RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES PARCOURS DE CYBERSÉCURITÉ : RAPPORT D'ACTIVITÉ 2022

Volet cyber de France Relance

Financé par l'Union européenne
NextGenerationEU

FRELANCE

Sommaire

Contexte et ambitions du volet cybersécurité de France Relance

Dans le cadre de France Relance, le gouvernement a alloué 1,7 milliards d'euros d'investissements à la transformation numérique de l'État et des territoires. Ce plan intègre un **« volet cybersécurité », piloté par l'ANSSI, qui s'est élevé à 176 millions d'euros sur la période 2021-2022.**

L'importance des moyens alloués à ce volet a permis à l'ANSSI de poursuivre une triple ambition :

ÉLEVER SUBSTANTIELLEMENT LE NIVEAU DE SÉCURITÉ NUMÉRIQUE DE L' ÉTAT ET DES SERVICES PUBLICS

Afin de renforcer leur cybersécurité face à une menace en forte croissance, le plan propose aux acteurs publics, à l'échelon national comme dans les territoires, de financer l'achat de prestations d'acteurs privés (audits de cybersécurité, conseil, accompagnement technique, etc.), de produits de sécurité et de formations. Le plan vise par ailleurs à accroître de façon significative la couverture des solutions de détection des cyberattaques, y compris les moyens de supervision de l'ANSSI.

CONTRIBUER AU RENFORCEMENT DU TISSU INDUSTRIEL FRANÇAIS DE CYBERSÉCURITÉ

En s'appuyant sur les services proposés par des prestataires privés et sur l'offre de produits de sécurité, le plan entend contribuer au développement d'une industrie française de cybersécurité. Essentielle à la sécurité de l'ensemble de la Nation, cette industrie se doit d'être pérenne, performante et capable de répondre aux besoins du plus grand nombre au sein des services de l'État et des services publics.

CRÉER UN EFFET DE LEVIER CONDUISANT À UN INVESTISSEMENT DURABLE DANS LA CYBERSÉCURITÉ

Les moyens alloués via France Relance étant par définition limités dans le temps, ils doivent constituer une amorce pour inciter les bénéficiaires à investir durablement dans leur cybersécurité et créer ainsi un effet de levier permettant de démultiplier les bénéfices du plan.

Bien que le volet cybersécurité de France Relance vise à profiter au plus grand nombre d'acteurs publics, en veillant à dépasser la sphère des acteurs régulés (opérateurs d'importance vitale et opérateurs de services essentiels), habituel cœur de cible des actions de l'ANSSI, les prestations financées s'adressent prioritairement à certains secteurs et entités parmi les plus critiques dont la cybersécurité nécessite un renforcement urgent et soutenu. Une importance particulière est ainsi accordée aux collectivités territoriales et aux organismes au service du citoyen, dont en particulier les établissements de santé.

Les Parcours de cybersécurité

1. Présentation du dispositif

Un lancement rapide issu d'une phase de co-construction

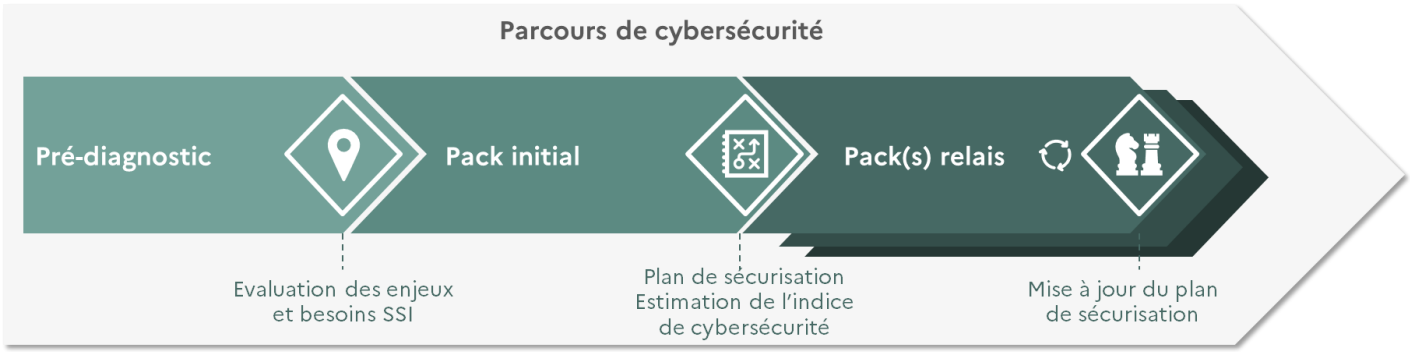
Un concept décliné opérationnellement

En moins de six mois, les Parcours de cybersécurité ont été définis, l'approche méthodologique formalisée et les priorités du dispositif arrêtées.

Cette rapidité dans la mise en place a été notamment permise par la capitalisation sur des concepts et guides préalablement produits par l'ANSSI : guide d'hygiène ou guide sur les attaques par rançongiciels, mais aussi par l'appui des experts de l'agence qui ont participé à la phase de cadrage et à la définition des Parcours. La conception par les experts de l'ANSSI assure ainsi la pertinence technique du dispositif. Les retours d'expérience opérationnels ont été pris en compte pour l'adapter au plus près des besoins.

Un accompagnement en trois temps

- Un **pré-diagnostic** permettant une première analyse du contexte, du niveau de maturité et des besoins du bénéficiaire.
- Un premier temps d'accompagnement, contenu sur quatre mois, via un **pack initial** qui comporte une série de prestations standardisées, assurées par un prestataire terrain, couvrant des actions de sensibilisation, et des audits techniques et organisationnels. Ce pack initial permet l'élaboration d'un **plan de sécurisation**.
- Enfin, l'activation d'un ou plusieurs **packs relais** pour mettre en œuvre les mesures de sécurisation du pack initial, via des prestations complémentaires comme l'acquisition et l'installation de matériels, logiciels ou services pertinents.



Une subvention versée en deux temps

Les subventions attribuées aux bénéficiaires des Parcours sont versées en deux temps :

- La première tranche de subvention vise à **financer la totalité des prestations du Pack initial**. Elle est attribuée en amont du lancement de ce premier volet du Parcours.
- La seconde tranche de subvention vise à **co-financer les prestations des Packs relais.** Son versement est conditionné à la bonne réalisation du Pack initial et à l'engagement des bénéficiaires à réaliser les travaux du Pack relais.

Un dispositif régi par des principes structurants

S'appuyer sur les prestataires pour décupler la capacité à faire

Un dispositif industrialisé, adaptable et opérationnel qui garantit une cohérence d'ensemble et un niveau homogène d'accompagnement

Du fait de leur structuration et leur contenu, les Parcours de cybersécurité sont cadrés et conçus pour être le plus largement industrialisés afin que l'ANSSI puisse déployer, par l'intermédiaire des prestataires, un accompagnement homogène et délivrer des prestations de qualité à l'ensemble des bénéficiaires. Les prestataires accompagnateurs sont les garants de cette cohérence globale à travers leur suivi continu auprès des bénéficiaires. Enfin, l'accent est mis sur le côté opérationnel des Parcours, en vue d'obtenir des résultats concrets et rapides.

En phase de conception, en amont de son lancement, un prestataire a fourni à l'ANSSI une aide pour formaliser le dispositif, et l'industrialiser. Il l'a ensuite assistée pour les relations avec les bénéficiaires.

Une logique d'accompagnement des bénéficiaires

L'accompagnement des bénéficiaires est au cœur de l'offre de service, et ce tout au long de leur Parcours. Ils sont tout d'abord accompagnés par la Cellule Relation Candidats lors des premières étapes des Parcours : lors du pré-diagnostic, dans les démarches administratives et de contractualisation. Une fois le Parcours engagé, le prestataire accompagnateur, expert de la démarche, assure le suivi de bout-en-bout du Parcours et est disponible pour répondre à leurs éventuelles interrogations.

Les bénéficiaires utilisent intégralement leur subvention pour contractualiser avec des prestataires terrain de leur choix.

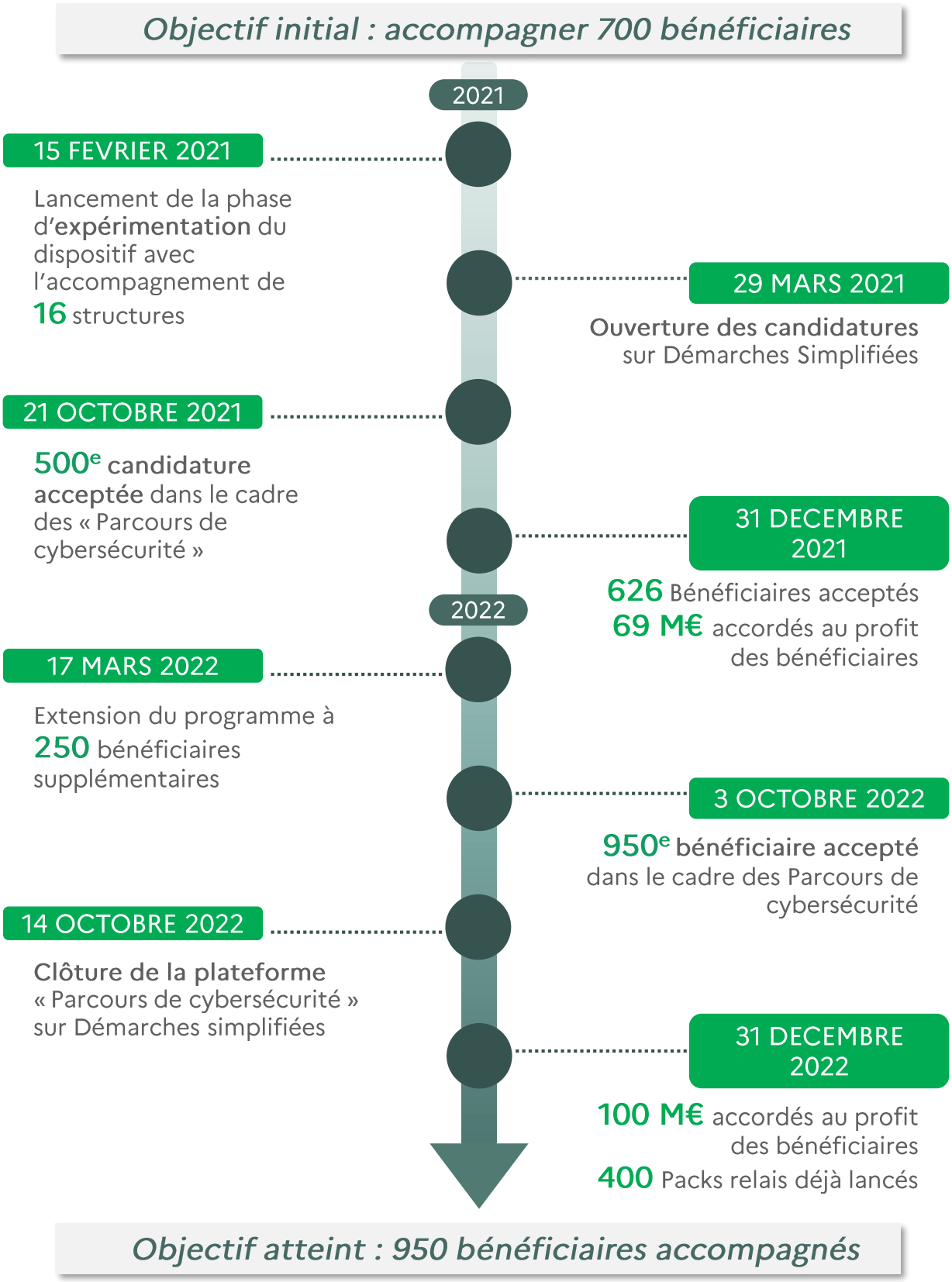
Une relation de partenariat avec le réseau de prestataires terrain

