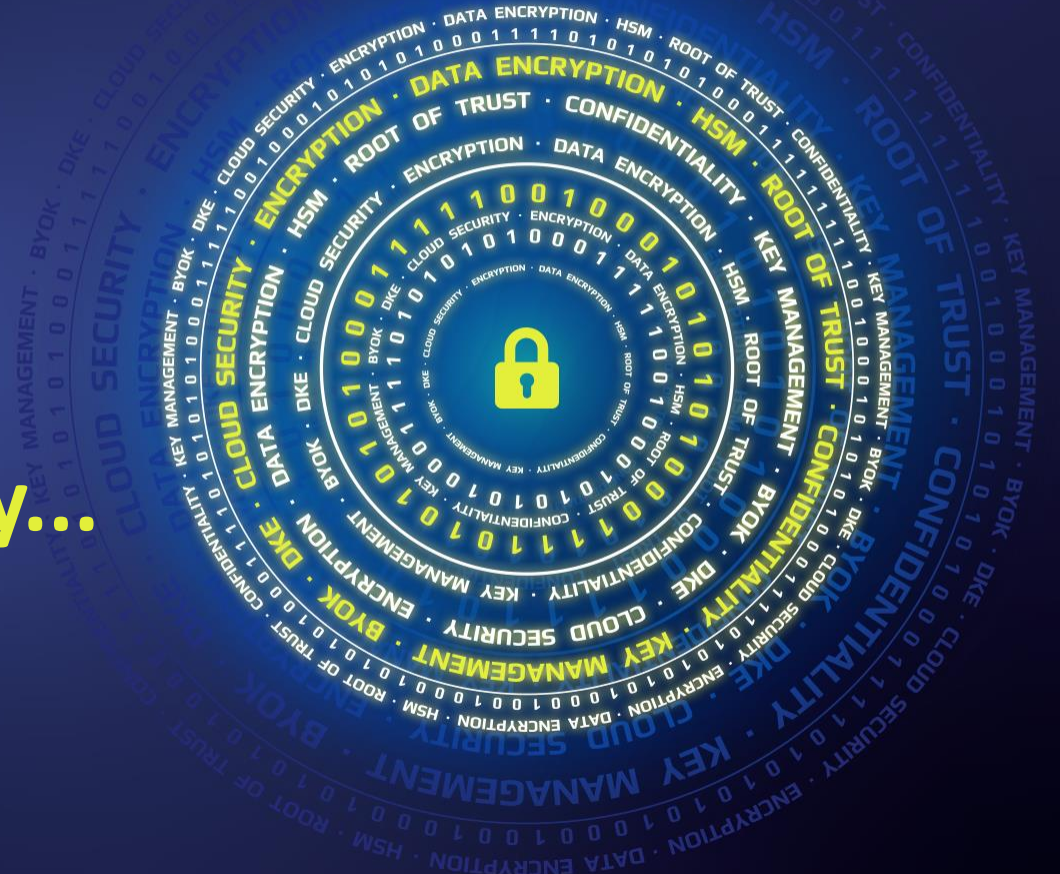
CryptoPanel

edycja #19

za chwilę zaczynamy...

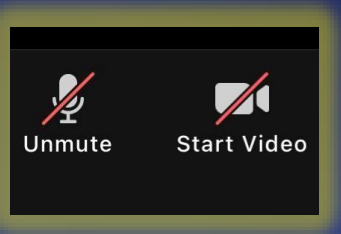


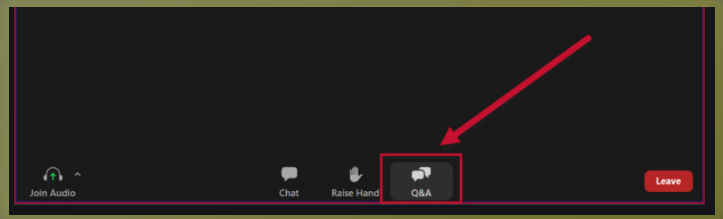
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #19

Konteneryzacja zmieniła podejście do wytwarzania i utrzymania aplikacji. Czy i jak można chronić dane poprzez szyfrowanie w środowisku Kubernetes i OpenShift?

CryptoPanel

TEST WIEDZY #19

Konteneryzacja zmieniła podejście do wytwarzania i utrzymania aplikacji. Czy i jak można chronić dane poprzez szyfrowanie w środowisku Kubernetes i OpenShift?

CryptoPanel

dziś dyskutują

Łukasz Urbański

Security Specialist
Lukasz.Urbanski@clico.pl
mob. +48 665 449 919

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

problem

co nas boli...

- Nasza firma dział na rynku finansowym.
- Posiadamy zaawansowaną aplikację do obsługi naszych klientów (AOK).
- W ramach rozwoju (m.in. oferowanie nowych usług i produktów) tworzymy platformę usługi mobilnych (PUM) współpracującą z aplikacją obsługi klientów.
- Nowy system będzie m.in. przetwarzał dane osobowe i zasilał nimi AOK.
- System będzie początkowo zlokalizowany w naszym centrum przetwarzania danych (faza projektowania i uruchamiania) a docelowo wdrażany produkcyjnie w zasobach jednego wybranego dostawcy chmurowego.
- PUM chcemy zrealizować z wykorzystaniem podejścia DevSecOps do tworzenia aplikacji z zachowaniem ochrony informacji wrażliwych

- ...chcemy rozszerzyć nasz system o możliwość pracy z urządzeniami mobilnymi,
- ...modyfikacja, rozszerzenie funkcjonalności AOK aby spełniał rolę PUM wymaga zbyt dużych nakładów pracy,
- ...ponadto, rozwój systemu w obecnej architekturze powoduje zbyt daleko idące kompromisy związane m.in. z brakiem wymaganej (RODO) ochrony przetwarzanych informacji,
- ...nie posiadamy wiedzy jak podejść do tematu bezpieczeństwa danych jeśli zastosujemy scenariusz wdrożenia PUM z wykorzystaniem środowiska chmurowego (CSP)
- …dodatkowe funkcje wspierające pracę zespołu DevSecOps będą zaletą

