

DÉLIBÉRATION N°CP 2022-123

DU 23 MARS 2022

FILIÈRE CYBER SÉCURITÉ

La commission permanente du conseil régional d'Île-de-France,

VU le Traité instituant la Communauté européenne et notamment ses articles 107 et 108 ;

VU le code général des collectivités territoriales ;

VU le code de la commande publique ;

VU le code de commerce ;

VU la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République ;

VU la délibération n° CR 230-16 du 14 décembre 2016 relative à l'adoption du Schéma régional de développement économique, d'innovation et d'internationalisation 2017-2021 ;

VU la délibération n° CR 2017-37 du 10 mars 2017 relative à mise en œuvre de la stratégie #Leader pour la croissance, l'emploi et l'innovation (SRDEII) ;

VU le budget de la région Île-de-France pour 2022 ;

VU l'avis de la commission du développement économique et de l'innovation ;

VU l'avis de la commission des finances et des fonds européens ;

VU le rapport n°CP 2022-123 présenté par madame la présidente du conseil régional d'Île-de-France ;

Après en avoir délibéré,

Article 1 : Création de CERT régional (Computer Emergency Response Team)

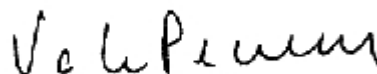
Approuve la convention de partenariat avec l'ANSSI telle que présentée en annexe à la présente délibération et autorise la présidente du conseil régional à la signer.

Article 2 : Action de sensibilisation des collectivités territoriales en IDF

Affecte une autorisation d'engagement de 48 000 € afin de mener une action de sensibilisation cyber auprès des collectivités territoriales en IDF.

Cette autorisation sera prélevée sur le chapitre 939, « Action économique », code fonctionnel 92 « Recherche et innovation », programme HP 92-002 (192002) « Soutien à l'innovation », action 19200207 « Evaluation, études et promotion », du budget 2022.

**La présidente du conseil régional
d'Île-de-France**



VALÉRIE PÉCRESSE

Acte rendu exécutoire le 23 mars 2022, depuis réception en préfecture de la région Île-de-France le 23 mars 2022
(référence technique : 075-237500079-20220323-lmc1144987-DE-1-1) et affichage ou notification le 23 mars 2022.

Dans les deux mois à compter de sa publication ou de sa notification, cet acte administratif est susceptible de recours
devant le tribunal administratif territorialement compétent.

ANNEXE A LA DELIBERATION

Convention CSIRT Ile-de-France



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Plan France Relance

CRÉATION DE CSIRT RÉGIONAL Convention de subvention n°

Entre

L'attributaire de la subvention, représenté par :

Le Secrétariat général de la défense et de la sécurité nationale

Sigle	:	SGDSN
Adresse	:	51, boulevard de La Tour-Maubourg – 75700 PARIS 07 SP
N° SIRET	:	120 001 029 00012
Code APE	:	8411Z
N° TVA intracommunautaire	:	FR 15 120 001 029
Représenté par	:	le chef du service de l'administration générale
Ci-après dénommé	:	le SGDSN

Et

Le bénéficiaire de la subvention, représenté par :

Nom du bénéficiaire

Sigle	:
Adresse	:
N° SIRET	:
Code APE	:
Représenté(e) par	:
Ci-après dénommé	:

Préambule

Dans le cadre du plan France relance, le SGDSN, et en son sein l'ANSSI, est attributaire de crédits avec pour objectif d'accélérer la sécurisation des systèmes numériques de l'État et des territoires face aux risques numériques.

Outre l'ambition d'élever substantiellement le niveau de sécurité numérique de l'État et des services publics, le volet cybersécurité du plan de relance vise à donner l'impulsion nécessaire à l'investissement durable des bénéficiaires dans la sécurisation de leurs systèmes d'information et de permettre au tissu industriel français de cybersécurité de se structurer et de se développer de manière significative.

Dans ce cadre, Computer Security Incident Response Team (CSIRT ou CERT) régionaux apporte une solution adaptée face à l'accroissement de la cybermenace dans les territoires. Elle doit permettre d'atteindre un objectif de traitement des incidents de cybersécurité intervenant chez les acteurs de taille intermédiaire (PME, ETI, collectivités territoriales, ds publics locaux et associations) implantés sur le territoire régional de façon progressive et mesurable.

Considérant le projet de création de CSIRT régional, fourni en pièce jointe,

Considérant les critères relatifs à ce type de projet listés en annexe 1 que le bénéficiaire s'engage à respecter,

Il est convenu ce qui suit :

Article 1 - Objet de la convention

Par la présente convention, le bénéficiaire de la présente convention - la Région Ile-de-France - s'engage à son initiative et sous sa responsabilité à soutenir la création d'un CSIRT régional respectant les critères définis en annexe 1 pour laquelle une subvention lui est attribuée.

Le SGDSN contribue financièrement à la mise en œuvre de ce projet sans attendre de contrepartie directe de cette subvention.

Article 2 - Durée de la convention

La convention est conclue au titre de l'année 2022 pour une durée de trois (3) ans.

Article 3 - Montant de la subvention

Le SGDSN contribue financièrement pour un montant maximal d'un million d'euros (1 000 000 €).

Cette subvention n'est acquise que sous réserve du respect par le bénéficiaire des obligations mentionnées aux articles 1, 5 et 6 de la présente convention et des décisions du SGDSN prises en application des articles 7 et 8 de la présente convention sans préjudice de l'application de l'article 10 de la présente convention.

Le financement public n'excède pas les coûts liés à la création du CSIRT et à la mise en œuvre des services listés en annexe 1. Les dépenses éligibles sur l'ensemble de l'exécution de la convention comprennent tous les coûts occasionnés par la mise en œuvre du projet, conformément au dossier de demande de subvention présenté par le bénéficiaire.

Article 4 - Modalités de versement de la subvention

Le SGDSN verse un million d'euros (1 000 000 €) à la notification de la convention.

La subvention est imputée sur les crédits du programme 363 « Compétitivité », action 04, sur le code activité 36304100002 « Accroissement de la couverture territoriale ».

La contribution financière est versée sur le compte du bénéficiaire selon les procédures comptables en vigueur.

Les versements seront effectués au compte ouvert au nom de - La Région Ile-de-France :

IBAN :

BIC-ADRESSE SWIFT :

L'ordonnateur de la dépense est le Secrétaire général de la défense et de la sécurité nationale.

Le comptable assignataire est le contrôleur budgétaire et comptable ministériel auprès des services du Premier ministre.

