



LES PARCOURS DE CYBERSÉCURITÉ : RAPPORT D'ACTIVITÉ 2021

Volet cyber de France Relance

SOMMAIRE

Contexte et ambitions du volet cybersécurité de France Relance	<i>Page 3</i>
Les Parcours de cybersécurité	<i>Page 4</i>
1. Une démarche fondée sur l'accompagnement	<i>Page 5</i>
1.1 Des objectifs concrets	<i>Page 5</i>
1.2 Un accompagnement en trois temps	<i>Page 6</i>
1.3 Un dispositif régi par des principes structurants	<i>Page 7</i>
2. Un bilan positif après une année de mise en service	<i>Page 8</i>
2.1 Une année rythmée par plusieurs temps forts	<i>Page 8</i>
2.2 Des défis relevés, fruits d'adaptions pragmatiques	<i>Page 13</i>
3. Des perspectives 2022 entre aboutissements et évolutions	<i>Page 14</i>
Annexe : quelques chiffres	<i>Page 15</i>

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'élève à 136 millions d'euros sur la période 2021-2022.

L'importance des moyens alloués à ce volet permet 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. UNE DÉMARCHE FONDÉE SUR L'ACCOMPAGNEMENT

1.1 Des objectifs concrets

S'adressant en premier lieu aux acteurs vulnérables à des cyberattaques d'un faible niveau de sophistication, un accompagnement sous la forme de «Parcours de cybersécurité» intégré a été conçu. Très modulaire, il peut s'adapter à des entités plus matures souhaitant disposer d'une évaluation de la sécurité de leurs systèmes d'information et d'un soutien pour atteindre un niveau de protection adapté aux enjeux et au niveau de menace auxquels ils font face.

Ces parcours sont ouverts aux entités publiques volontaires, disposant d'un système d'information de quelques dizaines de machines, d'un référent pour la sécurité des systèmes d'information et s'engageant à utiliser au moins 5% de leur budget informatique à leur cybersécurité.

L'objectif est de créer la dynamique d'une démarche de sécurisation et d'en maintenir durablement les effets. Ces parcours permettent d'accompagner chaque bénéficiaire sur l'ensemble des volets nécessaires à la mise en œuvre de cybersécurité :

- Sur le plan humain en apportant des compétences, *via* des prestataires de cybersécurité auprès de chaque bénéficiaire pour définir l'état de sécurité de son système d'information et les travaux les plus urgents à réaliser en fonction de ses enjeux ;
- Sur le plan technique *via* un encadrement méthodologique des parcours par l'ANSSI ;
- Sur le plan financier *via* une subvention de 140 k€ par établissement de santé, ou de 90 k€ par collectivité territoriale ou établissement public.

Objectifs d'accompagnements par typologie de structures

Pour chacune des catégories de structures retenues dans la priorisation, le nombre d'accompagnements prévus sur la durée du programme sont les suivants :