Les prestataires terrain agissent en tant que véritables partenaires de l'ANSSI et sont présents sur le terrain pour leur mise en œuvre. La méthodologie des Parcours et les livrables-type associés leur sont transmis afin de les guider au mieux dans le déploiement des Parcours. Une attention particulière est portée sur la diversification des prestataires terrain, afin de répondre à l'objectif de développement du tissu industriel français sur un maillage territorial et de participer ainsi à la relance de l'économie.

« L'approche collaborative et constructive de la démarche a créé une synergie et une cohésion avec les parties prenantes autour de la sécurité de nos systèmes d'information. »

Une commune en Bretagne

2. Retour sur le déroulement du dispositif en 2021 et 2022



I. Une réponse au besoin d'accompagnement des entités publiques

20
Candidatures déposées chaque semaine en moyenne

970
Parcours acceptés

710
Collectivités territoriales

133
Etablissements de santé

103
Etablissements publics

24
Abandons avant contractualisation

1. Un dispositif plébiscité sur l'ensemble du territoire

Un rythme élevé de dépôt de candidatures depuis le lancement du dispositif avec une dynamique qui s'est maintenue en 2022

Dans la continuité de l'année 2021, les Parcours ont attiré un nombre important de bénéficiaires sur l'ensemble du territoire, et ce jusqu'à la fermeture de la plateforme d'inscription, en octobre 2022.

Cette attractivité est à la fois le reflet de l'adéquation du dispositif aux besoins des entités publiques de sécuriser leurs systèmes d'information, à l'efficacité de l'action des délégués territoriaux et des coordinateurs sectoriels de l'ANSSI pour proposer ce dispositif, et à l'effet d'entraînement apporté par le haut niveau de satisfaction des premiers bénéficiaires.

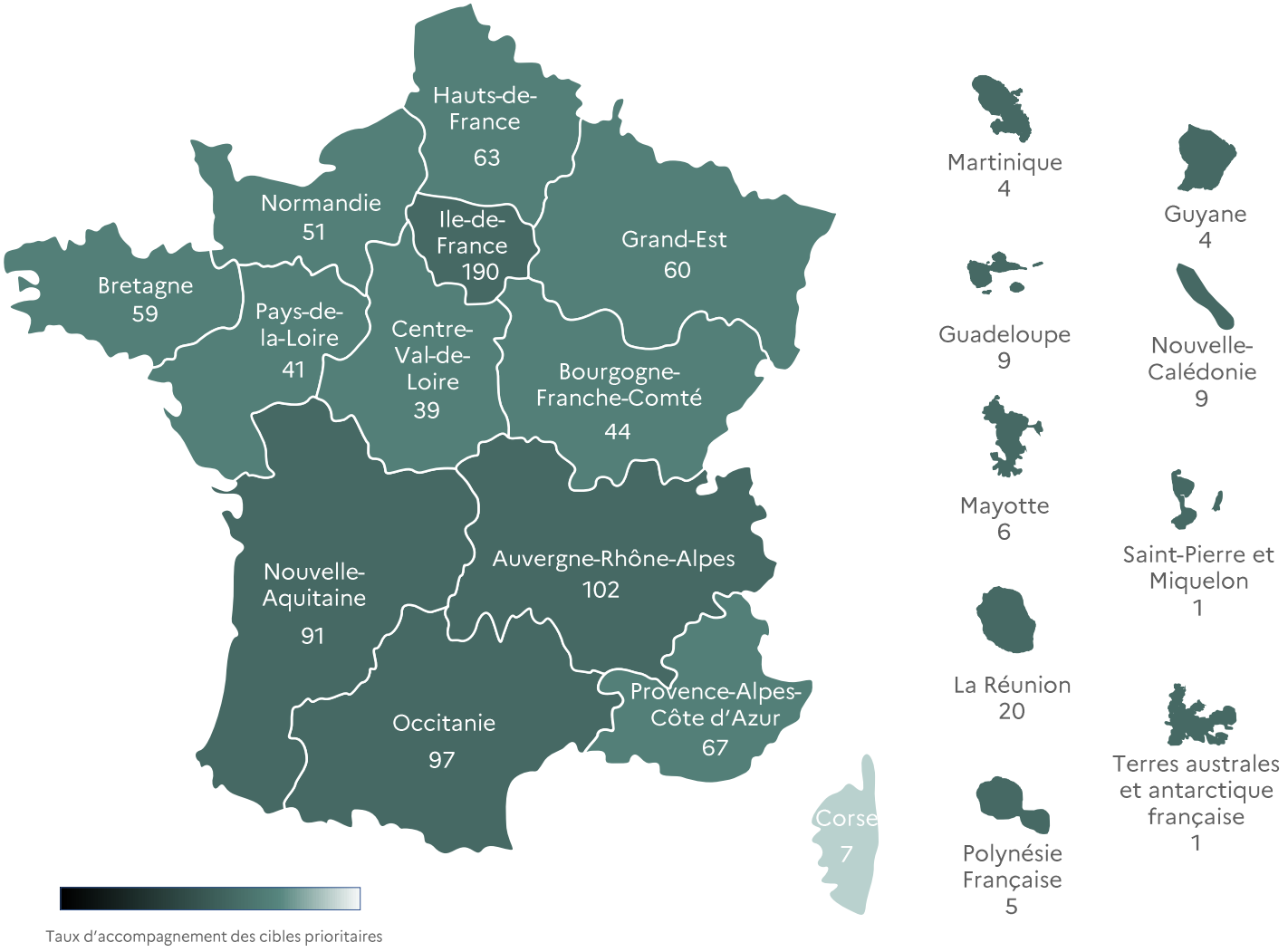
En réponse à ce fort besoin, une extension du dispositif à un plus grand nombre de bénéficiaires

Face au succès du dispositif, 250 nouveaux accompagnements ont été accordés en 2022 pour arriver à un total de 970 bénéficiaires acceptés. L'extension du dispositif s'est faite en bénéficiant toujours de manière équilibrée aux cibles prioritaires identifiées au lancement du dispositif : les collectivités territoriales et les établissements de santé.

En parallèle, plus de 680 candidatures ont été, après analyse, réorientées vers un service plus adapté à leurs besoins. Ainsi, les structures les plus matures ont pu être dirigées vers le dispositif d'appel à projet et les structures dont la taille du SI n'était pas adaptée ont été orientées vers des dispositifs ou interlocuteurs plus adaptés (opérateurs publics de services numériques - OPSN, appel à projets de licences mutualisées, etc.)

Une répartition des bénéficiaires assurant la couverture du territoire

Les bénéficiaires des Parcours de cybersécurité sont répartis sur l'ensemble du territoire français avec notamment 59 structures accompagnées dans les territoires d'Outre-Mer. Si la moitié de ces bénéficiaires sont concentrés sur quatre régions (Ile-de-France, Nouvelle-Aquitaine, Auvergne-Rhône-Alpes et Occitanie), 93% de la population française est couverte au titre d'une ou plusieurs collectivités territoriales.



Répartition des structures accompagnées sur le territoire

Plus de **93%*** des usagers ont recours à des services que sécurisent les parcours de cybersécurité

* Taux de couverture calculé sur le périmètre des collectivités territoriales et établissements publics de coopération intercommunale en Parcours

2. Une démarche d'accompagnement au cœur du dispositif

Une prise en charge rapide du bénéficiaire par la Cellule « Relations candidats »

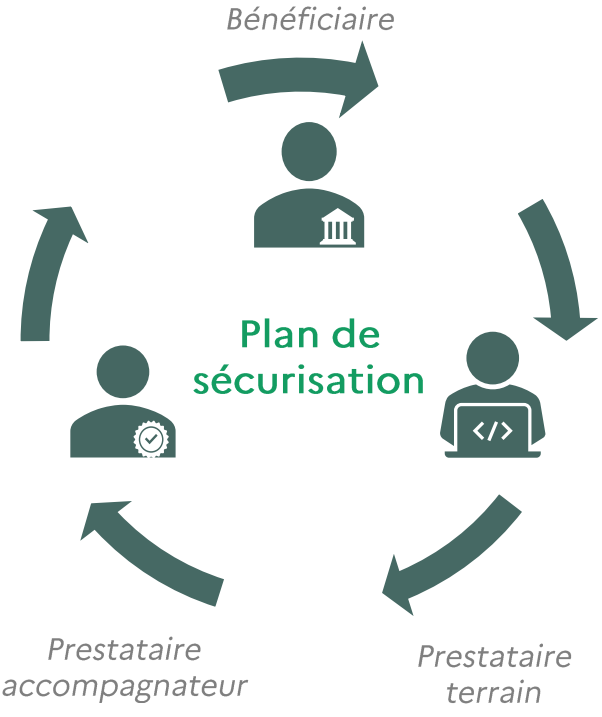
L'accompagnement des bénéficiaires est le maître-mot de cette offre de services. La **Cellule Relations Candidats** intervient dès l'entrée en Parcours des structures à plusieurs reprises :

- **Un premier temps d'échange** permet de présenter les enjeux et la structuration de la démarche aux bénéficiaires ;
- **Un pré-diagnostic** d'une durée de 2 heures donne lieu à une première analyse du niveau de maturité du SI et l'identification fine des besoins ;
- Une **restitution des éléments de cadrage** issus du pré-diagnostic auprès du bénéficiaire qui peut alors élaborer son cahier des charges sur cette base.