Article 5 - Justificatifs

Le bénéficiaire s'engage à fournir dans les six mois de chaque exercice budgétaire, les documents ci-après :

- un **compte rendu financier** qui atteste de la conformité des dépenses effectuées à l'objet de la subvention prévue dans la présente convention. Il est accompagné d'un compte rendu quantitatif et qualitatif du projet comprenant les éléments mentionnés à l'annexe 2 ;
- un **rapport d'activité**.

L'ANSSI procède, conjointement avec le bénéficiaire, à l'évaluation des conditions de réalisation du projet auquel elle a apporté son concours sur un plan quantitatif comme qualitatif.

Le SGDSN contrôle à l'issue de la convention que la contribution financière n'excède pas le coût de la mise en œuvre du projet. Conformément à l'article 43-IV de la loi n° 96-314 du 12 avril 1996 portant diverses dispositions d'ordre économique et financier, le SGDSN peut exiger le remboursement de la partie de la subvention supérieure aux coûts éligibles du projet.

Article 6 - Autres engagements

En cas d'inexécution, de modification substantielle ou de retard dans la mise en œuvre de la présente convention, le bénéficiaire informe le SGDSN sans délai par lettre recommandée avec accusé de réception.

Article 7 - Respect des obligations du bénéficiaire

En cas d'inexécution ou de modification substantielle, et en cas de retard significatif des conditions d'exécution de la convention par le bénéficiaire sans l'accord écrit de l'ANSSI, le SGDSN peut ordonner le reversement de tout ou partie des sommes déjà versées au titre de la présente convention, après examen des justificatifs présentés par le bénéficiaire.

Tout refus de communication ou toute communication tardive du compte rendu financier mentionné à l'article 5 entraîne la suppression de la subvention en application de l'article 112 de la loi n°45-0195 du 31 décembre 1945. Tout refus de communication des comptes entraîne également la suppression de la subvention conformément à l'article 14 du décret-loi du 2 mai 1938.

Article 8 - Contrôle du SGDSN et de l'ANSSI

Le suivi technique de la convention est assuré respectivement :

Pour l'ANSSI :

Service/coordonnées

Pour le bénéficiaire : XXXXXXXX

Service/coordonnées : XXXXXXXX

Le suivi technique de la convention s'effectuera notamment au travers de compte-rendu de l'avancée du projet qui sera transmis pour validation, a minima une fois par an.

Le bénéficiaire s'engage à fournir au terme de la convention, un bilan d'ensemble, qualitatif et quantitatif, de la mise en œuvre du projet.

L'ANSSI procède, conjointement avec le bénéficiaire, à l'évaluation des conditions de réalisation du projet auquel elle a apporté son concours.

Le SGDSN contrôle à l'issue de la convention que la contribution financière n'excède pas le coût de la mise en œuvre du projet. Conformément à l'article 43-IV de la loi n° 96-314 du 12 avril 1996 portant diverses dispositions d'ordre économique et financier, le SGDSN peut exiger le remboursement de la partie de la subvention supérieure aux coûts éligibles du projet.

Article 9 - Renouvellement – option évaluation

La conclusion éventuelle d'une nouvelle convention est subordonnée à la production des justificatifs et aux contrôles mentionnés à l'article 5 et à la réalisation d'une évaluation contradictoire avec le bénéficiaire des conditions de réalisation de la convention.

Article 10 - Avenant

La présente convention ne peut être modifiée que par avenant signé par le SGDSN et le bénéficiaire. La demande de modification de la présente convention est réalisée en la forme d'une lettre recommandée avec accusé de réception précisant l'objet de la modification, sa cause et toutes les conséquences qu'elle emporte. Dans un délai de deux mois suivant l'envoi de cette demande, l'autre partie peut y faire droit par lettre.

Article 11 - Résiliation de la convention

En cas de non-respect par l'une des parties de l'une de ses obligations résultant de la présente convention, celle-ci pourra être résiliée de plein droit par l'autre partie, sans préjudice des droits qu'elle pourrait faire valoir, à l'expiration d'un délai de deux mois suivant l'envoi d'une lettre recommandée avec accusé de réception valant mise en demeure de se conformer aux obligations contractuelles et restée infructueuse.

Article 12 - Recours

Tout litige résultant de l'exécution de la présente convention est du ressort du tribunal administratif de Paris.

Fait en deux exemplaires,

Pour le bénéficiaire
À Saint-Ouen, le

Pour le SGDSN
À Paris, le

Le chef du service de
l'administration générale

ANNEXE I – ENGAGEMENTS DU BÉNÉFICIAIRE

Soutien du Conseil régional :

Le bénéficiaire s'engage à conférer au CSIRT régional l'autorité nécessaire à l'accomplissement de sa mission et à promouvoir son action auprès de l'ensemble des acteurs de son territoire.

Par ailleurs, il s'engage à assurer la pérennité notamment juridique et financière du CSIRT régional et la continuité de son activité au-delà de la période de (3) ans couverte par la présente convention.

Enfin, il s'engage à veiller à ce que le CSIRT régional respecte le plan de financement prévisionnel ci-joint (cf. annexe 2, p.15-16)

Bénéficiaires et périmètre couvert :

Le bénéficiaire s'engage à veiller à ce que le CSIRT régional fournisse les services minimums, décrits ci-dessous au paragraphe 4, à l'ensemble des bénéficiaires de taille intermédiaire (listés dans les catégories ci-après) présents sur le territoire de la région au terme de sa troisième année d'existence :

- PME ;
- ETI ;
- collectivités territoriales et établissements publics associés ;
- associations nationales.

À ce titre, le bénéficiaire s'engage à valider et à veiller à ce que le CSIRT régional respecte dans son fonctionnement opérationnel la procédure de priorisation des demandes d'assistance qui sera définie avec l'ANSSI au cours du programme d'incubation.

Ressources humaines :

Le bénéficiaire s'engage à veiller à ce que le CSIRT régional respecte le schéma directeur RH prévisionnel ci-joint (cf. annexe 2, p.12)

Services minimums :

Le bénéficiaire s'engage à veiller à ce que le CSIRT régional propose de manière gratuite comme activités d'intérêt général à ses bénéficiaires les services suivants en jours ouvrés :

- Mise en œuvre d'une plateforme téléphonique et des moyens informatiques nécessaires à la réception des incidents informatiques ;
- Qualification et triage des incidents ;
- Suivi des incidents ;
- Mise en relation avec des prestataires labellisés **Expert_Cyber** ou qualifiés par l'ANSSI (par exemple, prestataires qualifiés d'audit de la sécurité des systèmes d'information ou de réponse aux incidents de sécurité) ;
- Information et conseil relatifs aux poursuites juridictionnelles ;
- Référencement des prestataires locaux labellisés et qualifiés en cohérence avec l'ANSSI et [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) ;
- Relais et transfert des informations pertinentes vers le CERT-FR, [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), les autres CSIRT (en particulier les autres CSIRT régionaux) et l'InterCERT-FR ;
- Consolidation de l'incidentologie régionale et partage du résultat avec le CERT-FR.

