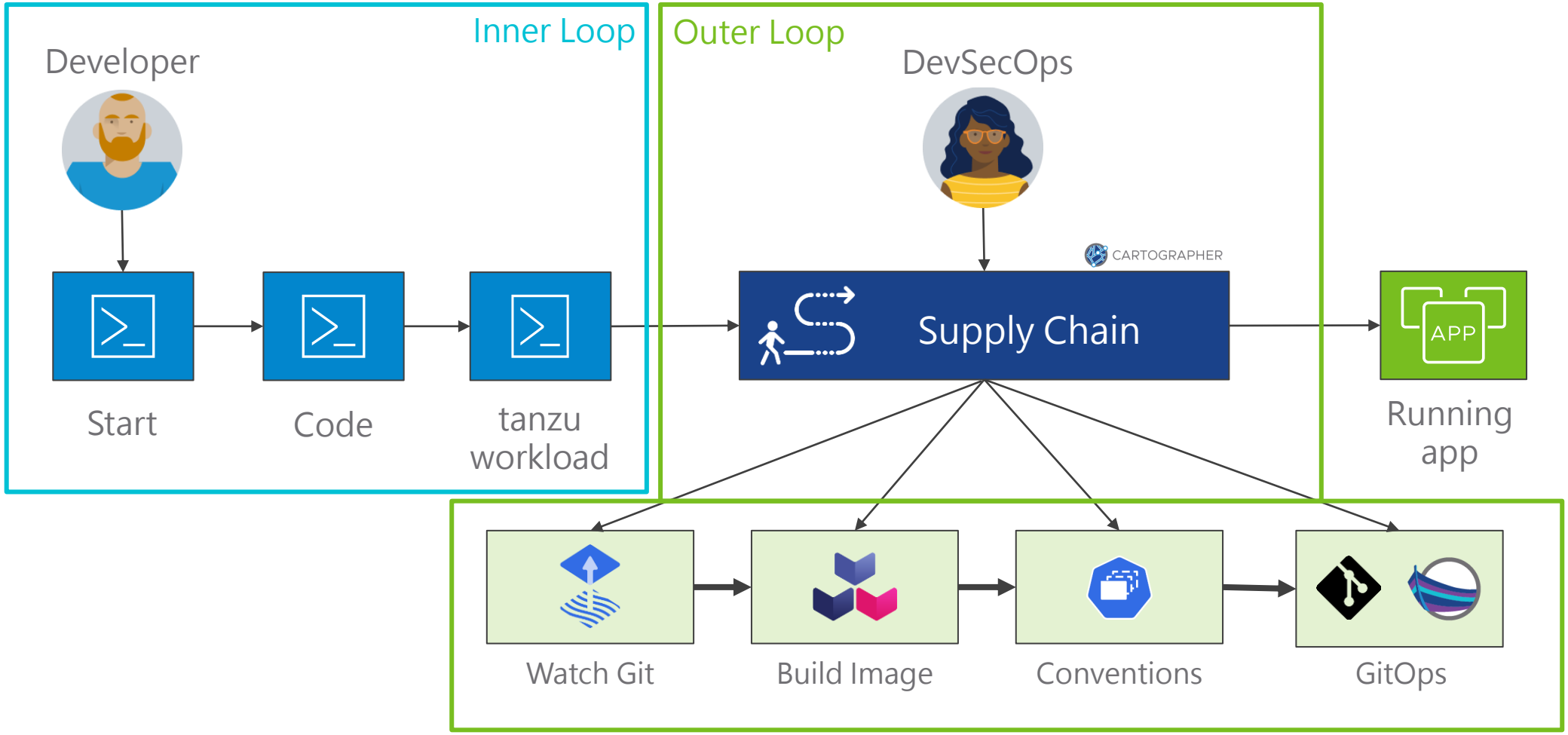
明確定義開發人員和操作人員的角色，團隊可以協同整合工作

平順的端到端DevSecOps 體驗

具有可重複的path to production，安全且彈性伸縮，可以在 Any Kubernetes上運行



透過Supply Chain機制快速達成上線之路



應用場景

開發

應用打包成鏡像也要我來寫？好吧，那寫Dockerfile要注意哪些地方？聽說有不少要留意的坑....., 還有用到的基礎鏡像如果有更新了，誰來負責更新到我們環境啊？

