Security Champions

La 1ere ligne de défense

Gabriel GOURRAT
Ancien DEV, Ancien OPS
-> DevOps + SC

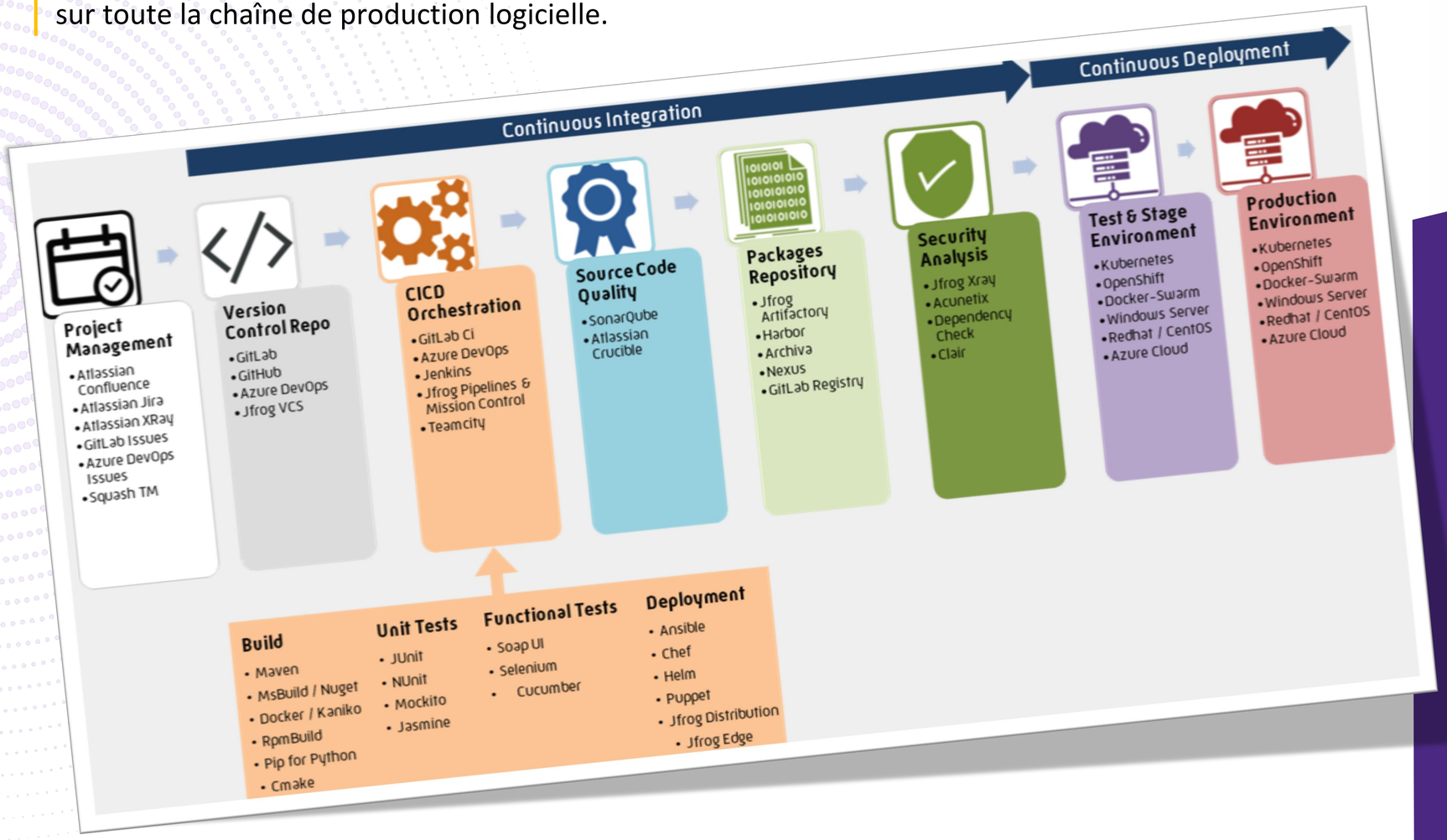
SCALIAN

SOMMAIRE

1. Contexte

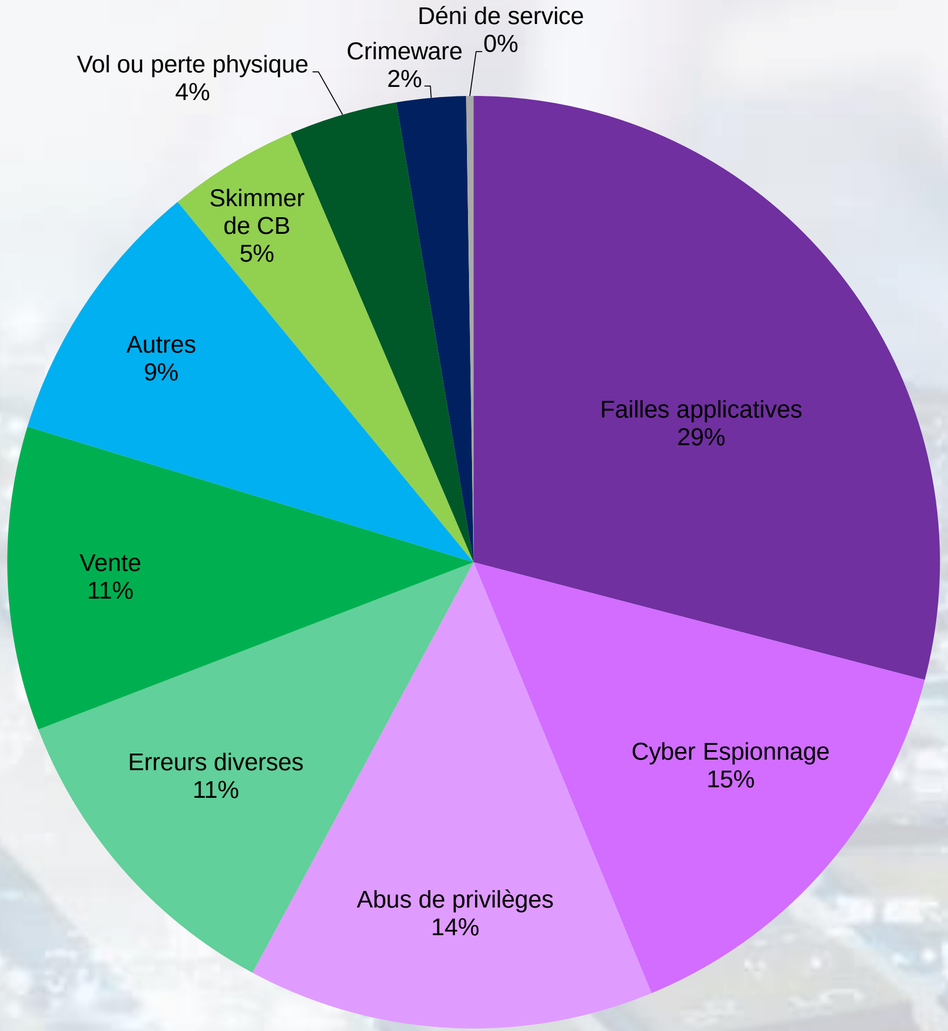
1.1 Notre vision du DEVOPS

Notre ambition : développer le DevOps sur Toulouse
Affirmer notre identité d'expert, faire la promotion de nos atouts auprès de nos clients afin d'offrir un service complet et de haute qualité sur toute la chaîne de production logicielle.



Collaboration entre les centres d'excellence DevOps et Sécurité de Rennes et Toulouse pour un améliorer notre réactivité et notre support, mais aussi dans une volonté d'amélioration continue interne.

1.2 Pourquoi faut il intégrer la sécurité ?



Sources de violation de données 2017, rapport Verizon

67%

Entreprises victimes de Cyber-attaques en 2019

59%

Entreprises impactées par des cyber-attaques

½

Entreprise piratée à son insu

Risques

- Pertes/Vol de données sensibles ou personnelles (RGPD, CNIL)
- Pertes financières
- Rupture de service
- Décrédibilisation de l'entreprise
- Fuite des utilisateurs
- Utilisation du SI comme machine zombie
- Placement publicitaire

Plus de détails sur OWASP

1.3 LES PHRASES RÉCURRENTES

Les développeurs ne sont pas ou peu formés aux bonnes pratiques en matière de sécurité

Les développeurs ne sont pas toujours correctement informés des politiques de sécurité de l'entreprise et de ses changements

L'équipe sécurité n'a pas de temps à consacrer à la formation des équipes de développement, ni à vérifier le code

NOUS N'AVONS PAS LE TEMPS POUR FAIRE DE LA SECURITÉ !!
(worst argument ever)