Gouvernance de la structure :

Le bénéficiaire s'engage à veiller au respect du schéma de gouvernance du CSIRT régional ci-joint (cf. annexe 2, p.13)

Comptabilité de la structure :

Le bénéficiaire s'engage à veiller à ce que le CSIRT régional dispose d'une comptabilité autonome, identifiant très clairement les éléments de bilan, de compte de résultat et de flux financiers associés au projet CSIRT et permettant l'identification de tout autre dispositif d'accompagnement public national ou européen pour le projet de CSIRT en précisant les coûts couverts.

Par ailleurs, le bénéficiaire s'engage à veiller à ce que le CSIRT régional respecte l'obligation de transparence et de *reporting* vis-à-vis de l'État, nécessaire à l'évaluation ex-post du projet et de son financement.

Programme d'incubation de l'ANSSI et intégration de l'InterCERT-FR :

Le bénéficiaire s'engage à veiller à ce que la personne en charge de la création du CSIRT régional et de son pilotage suive le programme d'incubation mis en place par l'ANSSI pour accompagner la création des CSIRT régionaux.

Il s'engage également à veiller à ce que le CSIRT régional rejoigne l'InterCERT-FR à l'issue du programme d'incubation, et plus particulièrement la communauté qui sera spécifiquement créée pour les CSIRT régionaux.

ANNEXE II – DOCUMENTS À JOINDRE À LA PRÉSENTE CONVENTION

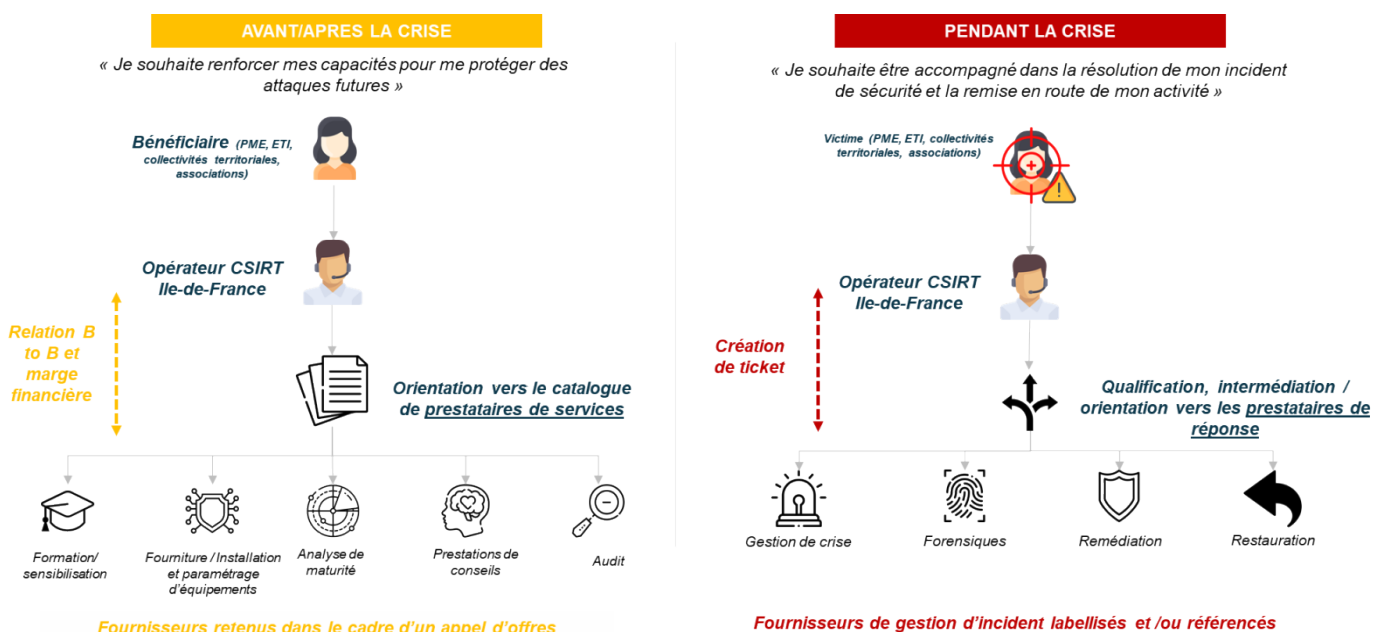
- Les statuts juridiques de la structure de rattachement du CSIRT régional ;
- Le schéma de gouvernance du CSIRT régional ;
- Le plan RH prévisionnel du CSIRT régional sur ses 3 premières années de fonctionnement ;
- Le budget et plan de financement prévisionnel du CSIRT régional sur ses 3 premières années de fonctionnement.

Le CSIRT Ile-de-France

Présentation générale

Le futur CSIRT Ile-de-France se veut être le point de contact privilégié des acteurs territoriaux dans le domaine de la sécurité. A ce titre, il interviendra comme intermédiaire en complément du CERT-FR (national), du ComCyberGend ou encore de la plateforme de déclaration d'incident [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr).

Figure 1 : un CSIRT positionné à chaque moment de la crise pour couvrir l'ensemble des besoins et jouer un rôle d'intermédiation entre les bénéficiaires et les fournisseurs de service et partenaires régionaux publics et privés



NB : Les services proposés sur la partie droite du schéma, correspondent à l'offre de « services socles », mis en œuvre dans le cadre de la convention dès la première année de fonctionnement du CSIRT Régional tandis que les services détaillés sur la partie gauche du schéma interviendront dans un second temps, sous réserve des analyses à approfondir en phase de préfiguration et à l'initiative de la gouvernance du CSIRT.

Le CSIRT Ile-de-France devra agir en collaboration étroite avec les initiatives locales déjà présentes dans le paysage cyber francilien. On peut dans ce contexte citer Campus Cyber, le Hub Cyber Systematic et Seine et Yvelines Numérique.

La conception, la précision du modèle et le déploiement du CSIRT Ile-de-France seront précisés au travers d'une démarche de préfiguration, qui bénéficiera du programme d'incubation de l'ANSSI :

- **Une phase de préfiguration** dont le rôle est d'affiner les éléments relatifs à l'ensemble de la stratégie du CERT : du modèle de fonctionnement, à la structure juridique, au modèle économique et financier

ainsi qu'à la gouvernance.

