#capabilitybuilding

#StrategicWorkforcePlanning

Beijaflore

Organisation CYBER pour une société 2.0

Plus de visibilité	Valoriser le travail de l'équipe face à une forte demande
Plus d'impact	Adopter une approche service business en pleine transfo
Plus d'efficacité	Optimiser la capacité humaine dans un marché de pénurie

Public

SOMMAIRE

Modèles observés

- Grandes entreprises
- Exposition forte de l'équipe sécurité
- Secteurs : Banque, Assurance, Luxe, Energie, Pharmacie, Médias, Transport, Logistique, Manufacturing, Aerospace, Defense.
- Localisations : France, Singapour, USA

Quelques constats

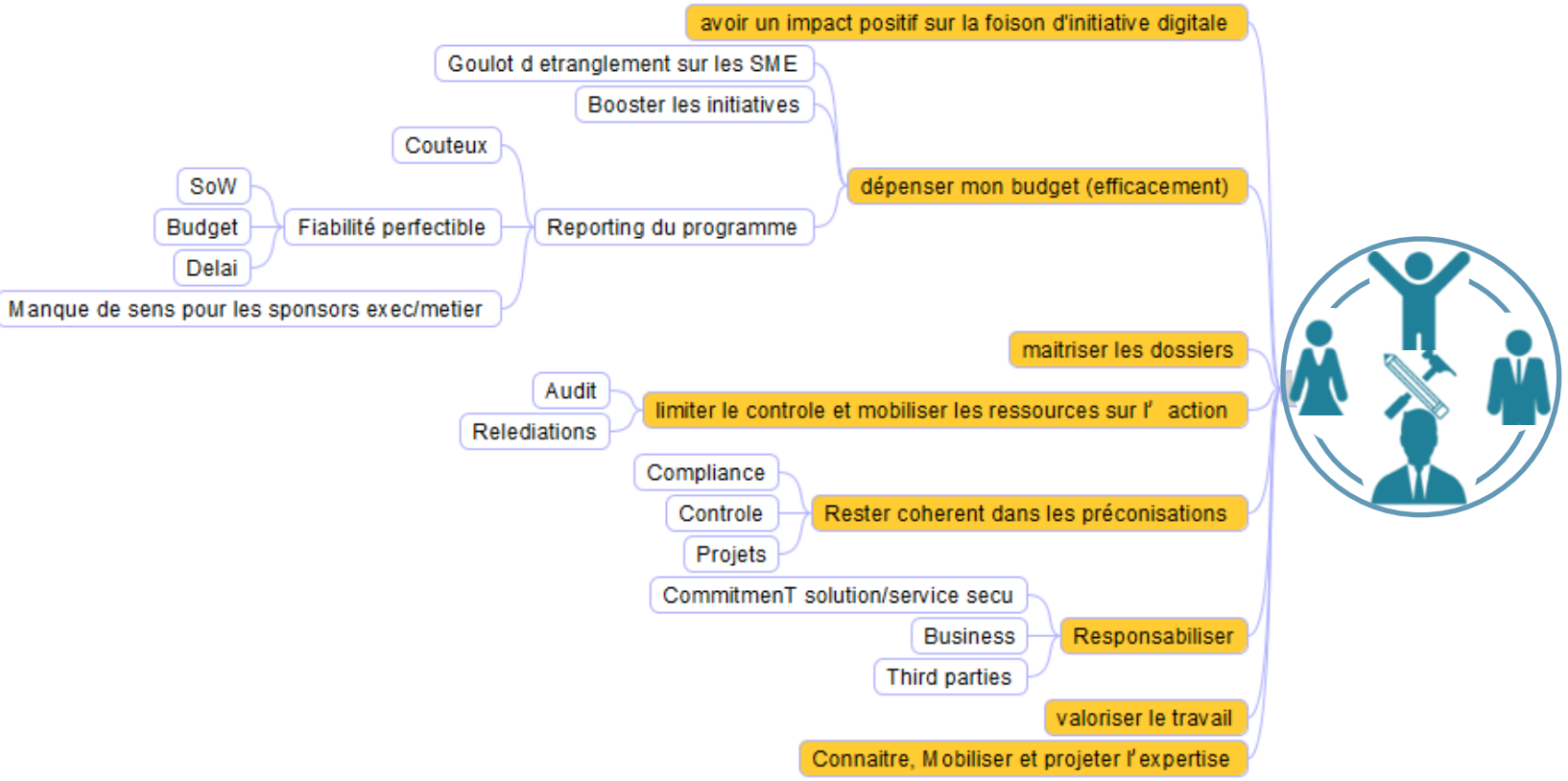
- La compromission est certaine
  - Plus de digital = plus d'attrait pour les mafias et les états + des assets plus exposés
  - Arsenal numérique facilement accessible
  - Impacts énormes sur nos entreprises, la santé des personnes, nos pays
  - Les capacités de détection/réaction doivent se développer → besoin d experts

- Les experts sont trop rares
  - Pénurie = tension sur le recrutement + tension sur la fidélisation
- Et ne produisent pas toujours de l'expertise
  - Temps consacré à d'autre tâches : Pédagogie perfectible, intérêt pour le business limité, mauvais chefs de projet
  - Au détriment du maintien à jour de leurs compétences

