RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES PARCOURS DE CYBERSÉCURITÉ : RAPPORT D'ACTIVITÉ 2023

Volet cybersécurité de France Relance

Financé par l'Union européenne
NextGenerationEU

SOMMAIRE

- **L'ensemble des données présentées dans ce rapport sont arrêtées au 31 décembre 2023.**
- **L'enquête de satisfaction des bénéficiaires a été réalisée du 27 avril 2021 au 31 décembre 2023.**
- **L'enquête de satisfaction des prestataires terrains a été réalisée du 20 janvier 2023 au 31 décembre 2023**

Les parcours de cybersécurité

1. Contexte et ambition du volet cybersécurité de France Relance

Dans le cadre du plan France Relance, le gouvernement a alloué 1,7 milliard d'euros d'investissements à la transformation numérique de l'État et des territoires. Ce plan intègre un **« volet cybersécurité », piloté par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui s'est élevé à 176 millions d'euros**.

100 millions d'euros ont été alloués spécifiquement au lancement et à la conduite du programme **« parcours de cybersécurité »** à destination des collectivités locales, d'établissements publics ciblés et des établissements de santé. Ce programme porte une **triple ambition** :

Elever le niveau de sécurité numérique de l'Etat et des services publics	Contribuer au renforcement du tissu industriel français de cybersécurité	Créer un effet de levier menant à un investissement durable dans la cybersécurité
Afin de renforcer la sécurité de leurs systèmes d'information, le plan propose aux acteurs publics de co-financer l'achat de prestations, de produits de sécurité et de formations. **Le programme vise en particulier à accroître de façon significative la couverture des solutions de détection des cyberattaques**.	**Le programme vise le développement de l'industrie de cybersécurité**, via notamment la promotion des services et produits de sécurité français et européens.	**Le programme incite les bénéficiaires à investir durablement dans la cybersécurité**, notamment en établissant un programme pluriannuel.

Les parcours de cybersécurité ont été conçus pour répondre de manière **rapide, personnalisée et directement opérationnelle** aux menaces les plus pressantes auxquelles font face les structures adressées. Une première étape de pré-diagnostic permet d'établir le niveau de maturité des systèmes d'information du bénéficiaire. Ensuite, l'accompagnement proposé se décompose en deux temps : **une phase d'audit standardisée** *(le pack initial)* et **une phase de mise en œuvre opérationnelle des mesures de sécurisation prioritaires** *(le pack relais)*.

Pack initial

- Série de **prestations standardisées** assurées par un prestataire terrain : actions de **sensibilisation, audits techniques et organisationnels**.
- Elaboration du plan de sécurisation.

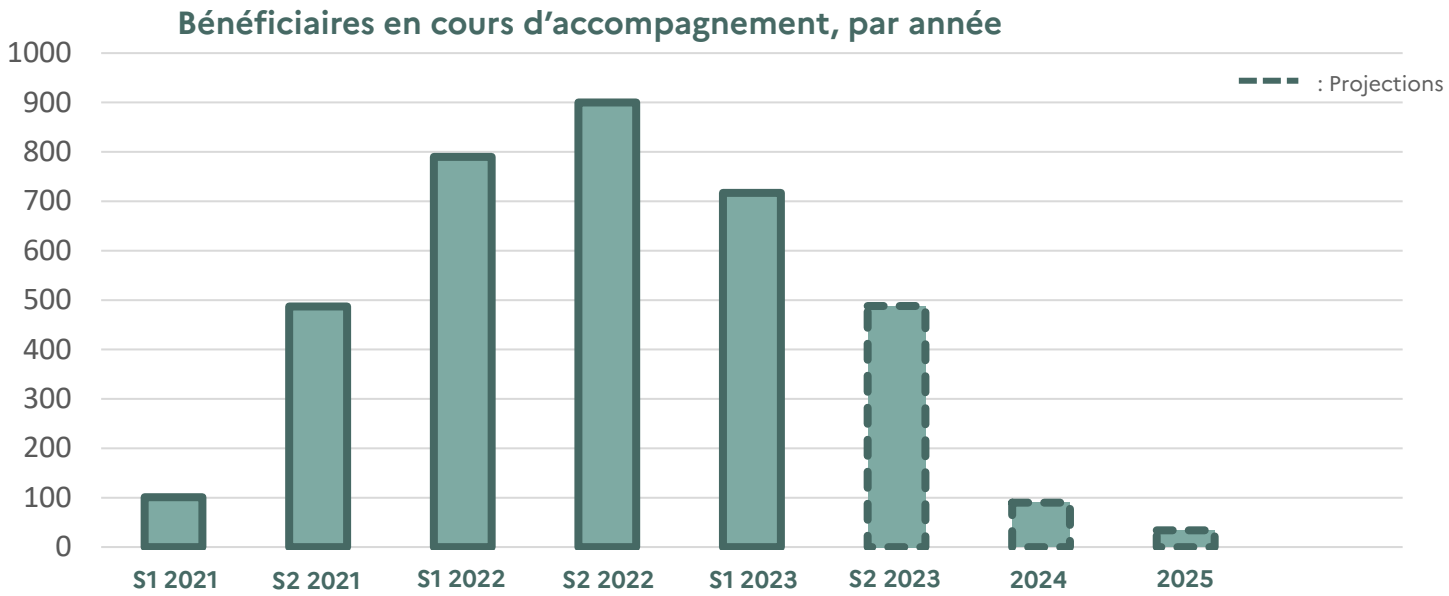
Pack relais

- **Mise en œuvre des mesures de sécurisation** : acquisition et installation de matériels et solutions de cybersécurité, recours à des prestations d'audit et d'expertise en cybersécurité.

« La démarche est réellement bien pensée. Elle privilégie une approche pragmatique de terrain à une démarche par conformité. »

Un prestataire terrain de la région Auvergne-Rhône-Alpes

2. Un programme pluriannuel en pleine phase opérationnelle en 2023

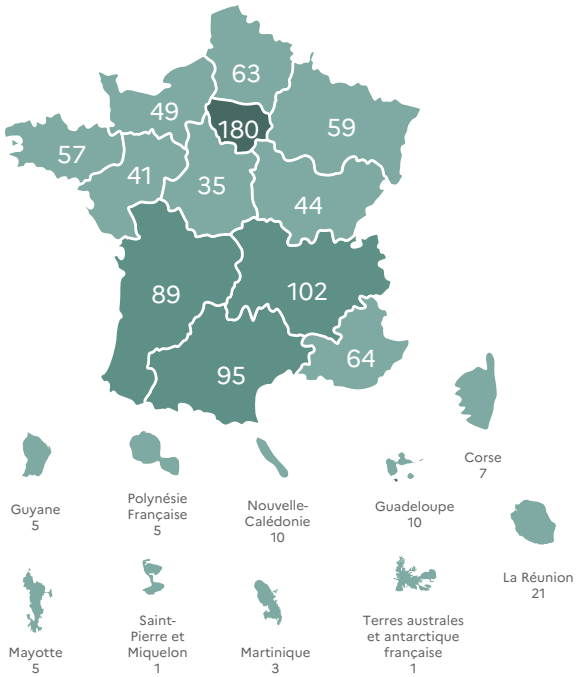


- **2021 a été l'année de lancement du programme.** Elle a permis, dans un délai particulièrement court, de concevoir le parcours, de l'éprouver avec des premières expérimentations, puis, une fois l'ensemble des acteurs mobilisés, de lancer la phase industrialisée des parcours avec le lancement **des premiers packs initiaux.**

- **2022 a permis au programme de passer en plein régime.** L'objectif fixé de 950 bénéficiaires, parmi des cibles pré-identifiées comme prioritaires et couvrant l'ensemble du territoire français, a été atteint. Par ailleurs, le programme a démontré son efficacité, illustrée tant par le haut niveau de satisfaction des bénéficiaires que par les premières réussites de conversion de packs initiaux en packs relais.

- **2023 a été marquée par la mise en œuvre effective des plans de sécurisation.** La grande majorité des bénéficiaires ont ainsi mis en œuvre les mesures urgentes identifiées lors des phases d'audit et ont pu s'engager dans des packs relais permettant la déclinaison opérationnelle des plans de sécurisation définis durant les packs initiaux.

Répartition géographique des bénéficiaires



- **2024 et 2025 seront les années d'atterrissage du programme.** L'enjeu sera de maintenir une bonne dynamique opérationnelle avec les bénéficiaires afin de faire aboutir les derniers packs relais au plus tard mi-2025.