- **Un programme d'incubation** d'une durée de 4 mois – proposée par l'ANSSI - dont l'objectif est de permettre aux équipes chargées de créer les CSIRT régionaux de concevoir leurs référentiels documentaires, leurs procédures opérationnelles et d'appréhender les outils propres aux activités de CSIRT : programme cible de la région Ile de France, au 2ème semestre 2022.

La préfiguration permettra donc de détailler les points suivants :

- Définition des modalités de collaboration avec les partenaires et de la gouvernance globale du dispositif
- Déclaration de mission et de la raison d'être
- Définition de la feuille de route juridique
- Définition de la feuille de route visant au référencement de la base d'entreprises fournisseuses de services/solutions
- Définition de l'écosystème de prestataires de réponses, précision des modalités de sollicitation tant contractuelles qu'en fonction du niveau de criticité de l'incident
- Affinement des hypothèses de dimensionnement RH, définition et mise en œuvre du plan RH (préparation des fiches de poste, campagnes de recrutement, tests d'aptitudes)
- Stabilisation des offres complémentaires à offrir en synergie avec l'écosystème cyber francilien
- Définition du modèle économique
- Evaluation détaillée (postes de dépenses et postes de recettes) et définition du planning de révision du Business Plan.

Dès lors que la candidature de la Région Ile-de-France sera retenue, l'intégration au programme d'incubation proposé par l'ANSSI et la préfiguration pilotée par le préfigurateur, en lien avec les parties prenantes, permettra de préciser les autres points suivants :

- Identification du phasage de déploiement du CSIRT (pilote et phase d'extension régionale) et planning
- Définition des phases de test (vérification d'aptitude et vérification de service régulier)
- Identification et mobilisation des partenaires qui seront associés à chacune des phases
- Mise en œuvre juridique de la structure du CSIRT (déclaration de statut auprès des autorités compétentes)
- Accompagnement à la mise en œuvre opérationnelle (sélection des outils, de l'architecture IT, définition des procédures sur la base des référentiels RFC 2350 et SIM3)
- Sélection et aménagement des locaux
- Identification des trajectoires possibles pour le CSIRT à partir de 2024 et définition de la feuille de route à long terme.

Un bouquet d'offres de services étoffé pour répondre à l'ensemble des besoins des bénéficiaires franciliens

Le CSIRT Ile-de-France sera chargé de répondre aux incidents de sécurité, par l'apport d'un support aux organismes touchés par une cyberattaque, l'orientation vers des interlocuteurs qualifiés pour prendre en charge la remédiation et la réponse à l'incident ainsi que le suivi de la résolution de l'incident.

Les prestations envisagées dans le cadre du CSIRT Régional d'Ile-de-France doivent permettre dans un premier temps de fournir des services d'urgence gratuits pour les acteurs des territoires couverts par le périmètre d'action du CSIRT. Ces services minimums sont qualifiés comme « services socles » dans la suite du document.

Dans un second temps, des prestations additionnelles, appelées ici « services complémentaires », pourraient permettre au CSIRT de diversifier ses ressources financières, au-delà des subventions publiques.

Il est également important de réfléchir aux prestations d'accompagnement à apporter en fonction des étapes de la crise cyber. Ainsi nous distinguerons les offres d'accompagnement à vocation d'anticipation (pré-crise), de réaction (durant la crise) et de suivi/renforcement (post-crise).

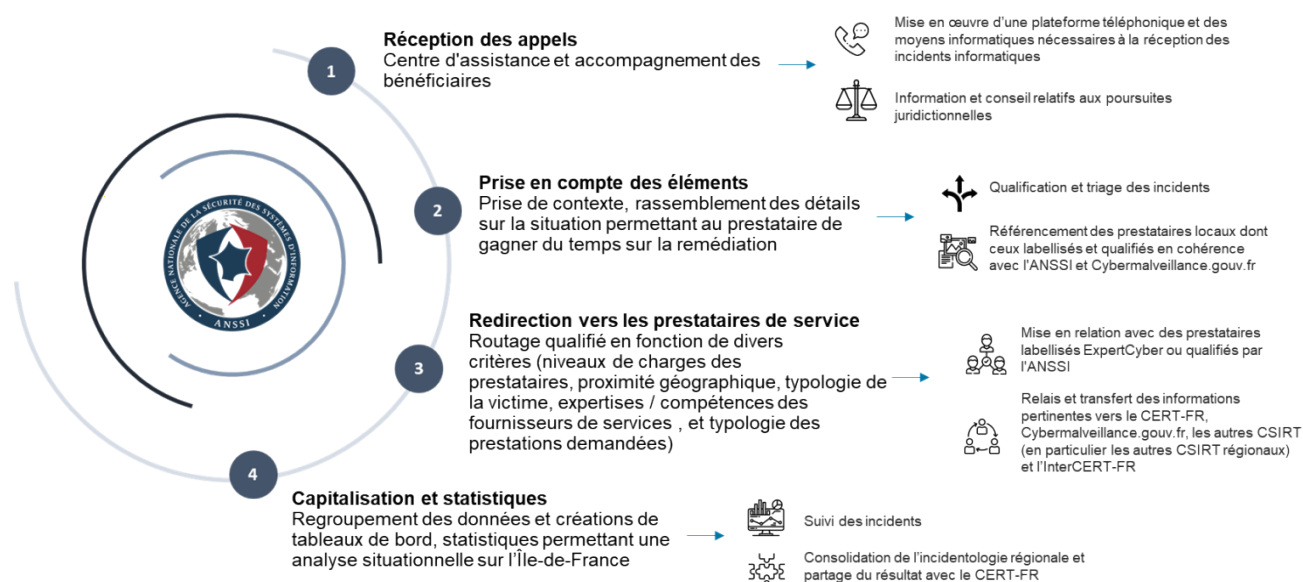
Des services socles portés gratuitement par le CSIRT, au titre de l'intérêt général

Les services socles du CSIRT exigés par l'ANSSI et offerts au titre de l'intérêt public comprendront donc :

- La mise en œuvre d'une plateforme téléphonique et des moyens informatiques nécessaires (helpdesk) à la réception des incidents informatiques.
- La qualification et triage des incidents sur la base de seuils de déclenchements qualitatifs et quantitatifs
- Le suivi des incidents et de leur prise en charge
- Le référencement des prestataires locaux labellisés et qualifiés en cohérence avec l'ANSSI et Cybermalveillance.gouv.fr

- La mise en relation avec des prestataires labellisés ou qualifiés (Expert Cyber, PRIS, PASSI) aptes à répondre au mieux à l'incident en fonction de sa nature et de la victime
- La centralisation et la capitalisation sur les incidents de sécurité sur le périmètre couvert (incidentologie régionale)
- Le conseil et la communication d'informations relativement aux poursuites judiciaires à engager par les victimes
- Le relais et transferts des informations pertinentes vers le CERT-FR, Cybermalveillance.gouv.fr, les autres CSIRT et l'interCERT-FR.

