RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Rapport d'activité sur le volet cyber du Plan national de relance et de résilience

FRANCE 2030

Financé par l'Union européenne
NextGenerationEU

Dans le cadre du volet cybersécurité du plan national de relance et de résilience (PNRR), l'ANSSI a mis en œuvre un certain nombre de mesures destinées à renforcer la sécurité des réseaux des services publics et de l'Etat.

A cet effet, quatre objectifs ont été poursuivis :

- Création d'équipes de réponses à incident dans les territoires ;
- Déploiement de packs de diagnostic et de sécurité pour les bénéficiaires éligibles ;
- Acquisition de produits de sécurité au profit de l'Etat et des services publics ;
- Augmentation de la capacité nationale de détection des cyberattaques.

1. Création d'équipes de réponse à incidents

Face à une augmentation de 255% des signalements d'attaques par rançongiciel[1] dans son périmètre par rapport à 2019, l'ANSSI, en tant que centre de réponse à incident cyber gouvernemental (*CERT-FR*), a proposé en 2020 de faire émerger, en lien étroit avec les ministères et les Régions, des centres de réponse à incident (*CSIRT-cyber security response team*). Véritables centres d'urgence cyber, ils ont pour objectif de proposer aux acteurs de taille intermédiaire présents sur leur territoire un service de réponse à incident de premier niveau adapté à leurs besoins, sous la forme d'un service d'intérêt général gratuit.

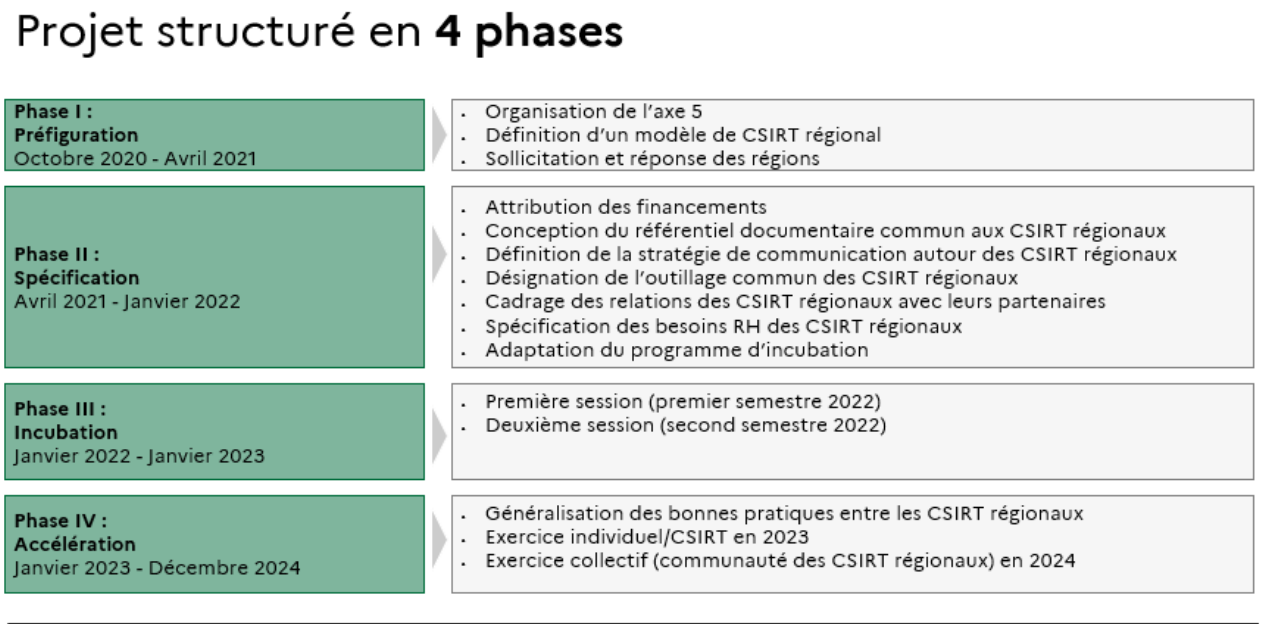
1.1 Accompagnement à la création de CSIRT

Les fonds du PNRR, mobilisés par l'ANSSI, ont permis le soutien à la création et l'accompagnement de CSIRT régionaux, incubés par l'agence. Ce programme a également permis la création de CSIRT sectoriels dont une partie a été incubée en même temps que les CSIRT régionaux.

1.1.1 La création de CSIRT régionaux

Afin d'accompagner la création des CERT, l'ANSSI a mis un place un programme d'incubation en quatre phases.

Les différentes phases d'incubation ont été les suivantes :



Une convention encadre les relations entre l'ANSSI et le CSIRT avant l'intégration dans le parcours d'incubation. Ces entités s'intègrent peu à peu aux méthodes de fonctionnement opérationnel du CERT-FR en participant à des points de situations bilatéraux entre eux et les agents du CERT-FR (tous les 15 jours) ainsi qu'une réunion bi-mensuelle multilatérale entre le CERT-FR et l'ensemble des CSIRT territoriaux.

Le suivi de ces parcours est régulièrement mis à jour dans la rubrique actualité du site: CSIRT territoriaux : un réseau essentiel face aux cybermenaces | ANSSI) .

[1] [1] Rapport menaces et incidents - CERT-FR (ssi.gouv.fr)

Par ailleurs, un bilan d'activité en application de la convention de création du CSIRT régional signée entre le SGDSN et la Région concernée est adressée chaque année à l'ANSSI. Il rappelle la structure de gouvernance du CSIRT, les points de contacts, les recrutements, les principales actions mises en œuvre, les bénéficiaires, le périmètre d'actions proposé et les résultats.

