RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES PARCOURS DE CYBERSÉCURITÉ : RAPPORT D'ACTIVITÉ 2024

Volet cybersécurité de France Relance

Financé par l'Union européenne
NextGenerationEU

FRELANCE

PRÉFACE

Courant 2020, face à une crise sanitaire inédite, le plan France Relance, voulu par le Président de la République, a insufflé un dynamisme nouveau dans notre société. Dans ce contexte de numérisation accélérée, le gouvernement a alloué 1,7 milliard d'euros d'investissements à la transformation numérique de l'État et des territoires, intégrant également un volet « cybersécurité » pour répondre à l'explosion des cyberattaques. Piloté par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), ce volet 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 de collectivités territoriales et d'établissements publics, dont des établissements de santé. L'ANSSI a conçu, piloté et déployé ce dispositif d'accompagnement. Ces « parcours de cybersécurité » avaient pour ambition d'élever la sécurité numérique de ces services publics, de dynamiser l'industrie de cybersécurité française et européenne et de favoriser des investissements durables au service de la cybersécurité des organisations.

Dès 2021, grâce à un écosystème de prestataires, le programme est déployé à grande échelle. Sur le territoire national, ce sont rapidement près de 900 bénéficiaires qui manifestent leur intérêt en s'engageant dans un « parcours », révélant ainsi un fort besoin de cybersécurité dans les services publics au sein des territoires. Toutefois, des défis apparaissent : montée en charge rapide, contraintes organisationnelles et besoin d'adaptation des prestataires eux-mêmes. L'ANSSI adapte le dispositif et met en place un cadre de suivi pour accompagner les bénéficiaires et assurer une transition efficace de leurs plans d'action en plans de réalisation.

L'année 2022 marque l'entrée en régime opérationnel du programme. L'objectif de 950 bénéficiaires sur tout le territoire est atteint. Le programme démontre son efficacité, avec un haut niveau de satisfaction des premières organisations qui achèvent leur parcours et une mobilisation accrue des collectivités territoriales et des établissements de santé, victimes emblématiques des attaques lors de la crise sanitaire. Une attention particulière est maintenue dans la coordination entre prestataires et bénéficiaires, tout en prenant en compte les défis budgétaires et administratifs de ces derniers.

En 2023, le programme amorce un nouveau virage : avec plus de 80 % de ses bénéficiaires engagés dans la réalisation effective de leurs chantiers de durcissement de leur sécurité, l'heure est aux premiers bilans et ils sont positifs. D'une part le score de maturité cyber moyen progresse en passant de « D+ » à « B », attestant d'un renforcement significatif de la cybersécurité des organisations, et d'autre part, l'offre nationale et européenne de produits cyber est renforcée et les prestataires locaux soutenus. L'ANSSI reste néanmoins vigilante face aux manques de ressources humaines, à certaines complexités techniques et aux délais de contractualisation qui ralentissent les bénéficiaires les plus en difficulté. Conséquemment, l'Agence met en place de nouveaux outils de suivi post-parcours et encourage la pérennisation des efforts.

Ce dernier rapport présente les travaux entrepris sur 2024, année de clôture du programme sur le plan financier. Si le travail nominal a été poursuivi dans l'accompagnement des bénéficiaires, un effort significatif a été produit sur les derniers mois pour « raccrocher » les structures les plus en difficulté, leur permettre de reprendre et clore leurs actions de sécurisation. Accompagner tout le monde, jusqu'au bout.

Plus qu'un projet, c'est une méthodologie qui a été coconstruite avec notre écosystème et est désormais mise à la disposition de tous, démontrant qu'il était possible collectivement d'avoir un impact concret sur la cybersécurité de nos services publics. C'est également un élan général qui se traduit par une dynamique pérenne et des bénéficiaires qui poursuivent désormais en autonomie leur feuille de route.

Vincent Strubel
Directeur général de l'ANSSI

SOMMAIRE

- **L'ensemble des données présentées dans ce rapport sont arrêtées au 31 décembre 2024.**
- **L'enquête de satisfaction des bénéficiaires a été réalisée du 27 avril 2021 au 31 décembre 2023.**
- **L'enquête de satisfaction des prestataires terrain a été réalisée du 20 janvier 2023 au 31 décembre 2023.**
- **Les résultats complets de ces enquêtes sont disponibles en annexe du rapport d'activité 2023 des parcours de cybersécurité.**

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, qui s'est élevé à 176 millions d'euros.

Le volet cybersécurité de France Relance est composé de 7 axes

1. Axe « Support interne »
2. Axe « Diagnostics, sécurisation et accompagnement »
3. Axe « Produits »
4. Axe « Cyberdéfense active »
5. Axe « Réseau des CSIRT territoriaux »
6. Axe « Dépollution des flux des opérateurs de communication »
7. Axe « Détection »

100 millions d'euros ont été alloués spécifiquement à l'axe 2 « Diagnostics, sécurisation et accompagnement », pour permettre la conception, le lancement et la conduite du **programme « parcours de cybersécurité ».** Destiné à des collectivités territoriales et à des établissements publics, dont des établissements de santé, ce programme s'inscrivait dans la continuité de la **Revue stratégique de cyberdéfense** de 2018 et couvrait une **triple ambition** :

1. Elever le niveau de sécurité numérique de l'Etat et des services publics

→ Afin de renforcer la sécurité de leurs systèmes d'information, le plan proposait aux acteurs publics de **cofinancer** l'achat de prestations et de produits de sécurité. **Le programme visait en particulier à accroître de façon significative la couverture des solutions de détection des cyberattaques.**

2. Contribuer au renforcement du tissu industriel français de cybersécurité

→ **Le programme visait le développement de l'industrie de cybersécurité**, via notamment la promotion des services et produits de sécurité français et européens. Essentielle à la sécurité de nos services publics, cette industrie se doit d'être pérenne et performante.

3. Créer un effet de levier menant à un investissement durable dans la cybersécurité

→ Le programme incite les bénéficiaires à **investir durablement dans la cybersécurité**, notamment en établissant un programme pluriannuel qui doit permettre de démultiplier les bénéfices et les déployer dans un temps long.

La nécessité d'apporter une réponse spécifique au besoin de sécurisation croissant des entités publiques

La cybercriminalité : des entités publiques ciblées

En **2021**, en moyenne,
1 incident / par semaine
intervenait dans une **entité du secteur de la santé**

Attaques par rançongiciel, défigurations de sites, fuites de données… les collectivités territoriales, les établissements de santé et les structures publiques de manière générale subissent **des cyberattaques qui gagnent en intensité**. Ces menaces compromettent la **continuité** et la **fiabilité de leurs services**, ainsi que la **protection de leurs données**. Le risque numérique devient systémique ; il devient stratégique de le maîtriser.