CryptoPanel

rozwiązanie

Kontenery

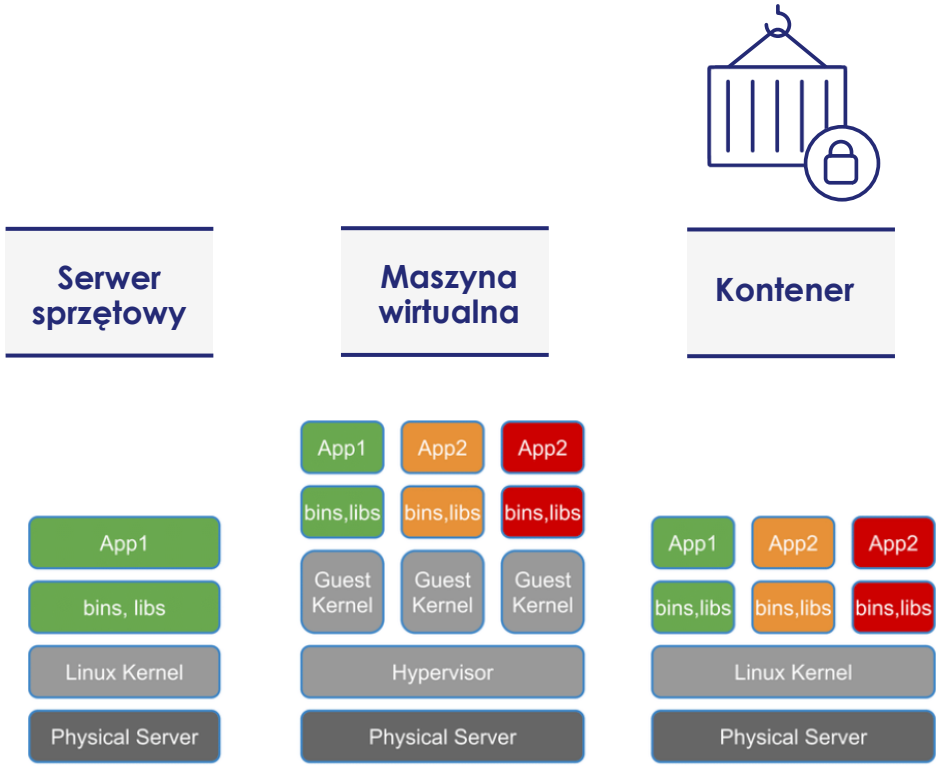
Kubernetes

OpenShift

Kontenery

Zalety korzystania z technologii konteneryzacji

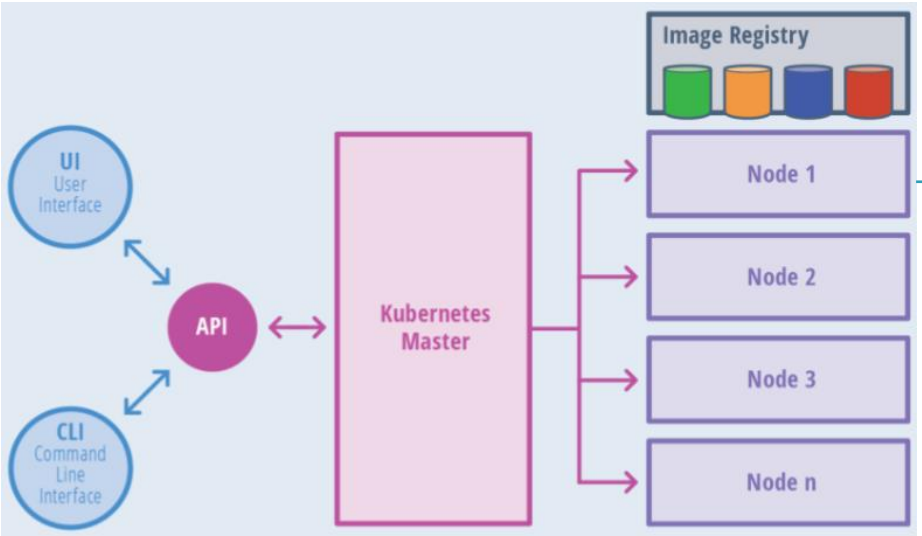
- Kontenery są izolowane od siebie
- Aplikacje mają wszystko, czego potrzebują
- Kontenery są znacznie bardziej elastyczne niż maszyny wirtualne
- Zwiększają elastyczność i skracają czas wprowadzenie rozwiązania na rynek (TTM)
- Zapewniają „lepszy" rozwój aplikacji