Bilan du dispositif

La mise en place du Plan France Relance s'est traduite par l'accompagnement de 12 CSIRT territoriaux (*Computer Security Incident Response Team*) et de 3 Centres de Ressources Cyber ultramarins[2], destinés à devenir des CSIRT ; ce qui constitue un réel succès par rapport aux objectifs initiaux.

Avec le recul de deux années de fonctionnement pour les plus anciens et de quelques semaines pour le plus récent, le constat est positif : peu à peu, les CSIRT régionaux se positionnent en acteurs centraux de la cybersécurité opérationnelle locale, en offrant une gamme de services commune à tous et en développant des services adaptés à leurs ressources et feuilles de route. Parmi ces services, se trouvent notamment :

- l'accompagnement de victimes dans le traitement de leurs incidents (gestion de crise, coordination de prestataires, accompagnement aux démarches légales et administratives) ;
- les activités de sensibilisation et de formation ;
- en fonction du développement de leurs activités, la veille sur les vulnérabilités de produits majeurs pour leurs bénéficiaires (petites entreprises ou de taille intermédiaire, collectivités locales, associations locales) ;
- en fonction du développement de leurs activités, la fourniture de services d'audit de sécurité (grâce à l'appui de prestataires).

Le niveau de confiance et de maturité des CSIRT territoriaux permet aujourd'hui de travailler de manière intégrée et de s'appuyer, avec l'accord explicite des victimes, les uns sur les autres lorsque nécessaire et/ou utile. Alors que le CERT-FR peut être aujourd'hui joint sur un numéro court (3218), son nouveau serveur vocal interactif (SVI) présente une opportunité de transfert d'appel en horaire non ouvré pour les CSIRT régionaux (hexagonaux et de Corse à date) vers le CERT-FR.

Des mécanismes de coordination sont aussi en cours de constitution avec la plate-forme *Cybermalveillance* pour organiser la complémentarité des actions d'assistance et/ou de remédiation.

La vocation des CSIRT relais est de rejoindre *l'InterCERT France*, association loi 1901 de CSIRT en France, dont l'objectif est de renforcer la capacité de chaque membre à détecter et à répondre aux incidents de sécurité impactant son périmètre et de devenir la « voix des CSIRT

[2] Bourgogne-Franche-Comté (opérationnel depuis le 03/10/2022), Bretagne (opérationnel depuis le 21/10/2023), Caraïbes (opérationnel depuis le 30/07/2024), le CSIRT-ATLANTIC regroupe les territoires des îles de Guadeloupe, de Guyane, de Martinique, de Saint-Barthélemy, de Saint-Martin et de Saint-Pierre et Miquelon, Centre-Val de Loire (opérationnel depuis le 20/03/2023), Corse (opérationnel depuis le 03/04/2024), Grand-Est (opérationnel depuis le 14/02/2023), Hauts-de-France (opérationnel depuis le 05/04/2023), Île-de-France : (opérationnel depuis le 27/11/2023), Normandie (opérationnel depuis mai 2022), Nouvelle-Aquitaine (opérationnel depuis avril 2022), Occitanie (opérationnel depuis le 15/03/2023), Pays de la Loire (opérationnel depuis le 13/09/2023), Provence-Alpes-Côte d'Azur (opérationnel depuis le 09/10/2023)

en France », complémentaire et autonome de celle du CERT-FR. Deux CSIRT régionaux ont déjà intégré l'association *InterCERT France* : le CSIRT Bourgogne-Franche-Comté et le CSIRT Bretagne. D'autres sont en train de candidater ou d'anticiper leurs candidatures pour cette fin d'année ou le début d'année prochaine.

En termes de missions, les CSIRT offrent notamment une réponse de premier niveau aux incidents d'origine cyber et surtout une réponse de proximité.

Ils sont complémentaires des autres acteurs cyber : le CERT-FR, *Cybermalveillance.gouv.fr*, les prestataires privés, etc.

La synthèse chiffrée proposée ci-dessous, fondée sur des échanges en bilatéral avec le CERT-FR, n'offre pas une vision exhaustive de l'activité des CSIRT territoriaux mais témoigne de leur montée en puissance progressive et de leur efficacité à connaître et se faire connaître rapidement de leurs écosystèmes respectifs.

- A ce stade, nous pouvons constater que les équipes des CSIRT régionaux opérationnels sont constituées de 4-5 personnes en moyenne et qu'ils reçoivent à peu près 20 appels par mois.
- Entre le 1er janvier et le 31 juillet 2024, les 11 CSIRT régionaux ouverts sur la période (dont le CSIRT Corse ouvert depuis le 3 avril) ont indiqué avoir traité au total 515 incidents avérés, et 534 signalements, 18% incidents avérés traités par les CSIRT dans la période étudiée concernent la compromission de systèmes d'information par le biais de rançongiciels, et 15% concernent des courriers électroniques malveillants.
- Les CSIRT territoriaux comptabilisent 826 sollicitations correspondant à des demandes relatives aux services proposés (scans d'infrastructures, demandes de formations, analyses de courriels, signalement de vulnérabilités, etc.). Certains CSIRT commencent également à diversifier leur offre de services pour évaluer le risque cyber des entités concernées.

Les actions mises en œuvre dans le cadre d'une réponse à incident dépendent du niveau de maturité des équipes des CSIRT voire également de la structuration de leur activité.

Par ailleurs, certains CSIRT territoriaux effectuent de la veille en sources ouvertes au profit des entités de leur région (veilles pouvant avoir différents types de focus type vulnérabilité ou accidentologie). Cette veille s'avère parfois bénéfique pour l'activité des CSIRT car elle leur permet de se faire connaître sur le territoire auprès des entités privées ou publiques avec lesquelles ils pourraient travailler.