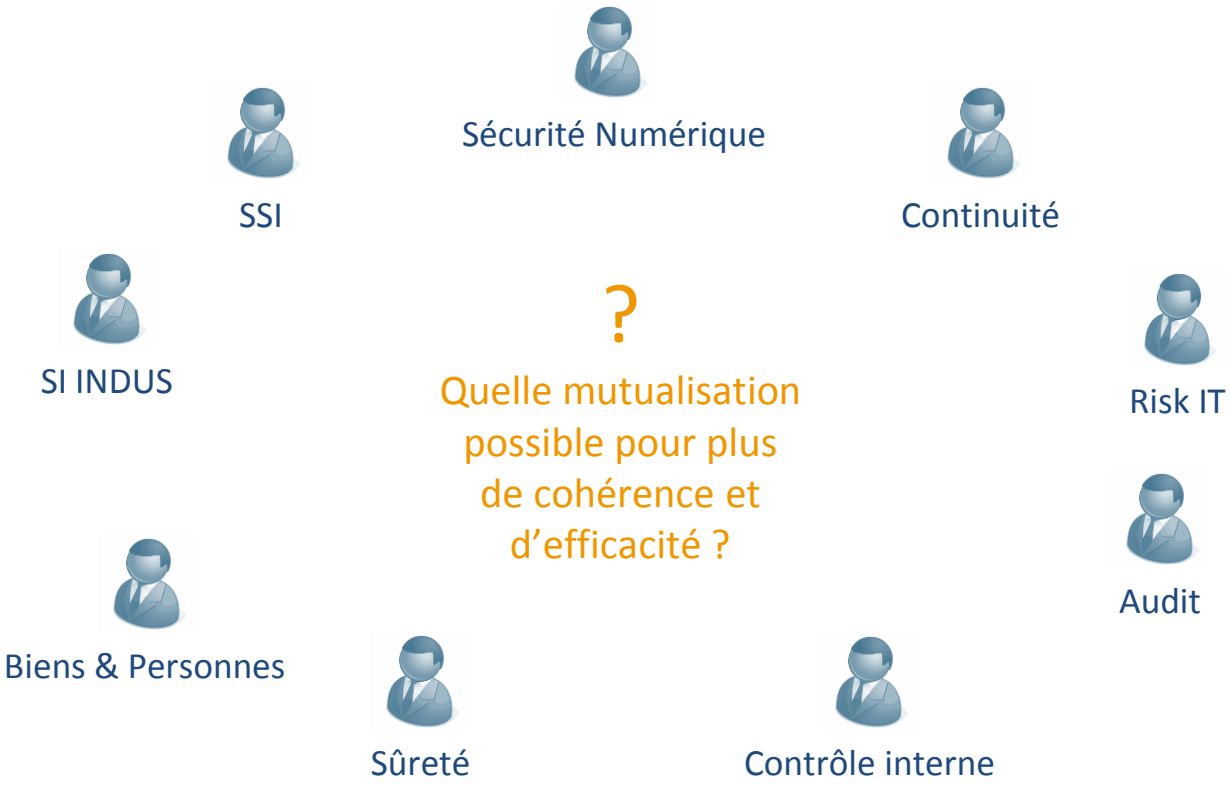
- La transformation numérique porte une dimension RH
  - + cloud = - IT admin et - CDP IT
  - + d IA = - de tâches simples

La question qui se pose : comment ?

accompagner la digitalisation de l'entreprise (croissance des besoins sécurité) et la nécessaire reconversion de ses collaborateurs



Les acteurs de l'écosystème Sécurité sont nombreux mais avec des **approches** et **domaines d'expertise voisins**



Le modèle organisationnel proposé actionne 3 leviers d'excellence opérationnelle

Le développement d'une relation de qualité par la **proximité** avec les **métiers** dans un contexte d'exposition croissante

[Multiplication des menaces liées à la digitalisation et des initiatives cyber impliquant les métiers]

