



BioTech

Mise en place d'une infrastructure sécurisée pour *BioTech*

Présentation

01

Objet du document

02

Plan du projet

03

Contexte

04

Expression de
besoin

05

Architecture
technique

06

Composition de
l'architecture technique

07

Livrable

- Lot 3 : Implémentation de l'infrastructure du système d'information (SI).
- Lot 4 : Axe d'amélioration de l'architecture technique pour réduire les SPOF (Single



01. Objet du document

Le présent document a pour objectif de détailler les besoins spécifiques de la société BioTech dans le cadre de l'appel d'offres relatif à la mise à disposition d'une infrastructure ultra-sécurisée et résiliente, afin de traiter les données particulièrement sensibles et critiques.

Les jalons de ce projet sont les suivants :

- Lot 1 : Organisation du projet qui sera présenté au RSSI tout le long du projet ;
- Lot 2 : Etude et proposition des choix techniques ;
- Lot 3 : Implémentation de l'infrastructure du SI ;
- Lot 4 : Axe d'amélioration de l'architecture technique pour réduire le SPOF ;

01. Objet du document

Les jalons de ce projet sont les suivants :

- Lot 5 : Sécuriser l'infrastructure ;
- Lot 6 : Test fonctionnel ;
- Lot 7 : Pentest de la robustesse de l'infra ;
- Lot 8 : Rédaction des DEX (Document d'exploitation des installation et les configurations) ;
- Lot 9 : Rédaction d'un dossier d'architecture technique (DAT) de la proposition ;
- Lot 10 : Prévoir un budget prévisionnel la réalisation du projet ;
- Lot 11 : Soutenance de la solution technique en comité d'architecture technique ;



BioTech

01. Plan du projet

▪ Objet du document

- Le projet se déroulera tout au long de la durée de la formation.
- La classe sera divisée en plusieurs groupes, chacun composé d'un chef de projet chargé de la conduite des opérations, d'un développeur responsable de la mise à disposition des outils, et d'un ingénieur système en charge du déploiement de la partie technique.
- Les groupes devront présenter et valider la partie technique avant la phase de déploiement.
- Pour implémenter la solution, le chef de projet de chaque groupe sera responsable de remonter l'information au responsable DSI de BioTech ;
- En fonction de l'avancement du projet, les groupes pourront tester d'autres outils afin de capitaliser sur l'expérience (par exemple, tester les puits de logs, la supervision, la sauvegarde, etc.).



03. Contexte

BioTech est une société filiale française spécialisée dans la sécurité numérique, la biométrie, l'identification et l'authentification, ainsi que l'analyse de données et de vidéos.

Elle est composée de plusieurs départements :

- Le site de Paris, qui centralise le traitement des données biométriques, avec un effectif de 1000 personnes.
- Le site de Rennes, dédié à l'administration, incluant les différentes entités (RH, paie, CE, etc.), avec un effectif de 100 salariés.
- Un site non déclaré, par mesure de sécurité, chargé de l'archivage des données très sensibles de BioTech, composé de 50 personnes.

03. Contexte

BioTech a pour priorité de protéger ses données sensibles contre les attaques croissantes. C'est pourquoi elle a lancé un appel d'offres auprès de plusieurs sociétés pour déployer et sécuriser l'ensemble de son infrastructure.

La société en charge de ce projet devra challenger ses choix techniques basés sur des solutions Open Source, afin de répondre aux préoccupations de BioTech.

Le client attend de la part de la société prestataire des propositions d'amélioration pour les points sensibles de l'infrastructure, selon son expression de besoin.

Le RSSI a également demandé la possibilité de réaliser un pentest de l'infrastructure pour garantir sa sécurité.



04. Expression de besoin

BioTech souhaiterait faire évoluer l'ensemble de son infrastructure afin de réduire les coûts. La DSI a demandé la mise en place d'une infrastructure informatique 100 % open source, dans la mesure du possible.

