CAMPUS CYBER

INSIDER : Présentation des livrables de la CI CyberAgile

25 mars 2025

00. SOMMAIRE.

01. ACTUALITÉS.

- **Cyber Breakfast -** vendredi 28 mars (8h30 – 11h30) - échange sur les actualités cyber avec le Campus Cyber Bretagne

- **Campus Cyber au FIC du 1er au 3 avril – Stand D7**

- **Lancement de la Méthodologie CyberSustainability -** jeudi 10 avril (8h30-11h30) au Skylounge (R+13)

Le Campus Cyber et Cyber4Tomorrow vous invitent au lancement de la Méthodologie CyberSustainability, la première approche permettant de mesurer et réduire l'empreinte carbone des mesures de cybersécurité. Expérimentée au sein de grandes entreprises et collectivités, elle aide les RSSI à mieux comprendre et agir sur leur impact environnemental.

- **Wiki du Studio des Communs : wiki.campuscyber.fr**

01. INTERVENANTS.

- **Benjamin CHOBERT**, BNP Paribas (Introduction)
- **Vincent FOURESTIER**, Banque de France (Stream Gouvernance)
- **Antoine RICHER**, Accenture (Stream Security Champions et SME AppSec)
- **Olivier DUPUY D'UBY**, IBM (Stream Technologies)

02. INTRODUCTION.

02. INTRODUCTION.

GT Cybersécurité Agile

ETA: Q2 2025

“Face à l’adoption croissante des méthodologie Agile visant à réduire le Time-To-Market, la Sécurité dans les développements doit répondre à de nouveaux impératifs de célérité.”

+ **Stream 1 : Gouvernance**
  Avancement: 95%
  5 contributeurs actifs

  Contenu du livrable :
  - Secure SDLC, processus, comitologie, …
  - Gestion des vulnérabilités en développement
  - Threat modeling

+ **Stream 2 : Security Champions & SME**
  Avancement: 85%
  5 contributeurs actifs

  Contenu du livrable :
  - Vade Mecum des Security Champions et SME AppSec
  - RACI des activités de Security Champions et SME AppSec

+ **Stream 3 : Technologies**
  Avancement: 85%
  5 contributeurs actifs

  Contenu du livrable :
  - Etat du marché
  - Stratégie de monté en maturité technologique