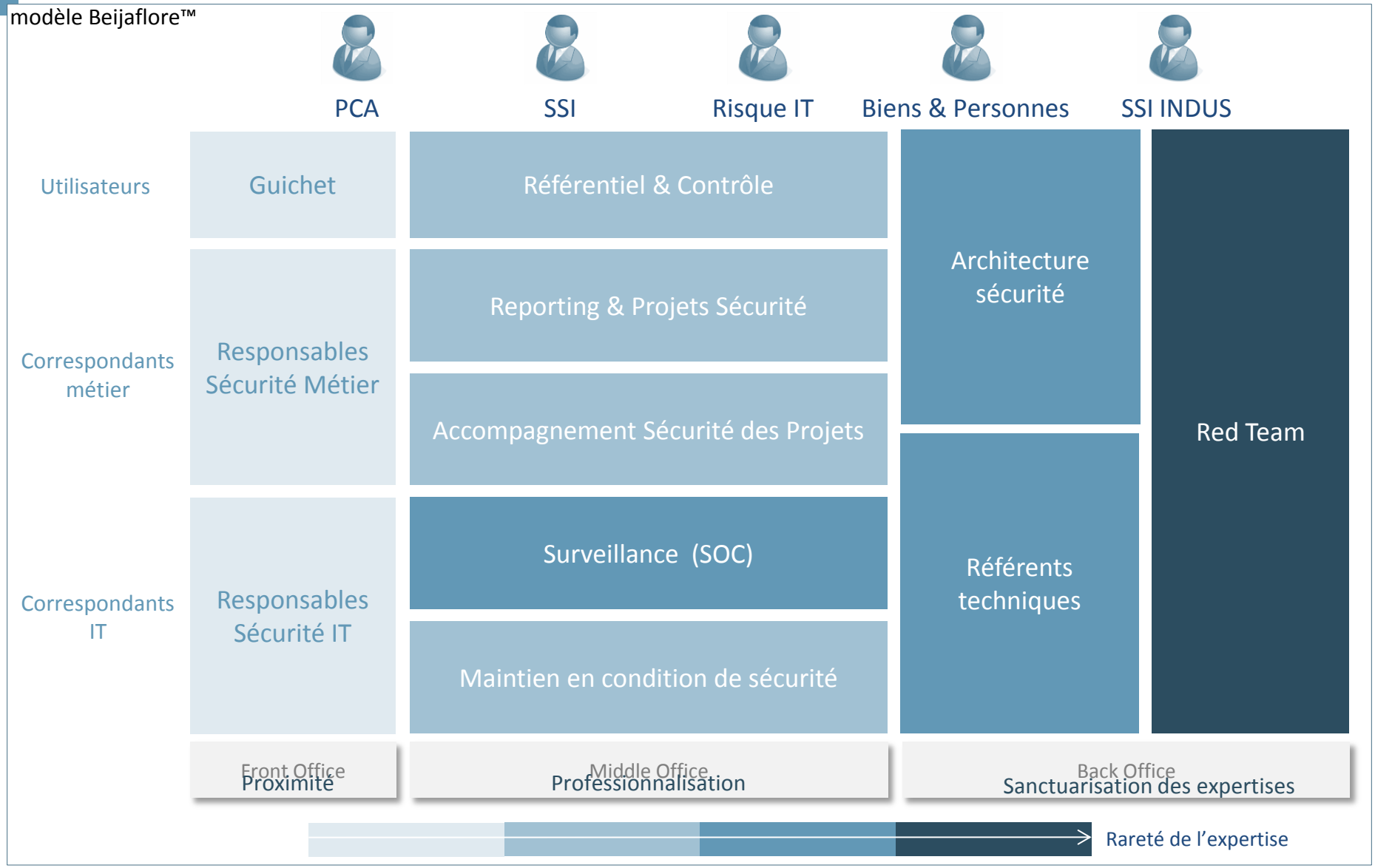
La **professionnalisation** des **activités** et la **responsabilisation verticale** permet une grande efficacité opérationnelle sur l'ensemble des sujets sécurité

[Croissance des équipes cyber plus lente que la croissance du volume d'activité]

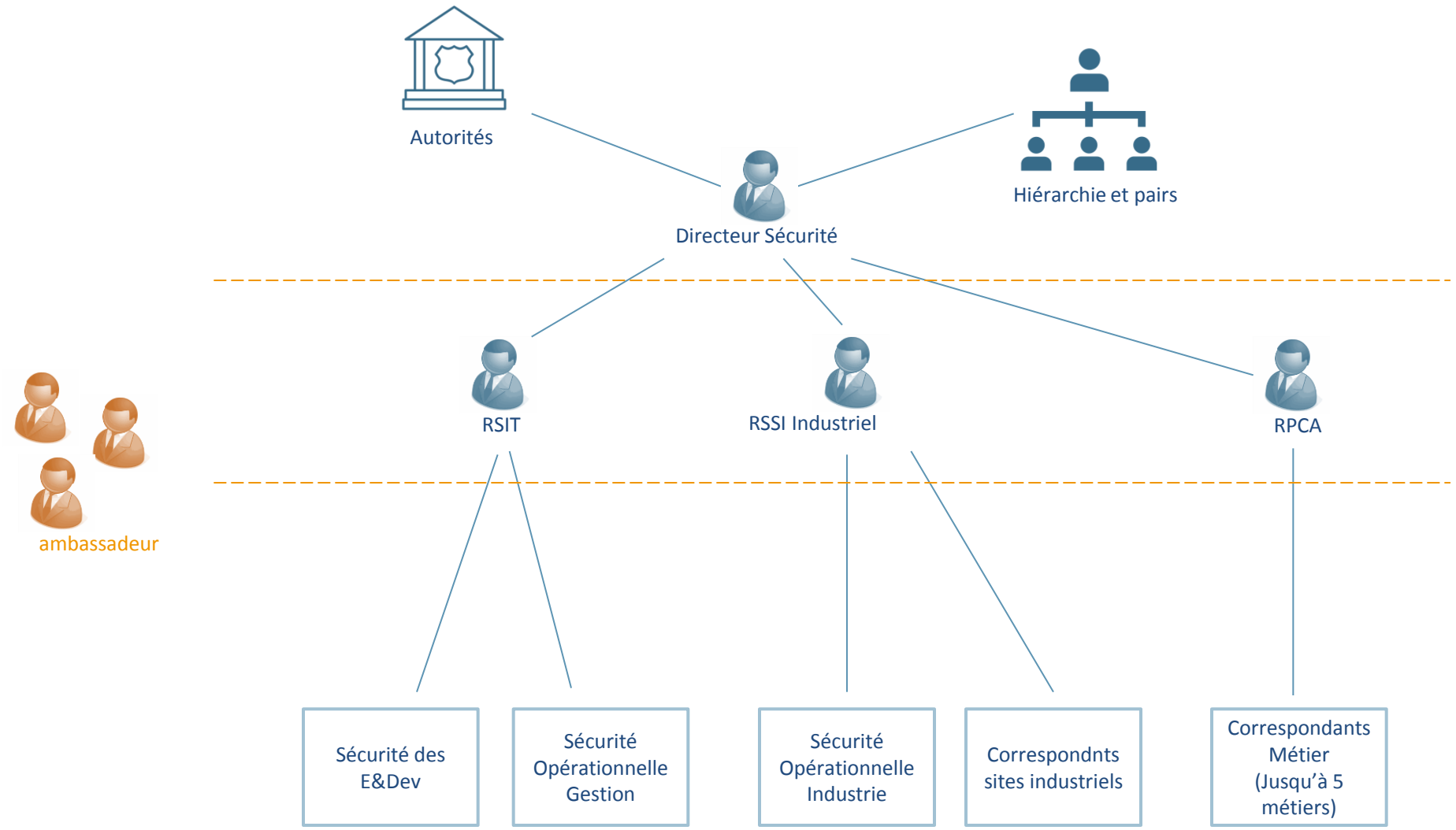
L'impératif besoin de **diversifier** les **sources de recrutement** dans un contexte de pénurie d'experts facilitée par la reconversion des internes impactés par l'hybridation du SI