Figure 2 : des services minimums d'intérêt général à fournir de manière gratuite à l'ensemble des bénéficiaires privés de taille intermédiaire, des associations et des collectivités territoriales et établissements publics locaux présents sur le territoire francilien



Des offres complémentaires à proposer pour couvrir les besoins et apporter des sources de revenus complémentaires aux différentes subventions

Dans l'objectif de dégager des pistes de financement complémentaires aux subventions versées, différentes offres complémentaires, répondant aux besoins de la cible, ont été identifiées.

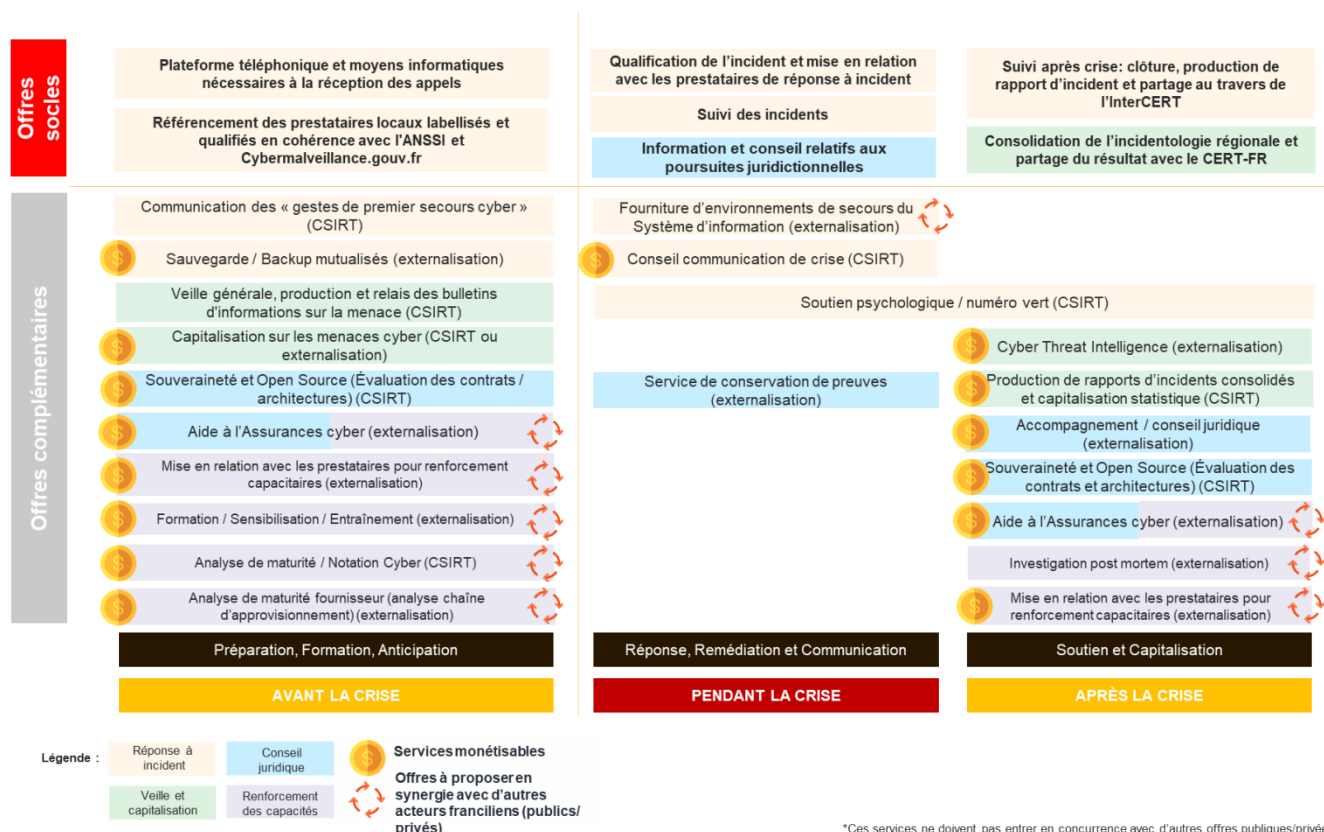
Ces offres peuvent être proposées via le CSIRT lui-même ou via un catalogue de services de prestataires partenaires (avec les contraintes juridiques associées). Ces offres seront proposées en adéquation et en coordination avec l'écosystème des initiatives cyber déjà en place en Ile-de-France, afin d'offrir une offre complémentaire et dans une perspective de collaboration, et de non-concurrence avec les acteurs privés.

A ce titre, nous pouvons citer les pistes d'offres complémentaires suivantes :

- Fourniture d'environnements de secours du Système d'information
- Sauvegarde / Back Up mutualisés
- Service de conservation de preuves
- Accompagnement à l'assurance cyber : revue des polices d'assurance, évaluation du niveau de protection et de conformité en amont de la contractualisation
- Mise en relation avec des prestataires pour renforcement capacitaire
- Accompagnement à la configuration et à la maintenance des équipements de sécurité
- Analyse des risques et évaluation globale de posture/maturité de sécurité
- Analyse de maturité cyber des fournisseurs : analyse de la chaîne d'approvisionnement
- Souveraineté et Open Source : Évaluation des contrats, des licences contaminantes (copyleft) et des architectures
- Sensibilisation et formation de premier niveau à la cybersécurité pour divers publics
- Accompagnement à la communication de crise
- Soutien psychologique post-crise pour les victimes
- Cyber entraînement et exercice de crise

La cartographie des offres envisagées peut être détaillée comme suit :

Figure 3 : en synthèse, vue synoptique du bouquet de services « socle » et « complémentaires » envisagés



Cette segmentation reste à approfondir, affiner durant les phases de préfiguration et d'incubation.

Le statut juridique du CSIRT Ile-de-France

Le statut juridique de ces CSIRTs n'est pas imposé par l'ANSSI. Il appartient donc à chaque région de mettre en place la structure juridique adéquate permettant de soutenir ses offres, son modèle économique à terme, sa gouvernance ou encore les modalités d'adressage des prestataires et des bénéficiaires tout en garantissant une prise en compte des enjeux publics comme privés.

Le statut de l'association loi 1901 semblerait être a priori la forme juridique plus adaptée au lancement d'un CERT francilien sous réserve d'une analyse plus approfondie à venir.