La cybersécurité : des entités publiques vulnérables

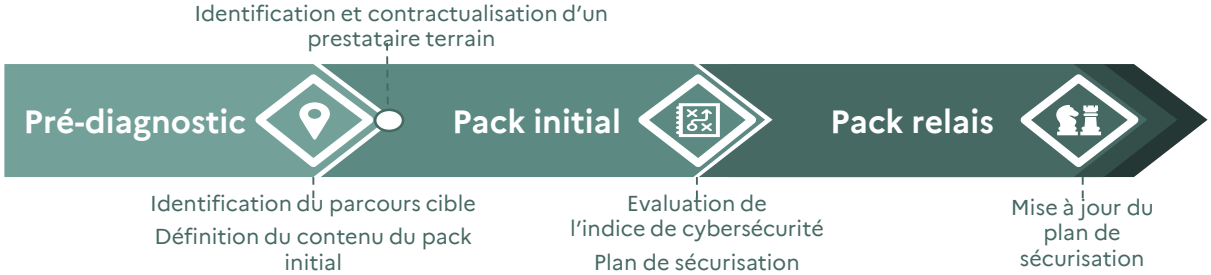
Ces attaques exploitent la **dette cyber** des entités publiques, souvent freinées par une faible culture numérique, à laquelle s'est ajoutée la mise en œuvre accélérée de la transformation numérique. Avec la dématérialisation des démarches administratives, la gestion des données sensibles des citoyens, l'interconnexion des systèmes, l'ouverture sur internet, il est urgent de faire de la cybersécurité une **priorité stratégique**, à la hauteur des nouveaux risques du numérique.

Les parcours de cybersécurité : proposer une démarche de sécurisation

Les entités publiques manquent encore de partenaires, de relais et de ressources pour **initier une démarche efficace de sécurisation** pourtant cruciale. Au travers de son programme « parcours de cybersécurité », l'ANSSI a souhaité répondre à ce défi. Ces parcours ont permis d'apporter des **moyens concrets**, notamment à travers **une subvention** dédiée, tout en **sensibilisant les dirigeants et les personnels** à l'importance de faire de la cybersécurité une priorité. De plus, le programme a favorisé une dynamique de collaboration en mettant **en lien les établissements publics et les acteurs de l'industrie cyber française**, posant ainsi les bases d'une sécurisation durable et cohérente.

> *Très bonne opération : un **excellent levier pour les établissements de santé**.*
>
> **Un centre hospitalier de la région Guyane**

Les parcours ont été conçus en **trois jalons clés** qui définissent des objectifs clairs et atteignables. 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).



2. 2021-2023 : Un programme qui « rencontre son public »

Les cibles prioritaires ont été atteintes

L'objectif était de répondre à la **diversification des cyberattaques**, qui ciblent aujourd'hui **un large éventail d'établissements publics**, allant des administrations centrales aux établissements d'enseignement supérieur et de recherche, en passant par les hôpitaux et les collectivités territoriales.

707 collectivités territoriales

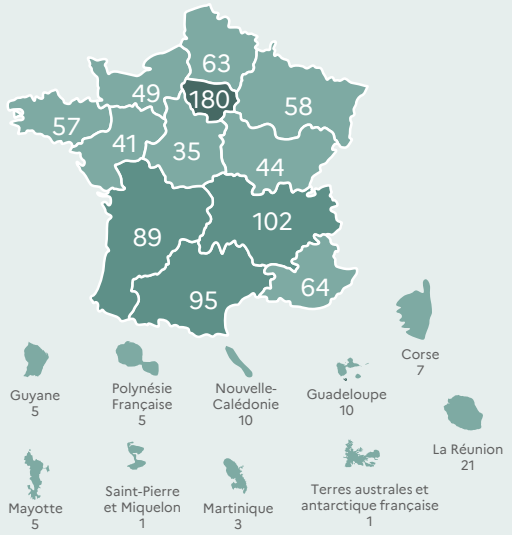
133 établissements de santé

88 établissements publics

Le programme a été conçu pour répondre aux besoins spécifiques des **collectivités territoriales,** des **établissements publics** et **de santé**, pour la plupart insuffisamment équipés pour faire face aux menaces cyber et pourtant au cœur de l'activité des territoires et de la vie des citoyens (plus de **93% des usagers ont recours à des services que sécurisent les parcours de cybersécurité**).

L'ensemble du territoire français a été couvert

L'ambition était **de portée nationale**, afin d'assurer une **sécurité numérique équitable** en protégeant au mieux **tous les territoires.** Dans les **territoires d'Outre-mer**, par exemple, des défis spécifiques, liés à leur éloignement géographique et à des besoins distincts en matière de développement numérique, ont mis en évidence la nécessité d'un accompagnement étendu et adapté, respectant les **particularités locales** tout en restant **aligné sur les objectifs nationaux.**

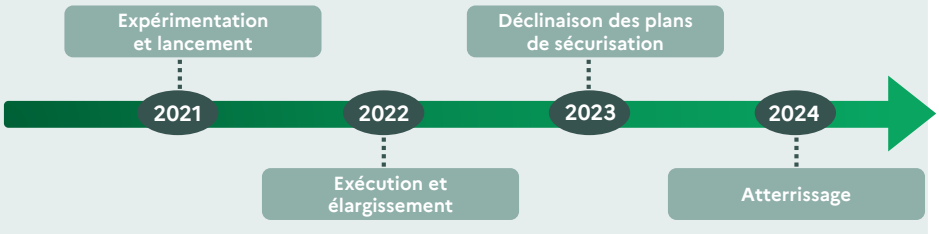


Des résultats rapides et tangibles ont été obtenus

Enfin, le programme avait pour exigence primordiale **un déploiement rapide**, répondant à l'urgence d'une **sécurisation concrète** face à la malveillance numérique. En s'engageant au sein d'un parcours, le bénéficiaire a cherché une **protection proactive** et **efficace** contre des menaces essentielles.

16 expérimentations
558 bénéficiaires
Lancement des premiers packs initiaux

606 bénéficiaires accompagnés
323 parcours clos
Mise en œuvre des mesures urgentes et déclinaison vers les packs relais



Objectif atteint de 945 bénéficiaires
Réalisation des audits des packs initiaux

3. 2024 : accompagner à terme et préparer l'avenir

Dernière année d'exécution budgétaire de France Relance, l'année 2024 portait des objectifs opérationnels définis par la nécessité de **réussir l'atterrissage du programme**.