Données à jour au 31/12/2023

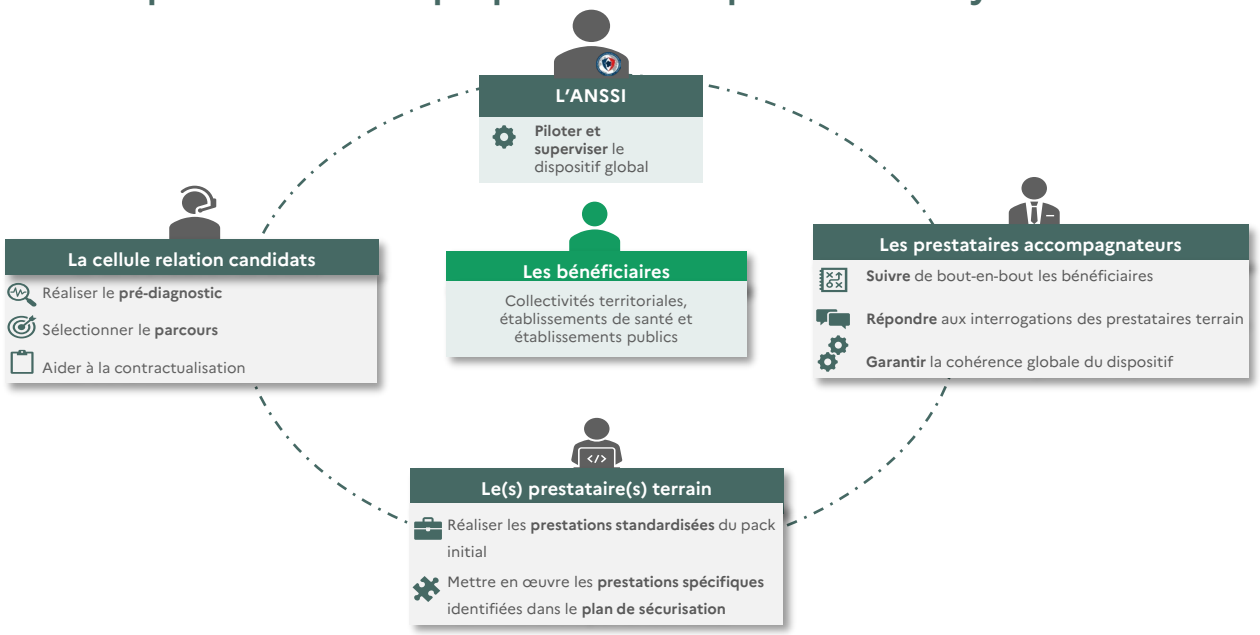
I. Une activité opérationnelle soutenue pour faire avancer et aboutir les parcours

1. La réussite des « packs initiaux » assurée par une forte mobilisation de tous les acteurs

La coordination des parties prenantes du programme

Le programme a été conçu pour **associer et coordonner un ensemble d'acteurs** au service de l'accompagnement des bénéficiaires.

Principaux acteurs impliqués dans les parcours de cybersécurité



Pour assurer la finalisation des packs initiaux, la mobilisation de l'ensemble des acteurs a été cruciale : **engagement des bénéficiaires** à conduire les travaux en parallèle de l'activité opérationnelle courante, **disponibilité des prestataires terrain** dans un contexte de tension du secteur de la cybersécurité, présence en continu des **prestataires accompagnateurs et des correspondants sectoriels et territoriaux de l'ANSSI** pour assurer un suivi respectant la vision stratégique et les objectifs du programme.

Grâce à la bonne coordination des parties prenantes, les parcours sont considérés comme **bénéfiques par une majorité de bénéficiaires et de prestataires**.

98%

des bénéficiaires se déclarent satisfaits de l'accompagnement proposé et du traitement de leur candidature

97%

des prestataires se déclarent satisfaits de la démarche proposée par les parcours

Une transition vers la phase opérationnelle matérialisée par l'élaboration concertée de « packs relais »

Le passage des packs initiaux vers les packs relais est un **moment sensible des parcours** pour toutes les parties prenantes. L'un des résultats clés de l'année 2023 est le **faible taux de sortie du parcours des entités bénéficiaires lors de cette transition.**

1,2%

des bénéficiaires seulement ont arrêté leur parcours à l'issue de leur pack initial

788

des 942 packs initiaux lancés depuis le début du programme ont d'ores et déjà été convertis en packs relais

Les **packs relais sont au cœur des objectifs du programme**. Ils sont élaborés **sur la base des plans de sécurisation** établis lors des packs initiaux, et sont construits de manière concertée par les entités bénéficiaires, les prestataires terrain, les prestataires accompagnateurs et avec la validation de l'ANSSI. Ils se concentrent sur la **mise en place de mesures de sécurité concrètes et opérationnelles** suivant quatre priorités.

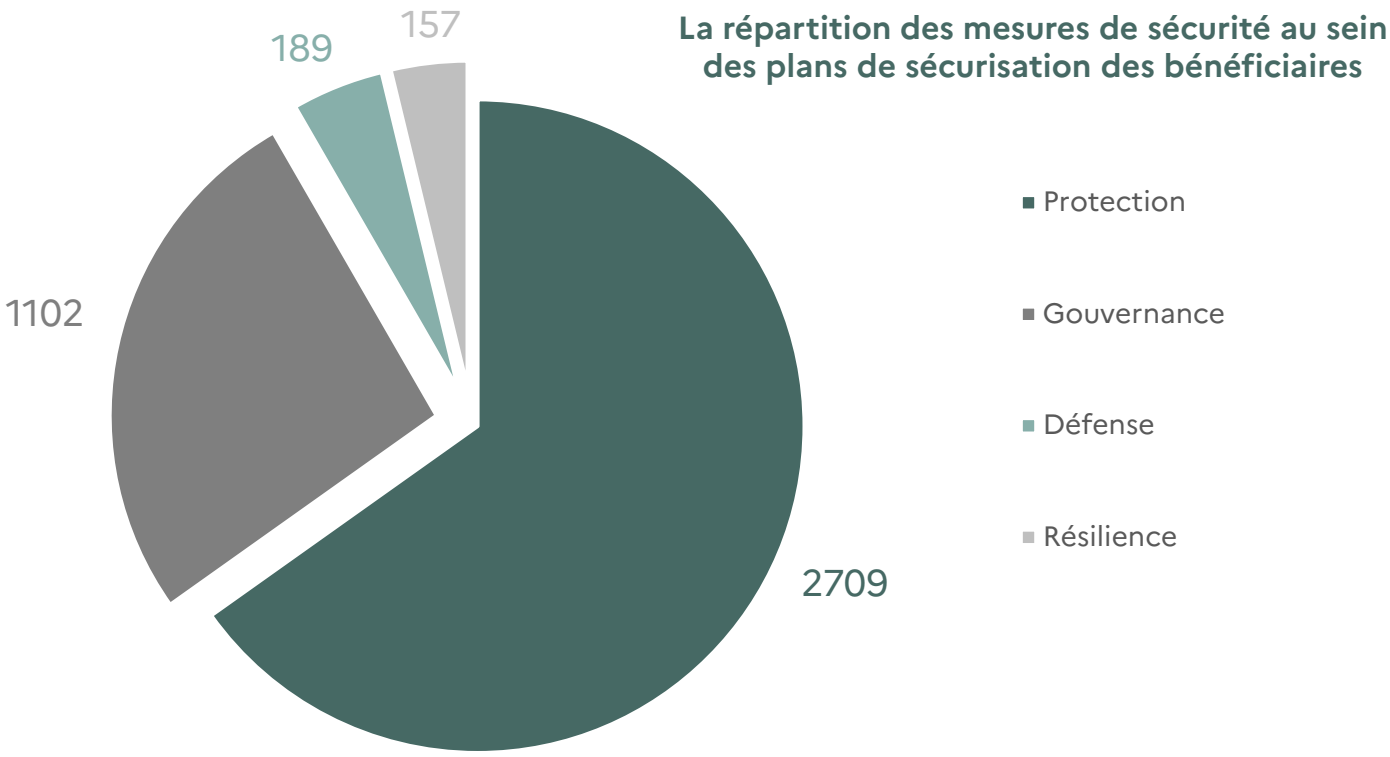
Protection : sécurisation de l'*active directory*, cloisonnement, filtrage pare-feu et *proxy*…

Gouvernance : veille, détection, journalisation, traitement des alertes…

Défense : politique de sécurité, sensibilisation au *phishing*…

Résilience : gestion des crises, plan de continuité d'activité, sauvegardes sécurisées…

La répartition des mesures de sécurité au sein des plans de sécurisation des bénéficiaires



Données à jour au 31/12/2023

2. Une bonne gestion des risques afin de faire aboutir les derniers parcours mi-2025

Moins standardisés et plus complexes opérationnellement, les packs relais présentent des **défis de mise en œuvre** nouveaux **pour les bénéficiaires** du programme :

> ***« Le rythme est très soutenu pour notre structure. Le manque de ressources humaines est un élément déterminant. »***
>
> Un centre hospitalier en région Auvergne-Rhône-Alpes

Une progression soutenue des packs relais

Grâce aux efforts et à la volonté des parties prenantes, l'avancement de l'ensemble des packs relais est globalement très satisfaisant. La **quasi-totalité des entités ont finalisé la majorité des actions** prévues dans leur plan de sécurisation **en moins d'un an**.

90%

des bénéficiaires ont effectué 50% ou plus des actions prévues dans leur pack relais à l'issue de leur parcours

Données à jour au 31/12/2023

Un suivi continu et rigoureux permettant l'atterrissage des packs relais

Fidèle à l'esprit initial du programme, qui vise à maximiser l'impact opérationnel des crédits, **les coûts de gestion sont maîtrisés.**

Dans une logique de prévention et de maîtrise des risques, **les accompagnateurs réalisent trois réunions de suivi** avec les bénéficiaires.

Ces points de suivi assurent le bon déroulement des parcours. Ils permettent **d'accompagner les bénéficiaires dans leurs démarches** et les **aider en cas de difficultés rencontrées lors de la mise en place des mesures** des plans de sécurisation.