Les besoins en ressources humaines

Pour accomplir ses missions, le CSIRT Ile-de-France doit pouvoir s'appuyer sur des ressources humaines spécifiquement déployées à ses fins. Ces ressources humaines doivent avoir un profil spécialisé et adapté à l'évolution de la structure et de la menace cyber en Ile-de-France.

Ainsi, ces ressources doivent être sélectionnées sur des compétences affirmées leur permettant de répondre aux missions de base d'un CSIRT et aux offres socles mentionnées dans le cadre de la présente convention de subvention tout en anticipant l'ouverture des offres complémentaires à horizon quatre ans.

Profils préemptés

L'équipe cœur du CSIRT Ile-de-France concentrera les profils (et missions) suivants :

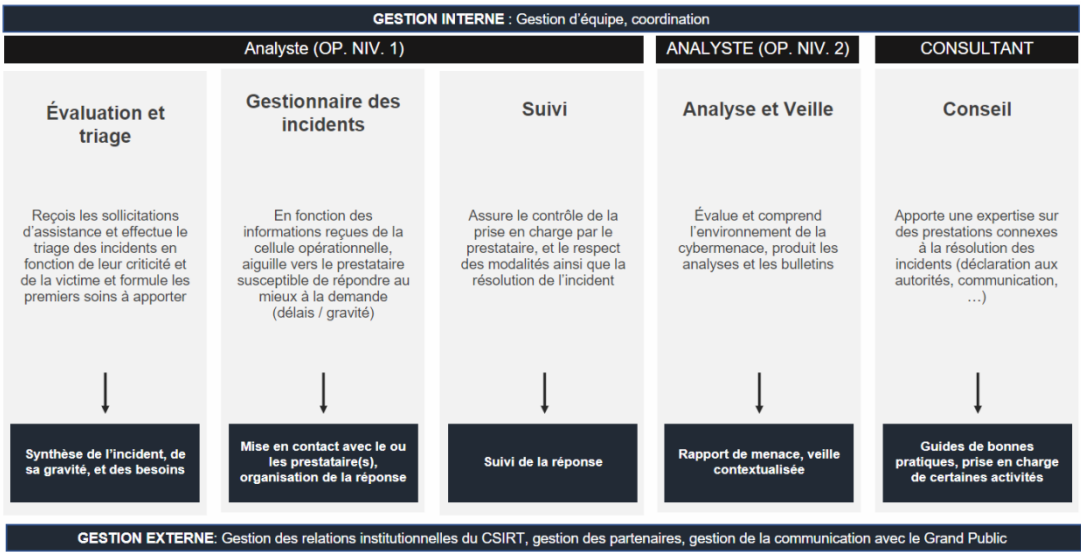
- **Responsable du CSIRT** : Responsable de la coordination et du bon fonctionnement du CSIRT régional, avec un rôle de représentation afin de faire connaître le CSIRT auprès des parties prenantes (partenaires, instances, autres CSIRTs, tissu des acteurs régionaux, pilotage du plan de communication).
- **Analyste CSIRT** : Collecte les informations relatives à l'incident, qualifie et transfère les incidents aux prestataires experts de la réponse en fonction de leur criticité, effectue la veille et transmet les mesures d'urgence de réponse, assure le suivi des incidents, la centralisation, la consolidation et la capitalisation de l'incidentologie.

Sous réserve de dégager des financements complémentaires :

- **Consultant juridique** : Transmet les informations et conseils relatifs aux poursuites juridictionnelles.
- **Consultant communication** : Prend en charge la communication vers les victimes et transmet les conseils en matière de stratégie de communication à adopter en interne et en externe.

Durant les 3 premières années de fonctionnement, le CSIRT sera alloué aux activités suivantes :

Figure 4 : principales activités du CSIRT Régional durant les 3 premières années

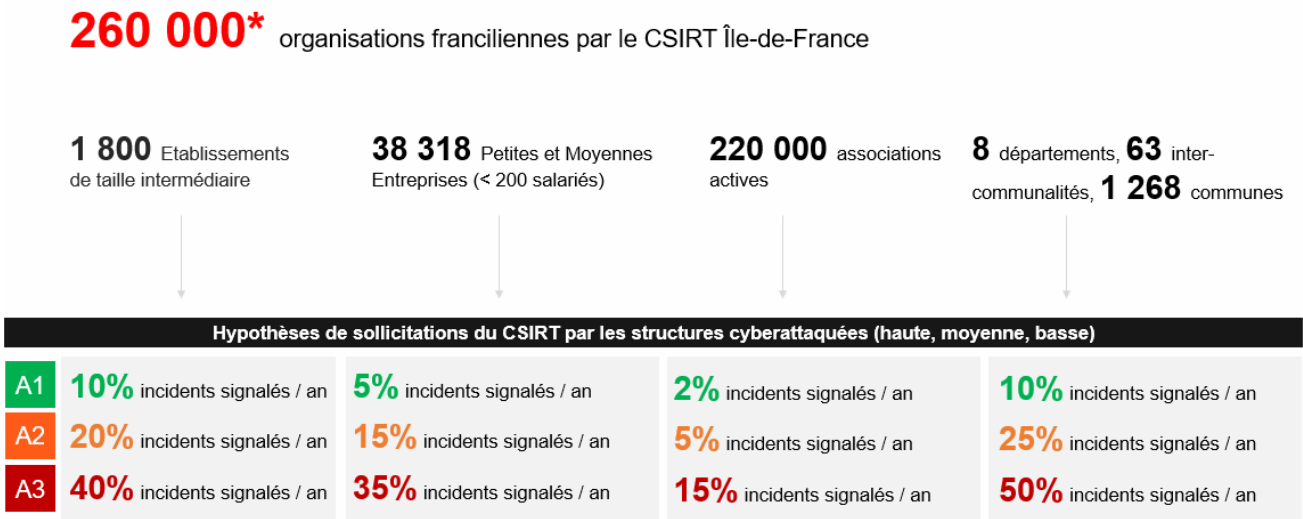


A ce titre, nous avons pu exprimer les besoins en ressources humaines sur les 3 premières années de vie du CSIRT Régional, en fonction de plusieurs facteurs de conjoncture prépondérants. Ces éléments sont listés dans la section ci-dessous.

Plan RH prévisionnel sur les 3 premières années

Sur la base de nos discussions et de la formulation de nos hypothèses, nous pouvons confronter deux modèles de calculs (l'un fondé sur les hypothèses de sollicitations des bénéficiaires et l'autre sur les capacités d'un analyste à traiter les sollicitations) et mettre en exergue leurs compatibilités afin de correctement dimensionner l'équipe de réponse à incident.