500 Collectivités territoriales



150 Etablissements de santé

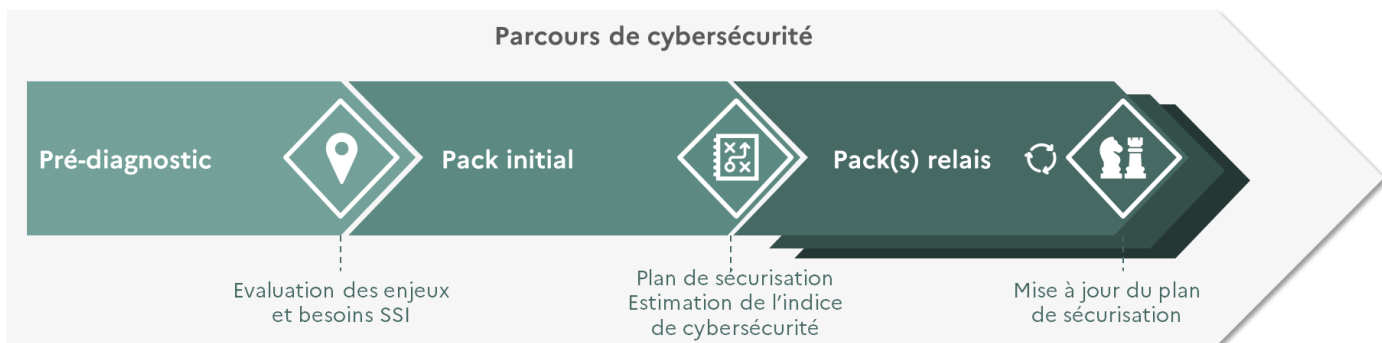


50 Etablissements publics

1.1 Un accompagnement en trois temps

Chaque parcours se décline en trois phases :

- Un **pré-diagnostic** permettant une première analyse du contexte, du niveau de maturité et des besoins du bénéficiaire. L'objectif est ici de définir le parcours le plus adapté à chaque structure.
- 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, qui couvre des actions de sensibilisation ainsi que 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** permet de mettre en œuvre opérationnellement les mesures de sécurisation du pack initial, via des prestations complémentaires comme l'acquisition et l'installation de matériels, logiciels ou services pertinents.



Déroulement d'un Parcours de cybersécurité

L'ensemble de la démarche a été conçue avec les experts de l'ANSSI assurant ainsi la pertinence technique du dispositif. Les retours d'expérience opérationnels ont été pris en compte pour l'adapter au plus près des besoins.

Chaque étape de ces parcours permet de définir, de construire et d'atteindre un objectif de cybersécurité de façon progressive, mesurable et adaptée à chaque bénéficiaire

1.2 Un dispositif régi par des principes structurants



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 en continu auprès des bénéficiaires. Enfin, l'accent est mis sur le côté opérationnel des parcours, en vue d'obtenir des résultats concrets et rapides.

Un prestataire a fourni à l'ANSSI une aide pour formaliser le dispositif, l'industrialiser et nous assister 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 terrains 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.



54*

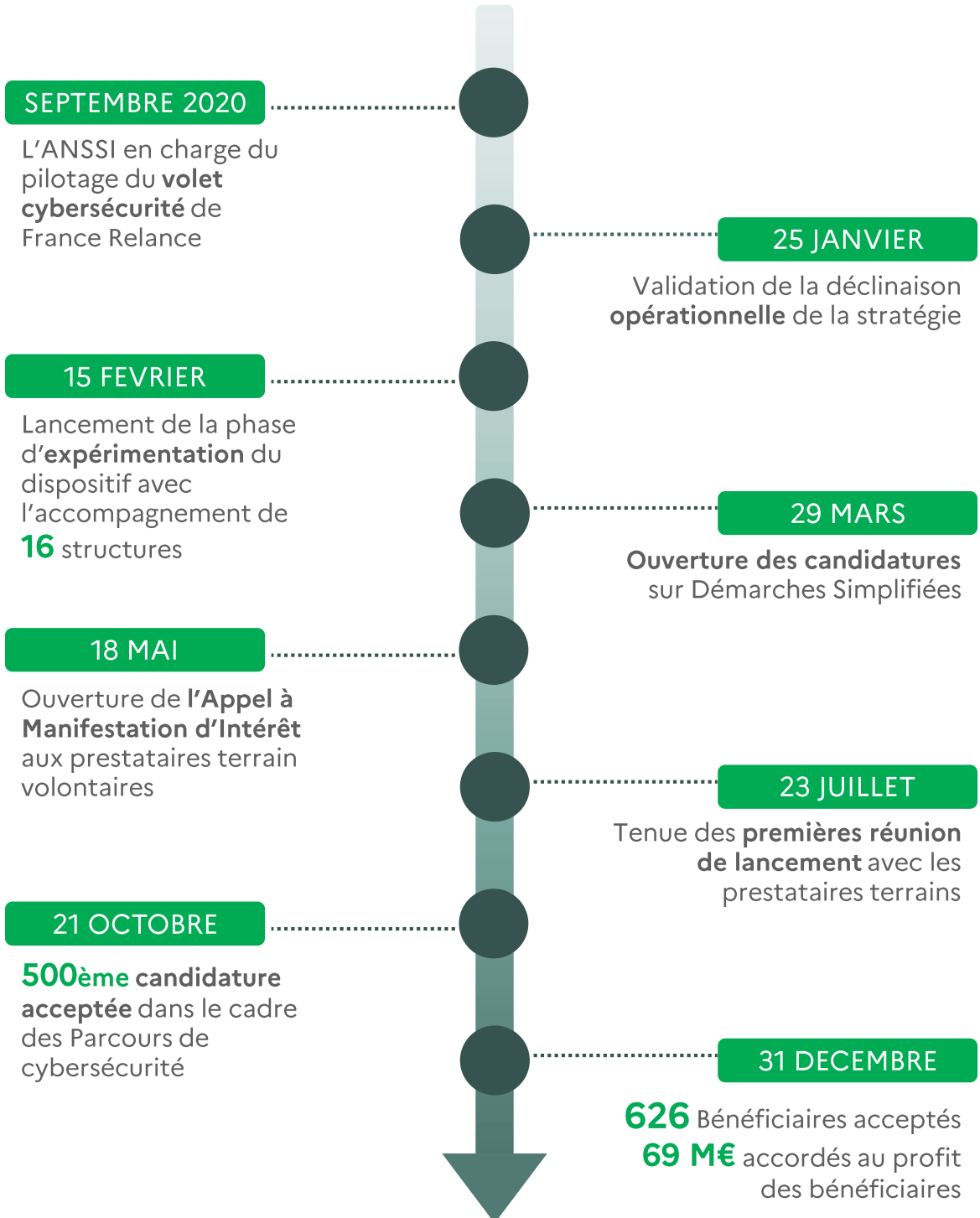
Prestataires terrains présents au côté des bénéficiaires

