2022-11-08

CYBERWAL

Journée des doctorants – **Cyber Factory**

Sebastien Dupont (CETIC), Nicolas Point (MULTITEL)

https://cyberwal.be
https://cyberexcellence.be

WHAT

What is a software factory?

01

WHY

Why a Cyber Factory?

02

Requirements

Partners needs for the factory

03

04

HOW

The Cyber Factory Architecture

05

Next Steps & Roadmap

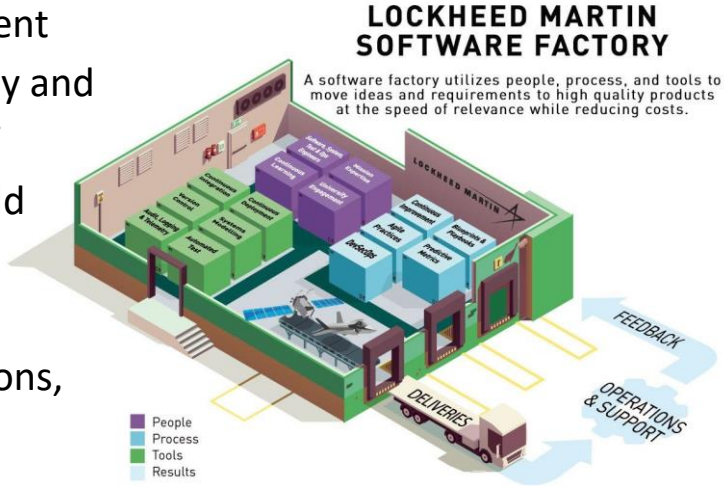
Integration environment

01

What is a software factory?

Software factory - WHAT

“A software factory is a structured collection of related software assets. When a software factory is installed in a development environment, it helps architects and developers predictably and efficiently create high-quality instances of specific types of applications. Each software factory is designed to help build applications that share an architecture and a feature set. Examples of such application types include mobile client applications, occasionally connected smart client applications, and transactional Web service applications.”



MSDN - Smart Client Software Factory 2010
http://msdn.microsoft.com/en-us/library/ff699235.aspx

Software factory - WHAT - Back Office

Back Office :

Les **briques logicielles** sont des contributions technologiques produites par des chercheurs Cyber Excellence dans le cadre d'un sujet de recherche que la factory va opérationnaliser, faciliter la diffusion et la valorisation.

L'usine logicielle CYBER Factory se matérialise par des **outils et méthodes** nécessaires à l'industrialisation du développement des briques de cybersécurité produites par le tissu scientifique wallon. Elle permet de favoriser la **collaboration** des développeurs sur des projets et d'améliorer ainsi la **qualité et la fluidité** dans les phases de développement.

Composants:

- Briques logicielles
- Connecteurs Open Science (source ou data)
- Environnement de virtualisation
- Outils d'automatisation

Software factory - WHAT - Front Office

Front Office :

La partie visible de la Factory permettra également de publier:

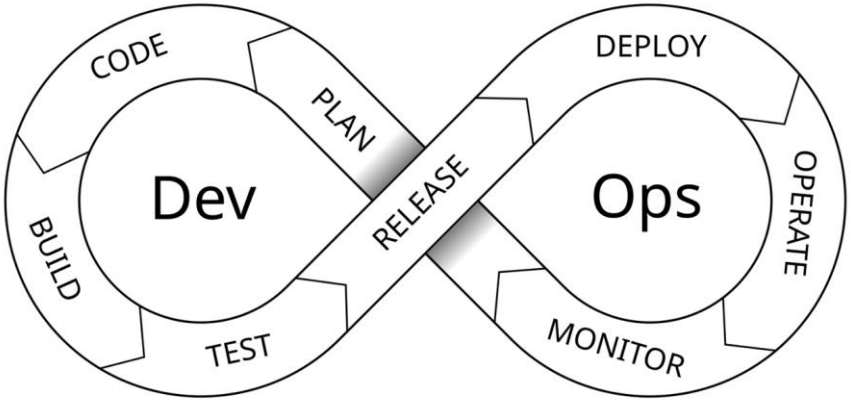
- Les **articles scientifiques** qui décrivent les travaux de recherches menant à la productions de ces briques logicielles,
- Les **méthodologies ou guidelines** fournies sous forme de white papers, articles de blog, etc.
- Les **offres de service** concernant les expertises ou infrastructures pour les entreprises.