Figure 5 : analyse sur les besoins en RH fondée sur le périmètre des bénéficiaires à couvrir



Il est à noter que les hypothèses supportant notre simulation seront à préciser et détailler dans l'étude de préfiguration afin de correctement calibrer les besoins et planifier leur recrutement.

En confrontant ces modèles, nous constatons que le format à 3 analystes est suffisant pour assurer une prise en charge des sollicitations des bénéficiaires durant les premières phases de développement du CSIRT (Année 1). Compte tenu du contexte de menace cyber mentionné précédemment et de la communication qui sera faite autour du CSIRT pour engager progressivement les bénéficiaires, nous pouvons construire le modèle de montée en charge RH suivant sur les 3 premières années :

Tableau 1 : plan RH prévisionnel

Profil	Année 1	Année 2	Année 3
Responsable CSIRT	1	1	1
Analyste CSIRT	3	5	8
Consultant juridique	0	0	0
Consultant communication	0	0	0
Mode de fonctionnement	3 analystes en journée normale (8h-20h), uniquement les jours ouvrés	5 analystes en fonctionnement 3x8h en jour ouvré avec 2 analystes par créneaux horaires pour assurer la continuité de l'activité.	8 analystes en 24h/24 7j/7

Ce modèle viable économiquement avec le Business Plan présenté plus loin permettra de couvrir les « offres socle ».

Cadre opérationnel de gestion des incidents de sécurité

Implantation physique

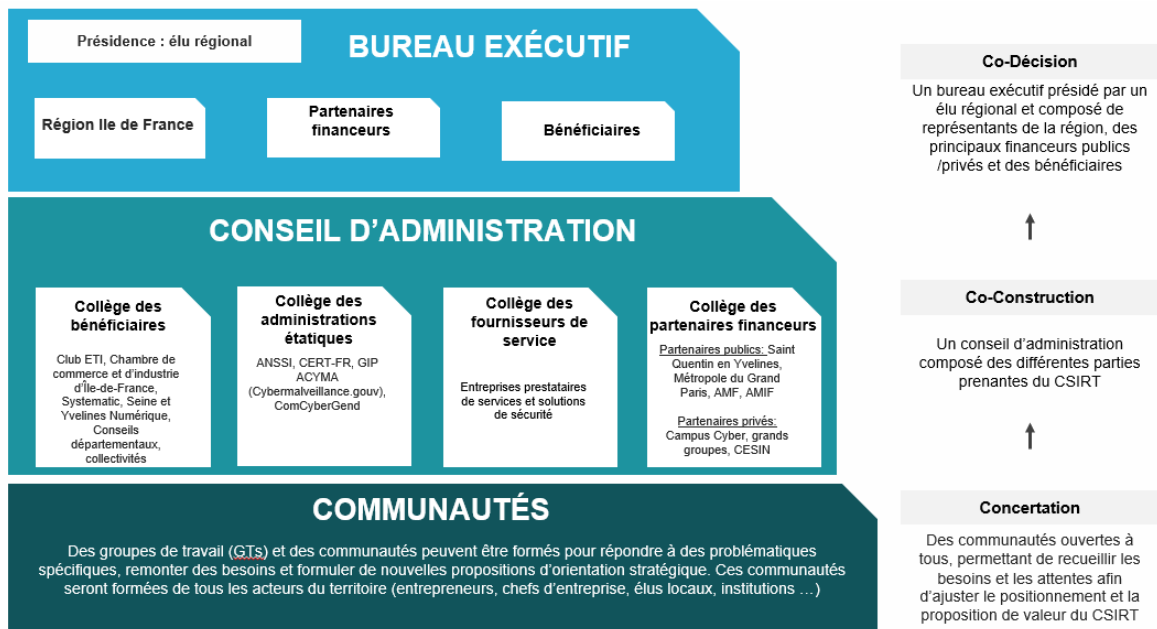
D'un point de vue logistique, l'implantation physique du CSIRT Ile-de-France sera située dans la ville de Saint Quentin en Yvelines. A ce titre, la communauté d'agglomération envisage de mettre en œuvre les mesures nécessaires (financière et opérationnelles) afin d'accueillir au mieux le CSIRT Régional.

Schéma de gouvernance et structure organisationnelle

Le CSIRT Régional mettra en œuvre une gouvernance impliquant l'ensemble des parties prenantes de l'écosystème cyber francilien. Cette gouvernance hybride entre le secteur public et le secteur privé avec une majorité publique au regard des missions d'intérêt général et cibles (collectivités locales notamment) identifiées. Là encore, cette gouvernance devra être précisée et validée durant la phase de préfiguration : des discussions avec les principales parties prenantes de l'écosystème francilien devront être tenues au plus vite pour en déterminer ses principaux acteurs.

Nous pouvons néanmoins d'ores et déjà esquisser une première organisation à la suite de notre étude et des échanges entre la région Ile-de-France, les acteurs franciliens de la cybersécurité, et en nous inspirant des structures mises en place dans les autres CSIRT :

Figure 6 : Proposition de schéma de gouvernance du CSIRT



Cette gouvernance comprend trois instances spécifiques :

- Une instance de décision (bureau exécutif)
- Une instance de construction (Conseil d'Administration)
- Une instance de concertation (communautés).

Cette gouvernance permettra une prise en compte des besoins et enjeux de chacun des types de contributeurs. Elle permet également la construction d'une structure prenant en compte les enjeux des secteurs privé et public.

Modèle économique

Pour rappel, le CSIRT Régional doit être autonome dans sa comptabilité et arriver à un modèle à l'équilibre à la fin des 3 premières années de fonctionnement. Cet équilibre entre recettes et dépenses est abordé ci-dessous et pourra être précisé durant la phase de préfiguration pour déterminer des seuils de rentabilité.

Modèle de coûts

Les deux principaux éléments qui devront être pris en compte dans le cadre des dépenses relatives au CSIRT sont :

- La fixation des heures de service en rythme de « croisière » (nominal et dégradé) – 7j/7, 24h/24, 365 jours par an à un niveau continu ou variable de qualité de service.
- Le nombre (et la qualité) des effectifs à affecter – dépendant du périmètre à couvrir et du nombre d'incidents à prendre en charge quotidiennement.

Comme indiqué précédemment, nous engageons une équipe composée d'un responsable CSIRT et de :

- 3 analystes la première année en journée normale (8h-20h), uniquement les jours ouvrés
- Puis 5 analystes en 2^{ème} année en fonctionnement 3x8h en jour ouvré avec 2 analystes par créneaux horaires pour assurer la continuité de l'activité
- Avant d'atteindre un rythme de « croisière » à 8 analystes en fonctionnement 24/7.