Par ailleurs, une part importante du temps d'activité des CSIRT vise à promouvoir leur activité et à développer les liens avec l'écosystème de cybersécurité local (prestataires privés, gendarmerie, collectivités, établissements publics de coopération intercommunale, chambre de commerce et d'industrie, chambre des métiers et de l'artisanat, associations…) voire plus étendu (autres CSIRT régionaux, CSIRT sectoriels…), gage d'un maillage progressif visant à optimiser les échanges entre ces acteurs et ainsi à se préparer progressivement au traitement d'incidents plus complexes ou plus fort impact pour les victimes.

Il convient ainsi de souligner que l'efficacité des CSIRT ne peut être mesurée que sur le plan de la réponse à incident. Leur investissement en matière de sensibilisation est conséquent : certains CSIRT ont déjà sensibilisé plusieurs milliers de personnes aux risques induits par l'utilisation du numérique, la plupart des CSIRT participent à des évènements de sensibilisation (journée européenne de la protection des données, journée de la sauvegarde, Cybermoi/s, Appel du Cyber Juin, Etats généraux de la cyber…) et organisent des réunions de sensibilisation. Ces équipes portent des missions de prévention, de sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs régions, qu'il s'agisse de prestataires de services cyber, de collectivités territoriales, d'associations, de TPE/PME et ETI.

Les CSIRT se font également les relais de dispositifs développés par l'ANSSI tels que « *MonAideCyber* » et « *Cyber PME* » et pourront plus tard faire valoir la pertinence d'autres projets comme le service d'analyse de fichier de l'ANSSI « *Je clique ou pas* ». D'autres missions de relais sont envisagées dans le cadre du projet de loi « *résilience*» via un agrément délivré par l'ANSSI.

L'adossement à la Région des CSIRT régionaux permet de créer des synergies entre les compétences de la Région (développement économique, formation initiale et continue) et leurs missions. Les CSIRT territoriaux peuvent également aiguiller leurs bénéficiaires vers des politiques de la Région pour rehausser leur niveau de cybersécurité.

La publication en 2024 d'une version actualisée du référentiel des prestataires de réponse aux incidents de sécurité (PRIS) qualifiés par l'ANSSI, plus accessible à des prestataires de taille intermédiaire, devrait alimenter la démarche engagée dans les territoires et les différents secteurs en permettant une plus grande diversité de prestataires répondant aux besoins des bénéficiaires en complément des prestataires labellisé « *expert cyber* » par le *GIP ACYMA*.

1.1.2 Projet TEMPO : création d'un réseau de CSIRT relais au niveau ministériel

Le plan de relancea également permis la création de CSIRT sectoriels dont une partie a été incubée en même temps que les CSIRT régionaux : Le *CERT Santé*[3], le *M-CERT*[4], le *CERT Aviation*[5], le *CERT Social*[6] et le *CERT CNES*[7], au travers d'un projet baptisé TEMPO.

Ce projet consiste en l'accompagnement des ministères dans le développement de capacités permettant la construction ou le renforcement de leur CSIRT en 4 phases :

- Phase I : Le diagnostic de maturité par le prestataire des entités permettant l'attribution d'un niveau à atteindre par le ministère dans la construction ou le renforcement de son CSIRT (88 000€ de janvier à avril 2022) ;
- Phase II : La révision et l'adaptation de la feuille de route en un plan d'action échelonné et détaillé (mobilisation RH ANSSI) ;
- Phase III : La mise en œuvre du plan d'action pour mettre en place les briques essentielles à la fonction de CSIRT grâce à l'accompagnement d'un prestataire. Une durée d'environ un an est prévue pour cet accompagnement (2,7M€ maximum de fin 2022 à décembre 2024) ;
- Phase IV : L'incubation des CSIRT ministériels une fois les prérequis en place (mobilisation RH ANSSI).

Dans le cadre du projet TEMPO, les ministères ont été évalués selon le référentiel SIM3 (*Security Incident Management Maturity Model*), publiée par *l'Open CSIRT Foundation* (OCF). À la suite d'un premier questionnaire déclaratif basé sur le référentiel SIM3, un premier état des lieux a été établi pour chaque ministère. Ceci a permis la construction d'une feuille de route par ministère définissant les objectifs respectifs à atteindre. On compte une réalisation de 206 livrables effectués pour l'ensemble des ministères, soit en moyenne 20 par entité.

En sortie de la prestation dont ils ont bénéficié, les CSIRT ministériels sont capables d'offrir un premier niveau de service dont la gestion d'évènements et d'incidents de sécurité, la gestion de vulnérabilités ainsi que des actions de sensibilisation face aux menaces. Par ailleurs, plusieurs ministères ont publié en ligne un document nommé RFC 2350. Ce document recense les différents services fournis par un CSIRT et les procédures qu'il applique. La publication de la RFC 2350 fait partie des bonnes pratiques d'un CSIRT et est un gage de maturité démontrant

[3] RFC 2350 (esante.gouv.fr)
[4] Maritime Computer Emergency Response Team (M-CERT) RFC 2350
[5] rfc2350_cert_aviation_france_v2_fr.pdf (cert-aviation.fr)
[6] CERT Social | L'Assurance Maladie (ameli.fr)
[7] RFC2350 CSIRT CNES VDef 1.0

qu'il est structuré pour se connecter à ses pairs. C'est d'ailleurs un prérequis pour intégrer différentes communautés de CSIRT.

Durant le premier semestre 2024, les différents ministères parties prenantes du projet TEMPO ont participé à la 4ème phase du projet dite phase d'incubation. Lors de cette phase, les ministères ont pris part à des ateliers d'échanges avec différentes équipes de l'ANSSI dans un but de capitalisation et de partage sur les méthodes de fonctionnement de l'Agence. On dénombre en moyenne 25 participants à ces ateliers, avec un minimum de deux représentants par ministère.

