PARCOURS DE CYBERSECURITÉ

—

Restitution

———

Bénéficiaire – jour mois année

Règles de diffusion du présent document

Ce document est mis à disposition sous un contrat Creative Commons CC-by-nc-nd
Attribution / Pas d'utilisation commerciale / Pas de modification

Vous êtes autorisé à :

Partager
Copier, distribuer et communiquer le matériel par tous moyens et sous tous formats

Adapter
Remixer, transformer et créer à partir du matériel

Selon les conditions suivantes :

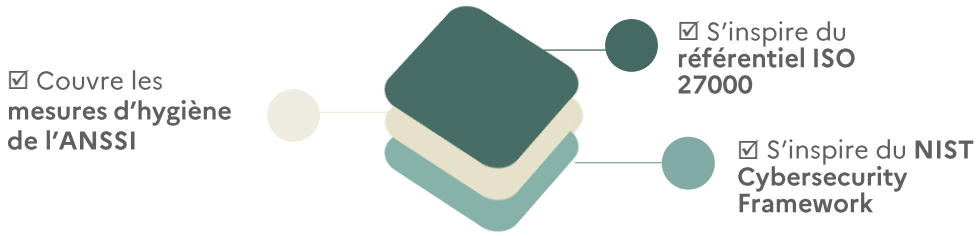
- **Attribution** — Vous devez créditer le document à l'ANSSI, intégrer un lien vers la licence et indiquer si des modifications ont été effectuées au livrable. Vous devez indiquer ces informations par tous les moyens raisonnables, sans toutefois suggérer que l'ANSSI vous soutient ou soutient la façon dont vous avez utilisé le document.
- **Pas d'Utilisation Commerciale** — Vous n'êtes pas autorisé à faire un usage commercial de ce document, tout ou partie du matériel le composant.
- **Partage dans les Mêmes Conditions** — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant le document original, vous devez diffuser le document modifié dans les mêmes conditions, c'est à dire avec la même licence avec lequel le document original a été diffusé.
- **Pas de restrictions complémentaires** — Vous n'êtes pas autorisé à appliquer des conditions légales ou des mesures techniques qui restreindraient légalement autrui à utiliser le document dans les conditions décrites par la licence.

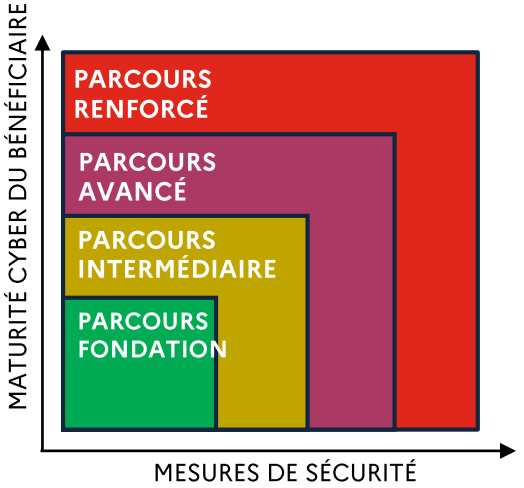
Références Creative commons	Creative Commons — Attribution-NonCommercial-NoDerivatives 4.0 International — CC BY-NC-ND 4.0 Creative Commons — Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International — CC BY-NC-SA 4.0

SOMMAIRE

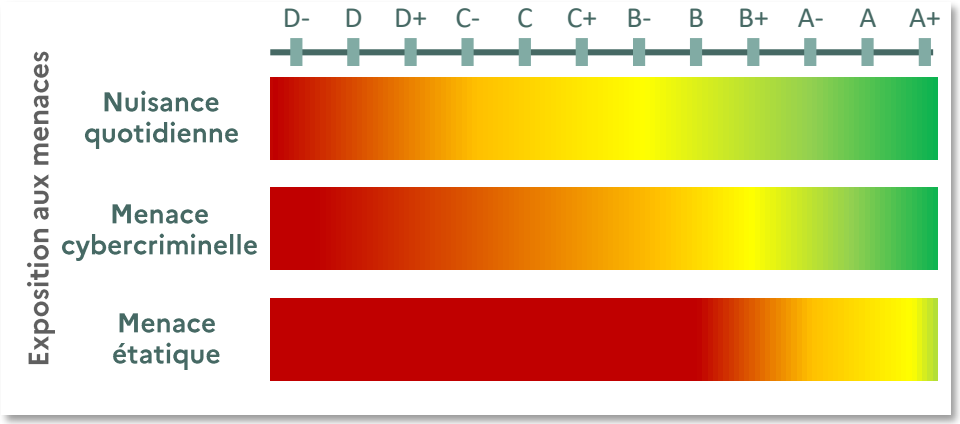
1. RAPPEL DE LA DÉMARCHE
2. CONTEXTE, ENJEUX ET MENACES
3. ETAT DES LIEUX
4. PLAN DE SÉCURISATION

Des parcours de cybersécurité conçus pour répondre aux enjeux et aux besoins de chaque organisation à travers 120 mesures progressives

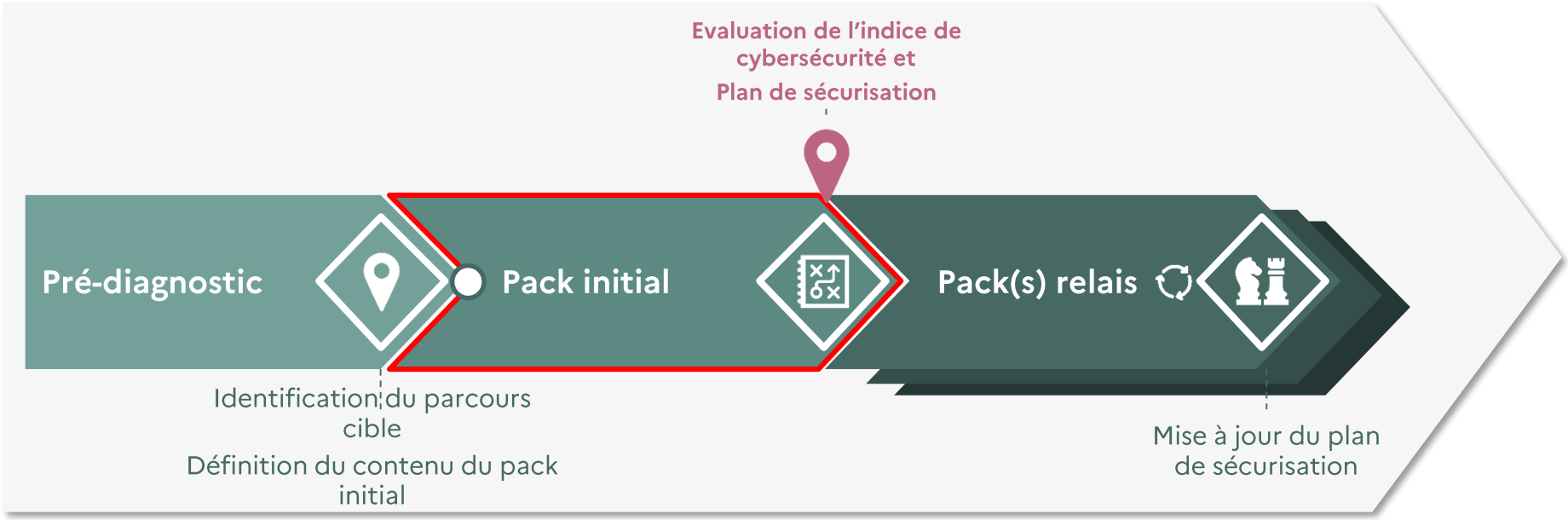




L'indice de cybersécurité, basé sur ces parcours cybersécurité, permet de suivre la maturité du bénéficiaire de façon benchmarkée