La phase de préfiguration nous permettra de préciser ce modèle de fonctionnement et notamment d'examiner de près avec les parties prenantes la nécessité réelle d'offrir des services 24 heures par jour et 7 jours par semaine.

Une fois les dépenses en ressources humaines quantifiées, il est nécessaire d'aborder les postes de dépenses en matériel : Automatisation, outils de gestion des tickets, Business Intelligence, outil d'informations sur les orientations juridictionnelles, locaux, infrastructure IT redondée, stockage sécurisé de la donnée. Enfin, il s'agit d'évaluer les dépenses en communication nécessaires pour faire connaître le CSIRT Ile-de-France à ses bénéficiaires potentiels.

Coûts de fonctionnement et coûts d'investissement

Les dépenses sont classées en 2 catégories : coûts de fonctionnement qui permettent au CSIRT d'exister et d'opérer ses missions, et coûts d'investissement regroupant les acquisitions de matériel et outils,

d'infrastructure, le paramétrage et le développement nécessaire au démarrage du CSIRT. Nous pouvons ainsi catégoriser les postes de dépense comme suit

Tableau 2 : principaux postes de coût de fonctionnement et d'investissement

Dépenses	TOTAL	Détails
Dépenses d'investissement à couvrir sur les 3 premières années		
Matériel informatique et outillage	250 000 €	Équipement informatique individuelle, écrans de contrôle, outils informatiques (BI, ticketing, licence E3)
Infrastructure IT (serveurs, réseau)	450 000 €	Système d'information, serveurs à disposition du CSIRT
Prestations externalisées	30 000 €	Pour les accompagnements juridiques plus approfondis (dépôt de plainte, relations CNIL, ...) à partir de la 3 ^{ème} année
Paramétrage et intégration	100 000 €	Développement web, intégration, paramétrage des outils et des interfaces, etc. Tendance à l'automatisation progressive
830 000 €		
Dépenses de fonctionnement annuelles en « régime de croisière » (à partir de l'année 3)		
Frais généraux	50 000 €	Bilan comptable, frais administratifs, imprévus
Maintien en Condition Opérationnelle	25 000 €	Maintenance des équipements, gestion des licences
Plan de communication	50 000 €	Communication envers les bénéficiaires pour faire connaître le CSIRT, ses modalités de contact et ses missions (coût moyen)
Locaux	35 000 €	A définir suivant les hypothèses de mise à disposition des locaux
Ressources Humaines	435 000 €	1 Resp. CERT 8 analystes pour couvrir la totalité des offres proposées
Frais de fonctionnement à couvrir via les offres complémentaires, par la Région, par les bénéficiaires, les partenaires et par les prestataires de services		
595 000 €		

Modèle de recettes

Pour équilibrer les dépenses, plusieurs pistes de recettes sont identifiées :

- Les subventions :
 - Subventions de la part des collectivités et de l'Etat
- Les Cotisations versées par divers acteurs régionaux :
 - Cotisations de la part des prestataires de services de sécurité (adhésion ou sponsoring)
 - Cotisation de la part des grands groupes qui peuvent tirer parti du CSIRT Régional pour bénéficier d'un état des lieux de la sécurité de leurs sous-traitants ou fournisseurs et être alertés en temps restreint d'une attaque sur ces derniers pour protéger leur infrastructure propre.
 - Cotisation de partenaires / acteurs majeurs de la Cyber pour un accès aux données d'incidentologie
- Pistes additionnelles :
 - Les services additionnels sous responsabilité du CSIRT et venant en complémentarité des services des prestataires (communication de crise, soutien psychologique, analyse de maturité des tiers...)
 - Marge sur les prestations de services des prestataires
 - Modèle Premium : aligné avec les modalités de priorisation ANSSI et en évitant de dénaturer l'égalité de traitement (dans ce cas, nécessite d'internaliser certaines offres complémentaires pour garantir la qualité de service)
 - Accès en ligne payant à des informations exclusives.
 - Production d'études et de rapports statistiques à la demande après retraitement des données d'incident

Ces pistes de recettes seront approfondies durant la phase de préfiguration.

En synthèse, plan de financement sur les 3 premières années de fonctionnement du CSIRT

Suivant les hypothèses de dimensionnement de l'équipe de réponse en année 1, 2 et 3 et en étudiant l'infrastructure et le matériel informatique pouvant être mis en œuvre dans le cadre du CSIRT, nous sommes

parvenus à construire un premier Business Plan à horizon 3 ans.

Ce Business Plan prend appui sur les deux subventions de l'ANSSI et de la Région Ile-de-France. Il est par ailleurs à noter que la subvention de la région Île-de-France sera à découpler en crédits de fonctionnement et crédits d'investissement.

Ainsi, à la suite de notre étude, nous pouvons conclure que le budget alloué répond bien aux exigences posées par l'ANSSI et aux niveaux de prise en charge pressentis par les bénéficiaires pour les 3 premières années de fonctionnement du CSIRT.

Ce plan sera à détailler en phase de préfiguration afin de consolider et préciser la totalité des postes de dépenses et de recettes.

Tableau 3 : plan de financement consolidé sur 3 ans

Année	Année 1	Année 2	Année 3	TOTAL
Dépenses	Dépenses			
Ressources Humaines	220 000 €	305 000 €	435 000 €	960 000 €
Locaux	35 000 €	35 000 €	35 000 €	105 000 €
Matériel informatique et outillage	150 000 €	50 000 €	50 000 €	250 000 €
Infrastructure IT (serveurs, réseau)	150 000 €	150 000 €	150 000 €	450 000 €
Paramétrage et intégration	50 000 €	20 000 €	30 000 €	100 000 €
Maintien en Condition Opérationnelle	25 000 €	25 000 €	25 000 €	75 000 €
Frais généraux	50 000 €	50 000 €	50 000 €	150 000 €
Plan de communication	80 000 €	40 000 €	30 000 €	150 000 €
Prestations externalisées	x	x	30 000 €	30 000 €
TOTAL				2 270 000 €
Recettes	Recettes			
Subvention ANSSI	1 000 000 €	x	x	1 000 000 €
Subvention Région Île-de-France	333 333 €	333 333 €	333 334 €	1 000 000 €

La subvention sollicitée de 1 000 000 €, objet de la présente demande représente44.... % du total des produits du projet (montant sollicité / total du budget) x 100

ATTESTATION

Je soussigné(e), (nom, prénom) : XXXXX

représentant(e) légal(e) de l'entité : Région Ile-de-France

déclare demander une subvention d'un montant de 1.000.000 €, au titre de l'année 2022, pour le projet détaillé ci-dessus.

Fait à, le

Signature