Au 31/12/2021

Un maillage territorial assuré par un réseau de prestataires terrain

2. UN BILAN POSITIF APRÈS UNE ANNÉE DE MISE EN SERVICE

1.2 Une année rythmée par plusieurs temps forts





Un concept décliné opérationnellement

Moins de six mois après le lancement du volet cybersécurité de France Relance, les Parcours de cybersécurité ont été définis, l'approche méthodologique formalisée et les priorités du programme arrêtées.

Cette rapidité dans la mise en place du dispositif 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.

« L'approche collaborative et constructive de la démarche a créé une synergie et une cohésion avec les parties prenantes autour de la SSI. »

Mairie de Vannes

La mise en place d'une organisation d'accompagnement

Afin d'accompagner de façon optimale les bénéficiaires lors des différentes étapes des parcours, un fonctionnement à plusieurs niveaux a été mis en place :



Acteurs impliqués dans les Parcours de cybersécurité

Une phase d'expérimentation a été réalisée auprès d'un échantillon représentatif des structures cibles permettant la mise en place progressive du dispositif.

Cette approche a permis d'éprouver la structuration des parcours et des contenus associés aux besoins concrets des structures accompagnées. Par la confrontation « à la réalité terrain », l'expérimentation avait également pour but de tirer des enseignements tactiques et opérationnels, d'ajuster et de préciser l'ensemble des facettes des Parcours de cybersécurité pour le passage à l'échelle.



**Une offre de service
éprouvée par une
expérimentation avec
16 structures**

**« La démarche était très dense mais était très intéressante et s'est très bien passée. »
CHU de Reims**



**L'ouverture de
plateformes de dépôt
de candidature et
d'appel à manifestation
d'intérêt pour les
prestataires terrain**

Afin d'optimiser le déploiement du dispositif, l'ANSSI s'appuie sur des outils interministériels existants, afin de réduire les coûts et délais de lancement du service et de concentrer ainsi les dépenses sur l'accompagnement opérationnel des bénéficiaires.