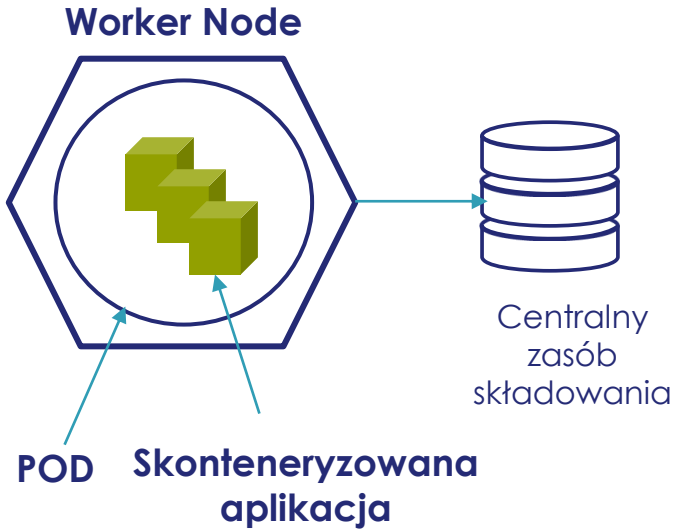


THALES

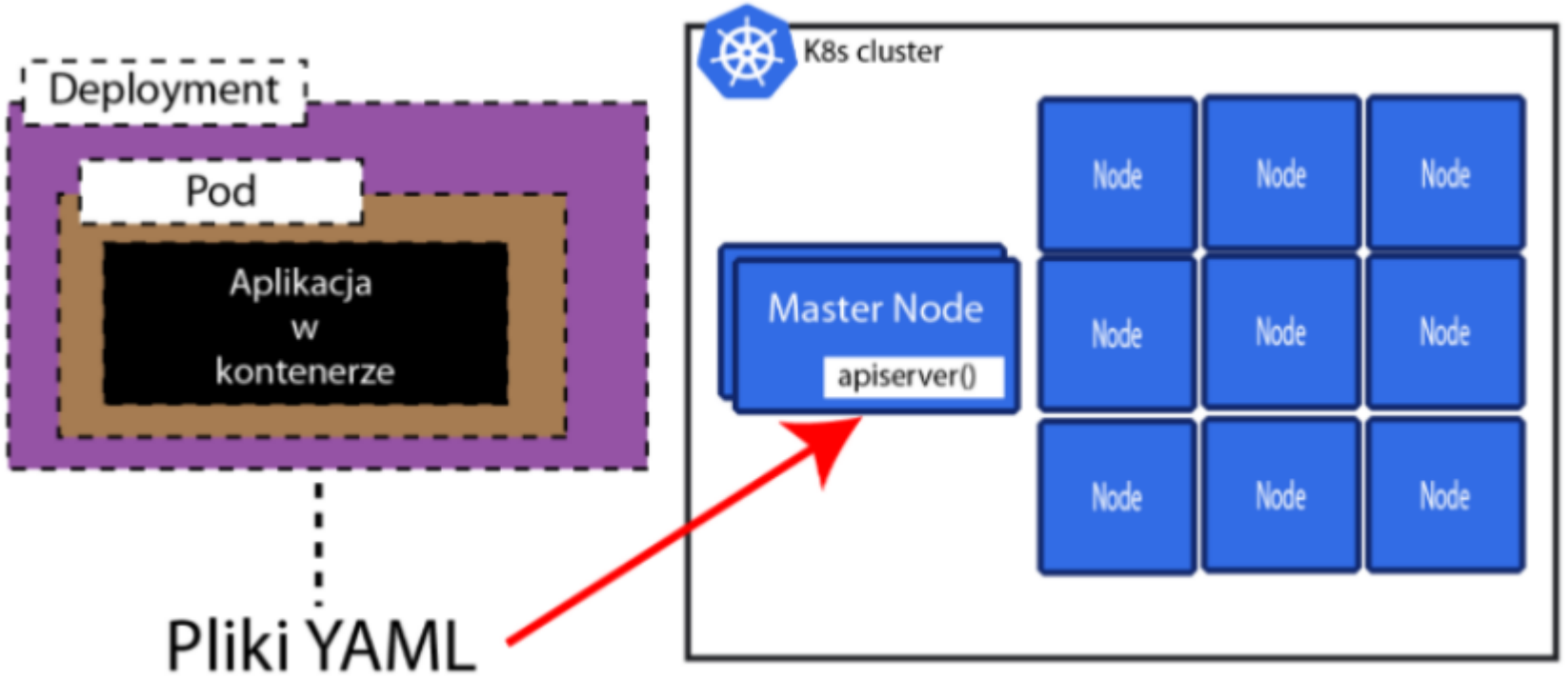
Kubernetes

Architektura

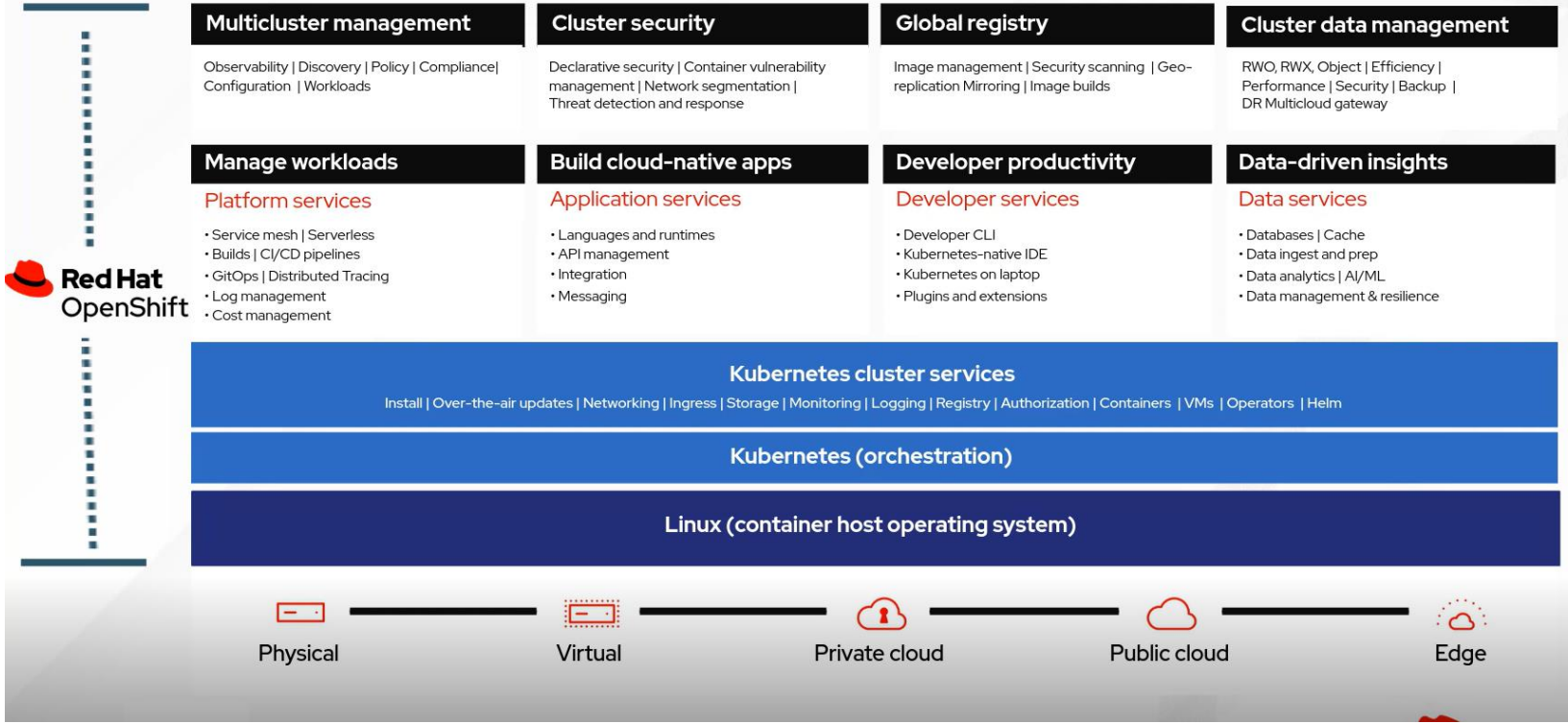




THALES



OpenShift Container Platform

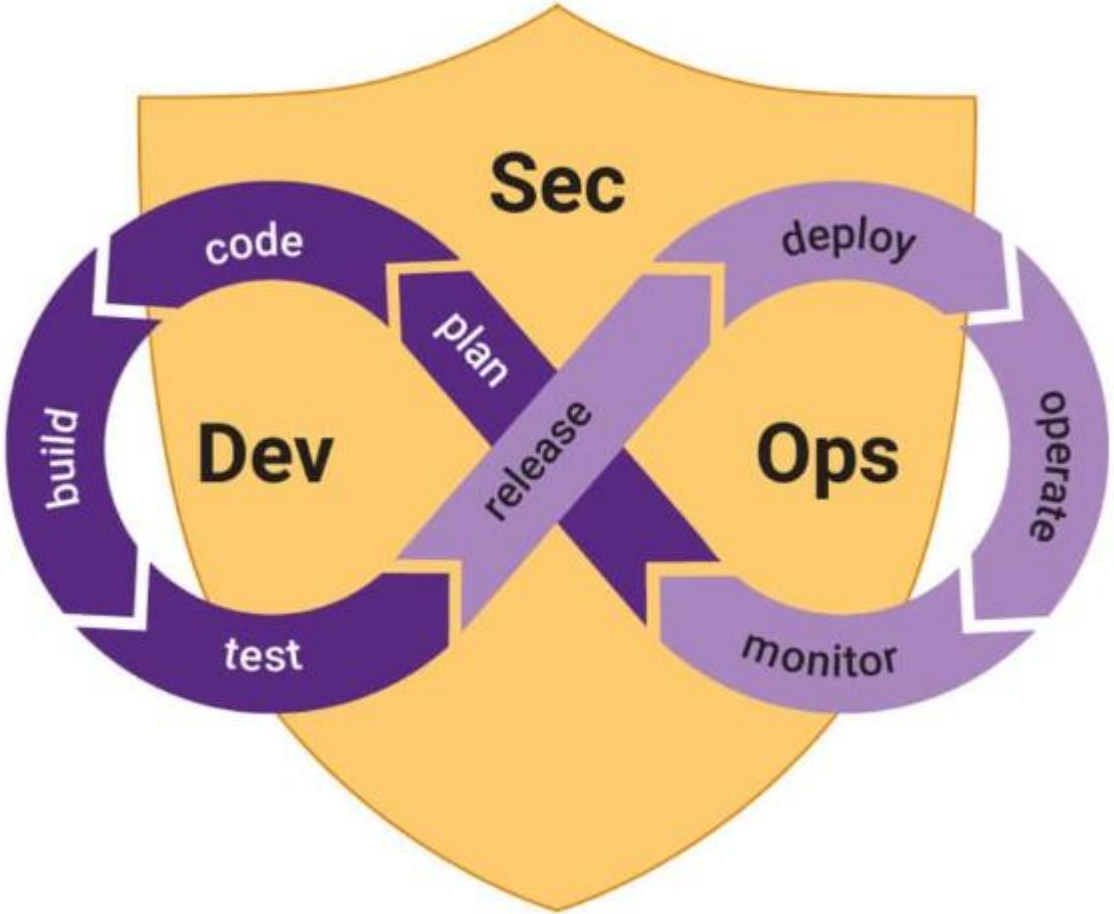


Źródło: BrightTalk

K8S wokół nas

Lokalnie	Google	AWS	Azure
Docker **OpenShift** **Kubernetes**	Google **Kubernetes** Engine Cloud Run Google Compute Engine	Elastic Container Services Elastic **Kubernetes** Services AWS Fargate EC2 AWS App Runner Amazon ECS Anywhere EKS Anywhere ROSA	Azure **Kubernetes** Service Azure Red Hat OpenShift Azure Container Apps Azure Functions Web-App for Container Container Instances Service Fabric Container Registry

DevSecOps a ochrona danych



Bezpieczeństwo a tworzenie aplikacji z wykorzystaniem kontenerów

1. Zarządzanie dostępem

- Unikaj uruchamiania procesów kontenerów jako użytkownik root, a także minimalizuj uprawnienia.
- Ogranicz dostępne zasoby (RAM, CPU).

2. Bezpieczeństwo obrazów

- Używaj oficjalnych, popularnych i minimalistycznych obrazów.
- Wymagaj od obrazów podpisu cyfrowego.