Le métier n'a pas toujours conscience de l'impact d'une feature sur la sécurité de l'application et, par extension, de l'entreprise

L'équipe sécurité n'est pas toujours consciente des contraintes des développeurs, notamment celle de Time to market

Le métier n'est pas toujours informé de l'impact d'une mesure de sécurité sur la valeur de l'application (utilisabilité, performance)

2.Security Champions

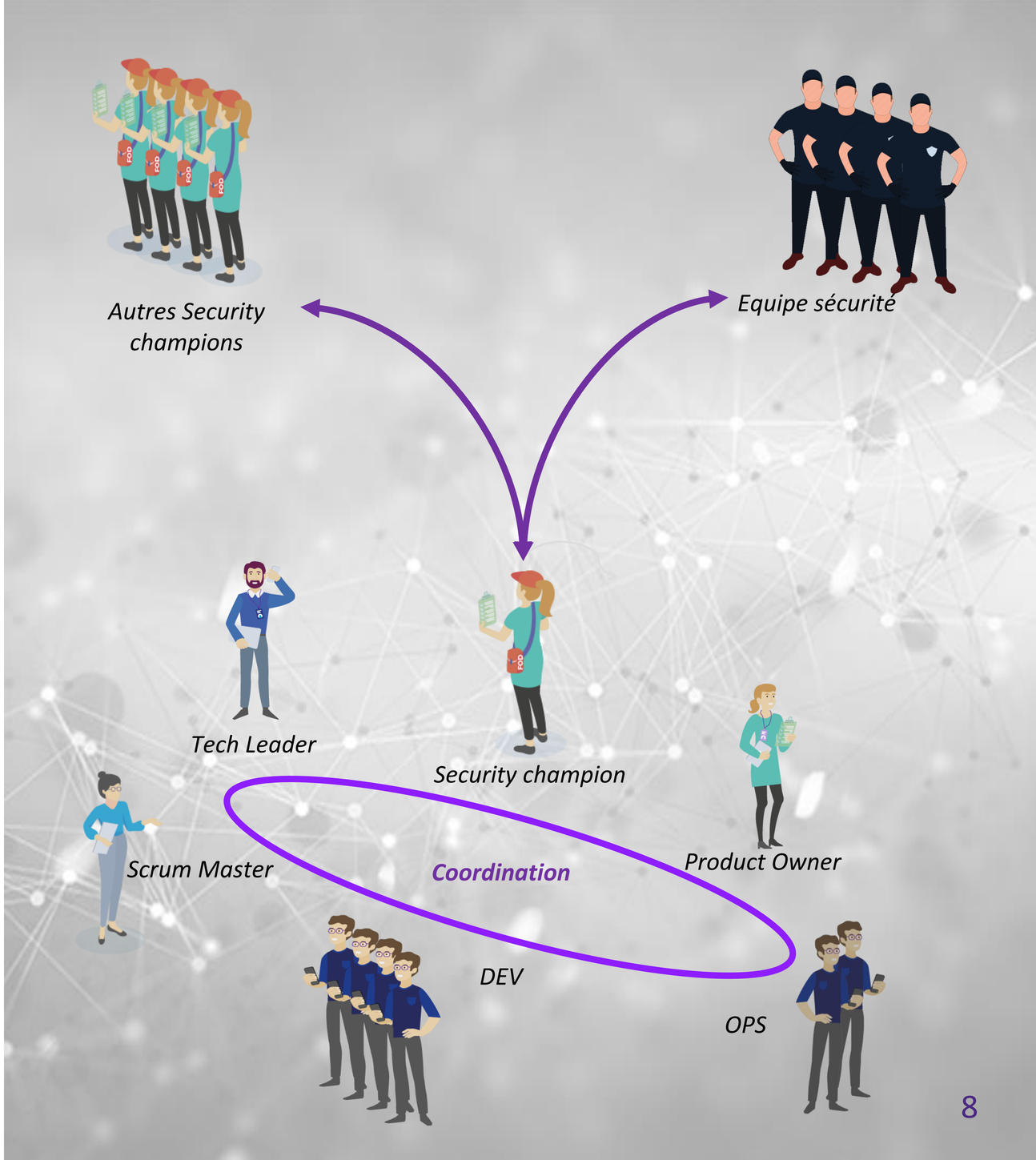
2.1 QU’EST-CE ?