Bilan :

Le projet TEMPO a permis la création d'une communauté de 10 CSIRT ministériels dont 4 sont considérés aujourd'hui comme opérationnels[8]. À la fin de l'incubation et pour maintenir cette dynamique impulsée par ce projet, les ministères continueront d'avoir des échanges entre eux (multilatéraux) et avec le CERT-FR (bilatéraux). Des points de synchronisation sont planifiés et débutent avec 6 d'entre eux (C2MI (CSIRT du MIOM), COSSIM (CSIRT du MinEdu), CERT-AE (MEAE), CSIRT Justice, CSIRT Ecologie, CSIRT-RIE) Ces points permettront de répondre aux besoins de cette communauté qui pourra continuer à gagner en maturité et s'ouvrir vers d'autres CSIRT comme par exemple le CALID (CSIRT du ministère des Armées, hors du programme TEMPO).

Les échanges opérationnels ont d'ores et déjà débuté et ont vocation à se renforcer. En effet, le CERT-FR reçoit des remontées de signalement d'incidents de leur part et partage des marqueurs sur la menace à intervalle régulier.

[8] Le CERT Santé pour les établissements de santé, le M-CERT pour le secteur maritime, le CERT Aviation pour le secteur de l'aviation civile, le CERT CNES et le CERT Social pour les caisses nationales.

2. Déploiement de parcours de cybersécurité

Les parcours de cybersécurité, mis en place par l'ANSSI dans le cadre du PNRR, ont pour objectif de contribuer, au travers d'une démarche d'accompagnement structurée, à la sécurisation des SI des bénéficiaires (collectivités territoriales, établissements publics, administrations).

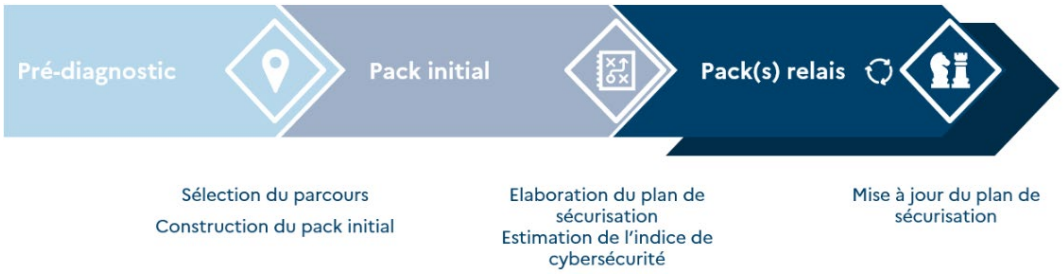
Ces parcours permettent d'atteindre un objectif de cybersécurité de façon progressive, mesurable et adaptée à chaque bénéficiaire, en adéquation avec le niveau de menace et de maturité.

Cette mesure fait l'objet d'un rapport public annuel, diffusé sur le site internet de l'ANSSI : https://cyber.gouv.fr/parcours-de-cybersecurite

Les parcours de cybersécurité, financés dans le cadre de France Relance, ont permis d'accompagner 945 bénéficiaires[9] au travers d'une démarche formalisée grâce à des concepts et guides préalablement produits par l'ANSSI (guide d'hygiène ou guide sur les attaques par rançongiciels notamment), mais aussi avec l'appui des experts de l'Agence qui ont participé à la phase de cadrage et à la définition des parcours.

Un parcours de cybersécurité se déroule en trois temps successifs :

1. En premier lieu, un *pré-diagnostic* permet d'orienter le bénéficiaire vers le parcours de cybersécurité le plus adapté au contexte et aux enjeux de sa structure, sur la base du cadrage du contenu du pack initial ;
2. Ensuite, un temps d'accompagnement d'une durée d'environ trois mois – le *pack initial* – consiste en une série de prestations standardisées s'achevant par l'élaboration d'un plan de sécurisation et de l'obtention d'un indice de cybersécurité ;
3. Enfin, la mise en œuvre opérationnelle des mesures de sécurisation via des *packs relais*.



1631 dossiers de candidatures ont ainsi été étudiés et 970 acceptés. Du fait d'abandon en cours de parcours par les bénéficiaires, 945 entités suivent (*ou ont suivi*) un parcours de cybersécurité.

Les parcours de cybersécurité portent sur les thématiques suivantes :

- Sensibilisation et organisation face au risque numérique ;
- Maîtrise des accès au SI ;
- Sécurisation des données, applications et services numériques ;
- Sécurisation des équipements de travail ;
- Protection du réseau ;
- Intégration des enjeux de la sécurité du numérique à la politique d'administration et d'exploitation ;
- Connaissance des vulnérabilités du SI ;
- Capacité à détecter et à réagir aux évènements de sécurité.

[9] Données au 4 octobre 2024.

Au 4 octobre 2024 l'état d'avancement des dossiers était le suivant :

Avancement du dossier	Nombre	Financement
Dossier pris en charge	0	Financement à verser (tranche 1+2 ou tranche 2)
Pack initial en attente de lancement	1	
Pack initial en cours	24	
Pack relais en attente de lancement	24	
Pack relais en cours	176	Financement versé en intégralité
Parcours clos	720	
Total	**945**	

Les différentes étapes du parcours font l'objet d'un suivi et de points d'étapes réguliers avec les agents de l'ANSSI. Le pack relais fait ainsi l'objet de 3 points de suivi qui conditionnent le versement de la subvention.

Etat d'avancement	
CNRS (*)	17
100%	103
75%	224
50%	136
<25%	63
Total	**543**

(*) : accompagnement direct par les équipes de l'ANSSI.