Un dispositif d'accompagnement structuré en trois phases



Des démarches du diagnostic et de la formalisation du plan de sécurisation menées sur des périmètres adaptés

État des lieux

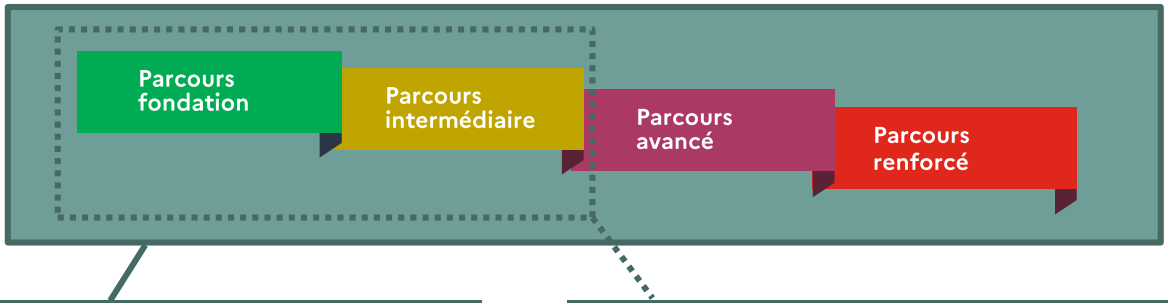
- Identification des enjeux métiers et DSI
- État des lieux SSI organisationnel et technique
- Cartographie des zones de vulnérabilités

Plan de sécurisation

- Identification des chantiers
- Planification du plan de sécurisation
- Présentation aux dirigeants
- Mise en œuvre des mesures urgentes

Autres travaux

- **Réalisation d'actions de sensibilisation**



UN ÉTAT DES LIEUX GÉNÉRAL …

L'état des lieux est réalisé sur l'ensemble des mesures de sécurité, quel que soit le parcours cible du bénéficiaire, afin de pouvoir établir un **benchmark** entre toutes les entités.

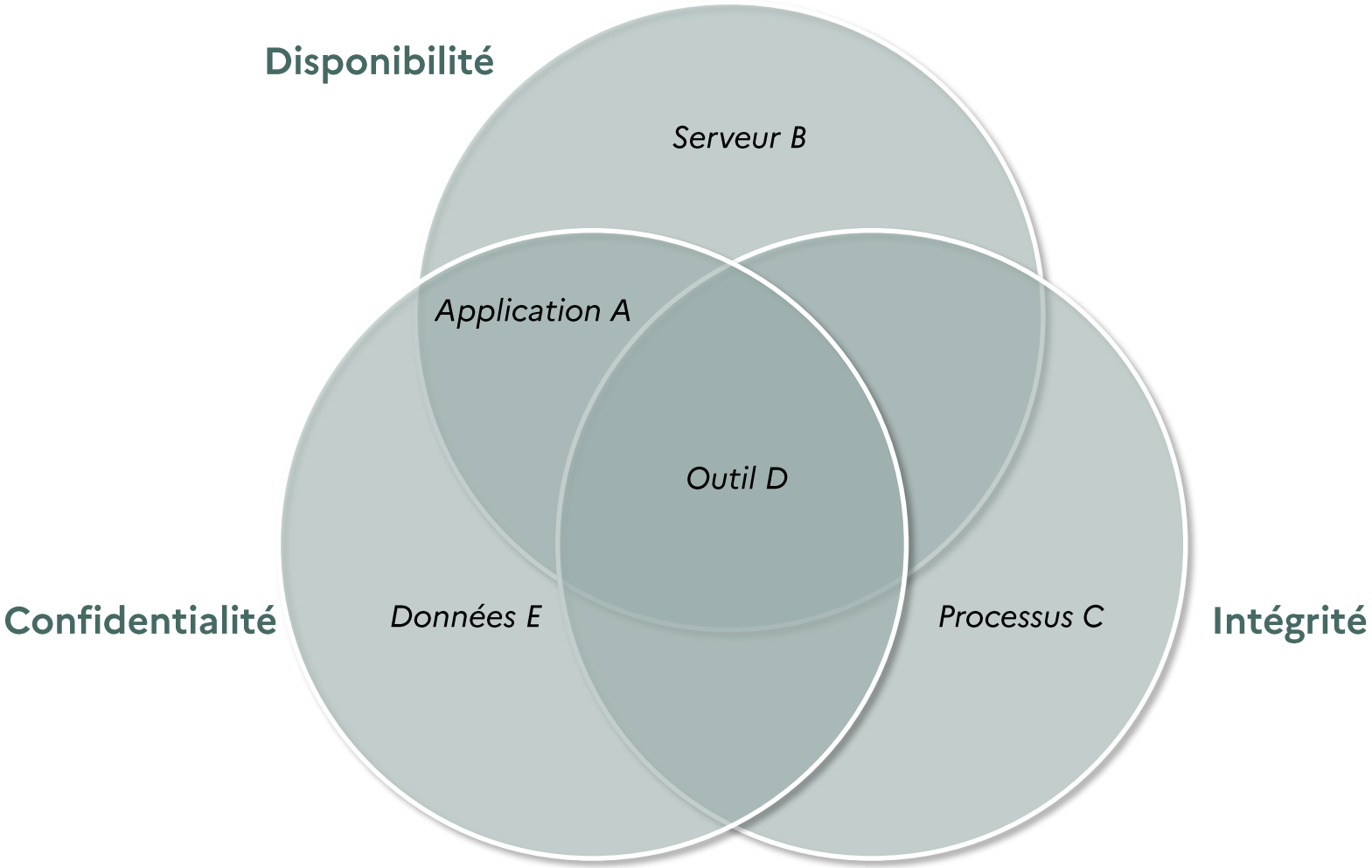
… MAIS UN PLAN DE SÉCURISATION CIBLÉ

Le plan de sécurisation est quant à lui **adossé à votre parcours cible** (XXX), afin de définir des objectifs de cybersécurité qui soient à la fois **adaptés, raisonnables et atteignables**.