Pour le client, la composition de son infrastructure doit inclure les choix essentiels pour traiter efficacement son activité :

- Installation des socles selon l'état de l'art, avec cloisonnement des systèmes de fichiers ;
- Cloisonnement et chiffrement, si nécessaire, de certaines données sensibles ;
- Mise en place de bases de données sécurisées avec stockage dédié ;
- Sauvegarde régulière des données ;
- Serveurs de fichiers sécurisés ;
- Mise en place de gardes-barrières pour protéger les zones sensibles ;

04. Expression de besoin

- Découpage des zones réseau.
- Annuaire centralisé et redondant pour tracer les connexions internes et externes.
- Outils de surveillance pour une gestion proactive de la sécurité.
- Sécurisation des connexions internes et externes, y compris pour le grand public, afin de permettre le dépôt en ligne de documents administratifs.
- Définition des rôles de connexion pour chaque équipe (Admin, SOC, Admin BDD, Admin Appli).
- Haute disponibilité sur certains composants critiques du SI

04. Expression de besoin

■ Evolution de l'expression des besoins de BioTech

Le client souhaite renforcer son infrastructure afin de sécuriser son patrimoine.

Les sujets ont été évoqués lors du comité technique, et Ynov a validé avec BioTech les besoins exprimés par la DSI :

- Installation des bases sur des volumes dédiés.
- Cloisonnement des serveurs web pour se protéger contre les attaques croissantes.
- Dump de la base de données (BBD) sur un volume chiffré, par mesure de sécurité, sur le site secondaire. L'accès aux données distantes permettra une restauration en cas de cyberattaque.

04. Expression de besoin

■ Évolution de l'expression des besoins de BioTech

- BioTech, ayant dépassé son budget, demande, à court et moyen terme, la mise en place d'un outil rapide pour sauvegarder les bases sensibles selon une fenêtre de sauvegarde quotidienne à 21h00, heure à laquelle le trafic est moins dense. Un script de programmation a été sélectionné pour le POC. La prochaine étape consistera à choisir un ordonnanceur OpenSource pour ce besoin.
- Concernant le dump de la base, un crash test est impérativement requis par BioTech afin de valider la procédure de sauvegarde. Ce test de sauvegarde – restauration devra figurer dans le DEX pour guider les exploitants en cas de récupération des données..