03. GOUVERNANCE.

03. PRESENTATION LIVRABLE GOUVERNANCE.

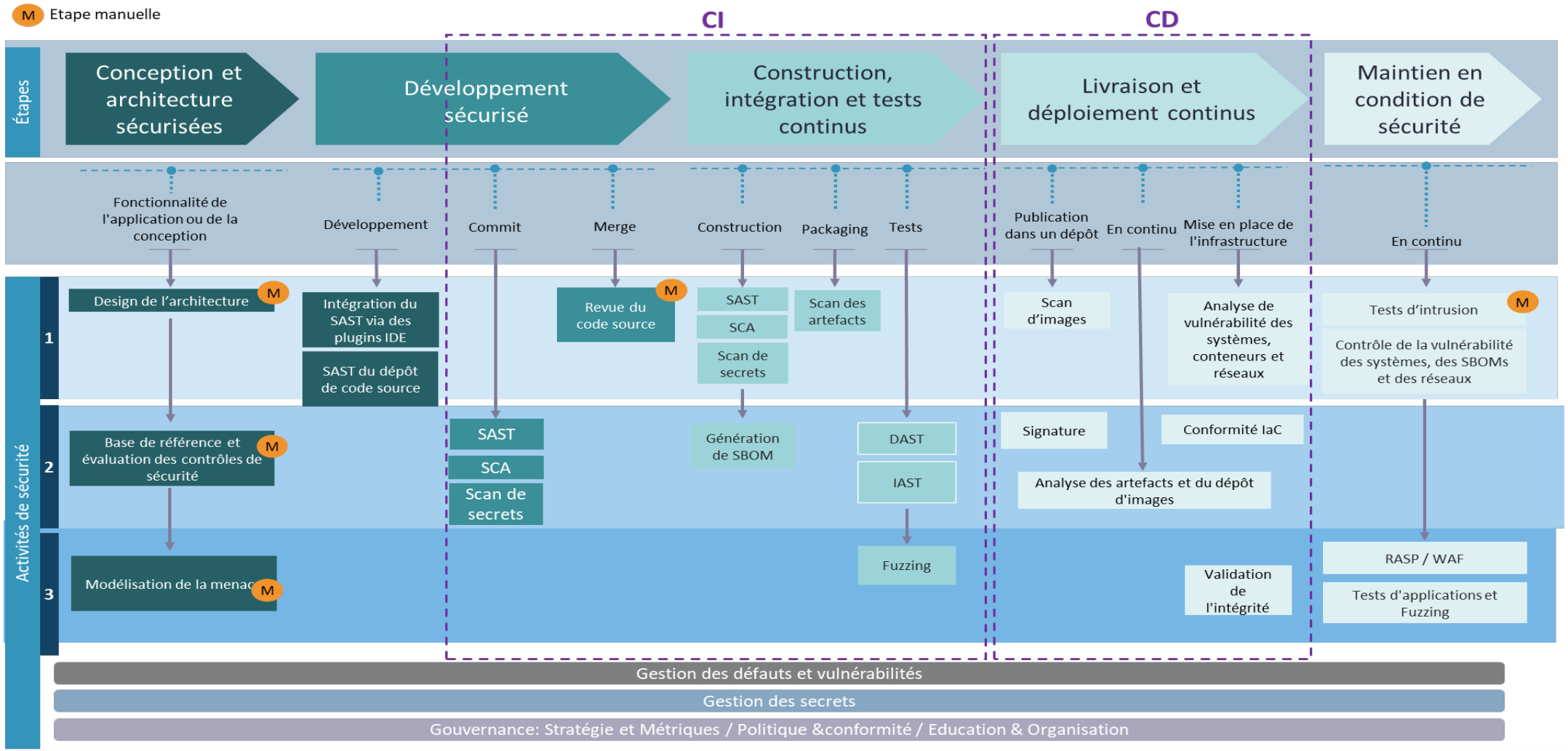
Liste des activités de sécurité du Secure SDLC :

- Définition de processus
- Mise en place d'outil de sécurité
- Contrôles de sécurité
- Rédaction de document

Regroupement selon les étapes du modèle DevOps

Classification selon 3 niveaux de maturité

03. PRESENTATION LIVRABLE GOUVERNANCE.



04. SECURITY CHAMPIONS & SME APPSEC.

04. PRESENTATION LIVRABLE SECURITY CHAMPIONS & SME APPSEC.

Objectif

Aider les responsables de sécurité, les responsables de programmes de Sécurité Applicative / DevSecOps et les chefs de projet, **à concevoir une organisation** au niveau de leurs équipes pour **répondre aux enjeux de sécurité dans les projets Agiles**.

⇒ **Applicable aux contextes Agiles** uniquement, quelle que soit la méthodologie Agile.

⇒ **Cadre à adapter** en fonction des besoins et du contexte de son organisation.

+ Vade Mecum des Security Champions et SME AppSec

Raisons de l'apparition des rôles de **Security Champion (SC)** et **Subject Matter Expert (SME) AppSec**, **activités typiques** qui incombent à chacun, les **modèles organisationnels**, les **compétences clés**.

+

Eléments de **décision** et de **suivi**, **écueils** possibles et **points de vigilance**.

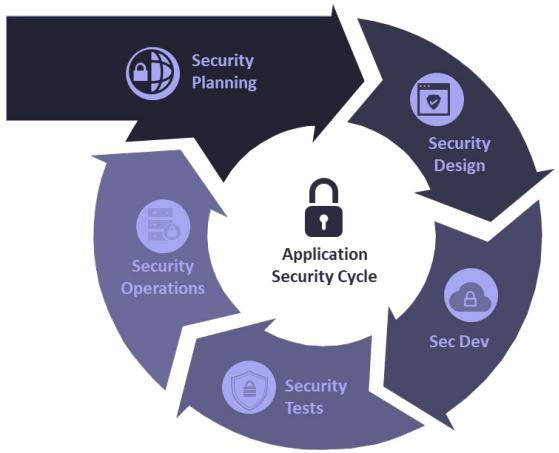
+ RACI des activités de Security Champions et SME AppSec

Modèle de **répartition des responsabilités des différents rôles par rapport aux activités de sécurité**, à l'échelle d'un produit (application) et d'un ensemble de produits (voire de toute l'organisation).