En janvier 2024 :

53
Bénéficiaires devaient finaliser les travaux de diagnostic et formaliser un plan de sécurisation

Accompagner les derniers packs initiaux

La bonne réalisation du pack initial est essentielle : par une phase d'audits standardisés et restitués aux décideurs, il permet d'identifier les vulnérabilités et de **fédérer toutes les parties prenantes autour du plan de sécurisation.**

66
Bénéficiaires devaient encore identifier et proposer un pack relais

Aider à la conception et au financement d'une feuille de route cyber

Pensé pour résoudre les failles identifiées, le programme incite chaque bénéficiaire à engager un effort de durcissement à travers un dispositif subventionné et un accompagnement structuré et resserré.

565
bénéficiaires devaient être accompagnés dans le déploiement de leur plan d'action

Apporter des solutions concrètes et des bonnes pratiques de cybersécurité durables

Le déploiement des packs relais est le temps fort du programme. Se concentrant sur la mise en place de mesures de sécurité opérationnelles, il amorce une dynamique dans laquelle les bénéficiaires **investissent durablement dans leur cybersécurité.**

Chiffres clefs du programme « parcours de cybersécurité »

100 M€ mobilisés

1 631 candidatures déposées

970 candidatures acceptées

25 abandons durant la phase de pré-diagnostic

945 bénéficiaires

3%

33 abandons

Dont 2 bénéficiaires ayant reçu l'intégralité de la subvention (pour l'audit et les chantiers de durcissement)

10%

95 parcours en cours

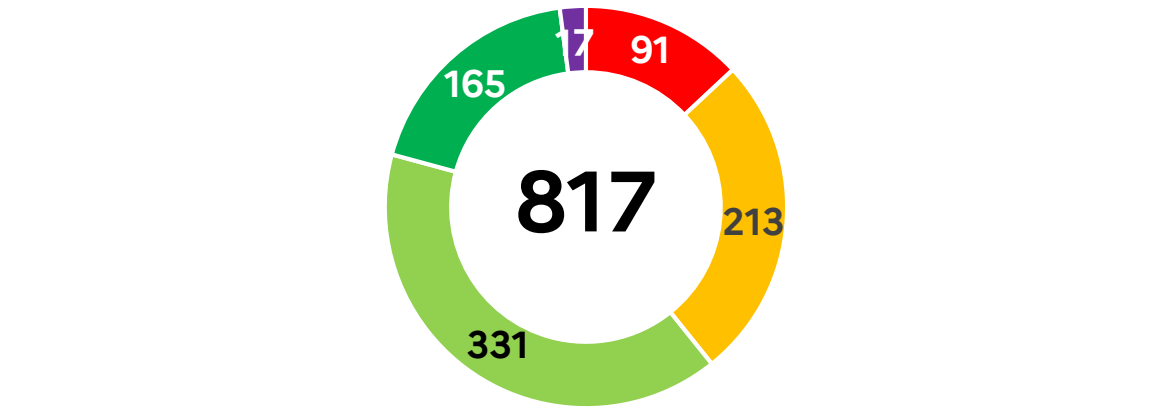
Dont 52 accompagnements assurés par l'ANSSI

87%

817 parcours arrivés à terme

Dont 127 nécessitant la poursuite d'un suivi

Répartition des parcours arrivés à terme en fonction du pourcentage d'avancement de leur pack relais



*17 centres de recherche du CNRS ont bénéficié de subventions France Relance par l'intermédiaire de l'ANSSI dont le suivi a été assuré par le CNRS lui-même et non par l'Agence.

I. Le pack initial : aider les bénéficiaires à dresser un état des lieux complet de leur maturité cyber

1. 2024 : clôturer les derniers packs initiaux

Préalable à la mise en œuvre du pack relais et conditionnant le versement de la part la plus importante de la subvention, **la bonne exécution du pack initial est la première étape essentielle des parcours de cybersécurité.**

Parmi les 945 bénéficiaires, seuls 53 n'avaient pas achevé cette étape en janvier 2024, en raison d'un **démarrage tardif** de leur parcours (8 nouveaux parcours) ou à cause de **difficultés majeures** rencontrées dans la mise en œuvre des différents chantiers.

14 mois
en moyenne ont été nécessaires pour réaliser le pack initial par les bénéficiaires en difficulté*

Principales contraintes rencontrées lors des parcours

Contraintes organisationnelles	Contraintes conjoncturelles	Contraintes contractuelles
€ Manque de ressource humaine ou budgétaire	Changement d'orientation des priorités et/ou des programmes suivis	Délai et défaut de contractualisation auprès des prestataires
Manque de stabilité des équipes SI et SSI	Changement politique	
Manque de disponibilité des décideurs	Cyberattaque	

Pour accompagner ces bénéficiaires qui devaient conduire l'ensemble des chantiers du pack initial à un rythme soutenu et/ou malgré des difficultés importantes, l'ANSSI a individualisé au maximum le suivi et l'accompagnement :

- **Le partage à intervalles rapprochées des actions, des difficultés et des risques** a permis de sécuriser les avancées.
- **La repriorisation, quand cela était nécessaire, des jalons essentiels** (audits, sensibilisation et restitution aux décideurs) a permis d'adapter le rythme des parcours aux contraintes spécifiques de chaque bénéficiaire, sans compromettre les ambitions ni la qualité des prestations.
- L'appui du programme, avec le relai **des délégués territoriaux et/ou sectoriels de l'ANSSI,** auprès des acteurs en charge du projet au sein des structures.

Janvier 2024
53 packs initiaux en cours

Décembre 2024
51 l'ont terminé
2 abandons

99% des bénéficiaires ont mené à son terme la première phase d'audit et d'état des lieux.

* Durée moyenne d'exécution du pack initial pour les 25% parcours les plus longs.
La durée médiane observée pour réaliser le pack initial a été de 7 mois.

2. Bilan des packs initiaux : fédérer toutes les parties prenantes autour d'une démarche de sécurisation

> ***Le financement à 100%** de l'audit initial **était indispensable pour lancer la démarche**.*
>
> **Une agglomération de la région Bourgogne-Franche-Comté**

Le dispositif d'attribution et de versement des subventions a été conçu afin de permettre aux bénéficiaires d'**engager au plus tôt les prestations,** dans un contexte de **contraintes budgétaires** et de **priorités multiples chez les bénéficiaires.** En effet, l'intégralité du pack initial a été financée par une première tranche de subvention (**40 000 €** pour les collectivités territoriales et les établissements publics, **50 000 €** pour les établissements de santé). Versées dès que l'engagement dans le parcours était officialisé, les subventions ont permis de rapidement contractualiser avec les prestataires, évitant ainsi des retards liés à des arbitrages budgétaires souvent longs et complexes.