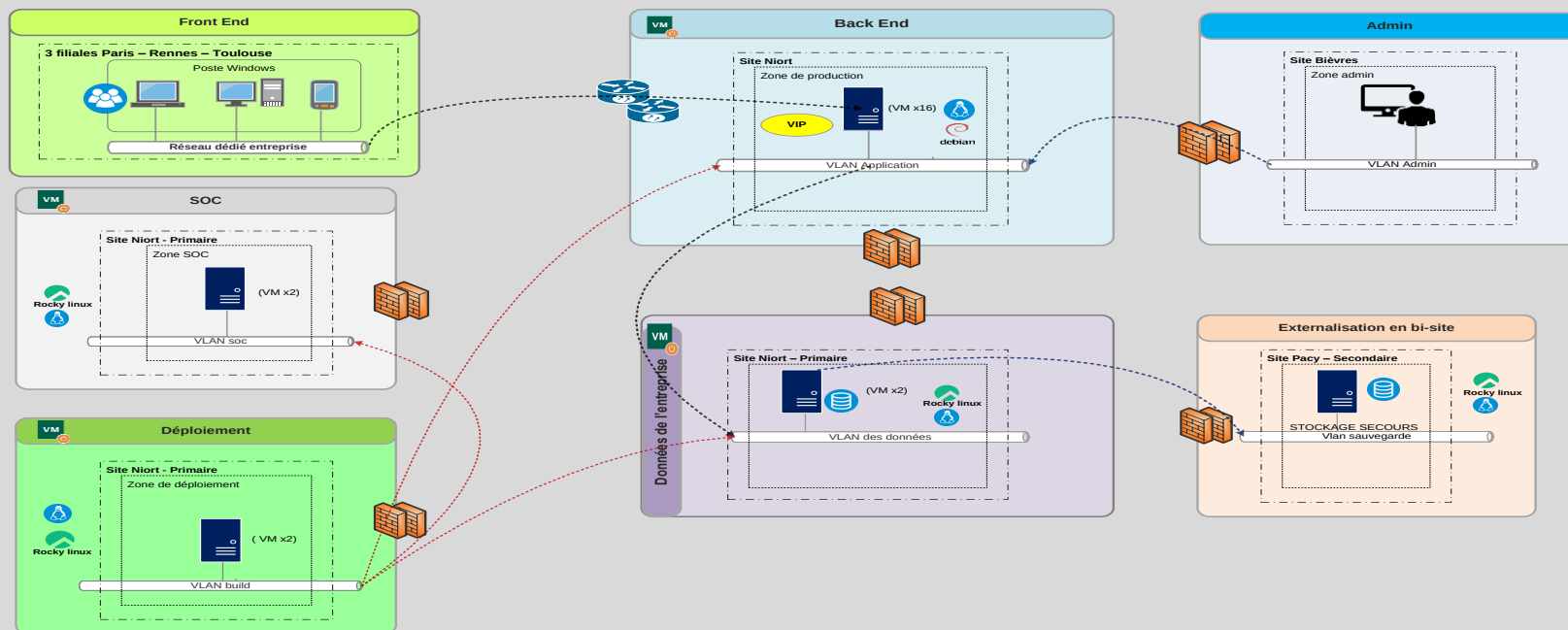
04. Expression de besoin

■ Evolution de l'expression des besoins de BIOTECH

- Sécuriser les connexions HAproxy pour supprimer le SPOF en cas de perte d'un nœud
- Protéger le serveur Web du système en cas d'intrus
- Sauvegarder toutes les données sensibles sur un volume chiffrés (Puit de logs, BDD) à travers un cronfile tous les jours à 21h00 l'heure à laquelle il y a moins de trafic
- L'infra doit disposer d'un environnement de patch Management local et protégé

04. Architecture technique

■ Vue simplifiée de l'architecture simplifié



04. Architecture technique

- L'architecture comprends 17 Vms installées dans différentes zones à travers des VLAN

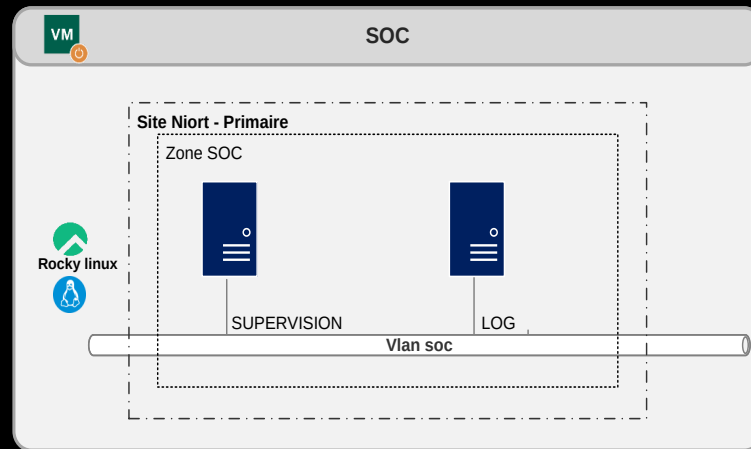
Serveur	Distribution	Rôle	Configuration	Zone
bthngs01p	Rocky	Surveillance	VM	SOC
bthrs01p	Rocky	Collecteur de données	VM	SOC
bthgdc01p	Rocky	Gestion de configuration	VM	DPL
bthpmt01p	Rocky	Patch Management	VM	DPL
bthhpx01p	Debian	Équilibrage de charge	VM	PROD
bthhpx02p	Debian	Équilibrage de charge	VM	PROD
bthadml01p	Rocky	Bastion	VM	PROD
bthkli01p	Linux	Kali	VM	PROD
bthwww01p	Rocky	Web 1	VM	PROD
bthwww02p	Rocky	Web 2	VM	PROD
bthftp01p	Rocky	Serveur de transfert	VM	PROD
bthmlxp01p	Rocky	Mail	VM	PROD
bthnfsp01p	Rocky	Serveur de fichiers	VM	PROD
bthanu01p	Rocky	Annuaire	VM	PROD
bthbdd01p	Rocky	Base de données	VM	PROD
bthbdd02p	Rocky	Base de données	VM	PROD
bthstk01p	Rocky	Stockage de secours	VM	PROD

04. Composition de l'architecture technique

■ **Le SOC (Security Operations Center)** : Le centre d'opérations de sécurité (SOC) assure la supervision continue et l'administration proactive de la sécurité du système d'information, en utilisant des outils avancés de collecte, de corrélation des événements et d'intervention à distance en temps réel, garantissant ainsi une réponse rapide aux incidents de sécurité.