Depuis fin mars, les formulaires de candidature sont déposés sur la plateforme « Démarches Simplifiées » et les premières structures peuvent candidater au dispositif. Sur cette même plateforme, en mai, l'ANSSI lance un appel à manifestation d'intérêt pour recenser les prestataires de services en cybersécurité se déclarant en mesure d'intervenir en tant que prestataire terrain. Cette liste de prestataires volontaires est mise à disposition de chacun des bénéficiaires en amont de la contractualisation.

Par ailleurs, l'outil « Resana », plateforme collaborative pour les agents de l'Etat, permet la capitalisation des données non sensibles échangées avec les différents acteurs du dispositif.



990

Candidatures déposées

Au 31/12/2021

*Une forte attente
des structures publiques*



496

Prestataires terrains
déclarés

Au 31/12/2021

*Une mobilisation importante
des prestataires*



La promotion du dispositif appuyée par les délégués régionaux et les coordinateurs sectoriels de l'ANSSI

Afin de promouvoir l'offre de service auprès des acteurs concernés, bénéficiaires et prestataires, l'ANSSI a réalisé plusieurs campagnes de communication, dynamiques et ciblées.

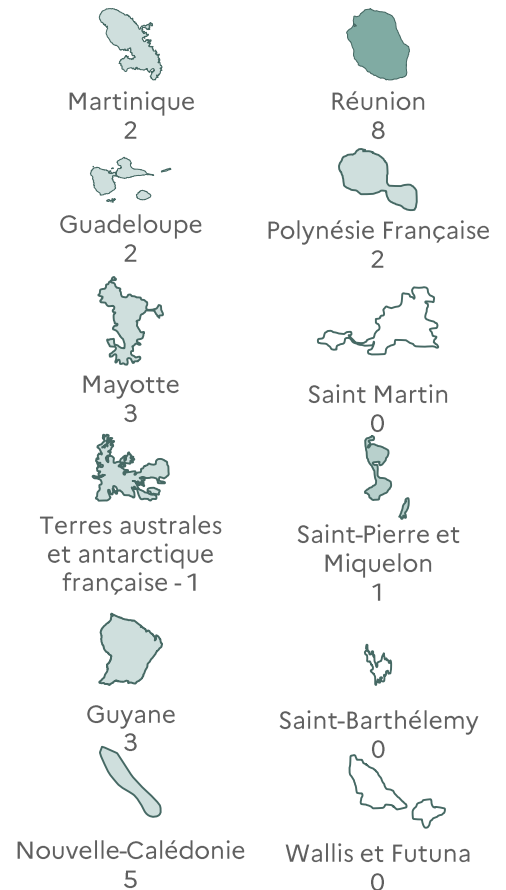
Les délégués régionaux et les coordinateurs sectoriels de l'ANSSI ont participé activement à la communication en faisant connaître le dispositif sur le terrain. Des efforts particuliers se sont notamment portés sur des structures identifiées comme prioritaires : métropoles, agglomérations, intercommunalités de tous types...



626

Bénéficiaires

Au 31/12/2021



Répartition des bénéficiaires du dispositif sur le territoire national

Après la phase d'expérimentation, le dispositif est passé pleinement en phase opérationnelle, avec un volume de candidatures important tout au long de l'année. Les équipes mobilisées, notamment dans la cellule relation candidats et chez les prestataires accompagnateurs, sont capables de s'adapter pour répondre rapidement à des montées de charge liées, par exemple, à des campagnes de communication.

La logique d'industrialisation des prestations est maintenue avec la mise à jour et l'amélioration continue des livrables standardisés. L'ANSSI, via les prestataires accompagnateurs, est attentive au bon avancement et à la qualité des prestations réalisées.