88% des parcours à terme ont un avancement des actions supérieur à 50%. Il est à noter que 12 parcours ont été clôturés à l'issue du pack initial, du fait de la décision de certains des bénéficiaires de ne pas poursuivre le parcours.

Les projections d'atterrissage des parcours au 01/04/2025, tels que présentées dans le rapport d'activité 2023 s'établissent ainsi :

Pack initial	3
Pack relais	66
Parcours clos	877

Plus de 170 prestataires terrain ont été impliqués dans ces parcours pour aider les bénéficiaires et les retours d'expérience opérationnels ont été pris en compte pour adapter le dispositif au plus près des besoins, au fur et à mesure de l'avancée du programme.

3. Acquisition de produits de sécurité au profit de l'Etat et des services publics

La troisième action du volet cyber du PNRR a consisté en la construction d'une offre pérenne de produits et services adaptés aux besoins de l'Etat :

- Création d'une offre de services
- Achat de produits et logiciels de sécurité pour répondre aux missions de l'ANSSI

Des Appel à projets ont également permis d'accompagner des bénéficiaires publics dans l'acquisition de produits de sécurité.

3.1 Création d'une offre de services

3.1.1 « Je clique ou pas »

Afin de lutter contre l'hameçonnage, qui représente aujourd'hui l'un des principaux vecteurs d'infection d'un système d'information, la plateforme « Jecliqueoupas », un service d'analyse de fichier 100% en ligne de l'ANSSI dédié aux agents de l'État, a été développée. Ce service permet d'obtenir un diagnostic simple sur le caractère malveillant de tout type de fichier.

Le service *Jecliqueoupas* est un service en ligne optionnel qui s'ajoute aux outils que les agents peuvent déjà avoir en place dans leurs ministères respectifs. Le marché a été attribué à la société Glimps, le 14 novembre 2022.

Le service a été ouvert aux ministères dans un premier temps puis progressivement aux établissements publics administratifs.

Une API[10] est actuellement en cours de développement (version en test avec les entités de beta.gouv.fr et intégration de France Transfert) pour une ouverture de service en 2025.

Afin de démocratiser son utilisation, le service a bénéficié de plusieurs soutiens promotionnels :

- Création d'un kit de communication ;
- Note interministérielle pour promouvoir JCOP par rapport à des solutions commerciales et impliquant la diffusion de fichiers professionnels sur Internet ;
- Citation du service dans le rapport « *État de la menace informatique des organismes de recherche et Think Tanks* »

Bilan du service

Le service a été ouvert à plus de 200 entités publiques et a fait émerger le besoin d'une version automatisée et systématique en plus de la version existante afin de sécuriser des applicatifs. Néanmoins, il a d'ores et déjà permis de détecter des campagnes malveillantes, démontrant son utilité.

3.1.2 « Typosquattage »

Le typosquattage est une technique malveillante consistant à créer des noms de domaine dont la graphie ou la phonétique est proche de celle d'un site très fréquenté ou d'une marque connue, afin que l'utilisateur faisant une faute d'orthographe ou une faute de frappe involontaire soit dirigé vers le site détenu par le pirate.

Dans le cadre du volet cybersécurité du plan France Relance, l'ANSSI a mis en place en janvier 2022 un service de lutte contre le cybersquattage des identités de l'État avec le soutien de la

[10] Application programming inteface, : interface qui connecte des logiciels, des services et des applications entre eux afin qu'ils puissent connecter leurs données

mission d'Appui au Patrimoine Immatériel de l'État (APIE) de la Direction des affaires juridiques du Ministère de l'Economie et des Finances.

Ce service repose sur un marché public confié à la société française Nameshield jusqu'à fin 2024. Il consiste en la surveillance des créations de noms de domaine reproduisant ou imitant de façon illégitime des signes identitaires de l'Etat. Le projet, dont le coût global avoisine les 900k€, sera repris en 2025 par l'APIE suite à un appel d'offre en cours de préparation.

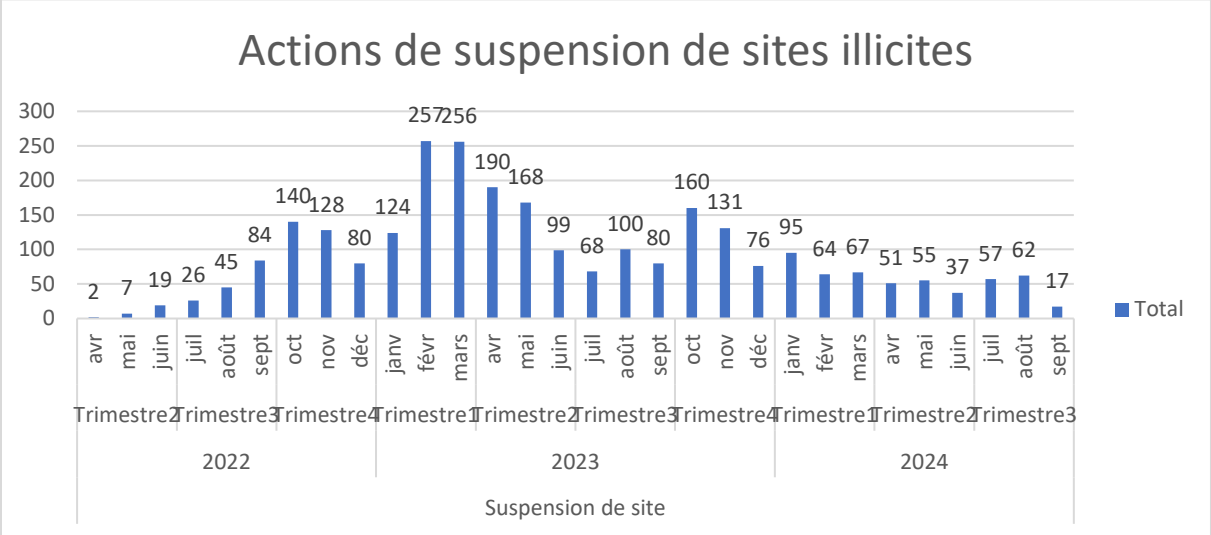
Finalité du service : Le service permet la surveillance sur Internet des créations de noms de domaine reproduisant ou imitant de façon illégitime des signes identitaires de l'Etat.