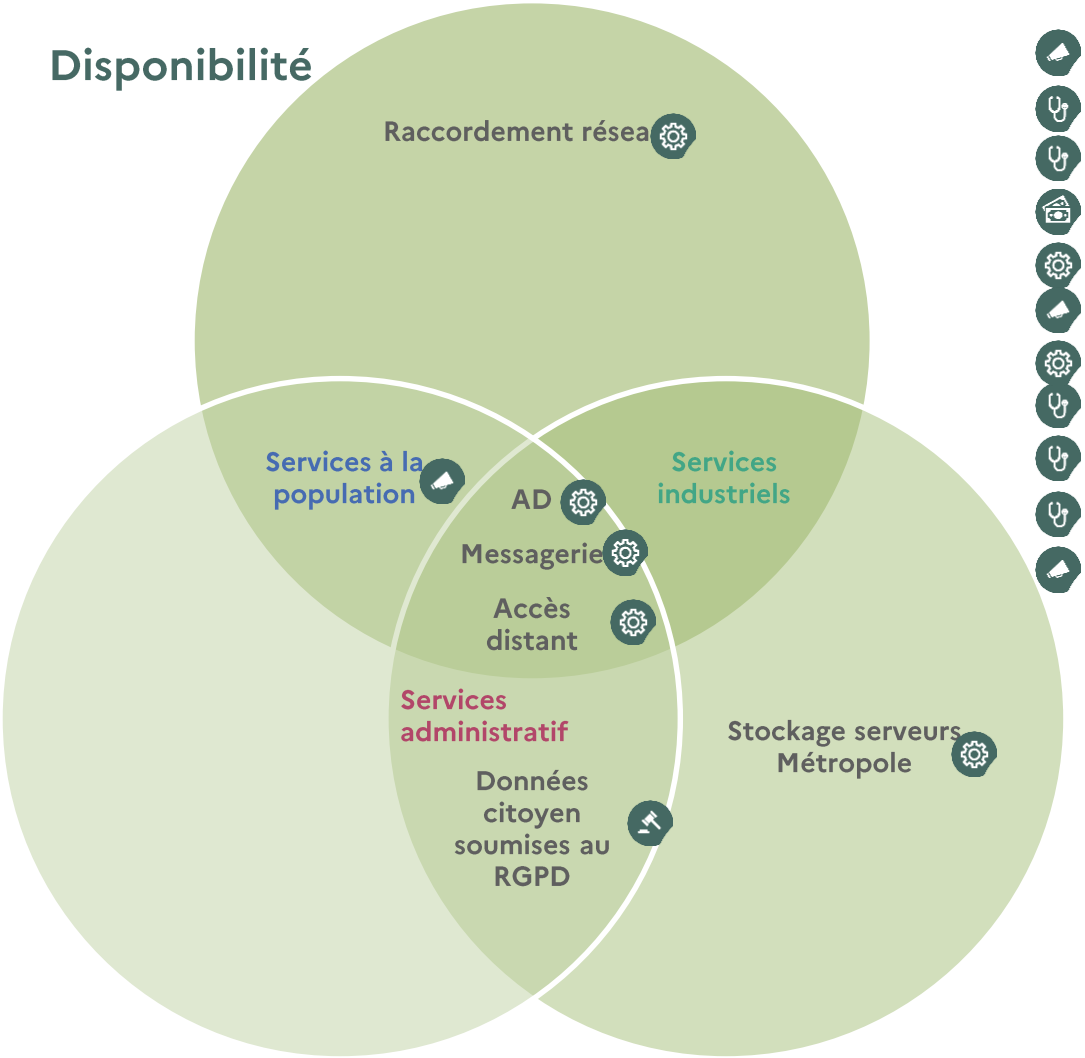
SOMMAIRE

1. RAPPEL DE LA DÉMARCHE
2. CONTEXTE, ENJEUX ET MENACES
3. ETAT DES LIEUX
4. PLAN DE SÉCURISATION

Les dispositifs de sécurité mis en œuvre doivent répondre à vos principaux enjeux sécurité



Exemple pour une collectivité territoriale



- Services numériques aux usagers
- Gestion de la vaccination
- Activités sociales du CCAS
- Logiciels de gestion financière
- Logiciels RH
- Évènementiel
- Vidéosurveillance
- Gestion du trafic routier
- Traitement des eaux usées
- Approvisionnement en eau
- Cuisine centrale / scolaire

Impact financier | Impact d'image | Impact opérationnel | Impact sur la santé des citoyens ou des agents | Impact juridique

Les dispositifs de sécurité qui seront mis en œuvre doivent également s'inscrire dans le cadre de vos évolutions

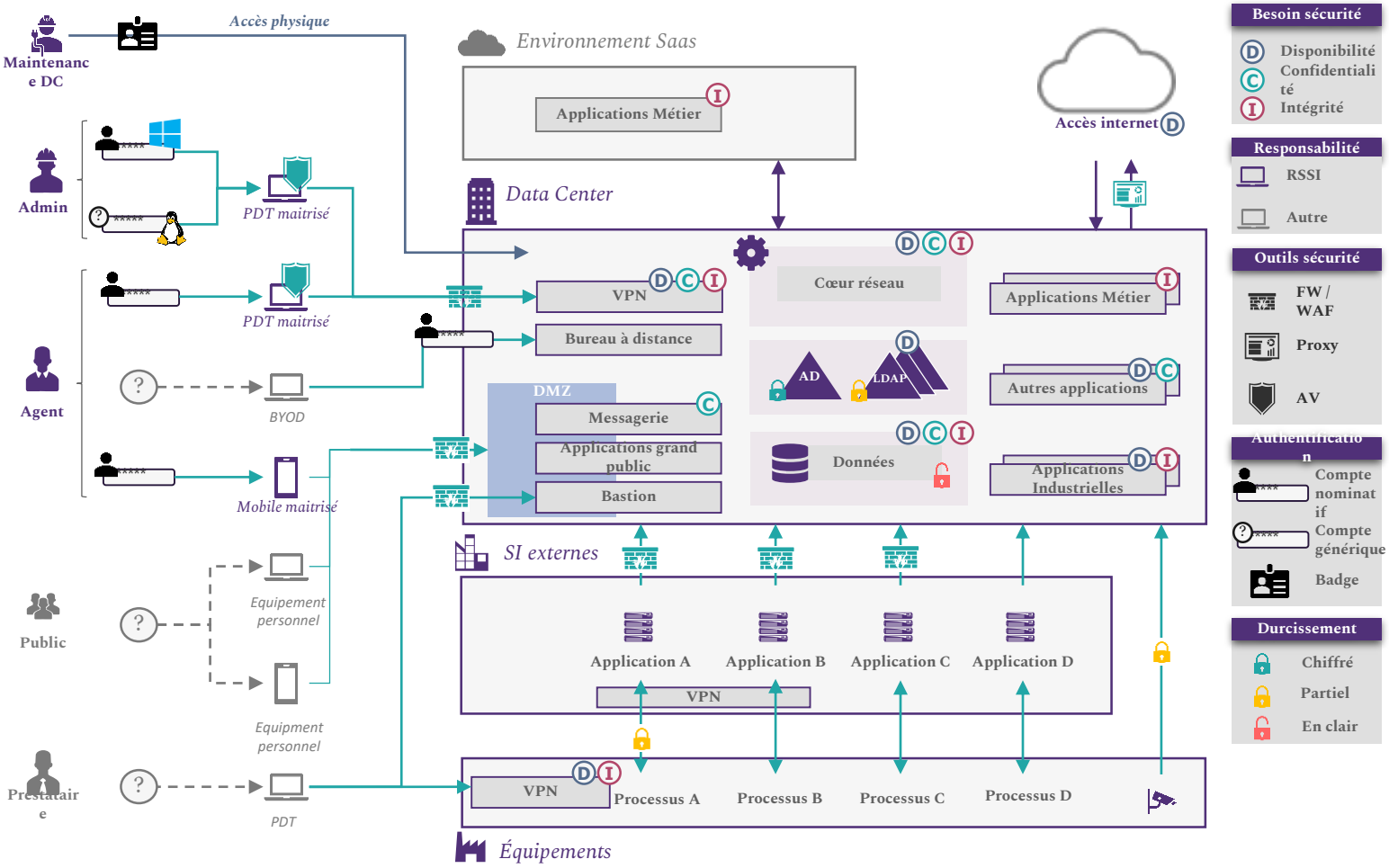
Un contexte métier et SI en pleine transformation dont il faut tenir compte

> Elément de contexte interne 1
> Elément de contexte interne 2
> Elément de contexte externe 1
> ...