Des actions de sécurisation adaptées

A l'issue de la phase de prise en charge par la Cellule Relations Candidats, le bénéficiaire contractualise avec le prestataire de son choix sur la base des éléments de cadrage identifiés. Dès lors, **la suite du Parcours (Pack initial et Packs relais) repose sur une étroite collaboration entre le prestataire terrain, le prestataire accompagnateur et le bénéficiaire, avec la présence de l'ANSSI aux phases-clés.**

La **déclinaison des mesures au sein des 4 Parcours** permet de proposer au bénéficiaire des actions adaptées à son niveau de maturité. Ce procédé garantit un haut degré de personnalisation des plans de sécurisation tout en garantissant l'homogénéité du dispositif.



« La gestion tripartite a été essentielle dans la bonne réalisation de la phase initiale. »

Un syndicat mixte en région Normandie

Un réseau d'acteurs mobilisé pour un suivi personnalisé

Afin de garantir un suivi et accompagnement personnalisé de chaque bénéficiaire, un fonctionnement multi-niveaux associant l'ensemble des parties prenantes a été mis en place.

- **Une Cellule Relation Candidats**, composée de **chargés de dossier**, représente le point de contact unique des bénéficiaires intégrant le parcours. Elle propose à la fois un accompagnement administratif (réponses aux candidats, suivi des dossiers de subvention, suivi de la contractualisation…) et méthodologique, en identifiant le parcours cohérent, en fonction des besoins spécifiques de chaque organisation.
- **Des prestataires accompagnateurs** assurent un suivi personnalisé et rapproché de l'ensemble des bénéficiaires engagés dans la réalisation de leur pack initial et pack relais. Chargés de faire l'interface avec l'ANSSI, ils s'assurent du bon déroulement de chaque Parcours et de la **cohérence des prestations réalisées avec les objectifs de la démarche**.
- **Des prestataires terrain** sont choisis par le bénéficiaire en amont de la réalisation de leur pack initial et pack relais afin de mettre en œuvre l'ensemble des travaux de la démarche (audit organisationnel, audit technique, sensibilisation et mesures de sécurisation).

Acteurs impliqués dans les Parcours de cybersécurité

Une **équipe d'appui au pilotage** du programme assure la définition et l'actualisation du contenu des Parcours, la coordination de l'ensemble des acteurs, le pilotage des actions transverses et la consolidation des éléments de suivi.

3. Une mise en œuvre maîtrisée

Des bénéficiaires satisfaits de cette offre de service et qui s'engagent durablement

Le questionnaire interroge les bénéficiaires sur le déroulé général du Parcours et les éléments méthodologiques proposés.

Dans un objectif d'amélioration continue, un **questionnaire de satisfaction** a été distribué à l'ensemble des bénéficiaires ayant achevé leur pack initial. **Près de 360 réponses ont été déjà été traitées et les retours sont très positifs.** Les participants saluent l'utilité et la qualité générale de l'accompagnement ainsi que la pertinence des plans de sécurisation au regard du contexte de leur structure.

« Nous sommes très satisfaits de cette première phase, la démarche est rigoureuse et porteuse de valeur pour notre structure. Nous comptons en tirer meilleur profit. »

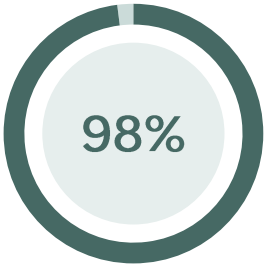
Une commune de plus de 10 000 habitants en région Provence-Alpes-Côte d'Azur

99%

des bénéficiaires sont globalement satisfaits de la démarche

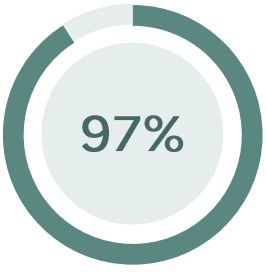
« Le chantier est conséquent, il faudra assurer sur la durée. »

Une métropole de la région Grand-Est



98% des bénéficiaires se déclarent **satisfaits** de l'accompagnement proposé et du traitement de leur candidature

98% des bénéficiaires confirment que **l'entretien de pré-diagnostic et le cadrage des prestations du pack initial ont permis de cibler leurs besoins**



97% des bénéficiaires considèrent que **le plan de sécurisation est pertinent au regard du contexte de leur structure**

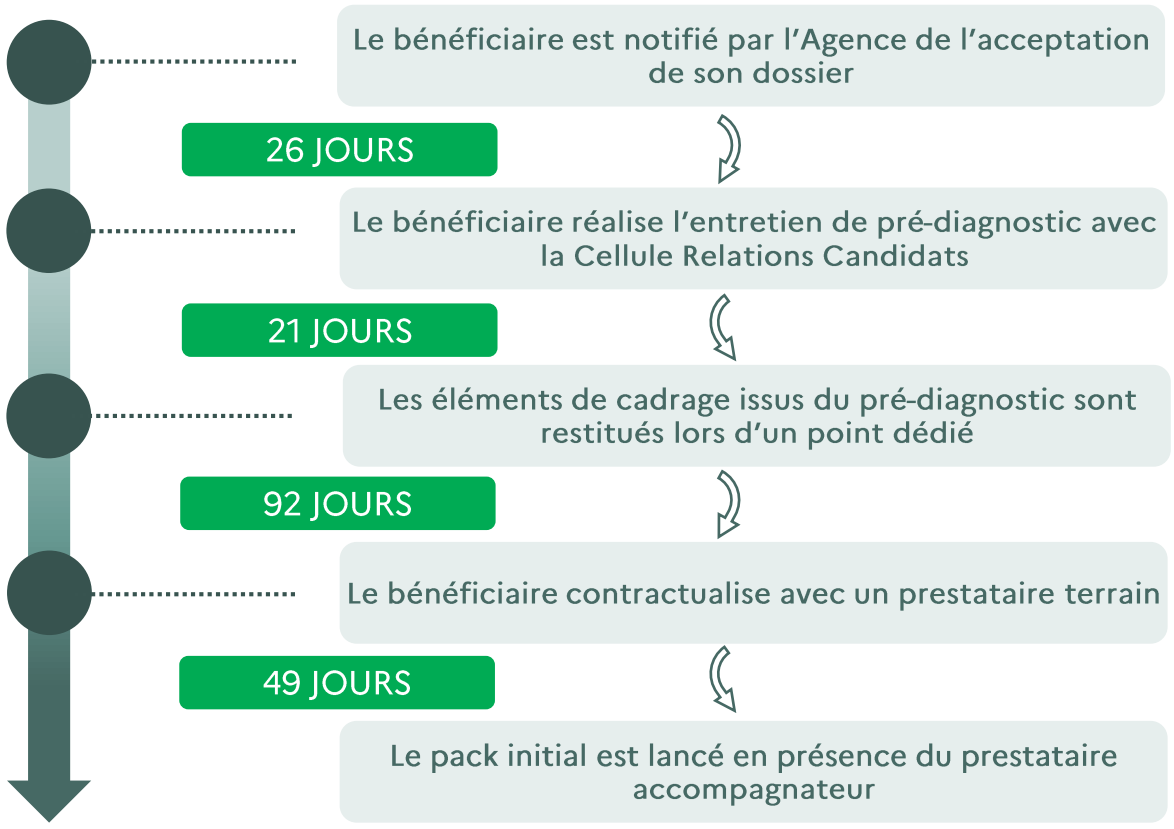
Des attentes fortes en matière de dynamique et d'engagement et peu d'abandon

L'adéquation du dispositif avec les attentes des bénéficiaires, et la satisfaction de ceux-ci avec les Parcours proposés, est également mesurable grâce au **très faible taux d'abandon en cours de Parcours, inférieur à 2%.** Ce haut niveau d'engagement est d'autant plus notable que les bénéficiaires font face à un contexte conjoncturel difficile en termes de disponibilité des ressources humaines et financières et que la majorité d'entre eux notent le caractère exigeant des Parcours.

< 2 %

Taux d'abandon en cours de Parcours

*Délais **médians** de démarrage des Parcours*



- Contraintes liées aux **stratégies d'acquisition et aux règles des marchés publics** ;
- **Fortes tensions sur le marché** des prestations intellectuelles en cybersécurité ;
- **Difficultés organisationnelles** propres aux bénéficiaires (changement d'interlocuteur, difficultés à obtenir des validations hiérarchiques, charge de travail importante) ;
- Contraintes imprévues liées à des **cyberattaques.**

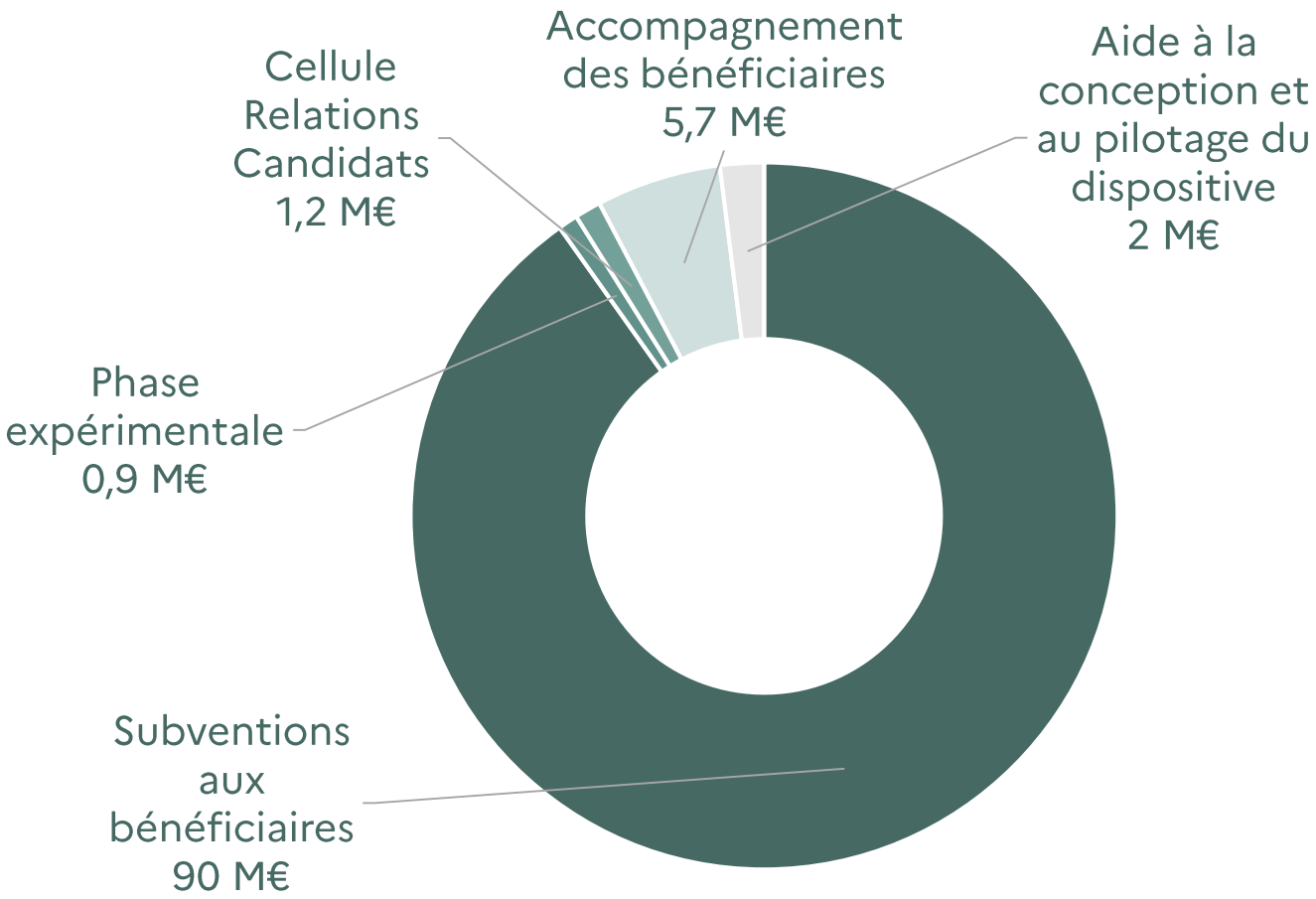
« Ce plan est très prenant mais nécessaire. La note obtenue [score de cybersécurité] est rude mais les actions à entreprendre sont claires »