1472

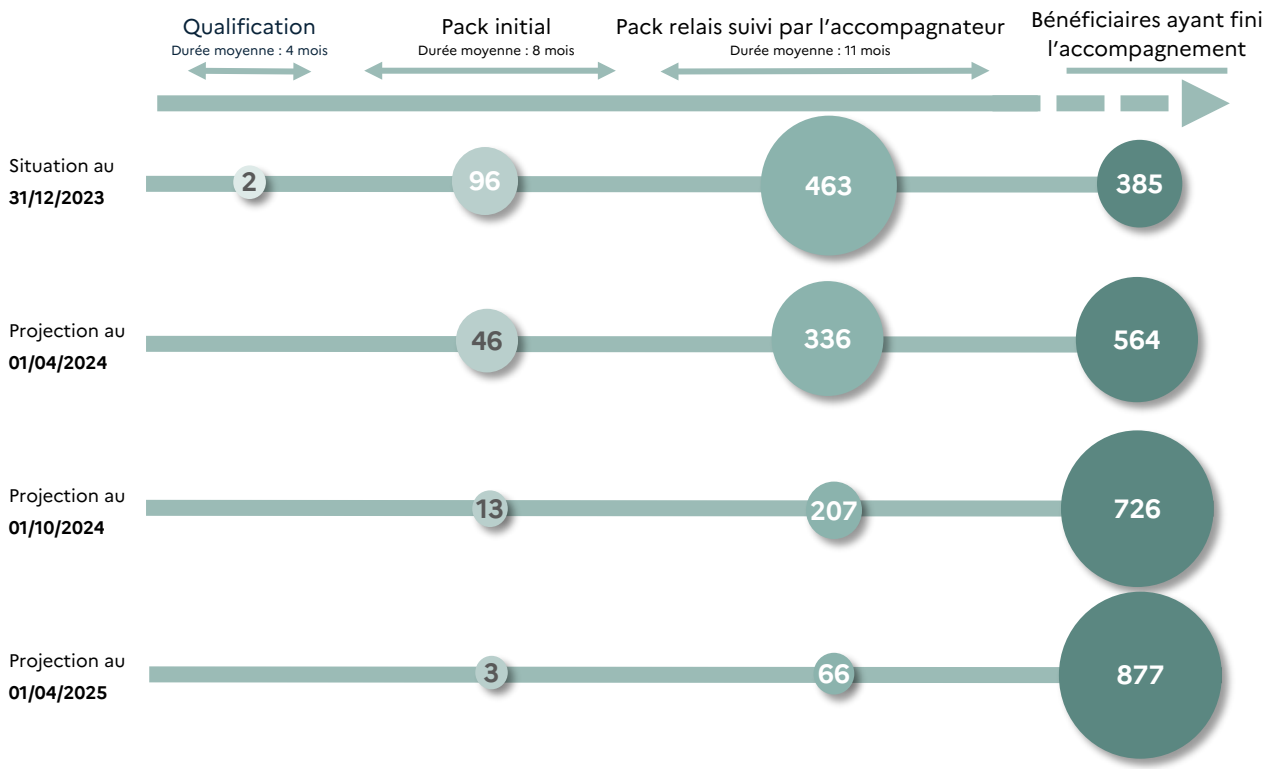
points de suivi effectués pour accompagner les plans de sécurisation sur la durée

« Tout a été conforme à nos attentes ! Le suivi est rassurant et sain dans une telle démarche. »

Une mairie de la région Provence-Alpes-Côte d'Azur

Une prévision de clôture des parcours à mi-2025 pour la quasi-totalité des bénéficiaires

La probabilité de rencontrer des risques augmente proportionnellement à la durée des parcours (rotation des équipes, changement d'orientation stratégique…). Par ailleurs, l'état de la menace rend impératif la sécurisation au plus tôt des systèmes d'information des bénéficiaires. **Il est donc nécessaire de finaliser un maximum de parcours dans un temps réduit.**



II. Les parcours de cybersécurité augmentent la protection et la défense des systèmes d'information

1. La cybersécurité repositionnée comme priorité stratégique

La sensibilisation des dirigeants, condition nécessaire à l'engagement d'une dynamique vertueuse et pérenne

La sensibilisation des dirigeants permet de leur **mettre en visibilité les vulnérabilités** de leurs systèmes d'information et les risques encourus.

96%

des prestataires terrain notent une amélioration de la sensibilité des dirigeants aux enjeux de cybersécurité à la suite des parcours

Les dirigeants sont **associés à l'ensemble de la démarche, de l'initialisation jusqu'à l'étape clé de la réunion de restitution en fin de pack initial**. Ils participent à la validation de leur plan de sécurisation, et à la préparation de la phase de pack relais.

« Beaucoup étaient déjà au courant de ce qu'il se passait, mais voir le score de maturité de leur entité, les actions prioritaires et la sensibilisation est très utile pour les dirigeants. C'est pour ça qu'il y a de bons retours sur la satisfaction. »

Un prestataire accompagnateur

Une re-priorisation des ressources humaines et budgétaires au service des enjeux de cybersécurité

En comprenant les enjeux liés à la cybersécurité, les dirigeants peuvent prendre des **décisions de manière plus éclairée**, ainsi qu'**allouer de manière plus optimale les ressources nécessaires pour renforcer leurs systèmes d'information**.

L'engagement des directions contribue à la mise en place de politiques, de bonnes pratiques et de mesures adéquates. **La cybersécurité devient alors une priorité stratégique des entités bénéficiaires**. Elle prend une place majeure au sein des feuilles de route numériques et bénéficie d'une augmentation des ressources humaines et budgétaires qui lui sont allouées.

En moyenne, le niveau d'investissement budgétaire des entités est

20% supérieur au montant prévu par le dispositif.

« Notre direction a été particulièrement bien sensibilisée à nos problématiques cyber et au besoin d'élever notre niveau. »

Un établissement public de la région Auvergne-Rhône-Alpes

2. L'impact durable des « packs initiaux » et des « packs relais » pour les bénéficiaires

Les objectifs des packs initiaux

- Sensibilisation des agents et des dirigeants
- Etat des lieux technique et organisationnel des systèmes d'information
- Accompagnement dans la définition et la mise en œuvre opérationnelle des actions de sécurisation

Un accent fort sur la sensibilisation des agents à la cybersécurité

8460

participants aux campagnes de sensibilisation

Des campagnes de sensibilisation ont été conduites auprès **de publics spécifiques** qui travaillent au plus proche des systèmes d'information vulnérables et qui **manipulent des données sensibles.**

Ressources humaines	Equipes achats	Développeurs	Administrateurs des systèmes d'information	Directions	Ingénieurs biomédicaux
• Accès aux données sensibles des employés • Gestion et accès aux contrats	• Accès aux contrats et informations financières sensibles • Interactions et échanges de documents fréquents avec les fournisseurs • Initiation des paiements aux prestataires	• Accès administrateurs • Accès aux codes sources et bases de données • Interactions avec des API et services externes	• Contrôle et gestion des systèmes informatiques • Accès aux identifiants et autorisations des utilisateurs • Gestion des pare-feu et autres dispositifs de sécurité	• Accès à des informations stratégiques • Influence forte sur la culture d'entreprise	• Accès à des données de santé sensibles des patients • Accès à des informations stratégiques liées à de nouveaux dispositifs médicaux

Publics visés et contenus des sensibilisations

Les principales vulnérabilités adressées par les campagnes de sensibilisation :

L'absence de politique de mot de passe, les postes de travail non sécurisés, les messageries exposées, l'absence d'isolation des sauvegardes…

Données à jour au 31/12/2023

Les audits organisationnels et techniques ont permis d'identifier et de prioriser les besoins les plus prégnants

La phase d'audit permet d'**identifier les failles et de mesurer le niveau de sécurité des systèmes d'information** des bénéficiaires. Elle permet de proposer des **recommandations concrètes pour renforcer la protection de leurs systèmes d'information** grâce à un **état des lieux complet.**

70%

des bénéficiaires estiment que le cadrage des prestations du pack initial a permis de mieux cibler leurs besoins

Les audits organisationnels et techniques sont complémentaires et permettent un état des lieux complet du niveau de sécurité des systèmes d'information des bénéficiaires

En **réponse aux constatations de la phase d'audits** organisationnels et techniques, **les entités comblent les failles les plus critiques de leurs systèmes d'information** grâce aux mesures correctives à court terme.

2655

mesures d'urgence de sécurisation validées

Parmi les **mesures de court terme les plus nécessaires**, se trouvent les mesures de **durcissement de l'*active directory***, le **cloisonnement des architectures**, mais aussi des mesures correctives **appliquées aux services exposés sur internet** via les applications web.

Le plan de sécurisation, schéma directeur de la cybersécurité des entités

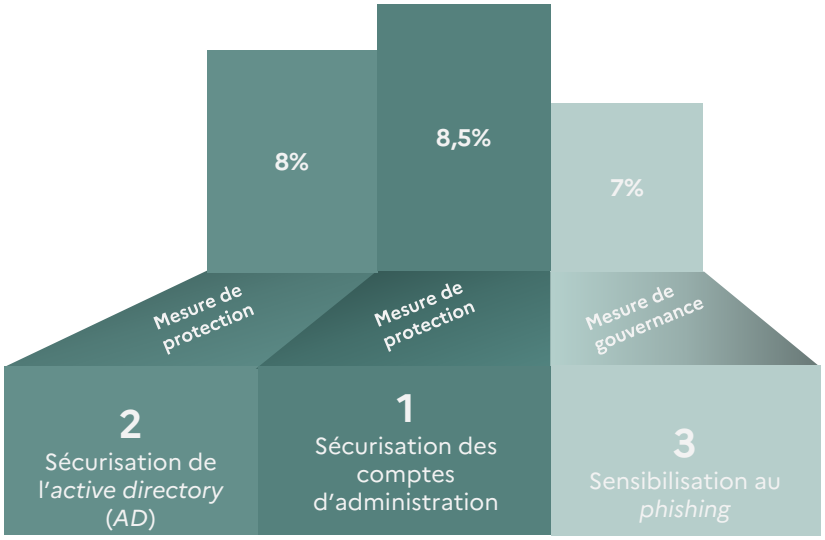
L'ensemble des travaux du pack initial permettent de **déterminer le plan de sécurisation**, qui constitue le **schéma directeur de la cybersécurité des entités** sur une période de 3 ans. Ce plan est **dimensionné au regard des capacités de la structure**, et **priorisé** en fonction des éléments analysés lors de la phase de pack initial.

Les parcours de cybersécurité ont pour but **d'accompagner à la mise en œuvre de la première partie de ce plan de sécurisation**, via la subvention et l'accompagnement des packs relais.