Près de 39 M€

de subventions ont été dédiés au financement des états de lieux et des restitutions des vulnérabilités.

98%

Des bénéficiaires estiment que **le pré-diagnostic et le cadrage** des prestations pack initial **ont ciblé leurs besoins**.

Les packs initiaux ont été conçus sur un modèle :

- **Standardisé,** traitant les besoins communs de l'ensemble des bénéficiaires ;
- **Industrialisé et outillé** au niveau du programme afin de disposer d'un cadre méthodologique homogène et de contenir les coûts ;
- **Instancié de manière individualisée** pour tenir compte des différences de maturité des structures, des travaux déjà menés et de la capacité à faire des organisations.

> *Le parcours de sécurisation nous a permis de **faire un constat avec un point de vue extérieur**. **Le but est de faire des entretiens guidés par le prestataire pour tester la maturité de l'établissement**. Le prestataire revient ensuite vers nous avec un plan d'action pour les dirigeants ; ce qui permet de leur en présenter les aspects stratégiques et chiffrables. La sécurisation est un peu un travail souterrain : **le parcours permet de le remonter auprès des directions et des métiers, montrer le travail déjà effectué, mais aussi tout ce qui reste à accomplir.***
>
> **Responsable informatique d'un groupement hospitalier de la région Grand Est**

- **Des audits organisationnels et techniques**
- **Des mesures urgentes**
- **La sensibilisation des agents clés**
- **La restitution aux dirigeants**

Objectiver les vulnérabilités de chaque bénéficiaire : la phase d'audit

Au cœur de la démarche du pack initial, un état des lieux à spectre large permet une revue exhaustive **des besoins** et une identification des **actions structurantes à mener**.

Les bénéficiaires ont apprécié l'accompagnement par des **prestataires capables d'apporter un regard extérieur et de formaliser une analyse experte**.

Ce premier temps a permis à chaque bénéficiaire de se situer globalement en termes de maturité cyber et de **construire un plan de sécurisation**, au regard des vulnérabilités identifiées.

> *Bonne compréhension des enjeux, les constats sont pertinents et reflètent la réalité.*
> **Un musée de la région Ile-de-France**

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

Répondre aux failles critiques : les mesures urgentes

2 698

mesures urgentes mises en œuvre

Une part du budget des packs initiaux a été sanctuarisée dès le lancement du parcours pour appliquer les mesures urgentes identifiées par les audits. Les bénéficiaires ont pu **combler les failles les plus critiques de leurs systèmes d'information** par des **mesures correctives sans attendre la finalisation du plan de sécurisation.**

Parmi les mesures urgentes les plus courantes :

Durcissement de l'*Active Directory*

Cloisonnement des infrastructures

Corrections nécessaires à l'amélioration immédiate de la couverture des vulnérabilités (services exposés sur internet, mot de passe, wifi, authentification)

Remettre en visibilité la responsabilité de tous : les campagnes de sensibilisation

La sécurisation durable des systèmes d'information (SI) repose notamment sur le comportement des agents au sein de la structure. De ce fait, plus de **3 700 jours ont été dédiés à des campagnes de sensibilisation**. Elles ont été réalisées auprès d'agents dont l'activité quotidienne constitue une porte d'entrée pour une potentielle cyberattaque.

Publics visés et contenus des sensibilisations

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

Les **bons réflexes** de ces agents face à la malveillance numérique sont essentiels : enclencher une **réflexion approfondie** sur les enjeux de cybersécurité s'est révélé crucial. Conçues pour encourager la participation active, les campagnes de sensibilisation ont permis d'**aligner les attentes et les comportements autour des objectifs de sécurisation.**

Regarder dans la même direction : les restitutions

Pour **initier la démarche de sécurisation,** il est essentiel de **convaincre et de fédérer les décideurs** autour des enjeux de sécurité numérique, **sujet qui peut paraître complexe et technique** pour certains d'entre eux. À cet égard, **l'implication des dirigeants tout au long de la démarche a été un véritable atout** : ils ont été présents lors du lancement et de la clôture du pack initial et ont participé activement à l'élaboration du plan de sécurisation. L'objectif était de les aider à prendre des décisions mieux informées sur l'intégration de la cybersécurité dans les réflexions stratégiques et les budgets.

Les apports des réunions de restitution aux dirigeants

- Une synthèse de l'analyse du niveau de maturité et une comparaison aux autres organisations tirée du parangonnage de l'ANSSI sur le dispositif
- Les principaux événements redoutés et les principaux besoins de sécurité associés
- Une cartographie macroscopique des vulnérabilités du SI
- Une restitution et validation du plan de sécurisation proposé
- Une liste des chantiers prioritaires pouvant faire l'objet de pack relais co-financés par l'ANSSI

93%

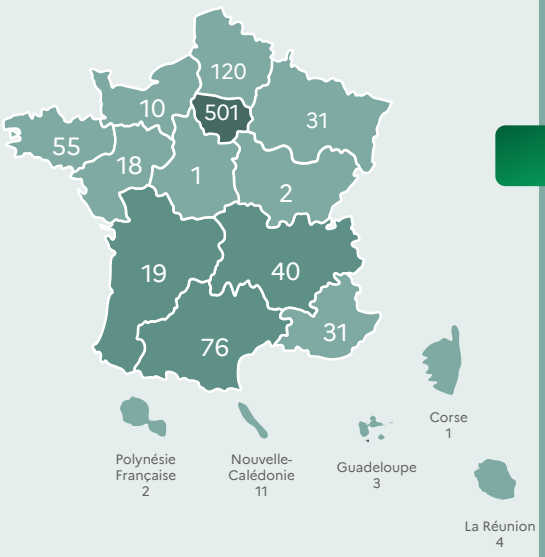
Des prestataires estiment que **cette démarche a permis de mettre en évidence l'importance de la cybersécurité auprès des dirigeants**, tout en **amorçant une pérennisation des investissements dans la sécurité des systèmes d'information**.