Un établissement public en région Ile-de-France

Une industrialisation de la démarche pour limiter le coût des prestations

La mise à disposition d'un ensemble d'outils et guides préalablement produits par l'ANSSI a permis de **maîtriser le coûts de la mise en œuvre des packs.** Les prestataires terrain peuvent s'appuyer sur des livrables-types (supports de sensibilisation, plan de sécurisation, etc.) et des éléments méthodologiques (guides d'entretien, etc.) et ainsi concentrer leur intervention sur l'apport d'expertise et d'accompagnement opérationnel.

Budget du dispositif de Parcours de cybersécurité



90% du budget *Parcours est* consacré aux subventions directes aux bénéficiaires pour leur permettre de réaliser les packs.

II. Une amélioration concrète du niveau de sécurité

1. Des « mesures urgentes » et des actions ciblées de sensibilisation

93%

des Parcours comprennent un volet de remédiation immédiate

Un des objectifs principaux du dispositif est **l'amélioration à court terme du niveau de sécurité des SI** des bénéficiaires afin de diminuer au plus tôt le risque d'une attaque ou d'en atténuer les effets.

Les audits organisationnels et techniques réalisés dans le cadre du Pack initial permettent l'identification des vulnérabilités et la priorisation des actions afin de déterminer les mesures correctives appropriées. Le Parcours inclut dès la première phase des actions de remédiation immédiate pour corriger les failles de sécurité les plus urgentes. Les prestations d'audits techniques et organisationnels réalisées permettent de détecter un grand nombre de vulnérabilités. Par exemple, 828 forêts Active Directory (AD) sont ainsi suivies régulièrement par le service *Active Directory Security* (ADS), accessible sur simple inscription auprès de l'ANSSI, et améliorées en moyenne de 9%.

9%

de progression moyenne sur les AD

La mise en œuvre des premières actions du plan de sécurisation

Le plan de sécurisation construit à l'issue du diagnostic initial met en lumière les enjeux de sécurisation spécifiques de la structure. Par l'intermédiaire du Pack relais plus de 1900 mesures ont déjà été validées, pour près de 450 bénéficiaires.

Comment le déploiement d'un *Endpoint Detection and Response* (EDR) a permis d'éviter le pire pour une intercommunalité pendant son Parcours

Un bénéficiaire, en Parcours depuis avril 2021, disposait d'un plan de sécurisation coconstruit avec les prestataires terrain et accompagnateurs dans lequel l'EDR était inscrit. Le 26 septembre 2022, les deux alertes générées par l'outil révèlent la présence de deux balises *Cobalt Strike*. L'intrusion est qualifiée et les deux machines affectées sont immédiatement isolées évitant ainsi un chiffrement des données par rançongiciel.

447

Packs relais déjà analysés par l'ANSSI

1630

Mesures urgentes de sécurisation validées

Des directions sensibilisées aux enjeux et prêtes à mettre à disposition les moyens nécessaires

Un des objectifs essentiels des Parcours de cybersécurité est de mettre la cybersécurité au cœur des priorités stratégiques des dirigeants. Pour cela, une attention particulière a été portée sur la sensibilisation des équipes dirigeantes des bénéficiaires accompagnés, notamment lors de la validation du plan de sécurisation.

96 %

des bénéficiaires ayant démarré leur Pack relais ont sensibilisé leurs dirigeants à leur plan de sécurisation.

« Le plan de sécurisation est ambitieux mais atteignable avec l'apport de ressources humaines supplémentaires identifié lors de l'audit. »

Une communauté d'agglomération de 80 000 habitants

« Malgré nos faibles moyens RH, nous sommes motivés et notre Direction générale a pleinement conscience des enjeux de la démarche. »

Un centre Hospitalier en région Provence-Alpes-Côte d'Azur

Des agents sensibilisés dès la phase initiale

Les bons réflexes des agents au sein des structures sont essentiels. Des campagnes de sensibilisation ont été conduites auprès d'agents ciblés, dont l'activité quotidienne constitue une porte d'entrée pour une potentielle cyberattaque. Ainsi, **six publics spécifiques ont été identifiés**, parmi eux, les équipes achats, les ressources humaines, les développeurs, les ingénieurs biomédicaux (pour les établissements de santé), les administrateurs du SI et la direction, dont les élus pour les collectivités territoriales. Ces sensibilisations ont lieu dès la phase initiale du Parcours.

6 600

participants aux campagnes de sensibilisation

2. Une réponse adaptée aux besoins de sécurité opérationnelle constatés lors des « Packs initiaux »

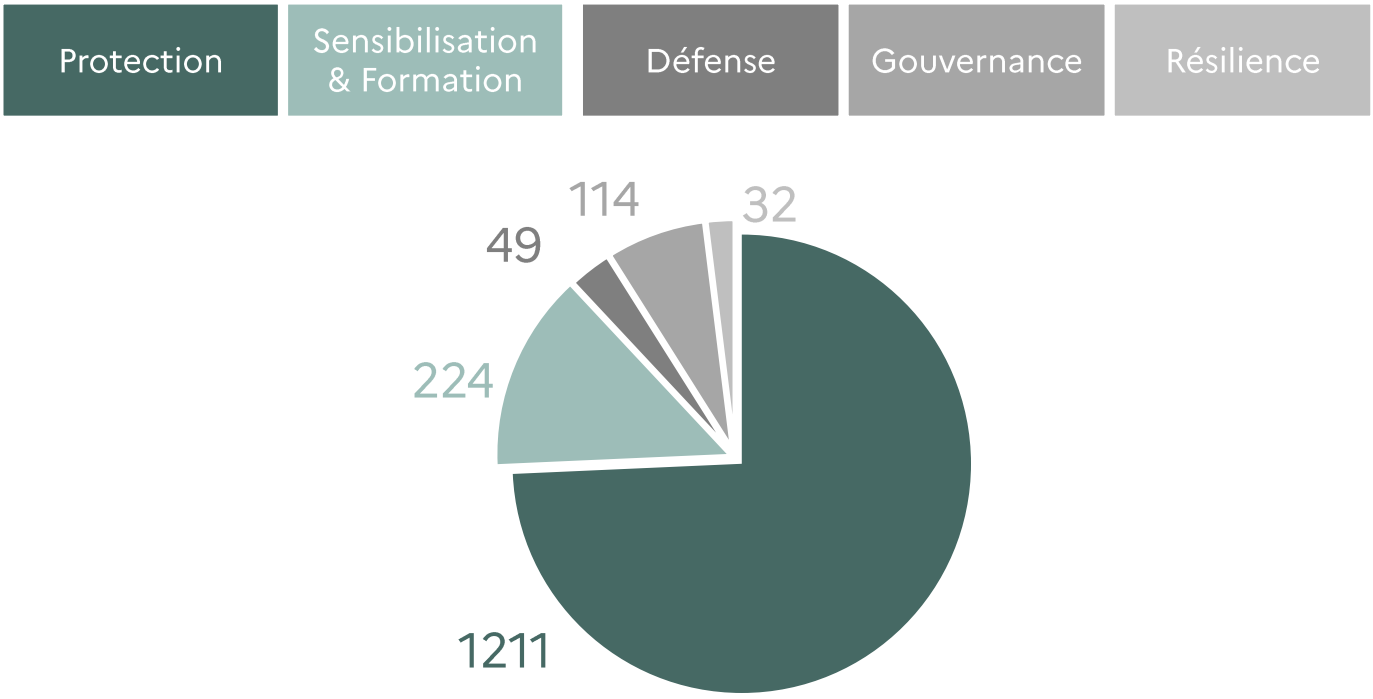
Principales vulnérabilités identifiées lors du diagnostic (Pack initial)

Cette liste représentative de constats largement établis au près d'autres acteurs publics illustre la nécessité d'adresser en priorité les **besoins fondamentaux** de la cybersécurité.

- Manque de sensibilisation des agents
- Absence de politique de mots de passe
- Messagerie exposée
- Absence de gestion de l'obsolescence et des mises à jour
- Accès administrateurs non centralisés
- Postes de travail non supervisés
- Réseaux décloisonnés
- Annuaires non sécurisés
- Absence d'isolation des sauvegardes

Répartition des mesures prioritaires identifiées

La part importante occupée par les **mesures de protection** souligne l'urgence d'augmenter rapidement, de façon concrète et efficace le niveau de sécurité numérique des bénéficiaires.