⇒ **Support** pour la **mise en place d'un modèle opérationnel cible** à base de SC et SME AppSec.

04. PRESENTATION LIVRABLE SECURITY CHAMPIONS & SME APPSEC.

Le Security Champion : Référent sécurité et point de contact privilégié



Equipe produit

Se concentre sur ce qui a de **la valeur ajoutée**, les fonctionnalités du produit, les délais, la qualité et **la sécurité**.

Security Champion

Sécurité de la conception

Sécurité du développement

Sécurité de l'exploitation et de la maintenance

Organiser la gestion des activités de sécurité au niveau du projet (définition et priorisation des tâches, vérifications, analyses, remédiation).
Favoriser la montée en compétences des développeurs sur le sujet de la sécurité.
Améliorer le pipeline, permettre la **fluidité des processus** et **l'utilisation des outils**.

Assurer la conformité de la sécurité aux politiques et aux directives de l'organisation.
Quérir de l'aide auprès du ou des **SME**.
Remonter les incidents et **travailler de concert avec le SOC**.

Equipes de sécurité

Gouvernance de la sécurité Etablir la politique de sécurité du SI (PSSI), faciliter sa déclinaison au sein des projets IT et en vérifier la conformité

SME AppSec

Sécurité Opérationnelle
Supervision de sécurité, traitement des incidents, gestion de crise

04. PRESENTATION LIVRABLE SECURITY CHAMPIONS & SME APPSEC.

Premier extrait du RACI : Activités dans le périmètre d'un seul produit

	ROLES											
	Equipe produit					Equipe de Cybersécurité					Processus et Outils	
	Product Manager / Owner	Technical Lead	Developer	CI/CD Maintainer	Security Champion	CISO	Governance & Compliance	Security Architect	SOC (Security Operation Center)	SME AppSec	AppSec tool maintenance team	Dev(Sec)Ops Engineer
ACTIVITES												
Périmètre d'un seul produit												
Etape SDLC - Conception et architecture sécurisées												
Déterminer les exigences de sécurité applicables parmi celles émanant de l'organisation	A	R	I	I	R	I	C	I	I	C		
Définir les mesures de sécurité permettant de respecter les exigences (Security User Stories)	A	R	C	C	R		I	C	C	C	C	C
Analyser les risques de sécurité portant sur le produit / Modéliser les menaces (Threat Modeling)	A	C	C	C	R	I	C	C	C	C		
Concevoir l'architecture du produit en prenant en compte les exigences et les risques de sécurité	A	R	C	C	R	I	I	C	C	C		C
Définir la politique de sécurité applicable et les indicateurs clés de suivi	A	R	I	R	R	I	C	I	I	C	I	C
Planifier les activités de sécurité au sein du pipeline	A	C	I	C	R		I	I	C	C	C	C
Etape SDLC - Développement sécurisé												
Implémenter les mesures de sécurité et les solutions de remédiation/atténuation/contournement des risques identifiés	C	A	R	R	C			I	I	C		C
Participer aux développements (code source de l'application et modèles d'Infrastructure as Code - IaC) en respectant les bonnes pratiques de sécurité	I	A	R	C	C			I		C		C
Réaliser des revues de code (par les pairs) en prenant en compte la sécurité	I	A	R	C	R					C		C
Secrets - Configurer la détection des secrets (dans le code et son ecosystème)	I	C	C	R	A					C	C	C
Secrets - Trier et qualifier les résultats de la détection des secrets	I	C	R	R	A					C		C
Secrets - Traiter les défauts (correction du défaut ou atténuation | acceptation | transfert du risque, suivi des tâches résultantes dans le backlog)	A	C	R	R	C	I	I	I	I	C		I
SAST - Configurer l'analyse statique de la sécurité du code source	I	C	R	R	A					C	C	C
SAST - Trier et qualifier les résultats de l'analyse statique de la sécurité du code source	I	C	R	I	A					C		
SAST - Traiter les défauts (correction du défaut ou atténuation | acceptation | transfert du risque, suivi des tâches résultantes dans le backlog)	A	C	R	I	C	I	I	I	I	C		
IaC - Configurer l'analyse statique de la sécurité des modèles IaC	I	C	C	R	A					C	C	C
IaC - Trier et qualifier les résultats de l'analyse statique de la sécurité des modèles IaC	I	C	R	R	A					C		C
IaC - Traiter les défauts (correction du défaut ou atténuation | acceptation | transfert du risque, suivi des tâches résultantes dans le backlog)	A	C	R	R	C	I	I	I	I	C		I
Etape SDLC - Construction, intégration et tests continus												