Au cœur des packs initiaux : des prestataires au contact des bénéficiaires

Les prestataires impliqués ont pleinement répondu à ces attentes. Certes, du fait d'une **forte tension du marché des prestataires en cybersécurité**, alimentée par une demande croissante liée à l'intensification des menaces, le déploiement des parcours a parfois rencontré des ralentissements. Mais, pour y répondre, **deux leviers majeurs ont été activés** : d'une part, **l'optimisation de la répartition des interventions**, en mobilisant une diversité de prestataires et en assurant une ventilation équilibrée des missions auprès des bénéficiaires ; d'autre part, la **structuration de l'offre des intervenants.**

197 prestataires présents sur l'ensemble du territoire français dont la moitié d'entre eux ont leur siège social hors Ile-de-France

Répartition géographique des prestataires



Le programme a contribué à équilibrer les opportunités entre différents types d'entreprises, favorisant ainsi un meilleur maillage territorial

L'implication en particulier **des petites et moyennes entreprises** (à plus de 64%) a permis de valoriser l'innovation locale et de renforcer leur positionnement dans des secteurs compétitifs. La participation des entreprises de taille intermédiaire et des grandes entreprises, bien que moindre en volume, démontre que **ces marchés publics étaient ouverts à une pluralité d'acteurs**.

85% des prestataires estiment que les **parcours ont mis en valeur les TPE** et leur **implantation locale**

L'élaboration des parcours sous forme de **prestations « packagées »** et la **capitalisation sur des outils, concepts et guides** préalablement produits par l'ANSSI ont permis **une adhésion rapide et une maitrise du dispositif**. Il était ainsi attendu du prestataire qu'il apporte, dans le cadre du parcours, le maximum de valeur ajoutée sur le **fond** plutôt que sur la **forme** au bénéficiaire. Cette réflexion de fond devait se concentrer notamment sur les états des lieux afin d'avoir une vision claire de la maturité en termes de sécurité des SI (SSI) du bénéficiaire mais également sur des travaux de compréhension du contexte et des enjeux du bénéficiaire (avec une approche par les risques, priorités métier, projets SI, orientations SSI du bénéficiaire et principales menaces le visant) afin d'orienter et de prioriser le plan de sécurisation de façon adéquate.

Tous les prestataires ont élaboré les plans de sécurisation en trouvant un équilibre entre une cible ambitieuse, visant à améliorer durablement la sécurité, et une cible réaliste validée par les équipes SSI, SI et dirigeantes. **Déployer une démarche de sécurisation, c'est aussi générer une motivation dans la mise en œuvre d'un plan qui pourra être immédiatement exploité dans le cadre des packs relais.**

II. La déclinaison en pack relais : concevoir une feuille de route cyber

1. 2024 : Accompagner la définition des derniers packs relais

Janvier 2024

805 packs relais lancés

Transformer les audits du pack initial en un levier de sécurisation concret

Par un **diagnostic à 360°,** le pack initial permet l'identification des vulnérabilités. Par **la réalisation et la restitution d'un plan de sécurisation**, il ouvre la démarche de sécurisation. Mais c'est le passage en pack relais qui œuvre concrètement à la déclinaison des solutions, de par :

Le co-financement des mesures de sécurisation

Dans le cadre du pack relais, les bénéficiaires s'engagent à **cofinancer les mesures de sécurisation à hauteur de 30%**. Ils sont invités par la suite à s'investir dans le programme sur le long terme, en fonction de leur capacités budgétaires.

La co-construction d'une feuille de route

En combinant la compréhension terrain des bénéficiaires avec l'expertise des accompagnateurs, **le plan reflète une vision réaliste et adaptée** aux contraintes techniques, organisationnelles et budgétaires des entités publiques.

Il a donc été crucial de **maintenir la dynamique opérationnelle et financière** pour accompagner un maximum de bénéficiaires, notamment les plus en difficulté, à s'engager sur un pack relais avant fin 2024.

Accompagner des parcours à risques

Le passage des packs initiaux vers les packs relais a été un moment sensible des parcours pour les bénéficiaires. Moins standardisée, cette phase est plus complexe et davantage sensible aux aléas politiques, budgétaires et organisationnels.

Contraintes organisationnelles	Contraintes conjoncturelles	Contraintes économiques
Coordination entre structures (ex. hôpitaux au sein d'un GHT ou communes partageant un système d'information)	Changement d'orientation des priorités et/ou des programmes suivis	Difficultés de financement interne
Fragmentation des responsabilités	Changement politique	Hausse des coûts et crise économique
Compatibilité entre les projets d'évolution fonctionnelle et les projets de sécurisation	Bouleversement géopolitique ou numérique (cyberattaque)	

Pour **assurer la transition des derniers packs initiaux en pack relais**, il a été essentiel de prendre en compte ces enjeux dès le début de l'année et d'adopter **une approche flexible** et **concertée entre toutes les parties prenantes.**

Depuis janvier 2024, **101** nouveaux packs relais ont ainsi été lancés.

Seuls **21** bénéficiaires sur 919 ayant défini un plan de sécurisation ont décidé d'abandonner leur parcours à l'issue du pack initial, renonçant à la phase de pack relais et au financement associé, souvent **en raison de contraintes externes insurmontables ou de priorités stratégiques réorientées.**

Décembre 2024

906 packs relais lancés

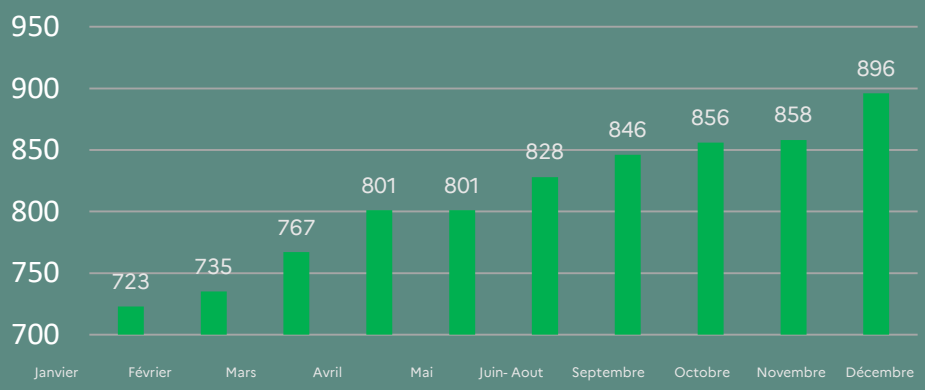
Des subventions déployées sous un suivi rigoureux

Une surveillance étroite de l'ANSSI pour sécuriser les fonds versés

Le déploiement du programme a bénéficié d'une **supervision attentive** ; le suivi opérationnel intégrant à chaque étape une **exigence de fourniture d'engagements et de justificatifs**. En effet, par sa demande de subvention, chaque bénéficiaire s'est engagé à compléter et à signer une **attestation de bonne exécution des travaux** à l'issue du pack initial et du pack relais. Le versement de la deuxième tranche de subvention est conditionné à la bonne réalisation des travaux du pack initial, tant en termes de conformité que de qualité, ainsi qu'à un engagement sur les travaux qui seront conduits au titre du pack relais.