Le déploiement à grande échelle des parcours

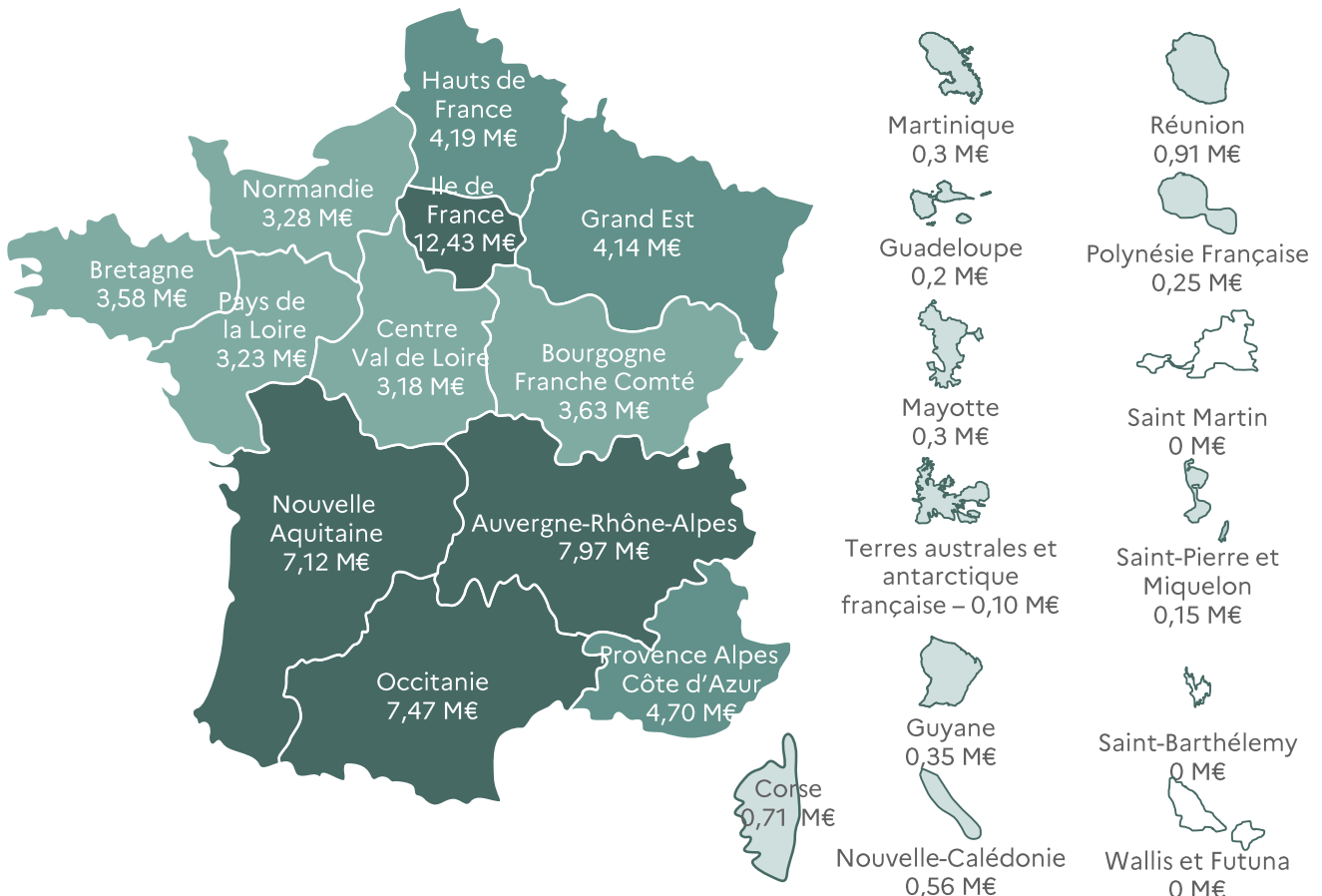


69 M€*

accordés au service des bénéficiaires

140

Parcours engagés opérationnellement



Répartition des budgets accordés sur le territoire, pour l'année 2021

* Dont 43,5 M€ effectivement engagés au 31/12/2021

2.2 Des défis relevés, fruits d'adaptions pragmatiques



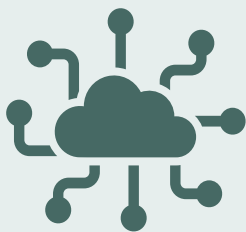
DONNER LES PERSPECTIVES D'UNE DÉMARCHE DE SÉCURISATION

L'un des enjeux des Parcours de cybersécurité est de donner aux bénéficiaires les perspectives d'une démarche de sécurisation en s'appuyant sur un diagnostic complet, tout en présentant un plan d'action atteignable et acceptable par les bénéficiaires et décideurs. Pour ce faire, les différentes actions identifiées dans le plan de sécurisation sont mises en perspective et priorisées au regard du degré d'urgence et de leur facilité de mise en œuvre, en s'appuyant notamment sur l'expertise des différents prestataires.



CONSERVER UNE DYNAMIQUE TOUT AU LONG DES PARCOURS

Lors de la phase d'expérimentation, des difficultés sur l'enchaînement des actions pour passer d'un plan de sécurisation à sa mise en œuvre (transition entre les packs initiaux et les packs relais) ont été rencontrées, mettant en exergue le défi de conserver une dynamique tout au long du parcours. Les bénéficiaires entament désormais la réflexion dès la phase de l'audit technique et le rôle du prestataire accompagnateur a été ajusté pour lui donner les moyens d'impulser le rythme et la dynamique des parcours.



FAIRE FACE À UNE FORTE TENSION DU MARCHÉ CYBER

Le marché des prestataires de service en cybersécurité est actuellement sous tension avec une demande très importante, liée aux menaces et attaques récurrentes. De ce fait, le dispositif a constaté des ralentissements dans le lancement et la mise en œuvre des parcours. Cependant, la grande diversité de prestataires sollicités dans le cadre du dispositif et leur ventilation auprès des bénéficiaires permettent d'atténuer partiellement cet effet.