Données à jour au 31/12/2023

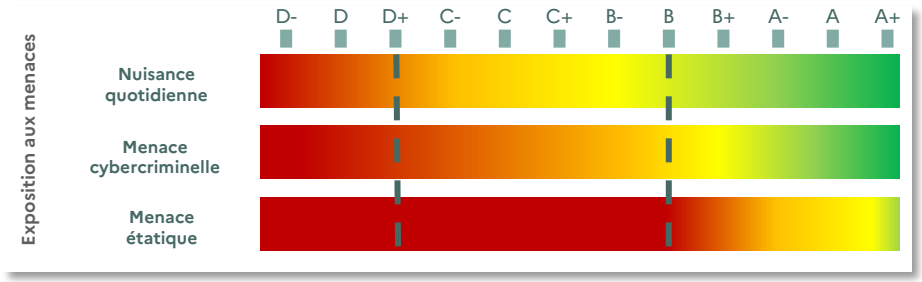
Les packs relais permettent d'améliorer la sécurité des systèmes d'information des entités bénéficiaires

Les packs relais permettent de mettre en œuvre les actions structurantes et prioritaires du plan de sécurisation. Ces actions peuvent relever de la prestation de service, de l'achat et l'installation de matériels ou de solutions. Parmi **l'ensemble des packs relais, les actions les plus mises en place sont** :



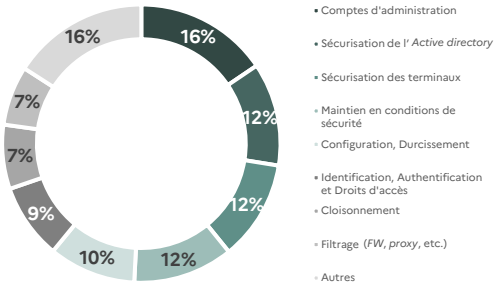
La mise en œuvre des packs relais permet **une amélioration à court terme du niveau de sécurité des systèmes d'information** des entités bénéficiaires.

Le relevé du cyberscore* de ces entités en début et en fin de parcours permet une évaluation globale des gains associés aux parcours. En moyenne, les bénéficiaires du parcours passent d'un cyberscore de D+ à B.

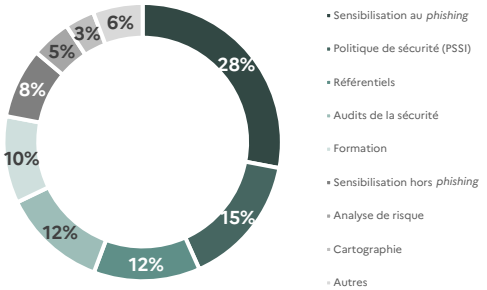


*Un détail méthodologique de lecture du cyberscore est disponible en annexe.

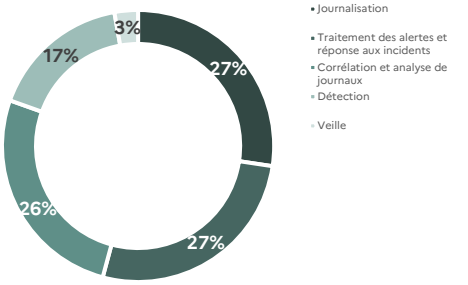
Protection



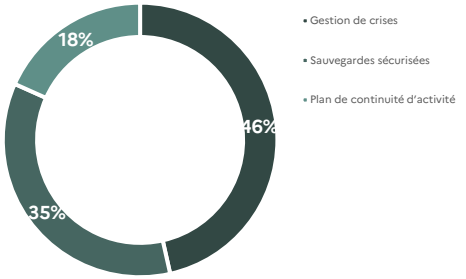
Gouvernance



Défense



Résilience



III. Un atout pérenne pour un renforcement global de la cybersécurité

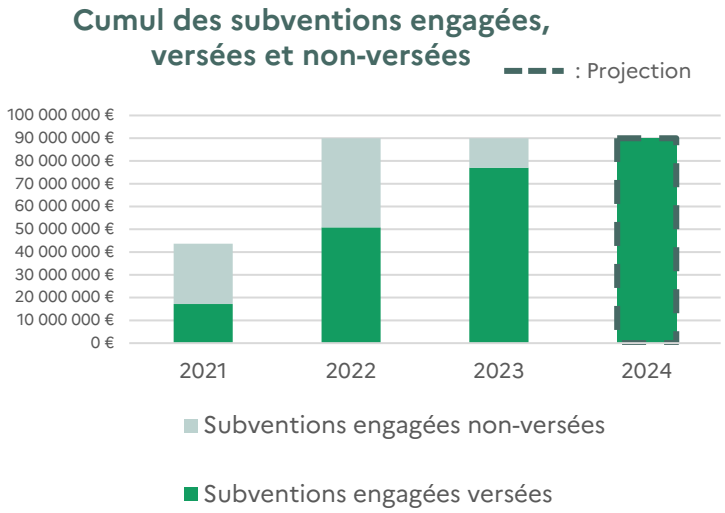
1. Des effets bénéfiques pour l'émergence d'acteurs de la cybersécurité sur le territoire français

Des avantages de long terme pour les bénéficiaires

Une fois les parcours finalisés, **l'amélioration de la sécurité des systèmes d'information doit être assurée de manière constante**. Grâce aux actions effectuées durant les parcours, **les bénéficiaires disposent des atouts nécessaires à l'amélioration continue de leur sécurité**.

Dans cette logique, l'ANSSI proposera des **outils de suivi** qui permettront aux entités bénéficiaires de **calculer leur cyberscore après avoir finalisé leur parcours**, mais aussi de **sensibiliser les nouveaux agents** au sein de leur structure de manière autonome.

Des avantages durables pour le tissu industriel français de cybersécurité



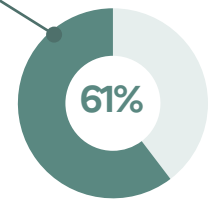
Les 90 millions d'euros de subventions engagés ont directement permis la **dynamisation de l'écosystème français et européen de la cybersécurité.** Grâce à **l'effet de levier, 123 millions d'euros ont été générés**.

193 prestataires différents ont ainsi contribué à la réalisation des packs initiaux et plus de 215 fournisseurs de solutions et de matériels ont été mobilisés pour les packs relais.

Les prestataires témoignent d'une **augmentation de la demande de services**, ainsi qu'une **augmentation en conséquence de leurs effectifs.**

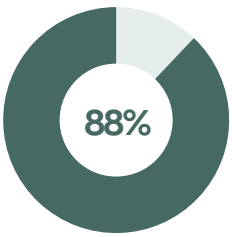
Impact sur les activités commerciales

61% des prestataires terrain déclarent que les parcours leur ont permis de **développer une offre de service similaire à destination d'autres organismes publics ou privés**



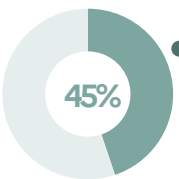
Impact sur les activités des entreprises

88% des prestataires terrain indiquent que le parcours a eu un **impact positif sur leur activité**



Impact sur le recrutement d'experts en cybersécurité

45% des prestataires terrain affirment que la demande générée par les parcours leur a permis de **renforcer leurs effectifs**



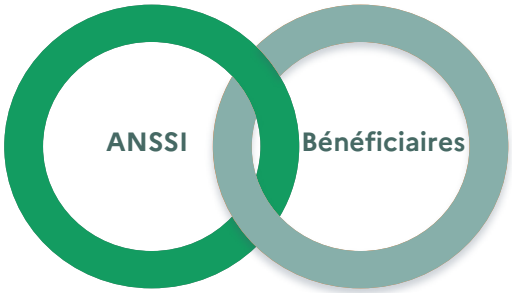
Données à jour au 31/12/2023

94%
des solutions mises en œuvre dans le cadre des packs relais sont françaises ou européennes

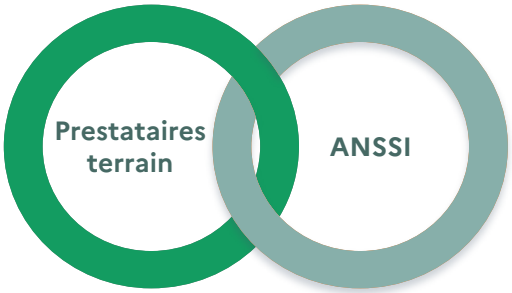
Les parcours de cybersécurité ont également permis de **redynamiser le tissu industriel de la cybersécurité** en France et en Europe.

Parmi les solutions mises en œuvre dans le cadre des packs relais, **79% sont des solutions françaises** et **15% sont des solutions européennes**.

Un renforcement des liens entre l'ANSSI et les bénéficiaires et prestataires impliqués dans les parcours de cybersécurité



Les parcours ont permis à l'ANSSI de **renforcer ses liens avec les bénéficiaires, et notamment avec certaines structures qui n'étaient pas les plus visibles ou accessibles** pour les correspondants sectoriels et territoriaux. Pour celles qui l'étaient déjà, cela a été l'occasion pour eux de **nouer ou de renforcer des liens avec les décideurs de haut niveau**.



L'ANSSI a pu échanger avec des prestataires s'étant avérés pertinents ou étant montés en compétence grâce aux parcours. Une **relation de confiance de long terme** en résulte. Cela permettra aux prestataires concernés de participer à long terme à la **mise en œuvre des différentes solutions proposées** dans l'offre de services de l'agence.

« Le programme nous a permis, via la relation contractuelle, de rentrer en contact avec le plus haut niveau de la collectivité. […] Le challenge est de poursuivre cette relation au-delà du parcours. »

Un correspondant territorial de l'ANSSI

Le renforcement des liens à la fois avec les bénéficiaires et les prestataires terrain est un effet bénéfique du programme pour toutes les parties prenantes et permet à l'ANSSI d'affirmer d'autant plus sa **place centrale dans l'écosystème de la cybersécurité** française.

Les parcours de cybersécurité offrent à l'ANSSI l'opportunité de maintenir des liens privilégiés avec les différents acteurs et bénéficiaires du programme.