Cette conditionnalité a garanti une utilisation efficace des fonds alloués et a souligné la crédibilité du programme auprès de l'ensemble des parties prenantes.

Un effort pour collecter les dernières attestations



Un accompagnement resserré durant 2024 pour collecter l'ensemble des attestations d'engagement

Un contrôle rigoureux de l'ANSSI pour des plans de sécurisation efficaces et adaptés

L'ANSSI a exercé un **contrôle rigoureux sur les plans de sécurisation** qui ne pouvaient être financés qu'après leur validation. Les plans doivent répondre à **quatre priorités stratégiques** : *défense, protection, résilience et gouvernance*. Le pack relais étant une phase de remédiation, les mesures de gouvernance y sont limitées à 25 % pour privilégier les actions opérationnelles. Cette vigilance a garanti la **crédibilité de l'offre,** la **solidité des parcours des bénéficiaires** et l'**efficacité des actions** face aux risques cyber.

2. Les parcours de cybersécurité : déployer des plans de sécurisation face aux failles les plus critiques

4 413
mesures de remédiation validées et co-financées

Près de 51 M €
de subventions ont été dédiés au co-financement des plans de sécurisation (acquisition et déploiement de solutions)

> *C'est un projet qui en vaut la peine, c'est **90 000 euros de subvention** qui vont permettre de mener des plans d'action pour **augmenter la sécurité de notre système d'information**.*
>
> **Une mairie de la région Nouvelle-Aquitaine**

Le dispositif a permis de sélectionner au sein des **quatre dimensions de la cyber** *(protection, gouvernance, défense, résilience)* des mesures permettant d'augmenter significativement les capacités opérationnelles cyber des bénéficiaires.

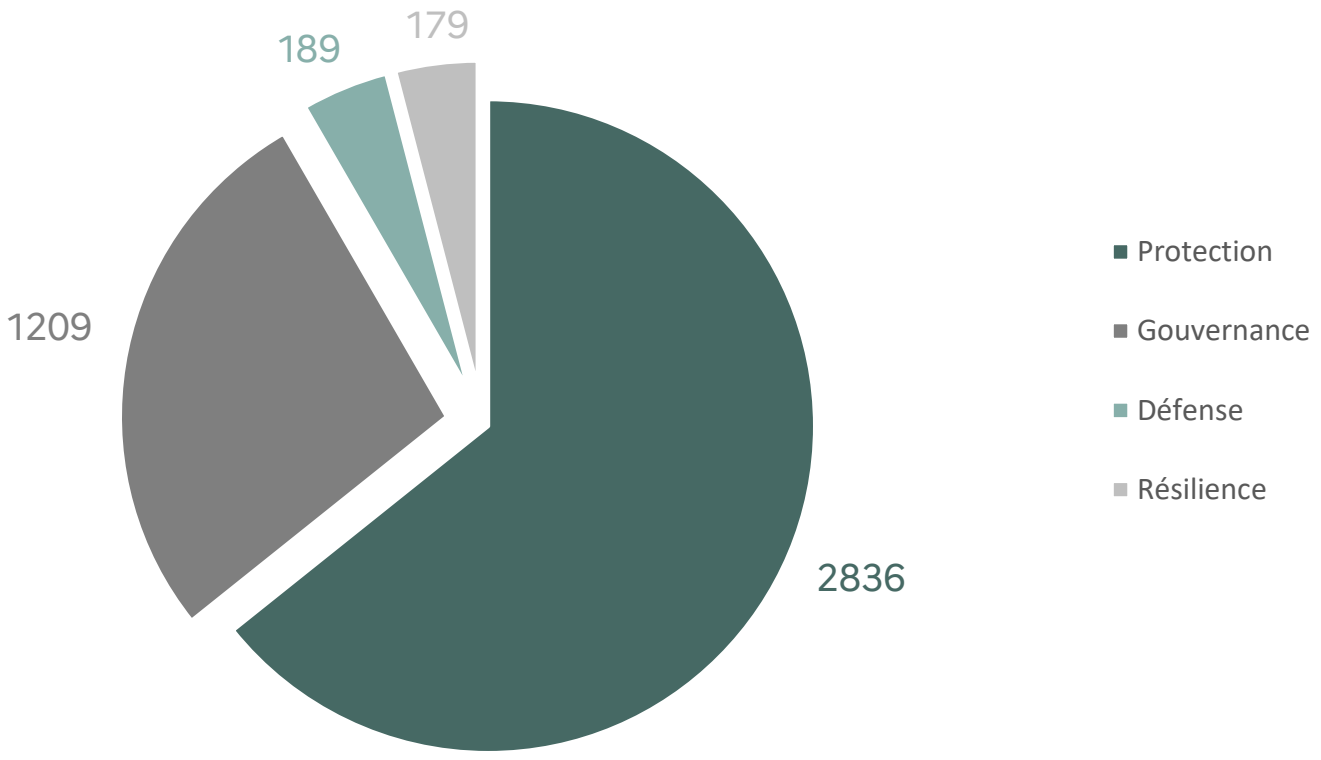
Répartition du nombre de mesures des packs relais selon les 4 axes cyber

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 de crise, plan de continuité d'activité, sauvegardes sécurisées…



Des solutions européennes innovantes

40 M€
investis dans l'acquisition de produits/éditeurs européens

33 M€
investis dans l'acquisition de produits/éditeurs français

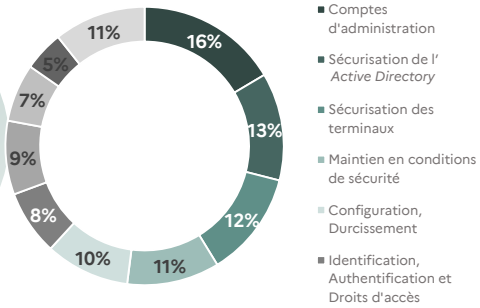
Les mesures de sécurité des packs relais améliorent la sécurité des systèmes d'information des entités bénéficiaires

Au sein de chacune des **quatre dimensions de la cyber** *(protection, gouvernance, défense, résilience)* des typologies particulières de mesures se détachent.

Protection

Les services publics interagissent avec de nombreux acteurs, multipliant ainsi les points d'entrée aux attaques.

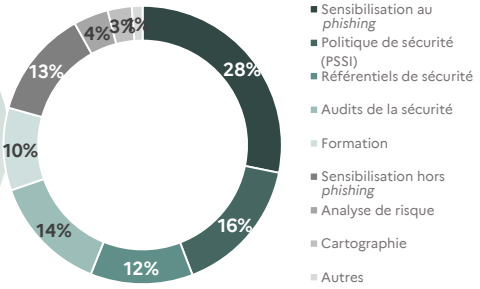
Une sécurisation des comptes, de l'*Active Directory* et des terminaux joue comme un rempart et renforce les défenses collectives.