Bénéficiaires : La prestation n'est disponible que pour les ministères et ne couvre pas ses opérateurs (établissements publics sous tutelle notamment).

Contenu du service : Le prestataire effectue un premier tri des noms de domaine selon leur criticité. Sur cette base, la mission APIE étudie les réponses à apporter aux différentes catégories de menaces. Dans ce cadre, elle peut demander à Nameshield d'engager des démarches pour suspendre l'accès aux sites manifestement illicites. En complément, elle engage les procédures juridiques nécessaires pour demander la suppression ou le transfert de certains noms de domaine au profit de l'État, après accord de l'administration concernée.

Bilan du service

La supervision mise en œuvre en février 2022 a généré depuis avril de la même année environ 2800 actions de suspension de sites illicites (confer graphique), prouvant ainsi sa pertinence. Les sites en lien avec la manipulation de flux financiers sont les plus visés (impôts, amendes, aides sociales) et portent un risque de fraudes dès lors qu'ils sont associés à des services publics pour lesquels les utilisateurs renseignent des informations personnelles (notamment bancaires, carte vitale, France Connect).



Les chiffres présentés supra pourraient sembler modestes mais ils ne montrent pas le travail conséquent de filtrage et d'analyse de la mission APIE et de Nameshield. En effet plus de 37 000 noms de domaine ont été remontés par le système avant d'être classés en fonction de leur criticité (listes noire, grise et blanche), les actions de suspension de sites illicites correspondant à la liste noire des noms de domaine traités (confer annexe sur la base du bilan intermédiaire réalisé en 2023, un bilan complet est prévu fin 2024).

Le marché passé par l'ANSSI prévoyait à l'origine 250 actions de suspension de sites illicites sur les trois années du marché. Aujourd'hui, plus de 2800 actions ont été réalisées, impliquant des

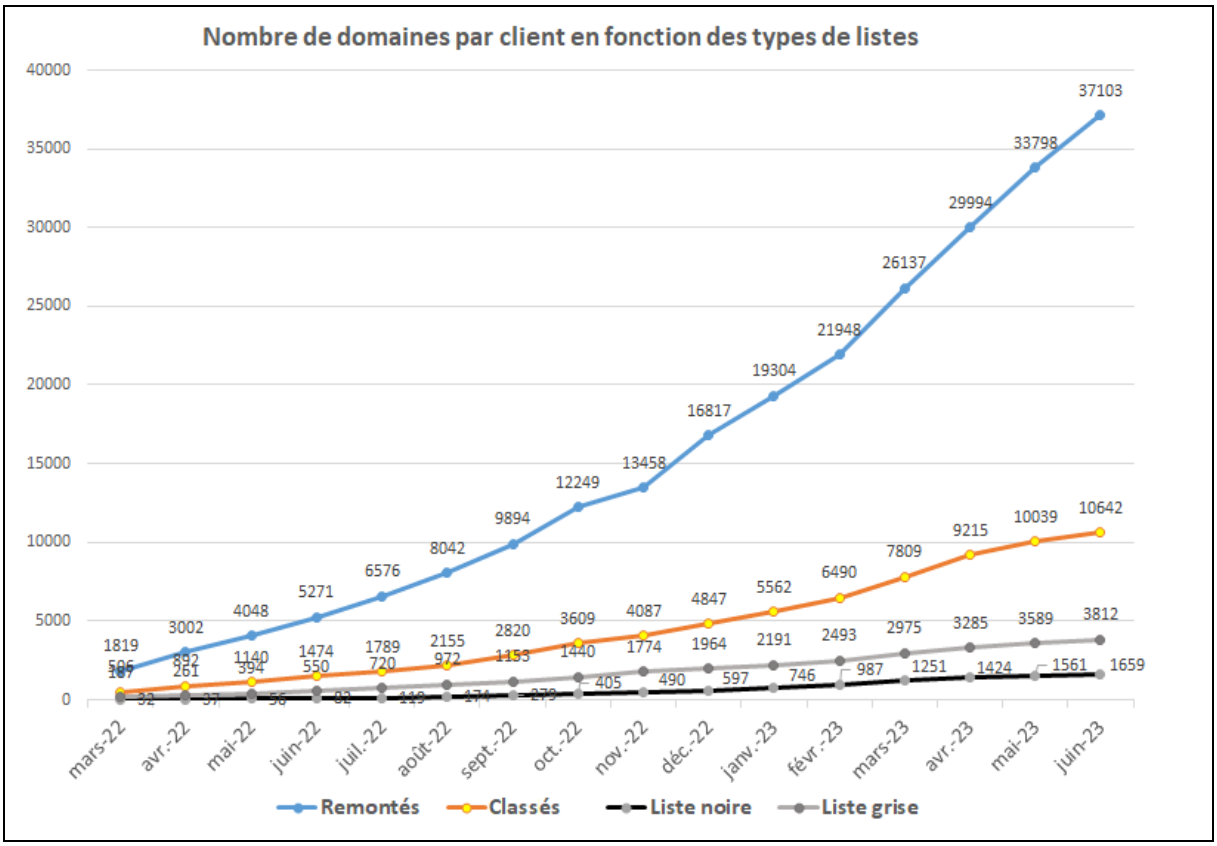
conséquences en matière de budget (les actions supplémentaires sont hors marché et pour l'instant assumées financièrement par l'ANSSI) et de charge de travail pour la mission APIE qui analyse la quasi-totalité des résultats des surveillances.