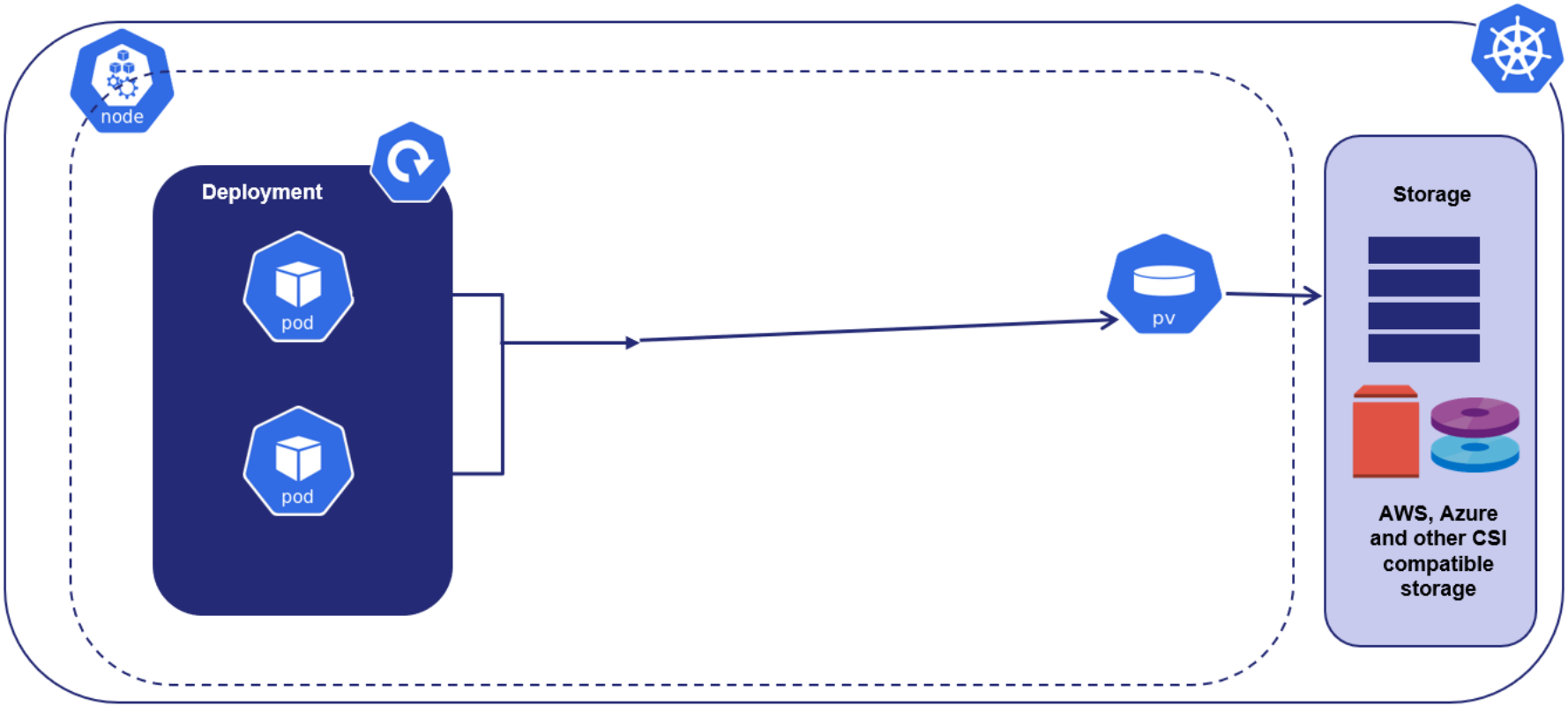
3. Zarządzanie sekretami

- Używaj sekretów lub wolumenów.
- Rozważ używanie sejfów.

4. Przechowuj wrażliwe dane w wolumenach, nigdy w kontenerach

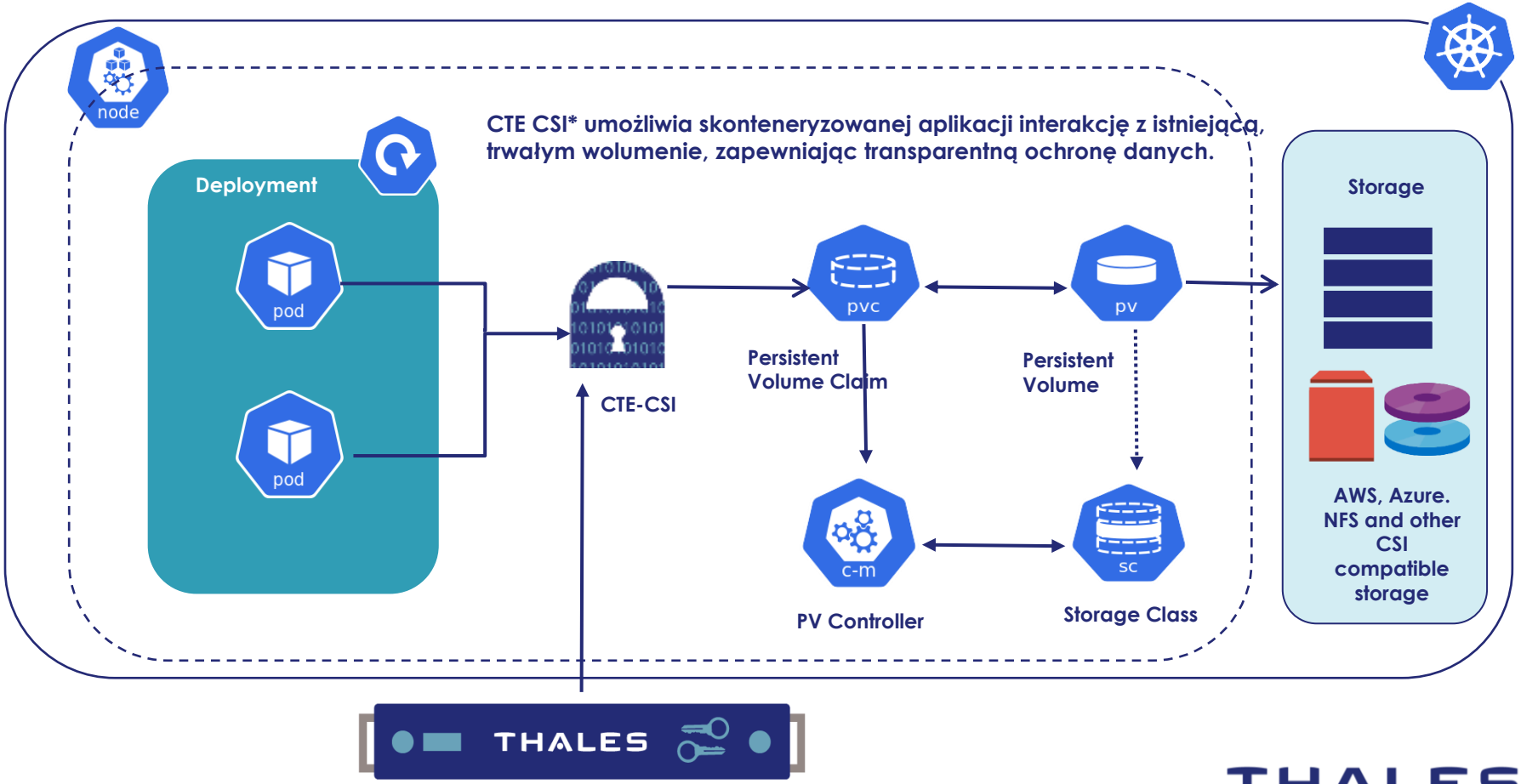
Rozwiązanie…

Aplikacja „v 0.1”