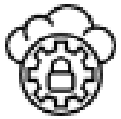
Des travaux majeurs de sécurité récemment menés par vos équipes

> Travaux 1
> Travaux 2
> ...

Cartographie du système d'information



Principales menaces et évènements redoutés

Source de menace	Evènement redouté	Vecteur d'attaque possible
Menace cybercriminelle  **Étatique**	**Vol de données de recherche**	• Application de recherche
Menace cybercriminelle  **Attaque opportuniste**	**Ransomware**	• Phishing • Interfaces exposées sur Internet
Menace étatique  **Crime organisé**	**Vol de données personnelles**	• Phishing • Interfaces exposées sur Internet

SOMMAIRE

1. RAPPEL DE LA DÉMARCHE
2. CONTEXTE, ENJEUX ET MENACES
3. ETAT DES LIEUX
4. PLAN DE SÉCURISATION

Un état des lieux organisationnel mettant en avant une capacité limitée/variable/forte à faire face à vos principales menaces

Principaux constats réalisés dans le cadre de l'état des lieux organisationnel

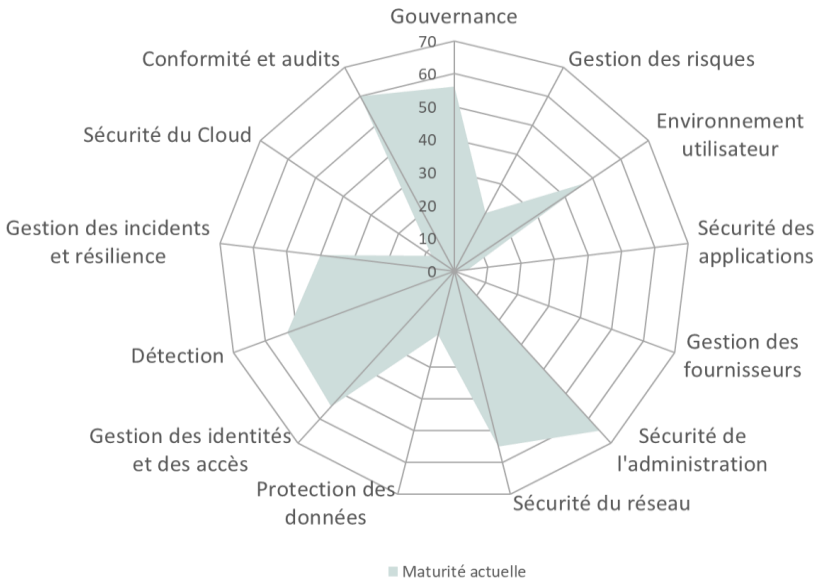
- Constat positif 1
- Constat positif 2

- Constat négatif 1
- Constat négatif 2

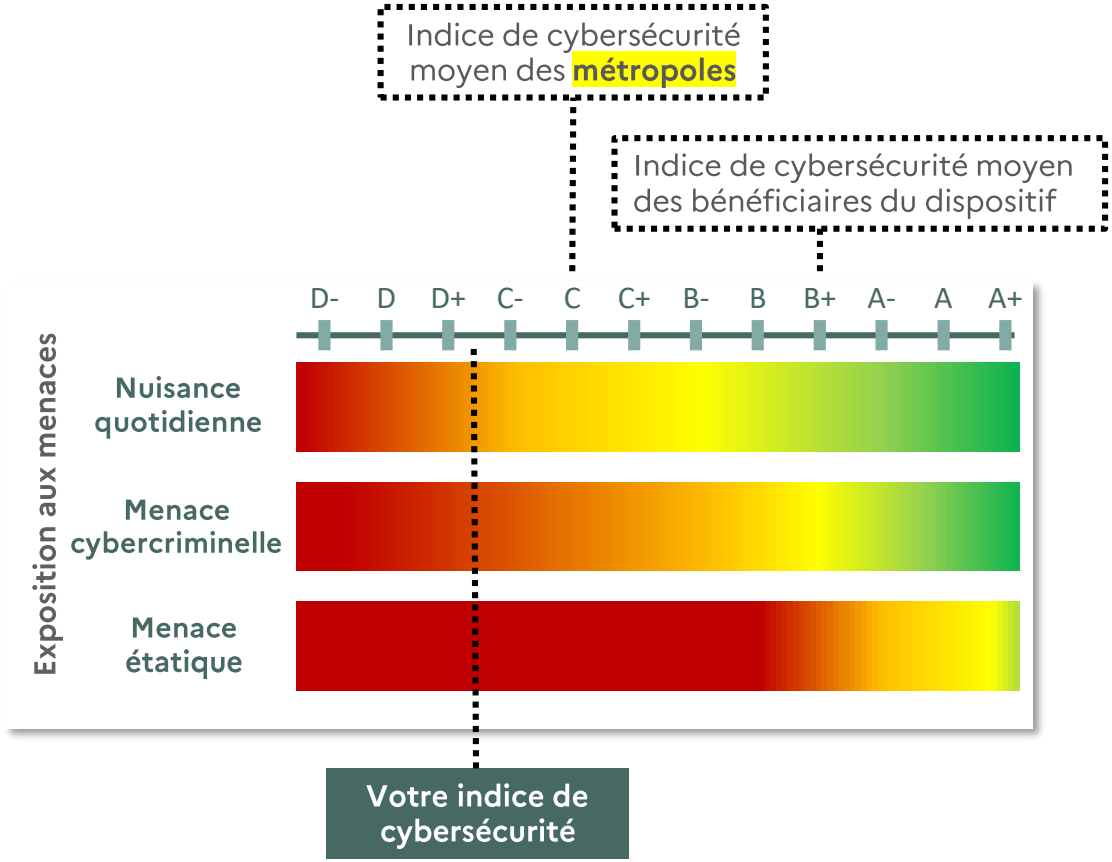
Indice de cybersécurité

D+

Score : 167/400



Position de votre organisation vis-à-vis des autres entités du secteur public



Tests techniques : synthèse

Rappel des tests réalisés et des périmètres couverts

- A préciser
- A préciser
- …
- …

Nbre **total** de vuln. identifiées	Nbre de vuln. **critiques** identifiées	**Score ADS** *(audit AD)*	**Score SILENE** *(scans externes)*
XX	XX	1 (2 3 4 5)	1 (2 3 4 5)
		33 pb importants	23 pb importants

Principaux constats réalisés dans le cadre des tests techniques

- Constat 1
- Constat 2

- Constat 1
- Constat 2

Tests techniques : exemple de synthèse

Rappel des tests réalisés et des périmètres couverts

- **Tests d'intrusion externes** : Cartographie des informations accessibles sur internet
- **Tests d'intrusion internes** : Cartographie et analyse des vulnérabilités du réseau - et analyse de l'Active Directory
- **Périmètre ciblé** : Les tests ont été menés sur l'environnement de production
- **Approche boite noire** (aucun authentifiant n'est transmis à l'auditeur) pour la phase externe et **approche boite grise** (l'auditeur dispose d'authentifiant utilisateur) pour la phase interne.