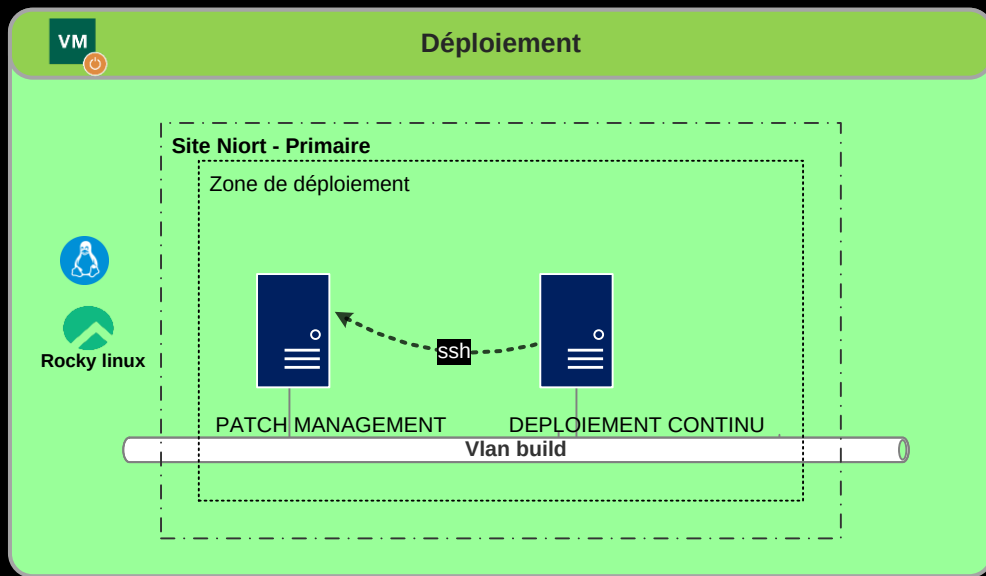
Il permet de superviser et collecter :

- Les trafics entrants et sortants
- L'état de serveurs en cas de dysfonctionnement
- L'utilisation des ressources des serveurs
- L'état des services réseaux
- Les données des systèmes
- En temps réel l'état de l'infrastructure
- Des activités inhabituelles
- La cartographie complète du SI
- Les seuils d'alerte
- Des audits pour analyser l'état de santé du SI de BioTech



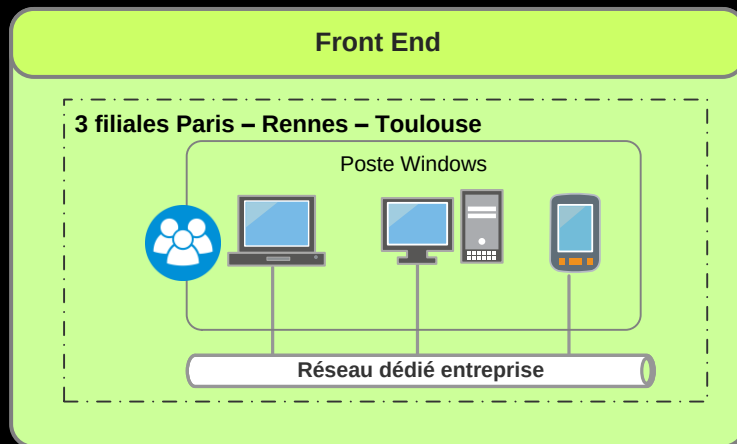
04. Composition de l'architecture technique

- **Le Déploiement** : Une plateforme d'industrialisation permettant de déployer, de mettre à jour et de gérer efficacement les souches ainsi que les environnements de manière rapide et automatisée, garantissant ainsi une mise en production fluide et sans interruption.