[Difficulté à croître et sur-sollicitation des équipes]

Le modèle Beijaflore consolide les meilleures pratiques d'organisation observées dans les grands groupes



Gouvernance - La supervision du Front Office (relais métier et IT) est assurée par les RSSI industriels, IT et le RPCA par exemple



La spécialisation des activités permet une grande efficacité opérationnelle et fidélise les profils les plus experts


PCA


SSI


Risque IT


Biens & Personnes


SSI INDUS

Guichet
Réponse aux demandes standard et redirection des autres

Responsable Sécurité Métier
Sensibilisation à destination des métiers
Analyse des risques
Coordination projets
Avancée des dossiers sécurité
Animation de la gouvernance

Responsable Sécurité IT
Sensibilisation à destination de la DSI
Analyse des risques
Coordination projets
Interface incidents
Gestion de la MOE
Avancée des dossiers sécurité
Animation de la gouvernance

Référentiel & Contrôle
Définition du cadre, des politiques et procédures opérationnelles
Elaboration et maintenance des catalogues (risques, incidents, solutions)
Pilotage des contrôles

Communication & Projets Sécurité
Pilotage des programmes/projets, plans de remédiation
Conduite du changement
Gestion des budgets
Consolidation des reportings et communication

Accompagnement Sécurité des Projets
Élargie à continuité, data privacy, risque IT…

Sécurité Opérationnelle
Surveillance (SOC)
SOC/CERT : veille, scans de vulnérabilités, audit, incident, DLP, SIEM, plans de contrôle / Reporting

Maintien en condition de sécurité
MOE Sécurité (config outils sécurité dont les use cases, config sécurité des systèmes et middleware, provisionning des droits, certificats et règles d'accès), Gestion du patch management, librairies/framework dev sécurisé

Architecture sécurité
Définition des architectures techniques sécurisées
Construction de catalogues solution

Référents techniques
Apport d'expertise sur les grands projets de sécurité (IAM, SOC, Crypto, Sûreté)
Etats de l'art
Expressions de besoins

Red Team
Tests d'intrusion, Reverse, Forensics,
Avis techniques de sécurité

Cette organisation diversifie les sources de recrutement dans un contexte de pénurie d'experts et facilite les reconversions

PCA | SSI | Risque IT | Biens & Personnes | SI INDUS

Guichet
Correspondants bureautiques

Responsable Sécurité Métier
MOA ou Responsables de processus métier

Responsable Sécurité IT
Managers IT (E &Dev ou Prod)

Référentiel & Contrôle
Qualiticiens
Contrôleurs

Communication & Projets Sécurité
Chef de Projet
Consultant

Accompagnement Sécurité des Projets
Business Analysts

Surveillance (SOC)
Techniciens/ingénieurs de production IT

Sécurité Opérationnelle

Maintien en condition de sécurité
Développeurs ou Ingénieurs de production IT

Architecture sécurité
Architectes systèmes & réseaux

Référents techniques

Red Team

Seuls deux types de profils doivent justifier d'une grande expérience en Sécurité SI

Les formations d'expertise sont concentrées sur la moitié des métiers, un vernis suffit pour les autres

Guichet
Initié

Référentiel & Contrôle
Initié

Architecture sécurité
Confirmé

Red Team
Expert

Responsable Sécurité Métier
Initié

Communication & Projets Sécurité
Initié

Accompagnement Sécurité des Projets
Confirmé

Responsable Sécurité IT
Initié

Surveillance (SOC)

Sécurité Opérationnelle
Confirmé

Maintien en condition de sécurité

Référents techniques
Expert

Les activités de chaque rôle sont regroupées par pool de compétences (connaissances, savoir-faire, savoir-être)