Données à jour au 31/12/2023

2. Un impact à long terme du programme grâce à la mise à disposition des outils et à la capitalisation des productions

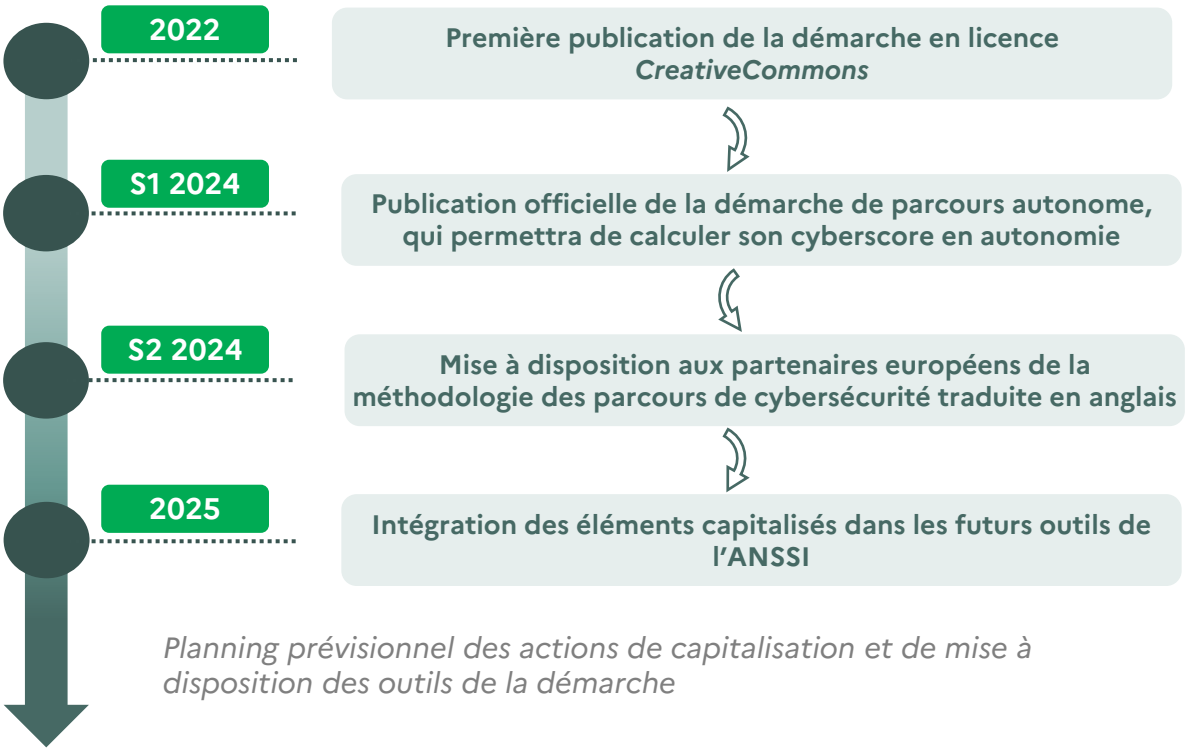
Une contribution de la France aux efforts internationaux relatifs à la cybersécurité

Les effets bénéfiques à long terme du programme s'étendent au-delà du territoire français. Les parcours **alimentent la contribution aux efforts internationaux en matière de cybersécurité**.

Cette contribution est permise par les **efforts de capitalisation des outils et productions du programme**. Le programme et ses méthodologies seront **traduits pour permettre aux agences de cybersécurité européennes de proposer le même type de parcours** à leurs entités publiques. De plus, l'ANSSI pourra **participer aux réflexions collectives au niveau international** grâce à l'expérience acquise avec la mise en œuvre des parcours de cybersécurité.

Un programme qui permettra d'alimenter l'offre de services de l'ANSSI

Les productions du programme et les méthodologies fournies par l'ANSSI **serviront de base de travail**, pour d'une part aider les bénéficiaires des parcours souhaitant poursuivre la sécurisation de leur système d'information dans le temps, et d'autre part alimenter l'offre de services de l'agence pour lui permettre de se préparer au mieux à accompagner les entités françaises dans leur conformité aux normes de sécurité des systèmes d'information.



Planning prévisionnel des actions de capitalisation et de mise à disposition des outils de la démarche

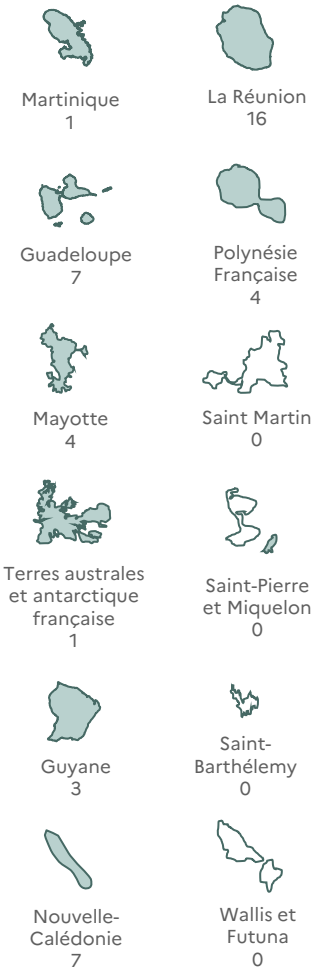
ANNEXES

SOMMAIRE DES ANNEXES

- L'ensemble des données présentées dans ce rapport sont arrêtées au 31 décembre 2023.
- L'enquête de satisfaction des bénéficiaires a été réalisée du 27 avril 2021 au 31 décembre 2023.
- L'enquête de satisfaction des prestataires terrains a été réalisée du 20 janvier 2023 au 31 décembre 2023

1. Répartition des collectivités territoriales accompagnées sur le territoire

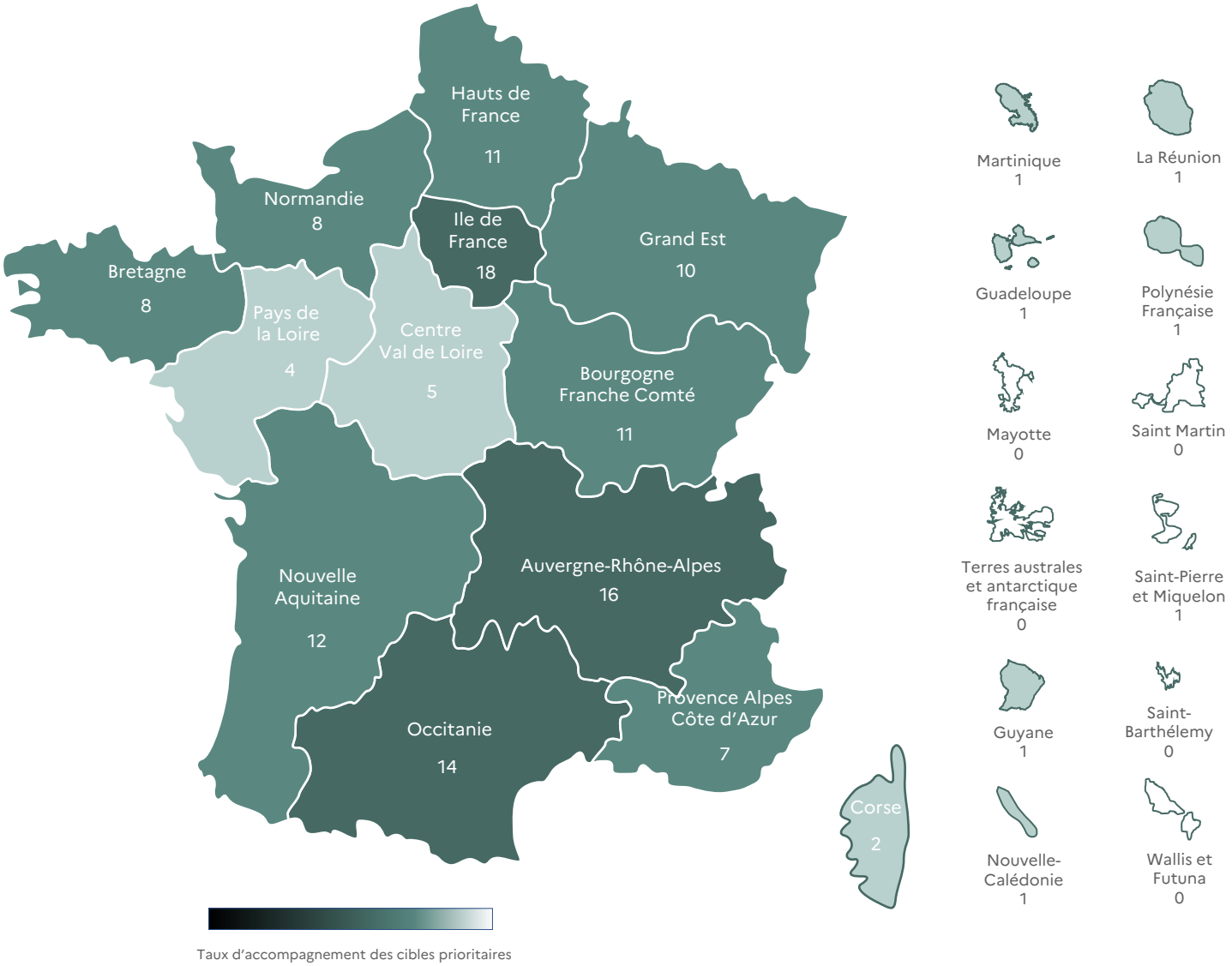
707
Collectivités territoriales accompagnées