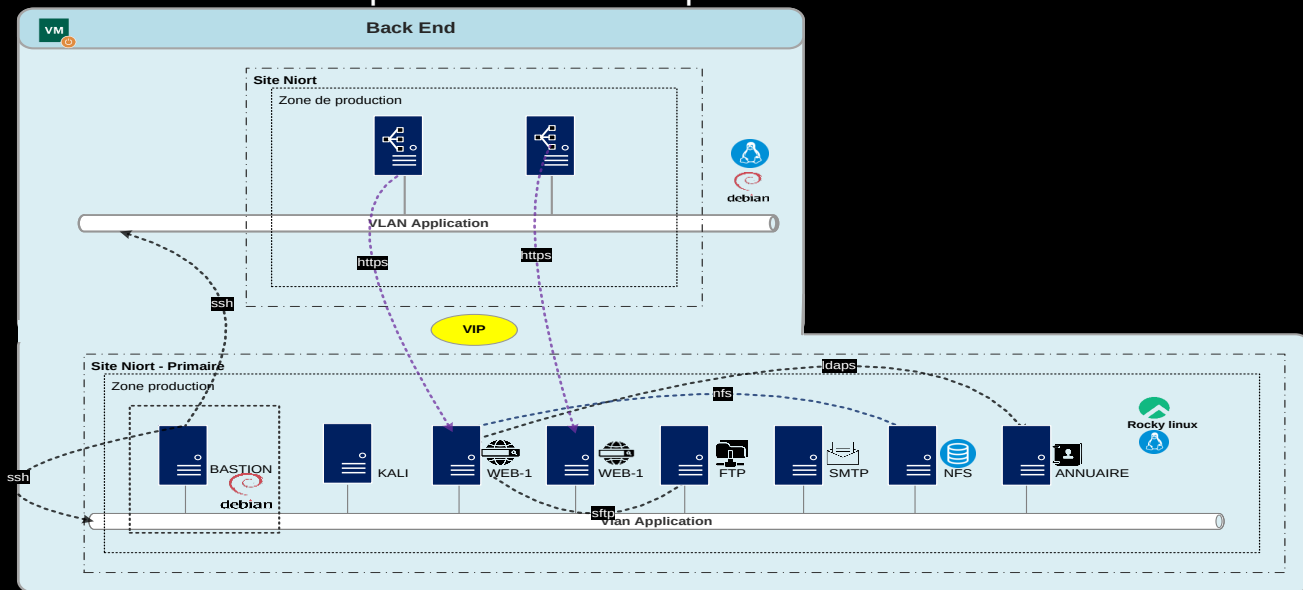
04. Composition de l'architecture technique

- **Le Front End** : Cette zone regroupe les trois filiales. Les collaborateurs de l'entreprise BioTech se connectent via un réseau dédié, à travers un VPN, depuis leurs PC de travail, leurs laptops pour ceux en télétravail, et leurs tablettes pour les commerciaux en déplacement.



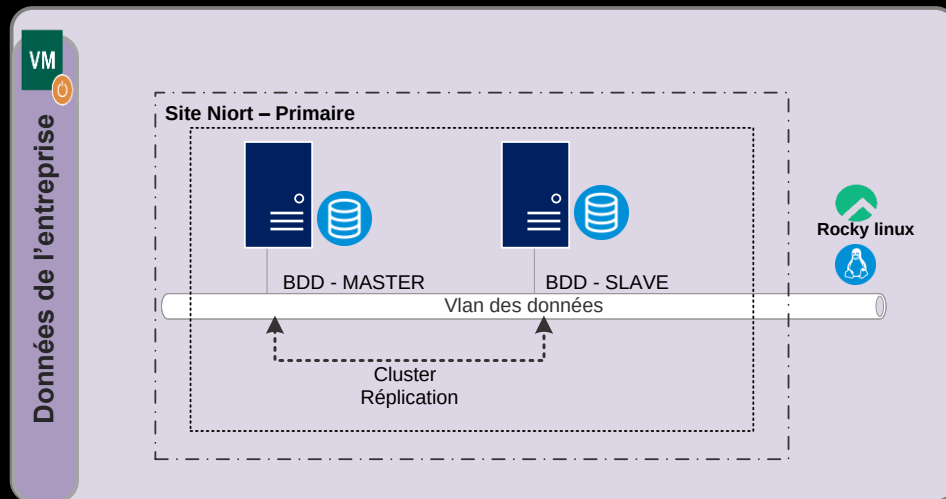
04. Composition de l'architecture technique