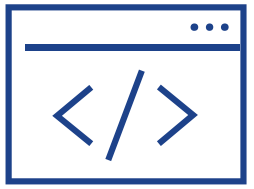
不用寫Dockerfile了，直接部署程式碼和應用，我們的**鏡像構建服務**會自動生成鏡像，無論是你的程式碼有更新，還是基礎鏡像有更新，都會自動觸發構建出新的鏡像，並保存到鏡像倉庫

架構師

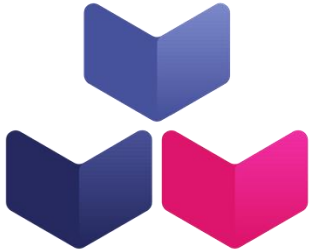
Cloud Native Buildpacks

code to image

Source Code



Cloud Native Buildpacks



OCI Compliant Containers

Java

node JS

GO

.NET Core

php

Open Source Buildpacks + Build Platform

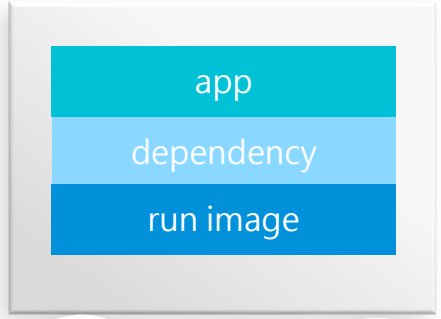
paketo buildpacks

vmware kpack

Enterprise Ready Buildpacks + Build Platform

VMware Tanzu Buildpacks

VMware Tanzu Build Service



Kubernetes

Public Clouds

應用場景

開發

我猜那麼多 K8s yaml 文件大概也要我來寫吧..... K8s還是太複雜了，我會用，但學藝不精，我怕用我寫的上生產環境會有問題.....