3. Un suivi planifié des Packs relais

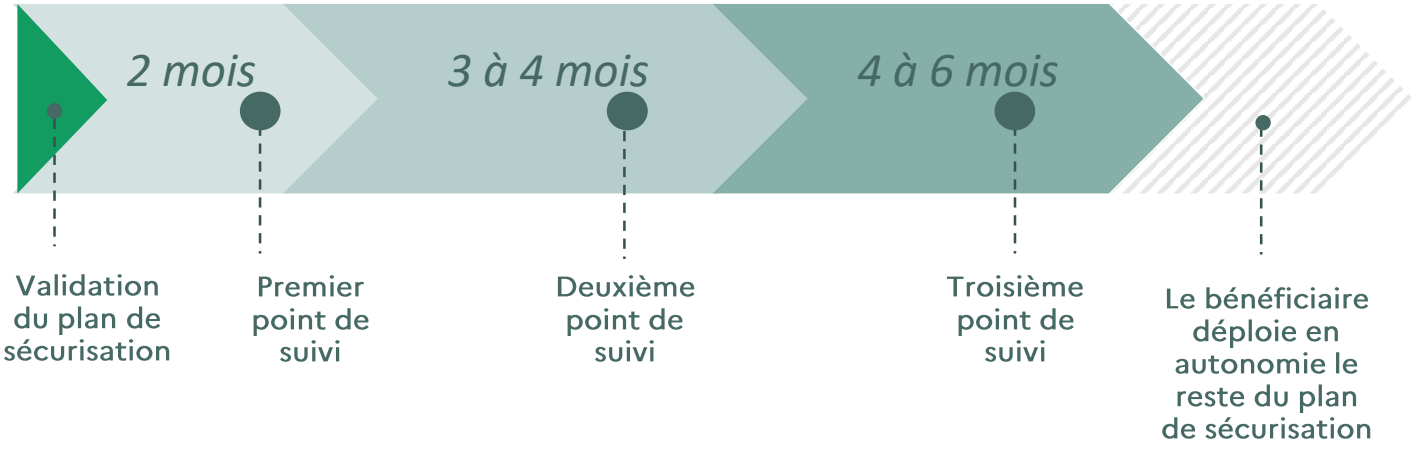
Les accompagnateurs réalisent des points de suivi réguliers avec les bénéficiaires afin de les aider dans leurs travaux d'implémentation des mesures prioritaires du plan de sécurisation.

Trois réunions sont ainsi planifiées, une première intervenant deux mois après la validation du plan de sécurisation. Pour les deux échéances suivantes, le rythme est modulable en fonction de l'avancée de chaque Parcours afin de répondre au mieux aux besoins des structures. L'ANSSI, par l'intermédiaire des délégués territoriaux et sectoriels, assure le suivi des bénéficiaires dans le prolongement des points assurés par les accompagnateurs.

+ de 2800

Points de suivi prévus pour accompagner la mise en œuvre des plans de sécurisation sur la durée

Un suivi des packs relais dans la durée



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

Une commune de 20 000 habitants en région Provence-Alpes-Côte d'Azur

III. Une contribution au renforcement du tissu industriel français de la cybersécurité

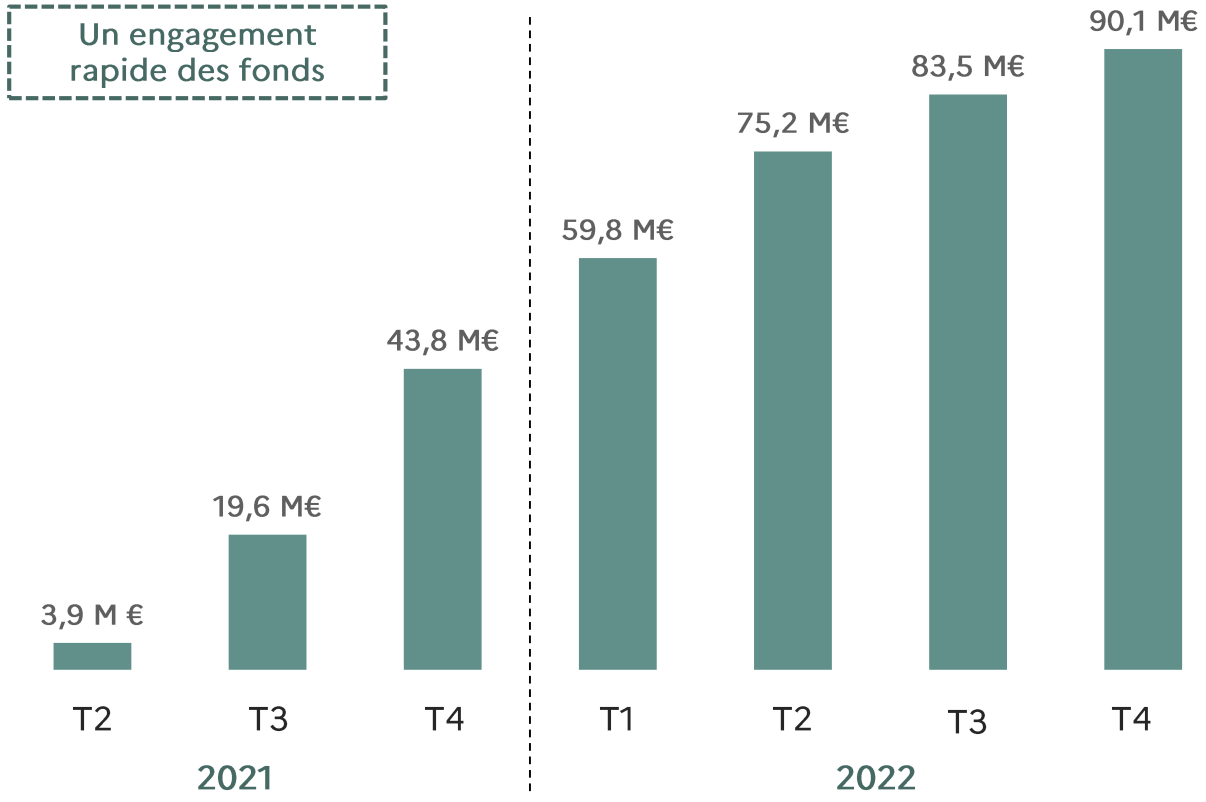
1. Une aide exceptionnelle de l'Etat et de l'Europe déployée rapidement sur le territoire

Les Parcours de cybersécurité s'inscrivent dans le cadre du plan de relance de l'économie et doivent donc être engagés avec célérité pour répondre aux enjeux. Le dispositif d'attribution et de versement des subventions a été conçu et piloté afin de permettre aux bénéficiaires d'engager au plus tôt les prestations.

Ce déploiement rapide ne s'est cependant pas fait au détriment d'un contrôle rigoureux. Le dispositif intègre ainsi à chaque étape une exigence de fourniture d'engagements et de justificatifs de la part des bénéficiaires.

90 M€

de subventions aux bénéficiaires



2. Des prestataires sur le terrain satisfaits de la démarche

Une méthodologie rapidement appréhendée

Suite à l'appel à manifestation d'intérêt organisé en mai 2021 pour recenser les entreprises susceptibles d'accompagner les bénéficiaires dans leurs Parcours en qualité de prestataire terrain, plus de **170 prestataires terrain différents** ont indiqué avoir contractualisé avec un bénéficiaire dans le cadre des seuls packs initiaux.

Cette grande diversité d'acteurs a permis de faire face à la **forte tension du marché du conseil cyber** en ne faisant pas reposer uniquement la demande sur les acteurs principaux du secteur.

60%
des prestataires terrains sont localisés en dehors de l'Ile-de-France

« La méthodologie définie s'est révélée très pertinente et les éléments documentaires mis à disposition nous ont permis de nous focaliser sur le contexte spécifique du bénéficiaire. »

Une entreprise de services du numérique (ESN) de 5 employés de la région Grand-Est

170* Prestataires terrains présents au côté des bénéficiaires

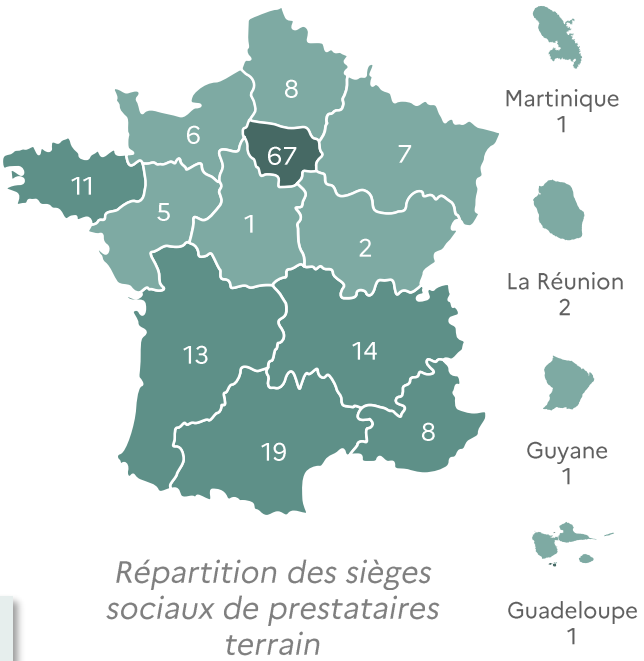
Au 31/12/2022

Les prestataires terrain ont fait part de leur satisfaction sur la structuration du dispositif, qui leur a permis d'être rapidement opérationnels et de délivrer des **prestations à coûts modérés** grâce notamment à deux éléments structurants de la démarche :

- **Un socle méthodologique** décliné au travers d'un corpus documentaire riche de guides, d'outils dédiés et de livrables-types.
- **L'expertise des prestataires accompagnateurs** qui ont capitalisé les retours d'expérience d'un grand nombre de Parcours.

96%
des prestataires terrain déclarent être satisfaits du déroulé des Parcours.

Un maillage territorial assuré par un réseau de prestataires terrain



Répartition des sièges sociaux de prestataires terrain

* 170 sociétés différentes mobilisées par des bénéficiaires dans le cadre des Packs initiaux au 31/12/2022

Un soutien à la dynamisation du secteur des prestations intellectuelles en cybersécurité

45 ESN différentes ont répondu au questionnaire de satisfaction

Afin d'obtenir un retour d'expérience des prestataires terrain sur le déroulé des Parcours de cybersécurité, un **questionnaire de satisfaction** a été distribué à l'ensemble des professionnels chargés d'accompagner les bénéficiaires dans la réalisation de leur Pack initial et Pack relais.