Nbre **total** de vuln. identifiées	**20**

Nbre de vuln. **critiques** identifiées	**7**

Score ADS *(audit AD)*	**1** 2 3 4 5

33 pb importants

Score SILENE *(scans externes)*	**1** 2 3 4 5

23 pb importants

Principaux constats réalisés dans le cadre des tests techniques

- Le **système d'information** est **globalement maintenu à jour** : aucun OS obsolète n'a été identifié et aucune vulnérabilité critique impactant les systèmes d'exploitation n'a pu être identifiée.
- Le réseau interne est **correctement cloisonné**. Il n'est pas possible d'accéder qu'à un nombre limité de ressources du réseau depuis un point donné.
- Les **interfaces du système d'information exposées sur Internet ne sont pas maintenues à jour**. De plus, elles exposent des **informations sensibles**.
- Il est d'ailleurs possible d'accéder à **des fichiers contenant des informations techniques sensibles** sans authentification.

Tests techniques : points d'attention

Texte
Sous texte
X

Texte
Sous texte
X%

Texte
Sous texte
X/XX

Texte
Sous texte
X/XX

Tests techniques : points d'attention – Exemples d'indicateurs

Nombre de services sensibles exposés sur Internet (portails d'administration et BDD) **5**

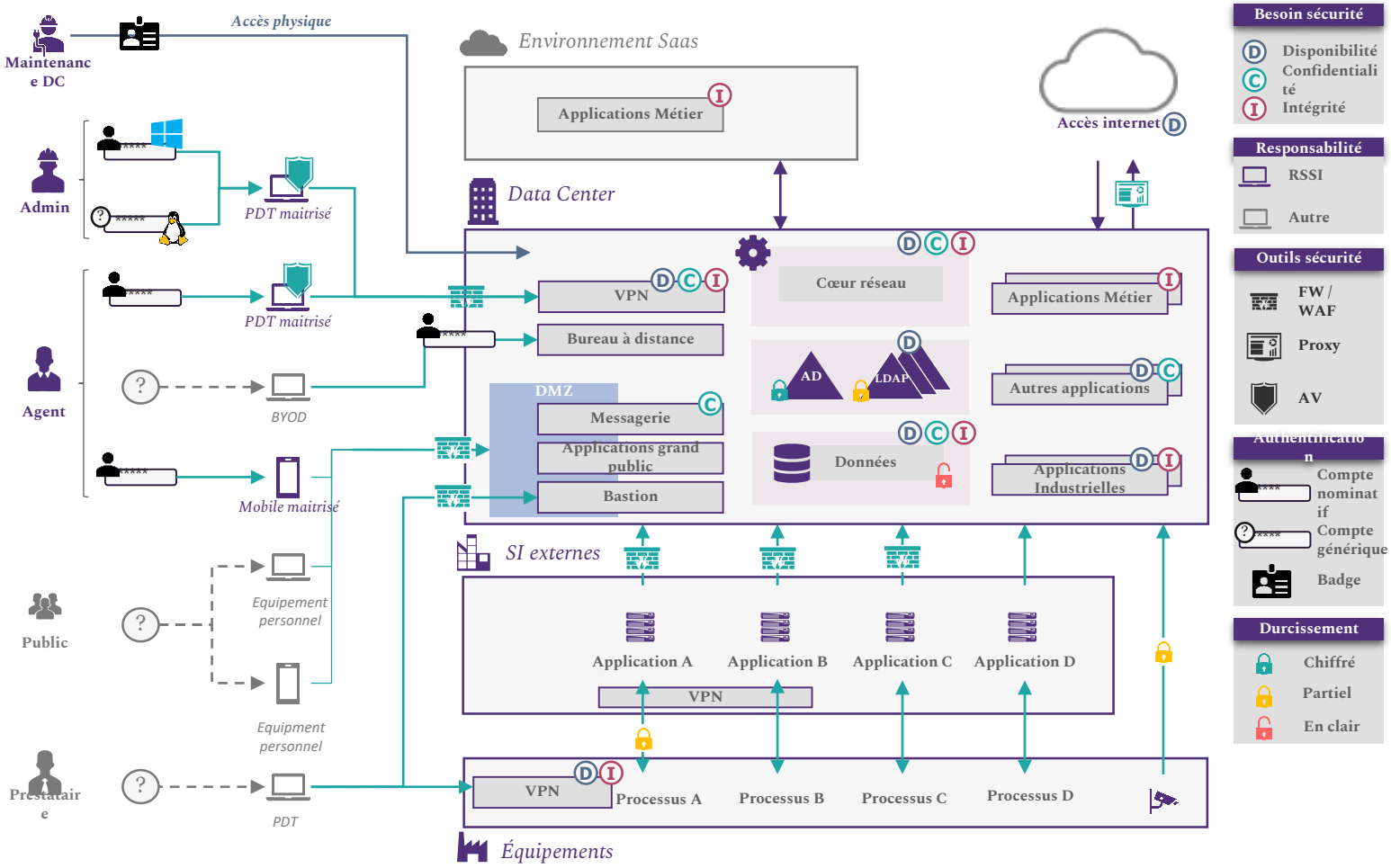
Application de gestion de congés, Gitlab, Serveur de gestion des mots de passe et 4 serveurs de base de données (MySQL)

Nombre de comptes avec mots de passe sans expiration **50/405**

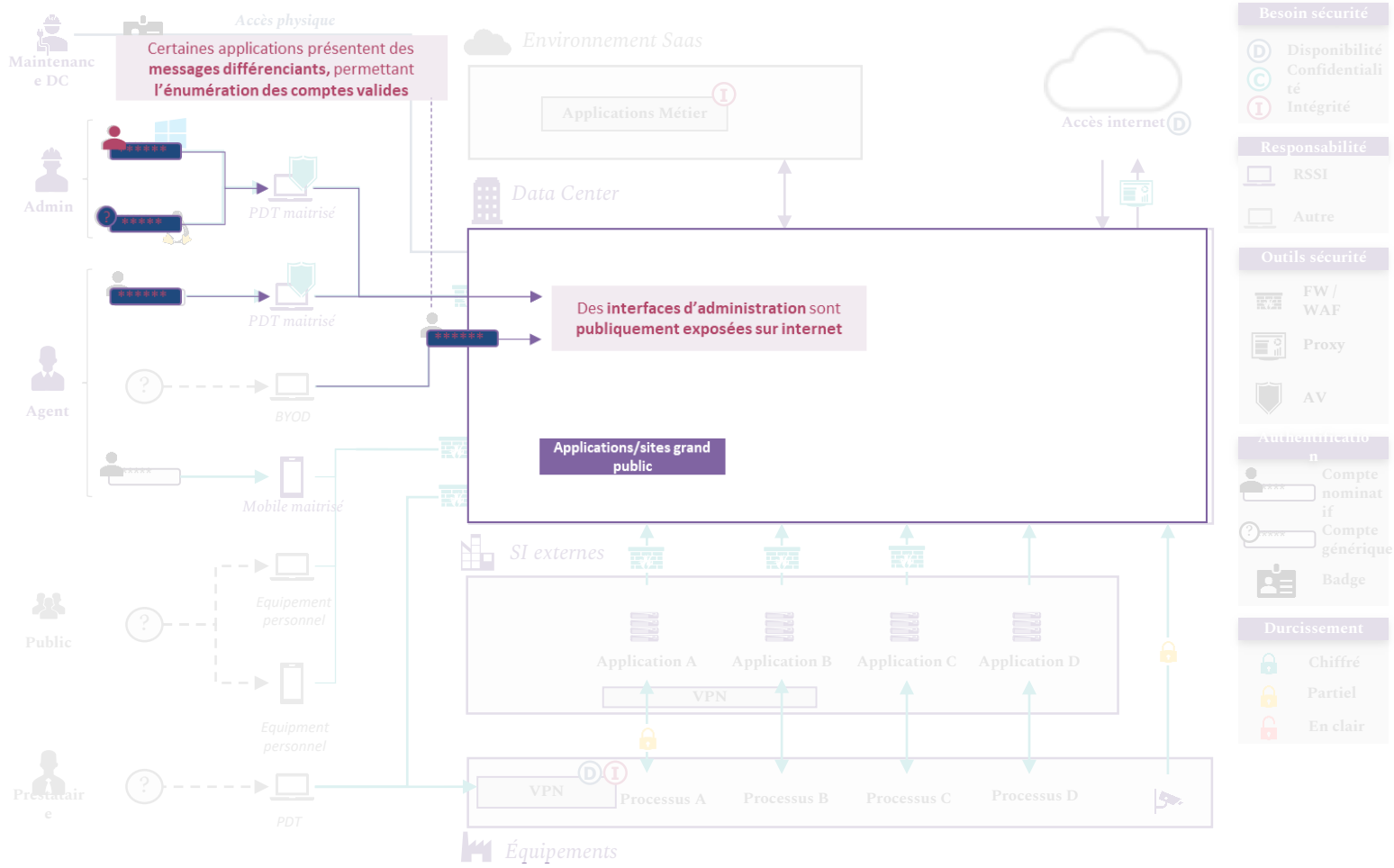
Nombre d'utilisateurs actifs étant administrateurs de domaine **25/405**