Suites à envisager

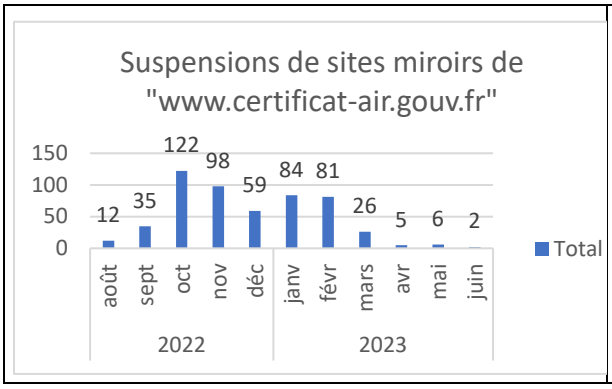
Ce dispositif a dépassé les objectifs initiaux. Pour autant, il n'est pas suffisant dans la mesure où il consiste à faire cesser les atteintes a posteriori , une fois qu'elles ont été constatées, sans que ces actions n'empêchent des acteurs malveillants de reprendre rapidement leurs activités malveillantes.

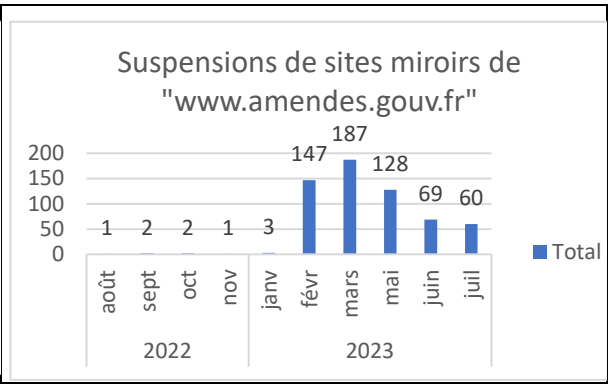
Pour augmenter son efficacité, ce dispositif doit s'accompagner d'un dépôt de plainte systématique afin que des poursuites judiciaires soient engagées pour agir contre les cybercriminels à l'origine des sites frauduleux.

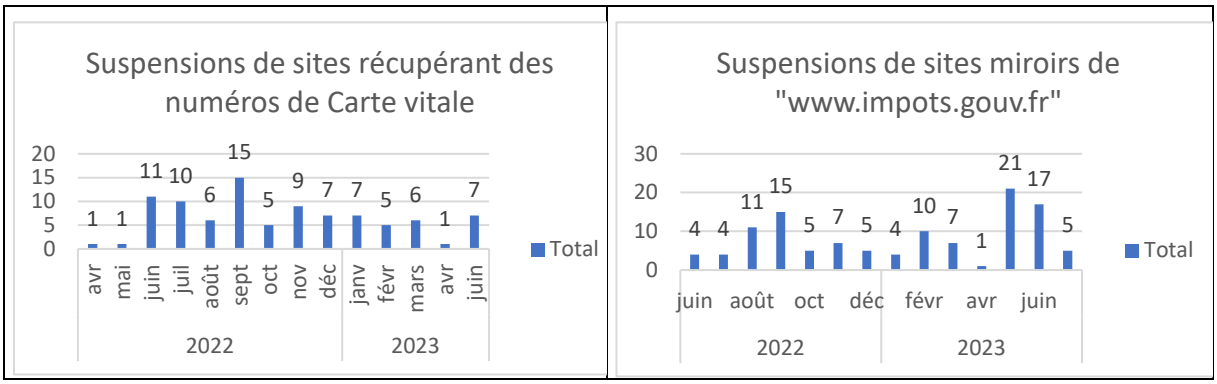
Statistiques du dispositif de typosquatting mis en place (bilan intermédiaire en 2023)



Source : Nameshield







3.2 Achat de produits et logiciels de sécurité pour répondre aux missions de l'ANSSI

L'ensemble de ces nouveaux services (« jecliqueoupas » et typosquattage) a nécessité de consolider l'infrastructure technique sous-jacente et entraîné l'acquisition d'équipements informatiques adaptés.

3.3 Appel à projets

L'objectif de l'appel à projet a été de renforcer de manière significative la sécurité des systèmes d'information de l'Etat et des services publics.

Les priorités ont été données aux acteurs publics offrant des services au profit direct des citoyens, à savoir :

- Les collectivités territoriales les plus importantes ;
- Le secteur de la santé, le social, la protection des citoyens et l'audiovisuel ;
- La sécurité de la Nation (protection du patrimoine scientifique et technique notamment).

Les critères d'appréciation d'un projet étaient :

- L'amélioration significative du niveau de cybersécurité (appréciée de manière qualitative ou quantitative), pour éviter par exemple des projets uniquement numériques sans apport de sécurité ;
- Le nombre d'agents ou de bénéficiaires concernés ;
- La maturité du projet, c'est-à-dire la possibilité, compte tenu du fait que cet appel à projet s'inscrivait dans le cadre du plan de relance, d'engager des crédits sur la période 2021-2022 ;
- Les solutions de cybersécurité envisagées, et les prestations de services associées pour leur déploiement et leur maintenance ;
- Le niveau de participation du bénéficiaire, sachant que les projets devaient être co-financés.

Pour se faire financer un projet, les porteurs devaient :

- Contacter leur référent ANSSI (coordinateur sectoriel ou territorial) ;
- Faire valider leur projet par leur chaine SSI (RSSI, FSSI) ;
- Déposer leur candidature.