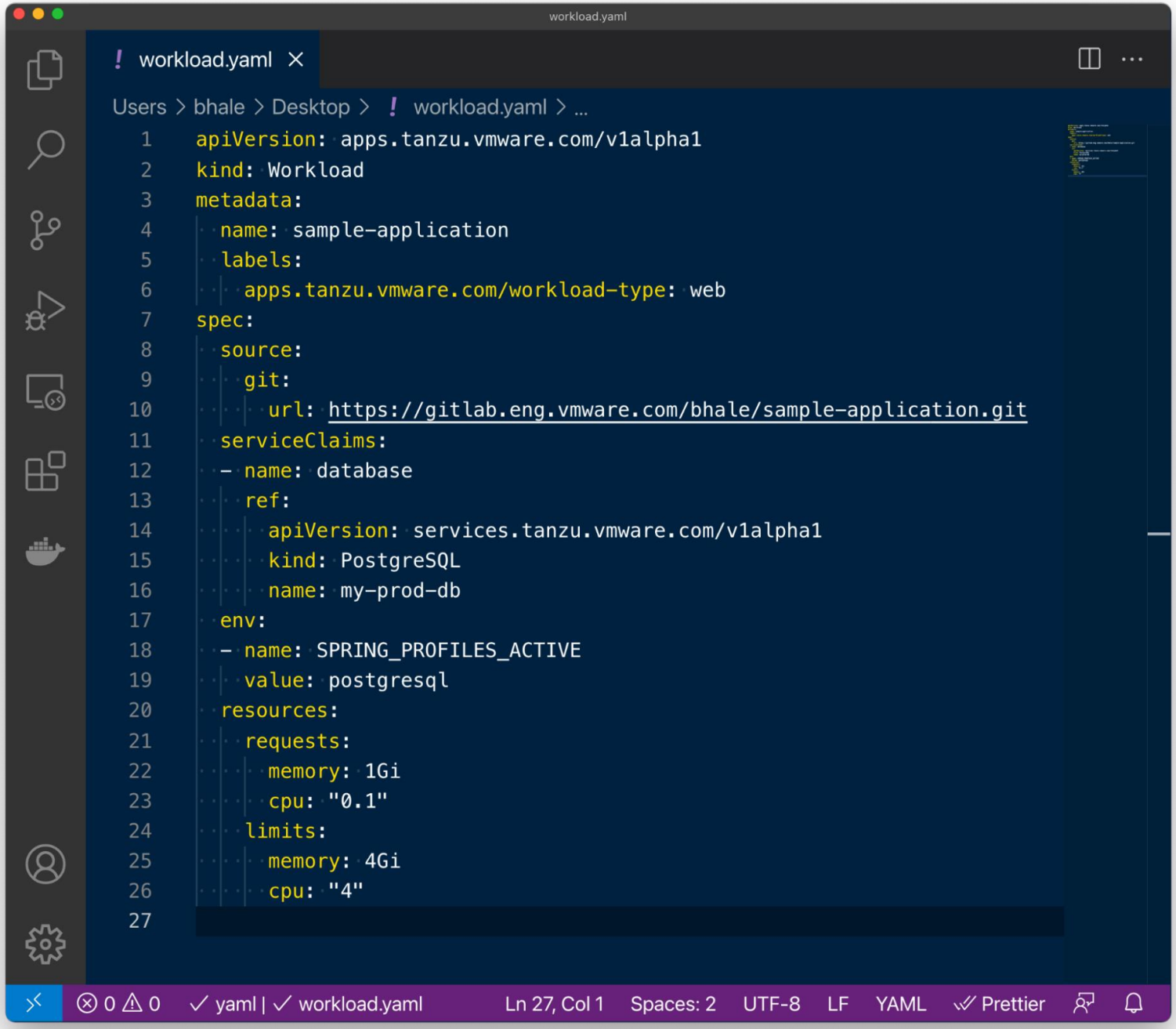
不用自己寫那麼多K8s yaml啦！只要寫一個**workload yaml** 就行了，這個是更簡單的應用抽象，只要聲明式的配置應用，最關鍵是指定應用所屬的類型