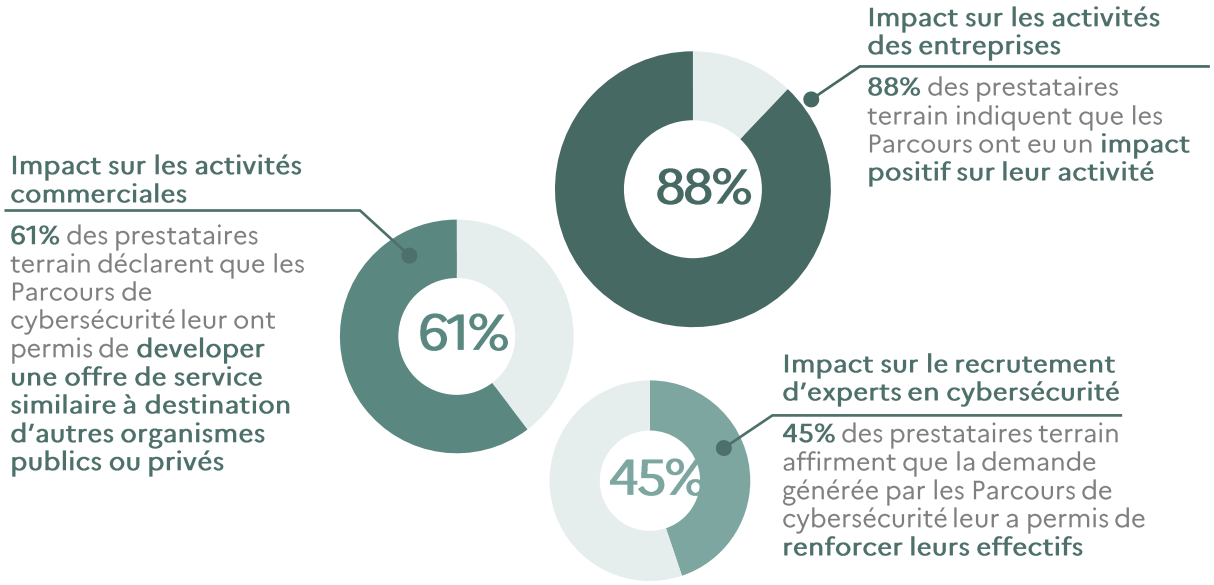
Près de **60 réponses** ont été traitées et les retours s'avèrent être très positifs, notamment au regard de **l'impact concret que le programme a pu avoir sur l'activité des entreprises du secteur de la cybersécurité.**

« Nous sommes mieux identifiés dans la région sur le sujet de la cybersécurité, les collectivités étant un secteur d'activité sur lequel nous avions du mal à nous positionner. »

Une ESN de 5 employés de la région Grand-Est

86%

des prestataires terrain affirment que les Parcours de cybersécurité ont fait appel aux entreprises locales et les ont mis en valeur.



« Nous sommes en train de structurer notre offre pour permettre une généralisation de ce type de dispositif à l'ensemble de nos clients. »

Une ESN de 5 employés de la région Grand-Est

Un plan de sécurisation bâti sur des solutions européennes

Le dispositif vient également soutenir le tissu industriel français et européen de cybersécurité et s'inscrit dans l'effort de relance général en réponse à la crise sanitaire. A cet effet, les actions de sécurisation identifiées dans les feuilles de route reposent essentiellement sur des **produits d'éditeurs français et européens.**

Ces solutions sont en partie financées par les bénéficiaires qui sont tenus de participer à leur mise en œuvre opérationnelle, *via* notamment un cofinancement.

95%

Des solutions retenues sont européennes

29,8 M€ d'investissement dans l'acquisition et l'implémentation de solutions françaises

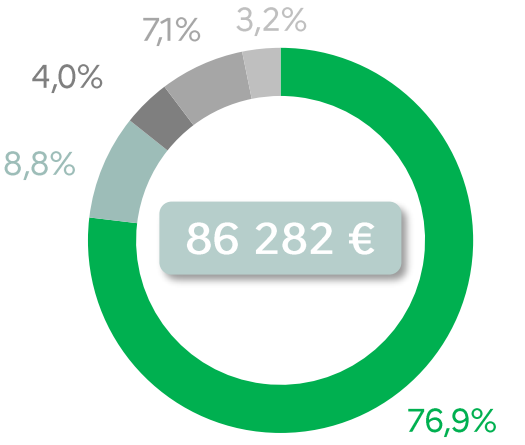
24,6 M€ de dépenses prévues en prestations de conseil d'acteurs français

54,7 M€

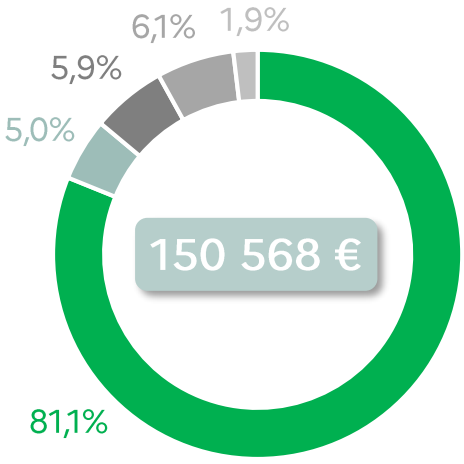
Des investissements significatifs en complément des subventions versées

Le niveau d'investissement que prévoient les bénéficiaires à court terme est significativement supérieur aux 72 000 euros attendus pour les collectivités et 130 000 euros pour les établissements de santé.

En moyenne, le niveau d'investissement sur les Packs relais est **22%** **supérieur au montant prévu par le dispositif**



Dépenses prévisionnelles pour un Pack relais de **collectivité territoriale ou établissement public**



Dépenses prévisionnelles pour un Pack relais **d'établissement de santé**

3. Une démarche qui s'inscrit dans la durée

Le manque de ressources est une difficulté récurrente exprimée par les responsables SI et SSI qui voient en ce dispositif une possibilité de disposer des moyens humains et financiers nécessaires pour poursuivre leur démarche de sécurisation, tout en restant mesurés dans leur optimisme.

> ***« La démarche est un vrai atout pour sensibiliser les dirigeants et accélérer la prise de décision. »***
>
> *Une ESN d'1 salarié en région Nouvelle-Aquitaine*

Les premiers résultats des Parcours sont cependant encourageants avec un faible taux d'abandon : la quasi-totalité des bénéficiaires ont confirmé leur engagement et poursuivi sur une deuxième phase, en investissant dans un pack relais, afin de mettre en œuvre le plan de sécurisation.

> ***« La question des moyens internes pour la mise en œuvre du plan de sensibilisation et de sécurisation reste un sujet. »***
>
> *Une communauté d'agglomération en Bretagne*

PERSPECTIVES 2023 : ENTRE ABOUTISSEMENTS ET ÉVOLUTIONS

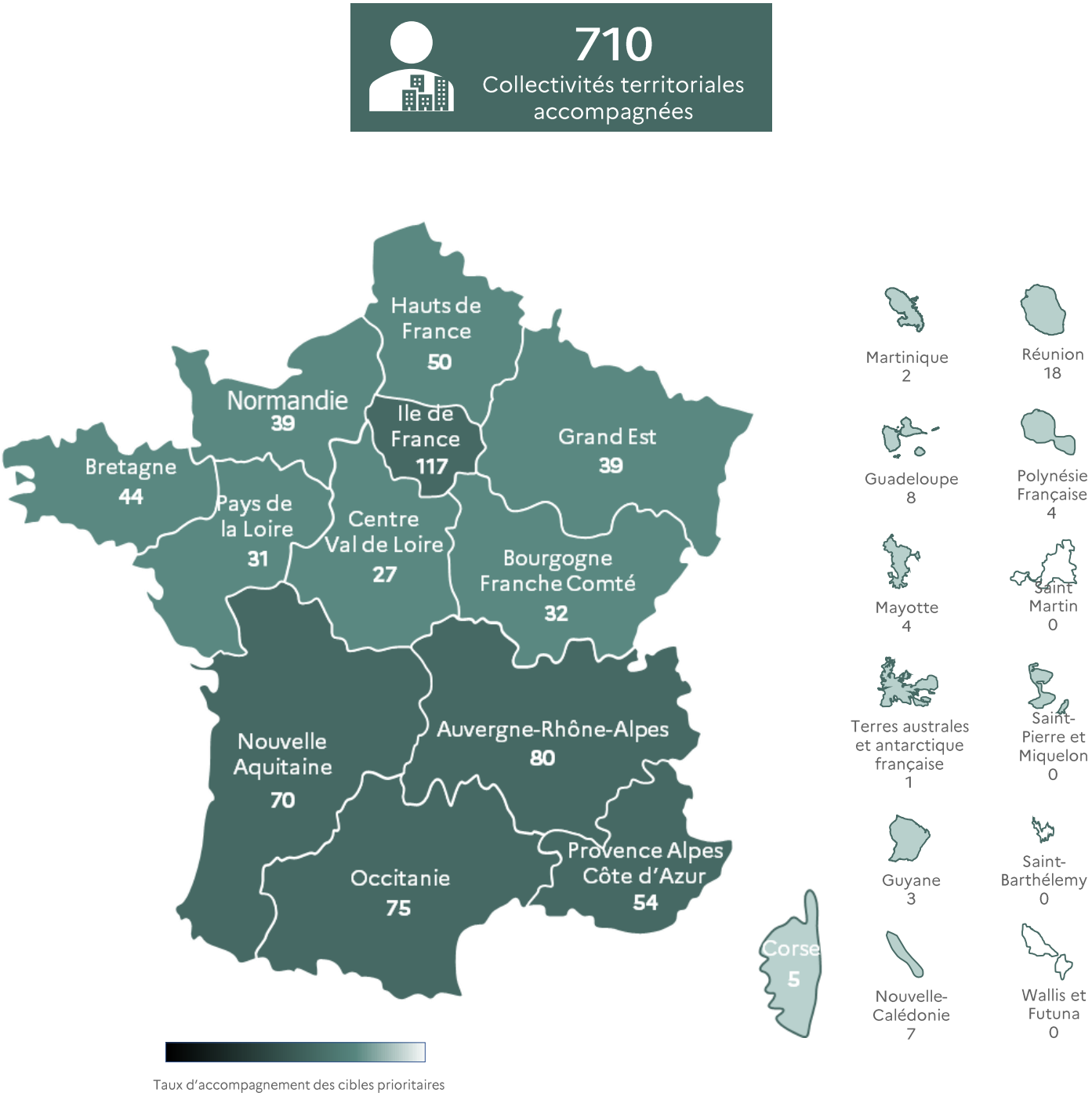
Le dispositif des Parcours a été élaboré de façon à pouvoir être reproduit en autonomie par le plus grand nombre de structures.

Dans cette logique, les outils diagnostic et le contenu du Parcours seront diffusés **sous licence libre** afin de permettre une appropriation méthodologique de ces informations par toute structure désireuse de sécuriser leur SI. Celles-ci seront en mesure d'utiliser ou d'adapter l'ensemble de ces contenus sous réserve de citer le Parcours cybersécurité de France Relance.