3. PERSPECTIVES 2022 : ENTRE ABOUTISSEMENTS ET ÉVOLUTIONS



Tenir les engagements et finaliser les accompagnements

Après de nombreuxancements de parcours sur l'année 2021, l'enjeu de l'année 2022 est de **finaliser ces accompagnements** avec l'aide du réseau de prestataires terrain mobilisés et ainsi **renforcer concrètement la cybersécurité** des bénéficiaires. Cela passe notamment par la **sécurisation de la dynamique** des packs relais.

En poursuivant son objectif d'élever le niveau de sécurité numérique de l'État et des services publics, l'ANSSI lance plusieurs nouvelles actions pour l'année 2022 :

- **La diffusion de la démarche** : la méthode des « Parcours de cybersécurité » sera publiée et partagée à la communauté pour permettre à d'autres structures de la conduire en autonomie.
- **Le développement de nouvelles offres** : afin de saisir l'opportunité de démultiplication offerte par certaines structures capables de déployer massivement des produits dans les entités publiques, de nouveaux dispositifs seront mis en place pour :
 - L'acquisition de licences mutualisées de certains produits ou applications, permettant ainsi d'adresser des structures publiques, notamment les plus petites, qui n'ont pas été directement accompagnées par un parcours ;
 - Des campagnes de *Bug Bounty** sur des applications largement déployées auprès des acteurs publics, notamment en fonction des vulnérabilités mises en évidence lors des Parcours de cybersécurité.

Il faut également noter le rôle essentiel des autres initiatives menées par tous les acteurs de la cybersécurité française : les fortes attentes relevées par le dispositif des parcours de cybersécurité viennent confirmer la pertinence des initiatives engagées par ailleurs (GIP ACYMA, Gendarmerie nationale, Ministère des Solidarités et de la Santé) afin d'adresser les enjeux des acteurs publics dans toute leur diversité.