02

Why a software factory?

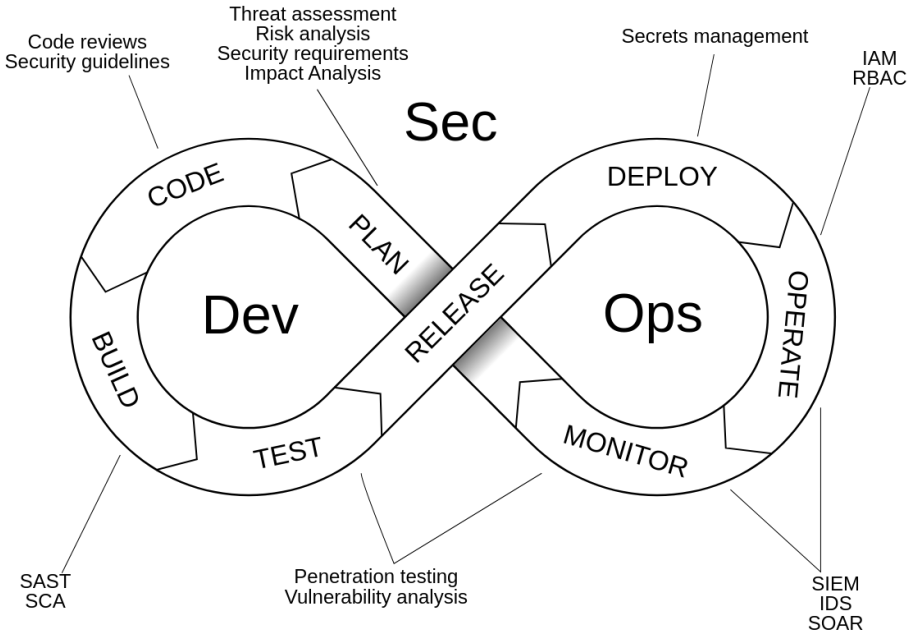
Software factory - WHY : DevOps

The **DevOps** approach, closely related to Agile software development method, combines software development (”Dev”) and operations (”Ops”) processes to ensure that new **features are added to a software solution in the shortest time possible, a**



Software factory - WHY : DevSecOps

The security problematic is not directly addressed in this approach and DevSecOps is aiming to correct this by **complementing DevOps with security processes and controls**.



DevSecOps:

- **left-shift in security** integration provides a better approach to security by intervening earlier in the deployment cycle and thus detecting security issues sooner,
- **automation of security**: continuous monitoring, minimal human intervention

Partners' "briques logicielles" (BL) can

1. benefit from this secure and automated CI/CD tooling
2. be integrated in a DevSecOps pipeline for testing and demonstration purposes

03

Cyber Factory Requirements

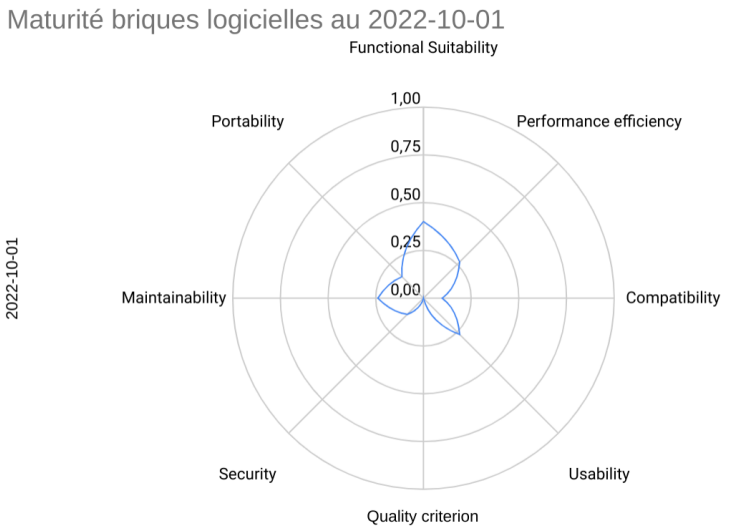
Software factory - Requirements

Briques logicielles déjà analysées:

- UMons (B. Quoitin) - Sécurisation protocoles de communication
- UNamur (S. Touch) - ASGARD - Adaptative Self Guarded Honeypot
- ULiege (B. Donnet) - Advanced observability
- UCLouvain (B. Duhoux) - Génération automatisée de scénarios d'attaque et défense de cyber-ranges
- ULB (J-M Dricot) - Smart grid, continuité edge-cloud

Software factory - Requirements

- Technologies **conteneurs** (principalement), machines virtuelles et bare metal
- Souhait d'extension de la factory dans les **Edge** des labos de recherche (VPN)
- Pas de besoin important de ressources (la plupart des BL "tiennent sur un laptop")
- Besoin d'un **espace de démonstration** des BL
- Plusieurs axes de **sécurisation** :
  a. de la factory
  b. des BL (security/quality checks)
  c. et des extensions edge
- Fonctionnalités moins prioritaires à priori pour les BL: SSO, quotas, gestion de datasets, GPU, ...



Software factory - Getting started !

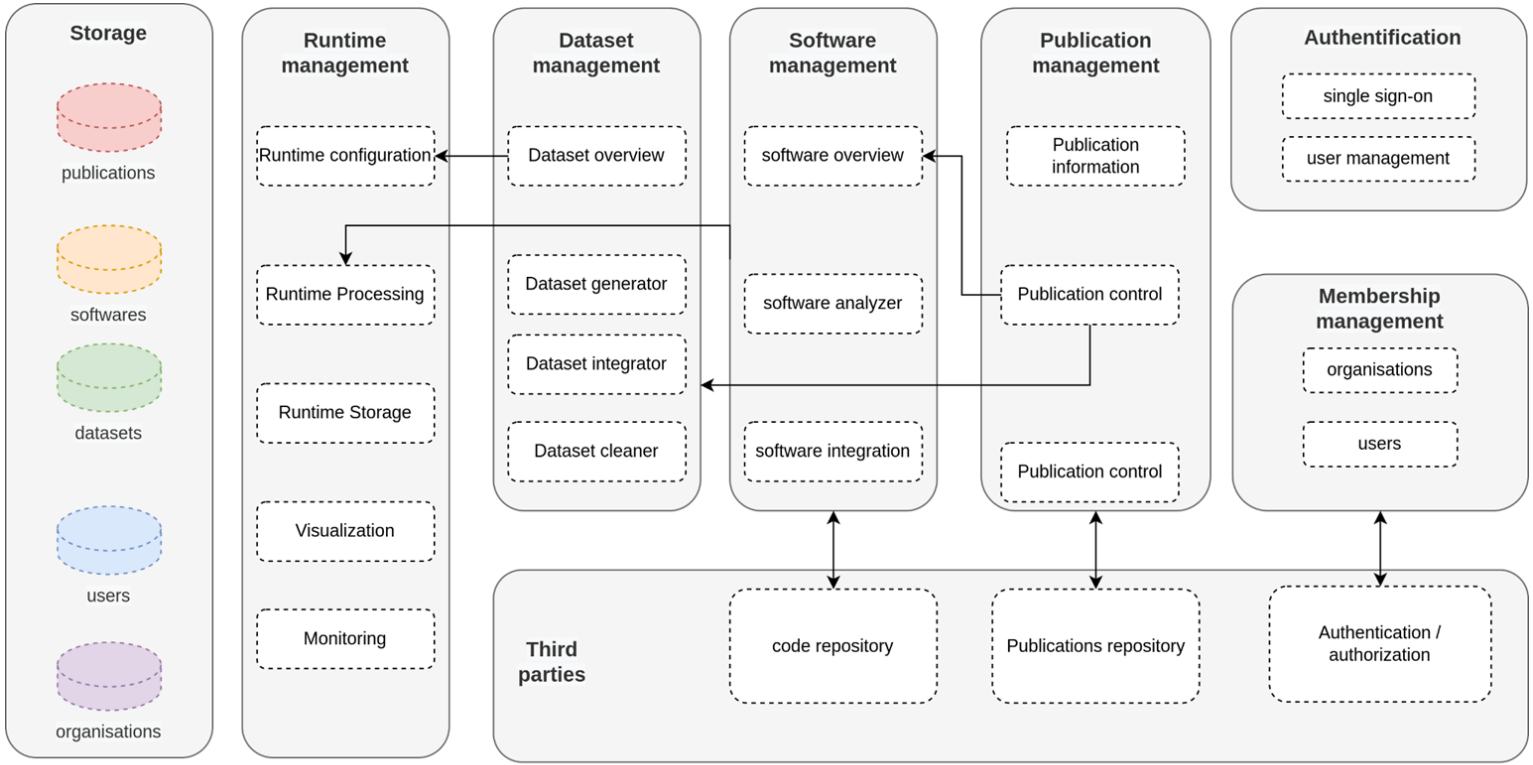
- Si vous avez des briques logicielles existantes ou en cours de développement, prévenez Sébastien Dupont (sdu@cetic.be) ou Nicolas Point (point@multitel.be) pour les recenser !