Données à jour au 31/12/2023

2. Répartition des établissements de santé accompagnés sur le territoire

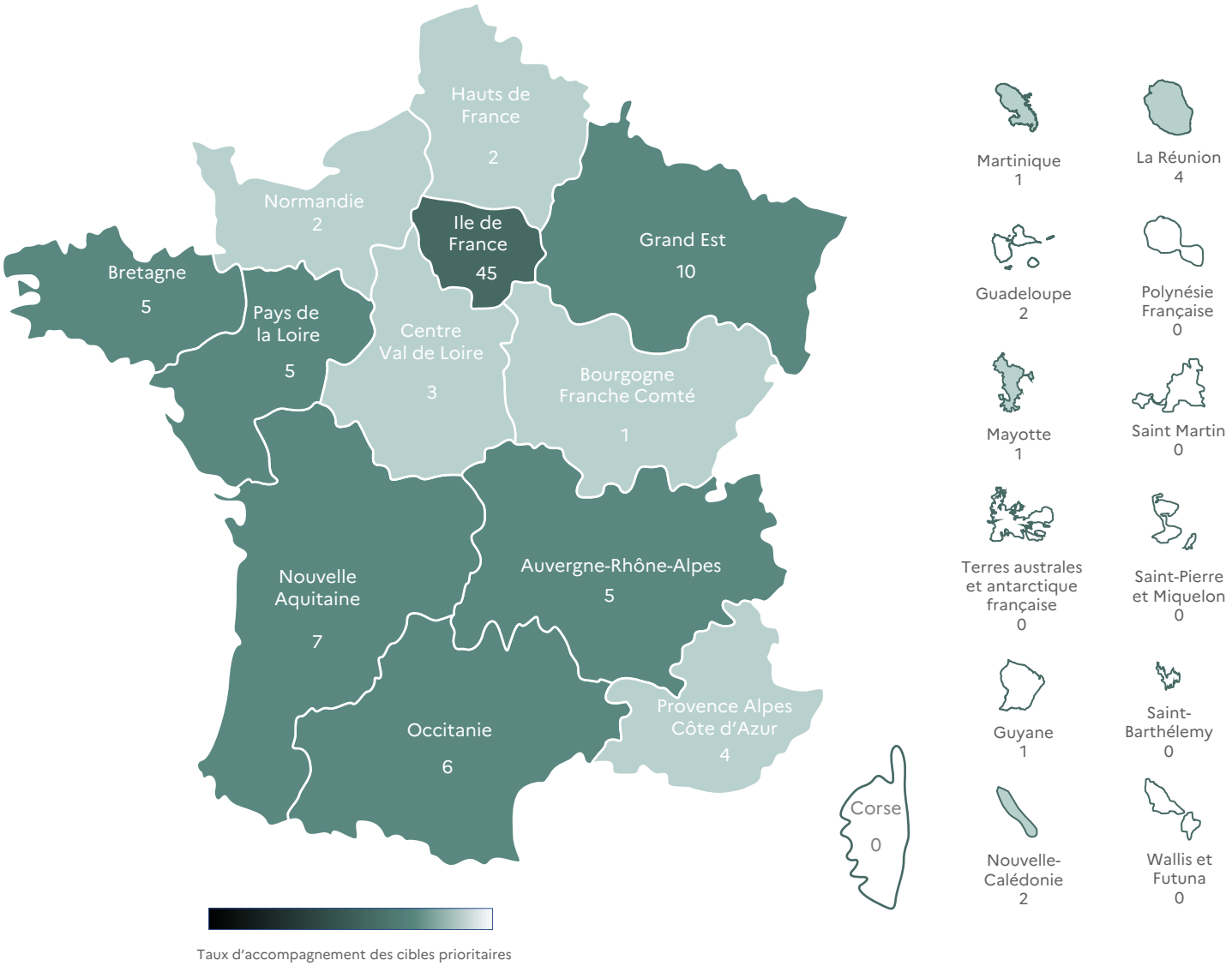
133
Etablissements de santé accompagnés



Données à jour au 31/12/2023

3. Répartition des établissements publics accompagnés sur le territoire

106
Etablissements publics accompagnés

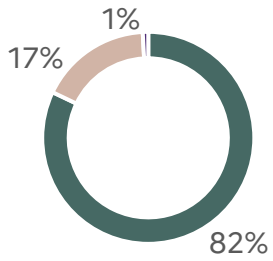


4. Résultats de l'enquête de satisfaction réalisée auprès des bénéficiaires (1/3)

Nombre total de répondants : 480

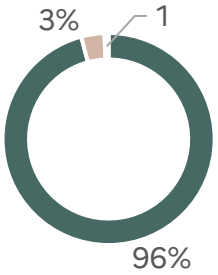
Je suis satisfait de l'offre de service des parcours de cybersécurité de l'ANSSI dont j'ai bénéficié

Tout à fait d'accord	394
Plutôt d'accord	82
Plutôt pas d'accord	4
Pas du tout d'accord	0



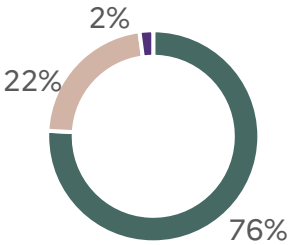
Je recommanderai les parcours de cybersécurité à d'autres structures publiques

8 ou plus	460
De 6 à 7	17
De 3 à 5	3
2 ou moins	0



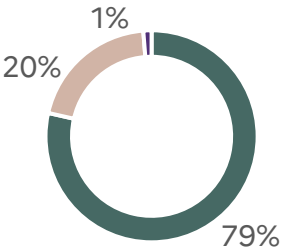
Lors de ma candidature, l'accompagnement proposé a été efficace et le traitement de celle-ci a été rapide

Tout à fait d'accord	364
Plutôt d'accord	106
Plutôt pas d'accord	10
Pas du tout d'accord	0



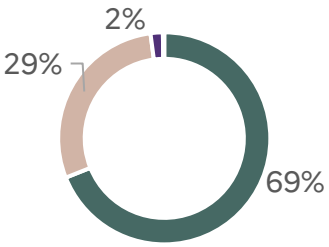
Les parcours de cybersécurité et les modalités de mise en œuvre m'ont bien été explicités

Tout à fait d'accord	377
Plutôt d'accord	97
Plutôt pas d'accord	6
Pas du tout d'accord	0



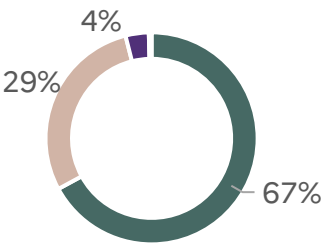
L'entretien de pré-diagnostic et le cadrage des prestations du pack initial ont permis de cibler mes besoins

Tout à fait d'accord	331
Plutôt d'accord	139
Plutôt pas d'accord	9
Pas du tout d'accord	1



La procédure de mise en relation et de contractualisation avec le prestataire terrain s'est bien déroulée et son délai de mise en œuvre a été rapide

Tout à fait d'accord	322
Plutôt d'accord	139
Plutôt pas d'accord	17
Pas du tout d'accord	2

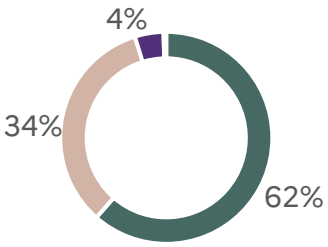


4. Résultats de l'enquête de satisfaction réalisée auprès des bénéficiaires (2/3)

Nombre total de répondants : 480

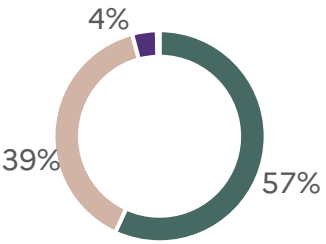
L'indice de cybersécurité qui m'a été attribué est compréhensible et pertinent

Tout à fait d'accord	295
Plutôt d'accord	162
Plutôt pas d'accord	21
Pas du tout d'accord	2



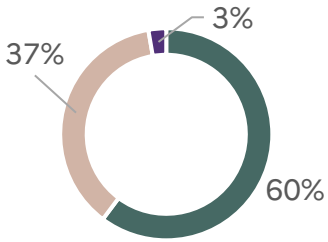
Les livrables de sensibilisation fournis étaient adaptés à mes besoins

Tout à fait d'accord	273
Plutôt d'accord	187
Plutôt pas d'accord	18
Pas du tout d'accord	2



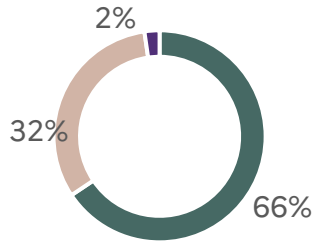
Les livrables d'état des lieux organisationnel fournis étaient adaptés à mes besoins

Tout à fait d'accord	289
Plutôt d'accord	178
Plutôt pas d'accord	13
Pas du tout d'accord	0



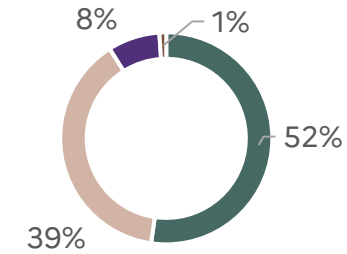
Les livrables d'état des lieux technique fournis étaient adaptés à mes besoins

Tout à fait d'accord	315
Plutôt d'accord	154
Plutôt pas d'accord	11
Pas du tout d'accord	0



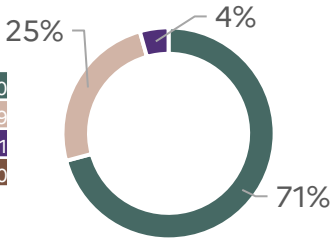
Le rythme de l'accompagnement et la charge de travail associée étaient appropriés

Tout à fait d'accord	251
Plutôt d'accord	186
Plutôt pas d'accord	38
Pas du tout d'accord	5



La répartition des rôles entre les différents interlocuteurs était claire

Tout à fait d'accord	340
Plutôt d'accord	119
Plutôt pas d'accord	21
Pas du tout d'accord	0

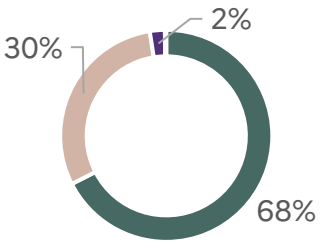


4. Résultats de l'enquête de satisfaction réalisée auprès des bénéficiaires (3/3)

Nombre total de répondants : 480

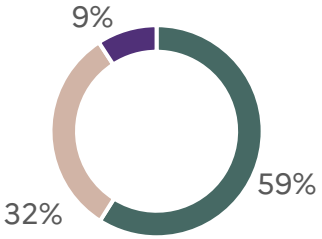
Le plan de sécurisation et les mesures associées me semblent pertinents au regard du contexte de ma structure

Tout à fait d'accord	324
Plutôt d'accord	144
Plutôt pas d'accord	11
Pas du tout d'accord	1



Quel est votre degré de confiance sur la capacité de votre organisation à mettre en œuvre ce plan de sécurisation ?