**Découpler les effets
du dispositif pour
apporter largement
des réponses au
plus grand nombre
de structures**

* Un *Bug Bounty* ou « prime aux bogues » permet de récompenser les personnes qui trouvent des vulnérabilités dans des logiciels

ANNEXE : QUELQUES CHIFFRES

Des prestataires nécessaires pour le suivi et l'accompagnement

En raison des délais contraints, l'ANSSI s'est appuyée sur des vecteurs contractuels existants (marchés de la Direction des Achats de l'Etat, centrale d'achat public) pour mobiliser les prestataires en charge de la cellule relations candidats et de l'accompagnement des bénéficiaires.



Dès 2021, Wavestone et Formind, suivis de la société BSSI en 2022, sont chargés d'accompagner les bénéficiaires.



La société Wavestone porte également la cellule relations candidats et l'aide au pilotage d'ensemble.

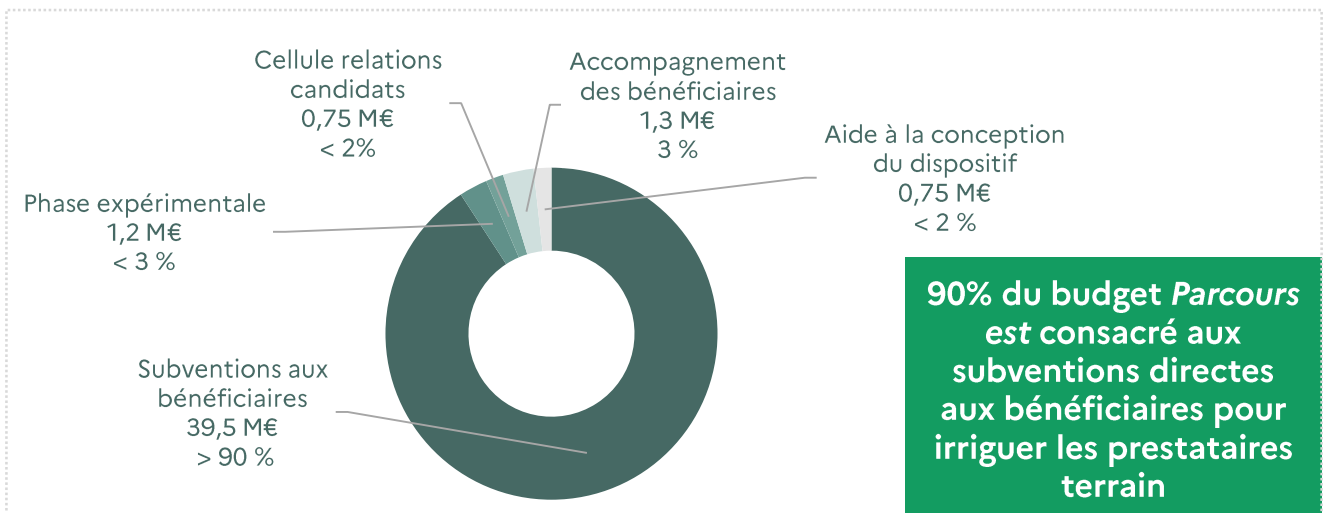
L'engagement financier nécessaire pour ces prestations est de l'ordre de 10% du montant total de ce dispositif et permet d'accompagner les bénéficiaires par des experts cyber pour faire grandir leur cybersécurité.

Des subventions qui profitent à la relance et à la cybersécurité

En 2021, 39,5 M€ ont été directement engagés pour des subventions aux bénéficiaires. Sur la durée du plan de relance, un total de 70 M€ sera versé sous forme de subventions pour ce dispositif, sur les 136 M€ du volet cybersécurité.

En moyenne, chaque subvention est utilisée :

- À hauteur de 30%, pour contractualiser avec des prestataires terrain et mener des prestations de sensibilisation, d'audits et de conseil ;
- A hauteur de 70%, pour mettre en œuvre, avec les prestataires terrain, les plans de sécurisation (formation, acquisition et déploiement de solution de sécurité)



90% du budget *Parcours* est consacré aux subventions directes aux bénéficiaires pour irriguer les prestataires terrain

Budget 2021 des *Parcours* de cybersécurité

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

Version 1.0 – **Février 2022**

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