- **Le Back End** : L'environnement est situé à Niort, sur le site principal de production de BioTech. Il est constitué de plusieurs serveurs dédiés, afin de garantir une réponse optimale aux exigences élevées et à la nature très sensible des opérations de l'entreprise.



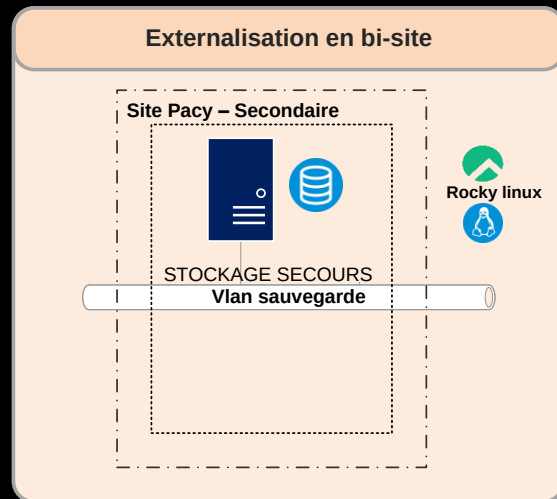
04. Composition de l'architecture technique

- **Les données de l'entreprise** : Cette zone est réservée au stockage des données en base. Afin d'assurer la continuité de l'activité, les bases de données (BDD) sont configurées en cluster répliqué, en mode Actif-Passif, garantissant ainsi la haute disponibilité des données en cas de défaillance d'un nœud.



04. Composition de l'architecture technique

- **Stockage de secours** : Afin de se prémunir contre les risques majeurs tels que les cyberattaques et les incendies susceptibles de compromettre de manière irréversible les données sensibles de l'entreprise BioTech, la Direction des Systèmes d'Information (DSI) a pris la décision stratégique de transférer ces données vers Pacy, un site secondaire sécurisé, garantissant ainsi leur préservation en cas de sinistre majeur.



04. Composition de l'architecture technique

- **La Production** : L'environnement de production, qui regroupe toutes les machines essentielles au bon fonctionnement de l'activité de BioTech, assurant ainsi la continuité des opérations critiques.
 - Zone de production
 - La zone PROD est constituée de plusieurs serveurs et regroupe l'ensemble des activités stratégiques de l'entreprise.
 - Elle est administrée par des personnes dûment habilitées. Les mises à jour des systèmes sont effectuées régulièrement pour se protéger des attaques, qu'elles soient externes ou internes.
 - Le RSSI exerce une vigilance accrue sur ce périmètre critique. Un détournement de ces informations mettrait gravement en péril la société BioTech.

04. Composition de l'architecture technique

- Des questions se posent constamment sur les meilleures façons de réduire la surface d'attaque face aux malveillants.
- Le prestataire doit être proactif en proposant des solutions techniques adaptées pour sécuriser chaque zone contre les intrusions et protéger l'intégrité du système.