Membre d’une équipe de développement qui prend la responsabilité des questions de sécurité applicative

- Intermédiaire et Facilitateur (comme le Scrum Master)
- Rôle Technique (comme le Technical Leader)
- Périmètre d’action : cycle de développement

- Interface entre l’équipe de développement, le métier, les autres Security Champions et l’équipe sécurité mais il est avant tout un porte-parole, un guide et un informateur.

- Minimum 1 par équipe projet, variable
- 50% de son temps (au-delà ajustez le curseur)
- Mutualisation multi-projets déconseillée



2.2 OBJECTIFS

Garantir le respect des politiques de sécurité et des bonnes pratiques lors des développements

Analyser les vulnérabilités et failles potentielles de l'application

Étudier les risques et prendre des décisions

Transmettre les messages relatifs à la sécurité

EN TANT QU'INTERMÉDIAIRE ET FACILITATEUR

- Remonter les questions de sécurité à l'équipe sécurité
- Informer le métier de l'impact que peut avoir une mesure de sécurité sur le produit (utilisabilité, performance, …)
- Organiser des points hebdomadaires avec l'équipe sécurité et les autres Security Champions
- Transmettre les messages importants relatifs à la politique de l'entreprise aux développeurs
- Transmettre les contraintes développement aux équipes métier et sécurité