Guichet
Réponse aux demandes standard et redirection des autres

Responsable Sécurité métier
Bonne connaissance de l'entreprise : réseaux de personnes, operating model, business model

Responsable Sécurité informatique
Education, sensibilisation, analyse des risques
Avancée des dossiers sécurité
Assurer la cohérence

Gouvernance & Contrôle
Définition et maintien du cadre : organisation, comités, politique, procédures, catalogues
Pilotage des contrôles

Accompagnement sécurité des projets

Communication & projets sécurité
Pilotage des programmes/projets, plans de remédiation (PMO)
Nb: Input fourni par les SME
Consolidation des reportings et communications

Surveillance
SOC/CERT : veille, scans de vulnérabilités, audit, incident, DLP, SIEM

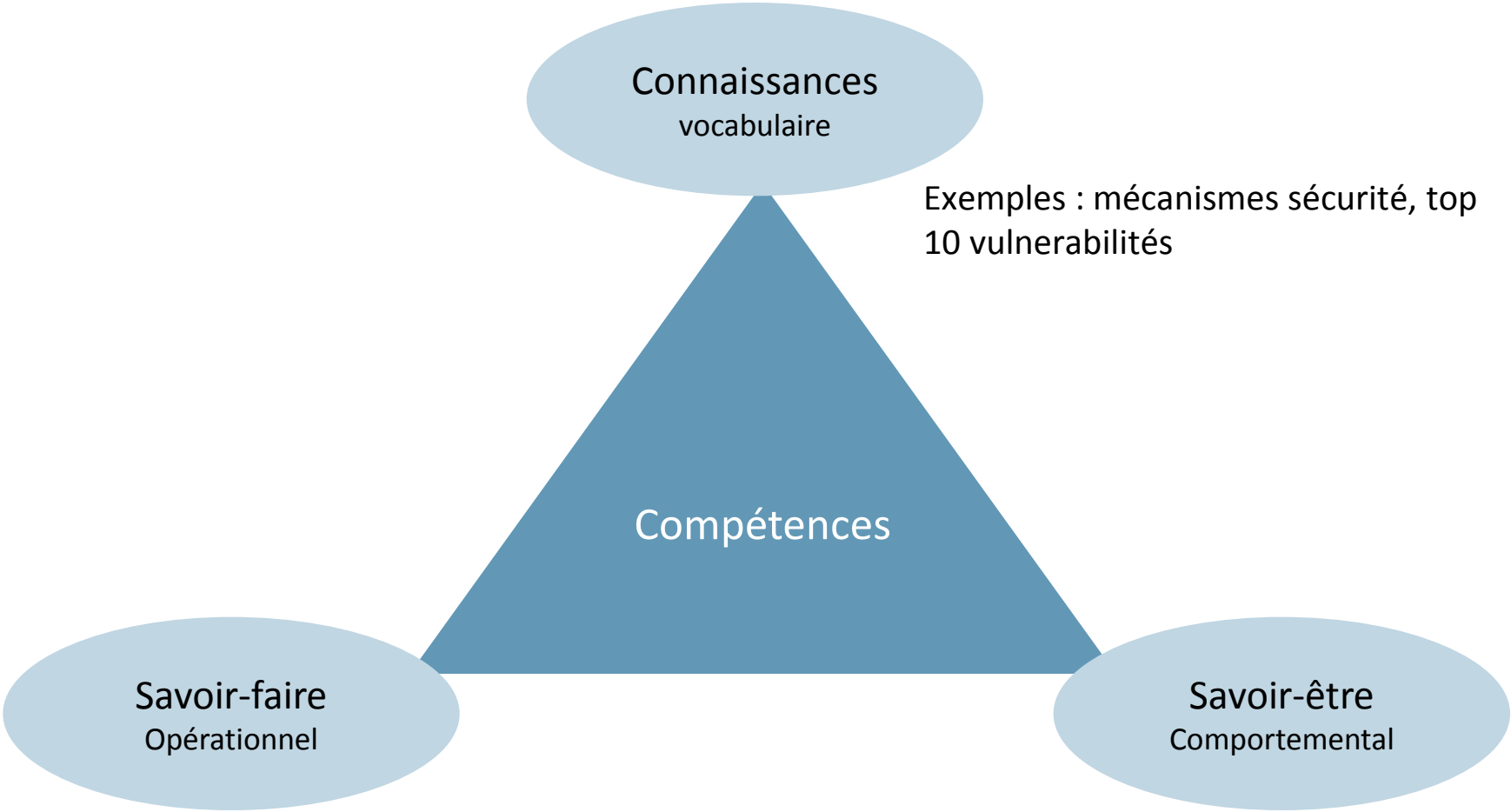
Maintien en condition de sécurité
MOE Sécurité
Patch management…

Architecture sécurité
Définition des architectures techniques sécurisées

SME
Experts IAM, SOC, crypto…
Apport d'expertise sur les grands projets de sécurité
Expressions de besoins

RED Team
Support niveau 3
Tests d'intrusion, Reverse, Forensic
Avis techniques de sécurité
Etudes
Courtes périodes de prestation (5 à 10 jours)