Ensuite, le dossier était instruit par l'ANSSI. Pour ceux jugés pertinents au regard des différents critères d'appréciation supra, la décision de financement était validée lors d'un jury regroupant le directeur général de l'Agence ou son représentant, le porteur du projet, et le coordinateur sectoriel ou territorial concerné. Une demande de subvention et un projet de convention étaient ensuite établis.

4. Augmentation de la capacité nationale de détection des cyberattaques.

Trois projets ont été mis en œuvre pour mener à bien cet objectif d'augmenter la capacité nationale de détection des cyberattaques :

- Le déploiement de sondes logicielles de détection sur de nouveaux périmètres ministériels ;
- L'accroissement du déploiement de sondes auprès des ministères déjà équipés, en assurant la remontée de données de détection vers l'ANSSI ;
- Le blocage automatique des sites malveillants via le réseau interministériel de l'Etat (RIE)/

4.1 Le déploiement de sondes logicielles de détection

A l'automne 2021, l'ANSSI a initié à l'attention des ministères un projet d'accompagnement de déploiement d'une solution logicielle (*sonde*) de détection d'attaque informatique sur les postes de travail et les serveurs (*EDR – Endpoint Detection Response*). Ce projet, basé sur un engagement volontaire de chaque bénéficiaire, a été intégralement financé par l'Agence dans le cadre du PNRR.

En septembre 2022, la validation d'une preuve de concept avec la société Harfang Lab a été suivie d'une première commande de 160.000 licences pour 3 années, avec une prestation de support au déploiement chez les bénéficiaires.

Ce déploiement s'inscrit dans une stratégie de multiplication des sources de données du service de supervision opéré par l'Etat, de recherche de compromission et de cyberdéfense automatisée.

En outre, ce projet entre dans le volet de consolidation de la capacité de cybersécurité mutualisée pour l'Etat. L'enjeu est d'augmenter massivement la capacité de détection des ministères et organismes étatiques.

Lors de la phase de lancement, en mai 2021, une présentation du projet a été faite à l'ensemble des Fonctionnaires de sécurité des systèmes d'information (FSSI) des ministères afin de leur faire part des travaux en cours au sein de l'ANSSI et de lancer un appel à manifestation d'intérêt. A l'issue de cette phase de recensement, six bénéficiaires se sont déclarés volontaires : le ministère de la justice, trois entités du ministère de l'économie, des finances et de l'industrie (Direction générale du Trésor, services de l'environnement professionnel, direction générale des douanes et des droits indirects), la Cour des Comptes et le Conseil d'Etat.

Une augmentation du périmètre couvert a entrainé l'acquisition de nouvelles licences. In fine le nombre de bénéficiaires de la prestation de sécurisation de leur parc informatique s'élève à 12 :

Bénéficiaire	**Début**	**Fin**
Cour des comptes	01/07/2022	01/07/2025
Conseil d'Etat	31/12/2022	31/12/2025
Ministère de la Justice	01/10/2022	01/01/2026
Douanes (DGDDI)	22/09/2022	28/09/2025
Direction générale du Trésor	31/12/2023	31/12/2026
Bercy/SNUM	2022	2025 *(à affiner)*

Gendarmerie (STIC)	01/07/2022	01/07/2025
DSAF	30/04/2023	30/04/2026
DILA	30/04/2023	30/04/2026
OSIIC	31/03/2023	30/04/2026
CISIRH	31/03/2023	31/03/2026
Ministère de la Culture	31/12/2022	31/12/2025

Le suivi de projet est assuré par :

- cinq comités de pilotage des déploiements par an depuis janvier 2022. Ces comités de pilotage permettent un suivi de projet de proximité et l'éventuel arbitrage sur des points d'attention. Le dernier date de juillet 2024 ;
- un point de synchronisation mensuel entre Harfang Lab et les bénéficiaires centré autour d'un rappel des objectifs initiaux, du calendrier et d'une synthèse des activités.

Bilan / fin de projet

Le projet arrivant à échéance d'ici un an, fin 2025, un courrier a été adressé aux bénéficiaires en septembre 2024 afin de leur rappeler l'expiration du financement par l'Agence des licences et la nécessité d'effectuer un renouvellement sur leurs fonds propres. Un point de vigilance réside dans le fait que certaines administrations pourraient se trouver dans l'impossibilité d'incorporer cette dépense à leur budget au vu du contexte budgétaire actuel.

Ce projet constitue un vrai succès pour le développement d'Harfang Lab et l'entreprise a pu étendre ses parts de marché à l'export auprès d'entités gouvernementales européennes.

4.2 Accroissement du déploiement de sondes matérielles auprès des ministères

L'ANSSI a également poursuivi le déploiement de sondes matérielles de supervision de la sécurité des systèmes d'information au sein des différents ministères (sondes) et a acheté des serveurs permettant la collecte, l'analyse et le partage à l'interministériel des données produites (journaux techniques) pour accroitre sa capacité de détections d'attaques informatiques.

4.3 Blocage des sites malveillants via le RIE

L'ANSSI a également développé, avec la direction interministérielle du numérique (*DINUM*), des fonctions de cyberdéfense automatisée sur le réseau interministériel de l'État (*RIE*) en bloquant l'accès à des sites malveillants.

L'ANSSI adresse un rapport chaque mois aux bénéficiaires du service de détection des blocages réalisés.

Ce service a été adopté par 18 bénéficiaires (*AIFE, Agriculture, CEREMA, Conseil d'Etat, Cour des Comptes, DGCCRF, DILA, DGFIP, DINUM, Elysée, Finances, IGN, INSEE, Justice, MTE, SGDSN, Santé/Travail/Sport, Sénat*).

Cette capacité de supervision comprend plus de 100 000 marqueurs de sites malveillants désormais accessibles pour les agents de ces bénéficiaires.