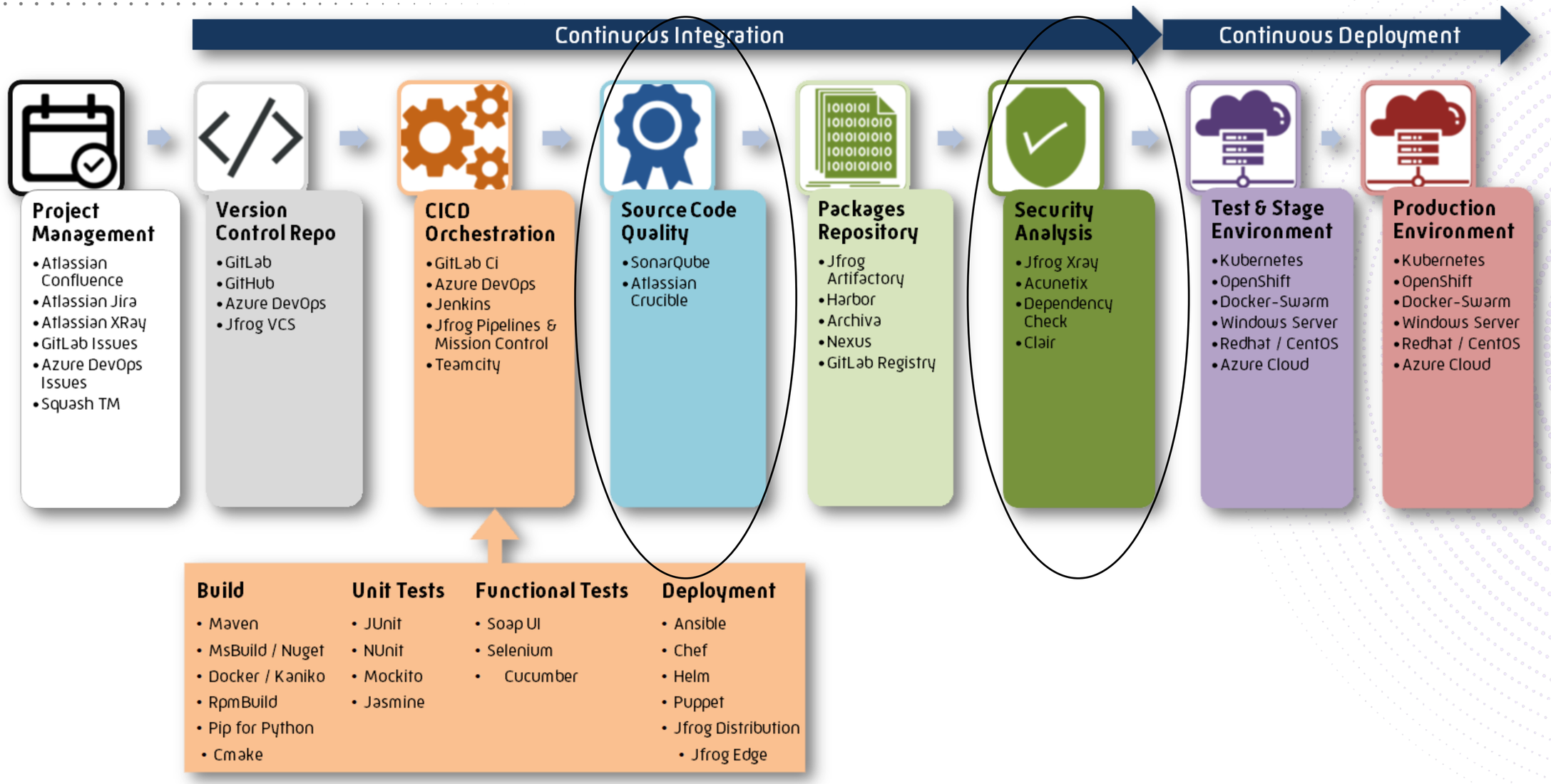
EN TANT QUE COACH SÉCURITÉ APPLICATIVE

- Insuffler un esprit "sécurité" à l'équipe en partageant de bonnes pratiques et les pièges à éviter
- Répondre aux questions sécurité de faible ou moyenne criticités
- Participer aux revues de code
- Analyser les résultats des outils de sécurité mis en place dans la CICD

EN TANT QUE GARANT DE LA SÉCURITÉ DE L'APPLICATION

- Rendre des comptes à l'équipe sécurité sur les décisions prises et les problèmes rencontrés
- Prendre des décisions au sein de son équipe sur les questions de sécurité
- Etablir les exigences de sécurité minimum en collaboration avec le métier et l'équipe sécurité
- Participer à l'élaboration du backlog pour prioriser correctement les différentes tâches relatives à la sécurité (selon les objectifs du métier)
- Participer à la rédaction de la documentation, en particulier sur les décisions de sécurité

2.4 QUELS OUTILS ?



3. REX

2.3 QUEL PROFIL ?

Bonne connaissance de l'application

Connaissances techniques de sécurité de base*

Curieux

Pas d'autre rôle majeur (ex.: Tech Lead)

Pas un expert sécurité

VOLONTAIRE

Dynamique

Ouvert d'esprit

Capacité à se mettre à la place d'un être malveillant

Pas d'enjeux opposés (ex.: OPS)