架構師

應用抽象：Workload

Workload manifest：

- 名稱
- 類型
- 標籤與註釋
- 程式碼位置
- 相依的服務
- 環境變數
- 參數
- 資源需求



應用場景

開發

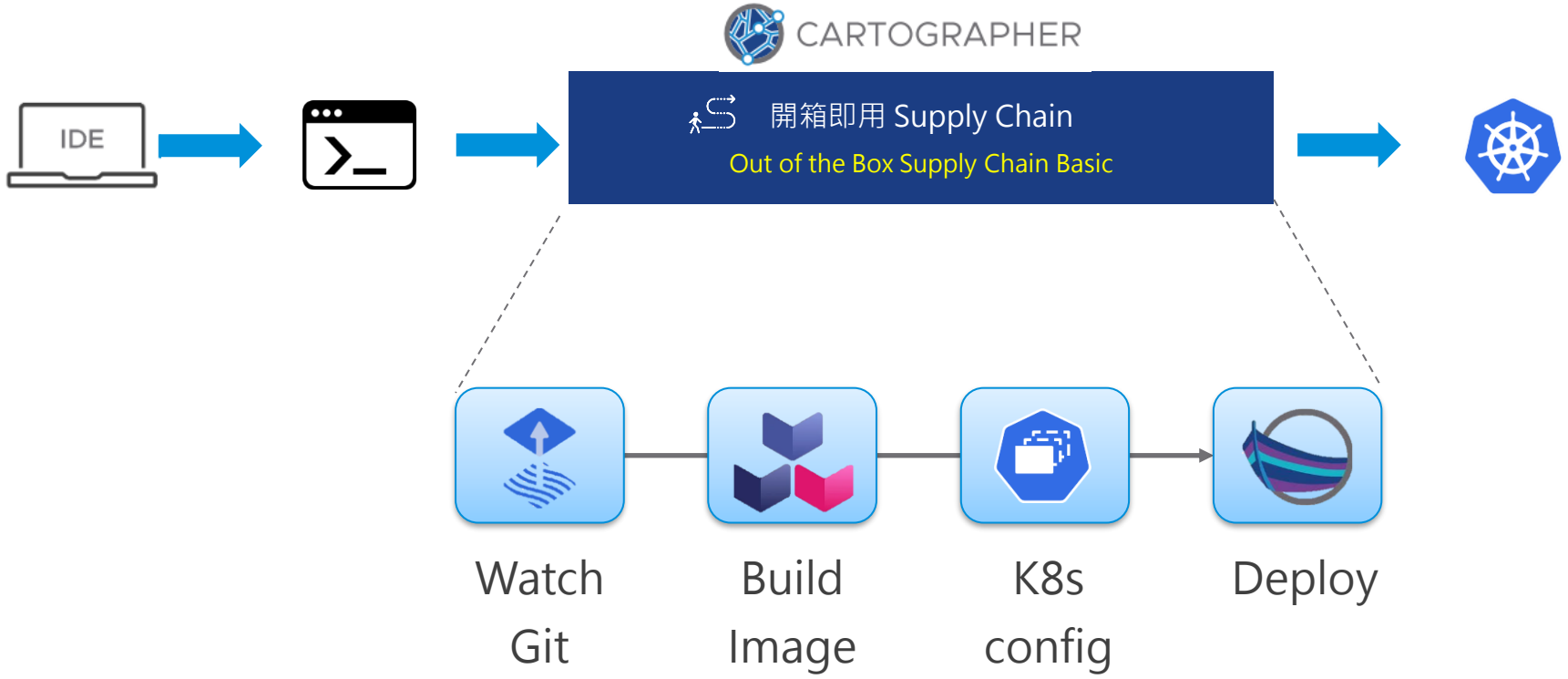
總算今天的任務開發的差不多了，不是提倡每日提交嗎？那提交後是一鍵部署嗎？執行的CI/CD pipeline 誰設定啊？有沒有現成的可以用？要是客製化的話找誰幫忙？大概要等多久？

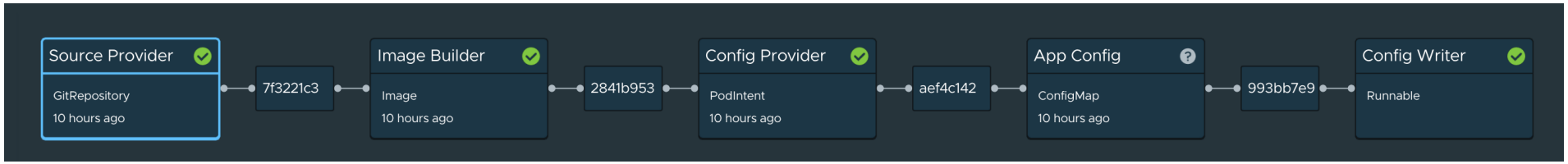
只要你指定的應用類型是平台支持的，就不需要配了，會自動適配平台預置的 **pipeline**，自動部署；當然了，如果是新的應用類型，那就要找平台團隊進行流水線客製化了，也不是太複雜和費時的