Les compétences métier sont réparties sur 3 axes principaux



Exemples : mécanismes sécurité, top 10 vulnerabilités

Exemples :
- Evaluation du risque
- Audit & Revue

Exemples :
- Communication écrite
- Analyse de problème

Les compétences requises pour chaque métier sont identifiées

Expertise/discipline = Savoir-faire & Connaissances

	Familles de compétences :	Métiers :	Accompagnement Sécurité des Projets et Architectes	Surveillance (SOC) et Maintien en Condition de Sécurité (MCS)	Risque IT
Savoir-faire & Connaissance	Gestion de la Sécurité de l'Information	A1 - Gouvernance			
		A2 - Politique et Standards	2		
		A3 – Stratégie de la Sécurité de l'Information			1
		A4 – Innovation & Amélioration Métier			1
		A5 – Sensibilisation et Formation à la Sécurité de l'Information			
		A6 – Environnement Légal et Réglementaire			1
		A7 – Gestion des Tierce-Parties			
	Gestion du Risque IT	B1 – Evaluation du Risque	1		1
		B2 – Gestion du Risque	2		1
	Implémentation de Systèmes Sécurisés	C1 – Architecture Sécurité	2	2	
		C2 - Développement Sécurisé	2		
	Méthodologies de Protection de l'Information et Test	D1 – Méthodologies de Protection de l'Information	1		1
		D2 – Test Sécurité	2	2	
	Gestion de la Sécurité Opérationnelle	E1 - Gestion Sécurisée des Opérations		1	
		E2 - Opérations Sécurisées & Service		1	
		E3 - Evaluation des Vulnérabilités		1	
	Gestion des incidents	F1 – Gestion des incidents		1	
		F2 – Investigation		1	

Savoir-être

Familles de compétences :	Métiers :	Accompagnement Sécurité des Projets et Architectes	Surveillance (SOC) et Maintien en Condition de Sécurité (MCS)	Risque IT
Communication	1. Communication Orale			1
	2. Présentation orale			
	3. Ecoute	1		2
	4. Persuasion			2
	5. Communication écrite	2		
Influence	6. Flexibilité comportementale			
	7. Leadership de groupe			
	8. Leadership individuel			2
	9. Développement du personnel			
	10. Impact			
	11. Travail d'équipe	1	2	
	12. Sensibilité	2		
	13. Sociabilité		1	1
Management	14. Délégation			
	15. Plannification et Organisation		2	
	16. Organisation d'équipe	2		
Résolution de problèmes	17. Créativité			
	18. Capacité à apprendre	1		2

Exemple : Sécurité opérationnelle (SOC et MCS)

Compétences **primaires**	Compétences **secondaires**
• Gestion Sécurisée des opérations • Opérations Sécurisées & Service • Evaluations des vulnérabilités • Gestion des incidents • Investigation	• Architecture Sécurité • Test Sécurité • Audit & Revue • Gestion de la Continuité d'Activité

Exemple : Sécurité opérationnelle (SOC et MCS)

Compétences **primaires**	Compétences **secondaires**
• Sociabilité • Analyse de problèmes • Ténacité	• Travail d'équipe • Plannification & Organisation • Energie • Initiative • Attention aux détails • Résistance au stress

- Les compétences **primaires** sont requises chez chacun des membres de l'équipe
- Les compétences **secondaires** sont requises chez au moins un membre de l'équipe

Les certifications requises pour chaque métier permettent de faciliter l'évaluation et la formation des experts tout en les valorisant

Métier	Organisation	Certification	Détail	À l'embauche	Cycle 1	Cycle 2	Cycle 3
RSSI	ISO	ISO 27005	Risk Manager	Primaire			
	ISO	ISO 27001	Lead Implementer	Primaire			
RPCASI	ISO	ISO 22301	Lead Implementer	Primaire			
Risque IT	ISO	ISO 27005	Risk Manager	Primaire			
	ISACA	CRISC (Risk and Inf. System Control) ou	Risk and Information Systems Control	Primaire			
	ISO	ISO 31000	Risk Manager	Primaire			
Architectes	SANS	Architectes techniques : SEC 401	GSEC : GIAC (Global Information Assurance Certification) Security Essentials		Primaire		
	ISC2	Architectes fonctionnels : CISSP - ISSAP	Information Systems Security Architecture Professional		Primaire		
	SANS	SEC 579	SEC 579 : Virtualisation and Private Cloud Security			Secondaire	
	SANS	SEC 566	Implementing and Auditing the Critical Security Controls - In depth (GCCC)			Secondaire	
	ISC2	CISSP	Certified Information Systems Security Professional				Primaire
Accompagnement Sécurité des	ISO	ISO 27005	Risk Manager	Primaire			
	SANS	SEC 401	GSEC : GIAC (Global Information Assurance Certification) Security Essentials	Optionnel			
	SANS	SEC 560	Network Penetration Testing and Ethical Hacking (GPEN)	Secondaire			
SOC (SECOP)	SANS	SEC 504	Hacker Tools, Techniques, Exploit, & Incident Handling (GCIH)	Primaire			
	SANS	SEC 501	Advanced Security Essentials - Enterprise Defender (GCED)	Optionnel			
	SANS	SEC 502	Perimeter Detection In-Depth (GPPA)	Optionnel			
	SANS	SEC 503	Intrusion Detection In-Depth (GCIA)	Optionnel			
	SANS	SEC 511	Continuous Monitoring and Security Operations (GMON)	Optionnel			
MCS (SECOP)	SANS	SEC 401	GSEC : GIAC (Global Information Assurance Certification) Security Essentials	Primaire			
	SANS	SEC 505	Securing Windows with PowerShell and the Critical Security Controls (GCWN)			Primaire	
	SANS	SEC 579	Virtualisation and Private Cloud Security			Primaire	