D'ores et déjà, certains prestataires terrains ont capitalisé sur les outils et les enseignements des Parcours qu'ils ont réalisés afin de proposer des prestations similaires, **notamment aux plus petites structures publiques n'ayant pas été directement accompagnées par un Parcours.** Grâce au calcul de leur indice de cybersécurité, les utilisateurs pourront comparer leur niveau de maturité de leur SI à celui de la moyenne des structures de nature et de taille comparables.

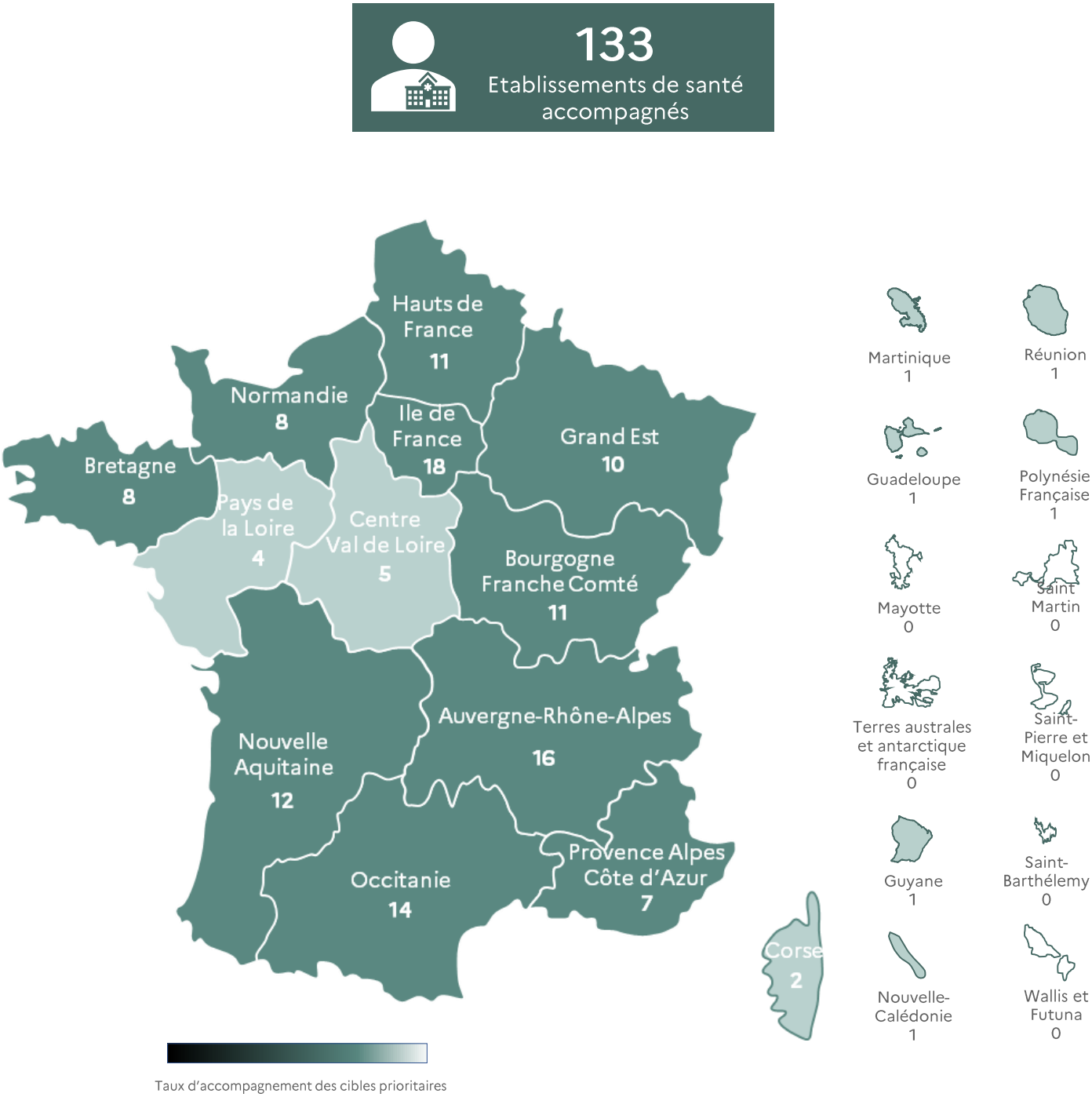
ANNEXES

1. Répartition des collectivités territoriales accompagnées sur le territoire



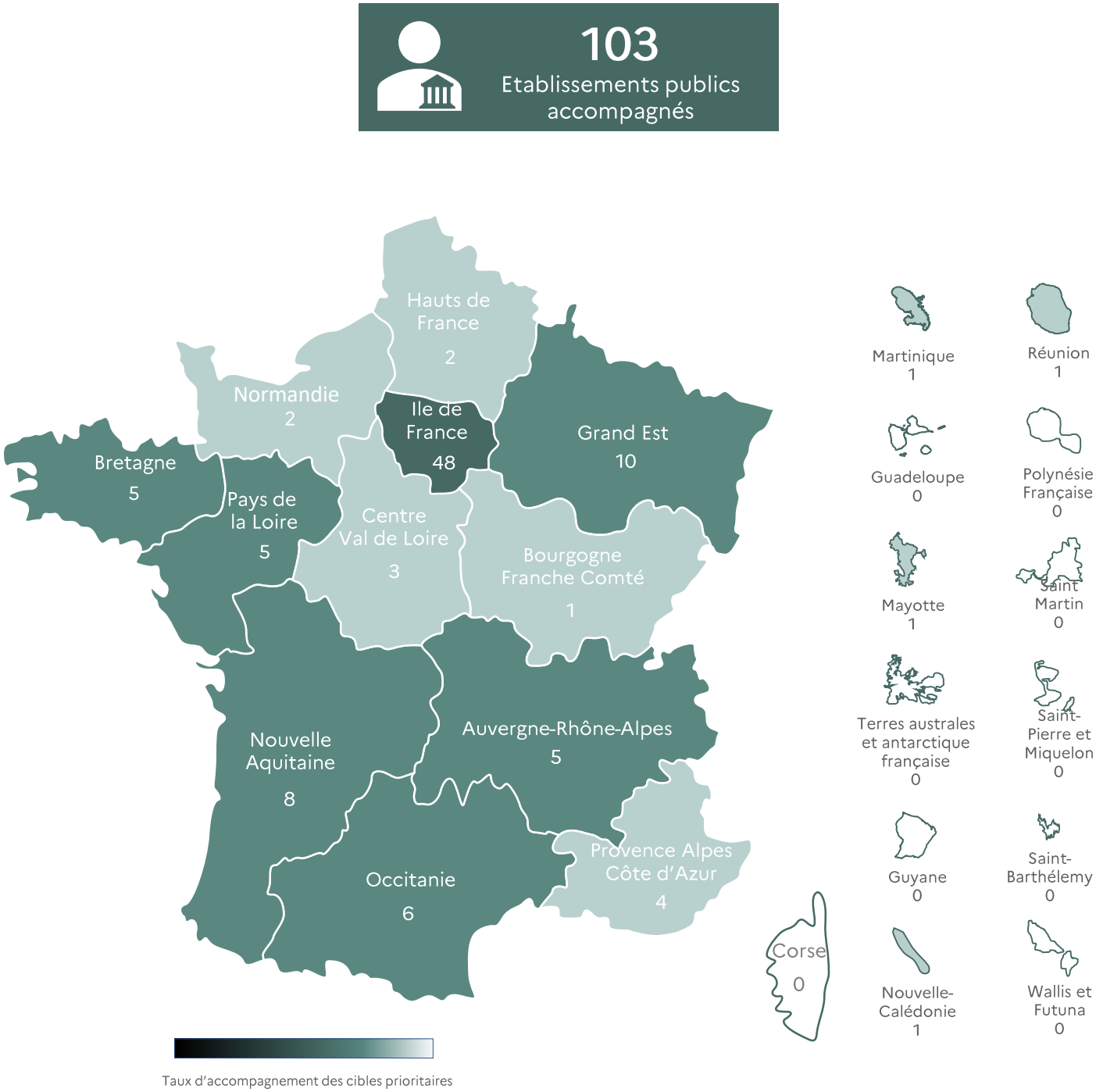
Répartition des collectivités territoriales accompagnées sur le territoire

2. Répartition des établissements de santé accompagnés sur le territoire



Répartition des établissements de santé accompagnés sur le territoire

3. Répartition des établissements publics accompagnés sur le territoire



Répartition des établissements publics accompagnés sur le territoire

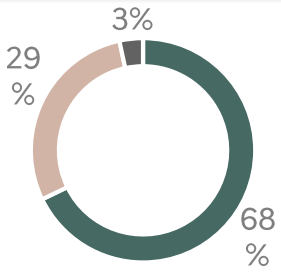
Exemples d'établissements publics accompagnés : musées, universités et laboratoires de recherche, associations reconnues d'utilité publique (action sociale)….