- Ceci nous permettra d'anticiper différentes actions :
  a. Faire la promotion sur le front office de la Factory
  b. Ne pas en faire la promotion publique mais la rendre disponible dans le back-office dès le début
  c. L'utiliser comme cas concret pour la mise au point du back-office (test des outils de CI/CD p/ex)

04

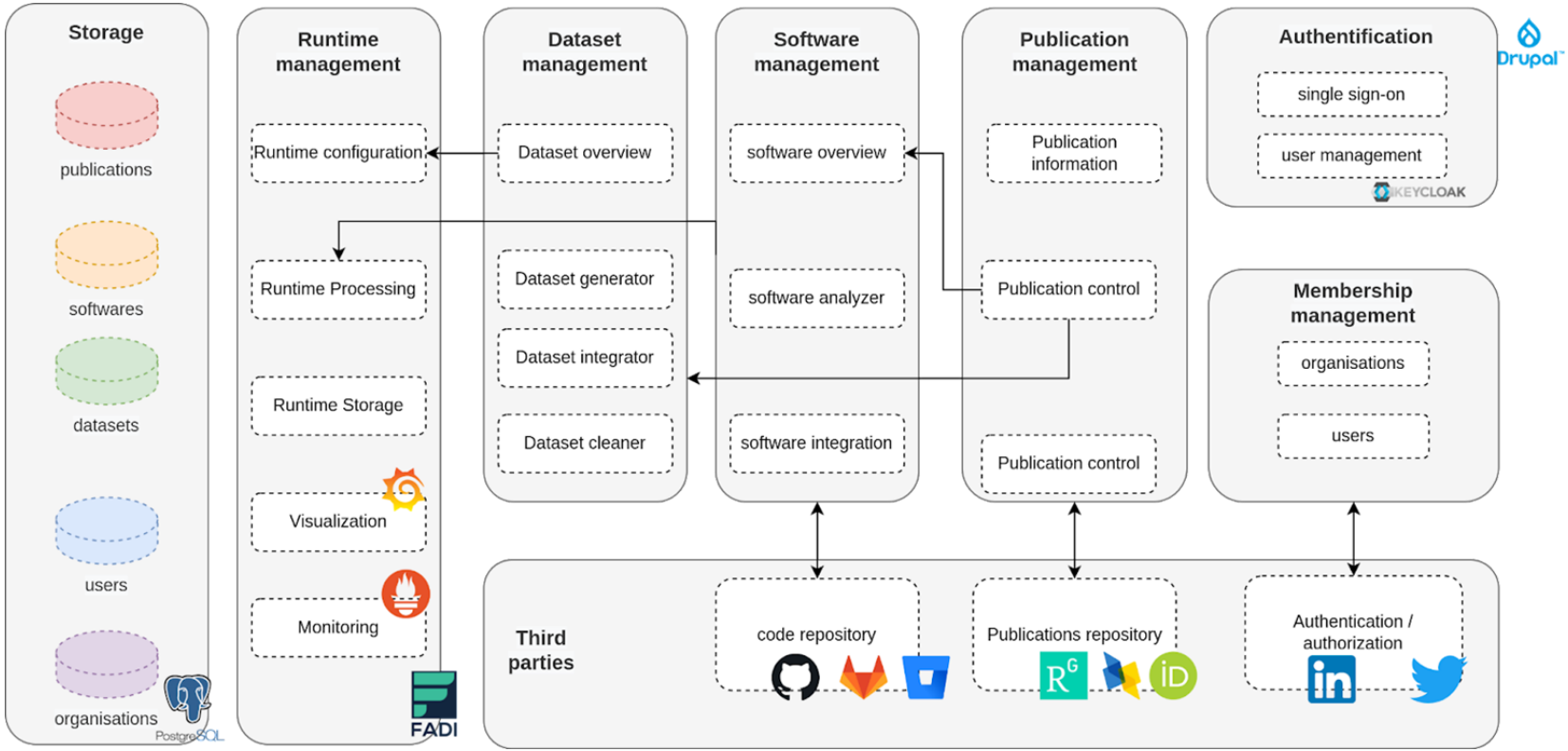
How? The Cyber Factory Architecture

Software factory - HOW - Architecture



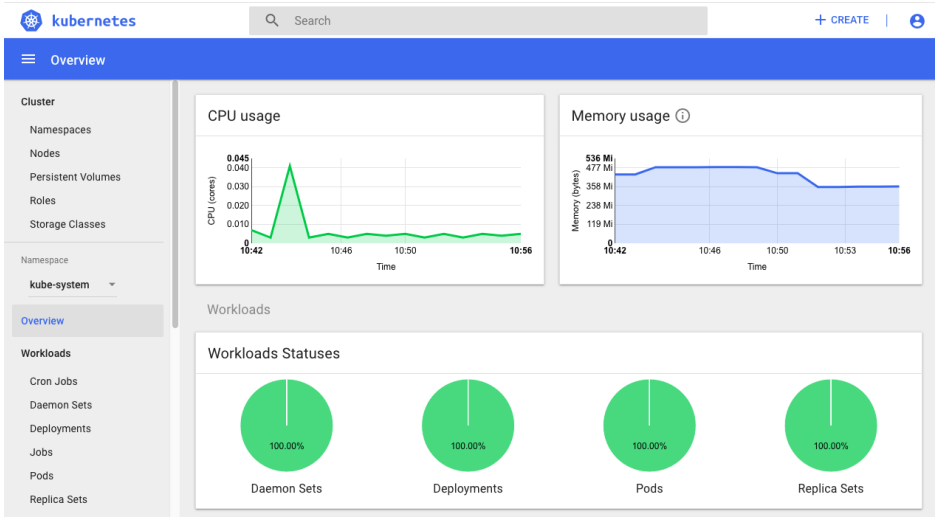
Factory - Logical view

Software factory - HOW - Architecture



Factory - Implementation view

Software factory - HOW - Containers



kubernetes

"Open-source system for automating deployment, scaling, and management of containerized applications."