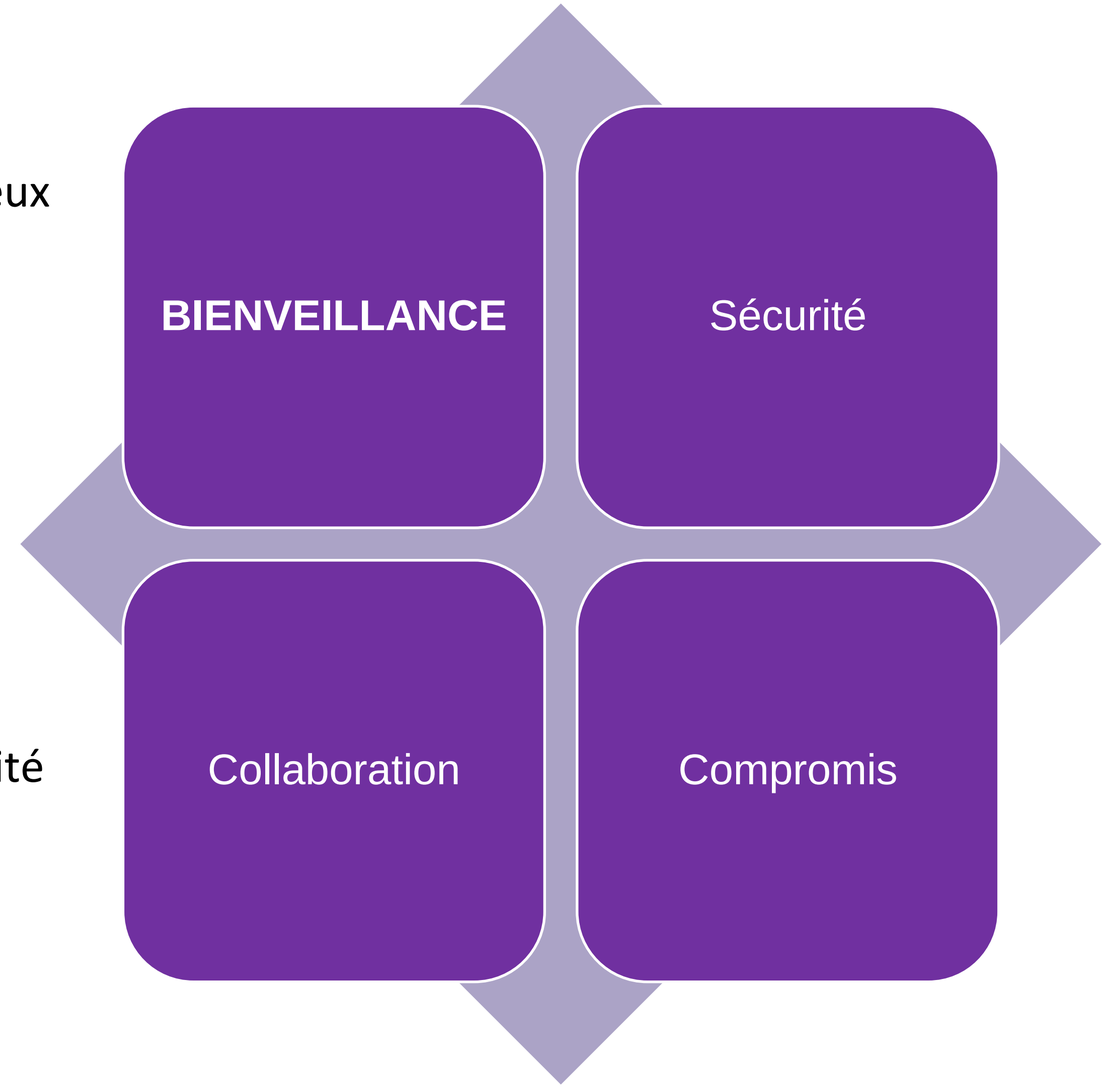
Communicant

Environnement technique

*Connaissances techniques de sécurité de base acquises par :
- Programme de formation
- Coaching par un expert en sécurité informatique présent au niveau de l'entreprise
- Communauté de Security Champions permettant l'entraide et l'autoformation.

2.4 UN BON SECURITY CHAMPION ?

- ✓ Compréhension des enjeux
- ✓ Climat de confiance
- ✓ Motivation
- ✓ Amélioration Continue



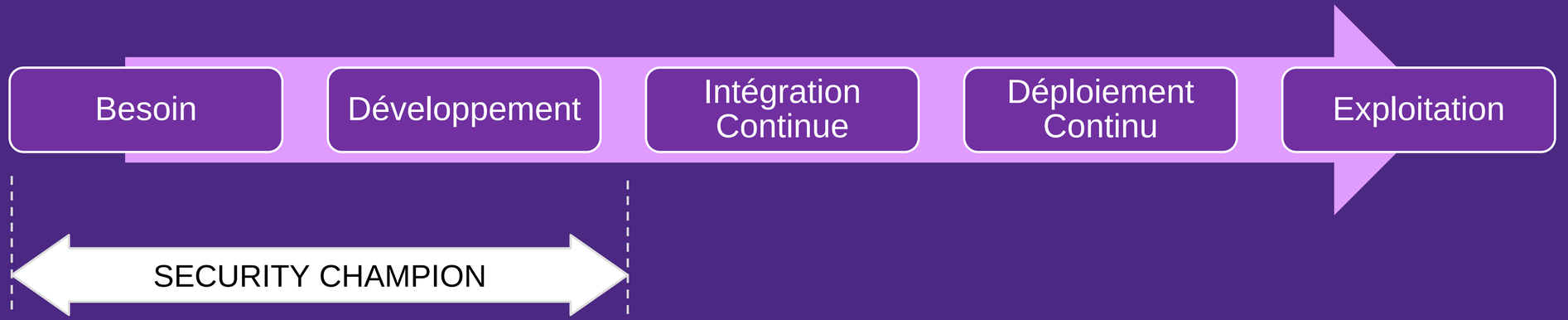
- ✓ Fiabilité
- ✓ Protection
- ✓ Moins d’astreintes

- ✓ Partage des avis
- ✓ Sensibilisation à la sécurité
- ✓ Pas de décisions solo

- ✓ Cohésion d’équipes
- ✓ Accord amiable
- ✓ Décision multilatérale

Un 1er pas vers le DevSecOps ?

OUI MAIS …



NE REMPLACE PAS UNE ÉQUIPE SÉCURITÉ

SCALIAN