- Les certifications **primaires** sont requises chez chacun des membres de l'équipe
- Les certifications **secondaires** sont requises chez au moins un membre de l'équipe

Notre processus d'évaluation est adapté à l'ensemble des compétences : connaissances, savoir-faire, savoir-être

Les savoir-être sont évalués au cours d'un entretien via un questionnement ciblé pour chaque compétence-clé

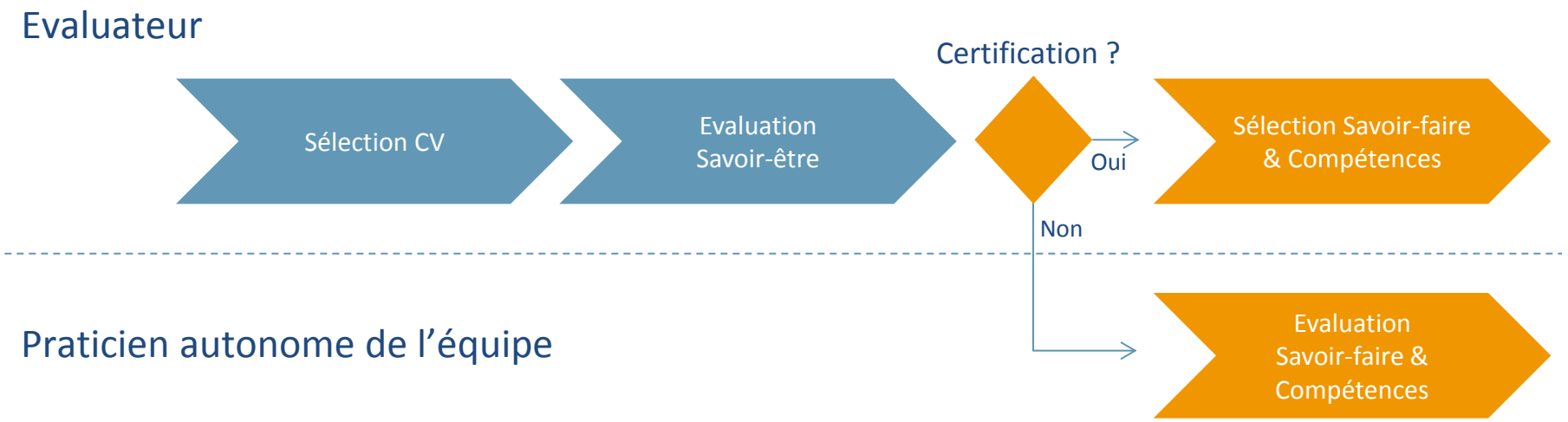
→ Des questions-types pour chaque compétence sont proposées par Beijaflore

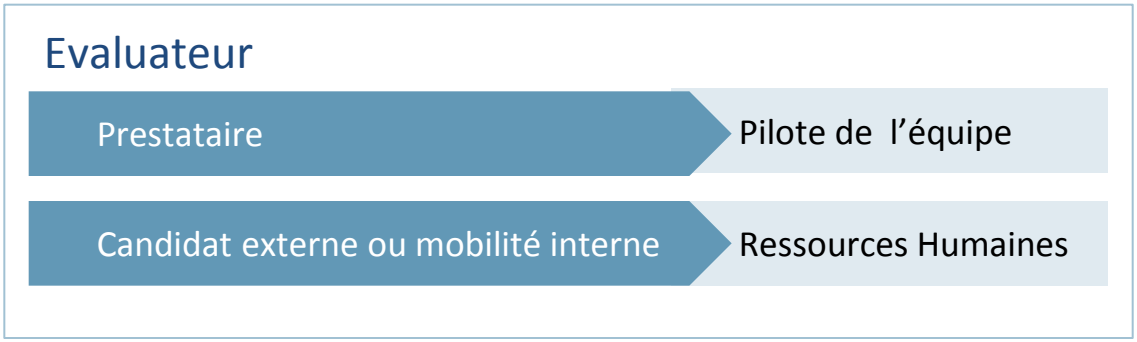
L'expertise est évaluée

- Profils initiés : maîtrise du vocabulaire sur les fondamentaux et mini cas avec alternative → QCM
- Profils confirmés et experts : QCM pour les connaissances + cas pratiques pour les savoir-faire lors d'un entretien

→ Les QCM et les cas pratiques sont construits par nos consultants expérimentés en utilisant la base de connaissances de notre CyberAckademy™ et le savoir-faire de Beijaflore

L'évaluation des compétences dans le processus de recrutement est indépendant de l'origine de la ressource





L'échelle d'évaluation est pragmatique et donne une visibilité claire de la marge de progression