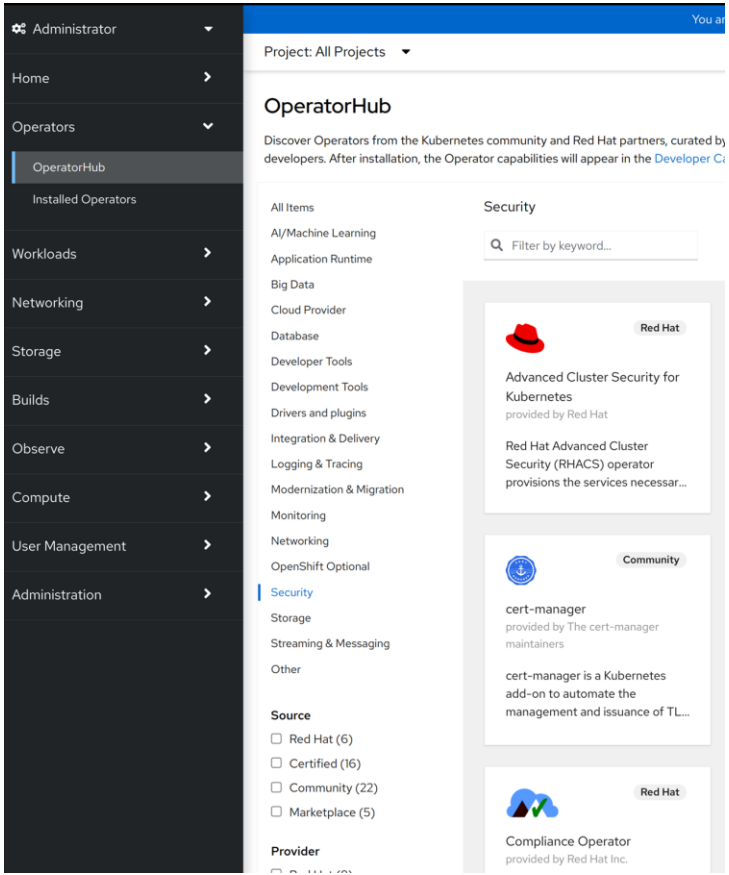
https://kubernetes.io/

- Favorise la **portabilité**: entre les environnements (local, dev, prod), clouds, …
- Orchestration de l'**élasticité horizontale** en fonction de la charge
- **Self healing**
- Gestion de la configuration, orchestration du stockage, gestion des secrets, …

Software factory - HOW - Architecture

PaaS vs CaaS

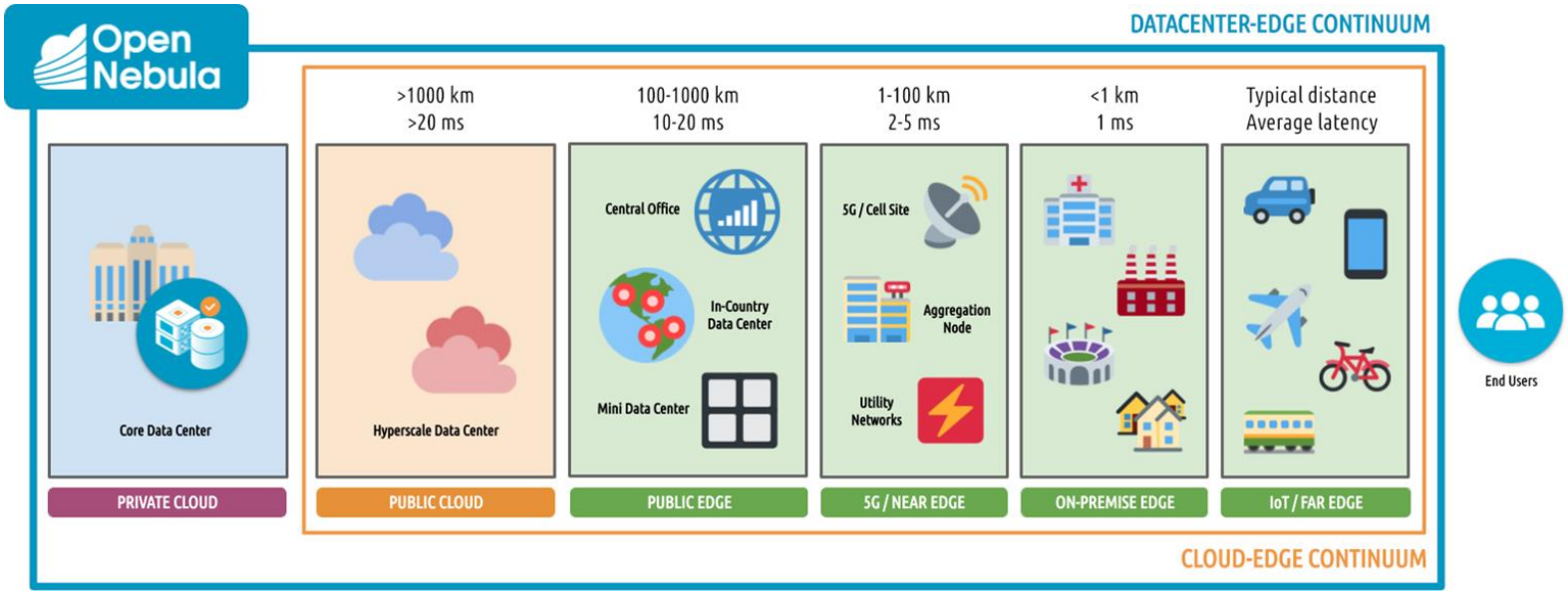
- OpenShift/OKD adds PaaS features over Kubernetes : web interface, catalog of services, CI/CD, stricter security policies, etc.
- The Red Hat OpenShift and VMWare Tanzu PaaS solutions are used as the base in various important software factories (US Army, Navy, Airforce, BE: Proximus, Smals, EHealth).
- OpenShift/OKD is the main distribution of Kubernetes with PaaS features, a community version (free), open source and that can be hosted on premises.
- Paying support, advanced security tooling, ... is available



Software factory - HOW - Edge computing

"Edge Computing is an optimization concept that consists of processing data and the intelligence of its processing on the periphery of the data source"

Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I., & Ahmed, A.