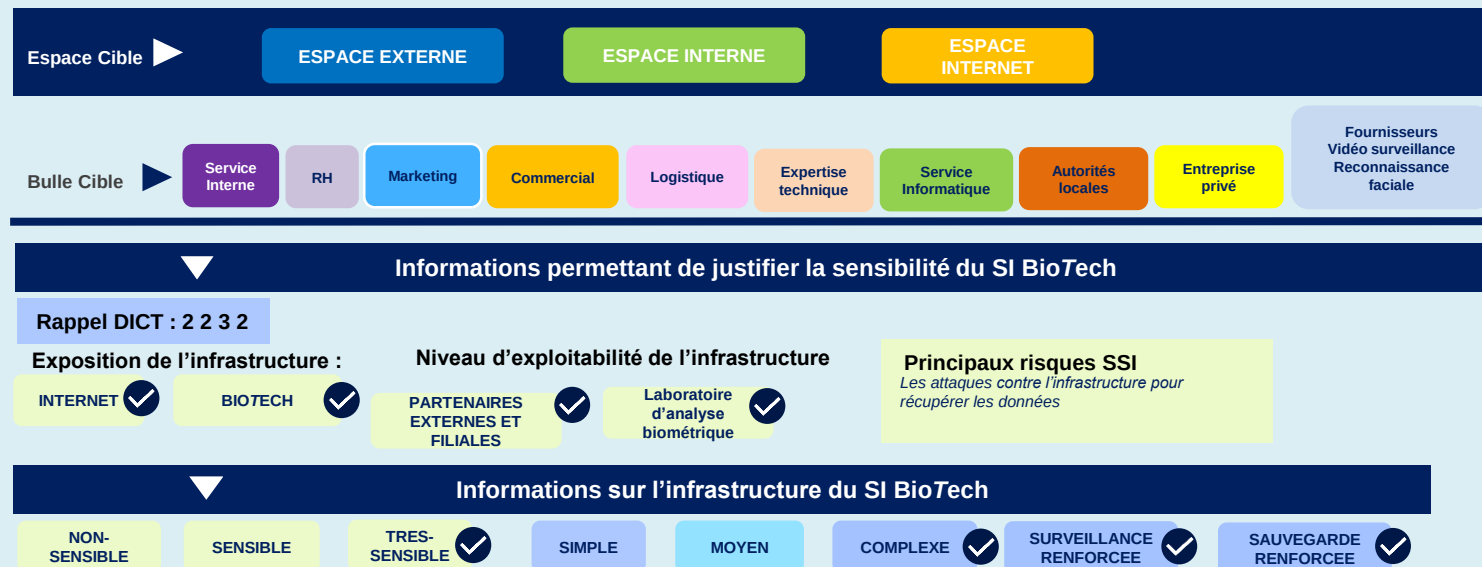
04. Architecture technique

■ L'architecture technique de la société BioTech

- La composition de l'infrastructure BioTech comprend PRA aucune perte de données est autorisée.
- La société a un plan de reprise d'activité :
 - PDMA PRA : La perte de données maximale admissible 4hrs
 - DIMA PRA : La durée maximale d'interruption admissible 4hrs

04. Architecture technique

■ Les indicateurs de sécurité de l'architecture technique de la société BioTech:



05. Livrable

■ Les livrables

- La présentation de la solution technique ;
- Le DAT décrivant tous les aspect techniques avec le modèle du document fourni ;
- Les DEX (Installation et configuration) que le client exige pour la mise en place de son infra. Ces documents seront remis à des exploitants pour installer toute l'infra ;
- Le plan de pentesting et le résultat des tests ;
- Les documents annexes qui ont permis de réaliser ce projet ;
- Un RETEX dans le document de présentation pour analyser les expériences du projet, en tirer des leçons et améliorer les pratiques futures lors de la présentation du 31/03/2026.

05. Livrable

■ Les Consignes

- Respecter les noms des machines pour faciliter les démonstrations pendant l'exposition ;
- Décrire vos documents techniques dans les templates à votre disposition ;
- Numéroter les pages de vos PPT pour faciliter les questions-réponses pendant l'oral ;
- Soigner votre présentation PPT, vous présentez une société pour cette RAO ;
- Relever toutes les informations pertinentes pour proposer une solution avec des axes d'amélioration ;
- Faites un Trello pour suivre vos travaux en rajoutant espace intervenant pour les commentaires ;
- Faire un plan de travail en regroupant toutes les expressions de besoin de BioTech ;



jramsamy@abcit.fr



[ABCIT Formation](#)

Propriété intellectuelle à ABCIT formation toute reproduction est interdite