Nombre de comptes utilisateurs inactifs **30/405**

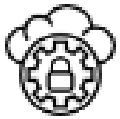
Cartographie du système d'information - Vulnérabilités externes (audit technique)



Cartographie du système d'information - Vulnérabilités internes (audit technique) - Exemple



Capacité à faire face aux principales menaces

	Source de menace	Evènement redouté	Niveau d'exposition à la menace estimé	Principales vulnérabilités
Menace cybercriminelle	 **Étatique**	**Vol de données de recherche**	**Fort**	• Serveurs de recherche obsolètes avec des failles critiques
Menace cybercriminelle	 **Attaque opportuniste**	**Ransomware**	**Très Fort**	• Manque de sensibilisation des utilisateurs • Niveau de sécurité de l'AD insuffisant
Menace étatique	 **Crime organisé**	**Vol de données personnelles**	**Moyen**	• Manque de sensibilisation des utilisateurs • Gestion des accès aux application peu mature

SOMMAIRE

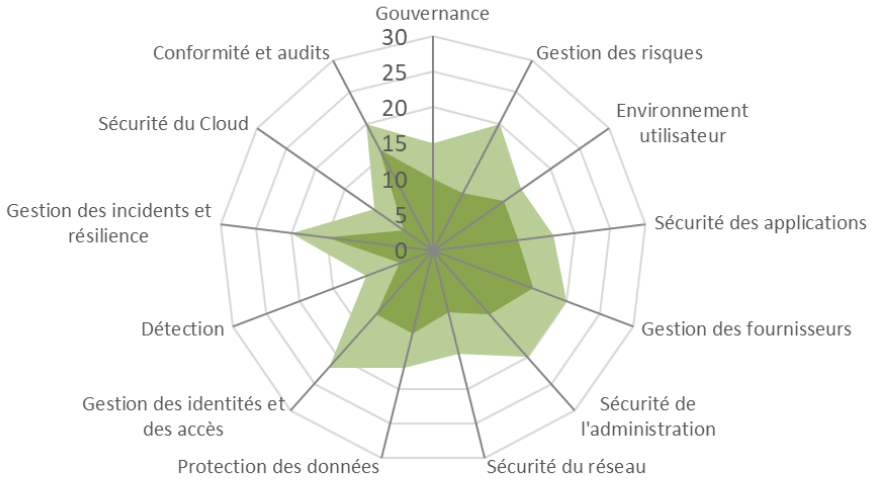
1. RAPPEL DE LA DÉMARCHE
2. CONTEXTE, ENJEUX ET MENACES
3. ETAT DES LIEUX
4. PLAN DE SÉCURISATION

Un plan de sécurisation adapté et atteignable, en plusieurs phases

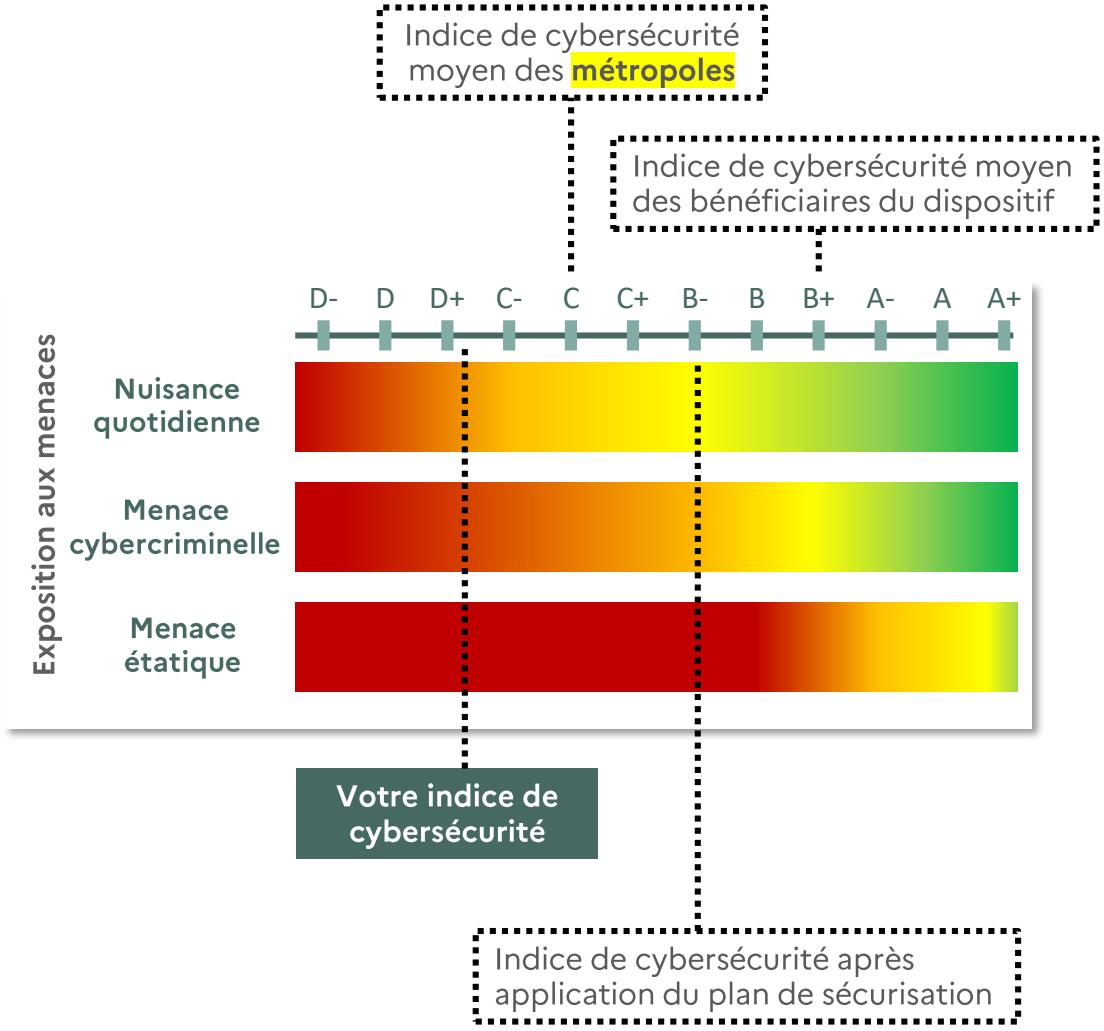
Total	P0/P1	P2	P3
Nombre d'actions : XX	Nombre d'actions : XX	Nombre d'actions : XX	Nombre d'actions : XX
Coût/Charge : XX jh XX €	Coût/Charge : XX jh XX €	Coût/Charge : XX jh XX €	Coût/Charge : XX jh XX €
	Planning : Tx 202x	Planning : Tx 202x	Planning : Tx 202x