架構師

開箱即用的軟件供應鏈

Out of the Box Supply Chain Basic





應用場景

開發

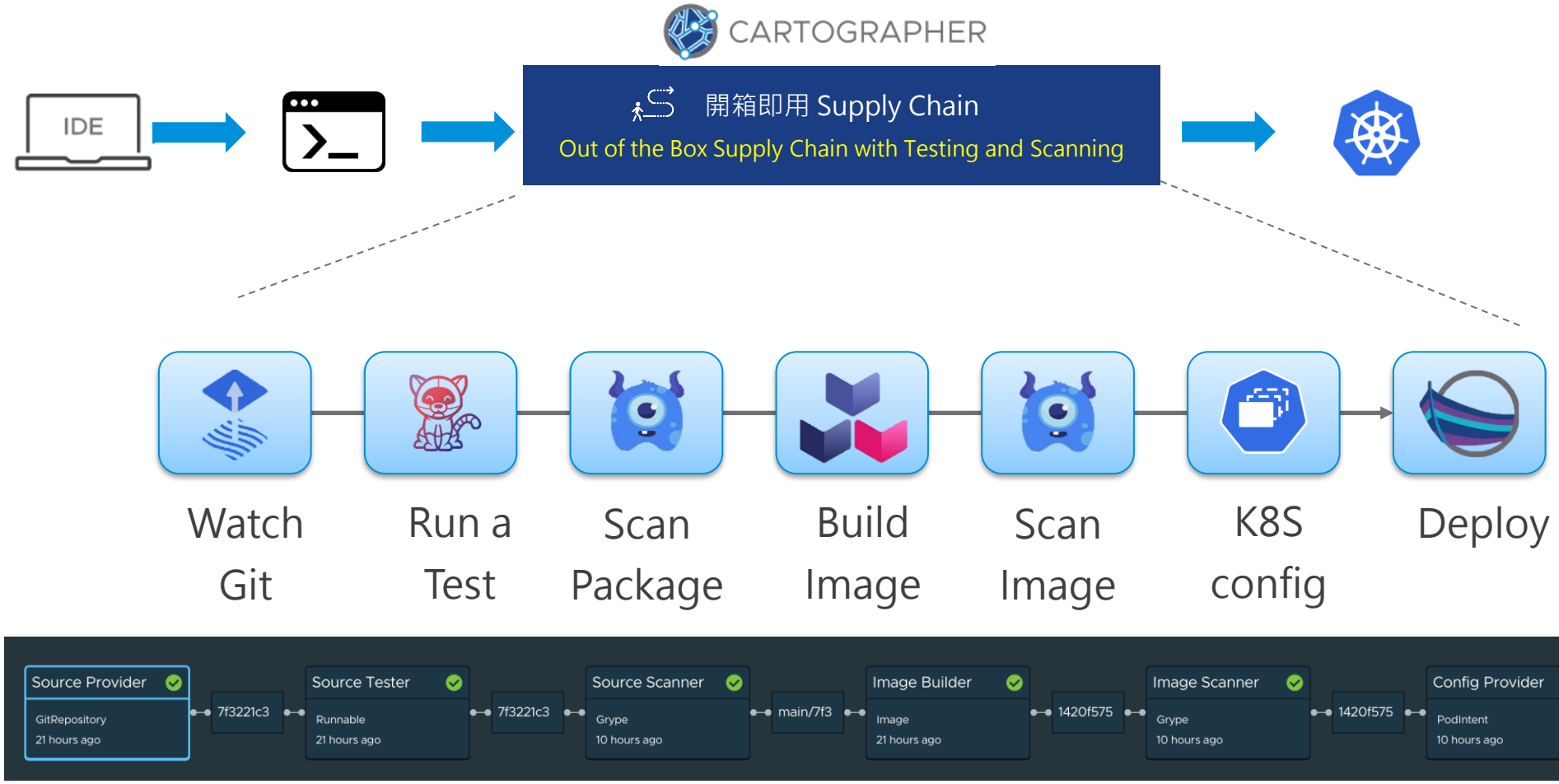
快要上線了，才說要做安全review，結果剛收到安全掃描結果，發現有一堆問題要改，怎麼也沒法按計劃上線了！

平台已經提供了**安全的供應鏈**，程式碼提交就開始進行程式碼掃描，以及後續的鏡像掃描，鏡像簽名，別忘了聲明安全策略，確保只有可信簽名和沒有高等級漏洞的鏡像才能部署到生產環境哦！