Source : "Building an Open Source Edge Computing Platform" A. Carrillo Aspiazu : https://opennebula.io/building-an-open-source-edge-computing-platform/

Software factory - HOW - Défis

- Défi 01: Automatisation de la vérification cyber de CPS
- Défi 02: Gestion des risques pour tests d'intrusion
- Défi 04: Cyber-sécurisation by design systèmes industrie 4.0 et spatiaux
- Défi 07: Configuration de transmission réseaux de données
- Défi 10: Sécurisation de la numérisation des réseaux énergétiques

Ces premiers défis seront étudiés dans la factory à travers plusieurs aspects:

edge, convergence IT/OT, observabilité, réaction, simulation de réseaux IoT, …

Conclusion and next steps

The software factory

- Helps CyberExcellence partners to build and demonstrate security tools (BL) **fast**, with a high level of **quality** and **security**
- Relies on the **OpenShift/OKD platform** that leverages containerisation and **Dev(Sec)Ops** practices

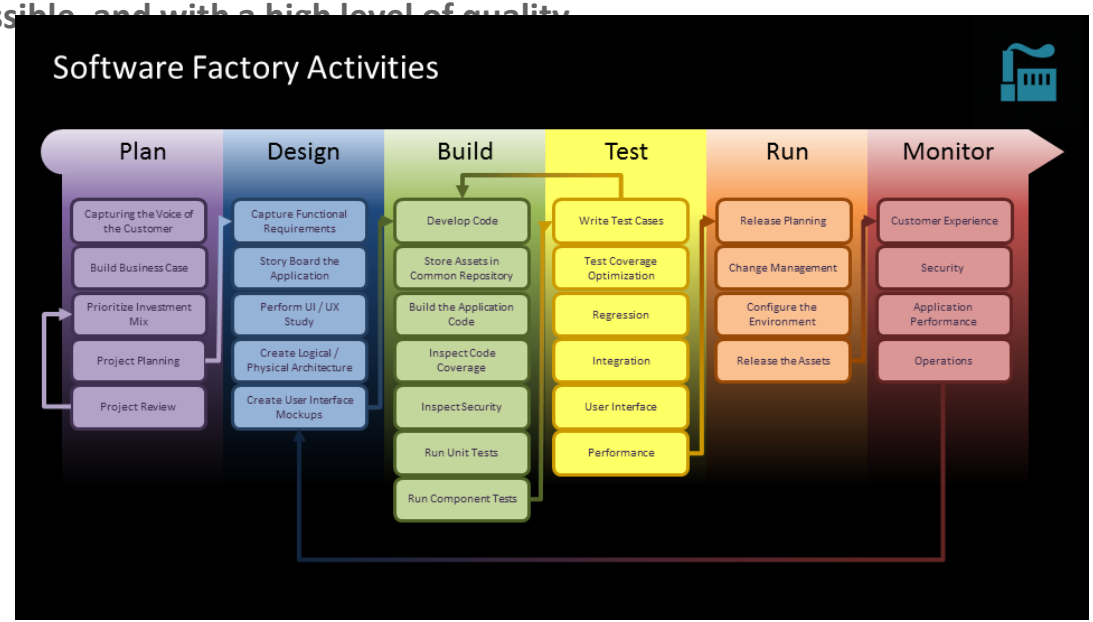
Next steps

- Continue to collect new and old “Briques Logicielles” requirements
- Easy onboarding into the factory for CyberExcellence partner’s “briques logicielles” through examples and documentation
- Deployment of the factory to a hosting environment

Merci de votre attention

Software factory - WHY

The **DevOps** approach, closely related to Agile software development method, combines software development (”Dev”) and operations (”Ops”) processes to ensure that new **features are added to a software solution in the shortest time possible, and with a high level of quality**



“The Modern Software Factory Series, Part I: Overview and Process”, Patrick Gryzan, Dec. 02, 16 - Agile Zone