04. PRESENTATION LIVRABLE SECURITY CHAMPIONS & SME APPSEC.

Deuxième extrait du RACI : Activités dans le périmètre de plusieurs produits / organisation

	ROLES											
	Equipe produit					Equipe de Cybersécurité					Processus et Outils	
	Product Manager / Owner	Technical Lead	Developer	CI/CD Maintainer	Security Champion	CISO	Governance & Compliance	Security Architect	SOC (Security Operation Center)	SME AppSec	AppSec tool maintenance team	Dev(Sec)Ops Engineer
Périmètre de plusieurs produits et/ou de l'ensemble de l'organisation												
Elaboration de la stratégie de sécurité												
Définir des exigences de sécurité cohérentes par rapport aux produits	I	C	I	I	C	A	R	R	C	R	C	C
Analyser les risques de sécurité portant sur les produits ou l'organisation	C	I	I	I	C	A	R	R	C	R		I
sécurité	I	C	I	I	C	A	C	R	C	R	C	C
Etablir la politique de sécurité globale, un modèle opérationnel établissant les rôles et responsabilités de chaque partie prenante et les indicateurs clés typiques de suivi	C	C	I	I	C	A	R	R	R	R	C	R
Proposer/Imposer un pipeline type intégrant les activités de sécurité et respectant la politique de sécurité globale	I	C	I	C	C	A	C	C	C	R	R	R
Etablir les plans/parcours de sensibilisation et de formation à la Sécurité Applicative (et réaliser les supports associés)	I	C	C	C	C	A	C	C	C	R	C	C
Etablir les plans d'audit de sécurité (revues d'architecture, de code, des configurations, tests d'intrusion) et les programmes de Bug Bounty	I	I	I	I	C	A	R	C	I	R	I	C
Initier une communauté de Sécurité Applicative, regroupant a minima les SME AppSec et les Security Champions	R	C	C	C	R	A	C	C	C	R	I	C
Mise en oeuvre de la stratégie de sécurité												
Dispenser des sessions de sensibilisation aux enjeux de la Sécurité Applicative					R	A	R	R		R		
Dispenser des sessions de formation à la Sécurité Applicative (principaux risques de sécurité, développement sécurisé, Cybersécurité dans un contexte agile, etc.)						A				R		
Animer la communauté de Sécurité Applicative (communications, organisation d'événements, tables rondes, ateliers, etc.)	I	I	I	I	C	A	I	I	I	R	I	I
Contribuer au sein de la communauté de Sécurité Applicative (partage de connaissance et de retours d'expérience, entre-aide, etc.)	I	R	R	R	R	I	R	R	R	A	R	R
Alimenter de manière continue les référentiels de sécurité (guides de développement sécurisé, de durcissement, bases de connaissances sur la sécurité, etc.)	I	C	C	C	R	A	R	R	C	R	C	C
Soutenir les Security Champions dans la démarche de Sécurité Applicative	R	R				A	R	R	R	R	R	R
Réaliser une veille de sécurité applicative	I	C	I	I	C	A	I	C	C	R	R	R
Maintenir les outils de Sécurité applicative (SAST, SCA, DAST, IAST, RASP, etc.)	I	I		I	I	I				A	R	C
Implémenter la collection automatisée et centralisée des indicateurs clés de suivi	I	I		C	C	A	C	C	C	R	C	C
Organiser les audits de sécurité et les programmes de Bug Bounty	I	I			C	A	R	C	I	R	I	I
Gérer les risques (en particulier les risques résiduels), les vulnérabilités et les contre-mesures au niveau de l'organisation	I	C	I	I	C	A	R	R	R	R	I	C
Contrôle et validation de sécurité												

05. TECHNOLOGIES.

05. PRESENTATION LIVRABLE TECHNOLOGIES.

+ **Une cartographie des technologies d'intérêt sur le domaine**

  Présentation des divers types d'outillages et de leurs interactions (SAST, SCA, DAST, RASP…)

  Support des orientations gouvernance et organisation (SSDLC et Security Champion)