Gouvernance

En renforçant la vigilance humaine, ces mesures complètent les dispositifs techniques.

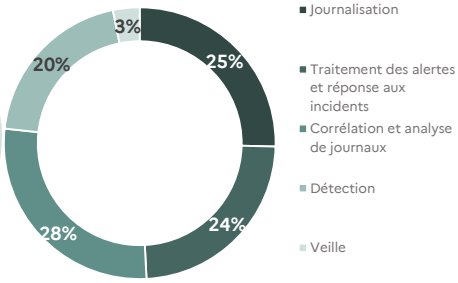
La sensibilisation au *phishing* joue un rôle crucial : elle permet d'éduquer les métiers à reconnaître et à éviter les tentatives de fraude.



Défense

Les services publics manipulent des données personnelles, citoyennes ou stratégiques.

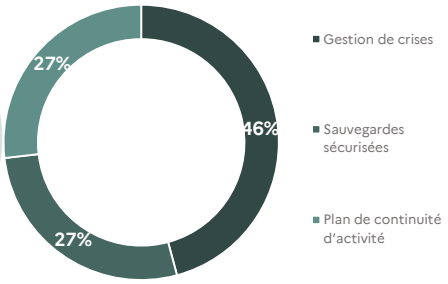
Adopter des solutions de détection, de veille et de journalisation efficaces, garantit la confidentialité et la disponibilité de ces données essentielles.



Résilience

Les cyberattaques sont de plus en plus sophistiquées et le nombre d'attaques augmente.

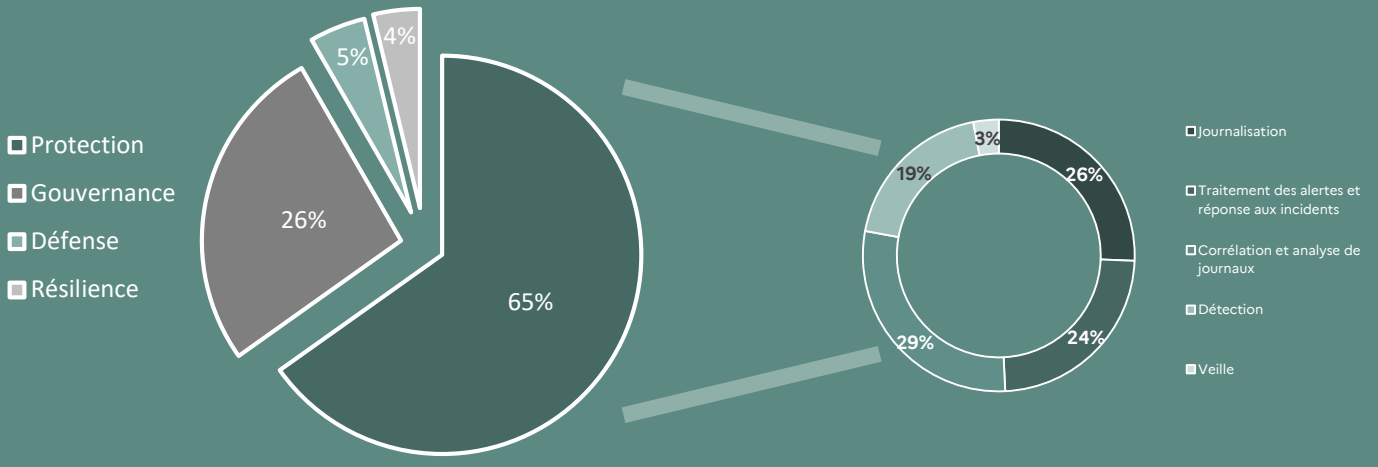
Disposer de plans de réponse et de sauvegardes est essentiel pour réagir rapidement et réduire les impacts.



Les solutions retenues par les établissements de santé

Parmi les **4 413 mesures de remédiation**, **12%** ont été destinées aux établissements de santé. Ces derniers se sont orientés en priorité sur des **mesures de protection** (sécurisation du réseau, des terminaux et des comptes d'administration), visant à réduire le risque d'incident affectant la continuité des soins ou la confidentialité des données de santé.

Ces actions se sont inscrites dans la stratégie de sécurisation des SI des groupements hospitaliers de territoire (GHT), en soutien des obligations réglementaires applicables à leurs établissements support dans le cadre de la directive NIS.



III. Le déploiement des packs relais : les bénéfices d'un accompagnement resserré et d'un parcours de cybersécurité

1. 2024 : continuer et terminer les derniers accompagnements

> *Le **rythme** et les **délais imposés** auraient pu être contreproductifs sans **la qualité de l'accompagnement** dont nous avons bénéficié.*
> ***Un conseil départemental de la région Pays de la Loire***

Janvier 2024

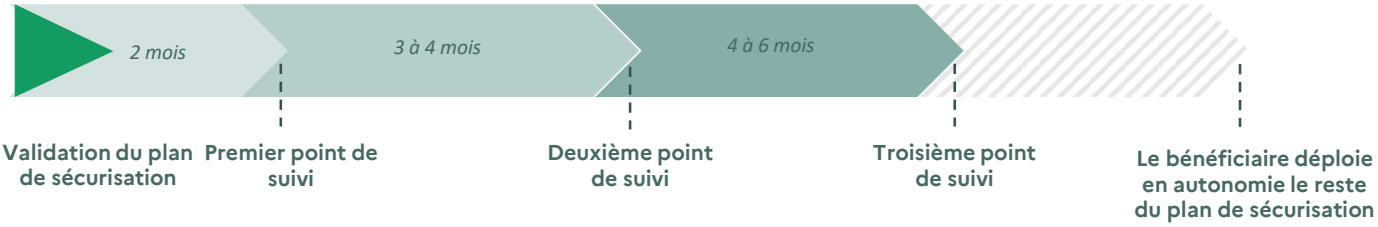
316 packs relais terminés

L'accompagnement des bénéficiaires a toujours été au cœur de l'offre de service de ce programme, et ce tout au long des parcours. Depuis la « Cellule Relations Candidats » durant la première phase de pré-diagnostic (**aide administrative à la contractualisation**) aux prestataires accompagnateurs durant les phases d'audits et de remédiation (**aide active à la sécurisation**), en passant par l'appui des délégués territoriaux et sectoriels de l'ANSSI (**aide à la maîtrise des risques**), le bénéficiaire a toujours été accompagné pour déployer le parcours avec succès et au bon rythme.