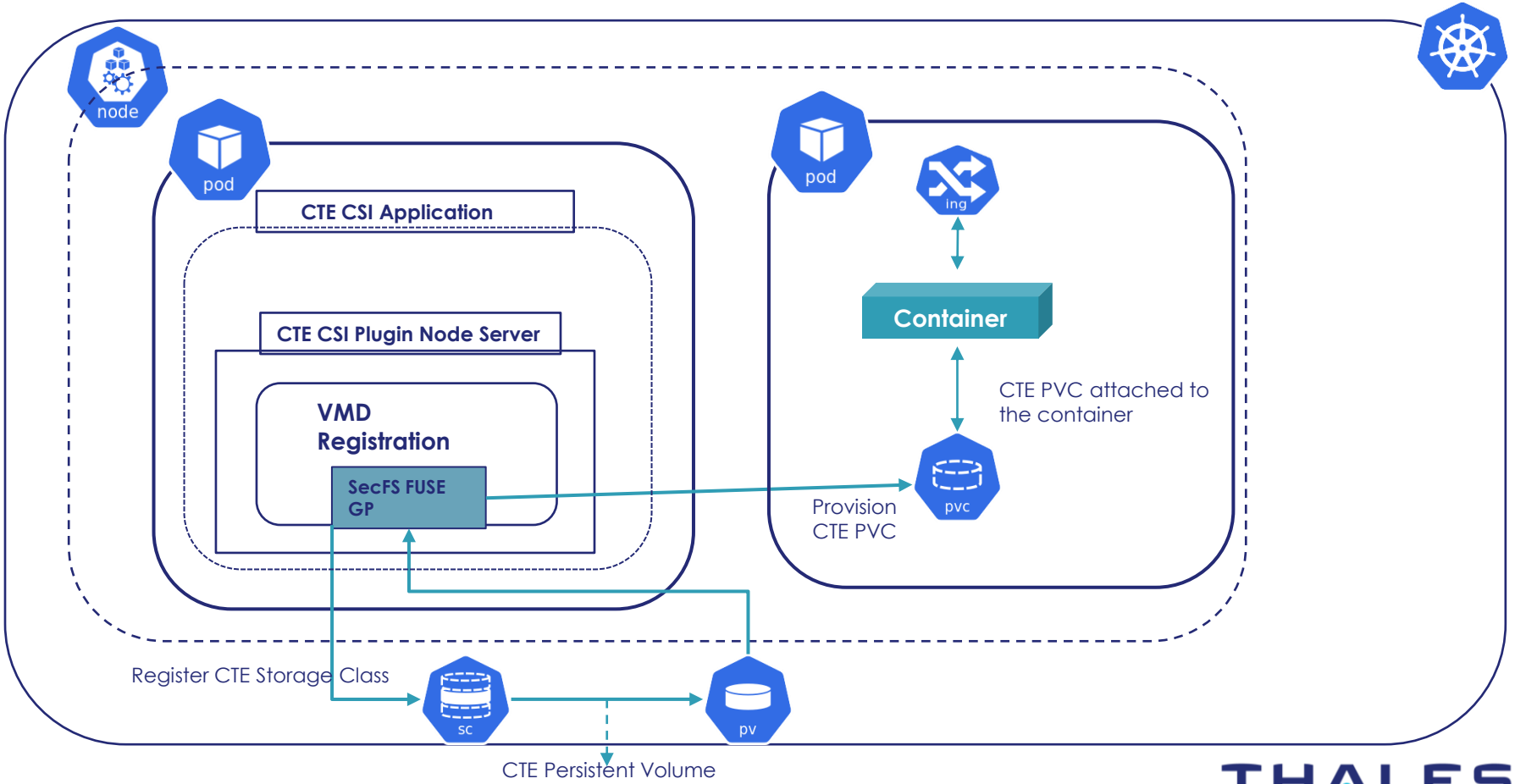
THALES

Aplikacja „v 1.0”!



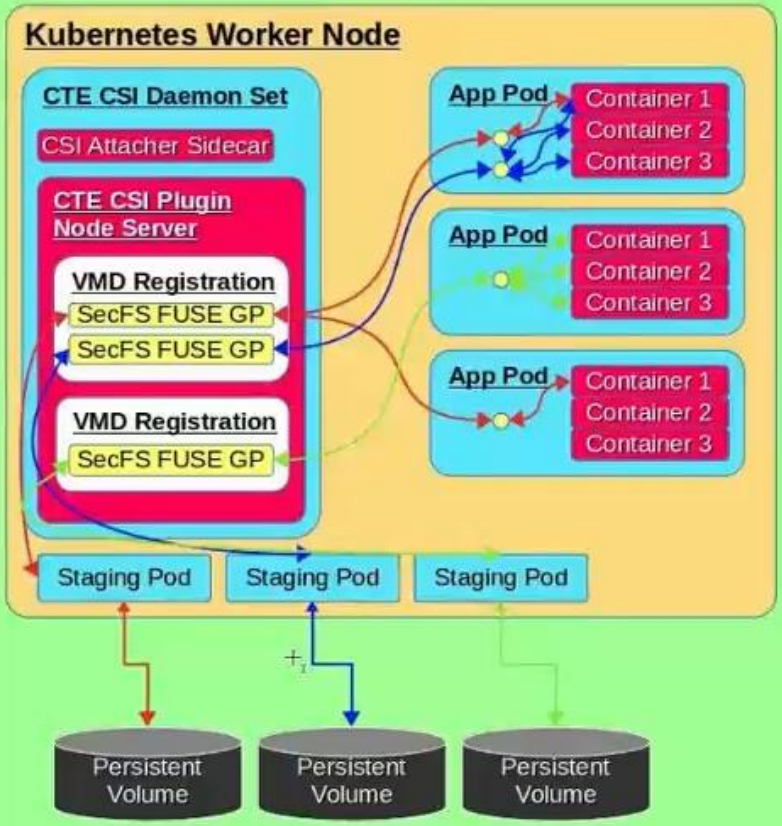
THALES

Zasada działania: CTE K8s i Container Storage Interface



THALES

Kubernetes Cluster



Kubernetes Master Node

CTE CSI Deployment Set

- CTE CSI Plugin Controller Server
- CSI Provisioner Sidecar (Modified)

RBAC Rules

- Create/List/Get/Delete Staging Pods
- List/Watch Persistent Volumes
- Create/Delete CTE Persistent Volumes

Storage Classes

- CM Registration Definition
- Support multiple registration per cluster

Config Maps

- Store configuration of CTE volumes in the cluster
- Running state recovery in the event of a CSI crash

Secrets

- VMD registration tokens

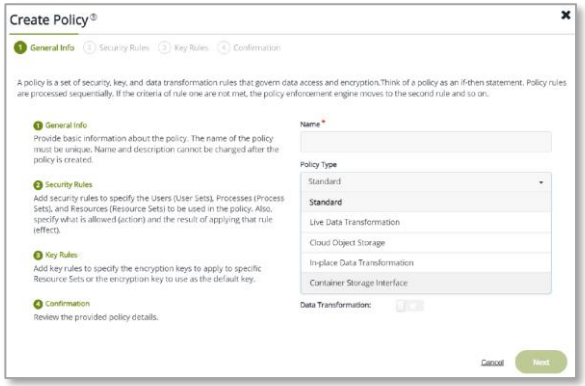
Legend:

- Kubernetes Cluster Node
- Kubernetes Pod
- Kubernetes Container
- Kubernetes CTE Configuration

CipherTrust Transparent Encryption dla Kubernetes

CTE kontroluje szczegółowo zabezpieczenia Pod-ów Kubernetes

- CTE-CSI jest dla Kubernetes (sam Docker to za mało)!
- CTE K8s jest zarządzane z poziomu CipherTrust Manager