8 ou plus	283
De 6 à 7	153
De 3 à 5	44
2 ou moins	0

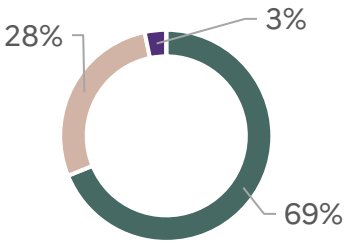


5. Résultats de l'enquête de satisfaction réalisée auprès des prestataires terrain (1/2)

Nombre total de répondants : 61

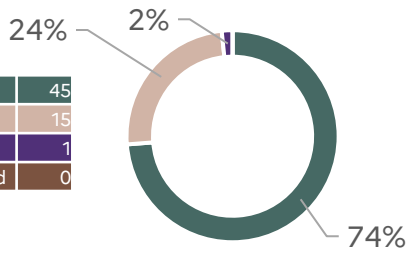
Je suis satisfait du déroulé du ou des parcours de cybersécurité que j'ai réalisé(s) en tant que prestataire terrain

Tout à fait d'accord	42
Plutôt d'accord	17
Plutôt pas d'accord	2
Pas du tout d'accord	0



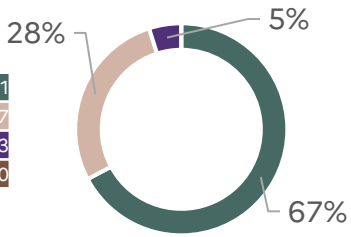
Le contenu des parcours de cybersécurité et les modalités de leur mise en œuvre m'ont été clairement explicités

Tout à fait d'accord	45
Plutôt d'accord	15
Plutôt pas d'accord	1
Pas du tout d'accord	0



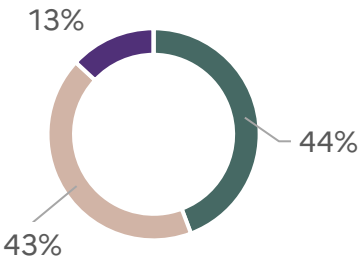
La démarche a permis à chaque bénéficiaire de construire un plan de sécurisation élevant durablement son niveau de sécurité

Tout à fait d'accord	41
Plutôt d'accord	17
Plutôt pas d'accord	3
Pas du tout d'accord	0



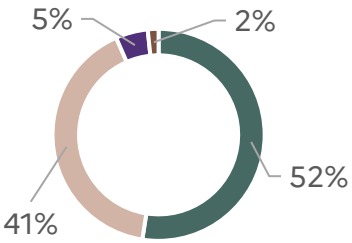
La démarche permet de sécuriser les SI des bénéficiaires au plus tôt grâce au volet « Mesures urgentes »

Tout à fait d'accord	27
Plutôt d'accord	26
Plutôt pas d'accord	8
Pas du tout d'accord	0



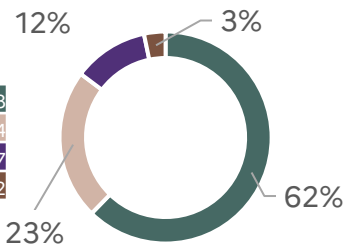
Cette démarche place les sujets de cybersécurité au cœur des priorités des dirigeants et constitue ainsi une amorce pour pérenniser l'investissement dans la SSI

Tout à fait d'accord	32
Plutôt d'accord	25
Plutôt pas d'accord	3
Pas du tout d'accord	1



Les parcours de cybersécurité ont fait appel aux prestataires locaux et les ont mis en valeur

Tout à fait d'accord	38
Plutôt d'accord	14
Plutôt pas d'accord	7
Pas du tout d'accord	2

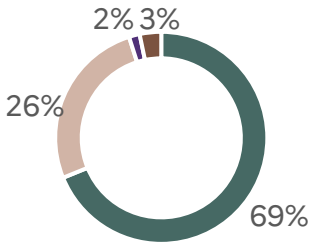


5. Résultats de l'enquête de satisfaction réalisée auprès des prestataires terrain (2/2)

Nombre total de répondants : 61

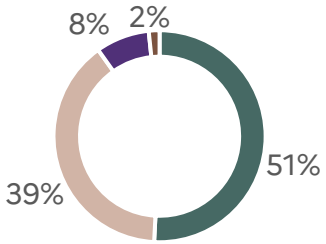
La démarche fournit une méthodologie claire et cohérente

Tout à fait d'accord	42
Plutôt d'accord	16
Plutôt pas d'accord	1
Pas du tout d'accord	2



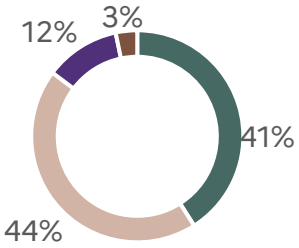
Les contenus, guides et modèles de livrables fournis dans le fond documentaire ont été rapidement appréhendés

Tout à fait d'accord	31
Plutôt d'accord	24
Plutôt pas d'accord	5
Pas du tout d'accord	1



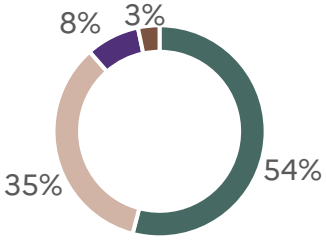
Les parcours de cybersécurité nous ont permis de monter en compétence grâce à l'appui méthodologique

Tout à fait d'accord	25
Plutôt d'accord	27
Plutôt pas d'accord	7
Pas du tout d'accord	2



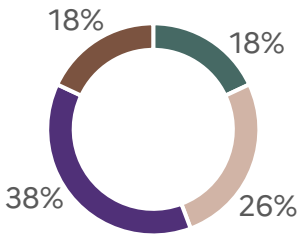
Les parcours de cybersécurité ont eu un impact positif sur notre activité

Tout à fait d'accord	33
Plutôt d'accord	21
Plutôt pas d'accord	5
Pas du tout d'accord	2



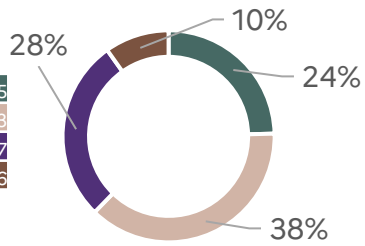
La demande générée par les parcours de cybersécurité a été l'occasion de renforcer nos effectifs

Tout à fait d'accord	11
Plutôt d'accord	16
Plutôt pas d'accord	23
Pas du tout d'accord	11



Les parcours de cybersécurité ont été l'occasion de développer une offre de services similaire à destination d'autres organismes publics ou privés

Tout à fait d'accord	15
Plutôt d'accord	23
Plutôt pas d'accord	17
Pas du tout d'accord	6



6. Indicateurs (1/3)

Indicateur	Résultat de l'indicateur
Nombre de parcours suivis	946 bénéficiaires
Nombre de collectivités territoriales bénéficiaires	707 collectivités territoriales
Nombre d'établissements de santé bénéficiaires	133 établissements de santé
Nombre d'établissements publics bénéficiaires	106 établissements publics
Nombre d'abandons avant contractualisation	11 bénéficiaires du programme l'ont abandonné avant de lancer leur pack initial
Taux des bénéficiaires n'ayant pas converti leur pack initial en pack relais	1,2% des bénéficiaires n'ont pas converti leur pack initial en pack relais
Nombre de pack initiaux convertis en packs relais depuis le début du programme	788 packs initiaux ont été convertis en pack relais depuis le début du programme
Taux de satisfaction des bénéficiaires vis-à-vis de la capacité de l'entretien de pré-diagnostic et de cadrage des prestations à cibler leurs besoins	98% des bénéficiaires se sont déclarés satisfaits
Taux de satisfaction des bénéficiaires envers l'accompagnement proposé lors du parcours et le traitement de leur candidature	98% des bénéficiaires se sont déclarés satisfaits
Taux de satisfaction global des prestataires terrain	97% des prestataires terrain se déclarent satisfaits du programme
Part des prestataires terrain indiquant que le programme a eu un impact positif sur leur entreprise	88% des prestataires terrain indiquent que le programme a eu un impact positif sur leur entreprise
Part des prestataires terrain déclarant que les parcours de cybersécurité leur ont permis de développer une offre similaire à destination d'autres organismes publics ou privés	61% des prestataires terrain déclarent que les parcours de cybersécurité leur ont permis de développer une offre similaire à destination d'autres organismes publics ou privés
Part des prestataires terrain affirmant que la demande générée par les parcours de cybersécurité leur a permis de renforcer leurs effectifs	45% des prestataires terrain affirment que la demande générée par les parcours de cybersécurité leur a permis de renforcer leurs effectifs
Part des prestataires terrain indiquant une amélioration de la sensibilité des dirigeants aux enjeux de cybersécurité à la suite des parcours	96% des prestataires terrain indiquent une amélioration de la sensibilité des dirigeants aux enjeux de cybersécurité à la suite des parcours