Indice de cybersécurité

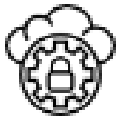
Actuel	Après P0 à P1	Après P0 à P3
D+	C	C
XX / 400	XX / 400	XX / 400



Le plan de sécurisation permettra à votre organisation de se repositionner vis-à-vis du benchmark



Capacité à faire face aux principales menaces

	Source de menace	Evènement redouté	Niveau d'exposition à la menace estimé avant plan d'actions	Niveau d'exposition après plan d'actions P0/P1	Niveau d'exposition après plan d'actions complet
Menace cybercriminelle	 **Étatique**	**Vol de données de recherche**	**Fort**	**Fort**	**Moyen**
Menace cybercriminelle	 **Attaque opportuniste**	**Ransomware**	**Très Fort**	**Fort**	**Moyen**
Menace étatique	 **Crime organisé**	**Vol de données personnelles**	**Moyen**	**Faible**	**Très faible**

Synthèse du plan de sécurisation

	Chantiers identifiés	Nombre d'actions			
		P0	P1	P2	P3
Gouvernance	• *Définition de la PSSI* • *Mise en place d'une comitologie*				
Sensibilisation					
Environnement utilisateur					
Applications					
Gestion des fournisseurs et des partenaires					
Administration des infrastructures					
Réseau					
Protection des données					
Gestion des identités et des accès					
Détection					
Gestion des incidents et résilience					
Cloud					
SI industriel					
Conformité et audits					
Total					

Actions de priorité 0

Les actions présentées ci-dessous ont été identifiées comme **urgentes pour la sécurisation du Système d'Informations du *{bénéficiaire}*** devront donc être **réalisées en priorité absolue**.

Actions transverses *(charge DSI & RSSI)*

Action	Charges estimées (JH)	Échéance de réalisation
Étendre l'usage d'ELK *Cadrage: RSSI* *Réalisation: DSI*	45-55	Au plus tôt

Actions à la charge de la DSI

Action	Charges estimées (JH)	Échéance de réalisation
Contenir les risques sur les actifs obsolètes	45-65	Au plus tôt
Sécuriser les flux applicatifs	25-30	
Sécuriser les comptes à privilèges	30	

Action à la charge du RSSI

Action	Charges estimées (JH)	Échéance de réalisation
Revoir la PSSI	10-15	Décembre 2021
Définir une charte pour les utilisateurs à privilèges	5	

La description détaillée ainsi que le chiffrage des actions sont présentés dans les fiches chantiers de chaque thématique adressée

Actions de priorité 1

Les actions présentées ci-dessous identifiées comme étant de priorité 1 pour la **sécurisation du Système d'Informations du *{bénéficiaire}*** et devront être réalisées au plus tard avant **l'échéance de décembre 2022**.

La description détaillée ainsi que le chiffrage des actions sont présentés dans les fiches chantiers de chaque thématique adressée

Actions de priorité 2

Les actions présentées ci-dessous identifiées comme étant de priorité 2 pour la **sécurisation du Système d'Informations du *{bénéficiaire}*** et devront être réalisées au plus tard avant **l'échéance de décembre 2023**.

La description détaillée ainsi que le chiffrage des actions sont présentés dans les fiches chantiers de chaque thématique adressée

Actions de priorité 3

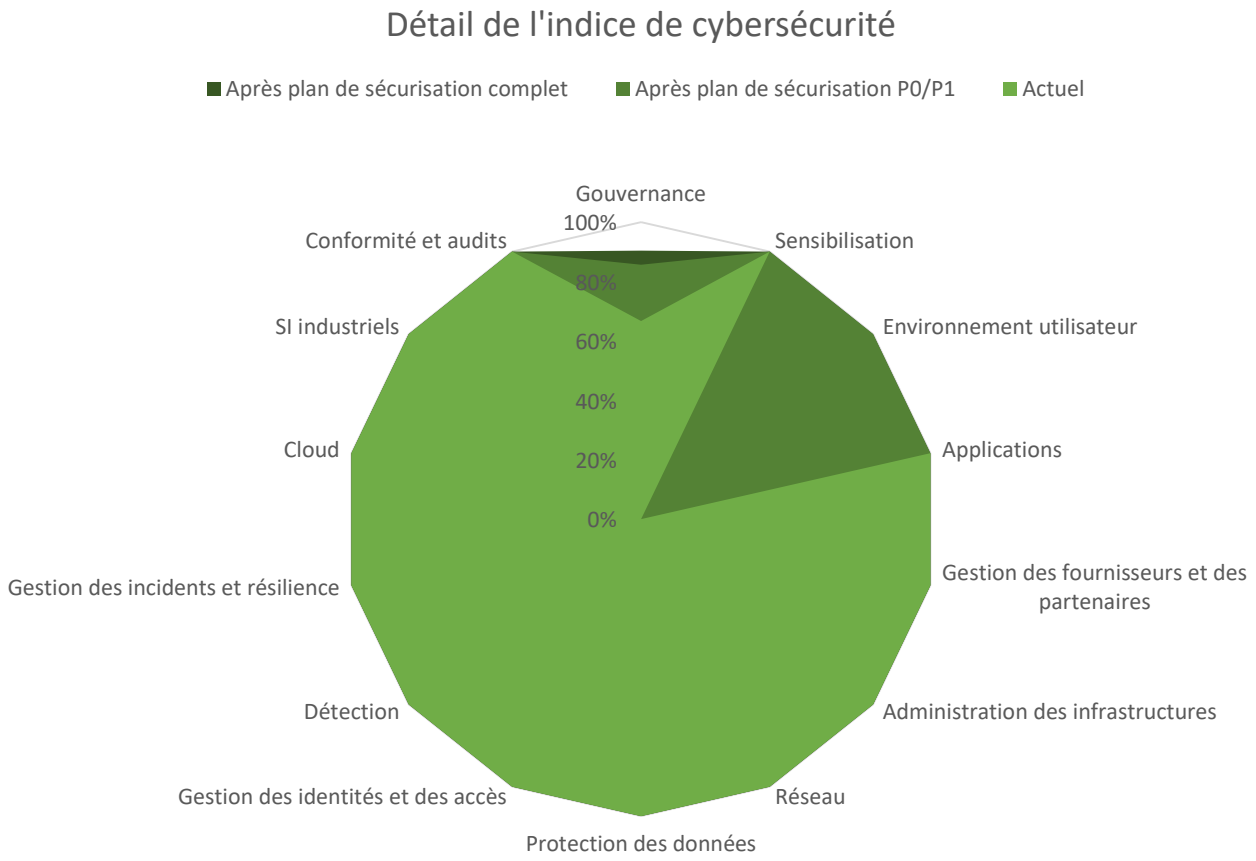
Les actions présentées ci-dessous identifiées comme étant de priorité 3 seront **dépendantes de la capacité du *{bénéficiaire}*** à fournir à l'équipe RSSI une **charge adéquate** pour leur bonne réalisation.