★★★★	Expert Capable de transmettre	• Fait autorité • Est reconnu par ses pairs • A démontré la compétences dans des situations nouvelles • Mène des travaux innovants pour développer la compétence
★★★★	Confirmé Pratique en autonomie	• Comprend la compétence et l'applique dans des situations complexes en autonomie • Fait preuve de responsabilité et a un besoin limité d'escalader • Est en veille sur les nouveaux développements liés à la compétence et à son utilisation • Contribue aux développements techniques et nouveaux champs d'application de la compétence
★★★★	Initié Pratique élementaire	• Observé mais avec plusieurs axes d'améliorations • Doit escalader sur les situations complexes • A besoin d'un référent
★★★★	Insuffisant Débute mais n'a pas suffisamment démontré	• Comprend la compétence et son application • A acquis et peut démontrer des connaissances basiques associées à la compétence • Comprend comment la compétence doit être appliquée mais n'a pas d'expérience pratique
★★★★		• N'a rien démontré, non observé

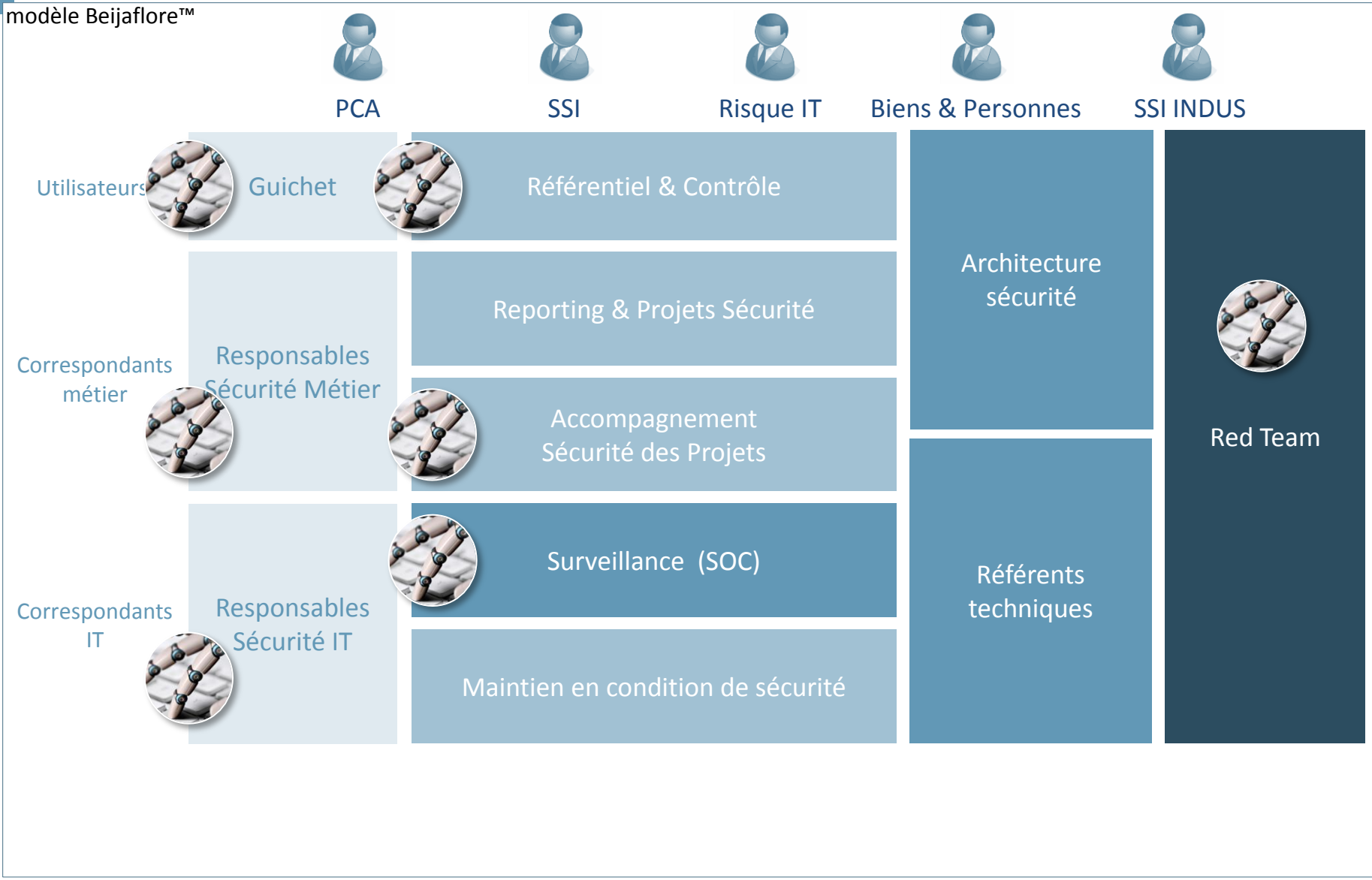
Pour aller plus loin dans le modèle, intégrer l'innovation dans l'organisation du RSSI

Une première étape de robotisation, chatbot

- 30 use case défini par un groupe de 5 RSSI
- 1 démo : ISP Waterfall ou Agile
  - 30% de savings par projet
  - Plus de projets captés
- Déployer une solution digitale pour mieux décloisonner

Comment tirer profit de la robotisation #IA ?

modèle Beijaflore™



MERCI

POUR VOTRE ATTENTION