Szyfrowanie, kontrola dostępu i bezpieczeństwa per POD

- Szyfruj dane generowane i przechowywane na trwałym woluminie dołączonym do aplikacji kontenerowej
- **Możliwość wdrożenia dla przypadków użycia *Kubernetes jak usługa***
- Kontroluj dostęp aplikacji kontenerowych uzyskujących dostęp do pamięci trwałej
- Brak zmian w aplikacjach kontenerowych

Dodatkowe korzyści z rozszerzeniem Kubernetes

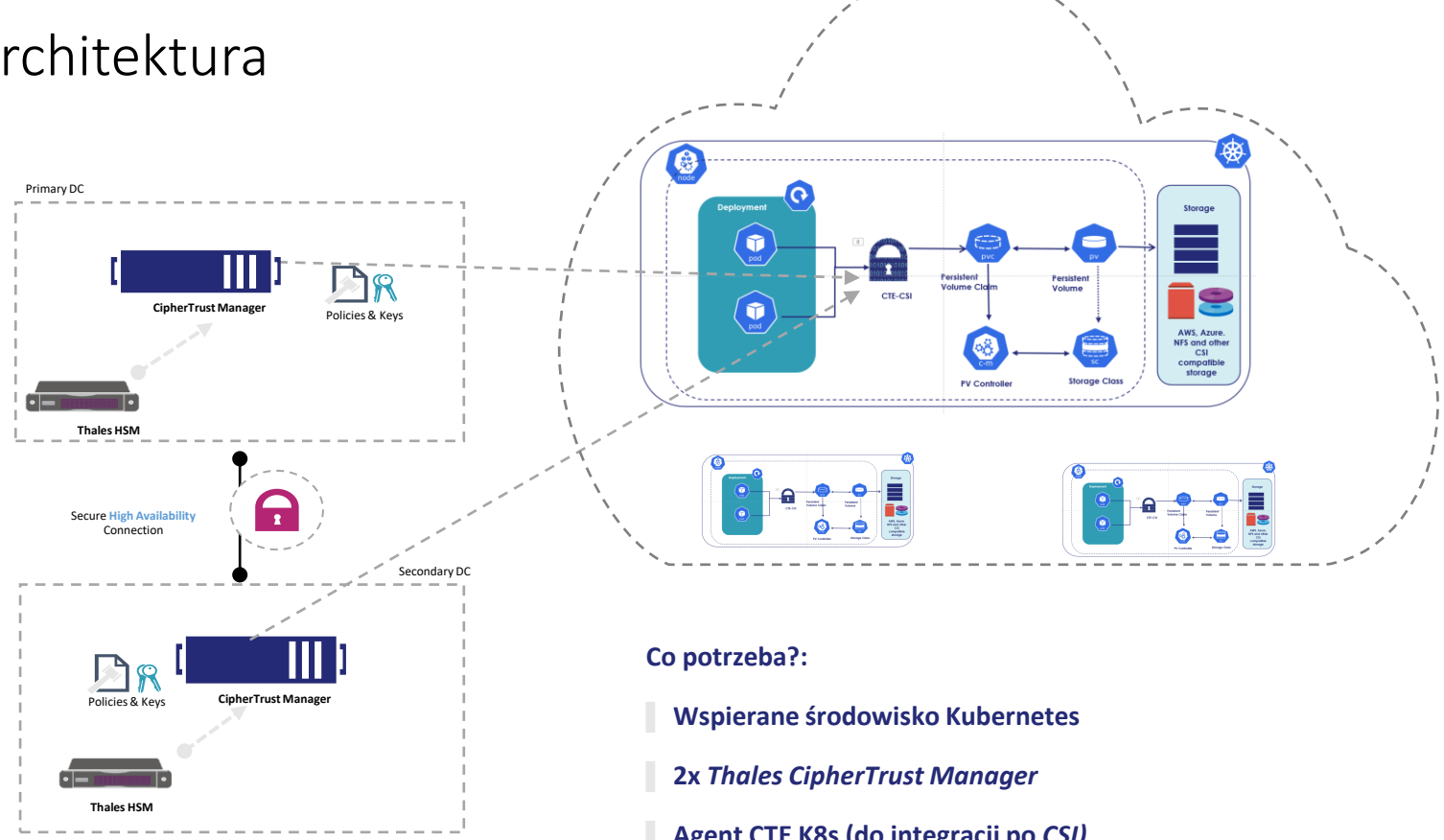
- Ochrona przed dostępem użytkowników root/uprzywilejowanych/nieautoryzowanych w kontenerach
- Chroń dane przed atakami eskalacji uprawnień z innych kontenerów
- Spełnij wymagania dotyczące zgodności w zakresie kontroli dostępu do danych i audytu na poziomie kontenera

THALES

CryptoPanel

podsumowanie

Architektura



Co potrzeba?:

- **Wspierane środowisko Kubernetes**
- **2x *Thales CipherTrust Manager***
- **Agent CTE K8s (do integracji po *CSI*)**
- **(opcjonalnie) 2x HSM to *Thales Luna seria A7xx lub seria S7xx***