La description détaillée ainsi que le chiffrage des actions sont présentés dans les fiches chantiers de chaque thématique adressée

Planification des chantiers

	Mai 21	Juin 21	Juillet 21	Août 21	Sept 21	Oct 21	Nov 21	Déc 21	Jan 22	Févr 22	Mars 22	Avril 22	Mai 22	Juin 22	Juillet 22	Août 22	Sept 22	Oct 22	Nov 22
Gouvernance																			
Sensibilisation																			
Environnement utilisateur																			
Applications																			
Gestion des fournisseurs et des partenaires																			
Administration des infrastructures																			
Réseau																			

Apports détaillés des bénéfices escomptés



Recommandations et prochaines étapes

Chantiers prioritaires à lancer dans le cadre des « pack relais » *

-
-
-

** Ces chantiers pourront être co-financés par l'ANSSI*

SOMMAIRE

Annexes – Détail de l’état des lieux

Constats détaillés

Gouvernance – XX %

Synthèse : A compléter

- Constat 1
- Constat 2

- Constat 1
- Constat 2

Sensibilisation – XX %

Synthèse : A compléter

- Constat 1
- Constat 2

- Constat 1
- Constat 2
- Constat 3
- Constat 4

Environnement utilisateur – XX %

Synthèse : A compléter

- Constat 1
- Constat 2
- Constat 3
- Constat 4

- Constat 1
- Constat 2

Constats détaillés

Applications – XX%

Synthèse : A compléter

- Constat 1
- Constat 2

- Constat 1
- Constat 2

Gestion des fournisseurs et des partenaires – XX%

Synthèse : A compléter

- Constat 1
- Constat 2

- Constat 1
- Constat 2
- Constat 3
- Constat 4

Administration des infra. – XX%

Synthèse : A compléter

- Constat 1
- Constat 2
- Constat 3
- Constat 4

- Constat 1
- Constat 2

Constats détaillés

Réseau – XX%	Protection des données – XX%	Gestion des identités et des accès – XX%
Synthèse : A compléter	**Synthèse :** A compléter	**Synthèse :** A compléter
• Constat 1 • Constat 2	• Constat 1 • Constat 2	• Constat 1 • Constat 2 • Constat 3 • Constat 4
• Constat 1 • Constat 2	• Constat 1 • Constat 2 • Constat 3 • Constat 4	• Constat 1 • Constat 2

Constats détaillés

Détection – XX%	Gestion des incidents et résilience – XX%	Cloud – XX%
Synthèse : A compléter	**Synthèse** : A compléter	**Synthèse** : A compléter
• Constat 1 • Constat 2	• Constat 1 • Constat 2	• Constat 1 • Constat 2 • Constat 3 • Constat 4
• Constat 1 • Constat 2	• Constat 1 • Constat 2 • Constat 3 • Constat 4	• Constat 1 • Constat 2

Constats détaillés

SI industriels – XX%	Conformité et audits – XX%
Synthèse : A compléter	**Synthèse : A compléter**
• Constat 1 • Constat 2	• Constat 1 • Constat 2
• Constat 1 • Constat 2	• Constat 1 • Constat 2

SOMMAIRE

Annexes – Détail des chantiers

Plan de sécurisation détaillé

Gouvernance

DSI RSSI — Priorité : P0 P1 P2 P3

Objectifs

Cadrer l'utilisation du SI à travers une PSSI à jour **et responsabiliser les utilisateurs** à privilèges

Prérequis

-

Démarche

1. *Revoir la PSSI – GOUV1*

   Mettre à jour la PSSI, la faire valider par la direction générale et en prévoir une revue annuelle. Fournir à chaque collaborateur une charte utilisateur basée sur la PSSI

2. *Définir une charte pour les utilisateurs à privilèges – GOUV2*

   Élaborer un charte utilisateur spécifique aux utilisateurs à privilèges

Indicateurs d'avancement ou de performance

Suivi de l'avancement de la feuille de route

Budget *(1 JH = 500-1000€)*

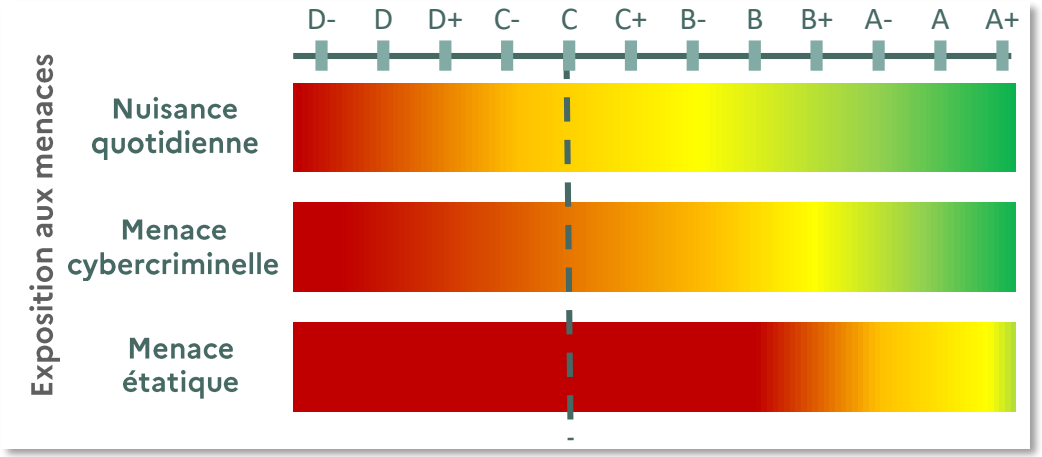
Phase	GOUV1	GOUV2	GOUV3	GOUV4
Cadrage	-	-	5 JH	-
Consultation	-	-	-	-
Réalisation	10-15 JH	5 JH	5-10 JH	-
Exploitation	-	-	-	-

Décision

En attente de

Validé

Présentation de l'indice de cybersécurité



Les 3 types de menaces :

Nuisance quotidienne

De nombreux acteurs plus ou moins malveillants, réalisent de manière automatisée des actions pouvant nuire au fonctionnement du système d'information. Les scans, campagnes de spams, tentatives massives d'exploitation de vulnérabilités font partie de cette nuisance quotidienne.

Menace cybercriminelle

A but essentiellement lucratif, ces attaques visent à générer du profit au travers d'un acte malveillant sur un système d'information. Il peut s'agir de vol de données propriétaires, d'accès ou à caractère personnel à des fins de revente, de rançonnage par chiffrement ou déni de service, ou encore de manipulation de système bancaires. Ces attaques revêtent toujours un aspect opportuniste, mais peuvent aussi cibler une catégorie d'entités.

Menace étatique

Opérée par des attaquants soutenus par des Etats et particulièrement sophistiquées, ces attaques ciblent précisément des entités afin de récolter des informations stratégiques, technologiques et économiques, ou encore de réaliser des actions de sabotage.