98% des bénéficiaires se déclarent **très satisfaits de l'accompagnement** proposé.

Pendant la mise en œuvre du pack relais, les bénéficiaires sont restés au contact du prestataire accompagnateur, notamment *via* **trois points de suivi** échelonnés sur 12 mois.

Un suivi des packs relais dans la durée



Ces points de suivi sont l'occasion de s'assurer du bon déroulement de l'avancement **(suivi des contractualisations et de l'avancement opérationnel)** et, le cas échéant, d'adapter et d'aider les parcours le nécessitant (gestion des difficultés, réorientation des feuilles de route, ….).

25 % des bénéficiaires ont effectué une nouvelle version de leur feuille de route cyber durant le parcours.

680 points de suivi des packs relais en janvier 2024

2 638 points de suivi effectués à la fin 2024

85% des bénéficiaires ont réalisé **plus de 50% de leurs actions à la fin de l'accompagnement.**

Décembre 2024

782 packs relais terminés

2. La force des parcours : déployer une feuille de route pour l'avenir

L'effet des parcours : accélérer le renforcement de la sécurité au-delà du plan de sécurisation

A travers les parcours de cybersécurité, l'ANSSI a accompagné les structures bénéficiaires dans la définition d'une feuille de route pluriannuelle et a financé les premières actions pour amorcer sa mise en œuvre essentielle à la sécurisation du SI. **La feuille de route est planifiée en moyenne sur deux années** afin de donner aux bénéficiaires de la visibilité sur les ressources techniques et financières à engager pour sa bonne réalisation. Tant du point de vue budgétaire qu'opérationnel, la démarche apparaît bien lancée, au-delà des limites calendaires du programme.

> *Démarche très intéressante que l'on a saisie pour accélérer le renforcement de notre sécurité **pour aller au-delà du plan de sécurisation**.*
>
> **Conseil départemental de la région Bourgogne-Franche-Comté**

En moyenne, le niveau d'investissement budgétaire des bénéficiaires a été **30%** supérieur au montant prévu par le dispositif.

En fin de parcours, les bénéficiaires les plus éloignés des préoccupations de sécurité numérique ont acquis un **lien direct avec l'ANSSI**, ont intégré un **écosystème local cyber** et se trouvent placés dans une **démarche de sécurisation à long terme**. Cette continuité garantit que les efforts ne s'arrêtent pas avec le dispositif, mais s'inscrivent dans une dynamique durable, portée par des actions autonomes et une vigilance renforcée.

Pour tous les bénéficiaires, **le programme a permis de structurer des bases solides pour anticiper les évolutions réglementaires**, comme celles imposées par la directive européennes NIS 2, notamment par la promotion d'une approche globale de la cybersécurité par les risques.

A la fin du parcours**, l'ANSSI reste le point de contact privilégié** pour les questions de cybersécurité des bénéficiaires. Elle peut également les orienter vers des acteurs de terrain.

Afin de s'assurer de l'effectivité sur la durée des parcours de cybersécurité, **les bénéficiaires s'engagent à s'inscrire sur la plateforme « Club SSI »** de l'ANSSI qui propose des services de diagnostics automatisés (*Active Directory*, etc.).

Les parcours de cybersécurité ont déjà inspiré d'autres programmes et l'ANSSI capitalise actuellement sur ces parcours pour définir un référentiel plus précis pouvant servir de base à de futurs programmes.

> *Un **grand merci** pour ce parcours, qui devrait même être obligatoire pour toutes les collectivités territoriales tant il est **indispensable pour la sécurisation des données** des administrés, des agents et des élus !*
>
> **Le Directeur informatique d'une mairie de la région Nouvelle-Aquitaine**

L'indice de cybersécurité permet de positionner et de suivre la maturité de son système d'information

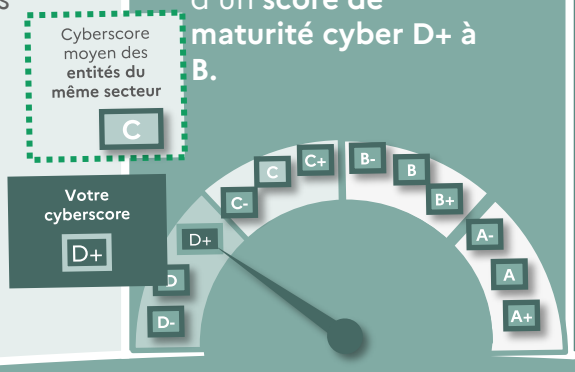
L'ANSSI fournira prochainement un outil de calcul du score de maturité cyber. Conçu comme un indicateur central du programme, il a été pensé pour évaluer avec précision le niveau de maturité cyber des bénéficiaires et **orienter leur parcours vers des actions adaptées** à leurs besoins. Cet outil, consolidé par l'expérience du programme, trouve désormais une nouvelle vocation. Il offre aux entités la possibilité de **piloter elles-mêmes leur progression en cybersécurité**, renforçant ainsi leur autonomie et leur engagement dans une démarche durable.

Outil d'analyse et de comparaison dans l'espace

L'indice de cybersécurité permet aux bénéficiaires de **mesurer leur maturité cyber** et de se **positionner** par rapport à d'autres entités de même nature.

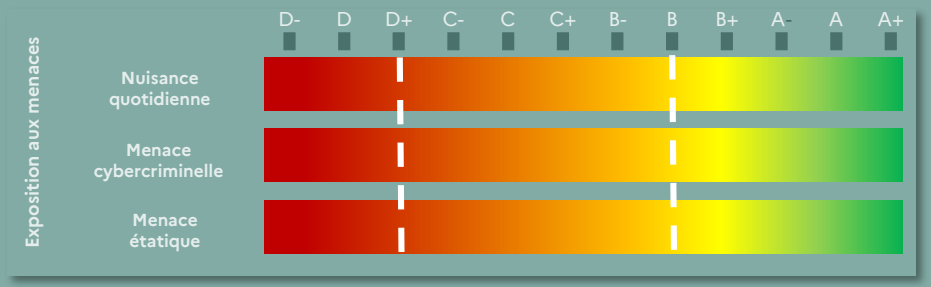
Outil d'évaluation et de comparaison dans le temps

A l'issue du pack relais, il est mis à jour pour refléter les progrès réalisés. En moyenne, les bénéficiaires du parcours passent d'un **score de maturité cyber D+ à B.**



Outil d'efficacité et de progression

L'évolution de l'indice de cybersécurité est ainsi **l'un des critères pour juger si le plan de sécurisation identifié est suffisant** pour être déployé.



FRELANCE

Version 1.0 – Avril 2025

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