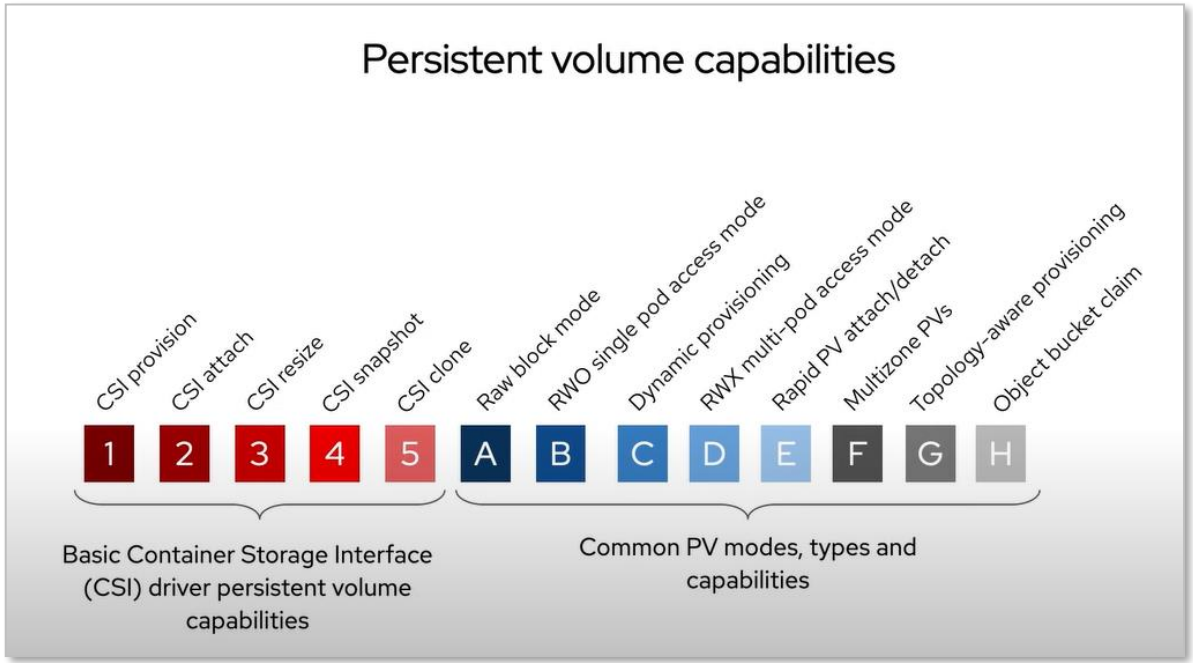
„Nauczki“, czyli *lessons learned*

- Czas zmienić paradygmat myślenia o tworzenia aplikacji…
  - *Container Technology is for Applications Developers*
- Dobre wyjaśnienie czym jest CSI i jak działa w K8s:
  - https://www.computerweekly.com/feature/Container-storage-101-What-is-CSI-and-how-does-it-work
- Dlaczego nas tu nie ma?: lista ponad 60 dostawców (sterowników) CSI dla Kubernetes
  - https://kubernetes-csi.github.io/docs/drivers.html
  - CTE-CSI nie jest na tej liście…bo nie jesteśmy dostawcą usługi składowania ☺
- Najnowszy CTE-CSI Deploy
  - https://github.com/thalescpl-io/cte-csi-deploy

„w dokumentacji raczej nie znajdziecie“

Które z właściwości CSI wspiera CTE K8s?

*In the CTE CSI implementation, we don’t actually store any data and rely on the underlying storage CSI driver for that. From the suggested capabilities we support: **1,2,B,C,D,F,G**. If the underlying storage driver supports additional capabilities, we won't restrict it and possibly work.*

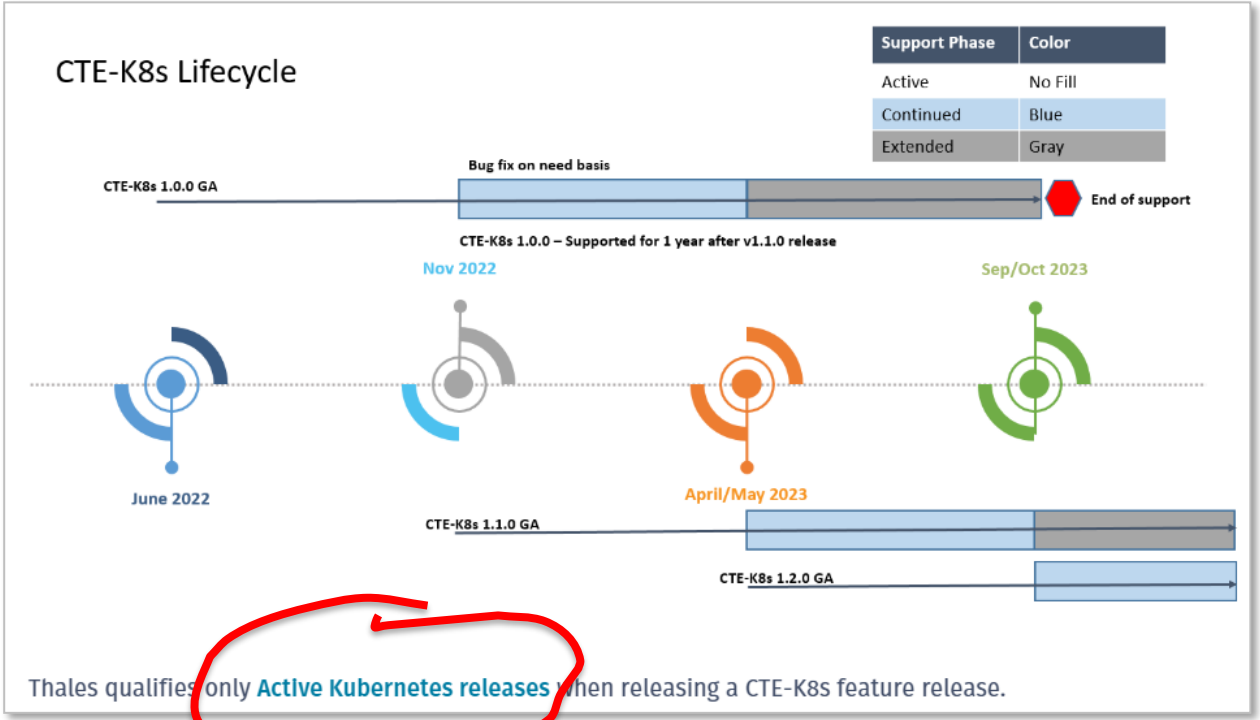


THALES

„w dokumentacji to znajdziecie“

No dobrze DevSecOps… a co z cyklem życia CTE K8s?

https://thalesdocs.com/ctp/cte-con/oslc/tx-k8s/index.html



CryptoPanel

CryptoPanel

TEST WIEDZY #19

Konteneryzacja zmieniła podejście do wytwarzania i utrzymania aplikacji. Czy i jak można chronić dane poprzez szyfrowanie w środowisku Kubernetes i OpenShift?

CryptoPanel #19 – bądź pierwszy, odbierz nagrody!

- Zapraszamy do testu wiedzy z tematu: *„Konteneryzacja zmieniła podejście do wytwarzania i utrzymania aplikacji. Czy i jak można chronić dane poprzez szyfrowanie w środowisku Kubernetes i OpenShift?*

- Uwaga: **5 najszybszych i poprawnych** odpowiedzi nagradzamy vouchery do Multikina (2 osobowe)

- Przy wypełnianiu formularza prosimy podać (aby móc zidentyfikować uczestnika!):
  - **Imię i Nazwisko**
  - **Adres e-mail**