Données à jour au 31/12/2023

6. Indicateurs (2/3)

Indicateur	Résultat de l'indicateur
Nombre de mesures de protection au sein des plans de sécurisation	2709 mesures de protection au sein des plans de sécurisation
Nombre de mesures de défense au sein des plans de sécurisation	189 mesures de défense au sein des plans de sécurisation
Nombre de mesures de gouvernance au sein des plans de sécurisation	1102 mesures de gouvernance au sein des plans de sécurisation
Nombre de mesures de résilience au sein des plans de sécurisation	157 mesures de résilience au sein des plans de sécurisation
Taux de bénéficiaires de packs relais ayant effectué 50% ou plus des actions prévues dans leur plan de sécurisation à l'issue de leur parcours	90% des bénéficiaires de packs relais ont effectué 50% ou plus des actions prévues dans leur plan de sécurisation à l'issue de leur parcours
Nombre de points de suivi effectués pour accompagner les plans de sécurisation	1472 points de suivi effectués depuis le début du programme
Nombre de bénéficiaires en qualification au 31/12/2023	2 bénéficiaires sont en qualification au 31/12/2023
Nombre de bénéficiaires en pack initial au 31/12/2023	96 bénéficiaires sont en cours de pack initial au 31/12/2023
Nombre de bénéficiaires en pack relais au 31/12/2023	463 bénéficiaires sont en cours de pack relais au 31/12/2023
Nombre de bénéficiaires ayant fini l'accompagnement au 31/12/2023	385 bénéficiaires ont fini l'accompagnement au 31/12/2023
Nombre d'agents sensibilisés aux bonnes pratiques et aux enjeux de cybersécurité dans le cadre du programme	8460 agents sensibilisés
Nombre de mesures d'urgence de sécurisation validées	2655 mesures d'urgence de sécurisation validées
Part de la mesure la plus la plus présente dans les plans de sécurisation	8,5% des plans de sécurisation contiennent une mesure de sécurisation des comptes d'administration

Données à jour au 31/12/2023

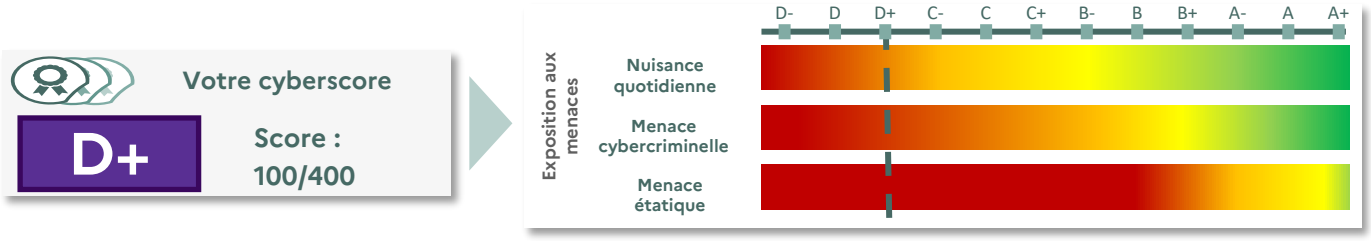
6. Indicateurs (3/3)

Indicateur	Résultat de l'indicateur
Part de la seconde mesure la plus présente dans les plans de sécurisation	8% des plans de sécurisation contiennent une mesure de sécurisation de l'*active directory*
Part de la troisième mesure la plus présente dans les plans de sécurisation	7% des plans de sécurisation contiennent une mesure de sensibilisation au *phishing*
Moyenne de supériorité du niveau d'investissement budgétaire des entités par rapport au montant prévu par le dispositif	En moyenne le niveau d'investissement budgétaire des entités est 20% supérieur au montant prévu par le dispositif
Cyberscore moyen des entités en début de parcours	D+
Cyberscore moyen des entités en fin de parcours	B
Subventions engagées en 2021 en euros	43 680 000€ de subventions engagés en 2021
Subventions engagées et versées en 2021 en euros	17 150 000€ de subventions versés en 2021
Subventions engagées en 2022 en euros, en cumulé	90 000 000€ de subventions engagés de 2021 à 2022
Subventions versées en 2022 en euros, en cumulé	50 820 000€ de subventions versés de 2021 à 2022
Subventions engagées en 2023 en euros, en cumulé	90 000 000€ de subventions engagés de 2021 à 2023
Subventions versées en 2023 en euros, en cumulé	77 040 000€ de subventions versés de 2021 à 2023

Données à jour au 31/12/2023

7. Qu'est-ce que le cyberscore ? (1/2)

Le cyberscore a pour but de visualiser concrètement le **niveau de vulnérabilité des systèmes d'information** face à trois types de menaces : les **nuisances quotidiennes**, les **menaces cybercriminelles** et les **menaces étatiques**. Il est synthétisé sur une échelle graduée allant de **de D- à A+**.



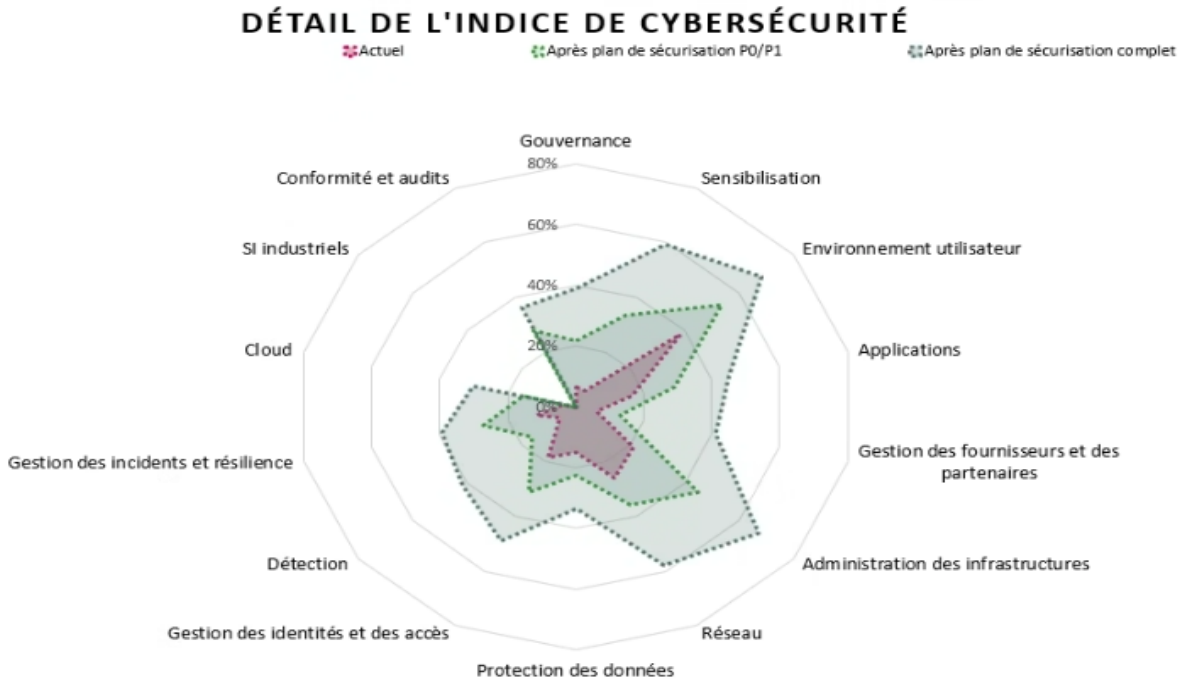
Il est **calculé à deux reprises lors des parcours** :

D'abord à partir de **l'état des lieux organisationnel** du pack initial, dont le résultat correspond au **score actuel** de l'entité.

Ensuite, lorsque le **plan de sécurisation** est défini, **deux projections du cyberscore** sont effectuées, dont le résultat varie en fonction du nombre de mesures qui seront mises en place.

Comment est calculé le cyberscore ?

Le cyberscore est noté sur un total de 400 points, sur la base d'une évaluation prenant en compte **14 thèmes de la cybersécurité** : le niveau de gouvernance des SI, la sécurité des réseaux, le niveau de protection des données ou encore la conformité des audits.

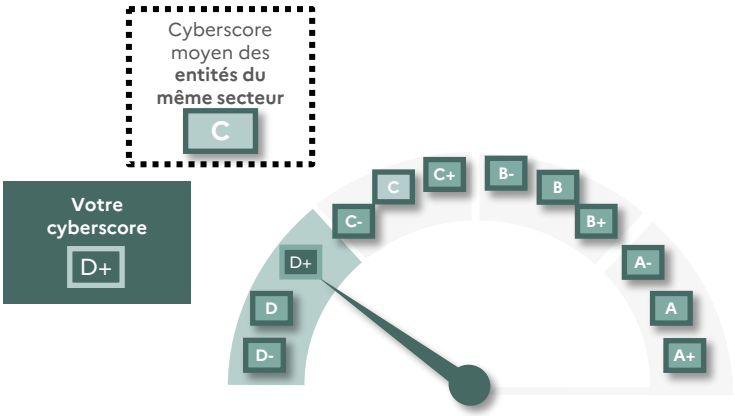


Données à jour au 31/12/2023

7. Qu’est-ce que le cyberscore ? (2/2)

Comment calculer son cyberscore en autonomie ?

L’ANSSI fournira prochainement un outil de calcul du cyberscore. Les entités pourront ainsi calculer leur cyberscore **en autonomie** pour suivre l’amélioration de leur cyberscore durant la mise en place des actions du plan de sécurisation, ainsi qu’à l’issue des parcours.



De plus, cet outil permettra aux entités de **comparer leur cyberscore à celui d’autres entités** du même secteur, et de taille similaire, afin **d’ajuster les objectifs** et la feuille de route relative à la sécurité de leur système d’information.

Pour en savoir plus sur les parcours de cybersécurité :
cyber.gouv.fr/parcours-de-cybersecurite

Version 1.0 – Mars 2024

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.cyber.gouv.fr