4. Résultats de l'enquête de satisfaction réalisée auprès des prestataires terrain

Nombre total de répondants : 59

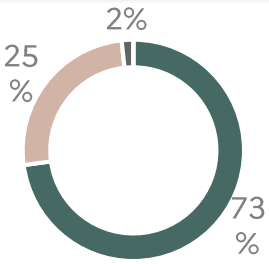
Je suis satisfait du déroulé du ou des « Parcours de cybersécurité » que j'ai réalisé(s) en tant que Prestataire terrain

Tout à fait d'accord	40
Plutôt d'accord	17
Plutôt pas d'accord	2
Pas du tout d'accord	0



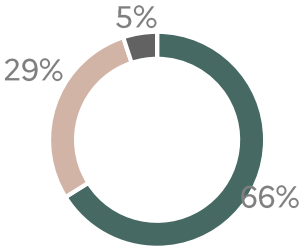
Le contenu des « Parcours de cybersécurité » et les modalités de leur mise en œuvre m'ont été clairement explicités

Tout à fait d'accord	43
Plutôt d'accord	15
Plutôt pas d'accord	1
Pas du tout d'accord	0



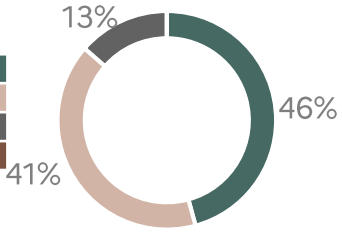
La démarche a permis à chaque bénéficiaire de construire un plan de sécurisation élevant durablement son niveau de sécurité

Tout à fait d'accord	39
Plutôt d'accord	17
Plutôt pas d'accord	3
Pas du tout d'accord	0



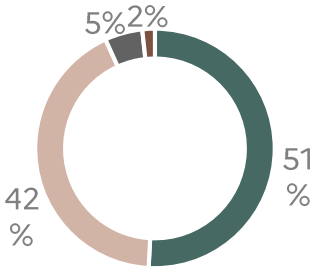
La démarche permet de sécuriser les SI des bénéficiaires au plus tôt grâce au volet « Mesures urgentes »

Tout à fait d'accord	27
Plutôt d'accord	24
Plutôt pas d'accord	8
Pas du tout d'accord	0



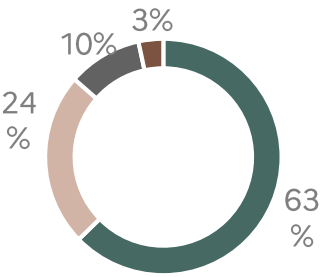
Cette démarche place les sujets de cybersécurité au cœur des priorités des dirigeants et constitue ainsi une amorce pour pérenniser l'investissement dans la SSI

Tout à fait d'accord	30
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	37
Plutôt d'accord	14
Plutôt pas d'accord	6
Pas du tout d'accord	2

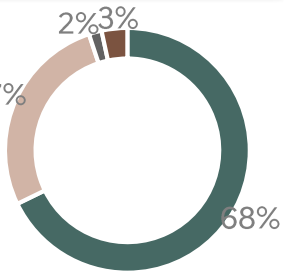


4. Résultats de l'enquête de satisfaction réalisée auprès des prestataires terrain

Nombre total de répondants : 59

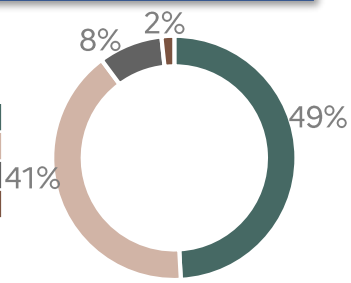
La démarche fournit une méthodologie claire et cohérente

Tout à fait d'accord	40
Plutôt d'accord	16
Plutôt pas d'accord	1
Pas du tout d'accord	2



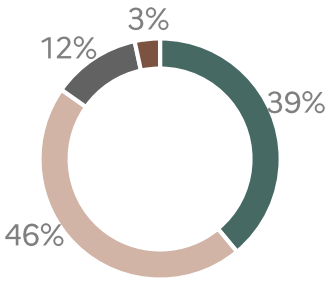
Les contenus, guides et modèles de livrables fournis dans le fond documentaire ont été rapidement appréhendés

Tout à fait d'accord	29
Plutôt d'accord	24
Plutôt pas d'accord	5
Pas du tout d'accord	1



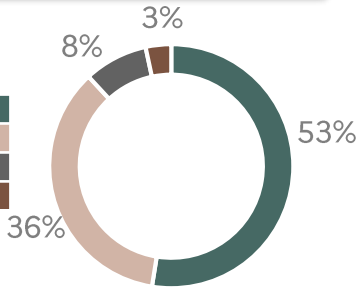
Les « Parcours de cybersécurité » nous ont permis de monter en compétence grâce à l'appui méthodologique

Tout à fait d'accord	23
Plutôt d'accord	27
Plutôt pas d'accord	7
Pas du tout d'accord	2



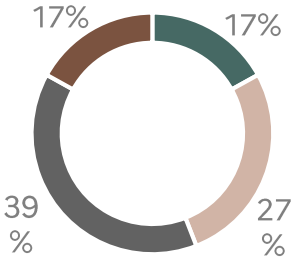
Le Parcours a eu un impact positif sur notre activité

Tout à fait d'accord	31
Plutôt d'accord	21
Plutôt pas d'accord	5
Pas du tout d'accord	2



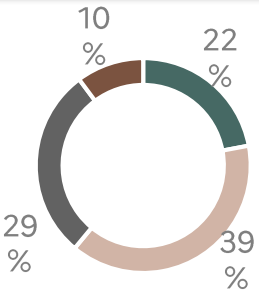
La demande générée par les « Parcours de cybersécurité » a été l'occasion de renforcer nos effectifs

Tout à fait d'accord	10
Plutôt d'accord	16
Plutôt pas d'accord	23
Pas du tout d'accord	10



Le Parcours a été l'occasion de développer une offre de services similaire à destination d'autres organismes publics ou privés.

Tout à fait d'accord	13
Plutôt d'accord	23
Plutôt pas d'accord	17
Pas du tout d'accord	6



5. Prestations et solutions financées

Défense

- Corrélation et analyse de journaux (SIEM, etc.)
- Détection (SOC, etc.)
- Veille
- Journalisation (Concentration, etc.)
- Traitement des alertes et réponses aux incidents

Résilience

- Plan de continuité d'activité
- Gestion de crises

Gouvernance

- Cartographie
- Formation
- Stratégie de sensibilisation
- Sensibilisation hors phishing
- Analyse de risque
- Audits de la sécurité (audit organisationnel, technique, scan de vulnérabilité, etc.)
- Référentiel de sécurité (chartes, processus, procédures, plans, etc. autres que PSSI)
- Homologation de sécurité
- Indicateurs
- Politique de sécurité (PSSI)
- Sensibilisation au phishing

Protection

- Cloisonnement (segmentation, Air gap, etc.)
- Configuration
- Comptes d'administration (accès des administrateurs/ utilisateurs à privilèges, Bastion, etc.)
- Sécurisation des terminaux (Antivirus/EDR, etc.)
- Sécurité physique et environnementale
- Filtrage (FW, Proxy, etc.)
- Identification, Authentification (sécurisation de l'authentification, SSO, etc.) et droits d'accès
- Procédure de maintien en conditions de sécurité (déploiement des correctifs de sécurité)
- Sécurisation des réseaux Wi-fi
- Sécurisation de l'AD
- Accès distant
- Sécurisation des applications (WAF, etc.)
- Sécurisation des mobiles (MDM, etc.)
- Systèmes d'information d'administration
- Sécurisation des mots de passe (coffre-fort numérique, etc.)
- Sécurisation de la messagerie

6. Indicateurs (1/3)

Indicateur	Résultat de l'indicateur
Nombre total de parcours acceptés	970 bénéficiaires
Nombre de collectivités territoriales bénéficiaires	710 collectivités territoriales
Nombre d'établissements publics bénéficiaires	133 établissements publics
Nombre d'établissements de santé bénéficiaires	103 établissements de santé
Nombre d'abandons avant contractualisation	24 bénéficiaires du programme l'ont abandonné avant de lancer leur pack initial
Taux de satisfaction global des bénéficiaires	99 % 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 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 vis-à-vis de la pertinence de leur plan de sécurisation	97% des bénéficiaires se sont déclarés satisfaits
Taux de satisfaction global des prestataires terrain	97% des prestataires terrain se déclarent satisfaits du Parcours
Part des prestataires terrain affirmant que le programme a fait appel aux entreprises locales et les a mises en valeur	86% des prestataires terrain affirment que le programme a fait appel aux entreprises locales et les a mises en valeur
Part des prestataires terrain indiquant que le Parcours a eu un impact positif sur leur entreprise	88% des prestataires terrain indiquent que le Parcours 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 de d'autres organismes public ou privés	61% des prestataires terrain déclarent que les Parcours de cybersécurité leur ont permis de développer une offre similaire à destination de d'autres organismes public ou privés
Part des prestataires terrain affirmant que la demande générée par les Parcours de cybersécurité leur ont permis de renforcer leurs effectifs	45% des prestataires terrain affirment que la demande générée par les Parcours de cybersécurité leur ont permis de renforcer leurs effectifs
Montant des subventions accordées depuis le lancement du programme	90 millions d'euros

6. Indicateurs (2/3)

Indicateur	Résultat de l'indicateur
Nombre de candidatures déposées en moyenne par semaine depuis l'ouverture de la plateforme (29/03/2021)	20 dossiers ont été déposés en moyenne par semaine
Nombre de candidatures déposées depuis l'ouverture de la plateforme	1 609 candidatures déposées
Taux d'abandon du Parcours	1,89% des bénéficiaires ont abandonné le Parcours en cours
Nombre de Pack initiaux lancés depuis le lancement du programme	827 Packs initiaux lancés
Nombre de Pack relais lancés depuis le début du programme	371 Packs relais lancés
Nombre de Pack relais analysés par l'ANSSI depuis le lancement du programme	447 Packs relais analysés*
Nombre d'agents sensibilisés aux bonnes pratiques et aux enjeux de cybersécurité dans le cadre du Parcours	6 600 agents sensibilisés
Détail des agents concernés par les sensibilisations	6 types de publics ont été concernés par les sensibilisations (équipes achats, ressources humaines, développeurs, ingénieurs biomédicaux, administrateurs SI, équipes dirigeantes)
Délai moyen nécessaire à la rédaction du plan de sécurisation	5 mois en moyenne
Part des plans de sécurisation présentés aux dirigeants par le RSSI	96 % des plans de sécurisation réalisés ont été présentés aux dirigeants
Nombre de plans de sécurisation élaborés depuis le lancement du programme	607 plans de sécurisation ont été élaborés
Part des bénéficiaires prioritaires	97 % des bénéficiaires du programme sont issus des structures cibles de priorité 1, 2, et 3

* Chaque bénéficiaire peut engager plusieurs packs relais, correspondant chacun à une action de leur plan de sécurisation

6. Indicateurs (3/3)

Indicateur	Résultat de l'indicateur
Nombre d'entreprises mobilisées dans le cadre du programme en tant que prestataire terrain au 31/12/2022	170 entreprises mobilisées
Répartition géographique des entreprises mobilisées	60% des prestataires terrain sont issus des territoires d'outre-mer et des régions hors Ile-de-France
Part des solutions européennes retenues dans le cadre de la réalisation des packs	95% des solutions utilisées sont européennes
Part des parcours comprenant un volet remédiation immédiate	93% des parcours comprennent un volet de remédiation immédiate
Part des usagers ayant recours à des services que sécurisent les parcours de cybersécurité	Plus de 93% des usagers
Somme des montants fléchés à date vers l'écosystème français après les packs initiaux	54,7 millions d'euros

FRELANCE

Pour tout savoir sur le volet cybersécurité de France Relance : www.ssi.gouv.fr/FranceRelance

---

Version 1.0 – Mai 2023

Licence Ouverte/Open Licence (Etalab — V1)

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