  Architecture de référence

+ **Des orientations pour accompagner les choix des organisations**

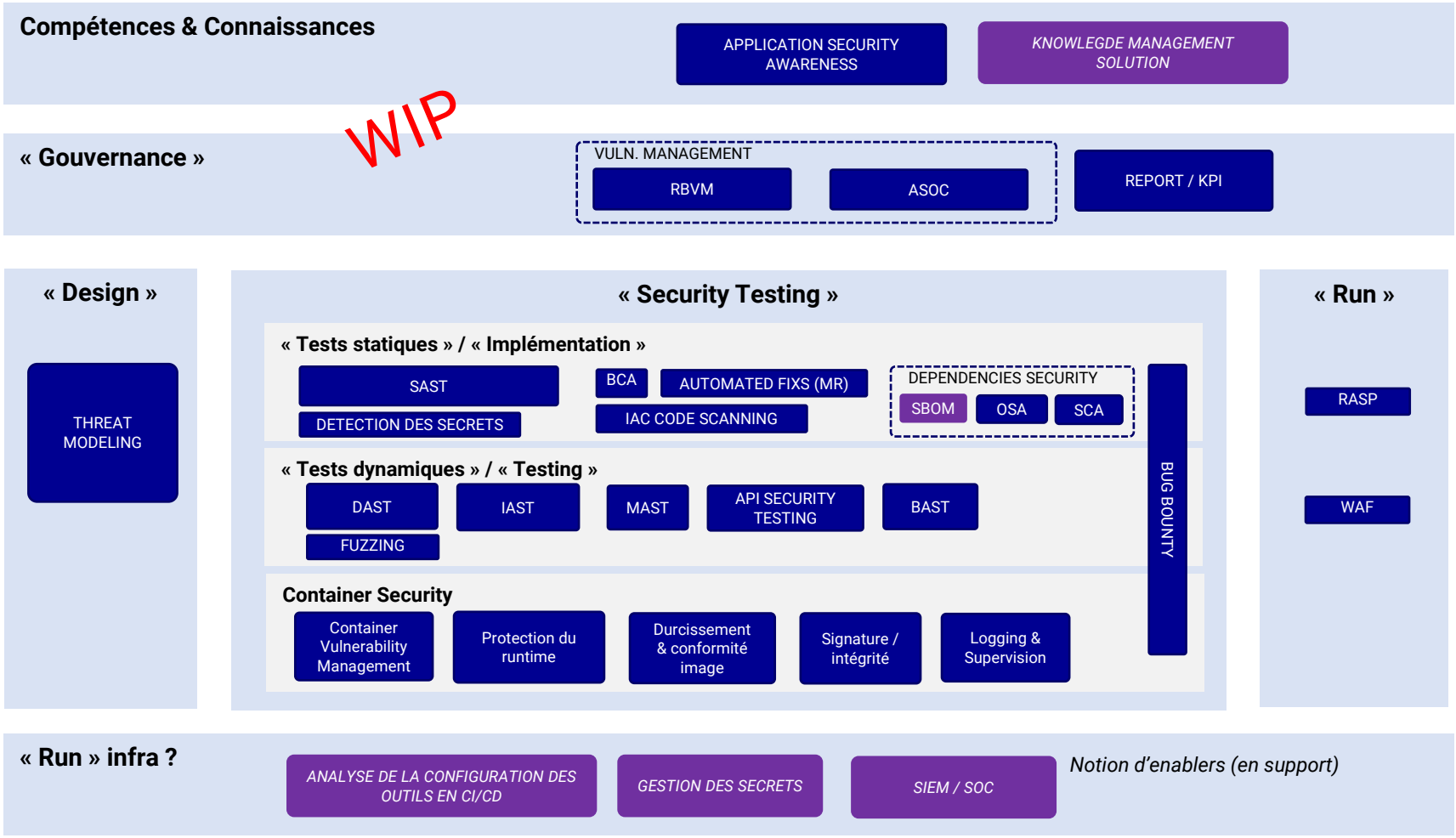
  Retours d'expérience, apports et potentielles contraintes pour chaque technologie

  Questionnements particuliers et orientations

  Priorités dans une optique de montée en maturité technologique

05. PRESENTATION LIVRABLE TECHNOLOGIES.

Cartographie des technologies étudiées



07. DES QUESTIONS ?


CAMPUS
CYBER