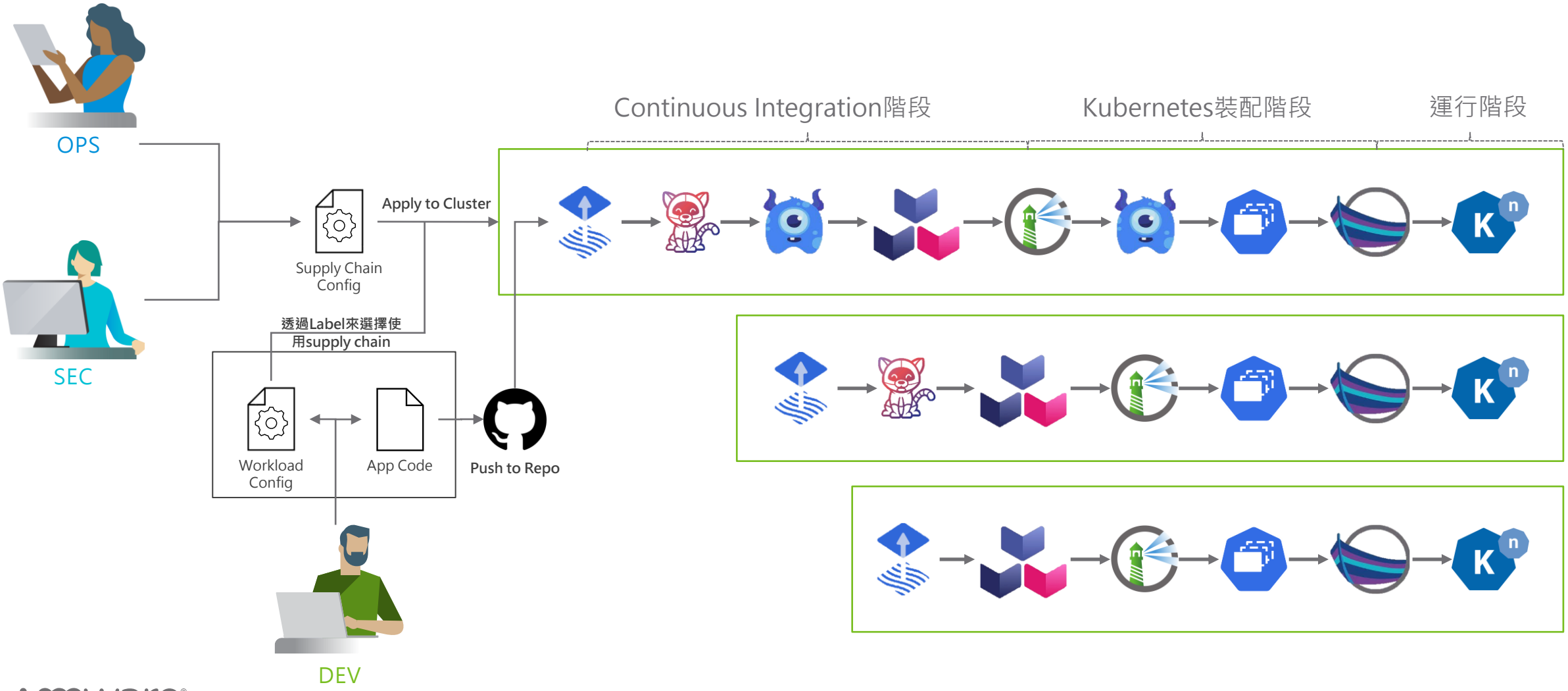
架構師

擁有安全機制的軟件供應鏈

Out of the Box Supply Chain with Testing and Scanning



隨選所需 - 多樣性開箱即用 Supply Chain



参考資料

VMware Tanzu Application Platform

https://docs.vmware.com/en/VMware-Tanzu-Application-Platform/1.2/tap/GUID-release-notes.html

Running Tanzu Application Platform Locally on Your Laptop

https://tanzu.vmware.com/developer/guides/tanzu-application-platform-local-devloper-install/

Thank You